



## OpenText™ Directory Services

### **Installation and Administration Guide**

Configure and administer OpenText Directory Services, OTDS, to manage user and group identity information for OpenText components.

OTDS250400-IWC-EN-01

---

**OpenText™ Directory Services  
Installation and Administration Guide**  
OTDS250400-IWC-EN-01  
Rev.: 2025-Sept-05

This documentation has been created for OpenText™ Directory Services CE 25.4.  
It is also valid for subsequent software releases unless OpenText has made newer documentation available with the product,  
on an OpenText website, or by any other means.

**Open Text Corporation**

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Tel: +1-519-888-7111  
Toll Free Canada/USA: 1-800-499-6544 International: +800-4996-5440  
Fax: +1-519-888-0677  
Support: <https://support.opentext.com>  
For more information, visit <https://www.opentext.com>

**© 2025 Open Text**

Patents may cover this product, see <https://www.opentext.com/patents>.

**Disclaimer**

No Warranties and Limitation of Liability

Every effort has been made to ensure the accuracy of the features and techniques presented in this publication. However,  
Open Text Corporation and its affiliates accept no responsibility and offer no warranty whether expressed or implied, for the  
accuracy of this publication.

---

# Table of Contents

<b>1</b>	<b>Installing OpenText Directory Services Version 25 .....</b>	<b>13</b>
1.1	Installation prerequisites .....	13
1.1.1	Configuration requirements .....	14
1.1.2	About the OTDS database requirement .....	17
1.2	When upgrading a multi-tenant OTDS environment from a previous version of Directory Services that relied on OpenDJ .....	20
1.3	When upgrading and importing data from previous versions of Directory Services .....	20
1.4	Install files for Directory Services .....	25
1.5	Installing Directory Services on Windows .....	26
1.5.1	Installing OTDS on Windows from the UI .....	26
1.5.2	Installing OTDS on Windows from the command line .....	30
1.6	Installing Directory Services on Linux .....	34
1.6.1	Installing OTDS on Linux interactively .....	35
1.6.2	Installing OTDS on Linux non-interactively .....	40
1.7	Verifying your installation .....	41
1.8	Updating the JDBC database connection password after installation ..	42
1.9	Uninstalling Directory Services .....	42
1.10	Backup and Recovery .....	44
<b>2</b>	<b>Getting Started .....</b>	<b>45</b>
2.1	Overview .....	45
2.1.1	Terminology .....	46
2.1.2	Architecture .....	54
2.1.3	Typical scenario .....	56
2.2	Setup checklists .....	56
2.3	Accessing Directory Services .....	58
2.3.1	If you imported data from OTDS 16.x or 20.x to 25.4.x .....	59
2.3.2	Setting up an OTDS server for synchronization and authentication ..	60
2.4	The OTDS user interface .....	61
<b>3</b>	<b>User partitions .....</b>	<b>65</b>
3.1	User partitions Actions menu options, buttons, and column headings ..	66
3.2	User partitions and the synchronization master host .....	68
3.3	OTDS Two-Factor Authentication .....	69
3.4	Naming the user partition .....	69
3.5	Defining user attributes .....	70
3.6	Defining group attributes .....	72
3.7	The OTDS unique ID .....	72
3.8	Synchronized User Partitions .....	74
3.8.1	Defining a synchronized user partition .....	74

3.8.1.1	Connecting to an identity provider .....	78
3.8.1.2	When to use encryption .....	79
3.8.1.3	Choosing an authentication method .....	79
3.8.1.4	Understanding locations .....	80
3.8.1.5	Applying filters .....	80
3.8.1.6	Applying user partition attribute mappings .....	83
3.8.1.7	Synchronization types .....	84
3.8.1.8	Search methods .....	85
3.8.1.9	Examples of UUIDs for supported servers .....	86
3.8.1.10	AD/LDAP user and group ID attributes .....	86
3.8.1.11	Importing users and groups .....	86
3.8.2	Creating a synchronized user partition .....	87
3.8.3	Editing a synchronized user partition .....	97
3.8.4	Setting a password policy for a synchronized user partition .....	98
3.8.5	Importing users and groups .....	98
3.8.6	Editing members of groups in a synchronized user partition .....	98
3.8.7	Restarting a synchronized user partition .....	99
3.8.8	Enabling two-factor authentication .....	99
3.8.9	Duplicating a synchronized user partition .....	100
3.8.10	Deleting a synchronized user partition .....	101
3.9	Non-synchronized user partitions .....	101
3.9.1	Defining a non-synchronized user partition .....	102
3.9.1.1	Configuring users in a non-synchronized user partition .....	102
3.9.1.1.1	Using WebAuthn to provide users the option of passwordless authentication .....	103
3.9.1.2	Creating groups in a non-synchronized user partition .....	105
3.9.1.3	Creating organizational units in a non-synchronized user partition ....	105
3.9.2	Creating a non-synchronized user partition .....	106
3.9.3	Editing a non-synchronized user partition .....	107
3.9.4	Deleting a non-synchronized user partition .....	108
3.9.5	Creating users in a non-synchronized user partition .....	109
3.9.6	Editing users in a non-synchronized user partition .....	111
3.9.7	Consolidating users in a partition .....	112
3.9.8	Resetting a user password in a non-synchronized user partition .....	113
3.9.9	Unlocking an account .....	114
3.9.10	Configuring partition restrictions .....	114
3.9.11	Enabling two-factor authentication .....	115
3.9.12	Deleting users in a non-synchronized user partition .....	115
3.9.13	Creating groups in a non-synchronized user partition .....	116
3.9.14	Editing groups in a non-synchronized user partition .....	117
3.9.15	Editing members of groups in a non-synchronized user partition .....	118
3.9.16	Editing administrators of groups in a non-synchronized user partition .....	119

3.9.17	Consolidating groups in a partition .....	120
3.9.18	Enabling two-factor authentication for a group .....	121
3.9.19	Deleting groups in a non-synchronized user partition .....	121
3.9.20	Creating an organizational unit in a non-synchronized user partition ..	122
3.9.21	Editing organizational units in a non-synchronized user partition .....	122
3.9.22	Editing administrators of organizational units in a non-synchronized user partition .....	123
3.9.23	Enabling two-factor authentication for an organizational unit .....	124
3.9.24	Deleting organizational units in a non-synchronized user partition ...	124
3.9.25	Password policy for non-synchronized user partitions .....	125
3.9.25.1	Defining a password policy for one non-synchronized user partition ..	125
3.9.25.2	Defining a global password policy for all non-synchronized user partitions .....	127
3.10	Consolidating users and groups in Partitions .....	128
3.10.1	Consolidating changes to users, groups, organizational units, and partitions .....	129
3.10.1.1	Setting the partition attribute to apply recursive consolidation for users or groups in a synchronized user partition .....	130
3.10.2	Setting notifications when a manual consolidation is required .....	131
3.10.3	Canceling consolidation of changes to users and groups .....	131
3.11	Partition attributes .....	132
3.11.1	Examples filtering one synchronized partition's deleted users and groups .....	132
3.11.2	Creating system or custom attributes for one partition .....	134
3.12	Disabling a user partition .....	135
3.12.1	Enabling or disabling a user partition .....	135
<b>4</b>	<b>Authentication Handlers .....</b>	<b>137</b>
4.1	Using authentication handlers .....	138
4.1.1	List of authentication handlers .....	138
4.1.2	Prioritizing authentication handlers .....	157
4.1.3	Configuration and use of OAuth authentication .....	158
4.1.4	Configuration and use of SAML authentication .....	159
4.1.5	Integrating Directory Services with Web Access Management applications .....	161
4.2	Creating an authentication handler .....	162
4.3	Editing an authentication handler .....	163
4.4	Deleting an authentication handler .....	164
4.5	Changing the priority of an authentication handler .....	164
4.6	Enabling or disabling an authentication handler .....	165
4.7	Configuring the http.negotiate authentication handler on Unix .....	165
4.8	Configuring the Oracle EBS authentication handler .....	166
4.9	Configuring SAML .....	167

4.10	Integrating Directory Services with Web Access Management applications .....	170
<b>5</b>	<b>Resources .....</b>	<b>173</b>
5.1	Resources Actions menu options, buttons and column headings .....	174
5.2	Non-synchronized resources .....	175
5.2.1	Creating a non-synchronized resource .....	176
5.2.2	Configuring a non-synchronized resource .....	178
5.2.3	Editing a non-synchronized resource .....	179
5.2.4	Deleting a non-synchronized resource .....	180
5.3	Synchronized resources .....	180
5.3.1	Configuring synchronized resources .....	180
5.3.1.1	User and group synchronization .....	181
5.3.1.2	Managing user and group permissions for this resource .....	181
5.3.1.3	Using resource attribute mappings .....	182
5.3.1.3.1	OTDS resource Format options .....	183
5.3.1.3.2	Support for javascript and multi-valued javascript in the Format column .....	183
5.3.1.3.3	Examples using resource attribute mappings to create groups .....	186
5.3.1.4	Connection parameters .....	188
5.3.1.4.1	Connection parameters for Archive Center resources .....	188
5.3.1.4.2	Connection parameters for eDocs DM resources .....	189
5.3.1.4.3	Connection parameters for MBPM resources .....	189
5.3.1.4.4	Connection parameters for OpenText Media Management resources ..	189
5.3.1.4.5	Connection parameters for Process Component Library resources ...	190
5.3.1.4.6	Connection parameters for REST (Generic) resources .....	190
5.3.1.4.7	Connection parameters for Service Center resources .....	190
5.3.1.4.8	Connection parameters for SCIM 2.0 .....	191
5.3.1.4.9	Connection parameters for WSM Delivery Server resources .....	191
5.3.1.4.10	Connection parameters for WSM Management Server resources .....	192
5.3.1.5	Configuring a synchronized resource for OpenText Content Management .....	193
5.3.1.5.1	Connection parameters for OpenText Content Management resources .....	194
5.3.1.5.2	Default OpenText Content Management user and group attribute mappings .....	201
5.3.1.5.3	Resource user attribute mappings supported by Content Web Services .....	203
5.3.1.5.4	Configuring Directory Services integration administration .....	203
5.3.1.5.5	Configuring Directory Services with multiple instances of OpenText Content Management .....	205
5.3.1.6	Configuring a synchronized resource for Enterprise Process Services .....	205
5.3.1.6.1	Connection parameters for Enterprise Process Services resources ..	206

5.3.2	Creating a synchronized resource .....	206
5.3.3	Creating a synchronized resource for Enterprise Process Services ..	211
5.3.4	Configuring a synchronized resource .....	213
5.3.5	Editing a synchronized resource .....	213
5.3.6	Consolidating a synchronized resource .....	217
5.3.7	Deleting a synchronized resource .....	218
5.3.8	OpenText Content Management-specific configuration tasks .....	218
5.3.8.1	Configuring access to your OpenText Content Management resource .....	218
5.3.8.2	Configuring Directory Services integration administration in OpenText Content Management .....	219
5.3.8.3	Migrating users and groups from OpenText Content Management 10.5 to Directory Services 25.4.x .....	221
5.3.8.4	Bypassing SSO when signing in to OpenText Content Management ..	223
5.4	Configuring access to your resources .....	224
5.4.1	Editing access roles for your resource .....	225
5.4.2	Editing notification settings for your resource .....	225
5.4.3	Editing impersonation settings .....	225
5.4.4	Turning user synchronization on or off .....	226
5.5	Activating your resource for authentication .....	226
5.5.1	Activating or deactivating your resource .....	227
5.5.2	Enabling or disabling authentication for your resource .....	228
<b>6</b>	<b>Access Roles .....</b>	<b>229</b>
6.1	Assigning members to an access role .....	230
6.2	Creating an access role .....	231
6.3	Assigning members to an access role or removing members from an access role .....	231
6.4	Assigning access roles to resources .....	233
6.5	Editing an access role .....	233
6.6	Deleting an access role .....	234
6.7	Including/excluding groups from organizational units .....	234
<b>7</b>	<b>Users and Groups .....</b>	<b>235</b>
7.1	Configuring two-factor authentication .....	237
7.1.1	Two-factor authentication with a third-party two factor authentication provider .....	239
7.1.2	Resetting a user's secret key .....	240
7.2	Configuring users .....	241
7.2.1	Searching for users .....	241
7.2.2	Adding users .....	241
7.2.3	Editing users .....	242
7.2.4	Consolidating users .....	243
7.2.5	Resetting a user password .....	244

7.2.6	Unlocking a user account .....	245
7.2.7	Enabling two-factor authentication .....	245
7.2.8	Allocate to license .....	247
7.2.9	View and edit allocated licenses .....	248
7.2.10	Deleting users .....	249
7.3	Configuring groups .....	249
7.3.1	Delegated administration .....	251
7.3.2	Searching for groups .....	251
7.3.3	Adding groups .....	251
7.3.4	Editing groups .....	252
7.3.5	Editing members of groups .....	253
7.3.6	Editing administrators of groups .....	254
7.3.7	Consolidating groups .....	255
7.3.8	Enabling two-factor authentication for a group .....	256
7.3.9	Deleting groups .....	256
7.3.10	Editing organizational units .....	257
7.3.11	Editing administrators of organizational units .....	258
7.3.12	Enabling two-factor authentication for an organizational unit .....	258
7.3.13	Deleting organizational units .....	259
<b>8</b>	<b>Application Roles .....</b>	<b>261</b>
8.1	Application roles and custom attributes .....	262
8.2	Difference between application roles and access roles .....	262
8.3	Defining application role attributes .....	262
8.4	Editing an application role .....	263
8.5	To assign users, groups, or application roles to an application role ...	264
8.6	To view all application roles (recursively) assigned to a specific user, group, or application role .....	266
8.7	To edit administrators of an application role .....	266
8.8	To set two-factor authentication for an application role .....	267
8.9	To create an application role .....	267
8.10	To delete an application role .....	268
<b>9</b>	<b>Recycle Bin .....</b>	<b>269</b>
9.1	Viewing recycle bin users, groups, or roles .....	270
9.2	Recycle bin settings .....	271
9.3	Manually restoring users and groups from the recycle bin .....	272
9.4	Manually deleting users and groups from the recycle bin .....	273
<b>10</b>	<b>OAuth Clients .....</b>	<b>275</b>
10.1	Creating an OAuth client .....	276
10.2	Editing an OAuth client .....	279
10.3	Editing impersonation settings .....	279

10.4	Deleting an OAuth client .....	280
<b>11</b>	<b>External Import .....</b>	<b>281</b>
11.1	XML file example .....	282
11.2	Enabling the external import tab .....	283
11.3	Creating an external import .....	283
11.4	Editing an external import .....	285
11.5	Beginning an external import .....	285
11.6	Deleting an external import .....	286
<b>12</b>	<b>System Config .....</b>	<b>287</b>
12.1	System Attributes .....	288
12.1.1	List of supported system attributes .....	288
12.1.2	Examples filtering system-wide deleted users and groups .....	315
12.1.3	Adding a system attribute .....	316
12.1.4	Editing a system attribute .....	317
12.1.5	Deleting a system attribute .....	318
12.2	SMTP Settings .....	318
12.3	Audit/Reporting Settings .....	319
12.4	Notifications Settings .....	320
12.4.1	Notifications areas .....	321
12.4.2	To configure notifications settings .....	322
<b>13</b>	<b>Multiple instances of Directory Services .....</b>	<b>325</b>
13.1	Changing the synchronization master host .....	326
<b>14</b>	<b>Trusted Sites .....</b>	<b>327</b>
14.1	Customizing trusted referrals .....	328
14.2	Adding a trusted referring address .....	328
14.3	Removing a trusted referring address .....	329
<b>15</b>	<b>License Keys .....</b>	<b>331</b>
15.1	Overview of License Keys tab .....	332
15.2	Understanding allocating and reserving licenses to users, groups, and partitions .....	336
15.2.1	Allocation and reviewing reserved seats .....	337
15.2.2	Sharing Licenses .....	338
15.2.2.1	Setting a shared License .....	338
15.2.2.2	Unsetting a Shared License .....	338
15.2.3	Licensees and counters .....	339
15.3	Creating and submitting a license key .....	339
15.4	Editing a license key .....	341
15.5	Reviewing reserved seats .....	342
15.6	Deleting a license key .....	343

15.7	Adding a license key .....	343
15.8	Viewing licensees .....	343
15.9	Viewing shared license usage .....	344
15.10	Generating a Report .....	345
15.11	Showing license certificates .....	345
15.12	Auditing Licensing events .....	346
15.13	Examining License Key Logging Information .....	346
<b>16</b>	<b>Single Sign On .....</b>	<b>347</b>
16.1	Customizing the login user name format .....	347
16.2	Single sign on scenarios .....	348
16.2.1	Basic single sign on .....	348
16.2.2	Single sign on with a portal-style application .....	349
16.2.3	Single sign on with integrated Windows authentication .....	349
16.2.4	Client to server .....	350
16.2.5	Server to server identity assertion .....	351
16.3	Single sign out .....	351
<b>17</b>	<b>Customizing Directory Services .....</b>	<b>353</b>
17.1	Customizing the sign-in page .....	354
17.2	Customizing OTDS emails .....	356
17.2.1	To customize OTDS emails .....	357
17.3	Customizing Directory Services mappings .....	358
<b>18</b>	<b>SCIM Support in OTDS .....</b>	<b>361</b>
<b>19</b>	<b>Jobs .....</b>	<b>363</b>
19.1	Types of Jobs .....	364
19.2	Job's information messages .....	364
19.3	Viewing a job's messages .....	365
19.4	Canceling a job .....	365
19.5	Clearing all completed jobs .....	365
19.6	Clearing all selected jobs .....	365
<b>20</b>	<b>Audit Reports .....</b>	<b>367</b>
20.1	Searching audit reports .....	368
20.2	An audit report's details .....	369
20.3	Finding an audit report's object .....	370
20.4	Retrieving an audit report's event count .....	370
<b>21</b>	<b>System Status .....</b>	<b>371</b>
21.1	Potential configuration issues .....	372
21.2	Downloading the OTDS configuration report .....	372
21.3	Viewing potential configuration issues .....	373

<b>22</b>	<b>Log Files .....</b>	<b>375</b>
22.1	otds.log .....	375
22.2	directory-provenance.log .....	376
22.3	directory-access.log .....	376
22.4	directory-audit.log .....	377
22.5	otds-installer.log .....	377
22.6	otdsDeploy.log .....	377
22.7	The OTDS replication log files .....	378
22.8	Viewing the Directory Services log files .....	378
22.9	Configuring the Directory Services log files .....	379
<b>23</b>	<b>OTDS Documentation .....</b>	<b>381</b>
23.1	About the Directory Services online help .....	383
23.1.1	Provide the online help on a local help server (Private Help Server) .	384
23.1.1.1	Configuring OTDS to use the Private Help Server .....	385
23.2	References to external websites .....	385
<b>24</b>	<b>Directory Services security settings and considerations .</b>	<b>387</b>
<b>25</b>	<b>Troubleshooting .....</b>	<b>389</b>
25.1	Installation issues .....	389
25.2	Logging issues .....	394
25.3	Enterprise sync issues .....	397
25.4	OpenText Content Management issues .....	398
25.5	Resource configuration issues .....	401
25.6	Single sign on issues .....	403
25.7	Performance issues .....	406
25.8	General issues .....	406



# Chapter 1

## Installing OpenText Directory Services Version 25



**Note:** This guide describes Directory Services (OTDS) versions 25.4.x and includes descriptions of some features only available if you have installed OTDS 25.4.x.

Directory Services 25 is supported on Microsoft Windows Server and Linux. For specific operating system requirements, see the *OTDS Release Notes*.

### 1.1 Installation prerequisites

To install and use OpenText Directory Services you must first install and configure the following 64-bit software:



**Note:** For the minimum versions required see the *Release Notes*. For more information, see *OpenText Directory Services - Installation and Administration Guide* (OTDS-IWC) and the **OTDS Release Notes**. You can find links to these documents in “OTDS Documentation” on page 381.

- **Java 64-bit.** You can download this from [java.com](http://java.com), see “[References to external websites](#)” on page 385. For information about configuring Java options, see “[Configuring Tomcat for OTDS](#)” on page 14.
- **Apache Tomcat 64-bit.** You can download this from [tomcat.apache.org](http://tomcat.apache.org), see “[References to external websites](#)” on page 385. For more information, see “[Configuring Tomcat for OTDS](#)” on page 14.
- **Database server.** Directory Services requires a separately installed and configured database server to store all OTDS data, including configuration, partitions, and user data.

For supported database servers, see the *Release Notes*. For more information, see “[About the OTDS database requirement](#)” on page 17.

### Prerequisites for the installing userID

OpenText recommends that the user installing or upgrading OTDS has administrative privileges:

1. On Windows, you can open a command prompt window as administrator, see “[References to external websites](#)” on page 385.
2. On Linux, you need to create the user and group to be used as the owner and group of the OTDS files.



### Caution

Do not use `root` to install OTDS. It can create security vulnerabilities when running the application server using a root, or equivalent, user.

The user you create must:

- Have full permissions to the destination directories for the install as well as to the `/etc/opentext` directory for the registry.
- Have *write* access to the path where Tomcat is installed.  
Because the user who runs Tomcat needs *read* access to all the files in the OTDS installation directory, you need to designate one user to both install OTDS and run Tomcat.
- Have a `PATH` statement that includes the `bin` directory for Java.

#### 1.1.1 Configuration requirements

- Mandatory: “Configuring Tomcat for OTDS” on page 14.
- Optional: “Securing your server using SSL” on page 17.

#### Configuring Tomcat for OTDS

##### To configure Tomcat for OTDS:

1. Ensure that the userid running Tomcat has *read* access to the complete OTDS installation directory.
2. If you are installing Tomcat on Linux, you could create an installation user `<otuser>` and the group `<otgroup>` to be used with Tomcat. Sign in as the `<otuser>` to begin the install.



### Caution

Do not use the `root` user to install Tomcat on Linux. It can create security vulnerabilities when running the server using a root, or equivalent, user.

Because the user who runs Tomcat needs *read* access to all the files in the OTDS installation directory, you could designate one user to both install OTDS and run Tomcat.



### Caution

If you are installing on Linux, do not use a package installer to install Tomcat. Some package installers split the installation of Tomcat across multiple directories. The OTDS installer assumes that Tomcat is installed in a single directory.

3. Download Apache Tomcat and follow the Tomcat instructions to install it. For information, see “References to external websites” on page 385.

4. On Windows, start the Monitor Apache Tomcat tool from **All Programs --> Apache Tomcat --> Monitor Tomcat**.

 **Tip:** You can also start the Monitor Apache Tomcat tool by starting the `<Tomcat_installdir>\bin\tomcat<version>w.exe` executable.

Next, do the following:

- a. In the **Initial memory pool** box, enter 256 MB.
- b. In the **Maximum memory pool** box, the value that you enter for **Maximum memory pool** should be proportional to the number of users OTDS will manage. OpenText recommends that you enter a minimum value for **Maximum memory pool**, as follows:
  - If your number of users is 25,000 users or less, you should enter a minimum value of 1024 MB
  - If your number of users is 25,000 to 50,000 users, you should enter a minimum value of 2048 MB
  - If your number of users is 50,000 to 100,000+ users, you should enter a minimum value of 4096 MB
5. Click **OK**.
6. If you are running the Tomcat service under a Windows service account, you will need to follow these steps.

 **Tip:** These steps are only necessary if you are using Kerberos or Windows SSO. In other words, if you intend to use the **Negotiate Token** or **HTTP Negotiate** authentication handlers. See “[List of authentication handlers](#)” on page 138.

- a. Create a dedicated service account for OTDS, `DOMAIN\serviceaccount`. Being a service account, the password for this service account must not expire.
- b. Open a command window as the service account you just created, and then run the following command:

```
setspn -a HTTP/otdsserver.domain.com DOMAIN\serviceaccount
```
7. On Linux, you need to specify the `CATALINA_OPTS` environment variable prior to starting Tomcat. The following is an example of the command you can type. You should choose the value you specified for the `Xmx` option depending on your number of users. See the information about numbers of users provided in [step 4.b](#) to determine your appropriate setting for the `Xmx` option.

Run the following command:

```
CATALINA_OPTS="-Xmx1024M $CATALINA_OPTS"
```



**Note:** This environment variable needs to be specified each time Tomcat is started. To avoid having to specify the environment variable manually each time, you can add the

CATALINA\_OPTS

line to the `setenv.sh` file that you create in the `<Tomcat_installdir>/bin` directory.

8. On Windows or Linux, edit the `<Tomcat_installdir>\conf\server.xml` file. Search for the connector definition line. For example, locate the following lines:

```
<Connector port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
```

Add a new attribute, `maxHttpHeaderSize="65536"`, for example:

```
<Connector port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" maxHttpHeaderSize="65536" />
```

9. If you are using OTDS with Archive Server, you need to add the following Tomcat Java setting:

```
-Dotds.config.file=as_bootstrap.yaml
```

This is required for a new OTDS installation so that it can bootstrap the administrative groups required by Archive Server. Those administrative groups are:

- otadsadmins
- otasadmins
- otldadmins
- otldagents

10. If you are running OTDS on Tomcat with the Java Security Manager enabled, you need to add the following initial security policy to `catalina.policy`:

```
// OTDS
grant codeBase "file:<OTDSINSTALLDIR>/ -" {
    permission java.io.FilePermission
        "${java.home}${file.separator}lib${file.separator}*", "read";
    permission java.io.FilePermission
        "${java.home}${file.separator}conf${file.separator}*", "read";
    permission java.io.FilePermission
        "${catalina.base}${file.separator}logs", "read";
    permission java.io.FilePermission
        "${catalina.base}${file.separator}logs${file.separator}-", "read, write,
delete";
    permission java.io.FilePermission
        "${java.io.tmpdir}", "read";
    permission java.io.FilePermission
        "${java.io.tmpdir}${file.separator}-", "read, write, delete";
    permission java.io.FilePermission
        "<OTDSINSTALLDIR>/otdswebs/WEB-INF/classes/-", "read";
    permission java.io.FilePermission
        "<OTDSINSTALLDIR>/otdswebs/WEB-INF/lib/-", "read";

    permission java.lang.RuntimePermission "*";
    permission java.lang.reflect.ReflectPermission "suppressAccessChecks";
    permission java.net.NetPermission "specifyStreamHandler";

    permission java.net.SocketPermission "localhost:0-", "accept,connect,listen";
```

```
    permission java.net.SocketPermission "*:0-", "connect";  
  
    permission java.security.SecurityPermission "insertProvider.ApacheXMLEDSig";  
    permission java.security.SecurityPermission "removeProvider.ApacheXMLEDSig";  
    permission java.security.SecurityPermission "putProviderProperty.ApacheXMLEDSig";  
    permission java.security.SecurityPermission "insertProvider.STRTTransform";  
    permission java.security.SecurityPermission "removeProvider.STRTTransform";  
    permission java.security.SecurityPermission "putProviderProperty.STRTTransform";  
    permission java.security.SecurityPermission "org.apache.xml.security.register";  
  
    permission java.util.PropertyPermission "*", "read,write";  
    permission java.util.logging.LoggingPermission "control";  
};
```



**Note:** Additional configuration may be required depending on the features you are using in your environment. One way to check whether additional configuration is required is to examine the `otds.log` file. If the `otds.log` file shows any `java.security.AccessControlException` errors, you need to add the permission associated with that exception. For more information about the log files, see “[otds.log](#)” on page 375.

11. Restart Tomcat.

## Securing your server using SSL

When enabling Secure Sockets Layer (SSL), OpenText recommends using a server certificate from a Certificate Authority that has a root certificate that is trusted by the JRE and is correctly installed in the keystore of the JRE. For example, `<Java_installdir>/lib/security/cacerts`.

For detailed information on enabling SSL on Tomcat, see “SSL Configuration How-to” in “[References to external websites](#)” on page 385.

### 1.1.2 About the OTDS database requirement

Directory Services requires a separately installed and configured database server to store all OTDS data, including configuration, partitions, and user data. For supported database servers and specific requirements for the database, see the *Directory Services Release Notes*.



#### Important

The database user name and password that you supply to OTDS during installation requires full permissions to the OTDS database that you created. An example of a database user with full permissions is the database owner.

OpenText recommends that the user ID designated as the database owner is the user ID you enter in the **Database Username** field in the **JDBC Parameters** window during installation.

Each of the supported databases has their own requirements for permissions when writing to a database. Whether installing or upgrading OTDS, check your database's documentation for those requirements.

You can use your database server to create a separate database that will be used exclusively by OTDS. For more information, see the documentation for your chosen database server.

Examples showing the information you need to give OTDS during installation can be found in “[Format for the Database JDBC connection string](#)” on page 18.

If you are using OTDS with OpenText Content Management:

- After you have created a separate database for use by OTDS, and completed your installation of OTDS, you can use OpenText Content Management's database management tools to manage that separate database. For more information, see *OpenText Content Management - Installation Guide (LLESCOR-IGD)*.
- Although you can connect OTDS to the same database that you created for OpenText Content Management, OpenText does not recommend this option because OTDS and OpenText Content Management may have different database configuration requirements.



**Note:** By default, OTDS creates its tables upon first startup in a schema named OTDS. In order to use the default schema of the database user instead, set the environment variable `OTDS_USEDEFAULTDBSCHEMA=true`, or the JVM system property `otds.usedefaultdbschema=true`.

## Format for the Database JDBC connection string

During installation, the form in which you type information in the **Database JDBC connection string** box depends on the database that you installed and configured. See the following examples for the forms required by each supported database.

---

### MS SQL Server

► **Example 1-1: A basic MS SQL Server database JDBC connection string**

```
jdbc:sqlserver://<hostname>:<portnumber>;databaseName=<MyDBname>
```



► **Example 1-2: An MS SQL example showing an included instance name**

```
jdbc:sqlserver://<hostname>:<portnumber>;instanceName=<MyInstance>;databaseName=<MyDBname>
```



### Oracle

► **Example 1-3: A basic “sid” Oracle database JDBC connection string**

```
jdbc:oracle:thin:@<hostname>:1521:<MyDBname>
```



► **Example 1-4: A basic “service” Oracle database JDBC connection string**

```
jdbc:oracle:thin:@//<hostname>:1521 / <MyDBname>
```



► **Example 1-5: Oracle database JDBC connection strings that require setting the TNS\_ADMIN\* environment variables**

If you need to set the TNS\_ADMIN\* environment variables, TNS\_ADMIN should specify the location of the TNSNAMES.ORA file. For example: %ORACLE\_HOME%\network\admin.

```
jdbc:oracle:thin:@<tns_entry>
```

```
jdbc:oracle:thin:@<network_service_name>
```



► **Example 1-6: An Oracle database JDBC connection string that uses a connect descriptor**

```
jdbc:oracle:thin:@<connect_descriptor>
```

An example of <connect\_descriptor> could be:

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP) (HOST=10.1.1.1) (PORT=1521)) (CONNECT_DATA=(SID = test)))
```



---

## PostgreSQL

► **Example 1-7: A basic PostgreSQL database JDBC connection string**

```
jdbc:postgresql://<hostname>:5432 / <MyDBname>
```



---

## SAP HANA

► **Example 1-8: A basic SAP HANA database JDBC connection string**

```
jdbc:sap://<hostname>:30077
```



► **Example 1-9: A basic SAP HANA database JDBC connection string with database name**

```
jdbc:sap://<hostname>:30015 / ?databaseName=<MyDBname>
```



If you need to change your database connection string after installation, see “How do I change my database connection information after I have installed OTDS?” in “[Installation issues](#)” on page 389.

## 1.2 When upgrading a multi-tenant OTDS environment from a previous version of Directory Services that relied on OpenDJ

There is nothing different about upgrading a multi-tenant versus a single-tenant OTDS installation. When you run the OTDS installer, OTDS will migrate data from OpenDJ to the database. At that time, all tenants in your environment are migrated.

From OTDS 22.1 onwards, tenant management is done strictly through the REST API. For information about the REST API, see [To access the developer documentation detailing the REST API](#): on page 381.

When upgrading, either a multi-tenant or a single-tenant OTDS installation, follow the instructions found in “[When upgrading and importing data from previous versions of Directory Services](#)” on page 20.

## 1.3 When upgrading and importing data from previous versions of Directory Services

When upgrading OTDS, a standard upgrade using the installer will ensure that all OTDS users, groups, passwords and OTDS customizations are brought into your new installation.

You may be upgrading from a version of OTDS that relies on OpenDJ or from a version of OTDS that relies on a database:

1. If you are upgrading from a version of OTDS that relies on OpenDJ, when you launch the OTDS installer to install your upgraded version of OTDS, the installer will retrieve all user, group, and configuration information from OpenDJ and will transfer that information to your newly created database.
2. If you are upgrading from a version of OTDS that relies on a database, when you launch the OTDS installer to install your upgraded version of OTDS, the installer will preserve all user, group, and configuration information from the database.

Choose one of the following procedures when upgrading a previous version of OTDS:

- “[If you are upgrading a stand-alone installation of OTDS, and your existing OTDS version is installed on the same physical machine](#)” on page 21
- “[If you are upgrading a stand-alone installation of OTDS, and your existing OTDS version is installed on a different physical machine](#)” on page 22
- “[If you are upgrading an internal version of OTDS that you installed as part of your OpenText Content Management installation](#)” on page 24

**If you are upgrading a stand-alone installation of OTDS, and your existing OTDS version is installed on the same physical machine:**

1. If you want to upgrade a stand-alone version of OTDS, and your existing version is installed on the same physical machine on which you want to install version 25.4.x, you will need to follow this procedure.

You can only upgrade using this procedure if you are upgrading from version 10.5 or higher.

2. If your existing version of OTDS is lower than version 10.5, you must upgrade your existing OTDS installation to version 10.5 before proceeding. For more information, see the Directory Services 10.5 Installation and Administration (<https://webapp.opentext.com/piroot/otds/v100500-01/otds-iwc/docovw.xml>) guide.

3. Confirm that each of the following is correct:

- a. Your existing version of OTDS is 10.5 or higher.
- b. All user, group, and configuration data is correct and accessible.

4. If your existing OTDS environment includes replicated servers, stop OTDS on all replicated servers.

This is required to prevent data from being created or updated in OpenDJ by one of the replicated servers after data has migrated from OpenDJ to your new database.

5. Run the OTDS 25.4.x installer on your primary server, the *synchronization master server*.

Follow the instructions to install a primary server found in either “[Installing Directory Services on Windows](#)” on page 26 or “[Installing Directory Services on Linux](#)” on page 34, depending on your operating system.



**Note:** Upon initial startup, OTDS will retrieve all user, group, and configuration information from OpenDJ and will transfer that information to your newly created database.

6. After the installation completes, verify that OTDS is operational and that your user, group, and configuration data is accessible.



**Note:** You can manually remove OpenDJ at a later time once you have verified that its content is no longer needed as a backup. To manually remove OpenDJ, see [How do I uninstall OpenDJ? on page 394](#).

7. If you do not have a replicated environment, with multiple instances of OTDS, your upgrade is complete.

8. If you have a replicated environment, you must now uninstall the existing version of OTDS on each server and then install version 25.4.x as a *supplementary installation* on each server. During each installation, follow the instructions to install a supplementary server found in “[Installing Directory](#)

Services on Windows” on page 26 or “Installing Directory Services on Linux” on page 34.



**Note:** While upgrading each supplementary server is possible, and depending on the previous version, you may need to manually copy the data encryption key to the `otds.properties` file. OpenText therefore recommends that you uninstall the existing version of OTDS on each server and then install version 25.4.x as a supplementary server.

**If you are upgrading a stand-alone installation of OTDS, and your existing OTDS version is installed on a different physical machine:**

1. If you want to upgrade a stand-alone version of OTDS, and your existing version is installed on a different physical machine than the machine on which you want to install version 25.4.x, you will need to follow this procedure.

Below is an example of how your environment might be configured that would require you to follow this upgrade procedure:

**Example:** If your existing version of OTDS is located on Machine-A and you want to upgrade this version to 25.4.x, but you want version 25.4.x installed on Machine-B, you need to follow this procedure.

The situation in this example detailed above is the fact that the existing source of the user, group, and configuration data (OpenDJ) is located on a different physical machine than the machine on which you want to install OTDS 25.4.x.

2. In this situation, you can only upgrade to 25.4.x if you are upgrading from version 16.4.1 or higher.

If your existing version of OTDS is lower than version 16.4.1, you will need to first upgrade your OTDS installation to version 16.4.1 before proceeding. For more information, see the Directory Services 16.4.1 Installation and Administration (<https://webapp.opentext.com/piroot/otds/v160401/otds-iwc/docovw.xml>) guide.

3. Once your existing version of OTDS is 16.4.1, or higher, verify that all user, group, and configuration data is both correct and accessible.
4. If your existing OTDS environment includes replicated servers, stop OTDS on all replicated servers.

This is required to prevent data from being created or updated in OpenDJ by one of the replicated servers after data has migrated from OpenDJ to your new database.

5. Run the OTDS 25.4.x installer on your primary server, the *synchronization master server*. From the examples detailed in **step 1**, you will run the installer on Machine-B.

Follow the instructions to install a primary server found in either “Installing Directory Services on Windows” on page 26 or “Installing Directory Services on Linux” on page 34, depending on your operating system.

6. During the installation, when you are prompted on the **Directory Services Data Import** page, select **Import data** and then do the following:

- a. In the **OpenDJ LDAP URL** box, you need to type the URL that accesses OpenDJ on the machine from which you will be importing OTDS data. This is the machine on which your previous version of OTDS was installed. Type the LDAP URL in the form:

```
ldap://<hostname>:<LDAP_port_number>
```

Where:

- <hostname> is the hostname or IP address of the machine on which OpenDJ is installed.
- <LDAP\_port\_number> is the port number on which LDAP listens on the hostname you typed above.

An example of an OpenDJ LDAP URL is:

```
ldap://Machine-A.opentext.com:389
```



**Note:** If you used the default communication port numbers when you installed OTDS, then the default LDAP communication port number on Windows is “389” and on Linux is “1389”.

- b. In the **OpenDJ Directory Manager password** box, type the password for the userid “cn=Directory Manager”. This password, also referred to as the “bindPassword”, is usually the password that was provided for the otadmin@otds.admin account at installation time.
- c. Click **Next**.
- d. On the **Directory Services Encryption Key** page, do the following:
  - i. If you are importing data from another installation of OTDS, in the **Encryption Key** box, type, or copy and paste, the value of the directory.bootstrap.CryptSecret field found in the otds.properties file on the machine on which the OpenDJ version from which you want to import data is installed.
  - ii. If you are setting up a supplementary installation of OTDS, in the **Encryption Key** box, type, or copy and paste, the value of the directory.bootstrap.CryptSecret field found in the otds.properties file on the machine on which you installed your primary instance of OTDS.



**Note:** The otds.properties file can be found at <OTDS\_installdir>\config.

Previously, the otds.properties file was found at <OTDS\_installdir>\otdswebs\WEB-INF\classes.

7. After the installation completes, verify that OTDS is operational and that your user, group, and configuration data is accessible.



**Note:** You can manually remove OpenDJ at a later time once you have verified that its content is no longer needed as a backup. To manually remove OpenDJ, see [How do I uninstall OpenDJ? on page 394](#).

8. If you do not have a replicated environment, with multiple instances of OTDS, your upgrade is complete.
9. If you have a replicated environment, you must now uninstall the existing version of OTDS on each server and then install version 25.4.x as a *supplementary installation* on each server. During each installation, follow the instructions to install a supplementary server found in [“Installing Directory Services on Windows” on page 26](#) or [“Installing Directory Services on Linux” on page 34](#).



**Note:** While upgrading each supplementary server is possible, and depending on the previous version, you may need to manually copy the data encryption key to the `otds.properties` file. OpenText therefore recommends that you uninstall the existing version of OTDS on each server and then install version 25.4.x as a supplementary server.

10. **Optional** After you have completed the installation of Directory Services 25, and if you imported data from one host to a new host, you must ensure the value in the **Synchronization Master Host** box references your new synchronization master host.

For more information, see [Synchronization Master Host on page 312](#).

#### If you are upgrading an internal version of OTDS that you installed as part of your OpenText Content Management installation:

1. When you upgrade OpenText Content Management to version 24.3 or above, and if you had previously installed an internal version of OTDS, your internal version of OTDS will be removed.
2. You will need to install a stand-alone version of OTDS. For more information, see *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)* and *OpenText Content Management - Installation Guide (LLESCOR-IGD)*.

### Content Web Services and upgrading to OTDS 25

As part of the upgrade process, you can optionally choose to change from the OpenText Runtime and Core Services (RCS) version of Content Web Services to the stand-alone version. If you are keeping RCS for other products, for example for Enterprise Library or Archive Server, then you will also need to keep the RCS version of Content Web Services. However, if you are uninstalling RCS, then you will need to deploy the stand-alone version of Content Web Services. For more information, see OpenText Content Web Services (<https://knowledge.opentext.com/knowledge/cs.dll?func=ll&objId=67792619&objAction=browse&viewType=1>).

If you choose to switch from the RCS version to the stand-alone version of Content Web Services, you must manually modify the **Authentication Service WSDL** box in

the OpenText Content Management resource's connection parameters. For more information about the modification you need to make, see **Authentication Service WSDL** in the “[Connection parameters for OpenText Content Management resources](#)” on page 194.

## 1.4 Install files for Directory Services

You obtain the Directory Services install files from OpenText My Support ([https://support.opentext.com/csm?id=kb\\_search&spa=1&query=Directory%20Services%20\(OTDS\)](https://support.opentext.com/csm?id=kb_search&spa=1&query=Directory%20Services%20(OTDS))). In the search bar, replace “Directory Services (OTDS)” with “<Version\_Number> Directory Services (OTDS)”.

File name	Description
OTDS-2540-LNX.tar	Archive file containing the install files required for installing Directory Services on Linux.
OTDS-2540-WIN.msi	Setup file containing the install files required for installing Directory Services on Windows.

### Defining the installation types for Directory Services

The following details the installation type options:

- If the OTDS installer detects a 10.5, 16.x, 20.x, or 21.x version of OTDS installed on the system, you can choose to import the data from your previous version. If you choose this option, all existing data and configuration will be preserved.
- If you intend to install only one instance of OTDS, a stand-alone server, then that server, by default, is your primary server and is designated the *synchronization master server*. As such, in the **Directory Services Parameters** window, do not choose a *supplementary server* installation.
- However, if you intend to install multiple instances of OTDS on multiple machines, your first installation, or primary server, will function as the *synchronization master server*. For your first installation, in the **Directory Services Parameters** window, do not choose a supplementary server installation. For each subsequent installation, choose a *supplementary server* installation.

## 1.5 Installing Directory Services on Windows

If you choose to upgrade a previous version of Directory Services, the installation will maintain the previous installation path. If, during installation, you neither upgrade nor change the default installation path:

Directory Services will install to: C:\OTDS\.

### 1.5.1 Installing OTDS on Windows from the UI

**To install Directory Services on Windows from the UI:**

1. Ensure you have installed the prerequisite software listed in “[Installation prerequisites](#)” on page 13.
2. You obtain the Directory Services install files from OpenText My Support ([https://support.opentext.com/csm?id=kb\\_search&spa=1&query=Directory%20Services%20\(OTDS\)](https://support.opentext.com/csm?id=kb_search&spa=1&query=Directory%20Services%20(OTDS))). In the search bar, replace “Directory Services (OTDS)” with “<Version\_Number> Directory Services (OTDS)”.
3. Right click the `.msi` installation file and select **Run as Administrator** to start the installation program.



**Tip:** If you want to run the installer so that it takes you through the UI prompts and also create an installation log file, do the following:

1. Open a command prompt window as administrator. For more information see “[References to external websites](#)” on page 385.
2. Run the OTDS-2540-WIN.msi installer from that administrator command prompt window by typing the command:

```
msiexec.exe /i OTDS-2540-WIN.msi /l*v otds-install-log.txt
```

4. In the **Welcome** window, click **Next**.
5. In the **License Agreement** window, read the license agreement in full. To accept it, select **I accept**, and then click **Next**.
6. In the **Destination Folder** window, do one of the following, and then click **Next**:
  - Accept the default installation folder for Directory Services.
  - Type a new, valid, path.
  - Click the ... button to browse your computer to select the installation folder.
7. In the **Java Virtual Machine** window, if the Directory Services installer has found the Java path on your computer, the Java path will appear in the **Path** box. Do one of the following, and then click **Next**:
  - Accept the path the Directory Services installer has provided.
  - Type a new, valid, path.
  - Click the ... button to browse your computer to select the Java path.



**Note:** An example of a valid path is: C:\Program Files\Java\jre1.8.0\_73.

8. In the **Apache Tomcat Directory** window:

- a. You need to specify either the service name for Tomcat or the installed path for Tomcat.

If the Directory Services installer has found the Tomcat path on your computer, the **service name** and **Path** boxes will be filled. You can choose to edit either the service name or the path.



**Important**

If the OTDS installer has not found Tomcat on your system, OpenText recommends that you specify the service name for Tomcat.

- b. Click **Next**.

9. In the **Directory Services Parameters** window, do the following:

- a. In the **Hostname** box, type the fully qualified hostname for the installation of OTDS.
- b. If you are setting up this installation of OTDS as the initial or primary server, do *not* select the box to designate this installation as a **supplementary server**. Proceed to [step 10](#).

If you are setting up this installation of OTDS as a supplementary server, select the box to designate this installation as a **supplementary server**. Proceed to [step 12](#).

- c. Click **Next**.

10. In the **OpenText Directory Services Data Import** window, do the following:

- a. If you are not importing any data, select **No import**, and then click **Next**. Proceed to [step 11](#).
- b. If you are importing data, you can find more information in “[When upgrading and importing data from previous versions of Directory Services](#)” on page 20. Select **Import data**, and then do the following:

- i. In the **OpenDJ LDAP URL** box, you need to type the URL that accesses OpenDJ on the machine from which you will be importing OTDS data. This is the machine on which your previous version of OTDS was installed. Type the LDAP URL in the form:

```
ldap://<hostname>:<LDAP_port_number>
```

Where:

- <hostname> is the hostname or IP address of the machine on which OpenDJ is installed.
- <LDAP\_port\_number> is the port number on which LDAP listens on the hostname you typed above.

An example of an OpenDJ LDAP URL is:

```
ldap://Machine-A.opentext.com:389
```



**Note:** If you used the default communication port numbers when you installed OTDS, then the default LDAP communication port number on Windows is “389” and on Linux is “1389”.

- ii. In the **OpenDJ Directory Manager password** box, type the password for the userid “cn=Directory Manager”. This password, also referred to as the “bindPassword”, is usually the password that was provided for the `otadmin@otds.admin` account at installation time.
- iii. Click **Next**.

Proceed to [step 12](#).

11. In the **OTDS Administrator** window, do the following:

- a. The **OTDS Administrator User Name** box cannot be edited. The value “`otadmin@otds.admin`” is the default for this box.
- b. In the **Password** box, type a password for the `otadmin@otds.admin` user. You can reset the “`otadmin@otds.admin`” password from the OTDS web client. See [“Resetting a user password” on page 244](#) for more information.
- c. In the **Confirm password** box, re-type the password exactly.
- d. Click **Next**.



**Note:** If you do not apply a strong password, the OTDS installer will warn you that you have applied a weak password and you are advised to return and type a stronger password.

A strong password must contain at least eight characters. Among those eight characters, you must have one of each of the following:

- A lowercase letter, for example “h”.
- An uppercase letter, for example “D”.
- A number, for example “5”.
- A special character, for example “!”.

An example of a strong password is: John5Doe!

You can choose to either return and type a stronger password or keep the password you initially typed.

12. On the **Directory Services Encryption Key** page, do the following:

- a. If you are importing data from another installation of OTDS, in the **Encryption Key** box, type, or copy and paste, the value of the `directory.bootstrap.CryptSecret` field found in the `otds.properties` file on the machine on which the OpenDJ version from which you want to import data is installed.

- b. If you are setting up a supplementary installation of OTDS, in the **Encryption Key** box, type, or copy and paste, the value of the `directory.bootstrap.CryptSecret` field found in the `otds.properties` file on the machine on which you installed your primary instance of OTDS.



**Note:** The `otds.properties` file can be found at `<OTDS_installdir>\config`.

Previously, the `otds.properties` file was found at  
`<OTDS_installdir>\otdswebs\WEB-INF\classes`.

13. In the **JDBC Parameters** window, you need to inform OTDS about the location of the database that you set up in “[Installation prerequisites](#)” on page 13. You also need to provide sign-in access to the database.



**Important**

You need to be careful when entering the information to this window. The installer cannot verify the information you provide. An error in this window will result in OTDS being unable to access your database. For more information, see [How do I change my database connection information after I have installed OTDS?](#) on page 393.

- a. In the **Database JDBC connection string** box, you will type:

- An indicator for the type of database you set up for OTDS to use.
- The hostname or IP address of the machine on which the database is installed.
- The port number on which the database listens.
- The name of the database that you set up for OTDS to use.
- You might optionally include connection parameters.

For information about the form that this string takes, see “[Format for the Database JDBC connection string](#)” on page 18.

- b. In the **Database username** box, type the userID for a user with administrative access to the database.

The userID you type must have full permissions to the database that you created for OTDS. OpenText recommends that the userID designated as the database owner is the userID you enter in the **Database Username** field in the **JDBC Parameters** window during installation.

- c. In the **Database password** box, type the password for the user that you typed in step 13.b.



**Note:** If you enter information incorrectly to the **JDBC** fields, OTDS will not be able to access your database. If this happens, see [How do I change my database connection information after I have installed OTDS?](#) on page 393 and “[Updating the JDBC database connection password after installation](#)” on page 42.

14. In the **Ready to Install** window, click **Install**.



**Note:** You may be prompted to allow the Directory Services installer to make changes on your system. If this prompt appears, click **Yes**.

15. Click **Finish**.



**Tip:** If you see an error message indicating that the installer cannot write to certain directories, it may be because you did not run the installer as administrator. See [step 3](#) for information about how to run the installer as administrator.



**Note:** “OpenText Directory Services 25” will appear in the **Programs and Features** pane of the Windows Control Panel.

16. Proceed to “[Verifying your installation](#)” on page 41.

## 1.5.2 Installing OTDS on Windows from the command line

Before you begin, ensure you have installed the prerequisite software listed in “[Installation prerequisites](#)” on page 13.

You obtain the Directory Services install files from OpenText My Support ([https://support.opentext.com/csm?id=kb\\_search&spa=1&query=Directory%20Services%20\(OTDS\)](https://support.opentext.com/csm?id=kb_search&spa=1&query=Directory%20Services%20(OTDS))). In the search bar, replace “Directory Services (OTDS)” with “<Version\_Number> Directory Services (OTDS)”.

### Windows: silent installation parameters

The parameters for silent installation are:

---

**/i OTDS-2540-WIN.msi**

Requires you to specify the name of the OTDS installer. This parameter is required.

---

**/qb**

Requires you to direct that a silent install will be performed. This parameter is required.

---

**/l\*v otds-installer.log**

Allows you to optionally set up a log file for the installation, and names that log file: `otds-installer.log`. This parameter is optional but recommended.

---

**OTDS\_PASSWORD=<your\_password>**

Requires you to specify your OTDS password for the “`otadmin@otds.admin`” user. This parameter is required.

---

**HOST\_NAME=<fully\_qualified\_domain\_name>**

Requires you to specify the fully qualified domain name of this installation of OTDS. This parameter is required. If omitted, the installer pases “localhost” for this parameter.

---

**JAVAHOME=<Java\_installdir>**

Allows you to specify your Java installation path. This parameter is optional.

**TOMCATSERVICENAME=<Tomcat\_service\_name>**

Allows you to specify your Tomcat service name. This parameter is optional.

**INSTALLDIR=<OTDS\_installdir>**

Allows you to specify the installation path for OTDS. This parameter is optional. If omitted, the installer passes "C:\OTDS\" for this parameter.

**ISREPLICA\_TOPOLOGY=TRUE|FALSE**

Allows you to specify if this installation is a supplementary installation. This parameter is optional. Valid values are TRUE or FALSE.

Omit this parameter, or specify "FALSE", if you are installing your synchronization master host. Specify "TRUE" if you are installing a supplementary installation of OTDS.

**ENCRYPTION\_KEY**

If you are importing data from another installation of OTDS, this parameter requires you to type the value of the `directory.bootstrap.CryptSecret` field found in the `otds.properties` file on the machine on which OpenDJ is installed. For more information about importing, see [step 10](#).



**Note:** The `otds.properties` file can be found at `<OTDS_installdir>\config`.

Previously, the `otds.properties` file was found at `<OTDS_installdir>\otdsws\WEB-INF\classes`.

If you are importing data, this parameter is required.

**JDBC\_CONNECTION\_STRING**

Requires you to specify the location of the database that you set up for this OTDS installation. This parameter is required. For more information, see ["Format for the Database JDBC connection string" on page 18](#).

**JDBC\_USERNAME**

Requires you to specify the userID of a user with permission to access the database you typed in **JDBC\_CONNECTION\_STRING**. This parameter is required.

The userID you type must have full permissions to the database that you created for OTDS. OpenText recommends that the userID designated as the database owner is the userID you enter in the **JDBC\_USERNAME** field during installation.

**JDBC\_PASSWORD**

Requires you to specify the password for the userID you typed in **JDBC\_USERNAME**. This parameter is required.

**MIGRATION\_OPENDJ\_URL**

If you are importing data from a previous version of OTDS, this parameter is required. You need to specify the LDAP OpenDJ URL to connect to the OpenDJ instance that was installed with that previous version of OTDS. For more information, see ["When upgrading and importing data from previous versions of Directory Services" on page 20](#).

Do not use this parameter unless you are migrating data.

#### MIGRATION\_OPENDJ\_PASSWORD

If you are importing data from a previous version of OTDS, this parameter is required. You need to specify the OpenDJ password, or bindPassword.

Do not use this parameter unless you are migrating data.

#### OTDS105\_16\_INSTALL\_TYPE

If you are importing data from a 10.5 version of OTDS, this parameter is required. You need to expressly inform the installer that you are migrating from a 10.5 version by including: OTDS105\_16\_INSTALL\_TYPE="105".

#### Example installing a stand-alone, or primary, OTDS from the command line without importing data

▶ **Example 1-10: To install OTDS as a stand-alone or primary server without importing:**

Open a command prompt window as administrator, for more information see “References to external websites” on page 385.

Run the OTDS-2540-WIN.msi installer from that administrator command prompt window by typing:

```
msiexec  
/i <OTDS_installer>  
/qb  
/l*v <otds-installer>.log  
INSTALLDIR="<OTDS_install_dir>"  
JAVAHOME="<Java_install_dir>"  
TOMCATSERVICENAME="<Tomcat_service_name>"  
HOST_NAME="<fully_qualified_domain_name>"  
ISREPLICA_TOPOLOGY=false  
IMPORTDATA=0  
JDBC_CONNECTION_STRING=<Connection_string_to_database>  
JDBC_USERNAME=<Database_user>  
JDBC_PASSWORD=<Database_user_password>  
OTDS_PASSWORD="<your_OTDS_admin_password>"
```

◀ **Example 1-11: To install OTDS as a stand-alone or primary server and import data:**

Open a command prompt window as administrator, for more information see “References to external websites” on page 385.

Run the OTDS-2540-WIN.msi installer from that administrator command prompt window by typing the command:

```
msiexec  
/i OTDS-2540-WIN.msi  
/qb  
/l*v otds22-installer.log  
INSTALLDIR="<OTDS_install_dir>"
```

```
JAVAHOME="<Java_install_dir>"  
TOMCATSERVICENAME="<Tomcat_service_name>"  
HOST_NAME="<fully_qualified_domain_name>"  
ISREPLICA_TOPOLOGY=false  
IMPORTDATA=1  
JDBC_CONNECTION_STRING=<Connection_string_to_database>  
JDBC_USERNAME=<Database_user>  
JDBC_PASSWORD=<Database_user_password>  
MIGRATION_OPENDJ_URL=<OpenDJ_LDAP_URL>  
MIGRATION_OPENDJ_PASSWORD=<bindPassword>  
ENCRYPTION_KEY=<encryption_key>
```



### Example installing OTDS as a supplementary server

**➤ Example 1-12: To install OTDS as a supplementary server:**

Open a command prompt window as administrator, for more information see “References to external websites” on page 385.

Run the OTDS-2540-WIN.msi installer from that administrator command prompt window by typing the command:

```
msiexec  
/i OTDS-2540-WIN.msi  
/qb  
/l*v otds-rep-installer.log  
INSTALLDIR=<OTDS_install_dir>  
JAVAHOME=<Java_install_dir>  
TOMCATSERVICENAME=<Tomcat_service_name>  
HOST_NAME="<fully_qualified_domain_name>"  
ISREPLICA_TOPOLOGY=true  
IMPORTDATA=0  
JDBC_CONNECTION_STRING=<Connection_string_to_database>  
JDBC_USERNAME=<Database_user>  
JDBC_PASSWORD=<Database_user_password>  
ENCRYPTION_KEY=<encryption_key>
```



### Example upgrading OTDS from version 10.5

**➤ Example 1-13: To upgrade from OTDS 10.5:**

Open a command prompt window as administrator, for more information see “References to external websites” on page 385.

Run the OTDS-2540-WIN.msi installer from that administrator command prompt window by typing the command:

```
msiexec.exe  
/i OTDS-2540-WIN.msi  
/qb  
/l*v otds-upgrade105.txt  
INSTALLDIR=<OTDS_install_dir>  
JAVAHOME=<Java_install_dir>  
TOMCATSERVICENAME=<Tomcat_service_name>  
ISREPLICA_TOPOLOGY=false  
JDBC_CONNECTION_STRING=<Connection_string_to_database>  
JDBC_USERNAME=<Database_user>
```

```
JDBC_PASSWORD=<Database_user_password>
OTDS105_16_INSTALL_TYPE=105
```



### Example upgrading OTDS from version 16.x and later

#### ► Example 1-14: To upgrade from OTDS 16.x or later:

Open a command prompt window as administrator, for more information see “[References to external websites](#)” on page 385.

Run the OTDS-2540-WIN.msi installer from that administrator command prompt window by typing the command:

```
msiexec.exe
/i OTDS-2540-WIN.msi
/qb
/l*v otds-upgrade105.txt
INSTALLDIR=<OTDS_install_dir>
JAVAHOME=<Java_install_dir>
TOMCATSERVICENAME=<Tomcat_service_name>
ISREPLICA_TOPOLOGY=false
JDBC_CONNECTION_STRING=<Connection_string_to_database>
JDBC_USERNAME=<Database_user>
JDBC_PASSWORD=<Database_user_password>
```



## 1.6 Installing Directory Services on Linux

If you choose to upgrade a previous version of Directory Services, the installation will maintain the previous installation path. If, during installation, you neither upgrade nor change the default installation path:

*Default installation path:*

Directory Services will install to: /usr/local/OTDS.

### Choose your installation method

---

Select from one of the following:

- If you want to install interactively, follow the instructions in “[Installing OTDS on Linux interactively](#)” on page 35.
- If you want to install non-interactively, follow the instructions in “[Installing OTDS on Linux non-interactively](#)” on page 40.

---

If you are installing Directory Services version 25 on the same machine on which you have a previous version of OTDS installed:

ensure you have followed “[When upgrading and importing data from previous versions of Directory Services](#)” on page 20 and then follow the UI instructions in “[Installing OTDS on Linux interactively](#)” on page 35.

## Linux pre-requisites before installing

### Linux pre-requisites before installing:

1. Sign in to your server as the user who will install and run Directory Services. This is the user and group you created in “[Prerequisites for the installing userID](#)” on page 13.
2. Before beginning the installation, ensure the following:
  - a. The user running the installer must have execute permission to run all files in the installer.
  - b. The following variables must be specified for both the user running the installer as well as for the user running the web application service, Tomcat:
    - i. Ensure that the `JAVA_HOME` variable is pointing to the root of your Java install. Specifically, this variable should not point to the `bin` directory.
    - ii. Ensure that the `PATH` variable includes the location of the Java executable.
    - iii. Optional You can choose to specify the `CATALINA_HOME` variable to the location of Tomcat.

### 1.6.1 Installing OTDS on Linux interactively

#### To install OTDS on Linux:

1. Ensure you have installed the prerequisite software listed in “[Installation prerequisites](#)” on page 13.
2. Sign in to your server as the user who will install and run Directory Services. This is the user and group you created in “[Prerequisites for the installing userID](#)” on page 13.
3. Make sure you followed all steps in “[Linux pre-requisites before installing](#)” on page 35.
4. You obtain the Directory Services install files from OpenText My Support ([https://support.opentext.com/csm?id=kb\\_search&spa=1&query=Directory%20Services%20\(OTDS\)](https://support.opentext.com/csm?id=kb_search&spa=1&query=Directory%20Services%20(OTDS))). In the search bar, replace “Directory Services (OTDS)” with “<Version\_Number> Directory Services (OTDS)”.  
The list of install files can be found in “[Install files for Directory Services](#)” on page 25.
5. In the directory in which you placed the install file, run the command:

```
tar -xvf <install_file>
```
6. Next, run the Directory Services setup script by running the command:

```
./setup -l otds-installer.log
```

7. On the **Welcome** page, press **N** and then press **ENTER**.
  8. On the **OpenText End User License Agreement** page, read the license agreement in full. To accept it, press **A** and then press **ENTER**.
  9. On the **Installation group name** page:
    - a. If you want to accept the current value provided by the installer, press **N**, and then press **ENTER**.
    - b. If you want to change the current value, press **M** to modify, and then type the name of an *existing* group to be used for the installation ownership.

This group must exist and the **Installation user name** you enter on the next page must be a member of this group. This is the group that you created in “[Prerequisites for the installing userID](#)” on page 13.
- Press **N** and then press **ENTER**.
10. On the **Installation user name** page:
    - a. If you want to accept the current value provided by the installer, press **N**, and then press **ENTER**.
    - b. If you want to change the current value, press **M** to modify, and then type the user name of an *existing* user to be used for the installation and installation directory ownership. Unless the setup was run with elevated privilege, this must be the user who ran the setup.

This is the user that you created in “[Prerequisites for the installing userID](#)” on page 13.
- Press **N** and then press **ENTER**.
11. On the **Installation directory** page, the default installation path for the OTDS install is `/usr/local/OTDS`.
    - a. If you want to accept the default value provided by the installer, press **N**, and then press **ENTER**.
    - b. If you want to change the default value, press **M** to modify, and then type the new installation location.

Press **N** and then press **ENTER**.
- If you set the environment variables detailed in “[Linux pre-requisites before installing](#)” on page 35, the path might be listed next to “Current value”.
- Press **N** and then press **ENTER**.
- If the installer indicates that the path is incorrect, check to ensure that all environment variables you specified in [step 2.b](#) were correct.
13. On the **Hostname** page, you must type the fully qualified hostname for this installation of OTDS. Press **M** to modify, and then type the fully qualified hostname.

Press **N** and then press **ENTER**.

14. On the **Directory Services Parameters** page, do one of the following:

- a. If this installation of Directory Services is the synchronization master host, or primary installation of OTDS, press **2**, then press **N** and **ENTER**. Proceed to [step 15](#).
- b. If this installation of Directory Services is a supplementary instance, press **1**, then press **N** and **ENTER**. Do the following:
  - i. On the **Encryption Key** page, type, or copy and paste, the value of the `directory.bootstrap.CryptSecret` field found in the `otds.properties` file on the machine on which you installed your primary instance of OTDS.



**Note:** The `otds.properties` file can be found at  
`<OTDS_installdir>\config`.

Previously, the `otds.properties` file was found at  
`<OTDS_installdir>\otdswebs\WEB-INF\classes`.

Press **N** and then press **ENTER**.

ii. Proceed to [step 17](#).

15. On the **OpenText Directory Services Data Import** page, do one of the following:

- a. If you will not be importing any data, press **N** to accept the default selection, “No Import”, and then press **ENTER**. Proceed to [step 16](#).
- b. If you want to import your data from OTDS 16.4.1 or later to this new 25 installation, press **2** and then press **ENTER**.

In each of the following pages, type the required information, then press **N** and **ENTER**.

- i. In the **Encryption Key** box, type, or copy and paste, the value of the `directory.bootstrap.CryptSecret` field found in the `otds.properties` file on the machine on which the OpenDJ version from which you want to import data is installed.



**Note:** The `otds.properties` file can be found at  
`<OTDS_installdir>\config`.

Previously, the `otds.properties` file was found at  
`<OTDS_installdir>\otdswebs\WEB-INF\classes`.

- ii. In the **OpenDJ LDAP URL** box, you need to type the URL that accesses OpenDJ on the machine from which you will be importing OTDS data. This is the machine on which your previous version of OTDS was installed. Type the LDAP URL in the form:

<code>ldap://&lt;hostname&gt;:&lt;LDAP_port_number&gt;</code>
---

Where:

- <hostname> is the hostname or IP address of the machine on which OpenDJ is installed.
- <LDAP\_port\_number> is the port number on which LDAP listens on the hostname you typed above.

An example of an OpenDJ LDAP URL is:

```
ldap://Machine-A.opentext.com:389
```



**Note:** If you used the default communication port numbers when you installed OTDS, then the default LDAP communication port number on Windows is “389” and on Linux is “1389”.

- iii. In the **OpenDJ Directory Manager password** box, type the password for the userid “cn=Directory Manager”. This password, also referred to as the “bindPassword”, is usually the password that was provided for the `otadmin@otds.admin` account at installation time.

Press N and then press ENTER.

Proceed to [step 17](#).

16. On the **OpenText Directory Services Administrator Password** page type the Directory Services administrator password.

At the **confirm password** prompt, re-type the password exactly.

You can reset the “`otadmin@otds.admin`” password from the OTDS web client. See “[Resetting a user password](#)” on page 244 for more information.



**Note:** If you do not apply a strong password, the OTDS installer will warn you that you have applied a weak password and you are advised to return and type a stronger password.

A strong password must contain at least eight characters. Among those eight characters, you must have one of each of the following:

- A lowercase letter, for example “h”.
- An uppercase letter, for example “D”.
- A number, for example “5”.
- A special character, for example “!”.

An example of a strong password is: John5Doe!

You can choose to either return and type a stronger password or keep the password you initially typed.

If you change your mind about your setting, press M to modify.

After you have finished, press N and then press ENTER.

17. In the **JDBC Parameters** window, you need to inform OTDS about the location of the database that you set up in “[Installation prerequisites](#)” on page 13. You also need to provide sign-in access to the database.

**! Important**

You need to be careful when entering the information to this window. The installer cannot verify the information you provide. An error in this window will result in OTDS being unable to access your database. For more information, see [How do I change my database connection information after I have installed OTDS?](#) on page 393.

- a. In the **Database JDBC connection string** box, you will type:
  - An indicator for the type of database you set up for OTDS to use.
  - The hostname or IP address of the machine on which the database is installed.
  - The port number on which the database listens.
  - The name of the database that you set up for OTDS to use.
  - You might optionally include connection parameters.

For information about the form that this string takes, see [“Format for the Database JDBC connection string”](#) on page 18.

- b. In the **Database username** box, type the userID for a user with administrative access to the database.

The userID you type must have full permissions to the database that you created for OTDS. OpenText recommends that the userID designated as the database owner is the userID you enter in the **Database Username** field in the **JDBC Parameters** window during installation.

- c. In the **Database password** box, type the password for the user that you typed in [step 17.b.](#)



**Note:** If you enter information incorrectly to the **JDBC** fields, OTDS will not be able to access your database. If this happens, see [How do I change my database connection information after I have installed OTDS?](#) on page 393 and [“Updating the JDBC database connection password after installation”](#) on page 42.

18. On the **OpenText Directory Services Component** review page, do one of the following:
  - To move back through the previous pages in order to change any of the parameters, press **P**, and then press **ENTER**.
  - To continue the installation, press **I**, and then press **ENTER**.
19. Proceed to [“Verifying your installation”](#) on page 41.

## 1.6.2 Installing OTDS on Linux non-interactively

Before you begin, ensure you have installed the prerequisite software listed in “[Installation prerequisites](#)” on page 13.

You obtain the Directory Services install files from OpenText My Support ([https://support.opentext.com/csm?id=kb\\_search&spa=1&query=Directory%20Services%20\(OTDS\)](https://support.opentext.com/csm?id=kb_search&spa=1&query=Directory%20Services%20(OTDS))). In the search bar, replace “Directory Services (OTDS)” with “<Version\_Number> Directory Services (OTDS)”.

Make sure you followed all steps in “[Linux pre-requisites before installing](#)” on page 35.

The list of install files can be found in “[Install files for Directory Services](#)” on page 25.

### Installation parameters

The parameters to install OTDS non-interactively are:

---

#### -xrf <file>

Allows you to generate a response file.



**Note:** Cannot be used with “-rf” or “-q(b)[i|m|r|x]”.

---

#### -rf <file>

Allows you to specify the response file.



**Note:** You can also type:

`-responsefile <file_name>`

---

#### -q(b)[i|m|r|x]

Determines the user interface that will be displayed during the installation:

- -q displays no user interface.
- -qb displays a basic user interface.

The options you can pass to -q are:

- i: to represent install. Can only be used with a response file.
- m: to represent modify. Can only be used with a response file.
- r: to represent repair.
- x: to represent uninstall.

For example,

`-qbi -responsefile <file_name>`

---

#### -l <logfile\_name>.log

Specifies that the OTDS installer log file, <logfile\_name>.log, should be generated.

**-debug**

Enables script debugging messages for the installation.

For example,

```
-qbi -responsefile <file_name> -debug
```

## Installing OTDS on Linux non-interactively

### To install OTDS on Linux non-interactively:

1. Generate the response file for this installation by typing the following: `./setup -xrf otdsresponse`
2. Follow the dialogs to enter the required information to the response file. For background information on these dialogs, see “[Installing OTDS on Linux interactively](#)” on page 35.



**Note:** The passwords will not be captured in the response file. You will need to manually modify the response file to add the passwords.

3. Begin the installation by typing the following: `./setup -rf otdsresponse -qi -l otds-installer.log`
4. Proceed to “[Verifying your installation](#)” on page 41.

## 1.7 Verifying your installation

### To verify your installation has concluded successfully:

1. Ensure that your application server, Tomcat, is started.
2. To verify that OTDS has completed startup, check the `<Tomcat_installdir>\logs\otds.log` file.  
If Directory Services started successfully, you will see the line: `INFO com.opentext.otds.as.AsServlet - OTDS STARTED`
3. If the installation failed, you will need to perform manual cleanup of files before you can begin the installation again. For information about manually cleaning up the files, see “[To uninstall Directory Services from Windows](#)” on page 42 or “[To uninstall Directory Services from Linux](#)” on page 43.



**Note:** For information about the log files, see “[Log Files](#)” on page 375.

4. Proceed to “[Getting Started](#)” on page 45.

## 1.8 Updating the JDBC database connection password after installation

The JDBC database connection password is set at the time of the OTDS installation. If, after installing OTDS, you want to change this password, you will need to do the following:

### To update the JDBC database connection password:

1. Open a command window, and then change directory to the OTDS installation path:

```
cd <OTDS_installdir>\install
```

2. Type one of the following commands:

```
java -jar otds-deploy.jar -resetpassword <password>
```

Where *<password>* is the new password for the JDBC database connection.

or

```
java -jar otds-deploy.jar -setdbpassword
```

When the prompt Enter the new database connection password: is displayed, type the password. The password is not displayed.



**Note:** Running either of the above commands will update the encrypted value of jakarta.persistence.jdbc.password in the otds.properties file.

## 1.9 Uninstalling Directory Services

Select one of the following procedures, depending on your operating system:

- “[To uninstall Directory Services from Windows](#)” on page 42
- “[To uninstall Directory Services from Linux](#)” on page 43

### To uninstall Directory Services from Windows:

1. Back up the following log files to the \Temp directory:

- otdsDeploy.log
- otds-installer.log
- otds.log

If you installed OTDS and Tomcat to the default directories, you will find the following:

- The otdsDeploy.log log file is in the C:\OTDS\install directory.
- The otds-installer.log file is in the directory in which you placed, and from which you ran, the OTDS-2540-WIN.msi installer.

- The otds.log file is found in the <Tomcat\_installdir>\logs directory.
2. Stop the web application service.  
You can stop the Tomcat service by typing the command: <Tomcat\_installdir>\bin\tomcat<version>.exe stop
3. You have two options when uninstalling OTDS. Choose one of the following:
- If you do *not* want to generate an uninstaller log, open Control Panel and select **Uninstall a program**. Click to highlight **OpenText Directory Services 25**. On the menu bar, click **Uninstall**, and then click **Yes** to confirm that you want to uninstall.
  - If you want to generate an uninstaller log file, open a command prompt window as administrator, for more information see "[References to external websites](#)" on page 385. Run the OTDS-2540-WIN.msi installer from that administrator command window by typing the command:  
`msiexec.exe /x OTDS-2540-WIN.msi /l*v otds-uninstall.log`
- You are running the same installer that you used to install OTDS. Next do the following:
1. In the **Windows Installer Welcome** window, click **Next**.
  2. In the **Ready to Remove** window, click **Remove** to confirm you want to uninstall the product.
  3. In the **Completing the removal** window, click **Finish**.
4. **[Optional]** When the uninstaller completes, and if you installed Directory Services to the default directory, you can delete the C:\OTDS\ directory.  
If you installed Directory Services to a custom directory, you can search for the folder OTDS, then delete that folder.

5. Delete the OTDS files otds\*.xml and ot-authws.xml, if they have not been removed by the uninstall process.

You will find the files in the <Tomcat\_installdir>\conf\Catalina\localhost directory.

For example, delete the following files:

- ot-authws.xml
- otds-admin.xml
- otdstenant.xml
- otds-usergroup.xml
- otds-v2.xml
- otdswebs.xml

#### To uninstall Directory Services from Linux:

1. Back up the following log files to the /tmp directory:
  - otdsDeploy.log
  - otds-installer.log

- `otds.log`

If you installed OTDS and Tomcat to the default directories, you will find the following:

- The `otdsDeploy.log` log file is in the `/usr/local/OTDS/install` directory.
- The `otds-installer.log` file is in the directory in which you placed, and from which you ran, the `OTDS-2540-LNX.tar` setup file.
- The `otds.log` file is found in the `<Tomcat_installdir>/logs` directory.

2. Stop the Tomcat service.

You can stop the Tomcat service by typing the command:

`<Tomcat_installdir>/bin/shutdown.sh`

3. Open a command prompt window as the user who installed Directory Services. Run the Directory Services setup script by typing:

`./setup`

4. On the **Change, Repair or Remove Installation** page, select **Uninstall**, and then press **ENTER**.

On the confirmation page, select **Uninstall**, and then press **ENTER**.

5. **[Optional]** If you installed Directory Services to the default directory, you can delete the `/usr/local/OTDS` directory.

If you installed Directory Services to custom directories, you can search for the folder `otds` and then delete that folder.

## 1.10 Backup and Recovery

The database used for OTDS stores all data used by OpenText Directory Services, including license usage and compliance information. See “[About the OTDS database requirement](#)” on page 17. In order to backup the database, consult your database administrator or the documentation for your database vendor’s management tools. In the event of a database system failure, the backup will need to be restored in order to recover the system.

In addition, the `otds.properties` file located in the installation directory contains the encryption key used for encrypting passwords or secrets used by OTDS to connect to external systems. This file should be backed up in order to avoid having to reconfigure these passwords after a restore. If you are using a Helm deployment, this secret is provided to the release at deployment time through the `Helm values.yaml` file.

# Chapter 2

## Getting Started

This documentation describes the configuration and maintenance of OpenText Directory Services (OTDS). It describes how to use OTDS to centralize user and group identity information and manage single sign on (SSO) between OpenText applications. This section contains the following areas:

- The “[Overview](#)” on page 45 area provides an introduction to Directory Services terminology and architecture.
- The “[Setup checklists](#)” on page 56 area provides a checklist for the general steps required to configure Directory Services.
- You can find detailed information about how to begin after installation in “[Accessing Directory Services](#)” on page 58.
- “[The OTDS user interface](#)” on page 61 describes the elements of the Directory Services UI.

### 2.1 Overview

Directory Services is a repository of user and group identity information and a collection of services to manage this information for OpenText applications. OTDS contains components for identity synchronization and single sign on for all OpenText applications.

Directory Services offers synchronization and authentication features that can help your organization save time, and administrative overhead, by enabling you to maintain user information in one directory, for use by multiple OpenText applications. For example, you can base your OpenText OpenText Content Management user information on the user information already contained in your Windows domain. If your organization maintains several Enterprise Server systems, they can all use the same central user directory.

Directory Services can synchronize with your identity provider to pull user and group information from your identity provider automatically. Directory Services then pushes these users and groups to your OpenText applications automatically and incrementally. This synchronization of user and group data across OpenText applications allows Directory Services to enable single sign on and secure access to all OpenText applications.

## 2.1.1 Terminology

To understand Directory Services, you must understand the following terms. These terms are presented in the order in which you will encounter them when configuring a Directory Services server.

### Identity Provider

An identity provider is a source of user and group data that can be imported into Directory Services. To import this data into Directory Services, you must create a synchronized user partition that represents this source. Directory Services currently supports the following identity providers:

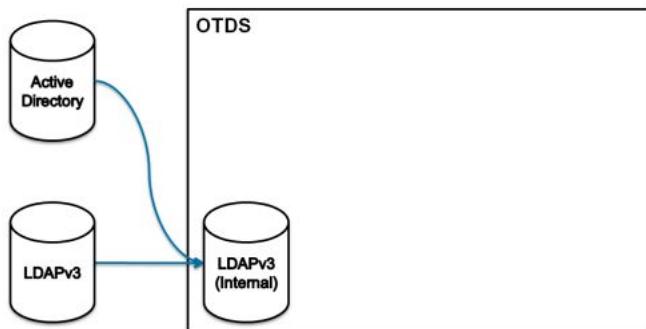
- Windows Server Active Directory. Supported Active Directory systems are:
  - Windows Server Active Directory (AD)
  - AD Global Catalog
  - Windows Server Active Directory Lightweight Directory Services (AD LDS)
- Lightweight Directory Access Protocol, LDAP. Supported LDAP systems are:
  - Oracle Directory Server Enterprise Edition
  - Oracle Internet Directory
  - IBM Lotus Domino
  - IBM Tivoli Directory Server
  - Novell eDirectory
  - Apache Directory Server
  - Windows Server Active Directory Lightweight Directory Services (AD LDS)



**Note:** For more information, see *OpenText Directory Services - Installation and Administration Guide* (OTDS-IWC) and the **OTDS Release Notes**. You can find links to these documents in “[OTDS Documentation](#)” on page 381.

Directory Services supports synchronization of user and group information from identity providers into a local Directory Services LDAP Directory Server. This will be a synchronization of information based on monitoring for changes in attributes or objects, or it will be a scheduled synchronization of all information. For more information, see “[Synchronization types](#)” on page 84.

Figure 2-1 shows identity providers being imported into a local Directory Services LDAP Directory Server. These identity providers will be represented by two or more synchronized user partitions.



**Figure 2-1: Identity providers**

### Synchronization

The Enterprise Sync component of Directory Services is responsible for gathering user and group data from your identity provider and ensuring it is imported into your synchronized user partition in Directory Services.

Synchronization of user and group data changes in the associated identity provider of a synchronized user partition is provided automatically by Directory Services. Changes to user and group information are delivered automatically unless they are paused by the administrator. Periodically, an administrator might want to temporarily pause updates from an identity provider. For example, if major changes were being made in the identity provider, an administrator might pause regular updates until the changes were completed.

Synchronization is one-way. There is no delivery of changes to user or group information from Directory Services back to the identity provider.

**! Important**

The **Restart Enterprise Sync** button, available on the main **Partitions** page, reboots the entire Enterprise Sync component, simulating the process that occurs when restarting Apache Tomcat.

It is used for troubleshooting when encountering issues. OpenText recommends that you do not perform an Enterprise Sync restart unless directed by OpenText technical support.

### Resources

Resources represent multi-user systems, or applications, that users can access. A resource may also maintain its own internal users and groups. Directory Services can be configured to push user and group information from the identity provider to the resource. Each resource in Directory Services is represented by a unique name and resource identifier. When you create a resource, Directory Services automatically creates an access role allowing the user who created the resource to access it. Examples of resources include “OpenText OpenText Content Management” and “OpenText Media Management”. For more information, see “[System Status](#)” on page 371 and “[Resources](#)” on page 173.

Directory Services supports the following types of resources:

- **Synchronized resources**

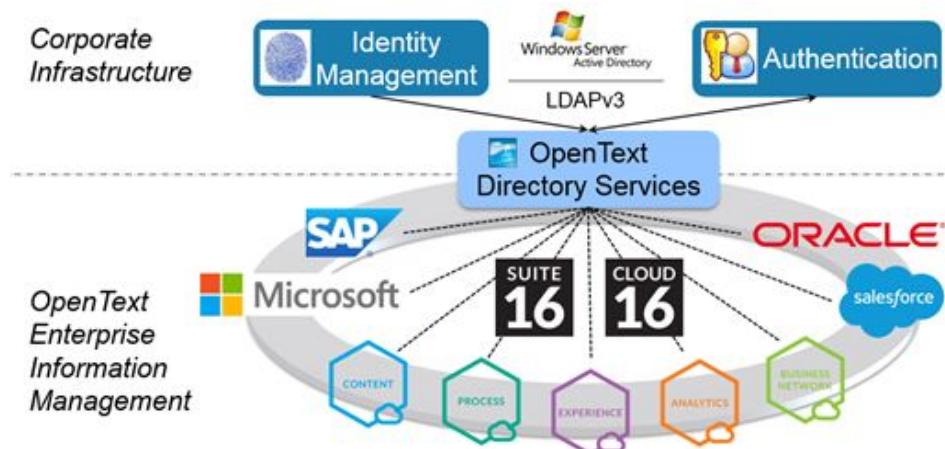
If a resource is synchronized, it means that the users and groups in the access roles assigned to the resource are added to the internal users and groups maintained by the application for which the resource is created.

Synchronized resources require that a connection to the application, for example OpenText OpenText Content Management, be established. This means that you can only create a synchronized resource after the application has been installed.

- **Non-synchronized resources**

Non-synchronized resources can still use Directory Services authentication for single sign on. Non-synchronized resources are created for applications that do not maintain an internal user and group directory that must be synchronized with the users and groups from Directory Services. You can create non-synchronized resources even if the applications for which they are intended are not yet installed.

**Figure 2-2** shows the centralization of user and group authentication for all ECM Suite applications. ECM Suite applications are represented by resources in Directory Services.



**Figure 2-2: Resources**

### Access Roles

Access roles are used to control which resources users can access. You can assign access roles to users, groups, organizational units, or user partitions. An access role is a way of identifying users who have the same sign in privileges. For example, you might create an Access to OpenText Content Management access role to give your development group sign in privileges to OpenText Content Management.

When you have created an access role, you can add members to it. Members can be individual users, whole groups, or whole partitions. An access role consists of

members that are connected to one or more resources. All users and groups in an access role may be pushed to all the connected resources.

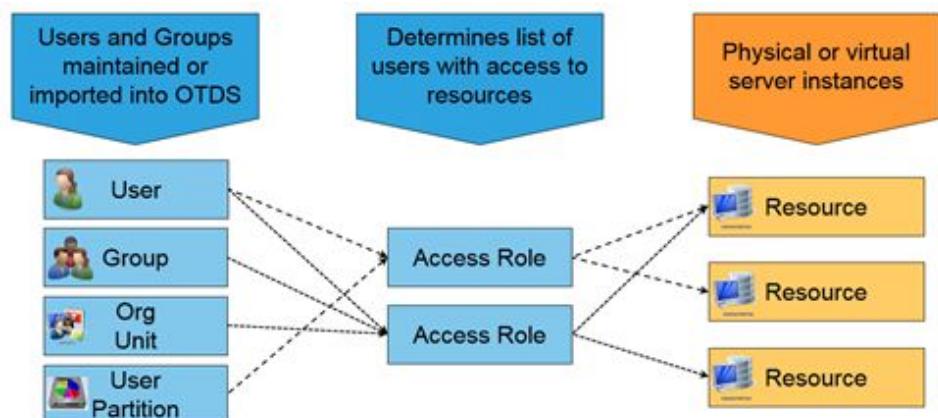
After you have created all your access roles and added members to each access role, you can add the access role to your resources. This allows users of that access role to sign in to these resources. Users and groups of that access role may be pushed to the resource.

For any particular user, single sign on is enabled between all resources that are connected to all that user's access roles. For more information, see “[Access Roles](#)” on page 229.



**Note:** Access roles should not be confused with the roles defined in an application. Directory Services does not define which functionality of an application a user is allowed to use, just if the user is granted access to it.

Figure 2-3 shows how access roles are used to control which resources users can access.



**Figure 2-3: Access roles**

### Authentication and Single Sign On

OTDS Authentication Services are a set of services and components that provide authentication and single sign on (SSO) services. A user is required to sign in only once per session. After that, the single sign on mechanism ensures that the same user is not asked to sign in to any subsequent OpenText applications that use Directory Services, when those applications are launched or visited. The authentication services provide a level of confidence that the user trying to access the system is authentic.

A user in Directory Services may have zero or one authentication providers. If a user does not possess an identity provider, then Directory Services becomes the authentication provider. An example of such a user may be a hired consultant who does not possess sign in rights to your identity provider's domain. In general, if the person is known to be a member of an organization's internal domain, authentication should be provided by that domain. If the person is not

a member of any internal domain, Directory Services assumes responsibility for authenticating that person.



### Notes

- Authorization to perform tasks in an application is provided by that application. Directory Services only provides authentication services allowing users to sign in to an application.
- A user can sign in using their <user\_name>, a fully qualified name in the form <user\_name>@<user\_partition>, or a user name in the form <domain>/<user\_name>. If multiple users exist with the same <user\_name> across multiple partitions, OTDS will attempt to resolve the <user\_name>. If this is not possible, the `directory-access.log` will contain a message to indicate that multiple identities for the given <user\_name> were found and the user will see an invalid credentials message.

For more information, see “[Authentication Handlers](#)” on page 137, “[Single sign on scenarios](#)” on page 348 and “[directory-access.log](#)” on page 376.

---

## Partitions

Partitions are self-contained copies of user information that allow you to organize your users into a structured hierarchy of users, groups and organizational units. A user partition in Directory Services is represented by a unique name. Content can be imported and synchronized with Active Directory (AD) and / or Lightweight Directory Access Protocol (LDAP) and can be managed fully within OTDS. OTDS supports multiple, concurrent user partitions. For more information, see “[User partitions](#)” on page 65, “[System Status](#)” on page 371 and “[User partitions](#)” on page 65.

Directory Services provides the following types of partitions:

---

### Synchronized user partition

Synchronized user partitions are synchronized with an identity provider, such as AD or LDAP. A synchronized user partition contains users, groups and organizational units that are imported from the identity provider when the user partition is created. A synchronized user partition can be automatically kept up-to-date with its source directory. Users who are imported from an identity provider into a synchronized user partition are authenticated by the identity provider.

---

### Non-synchronized user partition

Non-synchronized user partitions are created and maintained manually. Unlike a synchronized user partition, a non-synchronized user partition does not have an identity provider from which its users and groups are imported. Users and groups in a non-synchronized user partition are maintained entirely through the OTDS web client. Users who are created and maintained manually in a non-synchronized user partition are authenticated by Directory Services. Configurable password policies are available for non-synchronized user partitions.

### Non-synchronized administrative user partition

The non-synchronized administrative user partition, `otds.admin`, is installed by default when a Directory Services server is installed. This special non-synchronized user partition cannot be deleted or disabled. The predefined administrative user, `otadmin@otds.admin`, which is created when Directory Services is installed, is a member of the `otadmins` group in the `otds.admin` user partition. The `otadmins` group is automatically given access to any resource created by the `otadmin` user.

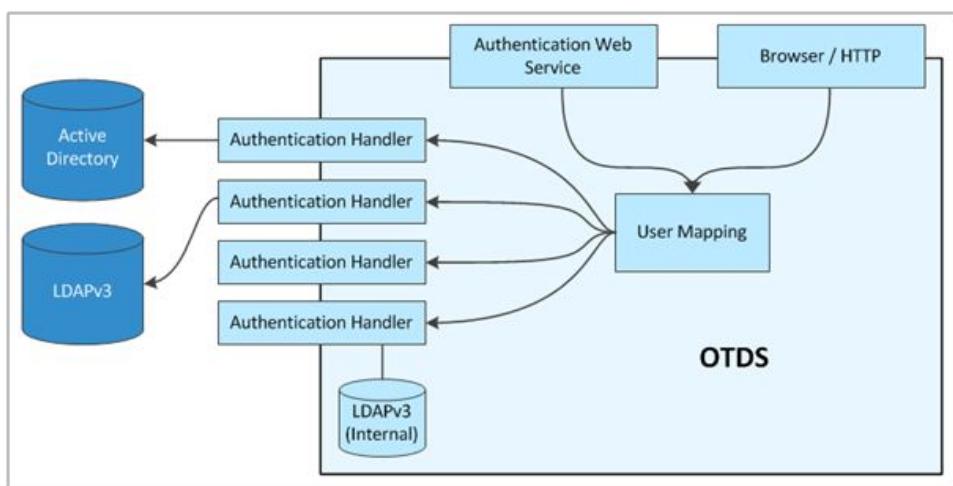
### Authentication Handlers

Because users will need to authenticate through a variety of mechanisms, no single authentication handler can be applied for any single user in all circumstances. For example, a user might use Kerberos from the desktop, but the next day may use credentials-based authentication through a Web site, and the next may use SAP token-based authentication from within a SAP portal.

Directory Services provides a hierarchy of authentication handlers that are sequentially evaluated until a definitive authentication result is reported by one of them. Global authentication handlers are automatically created by Directory Services. A local credentials-based authentication handler is provided when a user partition is created. Additional authentication handlers can also be created and applied locally to individual user partitions or globally to all user partitions. You can also prioritize the use of each authentication handler associated with a user partition.

For any known user, local authentication handlers will be tried before the global authentication handlers are invoked. When the user is not known, Directory Services will try all enabled authentication handlers in prioritized sequence. For more information, see “[Authentication Handlers](#)” on page 137.

[Figure 2-4](#) shows how multiple authentication handlers can be used to authenticate users in different sign in scenarios.

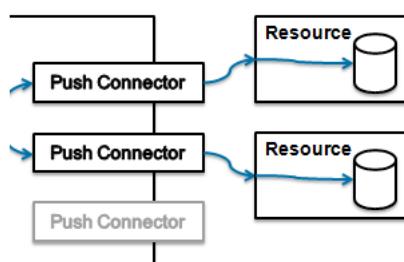


**Figure 2-4: Directory Services authentication**

### OTDS Connectors

OTDS connectors, or push connectors, are components of Directory Services that update user and group data in resources so that they remain consistent with the internal user data in Directory Services. Every synchronized resource has a specific connector that allows it to communicate with Directory Services.

Figure 2-5 shows the plugable push connector used by every synchronized resource in Directory Services.



**Figure 2-5: Push connectors**

---

### OTDS Push Layer

The OTDS push layer is a service that is responsible for ensuring that the user and group data in deployed resources is consistent with the user and group data in the Directory Services server. To do this, it accepts change notifications from the Directory Services server and ensures that all such changes are propagated to resources using the OTDS connectors.

---

### Consolidation

Directory Services uses various mechanisms to keep user and group data maintained in resources, current with data maintained in the identity provider, and in Directory Services itself. However, Directory Services cannot guarantee that such data is always up-to-date. For example:

- If a resource has a failure, and the backup brought online to replace it has old data.
- If a resource encounters an unknown transient error, or has been unreachable for some time, Directory Services may be prevented from delivering update messages.

Directory Services provides functionality for resynchronizing user and group data from the identity provider to the synchronized user partition and directly to your resources when such failures have occurred or have been suspected of occurring. This is known as consolidation. Consolidation performs the following two tasks:

- It ensures user and group data in synchronized resources matches the data in Directory Services.
- It also ensures user and group data in Directory Services matches the data in the identity provider.

---

For more information, see “[Consolidating users and groups in Partitions](#)” on page 128.

### Users, Groups and Organizational Units

Directory Services maintains an internal data schema for managing user and group information. Attributes of users and groups are mapped to their source in the identity provider if they are members of a synchronized user partition.

Attributes of users and groups are entered and maintained internally for users and groups that are members of a non-synchronized user partition.



**Note:** DN refers to the Distinguished Name of an entity. Every entity in OTDS has a distinguished name (DN). The DN is the name that uniquely identifies that entity in OTDS.

An organizational unit is similar to a folder and allows you to organize users and groups in a hierarchical structure. When an organizational unit is added as a member to an access role, only its users will be added to the attached resources. If you want to add groups to your resources, you will need to add these as members of your access role. When you add a group to an access role, all its member users and groups are allocated to the attached resources.

For more information, see “[Users and Groups](#)” on page 235.

### Impersonation

Impersonation allows a user of one resource to appear as a different user on a target resource and to potentially acquire all the privileges of the impersonated user in that resource.



#### Important

Impersonation against any resource should not be enabled unless your specific deployment requires it. The resource's documentation will specify whether impersonation is required.

For more information, see “[Editing impersonation settings](#)” on page 225.

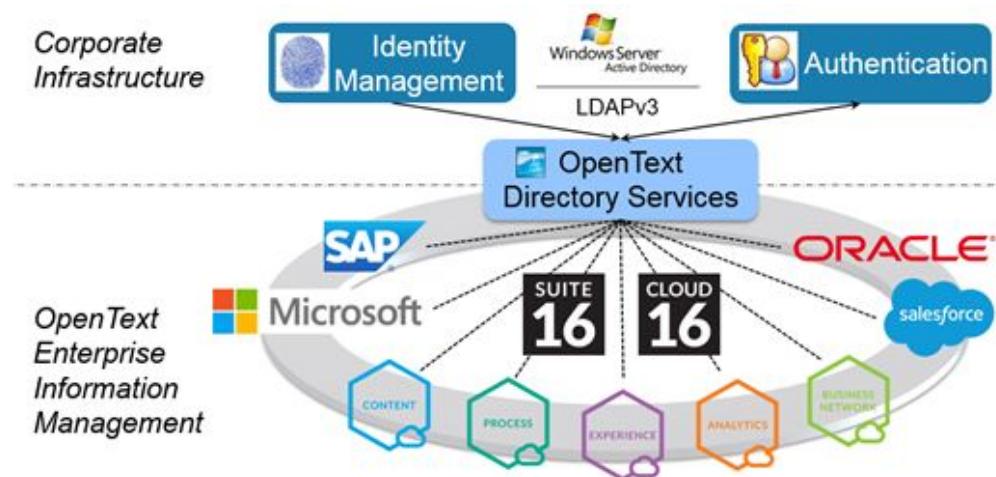
### Jobs

The **Job** tab displays a list of jobs, in progress and completed, in the Directory Services job queue. Each event records errors, warnings, and information messages to track the progress of the event. For more information, see “[Jobs](#)” on page 363.

## 2.1.2 Architecture

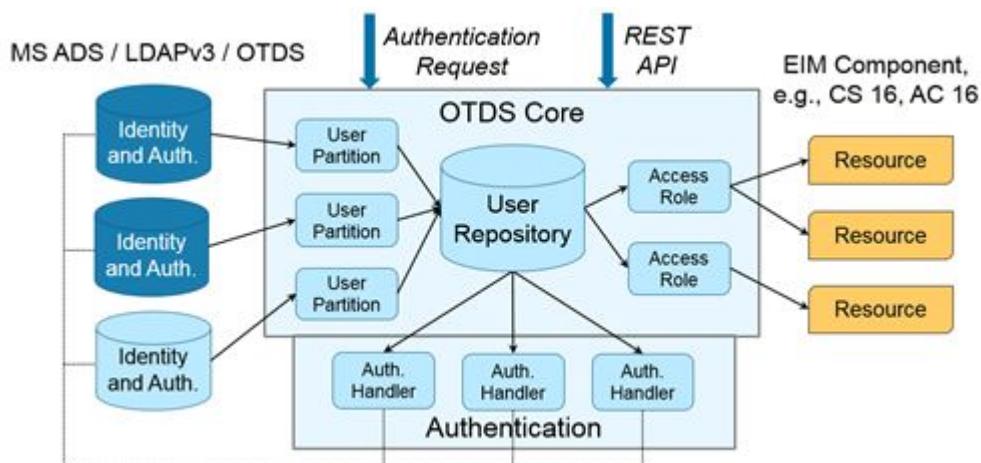
In a distributed environment where integrated OpenText applications are required to support single sign on, applications must connect to one instance of Directory Services to avoid point-to-point complexity. A single Directory Services server is installed and configured as the central authentication point for all other OpenText applications.

**Figure 2-6** shows an overview of Directory Services identity management and authentication in the OpenText ECM Suite.



**Figure 2-6: Directory Services common identity services**

**Figure 2-7** shows an overview of all Directory Services concepts together.



**Figure 2-7: Directory Services conceptual overview**

The mappings from Active Directory / LDAP to Directory Services are configured as part of the partition configuration. For more information, see “[AD/LDAP user and group ID attributes](#)” on page 86 and “[The OTDS unique ID](#)” on page 72.

The mappings from Directory Services to resources are configured through the NAME attribute mapping of users and groups in the resource configuration. For more information, see “[Using resource attribute mappings](#)” on page 182.

### 2.1.3 Typical scenario

In a typical scenario, a single Directory Services server is installed and configured as the central authentication point for all other OpenText applications. Each application using Directory Services authentication must have a resource representing itself created in the OTDS web client.

When creating a Directory Services server, the installation will create a non-synchronized administrative partition, `otds.admin`, containing predefined default groups:

Default Group ID	Description
<code>otadmins</code>	OpenText administrators.
<code>otdsadmins</code>	OpenText Directory Services administrators with full privileges.
<code>otdsreadonlyadmins</code>	OpenText Directory Services read-only administrators. Members of this group possess a sub-set of privileges of the members of <code>otadmins</code> group.
<code>otdsbusinessadmins</code>	OpenText Directory Services business administrators. Members of this group possess a sub-set of privileges of the members of <code>otadmins</code> group.   <b>Note:</b> If you have upgraded OTDS from a previous version, the <code>otdsbusinessadmins</code> group may not exist. In that case, and if you want to use its functionality, you must manually create this group. Create a group named <code>otdsbusinessadmins</code> in the <code>otds.admin</code> partition. There are no special requirements for the group.

For more information, see “[The Directory Services default administrative groups](#)” on page 249.

## 2.2 Setup checklists

---

### Basic Directory Services server

You can use the following checklist to configure a basic installation of Directory Services for demonstration:

Action	Completed
Install Java. For information, see “ <a href="#">Configuring Tomcat for OTDS</a> ” on page 14.	
Install Apache Tomcat. Start Tomcat and watch for startup success in the logs. For information, see “ <a href="#">Configuring Tomcat for OTDS</a> ” on page 14.	

Action	Completed
Create a database for OTDS to use.  For information, see “ <a href="#">Installation prerequisites</a> ” on page 13.	
Install OpenText Directory Services.  For more information, see the “ <a href="#">Install files for Directory Services</a> ” on page 25.	
Sign in to your server using the OTDS web client.  For more information, see “ <a href="#">Accessing Directory Services</a> ” on page 58.	
Optionally, specify the password settings for all users in an OTDS non-synchronized user partition.  For more information, see “ <a href="#">Defining a global password policy for all non-synchronized user partitions</a> ” on page 127.	
Optionally, specify the audit reporting settings and notification settings for OTDS.  For more information, see “ <a href="#">To configure audit/reporting settings</a> ” on page 319 and “ <a href="#">To configure notifications settings</a> ” on page 322.	
Define a user partition. It can be synchronized or non-synchronized.  For more information, see “ <a href="#">User partitions</a> ” on page 65.	
Configure an access role for your new user partition.  For more information, see “ <a href="#">Access Roles</a> ” on page 229.	

### Directory Services integrated with OpenText Content Management

You can use the following checklist to configure a basic installation of Directory Services integrated with OpenText Content Management:

Action	Completed
Install all products listed in <a href="#">Basic Directory Services server</a> on page 56.	
Install OpenText OpenText Content Management. During the installation of OpenText Content Management, ensure that you also install OpenText Content Web Services without a resource identifier.  For more information, see the <i>OpenText Content Management Installation Guide</i> <i>OpenText Content Management - Installation Guide (LLESCOR-IGD)</i> and “ <a href="#">OTDS Documentation</a> ” on page 381.	
Start the OTDS web client and sign in to your server to see the nodes: <b>OpenText Content Management</b> and <b>Directory Services</b> .  For more information, see “ <a href="#">Accessing Directory Services</a> ” on page 58.	
Define a synchronized OpenText Content Management resource.  For more information, see “ <a href="#">Creating a synchronized resource</a> ” on page 206.	

Action	Completed
Optionally, configure the enable password reset option in OTDS. Password reset is enabled by default, however, it requires configuration. For more information, see <a href="#">Enable Password Reset on page 299</a> .	
Optionally, specify the audit reporting settings and notification settings for OTDS.  For more information, see <a href="#">“To configure audit/reporting settings” on page 319</a> and <a href="#">“To configure notifications settings” on page 322</a> .	
Create a non-synchronized user partition that will store the users and groups either created in OpenText Content Management or migrated from the OpenText Content Management database.  For more information, see <a href="#">“Creating a non-synchronized user partition” on page 106</a> .	
Configure an access role for your new user partition to access your OpenText Content Management resource.  For more information, see <a href="#">“Access Roles” on page 229</a> .	
If your version of OTDS is installed on a different system than your installation of OpenText Content Management, you will need to add your OpenText Content Management URL as a trusted site in OTDS. For more information, see <a href="#">“Trusted Sites” on page 327</a> .	
Sign in to OpenText Content Management as admin. Configure OpenText Content Management in the <b>Directory Services Integration Administration</b> area of the <b>OpenText Content Management Administration</b> page.  For more information, see <a href="#">“Configuring Directory Services integration administration in OpenText Content Management” on page 219</a> .	
Restart the OpenText Content Management admin servers.	

## 2.3 Accessing Directory Services

### To access Directory Services:

1. In a web browser, open `http://<fully_qualified_domain_name_of_server>:<web_application_server_port_number>/otds-admin/`
  - Examples of `<fully_qualified_domain_name_of_server>` include:
    - my\_machine.opentext.net
    - 10.16.12.120
  - If you installed a stand-alone version of Directory Services, and you are using Tomcat, your default `<web_application_server_port_number>` is 8080.
2. On the sign in page, do the following:

- a. In the **User name** box, type:  
otadmin@otds.admin
- b. In the **Password** box, type the password you selected during the installation of OTDS.
- c. Click **Sign In**.

### 2.3.1 If you imported data from OTDS 16.x or 20.x to 25.4.x

When you installed OTDS 25.4.x, and if you imported data from a previous installation, some of the encrypted passwords from your previous installation might not have been migrated. Look for warnings in the `otds.log` file regarding passwords that were not migrated. You will need to manually add those passwords to 25.4.x. For more information, see “[otds.log](#)” on page 375.

**To manually add synchronized partition or synchronized resource passwords:**

1. In the OTDS administration page, click **Partitions**.
2. On the **Partitions** page, from the **Actions** menu of the first synchronized partition, select **Properties**.
  - a. On the `<partition_name>` page, select the **Authentication** tab.
  - b. On the **Authentication** page, enter the password for this synchronized partition to connect to the identity provider, and then click **Save**.
  - c. Return to [step 1](#) and complete these steps for each synchronized partition. When you have completed the steps for each synchronized partition, proceed to the next step.
3. In the OTDS administration page, click **Resources**.
4. On the **Resources** page, from the **Actions** menu of the first resource, select **Properties**.
  - a. On the `<resource_name>` page, select the **Connection Information** tab.
  - b. On the **Connection Information** page, enter the password for this synchronized resource.



**Note:** For a OpenText Content Management resource, you might have chosen to impersonate the specified user, in which case the account password is not required. For more information, see “[Connection parameters for OpenText Content Management resources](#)” on page 194.

- c. Click **Save**.
- d. Return to [step 3](#) and complete these steps for each synchronized resource.

### 2.3.2 Setting up an OTDS server for synchronization and authentication

To set up an OTDS server for user synchronization and authentication:

1. This procedure assumes you have installed Directory Services and signed in with the `otadmin@otds.admin` userid.  
For more information, see “[Installing OpenText Directory Services Version 25](#)” on page 13 and “[Accessing Directory Services](#)” on page 58. The most current versions of supported environments can be found in the *OpenText Directory Services Release Notes*. For more information, see “[OTDS Documentation](#)” on page 381.
2. Create a basic synchronized user partition to populate your Directory Services server with users and groups from your identity provider. For more information, see “[Defining a synchronized user partition](#)” on page 74. Alternatively, define your users and groups manually in a non-synchronized user partition. For more information, see “[Defining a non-synchronized user partition](#)” on page 102.
3. Define your synchronized resources and record their resource identifiers. You should define resources for *all* applications that will use Directory Services for authentication. Currently, the following applications *require* synchronized resources:

---

#### OpenText Content Management

For detailed information, see “[Configuring a synchronized resource for OpenText Content Management](#)” on page 193. You will also need Content Web Services installed before creating a resource for OpenText Content Management. For information on installing Content Web Services, see *OpenText Content Management Installation Guide*. For more information, see “[OTDS Documentation](#)” on page 381.

---

#### Enterprise Process Services

For detailed information, see “[Configuring a synchronized resource for Enterprise Process Services](#)” on page 205.



**Note:** Enterprise Process Services requires that you first create a non-synchronized resource in order to define a resource identifier. This resource identifier is used when installing Enterprise Process Services. You can then return to this resource to change it to a synchronized resource that points to your newly installed Enterprise Process Services server.

---

After you have defined resources for each additional application that will use Directory Services authentication, you need to record their resource identifiers. For detailed information, see “[Resources](#)” on page 173.

4. Complete the two-step authentication activation process. The first step of activation is triggered when the resource is created. However, authentication is

not activated until the resource completes the activation integration process. For detailed information, see “[Resources](#)” on page 173.

5. Define your access roles to control who can access your resources. You can create different access roles to restrict which users are allowed to sign in to the applications that use Directory Services. For more information, see “[Access Roles](#)” on page 229.

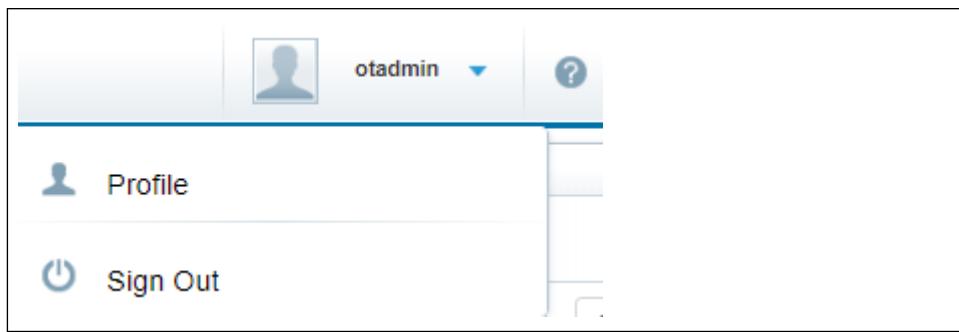
Assign access roles to the resources that connect Directory Services to the applications that use its services. For more information, see “[Editing access roles for your resource](#)” on page 225.

6. Configure Directory Services to listen for changes to users, groups, and organizational units in your identity provider. Your basic synchronized user partition will automatically be populated when it is created. However, you can manage this synchronization based on your organization's needs. You can also manage the delivery of updates in Directory Services to your synchronized resources. For more information, see “[Importing users and groups](#)” on page 86.

## 2.4 The OTDS user interface

The elements of the OTDS web client are as follows:

1. **Header**

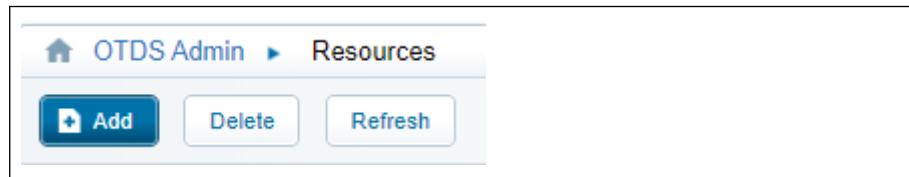


The header runs across the top of the OTDS web client page. The header contains the name of the product, “OpenText™ Directory Services”, and the following menus:

- a. The <userid> menu that contains:
  - A **Profile** menu item to allow you to view your userid profile.
  - A **Sign Out** menu item to allow you to sign out of the OTDS web client.
- b. A ? button that brings up the OTDS web client online help.
2. **Breadcrumb Trail, Button Bar, and Home button**

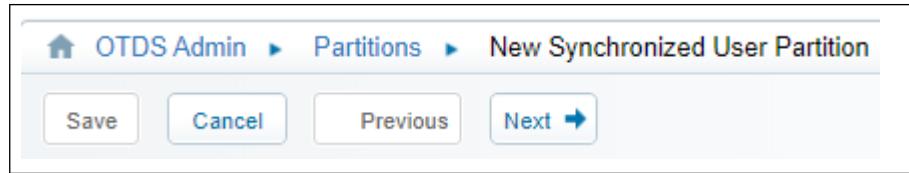
These appear below the header:

a. **Breadcrumb Trail**



In this graphic, the breadcrumb trail shows that the user is accessing the **Resources** page of Directory Services. In the graphic below, the breadcrumb trail shows that the user is accessing the **New Synchronized User Partition** assistant of the **Partitions** page of Directory Services.

b. **Button Bar**



As you can see from both the breadcrumb trail graphic and the button bar graphic, the buttons available on the button bar change depending on the administration page you are accessing.

c. **Home button**



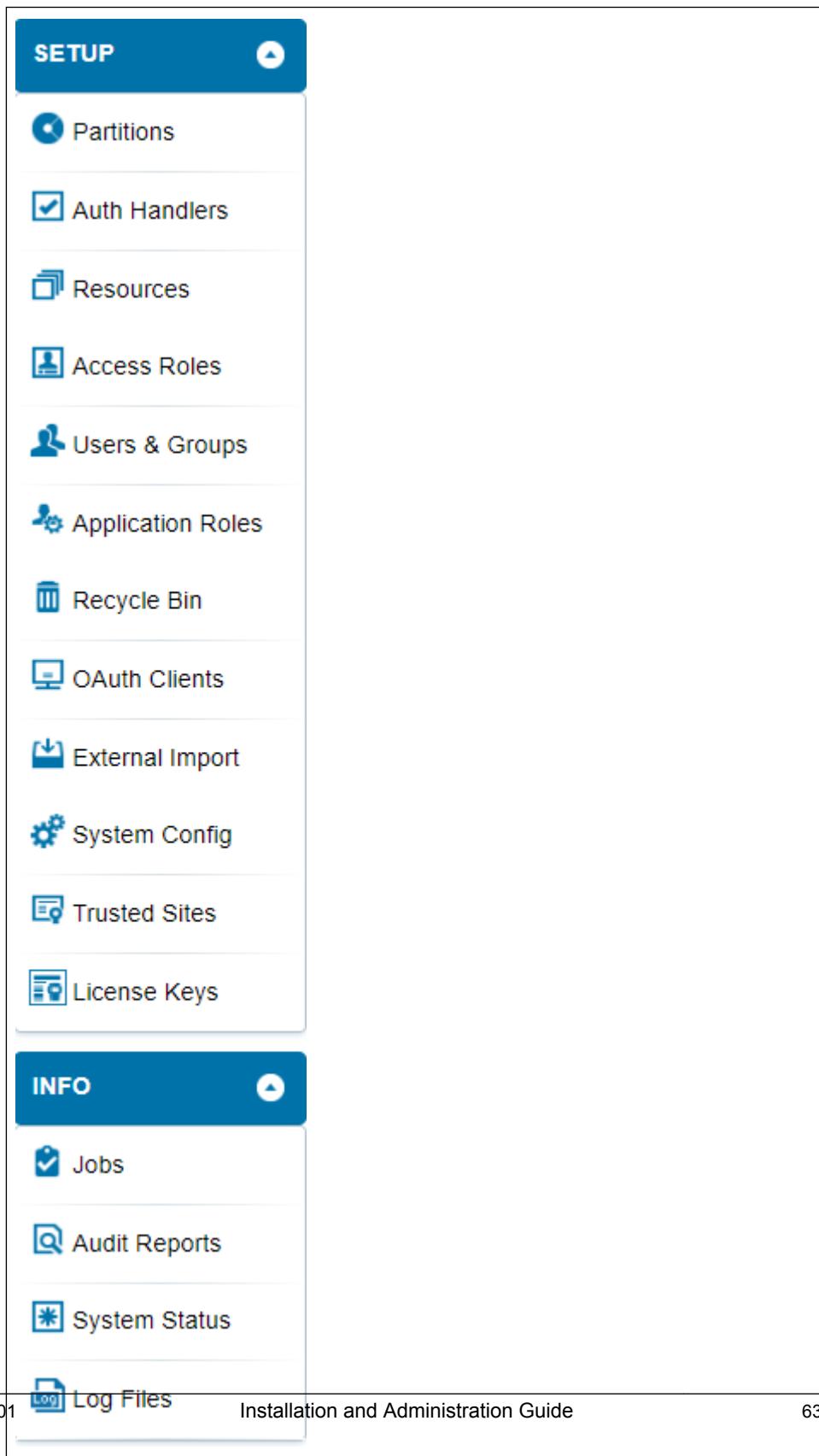
Clicking the OTDS **home** button takes you back to the main page.

3. **Action Menus**



The menu options available on the **Actions** menu change depending on the administration page you are accessing.

#### 4. Menu Bar



The menu bar appears at the left-hand side of the OTDS web client page. In addition to the menu items, each area has an **UP ARROW** that, when clicked, will roll up the menu items and hide them from view. The button now changes to a **DOWN ARROW**. Click the **DOWN ARROW** to display the menu items.



**Note:** The **External Import** menu item will not appear in the **Setup** menu until it has been enabled. For more information, see “[External Import](#)” on page 281.

The following menus appear on the menu bar:

a. The **Setup** menu contains the following areas:

- “User partitions” on page 65
- “Authentication Handlers” on page 137
- “Resources” on page 173
- “Access Roles” on page 229
- “Users and Groups” on page 235
- “Application Roles” on page 261
- “Recycle Bin” on page 269
- “OAuth Clients” on page 275
- “External Import” on page 281
- “System Config” on page 287
- “Trusted Sites” on page 327
- “License Keys” on page 331

b. The **Info** menu contains the following areas:

- “Jobs” on page 363
- “Audit Reports” on page 367
- “System Status” on page 371
- “Log Files” on page 375

## 5. Search area

Each administration page also contains a search area to allow you to filter the displayed results. In the search area, which appears under the button bar, you can choose to search by **Starts with** or **Contains**. Select one of the radio buttons to define your search filter and then type your search query in the associated box. Click **Search** to apply this search filter.

You can optionally choose to define the number of results that will display per page. The default is 25 results per page. If the search produces multiple pages of results, click **Previous** and **Next** to page through the results.

# Chapter 3

## User partitions

This section describes creating synchronized and non-synchronized user partitions, importing or creating users and groups in user partitions, and consolidating user and group data for all user partitions. The **Partitions** page displays an alphabetical list of all partitions. The **Partitions** page displays:

- the number of users and groups who are members of each partition
- the number of recycled users and recycled groups who are members of each partition
- whether the partition is enabled or not
- the **Actions** menu for each partition

### Important

The **Restart Enterprise Sync** button, available on the main **Partitions** page, reboots the entire Enterprise Sync component, simulating the process that occurs when restarting Tomcat.

It is used for troubleshooting when encountering issues. OpenText recommends that you do not perform an Enterprise Sync restart unless directed by OpenText technical support.



**Note:** For information about the **Global Settings** button on the button bar of the **Partitions** page, see “[Defining a global password policy for all non-synchronized user partitions](#)” on page 125 and “[Configuring two-factor authentication](#)” on page 237.

A user in Directory Services has one Directory Services identity that maps their user accounts across all resources. User information in Directory Services may be provided by mapping to an identity provider in a synchronized user partition or by entering data manually in a non-synchronized user partition.

A user partition is a logical grouping of users. A synchronized user partition is synchronized with a specific identity provider when it is created. You can create multiple user partitions that point to the same identity provider, choosing different users and groups for each user partition, or you can create one simple partition that encompasses all users and groups in an identity provider. A non-synchronized user partition lets you manually create and maintain users and groups. There is no limit to the number of user partitions you can create.

For a complete list of supported identity providers, see the *OpenText Directory Services Release Notes*. For more information, see “[OTDS Documentation](#)” on page 381.

## Synchronized User Partitions status indicated by color

Synchronized User Partitions are color-coded to indicate their status. For example, a synchronized user partition can appear with a background color to indicate that it requires the importing or consolidation of users and groups:

- **White:** no import or consolidation is required.
- **Green:** an import or a consolidation is in progress.
- **Yellow:** an import or a consolidation is required. For more information, see “[Importing users and groups](#)” on page 98 or “[Consolidating changes to users, groups, organizational units, and partitions](#)” on page 129.
- **Red:** an import or a consolidation failed.

### 3.1 User partitions Actions menu options, buttons, and column headings

On the main **Partitions** page, each partition has associated **Actions** menu options, buttons, and column headings. They depend on whether you are dealing with a synchronized or a non-synchronized partition. The following are quick links to the procedures associated with each:

#### User partitions Actions menu options

Actions menu option	Associated Procedure
Properties (synchronized partition only)	<a href="#">“Editing a synchronized user partition” on page 97</a>
Duplicate Partition (synchronized partition only)	<a href="#">“Duplicating a synchronized user partition” on page 100</a>
Edit Administrators (non-synchronized partition only)	<a href="#">“Editing administrators of groups in a non-synchronized user partition” on page 119</a>
View Members	The <b>View Members</b> menu option is used in several procedures related to editing groups. For example, see “ <a href="#">Consolidating changes to users, groups, organizational units, and partitions</a> ” on page 129.
Restart (synchronized partition only)	<a href="#">“Restarting a synchronized user partition” on page 99</a>
Import Users and Groups (synchronized partition only)	<a href="#">“Importing users and groups” on page 98</a>
Password Policy (non-synchronized partition only)	<a href="#">“Password policy for non-synchronized user partitions” on page 125</a>
Partition Restrictions (non-synchronized partition only)	<a href="#">“Configuring partition restrictions” on page 114</a>

Actions menu option	Associated Procedure
Consolidate	<p>“Consolidating changes to users, groups, organizational units, and partitions” on page 129</p> <p>The consolidate option is not available on a synchronized partition until an “Importing users and groups” on page 98 operation is run.</p>
Two Factor Auth Settings	“Enabling two-factor authentication” on page 245
Partition Attributes	“Creating system or custom attributes for one partition” on page 134
Enable/Disable Partition	You can select either <b>Enable</b> or <b>Disable</b> from any partition's <b>Actions</b> menu. The entry under the <b>Status</b> column will display the partition's enabled status.
Allocate to License	“Allocate to license” on page 247

## User partitions buttons

Button	Associated Procedure
Add	“Creating a synchronized user partition” on page 87 and “Creating a non-synchronized user partition” on page 106
Delete	“Deleting a synchronized user partition” on page 101 and “Deleting a non-synchronized user partition” on page 108
Refresh	Use the <b>Refresh</b> button to verify if OTDS has completed an action. For example, after deleting or after consolidating.
Restart Enterprise Sync	This button will reboot the entire Enterprise Sync component. OpenText recommends that you do not perform an Enterprise Sync restart unless directed by OpenText technical support.
Global Settings	“Defining a global password policy for all non-synchronized user partitions” on page 125 and “Configuring two-factor authentication” on page 237
Toggle Columns	<p>The <b>Toggle Columns</b> button will change the default view of the main <b>Partitions</b> page. The three toggle options are:</p> <ul style="list-style-type: none"> <li>• <b>Full view</b>, the default, displays the Name, Users, Groups, Recycled Users, Recycled Groups, Status, Description, and Actions columns.</li> <li>• <b>Partial view</b> removes both recycled columns. It displays Name, Users, Groups, Status, Description, and Actions columns.</li> <li>• <b>Limited view</b> displays the Name, Status, Description, and Actions columns.</li> </ul>
Help	Opens context-sensitive help for the page you are currently using.

### User partitions column headings

Column name	Description
Name	The name you provided when you created the partition.
Users	The number of users assigned to the partition.
Groups	The number of groups assigned to the partition.
Roles	The number of roles assigned to the partition.
Status	Displays either <b>disabled</b> or <b>enabled</b> on a synchronized partition to indicate if the partition is enabled or disabled. You can choose enable or disable from any partition's <b>Actions</b> menu.
Connection	Displays either <b>healthy</b> or <b>unhealthy</b> on a synchronized partition to indicate the status of the last connection attempt made by OTDS.  It is only updated when a connection attempt fails or succeeds. If there is no synchronization activity through incremental sync, scheduled sync, or consolidation, then the status will not be updated.   <b>Note:</b> The connection status is not an indicator of any errors or warnings during synchronization. It is strictly an indicator of the health of the network connection to the server.
Description	If, when you created your resource, you typed an entry in the optional <b>Description</b> box, that text is displayed here.
Actions	For information about the available actions, see " <a href="#">User partitions Actions menu options</a> " on page 66.

## 3.2 User partitions and the synchronization master host

To create, modify and/or delete a synchronized user partition, or to consolidate any user partition, the synchronization master host must be available. The OTDS web client may be connected to any of the replica servers, but the synchronization master host must be reachable.

### 3.3 OTDS Two-Factor Authentication

OTDS Two-Factor Authentication has been implemented using the Time-Based One-Time Password Algorithm (TOTP), RFC6238.

The administrator can choose to apply two-factor authentication at the user, group, organizational unit, or partition level. For more information, see “[Configuring two-factor authentication](#)” on page 237.

See also “[Enabling two-factor authentication](#)” on page 99.

### 3.4 Naming the user partition

The descriptive name of your user partition will appear in the OTDS web client and may be used by a different administrator than the one who set up the partition. You should choose a name that reflects the type of users that you have mapped to this user partition. You might also have multiple partitions connected to the same identity provider, so it is important that the name reflects your users, groups and mappings.

► **Example 3-1: Assume you must create partitions for Human Resources, Payroll, and all staff members of company ABC Incorporated:**

- When creating a user partition to include all Human Resources personnel, name your partition ABC HR.
- When creating a user partition containing all Payroll staff, name your partition ABC Payroll.
- When creating a user partition containing all staff members, name your partition ABC Staff.



#### Rules for user partition names

1. The user partition name can include upper and lowercase letters, numerals, blanks, and special characters.
2. The user partition name cannot contain any reserved special characters. Reserved special characters include @ , + " \ < > ' = / ;
3. The user partition name cannot contain a blank or # at the beginning.
4. The user partition name cannot contain a blank at the end.

For more information about reserved special characters, see the “[Distinguished Names](#)” page, which is referenced in “[References to external websites](#)” on page 385.

The user partition name must be unique within a Directory Services server. After the name of a user partition is specified, it cannot be changed.

## 3.5 Defining user attributes

The following table lists a partial set of attributes maintained by OTDS for users and their meaning:

Attribute	Meaning
c	Country or Region
cn	Common name. For example, the user's sign in name.
displayName	Display Name
facsimileTelephoneNumber	Fax Number
givenName	First Name
initials	Middle Name
l	City or Locale
mail	Email address
notes	Notes
o	Organization name
oTCompany	Company
oTDepartment	Department
oTExternalID1	< <i>user_name</i> >
oTExternalID2	< <i>user_name</i> >@< <i>user_partition</i> >
oTExternalID3	< <i>user_name</i> > or < <i>user_name</i> >@< <i>DNS_domain</i> > or < <i>user_name</i> >@< <i>user_partition</i> > For more information, see “ <a href="#">The OTDS unique ID</a> ” on page 72.
oTExternalID4	< <i>NETBIOS_DOMAIN_NAME</i> > \< <i>sAMAccountName</i> > or < <i>NETBIOS_DOMAIN_NAME</i> >\< <i>user_name</i> > or < <i>user_partition</i> >\< <i>user_name</i> >

Attribute	Meaning
oTExtraAttr0-9	Extra attributes available for importing information
oTStreetAddress	Street Address
physicalDeliveryOfficeName	Office
postalCode	Zip Code or Postal Code
sn	Surname or Last Name
st	State or Province
telephoneNumber	Phone Number
title	Job Title

**!** **Important**

oTExternalID1, oTExternalID2, oTExternalID3, and oTExternalID4 are the attributes that give a user the set of identifiers that are used to authenticate that user. In addition, one of these is also used as the user name format pushed to resources. These attributes are to be changed only if defaults do not provide desired values.

**Example:** An individual with the userid `franz` will have the following settings:

oTExternalID1:	franz
oTExternalID2:	franz@<partition>
oTExternalID3:	franz@<company>.com
oTExternalID4:	<COMPANY>\franz



**Note:** oTExternalID1 may or may not be unique for all users in Directory Services.

oTExternalID3 and oTExternalID4 are intended to be unique within Directory Services.

**!** **Important**

1. Because oTExternalID3 is used by Directory Services as the OTDS user ID, you must ensure that oTExternalID3 is unique for all users in Directory Services.
2. oTExternalID4 is used by default to find the user when authenticating for silent single sign on through Kerberos from the Windows Desktop. For silent single sign on to work, you must ensure that oTExternalID4 matches <NETBIOS\_DOMAIN\_NAME>\<samAccountName> of users in Active Directory.

## 3.6 Defining group attributes

The following table lists a partial set of attributes maintained by OTDS for groups and their meaning:

Attribute	Meaning
cn	Group Name
description	Description
displayName	Display Name
notes	Notes
oExternalID1	<groupname>
oExternalID2	<group_name>@<user_partition>
oExternalID3	<group_name>@<DNS_domain> or <group_name>@<user_partition>
oExternalID4	<NETBIOS_DOMAIN_NAME>\<group_name> or <user_partition>@<group_name>

## 3.7 The OTDS unique ID

The OTDS unique ID is used to specify which identity provider attribute uniquely defines your user.

**!** **Important**

OTDS Enterprise Sync will specify the values of each oExternalID when importing or consolidating users from an identity provider. The values for each oExternalID must never be manually specified.

### For Active Directory:

If you select **AD/LDAP attribute** for the **OTDS Unique ID**, the following mappings will be used:

- oExternalID1 - <AD/LDAP\_user\_ID\_attribute>
- oExternalID2 - <AD/LDAP\_user\_ID\_attribute>@<Partition\_name>
- oExternalID3 - <specified\_AD/LDAP\_attribute>, for example userPrincipalName

If you select **Generated OTDS Unique ID** for the **OTDS Unique ID**, the following mappings will be used:

- oExternalID1 - <AD/LDAP\_user\_ID\_attribute>

- oExternalID2 - <AD/LDAP\_user\_ID\_attribute>@<Partition\_name>
- oExternalID3 - <AD/LDAP\_user\_ID\_attribute>@<Domain\_name>
- oExternalID4 - <NETBIOS\_DOMAIN\_NAME>\<AD/LDAP\_user\_ID\_attribute>

Because the attribute specified for the unique ID, for example `userPrincipalName`, does not apply to groups, the mapping does not depend on the selected **OTDS Unique ID**, and is always:

- oExternalID1 - <AD/LDAP\_group\_ID\_attribute>
- oExternalID2 - <AD/LDAP\_group\_ID\_attribute>@<Partition\_name>
- oExternalID3 - <AD/LDAP\_group\_ID\_attribute>@<Domain\_name>
- oExternalID4 - <NETBIOS\_DOMAIN\_NAME>\<AD/LDAP\_group\_ID\_attribute>



**Note:** oExternalID4 must correspond to the <NETBIOS\_DOMAIN\_NAME>\<SAMAccountName> in Active Directory for silent single sign on from Windows workstations to work. For more information, see “[Defining user attributes](#)” on page 70.

## For LDAP:

If you select **AD/LDAP attribute** for the **OTDS Unique ID**, the following mappings will be used:

- oExternalID1 - <AD/LDAP\_user\_ID\_attribute>
- oExternalID2 - <AD/LDAP\_user\_ID\_attribute>@<Partition\_name>
- oExternalID3 - <specified\_AD/LDAP\_attribute>, for example `mail`
- oExternalID4 - <Partition\_name>\<AD/LDAP\_user\_ID\_attribute>

If you select **Generated OTDS Unique ID** for the **OTDS Unique ID**, the following mappings will be used:

- oExternalID1 - <AD/LDAP\_user\_ID\_attribute>
- oExternalID2 - <AD/LDAP\_user\_ID\_attribute>@<Partition\_name>
- oExternalID3 - <AD/LDAP\_user\_ID\_attribute>@<Partition\_name>
- oExternalID4 - <Partition\_name>\<AD/LDAP\_user\_ID\_attribute>

Because the attribute specified for the **OTDS Unique ID**, for example `mail`, does not apply to groups, the mapping does not depend on the selected **OTDS Unique ID**, and is always:

- oExternalID1 - <AD/LDAP\_group\_ID\_attribute>
- oExternalID2 - <AD/LDAP\_group\_ID\_attribute>@<Partition\_name>
- oExternalID3 - <AD/LDAP\_group\_ID\_attribute>@<Partition\_name>
- oExternalID4 - <Partition\_name>\<AD/LDAP\_group\_ID\_attribute>

## 3.8 Synchronized User Partitions

This section describes creating, editing, deleting, and importing user and group data in synchronized user partitions.

You will need to create a synchronized user partition if you want to import users and groups from your identity provider. After you have created a user partition, you may never need to change any of its settings. Occasionally, though, you might want to adjust the mapping of attributes from your identity provider into Directory Services. You might also want to adjust special settings that are only available when your user partition has been created. These special settings are internal Directory Services settings that are not mapped to your identity provider attributes.

### 3.8.1 Defining a synchronized user partition



**Note:** It is not possible to set a password policy for synchronized user partitions.

There are several options that you need to set when you create a synchronized user partition. These options are explained below:

---

#### Connection Information

You can optionally choose to create multiple connections. However, if you are going to create multiple connections, you need to ensure the following:

1. You can only specify one type of connection across all connections you create. In other words, each connection you create must have the same connection type, one of : AD, AD Global Catalog, or LDAP.
2. If you have multiple connections, and then you select **Test Authentication** on the **Authentication** page, that test is run on all connections with the same set of credentials.

However, if you select **Test** on any one of the **Locations**, **Mappings**, or **Attributes** pages, then that test is only run on the initial connection you created.

The functionality of the **Query Server Parameters** button on the **Authentication** page is also only run on the initial connection you created.

3. You need to be aware that when a synchronized user partition is saved, an LDAP Credentials Authenticator is created with parameters based on the initial connection you created.

On the **Connection Information** page, these are the fields you need to complete:

- In the **Hostname or address** box, type the name of your identity provider, Active Directory, Active Directory Global Catalog, or Lightweight Directory Access Protocol (LDAP). This can be the fully qualified hostname of the physical machine or the IP address. Each connection you create must be a unique hostname or IP address.

- In the **Port** box, type the port number of your identity provider, Active Directory, Active Directory Global Catalog, or Lightweight Directory Access Protocol (LDAP). The default is 636 for SSL encryption and 389 for no encryption. Set port number to 3268/3269 to connect to the Active Directory Global Catalog. For more information, see “[Connecting to an identity provider](#)” on page 78.
- In the **Encryption method** box, select **None** or **SSL**. If the specified host requires an SSL connection on the specified port, select **SSL**. The default is **SSL**. Changing the encryption method will reset the port to a default value. For more information, see “[When to use encryption](#)” on page 79.

## Authentication

You can choose one of the following three authentication methods to determine how the connection is handled: **None**, **Simple**, or **SASL (GSSAPI)**.



**Note:** If you select either **Simple** or **SASL (GSSAPI)**, the identity provider user name that you specify for authentication does not need special privileges. A read-only account is sufficient. However, the data that can be imported will depend on the access permission of the supplied user name.

In addition, functionality will be impaired if the account does not have sufficient permissions. OpenText recommends that you use a service account that can read the server's base DNs, schema, supported controls, all user and group locations that are to be imported, and all relevant attributes on the user and group objects. If you choose to have the password for this service account expire, the new password will need to be reconfigured on the partition.

- Select **None** as your authentication method only if your identity provider deployment demands anonymous binding. By default, Active Directory is not configured with anonymous binding. LDAP is frequently configured with anonymous binding.
- If you select **Simple**, enter or provide a user name and password that Directory Services will use to connect to your identity provider. You can specify the user name as any of the following:
  - full DN, for example `cn=jsmith,ou=people,dc=opentext,dc=com`
  - `<domain_name>\<user_name>`, for example `opentext\jsmith`
  - `<user_name>@<qualified_domain_name>`, for example `jsmith@opentext.net`
- If you select **SASL (GSSAPI)**, you must set the following boxes:
  - **Kerberos Credential Type:** select one of the following:
    - **Username and Password:** if you select this credential type, you will need to enter the user name and password required to connect to the identity provider. You will also need to define the Kerberos Realm and Kerberos KDC, for more information, see “[Configuration for the Kerberos Realm and the Kerberos KDC](#)” on page 76.

- **Key Tab File:** if you select this credential type, you need to define the Kerberos Realm and Kerberos KDC, for more information, see [“Configuration for the Kerberos Realm and the Kerberos KDC” on page 76](#).
- **Process Account:** if you select this credential type, you must set the following registry setting:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos
\Parameters
Value Name: allowtgsessionkey
Value Type: REG_DWORD
Value: 0x01
```

After setting the registry you must reboot the machine. You will also need to define the Kerberos Realm and Kerberos KDC, for more information, see [“Configuration for the Kerberos Realm and the Kerberos KDC” on page 76](#).

The **Process Account** credential type is only supported on Windows.

- **Service Principal Name:** must be set to a valid service principal that exists for the server that you typed in the **Host name or address** box. By default, this box will be populated.
- **Quality of Protection:** select one of the following:
  - **Authentication Only:** if you want to ensure that only the authentication is encrypted.
  - **Authentication with Integrity Protection:** if you want to ensure that the authentication is encrypted and that all traffic is assessed to determine whether it has been tampered with. The traffic is not encrypted. Make sure that you did not select **SSL** in the **Encryption method** box in the previous page if you want to set this level.
  - **Authentication with Integrity and Privacy Protection:** if you want to ensure that the authentication and all traffic is encrypted. Make sure that you did not select **SSL** in the **Encryption method** box in the previous page if you want to set this level.



**Note: Configuration for the Kerberos Realm and the Kerberos KDC –** if you selected **SASL (GSSAPI)**, you need to define the Kerberos Realm and Kerberos KDC in either the Java krb5.conf file or in the Java configuration options Tomcat configuration. The krb5.conf file can, by default, be found in the <Java\_install\_path>\lib\security\krb5.conf, for example, in C:\Program Files\Java\jre7\lib\security\krb5.conf.

An example of the definitions of the Realm and the KDC in the Tomcat configuration:

```
-Djava.security.krb5.realm=DOMAIN.LOCAL
-Djava.security.krb5.kdc=domainserver.domain.local
```

The default for the client keytab file is the krb5.keytab file in the home directory of the user name used to run Tomcat. For example, /home/jsmith/krb5.keytab or C:\users\jsmith\krb5.keytab.

On Windows, if Tomcat is being run as the system account, the file default is C:\krb5.keytab on Windows 2008 R2 and C:\Windows\System32\config\systemprofile\krb5.keytab on Windows 2012 R2.

For more information, see “[Choosing an authentication method](#)” on page 79.

## Monitoring

Select one of the following monitoring methods:

- **DirSync control:** by default, identity providers detected as Active Directory should use this built-in to monitor for changes.
- **USN query:** by default, identity providers detected as AD Global Catalog should use this built-in to monitor for changes.
- **Persistent search:** by default, identity providers detected as LDAP should use this built-in to monitor for changes. You may need to ensure that persistent search has been enabled on the LDAP server.



**Note:** The user specified on the **Authentication** page should have sufficient permissions in the identity provider to use the selected monitoring type. For example, in the case of a **USN query** method, the user should have permissions to read schema attributes and the deleted objects container.

If you intend making major changes, and you want to stop monitoring your identity provider for changes, clear the **Monitor changes** check box. For more information, see “[Synchronization types](#)” on page 84.

## Notifications and Search

Select one of the following search methods:

- **Paged search:** if you select this option you must also select a **Page size**.
- **Virtual list view search:** if you select this option you must select a **Page size**, and you can optionally enter a **Sorting attribute**.
- **Unlimited**

For more information, see “[Search methods](#)” on page 85.

## Extended Functionality

- Active Directory and LDAP servers usually have an internal universally unique identifier, **UUID**, assigned to every object. Active Directory has the **UUID objectGUID**. LDAP has the **UUIDs entryUUID** and **nsUniqueId**. IBM Directory servers have the **UUIDs ibm-entryuuid** and **guid**. For more information, see “[Examples of UUIDs for supported servers](#)” on page 86.
- The **AD/LDAP user and group ID** attributes are used to specify which identity provider attribute will be used to build some of the **oTExternalID** attributes in OTDS. For more information, see “[AD/LDAP user and group ID attributes](#)” on page 86.
- The **OTDS unique ID** requires that you select one of the following methods:

- Select **AD/LDAP attribute** when you want the **OTDS Unique ID** to be set to a specified attribute.
- Select **Generated OTDS unique ID** when you want the **OTDS Unique ID** to be the value derived from the attribute specified in the **AD/LDAP user ID attribute** box.

For more information, see “[The OTDS unique ID](#)” on page 72.

---

### 3.8.1.1 Connecting to an identity provider

An identity provider is a provider of user and group information. Directory Services currently supports the following identity providers:

- Windows Server Active Directory. Supported Active Directory systems are:
  - Windows Server Active Directory (AD)
  - AD Global Catalog
  - Windows Server Active Directory Lightweight Directory Services (AD LDS)
- Lightweight Directory Access Protocol, LDAP. Supported LDAP systems are:
  - Oracle Directory Server Enterprise Edition
  - Oracle Internet Directory
  - IBM Lotus Domino
  - IBM Tivoli Directory Server
  - Novell eDirectory
  - Apache Directory Server
  - Windows Server Active Directory Lightweight Directory Services (AD LDS)



**Note:** For more information, see *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)* and the **OTDS Release Notes**. You can find links to these documents in “[OTDS Documentation](#)” on page 381.

Before connecting to an identity provider, you must understand the following about your setup:

1. The network connection information for your identity provider. You will need the name and port or IP address of your identity provider.
2. The location of all the users and groups that are relevant to you in your identity provider.
3. The user and group information in your identity provider that you want to keep synchronized with your Directory Services server. You can selectively filter which users and groups you pull from your identity provider.
4. The mapping of user and group attributes from your identity provider to Directory Services. A default mapping is provided. You can modify this mapping to suit your needs.

For more information, see “[Defining a synchronized user partition](#)” on page 74.

### 3.8.1.2 When to use encryption

You should use encryption if your identity provider requires it. This secures your connection from Directory Services to your identity provider. OpenText recommends securing connections using SSL in production environments.

If you choose no encryption method, **None**, the user name and password that you supply on the **Authentication** page will be transmitted in clear text. For more information, see “[Defining a synchronized user partition](#)” on page 74.

### 3.8.1.3 Choosing an authentication method

The authentication method you choose depends on your identity provider. It must have the following permissions to ensure that Directory Services can retrieve information from your identity provider:

- If you select **None**, the identity provider must allow anonymous sign in to read from the identity provider. See the note below regarding the possible limitations for an anonymous account.
- If you select **Simple**, the authentication method that OpenText recommends using, or **SASL (GSSAPI)**, the user name that you provide must have sufficient permissions to read from the identity provider.

Directory Services can import what the user can Read and Search. Objects and attributes that the supplied user does not have Read or Search permission for will not be imported into your user partition. By default, a user has Read and Search access to most objects and attributes.

For LDAP servers, some other server-specific restrictions or limitations may apply. For example, the Oracle Directory Server Enterprise Edition 11 only returns the number of entries that are specified using the **Look Through Limit** restriction. You must ensure that the supplied user has sufficient permissions for the data you want to import from your identity provider.



1. The identity provider user name that you specify for authentication does not need special privileges. A read-only account is sufficient. However, the data that can be imported will depend on the access permission of the supplied user name.
2. In addition, functionality will be impaired if the account does not have sufficient permissions. OpenText recommends that you use a service account that can read the server's base DNs, schema, supported controls, all user and group locations that are to be imported, and all relevant attributes on the user and group objects. If you choose to have the password for this service account expire, the new password will need to be reconfigured on the partition.
3. To fully support monitoring by USN query for AD or AD Global Catalog, the specified account should be able to Read the deleted objects container.

For more information, see “[Defining a synchronized user partition](#)” on page 74.

### 3.8.1.4 Understanding locations

When you choose a location, you are specifying that you want to import the users or groups that are directly contained in that location. By default, all users and groups in your identity provider are selected, and all users and groups in those users and groups are recursively included.

Clicking **Add Location** will allow you to select known locations in your identity provider or browse the folder structure of your identity provider in a **Browse for Container** window. If you select **Recurse**, you are specifying that you want to import all users or groups from all sub-locations too.

On the **Group Locations** tab, you can select either groups or organizational units as group locations. You can optionally select **Import users from matched groups** to have Directory Services import users only from the groups that match the locations and filter specified. If you select **Import users from matched groups**, and you selected the **Recurse** option on the locations, all users and groups from nested groups will be imported. Note that the locations and filter specified on the **User Locations** tab are still enforced.

If **Import users from matched groups** is not selected, nested groups are not imported.



**Tip:** You can optionally apply a custom filter to identify deleted users and groups in this partition. For more information, see “[Examples filtering one synchronized partition's deleted users and groups](#)” on page 132.

### 3.8.1.5 Applying filters

The filters have been set up to include all users and groups from the locations specified on your identity provider. You can apply filters to choose only particular user accounts from a particular user location to include in this partition. If you reset the filters, they will automatically revert to the default filters so that the automatic importing of users and groups will work.



**Note:** If you change the filters on an existing user partition you will be changing which users and groups are included in this partition. You must run a consolidation because Enterprise Sync does not automatically import users and groups again as a result of a change in configuration. As soon as you consolidate, it will create and delete users and groups as necessary to match what is defined by the filters.

The filters you can apply to users and groups to determine if they will be imported:

1. **Object Filter:** this AD/LDAP search filter defines, to OTDS, a user or group object. After it has been defined, OTDS uses the definition to determine which user or group objects will be examined by OTDS for import, consolidation, and monitoring operations. An **Object Filter** must be defined or nothing will be imported.

2. **Attributes Filter:** this AD/LDAP search filter adds more restrictions to the user or group object definition. It is used to limit which of the objects defined in the **Object Filter** box are imported to OTDS. An entry to the **Attributes Filter** box is optional. If no **Attributes Filter** is defined, then only the **Object Filter** will be used for import operations.



**Note:** If the `memberOf` attribute is used in the **Attributes Filter**, then monitoring will not pick up updates on the identity provider that result from users and/or groups being added to, or removed from, OTDS. A sync schedule could be used to pick up any updates not picked up by monitoring.

Further, an attribute you choose to apply to the **Attributes Filter** must be mapped on the **User Mappings** and/or **Group Mappings** page. If you have not created the mapping, users and/or groups that should be added to, or removed from, OTDS based on changes on the identity provider, will not be picked up by monitoring.



**Tip:** Basic LDAP filter syntax can be found in *LDAP Query Basics* in the “Microsoft Tech Net Center”. For more information see “[References to external websites](#)” on page 385.

## User filters

The default user object filter in a synchronized user partition includes all users, including deleted users:

```
( | (sAMAccountType=805306368) (&(isDeleted=TRUE)(objectClass=user)) (!  
(objectClass=computer)))
```

The default user filter includes all users, including deleted users:

```
(&(objectClass=user) ( | (sAMAccountType=805306368) (isDeleted=TRUE)))
```

➡ **Example 3-2: User filter example:** If you want to include all users that are located in Ottawa or Austin, and who have the first name John, use the following in the **Attributes Filter**:

```
(&(givenName=John) ( | (l=Ottawa) (l=Austin)))
```



➡ **Example 3-3: User filter example:** If you want to include all users in the ABC123 group from the Users container in the ABC.company domain in Active Directory, use the following filter:

**Object Filter:**

```
(objectClass=user)
```

**Attributes Filter:**

```
(memberOf=CN=ABC123,CN=Users,DC=ABC.company,DC=com)
```



## Group filters

The default group object filter in a synchronized user partition includes all groups, including deleted groups:

```
(objectClass=groupOfUniqueNames)
```

The default group filter in a non-synchronized user partition includes all groups, including deleted groups:

```
(&(objectClass=group) (| (&(sAMAccountType=268435456) (| (groupType=2147483652) (groupType=2147483650) (groupType=2147483656))) (isDeleted=TRUE)))
```

► **Example 3-4: Group filter example: In the ABC.net domain, there is a large group: CN=ARC\_Global\_Default,OU=Exchange\_Archiving,OU=Groups, DC=ABC,DC=net. If you wanted to exclude this group from being imported into your user partition, use the following filter:**

### Object Filter:

```
(&(objectClass=group) (| (&(sAMAccountType=268435456) (| (groupType=2147483652) (groupType=2147483650))) (isDeleted=TRUE)))
```

### Attributes Filter:

```
(! (distinguishedName=CN=ARC_Global_Default,OU=Exchange_Archiving,OU=Groups,DC=ABC,DC=net))
```

► **Example 3-5: The OTDS group filter in sAMAccountType attributes in Active Directory**

In OTDS, the default group filter in a synchronized user partition uses the sAMAccountType attribute to filter the group type. In Active Directory, the sAMAccountType attributes for the different groups are:

- Universal Security = 268435456
- Global Security = 268435456
- Domain Local Security = 536870912

The default group filter for OTDS for Universal Security and Global Security groups is:

```
(&(objectClass=group) (| (&(sAMAccountType=268435456) (| (groupType=2147483652) (groupType=2147483650) (groupType=2147483656))) (isDeleted=TRUE)))
```

The default group filter for OTDS for Domain Local Security is:

```
(&(objectClass=group) (| (&(| (sAMAccountType=536870912) (sAMAccountType=268435456)) (| (groupType=2147483652) (groupType=2147483650) (groupType=2147483656))) (isDeleted=TRUE)))
```



### 3.8.1.6 Applying user partition attribute mappings

Attribute mappings will default to suggested mappings based on the type of identity provider object that you are mapping. You can use these defaults with no impact to Directory Services synchronization with your identity provider.

You might want to map attributes differently if you have special attributes in your identity provider schema that map to unusual Directory Services attributes.

#### Preserving AD/LDAP DN attributes

You can optionally choose to preserve AD/LDAP DN attributes. DN refers to the Distinguished Name of an entity. When OTDS imports users or groups from AD/LDAP, by default OTDS will translate the DN attributes to the OTDS internal DN. If you want to preserve the AD/LDAP DN attributes, in the **Format** box of the mapping, type %odn. Any DN attribute with the %odn format will preserve the original AD/LDAP value.

After applying the "%odn" format to any attribute, you need to consolidate the partition with the AD or LDAP server in order to change the attribute to the original DN. For more information, see ["Consolidating users and groups in Partitions" on page 128](#).

#### Examples of attribute mappings

##### ▶ Example 3-6: An example mapping the OTDS displayName attribute

You can map the OTDS displayName attribute to your Active Directory firstName and lastName, formatting the entry with the prefix "Dr." to indicate that all members of this user partition are medical doctors:

OTDS User Attribute	Active Directory Attribute(s)	Format
displayName	givenName,sn	Dr. %s %s



##### ▶ Example 3-7: An example formatting the OTDS homePostalAddress attribute

You can format the OTDS homePostalAddress attribute to include your LDAP streetAddress, street, "ON", and postal code attributes to indicate that all members of this user partition reside in Ontario:

OTDS User Attribute	Active Directory Attribute(s)	Format
homePostalAddress	streetAddress,street,postalCode	%s %s ON %s



▶ **Example 3-8: An example formatting the OTDS Manager attribute**

You can format the Manager attribute to preserve the original AD/LDAP value, thereby ensuring that OTDS will not translate it:

OTDS User Attribute	Active Directory Attribute(s)	Format
Manager	Manager	%odn



▶ **Example 3-9: An example formatting the OTDS group description attribute**

You can format your OTDS group description attribute to display only “Staff”:

OTDS Group Attribute(s)	Active Directory Attribute(s)	Format
description	description	Staff



### 3.8.1.7 Synchronization types

An identity provider detected as an Active Directory server will use the built-in Active Directory synchronization, **DirSync**, by default.

An Active Directory Global Catalog identity provider will use **USN query** synchronization by default. This type of synchronization monitors the identity provider for objects and attributes that have changed since the previous synchronization.

An identity provider detected as an LDAP server will use **Persistent Search** synchronization by default. This type of synchronization uses a search operation that finds the initial user and group data, and sends new copies of the data whenever an entry is modified. This is continuous monitoring.

**Full synchronization** is a scheduled synchronization of all user and group data regardless of whether it has changed or not. You set full synchronization on the **Scheduler** tab of a synchronized user partition. Because group and organizational unit membership must be resolved for each user entry, a full synchronization can take longer to complete depending on the number of users in groups and organizational units.

Full synchronization should be used in the following cases:

- If **DirSync**, **USN query** or **Persistent Search** are not available for your identity provider.
- If it is not possible to maintain a permanent connection between your identity provider and Directory Services.



**Note:** Directory Services will try to recover from broken connections when it uses **DirSync**, **USN query** and **Persistent search** monitor. Directory Services will synchronize changes made during periods where the connection to your identity provider is lost.

- If you are making major changes to your identity provider. It might be useful to schedule a full synchronization after major changes to your identity provider and then change your monitoring properties to schedule periodic synchronizations that update only changed entries.



**Tip:** You could also clear the **Monitor changes** check box when you are making major changes to your identity provider and then **Consolidate** when changes are complete.

- If your identity provider typically encounters constant changes. For example, if user entries are updated every time a user signs in to a single sign on application, you may want to use scheduled full synchronizations.

For more information, see “[Defining a synchronized user partition](#)” on page 74.

### 3.8.1.8 Search methods

An identity provider that supports **Paged search** will use a **Paged search** by default because it is the fastest method of searching. The paged search returns only a subset of entries based on the **Page size** that you provided. It may be used to review the search results a page at a time.

Some LDAP servers do not support **Paged search** and will use a **Virtual list view** (VLV) search by default. The VLV search method is also an iterative method but the results are sorted based on the **Sorting attribute** that you provide. It is slower than the **Paged search**. For example, the Oracle Directory Server uses VLV because it does not support paged search.

The **Unlimited** search method is the least preferred method of searching because most Active Directory or LDAP servers will return a fixed number of entries in one search result. This is set by the administrator of the server but it must be set to a number more than the expected maximum number of entries in order to retrieve them all in one search.



#### Important

The user running the search must have the proper rights to run an unlimited search.

For more information, see “[Defining a synchronized user partition](#)” on page 74 and “[Performance issues](#)” on page 406.

### 3.8.1.9 Examples of UUIDs for supported servers

Active Directory and LDAP servers usually have an internal universally unique identifier, UUID, assigned to every object. When an object is moved or renamed the unique identifier stays the same. When an object is deleted and another object with the same name is created, the new object will be given a different unique identifier. To support extended functionality, such as tracking deleted users and groups, you need to specify the name of a universally unique identifier for your identity provider.

Active Directory servers have the following universally unique identifier:

- objectGUID

Lightweight Directory Access Protocol (LDAP) servers have the following universally unique identifiers:

- entryUUID
- nsUniqueId

IBM Directory servers have the following universally unique identifiers:

- ibm-entryuuid
- guid

### 3.8.1.10 AD/LDAP user and group ID attributes

The AD/LDAP user and group ID attributes are used to specify which identity provider attribute will be used to build some of the oTExternalID attributes in OTDS. For example, sAMAccountName is the default sign in attribute used for the AD/LDAP user attribute for Active Directory user partitions.

### 3.8.1.11 Importing users and groups

You can start importing users and groups from your identity provider directly into Directory Services as soon as you create your user partition if you select the **Start importing users and groups automatically** check box on the **General** page of the user partition creation assistant. Users and groups are imported from your identity provider directly into an equivalent directory hierarchy in Directory Services. The mappings that you supplied are used to create users and groups that can be administered using the OTDS web client. This is a local copy of your identity provider and contains a snapshot of the data. There is no communication of data from Directory Services to your identity provider and changes made to users and groups in Directory Services do not affect your identity provider.

If, on the **General** page of the user partition creation assistant when you create a user partition, you select the **Start importing users and groups automatically** check box, it will automatically start importing users and groups from the identity provider after you click **Save**. If you want to delay the start of this time-consuming activity, clear the check box and, when you are ready to do the import, see “[Importing users and groups](#)” on page 98.



**Note:** When you select the **Start importing users and groups automatically** box, the user partition command **Import Users and Groups** will still appear in the **Actions** menu. However, if you select the **Import Users and Groups** menu option, it will display a message that users and groups have already been imported.

If the initial import of users and groups completes without errors, the user partition is automatically in a state where user and group changes in the associated identity provider are delivered into Directory Services. This is called user synchronization.

If any full import of users and groups from the identity provider into Directory Services encounters any errors or is stopped manually by an administrator, the user partition does not receive user and group changes from the identity provider. However, the incomplete user partition may be browsed and inspected. This might provide valuable information about why the import failed. After the problem has been resolved, you can choose the **Import Users and Groups** action in the OTDS web client. This will start a complete data import of all users and groups.

After making a change to filter strings or user locations, you should import data from your identity provider into Directory Services. You can do this by selecting **Consolidate** from the **Actions** menu in the OTDS web client.

### Cancelling the import operation

It is not possible to cancel the initial importing of users and groups into Directory Services when you first create a synchronized resource.

## 3.8.2 Creating a synchronized user partition

### To create a synchronized user partition:

1. From the web administration menu, click **Partitions**.
2. On the button bar, click **Add**. Next, from the **Add** list, select **New Synchronized User Partition**.
3. Before you begin, ensure you have met all prerequisites. For more information, see “[Connecting to an identity provider](#)” on page 78.
4. On the **Connection Information** page, to add a new connection, click **Add Connection** and then do the following:
  - a. In the **Host name or address** box, type the name of your identity provider, AD, AD Global Catalog, or LDAP. This can be the fully qualified hostname of the physical machine or the IP address. Each connection you create must be a unique hostname or IP address.
  - b. In the **Port** box, type the port number of your identity provider, AD, AD Global Catalog, or LDAP. For more information, see “[Defining a synchronized user partition](#)” on page 74.



**Note:** 389 is the default port number if you select **None** for the **Encryption method**.

636 is the default port number if you select **SSL** for the **Encryption method**.

- c. In the **Encryption method** box, if the specified server used SSL, select **SSL**. Otherwise, select **None**. For more information, see “[Defining a synchronized user partition](#)” on page 74 and “[When to use encryption](#)” on page 79.
- d. Click **Save**.
- e. **Optional** If you want to remove specific connections, click the box to the left of the connection and then click **Remove Selected**.  
If you want to remove all connections, click **Remove All**.



**Important**

A synchronized user partition must always have at least one connection. OpenText recommends that you save the configuration before you remove all connections.

- f. **Optional** To verify that you have entered your information correctly, select the box to the left of the item you want to test, and then click the **Test** button. If your test succeeds, a message indicating success appears. If your test fails, close the information window, and then make any necessary corrections.
- g. If you are creating, click **Next**. If you are editing, you can either save or select the next tab to edit.

5. On the **Authentication** page, for information about the options available, see “[Defining a synchronized user partition](#)” on page 74 and “[Choosing an authentication method](#)” on page 79.

- a. In the **Authentication Method** box, do one of the following:
  - If you require no authentication, select **None**. You can then proceed to either test your connection or [step 5.c](#).
  - If you require simple authentication, select **Simple**, and then do the following:
    1. In the **User name** box, enter a user name to access this partition.
    2. In the **Password** box, enter a password for the user name to access this partition.
  - If you require Kerberos SASL authentication, select **SASL (GSSAPI)**. You must then determine how you will be configuring this authentication as follows:
    1. From the **Kerberos Credential Type** list, select the credential method that will apply to this partition.

2. In the **User name** box, if you selected either **Username and Password** or **Key Tab File** in the **Kerberos Credential Type** box, type the name of the user that you configured in Kerberos.
3. In the **Password** box, if you selected **Username and Password** in the **Kerberos Credential Type** box, type the password for the Kerberos user.
4. The **Service Principal Name** box is filled with a default “ldap/ <Host\_name\_or\_address>” string, taken from the name you typed for this new partition.
5. From the **Quality of Protection** list, select the level of encryption that will be applied.

For more information, see [Authentication on page 75](#) and [“Choosing an authentication method” on page 79](#).

- b. **Optional** To verify that you have entered your information correctly, select the box to the left of the item you want to test, and then click the **Test** button. If your test succeeds, a message indicating success appears. If your test fails, close the information window, and then make any necessary corrections.
  - c. **Optional** To understand how your identity provider settings will be used in subsequent steps, click **Query Server Parameters**. This will display a set of parameters and values that will be used to populate the following pages. You cannot modify the parameters from the **Server Parameters** window. Read the results, and then close the window.
  - d. If you are creating, click **Next**. If you are editing, you can either save or select the next tab to edit.
6. On the **General** page, do the following:
    - a. In the **Name** box, type a name for this user partition. For more information, see [“Naming the user partition” on page 69](#).

**Important**  
After a user partition is created, you cannot change its name.
    - b. **Optional** You can click the **Verify Partition Name** button if you want to check that the name you entered in step 6.a is valid.
    - c. **Optional** In the **Description** box, type a description for this user partition.
    - d. **Optional** If you are creating this partition and you want to begin importing users and groups immediately, select **Start importing users and groups automatically upon completion**.
    - e. If you are creating, click **Next**. If you are editing, you can either save or select the next tab to edit.
  7. On the **Server Settings** page, do the following:
    - a. Accept the **Server type** that has been detected, or choose a different type from the **Server type** list.



**Note:** After your partition has been created, you cannot edit the **Server type** or **Naming context**.

- b. Accept the **Naming context** that has been detected, or choose a different starting point for your identity provider's hierarchy.
  - c. **Optional** To verify your changes, click **Verify Settings**. This will determine if any changes that you have made to the **Server type** or **Naming context** are valid for the server type detected. If your test succeeds, the message **Connected** appears. If your test fails, close the window, and then correct your server type or naming context information.
  - d. If you are creating, click **Next**. If you are editing, you can either save or select the next tab to edit.
8. On the **Group Locations** page, do the following:
    - a. In the **Group Locations** box, do the following:
      - i. Click **Add Search Location** to add all the group locations that you want to include in this profile of user accounts. For more information, see “[Understanding locations](#)” on page 80. In the **Add Search Location** box:
        - A. In the **Location** box, enter either an organizational unit or a group as a location.
        - B. **Optional** Select **Recurse** to select a group location and all of its child locations.
        - C. Click **Add**.
      - ii. **Optional** To edit an existing group location, in the **Group Locations** box, select the **Edit** link next to the location you want to edit. Make your edits in the **Edit Location** box, and then click **Save**.
      - iii. **Optional** To delete an existing group location, in the **Group Locations** box, select the **Delete** link next to the location you want to delete.
    - b. In the **Object Filter** and **Attributes Filter** area you can optionally choose to include only those groups that match your filter parameters. The default group location filters supplied by Directory Services will be sufficient for most systems. For more information and to see examples of filters for your server type, see “[Applying filters](#)” on page 80. If you want to apply filters, do the following:
      - i. In the **Object Filter** box, type the filter that defines which group objects will be examined by OTDS for import, consolidation, and monitoring operations. This box is mandatory.



### Important

There is no verification step. As soon as you click **Delete**, the location is removed.

- iv. **Optional** To reset group locations to the default naming context, click **Reset Locations(s) To Default**.

- b. In the **Object Filter** and **Attributes Filter** area you can optionally choose to include only those groups that match your filter parameters. The default group location filters supplied by Directory Services will be sufficient for most systems. For more information and to see examples of filters for your server type, see “[Applying filters](#)” on page 80. If you want to apply filters, do the following:
  - i. In the **Object Filter** box, type the filter that defines which group objects will be examined by OTDS for import, consolidation, and monitoring operations. This box is mandatory.

- ii. Optional In the **Attributes Filter** box you can optionally type a filter that defines further restrictions on which group objects, as defined in the **Object Filter** box, are imported, consolidated, and monitored.
- iii. Optional To reset the group filter to the default value, click **Reset Filters To Default**.
- c. Optional If you want to restrict the users imported by Directory Services to those who are members of the groups found by the locations and filters specified, select **Import users only from matched groups**.



**Note:** A user is deemed a member of a group if it is either directly a member, or indirectly a member through a nested group if, on the location, you selected the **Recurse** option.

The users to be imported are still subject to the locations and filters specified on the **User Locations** page described in the next step. Therefore, it is the intersection of all these conditions that determines whether a user is imported into Directory Services. For more information, see “[Understanding locations](#)” on page 80.

- d. Optional Click **Test Filters and Locations** to see the first 100 groups that will be included in your partition with your current settings. Read the information provided, then close the information window. Read the information in the **Test Filters and Locations** window, then close the window.



**Note:** The main purpose of **Test Filters and Locations** is to check that group filters and locations are correct. The **Import users only from matched groups** option is ignored by the test.

- e. If you are creating, click **Next**. If you are editing, you can either save or select the next tab to edit.
- f. If you subsequently make a change to the **Group Locations** page, and after you have finished editing your synchronized user partition, you need to consolidate the synchronized partition. For more information, see “[Consolidating changes to users, groups, organizational units, and partitions](#)” on page 129.

9. On the **User Locations** page, do the following:

- a. In the **User Locations** box, do the following:
  - i. Add all the user locations that you want to include in this profile of users. Click **Add Search Location** to enter at least one user location to include in this user partition. For more information, see “[Understanding locations](#)” on page 80.
  - ii. In the **Add Search Location** box:
    - A. In the **Location** box, enter either an organizational unit or a user as a location.
    - B. Optional Select **Recurse** to select a user location and all of its child locations.

### C. Click Add.

- iii. **Optional** To edit an existing user location, in the **User Locations** box, under the **Actions** column, click the **Edit** link next to the location you want to edit. Make your edits in the **Edit Location** box, and then click **Save**.
- iv. **Optional** To delete an existing user location, in the **User Locations** box, click the **Delete** link next to the location you want to delete.

**!** **Important**

There is no verification step. As soon as you click **Delete**, the location is removed.

- v. **Optional** To reset user locations to the default naming context, click **Reset Location(s) To Default**.
- b. In the **Object Filter** and **Attributes Filter** area you can optionally choose to include only those users that match your filter parameters. The default user location filters supplied by Directory Services will be sufficient for most systems. For more information and to see examples of filters for your server type, see “[Applying filters](#)” on page 80. If you want to apply filters, do the following:
- i. In the **Object Filter** box, type the filter that defines which user objects will be examined by OTDS for import, consolidation, and monitoring operations. This box is mandatory.
  - ii. **Optional** In the **Attributes Filter** box you can optionally type a filter that defines further restrictions on which user objects, as defined in the **Object Filter** box, are imported, consolidated, and monitored.
  - iii. **Optional** To reset the user filter to the default value, click **Reset Filters To Default**.
- c. **Optional** Click **Test Filters and Locations** to see the first 100 users that will be included in your partition with your current settings. Read the information provided, then close the information window. Read the information in the **Test Filters and Locations** window, then close the window.



**Note:** The main purpose of **Test Filters and Locations** is to check that user filters and locations are correct. The **Import users only from matched groups** option on the **Group locations** tab is ignored by the test.

- d. If you are creating, click **Next**. If you are editing, you can either save or select the next tab to edit.
  - e. If you subsequently make a change to the **User Locations** page, and after you have finished editing your synchronized user partition, you need to consolidate the synchronized partition. For more information, see “[Consolidating changes to users, groups, organizational units, and partitions](#)” on page 129.
10. On the **User Mappings** page, do the following:

- a. Map each Directory Services user attribute to the appropriate identity provider user attribute or attributes. To edit the boxes in the **Active Directory Attribute(s)**, **LDAP Attribute(s)** or **Format** columns, click in the cell you want to edit, then type your change. Use the **Format** box to customize your attribute mapping. For more information, see “[Applying user partition attribute mappings](#)” on page 83.

- b. **Optional** Click **Test Mappings** to verify the syntax of your user attribute mappings. This will display a **Test User Mapping** window showing the first 100 users and their attribute mappings according to your mapping settings. Close this window and, if needed, change your mappings.



**Note:** A warning message will be displayed if all *tested* users have some mapped attributes without values. Removing such mapped attributes will increase performance.

- c. **Optional** If you want to return to the default mappings, click **Reset to Default**.
- d. If you are creating, click **Next** or **Save**. If you are editing, you can either save or select the next tab to edit.
- e. If you subsequently make a change to the **User Mappings** page, and after you have finished editing your synchronized user partition, you need to consolidate the synchronized partition. For more information, see “[Consolidating changes to users, groups, organizational units, and partitions](#)” on page 129.

11. On the **Group Mappings** page, do the following:

- a. From the **Member Attribute** and **MemberOf Attribute** lists, select attributes to map to Directory Services **Member** and **MemberOf** attributes. You might need to custom map the **Member** and **MemberOf** attributes to adopt your LDAP Server schema. For example, for eDirectory Novell Server, map the **MemberOf** attribute to **groupMembership**.

- b. Map each Directory Services group attribute to the appropriate identity provider group attribute or attributes. To edit the boxes in the **Active Directory Attribute(s)**, **LDAP Attribute(s)** or **Format** columns, click in the cell you want to edit, then type your change. Use the values under the **Format** column to customize your attribute mappings. For more information, see “[Applying user partition attribute mappings](#)” on page 83.

- c. **Optional** Click **Test Mappings** to verify the syntax of your group attribute mappings. This will display a **Test Group Mapping** window showing the first 100 groups and their attribute mappings according to your mapping settings. Close this window and, if needed, change your mappings.



**Note:** A warning message will be displayed if all *tested* groups have some mapped attributes without values. Removing such mapped attributes will increase performance.

- d. **Optional** If you want to return to the default mappings, click **Reset to Default**.

- e. If you are creating, click **Next** or **Save**. If you are editing, you can either save or select the next tab to edit.
  - f. If you subsequently make a change to the **Group Mappings** page, and after you have finished editing your synchronized user partition, you need to consolidate the synchronized partition. For more information, see “[Consolidating changes to users, groups, organizational units, and partitions](#)” on page 129.
12. On the **Monitoring** page, do the following:
- a. **Optional** If you want to monitor your identity provider for changes, select **Monitor changes** and then, from the list, specify how Directory Services should monitor for changes. This is dependent on the type of identity provider that you are using to create this user partition.

 **Note:** If OTDS has determined your identity provider type, the recommended monitoring setting will appear selected, by default.

For more information, see “[Defining a synchronized user partition](#)” on page 74 and “[Synchronization types](#)” on page 84.

 **Note:** The user specified on the **Authentication** page should have sufficient permissions in the identity provider to use the selected monitoring type. For example, in the case of a **USN query** method, the user should have permissions to read schema attributes and the deleted objects container.

If you intend making major changes, and you want to stop monitoring your identity provider for changes, clear the **Monitor changes** check box.
  - b. **Optional** If you want to test the selected monitoring on your current identity provider, click **Test Monitoring**, and then do one of the following:
    - If you click **Test** when creating a partition, and if your test succeeds, the message **Connected Successfully** appears. If your test fails, close the window, and then make any necessary corrections.
    - If you click **Test** when editing a partition, read the information provided, and then close the window.
  - c. **Optional** If you want to return to the default monitoring settings for this type of identity provider, click **Reset to Default**.
  - d. If you are creating, click **Next** or **Save**. If you are editing, you can either save or select the next tab to edit.
13. On the **Scheduler** page, do the following:
- a. If you want to enable automated full synchronization with your AD/LDAP server, under the **Actions** column, select **Enable**. Any enabled schedule can be disabled at a later time by selecting **Disable**.
-  **Note:** The scheduler uses the date and time setting on the server that functions as the master host of Directory Services.

- b. Using the boxes, select the day and time for the scheduled synchronization. After making a selection in a box, click **Save**.

In the **Time** box, to access a more complex option, click **Advanced**. You can now select either **Every** or **On each selected**. If you select **Every**, you need to use the boxes to select one number for **Hour(s)** and one number for **Minutes**. If you select **On each selected**, you can select multiple numbers under **Hours** and multiple numbers under **Minutes**.

After making any selection, make certain you click **Save**.

- c. **Optional** To add a new schedule, click **Add Schedule**, and then select the schedule days and time in the boxes.
- d. **Optional** If you want to delete a schedule, under the **Actions** column, click **Remove** next to the schedule you want to delete.



**Note:** You must have at least one schedule appearing on this page, although it does not need to be enabled.

If you click **Remove** next to any schedule, that schedule is removed immediately, there is no confirmation step.

- e. If you are creating, click **Next** or **Save**. If you are editing, you can either save or select the next tab to edit.

14. On the **Notifications/Search** page, do the following:

- a. From the **Search method** list, select the search method that suits your identity provider. The defaults are set based on the detected identity provider in use. However, you may change the search method based on the amount of user and group data being searched.

Depending on the search method you select, you may need to enter information to the **Page size** and / or **Sorting attribute** boxes. For more information, see “[Defining a synchronized user partition](#)” on page 74 and “[Search methods](#)” on page 85.

- b. If the search method you selected, for example **Paged search**, requires a value in the **Page size** box, enter a value in that box.
- c. If the search method you selected, for example **Virtual list view search**, requires a value in the **Sorting attribute** box, enter a value in that box.
- d. **Optional** If you want to perform a search on your identity provider with the selected search control, click **Test Search**, and then do one of the following:
  - If you click **Test** when creating a partition, and if your test succeeds, the message **Verified** appears. If your test fails, a window indicating the reason appears. Read the information provided, close the window, then make any necessary corrections.
  - If you click **Test** when editing a partition, a window is displayed indicating if the search control succeeded on your identity provider. Read the information provided, and then close the window.
- e. If you want to return to the default search method detected for your identity provider, click **Reset to Default**.

- f. If you are creating, click **Next** or **Save**. If you are editing, you can either save or select the next tab to edit.
15. On the **Extended Functionality** page, do the following:
- a. In the **UUID attribute** box, provide an attribute to map to the universally unique identifier to track deleted and moved users and groups. For more information, see “[Examples of UUIDs for supported servers](#)” on page 86.
  - b. In the **AD/LDAP user ID attribute** box, specify which identity provider attribute will be used to build OTDS user names.

For example, `sAMAccountName` is the default sign in attribute used for the AD/LDAP user ID attribute for Active Directory user partitions.

Another example, `uid`, is the default sign in attribute used for the AD/LDAP user ID attribute for LDAP user partitions. For more information, see “[AD/LDAP user and group ID attributes](#)” on page 86.
  - c. In the **AD/LDAP group ID attribute** box, specify which identity provider attribute will be used to build OTDS group names.

For example, `cn` is the default group attribute used for the AD/LDAP group ID attribute for LDAP user partitions. For more information, see “[AD/LDAP user and group ID attributes](#)” on page 86.
  - d. In the **OTDS Unique ID** box, select a method for Directory Services to determine the OTDS unique ID. This determines the unique ID of the user or group in OTDS. Different defaults will display depending on your selection and your site's configuration.

Select either **AD/LDAP attribute** or **Generated OTDS unique ID**. For more information, see “[Defining a synchronized user partition](#)” on page 74 and “[The OTDS unique ID](#)” on page 72. If you select **AD/LDAP attribute**, you must also enter the attribute that you want to use in the next box.
  - e. If you selected **AD/LDAP attribute**, then in the **AD/LDAP attribute** box, enter the attribute that you want to use.
  - f. **Optional** To verify that you have entered your information correctly, select the box to the left of the item you want to test, and then click the **Test** button. If your test succeeds, a message indicating success appears. If your test fails, close the information window, and then make any necessary corrections.
  - g. **Optional** If you want to return to the default attributes for this type of identity provider, click **Reset to Default**.
  - h. Click **Save**.
  - i. If you subsequently make a change to the **Extended Functionality** page, and after you have finished editing your synchronized user partition, you need to consolidate the synchronized partition. For more information, see “[Consolidating changes to users, groups, organizational units, and partitions](#)” on page 129.



**Tip:** If available, you can click **Consolidate** from the **Actions** menu to make any changes to your users and groups effective. For more

information, see “[Consolidating users and groups in Partitions](#)” on page 128.

### 3.8.3 Editing a synchronized user partition

#### To edit a synchronized user partition:

1. From the web administration menu, click **Partitions**.
2. From the **Actions** menu associated with the partition you want to edit, click **Properties**.
3. Follow the instructions, beginning with step 4, found in “[Creating a synchronized user partition](#)” on page 87.
4. **[Optional]** Under the **Actions** heading, click **Actions** associated with any partition you want to edit, and then do the following:
  - If you want to duplicate this partition, click **Duplicate Partition**, and then see “[Duplicating a synchronized user partition](#)” on page 100.
  - If you want to edit members, click **View Members**, and then see “[Editing members of groups in a synchronized user partition](#)” on page 98.
  - If you want to restart this partition, click **Restart**, and then see “[Restarting a synchronized user partition](#)” on page 99.
  - If you want to import users and groups, click **Import Users and Groups**, and then see “[Importing users and groups](#)” on page 98.
  - If you want to set two-factor authentication, click **Two Factor Auth Settings**, and then see “[Enabling two-factor authentication](#)” on page 99.
  - If you want to create attributes for this partition, click **Partition Attributes** and then see “[Creating system or custom attributes for one partition](#)” on page 134.
  - If you want to enable or disable this partition, click **Enable/Disable Partition**, and then see “[Enabling or disabling a user partition](#)” on page 135.
  - If you want to allocate this partition to a license, click **Allocate to License** and then see “[Allocate to license](#)” on page 247.



#### Important

OpenText recommends that you do not select this option. No products currently use this functionality.

- If you want to delete this partition, see “[Deleting a synchronized user partition](#)” on page 101.
- If you want to consolidate changes to users and groups, see “[Consolidating changes to users, groups, organizational units, and partitions](#)” on page 129.

### 3.8.4 Setting a password policy for a synchronized user partition

It is not possible to set a password policy for synchronized user partitions.

### 3.8.5 Importing users and groups

Synchronized User Partitions are color-coded to indicate their status. For example, a synchronized user partition can appear with a background color to indicate that it requires the importing or consolidation of users and groups:

- **White:** no import or consolidation is required.
- **Green:** an import or a consolidation is in progress.
- **Yellow:** an import or a consolidation is required. For more information, see “[Importing users and groups](#)” on page 98 or “[Consolidating changes to users, groups, organizational units, and partitions](#)” on page 129.
- **Red:** an import or a consolidation failed.

#### To import users and groups:

1. From the web administration menu, click **Partitions**, and then click **Actions** next to your user partition.
2. From the **Actions** menu, click **Import Users and Groups**.



**Note:** The **Import Users and Groups** option is only available if you did not perform the import when you created your synchronized user partition. After you have successfully imported users and groups to the synchronized user partition, the **Import Users and Groups** option will no longer appear as an option on the menu. In the event you need to, you can perform a consolidate operation. For more information, see “[Consolidating changes to users, groups, organizational units, and partitions](#)” on page 129.

### 3.8.6 Editing members of groups in a synchronized user partition

You cannot modify members of groups in a synchronized user partition from OTDS. Any changes you want to make to group membership of a group in a synchronized user partition need to be made on the sync source.

### 3.8.7 Restarting a synchronized user partition

This operation is intended to assist you in troubleshooting when you encounter issues.

**!** **Important**

OpenText recommends that you do not perform a **Restart** action unless directed by OpenText technical support.

**To restart a synchronized user partition:**

1. From the web administration menu, click **Partitions**.
2. From the **Actions** menu of the synchronized user partition you want to restart, click **Restart**.
3. In the **Restart** confirmation box, click **Restart** to confirm.

### 3.8.8 Enabling two-factor authentication

**To enable two-factor authentication:**

You can choose to enable two-factor authentication:

- Globally, for *all* users, groups, organizational units, and partitions; or
- Individually, for *specific* users, groups, organizational units, and partitions.

You can choose to define settings at one level and then define at a lower level to override those settings. For example, you can enable two-factor authentication globally but define it as disabled for a specific user, group, organizational unit, or partition.

For background information describing these settings, see “[Configuring two-factor authentication](#)” on page 237.

1. **Optional** If you want to set two-factor authentication *global settings* for all users, groups, organizational units, and partitions:
  - a. From the web administration menu, click **Partitions**.
  - b. On the **Partitions** page, on the button bar, click **Global Settings**. From the **Global Settings** menu, click **Two Factor Auth Settings**.
  - c. In the **Two Factor Authentication Settings - Global** box, select **Enable two factor authentication**.
  - d. Select any of the options to apply two-factor authentication settings. For more information, see the **Define Settings** options in “[Configuring two-factor authentication](#)” on page 237.
  - e. Click **OK**.
2. **Optional** If you want to set two-factor authentication at a *specific* user, group, organizational unit, or partition level:

- a. From the web administration menu:
  - If you want to set two-factor authentication for a user, group, or organizational unit, click **Users & Groups**.
  - If you want to set two-factor authentication for a partition, click **Partitions**.
- b. On either the **Users & Groups** page or the **Partitions** page, find the user, group, organizational unit, or partition for whose users you want to enable two-factor authentication.
- c. From the **Actions** menu associated with the user, group, organizational unit, or partition you want to edit, click **Two Factor Auth Settings**.
- d. In the **Two Factor Authentication Settings - <item\_name>** box, from the **Two Factor Authentication Settings** list, select either **Inherit settings** or **Define settings**, and then, do the following:
  - i. If you select **Inherit settings** for a partition, an organizational unit, a group, or a user, and two-factor authentication has not been enabled for the parent object or in the *global settings* box, two-factor authentication will not be enabled. For information about enabling global settings, see the first step in this procedure.  
If you select **Inherit settings** for a partition, two-factor authentication will be enabled according to the *global settings*.  
The **Two Factor Authentication Settings** box will display, dimmed, the inherited settings that will be applied. If these are not the settings you want applied, change your selection to **Define settings** to make changes.
  - ii. If you select **Define settings** for a partition, an organizational unit, a group, or a user, select any of the options to apply two-factor authentication settings. For a description of these options, see [“Configuring two-factor authentication” on page 237](#).
  - iii. Click **OK**.



**Note:** For information about resetting a user's secret key, see [“Resetting a user's secret key” on page 240](#).

### 3.8.9 Duplicating a synchronized user partition

**To duplicate a synchronized user partition:**

1. From the web administration menu, click **Partitions**.



**Tip:** You may want to duplicate a synchronized user partition when you want to save a partition's configuration before making changes that you want to test.

2. From the **Actions** menu of the synchronized user partition you want to duplicate, click **Duplicate Partition**.

3. In the **Duplicate** box, in the **Duplicate Partition Name** box, type the name for this new user partition.
4. **[Optional]** Click **Verify Partition Name** if you want to verify that you have entered a unique partition name.
5. Click **OK**.

### 3.8.10 Deleting a synchronized user partition

**To delete a synchronized user partition:**

1. From the web administration menu, click **Partitions**.
2. Click to select the box to the left of the partition you want to delete, and then, on the button bar, click **Delete**.
3. You need to confirm that you want to delete this user partition and all the users and groups in it.

**!** **Important**

1. The users and groups will be removed from the resources that are using them.
2. Users and groups from a deleted partition(s) will not be moved to the Recycle Bin. Any users and groups from a deleted partition(s) currently in the Recycle Bin will be deleted.
4. In the **Delete Partition(s)** box, click **Delete**.



**Tip:** If there are a large number of users and groups in a user partition, this action may take a long time. The **deleting...** status indicator appears beside the user partition name until the server has completed the operation. Click **Refresh** to determine if the server has completed the deletion. For more information, see “[Jobs](#)” on page 363.

## 3.9 Non-synchronized user partitions

This section describes creating, editing, deleting and manually adding user and group data in non-synchronized user partitions.

### 3.9.1 Defining a non-synchronized user partition

You will need to create a non-synchronized user partition when you have users that are identified solely within the Directory Services server. These users might be administrators or temporary employees who are not identified by an identity provider.

#### 3.9.1.1 Configuring users in a non-synchronized user partition

The following sections deal with user accounts and passwords.

##### Password requirements

The minimum password requirements are determined by the **Password Policy** that applies to this user. Password policies apply to all users in a non-synchronized user partition. The default password policy requires the following when entering or changing a user account password:

1. Your password must be at least eight characters in length.
2. Your password must be complex. It must include one each of the following:
  - Lowercase letters (a through z)
  - Uppercase letters (A through Z)
  - Digits (0 through 9)
  - Non-alphanumeric characters. For example: , . ! @ # \$ %
3. You must supply at least three unique passwords before a password can be reused.

You can change the password policy for your non-synchronized user partition. For more information, see [“Password policy for non-synchronized user partitions” on page 125](#).



**Note:** In OpenText Content Management, there is a setting in the `opentext.ini` file called **ChangePWAtFirstLogin** that determines whether users are required to change their password at first sign in. If set to “TRUE”, an OpenText Content Management user will be presented with a **Welcome** window where they must enter and confirm a new password.

##### Password complexity

If you choose to leave the default password policy rules for users when they are setting their password, the following characters must be present:

- Lowercase letters (a through z)
- Uppercase letters (A through Z)
- Digits (0 through 9)
- Non-alphanumeric characters. For example: , . ! @ # \$ %

An example of a strong password is: Alps5Sud!



**Note:** In addition to the default password rules, you can choose to ensure that users cannot use sequential characters (uppercase or lowercase) from their username.

## User accounts can have a status of locked out, disabled, or expired

A user account is *locked out* after a user attempts to sign in using three consecutive incorrect passwords. The user account can be unlocked by waiting for the lockout period (default 15 minutes), or by explicitly unlocking the account by clearing the **Account is locked out** box, or by resetting the user's password. When locked out, an account can only be unlocked, or its password reset, by an administrator. For more information, see [“Unlocking an account” on page 114](#) and [“Resetting a user password in a non-synchronized user partition” on page 113](#).

A user's account status can be set to *disabled* by an administrator to temporarily prevent a user from signing in to their resources. For example, this can be used to temporarily prevent a user from having access to resources while they are on leave without removing their account or access roles. When the administrator clears the **Account is disabled** check box, the user will be allowed to sign in again.

A user's account status can be set to *expired* by an administrator setting an expiry date and time on that user's account. For more information, see **Account expires** in [“Creating users in a non-synchronized user partition” on page 109](#).

## What happens when a user password expires

When a user password expires, Directory Services Authentication Service will present a **Welcome** window where users can enter and confirm a new password.

### 3.9.1.1.1 Using WebAuthn to provide users the option of passwordless authentication

You can enable passwordless authentication for users using the WebAuthn authentication.

Passwordless authentication is a method of authenticating a user which requires only the user's unique identifier and a public key.

If you want to allow users to be able to choose to go passwordless, you will need to do the following:

#### To enable passwordless authentication for users:

1. If it has not already been created, create the **WebAuthn** authentication handler. This authentication handler can be applied globally or on a specific partition. For more information, see [WebAuthn on page 157](#) and [“Creating an authentication handler” on page 162](#).

**!** **Important**

When creating the WebAuthn authentication handler, ensure you select **entryDN** as the **Authentication principal attribute** on the **Configuration** tab.



**Note:** DN refers to the Distinguished Name of an entity. Every entity in OTDS has a distinguished name (DN). The DN is the name that uniquely identifies that entity in OTDS.

2. If it has not already been created, create the **directory.auth.TwoStepLogin** system attribute. Set this attribute to “true”. This attribute can be applied globally or on a specific partition. For more information, see [Two Step Login on page 313](#).
3. If it has not already been created, create the **directory.auth.WebAuthnPolicy** system attribute. This attribute can be applied globally or on a specific partition. You will need to choose one of the following as the **Value** of this system attribute:
  - **ALLOW**: users can choose whether or not to register with WebAuthn and enable passwordless authentication.
  - **REQUIRE**: users must register with WebAuthn.  
Organizations that want to enforce strong authentication, without passwords or two-factor authentication, might consider this option.
  - **BLOCK**: users cannot register with WebAuthn.  
Organizations that currently use a third party, two-factor authentication provider, and do not want to alter the current user experience, might consider this option.

For more information, see [WebAuthn Policy on page 314](#).

4. Users can now access the passwordless option at signup, at password reset, or at password change.
5. Administrators can see whether a user is using passwordless authentication in that user's account properties page. For information about user account settings, see [“Creating users in a non-synchronized user partition” on page 109](#).  
Administrators will see a warning that a user is using passwordless authentication if the administrator attempts to reset that user's password. For more information, see [“Resetting a user password in a non-synchronized user partition” on page 113](#).

For background information about Web Authentication, see WebAuthn (<https://en.wikipedia.org/wiki/WebAuthn>).

### 3.9.1.2 Creating groups in a non-synchronized user partition

To create a new group in a non-synchronized user partition, you must use the **New Group** assistant in the **Partitions** object. For more information, see “[Creating groups in a non-synchronized user partition](#)” on page 116.

You can only edit properties of groups in non-synchronized user partitions. For more information, see “[Editing groups in a non-synchronized user partition](#)” on page 117.

To delete a group from a non-synchronized user partition, you must use the **Delete** action in the **Partitions** object. For more information, see “[Deleting groups in a non-synchronized user partition](#)” on page 121.

### 3.9.1.3 Creating organizational units in a non-synchronized user partition

An organizational unit is another grouping of users and groups that helps you keep track of users and groups and their access roles in your non-synchronized user partition within the OTDS web client. An organizational unit is not generally considered to have members or to be a member of another object. An organizational unit may contain users, groups, and other organizational units, but the term *member* is generally reserved for group membership. An organizational unit may be added to an access role, but not to a group. Users, groups and organizational units in non-synchronized user partitions will be displayed in the **Users & Groups** object in the Directory Services web administration menu, and they may be deleted or edited from there. However, to create any of these objects, you must be exploring a non-synchronized user partition because that is the only place Directory Services supports their creation.

When an organizational unit has been added to an access role, only users in that organizational unit will be given accounts on resources to which the access role has been added. The groups in the organizational unit will not be pushed to the resources that the access role has been added to.

Organizational units in non-synchronized user partitions are structured folders for organizing users and groups. To add a user or a group to an organizational unit, you must create the organizational unit, select it, and then use the **New User** or **New Group** actions to add users or groups to that organizational unit. For more information, see “[Creating an organizational unit in a non-synchronized user partition](#)” on page 122.

To create a new organizational unit in a non-synchronized user partition, you must use the **New Organizational Unit** assistant in the **Partitions** object. For more information, see “[Creating an organizational unit in a non-synchronized user partition](#)” on page 122.

You can only edit properties of organizational units in non-synchronized user partitions. For more information, see “[Editing organizational units in a non-synchronized user partition](#)” on page 122.

You can only delete organizational unit from a non-synchronized user partition. You must use the **Delete** action in the **Partitions** object. For more information, see “[Deleting organizational units in a non-synchronized user partition](#)” on page 124.

It is possible to set a password policy that applies to all users in a non-synchronized user partition. For more information, see “[Password complexity](#)” on page 102.

### 3.9.2 Creating a non-synchronized user partition

**To create a non-synchronized user partition:**

1. From the web administration menu, click **Partitions**.
2. From the button bar, click **Add**. From the **Add** list, select **New Non-synchronized User Partition**, and then do the following:
  - a. In the **Name** box, type a descriptive name for your user partition. Use the same best practices for naming your non-synchronized user partition as you use for synchronized user partitions. For more information, see “[Naming the user partition](#)” on page 69. If your name is a unique partition name, the icon next to the **Name** box will display a green check mark.
  - b. **Optional** In the **Description** box, type a brief description of the purpose of this non-synchronized user partition.
  - c. Click **Save** to create your non-synchronized user partition.
3. **Optional** Add users to your non-synchronized user partition. For more information, see “[Creating users in a non-synchronized user partition](#)” on page 109.
4. **Optional** Add groups to your non-synchronized user partition. For more information, see “[Creating groups in a non-synchronized user partition](#)” on page 116.
5. **Optional** Add organizational units to your non-synchronized user partition. For more information, see “[Creating an organizational unit in a non-synchronized user partition](#)” on page 122.
6. **Optional** Configure a password policy for your non-synchronized user partition. For more information, see “[Password complexity](#)” on page 102.

### 3.9.3 Editing a non-synchronized user partition

#### To edit a non-synchronized user partition:

1. From the web administration menu, click **Partitions**.
2. The user partition **Name** box cannot be edited.
3. **Optional** Click in the **Description** box to edit your non-synchronized user partition description, and then click **Save**.
4. **Optional** Under the **Actions** heading, click **Actions** associated with the non-synchronized user partition you want to edit, and then do any of the following:
  - If you want to edit the administrators of this non-synchronized user partition, from the **Actions** menu, click **Edit Administrators**, and then follow the instructions in “[Editing administrators of groups in a non-synchronized user partition](#)” on page 119.
  - If you want to view the members of this non-synchronized user partition, from the **Actions** menu, click **View Members**, and then follow the instructions in “[Creating users in a non-synchronized user partition](#)” on page 109 or “[Creating groups in a non-synchronized user partition](#)” on page 116.
  - If you want to edit the password policy of this non-synchronized user partition, from the **Actions** menu, click **Password Policy**, and then follow the instructions in “[Defining a password policy for one non-synchronized user partition](#)” on page 125.
  - If you want to apply partition restrictions to this non-synchronized user partition, from the **Actions** menu, click **Partition Restrictions**, and then follow the instructions in “[Configuring partition restrictions](#)” on page 114.
  - If you want to consolidate this non-synchronized user partition, from the **Actions** menu, click **Consolidate**, and then follow the instructions in “[Consolidating changes to users, groups, organizational units, and partitions](#)” on page 129.
  - If you want to edit the two-factor authentication settings of this non-synchronized user partition, from the **Actions** menu, click **Two Factor Auth Settings**, and then follow the instructions in “[Enabling two-factor authentication](#)” on page 245.
  - If you want to create attributes for this non-synchronized partition, from the **Actions** menu, click **Partition Attributes**, and then follow the instructions in “[Partition attributes](#)” on page 132.
  - If you want to enable or disable this non-synchronized user partition, from the **Actions** menu, click **Enable Partition or Disable Partition** and then follow the instructions in “[Disabling a user partition](#)” on page 135.
  - If you want to allocate this non-synchronized user partition to a license, from the **Actions** menu, click **Allocate to License**, and then follow the instructions in “[Allocate to license](#)” on page 247.

**!** **Important**

OpenText recommends that you do not select this option. No products currently use this functionality.

- If you want to delete this non-synchronized user partition, see “[Deleting a non-synchronized user partition](#)” on page 108.

### 3.9.4 Deleting a non-synchronized user partition

**To delete a non-synchronized user partition:**

1. From the web administration menu, click **Partitions**.
2. Click to select the box to the left of the user partition name you want to delete, and then, from the button bar, click **Delete**.



**Note:** You cannot delete the non-synchronized user partition `otds.admin` because it contains administrative users and groups that allow you to make changes to all Directory Services. Without these users and groups you would not be allowed to sign in to your Directory Services server in the web administration client.

You further cannot disable the non-synchronized user partition `otds.admin` because disabling a user partition does not allow users in that partition to sign in to Directory Services.

3. Confirm that you want to delete this user partition and all the users and groups in it.

**Important**

1. The users and groups will be removed from the resources that are using them.
2. Users and groups from a deleted partition(s) will not be moved to the Recycle Bin. Any users and groups from a deleted partition(s) currently in the Recycle Bin will be deleted.
4. In the **Delete Partition(s)** box, click **Delete**.



**Tip:** If there are a large number of users and groups in a user partition, this action may take a long time. The **deleting** status indicator appears beside the user partition name until the server has completed the operation. Click **Refresh** to determine if the server has completed the deletion.

### 3.9.5 Creating users in a non-synchronized user partition

#### To create users in a non-synchronized user partition:

1. From the web administration menu, click **Partitions**.
2. From the **Actions** menu of the non-synchronized user partition in which you want to create a user, click **View Members**.
3. On the button bar, click **Add**. From the **Add** menu, select **New User**.
4. On the **General** page, do the following:
  - a. In the **User Name** box, type the name of this user.
  - b. **Optional** In the **First name** box, type the first name of the user.
  - c. **Optional** In the **Last name** box, type the last name of the user.
  - d. **Optional** All other boxes are optional. They allow you to supply additional information about this user, if you want.
  - e. If you have finished adding information for your new user, click **Save**. To continue to the next page, click **Next**.
5. On the **Account** page, do the following:
  - a. In the **Account Information** area, the **Last login time** field is informational only and cannot be edited. This field displays the date and time that the user last signed into OTDS in the form: <MM>/<DD>/<YYYY> <HR>:<MN> [AM | PM], where:
    - <MM> is a two digit number between 01 and 12, representing the month.
    - <DD> is a two digit number between 01 and 31, representing the day.
    - <YYYY> is a four digit year.
    - <HR> is a two digit number between 01 and 12, representing the hour.
    - <MN> is a two digit number between 01 and 59, representing the minute.

If the user is accessing OTDS with passwordless authentication, an information message will be displayed.

- b. **Optional** In the **Account Options** area, do the following:
  - i. The **Account is locked out** box will only be useable if the user account you are reviewing has been locked out by OTDS. In the event the user has been locked out, you can choose to clear this box to unlock that user's account. For more information, see “[User accounts can have a status of locked out, disabled, or expired](#)” on page 103.
  - ii. Select the **Account is disabled** box if you want to deny this user sign in privileges on your resources.

By default, a user account is enabled, allowing the user to sign in to the resources to which they have access. If you select this box, the user can

no longer sign in to those resources. For example, this can be used to temporarily prevent a user from having access to resources, while they are on leave, without removing their account or access roles. This can be changed later by editing the user. For more information, see “[User accounts can have a status of locked out, disabled, or expired](#)” on page 103.

- iii. Select the **Account expires** box if you want to set an absolute date and time beyond which this user cannot sign in to OTDS. After selecting the box, use the calendar picker to select the year, month, day, hour, and minute. You are also required to select either AM or PM. The expiry date you select can be changed or removed at any time.
- c. In the **Password Options** area, from the list, select one of the following:
  - **Require password change on reset:** to force the user to change their password when it has been reset by the administrator.
-  **Note:** This option also applies when a user is first created. This occurs because a newly set password constitutes a password reset.
- **Do not require password change on reset:** to ensure that the user does not need to change their password when it has been reset by the administrator.
- Under this option, to further manage password changes, you can also choose to select either or both of:
  - **User cannot change password**
  - **Password never expires**
- d. In the **Initial Password** area, do the following:
  - i. In the **Password** box, type the initial password of the new user. The password you type must meet the minimum complexity requirements. For more information, see “[Password requirements](#)” on page 102.
  - ii. In the **Confirm password** box, re-type the initial password of the new user. The passwords must be identical.
- e. If you have finished adding information for your new user, click **Save**. To continue to the next page, click **Next**.
6. **Optional** On the **Organization** page, you can choose to specify any general organization information. If you have finished adding information for your new user, click **Save**. To continue to the next page, click **Next**.
7. **Optional** On the **User Attributes** page, you can choose to specify any additional user attribute values. For more information, see “[Defining user attributes](#)” on page 70.
8. **Optional** On the **Custom Attributes** page, you can choose to specify any additional custom attribute values, or edit existing custom attributes.



**Note:** OpenText recommends that you do not create custom attributes. This option is intended for applications that integrate with OTDS to allow them to store their application properties.

- a. Click **Add Custom Attribute**.
    - i. In the **Type** box, enter the type of custom attribute you are defining.
    - ii. In the **Name** box, enter a name for this custom attribute.
    - iii. In the **Value** box, if you require it, enter a value for your custom attribute.
    - iv. Click **Save** to the right of your custom attribute.
  - b. To delete a custom attribute, select the check box to the left of the custom attribute you want to delete, and then click **Delete Selected Attributes**.
  - c. To remove all custom attributes, click **Clear All Attributes**.
9. On the button bar, click **Save**.



**Note:** If you did not meet the password requirements when you typed the user password, a warning message will appear detailing the minimum password requirements. You will not be able to save the user until you have met the minimum password requirements.

### 3.9.6 Editing users in a non-synchronized user partition

**To edit users in a non-synchronized user partition:**

1. From the web administration menu, click **Users & Groups**, and then select the **Users** tab.



**Tip:** You can also, from the web administration menu, click **Partitions** and then, from the non-synchronized user partition's **Actions** menu, select **View Members**. Select the **Users** tab.

2. From the **Actions** menu associated with the user you want to edit, click **Properties**. You can use the search box to find the user.
  - a. Follow the instructions, beginning with step 4, found in [“Creating users in a non-synchronized user partition” on page 109](#).
  - b. When you have finished editing, on the button bar, click **Save**.
3. **Optional** From the **Actions** menu associated with any user you want to edit, do the following:
  - If you want to consolidate this user, click **Consolidate**, and then see [“Consolidating users in a partition” on page 112](#).
  - If you want to set two factor authentication for this user, click **Two Factor Auth Settings**, and then see [“Enabling two-factor authentication” on page 115](#).

- If you want to edit the groups to which this user belongs, click **Edit Membership**, and then see “[Editing members of groups in a non-synchronized user partition](#)” on page 118.
- If you want to view recursive memberships for this user, click **View Recursive Membership**, and then see “[To view all application roles \(recursively\) assigned to a specific user, group, or application role](#)” on page 266.
- If you want to edit the application roles to which this user belongs, click **Edit Application Roles**, and then see “[Editing an application role](#)” on page 263.
- If you want to view the application roles to which this user belongs, click **View Effective Roles**, and then see “[Editing an application role](#)” on page 263.
- If you want to reset this user's password, click **Reset Password**, and then see “[Resetting a user password in a non-synchronized user partition](#)” on page 113.
- If you want to allocate this user to a license, click **Allocate to License**, and then see “[Allocate to license](#)” on page 247.

**!** **Important**

OpenText recommends that you do not select this option. No products currently use this functionality.

- If you want to delete this user, see “[Deleting users in a non-synchronized user partition](#)” on page 115.

### 3.9.7 Consolidating users in a partition

Choose one of the two procedures below, depending on whether you want to consolidate an existing user or consolidate a missing user.

#### To consolidate an existing user:

1. From the web administration menu, click **Users & Groups**.
2. In the center of the page, select the **Users** tab.



**Tip:** You can also, from the web administration menu, click **Partitions** and then, from the user partition's **Actions** menu, select **View Members**. Select the **Users** tab.

3. From the **Actions** menu associated with the user you want to consolidate, select **Consolidate**. You can use the **Search** box to find the user.
4. In the **Consolidate <userid>** box, do the following:
  - a. In the **Consolidate options** area, do the following:

- i. **Optional** If you are consolidating a synchronized user partition and you want to consolidate the selected object in OTDS with the identity provider, AD or LDAP, select **Consolidate with identity provider**.
- ii. **Optional** If you want to direct OTDS to verify and repair a discrepancy in its internal referential integrity attributes, for example `oTMember` or `oTMemberOf`, select **Verify and repair**.
 

 **Note:** OpenText recommends that you do not perform a **Verify and repair** operation unless directed to by OpenText technical support.
- b. If you are consolidating an object in a synchronized user partition, then in the **Consolidate with the following resources** area, select all resources with which the previously selected object will be consolidated with information in OTDS.
 

 **Note:** Consolidation operations may take a long time to complete. You can monitor the process through the ["directory-provenance.log" on page 376](#) file.
- c. Click **Consolidate** to consolidate user data for the selected existing user.

#### To consolidate a missing user:

If you know of a user who should be present in OTDS but is not listed, you can consolidate that missing user as follows:

1. From the button bar, click **Consolidate**.
2. From the **Consolidate** menu, click **Consolidate Missing User**.
3. In the **Account DN** box, enter the DN of the missing user in the **User DN** box.
4. Click **OK**.

### 3.9.8 Resetting a user password in a non-synchronized user partition

#### To reset a user password in a non-synchronized user partition:

1. From the web administration menu, click **Users & Groups**, and then select the **Users** tab.

 **Tip:** You can also, from the web administration menu, click **Partitions** and then, from the non-synchronized user partition's **Actions** menu, select **View Members**. Select the **Users** tab.

2. Select the user for whom you want the password reset, or use the **Search** box to find the user.

From the **Actions** menu associated with the user whose password you want to reset, select **Reset Password**.

3. If the user whose password you are attempting to reset is currently using passwordless authentication, you will see a warning. For more information, see ["Using WebAuthn to provide users the option of passwordless authentication"](#) on page 103.
4. In the **Reset Password** box, do the following:
  - a. The **User name** text box cannot be edited.
  - b. In the **New password** text box, enter a new password for this user.
  - c. In the **Confirm new password** text box, re-type exactly the new password for this user.
  - d. Click **Reset Password** to change the password.

### 3.9.9 Unlocking an account

**To unlock an account:**

1. From the web administration menu, click **Users & Groups**, and then select the **Users** tab.



**Tip:** You can also, from the web administration menu, click **Partitions** and then, from the non-synchronized user partition's **Actions** menu, select **View Members**. Select the **Users** tab.

2. Select the user whose account you want unlocked, or use the **Search** box to find the user.

From the **Actions** menu associated with the user whose account you want to unlock, select **Properties**.

3. On the **Account** tab, clear the **Account is locked out** box.
4. Click **Save**.

### 3.9.10 Configuring partition restrictions

**To configure partition restrictions:**

1. From the web administration menu, click **Partitions**.



#### Important

The **Partition Restrictions** option is intended for non-synchronized partitions that will be used in the OpenText cloud. Any restrictions created here will apply to objects created from Enterprise Directory Sync.

OpenText recommends that you do not apply partition restrictions to any non-synchronized partition unless directed to do so by OpenText.

2. From the **Actions** menu of the non-synchronized user partition you want to configure, click **Partition Restrictions**.

3. In the **Partition Restrictions <non-sync\_partition\_name>** box, in the **Maximum Number of Users** box, to restrict the number of users that can be created from Enterprise Directory Synchronization, enter the maximum number of users allowed.  
The default is “-1”, meaning no restriction on the number of users that can be created.
4. In the **Maximum Number of Groups** box, to restrict the number of groups that can be created from Enterprise Directory Synchronization, enter the maximum number of groups allowed.  
The default is “-1”, meaning no restriction on the number of groups that can be created.
5. **Optional** In the **Allowed Domains** box, if left blank, all domains will be allowed. If you include any domain in this box, OTDS will check to see if a user's or group's attribute has a configured domain. If so, the domain must be listed in this box before the user or group will be imported.  
OTDS will check the following attributes: email, oTExternalId1, oTExternalId2, oTExternalId3, or oTExternalId4.
  - a. You can optionally type or select a domain name. If left blank, the default setting, then all domains will be permitted.
  - b. To add or remove a domain to or from this non-synchronized partition, from the list, select an available domain, and then click **Add/Delete**.
6. The **Bind authentication to allowed domains** box is for OpenText internal use only.
7. Click **OK**.

### 3.9.11 Enabling two-factor authentication

You can enable two-factor authentication for one, or multiple, users. Look up the users for whom you want to enable two-factor authentication, and then follow the instructions found in [“Enabling two-factor authentication” on page 99](#).

### 3.9.12 Deleting users in a non-synchronized user partition

#### To delete users in a non-synchronized user partition:

1. From the web administration menu, click **Users & Groups**, and then select the **Users** tab.



**Tip:** You can also, from the web administration menu, click **Partitions** and then, from the non-synchronized user partition's **Actions** menu, select **View Members**. Select the **Users** tab.

2. Select the user that you want to delete or use the **Search** box to find the user. Select the box to the left of the user you want to delete, and then, from the button bar, click **Delete**.

3. Confirm that you want to delete this user by clicking **OK**.

### 3.9.13 Creating groups in a non-synchronized user partition

**To create groups in a non-synchronized user partition:**

1. From the web administration menu, click **Partitions**.
2. From the non-synchronized user partition's **Actions** menu, select **View Members**. Select the **Groups** tab.
3. On the button bar, click **Add**. From the **Add** menu, click **New Group**.
4. On the **General** page, do the following:
  - a. In the **Group name** box, type a name for this group.
  - b. **Optional** All other boxes are optional. They allow you to supply additional information about this group, if you want.
  - c. Click **Next** to access the next tab, or click **Save** if you have finished.
5. **Optional** On the **Group Attributes** page, specify any additional group attribute values, and then click **Next**. For more information, see “[Defining group attributes](#)” on page 72.
6. **Optional** On the **Custom Attributes** page, you can choose to specify additional custom attribute values, or edit existing custom attributes.



**Note:** OpenText recommends that you do not create custom attributes. This option is intended for applications that integrate with OTDS to allow them to store their application properties.

- a. On the **Custom Attributes** tab click **Add Custom Attribute**.
    - i. In the **Type** box, enter the type of custom attribute you are defining.
    - ii. In the **Name** box, enter a name for this custom attribute.
    - iii. In the **Value** box, if you require it, enter a value for your custom attribute.
    - iv. Click **Save** to the right of your custom attribute.
  - b. To delete a custom attribute, select the check box to the left of the custom attribute you want to delete, and then click **Delete Selected Attributes**.
  - c. To remove all custom attributes, click **Clear All Attributes**.
7. On the button bar, click **Save**.

### 3.9.14 Editing groups in a non-synchronized user partition

#### To edit groups in a non-synchronized user partition:

1. From the web administration menu, click **Users & Groups**, and then select the **Groups** tab.



**Tip:** You can also, from the web administration menu, click **Partitions** and then, from the non-synchronized user partition's **Actions** menu, select **View Members**. Select the **Groups** tab.

2. Select the group that you want to edit, or use the **Search** box to find the group. From the group's **Actions** menu, click **Properties**.
  - a. Follow the instructions, beginning with step 4, found in [“Creating groups in a non-synchronized user partition” on page 116](#).
  - b. When you have finished editing, on the button bar, click **Save**.
3. **[Optional]** From the **Actions** menu associated with any group you want to edit, do the following:
  - If you want to consolidate this group, click **Consolidate**, and then see [“Consolidating groups in a partition” on page 120](#).
  - If you want to set two factor authentication for this group, click **Two Factor Auth Settings**, and then see [“Enabling two-factor authentication” on page 99](#).
  - If you want to edit the groups to which this group belongs, click **Edit Membership**, and then see [“Editing members of groups in a non-synchronized user partition” on page 118](#).
  - If you want to view recursive memberships for this group, click **View Recursive Membership**, and then see [“To view all application roles \(recursively\) assigned to a specific user, group, or application role” on page 266](#).
  - If you want to edit the application roles to which this group belongs, click **Edit Application Roles**, and then see [“Editing an application role” on page 263](#).
  - If you want to view the application roles to which this group belongs, click **View Effective Roles**, and then see [“Editing an application role” on page 263](#).
  - If you want to edit the administrators of this group, click **Edit Administrators**, and then see [“Editing administrators of groups in a non-synchronized user partition” on page 119](#).
  - If you want to allocate this group to a license, click **Allocate to License**, and then see [“Allocate to license” on page 247](#).

**!** **Important**

OpenText recommends that you do not select this option. No products currently use this functionality.

- If you want to delete this group, see “[Deleting groups in a non-synchronized user partition](#)” on page 121.
- 4. On the button bar, click **Save**.

### 3.9.15 Editing members of groups in a non-synchronized user partition

**To edit members of groups:**

1. From the web administration menu, click **Users & Groups**, and then select the **Groups** tab.



**Tip:** You can also, from the web administration menu, click **Partitions** and then, from the **Actions** menu of the partition you want to edit, select **View Members**. Next, select the **Groups** tab.

2. Find the group that you want to edit, or use the **Search** box to find the group. From the **Actions** menu associated with the group whose members you want to edit, select **Edit Membership**.
3. On the `<group_name>@<partition_name>` page, on the **Members** tab, to add a member to this group, on the button bar, click **Add Member**:



**Note:** You cannot add any item to synchronized groups.

- a. In the **Users and Groups Associations** box, use the **Search** box to find members to add to the group. From the search results box, select the check box to the left of the members you want to add to the group, and then click **Add Selected**.
  - b. Continue searching for, and adding, members. After you have finished adding members to this group, in the **Users and Groups Associations** box, click **Close**.
4. If you want to add a member to the list of groups that this group, `<group_name>@<partition_name>`, is a “member of”, on the `<group_name>@<partition_name>` page, click the **Member Of** tab:
    - a. On the button bar of the `<group_name>@<partition_name>` page, click **Add To Group**.
    - b. In the **Users and Groups Associations** box, use the **Search** box to find a member to add to the group that this group is a “member of”. From the search results box, select the check box to the left of the members you want to add, and then click **Add Selected**.

- c. Continue searching for, and adding, members. After you have finished adding members, in the **Users and Groups Associations** box, click **Close**.
  5. **Optional** If you want to remove a user from the group:
    - a. On the  $<group\_name>@<partition\_name>$  page, click the **Members** tab. On the **Members** page, select the check box to the left of the user you want to remove, and then click **Remove Member**.
    - b. Confirm you want to remove this user.
-  **Note:** When you remove a user as a member of a group, you do not delete the user.
6. **Optional** If you want to remove a member from the group that this group is a "member of":
    - a. On the  $<group\_name>@<partition\_name>$  page, click the **Member Of** tab. On the **Member Of** page, select the check box to the left of the user you want to remove, and then click **Remove From Group**.
    - b. Confirm you want to remove this member.
-  **Note:** When you remove a member of a group, you do not delete the member.

### 3.9.16 Editing administrators of groups in a non-synchronized user partition

#### To edit administrators of groups:

1. From the web administration menu, click **Users & Groups**.
  2. In the center of the page, select the **Groups** tab.
-  **Tip:** You can also, from the web administration menu, click **Partitions** and then, from the non-synchronized user partition's **Actions** menu, select **View Members**. Select the **Groups** tab.
3. Select the group that you want to edit, or use the **Search** box to find the group.
  4. Click the **Actions** link next to the group whose administrators you want to edit. From the **Actions** menu, click **Edit Administrators**.
  5. On the  $<group\_name>@<partition\_name>$  page, click **Add Administrator**.
  6. Use the **Search** box to find users or groups to add to the administrators. From the search results box, select the users or groups you want to designate as administrators, and then click **Add Selected**.



**Note:** For more information on delegated administration, see "[Delegated administration](#)" on page 251.

7. Continue searching for, and adding, administrators. After you have finished adding administrators, in the **Users and Groups Associations** box, click **Close**.
8. **Optional** If you want to remove a user or group from the administrators:
  - a. On the <group\_name>@<partition> page, select the administrator you want to remove, and then click **Remove Administrator**.
  - b. Confirm you want to remove this administrator.



**Note:** When you remove a user or group as a member of the administrators, you do not delete the user or group.

### 3.9.17 Consolidating groups in a partition

Consolidation of a selected group allows you to push user data to the resources with which that selected group is associated. Choose one of the two procedures below, depending on whether you want to consolidate an existing group or consolidate a missing group.

#### To consolidate an existing group:

1. From the web administration menu, click **Users & Groups**.
2. In the center of the page, select the **Groups** tab.



**Tip:** You can also, from the web administration menu, click **Partitions** and then select **View Members** from the user partition's **Actions** menu. In the center of the page, select the **Groups** tab.

3. Next, do one of the following:
  - Select the group that you want to consolidate.
  - Use the **Search** box to find the group.
4. Click **Actions** next to the group you want to consolidate. From the **Actions** menu, click **Consolidate**.
5. On the **Consolidate** page, do the following:
  - a. In the **Consolidate options** area, do the following:
    - i. **Optional** If you are consolidating an object in a synchronized user partition and you want to consolidate the selected object in OTDS with the identity provider, AD or LDAP, select **Consolidate with identity provider**.
    - ii. **Optional** If you want to direct OTDS to verify and repair a discrepancy in its internal referential integrity attributes, for example `oTMember` or `oTMemberOf`, select **Verify and repair**.



**Note:** OpenText recommends that you do not perform the **Verify and repair** operation unless directed to by OpenText technical support.

- b. If you are consolidating an object in a synchronized user partition, in the **Consolidate with the following resources** area, select all resources with which the previously selected object will be consolidated with information in OTDS.



**Note:** Consolidation operations may take a long time to complete. You can monitor the process through the “[directory-provenance.log](#)” on page 376 file.

6. Click **Consolidate** to consolidate user data for the selected existing group across all selected resources.

#### To consolidate a missing group:

If you know of a group who should be present in OTDS but is not listed, you can consolidate that missing group as follows:

1. From the button bar, click **Consolidate**.
2. From the **Consolidate** menu, click **Consolidate Missing Group**.
3. In the **Account DN** box, enter the DN of the group.
4. Click **OK**.

### 3.9.18 Enabling two-factor authentication for a group

You can enable two-factor authentication for all users in a group. Look up the group for whose users you want to enable two-factor authentication, and then follow the instructions found in “[Enabling two-factor authentication](#)” on page 99.

### 3.9.19 Deleting groups in a non-synchronized user partition

#### To delete groups in a non-synchronized user partition:

1. From the web administration menu, click **Users & Groups**.
2. In the center of the page, select the **Groups** tab.



**Tip:** You can also, from the web administration menu, click **Partitions** and then, from the non-synchronized user partition's **Actions** menu, select **View Members**. Select the **Groups** tab.

3. Select the group that you want to delete, or use the **Search** box to find the group.
4. Select the box to the left of the group you want to delete. Next, from the button bar, click **Delete**.

5. Confirm that you want to delete this group by clicking **OK**.



**Note:** When you delete a group, you do not delete the users.

### 3.9.20 Creating an organizational unit in a non-synchronized user partition

**To create an organizational unit in a non-synchronized user partition:**

1. From the web administration menu, click **Partitions** and then, in the center of the page, click the **Actions** link associated with the non-synchronized user partition in which you want to create an organizational unit. From the **Actions** menu, click **View Members**.
  2. Select the **Organizational Units** tab.
- 
- Tip:** You can nest organizational units by navigating to an existing OU before selecting **Add**.
3. On the button bar, click **Add**. From the **Add** menu, select **New Organizational Unit**.
    - a. In the **Organizational Unit name** box, type a descriptive name for the organizational unit to be displayed in your non-synchronized user partition.
    - b. Optional In the **Description** box, type a longer description of the organizational unit. For example, you might explain that you have included all development managers from the French and German offices of your company.
  4. Click **Save**.

### 3.9.21 Editing organizational units in a non-synchronized user partition

**To edit organizational units in a non-synchronized user partition:**

1. From the web administration menu, click **Partitions**, and then click the **Actions** link associated with the non-synchronized user partition whose organizational unit you want to edit.
2. From the **Actions** menu, select **View Members**.
3. Select the **Organizational Units** tab. Select the **Actions** link next to the organizational unit you want to edit. From the **Actions** menu, click **Properties**.
  - a. Follow the instructions, beginning with step 3, found in “[Creating an organizational unit in a non-synchronized user partition](#)” on page 122.
  - b. When you have finished editing, on the button bar, click **Save**.

4. **Optional** From the **Actions** menu associated with any organizational unit you want to edit, do the following:
  - If you want to consolidate this organizational unit, click **Consolidate**, and then follow the instructions for consolidating groups, beginning with step 5, found in “[Consolidating changes to users, groups, organizational units, and partitions](#)” on page 129.
  - If you want to edit administrators for this organizational unit, click **Edit Administrators**, and then see “[Editing administrators of organizational units in a non-synchronized user partition](#)” on page 123.
  - If you want to set two factor authentication for this organizational unit, click **Two Factor Auth Settings**, and then see “[Enabling two-factor authentication for an organizational unit](#)” on page 124.
  - If you want to delete this organizational unit, see “[Deleting organizational units in a non-synchronized user partition](#)” on page 124.

### 3.9.22 Editing administrators of organizational units in a non-synchronized user partition

**To edit administrators of organizational units in a non-synchronized user partition:**

1. From the web administration menu, click **Partitions**, and then click the **Actions** link associated with the non-synchronized user partition whose administrators you want to edit.
2. From the non-synchronized user partition's **Actions** menu, select **View Members**.
3. Click the **Organizational Units** tab, and then click the **Actions** link next to the organizational unit you want to edit. From the **Actions** menu, click **Edit Administrators**.
4. Click **Add Administrator**. In the **Users and Groups Associations** box, use the **Search** box to find users or groups to add to the administrators. From the search results box, select the users or groups you want to designate as administrators, and then click **Add Selected**.



**Note:** For more information on delegated administration, see “[Delegated administration](#)” on page 251.

5. **Optional** If you want to remove a user or group from the administrators listed in the **Administrators** area:
  - a. Select the user or group you want to remove, and then click **Remove Administrator**.
  - b. Click **Delete** to confirm that you want to remove this administrator.



**Note:** When you remove a user or group as a member of the administrators, you do not delete the user or group.

### 3.9.23 Enabling two-factor authentication for an organizational unit

You can enable two-factor authentication for all users in an organizational unit. Look up the organizational unit for whose users you want to enable two-factor authentication, and then follow the instructions found in “[Enabling two-factor authentication](#)” on page 99.

### 3.9.24 Deleting organizational units in a non-synchronized user partition

**To delete organizational units in a non-synchronized user partition:**

1. From the web administration menu, click **Partitions**, and then click the **Actions** link associated with the non-synchronized user partition whose organizational unit you want to delete.
2. From the **Actions** menu, select **View Members**.
3. Select the **Organizational Units** tab. Select the box to the left of the organizational unit you want to delete, and then, from the button bar, click **Delete**.
4. Confirm that you want to delete this organizational unit by clicking **OK**.



#### Caution

When you delete an organizational unit, all users and groups in the organizational unit will be deleted and removed from the resources with which they are associated.



**Tip:** If there are a large number of users and groups in an organizational unit, this action may take a long time. The **deleting** status indicator appears beside the organizational unit until the server has completed the operation. Click **Refresh** to determine if the server has completed the deletion.

### 3.9.25 Password policy for non-synchronized user partitions

You can set a password policy for each non-synchronized user partition in OTDS, or you can define a global password policy that applies to all non-synchronized user partitions.

When you define a global password policy, OTDS will automatically apply it to all non-synchronized user partitions you create thereafter. You can still access each non-synchronized user partition and override the global password policy by setting a password policy for that one non-synchronized user partition.

OTDS applies the **Open Web Application Security Project (OWASP)** 10,000 worst passwords list as a default of disallowed passwords. If a user attempts to set as their password one of the words on this list, they will receive an error message. It is possible to configure an additional file or URL, using the system attribute [Common Password URL on page 292](#), with additional disallowed passwords. Any file or URL specified in this system attribute is a supplement to the default OWASP list. OpenText recommends that, if using a custom file, it be less than 1MB in size.

#### Defining a global password policy for all non-synchronized user partitions

It is possible to define a global password policy for all non-synchronized user partitions in OTDS.

When you follow the “[Defining a global password policy for all non-synchronized user partitions](#)” on page 127 procedure, you will set the global password policy for your OTDS environment. However, setting a global password policy will only apply that global policy to any existing non-synchronized user partition that is already set to use a global password policy.

Only newly created non-synchronized user partitions will use the global password policy by default. You still need to edit the password policy of each *existing* non-synchronized user partition and select the **Use global policy** box.

#### 3.9.25.1 Defining a password policy for one non-synchronized user partition

##### To define a password policy for one non-synchronized user partition:



**Note:** If you want to set a global password policy that can apply to all non-synchronized user partitions, see “[Defining a global password policy for all non-synchronized user partitions](#)” on page 127.

1. From the web administration menu, click **Partitions**, and then click the **Actions** link associated with the non-synchronized user partition whose password policy you want to set.
2. From the **Actions** menu, select **Password Policy**.

3. In the **Password Policy** box, to apply the global password policy you defined in the “Defining a global password policy for all non-synchronized user partitions” on page 127 procedure to this non-synchronized user partition, select **Use global policy**.
  4. If you cleared the **Use global policy** box, then, in the **Password Quality** area, do the following:
    - a. In the **Minimum number of characters** box, type the minimum number of characters that you require in a password. The default value is 8.
    - b. In the **Minimum number of digits** box, type the minimum number of numeric characters that you require in a password. The default is 1.
    - c. In the **Minimum number of symbols** box, type the minimum number of non-alphanumeric characters that you require in a password. The default is 1.
    - d. In the **Minimum number of uppercase characters** box, type the minimum number of uppercase characters that you require in a password. The default is 1.
    - e. In the **Minimum number of lowercase characters** box, type the minimum number of lowercase characters that you require in a password. The default is 1.
    - f. In the **Minimum number of changes to previous password** box, type the minimum number of changes that you require the user to make to their previous password. The default is 0, meaning that this setting is disabled.
    - g. In the **Number of unique passwords before an old password can be reused** box, enter the number of passwords that must be unique before an old password can be reused. The default value is 3.
    - h. In the **Maximum number of consecutive characters from username** box, enter the maximum number of sequential characters a user can repeat from their username when creating or changing their password. The default value is 0, meaning that this setting is disabled. The verification that OTDS applies is case-insensitive.
  - For example, to ensure a password does not contain 3 or more characters from the username, set this option to 2.
  - i. Select the **Block commonly used passwords** box if you want to prevent the user from choosing any commonly used password. This box is cleared by default, allowing users to choose a commonly used password.

For general background information about commonly used passwords, see [https://en.wikipedia.org/wiki/List\\_of\\_the\\_most\\_common\\_passwords](https://en.wikipedia.org/wiki/List_of_the_most_common_passwords).
5. In the **Security Options** area, do the following:
    - a. In the **Password can be changed in (days)** box, enter the minimum number of days before a new password can be changed. The default value is 1.
    - b. In the **Password expires in (days)** box, enter the number of days before the password expires and must be changed. The default value is 90.

- c. In the **Lockout Failure Count** box, enter the maximum number of invalid password attempts before the user is locked out. The default is 3.
  - d. In the **Lockout Duration (minutes)** box, enter a number, in minutes, that a user will be locked out from their account if they exceed the maximum number of invalid password attempts. The default is 15.
6. Click **OK**.

### 3.9.25.2 Defining a global password policy for all non-synchronized user partitions

**To define a global password policy for all non-synchronized user partitions:**



**Note:** If you want to define an individual password policy that applies to one non-synchronized user partition, see “[Password policy for non-synchronized user partitions](#)” on page 125.

1. From the web administration menu, click **Partitions**.
2. On the main **Partitions** page, on the button bar, click **Global Settings**. From the **Global Settings** menu, select **Password Policy**.
3. In the **Password Policy** box, in the **Password Quality** area, do the following:
  - a. In the **Minimum number of characters** box, type the minimum number of characters that you require in a password. The default value is 8.
  - b. In the **Minimum number of digits** box, type the minimum number of numeric characters that you require in a password. The default is 1.
  - c. In the **Minimum number of symbols** box, type the minimum number of non-alphanumeric characters that you require in a password. The default is 1.
  - d. In the **Minimum number of uppercase characters** box, type the minimum number of uppercase characters that you require in a password. The default is 1.
  - e. In the **Minimum number of lowercase characters** box, type the minimum number of lowercase characters that you require in a password. The default is 1.
  - f. In the **Minimum number of changes to previous password** box, type the minimum number of changes that you require the user to make to their previous password. The default is 0, meaning this setting is disabled.
  - g. In the **Number of unique passwords before an old password can be reused** box, enter the number of passwords that must be unique before an old password can be reused. The default value is 3.
  - h. In the **Maximum number of consecutive characters from username** box, enter the maximum number of sequential characters a user can repeat from their username when creating or changing their password. The default value is 0, meaning that this setting is disabled. The checking that OTDS applies is case-insensitive.

In order to ensure a password does not contain 3 or more characters from the username, set this option to 2.

4. In the **Security Options** area:
  - a. In the **Password can be changed in (days)** box, enter the minimum number of days before a new password can be changed. The default value is 1.
  - b. In the **Password expires in (days)** box, enter the number of days before the password expires and must be changed. The default value is 90.
  - c. In the **Lockout Failure Count** box, enter the maximum number of invalid password attempts before the user is locked out. The default is 3.
  - d. In the **Lockout Duration (minutes)** box, enter a number, in minutes, that a user will be locked out from their account if they exceed the maximum number of invalid password attempts. The default is 15.
5. Click **OK**.

## 3.10 Consolidating users and groups in Partitions

You can use **Consolidate** to:

1. Restart your synchronized updates from your identity provider to Directory Services in a *synchronized user partition*.  
If the filter strings or locations are changed on a synchronized user partition, you should always initiate a consolidation against the modified user partition.
2. Force a re-synchronization of users and groups in OTDS to your synchronized resources. This may be required to correct the state between OTDS and the resource, if, for example, OTDS could not connect to those resources for some period of time.

The **Consolidate** option is not available until an **Import Users and Groups** operation is run. For more information, see “[Importing users and groups](#)” on page 98. After you have successfully imported users and groups to the user partition, you can perform a “[Consolidating changes to users, groups, organizational units, and partitions](#)” on page 129 operation.

### To receive notifications when a manual consolidation is required

You can set OTDS to ensure that you receive notifications when a synchronized user partition requires consolidation. For more information, see “[Setting notifications when a manual consolidation is required](#)” on page 131.

For general information about OTDS notifications, see “[Notifications Settings](#)” on page 320.

### Cancelling a consolidation of user and group data

At any time after you have started a consolidation of user and group data from Directory Services into your synchronized resources, and provided it has not

completed, you can cancel the consolidation process. For more information, see “[Jobs](#)” on page 363.

### 3.10.1 Consolidating changes to users, groups, organizational units, and partitions

Synchronized User Partitions are color-coded to indicate their status. For example, a synchronized user partition can appear with a background color to indicate that it requires the importing or consolidation of users and groups:

- **White:** no import or consolidation is required.
- **Green:** an import or a consolidation is in progress.
- **Yellow:** an import or a consolidation is required. For more information, see “[Importing users and groups](#)” on page 98 or “[Consolidating changes to users, groups, organizational units, and partitions](#)” on page 129.
- **Red:** an import or a consolidation failed.

#### To consolidate changes to users, groups, organizational units, and partitions:

1. From the web administration menu, do one of the following:
  - If you want to consolidate a specific user:
    1. Click **Users & Groups**, and then select the **Users** tab.
    2. Find the specific user you want to consolidate, and then, from that user's **Actions** menu, click **Consolidate**.
  - By default, consolidation will occur on the selected user only. If you want to force a recursive consolidation, see “[Setting the partition attribute to apply recursive consolidation for users or groups in a synchronized user partition](#)” on page 130.
  - If you want to consolidate a specific group:
    1. Click **Users & Groups**, and then select the **Groups** tab.
    2. Find the specific group you want to consolidate, and then, from that group's **Actions** menu, click **Consolidate**.
  - By default, consolidation will occur on the selected group only. If you want to force a recursive consolidation, see “[Setting the partition attribute to apply recursive consolidation for users or groups in a synchronized user partition](#)” on page 130.
  - If you want to consolidate an organizational unit:
    1. Click **Partitions**.
    2. From the **Actions** menu of the partition containing the organizational unit you want to consolidate, select **View Members**.
    3. Select the **Organizational Units** tab.

4. Find the organizational unit you want to consolidate, and then, from that organizational unit's **Actions** menu, click **Consolidate**.
  - If you want to consolidate an entire user partition:
    1. Click **Partitions**.
    2. From the **Actions** menu of the partition you want to consolidate, select **Consolidate**.
  - 2. In the **Consolidate** box, in the **Consolidate options** area, do the following:
    - a. **Optional** If you are consolidating a synchronized user partition and you want to consolidate the selected object in OTDS with the identity provider, AD or LDAP, select **Consolidate with identity provider**.
    - b. **Optional** If you want to direct OTDS to verify and repair a discrepancy in its internal referential integrity attributes, for example `oTMember` or `oTMemberOf`, select **Verify and repair**.



**Note:** OpenText recommends that you do not perform a **Verify and repair** operation unless directed to by OpenText technical support.

3. If you are consolidating a synchronized user partition, in the **Consolidate with the following resources** area, select all resources with which this object will be consolidated with information in OTDS.
4. Click **Consolidate** to begin the consolidation process.



**Note:** A consolidation operation can take a long time to complete if consolidating organizational units or partitions with thousands of users and groups. You can monitor the process through either of the following:

- “Jobs” on page 363
- “directory-provenance.log” on page 376

### 3.10.1.1 Setting the partition attribute to apply recursive consolidation for users or groups in a synchronized user partition

By default, when consolidating an individual user or group, consolidation will only apply to the selected user or group in a synchronized user partition. If you want OTDS to force recursive consolidation of a user or group, meaning that the parents (`memberOf`) and/or children (`member`) will also be consolidated, you need to set the `otds.es.RecurseObjectConsolidation` attribute

You need to first create the `otds.es.RecurseObjectConsolidation` attribute and then set it to “true” on the synchronized user partition.

You can choose to set this attribute at either the partition level, such that it only applies to one synchronized user partition, or you can set this attribute at a system level, such that it applies to all partitions.

You set this attribute at a user partition level by adding it using the “[Creating system or custom attributes for one partition](#)” on page 134 procedure.

You set this attribute at a system level by adding it using the “[Adding a system attribute](#)” on page 316 procedure.

If this attribute is set at the user partition level that setting, for that user partition, will take precedence over any system level setting.

### 3.10.2 Setting notifications when a manual consolidation is required

**To set notifications when a manual consolidating is required:**

1. From the web administration menu, select **System Config**.
2. On the **System Config** page, select the **Notifications Settings** tab.



**Tip:** Make sure you have completed all requirements for enabling notifications as detailed in “[Requirements before enabling Notifications in OTDS](#)” on page 320.

3. On the **Notification Settings** tab, in the **General Notifications** area, in the **E-mail Addresses** box, type a comma-separated list of all email addresses that should receive this notification.
4. In the **Event Notifications** area, do the following:
  - a. Make sure **Enable OTDS Notifications** is selected.
  - b. In the **OTDS Notification Events** box, in the **Available Event IDs** box, click to select **Sync Partition - Partition Consolidation Required** and then click **ADD**.
  - c. From the **Event Level** list, select **WARN**.
5. On the menu bar, click **Save**.

### 3.10.3 Canceling consolidation of changes to users and groups

**To cancel consolidation of changes to users and groups:**

1. After you have started a consolidation from OTDS into your synchronized resources, and provided it has not completed, from the web administration menu, select **Jobs**.
2. From the **Actions** menu associated with the consolidation you want to cancel, click **Cancel Consolidation**.

## 3.11 Partition attributes

You can now add system or custom attributes to user partitions. Partition attributes can be applied to synchronized or non-synchronized partitions.

### Custom attributes

Custom attributes are for the use of applications. They are intended for applications that integrate with OTDS to allow them to store their application properties.



#### Important

OpenText recommends that you do not create custom attributes.

### System attributes

The system attributes you can create on a partition are the same as those in the “[System Attributes](#)” on page 288 tab. However, these partition system attributes only affect the behavior for users and groups within that partition, rather than to the entire system. They are currently used to enable auto-provisioning or two-factor authentication on a per-partition basis.

When you create a system attribute on a partition, as described in this chapter, that attribute applies only to the users and groups within that partition. When you create a system attribute in “[Adding a system attribute](#)” on page 316, that system attribute applies to all users and groups across all partitions.



#### Important

OpenText recommends that you only create system attributes on a partition if directed by OpenText support.

### 3.11.1 Examples filtering one synchronized partition's deleted users and groups

The **Value** field of a system attribute can store a custom filter. These examples show how to create partition-specific system attributes that apply to the users and groups in one synchronized partition. These examples can only be applied to synchronized partitions.



**Tip:** You may need to consult with your Active Directory system administrator to identify those system attributes that are saved in deleted users and groups in order to create your own filters.

To see these examples applied to all synchronized partitions, system-wide, see “[Examples filtering system-wide deleted users and groups](#)” on page 315. If any system attribute is created on the “[System Config](#)” page, and that system attribute is also created on a single synchronized partition on the “[Partition attributes](#)” page, the system attribute created on the **Partition Attributes** page will take precedence.

▶ **Example 3-10: Example creating a system attribute that is used to search for deleted users in one synchronized partition**

This example will filter deleted users. It will create a system attribute that applies to all users in one synchronized partition only.

1. In the OTDS administration page, click **Partitions**.
2. From the **Actions** menu of the partition to which you want these system attributes to apply, click **Partition Attributes**.

 **Note:** In order for this system attribute to function, the partition you select must have the **USN query** monitoring applied. For more information, see [Monitoring on page 77](#).

3. On the **System Attributes** tab, click **Add**, and then do the following:

- a. In the **Name** field, type:

```
otds.es.FilterDeletedUsers
```

- b. In the **Value** field, do one of the following:

- If the `mail` attribute is not saved when a user is deleted, type:

```
(&(!(objectClass=computer))(objectClass=user)(objectClass=person))
```

- If the `mail` attribute is saved when a user is deleted, type:

```
(&(!(objectClass=computer))(objectClass=user)(objectClass=person)(mail=*))
```



**Note:** You can consult with your Active Directory system administrator to identify those attributes that are saved in deleted users and groups.

- c. Click **Save** next to your system attribute.

4. On the button bar, click **Save**.



▶ **Example 3-11: Example creating a system attribute that is used to search for deleted groups in one synchronized partition**

This example will filter deleted groups. It will create a system attribute that applies to all groups in one synchronized partition only.

1. In the OTDS administration page, click **Partitions**.
2. From the **Actions** menu of the partition to which you want these system attributes to apply, click **Partition Attributes**.

 **Note:** In order for this system attribute to function, the partition you select must have the **USN query** monitoring applied. For more information, see [Monitoring on page 77](#).

3. On the **System Attributes** tab, click **Add**, and then do the following:

- a. In the **Name** field, type:

```
otds.es.FilterDeletedGroups
```

- b. In the **Value** field, type:

```
(&(objectClass=group) ((groupType=2147483652) (groupType=2147483650) (groupType=2147483656)))
```

- c. Click **Save** next to your system attribute.

4. On the button bar, click **Save**.



### 3.11.2 Creating system or custom attributes for one partition

#### To create a custom attribute for one partition:

1. From the **Actions** menu of the user partition on which you want to create an attribute, click **Partition Attributes**.



**Note:** OpenText recommends that you do not create custom attributes.

2. Click the **Custom Attributes** tab.
3. Click the **Add** button.
4. Enter a value to the **Type** box.
5. **[Optional]** Enter a value to the **Name** box.
6. **[Optional]** Enter a value to the **Value** box.
7. Next to the new attribute, click **Save**. If you are finished adding your attributes, on the button bar, click **Save**.
8. **[Optional]** If you want to remove specific attributes, click the box to the left of the attribute and then click **Remove Selected**.  
If you want to remove all attributes, click **Clear All**.

#### To create a system attribute for one partition:

1. From the **Actions** menu of the user partition on which you want to create an attribute, click **Partition Attributes**.
2. Click the **System Attributes** tab.
3. Click the **Add** button.
4. Enter a value to the **Type** box.
5. **[Optional]** Enter a value to the **Name** box.

6. **Optional** Enter a value to the **Value** box. You can type a filter in this field, provided this partition has the **USN query** monitoring method applied. For more information, see “[Examples filtering one synchronized partition's deleted users and groups](#)” on page 132 and [Monitoring](#) on page 77.
7. Next to the new attribute, click **Save**. If you are finished adding your attributes, on the button bar, click **Save**.
8. **Optional** If you want to remove specific attributes, click the box to the left of the attribute and then click **Remove Selected**.  
If you want to remove all attributes, click **Clear All**.

## 3.12 Disabling a user partition

It is possible to disable a user partition. If any user partition is disabled:

- Users cannot authenticate to that user partition.
- It is not possible to create, update, or delete any users or groups in that user partition.
- Monitoring of synchronized partitions is stopped and will not start if the **Restart Enterprise Sync** button is used.

The two default partitions created at installation, OAuthClients and otds.admin, cannot be disabled. For more information, see “[Enabling or disabling a user partition](#)” on page 135.

### 3.12.1 Enabling or disabling a user partition

**To enable or disable a user partition:**

1. From the web administration menu, click **Partitions**.
2. From the **Actions** menu of the user partition you want to enable, click **Enable**.

**To disable a user partition:**

1. From the web administration menu, click **Partitions**.
2. From the **Actions** menu of the user partition you want to disable, click **Disable**.



# Chapter 4

## Authentication Handlers

This section describes creating and configuring authentication handlers. Directory Services provides a set of authentication handler types for your use. Each authentication handler type may require specific configuration parameters.

The **Auth Handlers** page displays a list of all defined authentication handlers including default authentication handlers provided by Directory Services. The **Scope** column displays whether the authentication handler applies to specific partitions or all partitions. You can view the priority of an authentication handler. The priority determines the sequence in which the authentication handler is applied. You can also view whether the authentication handler is enabled or disabled.

 **Note:** If your environment has multiple OTDS server nodes, any configuration changes to “[Authentication Handlers](#)”, “[Trusted Sites](#)”, or “[System Config](#)” can take up to one minute to take effect across all OTDS server nodes.

### Disabling authentication handlers

Disabling an authentication handler does not change its priority or its configuration parameters. When multiple authentication handlers are evaluated based on the priorities of the assigned handlers, disabled handlers will be ignored.

### Authentication principal attribute

The authentication principal attribute is used to find the user in Directory Services. You must supply an attribute that will uniquely find a given user in Directory Services.

### OTDS Two-Factor Authentication

OTDS Two-Factor Authentication has been implemented using the Time-Based One-Time Password Algorithm (TOTP), RFC6238.

The administrator can choose to apply two-factor authentication at the user, group, organizational unit, or partition level. For more information, see “[Configuring two-factor authentication](#)” on page 237.

See also “[Enabling two-factor authentication](#)” on page 99.

### Authentication handler Actions menu options and buttons

On the main **Auth Handlers** page, each authentication handler has an associated **Actions** menu and buttons. The following are quick links to the procedures associated with each:

**Authentication handlers Actions menu items**

<b>Actions menu option</b>	<b>Associated Procedure</b>
Properties	<a href="#">“Editing an authentication handler” on page 163</a>
Enable/Disable	<a href="#">“Enabling or disabling an authentication handler” on page 165</a>

**Authentication handlers buttons**

<b>Button</b>	<b>Associated Procedure</b>
Add	<a href="#">“Creating an authentication handler” on page 162</a>
Delete	<a href="#">“Deleting an authentication handler” on page 164</a>
Refresh	Use the Refresh button to verify if OTDS has completed an action. For example, after deleting.
Help	Opens context-sensitive help for the page you are currently using.

## 4.1 Using authentication handlers

The **New Authentication Handler** assistant guides you through setting up your authentication handlers. This section describes the authentication handlers and their required parameters, which you will need to enter in the **New Authentication Handler** assistant.

### 4.1.1 List of authentication handlers

This page describes the authentication handler types, their purpose, and their usage.

---

**Custom REST Authenticator**

- **Description:** invokes a custom REST endpoint with HTTP basic authentication to provide credential-based authentication.
- **Default Status:** not displayed.
- **Parameters:**

<b>Parameter Name</b>	<b>Description</b>
Provider Name	The name of the authentication provider. This name is displayed on the sign in page.
URL	The URL for the authentication service.
HTTP Method	The HTTP method to use for the request.

Parameter Name	Description
Credentials Method	You need to state if you will be sending credentials through an Authorization header, or through a request body as a form, or through a request body as a JSON object. Allowed values are: HEADER/FORM/JSON.
HTTP header name <x>	Specifies the name of an additional HTTP header to send with every request. Where <x> is a positive integer.
HTTP header value <x>	Specifies the value of an additional HTTP header to send with every request. This value will be assigned to the corresponding <b>HTTP header name &lt;x&gt;</b> .
Allow Auto-Provisioning	Specifies whether to allow this handler to auto-provision users. If you set this value to <b>true</b> , auto-provisioning must also be explicitly enabled on the partition or system attributes in order for users to be automatically provisioned.
User Identifier Field	The field in the response corresponding to the user's unique ID at this provider. This box is only required if <b>Allow Auto-Provisioning</b> is set to <b>true</b> .
Response Field <x>	A field in the JSON response that should be mapped to an OTDS attribute. This value is case sensitive. Mapped fields are only relevant for auto-provisioned accounts.
OTDS Attribute <x>	OTDS user attribute to which the corresponding <b>Response Field &lt;x&gt;</b> should be mapped.

### Custom Web Service Authenticator

- **Description:** invokes a custom web service to provide credential-based authentication.
- **Default Status:** not displayed.
- **Parameters:**

Parameter Name	Description
WSDL	The WSDL for the authentication service.

### Guest Account

- **Description:** this authentication handler will succeed with the configured internal account name provided the user name entered matches the configured guest name.
- **Default Status:** not displayed.
- **Parameters:**

Parameter Name	Description
Guest name	The name that the user must type to the posted form in order to sign in as the guest account.
Guest account	The account internal name to which this guest account maps. This should be typed in the form: <i>&lt;account_name&gt;@&lt;partition_or_domain&gt;</i>

---

### HTTP Anonymous

- **Description:** always succeeds with the configured user name. Use this at the end of the authentication handler chain to grant anonymous access using the named guest account.  
If the **HTTP Anonymous** authentication handler is prioritized after the **http.negotiate** authentication handler, and domain users will use single sign on into their domain accounts, all other users will automatically end up as the guest account. See “Prioritizing authentication handlers” on page 157 and “Changing the priority of an authentication handler” on page 164.
- **Default Status:** not displayed.
- **Parameters:**

Parameter Name	Description
Display Name	The name to display for this authentication handler.
Guest Account Name	The user name with which this authentication handler will always succeed. This should be typed in the form: <i>&lt;guest_name&gt;@&lt;partition_name&gt;</i>
Active by Default	If set to <b>true</b> , any sign in request to the OTDS sign in page will be processed by this handler. If set to <b>false</b> , the handler must be explicitly specified.

---

### http.cookie

- **Description:** an authentication handler of type **OTDS HTTP Session Handler** on page 148. The **http.cookie** authentication handler allows for single sign on between different resources.

The **http.cookie** authentication handler maintains an HTTP session with the client browser through the use of HTTP cookies. This allows potentially expensive authentication requests to be bypassed for the duration of the browser session, as it avoids requiring users to reauthenticate as they access different resources.

- **Default Status:** displayed and enabled.

- **Default Authentication Handler Name:** http.cookie
- **Parameters:**

Parameter Name	Description
Idle timeout (minutes)	A positive integer representing the number of minutes of inactivity after which the Directory Services SSO cookie will expire. Any attempt to use the OTDS session after the cookie expires will result in a prompt for re-authentication.
Max timeout (minutes)	A positive integer representing the number of minutes after which the Directory Services SSO cookie will expire, regardless of activity. Any attempt to use the OTDS session after the cookie expires will result in a prompt for re-authentication.
Allow session persistence	The default value is <b>false</b> . The HTTP cookie will be stored as a session cookie. If you select <b>true</b> , a <b>Keep me signed in</b> option is displayed on the sign in page. If a user selects that <b>Keep me signed in</b> option, the HTTP cookie will be stored as a persistent cookie. The lifetime of the cookie does not change and remains subject to the settings the admin has entered to <b>Idle timeout</b> and <b>Max timeout</b> .

## HTTP Negotiate

- **Description:** handles Negotiate authentication with the browser. The **HTTP Negotiate** authentication handler deals with NTLM/Kerberos based authentication for the browser. For more information, see “[Configuring the http.negotiate authentication handler on Unix](#)” on page 165.

On the `http.negotiate` **Parameters** page, you can choose to enable this authentication handler for mobile browsers. If enabled, negotiate authentication will be performed with mobile browsers.

OTDS does not require Kerberos delegation functionality. Kerberos is only used to authenticate users directly with OTDS through its service principal name. Once Kerberos-based SSO occurs on OTDS, the application session takes over and Kerberos is no longer used. Therefore, the Windows account under which OTDS is running can be configured with “Do not trust this user/computer for delegation”.

- **Default Status:** displayed and enabled.
- **Default Authentication Handler Name:** http.negotiate
- **Parameters:**

Parameter Name	Description
Enable for mobile browsers	Select <b>true</b> to perform negotiate authentication with mobile browsers.
IP address whitelist	<p>The handler will <i>only</i> process requests from IP addresses found in this box.</p> <p>You can either type:</p> <ul style="list-style-type: none"><li>– A comma-separated list of IP addresses or subnet masks in CIDR notation.</li><li>– A file URI reference. An example of a file URI reference is: <code>file:///c:/OTDS_Files/&lt;filename&gt;.txt</code></li></ul> <p>The <code>&lt;filename&gt;.txt</code> file can contain a list of IP addresses or subnet masks in CIDR notation, each on its own line.</p>
IP address blacklist	<p>If an <b>IP address whitelist</b> is specified, this parameter is not used.</p> <p>The handler will <i>not</i> process requests from IP addresses found in this box.</p> <p>You can either type:</p> <ul style="list-style-type: none"><li>– A comma-separated list of IP addresses and subnet masks in CIDR notation.</li><li>– A file URI reference. An example of a file URI reference is: <code>file:///c:/OTDS_Files/&lt;filename&gt;.txt</code></li></ul> <p>The <code>&lt;filename&gt;.txt</code> file can contain a list of IP addresses or subnet masks in CIDR notation, each on its own line.</p>

---

### HTTP Post Handler

- **Description:** processes HTTP POST operations such as HTML form-based authentication. The **http.post** authentication handler takes care of dealing with the user name/password posted on the sign in page.
- **Default Status:** displayed and enabled.
- **Default Authentication Handler Name:** http.post

---

### Internal Authenticator

- **Description:** uses the internal repository to provide credentials-based authentication. For each non-synchronized user partition there is an **Internal Authenticator** authentication handler with the same name.
- **Default Status:** enabled.

- **Default Authentication Handler Name:** cred.internal

### Negotiate Token

- **Description:** handles token-based Negotiate authentication. The `token.negotiate` authentication handler deals with NTLM/Kerberos-based authentication from web services, called by rich clients such as Enterprise Connect.
- **Default Status:** displayed and enabled.
- **Default Authentication Handler Name:** token.negotiate

### OAuth 1.0a

- **Description:** implements the OAuth 1.0a protocol for authentication with an identity provider. If you require it, you can find information about OAuth 2.0, in [OAuth 2.0 / OpenID Connect on page 144](#).

If you want to enable auto-provisioning of OAuth accounts, see [Enable Auto-Provisioning of Accounts on page 297](#).

- **Default Status:** not displayed.
- **Parameters:**

Parameter Name	Description
Provider Name	The name of the authentication provider. This name is displayed on the sign in page.
Social Media Prefix	A prefix to identify this OAuth provider as a social media account provider. This should only be used to allow users to link various social media accounts to an OTDS account. This value should not be changed after users link their accounts with this provider.
Active By Default	Select <b>true</b> to activate this handler for any requests to the OTDS sign in page. If set to <b>true</b> , any sign in request to the OTDS sign in page will be redirected to this OAuth provider. If set to <b>false</b> , the user must select the provider on the sign in page.
Allow Auto-Provisioning	Specifies whether to allow this handler to auto-provision users. You must also explicitly enable auto-provisioning on the partition or system attributes in order for users to be automatically provisioned.
Consumer Key	The consumer key.
Consumer Secret	The consumer secret.
Request Token URL	The URL from which to retrieve the request token.
Authorization URL	The URL to which the user will be redirected in order to authenticate and authorize OTDS to access their account information.

Parameter Name	Description
Access Token URL	The URL from which to retrieve the access token.
User Info API URL	The URL from which to retrieve the user's information object. The object should be in JSON format.
User Identifier Parameter	The parameter corresponding to the user's unique ID at this provider.
Response Field <x>	A field in the JSON response that should be mapped to an OTDS attribute. This value is case sensitive. Mapped fields are only relevant for auto-provisioned accounts.
OTDS Attribute <x>	The OTDS user attribute to which the corresponding <b>Response Field &lt;x&gt;</b> value should be mapped.

See also “[Configuration and use of OAuth authentication](#)” on page 158.

### OAuth 2.0 / OpenID Connect

- **Description:** implements the OAuth 2.0 and OpenID Connect protocols for authentication with an identity provider. If you require it, you can find information about OAuth 1.0a in [OAuth 1.0a on page 143](#).  
If you want to enable auto-provisioning of OAuth accounts, see [Enable Auto-Provisioning of Accounts on page 297](#).
- **Default Status:** not displayed.
- **Parameters:**

Parameter Name	Description
Provider Name	The name of the authentication provider. This name is displayed on the sign in page.
OIDC Issuer	The <code>issuer</code> value for an OpenID Connect provider. This parameter is required if you are using OpenID Connect.
Social Media Prefix	A prefix to identify this OAuth provider as a social media account provider. This should only be used to allow users to link various social media accounts to an OTDS account. This value should not be changed after users link their accounts with this provider.
Active By Default	Select <code>true</code> to activate this handler for any requests to the OTDS sign in page. If set to <code>true</code> , any sign in request to the OTDS sign in page will be redirected to this OAuth provider. If set to <code>false</code> , the user must select the provider on the sign in page.
Allow Auto-Provisioning	Specifies whether to allow this handler to auto-provision users. You must also explicitly enable auto-provisioning on the partition or system attributes in order for users to be automatically provisioned.

Parameter Name	Description
Enable cred validation	Specifies whether to allow this handler to validate credentials sent directly to OTDS. The server must support the "OAuth2 Resource Owner Password Credentials Grant".
Enable token validation	Specifies whether to allow this handler to validate <code>OIDC id_token</code> tokens sent directly to OTDS through an API.
Client ID	The client ID.
Client Secret	The client secret. This value is required if the authentication method is based on a client secret.
Scope String	Specifies the space delimited scope values to send. Include <code>openid</code> to use OpenID Connect.
Use PKCE	Specifies whether or not OTDS should use PKCE in the authorization request. Some authorization servers may enforce PKCE by policy, but it is not required for a secure configuration.
OIDC Metadata Endpoint	The URL for the OpenID Connect Provider Metadata. If configured, all other endpoints do not need to be configured since they will be obtained from the provider's metadata.
OIDC JWKS Endpoint	This parameter is only required if you are using OpenID Connect with an implicit flow. For example, if you are using OpenID Connect without a token endpoint configured.  You have the option of specifying a URI to a file that should be used if OTDS cannot connect to the identity provider directly. An example of a file URI reference is: <code>file:///c:/OTDS_Files/&lt;filename&gt;</code> .
Authorization Endpoint	The URL to which to redirect the browser for authentication. It is used to retrieve the authorization code or an <code>OIDC id_token</code> .
Token Endpoint	The URL from which to retrieve the access token. Not strictly required with OpenID Connect if using the implicit flow.
Logout Endpoint	The URL to redirect to upon logout from Directory Services in order to terminate the identity provider session.
Logout Method	The HTTP method the browser should use to invoke the logout URL (GET / POST).
User Info Endpoint	The URL from which to retrieve the JSON object representing the authorized user.
Extra Authz Param Name <x>	The name of an additional parameter to send in the authorization request.
Extra Authz Param Value <x>	The value of the additional parameter to send in the authorization request. The value will be assigned to the corresponding <b>Extra Authz Param Name &lt;x&gt;</b> .
Extra Token Param Name <x>	The name of an additional parameter to send in the access token request.

Parameter Name	Description
Extra Token Param Value <x>	The value of the additional parameter to send in the access token request. The value will be assigned to the corresponding <b>Extra Token Param Name &lt;x&gt;</b> .
Use a popup window	Specifies whether to open a new (popup) window to perform the authorization grant for browser-based flows originating in a <frame> or <iframe>. This is only necessary when authentication occurs within a frame and the IdP blocks frame embedding. OTDS will only open a popup when it detects the request originated from a frame.
Send Access Token in Header	Specifies whether to send the access token in the HTTP Authorization header when invoking the user info URL. If set to <b>false</b> , the access token will be sent as a query parameter.
Authentication Method	Specifies the authentication method for the configured client ID.
KeyStore Description	Specifies a custom description of the keystore file. Alternatively, you can specify a URI to a file to be used instead of loading the keystore into OTDS. An example of a file URI reference is: <code>file:///c:/OTDS_Files/&lt;filename&gt;</code> .
KeyStore	The keystore, in PKCS#12 format, containing the private key to use. This parameter is only required if using the <code>private_key_jwt</code> or <code>tls_client_auth (mTLS)</code> authentication method.
KeyStore Password	The password for the KeyStore file.
KeyStore Alias	The alias for the public certificate and private key in the KeyStore file.
Workload Identity JWT path	<p>Specifies a URL or file path to a JWT to use for workload identity authentication. An example of a URL is: <code>http://metadata.google.internal/computeMetadata/v1/instance/service-accounts/default/identity?audience=xyz</code>. An example of a file path is: <code>///var/run/secrets/tokens/fed-token</code>.</p> <p>This parameter is only relevant for the <code>workload_identity_jwt</code> authentication method. Generally, this is only viable when OTDS is deployed in a managed environment. Additional configuration of the deployment is typically required to provide a suitable token.</p>
User Identifier Field	The field corresponding to the user's unique ID at this provider. Use square brackets, <code>[field][subfield]</code> , to delineate nested fields.
Impersonator Field	The field that contains the ID of the actor/impersonator for the user represented by the token. It must be in the same format as the user identifier field.

Parameter Name	Description
Security Clearance Field	The field that contains the user's security clearance level. This feature is specific to the <b>Security Clearance</b> module in OpenText Content Management.
Map all users to	Specifies the user name to which all authenticated users will be mapped once the user's token is verified. The format of the name should correspond with the authentication principal attribute configured for this handler. This feature is not compatible with auto-provisioning. Users will not be provisioned if this parameter is set.
IdP supports query in redirect URI	Some identity providers do not support query parameters in the redirect URI. If you are using one of those identity providers, you will need to set this parameter to <b>false</b> . An example of an identity provider who does not support query parameters in the redirect URI is Azure B2C.
ACR Values	Space-delimited values that should always be sent in the <code>acr_values</code> parameter of an authentication request.
Step-up ACR values	Space-delimited values that should be sent in the <code>acr_values</code> parameter of an authentication request when an application initiates step-up authentication. This is only used in specific use cases.
Trusted Audiences	Space-separated list of audience values in an <code>id_token</code> that can be trusted, in addition to the OTDS client ID.
Trusted Authorized Parties	Space-delimited list of authorized party values, <code>azp</code> , in an <code>id_token</code> that can be trusted, in addition to the OTDS client ID. Use an asterisk, *, to trust any <code>azp</code> claim.
Response Field <x>	A field in the JSON response that should be mapped to an OTDS attribute. This value is case sensitive. Mapped fields are only relevant for auto-provisioned accounts.
OTDS Attribute <x>	The OTDS user attribute to which the corresponding <b>Response Field &lt;x&gt;</b> value should be mapped.

See also “[Configuration and use of OAuth authentication](#)” on page 158.

- **Related Documentations:** Configuring the Google OAuth 2.0 Authentication Handler (<https://knowledge.opentext.com/knowledge/cs.dll/kcs/kbarticle/view/KB4960782>).

## Oracle EBS

- **Description:** allows for support of the xECM4oracle solution. It extracts authenticated user information from an EBS/ICX session. For information about configuring the Oracle EBS Authentication Handler, see “[Configuring the Oracle EBS authentication handler](#)” on page 166.
- **Default Status:** not displayed.
- **Parameters:**

Parameter Name	Description
Application DBC file description	Specifies a custom description for the corresponding DBC file.
Application DBC file	The DBC file for this application created with the AdminDesktop utility.
Application user name	The user name for this application.
Application user password	The password for this application.
Map all Oracle users to	Specify the OTDS user name to which all authenticated users will be mapped after their Oracle sign on session token is verified. The format of the name should correspond with the authentication principal attribute configured for this handler.

---

**otds.admin**

- **Description:** an authentication handler of type [Internal Authenticator on page 142](#). It uses the internal repository to provide credentials-based authentication for the administration user partition.
- **Default Status:** displayed and enabled.
- **Default Authentication Handler Name:** otds.admin
- **Default Authentication Handler Type:** [Internal Authenticator on page 142](#)

---

**OTDS Custom Location Handler**

- **Description:** returns location information with OTDS tickets using a custom IP address resolution mechanism.
- **Default Status:** not displayed.
- **Parameters:**

Parameter Name	Description
Custom Class Name	Specifies the class that implements the <b>LocationProvider</b> interface. The format for the <b>LocationProvider</b> is: <pre>public interface LocationProvider {     public String[]     getLocations(String ipAddress); }</pre>

---

**OTDS HTTP Session Handler**

- **Description:** maintains an HTTP session with the client browser through the use of HTTP cookies. This allows potentially expensive authentication

requests to be bypassed for the duration of the session, as it avoids requiring users to re-authenticate as they access different resources.

- **Default Status:** not displayed.
- **Parameters:**

Parameter Name	Description
Idle timeout (minutes)	The number of minutes of inactivity after which the Directory Services SSO cookie will expire. Any attempt to use the Directory Services session after expiry will result in a prompt for re-authentication.
Max timeout (minutes)	The number of minutes, regardless of activity, after which the Directory Services SSO cookie will expire. Any attempt to use the Directory Services session after expiry will result in a prompt for re-authentication.
Allow session persistence	The default value is false. The HTTP cookie will be stored as a session cookie. If you select <b>true</b> , a <b>Keep me signed in</b> option is displayed on the sign in page. If a user selects that <b>Keep me signed in</b> option, the HTTP cookie will be stored as a persistent cookie. The lifetime of the cookie does not change and remains subject to the settings the admin has entered to <b>Idle timeout</b> and <b>Max timeout</b> .

---

### OTDS Location Handler

- **Description:** returns location information with OTDS tickets.
- **Default Status:** not displayed.
- **Parameters:**

Parameter Name	Description
Mappings File Description	Specifies a custom description for the mapping file.

Parameter Name	Description
Mappings File	<p>Specifies the mapping file to be used to translate IP addresses to location names. This is an XML file with the following syntax:</p> <pre>&lt;Mappings&gt; &lt;Mapping&gt; &lt;IP&gt;192.168.0.0/16&lt;/IP&gt; &lt;Name&gt;NORTH_AMERICA&lt;/Name&gt; &lt;/Mapping&gt; &lt;/Mappings&gt;</pre>
Default Location	Specifies the default location for IP addresses that are not matched to any defined in the mapping file.

## SAML 2.0

- Description:** allows for delegating authentication to a SAML 2.0 compliant Identity Provider. Directory Services acts as a service provider, otherwise known as a relying party, that recognizes SAML 2.0 assertions.
- Default Status:** not displayed.
- Parameters:**

Parameter Name	Description
Identity Provider (IdP) Name	The name of the identity provider. OpenText recommends that you type a single word, without spaces, as this will be part of the metadata URL.
IdP Metadata URL	The URL for the IdP's federation metadata, or a file description if a file is selected in the <b>IdP Metadata File</b> field. When a URL is specified, the metadata is automatically updated by OTDS, daily, at midnight.
IdP Metadata File	The metadata XML file of the identity provider. This parameter is not necessary if you provided a URL in the <b>IdP Metadata URL</b> field.
WS-Trust Metadata URL	The URL for the IdP's WS-MetaDataExchange, WS-Trust metadata. This is required for OTDS to validate credentials with the identity provider.

Parameter Name	Description
IdP NameID Format	<p>Specifies which NameID format supported by the identity provider contains the desired user identifier. The value in this identifier must correspond to the value of the user attribute specified for the authentication principal attribute. This value is usually set to one of the following:</p> <ul style="list-style-type: none"> <li>- urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</li> <li>- urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</li> </ul> <p>Please ensure this is consistent with the identity provider's configuration.</p>
OTDS SP Endpoint	<p>Specifies the service provider URL that will be used to identify OTDS to the identity provider. If not specified, the URL will be taken from the request. This generally needs to be configured for environments in which OTDS is behind a reverse-proxy.</p>
Trusted Audiences	<p>Space-separated list of service provider audience values that should be trusted, in addition to the OTDS SP URL. OTDS will accept assertions intended for these audiences as though they were unsolicited. The <code>InResponseTo</code> attribute on a <code>SubjectConfirmationData</code> element will not be verified.</p>
Active By Default	<p>Determines whether Directory Services should delegate authentication to the SAML identity provider. If this option is set to <code>true</code>, any sign in request to the OTDS sign in page will be redirected to the IdP. If this option is set to <code>false</code>, then IdP-Initiated SSO will still be possible, but Directory Services will not redirect users to the Identity Provider to authenticate, the users will have to select the provider on the sign in page.</p>
Allow Auto-Provisioning	<p>Specifies whether to allow this handler to auto-provision users. You must explicitly enable auto-provisioning on the partition or system attributes in order for users to be automatically provisioned.</p>

Parameter Name	Description
Grace Period	Specifies the number of minutes to allow for “NotBefore” and “NotOnOrAfter” boxes when validating assertions in order to account for any time difference between the identity provider and this service provider. The default value is 5.
Auth Request Binding	Specifies the SAML binding to use for sending the AuthnRequest, provided it is supported by the identity provider.
Auth Response Binding	Specifies the SAML binding to use for the response to an AuthnRequest.
Use AssertionConsumerServiceURL	Set this parameter to <b>true</b> to have the SAML AuthnRequest use AssertionConsumerServiceURL instead of AssertionConsumerServiceIndex.
KeyStore Description	<p>Specifies a custom description of the keystore file. Alternatively, you can specify a URI to a file that will be used instead of loading the keystore into OTDS. An example of a file URI reference is: <code>file:///c:/OTDS_Files/&lt;filename&gt;</code>.</p> <p>You can specify <b>SYSTEM</b> in this field in order to make OTDS use its internally generated keystore for signing.</p>
KeyStore	The keystore, in PKCS#12 format, containing the certificate and private key for this service provider's XML signing and encryption. Directory Services is an example of a service provider. This parameter is only required if signing/encryption is required by the identity provider. You can specify either this keystore or the public certificate and private keys separately.
KeyStore Password	The password for the keystore file.
KeyStore Alias	The alias for the public certificate and private key for Directory Services in the keystore file.
Certificate Description	Specifies a custom description of the certificate file. Alternatively, you can specify a URI to a file that will be used instead of loading the certificate into OTDS. For example, <code>file:///c:/OTDS_Files/&lt;filename&gt;</code> .

Parameter Name	Description
Certificate	This service provider's X.509 (PEM) public certificate for XML signing and encryption. Directory Services is an example of a service provider. This parameter is only required if signing/encryption is required by the identity provider. You do not need to specify this parameter if using a PKCS#12 keystore instead.
Private Key Description	Specifies a custom description of the private key file. Alternatively, you can specify a URI to a file that will be used instead of loading the private key into OTDS. For example, <code>file:///c:/OTDS_Files/&lt;filename&gt;</code> .
Private Key	This service provider's PKCS#8 DER encoded private key for XML signing and encryption. Directory Services is an example of a service provider. This parameter is only required if signing/encryption is required by the identity provider. You do not need to specify this parameter if using a PKCS#12 keystore instead.
Private Key Password	This parameter is only required if the PKCS#8 private key file or the private key in the PKCS#12 keystore is encrypted.
XML Signature Algorithm	This parameter is only relevant when <b>Certificate</b> and <b>Private Key</b> are configured. Valid values are defined in the "W3.org Algorithms" document referenced in " <a href="#">References to external websites</a> " on page 385.
Message Digest Algorithm	This parameter is only relevant when certificate and private key are configured.. Valid values are defined at <a href="https://www.w3.org/TR/xmldsig-core1/#sec-MessageDigests">https://www.w3.org/TR/xmldsig-core1/#sec-MessageDigests</a> .
Claim for impersonating user	A claim that contains the ID of the actor/impersonator for the user identified by NameID. It must be in the same format as NameID.
Claim for security clearance level	A claim that contains the user's security clearance level. This feature is specific to the <b>Security Clearance</b> module in OpenText Content Management.

Parameter Name	Description
Map all users to	Specifies the user name to which all authenticated users will be mapped once the SAML assertion is verified. The format of the name should correspond with the authentication principal attribute configured for this handler. This feature is not compatible with auto-provisioning. Users will not be provisioned if this parameter is set.
Claim <x>	SAML attribute/claim that should be mapped to a corresponding <b>OTDS Attribute &lt;x&gt;</b> . This value is case sensitive. Mapped claims are only relevant if the corresponding account is auto-provisioned in OTDS. If you want to enable auto-provisioning of SAML accounts, see <a href="#">Enable Auto-Provisioning of Accounts on page 297</a> .
OTDS Attribute <x>	The OTDS user attribute to which the corresponding SAML <b>Claim &lt;x&gt;</b> attribute/claim should be mapped.
AuthnContextClass <x>	Specifies a value to send in the AuthnContextClassRef element of a SAML AuthnRequest.
Step-up AuthnContextClass <x>	Specifies a value to send in the AuthnContextClassRef element of a SAML AuthnRequest when an application initiates step-up authentication. This is only used in specific use cases.
Authn Context Class Comparison	The Comparison attribute value to send in the AuthnRequest when one or more AuthnContextClass values are configured.

For more information, see “[Configuration and use of SAML authentication](#)” on page 159.

#### SAPSSOEXT

- **Description:** enables applications to verify SAP sign on tickets and extract the user ID from the sign on ticket. Validates SAP tokens using SAP certificates stored in password-protected Personal Security Environment .pse files. If you need to provide more certificates than the authentication handler allows, add another authentication handler. OTDS calls the SAPSSO libraries to validate and decrypt the SAP tokens.
- **Default Status:** not displayed.

- **Parameters:**

Parameter Name	Description
Map all SAP users to	Specify the OTDS user name to which all authenticated SAP users will be mapped after their sign on ticket is verified. The format of the name should correspond with the authentication principal attribute configured for this handler. For example, use the same format that would have been contained in the SAP sign on ticket.
SAP Certificate <x> Description	Specifies a custom description for the corresponding certificate.
SAP Certificate (PSE) <x>	Specifies a certificate, a .pse file, to use to decode SAP tokens. Note that the selected file does not need to reside on the server because only its contents will be stored on the server. Clear the string in this box to delete the certificate stored on the server.
SAP Certificate <x> Password	Specifies the password for the corresponding .pse file.

### Simple LDAP Authenticator

- **Description:** uses LDAP credentials and simple authentication or SASL authentication. For each synchronized user partition there is a **Simple LDAP Authenticator** authentication handler with the same name.
- **Default Status:** not displayed.
- **Parameters:**

Parameter Name	Description
Host(s)	The hostname or the IP address of the LDAPv3 server. Use a comma-separated list of hostnames or IP addresses to specify multiple servers.
Port(s)	The LDAPv3 port number. Use a comma-separated list of ports to specify multiple hosts.
Use SSL	Select <b>true</b> if this authentication handler will use SSL.
Bind Mechanism	The LDAP bind mechanism, either Simple or SASL/GSSAPI.
LDAP SPN (for SASL)	Kerberos Service Principal Name to be used with the SASL/GSS bind mechanism.

Parameter Name	Description
Timeout (seconds)	A positive integer representing the number of seconds until the authentication handler will timeout when connecting to, and reading from, the LDAP server.

### Web Access Management

- **Description:** extracts authenticated user information from configured HTTP headers. Used for environments with third-party authentication products such as CA SiteMinder, Entrust TruePass, Entrust GetAccess, RSA Access Manager, and any other product that sets an HTTP header or cookie to provide the identity of the user. For more information, see [“Integrating Directory Services with Web Access Management applications” on page 161](#).
- **Default Status:** not displayed.
- **Parameters:**

Parameter Name	Description
HTTP Header Name	Defines the HTTP header that contains the user's identity.
HTTP Header Encoding	Defines the encoding of the HTTP header's data. Valid values include none, base64, and url.
LDAP Resolution Required	Defines whether the value in the HTTP header needs to be resolved through an LDAP server. If so, you must provide the LDAP information below. Valid values are true or false.
LDAP Host	The hostname or IP Address of the LDAPv3 Server.
LDAP Port	The LDAPv3 port number.
LDAP SSL	Determines whether to use SSL. Valid values are true or false.
LDAP User Name	The simple bind user name.
LDAP Password	The simple bind password for the user entered in <b>LDAP User Name</b> .
HTTP Header Contains DN	Determines whether the HTTP header contains the DN of the user. Valid values are true or false.
LDAP Search Base	The search base (DN).
LDAP Search Timeout	A positive integer determining the timeout for LDAP searches, specified in seconds. Leave blank for infinite.
LDAP Lookup Filter	Defines the LDAP query to search for the user based on the information in the HTTP header. Specify “ as the placeholder for the information provided in the HTTP header.

Parameter Name	Description
LDAP User ID Attribute	Defines the name of the LDAP attribute that will be retrieved by the search that will be mapped to the OTDS user information.
WAM HTTP Cookie	Specifies the name of the HTTP cookie used by the WAM product. This parameter is used to provide a mechanism for OTDS clients to ensure OTDS tickets correspond to the WAM cookie as it was at authentication time.

### WebAuthn

- **Description:** authenticates users using WebAuthn passwordless authentication.  
For related information, see:
  - “Using WebAuthn to provide users the option of passwordless authentication” on page 103
  - Two Step Login on page 313
  - WebAuthn Policy on page 314
- **Default Status:** displayed and enabled.
- **Configuration:**

Configuration Requirement	Description
entryDN	This parameter is required. You must select and add <b>entryDN</b> as the <b>Authentication principal attribute</b> on the <b>Configuration</b> tab.

### Web Server

- **Description:** extracts authenticated user information set by the web or application server, such as Integrated Windows Authentication on IIS.
- **Default Status:** not displayed.

## 4.1.2 Prioritizing authentication handlers

Authentication handlers are evaluated according to priority. The lower the priority number, the higher the priority of the authentication handler. If there is only one authentication handler in use for a user partition, the priority has no meaning. If there are multiple authentication handlers in use for a user partition, they may share the same priority. This means that it is not important which authentication handler is applied first.

A priority is required when you are using multiple authentication handlers for user partitions on your Directory Services server. Every user partition will use a default authentication handler that has a default priority. Usually, this default is sufficient to

correctly apply authentication handlers according to the type of sign in attempt being authenticated.

For credentials-based sign in attempts, with a user name and password, authentication handlers for the user partition are evaluated first, in priority order, then, if no sign in has been achieved, global handlers are evaluated.

For non-credentials-based sign in attempts, only global handlers are evaluated, in priority order.

When new handlers are applied locally to a user partition or globally to all user partitions, you need to set a priority to control which authentication handler is evaluated first.

For more information, see “[Changing the priority of an authentication handler](#)” on page 164.

The following graphic shows authentication handlers that have been defined with priorities. Taking two of these authentication handlers as an example, they will be used in the following order:

1. `http.cookie`, the Directory Services SSO authentication handler, is assigned the priority 1 and will be used first.
2. `http.negotiate`, the Windows SSO authentication handler, is assigned the priority 20 and will be used last.

The screenshot shows the OTDS Admin interface with the 'Authentication Handlers' page selected. On the left, there is a sidebar with 'Partitions' (selected), 'Authentication Handlers' (checked), 'Resources', and 'Access Roles'. The main area has a title bar 'OTDS Admin > Authentication Handlers' with 'Add', 'Delete', and 'Refresh' buttons. Below is a search bar with 'Starts with' and 'Contains' options, a 'Search' button, and a 'Results per page' dropdown set to 25. A table lists two authentication handlers:

Name	Description	Scope	Priority	Status	Actions
http.cookie	Maintains an HTTP Session with...		1	enabled	Actions
http.negotiate	Handles "Negotiate" authenticati...		20	enabled	Actions

### 4.1.3 Configuration and use of OAuth authentication

The protocols available are:

1. If you select the **OAuth 1.0a** protocol you need to configure it with a Consumer Key and a Consumer Secret on the **Parameters** page.
2. If you select the **OAuth 2.0** protocol you need to configure it with a Client ID and a Client Secret on the **Parameters** page.

These values are obtained after the OTDS instance, your specific installation, is registered with the OAuth provider. In order to register your instance of OTDS with the provider, or site, that you want OTDS to access, you will first need to have an account with that site.

For example, if you want to register OTDS to access Facebook, you will need a Facebook account that you can sign into and register the OTDS instance.

See the URL references in “[References to external websites](#)” on page 385.

If you want to enable auto-provisioning of OAuth accounts, see [Enable Auto-Provisioning of Accounts](#) on page 297.

## Configuring an OAuth authentication handler to authenticate synchronized users by their email address

In the synchronized partition, add a user attribute mapping. For example:

- OTDS Attribute: oTUserID1
- Active Directory Attribute: mail
- Format: <Provider>://%



**Note:** The “<Provider>://” prefix must match the prefix configured on the authentication handler.

On the OAuth authentication handler, do the following:

- Change the **User Identifier Parameter** to the parameter containing the email address of the user.
- Change the authentication principal attribute to use oTUserID1.

### 4.1.4 Configuration and use of SAML authentication

The SAML 2.0 authentication handler implements:

- The Web Browser SSO profile, the HTTP authentication handler, which will redirect to the identity provider to authenticate and parse the SAML token and verify the signature on the token.
- The SAML token profile 1.1, the Token authentication handler, which will ensure that the entire <wsse:Security> header XML is picked up by OTDS and passed, as a token, to OTDS through `authenticateToken()`. It will parse the entire <wsse:Security> header to retrieve the <ds:SignedInfo> section of the SOAP request, and verify the signature of the caller.



1. Any change to certificates on either the Service Provider or Identity Provider requires metadata to be re-imported on the other entity. If the IdP Metadata URL was provided, OTDS will automatically retrieve the metadata from the IdP daily at midnight.
2. The SAML authentication handler can be bypassed by appending the query parameter “`otdsauth=no-saml`” to any resource URL or to the OTDS sign in page URL.
3. If you require a URL for IdP-initiated SSO, temporarily disable the SAML, and any other SSO handlers, in OTDS. Navigate to the desired destination URL. You will end up on the OTDS sign in page with a URL in the browser's address bar that can be used for IdP-initiated SSO.

For more information, see “Configuring SAML” on page 167 and Enable Auto-Provisioning of Accounts on page 297.

## Specifying mappings of claims in the SAML assertion

You can specify mappings of claims, or attribute statements, in the SAML assertion to OTDS attributes. You specify these mappings in the **Claim 1-20** and **OTDS Attribute 1-20** boxes. These mappings can *only* be used to set and update attributes on an auto-provisioned SAML account.

An account is auto-provisioned by OTDS when the following two conditions are met:

1. Auto-provisioning of accounts is enabled, see [Enable Auto-Provisioning of Accounts on page 297](#).
2. There is no pre-existing account in OTDS for the user identified in the SAML assertion.

If OTDS automatically provisions an account for the user, it is also possible to configure the handler to auto-provision the direct groups to which the user belongs.

In order to accomplish this, you must map the claim, or attribute, statement containing the group name. For example, map one of <https://schemas.microsoft.com/ws/2008/06/identity/claims/role> or <https://schemas.xmlsoap.org/claims/Group> to the `oTMemberOf` OTDS attribute. These examples are set by default when creating a new SAML 2.0 authentication handler.

## Support for WS-Trust

There is a new box, **WS-Trust**, in the SAML authentication handler to support WS-Trust. This box has been added to support validation of credentials through WS-Trust in environments where OTDS is not deployed on-site, or when there is no access to Active Directory/LDAP. In other words, when OTDS is deployed “in the cloud”.

Validating credentials directly is necessary in non-web based scenarios where a SAML-based redirection to the identity provider's sign in page is not possible. It is also necessary to allow certain applications integrated with OTDS to obtain tokens for other relying parties configured on the identity provider.

Some OTDS-integrated applications may use a Kerberos token to authenticate a user through OTDS with WS-Trust in order to achieve SSO to other relying parties. For the Kerberos scenario to work when Microsoft Active Directory Federation Services (ADFS) is used as the identity provider, the `ExtendedProtectionTokenCheck` setting on ADFS must be set to `None`.



**Note:** WS-Trust functionality has only been tested with ADFS. If using another identity provider, it must have a WS-MEX metadata URL that must be specified for the WS-Trust Metadata URL.

For more information, see “Configuring SAML” on page 167.

## 4.1.5 Integrating Directory Services with Web Access Management applications

Web Access Management, WAM, applications include the following:

- CA SiteMinder
- Entrust TruePass
- Entrust GetAccess
- RSA Access Manager
- Any other product that sets an HTTP header or cookie to provide the identity of the user.

The following table shows default values for the HTTP header for each product.

Product	Default HTTP header value
CA SiteMinder	SM_USER
Entrust GetAccess	USER
Entrust TruePass	ENTRUST-CLIENT
RSA Access Manager	CT-REMOTE-USER

Most third-party authentication product agents do not have agents for either Tomcat. Therefore, a web server is required and it must be configured to proxy requests to Tomcat.

A connector is required to configure a web server to make Directory Services accessible through the web server port and to forward web server traffic destined for Directory Services.

The Apache Tomcat connector, and associated reference guide, is available from the “Apache Tomcat Connectors web site”, “[tomcat.apache.org/connectors-doc/](http://tomcat.apache.org/connectors-doc/)”, see “[References to external websites](#)” on page 385.



**Note:** For SAP NetWeaver, the third-party authentication product must support the platform directly. The integration is often achieved through a SAML-based interaction. Contact your third-party authentication product vendor for details.

For more information, see “[Integrating Directory Services with Web Access Management applications](#)” on page 170.

## 4.2 Creating an authentication handler

### To create an authentication handler:

1. From the web administration menu, click **Auth Handlers**.
2. From the button bar, click **Add**. The **New Authentication Handler** wizard will guide you through the steps.
3. On the **General** page, do the following:
  - a. In the **Authentication Handler name** box, type a name for your authentication handler.
  - b. From the **Authentication Handler type** list, select an authentication handler type. For information about authentication handler types and their requirements, see “[List of authentication handlers](#)” on page 138.
  - c. **Optional** In the **Description** box, the description of the authentication handler is provided by Directory Services based on your selection of the authentication handler type. You can change this description to reflect how you intend to use this authentication handler. For example, you could create a [Guest Account on page 139](#) authentication handler and change the description to “This handler is applied to all guest users in opentext.net”.
  - d. Click **Next**.
4. On the **User Partition** page, select one of the following, and then click **Next**:
  - Select **Global** to apply this authentication handler to all user partitions on this Directory Services server.
  - Select **User partition** and choose a user partition to apply this authentication handler to an existing user partition.

When you begin typing, an alphabetical list of user partitions that begin with the first letter you typed will appear, and you can select the user partition from that list.



**Note:** Only credentials-based authentication handlers, ones that take a user name and password, can be assigned to a user partition. This occurs because Directory Services needs the user name before authentication in order to determine the name of the partition to which the user belongs. Other authentication handlers can only provide the user name after authentication has happened.

5. If the authentication handler you chose has required parameters, you will see the **Parameters** page. On the **Parameters** page, enter those required parameters and then click **Next**.

For information about authentication handler required parameters, in the web admin UI, on the **Parameters** page, click **Parameters Descriptions**. You can also view descriptions of the parameters in the “[List of authentication handlers](#)” on page 138.

6. On the **Configuration** page, do the following:
  - a. **Optional** Clear the **Enable authentication handler** box if you *do not* want to enable this authentication handler. By default, this box is selected and the authentication handler is enabled when it is created.
  - b. In the **Priority** box, specify a priority to explicitly control the order in which authentication handlers are evaluated. For more information, see “[Prioritizing authentication handlers](#)” on page 157.
  - c. From the list box, select an attribute that will uniquely find a given user in Directory Services.
  - d. As soon as you have the attribute, click **Add** to add the attribute to the **Authentication principal attribute** box. If you need to make changes, highlight the attribute in the **Authentication principal attribute** box and click **Delete** to remove it.

For more information, see “[Authentication principal attribute](#)” on page 137.

7. Click **Save**.

## 4.3 Editing an authentication handler

### To edit an authentication handler:

1. From the web administration menu, click **Auth Handlers**.
2. From the **Actions** menu of the authentication handler you want to edit, click **Properties**. The **Edit Authentication Handler** assistant will guide you through the steps to edit an existing authentication handler.
3. On the **General** page, do the following:
  - a. You cannot change the value in the **Authentication Handler name** box.

 **Note:** Authentication handlers that were automatically created when the user partition was created will have the same name as the user partition.
  - b. You cannot change the **Authentication Handler type** list. For information about authentication handler types and their requirements, see “[List of authentication handlers](#)” on page 138.
  - c. **Optional** In the **Description** box, the description of the authentication handler is provided by Directory Services based on your selection of the authentication handler type. You can change this description to reflect how you intend to use this authentication handler. For example, you could create a [Guest Account](#) on page 139 authentication handler and change the description to “This handler is applied to all guest users in opentext.net”.
  - d. Click **Save** if you have finished editing your authentication handler, or click the **User Partition** tab.
4. You can view descriptions of the boxes you can edit in the “[Creating an authentication handler](#)” on page 162 procedure.

5. Click **Save**.

## 4.4 Deleting an authentication handler

**To delete an authentication handler:**

1. From the web administration menu, click **Auth Handlers**.



### Caution

Deleting an authentication handler cannot be undone.

2. Select the box to the left of the authentication handler you want to delete, and then, on the button bar, click **Delete**.



**Note:** Some authentication handlers installed by Directory Services cannot be deleted. If you delete an authentication handler that was created when a user partition was created, the global authentication handlers will be used.

3. In the **Delete** box, click **OK** to confirm or click **Cancel** to keep the authentication handler.

## 4.5 Changing the priority of an authentication handler

**To change the priority of an authentication handler:**

1. From the web administration menu, click **Auth Handlers**.
2. From the **Actions** menu of the authentication handler whose priority you want to change, click **Properties**.
3. Select the **Configuration** tab.
4. On the **Configuration** page, in the **Priority** box, type the new priority.
5. Click **Save**.

## 4.6 Enabling or disabling an authentication handler

### To enable an authentication handler:

1. From the web administration menu, click **Auth Handlers**.
2. From the **Actions** menu of the authentication handler you want to enable, click **Enable**.

### To disable an authentication handler:

1. From the web administration menu, click **Authentication Handlers**.
2. From the **Actions** menu of the authentication handler you want to disable, click **Disable**.

## 4.7 Configuring the http.negotiate authentication handler on Unix

### To configure the http.negotiate authentication handler on Unix:



**Note:** Before beginning this procedure, use the command: nslookup <IP\_address\_of\_server>

Ensure that this command succeeds on your OTDS server, and that it returns otdsserver.domain.com, or the matching server name in the SPN.

1. Create a dedicated service account for OTDS, DOMAIN\serviceaccount. Being a service account, the password for this service account must not expire.
2. Get a keytab file by following these steps:
  - a. Open a command prompt window as the service account you created in [step 1](#), then run the following commands:
    1. setspn -a HTTP/otdsserver.domain.com DOMAIN\serviceaccount
    2. ktpass -princ HTTP/otdsserver.domain.com@DOMAIN.COM -out krb5kt -mapuser DOMAIN\serviceaccount -mapOp set -pass <PASSWORD> -ptype KRB5\_NT\_PRINCIPAL -crypto AES256-SHA1
  - b. Move the krb5kt file to the Tomcat current working directory.  
The current working directory can be determined by running the command: pwdx <pid>  
Where <pid> is the process ID of the Tomcat process.
3. Set the Java system properties by choosing *one* of the following options:
  - Your first option is to run the following commands:
    1. Run the command: set java.security.krb5.realm = DOMAIN.COM

2. Run the command: `set java.security.krb5.kdc = kdc.domain.com`
- Your second option is to run the command: `set java.security.krb5.conf = conf/krb5.conf`
- Your third option is to set up a default `/etc/krb5.conf` file. Next, read the manual entry by running the `man krb5.conf` command.

**!** **Important**

1. If you change the service account's password you will require a new keytab file.
2. If you change the keytab file you must restart Tomcat.
3. Any client workstations that have authenticated with OTDS using the previous keytab file will need to sign out, then sign back in.
4. OpenText recommends that this procedure should be performed one time, at OTDS installation time only, and subsequent updates to the keytab file should be avoided.

## 4.8 Configuring the Oracle EBS authentication handler

### To configure the Oracle EBS authentication handler:

1. Obtain the “Oracle E-Business Suite Software Development Kit for Java”:
  - a. Sign in to the “My Oracle Support” web site, for more information see “[References to external websites](#)” on page 385.
  - b. Download the “Oracle E-Business Suite Software Development Kit for Java, document number 974949.1”, for more information see “[References to external websites](#)” on page 385.
  - c. Copy the `fndext.jar` file to your `<Tomcat_home>/lib` directory.
2. Navigate to the `<OTDS_installdir>\otds\WEB-INF\lib` directory.
3. Type the following command:

```
java -cp fndext.jar;ojdbc6.jar oracle.apps.fnd.security.AdminDesktop
<applications_username>/<applications_username_pwd> CREATE NODE_
NAME=<OTDS_server_node_name> IP_ADDRESS=<OTDS_server_IP_address>
DBC=<EBS_System_DBC_file>
```

Where:

`<applications_username>/<applications_username_pwd>`

is an Oracle E-Business Suite user name and password, an applications user, that you create for OTDS to use. That applications user must have the UMX | APPS\_SCHEMA\_CONNECT role assigned to it.

You will provide these credentials, the user name and password that you create here, in the Oracle EBS authentication handler.

*<OTDS\_server\_node\_name>*  
is the node name of the OTDS server.

*<OTDS\_server\_IP\_address>*  
is the IP address of the OTDS server.

*<EBS\_System\_DBC\_file>*  
is the location of your standard Oracle EBS system DBC file.

For Oracle E-Business Suite 11i, the DBC file is typically located under \$FND\_TOP/secure. For Release 12, the DBC file is typically located under \$FND\_SECURE. If the DBC file does not exist, the system administrator should generate it using Autoconfig. See the **Oracle E-Business Suite System Administrator's Guide - Configuration** for more information on the DBC file.

4. After this command completes, it will generate a Desktop DBC file that you must then specify in the Oracle EBS authentication handler created in OTDS.
5. You must now provide the credentials, *<applications\_username>/<applications\_username\_pwd>*, for the applications user in the Oracle EBS authentication handler in OTDS.

## 4.9 Configuring SAML

### To configure SAML:

1. Export the Identity Provider, IdP, metadata from the IdP into XML format. Consult the provider's documentation for details.
2. Create a SAML 2.0 Authentication Handler. During the creation of your SAML authentication handler, enter the parameters as follows:
  - a. In the **Identity Provider (IdP) Name** box, enter any name for the Identity Provider. This should be a single word, since it will be part of the metadata URL.
  - b. You must specify only one of either **IdP Metadata URL** or **IdP Metadata File**.
    - Choose **IdP Metadata URL** if you are not intending to specify a *<filename>.xml* file in the **IdP Metadata File** box below, you must provide the URL to the IdP's metadata. Providing a URL allows OTDS to automatically update the metadata, daily, at midnight. This is useful for handling certificate changes on the IdP.
    - Choose **IdP Metadata File** if you are not intending to provide a URL for the **IdP Metadata URL**. You must then browse to select the *<filename>.xml* file containing your IdP's metadata.
  - c. In the **WS-Trust Metadata URL** box, specify the URL to support validation of credentials through WS-Trust in environments where OTDS is not deployed on-site or there is no access to Active Directory or LDAP. In other

words, when OTDS is deployed “in the cloud”. For more information, see [“Support for WS-Trust” on page 160](#).

 **Note:** WS-Trust functionality has only been tested with ADFS. If using another identity provider, it must have a WS-MEX metadata URL that must be specified for the WS-Trust Metadata URL.

- d. In the **IdP NameID Format** box, indicate the NameID format that OTDS will specify in authentication requests. The NameID's value returned for users must correspond to the value of the attribute specified for the Authentication Principal Attribute in the authentication handler, which is configured in [step 3](#).
- e. In the **OTDS SP Endpoint** box, specify the service provider URL that will be used to identify OTDS to the identity provider. If this box is left blank, the URL will be taken from the request. You should enter a value to this box if your environment has OTDS behind a reverse-proxy.
- f. In the **Trusted Audiences** box, type a space-separated list of service provider audience value that should be trusted, in addition to the OTDS SP URL.
- g. In the **Active By Default** box, select either true or false. If set to true, all authentication requests to OTDS will be redirected to the SingleSignOnService URL of the IdP, as specified in its metadata. Set this to false if SAML will only be used for authenticating web service calls.
- h. In the **Allow Auto-Provisioning** box, state whether to allow this handler to auto-provision users.
- i. In the **Grace Period** box, type the amount of time to allow for differences in the system clocks between OTDS and the IdP. The grace period is used to avoid rejecting SAML assertions due to minor clock differences between the SP and IdP.
- j. In the **Auth Request Binding** box, you can specify the preferred SAML binding to use for sending the AuthnRequest, provided it is supported by the identity provider.
- k. In the **Auth Response Binding** box, you can specify the SAML binding to use for the response to an AuthnRequest.
- l. In the **Use AssertionConsumerServiceURL** box, you can set this to “true” if you want to have the SAML AuthnRequest use AssertionConsumerServiceURL instead of AssertionConsumerServiceIndex.
- m. In the **KeyStore Description** box, you can specify a custom description of the KeyStore file.
- n. In the **KeyStore** box, you can specify the KeyStore, in PKCS#12 format, containing the certificate and private key for this service provider for XML signing and encryption.
- o. In the **KeyStore Password** box, you can specify the password for the KeyStore file.
- p. In the **KeyStore Alias** box, you can specify the alias for the public certificate and private key for OTDS in the KeyStore file.

- q. In the **Certificate Description** box, you can specify a custom description of the **Certificate** file.
- r. In the **Certificate** box, enter the certificate for OTDS. This must be an X.509 (PEM) certificate.
- s. In the **Private Key Description** box, you can specify a custom description of the **Private Key** file.
- t. In the **Private Key** box, enter the private key for OTDS. This must be a PKCS#8 DER encoded private key.



**Note:** The private key and certificate for OTDS are only required if the IdP requires signed authentication requests, or if the IdP sends encrypted assertions, or if the IdP encrypts the NameID.

- u. In the **Private Key Password** box, you only need an entry to this box if the PKCS#8 private key file or if the private key in the PKCS#12 keystore is encrypted.
  - v. In the **XML Signature Algorithm** box, you only need an entry to this box when the **Certificate** and **Private Key** are configured. Valid values are defined at: <http://www.w3.org/TR/xmldsig-core1/#sec-AlgID>
  - w. In the **Message Digest Algorithm** box, you only need an entry to this box when the **Certificate** and **Private Key** are configured. Valid values are defined at: <https://www.w3.org/TR/xmldsig-core1/#sec-MessageDigests>
  - x. In the **Claim for impersonating user** box, you can specify a claim that contains the ID of the actor/impersonator for the user identified by NameID. It must be in the same format as NameID.
  - y. In the **Claim for security clearance level** box, you can specify a claim that contains the user's security clearance level. This feature is specific to the Security Clearance module in OpenText Content Management.
  - z. In the **Map all users to** box, you can specify the user name to which all authenticated users will be mapped once the SAML assertion is verified.
  - aa. In the **Claim <x>** and **OTDS Attribute <x>** boxes, you can specify mappings of claims, or attribute statements, in the SAML assertion to OTDS attributes. These mappings can *only* be used to set and update attributes on an auto-provisioned SAML account. For more information, see “[Specifying mappings of claims in the SAML assertion](#)” on page 160.
  - ab. In the **AuthnContextClass <x>** box, you can specify a value to send in the **AuthnContextClassRef** element of a SAML **AuthnRequest**.
  - ac. In the **Step-up AuthnContextClass <x>** box, you can specify a value to send in the **AuthnContextClassRef** element of a SAML **AuthnRequest** when an application initiates step-up authentication. This is only used in specific use cases.
3. On the **Configuration** tab, in the **Authentication Principal Attribute** box, you must specify an attribute that contains the value that will be returned for NameID. For example, if `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress` was specified for NameID format, then `mail` can be the

attribute to select for the **Authentication Principal Attribute**. You can view the properties of any user to verify the desired attribute.

4. Obtain the OTDS Service Provider, SP, metadata to be imported into the IdP by accessing the URL: `http(s)://<OTDSserver:port>/otdsws/login?SAMLMetadata=<name>`, where `<name>` is the value entered in the **Identity Provider Name** box of the handler's parameters.
5. Import OTDS' metadata from [step 4](#) into the IdP.

## 4.10 Integrating Directory Services with Web Access Management applications

### To integrate Directory Services with Web Access Management Applications:

1. The WAM web server agent must be configured to intercept calls to Directory Services. To allow the agent to intercept calls to Directory Services on Tomcat, it is necessary to have the web server act as a reverse proxy to Directory Services. As a result, Directory Services will be accessible through the web server port, typically port 80. If you want the web server to forward traffic destined for Directory Services, you must configure the web server.

If you are using Apache Tomcat, you can use the Tomcat Connector for this purpose.



**Note:** Any native capability in the web server, such as the Application Request Routing (ARR) for IIS, will not work if it routes requests before the web server agent has processed the request.

The Tomcat Connector is available for IIS, Apache Web Server, and Sun ONE Web Server from the “Apache Software Download web site”, for more information see [“References to external websites” on page 385](#).

2. All Directory Services application paths must be configured to be processed by the connector in the `uriworkermap.properties` file. This includes the following paths:

- `/OTDSConnectors/*`
- `/ot-auth/*`
- `/ot-authws/*`
- `/ot-reg/*`
- `/ot-transfer/*`
- `/ot-trigger/*`
- `/ot-universaladmin/*`
- `/otds-system-configuration/*`
- `/otds-usergroup/*`
- `/otds-v2/*`
- `/otdsws/*`

The complete list can be viewed through the Tomcat Manager user interface.

3. The WAM agent must be configured to intercept calls *only* to /otdswebs/login, and its sub-paths, for example, /otdswebs/login\*. All other paths are web service SOAP endpoints that are used by web services clients and cannot handle HTTP redirects and intercepts by a web agent.
4. The Web Access Management authentication handler must be created in the OTDS web client in Directory Services. The configuration parameters vary depending upon which Web Access Management application you are using and how you are using it. Set a priority of 0 for the handler to ensure it is invoked prior to any other handler.
5. Resources, such as OpenText Content Management, must be configured so that client requests are sent through the WAM agent. When configuring your resource for Directory Services integration, you should specify the web server port, and not the Tomcat port, when specifying the Directory Server location.



**Note:** After configuring the environment as described in this procedure, open a new browser instance and attempt to sign in to Directory Services by opening the URL <http://otdsserver.opentext.com/otdswebs/login>. Your request will be intercepted by the web agent and you will be prompted for sign in credentials by the agent. After entering your credentials, you should see the **Directory Services Welcome** page that shows your Directory Services user id. No sign in prompt from Directory Services should be shown.



# Chapter 5

## Resources

This section describes creating, editing, and deleting resources. This section also describes how to deliver user and group data to synchronized resources and how to configure *synchronized* and *non-synchronized* resources for authentication.

You will need to create a new resource in Directory Services to represent each application that you want to connect to your Directory Services server for synchronization and authentication. You can create a non-synchronized resource or a synchronized resource.

The **Resources** page displays an alphabetical list of all resources that you have defined to represent the enterprise applications. It also displays the resource ID for that resource, the display name, and the description.

By selecting any resource's **Actions** link, you can view and edit the **Access Roles** that apply to this resource. You can also allow users on your resource to impersonate users on another resource, manage synchronization of data from Directory Services to your resource, and control authentication of users on this resource. In certain cases, the control of authentication is a two-step process that requires initiation of authentication in Directory Services followed by the actual activation of authentication at the enterprise application.

### Resources added to trusted sites

When the product for which you are creating a resource is located on a different system than your installation of OTDS, you must add your product's URL to the trusted sites in OTDS. For more information, see “[Trusted Sites](#)” on page 327. An example of a trusted site is: <http://mymachine.opentext.net>

### Resources and single sign out

When implementing single sign out for OTDS and resources, your resource's documentation will provide the information required by OTDS' **Sign out URL** and **Sign out Method** text boxes. For more information about single sign out in OTDS, see “[Single sign out](#)” on page 351.

## 5.1 Resources Actions menu options, buttons and column headings

On the main **Resources** page, each resource has associated **Actions** menus and applicable buttons. The available options depend on whether you select a synchronized or a non-synchronized resource.

These pages detail the **Actions** menu options, buttons, and column headings of the **Resources** page.

### Resources Actions menu items

This table details the options available in the **Actions** menu for a resource. There are quick links to the procedures associated with each action.

Actions menu option	Associated Procedure
Properties	<a href="#">"Editing a non-synchronized resource" on page 179</a> and <a href="#">"Editing a synchronized resource" on page 213</a>
Activation Status	If you want to view or copy the resource identifier of your non-synchronized resource, or if you want to verify your activation status, click <b>Activation Status</b> .
Edit Access Roles	<a href="#">"Editing access roles for your resource" on page 225</a>
Notifications	<a href="#">"Editing notification settings for your resource" on page 225</a>
Impersonation Settings	<a href="#">"Editing impersonation settings" on page 225</a>
Activate/Deactivate Resource	<a href="#">"Activating or deactivating your resource" on page 227</a>
Enable/Disable Authentication for the Resource	<a href="#">"Enabling or disabling authentication for your resource" on page 228</a>
Turn Synchronization On/Off	<a href="#">"Turning user synchronization on or off" on page 226</a>
Consolidate	<a href="#">"Consolidating a synchronized resource" on page 217</a>

### Resources buttons

Button	Associated Procedure
Add	<a href="#">"Creating a non-synchronized resource" on page 176</a> and <a href="#">"Creating a synchronized resource" on page 206</a>
Delete	<a href="#">"Deleting a non-synchronized resource" on page 180</a> and <a href="#">"Deleting a synchronized resource" on page 218</a>
Refresh	Use the <b>Refresh</b> button to verify if OTDS has completed an action. For example, after deleting.
Help	The <b>Help</b> button will open context-sensitive help for the page you are currently using.

## Resources column headings

Column name	Description
Resource Name	The name you provided when you created the resource.
Resource ID	The resource ID provided by OTDS when you created the resource.
Display Name	If, when you created your resource, you typed an entry in the optional <b>Display Name</b> box, that text is displayed here.
Description	If, when you created your resource, you typed an entry in the optional <b>Description</b> box, that text is displayed here.
Sync	Displays either <b>disabled</b> or <b>enabled</b> on a synchronized resource to indicate if synchronization is enabled. For more information, see <a href="#">“Turning user synchronization on or off” on page 226</a> .
Authentication	Displays either <b>disabled</b> or <b>enabled</b> on a synchronized resource to indicate if authentication is enabled. For more information, see <a href="#">“Enabling or disabling authentication for your resource” on page 228</a> .
Connection	<p>Displays either <b>healthy</b> or <b>unhealthy</b> on a synchronized resource to indicate the status of the last connection attempt made by OTDS.</p> <p>It is only updated when a connection attempt fails or succeeds. If there is no synchronization activity through incremental sync, scheduled sync, or consolidation, then the status will not be updated.</p> <p> <b>Note:</b> The connection status is not an indicator of any errors or warnings during synchronization. It is strictly an indicator of the health of the network connection to the server.</p>
Actions	For information about the available actions, see <a href="#">“Resources Actions menu items” on page 174</a> .

## 5.2 Non-synchronized resources

Non-synchronized resources are created for applications that do not rely on users and groups being pushed from Directory Services. You can create non-synchronized resources even if the applications for which they are intended are not yet installed. A non-synchronized resource uses Directory Services authentication for single sign on. If you have created a non-synchronized resource, you are automatically configured to authenticate users who have access permission to this resource.

It is possible to create a resource without selecting user and group synchronization. You can edit the resource later to enable synchronization and create user and group attribute mappings. This would be necessary when you are creating a resource in your Directory Services server for an application that has not been installed yet. If

the installation of the resource requires the resource identifier from Directory Services, then you must create a non-synchronized resource, install your resource, and then change your non-synchronized resource to a synchronized resource and map it to the installed resource.

This section describes creating, editing, and deleting non-synchronized resources.

### The \_\_NAME\_\_ user attribute

1. The \_\_NAME\_\_ attribute mapping must be configured to the user or sign in name format desired for your resource. Select an OTDS attribute that will ensure that the user/sign in names in the resource will be unique across all users pushed. If users from only one partition will be accessing the resource, or you are certain there are no user name conflicts between your partitions, you can use `oExternalID1`. Otherwise, use `oExternalID3` or `oExternalID4`, depending on the desired format.
2. You cannot specify a compound mapping for the \_\_NAME\_\_ attribute. A simple mapping is required to do reverse lookups in Directory Services. Authentication requires reverse-lookup of a user name, from the name in the resource to the actual user object in your database. Because OTDS cannot perform the reverse lookup if the account name is a compound value, user names in the resource must not be computed as a compound mapping.
3. You can set whether to preserve the case of user and group names being pushed to OpenText Content Management or whether to set them to either lower or upper case. You can set user name case sensitivity on the **User Attribute Mappings** page. You can set group name case sensitivity on the **Group Attribute Mappings** page.

In the **Format** text box:

- To preserve case, leave the default setting, "%s".
- To set lower case, type: %l
- To set upper case, type: %u
- If values are DNs, type: %v to translate to the user name or group name of the target DN.

#### 5.2.1 Creating a non-synchronized resource

##### To create a non-synchronized resource:

1. From the web administration menu, click **Resources**.
2. On the button bar, click **Add**. The **New Resource** wizard will guide you through the steps to create a new resource.
3. On the **General** page, do the following:
  - a. In the **Resource name** box, type a descriptive name for this resource. Because a resource can be used by multiple products, you might consider using the environment and purpose as your resource name. For example,

“Production document processing” or “Test billing system”. The name you type here cannot be edited later.

- b. **Optional** In the **Display Name** box, if you want this resource's displayed name to be different than the name you provided in the previous box, the **Resource name** box, type the name you want displayed on the **Resources** page in this box. This box can be edited at a later date.
- c. **Optional** In the **Description** box, type a short description of this resource.



**Note:** The resource identifier will not appear for a **New Resource** creation but will be available for selection when editing an existing resource. See “[Editing a synchronized resource](#)” on page 213 for more information.

- d. From the **Sign in UI Version** list, select which OTDS user interface to display at the OTDS sign in page. To accept the default of the resource, select “default” from the list. For more information, see “[Customizing the sign-in page](#)” on page 354.
- e. **Optional** In the **Sign in UI Style** box, type the full file name with extension of the customized graphic to be applied to the OTDS login page. For example, type “my\_company\_graphic.png”. For more information, see “[Customizing the sign-in page](#)” on page 354.
- f. **Optional** In the **Sign out URL** box, if you want to implement OTDS' single sign out functionality, you must enter a value in this box and the **Sign out Method** box.

Check the documentation for this resource being created for the value to enter in this box. For more information, see “[Single sign out](#)” on page 351.

- g. **Optional** From the **Sign out Method** list, if you want to implement OTDS' single sign out functionality, you must enter a value in this box and the previous box, the **Sign out URL** box.

The value you type to this box is supplied in the documentation for the resource for which this is being created. For more information, see “[Single sign out](#)” on page 351.

- h. Click **Next**.
4. On the **Synchronization** page, clear the **User and group synchronization** box, and then click **Next**.
  5. On the **User Attribute Mappings** page, do the following:
- a. The **Resource Attribute** NAME needs to be mapped to an OTDS attribute. This attribute will be used as the user name in the resource.



**Note:** The default, oTExternalID3, appears as <username>@<domainname> and a user would use this form to sign in to the resource. This administrator can choose any user attribute to represent the user name. For example, oTExternalID1 appears as <username>, oTExternalID2 appears as <username>@<user-partition-

*name*>, and oTExternalID4 appears as <NETBIOS\_DOMAIN\_NAME>\<username>.

- b. In the **OTDS Attribute(s)** text box, type the OTDS user attribute name.
  - c. In the **Format** text box, type the format to be used. For more information, see “[Support for javascript and multi-valued javascript in the Format column](#)” on page 183.
  - d. Click **Save**.
6. In the **Resource Activation** window, do the following:
- a. **Optional** If you are going to configure the resource to activate it with Directory Services now, highlight and copy the resource identifier to use in the resource's configuration.  
If you are going to configure the resource to activate it with Directory Services later, see “[Editing a synchronized resource](#)” on page 213 for information on how to retrieve the resource identifier.
  - b. **Optional** Click **Verify Activation** to check that the resource has activated with Directory Services. An information box appears. Read the information, then close the information box.



#### Important

After your resource has been created, you should configure access roles to allow users with those access roles to sign in to your resource. A default access role, Access to <Resource name> is created when you create a resource. The group, `otdsadmins@otds.admin` is automatically added to this access role. This allows the user `otadmin@otds.admin` to access your resource. For more information on configuring access roles, see “[Editing access roles for your resource](#)” on page 225.

7. If you have created this non-synchronized resource for Enterprise Process Services, install User Management Server using the resource identifier copied to the clipboard. For more information, see *OpenText User Management Server - Installation Guide (UM-IGD)*.

## 5.2.2 Configuring a non-synchronized resource

### To configure a non-synchronized resource:

1. From the web administration menu, click **Resources**, and then select the non-synchronized resource you want to configure.
2. In the center pane, from the **Actions** menu associated with the non-synchronized resource you want to configure, select one of the following:
  - If you want to edit the non-synchronized resource, click **Properties**, and then follow the instructions found in “[Editing a non-synchronized resource](#)” on page 179.

- If you want to view or copy the resource identifier of your non-synchronized resource, or if you want to verify your activation status, click **Activation Status**.
- If you want to edit the access roles for this non-synchronized resource, click **Edit Access Roles**, and then follow the instructions in “[Editing access roles for your resource](#)” on page 225.
- If you want to edit the impersonation settings for this non-synchronized resource, click **Impersonation Settings**, and then follow the instructions in “[Editing impersonation settings](#)” on page 225.

### 5.2.3 Editing a non-synchronized resource

#### To edit a non-synchronized resource:

1. From the web administration menu, click **Resources**.
2. From the **Actions** menu associated with the non-synchronized resource you want to edit, click **Properties**.
3. On the **General** page, do the following:
  - a. The **Resource name** box is not editable.
  - b. **Optional** If you want this resource's name to display differently from the name it was given when it was created, you can type or edit that name in the **Display Name** text box.
  - c. **Optional** In the **Description** text box, you can type a short description of this resource.
  - d. **Optional** If you are going to configure the resource to activate it with Directory Services now, copy the **Resource identifier** to save it to use in the resource's configuration.
  - e. If you have finished editing your non-synchronized resource, click **Save**. To continue editing this resource, select the **Synchronization** tab.
4. On the **Synchronization** page, the **User and group synchronization** check box is cleared because this is a non-synchronized resource.  
Click the **Principal Attribute** tab.
5. On the **Principal Attribute** page, do the following:
  - From the **Authentication principal attribute** list, choose an attribute that uniquely defines a given user in Directory Services. This attribute will be used as the user name in the resource.  
The default, `oTExternalID3`, appears as `<username>@<domainname>` and a user would use this form to sign in to the resource. This administrator can choose any user attribute to represent the user name. For example, `oTExternalID1` appears as `<username>`, `oTExternalID2` appears as `<username>@<user-partition-name>`, and `oTExternalID4` appears as `<NETBIOS_DOMAIN_NAME>\<username>`.

6. Click **Save**.

### 5.2.4 Deleting a non-synchronized resource

**To delete a non-synchronized resource:**

1. From the web administration menu, click **Resources**, and then click the select box to the left of the resource name you want to delete.
2. On the button bar, click **Delete**.
3. Confirm that you want to delete this resource by clicking **OK**.



**Note:** You may want to click **Refresh** to confirm that the resource has been deleted.

## 5.3 Synchronized resources

Synchronized resources are created when users and groups from Directory Services need to be pushed to the application for which the resource is created. For example, you would create a synchronized resource for OpenText Content Management so that users and groups could be automatically created from your users and groups in your user partition. Synchronized resources require that a connection to the application be established. This means that you can only create a synchronized resource after the application is installed.

This section describes creating, editing, deleting, and importing user and group data in synchronized resources.

### 5.3.1 Configuring synchronized resources

The following pages describe the configuration options when creating a synchronized resource. You can also see “[Creating a synchronized resource](#)” on page 206.

You can create the following types of synchronized resources:

- Archive Center: see “[Connection parameters for Archive Center resources](#)” on page 188
- OpenText Content Management: see “[Configuring a synchronized resource for OpenText Content Management](#)” on page 193



#### Important

You must install Content Web Services before creating a synchronized resource for OpenText Content Management. For more information on installing Content Web Services, see *OpenText Content Management - Installation Guide (LLESCOR-IGD)*.

- eDocs DM: see “[Connection parameters for eDocs DM resources](#)” on page 189

- Enterprise Process Services: see “[Configuring a synchronized resource for Enterprise Process Services](#)” on page 205
- MBPM: see “[Connection parameters for MBPM resources](#)” on page 189
- Media Management: see “[Connection parameters for OpenText Media Management resources](#)” on page 189
- Process Component Library: see “[Connection parameters for Process Component Library resources](#)” on page 190
- REST (Generic): see “[Connection parameters for REST \(Generic\) resources](#)” on page 190
- Service Center: see “[Connection parameters for Service Center resources](#)” on page 190
- WSM Delivery Server: see “[Connection parameters for WSM Delivery Server resources](#)” on page 191
- WSM Management Server: see “[Connection parameters for WSM Management Server resources](#)” on page 192

### 5.3.1.1 User and group synchronization

If a resource is synchronized, it means that the users and groups in the access roles assigned to the resource are added to the internal users and groups maintained by the application for which the resource is created. For example, if you are creating a synchronized OpenText Content Management resource, users and groups that are allowed to access your OpenText Content Management will be created in OpenText Content Management automatically.

You can also customize the rights that Directory Services has to create, modify, or delete users in your resource. For more information, see “[Managing user and group permissions for this resource](#)” on page 181.

### 5.3.1.2 Managing user and group permissions for this resource

For a synchronized resource, it is important to manage how changes to users in Directory Services will be reflected in the synchronized resource. To manage this, there are three distinct permissions for every synchronized resource:

---

#### Create users and groups

By default, this option is selected and users are created in the resource. An administrator setting up a synchronized resource may not initially want to push users and groups to the resource. Clearing this option allows the administrator to delay the creation of users and groups in the resource.

---

#### Modify users and groups

By default, this option is selected and modifications to all users are automatically propagated to the resource. An administrator may want to make major changes to users and groups but not immediately push these changes to the resource. Clearing this option allows the administrator to delay the modification of users and groups in the resource.

**Delete users and groups**

By default, this option is cleared and users who have access to the removed resource are not immediately deleted from that resource. By default, the user remains in the resource, however, the user's access to the resource is denied. Selecting this option means that the user is deleted from the resource when access to the resource is removed in Directory Services.



**Tip:** Whenever these permissions are changed, you should **Consolidate** all users and groups that have access to this resource. For more information, see “[Consolidating users and groups in Partitions](#)” on page 128.

### 5.3.1.3 Using resource attribute mappings

User and group attribute mappings are used to map Directory Services user and group information to resource user and group information. Each attribute mapping can apply multiple attributes of Directory Services to an attribute in your resource.

**Important**

The `__NAME__` attribute mapping must be configured to the user or sign in name format desired for your resource. Select an OTDS attribute that will ensure that the user/sign in names in the resource will be unique across all users pushed. If users from only one partition will be accessing the resource, or you are certain there are no user name conflicts between your partitions, you can use `oTExternalID1`. Otherwise, use `oTExternalID3` or `oTExternalID4`, depending on the desired format.

See “[User partitions](#)” on page 65 for a description of `oTExternalID14` and other user attributes.

You cannot specify a compound mapping for the `__NAME__` attribute. A simple mapping is required to do reverse lookups in Directory Services. Authentication requires reverse-lookup of a user name, from the name in the resource to the actual user object in your database. Because OTDS cannot perform the reverse lookup if the account name is a compound value, user names in the resource must not be computed as a compound mapping.

For more information about the `__NAME__` attribute mapping, see [“`\_\_NAME\_\_`” on page 202](#).

### Content Web Services supported resource attribute mappings

Content Web Services supports mapping a limited number of resource user attributes. For more information, see “[Resource user attribute mappings supported by Content Web Services](#)” on page 203.

### 5.3.1.3.1 OTDS resource Format options

When creating or editing a synchronized resource in OTDS, you have the option of creating user and group attribute mappings between OTDS and your synchronized resource. You can also customize the format of these mappings as follows:

Format	Description
%l	Format the string as lowercase.
%s	Maintain the string as entered.
%u	Format the string as uppercase.
%v	Use this format option with values that are DN's in order to translate to the user name or group name of the target DN.

In general, you can use the Java Formatter syntax in addition to the specific options listed in the table. For more information, see the “Java Formatter” reference in “References to external websites” on page 385.

### 5.3.1.3.2 Support for javascript and multi-valued javascript in the Format column

The **Format** column supports a one-to-one mapping of OTDS to resource attribute mapping when using %js. Each OTDS attribute value is converted, using the formatting specified in the **Format** column, into a value to be passed to the resource.

The **Format** column also supports the use of %mvjs in order to be able to converge multiple OTDS attribute values into a single resource attribute value.

#### javascript (%js)

Javascript is supported in the form “%js:<javascript>”. When using %js, the javascript is invoked once for each attribute value.

#### multi-valued javascript (%mvjs)

Multi-valued javascript is supported in the form “%mvjs:<javascript>”. When using %mvjs, the javascript is invoked once, with all OTDS attribute values passed to the script as an array of values. The expected return value of %mvjs is either:

- An array of attribute values corresponding to the OTDS attribute values.
- A single string value. This is suitable when the resource expects a single attribute value. For example, for either the **SecurityClearanceLevel** attribute or the **GroupID** attribute on OpenText Content Management.

<javascript> is one of:

- A URI to a file containing javascript. For example, “file:/c:/temp/myjavascript.js”.
- The javascript code, itself.

The javascript must be a function called “format”. The parameters are the values of the OTDS attributes.

Examples showing four options for javascript in the **Format** column:

➡ **Example 5-1: An example showing a javascript file referenced in the Format column**

This option references a URI to a file. If, for example, you have the following mapping in OTDS:

- In the **Resource Attribute** text box: \_\_NAME\_\_
- In the **OTDS Attribute(s)** text box: cn,oTExtraAttr6
- In the **Format** text box, type one of:
  - %js:file:/c:/temp/eFileNameConversion.js
  - %mvjs:file:/c:/temp/eFileNameConversion.js

You now need a file called eFileNameConversion.js located in the C:\temp directory. For the purposes of this example and [Example 5-2, “An example showing javascript directly in the Format column” on page 184](#), consider the following as the content of the C:\temp\eFileNameConversion.js file:

```
function format(name, type)
{
    if (type == "1")  return "wg_"+name;
    else if (type == "2") return "ag_"+name;
    else return name";
}
```

➡ **Example 5-2: An example showing javascript directly in the Format column**

The second option is to place the javascript in the **Format** column directly. Drawing from [Example 5-1, “An example showing a javascript file referenced in the Format column” on page 184](#), type one of the following in the **Format** column:

```
%js:function format(name, type){ if (type == "1")  return "wg_"+name; else if (type ==
"2") return "ag_"+name; else return name";}

%mvjs:function format(name, type){ if (type == "1")  return "wg_"+name; else if (type ==
"2") return "ag_"+name; else return name";}
```

➡ **Example 5-3: An example showing a javascript file referenced in the Format column to implement a mapping for display language**

This example shows one way to implement a mapping for a user's preferred language as described in [DisplayLanguage on page 200](#). This example references a URI to a file. If, for example, you have the following mapping in OTDS:

- In the **Resource Attribute** text box: DisplayLanguage
- In the **OTDS Attribute(s)** text box: PreferredLanguage
- In the **Format** text box, type one of the following:

- %js:file:/c:/temp/DisplayLanguageFile.js
- %mvjs:file:/c:/temp/DisplayLanguageFile.js

You now need a file called `DisplayLanguageFile.js` located in the `C:\temp` directory. This file must provide all information required to translate all possible values for the language attribute in OTDS to the OpenText Content Management language code. It must also provide the desired, default language. If all language packs are installed, consider the following as the content of the `C:\temp\DisplayLanguageFile.js` file:

```
function format(lang) {
    /* CS cannot handle a blank value so always return the desired default */
    if (!lang) return "_en_US";
    lang=lang.toLowerCase().trim();
    if (lang.indexOf("ar")>=0) {
        return "_ar";
    } else if (lang.indexOf("ca")>=0) {
        return "_ca_ES";
    } else if (lang.indexOf("de")>=0) {
        return "_de";
    } else if (lang.indexOf("en")>=0) {
        return "_en_US";
    } else if (lang.indexOf("es")>=0) {
        return "_es";
    } else if (lang.indexOf("fi")>=0) {
        return "_fi_FI";
    } else if (lang.indexOf("fr")>=0) {
        return "_fr";
    } else if (lang.indexOf("it")>=0) {
        return "_it";
    } else if (lang.indexOf("iw")>=0) {
        return "_iw";
    } else if (lang.indexOf("ja")>=0) {
        return "_ja";
    } else if (lang.indexOf("kk")>=0) {
        return "_kk_KZ";
    } else if (lang.indexOf("ko")>=0) {
        return "_ko_KR";
    } else if (lang.indexOf("nl")>=0) {
        return "_nl";
    } else if (lang.indexOf("pl")>=0) {
        return "_pl_PL";
    } else if (lang.indexOf("pt")>=0) {
        return "_pt";
    } else if (lang.indexOf("ru")>=0) {
        return "_ru_RU";
    } else if (lang.indexOf("sv")>=0) {
        return "_sv";
    } else if (lang.indexOf("zh")>=0) {
        if (lang.indexOf("tw")>=0 || lang.indexOf("hk")>=0) {
            return "_zh_TW";
        }
        return "_zh_CN";
    } else if (lang.indexOf("uk")>=0) {
        return "_uk_UA";
    }
    return "_en_US";
}
```

You need to modify the text above to remove any conditions for language packs that are not installed on your system.



▶ **Example 5-4: An example showing javascript directly in the Format column to implement a mapping for gender**

This example shows one way to implement a mapping for a user's gender as described in [Gender on page 201](#). This example places the javascript in the **Format** column directly, and can be used if the gender attribute accepts either "m" or "f" in OTDS. You would need to adapt this javascript for other cases.

You have the following mapping in OTDS:

- In the **Resource Attribute** text box: gender
- In the **OTDS Attribute(s)** text box: Gender
- In the **Format** text box, type one of the following:

```
- %js:function format(gender) {  
    if ("m".equals(gender)) {  
        return 0;  
    } else if ("f".equals(gender)) {  
        return 1;  
    }  
    return null;  
}  
  
- %mvjs:function format(gender) {  
    if ("m".equals(gender)) {  
        return 0;  
    } else if ("f".equals(gender)) {  
        return 1;  
    }  
    return null;  
}
```



#### 5.3.1.3.3 Examples using resource attribute mappings to create groups

You can also use resource attribute mappings to automatically create groups in your resource based on attributes of the users.

The following examples walk you through some common scenarios. To access the **Add User Attribute to Mapping** dialog box referenced in these examples, do the following:

1. From the web administration menu, click **Resources**.
2. From the **Actions** menu associated with the synchronized resource you want to edit, click **Properties**.
3. Click the **User Attribute Mappings** tab.
4. On the **User Attribute Mappings** page, click **Add User Attribute to Mappings**.

▶ **Example 5-5: If a user has a Type=contractor, you can automatically create a group called Group Employeetype Contractor**

You do this by adding a user attribute mapping from your Directory Services attribute to your resource. In the **Add User Attribute to Mapping** dialog box, do the following:

1. In the **Resource Attribute** text box, type: \_\_GROUP\_\_
2. In the **OTDS Attribute(s)** text box, type: type
3. In the **Format** text box, type: Employeetype %s
4. Click **Save**.



► **Example 5-6: You can also create groups for each department using a user attribute mapping**

The group name in the resource will be taken from the department number in Directory Services.

1. In the **Resource attribute** text box, type: \_\_GROUP\_\_
2. In the **OTDS Attribute(s)** text box, type: oTDepartment
3. In the **Format** text box, type: %s
4. Click **Save**.



► **Example 5-7: If you add “department” to the format and a user has oTDepartment=Finance, then that user will be added to the Finance department resource group using the following mapping:**

1. In the **Resource Attribute** text box, type: \_\_GROUP\_\_
2. In the **OTDS Attribute(s)** text box, type: oTDepartment
3. In the **Format** text box, type: %s department
4. Click **Save**.



► **Example 5-8: You can also specify multiple source attributes**

Multiple source attributes should each have a %s in the format. If you have a user with the following attribute values:

- firstName=Fred
- surname=Smith
- title=Mr

Then using the following mapping, the value for Fred's displayName in the resource will be "Mr. Fred Smith".

1. In the **Resource Attribute** text box, type: displayName
2. In the **OTDS Attribute(s)** text box, type: title,firstName,surname
3. In the **Format** text box, type: %s . %s %s

4. Click **Save**.



#### 5.3.1.4 Connection parameters

If, when creating your resource, you selected **User and group synchronization**, you may be required to enter connection parameters. In that case, you will see the **Connection Information** page. The following tables detail the connection parameters required for each of the following:

- “Connection parameters for Archive Center resources” on page 188
- “Connection parameters for OpenText Content Management resources” on page 194: note that this table is found in the “Configuring a synchronized resource for OpenText Content Management” on page 193 section.
- “Connection parameters for eDocs DM resources” on page 189
- “Connection parameters for Enterprise Process Services resources” on page 206: note that this table is found in the “Configuring a synchronized resource for Enterprise Process Services” on page 205 section.
- “Connection parameters for MBPM resources” on page 189
- “Connection parameters for OpenText Media Management resources” on page 189
- “Connection parameters for Process Component Library resources” on page 190
- “Connection parameters for REST (Generic) resources” on page 190
- “Connection parameters for Service Center resources” on page 190
- “Connection parameters for WSM Delivery Server resources” on page 191
- “Connection parameters for WSM Management Server resources” on page 192

##### 5.3.1.4.1 Connection parameters for Archive Center resources

**Table 5-1: Archive Center connection parameters**

Connection Parameter Name	Description
<b>Base URL</b>	The URL Endpoint for user/group provisioning REST API.
<b>User Name</b>	The name of the user who performs user and group synchronization.
<b>Password</b>	The password for the user who performs user and group synchronization.

#### 5.3.1.4.2 Connection parameters for eDocs DM resources

**Table 5-2: eDocs DM connection parameters**

Connection Parameter Name	Description
eDOCS Server Name	The host name of the server that hosts eDOCS.
eDOCS Server Port	The eDOCS port. If the connection protocol is http, the default value is 8080.
Library	The eDOCS library name.
Username	The name of a user who has administrative privileges for connecting to the eDOCS library.
Password	The password for the user with administrative privileges for connecting to the eDOCS library.

#### 5.3.1.4.3 Connection parameters for MBPM resources

**Table 5-3: MBPM connection parameters**

Connection Parameter Name	Description
MBPM Database URL	MBPM Database URL, the JDBC connection for Oracle or SQL Server.
Enable MBPM Process Synchronization	If you select "True", this will synchronize extra, optional attributes with the MBPM database.

#### 5.3.1.4.4 Connection parameters for OpenText Media Management resources

**Table 5-4: Media Management connection parameters**

Connection Parameter Name	Description
Media Management URL	The URL for the Media Management web service. Use the fully qualified host name.
User name of Administrator	The name of a user who has administrative privileges for connecting to Media Management.
Password of Administrator	The password for the user with administrative privileges for connecting to Media Management.

#### 5.3.1.4.5 Connection parameters for Process Component Library resources

**Table 5-5: PCL connection parameters**

Connection Parameter Name	Description
OpenText Cordys URL	The URL for the OpenText Cordys Server web service. Use the fully qualified host name with the port number. For example: <code>http://mymachine.opentext.net:305</code>
User Name	The name of a user who has administrative privileges for connecting to the Cordys Server.
Password	The password for the user with administrative privileges for connecting to the Cordys Server.
Organization Name	The organization name in Cordys in which users must be created. The default value is <code>system</code> .
Cordys ResourceID	The resource ID of Cordys push connector.

#### 5.3.1.4.6 Connection parameters for REST (Generic) resources

**Table 5-6: REST (Generic) connection parameters**

Connection Parameter Name	Description
Base URL	The URL Endpoint for user or group provisioning REST API. Use the fully qualified host name with the port number. For example: <code>http://mymachine.opentext.net:305</code>
User Name	The name of a user who has administrative privileges.
Password	The password for the user with administrative privileges.

#### 5.3.1.4.7 Connection parameters for Service Center resources

**Table 5-7: Service Center connection parameters**

Connection Parameter Name	Description
OpenText Cordys URL	The URL for the OpenText Cordys Server web service. Use the fully qualified host name with the port number. For example: <code>http://mymachine.opentext.net:305</code>
User Name	The name of a user who has administrative privileges for connecting to the Cordys Server.
Password	The password for the user with administrative privileges for connecting to the Cordys Server.
Organization Name	The organization name in Cordys in which users must be created. The default value is <code>system</code> .

#### 5.3.1.4.8 Connection parameters for SCIM 2.0

**Table 5-8: SCIM 2.0 connection parameters**

Connection Parameter Name	Description
<b>Base URL</b>	The base URL of the SCIM web service. OpenText recommends that you use the fully qualified host name.
<b>Username</b>	If you are using basic authentication, this is the name of a user with administrative privileges
<b>Password</b>	If you are using basic authentication, this is the password for the user with administrative privileges.
<b>OAuth Token URL</b>	If you are using OAuth2 client credentials authentication, this is the OAuth Token Endpoint.
<b>Client ID</b>	If you are using OAuth2 client credentials authentication, this is the OAuth Client ID.
<b>Client Secret</b>	If you are using OAuth2 client credentials authentication, this is the OAuth Client Secret.

#### 5.3.1.4.9 Connection parameters for WSM Delivery Server resources

**Table 5-9: WSM Delivery Server connection parameters**

Connection Parameter Name	Description
<b>Web service URL</b>	The URL of the Delivery Server “UserService” web service. This web service is used to create, update, and delete users and groups. OpenText recommends that you use the fully qualified host name.
<b>User name</b>	The name of a Delivery Server user who has the “developer” role assigned.
<b>Shared key</b>	An arbitrary, shared key to handle the single sign-on connection between OTDS and Delivery Server. For synchronized resources, you must enter the shared key in the <b>Shared Key</b> text box of the OTDS authentication connector in Delivery Server later.

#### 5.3.1.4.10 Connection parameters for WSM Management Server resources

**Table 5-10: WSM Management Server connection parameters**

Connection Parameter Name	Description
<b>RQL Web service URL</b>	The URL of the Management Server web service. This web service is used to create, update, and delete users and groups. OpenText recommends that you use the fully qualified host name.
<b>User name</b>	The name of a Management Server user who has the Server Manager module assigned. This user is required to create and edit users and groups in Management Server.
<b>Password</b>	The password of the Management Server user.
<b>Language of user interface</b>	Select the language in which the user will work in Management Server. Users can change this setting later.
<b>Locale</b>	Select a locale that will determine the date format.
<b>Projects</b>	<p>Enter one or more projects that you want to assign to users in Management Server. Each project must be separated by a semi-colon. By default, users get the “Author” role assigned for these projects.</p> <p>To assign a specific role to a project, you add the role abbreviation, separated by a comma. For example: xample, Ad;wsgpp,Ed;intranet</p> <p>You can use the following role abbreviations. In brackets, you find the modules and options that are assigned to each role by default:</p> <ul style="list-style-type: none"> <li>• <b>Ad:</b> Administrator (assets, smartedit, smarttree, templateeditor, translation, publication, project settings).</li> <li>• <b>Si:</b> Site Builder (assets, smartedit, smarttree, templateeditor, translation, publication, project settings).</li> <li>• <b>Ed:</b> Editor (assets, smartedit).</li> <li>• <b>Au:</b> Author (assets, smartedit).</li> <li>• <b>Vi:</b> Visitor (smartedit).</li> </ul> <p>If you choose not to specify a project, no user groups are created in Management Server because user groups are project-specific.</p>

Connection Parameter Name	Description
<b>Additional modules</b>	<p>Type any additional modules that are enabled and assigned to users. This is a list of modules in addition to those automatically assigned to users based on the selected user level and user role.</p> <p>Type one or more modules that you want to assign to users in Management Server. Modules must be separated by semicolon. For example: templateeditor;translation</p> <p>Modules might be:</p> <ul style="list-style-type: none"> <li>• assets</li> <li>• servermanager</li> <li>• smartedit</li> <li>• smarttree</li> <li>• templateeditor</li> <li>• translation</li> </ul>
<b>Create groups</b>	Set to "True" to create user groups in the Management Server repository.

### 5.3.1.5 Configuring a synchronized resource for OpenText Content Management

**!** **Important**

You must install Content Web Services before creating a synchronized resource for OpenText Content Management. For more information on installing Content Web Services, see *OpenText Content Management - Installation Guide (LLESCOR-IGD)*.

**To configure a synchronized resource for OpenText Content Management:**

1. Create a synchronized resource for OpenText Content Management. See “[Creating a synchronized resource](#)” on page 206.
2. Configure access roles for this resource. See “[Configuring access to your OpenText Content Management resource](#)” on page 218.
3. Complete the authentication activation process for this resource with the administrative interface of OpenText Content Management. You will use Directory Services Integration Administration to connect your Directory Services resource to your OpenText Content Management. See “[Configuring Directory Services integration administration in OpenText Content Management](#)” on page 219.



**Tip:** If your Directory Services server is part of a cluster using a load balancer, supply the fully-qualified domain name of the load balancer as your Directory Services server.

### 5.3.1.5.1 Connection parameters for OpenText Content Management resources

This section defines the connection parameter options that you need to enter in the **Advanced Connection Information** page of the resource creation assistant when you are creating a synchronized resource for OpenText Content Management. The connection parameters are required for Directory Services to communicate with OpenText Content Management:

Connection Parameter Name	Description
<b>Member Service WSDL</b>	<p>The server, port and web service on which Content Web Services is installed.</p> <p>The default if you are using Tomcat is <code>http://&lt;server-name&gt;:8080/cws/services/MemberService?wsdl</code></p> <p>The default if you are using MS IIS is <code>http://&lt;server-name&gt;/cws/MemberService.svc?wsdl</code></p> <p>Do not use localhost.</p>
<b>Security Clearance WSDL</b>	<p>The server, port and web service on which Security Clearance Web Services is installed.</p> <p>The default if you are using Tomcat is <code>http://&lt;otds-server-name&gt;:8080/cs-services-rmsecmanagement/services/RMSecManagement?wsdl</code></p> <p>The default if you are using MS IIS is <code>http://&lt;otds-server-name&gt;/cs-services-rmsecmanagement/RMSecManagement.svc?wsdl</code></p> <p>Do not use localhost.</p>
<b>Authentication Service WSDL</b>	<p>The server, port, and authentication service of the server on which Directory Services is installed.</p> <p>The default if you are using Tomcat is <code>http://&lt;server-name&gt;:8080/cws/services/Authentication?wsdl</code></p> <p>The default if you are using MS IIS is: <code>http://&lt;server-name&gt;/cws/Authentication.svc?wsdl</code></p> <p>Do not use localhost.</p>

Connection Parameter Name	Description
<b>REST API URL</b>	<p>The URL to OpenText Content Management's REST API. The push connector will use the REST API when necessary, for example if Content Web Services URLs are not provided, or if any of the personal attributes of the user are mapped. This text box can be used to synchronize any one of the personal user attributes detailed in <a href="#">"User attribute mappings supported by REST API" on page 198</a>.</p> <p>The default is <code>http://&lt;server-name&gt;/&lt;OpenText Content Management_service_name&gt;/cs.exe/api</code></p> <p> 1. The REST API or Content Web Services URLs are not mandatory, but one or the other must be provided. The following conditions apply:</p> <ul style="list-style-type: none"> <li>• Content Web Services is required to synchronize users to OpenText Content Management domains.</li> <li>• Content Web Services is required to synchronize external, for example Tempo, users and groups.</li> <li>• The REST API is required to synchronize user's Photo, Manager, or any of the personal attributes detailed in <a href="#">"User attribute mappings supported by REST API" on page 198</a>.</li> </ul>
<b>User name</b>	<p>The account you choose must have add privilege and delete privilege for both users and groups in OpenText Content Management. The OpenText Content Management administrator account has the required privileges.</p>
<b>Password</b>	<p>The password must correspond to the user name that you supply in the <b>User name</b> field.</p> <p>This field is not required if you have set <b>Impersonate</b> to "True".</p>
<b>Impersonate</b>	<p>If you set this parameter to "True", OTDS will impersonate the synchronization account you typed in <b>User name</b>. Provided OpenText Content Management uses this OTDS for authentication, this option avoids the need to store and maintain the synchronization account password in OTDS.</p> <p>If this parameter is set to "False", the synchronization account will be required to explicitly authenticate with OpenText Content Management, and OTDS will store and maintain the synchronization account password.</p>

Connection Parameter Name	Description
<b>Default group</b>	<p>The default group for users that Directory Services should set as a user's department when the department is not otherwise specified by the GroupID attribute mapping. This is a OpenText Content Management value and should not be confused with a Directory Services group.</p> <p>The default value is <code>__DEFAULT__</code> and is always treated as group ID 1001.</p> <p>You can optionally set this value to <code>__DOMAIN__</code> if you want to set the default group to the same name as the domain when using OpenText Content Management domain mappings.</p>
<b>External users default group</b>	<p>The default group for external users. See the description for <b>Default group</b> above.</p> <p> <b>Note:</b> External Users are, in general, created by Tempo products. This setting is used to set the default group for such users, and should not be changed. This setting corresponds with the value expected by Tempo products.</p>
<b>Default permission mask</b>	<p>The default OpenText Content Management permission mask. This is a OpenText Content Management value and does not apply to a Directory Services group.</p>
<b>Disable deleted users</b>	<p>Set this parameter to "True" when you want to remove the sign in enabled privilege from users deleted by OTDS, instead of deleting them.</p> <p>Set this parameter to "False" in order to flag users as deleted in OpenText Content Management. Deleted accounts cannot be undeleted.</p>

Connection Parameter Name	Description
<b>Domain Mappings</b>	<p>This option requires that domain support be enabled in OpenText Content Management. It specifies XML-formatted mappings of OTDS partitions to OpenText Content Management domains.</p> <p>The format is:</p> <pre data-bbox="796 551 1078 868">&lt;Mappings&gt; &lt;M&gt;   &lt;P&gt;Partition Name 1&lt;/P&gt;   &lt;D&gt;CS Domain X&lt;/D&gt; &lt;/M&gt; &lt;M&gt;   &lt;P&gt;Partition Name 2&lt;/P&gt;   &lt;D&gt;CS Domain Y&lt;/D&gt; &lt;/M&gt; &lt;M&gt;   &lt;P&gt;Partition Name 3&lt;/P&gt;   &lt;D&gt;CS Domain X&lt;/D&gt; &lt;/M&gt; &lt;/Mappings&gt;</pre> <p>Type the symbol for ditto " " for the CS domain if you want to use the same name as the partition name:</p> <pre data-bbox="796 973 1078 1100">&lt;Mappings&gt; &lt;M&gt;   &lt;P&gt;Partition Name 1&lt;/P&gt;   &lt;D&gt;"&lt;/D&gt; &lt;/M&gt; &lt;/Mappings&gt;</pre> <p>You can specify a URL to an XML file that contains the domain mappings: <code>file:///c:/OTDS_Files/domain_mappings.xml</code></p> <p>Multiple OTDS partitions can be mapped to the same OpenText Content Management domain. Leave this parameter empty if you are not using OpenText Content Management Domains.</p>

Connection Parameter Name	Description
<b>Department Mappings</b>	<p>Previously, the CSDS department mappings feature allowed an administrator to map the AD/LDAP department attribute to the corresponding OpenText Content Management group that will be set as a user's department in OpenText Content Management.</p> <p>This attribute allows the administrator to map the department attribute from the synchronized resource to the department of the user in OpenText Content Management.</p> <p>The format is:</p> <pre>&lt;Mappings&gt; &lt;M&gt; &lt;OTDS&gt;OTDS department 1&lt;/OTDS&gt; &lt;CS&gt;Resource department X&lt;/CS&gt; &lt;/M&gt; &lt;M&gt; &lt;OTDS&gt;OTDS department 2&lt;/OTDS&gt; &lt;CS&gt;Resource department Y&lt;/CS&gt; &lt;/M&gt; &lt;/Mappings&gt;</pre> <p>If there is no mapping for a given user's OTDS department, OTDS will keep the department value unaltered. If, instead, you want OTDS to assign a default value, specify the default value in a <code>&lt;Default&gt;</code> tag under <code>&lt;Mappings&gt;</code> in the form:</p> <pre>&lt;Mappings&gt; &lt;Default&gt;MyDefaultGroup&lt;/Default&gt; &lt;/Mappings&gt;</pre> <p>You can specify a URL to an XML file that contains the department mappings: <code>file:///c:/OTDS_Files/department_mappings.xml</code></p>

## User attribute mappings supported by REST API

The personal user attribute mappings detailed in this section are supported and synchronized by the **REST API URL** as detailed in “[Connection parameters for OpenText Content Management resources](#)” on page 194.

Personal User Attribute	Description
Photo	The user's profile photo. For more information, see <a href="#">Photo on page 199</a> .
Manager	The user's manager. For more information, see <a href="#">Manager on page 199</a> .
PersonalEmail	The user's personal email address.
PersonalInterests	The user's personal interests.
PersonalWebsite	The user's personal website.
PersonalUrl1	The user's personal URL 1.

Personal User Attribute	Description
PersonalUrl2	The user's personal URL 2.
PersonalUrl3	The user's personal URL 3.
CellPhone	The user's cell phone number.
Pager	The user's pager number.
DisplayLanguage	The user's preferred, displayed language. The language pack must be installed on OpenText Content Management. For more information, see <a href="#">DisplayLanguage on page 200</a> .
HomeAddress1	The user's home address 1.
HomeAddress2	The user's home address 2.
HomePhone	The user's home phone number.
HomeFax	The user's home fax number.
BirthDate	The user's birth date.
Gender	The user's gender. For more information, see <a href="#">Gender on page 201</a> .

### Photo

This optional user attribute mapping needs to be created by the administrator. It allows you to map a OpenText Content Management photo attribute to either a JPEG photo or a photo in OTDS, pushed from the synchronized partition.

In addition to creating the mapping for the **Photo** user attribute in OTDS, you will also need to edit the **REST API URL** text box. For more information, see the **REST API URL** information in [“Connection parameters for OpenText Content Management resources” on page 194](#).

To map this photo in OTDS, do the following:

1. In OTDS, in **Resources**, from your OpenText Content Management's **Actions** menu, click **Properties**.
2. On the **Connection Information** page, in the **REST API URL** parameter, type:  

```
http://<fully_qualified_server_name>/<OpenText Content Management_service_name>/cs.exe/api
```
3. On the **User Attribute Mappings** page, click the **Add Attribute to Mappings** button and then enter the following values:
  - In the **Resource Attribute** text box type: Photo
  - In the **OTDS Attribute(s)** text box type one of: photo / jpegPhoto
  - In the **Format** text box type: %s

### Manager

This optional user attribute mapping needs to be created by the administrator. It allows you to map a OpenText Content Management manager attribute to the

OTDS attribute “manager”, which is a DN of a user in OTDS. In a synchronized user partition, this user attribute mapping is typically synchronized from AD/LDAP.

In addition to creating the mapping for the **Manager** user attribute in OTDS, you will also need to edit the **REST API URL** text box. For more information, see the **REST API URL** information in [“Connection parameters for OpenText Content Management resources” on page 194](#).

To map the manager attribute in OTDS, do the following:

1. In OTDS, in **Resources**, from your OpenText Content Management's **Actions** menu, click **Properties**.
2. On the **Connection Information** page, in the **REST API URL** parameter, type:  

`http://<fully_qualified_server_name>/<OpenText_Content_Management_service_name>/cs.exe/api`
3. On the **User Attribute Mappings** page, click the **Add Attribute to Mappings** button and then enter the following values:
  - In the **Resource Attribute** text box type: Manager
  - In the **OTDS Attribute(s)** text box type: manager
  - In the **Format** text box type: %v

### DisplayLanguage

This optional user attribute mapping needs to be created by the administrator. It allows you to set the user's **PreferredLanguage** setting in OpenText Content Management.

In addition to creating the mapping for the **DisplayLanguage** user attribute in OTDS, you will also need to edit the **REST API URL** text box. For more information, see the **REST API URL** information in [“Connection parameters for OpenText Content Management resources” on page 194](#).

To map this language in OTDS, do the following:

1. In OTDS, in **Resources**, from your OpenText Content Management's **Actions** menu, click **Properties**.
2. On the **Connection Information** page, in the **REST API URL** parameter, type:  

`http://<fully_qualified_server_name>/<OpenText_Content_Management_service_name>/cs.exe/api`
3. On the **User Attribute Mappings** page, click the **Add Attribute to Mappings** button and then enter the following values:
  - In the **Resource Attribute** text box type: DisplayLanguage
  - In the **OTDS Attribute(s)** text box type: PreferredLanguage
  - In the **Format** text box, you need to use the javascript formatting feature in OTDS. For more information, see [“Support for javascript and multi-valued javascript in the Format column” on page 183](#) and [Example 5-3, “An example showing a javascript file referenced in the Format column to implement a mapping for display language” on page 184](#).

### Gender

This optional user attribute mapping needs to be created by the administrator. It allows you to set the user's **Gender** setting in OpenText Content Management.

In addition to creating the mapping for the **Gender** user attribute in OTDS, you will also need to edit the **REST API URL** parameter. For more information, see the **REST API URL** information in “[Connection parameters for OpenText Content Management resources](#)” on page 194.

To map this gender in OTDS, do the following:

1. In OTDS, in **Resources**, from your OpenText Content Management's **Actions** menu, click **Properties**.
2. On the **Connection Information** page, in the **REST API URL** text box, type:

```
http://<fully_qualified_server_name>/<OpenText Content Management_service_name>/cs.exe/api
```

3. On the **User Attribute Mappings** page, click the **Add Attribute to Mappings** button and then enter the following values:

- In the **Resource Attribute** text box type: gender
- In the **OTDS Attribute(s)** text box type: Gender
- In the **Format** text box, you need to use the javascript formatting feature in OTDS. For more information, see “[Support for javascript and multi-valued javascript in the Format column](#)” on page 183 and [Example 5-4, “An example showing javascript directly in the Format column to implement a mapping for gender”](#) on page 186.

#### 5.3.1.5.2 Default OpenText Content Management user and group attribute mappings

OpenText Content Management Attribute	OTDS User Attribute	OTDS Group Attribute
MiddleName	initials	
MailAddress	mail	
Title	title	
Phone	oTTelephoneNumber	
LastName	sn	
OfficeLocation	l	
<u>_NAME_</u> See <a href="#">_NAME_ on page 202</a> below.	oTExternalID1	cn
GroupID See <a href="#">GroupID on page 202</a> below.	oTDepartment	
Type	oTType	oTType

OpenText Content Management Attribute	OTDS User Attribute	OTDS Group Attribute
Fax	oTFacsimileTelephoneNumber	
FirstName	givenName	
AccountDisabled	ds-pwp-account-disabled	

### NAME

You can set whether to preserve the case of user and group names being pushed to OpenText Content Management or whether to set them to either lower or upper case. You can set user name case sensitivity on the **User Attribute Mappings** page. You can set group name case sensitivity on the **Group Attribute Mappings** page.

In the **Format** text box:

- To preserve case, leave the default setting, "%s".
- To set lower case, type: %l
- To set upper case, type: %u
- If values are DNs, type: %v to translate to the user name or group name of the target DN.

For more information, see “[Using resource attribute mappings](#)” on page 182.



**Note:** If you want to manage users through the OpenText Content Management user interface instead of the OTDS administration UI, set the [Disable Resource Name Formatting](#) on page 293 and [Disable Resource Name Mapping](#) on page 293 system attributes to “true” on the **OpenText Content Management Members** partition when the OpenText Content Management resource is using a non-default NAME attribute mapping.

### **GroupID**

The default mapping between the OpenText Content Management attribute **GroupID** and the OTDS attribute **oTDepartment** defines the user's base group, for example the department, in OpenText Content Management. The user's department in OpenText Content Management is equivalent in concept to a Unix user's primary GID, and, as such, a group must exist in OpenText Content Management to represent this department.

For this reason, you should be aware of the mapping of the OTDS attribute **oTDepartment** in your synchronized user partition's user attribute mappings, and realize that a group will be created in OpenText Content Management to represent the user's department.

If you remove the default mapping between the OpenText Content Management attribute **GroupID** and the OTDS attribute **oTDepartment**, users will be created in the OpenText Content Management Default Group.

### 5.3.1.5.3 Resource user attribute mappings supported by Content Web Services

Content Web Services supports mapping a limited number of the resource user attributes. The following table lists the resource user attributes that Content Web Services supports mapping:

Attribute	Meaning
FirstName	First Name
MiddleName	Middle Name
LastName	Last Name
Phone	Phone Number
Fax	Fax Number
GroupID	Department
Title	Job Title
MailAddress	Email Address
OfficeLocation	Office Location
TimeZone	Time Zone
UserPrivileges	Privileges

### 5.3.1.5.4 Configuring Directory Services integration administration

The Directory Services **Configure Integration Settings** page in OpenText Content Management is used to:

- Inform OpenText Content Management about OTDS' location. See [Global Integration Settings on page 204](#).
- Configure how users will authenticate with OpenText Content Management. See [Web Server Authentication on page 203](#).

OpenText Content Management supports Single Sign On (SSO) and authentication services provided by an installation of OTDS.

You can configure the following authentication options:

---

#### Web Server Authentication

You can choose to enable **Web Server Authentication** to retrieve authenticated user information directly from your Web Server. You would enable this option if your Web Server is configured to authenticate users as they access OpenText Content Management URLs. For example, if you are using Microsoft Internet Information Services (IIS), your server may be configured to authenticate users with Integrated Windows Authentication (IWA), in which case IIS will populate the Web Server environment variable `REMOTE_USER` with the account name of the authenticated user. The format of `<username>` can be supplied and configured as detailed below.

### Environment Variable

The **Environment Variable** parameter allows you to choose which variable to use for determining the user name. By default, this will be set to REMOTE\_USER. Other authentication schemes may set **Environment Variable** to a different value, such as Siteminder, which uses the value HTTP\_SM\_USER.

### Username Formatting

The **Username Formatting** area allows you to select how to format the value in the above environment variable.

- **Remove domain name:** this will display the user name only. Choose this option if uniqueness of user names is guaranteed *across all domains* in your Windows domain registry. This is the default selection.
- **Do not format:** this will leave the user name unchanged. Choose this option if uniqueness of user names is guaranteed *only within each domain* in your Windows domain registry.
- **Resolve through OTDS:** the value from REMOTE\_USER is sent to OTDS in order to find the corresponding user name in OpenText Content Management. You must configure OpenText Directory Services. For more information, see *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)* and the **OTDS Release Notes**. You can find links to these documents in “[OTDS Documentation](#)” on page 381.



**Note:** A Web Access Management authentication handler must be configured on OTDS for this option to work. For more information, see the “Web Access Management” authentication handler documented in “[Using authentication handlers](#)” on page 138.

### Username Case Sensitivity

Case sensitivity for the <username> can be configured to preserve case or change case to all lowercase. You may wish to change case to lowercase when you have a case-sensitive database and synchronization is configured to lowercase.

If Web Server authentication is enabled but user information is not available, authentication will try OTDS authentication.

### Global Integration Settings

This area provides OpenText Content Management with the information it needs to access OTDS. Both fields in this area are required fields.

The Admin must first create a OpenText Content Management resource in OTDS. During the process, a unique identifier, called the *resource ID*, is generated. The resource ID and the OpenText Directory Services server URL are required values and must be entered to set up OTDS Authentication in OpenText Content Management. For more information, see *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)* and the **OTDS Release Notes**. You can find links to these documents in “[OTDS Documentation](#)” on page 381.

---

#### Local Integration Settings

The **OTDS Sign In URL** field provides the option to specify a URL to which users are redirected when they sign in. You also have the option of displaying a sign out option for users that authenticate with single sign on.

#### 5.3.1.5.5 Configuring Directory Services with multiple instances of OpenText Content Management

If you want to connect Directory Services to a second installation of OpenText Content Management, you must deploy a second set of Content Web Services on a separate application server. For information about deploying Content Web Services, see *OpenText Content Management - Installation Guide (LLESCOR-IGD)* and OpenText My Support ([https://knowledge.opentext.com/knowledge/cs.dll/fetch/-15106263/15106294/15106295/17990637/62345549/setup\\_Tomcat.html](https://knowledge.opentext.com/knowledge/cs.dll/fetch/-15106263/15106294/15106295/17990637/62345549/setup_Tomcat.html)).

##### To define a resource for the second installation of OpenText Content Management:

1. In the web administration client, click **Resources**, and then create a resource for the second OpenText Content Management using the **New Synchronized Resource** wizard.  
Make sure you enter the fully-qualified domain names for the two WSDL definitions of your second Tomcat instance.
2. On the second OpenText Content Management administration page, complete the **Directory Services Integration Administration**.
3. Add users and groups to the access role for your second OpenText Content Management.

#### 5.3.1.6 Configuring a synchronized resource for Enterprise Process Services

Enterprise Process Services requires that you first create a non-synchronized resource in order to create a resource identifier. This resource identifier is used when installing Enterprise Process Services. You can edit this resource to create a synchronized resource pointing to your newly installed Enterprise Process Services server.

### 5.3.1.6.1 Connection parameters for Enterprise Process Services resources

This section defines the connection parameter options that you need to enter in the **Connection Information** page of the resource creation assistant when you are creating a synchronized resource for Enterprise Process Services. The connection parameters are required for Directory Services to communicate with Enterprise Process Services:

The following parameters describe your connection options when you are creating your resource:

Connection Parameter Name	Description
<b>UMS URL</b>	The fully qualified host name of the User Management Server. If necessary, adjust the port.  In a cluster scenario, enter the URLs for all User Management Server cluster nodes separated by commas. You can use the fully qualified URL to the load balancer of User Management Server. You should always use the fully qualified hostname.
<b>User name</b>	The name of a User Management Server user who has the permission to push users to User Management Server. The default user OTDSConnector is a valid user that has the necessary permission.
<b>User password</b>	The password of the User Management Server user. The password of the OTDSConnector user was set during the installation of User Management Server, in the property <b>Internal users default password</b> .
<b>User domain</b>	The domain of the User Management Server user. The default value, _internal, is the domain of the default OTDSConnector user.
<b>Assoc UID separator</b>	The separator string for the synchronization of the Enterprise Process Services resource. Do not change the default value, __com.opentext.otds.connectors.reserved.string__.

## 5.3.2 Creating a synchronized resource

### To create a synchronized resource:

1. From the web administration menu, click **Resources**.
2. From the button bar, click **Add**. The **New Resource** assistant will guide you through the steps to create a new resource.
3. On the **General** page, do the following:
  - a. In the **Resource name** box, type a descriptive name for this resource. Because a resource can be used by multiple products, you might consider

using the environment and purpose as your resource name. For example, “Production document processing” or “Test billing system”. The name you type here cannot be edited later.

- b. **Optional** In the **Display Name** box, if you want this resource's displayed name to be different than the name you provided in the previous box, the **Resource name** box, type the name you want displayed on the **Resources** page in this box. This box can be edited at a later date.
- c. **Optional** In the **Description** box, type a short description of this resource.



**Note:** The resource identifier will not appear for a **New Resource** creation but will be available for selection when editing an existing resource. See “[Editing a synchronized resource](#)” on page 213 for more information.

- d. From the **Sign in UI Version** list, select which OTDS user interface to display at the OTDS sign in page. To accept the default of the resource, select “default” from the list. For more information, see “[Customizing the sign-in page](#)” on page 354.
- e. **Optional** In the **Sign in UI Style** box, type the full file name with extension of the customized graphic to be applied to the OTDS login page. For example, type “my\_company\_graphic.png”. For more information, see “[Customizing the sign-in page](#)” on page 354.
- f. **Optional** In the **Sign out URL** box, if you want to implement OTDS' single sign out functionality, you must enter a value in this box and the **Sign out Method** box.

Check the documentation for this resource being created for the value to enter in this box. For more information, see “[Single sign out](#)” on page 351.

- g. **Optional** From the **Sign out Method** list, if you want to implement OTDS' single sign out functionality, you must enter a value in this box and the previous box, the **Sign out URL** box.

The value you type to this box is supplied in the documentation for the resource for which this is being created. For more information, see “[Single sign out](#)” on page 351.

- h. Click **Next**.

4. On the **Synchronization** page, do the following:

- a. Select the **User and group synchronization** check box.
- b. From the **Synchronization connector** list, select your preferred connector. One of **Archive Center**, **OpenText Content Management**, **eDocs DM**, **Enterprise Process Services**, **MBPM**, **OpenText Media Management**, **Process Component Library**, **REST (Generic)**, **Service Center**, **WSM Delivery Server**, or **WSM Management Server**. The next pages of the wizard will depend on your choice in this text box.

For more information about user and group synchronization, see “[User and group synchronization](#)” on page 181.

- c. **Optional** In the **This connector will** area, grant rights to allow Directory Services to create and modify users and groups in your connector by selecting any or all of **Create users and groups**, **Modify users and groups** and/or **Delete users and groups** check boxes. For more information, see “[Managing user and group permissions for this resource](#)” on page 181.

 **Tip:** When creating a OpenText Content Management resource, leave the **Delete users and groups** check box cleared to ensure that Directory Services does not delete any OpenText Content Management users or groups.
  - d. Click **Next**.
5. On the **Connection Information** page, do the following:
    - a. Depending on your choice of **Synchronization connector** on the **Synchronization** tab, enter the correct connection information for your connector. Links to the descriptions for each synchronization connector are found in the following list. You also have the option of clicking **Parameters Descriptions** in the web admin UI to open these descriptions.
      - [“Connection parameters for Archive Center resources” on page 188](#)
      - [“Connection parameters for OpenText Content Management resources” on page 194](#)
      - [“Connection parameters for eDocs DM resources” on page 189](#)
      - [“Connection parameters for Enterprise Process Services resources” on page 206](#)
      - [“Connection parameters for MBPM resources” on page 189](#)
      - [“Connection parameters for OpenText Media Management resources” on page 189](#)
      - [“Connection parameters for Process Component Library resources” on page 190](#)
      - [“Connection parameters for REST \(Generic\) resources” on page 190](#)
      - [“Connection parameters for Service Center resources” on page 190](#)
      - [“Connection parameters for WSM Delivery Server resources” on page 191](#)
      - [“Connection parameters for WSM Management Server resources” on page 192](#)
    - b. **Optional** To verify that you have entered your connection information correctly, click **Test Connection**.
    - c. Click **Next**.
  6. On the **User Attribute Mappings** page, do the following:

**!** **Important**

1. Take care when entering values to this page as the information entered here cannot be verified by OTDS.
2. Any user attribute or any group attribute that Directory Services should *not* synchronize to the resource should be removed entirely. Do not simply remove the value from the **OTDS attribute** box, as this can result in the synchronization of an empty, or a default, attribute value.
  - a. Map your Directory Services user attributes to the equivalent user attribute in the resource. For more information about attribute mappings, see “[Using resource attribute mappings](#)” on page 182.

To edit the text boxes in the **Resource Attribute**, **OTDS Attribute(s)** or **Format** columns, click in the cell you want to edit, then type your change. Use the **Format** text box to customize your attribute mapping. For more information, see “[Applying user partition attribute mappings](#)” on page 83.
  - b. **Optional** If you want to add another user attribute, click **Add Attribute to Mappings**. In the three text boxes, do the following:
    - i. In the **Resource Attribute** text box, type the resource attribute name.
    - ii. In the **OTDS Attribute(s)** text box, type the OTDS user attribute name.
    - iii. In the **Format** text box, type the format to be used. For more information, see “[Support for javascript and multi-valued javascript in the Format column](#)” on page 183.
    - iv. Click **Save**.
  - c. **Optional** If you want to delete a user attribute, click the select box to the left of the attribute you want to delete, and then click **Delete Selected**.

**!** **Important**

There is no delete confirmation box. Be cautious when deleting a user attribute mapping.

- d. **Optional** If you want to return to the default mappings, click **Reset to Default**.

By clicking **Reset to Default**, all OTDS user attribute mappings will be reverted to the default settings at installation, and all custom user attribute mappings you have created will be deleted.

- e. Click **Next**.

7. On the **Group Attribute Mappings** page, do the following:

**!** **Important**

1. Take care when entering values to this page as the information entered here cannot be verified by OTDS.
2. Any user attribute or any group attribute that Directory Services should *not* synchronize to the resource should be removed entirely. Do

not simply remove the value from the **OTDS attribute** box, as this can result in the synchronization of an empty, or a default, attribute value.

- a. Map your Directory Services group attributes to the equivalent group attribute in the resource. For more information about attribute mappings, see “[Using resource attribute mappings](#)” on page 182.

To edit the text boxes in the **Resource Attribute**, **OTDS Attribute(s)** or **Format** columns, click in the cell you want to edit, then type your change. Use the **Format** text box to customize your attribute mapping. For more information, see “[Applying user partition attribute mappings](#)” on page 83.
  - b. **Optional** If you want to add another group attribute, click **Add Attribute to Mappings**. In the three text boxes, do the following:
    - i. In the **Resource Attribute** text box, type the resource attribute name.
    - ii. In the **OTDS Attribute(s)** text box, type the OTDS group attribute name.
    - iii. In the **Format** text box, type the format to be used. For more information, see “[Support for javascript and multi-valued javascript in the Format column](#)” on page 183.
    - iv. Click **Save**.
  - c. **Optional** If you want to delete a group attribute, click the select box to the left of the attribute you want to delete, and then click **Delete Selected**.
- !** **Important**  
There is no delete confirmation box. Be cautious when deleting a group attribute mapping.
- d. **Optional** If you want to return to the default mappings, click **Reset to Default**.

By clicking **Reset to Default**, all OTDS group attribute mappings will be reverted to the default settings at installation, and all custom group attribute mappings you have created will be deleted.
  - e. On the button bar, click **Save**.
8. In the **Resource Activation** window:
    - a. Copy the resource identifier to use the resource identifier in the resource's configuration to activate the resource with Directory Services.

**Tip:** You can **Edit** a resource to copy the resource identifier at any time. For more information, see “[Editing a synchronized resource](#)” on page 213.
    - b. **Optional** Click **Verify Activation** to check that the resource has activated with Directory Services.
- !** **Important**  
After your resource has been created, you should configure access roles to allow users with these access roles to sign in to your resource.

A default access role, Access to <Resource name>, is created when you create a resource. The group, otdsadmins@otds.admin, is automatically added to this access role. This allows the user otadmin@otds.admin to access your resource. For more information on configuring access roles, see “[Editing access roles for your resource](#)” on page 225.

- c. Click **OK** to close the **Resource Activation** window.
9. If you created this resource as a synchronized resource for OpenText Content Management, proceed to “[Configuring a synchronized resource for OpenText Content Management](#)” on page 193.

### 5.3.3 Creating a synchronized resource for Enterprise Process Services

#### To create a synchronized resource for Enterprise Process Services:

1. From the web administration menu, click **Resources**, and then select the non-synchronized resource you created for Enterprise Process Services in “[Creating a non-synchronized resource](#)” on page 176. If you have not created a non-synchronized resource, follow the steps in “[Creating a non-synchronized resource](#)” on page 176, and then return to these steps.
2. In the center pane, from the **Actions** menu associated with the non-synchronized resource you created for Enterprise Process Services, click **Properties**.
3. On the **General Information** page, make any changes you want to the general resource properties, and then click the **Synchronization** tab.
4. On the **Synchronization** page, do the following:
  - a. Select the **User and group synchronization** check box.
  - b. From the **Synchronization connector** list, choose **Enterprise Process Services**. For more information about user and group synchronization, see “[User and group synchronization](#)” on page 181.
  - c. In the **This connector will** area, allow Directory Services to create, modify and delete users and groups in Enterprise Process Services by selecting the **Create users and groups**, **Modify users and groups** and **Delete users and groups** check boxes.



**Note:** Users and groups will not be deleted in User Management Server. Instead, their status will be set to disabled. If a user or group with the same name is created again during synchronization of the Enterprise Process Services resource, the status of the existing user or group will be changed to enabled in User Management Server. For more information, see “[Managing user and group permissions for this resource](#)” on page 181.

- d. Click the **Connection Information** tab.

5. On the **Connection Information** page, do the following:
    - a. Enter the connection parameters that are required for Directory Services to communicate with Enterprise Process Services.

 **Tip:** To find out more about the connection parameters required by this resource, see “[Connection parameters for Enterprise Process Services resources](#)” on page 206.
    - b. To verify that you have entered your connection information correctly, click **Test Connection**.
    - c. Click the **User Attribute Mappings** tab.
  6. On the **User Attribute Mappings** page, do the following:
    - a. Map your Directory Services user attributes to the equivalent user attribute in the resource. For more information about attribute mappings, see “[Using resource attribute mappings](#)” on page 182.
    - b. Click the **Group Attribute Mappings** tab.
  7. On the **Group Attribute Mappings** page, do the following:
    - a. Map your Directory Services group attributes to the equivalent group attribute in the resource. For more information about attribute mappings, see “[Using resource attribute mappings](#)” on page 182.
    - b. Click **Save**.
  8. In the **Resource Activation** window, do the following:
    - a. Copy the resource identifier to use the resource identifier in the resource's configuration to activate the resource with Directory Services.
    - b. Optional If you want to check that the resource has activated with Directory Services, click **Verify Activation**.
    - c. Close the **Resource Activation** window.
-  **Important**  
After your resource has been created, you should configure access roles to allow users with those access roles to sign in to your resource. A default access role, **Access to <Resource name>** is created when you create a resource. The group, `otdsadmins@otds.admin` is automatically added to this access role. This allows the user `otadmin@otds.admin` to access your resource. For more information on configuring access roles, see “[Editing access roles for your resource](#)” on page 225.
-  **Tip:** You can **Edit** a resource to copy the resource identifier at any time.
9. Edit the **Access to <your resource>** access role to allow users and groups in the Enterprise Process Services access role to access your User Management Server. For more information, see “[Access Roles](#)” on page 229. These users and groups will be pushed to User Management Server.

They will appear in the web administration client in **Enterprise Process Services > User Management Server > Users and Groups**.

After you change a user, group, or access role in Directory Services, User Management Server will be automatically synchronized. If a user or group is removed from the access role, the user will be disabled in User Management Server.

### 5.3.4 Configuring a synchronized resource

#### To configure a synchronized resource:

1. From the web administration menu, click **Resources**, and then select the synchronized resource you want to configure.
2. In the center pane, from the **Actions** menu associated with the synchronized resource you want to configure, select one of the following:
  - If you want to edit the synchronized resource, click **Properties**, and then follow the instructions found in "[Editing a synchronized resource](#)" on page 213.
  - If you want to view or copy the resource identifier of your synchronized resource, or if you want to verify your activation status, click **Activation Status**.
  - If you want to edit the access roles for this synchronized resource, click **Edit Access Roles**, and then follow the instructions in "[Editing access roles for your resource](#)" on page 225.
  - If you want to edit the impersonation settings for this synchronized resource, click **Impersonation Settings**, and then follow the instructions in "[Editing impersonation settings](#)" on page 225.
  - If you want to turn user synchronization on or off, click **Turn User Synchronization On/Off**, and then follow the instructions in "[Turning user synchronization on or off](#)" on page 226.
  - If you want to consolidate the resource, click **Consolidate**, and then follow the instructions in "[Consolidating a synchronized resource](#)" on page 217.

### 5.3.5 Editing a synchronized resource

#### To edit a synchronized resource:

1. From the web administration menu, click **Resources**, and then select the synchronized resource you want to edit.
2. In the center pane, from the **Actions** menu associated with the synchronized resource you want to edit, click **Properties**.
3. On the **General** page, do the following:
  - a. The **Resource name** box cannot be edited.

- b. In the **Display Name** text box, if you want the name of this resource to display differently from the value located in the **Resource name** text box, type that displayed name here.
  - c. **Optional** In the **Description** text box, you can choose to add or edit a short description of this resource.
  - d. **Optional** If you are going to configure the resource to activate it with Directory Services now, copy the **Resource identifier** to save it to use in the resource's configuration.
  - e. From the **Sign in UI Version** list, you can change which OTDS user interface to display at the OTDS sign in page. To accept the default of the resource, select "default" from the list. For more information, see "["Customizing the sign-in page" on page 354](#)".
  - f. **Optional** In the **Sign in UI Style** text box, you can choose to type the full file name with extension of the customized graphic to be applied to the OTDS sign in page. For example, type "my\_company\_graphic.png". For more information, see "["Customizing the sign-in page" on page 354](#)".
  - g. **Optional** In the **Sign out URL** text box, if you want to implement OTDS' single sign out functionality, you must enter a value in this text box and the next text box.

The value you type in this text box is supplied in the documentation for the resource for which this is being created. For more information, see "["Single sign out" on page 351](#)".
  - h. **Optional** From the **Sign out Method** list, if you want to implement OTDS' single sign out functionality, you must enter a value in this text box and the previous text box.

The value you type to this text box is supplied in the documentation for the resource for which this is being created. For more information, see "["Single sign out" on page 351](#)".
  - i. Click **Save** if you have finished editing your resource, or click **Synchronization** to proceed to the next page.
4. On the **Synchronization** page, do the following:
    - a. The **User and group synchronization** check box is selected because this is a synchronized resource. You can optionally change this resource to a non-synchronized resource by clearing the **User and group synchronization** check box.
    - b. From the **Synchronization connector** list, select your desired connector.

For more information about user and group synchronization, see "["User and group synchronization" on page 181](#)".
    - c. In the **This connector will** area, grant rights to allow Directory Services to create and modify users and groups in your connector. You can select the **Create users and groups**, **Modify users and groups** and/or **Delete users and groups** check boxes.



**Tip:** Leave the **Delete users and groups** check box cleared when creating a OpenText Content Management resource to ensure that Directory Services does not delete any OpenText Content Management users and groups. For more information, see “[Managing user and group permissions for this resource](#)” on page 181.

- d. Click **Save** if you have finished editing your resource, or click **Connection Information** to proceed to the next page.
5. On the **Connection Information** page, do the following:
  - a. You can edit the connection information for your connector. Connection parameters descriptions for each synchronization connector are linked below. You also have the option of clicking **Parameters Descriptions** to open these descriptions.
    - “[Connection parameters for Archive Center resources](#)” on page 188
    - “[Connection parameters for OpenText Content Management resources](#)” on page 194
    - “[Connection parameters for eDocs DM resources](#)” on page 189
    - “[Connection parameters for Enterprise Process Services resources](#)” on page 206
    - “[Connection parameters for MBPM resources](#)” on page 189
    - “[Connection parameters for OpenText Media Management resources](#)” on page 189
    - “[Connection parameters for Process Component Library resources](#)” on page 190
    - “[Connection parameters for REST \(Generic\) resources](#)” on page 190
    - “[Connection parameters for Service Center resources](#)” on page 190
    - “[Connection parameters for WSM Delivery Server resources](#)” on page 191
    - “[Connection parameters for WSM Management Server resources](#)” on page 192
  - b. **Optional** To verify that you have entered your connection information correctly, click **Test Connection**.
  - c. Click **Save** if you have finished editing your resource, or click **User Attribute Mappings** to proceed to the next page.
6. On the **User Attribute Mappings** page, do the following:



### Important

1. Take care when entering values to this page as the information entered here cannot be verified by OTDS.
2. Any user attribute or any group attribute that Directory Services should *not* synchronize to the resource should be removed entirely. Do not simply remove the value from the **OTDS attribute** box, as this can result in the synchronization of an empty, or a default, attribute value.

- a. Map your Directory Services user attributes to the equivalent user attribute in the resource. For more information about attribute mappings, see “[Using resource attribute mappings](#)” on page 182.
- b. Optional If you want to add another user attribute, click **Add Attribute to Mappings**. In the three text boxes, do the following:
  - i. In the **Resource Attribute** text box, type the resource attribute name.
  - ii. In the **OTDS Attribute(s)** text box, type the OTDS user attribute name.
  - iii. In the **Format** text box, type the format to be used.
  - iv. Click **Save**.
- c. Optional If you want to delete a user attribute, click the select box to the left of the attribute you want to delete, and then click **Delete Selected**.

**!** **Important**

There is no delete confirmation box. Be cautious when deleting a user attribute mapping.

- d. Optional If you want to return to the default mappings, click **Reset to Default**.

By clicking **Reset to Default**, all OTDS group attribute mappings will be reverted to the default settings at installation, and all custom group attribute mappings you have created will be deleted.

- e. Click **Save** if you have finished editing your resource, or click **Group Attribute Mappings** to proceed to the next page.

7. On the **Group Attribute Mappings** page, do the following:

**!** **Important**

1. Take care when entering values to this page as the information entered here cannot be verified by OTDS.
  2. Any user attribute or any group attribute that Directory Services should *not* synchronize to the resource should be removed entirely. Do not simply remove the value from the **OTDS attribute** box, as this can result in the synchronization of an empty, or a default, attribute value.
- a. Map your Directory Services group attributes to the equivalent group attribute in the resource. For more information about attribute mappings, see “[Using resource attribute mappings](#)” on page 182.
  - b. Optional If you want to add another group attribute, click **Add Attribute to Mappings**. In the three text boxes, do the following:
    - i. In the **Resource Attribute** text box, type the resource attribute name.
    - ii. In the **OTDS Attribute(s)** text box, type the OTDS group attribute name.
    - iii. In the **Format** text box, type the format to be used.
    - iv. Click **Save**.

- c. **Optional** If you want to delete a group attribute, click the select box to the left of the attribute you want to delete, and then click **Delete Selected**.

**!** **Important**

There is no delete confirmation box. Be cautious when deleting a group attribute mapping.

- d. On the button bar, click **Save**.

### 5.3.6 Consolidating a synchronized resource

#### To consolidate resources:

1. From the web administration menu, click **Resources**, and then select the synchronized resource you want to consolidate.
2. In the center pane, from the **Actions** menu associated with the synchronized resource you want to consolidate, click **Consolidate**.



**Note:** The product or resource may not support the following delete functionality. If the product or resource does not support this delete functionality, an error will be written to the `otds.log` file.

3. In the **Consolidate <resource\_name>** box:
  - a. **Optional** Select **Delete users that are not consolidated** if either of the following is true:
    - If you need to remove users created in the resource by means other than through OTDS.
    - If you need to deal with cases where OTDS could not reach the resource, for whatever reason, in order to delete users when they are deleted in OTDS.
  - b. **Optional** Select **Delete groups that are not consolidated** if either of the following is true:
    - If you need to remove groups created in the resource by means other than through OTDS.
    - If you need to deal with cases where OTDS could not reach the resource, for whatever reason, in order to delete groups when they are deleted in OTDS.
  - c. Click **Consolidate**.

### 5.3.7 Deleting a synchronized resource

**To delete a synchronized resource:**

1. From the web administration menu, click **Resources**.
2. Click the select box to the left of the synchronized resource you want to delete, and then, on the button bar, click **Delete**.



**Note:** Because this is a synchronized resource, any changes to users and groups with access to this resource will not be delivered to the application with which this resource is associated.

3. Confirm that you want to delete this resource by clicking **OK**.

### 5.3.8 OpenText Content Management-specific configuration tasks

There are a number of OpenText Content Management-specific configuration tasks you can choose to perform.

For more information, see:

- *OpenText Content Management - Directory Services Integration Administration Guide (LLESDSI-AGD)*
- *OpenText Content Management - Installation Guide (LLESCOR-IGD)*
- *OpenText Content Management - System Administration Guide (LLESWBA-AGD)*

#### 5.3.8.1 Configuring access to your OpenText Content Management resource

**To configure access to your OpenText Content Management resource:**

1. From the web administration menu, click **Access Roles**.
2. From the **Actions** menu associated with the Access to <Resource name> access role, click **View Access Role Details**. Add any additional users, groups, or organizational units. For more information, see “[Assigning members to an access role](#)” on page 230.



**Note:** The group `otdsadmins@otds.admin` will be automatically added to the access role Access to <Resource name> and will be allowed to administer your OpenText Content Management resource. This means that the user `otadmin@otds.admin` will be automatically pushed to your OpenText Content Management resource when **Directory Services Integration** is configured.

3. Click **Save**.

### 5.3.8.2 Configuring Directory Services integration administration in OpenText Content Management

Sign in to OpenText Content Management as the admin and open the **OpenText Content Management Administration** page.

#### To configure Directory Services integration settings:

1. On the **OpenText Content Management Administration** page, in the **Directory Services Integration Administration** area, click the **Configure Integration Settings** link.

 **Tip:** You can use a shortcut to access this page directly, `https://<fully_qualified_server_name>/<OpenText Content Management_service_name>/cs.exe?func=otdsintegration.settings`.

An example of a URL is: `https://machine1.opentext.com/OTCS/cs.exe?func=otdsintegration.settings`

2. In the **Web Server Authentication** area, do the following:
  - a. **Optional** Select **Enabled** if you want to retrieve authenticated user information directly from your Web Server.
  - b. In the **Environment Variable** box, enter the variable used to validate user credentials or leave the default, `REMOTE_USER`.
  - c. In the **Username Formatting** area, select the option that corresponds to the format of users' login (or sign-in) names in OpenText Content Management:
    - **Remove domain name:** this will display the user name only. This is the default selection.
    - **Do not format:** this will leave the user name unchanged.
    - **Resolve through OTDS:** the value from `REMOTE_USER` is sent to OTDS in order to find the corresponding user name in OpenText Content Management. You must configure OpenText Directory Services. For more information, see *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)*.
  - d. **Note:** A Web Access Management authentication handler must be configured in OTDS in order for this option to work.  
For more information, see the "Web Access Management" authentication handler in "["List of authentication handlers" on page 138](#)".
  - d. In the **Username Case Sensitivity** area, select one of the following:
    - Select **Preserve Case** to preserve the user name when the user signs in to OpenText Content Management.
    - Select **Lowercase** to change the user name to all lowercase letters when the user signs in to OpenText Content Management.

3. In the **Global Integration Settings** area, do the following:
  - a. In the **OTDS Server URL** box, enter the URL of the Directory Services server.  
The URL must include the fully-qualified domain and port number of the Directory Services server. For example, the URL would be one of:
    - `http://<server_name>:<port_number>`
    - `https://<server_name>:<port_number>`

 **Note:** If your Directory Services server has been installed in a cluster, you must enter the fully-qualified domain and port number of the load balancer in the **OTDS Server URL** box.

An example of a valid URL when using a stand-alone, installation of OTDS is: `https://mymachine.opentext.com:8443`
  - b. In the **Resource Identifier** box:
    - Enter the unique ID that was generated when you created a synchronized OpenText Content Management resource in Directory Services.
    - c. You can choose to click **Test Settings** to confirm that the URL entered in the **OTDS Server URL** box is valid.

 **Note:** The connection test does not check whether the **OpenText Directory Server** is configured properly with OpenText Content Management. It only checks that the URL provided in the **OTDS Server URL** box is valid.
4. **Optional** In the **Local Integration Settings** area, do the following:
  - a. In the **OTDS Sign In URL** box, you can choose to specify a URL to redirect users to sign in to OTDS. For an example of the URL convention, see [step 3.a.](#)

 **Note:** You might choose to select this option when OTDS is only accessible to users through an external URL.
  - b. If you want to display a sign-out option for users that are authenticated with single sign on, select **Show log-out option for SSO users**.
5. In the **Web Administrator Password** area, type the OpenText Content Management **Web Administrator Password** in the box provided, and then click **Save**.
6. Next, do the following:
  - a. On the **OpenText Content Management Administration** page, in the **Base Settings - Security Configuration** area, select **Security Parameters**.

- b. On the **Configure Security Parameters** page, in the **Trusted Relationships** area, in the **Referring Websites** box, ensure that the **OTDS Server** name from [step 3.a](#) is listed.



**Tip:** You can optionally select **Include OTDS Server and Sign-in URLs** to direct OpenText Content Management to include these URLs automatically.

- c. Click **Save Changes**.
- d. Restart OpenText Content Management.

### 5.3.8.3 Migrating users and groups from OpenText Content Management 10.5 to Directory Services 25.4.x

If you have OpenText Content Management 10.5 in your existing environment, and you install OpenText Content Management 25.4.x, you can select an option to migrate all OpenText Content Management 10.5 users and groups into the new installation of OTDS.

Following this migration, all existing users and groups in OTDS contained in the **OpenText Content Management Members** partition, and any OpenText Content Management domain partitions, will be replaced with users and groups in the current database.

First follow these steps to access the **User and group migration** page:

1. Sign in to OpenText Content Management as the admin and open the **OpenText Content Management Administration** page.
2. After signing into the **OpenText Content Management Administration** page as the admin, type the following to access the migration page directly, `http://<fully_qualified_server_name>/<OpenText Content Management_service_name>/cs.exe?func=otdsintegration.migrate`

An example of a URL is: `http://machine1.opentext.com/OTCS/cs.exe?func=otdsintegration.migrate`

#### To migrate OTDS data:

1. If you are upgrading your installation of OpenText Content Management, you need to follow these instructions:

During the process of changing your OpenText Content Management database or upgrading your OpenText Content Management installation, you will see the **User and group migration** page.
2. On the **User and group migration** page, in the **OTDS Partition** box, type the name of the OTDS partition that will be used by OpenText Content Management. This is the OTDS partition that stores any users and groups created in OpenText Content Management or migrated from the OpenText Content Management database.



**Note:** The partition name you enter will only be used when users and/or groups are migrated from the OpenText Content Management database, or when users and/or groups are created directly in OpenText Content Management instead of being created through OTDS.

3. In the **Migrate** area, do the following:

- a. If you are upgrading to a stand-alone installation of OTDS, and prior to beginning the migration, you must ensure that the access role has been created in OTDS correctly.

For example, make certain that the “OpenText Content Management Members” partition has been added to the OpenText Content Management access role. You must also ensure that the **Include groups** option has been selected on that OpenText Content Management access role.

- b. If OTDS has never been used with OpenText Content Management, select the **Migrate** box to migrate users and groups from the OpenText Content Management database to OTDS. The **Migrate** option applies to migration of users and groups only.



**Important**

The migration function cannot distinguish users synchronized from OTDS from internal OpenText Content Management users. If you have already synchronized new users and/or groups from OTDS to OpenText Content Management, and you use the migration option, you will end up with duplicate users and groups.

There are three options associated with the **Migrate** option. You can select any of the following:

- i. If you want to migrate internal users and groups, select **Migrate internal users and groups**.

All existing users and groups in OTDS contained in the partition you entered in [step 2](#), and any OpenText Content Management domain partitions will be replaced with users and groups in the current database.

- ii. If you want to migrate external users and groups, select **Migrate (Tempo) external users and groups**. This option relates to the OpenText Tempo product.

All existing users and groups in OTDS contained in the partition you entered in [step 2](#), and any OpenText Content Management domain partitions will be replaced with users and groups in the current database.

- iii. If the migrate option has identified an OpenText Content Management Directory Services module's synchronization sources that you can migrate to OTDS, those synchronization sources will be listed for you to select.



**Note:** The migration function does not migrate CSDS users and groups. It migrates the CSDS sync profile into OTDS, which can then be used to import the same set of users.

If your internal OpenText Content Management groups have synchronized CSDS members, you need to ensure that synchronized users and groups exist in OTDS prior to migrating the internal OpenText Content Management groups into OTDS. You can check to see if any of your OpenText Content Management groups, that are not synchronized by CSDS, contain synchronized CSDS members.

This is necessary so that the migration can find the DN of the synchronized user or group in OTDS in order to create or designate that user or group as a member of the migrated internal group.

Under these circumstances, run the migration to migrate your CSDS synchronized sources only. When all your synchronized users and groups exist in OTDS, you can run the migration tool a second time to migrate the internal users and groups.

4. Type the OpenText Content Management **Web Administrator Password** in the box provided, and then click **Continue**. This process may take a few minutes.

#### 5.3.8.4 Bypassing SSO when signing in to OpenText Content Management

##### To bypass SSO when signing in to OpenText Content Management:

- To bypass single sign on when signing in to OpenText Content Management, do one of the following:
  - a. Append the `otdsauth=no-sso` query parameter to the OpenText Content Management URL. For example: `<my_OpenText_Content_Management_URL>&otdsauth=no-sso`
  - b. You can also sign out of OpenText Content Management by selecting **Log-out** from the OpenText Content Management **My Account** menu. Next, sign in to OpenText Content Management as another user.

## 5.4 Configuring access to your resources

After you have created a resource, you can continue with the following actions:

- Grant users in selected access roles permission to sign in to your resource.
- After your resource is set up you will need to create access roles and assign access roles to the resources that connect Directory Services to the applications that use its services. For information about granting existing access roles permission to sign in to your resource, see “[Editing access roles for your resource](#)” on page 225. For information about creating an access role, see “[Access Roles](#)” on page 229 and “[Creating an access role](#)” on page 231.
- After your resource is set up you may need to allow this resource to impersonate users of another resource.

For more information, see “[Using impersonation](#)” on page 224 and “[Editing impersonation settings](#)” on page 225.

- Turn on synchronization of changes made in Directory Services so that they are delivered to your synchronized resource automatically using the resource connector.

After your synchronized resource is set up you can manage synchronization of data changes from Directory Services to your resource. You may want to **Consolidate** changes to users and groups in your user partitions to deliver bulk updates to your resource after you have turned on user synchronization. For more information, see “[Turning user synchronization on or off](#)” on page 226.

### Using impersonation

Impersonation should only be allowed when an application needs to perform actions in the system as another user. This can be required, for example, if an application runs background jobs on behalf of users. The corresponding application's documentation will specify whether impersonation is required.

A resource can only impersonate users that have been granted access to that resource.

For more information, see “[Editing impersonation settings](#)” on page 225.

### 5.4.1 Editing access roles for your resource

#### To edit access roles for your resource:

1. From the web administration menu, click **Resources**. From your resource's **Actions** menu, click **Edit Access Roles**.
2. On the **Edit Access Roles for resource <resource\_name>** page, select check boxes for each **Access Role** to be granted permission to sign in to this resource. All users and groups in this access role will be allowed to sign in to this resource.
3. Click **OK**.



**Note:** For information about creating an access role, see “Access Roles” on page 229 and “Creating an access role” on page 231.

### 5.4.2 Editing notification settings for your resource

#### To edit notification settings for your resource:

1. From the web administration menu, click **Resources**. From your resource's **Actions** menu, click **Notifications**.
2. In the **Resource Notifications - <resource\_name>** dialog box:
  - a. Select the **Disable Notifications** check box if you do not want notifications for license usage for this resource.
  - b. In the **E-mail Addresses** text box, type, each on a new line, the email addresses of each individual who should receive these notifications.  
If no email addresses are specified, the email address from the **General Notifications** area in “Notifications Settings” on page 320 will be used. If there is no email address in either text box, no notifications will be sent.
  - c. In the **Threshold** text box, type a positive integer to represent the percentage of license usage at which point OTDS will send a notification.  
If nothing is specified, the default is “80”.
  - d. Click **OK**.

### 5.4.3 Editing impersonation settings

#### To edit impersonation settings:



**Note:** You can edit impersonation settings for a resource or for an OAuth client.

1. From the web administration menu, do one of the following:
  - To edit impersonation settings for a resource, click **Resources**. From your resource's **Actions** menu, click **Impersonation Settings**.

- To edit impersonation settings for a resource, click **OAuth Client**. From your OAuth client's **Actions** menu, click **Impersonation Settings**.
2. On the **Impersonation Settings** page, select **Allow this resource/client to impersonate users**. For more information, see "[Using impersonation](#)" on page 224.
  3. **Optional** If you want to restrict impersonation tokens to apply only to defined resources, select the box next to each resource.
  4. Click **OK** to apply your impersonation settings.

#### 5.4.4 Turning user synchronization on or off

**To turn user synchronization on:**

1. From the web administration menu, click **Resources**.
2. Select your synchronized resource's **Actions** menu, and then click **Turn User Synchronization On**.

**To turn user synchronization off:**

1. From the web administration menu, click **Resources**.
2. Select your synchronized resource's **Actions** menu, and then click **Turn User Synchronization Off**.

### 5.5 Activating your resource for authentication

After your resource is set up, your resource is waiting for activation. Neither the **Disable Authentication** nor the **Deactivate Resource** actions are available. You must first activate Directory Services authentication on the resource.

For example, OpenText Content Management requires that you use the **Directory Services Integration Administration** page in **OpenText Content Management Administration** to activate authentication. When you activate OpenText Content Management for authentication using **Directory Services Integration Administration** you will need to supply the `<server name>` and `<port>` of your Directory Services server and the resource identifier that you were given when you created your synchronized OpenText Content Management resource.



**Tip:** Refresh your resource in the web administration client after completing activation on your resource.

You can perform the following actions:

---

#### Activate your resource for authentication by Directory Services in the administrative interface of the resource

This must be done before Directory Services will allow users to sign in to your resource. For more information, see "[Activating or deactivating your resource](#)" on page 227.

---

**Enable authentication in Directory Services**

After a resource is activated at the resource, it will be enabled and activated for authentication. However, if authentication is turned off, this option turns on authentication for a resource so that all user authentication requests for this resource are processed. For more information, see “[Enabling or disabling authentication for your resource](#)” on page 228.

---

After a resource is activated and enabled for authentication, the following actions will be available:

---

**Disable Authentication from the web administration client**

A resource can be disabled from that resource's **Actions** menu. Disabling a resource from Directory Services means that all user authentication requests for this resource will be ignored until authentication is enabled again. If it is enabled in the web administration client and reactivated at the resource, authentication will resume. For more information, see “[Enabling or disabling authentication for your resource](#)” on page 228.

---

**Deactivate Resource from the web administration client**

A resource can be deactivated from that resource's **Actions** menu. Deactivating the resource in the web administration client will force the resource to reactivate with Directory Services, thereby establishing a new secret key. For more information, see “[Activating or deactivating your resource](#)” on page 227.

---

**Deactivate resource from the resource**

Some resources can be deactivated at the resource. If a resource is deactivated at the resource, it will return to the waiting for activation state in which the **Disable Authentication** and **Deactivate Resource** actions are not available. To resume authentication for the resource in this state, you must reactivate authentication in the resource. For more information, see “[Activating or deactivating your resource](#)” on page 227.

---

## 5.5.1 Activating or deactivating your resource

**To activate your resource:**

1. Using the administrative interface of your resource, reactivate authentication for this resource. For example, for OpenText Content Management resources, use the **Directory Services Integration Administration** page of the OpenText Content Management administration interface to activate Directory Services Authentication.
2. If necessary, restart your resource.
3. Refresh your resource in the web administration menu.

**To deactivate your resource:**

1. From the web administration menu, click **Resources**.
2. From your resource's **Actions** menu, click **Deactivate Resource**.

3. Confirm that you want to deactivate this resource.

## 5.5.2 Enabling or disabling authentication for your resource

### To enable authentication for your resource:

1. From the web administration menu, click **Resources**. From your resource's **Actions** menu, click **Enable Authentication**.
2. Confirm that you want to enable authentication for this resource, and then click **Enable Authentication**.
3. Using the administrative interface of your resource, reactivate authentication for this resource. For example, for OpenText Content Management resources, use the **Directory Services Integration Administration** page of the OpenText Content Management administration interface to activate Directory Services Authentication.
4. If necessary, restart your resource.
5. Refresh your resource in the web administration client.

### To disable authentication for your resource:

1. From the web administration menu, click **Resources**. From your resource's **Actions** menu, click **Disable Authentication**.
2. Confirm that you want to disable authentication for this resource, and then click **Disable Authentication**.

# Chapter 6

## Access Roles

This section describes creating, editing, and deleting access roles. This section also describes how to assign members to access roles and allow users with particular access roles to sign on to selected resources.

You will need to create access roles to define for which resources you want your users and groups to have sign in privileges. An access role can be assigned to users or groups for any number of resources.

 **Note:** An access role will only enable authentication for a resource. The resource may still deny access based on authorization to use a function. Directory Services does not manage authorization for components.

The **Access Roles** page displays a list of all access roles that you have defined to control who can access which resources. This page also displays whether groups are included in this access role.

When you select an access role's **Actions** menu, you can view the **Members** of that access role and the **Resources** that they are allowed to access. Members of an access role can be user partitions, organizational units, individual users, groups, or application roles. You can also view the resources that members of this access role are allowed to access. Both the members and the resources can be edited.

### Access roles Actions menu options and buttons

On the main **Access Roles** page, each access role has an associated **Actions** menu and applicable buttons. The following are quick links to the procedures associated with each:

#### Access roles Actions menu items

Actions menu option	Associated procedure
Include/Exclude Groups	<a href="#">"Including/excluding groups from organizational units" on page 234</a>
View Access Role Details	This page will show you all user partitions, organizational units, users, groups, applications roles, and resources that are assigned to this access role. You can optionally choose to add or delete user partitions, organizational units, users, groups, application roles, and resources to/from this access role.

### Access roles buttons

Button	Associated procedure
Add	<a href="#">“Creating an access role” on page 231</a>
Delete	<a href="#">“Deleting an access role” on page 234</a>
Save	<a href="#">“Assigning members to an access role or removing members from an access role” on page 231</a>
Refresh	Use the <b>Refresh</b> button to verify if OTDS has completed an action. For example, after deleting.
Help	The <b>Help</b> button will open context-sensitive help for the page you are currently using.

## 6.1 Assigning members to an access role

After you have created an access role you will need to add members to that access role.

### Including groups in an access role

When adding a group to an access role, the group and any members of the group will be added to the resource. Members of groups may be users or other groups.

### Including organizational units in an access role

When you are editing members of an access role, you can selectively choose which organizational units to include in an access role. When adding an organizational unit to an access role, the following will be added to the resource:

- All the users in that organizational unit and sub-organizational units.
- All the groups in that organizational unit and sub organizational units, if group inclusion is enabled.

If you add an organizational unit to a resource, you cannot selectively exclude individual users, groups or child organizational units.

For more information, see [“Assigning members to an access role or removing members from an access role” on page 231](#).

### Including groups from organizational units in an access role

To provide for more flexible group management, by default, when you add a partition or organizational unit to an access role, the groups in that partition or organizational unit will not be synchronized to the access role's resources.

Groups that should be synchronized to resources need to be explicitly added to the access role. Alternatively, to synchronize all groups within any partition or organizational unit added to an access role, you must select **Include Groups from Organizational Units** on the access role.

For more information, see “[Including/excluding groups from organizational units](#)” on page 234.

## 6.2 Creating an access role

### To create an access role:

1. From the web administration menu, click **Access Roles**.
2. On the button bar, click **Add**.
3. In the **Name** text box, type the name of this new access role.  
The name of the access role should clearly indicate what type of users you are describing with this particular access privilege. For example, Development Managers, Development Managers (NA), Employees. Access role names must be unique. The name Local RCS Administrators is a reserved access role name.
4. **Optional** In the **Description** text box, type a description of this new access role.
5. Click **Save**.

## 6.3 Assigning members to an access role or removing members from an access role

### To assign members to an access role or remove members from an access role:

1. From the web administration menu, click **Access Roles**.
2. From your access role's **Actions** menu, click **View Access Role Details**.
3. On the <*your\_access\_role\_name*> page, click to select one of the following tabs, depending on which members you wish to add:
  - If you want to add all members in a user partition to an access role, click to select the **User Partitions** tab.
  - If you want to add all users in an organizational unit to an access role, click to select the **Organizational Units** tab. This adds all users in the organizational unit to this access role. Groups within organizational units are not added by default. For more information, see “[Including groups from organizational units in an access role](#)” on page 230. Organizational units appear with an organizational unit icon after they are added.

You cannot selectively exclude users from this access role after your organizational unit has been added to this access role. For more information, see “[Including organizational units in an access role](#)” on page 230.

- If you want to add specific users to an access role, click to select the **Users** tab. Users appear with a user icon after they are added.



**Note:** Users found by the search that are already members of the access role are shown in the results but you cannot select and add them again.

- If you want to add all members in a group to an access role, click to select the **Groups** tab. Groups appear with a group icon after they are added.
- For information about the **Resources** tab, see “[Assigning access roles to resources](#)” on page 233.
- If one of your OpenText products has created an application role in your OTDS environment, you may also have the opportunity to add all members in an application role to an access role. Click to select the **Roles** tab. For more information, see “[Application Roles](#)” on page 261.

4. On the tab you have selected, click **Add**.
5. On the **Add <item> - <access\_role\_name>** page, select the check box to the left of each <item> whose members you want to assign to this access role. If you are adding users, click to select each specific user you want to add. This will add either the specific user selected, or all users in the partition, organizational unit, or group to your access role.
6. Click **Add Selected Items to Access Role**, and then click **Close Dialog**.
7. On the button bar, click **Save**.
8. **[Optional]** If you want to remove members in a user partition, organizational unit, group, application role, or a specific user from an access role:
  - a. From the web administration menu, click **Access Roles**.
  - b. From your access role's **Actions** menu, click **View Access Role Details**.
  - c. Select the relevant tab to display the members in the access role. Select one of **User Partitions**, **Organizational Units**, **Users**, **Groups**, **Roles** or **Resources** depending on what you want to remove from the access role.
  - d. Select the check box to the left of the item you want to remove from the access role, and then, click **Delete**.
  - e. Click **Save**.

## 6.4 Assigning access roles to resources

### To assign access roles to resources:

1. From the web administration menu, click **Access Roles**.
2. From the access role's **Actions** menu, click **View Access Role Details**.
3. Select the **Resources** tab.
4. Click **Add**.
5. On the **Add Resources - <resource\_name>** page:
  - a. Click to select all resources to which the access role members will be allowed to sign in.
  - b. Click **Add Selected Items to Access Role**, and then click **Close Dialog**.
6. On the button bar, click **Save**.
7. **[Optional]** If you want to remove an access role previously assigned to a resource:
  - a. From the web administration menu, click **Access Roles**.
  - b. From your access role's **Actions** menu, click **View Access Role Details**.
  - c. Select the **Resources** tab.
  - d. Select the check box to the left of the resource you want to remove from the access role, and then, click **Delete**.
  - e. Click **Save**.

## 6.5 Editing an access role

### To edit an access role:

1. From the web administration menu, click **Access Roles**, and then click in the **Description** text box of the access role you want to edit.
2. Edit the description of this access role. No other text boxes can be edited.
3. Click **Save**.

## 6.6 Deleting an access role

**To delete an access role and remove users' access to its resources:**

1. From the web administration menu, click **Access Roles**.
2. On the **Access Roles** page, click the select box to the left of your access role, and then click **Delete**.

**!** **Important**

After an access role has been deleted, users in this access role will no longer have access to its resources unless they are also mapped to this resource through another access role.

3. Click **OK** to confirm that you want to delete this access role.

## 6.7 Including/excluding groups from organizational units

**To include groups from organizational units:**

1. From the web administration menu, click **Access Roles**.
2. From your access role's **Actions** menu, click **Include Groups**.
3. Read the information provided, and if you want to continue, click **OK** to confirm.

**To exclude groups from organizational units:**

1. From the web administration menu, click **Access Roles**.
2. From your access role's **Actions** menu, click **Exclude Groups**.
3. Read the information provided, and if you want to continue, click **OK** to confirm.

# Chapter 7

## Users and Groups

This section describes viewing, editing, and consolidating user and group information. The **Users and Groups** page provides a common access point to all the users and groups that are found in all user partitions in Directory Services. This includes both synchronized users and non-synchronized users.

The **Users and Groups** page displays all users and groups across all partitions. You can view details such as the user partition to which the user or group belongs, and the location, in that partition, of the user or group.

 **Tip:** The number of users and groups displayed is defined by the **Results per page** list. Click **Previous** or **Next** to page through the results. The search box can also be used to find particular users or groups to limit your display.

From any user's or group's **Actions** menu, you can view user details such as the groups of which a user is a member. You can view group details such as the list of users who belong to a group and the groups of which a particular group is a member. The search function allows you to display a specific number of users and groups that match your search criteria.

 **Note:** OTDS searches only attributes related to the user's identifier and name.

### Users and groups Actions menu options and buttons

On the main **Users and Groups** page, each user and group has an associated **Actions** menu and applicable buttons. The following are quick links to the procedures associated with each:

#### Users and groups Actions menu options

Actions menu option	Associated procedure
Properties	<a href="#">"Editing users" on page 242</a> and <a href="#">"Editing groups" on page 252</a>
Consolidate	<a href="#">"Consolidating users" on page 243</a> and <a href="#">"Consolidating groups" on page 255</a>
Two Factor Auth Settings	<a href="#">"Enabling two-factor authentication" on page 245</a>
Edit Membership	The <b>Edit Membership</b> menu option is used in several procedures related to editing groups. For example, see <a href="#">"Editing members of groups in a synchronized user partition" on page 98</a> .
View Recursive Membership	<a href="#">"To view all application roles (recursively) assigned to a specific user, group, or application role" on page 266</a>

Actions menu option	Associated procedure
Edit Application Roles	<a href="#">"Editing an application role" on page 263</a>
Edit Administrators	The <b>Edit Administrators</b> menu option is used in several procedures related to editing administrators of groups and organizational units. For example, see <a href="#">"Editing administrators of groups" on page 254</a> .
Reset Password	<a href="#">"Resetting a user password" on page 244</a>
View Effective Roles	If you want to view the application roles to which this user belongs, click <b>View Effective Roles</b> . For more information, see <a href="#">"To view all application roles (recursively) assigned to a specific user, group, or application role" on page 266</a> .
Allocate to License	<a href="#">"Allocate to license" on page 247</a>
View and Edit Allocated Licenses	<a href="#">"View and edit allocated licenses" on page 248</a>

### Users and groups buttons

Button	Associated procedure
Consolidate	<a href="#">"Consolidating users" on page 243</a> and <a href="#">"Consolidating groups" on page 255</a>
Delete	<a href="#">"Deleting users" on page 249</a> and <a href="#">"Deleting groups" on page 256</a>
Refresh	Use the <b>Refresh</b> button to verify if OTDS has completed an action. For example, after deleting or after consolidating.
Help	The <b>Help</b> button will open context-sensitive help for the page you are currently using.

## Users

When you select **Edit Membership** from any user's **Actions** menu, a list of groups that this user is a **Member Of** is displayed. For more information on viewing and editing users, see ["Configuring users" on page 241](#).

Selected users can be consolidated to all their resources. For more information, see ["Consolidating users" on page 243](#).

## Groups

When you select **Edit Membership** from any group's **Actions** menu, the following is displayed:

- The **Members** tab displays a list of the members of that group.
- The **Member Of** tab displays a list of groups that this group is a member of.

For more information on viewing and editing groups, see ["Configuring groups" on page 249](#).

Selected groups can be consolidated to all their resources. For more information, see “[Consolidating groups](#)” on page 255 to consolidate a selected group.

## 7.1 Configuring two-factor authentication

You can choose to enable two-factor authentication for a single user, for all users in a group, for all users in an organizational unit, or for all users in a partition. When you enable two-factor authentication for users, you ensure that those users must complete a two-stage login procedure when they login to OTDS.

Directory Services uses a Time-Based One-Time Password Algorithm (TOTP). After two-factor authentication has been enabled for a user, that user must have a *TOTP client* application to obtain the authentication codes required to login to OTDS. An example of a TOTP client is Google Authenticator. TOTP clients are available through Google Play or Apple iTunes.

When the user logs into OTDS for the first time:

1. The user will be taken to a **Secret Key** page. The user will need to enter the secret key to their TOTP client.
2. Their TOTP client will then provide them with a time-sensitive authentication code. The user must enter the authentication code to the **Authentication Code** text box on the OTDS sign in page.

When you configure two-factor authentication for a user, a group, an organizational unit, or a partition, you can choose to define the two-factor authentication settings or you can choose to inherit the two-factor authentication settings from the parent object. Select one of the following:

---

### Inherit settings

If you select this option, the two-factor authentication settings defined for the parent object will take effect. OTDS will first check to see if there is an existing setting for two-factor authentication on a parent. If there is no parent two-factor authentication setting to inherit, OTDS will apply the global setting.

The order of inheritance that OTDS checks:

1. organizational unit membership
2. partition
3. global settings



**Note:** If you enable two-factor authentication for a group, that is equivalent to manually enabling two-factor authentication for every individual user that is directly, or indirectly, a member of that group.

When you select **Inherit settings**, the settings that will be inherited will be displayed, dimmed. This allows you to see the inherited settings that you will be applying, including whether two-factor authentication has been enabled. If these are not the settings you want applied, change your selection to [Define settings](#) on page 238 to make changes.

---

**Define settings**

If you select this option, you will need to choose your two-factor authentication settings from the options below. These settings will override the settings on any parent object.

You must first select **Enable two-factor authentication** to allow you to choose from among the following settings. This option enables two-factor authentication for users in the partition, organizational unit, or group. If you clear this option, you will disable two-factor authentication for those users.

---

**Enable for users authenticated by SSO**

Select this option to apply two-factor authentication to those users who are authenticated by SSO, for example Kerberos or SAML.

---

**Require a client certificate**

Select this option if you want the second factor or the two-factor authentication to be a client certificate, as opposed to a configured mechanism. OpenText recommends that you only enable this option for service accounts. A client certificate must be provided through an https connection, in order to authenticate with the account on which this option is enabled.

If a proxy is used in front of OTDS, the proxy must accept client certificates and the [HTTP Header for Proxied Client Certificate on page 302](#) system attribute must be configured.

---

**Enable only for requests originating from Extranet IP addresses**

Select this option to apply two-factor authentication to users only when the request originates from an external IP address. There are two system attributes you can configure for this two-factor setting:

- Intranet subnets that aren't within the standard private IP ranges can be configured using the OTDS system attribute [otds.as.intranetSubnets on page 305](#).
- To ensure that the values in the **X-Forwarded-For** header or the **Forwarded** header are trusted, all proxies in the request, including the immediate caller's IP, need to be listed in the OTDS system attribute [otds.as.trustedProxies on page 306](#).

---

**Allow skipping**

Select this option to allow the users to skip two-factor authentication when they login from a remembered device. A remembered device is a client from which the users has successfully logged in to OTDS with an authentication code previously.

---

**Reset Secret Key**

Click this button to reset the users secret key on their TOTP client. For more information, see [“Resetting a user's secret key” on page 240](#).

For more information, see [“Enabling two-factor authentication” on page 245](#).

### 7.1.1 Two-factor authentication with a third-party two factor authentication provider

Two-factor authentication can be implemented with a third-party two factor authentication provider instead of OTDS' embedded two-factor authentication. For more information, see [Third-Party Two-Factor Authentication Provider on page 312](#) and [“References to external websites” on page 385](#). Currently, OTDS supports the following third-party two factor authentication providers:

- “[Duo Security and two-factor authentication](#)” on page 239
- “[Symantec VIP and two-factor authentication](#)” on page 239

#### Duo Security and two-factor authentication

Two-factor authentication can be implemented with “Duo Security”, for more information about Duo Security, see [“References to external websites” on page 385](#). You need to complete the following in order to enable two-factor integration using Duo Security:

1. Complete the registration of a Web SDK integration in your “Duo Security” account for OTDS. This will ensure you have an integration key, a secret key, and an API hostname that you need to enter in OTDS. For more information about Duo Security, see [“References to external websites” on page 385](#).
2. Configure the following OTDS system attributes:
  - `directory.auth.ThirdPartyTwoFactorProvider=duo`  
For more information, see [Third-Party Two-Factor Authentication Provider on page 312](#).
  - `duo.akey=<DUO application secret key>`. This value is generated by OTDS and should not be manually configured.  
For more information, see [duo.akey on page 295](#).
  - `duo.host=<DUO API hostname>`  
For more information, see [duo.host on page 295](#).
  - `duo.ikey=<DUO integration key>`  
For more information, see [duo.ikey on page 295](#).
  - `duo.skey=<DUO secret key>`  
For more information, see [duo.skey on page 296](#).
3. As with embedded two-factor authentication in OTDS, the two-factor authentication must be configured in OTDS on the users, groups, or partitions as detailed in [“Enabling two-factor authentication” on page 99](#).

#### Symantec VIP and two-factor authentication

Two-factor authentication can be implemented with “Symantec VIP”, for more information about Symantec VIP, see [“References to external websites” on page 385](#). The hostname used for OTDS must be added as a trusted URL in the Symantec VIP

manager. For more information about Symantec VIP, see “[References to external websites](#)” on page 385.

You need to complete the following in order to enable two-factor integration using Symantec VIP:

1. Register OTDS in Symantec VIP Manager, and then:
  - a. Add the OTDS URL as a trusted site.
  - b. Obtain a PKCS12 keystore for OTDS to use to connect to Symantec VIP.
2. Configure the following OTDS system attributes:
  - a. **directory.auth.ThirdPartyTwoFactorProvider=symantec**  
For more information, see [Third-Party Two-Factor Authentication Provider on page 312](#).
  - b. **symantec.appid=<account VIP application ID>**  
Your account's VIP application ID, available in VIP manager. For more information, see [symantec.appid on page 311](#).
  - c. **symantec.keystore=<URL to the keystore OTDS should use to connect to VIP services>**  
The keystore must have been exported from VIP manager in PKCS12, for example, `file:/C:/certificates/otdsvip.p12`. The keystore must be accessible on all OTDS servers handling authentication. For more information, see [symantec.keystore on page 311](#).
  - d. **symantec.keystorepassword=<password used for keystore>**  
For more information, see [symantec.keystorepassword on page 311](#).
  - e. **symantec.usernameattr=<OTDS attribute name>**  
The OTDS attribute name that contains the value corresponding to the users' username in Symantec VIP. For more information, see [symantec.usernameattr on page 311](#).
3. As with embedded two-factor authentication in OTDS, the two-factor authentication must be configured in OTDS on the users, groups, or partitions as detailed in “[Enabling two-factor authentication](#)” on page 99.

### 7.1.2 Resetting a user's secret key

**To reset a user's secret key:**

1. From the web administration menu, find the user for whom you want to reset the secret key.
2. From the **Actions** menu associated with the user you want to edit, click **Two Factor Auth Settings**.
3. In the **Two Factor Authentication Settings** box, click **Reset Secret Key** to reset the secret key for the user. The user will be provided a new secret key for their TOTP client the next time they login. For more information, see “[Configuring two-factor authentication](#)” on page 237.

## 7.2 Configuring users

On the **Users and Groups** page, the **Users** tab displays a fixed number of users that can be displayed on the page. An indicator in the top panel indicates the number of users being displayed, for example: “Results per page 25”. If the number of users exceeds the maximum allowable for this display, click **Next** to scroll through the pages of users.

Only users in non-synchronized user partitions may be edited. To create a new user in a non-synchronized user partition, you must use the **New User** assistant from the **User Partitions** page. For more information, see “[Creating users in a non-synchronized user partition](#)” on page 109.

To delete a user from a non-synchronized user partition, you must use the **Delete** action from the **User Partitions** page. For more information, see “[Deleting users](#)” on page 249.

### The Directory Services default administrative user

Directory Services installs a default administrative user: `otadmin`

This is the special administrative user that must be used to configure the Directory Services server. It is automatically added as a member of each of the default groups.

#### 7.2.1 Searching for users

##### To search for users:

1. From the web administration menu, select **Users and Groups**.
2. On the **Users and Groups** page, click the **Users** tab.
3. Below the button bar, select one of the two search options, either **Starts with** or **Contains**.
4. In the **Search** text box, type the text for which you want to search.
5. Click **Search**.

#### 7.2.2 Adding users

You can only add users to a non-synchronized user partition. For more information, see “[Creating users in a non-synchronized user partition](#)” on page 109.

### 7.2.3 Editing users

You can only edit users from a non-synchronized user partition.

#### To edit users in a non-synchronized user partition:

1. From the web administration menu, click **Users & Groups**, and then select the **Users** tab.



**Tip:** You can also, from the web administration menu, click **Partitions** and then, from the non-synchronized user partition's **Actions** menu, select **View Members**. Select the **Users** tab.

2. From the **Actions** menu associated with the user you want to edit, click **Properties**. You can use the search box to find the user.
  - a. Follow the instructions, beginning with step 4, found in “[Creating users in a non-synchronized user partition](#)” on page 109.
  - b. When you have finished editing, on the button bar, click **Save**.
3. **Optional** From the **Actions** menu associated with any user you want to edit, do the following:
  - If you want to consolidate this user, click **Consolidate**, and then see “[Consolidating users in a partition](#)” on page 112.
  - If you want to set two factor authentication for this user, click **Two Factor Auth Settings**, and then see “[Enabling two-factor authentication](#)” on page 115.
  - If you want to edit the groups to which this user belongs, click **Edit Membership**, and then see “[Editing members of groups in a non-synchronized user partition](#)” on page 118.
  - If you want to view recursive memberships for this user, click **View Recursive Membership**, and then see “[To view all application roles \(recursively\) assigned to a specific user, group, or application role](#)” on page 266.
  - If you want to edit the application roles to which this user belongs, click **Edit Application Roles**, and then see “[Editing an application role](#)” on page 263.
  - If you want to view the application roles to which this user belongs, click **View Effective Roles**, and then see “[Editing an application role](#)” on page 263.
  - If you want to reset this user's password, click **Reset Password**, and then see “[Resetting a user password in a non-synchronized user partition](#)” on page 113.
  - If you want to allocate this user to a license, click **Allocate to License**, and then see “[Allocate to license](#)” on page 247.

**!** **Important**

OpenText recommends that you do not select this option. No products currently use this functionality.

- If you want to delete this user, see “[Deleting users in a non-synchronized user partition](#)” on page 115.

## 7.2.4 Consolidating users

Consolidation of a selected user allows you to push user data to the resources with which a selected user is associated. Choose one of the two procedures below, depending on whether you want to consolidate an existing user or consolidate a missing user.

### To consolidate an existing user:

1. From the web administration menu, click **Users & Groups**.
2. In the center of the page, select the **Users** tab.



**Tip:** You can also, from the web administration menu, click **Partitions** and then, from the user partition's **Actions** menu, select **View Members**. Select the **Users** tab.

3. From the **Actions** menu associated with the user you want to consolidate, select **Consolidate**. You can use the **Search** box to find the user.
4. In the **Consolidate <userid>** box, do the following:

- a. In the **Consolidate options** area, do the following:

- i. **Optional** If you are consolidating a synchronized user partition and you want to consolidate the selected object in OTDS with the identity provider, AD or LDAP, select **Consolidate with identity provider**.
- ii. **Optional** If you want to direct OTDS to verify and repair a discrepancy in its internal referential integrity attributes, for example oTMember or oTMemberOf, select **Verify and repair**.



**Note:** OpenText recommends that you do not perform a **Verify and repair** operation unless directed to by OpenText technical support.

- b. If you are consolidating an object in a synchronized user partition, then in the **Consolidate with the following resources** area, select all resources with which the previously selected object will be consolidated with information in OTDS.



**Note:** Consolidation operations may take a long time to complete. You can monitor the process through the “[directory-provenance.log](#)” on page 376 file.

- c. Click **Consolidate** to consolidate user data for the selected existing user.

**To consolidate a missing user:**

If you know of a user who should be present in OTDS but is not listed, you can consolidate that missing user as follows:

1. From the button bar, click **Consolidate**.
2. From the **Consolidate** menu, click **Consolidate Missing User**.
3. In the **Account DN** box, enter the DN of the missing user in the **User DN** box.
4. Click **OK**.

### 7.2.5 Resetting a user password

You can only reset a user password for an existing user in a non-synchronized user partition.

**To reset a user password in a non-synchronized user partition:**

1. From the web administration menu, click **Users & Groups**, and then select the **Users** tab.



**Tip:** You can also, from the web administration menu, click **Partitions** and then, from the non-synchronized user partition's **Actions** menu, select **View Members**. Select the **Users** tab.

2. Select the user for whom you want the password reset, or use the **Search** box to find the user.

From the **Actions** menu associated with the user whose password you want to reset, select **Reset Password**.

3. If the user whose password you are attempting to reset is currently using passwordless authentication, you will see a warning. For more information, see ["Using WebAuthn to provide users the option of passwordless authentication"](#) on page 103.

4. In the **Reset Password** box, do the following:

- a. The **User name** text box cannot be edited.
- b. In the **New password** text box, enter a new password for this user.
- c. In the **Confirm new password** text box, re-type exactly the new password for this user.
- d. Click **Reset Password** to change the password.

## 7.2.6 Unlocking a user account

### To unlock an account:

1. From the web administration menu, click **Users & Groups**, and then select the **Users** tab.



**Tip:** You can also, from the web administration menu, click **Partitions** and then, from the non-synchronized user partition's **Actions** menu, select **View Members**. Select the **Users** tab.

2. Select the user whose account you want unlocked, or use the **Search** box to find the user.

From the **Actions** menu associated with the user whose account you want to unlock, select **Properties**.

3. On the **Account** tab, clear the **Account is locked out** box.
4. Click **Save**.

## 7.2.7 Enabling two-factor authentication

### To enable two-factor authentication:

You can choose to enable two-factor authentication:

- Globally, for *all* users, groups, organizational units, and partitions; or
- Individually, for *specific* users, groups, organizational units, and partitions.

You can choose to define settings at one level and then define at a lower level to override those settings. For example, you can enable two-factor authentication globally but define it as disabled for a specific user, group, organizational unit, or partition.

For background information describing these settings, see “[Configuring two-factor authentication](#)” on page 237.

1. **Optional** If you want to set two-factor authentication *global settings* for all users, groups, organizational units, and partitions:
  - a. From the web administration menu, click **Partitions**.
  - b. On the **Partitions** page, on the button bar, click **Global Settings**. From the **Global Settings** menu, click **Two Factor Auth Settings**.
  - c. In the **Two Factor Authentication Settings - Global** box, select **Enable two factor authentication**.
  - d. Select any of the options to apply two-factor authentication settings. For more information, see the **Define Settings** options in “[Configuring two-factor authentication](#)” on page 237.
  - e. Click **OK**.

2. **Optional** If you want to set two-factor authentication at a *specific* user, group, organizational unit, or partition level:
  - a. From the web administration menu:
    - If you want to set two-factor authentication for a user, group, or organizational unit, click **Users & Groups**.
    - If you want to set two-factor authentication for a partition, click **Partitions**.
  - b. On either the **Users & Groups** page or the **Partitions** page, find the user, group, organizational unit, or partition for whose users you want to enable two-factor authentication.
  - c. From the **Actions** menu associated with the user, group, organizational unit, or partition you want to edit, click **Two Factor Auth Settings**.
  - d. In the **Two Factor Authentication Settings - <item\_name>** box, from the **Two Factor Authentication Settings** list, select either **Inherit settings** or **Define settings**, and then, do the following:
    - i. If you select **Inherit settings** for a partition, an organizational unit, a group, or a user, and two-factor authentication has not been enabled for the parent object or in the *global settings* box, two-factor authentication will not be enabled. For information about enabling global settings, see the first step in this procedure.  
If you select **Inherit settings** for a partition, two-factor authentication will be enabled according to the *global settings*.  
The **Two Factor Authentication Settings** box will display, dimmed, the inherited settings that will be applied. If these are not the settings you want applied, change your selection to **Define settings** to make changes.
    - ii. If you select **Define settings** for a partition, an organizational unit, a group, or a user, select any of the options to apply two-factor authentication settings. For a description of these options, see ["Configuring two-factor authentication" on page 237](#).
    - iii. Click **OK**.



**Note:** For information about resetting a user's secret key, see ["Resetting a user's secret key" on page 240](#).

## 7.2.8 Allocate to license

### To allocate a user to a license:

To view explanatory information about allocating licenses, see “[Understanding allocating and reserving licenses to users, groups, and partitions](#)” on page 336.

1. From the web administration menu, you can choose a user, group, or partition to allocate to a license. Select either **Partitions** or **Users & Groups**.

**!** **Important**

Previously, products did not use this functionality. This functionality became available with OTDS 20.4.2.

OpenText recommends that you do not select the allocate option unless you have advanced knowledge of licensing for your product. For more information, see “[License Keys](#)” on page 331.

2. Find the partition, user, or group that you want to allocate to a license or counter. From that partition's, user's, or group's **Actions** menu, click **Allocate to License**.



**Note:** If your installation of OTDS does not contain licenses, the **Allocate to License** box does not appear.

3. In the **Allocate to License** dialog box, do the following:

- a. From the **License** list, select the license to which this user, group, or partition will be allocated.



**Note:** When you allocate a group, all members of that group are allocated to the license. When you allocate a partition, all members of that partition are allocated to the license.

- b. From the **Counter** list, select either the product or the feature of the product to which this user, group, or partition will be allocated.



**Note:** If you select the main product from this list, then the user, group, or partition members will be recursively allocated to the main product and to all features of the product.

This list is only available if you are using OTDS 20.4.2.

- c. Some selections from the **Counter** list may display a **License Type** field. If this field appears, it is not editable.

- d. Click **Allocate to License**.

4. View the information message “license allocation has begun”. You can monitor license actions in the “[otds.log](#)” on page 375 log file.

## 7.2.9 View and edit allocated licenses

### To view and edit allocated licenses:

For information about allocating licenses, see “[Understanding allocating and reserving licenses to users, groups, and partitions](#)” on page 336.

1. From the web administration menu, you can choose a user, group, or partition to view and edit allocated licenses. Select either **Partitions** or **Users & Groups**.
2. Find the partition, user, or group whose allocated licenses you want to view or edit. From that partition's, user's, or group's **Actions** menu, click **View and Edit Allocated Licenses**.



**Note:** If you allocated a group, all members of that group are allocated to the license. If you allocated a partition, all members of that partition are allocated to the license.

3. On the page that lists all the licenses in the system, you can optionally do the following:
  - a. From the **Actions** menu of any license, you can choose to do one of the following:
    - i. **View Recursive Licenses:** this page details whether the partition, user, or group is allocated to the license. It also details the kind of license counter or product the partition, user, or group is allocated.  
This page displays:
      1. Licenses that are directly applied to the partition, user, or group.
      2. Licenses that are inherited by any partition, user, or group based on membership. Users inherit membership from groups and partitions to which they belong. Groups inherit membership from partitions to which they belong.
    - ii. **Edit Licenses:** from each license's **Actions** menu, you can choose to deallocate any license from this partition, user, or group. This will remove the user's, or group's, or partition's authorization to reserve a seat for this license. For information about allocating a license, see “[Allocate to license](#)” on page 247. For information about the columns on this page, see “[Licensees and counters](#)” on page 339.



**Note:** If the license was applied to a main product, then the user, group members, or partition members are recursively allocated to that main product and to all features of that product.

- b. You can click the **Show Certificates** button if you want to view the license certificates used by the licenses on this page.

The license certificates will display the certificate name and expiry date. You cannot delete a license certificate if it is in use by a license.

## 7.2.10 Deleting users

You can only delete users from a non-synchronized user partition.

**To delete users in a non-synchronized user partition:**

1. From the web administration menu, click **Users & Groups**, and then select the **Users** tab.



**Tip:** You can also, from the web administration menu, click **Partitions** and then, from the non-synchronized user partition's **Actions** menu, select **View Members**. Select the **Users** tab.

2. Select the user that you want to delete or use the **Search** box to find the user. Select the box to the left of the user you want to delete, and then, from the button bar, click **Delete**.
3. Confirm that you want to delete this user by clicking **OK**.

## 7.3 Configuring groups

On the **Users and Groups** page, the **Groups** tab displays a fixed number of groups that can be displayed on the page. An indicator in the top panel indicates the number of groups being displayed, for example: "Results per page 25". If the number of groups exceeds the maximum allowable for this display, click **Next Results** to scroll through the pages of groups.

Only groups, and members of groups, in a non-synchronized user partition may be edited or deleted. To create a new group in a non-synchronized user partition, you must use the **New Group** assistant from the **User Partition** page. For more information, see "[Creating groups in a non-synchronized user partition](#)" on page 116.

### The Directory Services default administrative groups

Directory Services installs several default groups:

**Table 7-1: Default Directory Services group names**

Group ID	Description
otadmins	Administrators of all OpenText products.  Adding users to this group makes them an administrator in OTDS. However, each product may have its own mechanism for determining its administrators. Check each product's documentation for additional requirements to have those users administer that product.
otadsadmins	OpenText Administration Services administrators.

Group ID	Description
otasadmins	OpenText Archive Server administrators.
otdsadmins	OpenText Directory Services administrators with full privileges. The complete OTDS admin UI is available.
otdsreadonlyadmins	<p>Users who are OTDS read-only administrators. A read-only administrator is a user who can view all OTDS configuration, reset user passwords, and consolidate individual users. In order for a user to be a read-only administrator:</p> <ul style="list-style-type: none"> <li>• A group called <code>otdsreadonlyadmins</code> must be created in the <code>otds.admin</code> partition.</li> <li>• The user must be a member of the <code>otdsreadonlyadmins</code> group, either directly or indirectly by way of another group.</li> </ul> <p>A user who is a member of the <code>otdsreadonlyadmins</code> group, and who is also a member of the <code>otadmins</code> or <code>otdsadmins</code> group will still have full administrative rights to OTDS.</p>
otdsbusinessadmins	<p>Any user assigned to this group can perform most user and group administration tasks in OTDS with the exception of system-related tasks. The admin UI will only display those functions the user can access.</p> <p> <b>Note:</b> If you have upgraded OTDS from a previous version, the <code>otdsbusinessadmins</code> group may not exist. In that case, and if you want to use its functionality, you must manually create this group. Create a group named <code>otdsbusinessadmins</code> in the <code>otds.admin</code> partition. There are no special requirements for the group.</p>
otldadmins	OpenText Solution Registry administrators.
otldagents	OpenText Solution Registry agents.

The special administrative user, `otadmin`, is automatically added as a member of each of these groups. The administrative user, `otadmin`, must be used to configure the Directory Services server.

 **Note:** You must add users directly to these groups to allow them to act as administrators. For example, each user allowed to administer Archive Center must be added to the `otasadmins` group.

### 7.3.1 Delegated administration

A user or group can be granted administration rights on a group, organizational unit, or user partition. Such a delegated administrator has the same privileges on the object as an OTDS administrator. However, they can only administer the object to which they have been granted administration rights. Thus, a delegated administrator acquires the following privileges:

- **On a group:** modify the group attributes, add/remove members, delete the group, and create a *sub-group* in the group.
- **On an organizational unit:** create/delete users and groups within the organizational unit and any of its sub organizational units, in addition to administering groups.
- **On a user partition:** administer all organizational units within the partition.



**Note:** These privileges apply across nested groups within the same user partition. Thus, if Group B is a member of Group A, and User X is a delegated administrator of Group A, then User X can administer *both* Group A and Group B. Likewise, if User X is a delegated administrator of the organizational unit in which Group A is located, User X can administer *both* Group A and Group B.

### 7.3.2 Searching for groups

#### To search for groups:

1. From the web administration menu, select **Users and Groups**.
2. On the **Users and Groups** page, click the **Groups** tab.
3. Select one of the **Search options** radio buttons: **Starts with** or **Contains**.
4. In the **Search** text box, type the text for which you want to search.
5. Click **Search**.

### 7.3.3 Adding groups

You can only add groups to a non-synchronized user partition. For more information, see “[Creating groups in a non-synchronized user partition](#)” on page 116.

### 7.3.4 Editing groups

Only properties of groups in non-synchronized user partitions may be edited.

**To edit groups in a non-synchronized user partition:**

1. From the web administration menu, click **Users & Groups**, and then select the **Groups** tab.



**Tip:** You can also, from the web administration menu, click **Partitions** and then, from the non-synchronized user partition's **Actions** menu, select **View Members**. Select the **Groups** tab.

2. Select the group that you want to edit, or use the **Search** box to find the group. From the group's **Actions** menu, click **Properties**.
  - a. Follow the instructions, beginning with step 4, found in “[Creating groups in a non-synchronized user partition](#)” on page 116.
  - b. When you have finished editing, on the button bar, click **Save**.
3. **Optional** From the **Actions** menu associated with any group you want to edit, do the following:
  - If you want to consolidate this group, click **Consolidate**, and then see “[Consolidating groups in a partition](#)” on page 120.
  - If you want to set two factor authentication for this group, click **Two Factor Auth Settings**, and then see “[Enabling two-factor authentication](#)” on page 99.
  - If you want to edit the groups to which this group belongs, click **Edit Membership**, and then see “[Editing members of groups in a non-synchronized user partition](#)” on page 118.
  - If you want to view recursive memberships for this group, click **View Recursive Membership**, and then see “[To view all application roles \(recursively\) assigned to a specific user, group, or application role](#)” on page 266.
  - If you want to edit the application roles to which this group belongs, click **Edit Application Roles**, and then see “[Editing an application role](#)” on page 263.
  - If you want to view the application roles to which this group belongs, click **View Effective Roles**, and then see “[Editing an application role](#)” on page 263.
  - If you want to edit the administrators of this group, click **Edit Administrators**, and then see “[Editing administrators of groups in a non-synchronized user partition](#)” on page 119.
  - If you want to allocate this group to a license, click **Allocate to License**, and then see “[Allocate to license](#)” on page 247.

**!** **Important**

OpenText recommends that you do not select this option. No products currently use this functionality.

- If you want to delete this group, see “[Deleting groups in a non-synchronized user partition](#)” on page 121.
4. On the button bar, click **Save**.

### 7.3.5 Editing members of groups

Groups in user partitions may have members added as well as members removed, however, you cannot add any item to synchronized groups.

**To edit members of groups:**

1. From the web administration menu, click **Users & Groups**, and then select the **Groups** tab.



**Tip:** You can also, from the web administration menu, click **Partitions** and then, from the **Actions** menu of the partition you want to edit, select **View Members**. Next, select the **Groups** tab.

2. Find the group that you want to edit, or use the **Search** box to find the group. From the **Actions** menu associated with the group whose members you want to edit, select **Edit Membership**.
3. On the `<group_name>@<partition_name>` page, on the **Members** tab, to add a member to this group, on the button bar, click **Add Member**:



**Note:** You cannot add any item to synchronized groups.

- a. In the **Users and Groups Associations** box, use the **Search** box to find members to add to the group. From the search results box, select the check box to the left of the members you want to add to the group, and then click **Add Selected**.
- b. Continue searching for, and adding, members. After you have finished adding members to this group, in the **Users and Groups Associations** box, click **Close**.
4. If you want to add a member to the list of groups that this group, `<group_name>@<partition_name>`, is a “member of”, on the `<group_name>@<partition_name>` page, click the **Member Of** tab:
  - a. On the button bar of the `<group_name>@<partition_name>` page, click **Add To Group**.
  - b. In the **Users and Groups Associations** box, use the **Search** box to find a member to add to the group that this group is a “member of”. From the search results box, select the check box to the left of the members you want to add, and then click **Add Selected**.

- c. Continue searching for, and adding, members. After you have finished adding members, in the **Users and Groups Associations** box, click **Close**.
5. **Optional** If you want to remove a user from the group:
  - a. On the <group\_name>@<partition\_name> page, click the **Members** tab. On the **Members** page, select the check box to the left of the user you want to remove, and then click **Remove Member**.
  - b. Confirm you want to remove this user.  
 **Note:** When you remove a user as a member of a group, you do not delete the user.
6. **Optional** If you want to remove a member from the group that this group is a "member of":
  - a. On the <group\_name>@<partition\_name> page, click the **Member Of** tab. On the **Member Of** page, select the check box to the left of the user you want to remove, and then click **Remove From Group**.
  - b. Confirm you want to remove this member.  
 **Note:** When you remove a member of a group, you do not delete the member.

### 7.3.6 Editing administrators of groups

**To edit administrators of groups:**

1. From the web administration menu, click **Users & Groups**.
2. In the center of the page, select the **Groups** tab.
-  **Tip:** You can also, from the web administration menu, click **Partitions** and then, from the non-synchronized user partition's **Actions** menu, select **View Members**. Select the **Groups** tab.
3. Select the group that you want to edit, or use the **Search** box to find the group.
4. Click the **Actions** link next to the group whose administrators you want to edit. From the **Actions** menu, click **Edit Administrators**.
5. On the <group\_name>@<partition\_name> page, click **Add Administrator**.
6. Use the **Search** box to find users or groups to add to the administrators. From the search results box, select the users or groups you want to designate as administrators, and then click **Add Selected**.
-  **Note:** For more information on delegated administration, see "[Delegated administration](#)" on page 251.
7. Continue searching for, and adding, administrators. After you have finished adding administrators, in the **Users and Groups Associations** box, click **Close**.

8. **Optional** If you want to remove a user or group from the administrators:
  - a. On the <group\_name>@<partition> page, select the administrator you want to remove, and then click **Remove Administrator**.
  - b. Confirm you want to remove this administrator.

 **Note:** When you remove a user or group as a member of the administrators, you do not delete the user or group.

### 7.3.7 Consolidating groups

Consolidation of a selected group allows you to push user data to the resources with which that selected group is associated. Choose one of the two procedures below, depending on whether you want to consolidate an existing group or consolidate a missing group.

#### To consolidate an existing group:

1. From the web administration menu, click **Users & Groups**.
2. In the center of the page, select the **Groups** tab.

 **Tip:** You can also, from the web administration menu, click **Partitions** and then select **View Members** from the user partition's **Actions** menu. In the center of the page, select the **Groups** tab.

3. Next, do one of the following:
  - Select the group that you want to consolidate.
  - Use the **Search** box to find the group.
4. Click **Actions** next to the group you want to consolidate. From the **Actions** menu, click **Consolidate**.
5. On the **Consolidate** page, do the following:

- a. In the **Consolidate options** area, do the following:
  - i. **Optional** If you are consolidating an object in a synchronized user partition and you want to consolidate the selected object in OTDS with the identity provider, AD or LDAP, select **Consolidate with identity provider**.
  - ii. **Optional** If you want to direct OTDS to verify and repair a discrepancy in its internal referential integrity attributes, for example oTMember or oTMemberOf, select **Verify and repair**.

 **Note:** OpenText recommends that you do not perform the **Verify and repair** operation unless directed to by OpenText technical support.

- 
- b. If you are consolidating an object in a synchronized user partition, in the **Consolidate with the following resources** area, select all resources with which the previously selected object will be consolidated with information in OTDS.



**Note:** Consolidation operations may take a long time to complete. You can monitor the process through the “[directory-provenance.log](#)” on page 376 file.

- 
- 
- 
- 
- 
6. Click **Consolidate** to consolidate user data for the selected existing group across all selected resources.

#### To consolidate a missing group:

If you know of a group who should be present in OTDS but is not listed, you can consolidate that missing group as follows:

1. From the button bar, click **Consolidate**.
2. From the **Consolidate** menu, click **Consolidate Missing Group**.
3. In the **Account DN** box, enter the DN of the group.
4. Click **OK**.

### 7.3.8 Enabling two-factor authentication for a group

You can enable two-factor authentication for all users in a group. Look up the group for whose users you want to enable two-factor authentication, and then follow the instructions found in “[Enabling two-factor authentication](#)” on page 245.

### 7.3.9 Deleting groups

You can only delete groups from a non-synchronized user partition.

#### To delete groups in a non-synchronized user partition:

1. From the web administration menu, click **Users & Groups**.
  2. In the center of the page, select the **Groups** tab.
- 
- Tip:** You can also, from the web administration menu, click **Partitions** and then, from the non-synchronized user partition’s **Actions** menu, select **View Members**. Select the **Groups** tab.
3. Select the group that you want to delete, or use the **Search** box to find the group.
  4. Select the box to the left of the group you want to delete. Next, from the button bar, click **Delete**.
  5. Confirm that you want to delete this group by clicking **OK**.



**Note:** When you delete a group, you do not delete the users.

### 7.3.10 Editing organizational units

You can only edit organizational units from a non-synchronized user partition.

#### To edit organizational units in a non-synchronized user partition:

1. From the web administration menu, click **Partitions**, and then click the **Actions** link associated with the non-synchronized user partition whose organizational unit you want to edit.
2. From the **Actions** menu, select **View Members**.
3. Select the **Organizational Units** tab. Select the **Actions** link next to the organizational unit you want to edit. From the **Actions** menu, click **Properties**.
  - a. Follow the instructions, beginning with step 3, found in “[Creating an organizational unit in a non-synchronized user partition](#)” on page 122.
  - b. When you have finished editing, on the button bar, click **Save**.
4. **[Optional]** From the **Actions** menu associated with any organizational unit you want to edit, do the following:
  - If you want to consolidate this organizational unit, click **Consolidate**, and then follow the instructions for consolidating groups, beginning with step 5, found in “[Consolidating changes to users, groups, organizational units, and partitions](#)” on page 129.
  - If you want to edit administrators for this organizational unit, click **Edit Administrators**, and then see “[Editing administrators of organizational units in a non-synchronized user partition](#)” on page 123.
  - If you want to set two factor authentication for this organizational unit, click **Two Factor Auth Settings**, and then see “[Enabling two-factor authentication for an organizational unit](#)” on page 124.
  - If you want to delete this organizational unit, see “[Deleting organizational units in a non-synchronized user partition](#)” on page 124.

### 7.3.11 Editing administrators of organizational units

You can only edit administrators of organizational units from a non-synchronized user partition.

**To edit administrators of organizational units in a non-synchronized user partition:**

1. From the web administration menu, click **Partitions**, and then click the **Actions** link associated with the non-synchronized user partition whose administrators you want to edit.
2. From the non-synchronized user partition's **Actions** menu, select **View Members**.
3. Click the **Organizational Units** tab, and then click the **Actions** link next to the organizational unit you want to edit. From the **Actions** menu, click **Edit Administrators**.
4. Click **Add Administrator**. In the **Users and Groups Associations** box, use the **Search** box to find users or groups to add to the administrators. From the search results box, select the users or groups you want to designate as administrators, and then click **Add Selected**.



**Note:** For more information on delegated administration, see “[Delegated administration](#)” on page 251.

5. **[Optional]** If you want to remove a user or group from the administrators listed in the **Administrators** area:
  - a. Select the user or group you want to remove, and then click **Remove Administrator**.
  - b. Click **Delete** to confirm that you want to remove this administrator.



**Note:** When you remove a user or group as a member of the administrators, you do not delete the user or group.

### 7.3.12 Enabling two-factor authentication for an organizational unit

You can enable two-factor authentication for all users in an organizational unit. Look up the organizational unit for whose users you want to enable two-factor authentication, and then follow the instructions found in “[Enabling two-factor authentication](#)” on page 245.

### 7.3.13 Deleting organizational units

You can only delete organizational units from a non-synchronized user partition.

**To delete organizational units in a non-synchronized user partition:**

1. From the web administration menu, click **Partitions**, and then click the **Actions** link associated with the non-synchronized user partition whose organizational unit you want to delete.
2. From the **Actions** menu, select **View Members**.
3. Select the **Organizational Units** tab. Select the box to the left of the organizational unit you want to delete, and then, from the button bar, click **Delete**.
4. Confirm that you want to delete this organizational unit by clicking **OK**.



#### Caution

When you delete an organizational unit, all users and groups in the organizational unit will be deleted and removed from the resources with which they are associated.



**Tip:** If there are a large number of users and groups in an organizational unit, this action may take a long time. The **deleting** status indicator appears beside the organizational unit until the server has completed the operation. Click **Refresh** to determine if the server has completed the deletion.



# Chapter 8

## Application Roles

Directory Services supports the ability of an OpenText application to create and define application roles in OTDS. These application roles, if an OpenText application has created one, can be viewed on the **Application Roles** tab.

After an application role is created, you can assign it users, groups, and application roles. The role is an opportunity to identify rights, responsibilities, and permissions for those users and groups assigned to that role. The rights, responsibilities, and permissions are defined and managed in the OpenText application. The application, for example Process Suite, will create and manage the roles it requires. You can only assign users, groups, or roles to a role from within OTDS.

You can consult your OpenText application's documentation for information about whether that application supports creating and defining application roles in OTDS. Your application's documentation will also provide the specific information about the application roles it creates as well as their definition and impact.

OpenText applications will define an application role within non-synchronized user partitions. Application roles cannot be synchronized from external sources to a synchronized user partition.

### Application roles Actions menu options and buttons

On the main **Application Roles** page, each application role has an associated **Actions** menu and applicable buttons. The following are quick links to the procedures associated with each:

#### Application role Actions menu options

Actions menu option	Associated procedure
Properties	<a href="#">"Editing an application role" on page 263</a>
Edit Application Roles	<a href="#">"To assign users, groups, or application roles to an application role" on page 264</a>
View Effective Roles	<a href="#">"To view all application roles (recursively) assigned to a specific user, group, or application role" on page 266</a>
Edit Administrators	<a href="#">"To edit administrators of an application role" on page 266</a>
Two Factor Auth Settings	<a href="#">"To set two-factor authentication for an application role" on page 267</a>

### Users and groups buttons

Button	Associated Procedure
Assign Roles	<a href="#">"To assign users, groups, or application roles to an application role" on page 264</a>
Unassign Roles	<a href="#">"To assign users, groups, or application roles to an application role" on page 264</a>
Delete	<a href="#">"To delete an application role" on page 268</a>
Refresh	Use the Refresh button to verify if OTDS has completed an action. For example, after deleting.
Help	Opens context-sensitive help for the page you are currently using.

## 8.1 Application roles and custom attributes

You can create custom attributes for any existing application role. OTDS does not enforce any rules that have been defined by the OpenText product for any application role. It is entirely up to the application to define the requirements of its application roles. However, you can use any application role's custom attributes to contribute to the definition of that application role. For more information, see ["Editing an application role" on page 263](#).

## 8.2 Difference between application roles and access roles

Application roles are created and defined by an OpenText application. The OTDS administrator can then assign a user or a group to those application roles. If you do not see existing application roles in OTDS it is because your application has not yet created those application roles.

Access roles are created by the OTDS administrator. They define a partition, user, group, or organizational unit's access to a particular resource. For more information, see ["Access Roles" on page 229](#).

## 8.3 Defining application role attributes

The following table lists a partial set of attributes maintained by OTDS for application roles and their meaning:

Attribute	Meaning
cn	Group Name
description	Description
displayName	Display Name
notes	Notes

Attribute	Meaning
oTExternalID1	<rolename>
oTExternalID2	<rolename>@<user_partition>
oTExternalID3	<rolename>@<user_partition>
oTExternalID4	<rolename>@<user_partition>

## 8.4 Editing an application role

### To edit an application role:

- From the web administration menu, click **Application Roles**.



**Note:** Although you can create application roles yourself, OpenText does not advise you to do so unless directed by your OpenText application or by OpenText support. For more information, see “[To create an application role](#)” on page 267.

- From the **Actions** menu of the application role you want to edit, click **Properties**.
- On the **General** tab, do the following:
  - In the **Role Name** box, make any changes to the role's name. The **Role Name** box is mandatory.
  - Optional** In the **Display Name** box, you can optionally type the string that will be displayed in the UI for this application role.
  - Optional** In the **Description** box, you can optionally type a description of this application role.
  - Optional** In the **Notes** box, you can optionally type reference notes relating to this application role.
  - The **UUID** box cannot be edited. This box contains a string that is the internal ID of this application role.
  - On the button bar, click **Next**.
- Optional** On the **Role Attributes** page:
  - You can choose to specify any additional role attribute values. For information about role attributes, see “[Defining application role attributes](#)” on page 262.
  - On the button bar, click **Next**.
- Optional** On the **Custom Attributes** page, you can choose to specify any additional custom attribute values, or edit existing custom attributes.



**Note:** OpenText recommends that you do not create custom attributes. This option is intended for applications that integrate with OTDS to allow

them to store their application properties. For more information, see “[Application roles and custom attributes](#)” on page 262.

- a. Click **Add Custom Attribute**.
  - i. In the **Type** box, enter the type of custom attribute you are defining.
  - ii. In the **Name** box, enter a unique name for this custom attribute.
  - iii. In the **Value** box, if you require it, enter a value for your custom attribute.
  - iv. Click **Save** to the right of your custom attribute.
- b. To remove one or all custom attributes:



### Caution

There is no confirmation step. After you click either **Delete Selected Attributes** or **Clear all Attributes**, one specific, or all, custom attributes in this tab will be removed, depending on which remove action you selected. This action cannot be undone.

- i. If you want to remove *one* custom attribute, select the check box to the left of the custom attribute you want to remove, and then click **Delete Selected Attributes**.
  - ii. If you want to remove *all* custom attributes, click **Clear all Attributes**.
6. On the button bar, click **Save**.

## 8.5 To assign users, groups, or application roles to an application role

You can make this assignment in one of two different ways:

- If you want to first find the user, group, or application role you want to assign, follow this procedure: “[To find a user, group, or application role to assign to an application role](#)” on page 264.
- If you want to first find the application role and then add member(s) to it, follow this procedure: “[To find an application role and then assign it members](#)” on page 265.

If you want to remove a user, group, or application role from an application role, see “[To remove a user, group, or application role from an application role](#)” on page 265.

### To find a user, group, or application role to assign to an application role:

1. From the web administration menu:
  - a. If you want to find a user or group, click **Users & Groups**. Next click either the **Users** or **Groups** tab and scroll or use the search option to find the member you want.

- b. If you want to find an application role, click **Application Roles**.
2. From the **Actions** menu of the entity you want you want to add to an application role, click **Edit Application Roles**.
3. On the **Roles** tab, click the selection box to the left of the application role you want assigned to the user, group, or application role. Next, on the button bar, click **Assign Roles**.
4. In the **Member Selection** box, click all role(s) selection boxes to select all role(s) you want to add to this member.
5. On the button bar, click **Add Selected**.
6. When you have finished adding all role(s), click **Close**.
7. If you have finished, on the button bar click **Back**.

**To find an application role and then assign it members:**

1. From the web administration menu, click **Application Roles**.
2. From the **Actions** menu of the application role to which you want to add a user or group, click **Edit Application Roles**, and then do any of the following:
  - a. If you want to assign a user or a group to this application role, click the **Members** tab, and then do the following:
    - i. On the button bar click **Assign to Members**.
    - ii. In the **Member Selection** box, click all user(s) or group(s) selection boxes, the box to the left of the user or group name, to select all user(s) and/or group(s) you want to add to this application role.
    - iii. On the button bar, click **Add Selected**.
    - iv. When you have finished adding all user(s) and/or group(s), click **Close**.
  - b. If you want to add an application role to this application role, click the **Roles** tab, and then do the following:
    - i. On the button bar click **Assign Roles**.
    - ii. In the **Member Selection** box, click all role(s) selection boxes, the box to the left of the application role name, to select all role(s) you want to add to this application role.
    - iii. On the button bar, click **Add Selected**.
    - iv. When you have finished adding all role(s), click **Close**.
3. If you have finished, on the button bar click **Back**.

**To remove a user, group, or application role from an application role**

1. From the web administration menu, click **Application Roles**.

2. From the **Actions** menu of the application role from which you want to remove a user or group or application role, click **Edit Application Roles**.
3. If you want to remove a user or group, click the **Members** tab, and then do the following:
  - a. Click the box to the left of the user or group name that you want to remove, and then, on the button bar, click **Remove from Members**.
  - b. Confirm that you want to remove these user(s) and/or group(s) from the application role, and then click **Delete**.
4. If you want to remove an application role, click the **Roles** tab, and then do the following:
  - a. Click the box to the left of the role name that you want to remove, and then, on the button bar, click **Unassign Roles**.
  - b. Confirm that you want to remove these role(s) from the application role, and then click **Delete**.

## **8.6 To view all application roles (recursively) assigned to a specific user, group, or application role**

**To view all application roles (recursively) assigned to a specific user, group, or application role:**

1. Find the user, group, or application role for which you wish to view effective roles.
2. From that items **Actions** menu, click **View Effective Roles**.
3. If you have finished viewing this application role's recursive items, on the button bar click **Back**.

## **8.7 To edit administrators of an application role**

**To edit administrators of an application role:**

1. From the web administration menu, click **Application Roles**.
2. From the **Actions** menu of the application role whose administrators you want to edit, click **Edit Administrators**.
3. If you want to add an administrator to this application role:
  - a. On the button bar click **Add Administrators**.
  - b. In the **Member Selection** box, click all user(s) or group(s) selection boxes, the box to the left of the user or group name, to select all member you want to add as administrator to this application role.

- c. On the button bar, click **Add Selected**.
4. If you want to remove an administrator from this application role:
  - a. Click the box to the left of each user or group name that you want to remove, and then, on the button bar, click **Remove Administrator**.
  - b. Confirm that you want to remove these members from the application role, and then click **Delete**.
5. When you have finished adding or removing all members, on the button bar click **Back**.

## 8.8 To set two-factor authentication for an application role

### To set two-factor authentication for an application role

1. From the web administration menu, click **Application Roles**.
2. From the **Actions** menu of the application role whose administrators you want to edit, click **Two Factor Auth Settings**.
3. In the **Two Factor Authentication Settings - <item\_name>** box, from the **Two Factor Authentication Settings** list, select either **Inherit settings** or **Define settings**, and then, do the following:
  - a. If you select **Inherit settings**, and two-factor authentication has not been enabled for the parent object or in the *global settings* box, two-factor authentication will not be enabled.  
The **Two Factor Authentication Settings** box will display, dimmed, the inherited settings that will be applied. If these are not the settings you want applied, change your selection above to **Define settings** to make changes.
  - b. If you select **Define settings**, select any of the options to apply two-factor authentication settings. For more information, see "[Configuring two-factor authentication](#)" on page 237.
  - c. Click **OK**.

## 8.9 To create an application role

### To create an application role:

1. From the web administration menu, click **Partitions**.
2. From the **Actions** menu of the non-synchronized user partition for which you want to create an application role, click **View Members**.
3. On the button bar, from the **Add** menu, click **New Role**.
4. Next, follow the information found in "[Editing an application role](#)" on page 263.

## 8.10 To delete an application role

### To delete an application role:

1. From the web administration menu, click **Application Roles**.
2. Click the box to the left of each application role that you want to remove, and then, on the button bar, click **Delete**.
3. Confirm that you want to remove these members from the application role, and then click **OK**.

# Chapter 9

## Recycle Bin

The **Recycle Bin** page displays all deleted users and deleted groups across all partitions. You can view details such as the user partition of a deleted user or group. You can also view the location, in OTDS, of the deleted user or group. The search function allows you to display a specific number of either deleted users or deleted groups that match your search criteria.

You can configure automatic delete for the users and groups stored in recycle bin to ensure they are ultimately deleted, and to manage the amount of storage being used. For more information, see “[Recycle bin settings](#)” on page 271. You can also manually delete users and groups on the **Recycle Bin** page.

 **Note:** Directory Services searches only attributes related to the user's identifier and name.

### Recycle bin and synchronized user partitions

You can choose to enable the option to recycle members in a synchronized user partition. When enabled, when a user or group is deleted from the identity provider, or is otherwise moved out of the scope of a synchronized user partition, and that deletion or change is propagated to OTDS, that member will be moved, by OTDS, to recycle bin.

You can manually select that user or group to be restored to their original partition from the **Recycle Bin** page. After that member has been restored, and the original problem that caused their deletion from the identity provider is corrected, you can consolidate to bring the member back to their current state with the identity provider. For more information about consolidation, see “[Consolidating users and groups in Partitions](#)” on page 128.

 **Note:** If OTDS, through monitoring or consolidation, detects a change on the identity provider that causes OTDS to add a user or group back to OTDS, then that member in recycle bin will be restored automatically.

However, if a user or group is manually restored from recycle bin by the OTDS administrator, without any commensurate change on the identity provider, that user or group will, again, be removed from the partition the next time a consolidation on that partition is performed.

### Recycle bin buttons

On the main **Recycle Bin** page, each user or group has buttons on the button bar specific to this page. The following are quick links to the procedures associated with each:

### Recycle bin buttons

Button	Associated procedure
Recycle Bin Properties	<a href="#">"Recycle bin settings" on page 271</a>
Restore by Search Criteria	<a href="#">"Manually restoring users and groups from the recycle bin" on page 272</a>
Restore Selected	<a href="#">"Manually restoring users and groups from the recycle bin" on page 272</a>
Delete by Search Criteria	<a href="#">"Manually deleting users and groups from the recycle bin" on page 273</a>
Delete Selected	<a href="#">"Manually deleting users and groups from the recycle bin" on page 273</a>
Refresh	Used to verify if OTDS has completed an action. For example, after deleting or after consolidating.
Help	Opens the context-sensitive help for the page you are currently using.

### When viewing users and groups in the recycle bin

The following information is available for all users and groups that have been moved to the recycle bin:

- User or group name.
- User or group ID.
- The display name for the user or group.
- The name of the user partition from which the user or group was moved to the recycle bin.
- The location of the user or group within the partition.
- The date and time that the user or group was moved to the recycle bin.

## 9.1 Viewing recycle bin users, groups, or roles

### To view recycle bin users, groups, or roles:

1. From the web administration menu, click **Recycle Bin**.
2. Do one of the following:
  - If you want to view the users that have been deleted from OTDS and are now stored in recycle bin, click the **Users** tab.
  - If you want to view the groups that have been deleted from OTDS and are now stored in recycle bin, click the **Groups** tab.
  - If you want to view the roles that have been deleted from OTDS and are now stored in recycle bin, click the **Roles** tab.
3. **[Optional]** On the button bar, you can click **Refresh**, to refresh the list on the **Recycle Bin** page.

4. **Optional** You can use the search area to filter the results displayed. You can choose to enter values to any one or all of the following text boxes to narrow the search criteria:
  - a. **Starts with/Contains:** begin by selecting one of the buttons. Next, in the text box, type the search criteria.
  - b. **Start Date:** click in the text box to open the calendar, and then select a date. The search will then only display results that were added to recycle bin on or after that date.
  - c. **End Date:** click in the text box to open the calendar, and then select a date. The search will then only display results that were added to recycle bin before or on that date.
  - d. **Partition:** click in the text box and begin typing the partition name. As you type the partition names matching your text will appear. Choose the partition from the list. The search will then only display results that were added to recycle bin from that partition.
  - e. Click **Search**.

## 9.2 Recycle bin settings

### To configure recycle bin settings:

1. From the web administration menu, click **Recycle Bin**.
2. On the **Recycle Bin** page, on the button bar, click **Recycle Bin Properties**.
3. In the **Recycle Bin Properties** dialog box:
  - a. **Optional** If you want OTDS to move users and groups deleted from synchronized partitions automatically to recycle bin, select **Recycle members deleted in sync partitions**.
  - b. **Optional** If you want OTDS to move users and groups deleted from non-synchronized partitions automatically to recycle bin, select **Recycle members deleted in non-sync partitions**.
  - c. **Optional** If, when a user or group is selected to be restored from recycle bin, and OTDS sees an existing, identical user or group in that partition, you want the existing user or group over-written, select **Replace existing members on restore**.  
If you do not want OTDS to over-write existing users and groups when restoring from recycle bin, leave this check box cleared.
  - d. **Optional** If you want OTDS to automatically delete users and groups stored in recycle bin, select **Automatically delete recycled members**. If you choose to select auto delete, you must set the following:
    - i. In the **Retention lifetime (days)** text box, type a positive integer representing the number of days after which users and groups stored in recycle bin will be deleted.

- ii. In the **Deletion interval (hours)** text box, type a positive integer representing the number of hours that will elapse between maintenance activity on the recycle bin.
- iii. Click **OK**.

## 9.3 Manually restoring users and groups from the recycle bin

**To manually restore users and groups from the recycle bin:**

1. From the web administration menu, click **Recycle Bin**.
2. On the **Recycle Bin** page, if you want to restore users from recycle bin, click the **Users** tab. If you want to restore groups from recycle bin, click the **Groups** tab. If you want to restore access roles from recycle bin, click the **Roles** tab.
3. Next, do one of the following:
  - If you want to restore a few objects, find the objects that you want to restore to OTDS.  
Click the select box to the left of each user, group, or role you want to restore, and then, on the button bar, click **Restore Selected**.
  - If you want to restore many objects, use the search bar and type or click any of the search parameters to list those users, groups, or roles. You can select from **Start Date**, **End Date**, **Partitions**, **Starts with**, or **Contains**.  
After you click **Search**, the users, groups, or roles matching your search query will be displayed. On the button bar, do one of the following:
    - If you want to restore all objects that match the search criteria you input above, click **Restore by Search Criteria**.
    - If you want to restore selected objects from the search display, click to select each object you want to restore, and then click **Restore Selected**.

4. Click **OK** to confirm the restore.



**Note:** It is the case that, if a user or group is manually restored from recycle bin by the OTDS administrator, without any commensurate change on the identity provider, that object will, again, be removed from the partition the next time a consolidation on that partition is performed.

Therefore, if the condition that caused an undesired deletion is corrected on the identity provider, you can proceed to consolidate. However, if the condition still exists on the identity provider, consolidation will result in the user or group being deleted again.

5. **Optional** If you want to consolidate, then on the web administration menu, click **Partitions**. On the **Partitions** page:
  - a. Find the partition to which you have just restored the user or group.



**Note:** If you do not want to consolidate the entire partition, you can choose to consolidate specific users or groups. For more information, see “[Consolidating users](#)” on page 243 or “[Consolidating groups](#)” on page 255.

- b. From the **Actions** menu of the partition to which you have just restored the user or group, click **Consolidate**.
- c. In the **Consolidate <partition\_name>** dialog box, click **Consolidate**.
- d. Wait until the consolidate operation has completed. You can view the progress of the consolidate operation on the “[Jobs](#)” on page 363 page.

Next, on the **Partitions** page, from the **Actions** menu of the partition you have just consolidated, click **View Members**.

Examine the **Users** tab and the **Groups** tab to confirm that the user or group you restored has been recreated in the partition.

## 9.4 Manually deleting users and groups from the recycle bin

### To manually delete users and groups from the recycle bin:

1. From the web administration menu, click **Recycle Bin**.
2. On the **Recycle Bin** page, if you want to delete users from recycle bin, click the **Users** tab. If you want to delete groups from recycle bin, click the **Groups** tab.
3. Next, do one of the following:
  - If you want to delete a few users or groups, find the users or groups that you want to delete from Recycle Bin.  
Click the select box to the left of each user or group you want to delete, and then, on the button bar, click **Delete Selected**.
  - If you want to delete many users or groups, use the search bar and type or click any of the search parameters to list those users or groups. You can select from **Start Date**, **End Date**, **Partitions**, **Starts with**, or **Contains**.  
After you click **Search**, the users or groups matching your search query will be displayed. On the button bar, do one of the following:
    - If you want to delete all users or groups that match the search criteria you input above, click **Delete by Search Criteria** to delete all users or groups in the search display.
    - If you want to delete selected users or groups from the search display, click to select each user or group you want to delete, and then click **Delete Selected**.
4. Click **OK** to confirm the deletion.



**Note:** You do not need to consolidate to propagate the deletion. After you click **OK** these users or groups are removed from recycle bin. Further,

provided the **Delete users and groups** option was enabled when the resource was created, these users or groups will now be deleted from any resources, for example from OpenText Content Management, with which those users or groups were synchronized.

## Chapter 10

# OAuth Clients

OTDS has implemented an OAuth 2.0 authorization server functionality. To use OAuth 2.0 with OTDS you must register an OAuth client in OTDS. In the Directory Services **OAuth Clients** tab you can register your OAuth clients in OTDS.

This section describes registering OAuth clients in OTDS for the purpose of using an OAuth 2.0-based integration with OTDS. When creating an OAuth client:

- You need to decide if this OAuth client will be public or confidential.  
You make this choice on the **General** page when you create your OAuth client by selecting or clearing **Confidential**.
- You need to set the valid, registered URLs associated with the OAuth client.  
You can specify a Regular Expression, regex, in the **Redirect URL** text box. If not using a regular expression, the configured value is treated as a prefix for string comparison. You can see examples of the types of entries you can make to this text box in “[Customizing trusted referrals](#)” on page 328.



**Note:** The secret key for a confidential OAuth client is only revealed when the OAuth client is created. To reset the secret key of a confidential client, do one of the following:

- Delete the OAuth client and then recreate it.
- Edit the OAuth client, change it to a public client by clearing the **Confidential** check box, and then save the OAuth client. Next, edit the OAuth client again, select the **Confidential** check box, and then save the OAuth client.

## OAuth clients and single sign out

When implementing single sign out for OTDS and OAuth clients, the OAuth client documentation will provide the information required by OTDS’ **Sign out URL** and **Sign out Method** text boxes. For more information about single sign out in OTDS, see “[Single sign out](#)” on page 351.

## OAuth clients Actions menu options and buttons

On the main **OAuth Clients** page, each OAuth client has an associated **Actions** menu and applicable buttons. The following are quick links to the procedures associated with each:

**OAuth clients menu options**

<b>Actions menu option</b>	<b>Associated procedure</b>
Properties	"Editing an OAuth client" on page 279

**OAuth clients buttons**

<b>Button</b>	<b>Associated procedure</b>
Add	"Creating an OAuth client" on page 276
Delete	"Deleting an OAuth client" on page 280
Refresh	Verifies if OTDS has completed an action. For example, after deleting.
Help	Opens context-sensitive help for the page you are currently using.

## 10.1 Creating an OAuth client

**To create an OAuth client:**

1. From the web administration menu, click **OAuth Clients**.
2. From the button bar, click **Add**. The **New OAuth client** wizard will guide you through the steps.
3. On the **General** page, do the following:
  - a. In the **Client ID** text box, type a unique name for your new OAuth client. The client ID text box is mandatory.
  - b. **Optional** In the **Display Name** box, you can type a more descriptive display name for this OAuth client.
  - c. **Optional** In the **Description** box, you can type a description of this OAuth client.
  - d. **Optional** You can select **Disabled** if you want to ensure this OAuth client is not active.
  - e. **Optional** You can select **Confidential** to create a confidential client. A confidential client must be able to securely maintain a client secret.
  - f. From the **Authentication Method** list, if you selected **Confidential** in step 3.e, you must select your preferred authentication method. Select one of:
    - Client Secret
    - Symmetric JWT
    - Asymmetric JWT
    - mTLSIf you select **mTLS**, you must also define one of the following custom attributes on the OAuth client:
    - `tls_client_auth_subject_dn`

- `tls_client_auth_san_dns`
- `tls_client_auth_san_uri`
- `tls_client_auth_san_ip`
- `tls_client_auth_san_email`

For more information about defining a custom attribute, see [step 7](#).

- g. In the **Public Key(s)/Certificate(s)** box, if you selected **Confidential** in [step 3.e](#) and either **Asymmetric JWT** or **mTLS** in [step 3.f](#), you must type or paste your public key or certificate.
- h. **Optional** In the **Sign out URL** text box, if you want to implement OTDS' single sign out functionality, you must enter a value in this text box and the next text box.  
The value you type to this text box is supplied in the documentation for the product for which this OAuth client is being created.
- i. **Optional** From the **Sign out Method** list, if you want to implement OTDS' single sign out functionality, you must enter a value in this text box and the previous text box.  
The value you type to this text box is supplied in the documentation for the product for which this OAuth client is being created.
- j. If you have finished creating your OAuth client, click **Save**, otherwise, click **Next**.

4. **Optional** On the **User Partition** page, do the following:
  - a. You can choose to restrict authentication through this new OAuth client to users within a specific user partition. To do this, select **User Partition**, and then type the name of the user partition whose users will be allowed to authenticate through this OAuth client.  
When you begin typing, an alphabetical list of user partitions that begin with the first letter you type will appear, and you can select the user partition from that list.
  - b. If you select **Global**, no restrictions will be applied.
  - c. If you have finished creating your OAuth client, click **Save**, otherwise, click **Next**.

5. **Optional** On the **Advanced** page, do the following:
  - a. If you want to allow this OAuth client to be able to obtain a refresh token, select **Grant refresh token (when protocol permits)**.
  - b. If you selected the **Grant refresh token** box, you can also choose to force the lifetime of the refresh token to be limited to the lifetime of the session that OTDS establishes with the browser used by the user to authenticate, by selecting **Use session lifetime as refresh token lifetime**.



**Note:** The OTDS session is controlled by the [http.cookie](#) on page 140 authentication handler.

- c. If you want to specify a limit, in seconds, for the access token lifetime, enter a positive integer in the **Access token lifetime (seconds)** text box. The default is 3600, or 1 hour.
  - d. A refresh token can be used to request a new access token when the application needs it. The refresh token lifetime is infinite by default.  
If you want to set a limit, in seconds, for the lifetime of the refresh token, enter a positive integer in the **Refresh token lifetime (seconds)** text box. This text box will be unavailable if you selected **Use session lifetime as refresh token lifetime** above.
  - e. In the **Permissible scopes** text box, you can choose to define application-specific scopes, unknown to OTDS, that this client can request.
    - i. To add a permissible scope to this OAuth client:
      - A. In the **Permissible scopes** area, click **Add/Delete**.
      - B. In the **Permissible scopes** text box, type the new scope and then click **Add**
      - C. After you have finished adding all your permissible scopes, click **Save**.
    - ii. To delete a permissible scope from this OAuth client:
      - A. In the **Permissible scopes** area, click **Add/Delete**.
      - B. In the **Permissible scopes** dialog box, in the **Permissible scopes** area, click the select box to the left of the scope you want to delete, and then click **Delete Selected**  
 **Note:** There is no confirmation step. After you click **Delete Selected** the scope is removed.
      - C. After you have finished deleting your permissible scopes, click **Save**.
  - f. If you have finished creating your OAuth client, click **Save**, otherwise, click **Next**.
6. On the **Redirect URLs** page, do the following:
    - a. To add a redirect URL from this OAuth client:
      - i. On the button bar click **Add**.
      - ii. In the **Redirect URLs** text box, type either the URL or the regular expression to be associated with this client, and then click **Save** to the right of the new URL. An example of a redirect URL you can enter:  
`https://mysite.com/oauth2`  
Further examples can be found in “[Customizing trusted referrals](#)” [on page 328](#).
    - b. To delete a redirect URL from this OAuth client:
      - i. Click the select box to the left of the redirect URL you want to delete.

- ii. On the **Redirect URL** button bar, click **Delete**.
7. On the **Custom Attributes** page, if you want to add a custom attribute, do the following:
  - a. Click the **Add Custom Attribute** button.
  - b. Type your required text in the fields for **Type**, **Name**, and **Value**.
  - c. Click **Save**.

 **Tip:** You can delete any one attribute by clicking that attribute's select box and then clicking the **Delete Selected Attributes** button.  
To delete all custom attributes, click the **Clear All Attributes** button.  
There is no confirmation step, once you click either of these buttons, your attribute, or all attributes, are removed.

 **Note:** If you selected **mTLS** in [step 3.f](#), you must create one custom attribute. See [step 3.f](#) for more information.
8. On the button bar, click **Save**.

## 10.2 Editing an OAuth client

### To edit an OAuth client:

1. From the web administration menu, click **OAuth Clients**.
2. From the **Actions** menu of the OAuth client you want to edit, click **Properties**.
3. You can view descriptions of the text boxes you can edit in the “[Creating an OAuth client](#)” on page 276 procedure.
4. Click **Save**.

## 10.3 Editing impersonation settings

### To edit impersonation settings:

 **Note:** You can edit impersonation settings for a resource or for an OAuth client.

1. From the web administration menu, do one of the following:
  - To edit impersonation settings for a resource, click **Resources**. From your resource's **Actions** menu, click **Impersonation Settings**.
  - To edit impersonation settings for a resource, click **OAuth Client**. From your OAuth client's **Actions** menu, click **Impersonation Settings**.
2. On the **Impersonation Settings** page, select **Allow this resource/client to impersonate users**. For more information, see “[Using impersonation](#)” on page 224.

3. Optional If you want to restrict impersonation tokens to apply only to defined resources, select the box next to each resource.
4. Click **OK** to apply your impersonation settings.

## 10.4 Deleting an OAuth client

**To delete an OAuth client:**

1. From the web administration menu, click **OAuth Clients**.



### Caution

Deleting an OAuth client cannot be undone.

2. Click the select box to the left of the OAuth client you want to delete, and then, on the button bar, click **Delete**.
3. In the **Delete** dialog box, click **OK** to confirm or click **Cancel** to keep the OAuth client.

# Chapter 11

## External Import

Directory Services provides the **External Import** tab in OTDS to create and configure external import.

To view the **External Import** tab in OTDS, you must enable the external import system attribute. For more information, see [“Enabling the external import tab” on page 283](#).

You can choose to create an import unit that reads and imports from a database or an import unit that reads and imports from an XML file.

### External import Actions menu options and buttons

On the main **External Import** page, each external import has an associated **Actions** menu and applicable buttons. The following are quick links to the procedures associated with each:

#### External import Actions menu options

Actions menu option	Associated procedure
Properties	<a href="#">“Editing an external import” on page 285</a>
Import to Partition	<a href="#">“Beginning an external import” on page 285</a>

#### External import buttons

Button	Associated procedure
Add	<a href="#">“Creating an external import” on page 283</a>
Delete	<a href="#">“Deleting an external import” on page 286</a>
Refresh	Verifies if OTDS has completed an action. For example, after deleting or after consolidating.
Help	Opens context-sensitive help for the page you are currently using.

## 11.1 XML file example

If you intend to import from an XML file, the following example shows the format your XML file might follow:

```
<?xml version="1.0" encoding="UTF-8"?>

<migration-data>

  <users>

    <user-data>
      <cn>jamesgrey</cn>
      <first_name>James</first_name>
      <last_name>Grey</last_name>
      <email>jamesgrey@company.com</email>
      <full_name>James Grey</full_name>
      <userpwd>!jamesgrey!</userpwd>
    </user-data>

    <user-data>
      <cn>jacquesgris</cn>
      <first_name>Jacques</first_name>
      <last_name>Gris</last_name>
      <email>jacquesgris@company.com</email>
      <full_name>Jacques Gris</full_name>
      <userpwd>@jacquesgris@</userpwd>
    </user-data>

    <user-data>
      <cn>hamishglas</cn>
      <first_name>Hamish</first_name>
      <last_name>Glas</last_name>
      <email>hamishglas@company.com</email>
      <full_name>Hamish Glas</full_name>
    </user-data>

  </users>

  <groups>

    <group-data>
      <groupcn>Arran</groupcn>
      <groupname>Arran</groupname>
    </group-data>

    <group-data>
      <groupcn>Bute</groupcn>
      <groupname>Bute</groupname>
    </group-data>

    <group-data>
      <groupcn>Cava</groupcn>
      <groupname>Cava</groupname>
    </group-data>

  </groups>

  <associations>
    <member CHILDID="jamesgrey" ID="Arran"/>
    <member CHILDID="jacquesgris" ID="Bute"/>
    <member CHILDID="hamishglas" ID="Cava"/>
    <member CHILDID="Arran" ID="Bute" GROUP="true"/>
  </associations>

</migration-data>
```

## 11.2 Enabling the external import tab

### To enable the external import tab:

1. From the web administration menu, select the **System Attributes** tab.
2. Click the `directory.config.EnableImportSource` system attribute, and then type `true` in the **Value** box.
3. Click **Save**.
4. Refresh your browser page. You can now see the **External Import** tab in the **Setup** menu.

## 11.3 Creating an external import

### To create an external import:

1. From the web administration menu, click **External Import**.
2. From the button bar, click **Add**. The **New External Import** wizard will guide you through the steps.
3. On the **Information** page, do the following:
  - a. In the **Name** box, type a unique name for your new external import. The **Name** box is mandatory.
  - b. **Optional** In the **Description** box, you can optionally type a description of this external import.
  - c. From the **Import Source** list, select either **Import from Database** or **Import from XML File**.
  - d. From the **Target Partition** list, select the partition to which you will be importing.
  - e. **Optional** Select **Start importing...** if you want to begin importing users and groups immediately. To import the data at a later date, see “[Beginning an external import](#)” on page 285.
  - f. Click **Next**.
4. Depending on the selection you made from the **Import Source** list on the previous page, when you click **Next** you will either see the **Database Information** or the **XML Information** page.
  - a. If you selected **Import from Database**, then on the **Database Information** page:
    - i. In the **Database Server Type** list, select your database application.
    - ii. In the **Database Server** box, type the fully qualified domain name of the server on which your database is installed.
    - iii. In the **Database Port** box, type the port number on which the database listens.

- iv. In the **Database Username** box, type the name of the user with administrative access to the database.
  - v. In the **Database Password** box, type the password for the user with administrative access to the database.
  - vi. In the **Database Name** box, type the name of the database from which you will be importing.

If you selected “Oracle” from the **Server Type** list, then you need to enter the Oracle server SID or service name in this box.
  - vii. **Optional** If you want to test that you have entered the data correctly on the **Database Information** page, click **Test Database Connection**.
- b. If you selected **Import from XML**, then on the **XML Information** page:
    - i. In the **XML File Path on Server** box, type the full path name and file name of the XML file. “C:\xml\_import\xml\_testfile.xml” is an example of a valid path name and file name. For an example of a valid XML file, see “[XML file example](#)” on page 282.
    - ii. Or, in the **Upload an XML File** box, browse to select an external XML file. The file cannot be empty, or be more than 16MB.
    - iii. You can optionally choose to have OTDS run a test on the XML file by clicking **Test XML Configuration**. After the test completes, read the information message then close it. If any configuration issues were discovered, you will need to fix them in your XML file before continuing.
- c. If you have finished creating your external import, click **Save**, otherwise, click **Next**.
5. On the **User Mappings** page, do the following:
    - a. If you are in the process of creating an external import from database, you will see the **Select Users SQL** box. In this box you must type the SQL statement for the users' import. After you have correctly typed your SQL statement, click **Populate Columns**.

If you are in the process of creating an external import from an XML file, OTDS populates the columns automatically.
    - b. You will see a table called **Mandatory OTDS Attribute**. Each attribute in this table must be mapped.
    - c. You can optionally map any other OTDS attribute listed in the **Optional OTDS Attribute** table.
    - d. If you have finished creating your external import, click **Save**, otherwise, click **Next**.
6. On the **Group Mappings** page, do the following:
    - a. If you are in the process of creating an external import from database, you will see the **Select Groups SQL** box. In this box you must type the SQL statement for the groups import. After you have correctly typed your SQL statement, click **Populate Columns**.

If you are in the process of creating an external import from an XML file, OTDS populates the columns automatically.

- b. You will see a table called **Mandatory OTDS Attribute**. Each attribute in this table must be mapped.
  - c. You can optionally map any other OTDS attribute listed in the **Optional OTDS Attribute** table.
  - d. If you have finished creating your external import, click **Save**, otherwise, click **Next**.
7. On the **Membership Mappings** page, do the following:
- a. If you are in the process of creating an external import from database, you will see the **Select Membership Mappings SQL** box. In this box you must type the SQL statement for the membership import. After you have correctly typed your SQL statement, click **Populate Columns**.  
If you are in the process of creating an external import from an XML file, OTDS populates the columns automatically.
  - b. You will see a table called **Mandatory OTDS Attribute**. Each attribute in this table must be mapped.
8. Click **Save**.

## 11.4 Editing an external import

### To edit an external import:

1. From the web administration menu, click **External Import**.
2. From the **Actions** menu of the import you want to edit, click **Properties**. The **Edit Import** wizard will guide you through the steps to edit an existing authentication handler.
3. You can view descriptions of the boxes you can edit in the “[Creating an external import](#)” on page 283.
4. Click **Save**.

## 11.5 Beginning an external import

### To begin an external import:

1. From the web administration menu, click **External Import**.
2. From the **Actions** menu of the import you want to start, click **Import to Partition**. This may take some time. Wait until the information message appears, read it, then close it.

## 11.6 Deleting an external import

**To delete an external import:**

1. From the web administration menu, click **External Import**.



**Caution**

Deleting an external import cannot be undone.

2. Select the box to the left of the import you want to delete, and then, on the button bar, click **Delete**.
3. In the **Delete** box, click **OK** to confirm or click **Cancel** to keep the import.

# Chapter 12

## System Config

The **System Config** menu option allows the administrator to configure the settings for SMTP, OTDS notifications, and system attributes. You can configure notifications for OTDS specific information and for license-key specific information. There are three tabs on which you need to enter information:

The **System Config** menu option allows the administrator to configure the settings for system attributes. There is one tab on which you need to enter information:

- “[System Attributes](#)” on page 288: where you set the OTDS system attributes. Prior to the 16.2.2 release, the system attributes were available from the **Setup** menu.
- “[SMTP Settings](#)” on page 318: where you set the server information for the SMTP server that OTDS will use to send the notifications. In addition to notifications, these SMTP settings will be used for OTDS emails related to account sign-up and password reset.
- “[Audit/Reporting Settings](#)” on page 319: where you can choose to enable auditing of OTDS operations in order to generate reports.
- “[Notifications Settings](#)” on page 320: where you can choose to enable OTDS-specific notifications and/or license key-specific notifications, and enter the email addresses to be notified. On this page you also choose the type and level of event that generates a notification email, as well as the frequency of the email notifications and the default language.



**Note:** If your environment has multiple OTDS server nodes, any configuration changes to “[Authentication Handlers](#)”, “[Trusted Sites](#)”, or “[System Config](#)” can take up to one minute to take effect across all OTDS server nodes.

### System Config buttons

On the main **System Config** page, there are buttons on the button bar specific to this page. The following are quick links to the procedures associated with each:

Button	Associated procedure
Add Attribute	“ <a href="#">Adding a system attribute</a> ” on page 316
Delete	“ <a href="#">Deleting a system attribute</a> ” on page 318
Save	“ <a href="#">To configure SMTP settings</a> ” on page 318 and “ <a href="#">Notifications Settings</a> ” on page 320
Refresh	Verifies if OTDS has completed an action. For example, after deleting.
Help	Opens context-sensitive help for the page you are currently using.

## 12.1 System Attributes

This section describes using the Directory Services system attributes. The OTDS system attributes are stored in the database you set up when you installed OTDS. Because of this, when you change a system attribute on any installation, that change is replicated across all OTDS installations.

The **System Attributes** page displays a list of default OTDS attributes that ship with the product. You can edit these attributes and add new attributes.



### Caution

OpenText recommends that you use extreme caution when modifying the system attributes. Improper or inaccurate changes to these attributes can negatively impact your entire OTDS environment.

The system attributes located on the **System Attributes** tab apply to all partitions in the system. You can also create custom, partition attributes that only affect the behavior for users and groups in one partition. For more information, see “[Partition attributes](#)” on page 132.

### Display status of system attributes

The system attributes in “[List of supported system attributes](#)” on page 288 are those attributes supported by OTDS. Not all supported system attributes appear in the UI, by default. Some supported attributes must be manually added to the **System Attributes** list. For more information, see “[Adding a system attribute](#)” on page 316.

If you are patching a previous version of OTDS, system attributes that are new in that patch will not display by default.

### 12.1.1 List of supported system attributes

---

#### Account Creation Notification Enabled

- **Name:** directory.system.AccountCreationNotificationEnabled
- **Description:** set this system attribute on a non-synchronized partition to true if you want OTDS to send an email to a user when an account is created for them in that non-synchronized user partition. This attribute needs to be set as a partition system attribute, for more information see, “[System attributes](#)” on page 132.
- **Default Value:** false

---

#### Additional Signup Attributes

- **Name:** directory.auth.SignupAttributes
- **Description:** a list of user attributes that define additional information you can collect on the **Sign up** page. These attributes contain the mappings

between attribute display names and their associated OTDS attributes. For these attributes to appear, you must first have configured [Enable Self-Provisioning of Accounts on page 300](#).

The format is the following: attribute1=Display\_Name\_1 | attribute2=Display\_Name\_2 | attribute3=Display\_Name\_3\*

- A pipe character, |, is used to separate mappings.
- An equal character, =, is used to separate the attribute name from the display name.
- If you want any sign up box to be a required box, you must append an asterisk character, \*, to that box. If there is no asterisk character, the sign up box is treated as optional.

#### **Example:**

1. initials=Middle Initial(s)|gender=Gender\*|birthDate=Date of Birth

2. oTTelephoneNumber=Phone Number\*|oTFacsimileTelephoneNumber=Fax Number

3. title=Position|oTDepartment=Department|oTCompany=Organization\*|oTIndustry=Industry

4. physicalDeliveryOfficeName=Office|street=Street

5. l=City|st=State/Province|postalCode=ZIP/Postal Code\*|co=Country\*

6. preferredLanguage=Language\*

If you need multilingual support:

1. For *each* language you want to support, create a login\_custom\_<xy>.properties file in the <OTDS\_home>/otdsws/WEB-INF/classes directory, where <xy> is two letters representing the language. For example, when implementing support for German, create a login\_custom\_de.properties file.

When creating the login\_custom\_<xy>.properties file, follow the same file name conventions as for the OTDS login.properties file, found in the same directory.

2. For the attribute display name, type “prompt.<attribute\_name>” without the quote marks. For example, type prompt.initials.

The format of the login\_<custom>.properties file should be:  
prompt.<attribute\_name>=<display\_name>. For example: prompt.initials=Initials

3. Restart Tomcat.

- **Default Value:** null
- **Requirements:** if you create a login\_custom\_<xy>.properties file, you must restart Tomcat.

### Allow Non-Admin UI Access

- **Name:** directory.auth.AllowNonAdminUIAccess
- **Description:** when this attribute is set to “false”, the default, non-admin users will get the message “Access Denied” when attempting to access the OTDS web administration page. Only members of `otadmin`, `otdsreadonlyadmins`, and `otdsbusinessadmins` are still allowed access.  
When this attribute is set to true, all users will be able to access the OTDS web administration page. Users who are not members of `otadmin`, `otdsreadonlyadmins`, or `otdsbusinessadmins` will have a restricted view of the administration page that only shows the **Users & Groups** page. When these non-admin users have this access, they cannot see any other OTDS object and they cannot modify users or groups.
- **Default Value:** false

---

### Allowed Email Domains

- **Name:** directory.auth.AllowedEmailDomains
- **Description:** a comma separated list of email domains that will be accepted for self-provisioning of accounts. All email domains are accepted by default.
- **Default Value:** null

---

### Authentication Service Principal Name

- **Name:** `otds.as.spn`
- **Description:** the Kerberos service principal name that OTDS will use. By default, this is determined dynamically and does not need to be configured. The value is automatically determined by OTDS. You only need to set this if users are connecting to a load balancer in front of multiple OTDS instances. For more information, see “[Single sign on issues](#)” on page 403.  
OTDS does not require Kerberos delegation functionality. Kerberos is only used to authenticate users directly with OTDS through its service principal name. Once Kerberos-based SSO occurs on OTDS, the application session takes over and Kerberos is no longer used. Therefore, the Windows account under which OTDS is running can be configured with “Do not trust this user/computer for delegation”.
- **Default Value:** null

---

### Auto-Provisioned Accounts Partition

- **Name:** directory.auth.AutoProvisionedAccountsPartition
- **Description:** the name of the partition in which auto-provisioned accounts are created. If this partition does not already exist, OTDS will automatically create it.

- **Default Value:** Auto-Provisioned Accounts
- **Requirements:** you must first enable the [Enable Auto-Provisioning of Accounts on page 297](#) system attribute.

---

### Auto-Provisioned Default Group

- **Name:** directory.auth.AutoProvisionedDefaultGroup
- **Description:** specifies the name of the group to which the auto-provisioned user will be added automatically.
- **Default Value:** null
- **Requirements:** you must first enable the [Enable Auto-Provisioning of Accounts on page 297](#) system attribute.

---

### Blocked Read-Only Access

- **Name:** directory.system.BlockedReadOnlyAccess
- **Description:** if set to “true”, users who are not administrators in OTDS, or who are not members of the otds.admin partition, cannot access any of the OTDS APIs.  
Non-admin users will only be able to query themselves, they will not have access to any other users' information.
- **Default Value:** false
- **Requirements:** this system attribute is mutually exclusive with the [Restricted Read-Only Access on page 308](#) system attribute. You must first disable the [Restricted Read-Only Access on page 308](#) system attribute.

---

### CAPTCHA Incorrect Password Count

- **Name:** directory.auth.CaptchaIncorrectPasswordCount
- **Description:** the number of incorrect password attempts that will trigger the display of a CAPTCHA. This box takes either zero or a positive integer.
- **Default Value:** null
- **Requirements:** you must have configured [reCAPTCHA Private Key on page 307](#) and [reCAPTCHA Public Key on page 307](#) in order for the CAPTCHA to be displayed.

---

### CAPTCHA Incorrect Password Timespan

- **Name:** directory.auth.CaptchaIncorrectPasswordTimespan
- **Description:** the time interval, in seconds, within which the number of incorrect password attempts, as defined by [CAPTCHA Incorrect Password Count on page 291](#), must occur before a CAPTCHA is triggered.

The default value is null, meaning not configured. This is the equivalent of setting zero, which sets an infinite interval. This box takes either zero or a positive integer.

- **Default Value:** null
- **Requirements:** you must have configured [reCAPTCHA Private Key on page 307](#) and [reCAPTCHA Public Key on page 307](#) in order for the CAPTCHA to be displayed.

---

### Common Password URL

- **Name:** directory.auth.CommonPasswordURL
- **Description:** either a file reference or a URL referencing user passwords that will be disallowed. This file or URL will be used in addition to the OWASP list. For more information, see [“Password policy for non-synchronized user partitions” on page 125](#).

The default value is null, meaning no additional disallowed passwords have been set. Any file or URL specified in this system attribute is a supplement to the default OWASP list. OpenText recommends that, if using a custom file, it be less than 1MB in size.

- **Default Value:** null

---

### Configurable Session Limit

- **Name:** directory.auth.MaxSessionsPerUser
- **Description:** maximum number of sessions per user.
- **Default Value:** 32

---

### Default Authentication Partition

- **Name:** directory.auth.DefaultPartition
- **Description:** the name of the partition to assume as default in case of user name conflict. By default, when a user attempts to log in using a user name that resolves to two or more users in different partitions, OTDS will disallow the login. This attribute allows you to set the partition name that OTDS should assume to be the default and allow such logins to succeed.
- **Default Value:** null
- **Requirements:** this system attribute does not appear in the **System Attributes** list by default, it must be manually added. For more information, see [“Adding a system attribute” on page 316](#).

---

### Default HTTP Cookie Domain

- **Name:** otds.ticket.cookie.domain

- **Description:** the DNS domain in which OTDS tickets should be transferred. This is only used when passing OTDS tickets to resources through a domain-level cookie rather than having the browser POST the ticket. By default, this is determined dynamically and does not need to be configured. The value is automatically determined by OTDS. For more information, see “[Resource configuration issues](#)” on page 401.
- **Default Value:** null

### Disable Resource Name Formatting

- **Name:** directory.system.DisableResourceNameFormatting
- **Description:** setting this attribute to “true” directs OTDS to ignore the formatting configured on the NAME attribute mapping on resources for users and groups within the partition on which this system attribute is set. For more information about NAME, see “[Using resource attribute mappings](#)” on page 182 and NAME on page 202.
  - 1. This system attribute, and [Disable Resource Name Mapping on page 293](#), should be set on the **OpenText Content Management Members** partition when the OpenText Content Management resource is using a non-default NAME attribute mapping, and administrators wish to manage users through the OpenText Content Management user interface instead of the OTDS administration UI.
  - 2. This system attribute, and [Disable Resource Name Mapping on page 293](#), can only be configured on a partition level.
- **Default Value:** false

### Disable Resource Name Mapping

- **Name:** directory.system.DisableResourceNameMapping
- **Description:** setting this attribute to “true” forces OTDS to use the user name of the user, the user's cn attribute, instead of the attribute specified on the NAME attribute mapping on resources for users and groups within the partition on which the system attribute is set. For more information about NAME, see “[Using resource attribute mappings](#)” on page 182 and NAME on page 202.
  - 1. This system attribute, and [Disable Resource Name Formatting on page 293](#), should be set on the **OpenText Content Management Members** partition when the OpenText Content Management resource is using a non-default NAME attribute mapping, and administrators wish to manage users through the OpenText Content Management user interface instead of the OTDS administration UI.

2. This system attribute, and [Disable Resource Name Formatting on page 293](#), can only be configured on a partition level.

- **Default Value:** false

---

### Enable File Upload APIs

- **Name:** directory.system.AllowFileUpload
- **Description:** setting this attribute to “false” disables all file upload API endpoints. This may be necessary to satisfy security compliance requirements.

When this attribute is set to “true”, the default, all file upload API endpoints are enabled.

When this attribute is set to “false”, the following features will be unusable:

- Uploading keystore/certificate for a SAML auth handler. If required, these will need to be manually configured using the REST API.
- Uploading of files for binary attributes on users, examples include profile photos or certificates. If required, these attributes would need to be synchronized or manually set using the REST API.
- Import Units using XML files.
- **Default Value:** true
- **Requirements:** this system attribute does not appear in the **System Attributes** list by default, it must be manually added. For more information, see [“Adding a system attribute” on page 316](#).

---

### Enable Two Factor On Groups

- **Name:** directory.auth.Enable2FactorOnGroups
- **Description:** setting this attribute to “true” enables the additional processing of two factor authentication settings on groups.

When this attribute is set to “false”, the default, any two factor authentication settings on groups are ignored.

OpenText recommends that you only set this attribute to “true” if you require the configuration of two factor authentication settings on groups, as opposed to configuring two factor authentication on individual users or partitions.

- **Default Value:** false
- **Requirements:** this system attribute does not appear in the **System Attributes** list by default, it must be manually added. For more information, see [“Adding a system attribute” on page 316](#).

---

### Directory Services Base URL

- **Name:** directory.auth.BaseURL

- **Description:** sets the URL through which the OTDS login page can be accessed. This setting will override the value automatically detected by OTDS. This setting can be useful in situations where users access OTDS through a reverse proxy or load balancer. For example: `https://mycompany.domain.com:8443/otdswebs/login`  
This setting affects links returned to end users, for example:
  - Emails sent by OTDS.
  - Redirect URL for OAuth authentication handlers.
- **Default Value:** null

---

#### Disallowed Email Domains

- **Name:** directory.auth.DisallowedEmailDomains
- **Description:** a comma separated list of email domains that will not be accepted for self-provisioning of accounts. All email domains are accepted by default.
- **Default Value:** null

---

#### duo.akey

- **Name:** duo.akey
- **Description:** this attribute's value is generated by OTDS. You should not manually edit this value.
- **Requirements:** this system attribute does not appear in the **System Attributes** list by default, it must be manually added. For more information, see “[Adding a system attribute](#)” on page 316 and “[References to external websites](#)” on page 385.

---

#### duo.host

- **Name:** duo.host
- **Description:** this attribute's value is provided to you by the third-party two-factor authentication provider. For more information see “[References to external websites](#)” on page 385. The value you enter to this attribute is the DUO API hostname. For more information, see “[Duo Security and two-factor authentication](#)” on page 239.
- **Default Value:** null
- **Requirements:** this system attribute does not appear in the **System Attributes** list by default, it must be manually added. For more information, see “[Adding a system attribute](#)” on page 316.

---

#### duo.ikey

- **Name:** duo.ikey

- **Description:** this attribute's value is provided to you by the third-party two-factor authentication provider. For more information see “[References to external websites](#)” on page 385. The value you enter to this attribute is the DUO integration key. For more information, see “[Duo Security and two-factor authentication](#)” on page 239.
- **Default Value:** null
- **Requirements:** this system attribute does not appear in the **System Attributes** list by default, it must be manually added. For more information, see “[Adding a system attribute](#)” on page 316.

---

#### duo.skey

- **Name:** duo.skey
- **Description:** this attribute's value is provided to you by the third-party two-factor authentication provider. For more information see “[References to external websites](#)” on page 385. The value you enter to this attribute is the DUO secret key. For more information, see “[Duo Security and two-factor authentication](#)” on page 239.
- **Default Value:** null
- **Requirements:** this system attribute does not appear in the **System Attributes** list by default, it must be manually added. For more information, see “[Adding a system attribute](#)” on page 316.

---

#### Enable 2Factor Suspend

- **Name:** directory.auth.Enable2FactorSuspend
- **Description:** when set to true, a link will display on the native two-factor authentication page. The link will read: “I lost my device”. When a user clicks that link, they will be able to enter their email address or user name to receive an email which will then allow that user to temporarily suspend two-factor authentication on their account.
- **Default Value:** false
- **Requirements:**
  1. This system attribute does not appear in the **System Attributes** list by default, it must be manually added. For more information, see “[Adding a system attribute](#)” on page 316.
  2. You must configure your SMTP server information in order for 2 factor suspend to work. For more information, see “[SMTP Settings](#)” on page 318. Each of the following SMTP server attributes must be configured:
    - From (email)
    - SMTP Host
    - SMTP Password

- SMTP Port
  - Use SSL
  - SMTP User Name
3. For the user to receive the email, the userid account must have a valid email address configured.
  4. For general information about two-factor authentication configuration in OTDS, see “OTDS Two-Factor Authentication” on page 69, “Enabling two-factor authentication” on page 99, and “Configuring two-factor authentication” on page 237.

---

### Enable Auto-Consolidation On Connection Change

- **Name:** otds.es.EnableAutoConsolidationOnConnectionChange
- **Description:** set this attribute to “true” if you want to implement automatic consolidation whenever any AD connection is changed. It is used to enable or disable automatic consolidation for AD connection change. For more information, see “Connection Information” in “Defining a synchronized user partition” on page 74.

This attribute can be set to “true” in either a specific user partition or at the global level in a system attribute:

- Global: if the system attribute is located on the **System Attributes** tab of the **System Config** section, it applies to all user partitions.
- Specific: if the system attribute is located on the **System Attributes** tab of a specific user partition, it applies to that user partition only, and overrides the global setting.

You set this system attribute for a specific user partition from the **Actions** menu of that user partition by selecting **Partition Attributes**, then adding **otds.es.EnableAutoConsolidationOnConnectionChange** to the **System Attributes** tab. For more information, see “Partition attributes” on page 132.

- **Default Value:** false
- **Requirements:** this attribute will only take effect after the user partition is restarted or reloaded. OpenText recommends that you create and set this attribute before you enable a partition and perform an import to that partition.

---

### Enable Auto-Provisioning of Accounts

- **Name:** directory.auth.AutoProvisionAccounts
- **Description:** for use with OAuth, OpenID and or SAML. This attribute controls the behavior of the system when users sign in with external accounts that do not have a corresponding account in OTDS.

When this attribute is set to false, the first time a user signs in with an OAuth or OpenID provider, such as Facebook or Twitter, they will be prompted to link that external account to an existing account in OTDS.

Users link their accounts by providing their OTDS account credentials. This means that users must either create an account or have an existing account in OTDS before they can sign in with these services. However, some deployments of OTDS may prefer to create separate accounts in OTDS for users that sign in with external accounts, so that no sign up process is required.

To accomplish this, you must set this attribute to true. When enabled, all logins with OAuth or OpenID that are not associated with an existing account in OTDS will have a new account created in the partition called “Auto-Provisioned Accounts”. This means that when a user signs in with Twitter one day and Facebook another day, they will be signing in with a different account into OTDS each time. This may or may not be desirable, and largely depends on the application for which OTDS is ultimately being used.

- **Default Value:** false
- **Requirements:**
  1. The user partition “Auto-Provisioned Accounts” must be manually added by the administrator to the access roles that will grant these provisioned users permission to access the desired resources.
  2. The OAuth or OpenID authentication handler needs to be enabled. For information about how to enable sign in with OAuth or OpenID providers, see “[List of authentication handlers](#)” on page 138.

---

### Enable Email On Password Change

- **Name:** directory.auth.EnableEmailOnPasswordChange
- **Description:** when you set this attribute's value to “true”, and a user changes their password on the OTDS sign in page, an email is sent to the user to confirm that their password has been changed.
- **Default Value:** false
- **Requirements:** you must have enabled [Enable Password Reset](#) on page 299.

---

### Enable Enterprise Sync

- **Name:** directory.bootstrap.EnableES
- **Description:** controls whether the Enterprise Sync feature is enabled. Enterprise Sync is responsible for operating synchronized partitions. This feature is typically only disabled for cloud-based installations of Directory Services, where access to an on-premises Active Directory or LDAP server is either not required or not possible.
- **Default Value:** true

---

### Enable Expired User Deletion

- **Name:** directory.system.EnableExpiredUserDeletion



**Note:** Some features are only available if you are using OTDS version 20.4.2 or higher.

- **Description:** this attribute, set on a partition, can be set to “true” if you want to enable the deletion of expired user IDs after a set retention period. If you want to change the default of fifteen days, see [Expired User Retention Period on page 301](#).

This attribute must be set as a partition attribute, for more information, see [“System attributes” on page 132](#).

- **Default Value:** false
- **Requirements:** you must first set [Enable Maintenance on page 299](#) to “true”.

---

### Enable Import Source Configuration

- **Name:** directory.config.EnableImportSource
- **Description:** when you set this attribute's value to “true”, the **External Import** menu option will be displayed on the main menu.
- **Default Value:** false
- **Requirements:** you may need to refresh your browser window to see this menu option.

---

### Enable Maintenance

- **Name:** directory.system.EnableMaintenance



**Note:** Some features are only available if you are using OTDS version 20.4.2 or higher.

- **Description:** set this attribute's value to “true” if you want to allow maintenance tasks at the system level.  
For more information about the maintenance tasks you can set, see [Enable Expired User Deletion on page 298](#) and [Expired User Retention Period on page 301](#).
- **Default Value:** false
- **Requirements:** you must restart OTDS after you change the default setting of this attribute for your change to take effect.

---

### Enable Password Reset

- **Name:** directory.auth.EnablePasswordReset
- **Description:** set this attribute to “false” to disable the **Password Reset** option on the OTDS sign in page. By default, password reset is enabled and users at the OTDS sign in page can select either **forgot password** or **reset it here** to receive an email that provides them with a password reset so that they can sign in.

The setting of the [Validation Token Lifetime](#) on page 314 system attribute has an impact on this attribute.

- **Default Value:** true
- **Requirements:**
  1. You must configure your SMTP server information in order for password reset to work. For more information, see [“SMTP Settings” on page 318](#). Each of the following SMTP server attributes must be configured:
    - From (email)
    - SMTP Host
    - SMTP Password
    - SMTP Port
    - Use SSL
    - SMTP User Name
  2. For the user to receive the email, the userid account must have a valid email address configured.

---

### Enable Self-Provisioning of Accounts

- **Name:** directory.auth.SelfProvisionAccounts
- **Description:** after you enable this attribute, users will see a **Sign up** option on the OTDS login page. Users must go through the process of validating their email address before they can sign in to OTDS. Self-provisioned accounts are assigned a GUID for the user identifier, and users are expected to sign in with their email address. To accomplish this, you must set this attribute to true. Self-provisioned accounts are created in the user partition “Self-Provisioned Accounts”.

The user attributes collected on the **Sign up** page can be configured using the **Additional Signup Attributes** system attribute. See [Additional Signup Attributes on page 288](#) for more information.

- **Default Value:** false
- **Requirements:**
  1. You must configure your SMTP server information in order for self-provisioning to work. For more information, see [“SMTP Settings” on page 318](#). Each of the following SMTP server attributes must be configured:
    - From (email)
    - SMTP Host
    - SMTP Password
    - SMTP Port
    - Use SSL
    - SMTP User Name

2. The user partition “Self-Provisioned Accounts” must be manually added by the administrator to the access roles that will grant these provisioned users permission to access the desired resources.
3. When enabling self-provisioning, OTDS must be configured to allow login through email address. Verify that the [Login User Name Attributes on page 305](#) system attribute has “mail” in the list of allowed attributes. For example, the default value for **Login User Name Attributes** is “oTExternalID1|oTExternalID3|oTExternalID4|mail”. However, in a migrated or non-default configuration, the default value may have changed. If you are enabling self-provisioning, make sure that “mail” is included in the list of allowed attributes for **Login User Name Attributes**.

---

### Expired User Retention Period

- **Name:** directory.system.ExpiredUserRetentionPeriod



**Note:** Some features are only available if you are using OTDS version 20.4.2 or higher.

- **Description:** this attribute, set on a partition, can be set to the number of days after which a user ID is deleted from OTDS once that user ID has expired.

This attribute must be set as a partition attribute, for more information, see [“System attributes” on page 132](#).

- **Default Value:** 15
- **Requirements:** you must first set [Enable Maintenance on page 299](#) to “true” and then set [Enable Expired User Deletion on page 298](#).

---

### help.config.HelpTenant

- **Name:** help.config.HelpTenant
- **Description:** a help session identifier. Do not modify this attribute unless instructed by OpenText.
- **Default Value:** 1

---

### help.config.HelpType

- **Name:** help.config.HelpType
- **Description:** a help type identifier. Do not modify this attribute unless instructed by OpenText. If you modify this attribute incorrectly, you may cause the online help system to stop working.
- **Default Value:** ofh1

---

**help.config.HelpURL**

- **Name:** help.config.HelpURL
  - **Description:** the help system base URL. Only modify this attribute if you are configuring the OpenText Private Help Server. For more information, see “About the Directory Services online help” on page 383.
  - **Default Value:** `http://docsapi.opentext.com/mapperpi`
- 

**HTTP Header for Proxied Client Certificate**

- **Name:** directory.auth.ClientCertProxyHeader
  - **Description:** the name of the HTTP header set by an upstream proxy server that contains the client certificate used to establish the HTTPS connection.  
This is only required when using the client-certificate based two-factor authentication feature alongside a web server and proxy in front of OTDS. For more information, see “Require a client certificate” in the **Define Settings** options in “Configuring two-factor authentication” on page 237.
  - **Default Value:** null
- 

**Trusted Proxies for Proxied Client Certificate**

- **Name:** directory.auth.ClientCertProxyIPs
  - **Description:** a comma-separated list of the IP addresses, or subnets, of the proxies that can be trusted to provide the header specified in [HTTP Header for Proxied Client Certificate on page 302](#). This attribute is set to OFF if this validation is not required. For example, if OTDS can only be accessed through the proxies responsible for providing the header.  
This is only required if you have first set [HTTP Header for Proxied Client Certificate on page 302](#).
  - **Default Value:** null
- 

**directory.security.HttpProxyPassword**

- **Name:** directory.security.HttpProxyPassword
  - **Description:** sets the password to be sent to a proxy for outgoing HTTP requests from Directory Services.
  - **Default Value:** null
- 

**directory.security.HttpProxyUser**

- **Name:** directory.security.HttpProxyUser
  - **Description:** sets the username to be sent to a proxy for outgoing HTTP requests from Directory Services.
-

- **Default Value:** null

### LDAP Retry Delay

- **Name:** otbs.es.ConnectionsRetryDelay
- **Description:** if you have created and set the [LDAP Retry Number on page 303](#) attribute, you can choose to set a delay, in seconds, before retrying to connect to the LDAP server.

When you create this attribute, type a positive integer in the **Value** box to set the number of seconds before retrying the connection. For more information, see “Connection Information” in [“Defining a synchronized user partition” on page 74](#).

This attribute is used to control the retry of a connection, if that connection becomes temporarily unavailable.

This attribute can be set in either a specific user partition or at the global level in a system attribute:

- Global: if the system attribute is located on the **System Attributes** tab of the **System Config** section, it applies to all user partitions.
- Specific: if the system attribute is located on the **System Attributes** tab of a specific user partition, it applies to that user partition only, and overrides the global setting.

You set this system attribute for a specific user partition from the **Actions** menu of that user partition by selecting **Partition Attributes**, then adding **otbs.es.ConnectionsRetryDelay** to the **System Attributes** tab. For more information, see [“Partition attributes” on page 132](#).

- **Default Value:** 20
- **Requirements:** you must first create and set the [LDAP Retry Number on page 303](#) system attribute. This attribute will only take effect after the user partition is restarted or reloaded.

---

### LDAP Retry Number

- **Name:** otbs.es.ConnectionsRetryNum
- **Description:** type a positive integer in the **Value** box to set the maximum retry attempts permitted when connecting to the LDAP server. For more information, see “Connection Information” in [“Defining a synchronized user partition” on page 74](#).

This attribute is used to control the retry of a connection, if that connection becomes temporarily unavailable.

This attribute can be set in either a specific user partition or at the global level in a system attribute:

- Global: if the system attribute is located on the **System Attributes** tab of the **System Config** section, it applies to all user partitions.

- Specific: if the system attribute is located on the **System Attributes** tab of a specific user partition, it applies to that user partition only, and overrides the global setting.

You set this system attribute for a specific user partition from the **Actions** menu of that user partition by selecting **Partition Attributes**, then adding **otds.es.ConnectionsRetryNum** to the **System Attributes** tab. For more information, see “[Partition attributes](#)” on page 132.

- **Default Value:** 3
- **Requirements:** you must also create and set the [LDAP Retry Delay](#) on page 303 system attribute. This attribute will only take effect after the user partition is restarted or reloaded.

---

#### otds.es.LDAPSsyncMethod

- **Name:** otds.es.LDAPSsyncMethod
- **Description:** this system attribute is only applicable to synchronized user partitions that have the **Import users only from matched groups** option selected and that have the **USN query** monitoring type.

It controls the import and consolidation method. For example, if you are intending to import and consolidate a sub-section of a large data set of users and groups, you can choose to set this system attribute to “TRAVERSAL” to optimize the performance of the import and consolidation. There are two valid values: FULL and TRAVERSAL. The default setting is “FULL”.

This system attribute can be set to apply to all synchronized partitions that have the required settings, or can apply to a specific synchronized partition:

- Global: if the system attribute is located on the **System Attributes** tab of the **System Config** section, it applies to all synchronized partitions that have the selected option and monitoring type requirements detailed above.
- Specific: if the system attribute is located on the **System Attributes** tab of a specific synchronized partition, it applies to that partition only, and overrides the global setting.

You set this system attribute for a specific synchronized partition from the **Actions** menu of that partition by selecting **Partition Attributes**, then adding **otds.es.LDAPSsyncMethod** to the **System Attributes** tab. For more information, see “[Partition attributes](#)” on page 132.

Before setting this system attribute on a specific partition, during the creation of the partition:

- Disable the **Start importing users and groups automatically upon completion** option. For more information, see “[Creating a synchronized user partition](#)” on page 87.
- Ensure **Import users only from matched groups** is selected. For more information, see “[Creating a synchronized user partition](#)” on page 87.

- Ensure the **USN query** monitoring type is selected. For more information, see “[Synchronized User Partitions](#)” on page 74.

Once the partition is created, set the **otds.es.LDAPSyncMethod** system attribute on the partition, and then start the partition import.

- **Default Value:** FULL

---

### Login Screen Message

- **Name:** directory.auth.LoginScreenMessage
- **Description:** you can choose to include HTML content to show on the OTDS login page.

If you do not require multilingual support, in the **Value** box, enter the HTML content that you want to show on the OTDS login page.

If you need multilingual support, do the following:

1. In the **Value** box, type “prompt.loginmessage” without the quote marks.
2. For *each* language you want to support, create a `login_custom_<xy>.properties` file in the `<OTDS_home>/otdswebs/WEB-INF/classes` directory, where `<xy>` is two letters representing the language. For example, when implementing support for German, create a `login_custom_de.properties` file.

When creating the `login_custom_<xy>.properties` file, follow the same file name conventions as for the OTDS `login.properties` file found in the same directory.

3. For *each* file you create, type:

```
prompt.loginmessage=<desired_HTML_content>
```

4. Restart Tomcat.

- **Default Value:** null
- **Requirements:** you must restart Tomcat after creating a `login_custom_<xy>.properties` file.

---

### Login User Name Attributes

- **Name:** directory.auth.UserNameAttributes
- **Description:** the set of attributes that OTDS uses to search for a user name provided on the login form. For more information, see “[Customizing the login user name format](#)” on page 347.
- **Default Value:** oTExternalID1|oTExternalID3|oTExternalID4|mail

---

### otds.as.intranetSubnets

- **Name:** otds.as.intranetSubnets

- **Description:** if you have enabled [Enable only for requests originating from Extranet IP addresses on page 238](#) two-factor authentication, this system attribute allows you to define a private IP range. Intranet subnets that are not within standard private IP ranges can be configured in this system attribute.
- **Default Value:** null.
- **Example:** `otds.as.intranetSubnets = 149.235.0.0/16, 149.234.0.0/16`

---

#### otds.as.trustedProxies

- **Name:** otds.as.trustedProxies
- **Description:** if you have enabled [Enable only for requests originating from Extranet IP addresses on page 238](#) two-factor authentication, this system attribute allows you to list all proxies that should be trusted.
- **Default Value:** null.
- **Example:** `otds.as.trustedProxies = 23.45.67.89, 9.9.9.9`

---

#### OTDS Log Level

- **Name:** otds.log.level
- **Description:** the level of logging written to the `otds.log` file. Valid values are:
  - OFF: nothing is written to the log.
  - FATAL: details events that halt Directory Services, and prevent it from running.
  - ERROR: details error events that, although they have occurred, could still allow Directory Services to continue running.
  - WARN: details potentially harmful situations.
  - INFO: details informational messages that highlight the progress of Directory Services. This is the default level.
  - DEBUG: details very specific informational events that are most useful when debugging Directory Services.
  - TRACE: provides greater detail than the DEBUG level.
- **Default Value:** INFO

---

#### Password Reset URL for Synchronized Users

- **Name:** directory.auth.PasswordResetURL
- **Description:** a URL to which synchronized users will be redirected in order to reset their password.
- **Default Value:** null

---

### reCAPTCHA Private Key

- **Name:** directory.auth.RecaptchaPrivateKey
- **Description:** when using account self-provisioning, the OTDS sign up page can be configured with a CAPTCHA using Google reCAPTCHA for use cases where OTDS is internet accessible. For the [reCAPTCHA Private Key on page 307](#) attribute, enter your reCAPTCHA secret.
- **Default Value:** null
- **Requirements:**
  1. You need to create a reCAPTCHA integration on Google, using your Google account. See “Google’s reCAPTCHA” website for information about setting up your reCAPTCHA integration. For more information see [“References to external websites” on page 385](#).
  2. After you set up your reCAPTCHA integration, you need to set two OTDS system attributes: [reCAPTCHA Private Key on page 307](#) and [reCAPTCHA Public Key on page 307](#).

---

### reCAPTCHA Public Key

- **Name:** directory.auth.RecaptchaPublicKey
- **Description:** when using account self-provisioning, the OTDS sign up page can be configured with a CAPTCHA using Google reCAPTCHA for use cases where OTDS is internet accessible. For the [reCAPTCHA Public Key on page 307](#) attribute, enter your reCAPTCHA site key.
- **Default Value:** null
- **Requirements:**
  1. You need to create a reCAPTCHA integration on Google, using your Google account. See “Google’s reCAPTCHA” website for information about setting up your reCAPTCHA integration. For more information see [“References to external websites” on page 385](#).
  2. After you set up your reCAPTCHA integration, you need to set two OTDS system attributes: [reCAPTCHA Private Key on page 307](#) and [reCAPTCHA Public Key on page 307](#).

---

### Restrict Admin Login Subnets

- **Name:** directory.auth.RestrictAdminLoginSubnets
- **Description:** this system attribute allows you to define an IP or subnet range. If defined, authentication of privileged administrative accounts is restricted to that IP or subnet range.  
Privileged administrative accounts are those that both reside in a system partition, for example the `otds.admin` partition, and have been assigned OTDS administration rights.

- **Default Value:** null
- **Example:** `directory.auth.RestrictAdminLoginSubnets = 10.0.0.0/8, 192.168.0.0/16`

---

### Restricted Read-Only Access

- **Name:** `directory.system.RestrictedReadOnlyAccess`
- **Description:** if set to “true”, users who are not administrators in OTDS will not be able to look up any information on partitions to which they are not a member. They will also be restricted from looking up any information on any users, groups, or organizational units that are not within their partition.
- **Default Value:** `false`
- **Requirements:** this system attribute is mutually exclusive with the [Blocked Read-Only Access on page 291](#) system attribute. You must first disable the [Blocked Read-Only Access on page 291](#) system attribute.

---

### SameSite Cookie Attribute

- **Name:** `otds.as.SameSiteCookieVal`
- **Description:** The SameSite attribute can prevent the browser from sending a cookie along with cross-site requests. This attribute allows you to set the value for SameSite that OTDS should set on its cookies. The value can be any one of:
  - `Lax`: OTDS cookies will be sent if you are navigating within the website, or if you are being redirected to the website. This is the default value set by many browsers.
  - `None`: OTDS cookies will be sent with requests crossing the website origin bounds.



**Note:** The `Strict` option is not supported by OTDS because the OTDS sign in page requires cookies in redirect scenarios from integrated applications.

For integrations where the OTDS login page is expected to be used in an `<iframe>` scenario, you must set the SameSite attribute (`otds.as.SameSiteCookieVal`) to `None`.

- **Default Value:** null.

---

### SAPSSOEXT Log Level

- **Name:** `directory.auth.SAPSSOEXTLogLevel`
- **Description:** sets the log level OTDS should configure for the SAPSSOEXT library used by the [SAPSSOEXT on page 154](#). A value of zero, 0, disables logging by the library.

Allowed values are: 0, 1, 2, and 3.

If you installed your application server to the default location, you will find the log file at `<app_srvr_installdir>\logs\sapssoext_otds.log`. If you are using a container, the logging information will be written to `stdout` by the container.

- **Default Value:** 0

---

### Self-Provisioned Accounts Partition

- **Name:** directory.auth.SelfProvisionedAccountsPartition
- **Description:** the name of the partition in which self-provisioned accounts are created. If this partition does not already exist, OTDS will automatically create it.
- **Default Value:** Self-Provisioned Accounts

---

### Self-Provisioned Default Group

- **Name:** directory.auth.SelfProvisionedDefaultGroup
- **Description:** specifies the name of the group to which the self-provisioned user will be added automatically.
- **Default Value:** null
- **Requirements:** You must first enable the [Enable Self-Provisioning of Accounts on page 300](#) system attribute.

---

### Show Custom Auth Handlers On Login Page

- **Name:** directory.auth.ShowCustomAuthHandlersOnLoginPage
- **Description:** if set to “false”, any custom OAuth or SAML authentication handlers will not be displayed on the OTDS login page. Custom OAuth or SAML authentication handlers will be displayed on the OTDS login page by default.
- **Default Value:** true

---

### Show Error If Account Does Not Exist

- **Name:** directory.auth.ShowErrorIfAccountNotExist
- **Description:** when you set this attribute to “true”, OTDS will display an error on the sign in page if the user authenticated with SSO does not exist in Directory Services.
- **Default Value:** false

---

### Show Logged Out Page

- **Name:** directory.auth.ShowLoggedOutPage

- **Description:** when you set this attribute to “true”, OTDS will display a **Logged Out** page when the user signs out of Directory Services.
- **Default Value:** false

---

### Show Login Button On Logged Out Page

- **Name:** directory.auth.ShowLoginButtonOnLoggedOutPage
- **Description:** if you set this attribute to “true”, OTDS will show a **Go to Sign In Page** button on the OTDS logged out page. Clicking the button will bring users to the OTDS login page. The default setting, “false”, does not display this button.
- **Default Value:** false

---

### Show Login Screen Languages

- **Name:** directory.auth.ShowLangsOption
- **Description:** this attribute, when set to “true”, displays an option to select the display language for the OTDS login page. By default, the OTDS login page is displayed in the browser's selected language. In other words, as per the Accept-Language HTTP header.  
 **Note:** This setting does not affect the display language in other OpenText products.
- **Default Value:** false
- **Requirements:** this system attribute does not appear in the **System Attributes** list by default, it must be manually added. For more information, see “[Adding a system attribute](#)” on page 316.

---

### Show Native Login After Logout

- **Name:** directory.auth.ShowNativeLoginAfterLogout
- **Description:** if set to false, then when users sign back in, after signing out through OTDS, the user's browser will be redirected to sign in using the authentication mechanism configured through authentication handlers. Examples of authentication handlers include SAML and Negotiate.  
If this system attribute is set to true, then when users sign back in, after signing out through OTDS, the user's browser will be shown the OTDS sign in page. This allows an administrative user to log in using an admin account rather than their personal SSO / desktop account.
- **Default Value:** true

---

### SSO Ticket Time-To-Live

- **Name:** otds.as.sso.ttl

- **Description:** the number of seconds for which an OTDS SSO ticket is valid.
- **Default Value:** 28200

---

#### symantec.appid

- **Name:** symantec.appid
- **Description:** if you are setting up the third-party authentication provider, Symantec VIP, you need to add this system attribute. You will type your account's VIP application ID as the value of the attribute. This information is available in VIP manager. For more information, see [“Adding a system attribute” on page 316](#) and [“Symantec VIP and two-factor authentication” on page 239](#).
- **Default Value:** null

---

#### symantec.keystore

- **Name:** symantec.keystore
- **Description:** if you are setting up the third-party authentication provider, Symantec VIP, you need to add this system attribute. You will type the URL to the keystore OTDS should use to connect to VIP services. The keystore must be accessible on all OTDS servers handling authentication. For more information, see [“Adding a system attribute” on page 316](#) and [“Symantec VIP and two-factor authentication” on page 239](#).
- **Default Value:** null

---

#### symantec.keystorepassword

- **Name:** symantec.keystorepassword
- **Description:** if you are setting up the third-party authentication provider, Symantec VIP, you need to add this system attribute. You will type the password used for the keystore. For more information, see [“Adding a system attribute” on page 316](#) and [“Symantec VIP and two-factor authentication” on page 239](#).
- **Default Value:** null

---

#### symantec.usernameattr

- **Name:** symantec.usernameattr
- **Description:** if you are setting up the third-party authentication provider, Symantec VIP, you need to add this system attribute. You will type the OTDS attribute name that contains the value corresponding to the users' <username> in Symantec VIP. For more information, see [“Adding a system attribute” on page 316](#) and [“Symantec VIP and two-factor authentication” on page 239](#).
- **Default Value:** null

### Synchronization Master Host

- **Name:** directory.bootstrap.MasterHost
- **Description:** defines the fully qualified domain name of the master host.  
Examples of valid values include: myserver.mycompany.net and 10.4.33.29

! **Important**

The **Synchronization Master Host** system attribute must always contain the hostname of the server functioning as the synchronization master host in your environment. Each OTDS installation is looking for the value of **Synchronization Master Host** at startup. If a value for the system attribute **Synchronization Master Host** does not exist, the first OTDS installation in your Directory Services environment will create and populate it, thereby becoming the master host.

- **Default Value:** <fully\_qualified\_domain\_name\_of\_server>
- **Requirements:**
  1. The *Synchronization Master Host* system attribute cannot be null. It must always have a correct value.
  2. If the server ever changes, or is renamed, you *must* update the **Synchronization Master Host** system attribute with the new server name.

---

### Third-Party Two-Factor Authentication Provider

- **Name:** directory.auth.ThirdPartyTwoFactorProvider
- **Description:** to enable third-party two-factor authentication with either “Duo Security” or “Symantec VIP” authentication providers, set this system attribute to:
  - If you are configuring Duo security, set this system attribute to: “duo”.
  - If you are configuring Symantec VIP, set this system attribute to: “symantec”.

For more information, see “[Two-factor authentication with a third-party two-factor authentication provider](#)” on page 239 and “[References to external websites](#)” on page 385.

- **Default Value:** null

---

### TOTP Issuer Name

- **Name:** directory.auth.TOTPIssuerName
- **Description:** controls the name of the issuer in the secret key issued by OTDS for native TOTP-based two-factor authentication.
- **Default Value:** OpenText

---

## Two Step Login

- **Name:** directory.auth.TwoStepLogin
- **Description:** when this attribute is set to “true”, users are required to use a two step login procedure.  
For more information, see:
  - “Using WebAuthn to provide users the option of passwordless authentication” on page 103
  - WebAuthn on page 157
  - WebAuthn Policy on page 314
- **Default Value:** false

---

## Validate LDAP SSL Certificates

- **Name:** directory.security.ValidateLDAPSSLCerts
- **Description:** set this attribute to “true” in order to verify certificates for connections from OTDS synchronized user partitions to an LDAP server.  
If the LDAP server is configured with a certificate signed by an unknown source, for example, a self-signed certificate, the certificate will need to be imported to the Java truststore on *every* OTDS server.
- **Default Value:** false

---

## Validate SAML SCD Address

- **Name:** directory.auth.ValidateSAMLSCDAddress
- **Description:** set this attribute to “true” to direct OTDS to validate that the client IP address matches the address in a SAML assertion's SubjectConfirmationData element.  
If this attribute is set to “true” and OTDS cannot validate that the client IP address matches the address in a SAML assertions' SubjectConfirmationData element, OTDS will log the error message “Client IP does not match Address”, and refuse to authenticate the user.
- **Default Value:** true

---

## Validate SAML SSL Certificates

- **Name:** directory.security.ValidateSAMLSSLCerts
- **Description:** set this attribute to “true” in order to verify certificates for a SAML identity provider.  
If the SAML identity provider is configured with a certificate signed by an unknown source, for example, a self-signed certificate, the certificate will need to be imported to the Java truststore on *every* OTDS server.
- **Default Value:** true

### Validate SMTP SSL Certificates

- **Name:** directory.security.ValidateSMTPSSLCerts
- **Description:** set this attribute to “true” in order to verify certificates for an SMTP server connection.  
If the SMTP server connection is configured with a certificate signed by an unknown source, for example, a self-signed certificate, the certificate will need to be imported to the Java truststore on *every* OTDS server.
- **Default Value:** true

### Validation Token Lifetime

- **Name:** directory.auth.ValidationTokenLifetime
- **Description:** number of hours for which validation tokens related to account self-provisioning are valid. This system attribute sets a time limit for all email links sent by OTDS, including email address confirmation and [Enable Password Reset on page 299](#).
- **Default Value:** 24

### Want Secure Cookies

- **Name:** otds.as.wantSecureCookies
- **Description:** when this attribute is set to “true”, cookies are marked as Secure when used over SSL connections.  
Cookies marked as Secure are prefixed with \_\_Secure- and the Partitioned attribute is added.
- **Default Value:** true

### WebAuthn Policy

- **Name:** directory.auth.WebAuthnPolicy
- **Description:** setting this system attribute configures the WebAuthn registration policy for users.

Allowed values are:

- **ALLOW:** users can choose whether or not to register with WebAuthn and enable passwordless authentication.
- **REQUIRE:** users must register with WebAuthn.  
Organizations that want to enforce strong authentication, without passwords or two-factor authentication, might consider this option.
- **BLOCK:** users cannot register with WebAuthn.  
Organizations that currently use a third party, two-factor authentication provider, and do not want to alter the current user experience, might consider this option.

For more information, see:

- “Using WebAuthn to provide users the option of passwordless authentication” on page 103
- WebAuthn on page 157
- Two Step Login on page 313
- **Default Value:** BLOCK

## 12.1.2 Examples filtering system-wide deleted users and groups

The **Value** field of a system attribute can store a custom filter. These examples show how to create system-wide system attributes that apply to users and groups in all synchronized partitions. These examples can only be applied to synchronized partitions.



**Tip:** You may need to consult with your Active Directory system administrator to identify those system attributes that are saved in deleted users and groups in order to create your own filters.

To see these examples applied to one synchronized partition only, see “[Examples filtering one synchronized partition's deleted users and groups](#)”. If any system attribute is created on the “[System Config](#)” page, and that system attribute is also created on a single synchronized partition on the “[Partition attributes](#)” page, the system attribute created on the **Partition Attributes** page will take precedence.

### ► Example 12-1: Example creating a system attribute that is used to search for deleted users system-wide

This example will filter deleted users. It will create a system attribute that applies to all users in all synchronized partitions, system-wide.

1. In the OTDS administration page, click **System Config**.

2. On the **System Attributes** tab, click **Add Attribute**.

3. In the **Name** field, type:

```
otds.es.FilterDeletedUsers
```

4. In the **Value** field, do one of the following:

- If the `mail` attribute is not saved when a user is deleted, type:

```
(&(!objectClass=computer))(objectClass=user)(objectClass=person))
```

- If the `mail` attribute is saved when a user is deleted, type:

```
(&(!objectClass=computer))(objectClass=user)(objectClass=person)(mail*))
```



**Note:** You can consult with your Active Directory system administrator to identify those attributes that are saved in deleted users and groups.

5. Click **Save**.



#### **Example 12-2: Example creating a system attribute that is used to search for deleted groups system-wide**

This example will filter deleted groups. It will create a system attribute that applies to all groups in all synchronized partitions, system-wide.

1. In the OTDS administration page, click **System Config**.

2. On the **System Attributes** tab, click **Add Attribute**.

3. In the **Name** field, type:

```
otds.es.FilterDeletedGroups
```

4. In the **Value** field, type:

```
(&(objectClass=group)(|(groupType=2147483652)(groupType=2147483650)(groupType=2147483656)))
```

5. Click **Save**.



### **12.1.3 Adding a system attribute**

**To add a global system attribute:**



#### **Caution**

OpenText recommends that you use extreme caution when modifying the system attributes. Improper or inaccurate changes to these attributes can negatively impact your entire OTDS environment.

1. If you want to add a system attribute that applies across the entire OTDS environment, from the web administration menu, select **System Config**.
2. On the **System Config** page, select the **System Attributes** tab.
3. On the button bar, click **Add Attribute**.
4. In the **Name** box, type the name of your new attribute.



**Note:** After you create your new attribute, you cannot edit its name.

5. You cannot assign a value in the **Display Name** box.

6. In the **Value** box, type an allowed value for your new attribute. You can type a custom filter in this field.

For more information, see “[Examples filtering system-wide deleted users and groups](#)” on page 315.

7. Click **Save**.

**To add a system attribute to one partition:**

1. If you want to add a system attribute that applies to one partition only, from the web administration menu, select **Partitions**.
2. From the **Actions** menu of the partition to which you want to add a system attribute, select **Partition Attributes**.
3. On the **System Attributes** tab, select **Add**.
4. In the **Name** box, type the name of the system attribute. For a list of system attribute names, see “[List of supported system attributes](#)” on page 288.



**Note:** After you create your new attribute, you cannot edit its name.

5. You cannot assign a value in the **Display Name** box.
6. In the **Value** box, type an allowed value for the system attribute. For a list of system attribute values, see “[List of supported system attributes](#)” on page 288.
7. Click **Save**.

#### 12.1.4 Editing a system attribute

**To edit a system attribute:**



**Caution**

OpenText recommends that you use extreme caution when modifying the system attributes. Improper or inaccurate changes to these attributes can negatively impact your entire OTDS environment.

1. From the web administration menu, select **System Config**.
2. On the **System Config** page, select the **System Attributes** tab.
3. In the list of system attributes, find the attribute you want to edit.
4. The **Name** box cannot be edited. The **Display Name** box cannot be edited.
5. **Optional** Click in the **Value** box associated with the system attribute you want to edit. Type a value for this attribute.
6. Click **Save**.

### 12.1.5 Deleting a system attribute

**To delete a system attribute:**



#### Caution

Exercise extreme caution when deleting a system attribute as this action cannot be undone.

1. From the web administration menu, select **System Config**.
2. On the **System Config** page, select the **System Attributes** tab.
3. Select the box to the left of the system attribute you want to delete.
4. On the button bar, click **Delete**.
5. In the **Delete System Attribute(s)** box, click **OK**.

## 12.2 SMTP Settings

To enable notification emails for either OTDS operations or for license key operations, you must first configure the SMTP information.

The boxes you must configure include the host and port of the SMTP server. You will also need to enter the email address from which the notification emails will be sent. If required by the SMTP server, you may also need to enter a user name and password for the connection to the SMTP server. Finally, you must select a time-out value for the connection to the SMTP server when sending email.

The boxes that you can optionally configure include the name from which the notification emails will be sent and whether you will use SSL. It may be the case that SSL is a requirement for you, depending on the configuration of your SMTP server.



#### Important

You can only choose to test your SMTP settings when you first save them. If you try to navigate to the page to test at a later date, that test will fail, even if your settings are correct.

### To configure SMTP settings

**To configure SMTP settings:**

1. From the web administration menu, select **System Config**.
2. On the **System Config** page, select the **SMTP Information** tab.
3. On the **SMTP Information** page, in the **SMTP Host** box, type the fully qualified hostname of the SMTP server to which OTDS will connect in order to send email.
4. In the **SMTP Port** box, type the port number used by the SMTP server.

5. **Optional** If your SMTP server requires it, in the **SMTP User Name** box, type the user name to be used in the connection to the SMTP server.
6. **Optional** If your SMTP server requires it, in the **SMTP User Password** box, click **Edit Password**, and then type the password for the user name you typed in **step 5**.
7. **Optional** Select the **Use SSL** box if you want to use SSL, or if SSL is required, to connect to the SMTP server.
8. In the **Timeout** box, type a positive integer to set the number of seconds the server will continue trying to send the emails before it times out.
9. In the **From (email)** box, type the email address that will be used as the "From" address in the email sent by OTDS.
10. **Optional** In the **From (name)** box, type the name that will be used as the "From" name in the email sent by OTDS.
11. After you have completed your entries to the boxes, on the button bar click **Save**.
12. If you entered your SMTP settings for the first time, and after you save those settings, you can click **Test SMTP Connection**.  
However, if you previously saved your settings and then navigated away from this page, clicking **Test SMTP Connection** will fail.

## 12.3 Audit/Reporting Settings

The **Audit/Reporting Settings** tab of the **System Config** page allow you to set or select:

- **Enable Audit/Reporting:** to enable the auditing of OTDS operations so that a report can be generated.
- **Days to keep Audit record:** the number of days that OTDS will store the audit record.
- **OTDS Notification Events:** the types of operations that OTDS will begin storing information for reports.

To view the reports generated when audit reporting is enabled in OTDS, see *OpenText Directory Services - Web Client Help (OTDS-H-AWC)*.

### To configure audit/reporting settings

#### To configure audit/reporting settings:

1. From the web administration menu, select **System Config**.
2. On the **System Config** page, select the **Audit/Reporting Settings** tab.
3. **Optional** If you want to enable audit reporting in OTDS, select **Enable Audit/Reporting**.

4. Type a positive integer to represent the number of days that OTDS will store the audit record.
5. From the **Available Event IDs** box, click to select each OTDS operation whose audit record you want stored. Press and hold **Ctrl** to select multiple events. After you have selected the events, click **ADD**.

These selected events will now move to the **Selected Event IDs** box. If you want to remove any event, then click to select that event in the **Selected Event IDs** box, and then click **REMOVE**.

Licensing events are always recorded and tracked.

6. If you have finished configuring your audit/reporting settings, on the button bar click **Save**.



**Tip:** If you want to set your notification settings for license usage of your resources, see “[Editing notification settings for your resource](#)” on page 225.

## 12.4 Notifications Settings

The **Notifications Settings** tab of the **System Config** page allows you to set or select notifications for OTDS events, license key expiration, or password expiration.

### Requirements before enabling Notifications in OTDS

Before you enable OTDS event, license key, or password notifications, you must ensure the following:

1. In the **General Notifications** area of the **Notifications Settings** page, you must have valid entries in each of the four boxes.  
For more information, see **General Notifications** in “[Notifications areas](#)” on page 321.
2. In the **SMTP Host**, **SMTP Port**, and **From (email)** boxes on the **SMTP Settings** page, you must have valid entries.  
For more information, see “[SMTP Settings](#)” on page 318.
3. If you intend to enable **Password Expiry Notifications**, you must have a valid entry in the **directory.auth.BaseURL** box on the **System Attributes** page.  
An example of a valid entry is: <http://mymachine.opentext.net:8080/otdsws/login>  
For more information, see [Directory Services Base URL](#) on page 294.

## 12.4.1 Notifications areas

- **General Notifications**
  - **Notification Send Interval (seconds)**: the frequency, in seconds, that OTDS will check to see if a notification email is waiting to be sent. This box is mandatory, and it must contain a positive integer. The default value is 30.
  - **Max retries**: the maximum number of times that OTDS will attempt to send out a notification email. This box is mandatory, and it must contain a positive integer. The default value is 5.
  - **Default Language**: the default language used in the notification emails. This box is mandatory.
  - **E-mail Addresses (comma-separated)**: a comma separated list of email addresses to which both OTDS-specific and license key-specific notifications will be sent.
- **Event Notifications**: before enabling OTDS notifications, you must first complete the requirements listed in “[Requirements before enabling Notifications in OTDS](#)” on page 320.
  - **Enable OTDS Notifications**: determines whether notification emails should be sent for OTDS-specific information.
  - **OTDS Notification Events**: the OTDS events which, if they occur, will be reported in the notification emails.
  - **Event Level**: the OTDS reporting level at, or above which, events will be included in the notification emails. The options are: INFO, WARN, ERROR.  
This box is mandatory. The default value is INFO.
- **License Key Notifications**: before enabling license key notifications, you must first complete the requirements listed in “[Requirements before enabling Notifications in OTDS](#)” on page 320.
  - **Enable License Key Notifications**: determines whether notification emails are enabled for license key-specific information.
  - **License Key Expiration (days)**: the number of days before a license key expires that a notification email is sent.  
If you enabled license key notifications, this box is mandatory. The default value is 14. If you type the number zero in this box, the notification will be sent the day the license expires. If you save a null value to this box, OTDS assumes a zero value.
  - **Expiration Notification Interval (hours)**: the frequency, in hours, that OTDS will check to see if a license key expiration notification email needs to be sent. This box requires a positive integer.  
If you enabled license key notifications, this box is mandatory. The default value is 24.
- **Password Expiry Notifications**: before enabling password expiry notifications, you must first complete the requirements listed in “[Requirements before enabling Notifications in OTDS](#)” on page 320.

- **Enable Password Expiration Notifications:** determines whether notification emails should be sent to notify the administrator when passwords are due to expire.
- **Password Expiration (days, comma-separated):** the number of days before a password expires that a notification email is sent. You can list multiple days separated by commas.

The default setting sends out three notifications before a password expires. Notifications are sent out 30 days prior to expiry, 15 days prior to the expiry, and 5 days prior to the expiry of a user's password.

## 12.4.2 To configure notifications settings

### To configure notifications settings:

1. From the web administration menu, select **System Config**.
2. On the **System Config** page, select the **Notifications Settings** tab.
3. In the **General Notifications** area:
  - a. In the **Notification Send Interval** box, type a positive integer to set the number of seconds that OTDS will wait between checks to see if a notification email needs to be sent.
  - b. In the **Max Retries** box, type a positive integer to set the maximum number of times that OTDS will attempt to send out a notification email. When the number of times set here is reached without the notification email being sent, OTDS will stop trying to send the email.
  - c. From the **Default Language** list, select the default language in which the notification emails will be written. These language files are made available by OTDS. You cannot add your own language or language files for notification emails.
  - d. In the **E-mail Addresses** box, type a comma-separated list of the email addresses to which you want the notifications sent.
4. In the **Event Notifications** area:
  - a. If you want to enable notifications for OTDS-specific information, select **Enable OTDS Notifications**.
  - b. In the **OTDS Notification Events** box, in the **Available Event IDs** box, select each type of OTDS event that, if it occurs, should trigger a notification email, and then click **Add**. To select multiple events, hold the **CTRL** key while selecting each of the event types.

After an event has been added to the **Selected Event IDs** box, you can remove that event by selecting it and then clicking **Remove**.
  - c. In the **Event Level** box, select the level of OTDS events that will trigger a notification email.

If you select "Info" you will receive email notifications for every INFO, WARN, and ERROR event associated with the event IDs you selected in **Selected Event IDs**.

If you select “Warn” you will receive email notifications for every WARN and ERROR event associated with the event IDs you selected in **Selected Event IDs**.

If you select “Error” you will receive email notifications for every ERROR event associated with the event IDs you selected in **Selected Event IDs**.

5. In the **License Key Notifications** area:
  - a. If you want to enable notifications for license key-specific information, select **Enable License Key Notifications**.
  - b. In the **License Key Expiration** box, type a positive integer to indicate the number of days before a license key will expire that a notification email will be sent.

If you type “0”, zero, your email notification will be sent the day that the license key expires.
  - c. In the **Expiration Notification Interval** box, type a positive integer to indicate the number of hours that OTDS will wait between checks to see if a license key expiration notification needs to be sent.
6. In the **Password Expiry Notifications** area:
  - a. If you want to enable notifications prior to a password expiring, select **Enable Password Expiration Notifications**.
  - b. If you want to change the number of notifications sent, or the number of days prior to password expiry that a notification is sent, edit the **Password Expiration (days, comma-separated)** box.



## Chapter 13

# Multiple instances of Directory Services

An administrator can set up multiple instances of OTDS across multiple servers. This section describes setting up and administering multiple instances of Directory Services.

At installation time, the administrator chooses whether that specific OTDS installation is the initial OTDS instance or a supplementary instance in an existing environment. On the **Directory Services Parameters** window of the OTDS installation wizard, the administrator is prompted to select a box if they want this particular installation to function as a supplementary instance. When installing the initial instance, the **Synchronization Master Host** will be set to that instance.

For more information, and depending on your operating system, see either “[Installing OTDS on Windows from the UI](#)” on page 26 or “[Installing OTDS on Linux interactively](#)” on page 35.

Because multiple instances within an OTDS environment function as multi-master, there is no “master” host. The **Synchronization Master Host** is the instance responsible for running synchronized user partitions. Administrators can designate any server in their OTDS environment as their **Synchronization Master Host**. The **Synchronization Master Host** setting is stored in the database. It is therefore read by, and applies to, all instances. For more information, see “[Changing the synchronization master host](#)” on page 326.

## Benefits and restrictions of multiple instances

### Benefits:

1. Setting up multiple instances will allow you to avoid single point of failure.
2. All OTDS instances connect to the same database. This means that all instances can be written to, as well as read from.
3. OTDS allows you to set up as many servers as you need.

### Restriction:

Enterprise Sync, used for synchronization of AD and LDAP partitions, can only run on one server, the **Synchronization Master Host**.

## If you are upgrading a replicated environment of OTDS from an older version that uses OpenDJ to version 25 or newer

If your existing OTDS environment is a replicated environment, and you want to upgrade to version 25, you need to follow these steps:

1. Stop OTDS on each replica in your environment by stopping your web application server.  
This is required to prevent data from being created or updated in OpenDJ by a secondary instance after data has been migrated by the primary instance.
2. On the server that has the primary instance of OTDS installed, run the OTDS version 25 installer, and upgrade the primary instance. Next, do the following:
  - Ensure the server is operational and content from OpenDJ has been imported successfully to the database.
  - Manually remove OpenDJ from the server once it is no longer needed as a backup. To manually remove OpenDJ, see [How do I uninstall OpenDJ? on page 394](#).
3. OpenText recommends that you uninstall OTDS on each replica server.  
Although patching each replica server is possible, depending on your previous version, the data encryption key may need to be manually copied to each `otds.properties` file.
4. Reinstall OTDS on each replica server in your environment. During installation, on the **Directory Services Parameters** page, select the option to install as a supplementary instance. You will be prompted to provide the encryption key from the primary instance.

For more information, see “[When upgrading and importing data from previous versions of Directory Services](#)” on page 20.

## 13.1 Changing the synchronization master host

### To change the synchronization master host:

1. From the web administration menu, select **System Config**. On the **System Config** page, select the **System Attributes** tab.
2. On the **System Attributes** page, find the **Synchronization Master Host** system attribute.
3. In the **Value** box, type the fully qualified server name or the IP address of your new master host. For example: “computer60.mycompany.net” or “101.5.8.93”.
4. Click **Save**.
5. Restart Tomcat on all OTDS instances in your environment.

# Chapter 14

## Trusted Sites

The **Trusted Sites** page allows you to specify a list of trusted addresses that Directory Services will allow to refer to a forwarding address. During authentication, if the referring URL contains a forwarding address, Directory Services will redirect the user's browser to that address. This is necessary so that Directory Services can point the user's browser back to the originating address. For example, the user accesses OpenText Content Management and OpenText Content Management redirects to Directory Services for authentication. After authenticating, Directory Services will redirect the user's browser back to OpenText Content Management if the OpenText Content Management URL is a trusted referring address.

An example of a trusted site is: `http://mymachine.opentext.net/`

Trusted sites can be entered as a URL or entered as a Regular Expression (regex). If you do not use a Regular Expression, the configured value is treated as a prefix for string comparison.

**!** **Important**

A full URL is required when entering a trusted address. OTDS will ignore the string “http” or “https”, if either is listed alone, without a hostname.

For more information, see the examples in “[Customizing trusted referrals](#)” on page 328.



**Note:** If your environment has multiple OTDS server nodes, any configuration changes to “[Authentication Handlers](#)”, “[Trusted Sites](#)”, or “[System Config](#)” can take up to one minute to take effect across all OTDS server nodes.

### Trusted Sites buttons

On the main **Trusted Sites** page, there are buttons on the button bar specific to this page. The following are quick links to the procedures associated with each:

Button	Associated procedure
Add	<a href="#">“Adding a trusted referring address” on page 328</a>
Delete	<a href="#">“Removing a trusted referring address” on page 329</a>
Help	Opens context-sensitive help for the page you are currently using.

## 14.1 Customizing trusted referrals

➡ **Example 14-1: If the list of “Addresses Directory Services will redirect requests to” includes `http://mysafesite.domain.com/`, the following redirect URLs would be allowed to redirect:**

- `http://mysafesite.domain.com/my-application`
- `http://mysafesite.domain.com/my-other-application`

and the following will be disallowed:

- `http://unsafesite.domain.com/xyz`



➡ **Example 14-2: If Directory Services should allow redirect to all https sites on opentext.com, include the following Regular Expression (regex) to the list of “Addresses Directory Services will redirect request to”:**

`https://[A-Za-z0-9-]+\.opentext\.com/.*`



## 14.2 Adding a trusted referring address

**To add a trusted referring address:**

1. From the web administration menu, click **Trusted Sites**.
2. In the **Trusted Sites** page, from the button bar, click **Add**.
3. In the **Addresses Directory Services will redirect requests to** box, enter an address that you would like to be trusted to redirect incoming authentication requests to a forwarding address. See “[Customizing trusted referrals](#)” on page 328 for examples.



**Note:** A full URL is required. OTDS will ignore the string “http” or “https”, if either is listed alone, without a hostname.

4. Click **Save**. You may need to refresh the page to see the trusted address in the **Addresses Directory Services will redirect requests to** box.
5. **Optional** Repeat these steps until you have added all trusted addresses.

## 14.3 Removing a trusted referring address

### To remove a trusted referring address:

1. From the web administration menu, click **Trusted Sites**.
2. In the **Trusted Sites** page, select the box to the left of the trusted site you want to delete.
3. From the button bar, click **Delete**. There is no confirmation step. After you click **Delete**, the trusted site is removed.
4. **[Optional]** Repeat these steps until you have deleted all the trusted addresses you want to remove.



# Chapter 15

## License Keys

Directory Services provides the **License Keys** tab in OTDS to create, implement, and manage all licenses for OpenText products. Some OpenText products require a license to ensure that the full functionality of that product is available to users. Examples of OpenText products that require a license include:

- **OpenText Content Management**
- **WebReports**
- **Object Importer / Object Exporter**

OpenText recommends that you install OTDS prior to installing the OpenText product that you will be licensing. Provided you have installed the two products in that order, your OpenText product, at installation, may create a partially completed license in OTDS ready for you to edit and complete. This partially completed license is referred to as a license stub.

After you complete a license in OTDS, you need to acquire a license file from OpenText and then apply that license file to the **License Key** box in OTDS.

### License keys Actions menu options and buttons

On the **License Keys** pages, each license has an associated **Actions** menu and applicable buttons. The following are quick links to the procedures associated with each:

#### License keys Actions menu options

Actions menu option	Procedure or background section
Properties	<a href="#">"Editing a license key" on page 341</a>
View Counters	<a href="#">"Understanding allocating and reserving licenses to users, groups, and partitions" on page 336</a>
Generate Report	<a href="#">"Generating a Report" on page 345</a>
Set Shared	<a href="#">"Sharing Licenses" on page 338</a>
View Licensees	<a href="#">"Viewing licensees" on page 343</a>
Add License Key	<a href="#">"Adding a license key" on page 343</a>
View Reserved Seats	<a href="#">"Reviewing reserved seats" on page 342</a>
Allocate to License	<a href="#">"Allocate to license" on page 247</a>  This menu option can be accessed from the <b>Users and Groups</b> page.

### License keys buttons

Button	Associated Procedure
Add	<a href="#">"Creating and submitting a license key" on page 339</a>
Delete	<a href="#">"Deleting a license key" on page 343</a>
Refresh	Use the <b>Refresh</b> button to verify if OTDS has completed an action. For example, after deleting.
Generate Report	<a href="#">"Generating a Report" on page 345</a>
Show Certificates/Show License Keys	<a href="#">"Showing license certificates" on page 345</a>
Help	Opens the context-sensitive help for the page you are currently using.

## 15.1 Overview of License Keys tab

The **License Keys** tab of the OTDS web admin client provides the full functionality to create and manage licenses for your users. Descriptions of the terms used in this section are:

---

#### License Key

The secured content that enables specific features within an application. There are two formats for license keys supported by OTDS:

- The SafeNet format is a single line that is difficult to read.
- The OpenText Format uses an INI style of formatting and is easy to read.

---

#### License Key File

A file containing license key content and a license key certificate.

---

#### License Certificate

A feature of a license key that is used to prove the license key content is valid and has not been damaged. A license certificate may or may not be shared among multiple license keys.

---

#### Floating License

A license key that allows the temporary use of the product, or a feature of the product, for a defined period.

---

#### License Record

A record within Directory Services used to store the license key, usage information, and the connection between a product and resources.

---

#### License Stub or Partial License

Some products can create placeholder license records to make it easier to install license keys by pre-populating many boxes in a license record. Some products require specific names for their license records and an automatically generated stub reduces the possibility of errors in the license record creation. This is the

primary reason why it is recommended to install OTDS before installing the product to be licensed. If you install the product to be licensed first, the product will not be able to create the stub.

## License keys fields

The following list describes the required and optional boxes for licenses. Some of these boxes are displayed on the main **License Keys** page.

### License Key Name

- **Description:** the unique name that was assigned when your license was created. If the OpenText product you are licensing has supplied the name to your license you cannot edit this box. If you are creating a license, you must type a unique name. The license name is stored in LDAP.
- **Default Status:** displayed.

---

### ID

- **Description:** this box cannot be edited. It will contain the unique name entered in the **License Key Name** box.  
An example of a license key ID: dc=unique\_license\_key\_name,ou=Licenses,dc=identity,dc=opentext,dc=net
- **Default Status:** not displayed.

---

### Description

- **Description:** you can optionally type a description for your license.
- **Default Status:** not displayed.

---

### Resource ID

- **Description:** every license must be linked to a resource. If the OpenText product you are licensing has applied the resource ID to your license you cannot edit this box. While multiple licenses can be linked to the same resource, most resources will have only one license linked.
- **Default Status:** displayed.

---

### Application Fingerprint

- **Description:** if you have a license stub, this box will have been pre-populated during the stub creation, otherwise, you should populate it with the appropriate value from your application. The value in this box will be added to the license key file that is generated. You can edit this box.

You will need to copy the string from this box and enter it into the **License Fingerprint** box on the OpenText Product Activation form to send to

OpenText support. After you send the string to OpenText support, they will provide you with a license key.

- **Default Status:** not displayed.

---

#### License Fingerprint

- **Description:** this box cannot be edited. It is populated from the license file.
- **Default Status:** not displayed.

---

#### Product

- **Description:** if the OpenText product you are licensing has supplied information to the boxes of this license, you cannot edit this box. It will be populated from the license file that you apply to the license.
- **Default Status:** displayed.

---

#### Version

- **Description:** if the OpenText product you are licensing has supplied information to the boxes of this license, you cannot edit this box. It will be populated from the license file that you apply to the license.
- **Default Status:** not displayed.

---

#### Model

- **Description:** this box cannot be edited. It describes the nature of the license. It will be populated from the license file that you apply to the license. Possible values include: TRANSACTION\_BASED, USER\_BASED, and VOLUME\_BASED.
- **Default Status:** not displayed.

---

#### Creation Date

- **Description:** the date that this license was created. This date is coded in the **License File** that OpenText support sends you.
- **Default Status:** not displayed.

---

#### Expiry Date

- **Description:** the date that your license will expire. This date is coded in the **License File** that OpenText support sends you.
- **Default Status:** displayed.

---

### Last Modified Date

- **Description:** the date of the last time that your license was used. This date is coded in the **License File** that OpenText support sends you.
  - **Default Status:** not displayed.
- 

### License Key Type

- **Description:** this box cannot be edited. It will be populated from the **License File** that you apply to the license. Possible values include: NON\_PRODUCTION, PRODUCTION, and TEMPORARY.
  - **Default Status:** not displayed.
- 

### Unit of Measurement

- **Description:** if your license is user-based, then this value is set to “user”. If your license is volume-based, then this value is set to a positive integer representing the number of bytes. If your license is transaction-based, then this value is set to a positive integer representing the number of transactions. This information is coded in the **License File** that OpenText support sends you.
  - **Default Status:** not displayed.
- 

### Unit Measurement Reset

- **Description:** this box contains either a unit of time or “never”. It indicates the frequency of the reset for recurring usage allocations. Examples include “10GB per Month” and “1000000 Transactions per Year”. This information is coded in the **License File** that OpenText support sends you.
  - **Default Status:** not displayed.
- 

### Total Users Allowed

- **Description:** the total number of users permitted by this license to access the product to which it relates.
  - **Default Status:** not displayed as its own field, but total users can be viewed in **License Key Usage**.
- 

### Current Users

- **Description:** the number of current users accessing the product relating to this license.
  - **Default Status:** not displayed as its own field, but current users can be viewed in **License Key Usage**.
-

### License Key Usage

- **Description:** the usage statistics for the main product of your license. The format is: <current\_users>/<total\_users>. If you want to see usage statistics for separately licensed features of your product, see “[Licensees and counters](#)” on page 339.
- **Default Status:** displayed.

---

### Status

- **Description:** you cannot edit this box. It displays the current status of your license. Possible values include: VALID, INVALIDFP, or EXPIRED.  
INVALIDFP indicates that the application fingerprint does not match the license's content. It is intended to indicate if an incorrect license file has been loaded into an incompatible license record. If this happens, the license will still be served to the application, but it will most likely fail to load. If you see a status of INVALIDFP, update the application fingerprint to match the actual installation, or load a different license file.
- **Default Status:** not displayed.

---

## 15.2 Understanding allocating and reserving licenses to users, groups, and partitions

The license you receive from OpenText for your product is one that you have negotiated with OpenText. There can be different variations for licensing. In general, a license is based on either:

- Different users accessing and using the product, or feature of the product, with their individual userID.
- Different locations accessing and using the product, or features of the product, with their individual access fingerprints. Your product implementation determines the fingerprint format. Two examples of fingerprint format include: computer IP address, or the location of the installed product.
- Use of the product, or features of the product, transactionally. Each transaction will be tracked by OTDS.

For more information, see “[Allocate to license](#)” on page 247 and “[Viewing licensees](#)” on page 343.

### Counters

The use of the product is tracked by counters. A counter might refer to a product or to a feature of a product. These counters can be viewed on the **License Keys** page. Counters track the usage of the features of the product you licensed.

For example, a product might be licensed for usage in its entirety, and it might also be licensed at the level of each individually defined feature of that product. If your

product can be licensed at multiple levels, you can view the individual license options by selecting **View Counters** from the license's **Actions** menu. The top listed counter tracks the usage or transaction for the main level of the product.

If your product is licensed at the main level only, selecting **View Counters** from the license's **Actions** menu will display only one counter for that main license.

For more information, see “[Reviewing reserved seats](#)” on page 342.

If your product is licensed to use shared licenses, you can view the individual license usage by selecting **View usage** from the license's Actions menu on the **Counters** page. For more information, see “[Viewing shared license usage](#)” on page 344.

### 15.2.1 Allocation and reviewing reserved seats

Allocation gives a user, group, or partition permission to use the product or feature. Products and features of products with any usage type can be allocated. The administrator allocates a user, group, or partition.

If a user, group, or partition is allocated to the main level of the product, then that user, group, or partition is allocated to all individually defined features of that product.

Reserving occurs when the product or feature is used. Reserving does not apply when the usage of the product, or feature of the product, is of usage type “Transactions”. Users can be reserved to the product, or to features of the product, when the usage of the product is of usage type “Users”. Any user can reserve, provided that user, or the group or partition to which they belong, have first been allocated.

The administrator determines which users have permission to access a product or a feature of a product. The administrator can allocate to a user, a group, or a partition. Allocating a user, group, or partition to a license does not affect the unit usage count on a **Counters** page. When a user is allocated to a product, or a feature of a product, they only have permission to access that product or feature. They must then make use of that product or feature for that usage to show up in the unit usage count.

Once a user makes use of that allocation, that use is called reserving a count in the license count. In other words, using their allocation, reserves one of the available counts in the product, or feature of the product. This action is tracked by OTDS.

When the administrator examines the reserved seats for any license, each reserved seat represents a specific userID accessing the product or feature of the product.

For more information, see “[Allocate to license](#)” on page 247, “[Viewing licensees](#)” on page 343, and “[Reviewing reserved seats](#)” on page 342.

## 15.2.2 Sharing Licenses

Several tenants who use one OTDS system are able to share licenses, provided:

1. The product must allow a license to be shared.
2. The setting, `shared` must be enabled in the license file.
3. The license must be installed in an OTDS system tenant.

No information is shared between tenants, and they cannot see each others' user groups or partitions. A license is installed once, then shared among the tenants. Only your system tenant administrator can see the license usage by each tenant.

### 15.2.2.1 Setting a shared License

**To set a shared license:**

1. From the web administration menu, click **License Keys**.
2. From the **Actions** menu associated with the license you want to share, click **Set Shared**.



**Note:** A **License: Set Shared** message asks you to confirm:

- Users in all tenants will have access to this license.
- It will not be possible to unshare the license if it has been allocated, reserved, or used.
- It will not be possible to unshare the license if it has been assigned to any users, groups, or partitions.

3. If this license is available to be shared, when you click **OK**, the **Shared** column will indicate **Yes**.

A message will appear if this license cannot be shared.

4. An OTDS administrator has the option to click the **Show Shared License Keys** button to display only shared licenses.

### 15.2.2.2 Unsetting a Shared License



**Important**

OpenText recommends that you do not select the unshare option unless you have advanced knowledge of licensing for your product.

**To unset a shared license:**

1. From the web administration menu, click **License Keys**.
2. From the **Actions** menu associated with the license you want to unshare, click **Unset Shared**.



**Note:** A “License: Unset Shared” message asks you to confirm, since you cannot unshare a license if it is allocated, reserved, or used.

When you click **OK**, a warning message is displayed if the license has allocated objects or some usage.

### 15.2.3 Licensees and counters

On the **License Keys** page, select **View Counters** from any license's **Actions** menu. On this page you will see:

---

#### Counter name

The name of the licensed product appears in the first position. If your **Counters** page contains multiple entries, the subsequent entries are the individually licensed features of that product.

---

#### Unit name

The type of licensing used for this product and its features. This may be:

- **Users:** this license specifies the number of unique users, as determined by userID, who can access the product or feature of the product.
- **Seats:** this license specifies the number of unique computers, as determined by the fingerprint, that can access the product or feature of the product.
- **Transactions:** this license specifies the number of unique transactions that can be performed using this product or feature of the product.

---

#### Unit count

The total number of available users, seats, or transactions.

---

#### Unit usage

The number of users, seats, or transactions in the license that are currently in use.

---

#### Actions

The menu that allows you to **View Licensees** and to **View Reserved Seats**. For more information, see “[Viewing licensees](#)” on page 343 and “[Reviewing reserved seats](#)” on page 342.

## 15.3 Creating and submitting a license key

### To create and submit a license key:

1. From the web administration menu, click **License Keys**.
2. On the **License Keys** page, do one of the following:
  - The product you want to license may have created a partial license stub that you will see on this page. Do one of the following:

- If a partially completed license stub appears in the list of licenses on this page, and you have retrieved your license file from OpenText, you can proceed to “[Adding a license key](#)” on page 343.
  - If a partially completed license stub appears in the list of licenses on this page, and you have *not* yet retrieved your license file from OpenText, then from the **Actions** menu of this license stub, click **Properties**.
- If no partially completed license stub appears, from the button bar click **Add**.
3. On the **General** page, do the following:
    - a. The **License Key Name** box is mandatory. In the **License Key Name** box, choose one of the following:
      - If you are completing a partial license stub, the **License Key Name** box cannot be edited.
      - If you are creating your license, type a unique name for this license. You will not be able to edit this name later, and a license cannot be deleted after usage. OpenText recommends that you type a name that references the product you are licensing. Two examples of possible license key names:
        - Production Content\_Server License
        - Production WebReports License
    - b. The **License Key ID** box cannot be edited. The license key ID will appear according to the value found in the **License Key Name** box.

For example, “dc=Content\_Server License  
16.2,ou=Licenses,dc=identity,dc=opentext,dc=net”.
    - c. **Optional** In the **Description** box, you can choose to type a description of this license. The **Description** box is optional, however if you leave this box empty, OTDS will input the product name and version of the product for which this license was created, which you can later edit.
    - d. The **Resource ID** box is mandatory, as every license must be linked to a resource. From the **Resource ID** list:
      - If you are completing a partial license stub, the OpenText product you are licensing has applied the resource ID, and you cannot edit this box.
      - If you are creating your license, you must have first created a resource in Directory Services for this OpenText product. For information about resources, see “[Resources](#)” on page 173.

Select the resource ID corresponding to the OpenText product that you will be licensing. The **Resource ID** box cannot, later, be edited.
    - e. In the **Application Fingerprint** box, if you are licensing OpenText Content Management, and if you are directed by the licensing process, type the source to be used to generate the license. The **Application Fingerprint** box will generate an encrypted string in the **License Fingerprint** box.

If you are not licensing OpenText Content Management, this box is not applicable.

4. Copy the text in the **License Fingerprint** box. Sign in to support.opentext.com with your userid and password, and then:
  - a. On the main support page, from the **Accounts** menu, select **Activations/Keys**.
  - b. On the **Product Activation** page, find the product that you will be licensing. Under the **Actions** heading, click **Produce License Key**.
  - c. In the **Activations** box, paste the text that you copied from the **License Fingerprint** box.
5. You will receive a **License File** from OpenText. Back in the OTDS user interface, select the **License Key** tab.
6. On the **License Key** page, you can type, paste, or upload the license file that was provided to you by OpenText. To browse your system, click **Get License File**. The **License Key** box is mandatory.
7. Click **Save**.

## 15.4 Editing a license key

### To edit a license key:

1. From the web administration menu, click **License Keys**.
2. From the **Actions** menu of the license you want to edit, click **Properties**.  
The **Edit License** wizard will guide you through the steps to edit an existing license.
3. On the **General** page, there are only two boxes that can be edited: **Description** and **Application Fingerprint**. Do the following:
  - a. You cannot change the **License Key Name** box.
  - b. You cannot change the **License Key ID** box.
  - c. **Optional** In the **Description** box, you can change the description to reflect how this license is used and applied.
  - d. You cannot change any other box on this page.
  - e. Click **Save** if you have finished editing your license, or click the **License Key** tab.
4. On the **License Key** page, enter the new license file that has been provided to you by OpenText. Putting a new license file into this box will only update the license key. Your usage units for this license will not be affected.  
You can click **Get License File** to browse to select your license key file and apply it.
5. The **License Certificate** page cannot be edited.

6. On the button bar, click **Save**.

## 15.5 Reviewing reserved seats

**To review reserved seats:**

1. From the web administration menu, click **License Keys**.



**Note:** View reserved seats to view actual usage of the license. If, instead, you want to view users allocated to a license, see “[Viewing licensee](#)s” on page 343.

2. From the **Actions** menu associated with the license whose licensee's usage you want to view, click **View Counters**.



**Note:** If the license you chose showed a **Unit Usage** of zero, “0”, then the **View Reserved Seats** page will be blank, because no allocated resource used that license.

3. On the **Counters** page, from the **Actions** menu of the counter whose licensee's you want to view, click **View Reserved Seats**. This only applies to counters with a **Unit Name** of “Users”.
4. Review the information provided. The information includes:

- **Name:** the name of the user.
- **ID:** the ID of the user.
- **Tenant:** the organizations that share this OTDS system, and also share this license. You can use the search box to find tenants.
- **User Partition:** the user partition to which the user belongs.
- **Actions:** from this menu you can select **Revoke Reservation** to remove the user's current reservation of a seat in the license.

Only the OTDS administrator can select this option. An administrator might revoke a reservation when a user changes departments and no longer requires access to the product or feature of the product.

**!** **Important**

- The OTDS administrator will only be able to revoke a reserved seat if the permissions set on the license allow for revocation of reservations. Your license determines if you are permitted to revoke reservations.
- OpenText recommends that you do not select the revoke option unless you have advanced knowledge of licensing for your product.

## 15.6 Deleting a license key

### To delete a license key:

1. From the web administration menu, click **License Keys**.



#### Caution

Deleting a license key cannot be undone.

2. Select the box to the left of the license you want to delete, and then, on the button bar, click **Delete**.



**Note:** Any license that has licensees, who generate usage records, cannot be deleted, as usage records cannot be deleted.

3. In the **Delete** box, click **OK** to confirm or click **Cancel** to keep the license.

## 15.7 Adding a license key

### To add a license key:

1. From the web administration menu, click **License Keys**.
2. If you have a license stub that has been created for you, from the **Actions** menu of that license stub click **Add License Key**.
3. In the **Add License Key <product\_name>** box, and provided you have already retrieved your license key file from OpenText, click **Get License File** to select the license key file.
4. After your license key file content appears in the **License Key** box, click **OK**.

## 15.8 Viewing licensees

### To view licensees:

1. From the web administration menu, click **License Keys**.



**Note:** This page displays users allocated to a license. If, instead, you want to view actual usage of the license, see “[Reviewing reserved seats](#)” on page 342.

2. From the **Actions** menu associated with the license whose licensees you want to view, click **View Counters**.
3. On the **Counters** page, from the **Actions** menu of the counter whose licensees you want to view, click **View Licensees**.
4. Review the information provided. You can select the **Users**, **Groups**, or **Partitions** tab to view the licensees by users, group, or partition.

All users who are members of a group or partition will not be displayed. Only those users who have been directly allocated to the license.

The information includes:

- **Name:** the name of the user, group, or partition licensee.
- **ID:** the ID of the user, group, or partition.
- **User Partition:** the user partition to which the licensee belongs.
- **Actions:** from this menu you can select **Deallocate from License**. For more information, see “[Allocate to license](#)” on page 247.

**!** **Important**

OpenText recommends that you do not select the de-allocate option unless you have advanced knowledge of licensing for your product.

## 15.9 Viewing shared license usage

After a license is shared, you can see the usage. For more information, see “[Sharing Licenses](#)” on page 338.

### To view shared licenses usage:

1. From the web administration menu, click **License Keys**.
2. From the **Actions** menu associated with the license whose licensees you want to view, click **View Counters**.
3. On the **Counters** page, from the **Actions** menu of the counter whose licensees you want to view, click **View usage**.



**Note:** A **Tenant Usages** message box displays the Tenant names, and their associated Usage numbers. Only the OTDS administrator can see the numbers for all tenants. Usage information is not shared among different tenants.

4. Review the information provided. You can select the **Users**, **Groups**, or **Partitions** tabs to view the licensees by users, group, or partition.

All users who are members of a group or partition will not be displayed. Only those users who have been directly allocated to the shared license will be displayed.

The information includes:

- **Name:** the name of the user, group, or partition licensee.
- **ID:** the ID of the user, group, or partition.
- **Display Name:** an optional entry, if defined
- **Tenant:** the organizations that share this OTDS system, and also share this license. You can use the search box to find tenants.
- **User Partition:** the user partition to which the licensee belongs.
- **Actions:** from this menu you can select **Deallocate from License**. For more information, see “[Allocate to license](#)” on page 247.

## 15.10 Generating a Report

### To generate a report:

1. From the web administration menu, click **License Keys**.
2. From the **Actions** menu associated with the license whose report you want to generate, click **Generate Report**.
3. On the **Generated Report - <license\_name>** page, you need to select the parameters that will be used to generate this report, as well as the type of report you want to generate:
  - **Start Date:** from the list boxes, select the month and year that will be the start date for the data this report will generate.
  - **End Date:** from the list boxes, select the month and year that will be the end date for the data this report will generate.
  - **Report:** from the list boxes, select the type of report that you want to generate. Reports can be generated for a single license record or for multiple license records. Your options are:
    - **Compliance:** select this report to generate statistics on your usage compliance with your license.
    - **Summary:** select this report to generate high-level information about your license usage.
    - **Details:** select this report to generate detailed information about your license usage.
    - **User Reallocation:** select this report to generate information about the allocation of users to this license.
4. If you want to generate the report on the page, click **Generate Report**. If you want to save the report to your system, click **Download Report**.
5. Click **OK**.

## 15.11 Showing license certificates

### To show license certificates:

1. From the web administration menu, click **License Keys**.  
The default display is the **License Keys** display which shows the following columns: License Key Name, Resource ID, Expiry Date, License Key Usage, Product, Actions.
2. On the **License Keys** button bar, click **Show Certificates**.
3. The columns on the main **License Keys** page have now changed to show the data for the OpenText certificate associated with each license. The columns now displayed are: Certificate Name, Expiry Date, Actions.

4. After you have examined the license certificates information, click **Show License Keys** to return to the main licenses box display.



**Note:** A license certificate cannot be deleted if it is in use by a license.

## 15.12 Auditing Licensing events

You can audit licensing events on the **Audit Reports** page. The licensing events you can review on this page include:

- Add license: an audit event is recorded to document adding, changing, or deleting licenses.
- Update license: an audit event is recorded to document adding, changing, or deleting licenses.
- Delete license: an audit event is recorded to document adding, changing, or deleting licenses.
- Change usage: an audit event is recorded to document a change to the use of the license by users.
- Replace usage: an audit event is recorded to document the use of the license by users.
- Reset usage: an audit event is recorded to document when the use of the license by users is reset.
- Allocate user or group or partition: an audit event is recorded when any user, group, or partition is allocated to the license or to a feature of the license.
- Deallocate user or group or partition: an audit event is recorded when any allocated user, group, or partition is removed from the license or from a feature of the license.
- Reserve seat: an audit event is recorded when a user is first reserved to a license.
- Revoke seat: an audit event is recorded when a user's reservation is removed from a license.

For more information, see “[Audit Reports](#)” on page 367.

## 15.13 Examining License Key Logging Information

Directory Services license key issues are logged to the “[otds.log](#)” on page 375 file.

# Chapter 16

## Single Sign On

This section describes password interactions with single sign on; provides some background and direction on the service principal name system attribute; describes customizing the login user name format; describes some common single sign on scenarios; and explains single sign out.

### Password interactions with web-based single sign on

This section describes password interactions with web-based single sign on. When a user from a non-synchronized user partition tries to sign in with an expired password, they must provide and confirm a new password that satisfies the password policy. The new password interaction will require the user to specify their current, expired password.

 **Note:** A password is considered *expired* if **Require password change on reset** is selected when the password of a non-synchronized user is reset. For more information, see “[Resetting a user password in a non-synchronized user partition](#)” on page 113.

When a user from a synchronized user partition tries to sign in with an expired password, they will be rejected. Error conditions will be sent back from the LDAP provider to indicate why the user's password was rejected. In this scenario, the user will not be able to sign in through the Directory Services web interface until they have obtained a valid password from their resource.

The Directory Services web-based sign-in page may be customized to match your local interface standards. To customize the sign-in page, you can edit the .jsp files found in `<OTDS_installdir>\otdswebs\WEB-INF\jsp`. You can also add product specific banners in `<OTDS_installdir>\otdswebs`. See “[Customizing Directory Services](#)” on page 353 for information about how to perform these edits.

### 16.1 Customizing the login user name format

By default, a user can enter a user name that corresponds to values stored in their `oTExternalID1`, `oTExternalID3` and `oTExternalID4` attributes. For example, a user `OPENTEXT\franz` would have the following attributes:

- `oTExternalID1 = franz`
- `oTExternalID3 = franz@opentext.net`
- `oTExternalID4 = OPENTEXT\franz`

 **Note:** The values in `oTExternalID1-4` attributes in synchronized partitions depend upon the configuration of the synchronized user partition. For more information, see “[The OTDS unique ID](#)” on page 72.

Users can use any of these formats to sign in. To change this behavior, and allow users to sign in with a value corresponding to a different attribute, for example mail, modify the **Login User Name Attributes** property value. See [Login User Name Attributes on page 305](#) for more information.



**Note:** If more than one account is found using the login name entered, the user will not be able to sign in. A corresponding message with the string MULTIPLE\_IDENTITIES\_FOR\_USER\_NAME will be logged in the file directory-access.log. In this condition, no actual authentication attempt is performed against the LDAP server in order to prevent locking out accounts. See [How do I resolve “MULTIPLE\\_IDENTITIES\\_FOR\\_USER\\_NAME” errors when different users are registered with the same email account in OTDS? on page 407](#) for more information.

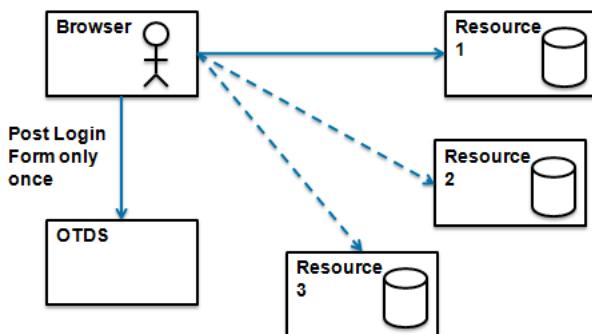
## 16.2 Single sign on scenarios

This section describes the following single sign on scenarios:

- “Basic single sign on” on page 348
- “Single sign on with a portal-style application” on page 349
- “Single sign on with integrated Windows authentication” on page 349
- “Client to server” on page 350
- “Server to server identity assertion” on page 351

### 16.2.1 Basic single sign on

In this scenario, Directory Services provides single sign on to multiple resources accessed from a browser window. Sign-on credentials are only requested once.



**Figure 16-1: Basic single sign on**

## 16.2.2 Single sign on with a portal-style application

In this scenario, a portal-style application embeds a resource HTML user interface.

1. The user signs in to the Portal Application which is not aware of Directory Services.
2. A custom HTTP authentication handler for the Portal Application user ticket is invoked.
3. The user is signed in silently to the embedded resources.

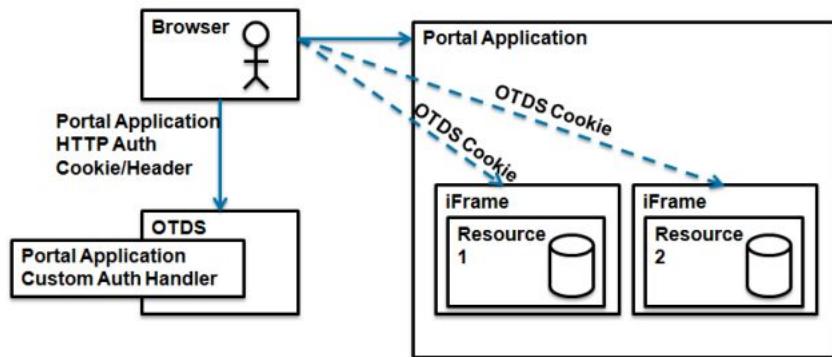


Figure 16-2: Single sign on with a portal-style application

## 16.2.3 Single sign on with integrated Windows authentication

In this scenario, Integrated Windows Authentication is used. There is no form to post. Directory Services handles the Kerberos/NTLM token. The resource does not need to be Kerberos-enabled.

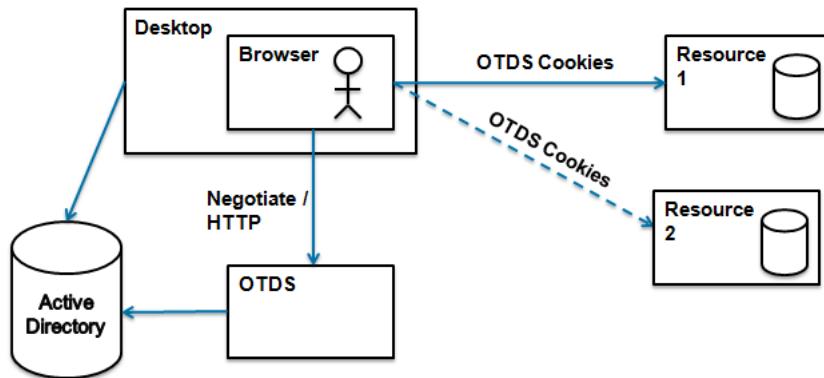
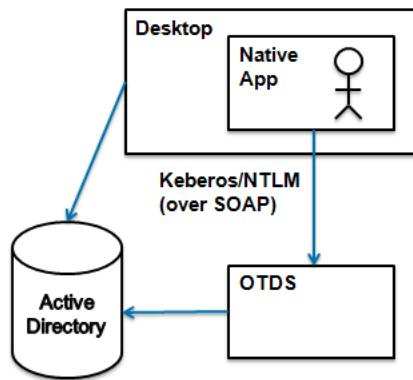


Figure 16-3: Single sign on with integrated Windows authentication

### 16.2.4 Client to server

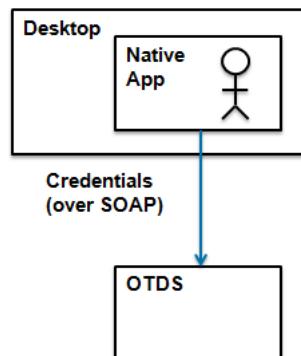
In this scenario, Directory Services client to server interactions are shown for Integrated Windows Authentication and basic user name and password authentication.

Integrated Windows authentication:



**Figure 16-4: Integrated Windows authentication**

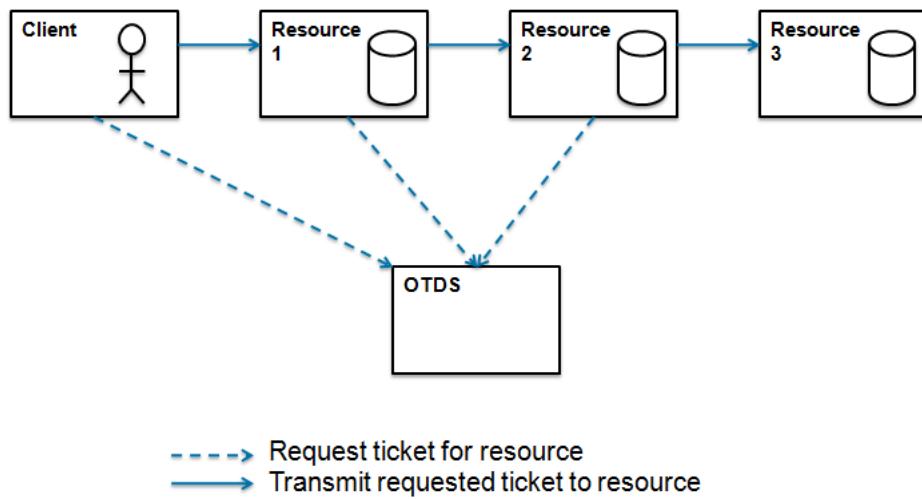
User name and password:



**Figure 16-5: User name and password**

### 16.2.5 Server to server identity assertion

In this scenario, Directory Services securely carries user information between integrated resources.



**Figure 16-6: Server to server identity assertion**

## 16.3 Single sign out

When a user can access OTDS for single sign on, that user can be signed in to multiple applications, depending on how the administrator has set up the OTDS environment. In effect, the user signs in once to OTDS, and is then silently signed in to different applications.

OTDS will now support single sign out across all OpenText products, after those products have also implemented this support. OTDS will inform all applications that are part of the user's sign-in session that the user wants to sign out. The applications will sign the user out and clear their authentication token or cookie. OTDS will also clear its authentication token or cookie.

The administrator needs to configure this option for users by applying the necessary information to either the resource or the OAuth client. For more information, see the **Sign out URL** and **Sign out Method** boxes in “[OAuth Clients](#)” on page 275 or “[Resources](#)” on page 173.

If the OpenText product has implemented this support, that product's documentation will supply the necessary information for the OTDS required boxes.

### Exception to single-sign out

It is possible for an OpenText product to direct that when a user signs out of that product, only that product will sign the user out and clear their authentication token

or cookie. Under those circumstances, OTDS will not clear its authentication token or cookie. The OpenText product effects this direction using the **Sign out URL** and **Sign out Method** boxes. That OpenText product's documentation will supply the necessary information. For more information, see the **Sign out URL** and **Sign out Method** boxes in “[OAuth Clients](#)” on page 275 or “[Resources](#)” on page 173.

Generally, the OpenText product's resource in OTDS will need its **Sign out URL** box set to:

```
<product_URL>/?func=otdsintegration.logout
```

This will direct the user to a product-specific sign out page to ensure that the user only signs out of that product. The user will remain signed in to OTDS.

# Chapter 17

## Customizing Directory Services

This section describes how to customize the OTDS sign-in page and the emails that OTDS sends to your users. It also describes how to customize the user and group attribute mappings that you can define between OTDS and your resource, for example OpenText Content Management.

### Customizing the sign-in page and emails

OTDS includes a number of XSLT stylesheets and graphics that you can edit to effect sign-in page and email customization. These files can be found in the `<OTDS_install_path>/otdsws/WEB-INF/email` directory. If you installed OTDS to the default path, you can find the files in:

- On Windows: `C:\OTDS\otdsws\WEB-INF\email`
- On UNIX or Linux: `/usr/local/OTDS20/otdsws/WEB-INF/email`

For more information, see “[Customizing the sign-in page](#)” on page 354 and “[Customizing OTDS emails](#)” on page 356.

### Customizing Directory Services resource mappings

Mappings that can be defined include those for object filters, name mappings, group mappings, and user locations. For more information about these mappings, see “[Defining a synchronized user partition](#)” on page 74. Directory Services includes a number of template files that you can edit in order to customize these mappings. These files can be found in the `<Directory Services_install_path>/otdsws/WEB-INF/classes` directory.

**!** **Important**

OpenText recommends that you use extreme caution when modifying the template files. Improper or inaccurate changes to these template files can negatively impact your Directory Services environment.

For more information, see “[Customizing Directory Services mappings](#)” on page 358.

## 17.1 Customizing the sign-in page

You can apply the following customizations to the OTDS sign-in page:



**Tip:** You apply customizations to the **Sign in UI Version** and **Sign in UI Style** boxes when configuring your resource.

For more information, see the **General** tab information in “[Creating a non-synchronized resource](#)” on page 176 or “[Creating a synchronized resource](#)” on page 206.

1. You can customize the user interface version on the resource through the **Sign in UI Version** box. This box determines whether your users will see:

- The traditional OTDS sign-in page, called “login1”.
- The OTDS sign-in page based on OpenText Content Management Smart View, called “login2”.
- The OTDS sign-in page based on JATO, called “login3”.

The files for each of these sign-in pages are found in the `otdsws` directory.

The default is “login2”, if integrated products do not specify otherwise.

2. You can customize the sign-in graphic on the resource through the **Sign in UI Style** box:

- a. First, create and save your customized graphic:

- If you are using the traditional OTDS sign-in page, place your customized graphic in the `<OTDS_install_path>/otdsws/login1` directory.
- If you are using the OTDS sign-in page based on OpenText Content Management Smart View, place your customized graphic in the `<OTDS_install_path>/otdsws/login2` directory.
- If you are using the OTDS sign-in page based on JATO, place your customized graphic in the `<OTDS_install_path>/otdsws/login3` directory.

- b. Next, when creating your resource, on the **General** tab, in the **Sign in UI Style** box, type the file name with extension of your customized graphic.

3. You can enable the password reset option on the OTDS sign-in page. After you enable the password reset option, from the OTDS sign-in page, users can select either **Forgot Password** or **reset it here** to receive an email that provides them with a password reset so that they can sign in.

The password reset option is controlled by the system attribute [Enable Password Reset](#) on page 299. By default, this attribute is enabled. To remove the password reset option from the OTDS sign-in page, set the [Enable Password Reset](#) on page 299 attribute to “false”.

To enable this option, you must configure your SMTP server information. For more information, see “[SMTP Settings](#)” on page 318.

 **Note:** For the user to receive the email, the userid account must have a valid email address configured.

4. You can choose to use a custom third-party image for your authentication handlers. Currently, OTDS provides the following built-in third-party handlers images:

- third\_party\_facebook\*
- third\_party\_google\*
- third\_party\_linkedin\*
- third\_party\_microsoft\*
- third\_party\_twitter\*
- third\_party\_yahoo\*

If you choose to provide a custom image to represent your authentication handler, save your custom image with the file name: <OTDS\_install\_path>/otdsws/login<x>/third\_party\_custom\_<name>. <ext>

where:

Variable	Description
<OTDS_install_path>	The path to which you installed OTDS.
login<x>	The folder name depending on which OTDS sign-in page you are using: <ul style="list-style-type: none"> <li>• If you are using the traditional OTDS sign-in page, the folder name is “login1”.</li> <li>• If you are using the OTDS sign-in page based on OpenText Content Management Smart View, the folder name is “login2”.</li> <li>• If you are using the OTDS sign-in page based on JATO, the folder name is “login3”.</li> </ul>
<name>	The provider name property configured on the authentication handler in OTDS.
<ext>	Can be any image format. Examples include: jpg, svg, gif, png

You must also create a .css file containing a style definition for that custom image:

- a. Choose which `login_custom.css` you need to create:

- If you are using the traditional OTDS sign-in page, the file you create must be named: `login_custom.css`
- If you are using the OTDS sign-in page based on OpenText Content Management Smart View, the file you create must be named: `login2_custom.css`

- If you are using the OTDS sign-in page based on JATO, the file you create must be named: `login3_custom.css`
- b. An example of the content you might include in your new `.css` file:

**Example:**

```
.third_party_custom_okta {  
    background-image: url('third_party_custom_okta.png');  
    background-position: 0px 0px;  
    background-size: auto;  
    width: 32px;  
    height: 32px;  
    margin: 0 0 0 0px;  
    border: 0px solid white;  
    cursor: pointer;  
}
```

## 17.2 Customizing OTDS emails

You can customize the email header and email text that OTDS sends in emails to users.

### The email files you can edit

The files that you need to edit, in order to customize the emails that OTDS sends, can be found in the `<OTDS_install_dir>/otdsws/WEB-INF/email` directory. You can customize the following email files:

1. **2fsuspendemail.xsl**: this is the email stylesheet used when a two-factor account is suspended.
2. **2fsuspendemail-subject.xsl**: this is the subject line stylesheet, used in an email, when a two-factor account is suspended.
3. **en.xml**: this is the file that contains the English language text that is included in the OTDS emails.
4. **newemailvalidationemail.xsl**: this is the new email validation stylesheet.
5. **newemailvalidationemail-subject.xsl**: this is the new email validation subject line stylesheet.
6. **ot\_email\_header.png**: this is the banner graphic that OTDS includes as the email header.
7. **passwordexpireemail.xsl**: this is the password has expired stylesheet.
8. **passwordexpireemail-subject.xsl**: this is subject line stylesheet, used in an email, when the password has expired.
9. **passwordresetemail.xsl**: this is the password reset stylesheet.
10. **passwordresetemail-subject.xsl**: this is the subject line stylesheet, used in an email, when the password is reset.
11. **validationemail.xsl**: this is the validation email stylesheet.
12. **validationemail-subject.xsl**: this is the subject line stylesheet, used in an email, when a validation email is sent.

## 17.2.1 To customize OTDS emails

When OTDS sends out an email, it first looks for an `<OTDS_install_dir>/otdsws/WEB-INF/email-custom` directory and uses the files it finds in that directory. If no `email-custom` directory exists, OTDS uses the default email files it finds in the `<OTDS_install_dir>/otdsws/WEB-INF/email` directory.

**!** **Important**

OpenText recommends that you never edit the original files located in the `<OTDS_install_dir>/otdsws/WEB-INF/email` directory.

### To customize the emails that OTDS sends out

#### To customize the emails that OTDS sends out:

1. Copy the `<OTDS_install_dir>/otdsws/WEB-INF/email` directory, and all files contained in that directory, to a new `<OTDS_install_dir>/otdsws/WEB-INF/email-custom` directory.
2. After you have created your `email-custom` directory, you can edit any of the files located in that custom directory as you wish. For descriptions of the files you can edit, see “[The email files you can edit](#)” on page 356.



**Note:** If, at a future date, you upgrade your OTDS installation, the customizations you implemented to your `email-custom` directory will not be over-written. However, any updates that OTDS writes to the `email` directory will not be applied to your `email-custom` directory.

After an upgrade, if you want the latest `email` updates applied, you will need to follow these directions again.

### To translate the English language text of OTDS emails to another language

#### To translate the English language text of OTDS emails to another language:

1. Make sure that you copied the `email` directory as stated in the first step. All further steps in this section refer to the files found in the new `<OTDS_install_dir>/otdsws/WEB-INF/email-custom/` directory.
2. In the `<OTDS_install_dir>/otdsws/WEB-INF/email-custom/` directory, copy the `en.xml` file to `<language_code>.xml`. For example:
  - a. If you want to create a German language file, copy `en.xml` to `de.xml`.
  - b. Edit the text of the `de.xml` file to translate the text to German.

All emails that an OTDS German UI sends will now pick up your custom German text.

## 17.3 Customizing Directory Services mappings

When creating or configuring a synchronized user partition, you have the option of defining user and group attribute mappings between Directory Services and your resource. The files you can edit are:

- **ADIdentityProviderTemplate.xml**: edit this file if your identity provider is Windows Server Active Directory (AD).
- **ADLDSIdentityProviderTemplate.xml**: edit this file if your identity provider is Windows Server Active Directory Lightweight Directory Services (AD LDS).
- **LDAPV3IdentityProviderTemplate.xml**: edit this file if your identity provider is Lightweight Directory Access Protocol (LDAP).

In a synchronized user partition, Directory Services provides some pre-defined user and group attribute mappings, which are documented in the three template files listed above. You can edit these pre-defined mappings or create entirely new mappings.

### Example 17-1: Example of a pre-defined user attribute mapping

```
<userAttributeMapping>
  <mapping>
    <source>
      <value>facsimileTelephoneNumber</value>
    </source>
    <target>oTFacsimileTelephoneNumber</target>
    <format>%s</format>
  </mapping>
</userAttributeMapping>
```

Where:

- **userAttributeMapping**: is the tag within which all pre-defined user attribute mappings are found.
- **mapping**: is the tag within which one pre-defined user attribute mapping or one group attribute mapping is defined.
- **source**: is the tag within which the mapped value in the resource is defined. Only those mappings that have been pre-defined will have **source**.
- **value**: is the mapped value. Only those mappings that have been pre-defined will have **value**.
- **target**: is the Directory Services parameter name being mapped. All mappings have **target**.



### Caution

OpenText strongly recommends that you do not edit **target**.

- **format**: is the definition of the format for the mapping. All mappings have **format**. For more information about format, see “[Applying user partition attribute mappings](#)” on page 83.



After you modify any of these template files, when you create a new synchronized user partition, Directory Services will access the values that you saved to the template. Those values will appear in the assistant. You will still have the option of editing the values in the assistant during the creation or editing process.

You can add a new mapping to your template file, however, if you provide an attribute that does not exist in your database, Directory Services will try to add that mapping. Your results may not be as expected. OpenText recommends that you do not add a new mapping.



# Chapter 18

## SCIM Support in OTDS

Directory Services supports the System for Cross-domain Identity Management (SCIM) protocol to synchronize users into OTDS. For more information see “[References to external websites](#)” on page 385.

 **Note:** Only SCIM 2.0 is supported. OTDS does not support SCIM 1.1.

To synchronize users to OTDS through SCIM, you must have OTDS version 16.2.0 or later installed.

OTDS uses OAuth2 access tokens to secure its SCIM API. The SCIM client must use an OAuth2 grant in order to obtain an access token.

### To synchronize users into OTDS through SCIM:

#### To implement SCIM support in OTDS:

1. From the web administration menu, click **OAuth Clients**.
2. On the **OAuth Clients** page, on the button bar, click **Add**.
3. In the **General** tab, in the **Client ID** box, type a descriptive name for OAuth client. For example, type: SCIM-Client
4. In the **Description** box, type a more detailed description for this OAuth client. For example, type: OAuth client to allow SCIM support.
5. Click to select **Confidential**.
6. On the button bar, click **Save**.

**!** **Important**

After you click **Save**, OTDS will display a **Secret Key** box. You must make note of this generated client secret key. OTDS only displays this key once. If you lose it, you will either need to delete this OAuth client and re-create it, or edit it to remove the confidential setting, save it, and then reapply the confidential setting. For more information, see “[OAuth Clients](#)” on page 275.

7. Because the third-party service you have selected, for example Microsoft Azure AD, will be synchronizing into OTDS, you need to create a non-synchronized partition:
  - a. From the web administration menu, click **Partitions**.
  - b. On the **Partitions** page, on the button bar, click **Add**. From the **Add** menu, select **New Non-synchronized User Partition**.

- c. In the **Name** box, type a descriptive name for this partition. For example, type: SCIM-partition  
d. In the **Description** box, type a more detailed description for this partition. For example, type: Non-synchronized partition to allow SCIM support.  
e. Under the **Actions** column, click **Save**.
  8. Ensure that the OAuth client you created in **step 1** is added as an administrator of the non-synchronized user partition you created in **step 7**:
    - a. From the web administration menu, click **Partitions**.
    - b. From the **Actions** menu of the non-synchronized user partition you created in **step 7**, click **Edit Administrators**.
    - c. On the **Users & Groups** <*partition\_name*> page, on the button bar, click **Add Administrator**.
    - d. In the **Users and Groups Associations** box, click to select the box to the left of the OAuth client you created in **step 1**. Based on the examples given in this procedure, select “SCIM-Client@OAuthClients”.
    - e. Click **Add Selected**, view the information message, and then click **Close**.
  9. You will now need to configure the service, such as Microsoft Azure AD, that you will be using to enable SCIM support in OTDS.
  10. After you have completed all configuration steps listed here, you can access the base URL for SCIM. The form of this URL is: [https://otdsserver/otdswebs/scim/<partition\\_name>](https://otdsserver/otdswebs/scim/<partition_name>)
- Using the example provided in **step 7**, the URL is: <https://otdsserver/otdswebs/scim/SCIM-partition>

## Chapter 19

# Jobs

Directory Services provides the **Jobs** tab in OTDS to monitor the progress of user-initiated jobs and system jobs running as asynchronous background operations on the server. The following is a partial list of the jobs that OTDS will track on the **Jobs** tab:

- Import
- Consolidate
- Monitoring
- Scheduled Sync

Each job provides details such as:

- The **Name** of the OTDS function that is running a job that the **Jobs** tab is tracking.
- The **Target** of the job that is running. For example, if the Recycle Bin has run a job, and its target is **Auto delete scheduler**, this job is running the automatic delete function that was scheduled in “[Recycle bin settings](#)” on page 271.
- The job's **Start Time** and **Finish Time**.

The times displayed depend on the system on which you are accessing the web administration UI, not the system on which OTDS is installed.

- The number of **Errors**, **Warnings**, and **Information Messages** associated with the job.
- The **Status** of the job can be one of: Running, Canceled, Failed, or Completed.

You can select **Refresh** to see the most recent events.

### Jobs Actions menu options and buttons

On the main **Jobs** page, each job has an associated **Actions** menu and applicable buttons.

#### Jobs Actions menu options

<b>Actions menu option</b>	<b>Associated Procedure</b>
View Info/Error/Warning Messages	“ <a href="#">Viewing a job's messages</a> ” on page 365
Cancel Job	“ <a href="#">Canceling a job</a> ” on page 365

**Jobs buttons**

Button	Associated Procedure
Clear All Completed Jobs	Removes all jobs that are no longer running from the <b>Jobs</b> page. For example, any job with the <b>Status</b> of either <b>COMPLETED</b> or <b>FAILED</b> .
Clear Selected Job(s)	Removes all jobs you have selected by clicking the box to the left of that box from the <b>Jobs</b> page.
Refresh	Verifies if OTDS has completed an action.
Help	Opens context-sensitive help for the page you are currently using.

## 19.1 Types of Jobs

The following are the two types of jobs that OTDS tracks:

### System jobs

There is only one SYSTEM job. It appears with a **Name** of “SYSTEM” and a **Target** of “SYSTEM”. It is a placeholder for operations performed by OTDS in the background that are not directly associated with a user-initiated job, or other jobs that are owned by their component such as Enterprise Sync Monitoring, Scheduled Sync, or Recycle Bin auto delete. Whether the system job can be canceled or not is dependent on the operation being performed.

Recycle Bin's “auto delete” job cannot be canceled. To change the setting for Recycle Bin's auto delete, see “[Recycle bin settings](#)” on page 271.

### User-initiated jobs

Cancelling a user-initiated job requires confirmation and does not undo any work already completed. When a job has been canceled, the **Status** will show the text **Canceled**. A canceled job cannot be restarted.

## 19.2 Job's information messages

From each job's **Actions** menu, you can view more details about any information messages generated by this job. The information available in an information message, includes:

- **Source:** details the source of the information message. For example, if the source is listed as **Recycle Bin**, then the recycle bin function has generated this information message.
- **Type:** details the type of action that required the *source* to generate an information message.
- **Time:** the time that the *source* generated the information message.

- **Message:** the message that the *source* generated.

## 19.3 Viewing a job's messages

### To view a job's messages:

1. From the web administration menu, select the **Jobs** tab.
2. From the **Actions** menu associated with the job click **View Errors**, **View Warnings**, or **View Info Messages**.
3. In the information box, you can read the **Source**, **Type**, **Time**, and **Message**. There is no action you can take in this box.
4. After you have read the information you need, click **Close**.

## 19.4 Canceling a job

### To cancel a job:

1. From the web administration menu, select the **Jobs** tab. Whether or not you have the option of canceling a job is dependent on the type of job.
2. From the **Actions** menu of the job you want to cancel, select **Cancel Job**.
3. In the **Confirm Job Cancellation** window, click **Yes** to confirm that you want to cancel the job. Click **No** to allow the job to continue.

## 19.5 Clearing all completed jobs

### To clear all completed jobs:

1. From the web administration menu, select the **Jobs** tab.
2. In the **Jobs** window, from the button bar, click **Clear All Completed Jobs**.
3. All jobs with a **Status** of “COMPLETED” will be removed from the **Jobs** tab immediately.

## 19.6 Clearing all selected jobs

### To clear all selected jobs:

1. From the web administration menu, select the **Jobs** tab.
2. You can now either manually select the box to the left of every job that you want to clear, or you can use the search bar to narrow the jobs that appear on the **Jobs** tab.
3. After you have selected the box to the left of every job that you want to clear, on the button bar, click **Clear Selected Job(s)**.



# Chapter 20

## Audit Reports

Directory Services provides reporting derived from audits of OTDS functions that have occurred within a specified time frame. Examples of reports you can view on the **Audit Reports** tab include:

- Number of consolidation operations completed.
- Number of users or groups created, and their user or groups names.
- Number of failed sign in attempts, and their user names.
- Number of OTDS errors.
- Number of users or groups moved to the recycle bin.
- Peak number of allocated licenses.

You can set the auditing parameters in the **Audit/Reporting Settings** area of the **System Config** page. You should also set the **Notification Settings** area of the **System Config** page at the same time. See “[Audit/Reporting Settings](#)” on page 319 and “[Notifications Settings](#)” on page 320 for more information.

### Audit reports Actions menu options and buttons

On the main **Audit Reports** page, each audit report has an associated **Actions** menu and applicable buttons. The following are quick links to the procedures associated with each:

#### License keys Actions menu options

Actions menu option	Associated Procedure
Details	<a href="#">“Retrieving an audit report's details” on page 370</a>
Go to object	<a href="#">“Finding an audit report's object” on page 370</a>

#### Audit report buttons

Button	Associated Procedure
Refresh	Verifies if OTDS has completed an action. For example, after deleting.
Event count	<a href="#">“Retrieving an audit report's event count” on page 370</a>
Help	Opens context-sensitive help for the page you are currently using.

## 20.1 Searching audit reports

### To search audit reports:

- There are two different ways to search audit reports:
  - You can search for specific audit reports.
  - You can retrieve a count of the number of a specific event type.

Do one of the following:

- a. If you want to search for a specific audit report, do the following:
  - i. **Optional** You can choose to search by **Starts with** or **Contains**. Select one of the radio buttons to define your search filter, and then type your search query in the associated box.
  - ii. You can optionally choose to define the number of results that will display per page. The default is 25 results per page. If the search produces multiple pages of results, click **Previous** and **Next** to page through the results.
  - iii. **Optional** You can optionally make a selection in any other attribute box:
    - The **Start Date** and **End Date** boxes allow you to define dates within which the audit report was generated.
    - The **Partition** box allows you to restrict this search to one partition.
    - You can further restrict the search parameters by making selections from the **Results** and **Sources** lists.
    - Finally, you can type text to either the **Audit Object ID** or **Audit user** boxes to restrict your search to a specific object ID or user.
- b. If you want to retrieve a count of the number of a specific event type, do the following:
  - i. The only attribute box that is applicable when performing this type of search is the **Types** box.  
You must make a selection from the **Types** list to specify the type of audit report you want to search.
  - ii. On the button bar, click **Event count**.
  - iii. Read the count that is returned, then close the information bar.

## 20.2 An audit report's details

Each audit report's details can be retrieved and viewed. The boxes on an audit report's details page are:

---

### ID

The unique identification number for this audit report. OTDS generates this identification number for each audit report.

### Description

The description of the nature of the audit report. Not every audit report will have a description.

### Time

The date and time on which the audit report was generated. The time appears in the form: <YYYY>-<MM>-<DD> <HH>:<MM>:<SS>

The time zone is UTC.

---

### Event Type

The type of audit report. Examples of types include: group create, group modify, user create. You can see the full list of possible event types in the **Types** box under the search area on this page.

---

### Result

Gives the status of the event. Possible values include: success, warning, failed, unknown. You can see the full list of possible results in the **Results** box under the search area on this page.

---

### Audit User

The userid of the user who instigated the event.

---

### Source

The name of the service responsible for the event. You can see the full list of possible sources in the **Sources** box under the search area on this page.

---

### Audit Object

Every entity, for example every user or every group, has a unique identification number assigned by OTDS. You can run a search on this number to find all audit reports that apply to this entity.

---

### Partition Name

The name of the partition within which the event occurred. Not every audit report will have a value in this box. For example, global actions will not have a value in the partition box as a global action applies to all partitions.

---

### Data

The specific attributes of the event.

## Retrieving an audit report's details

### To retrieve an audit report's details:

1. From the web administration menu, click **Audit Reports**.
2. From the **Actions** menu of the audit report whose details you want to view, click **Details**.
3. Read the information presented in the **Details** box. For information about the boxes on the **Details** dialog box, see “[An audit report's details](#)” on page 369.
4. Click **Cancel**.

## 20.3 Finding an audit report's object

### To find an audit report's object:

1. From the web administration menu, click **Audit Reports**.
2. From the **Actions** menu of the audit report whose object you want to view, click **Go to object**.
3. You have now left the **Audit Reports** page. To view your precise location, see the breadcrumb trail at the top.
4. Examine the report that you have been taken to view and make any changes you need to make. If you make changes, on the button bar, click **Save**. To exit this page without making any changes, click **Cancel**.

## 20.4 Retrieving an audit report's event count

### To retrieve an audit report's event count:

1. From the web administration menu, click **Audit Reports**.
2. Near the top of the page, just under the search area, from the **Results** box, optionally choose a result for this query. Your options are success, warning, failed, unknown. To include all results options, leave this box blank.
3. From the **Sources** box, optionally choose a source that will be searched for this query. To include all sources, leave this box blank.
4. You must select a type from the **Types** box. The types listed here are the events that OTDS tracks for audit reports.
5. After you have made your selections, on the button bar, click **Event count**. You will see an information bar appear on the page with the number of events that OTDS has recorded.

# Chapter 21

## System Status

The **System Status** page lets you view an **OTDS Configuration Report**, version information for the Directory Services product, and highlights **Potential Configuration Issues**. Information on the **System Status** page can be refreshed.

The **System Status** page has the following areas:

- The **Version Information** area shows the product build date, build number, product version, and hardware fingerprint.

 **Note:** The hardware fingerprint value may be requested by OpenText support. This is not a value that you should use unless directed by OpenText or by an OpenText application's documentation.
- The **Potential Configuration Issues** area shows a list of issues that are not expected in a finalized configuration of Directory Services. You can click any issue to immediately be directed to the best solution for each issue. For more information, see “[Potential configuration issues](#)” on page 372.
- You can select **Download OTDS Configuration Report** to get a report of your Directory Services configuration directly from its LDAP backend. This report can be used when reporting issues to OpenText Support. You can attach the report to a customer support ticket to assist in identifying problems.

### System status buttons

On the main **System Status** page there are buttons on the button bar specific to this page. The following are quick links to the procedures associated with each:

Button	Associated procedure
Refresh	Verifies if OTDS has completed an action.
Download OTDS Configuration Report	“ <a href="#">Downloading the OTDS configuration report</a> ” on page 372
Help	Opens context-sensitive help for the page you are currently using.

## 21.1 Potential configuration issues

The **Potential Configuration Issues** area of the **System Status** page shows you potential issues with your current Directory Services configuration.

Potential issues include:

- Resource <My\_OpenText Content Management> has not been activated.
- Content Web Services for resource <My\_OpenText Content Management> appears to be incorrectly configured.
- Resource <My\_OpenText Content Management> and resource <My\_Other\_OpenText Content Management> are both configured to synchronize users and groups to the same OpenText Content Management.
- User and group synchronization is configured but disabled for resource <My\_OpenText Content Management>.
- You have not given members of <My\_Partition> access to any resources.
- You have not given anyone access to the resource <My\_OpenText Content Management>.
- The synchronized partition <My\_Partition> has no users or groups.
- The synchronized partition <My\_Partition> failed to import users and groups.



### Tips

- Click each **Potential Configuration Issue** in turn to correct the issue.
- You will be directed to the easiest solution to the issue.

For example, if the issue is that you have not given anyone access to <Resource A>, clicking that issue will direct you to the **Resources** object in the Directory Services tree, where you can click **Edit Access Roles** to add members to the Access to <Resource A> access role.

For more information about the **Potential Configuration Issues** area of the **System Status** page, see “[Viewing potential configuration issues](#)” on page 373.

## 21.2 Downloading the OTDS configuration report

**To download the OTDS configuration report:**

1. From the web administration menu, under the **Info** heading, click **System Status**.
2. On the **System Status** page, click **Download OTDS Configuration Report**.
3. In the **Save As** window, select the location to which this file will be downloaded and then click **Save**. Accept the default name “otds\_system\_config\_report.txt” or type a new name.
4. The OTDS configuration report will download to your machine. An information box will display, depending on your browser settings, that you can click to display the report.

## 21.3 Viewing potential configuration issues

### To view potential configuration issues:

1. From the web administration menu, under the **Info** heading, click **System Status**.
2. On the **System Status** page, if configuration issues have been detected, they will be displayed in the **Potential Configuration Issues** area.  
If no configuration issues were detected, the message “No Configuration Issues detected!” will be displayed below the button bar.  
If configuration issues are displayed, you can click each issue in turn to be directed to the solution to that issue.
3. You will be directed to the Directory Services object in which you can correct the configuration issue.



# Chapter 22

## Log Files

To zip and download the log files, from the web administration menu click **Log Files**, and then, from the button bar, click **Zip and Download Log Files**. When the zip file is ready, choose to save it to a directory of your choice. This section describes the information recorded to the log files about Directory Services.

### Log files buttons

On the main **Log Files** page, there are buttons on the button bar specific to this page. The following are quick links to the procedures associated with each:

Button	Associated Procedure
Toggle Wrap	By default, OTDS displays the log text on the page unwrapped. If you want the log text to wrap within the browser, then from the button bar, click <b>Toggle Wrap</b> .
Zip and Download Log Files	If you want to zip and download the log files, from the button bar, click <b>Zip and Download Log Files</b> . When the zip file is ready, choose to save it to a directory of your choice.
Help	Opens context-sensitive help for the page you are currently using.

### 22.1 otds.log

The `otds.log` file contains a record of actions, such as starting and stopping, performed by Directory Services. The `otds.log` file can be accessed from the web administration client. It is found in the Tomcat directory. If you installed your application server to the default location, you will find the log file at `<app_svr_installdir>\logs`.

Instructions to view the OTDS log files can be found in “Viewing the Directory Services log files” on page 378. This log file is configured to have a maximum size of 50MB and permit ten archived versions before rolling over. To change these settings, see “Configuring the Directory Services log files” on page 379.

## 22.2 directory-provenance.log

The `directory-provenance.log` file traces the lifecycle and relationships of objects and events related to user and group synchronization. It will also write consolidation messages.

Directory Services has stricter syntax checking than Active Directory for some types. As a result, some user or group entries exist in Active Directory, but do not make it to Directory Services. The `directory-provenance.log` will record these types of import or synchronization failures.

The `directory-provenance.log` file can be accessed from the web administration client. It is found in the Tomcat directory. If you installed your application server to the default location, you will find the log file at `<app_srvr_installdir>\logs`. This is a CSV log. For information about reading CSV log files, see [How do I understand comma separated value \(CSV\) log entries? on page 395](#).

Instructions to view the OTDS log files can be found in [“Viewing the Directory Services log files” on page 378](#). This log file is configured to have a maximum size of 50MB and permit ten archived versions before rolling over. To change these settings, see [“Configuring the Directory Services log files” on page 379](#).

## 22.3 directory-access.log

The `directory-access.log` file contains entries relating to successful and unsuccessful authentication attempts. This log file details userid sign in and sign out attempts to and from OTDS.

For example, if multiple users exist with the same `username` across multiple partitions, OTDS will attempt to resolve the `username`. If this is not possible, the `directory-access.log` will contain a message, with the string `MULTIPLE_IDENTITIES_FOR_USER_NAME`, to indicate that multiple identities for the given `username` were found. See [How do I resolve “MULTIPLE\\_IDENTITIES\\_FOR\\_USER\\_NAME” errors when different users are registered with the same email account in OTDS? on page 407](#) for more information.

This is also the log file that you should check to see whether the SAP user is mapped correctly to OTDS and to OpenText Content Management.

The `directory-access.log` file can be accessed from the web administration client. It is found in the Tomcat directory. If you installed your application server to the default location, you will find the log file at `<app_srvr_installdir>\logs`. This is a comma separated value (CSV) log. For information about reading CSV log files, see [How do I understand comma separated value \(CSV\) log entries? on page 395](#).

Instructions to view the OTDS log files can be found in [“Viewing the Directory Services log files” on page 378](#). This log file is configured to have a maximum size of 50MB and permit ten archived versions before rolling over. To change these settings, see [“Configuring the Directory Services log files” on page 379](#).

## 22.4 directory-audit.log

The `directory-audit.log` file records administrative actions and changes to configuration performed in Directory Services.

The `directory-audit.log` file can be accessed from the web administration client. It is found in the Tomcat directory. If you installed your application server to the default location, you will find the log file at `<app_srvr_installdir>\logs`. This is a CSV log. For information about reading CSV log files, see [How do I understand comma separated value \(CSV\) log entries? on page 395](#).

Instructions to view the OTDS log files can be found in [“Viewing the Directory Services log files” on page 378](#). This log file is configured to have a maximum size of 50MB and permit ten archived versions before rolling over. To change these settings, see [“Configuring the Directory Services log files” on page 379](#).

## 22.5 otds-installer.log

The `<otds-installer>.log` file contains a record of install actions performed by Directory Services. To create this log file, during installation you need to use the following parameters:

- On Windows, use the `msiexec` utility with the `/l*v <your_logfile_name>.log` parameter.  
For directions on using the `msiexec` utility, see [“Installing OTDS on Windows from the command line” on page 30](#).
- On UNIX or Linux use the Directory Services setup script with the `-l <your_logfile_name>.log` parameter.  
For directions on using the `setup` script, see [“Installing OTDS on Linux non-interactively” on page 40](#).

Instructions to view the OTDS log files can be found in [“Viewing the Directory Services log files” on page 378](#).

## 22.6 otdsDeploy.log

The `otdsDeploy.log` file contains a record of install actions performed by Directory Services.

Instructions to view the OTDS log files can be found in [“Viewing the Directory Services log files” on page 378](#).

## 22.7 The OTDS replication log files

The **OTDS replication** log files are used to troubleshoot and debug problems associated with Directory Services replications.

Instructions to view the OTDS log files can be found in “Viewing the Directory Services log files” on page 378.

## 22.8 Viewing the Directory Services log files

**To view the Directory Services log files:**

1. If you want to view any of these log files:

- otds.log
- directory-provenance.log
- directory-access.log
- directory-audit.log

do the following:

- a. From the web administration menu, click **Log Files**.
  - b. On the **Logs** page, select one of the following:
    - the **otds** tab
    - the **directory-provenance** tab
    - the **directory-access** tab
    - the **directory-audit** tab
  - c. **Optional** By default, these log files display the text on the page unwrapped. If you want the log text to wrap within the browser, from the button bar, click **Toggle Wrap**. To reset the default display, from the button bar, click **Toggle Wrap**.
  - d. **Optional** If you want to zip and download the log files, from the button bar, click **Zip and Download Log Files**. As soon as the zip file is ready, choose to save it to a directory of your choice.
2. If, when you installed OTDS, you created an installation log file, you will find the `<your_logfile_name>.log` file in the directory in which you placed, and from which you ran, the OTDS installer file.
  3. If you want to view the `otdsDeploy.log` file, and you installed OTDS to the default location:
    - On Windows: C:\OTDS\install

- On UNIX or Linux: /usr/local/OTDS/install

## 22.9 Configuring the Directory Services log files

**To configure the Directory Services log files:**

1. If you want to configure any of these log files:
  - otds.log
  - directory-provenance.log
  - directory-access.log
  - directory-audit.log
2. Open the `<OTDS_INSTALLDIR>/otdsws/WEB-INF/classes/log4j2.files.xml` file in a text editor.
3. **Optional** If you want to change the maximum file size permitted for these log files, find the **SizeBasedTriggeringPolicy** setting for that log file and change the value.
4. **Optional** If you want to change the log file rotation value for these log files, find the **DefaultRolloverStrategy** setting for that log file and change the value.



# Chapter 23

## OTDS Documentation

There are many documents that can assist you with your Directory Services environment and configuration. The main document is the *OpenText Directory Services - Installation and Administration Guide* (OTDS-IWC). This section details, and provides access to, the most helpful Directory Services documentation.

To access the product page on OpenText My Support, see Directory Services (OTDS) ([https://support.opentext.com/csm?id=csm\\_enterprise\\_product&sys\\_id=dd693081470c9110808596f8536d436d](https://support.opentext.com/csm?id=csm_enterprise_product&sys_id=dd693081470c9110808596f8536d436d)).

To access the documentation list for Directory Services, with links to the *Release Notes*, see OpenText Directory Services Version CE 25.4.0 ([https://webapp.opentext.com/piroot/\\_doclists/p-otds-basic.250400.xml](https://webapp.opentext.com/piroot/_doclists/p-otds-basic.250400.xml)).

---

### To access the current OTDS documentation:

---

1. OpenText Directory Services Installation and Administration Guide ([https://webapp.opentext.com/piroot/otds/v250400/otds-iwc/en/html/\\_manual.htm](https://webapp.opentext.com/piroot/otds/v250400/otds-iwc/en/html/_manual.htm)).
2. OpenText Directory Services Cloud Deployment Guide ([https://webapp.opentext.com/piroot/otds/v250400/otds-cgd/en/html/\\_manual.htm](https://webapp.opentext.com/piroot/otds/v250400/otds-cgd/en/html/_manual.htm)): for information about the configuration and use of the stand-alone, containerized OpenText Directory Services.
3. OpenText Directory Services Integration Administration Guide ([https://webapp.opentext.com/piroot/llesdsi/v250400/llesdsi-agd/en/html/\\_manual.htm](https://webapp.opentext.com/piroot/llesdsi/v250400/llesdsi-agd/en/html/_manual.htm)): for information about how to configure how users will authenticate with OpenText Content Management.

---

### To access the developer documentation detailing the REST API:

---

The OTDS REST API developer documentation can be accessed by bringing up *one* of the following URLs in your browser:

- <http://localhost:8080/otdswebs/v1>
- <http://localhost:8080/otdswebs/rest>

To access a document detailing common API endpoints available in OpenText Directory Services, see OTDS API Endpoints ([https://support.opentext.com/csm?sys\\_kb\\_id=03cb6419dbe9d9101337173605961941&id=kb\\_article\\_view&sysparm\\_rank=4&sysparm\\_tsqueryId=f7145eec976e65901a47b3d3f153afc0](https://support.opentext.com/csm?sys_kb_id=03cb6419dbe9d9101337173605961941&id=kb_article_view&sysparm_rank=4&sysparm_tsqueryId=f7145eec976e65901a47b3d3f153afc0)).

---

### To access developer documentation for Azure AD and OTDS:

---

#### To access the OTDS developer documentation for Azure AD:

1. Azure AD to OpenText Directory Services Authentication ([https://support.opentext.com/csm?sys\\_kb\\_id=c0a033954742e5103a95a877536d4341&id=kb\\_article\\_view&](https://support.opentext.com/csm?sys_kb_id=c0a033954742e5103a95a877536d4341&id=kb_article_view&)

- ```
sysparm_rank=1&
sysparm_tsqueryId=fde45a6097ae65901a47b3d3f153af14)
2. Azure AD to OpenText Directory Services Provisioning (https://support.opentext.com/csm?sys\_kb\_id=21e077d54742e5103a95a877536d43f5&id=kb\_article\_view&sysparm\_rank=1&sysparm\_tsqueryId=8ba5d2e097ae65901a47b3d3f153afb0)
```

---

**To access the Microsoft Azure AD developer documentation for OTDS:**

1. Azure AD SSO integration with OpenText Directory Services (<https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/opentext-directory-services-tutorial>)
2. Configure OpenText Directory Services for automatic user provisioning (<https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/open-text-directory-services-provisioning-tutorial>)

---

**To access OpenText support documentation for OTDS:**

OpenText maintains a **Knowledge Base** on OpenText My Support ([https://support.opentext.com/csm?id=ot\\_kb\\_search\\_results&spa=1s&kb\\_category=f3a10f1a87ca591028eafe28cebb3566](https://support.opentext.com/csm?id=ot_kb_search_results&spa=1s&kb_category=f3a10f1a87ca591028eafe28cebb3566)) containing articles written by OpenText support. These articles contain information that can assist you in setting up your OTDS installation with your provider. The following lists some examples of these articles.

1. OTDS Checklist - SAML 2.0 authentication ([https://support.opentext.com/csm?sys\\_kb\\_id=181b07ea47ed1550d8047d1e436d43ee&id=kb\\_article\\_view&sysparm\\_rank=1&sysparm\\_tsqueryId=ea66966497ae65901a47b3d3f153af09](https://support.opentext.com/csm?sys_kb_id=181b07ea47ed1550d8047d1e436d43ee&id=kb_article_view&sysparm_rank=1&sysparm_tsqueryId=ea66966497ae65901a47b3d3f153af09))
2. Reset otadmin password for OTDS ([https://support.opentext.com/csm?sys\\_kb\\_id=3b1925de1b707d10e7fe0dc6cc4bcb0a&id=kb\\_article\\_view&sysparm\\_rank=1&sysparm\\_tsqueryId=54a7ff681baace5027e5766ecc4bcb44](https://support.opentext.com/csm?sys_kb_id=3b1925de1b707d10e7fe0dc6cc4bcb0a&id=kb_article_view&sysparm_rank=1&sysparm_tsqueryId=54a7ff681baace5027e5766ecc4bcb44))
3. OAuth 2.0 Authentication with OTDS (<https://forums.opentext.com/forums/developer/discussion/308065/oauth-2-0-authentication-with-otds>)

---

**To access documentation for previous versions of OTDS:**

| Version | Guide                                                                                                                                                                                                                                                                                                         |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10      | OpenText Directory Services with the OTDS Web Client Installation and Administration Guide 10.5.1 ( <a href="https://knowledge.opentext.com/knowledge/piroot/otds/v100500-01/otds-iwc/en/html/_manual.htm">https://knowledge.opentext.com/knowledge/piroot/otds/v100500-01/otds-iwc/en/html/_manual.htm</a> ) |
| 16      | OpenText Directory Services Installation and Administration Guide 16.6.3 ( <a href="https://knowledge.opentext.com/knowledge/piroot/otds/v160603/otds-iwc/en/html/_manual.htm">https://knowledge.opentext.com/knowledge/piroot/otds/v160603/otds-iwc/en/html/_manual.htm</a> )                                |

| Version | Guide                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 20      | OpenText Directory Services Installation and Administration Guide 20.4.1 ( <a href="https://knowledge.opentext.com/knowledge/piroot/otds/v200401/otds-iwc/en/html/_manual.htm">https://knowledge.opentext.com/knowledge/piroot/otds/v200401/otds-iwc/en/html/_manual.htm</a> )                                                                                                                                                                                                                |
| 21      | OpenText Directory Services Installation and Administration Guide 21.3.0 ( <a href="https://knowledge.opentext.com/knowledge/piroot/otds/v210300/otds-iwc/en/html/_manual.htm">https://knowledge.opentext.com/knowledge/piroot/otds/v210300/otds-iwc/en/html/_manual.htm</a> )                                                                                                                                                                                                                |
| 22      | OpenText Directory Services Installation and Administration Guide 22.4.0 ( <a href="https://webapp.opentext.com/piroot/otds/v220400/otds-iwc/en/html/_manual.htm">https://webapp.opentext.com/piroot/otds/v220400/otds-iwc/en/html/_manual.htm</a> )<br>OpenText Directory Services Cloud Deployment Guide 22.4.0 ( <a href="https://webapp.opentext.com/piroot/otds/v220400/otds-cgd/en/html/_manual.htm">https://webapp.opentext.com/piroot/otds/v220400/otds-cgd/en/html/_manual.htm</a> ) |
| 23      | OpenText Directory Services Installation and Administration Guide 23.4.0 ( <a href="https://webapp.opentext.com/piroot/otds/v230400/otds-iwc/en/html/_manual.htm">https://webapp.opentext.com/piroot/otds/v230400/otds-iwc/en/html/_manual.htm</a> )<br>OpenText Directory Services Cloud Deployment Guide 23.4.0 ( <a href="https://webapp.opentext.com/piroot/otds/v230400/otds-cgd/en/html/_manual.htm">https://webapp.opentext.com/piroot/otds/v230400/otds-cgd/en/html/_manual.htm</a> ) |
| 24      | OpenText Directory Services Installation and Administration Guide 24.4.0 ( <a href="https://webapp.opentext.com/piroot/otds/v240400/otds-iwc/en/html/_manual.htm">https://webapp.opentext.com/piroot/otds/v240400/otds-iwc/en/html/_manual.htm</a> )<br>OpenText Directory Services Cloud Deployment Guide 24.4.0 ( <a href="https://webapp.opentext.com/piroot/otds/v240400/otds-cgd/en/html/_manual.htm">https://webapp.opentext.com/piroot/otds/v240400/otds-cgd/en/html/_manual.htm</a> ) |

## 23.1 About the Directory Services online help

OTDS online help is delivered through the OpenText Global Help Server, a live, Internet-based help system that provides OTDS users with access to the most accurate and continuously updated online help.

If your site does not have Internet access, or if you wish to opt out of using the Global Help Server, you can redirect help requests to the OpenText Private Help Server. The Private Help Server is a local help server utility that allows you to set up a local help server within your network.

The OpenText Private Help Server is available in OpenText My Support. See the Private Help Server Administration Guide (<https://support.opentext.com/csm?id=search&spa=1&q=%23GlobalHelpServer24.3>) for more information.

### 23.1.1 Provide the online help on a local help server (Private Help Server)

The online help for this module is delivered using the OpenText Global Help Server (GHS) system, which provides your users with live access to the latest version of the help. If you cannot use the GHS system, for example, if your site does not have internet access, you can install the OpenText Private Help Server (PHS), a local version of the help system that can host your OpenText online help on your organization's network. After the PHS is installed, you can then configure your OpenText module(s) to forward all online help requests to your PHS. For detailed information about installing the PHS, see *OpenText Help System - Private Help Server Administration Guide* (OTHS-AGD).



#### Notes

- The Private Help Server can support multiple OpenText modules. If the Private Help Server has already been installed within your organization to support another OpenText module, you can add additional OpenText module online helps to that installation.
- If you are replacing a previous PHS installation, see Section 2.5 “Updating a Private Help Server installation” in *OpenText Help System - Private Help Server Administration Guide* (OTHS-AGD).
- If the server you want to use for the PHS installation cannot connect to the internet, see Section 1.1 “Deploying online help files in an environment without Internet access” in *OpenText Help System - Private Help Server Administration Guide* (OTHS-AGD).

Once the PHS is installed or upgraded, you can use its Online Help Deployer to download online helps from the GHS system by entering the help deployment codes listed in “[Help deployment codes](#)” on page 384. For more information about using the codes, see Section 3 “Adding product online help to the Private Help Server” in *OpenText Help System - Private Help Server Administration Guide* (OTHS-AGD).

**Table 23-1: Help deployment codes**

| Code           | Product                             |
|----------------|-------------------------------------|
| OTDS250400-IWC | OpenText Directory Services CE 25.4 |

### 23.1.1.1 Configuring OTDS to use the Private Help Server

First, make sure you followed the instructions to download the OpenText Private Help Server and install the product online help. See the Private Help Server Administration Guide (<https://knowledge.opentext.com/knowledge/cs.dll?func=ll&objId=74951271&objAction=browse&viewType=1>) for more information. Specifically, see *OpenText Help System - Private Help Server Administration Guide (OTHS-AGD)* and *OpenText Help System - Private Help Server Administration Guide (OTHS-AGD)*.

#### To set your Private Help Server URL:

1. From the web administration menu, select **System Config**, and then select the **System Attributes** tab.
2. In the list of system attributes, find the **help.config.HelpURL** on page 302 system attribute. If this system attribute does not exist you will need to add it. To add the system attribute, on the button bar, click **Add**.  
In the **Name** box, type “**help.config.HelpURL**”.
3. In the **Attribute value** box, type the fully qualified domain name and port number of the local server to which you have downloaded and unzipped the OTDS online help file.  
This is the base URL that you typed in the **Server URL** box during the installation of Private Help Server. For example, type: `http://mymachine.opentext.com:8080/OTHelpServer/mapperpi`
4. Click **Save**.

## 23.2 References to external websites

These external website URLs may be helpful:

- Java reference: <https://www.java.com>
- Apache Tomcat reference: <https://tomcat.apache.org>
- To open a Windows command prompt as an administrator: [https://technet.microsoft.com/en-us/library/cc947813\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc947813(v=ws.10).aspx)
- SSL Configuration How-to reference: <https://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html>
- Distinguished Names reference: <https://msdn.microsoft.com/en-us/library/aa366101%28v=vs.85%29.aspx>
- Microsoft Tech Net Center's LDAP Query Basics reference: <https://technet.microsoft.com/en-us/library/aa996205%28EXCHG.65%29.aspx#BasicLDAPSyntax>
- My Oracle Support reference: <https://support.oracle.com/>
- Oracle E-Business Suite Software Development Kit for Java reference: <https://support.oracle.com/epmos/faces/ui/km/DocumentDisplay.jspx?id=974949.1>

- Tomcat Connector reference: <https://tomcat.apache.org/connector-doc/>
- Java Formatter reference: <https://docs.oracle.com/javase/7/docs/api/java/util/Formatter.html>
- Duo Security reference: <https://www.duosecurity.com>
- System for Cross-domain Identity Management (SCIM) reference: <https://tools.ietf.org/wg/scim/>
- Google's reCAPTCHA reference: <https://www.google.com/recaptcha>
- W3.org Algorithms reference: <https://www.w3.org/TR/xmldsig-core1/#sec-AlgID>
- The Log4j documentation: <https://logging.apache.org/log4j/2.x/>
- To synchronize time throughout your entire network: <https://www.techrepublic.com/article/synchronize-time-throughout-your-entire-windows-network/>
- The Symantec VIP documentation: <https://vip.symantec.com>

## Chapter 24

# Directory Services security settings and considerations

This chapter describes some security settings that you may choose to apply to OTDS:

- “OTDS and password policies” on page 387
- “OTDS and two-factor authentication” on page 387
- “Trusted sites and OAuth Client redirect URLs” on page 387
- “Auditing” on page 387
- “System attributes” on page 388

You may also want to take a look at any one of the available Tomcat hardening guides, which can be found with a web search.

### OTDS and password policies

OTDS ships with a password policy that is acceptable for most customers.

You can also choose to make password policies much more restrictive.

See “Defining a global password policy for all non-synchronized user partitions” on page 127 and “Password policy for non-synchronized user partitions” on page 125.

### OTDS and two-factor authentication

Two-factor authentication is disabled by default. You can choose to enable it at various levels.

See “OTDS Two-Factor Authentication” on page 69 and “Enabling two-factor authentication” on page 245.

### Trusted sites and OAuth Client redirect URLs

Trusted sites and OAuth Client redirect URLs should be set appropriately to only allow redirection to required sites.

See “Trusted Sites” on page 327 and “OAuth Clients” on page 275.

### Auditing

Auditing can be enabled and configured to keep track of changes made to OTDS.

See “Audit/Reporting Settings” on page 319.

## System attributes

OTDS has a number of system attributes that can be modified to change its function. The complete list of system attributes can be examined to determine your desired behavior. See “[System Attributes](#)” on page 288.

System attributes you might consider:

- [Configurable Session Limit](#) on page 292
- [Enable 2Factor Suspend](#) on page 296
- [Enable Email On Password Change](#) on page 298
- [Restrict Admin Login Subnets](#) on page 307
- [WebAuthn Policy](#) on page 314

# Chapter 25

## Troubleshooting

This section helps you resolve issues with your Directory Services configuration.

### 25.1 Installation issues

---

Using a silent install from the command line to create an installer log file

---

To troubleshoot any installer issues you should run the installer from the command line with the installer log file parameter:

- On Windows, use the `msiexec` utility with the `/l*v <your_logfile_name>.log` parameter.  
For directions on using the `msiexec` utility, see “[Installing OTDS on Windows from the command line](#)” on page 30.
- On UNIX or Linux use the Directory Services setup script with the `-l <your_logfile_name>.log` parameter.  
For directions on using the setup script, see “[Installing OTDS on Linux non-interactively](#)” on page 40.

The silent install will create a log file, `<your_logfile_name>.log` in the same directory that you placed, and ran, the OTDS installer file.

By inspecting these files you will be able to find the location of installation failure.



**Note:** If you installed OTDS to the default location, you will find these log files:

- On Windows, in the `C:\OTDS\install` directory.
- On UNIX or Linux, in the `/usr/local/OTDS/install` directory.

For more information about log files, see “[Log Files](#)” on page 375.

---

Kerberos token is too big for Tomcat default configuration

---

Single sign on calls initiated from a browser will fail.

If you look at a network trace you will see an HTTP error 400 (Bad request) returned by the server. This error is returned because Tomcat's default HTTP handler does not allow headers greater in length than 8192 bytes, and in this case the authorization header is larger than that.

**To adjust Tomcat settings for large Kerberos tokens:**

1. Edit `server.xml` in the `<Tomcat_installdir>\conf` folder. Search for the connector definition line. For example:

```
<Connector port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000" redirectPort="8443" />
```

2. Add a new attribute: `maxHttpHeaderSize="65536"`. For example:

```
<Connector port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" maxHttpHeaderSize="65536" />
```

3. Restart Tomcat.

---

**Directory Services installation error codes descriptions**

---

On Windows, installation error codes are called “Error Number”. On UNIX, installation error codes are called “Status Code”.

When you see a Directory Services installation error code, you should always check the following log files:

- “`otds-installer.log`” on page 377
- “`otdsDeploy.log`” on page 377

| OTDS Installation Error Code Number | Description                                                                                                                                                              |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0                                   | The OTDS installation has succeeded.                                                                                                                                     |
| 1                                   | The OTDS installation has experienced a Java exception. For example, if you try to apply an OTDS patch without first stopping Tomcat, you will generate this error code. |
| 2                                   | The OTDS installation has encountered incorrect parameters.                                                                                                              |
| 3                                   | The OTDS installation could not remove a directory.                                                                                                                      |
| 4                                   | The OTDS installation has encountered an incorrect configuration.                                                                                                        |
| 5                                   | The OTDS installation has encountered an invalid number of parameters.                                                                                                   |
| 6                                   | The OTDS installation has encountered invalid parameters.                                                                                                                |
| 7                                   | The OTDS installation has discovered that the port is in use.                                                                                                            |
| 8                                   | The OTDS installation has encountered an unknown application server type.                                                                                                |
| 9                                   | The OTDS installation has encountered an error with the installation binaries.                                                                                           |
| 14                                  | During an upgrade of OTDS, the OTDS installation has encountered an input/output exception.                                                                              |

| OTDS Installation Error<br>Code Number | Description                                                                                                                                                              |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15                                     | During an OTDS replication server installation, the OTDS server (Tomcat) was not started. To configure replication, the application server (Tomcat) needs to be started. |
| 16                                     | During an upgrade of OTDS, the OTDS installation could not find the OTDS Global Config.                                                                                  |
| 17                                     | During an upgrade of OTDS, the OTDS installation could not find the DN "otadmin".                                                                                        |

---

When attempting to uninstall OTDS using Control Panel, the error message “Please provide valid path to JRE installation folder.” appears and the attempt to uninstall fails.

---

This error message appears when the Java path that you provided during the installation of OTDS has changed since you installed. If you upgraded Java after OTDS was installed, the OTDS installer does not have the correct Java path.

You should contact OpenText support for assistance to edit the OTDS registry entry for JavaBinPath to ensure that the correct Java path is listed.

---

When installing OTDS 25, if you subsequently need to switch to a different version of Apache Tomcat from the version you listed during the installation:

---

Follow these steps:

**To change the version of Tomcat after installing OTDS 25.x:**

1. Stop the current installation of Tomcat and, if you want, uninstall it.
2. Install the new version of Tomcat. Make note of the installation path of this new version of Tomcat.
3. Open a command prompt window and change directory to the OTDS installation directory. If you installed to the default path, on Windows change to the C:\OTDS\install directory and on UNIX change to the /usr/local/OTDS/install directory.
4. Open a text editor and edit the otds-deploy.config file. Find the **applicationServerDirectory** variable. It points to your current version of Tomcat. Change the directory to point to your new version of Tomcat. Take care to keep the same syntax and ensure that you pay close attention to the slashes.
5. In your command prompt window, run the following command:

```
java -jar otds-deploy.jar -patch
```

This will create the context files for OTDS in your new Tomcat directory.

6. If you are running on Windows, update any values in the following registry key to point to the new Tomcat path or service name:

HKEY\_LOCAL\_MACHINE\SOFTWARE\OpenText\otds

7. If you are running on UNIX, update the /etc/opentext/unixsetup/OTDS\_parameters.txt file or the /etc/opentext/unixsetup/OTDS\_parameters\_1.txt file.
8. Start your new Tomcat installation.

---

**What are the default installation paths?**

---

If you install OTDS 25 to a system with no previous version installed, OTDS will install on Windows to C:\OTDS and on UNIX to /usr/local/OTDS.

However, if you upgraded a previous version to the 25 version, the new version will install to the path of the previous version.

---

**What is the problem if I see the error “Unrecognized option: -d64” in my catalina.out log file?**

---

The “-d64” option must be included with some Java versions and cannot be included with others. For example, if you are using Java version 11, and you attempt to start Tomcat with the “-d64” option, you will see the “Unrecognized option” error. For more information, see [“Configuration requirements” on page 14](#).

---

**After upgrading OTDS 10.5.x to 25, the installation appears successful but OTDS fails to deploy.**

---

If OTDS fails to deploy after an upgrade, you will see a message to contact OpenText support. An error occurred during the upgrade process. OpenText support will need to fix that error and then manually deploy the version 25 installation of OTDS.

---

**Why, after upgrading my java runtime environment (JRE) or Tomcat installations, does my OTDS fail?**

---

When upgrading your JRE or Tomcat installation, OpenText recommends that you follow these steps:

1. Stop the existing Tomcat <version> service.
2. Download and install JRE <new\_version> (64-bit).
3. Download and install Tomcat <new\_version> (64-bit).
4. Configure the settings in Tomcat <new\_version> for OTDS. For more information, see [“Configuring Tomcat for OTDS” on page 14](#).
5. Backup the Windows Registry files SYSTEM.DAT and USER.DAT, and then do the following:

**!** **Important**

OpenText strongly recommends that, if you intend modifying the Windows Registry for any reason, you always first make a backup of your Microsoft Windows Registry files: SYSTEM.DAT and USER.DAT. OpenText is not responsible for improper modification of the system registry. Using Windows Registry Editor incorrectly can cause serious issues that may require you to reinstall Windows.

- a. Modify the registry to update the Tomcat and Java locations and update the Tomcat service names.
- b. Modify HKEY\_LOCAL\_MACHINE/SOFTWARE/OpenText/otds16 as follows:
  - i. Update 'ServiceName' to Tomcat<*new\_version*>. For example, 'Tomcat10'.
  - ii. Update 'ServicePath' to \Tomcat <*new\_version*>\. For example, '\Tomcat 10.0\'.
  - iii. Update 'JavaBinPath' to jre<*new\_version*>. For example, 'C:\Program Files\Java\jdk-11\bin\'.
6. Start Tomcat<*new\_version*> and verify there are no service startup errors in the <*Tomcat\_installdir*>\logs directory.
7. Backup and then edit the <*OTDS\_installdir*>\install\otds-deploy.config file. Paying attention to escaped backslash characters, modify the applicationServerDirectory line to point to Tomcat <*new\_version*>.
8. As an administrator, open a command prompt window, and navigate to the <*OTDS\_home*>\install\ directory. Type java -jar otds-deploy.jar -patch to re-create the required context files in Tomcat <*new\_version*>.
9. Monitor the Tomcat <*new\_version*>\logs\otds.log file for a successful startup.

---

How do I change my database connection information after I have installed OTDS?

---

When you install OTDS you are prompted for your database connection string, as well as for a userID and password that can connect to the database. If, after installation, you need to change the database connection string, or the database user, you will need to edit the otds.properties file. If you need to change the database password, see “[Updating the JDBC database connection password after installation](#)” on page 42.

The otds.properties file contains the following variables:

1. jakarta.persistence.jdbc.url: modify the value assigned to this variable if you need to change your database connection string. For more information about the form for the database connection information, see “[Format for the Database JDBC connection string](#)” on page 18.
2. jakarta.persistence.jdbc.user: modify the value assigned to this variable if you need to change the userID of the user with access to the database you set up for OTDS.



**Note:** The `otds.properties` file can be found at `<OTDS_installdir>\config`.

Previously, the `otds.properties` file was found at `<OTDS_installdir>\otdsws\WEB-INF\classes`.

---

#### How do I uninstall OpenDJ?

---

To manually remove OpenDJ, do the following:

1. Stop the OpenDJ service, if it is running.
2. If you are running OpenDJ on Windows, run the following command to remove the Windows Service:  
`opendj/bat/windows-service.bat -d`
3. Delete the OpenDJ directory.

---

#### Why am I seeing database permissions issues when I install or upgrade OTDS?

---

OTDS supports the use of different databases. Each database has permission requirements that are specific to that product. If you experience difficulties writing to the database when trying to install or upgrade OTDS, you need to check the permissions that were assigned to the UserID tasked with writing to the database.

This is the UserID that you typed in the **JDBC Parameters** area during installation. Check your database documentation to determine the correct permissions that you need to assign to that UserID.

## 25.2 Logging issues

---

#### How do I use logs to troubleshoot installation?

---

You can generate logs by running the installer from the command prompt with these options:

- On Windows: `/l*v otds-installer.log`
- On UNIX: `-l otds-installer.log`

For directions on using the `msiexec` utility on Windows with the `/l*v` option, see “[Installing OTDS on Windows from the command line](#)” on page 30.

For directions on using the `setup` script on UNIX with the `-l` option, see “[Installing OTDS on Linux non-interactively](#)” on page 40.

This will create a log file, `otds-installer.log` in the same directory as the `msi` installer file on Windows or the `tar` installer file on UNIX.



**Note:** If you installed OTDS to the default location, you will find these log files:

- On Windows, in the `C:\OTDS\install` directory.

- On UNIX or Linux, in the /usr/local/OTDS/install directory.

For more information about log files, see “[Log Files](#)” on page 375.

---

#### How do I understand comma separated value (CSV) log entries?

**Example:**

```
2014-04-15 16:13:28.962 INFO - ,2014/04/15 16:13:28 EDT,0,0,
Configuration Service, Information, 37, Remove Access Role from
Resource, otadmin@otds.admin, opentext.ot.com, "Access
Role 'cn=psmith,ou=AccessRoles,dc=identity,dc=opentext,
dc=net' removed from Resource 'cn=opentext.ot.com,
ou=Resources,dc=identity,dc=opentext,dc=net'"
```

CSV information:

- **Time, date, and type of event:** In the example above, the time, date, and type of event are: 2014-04-15 16:13:28.962 INFO - ,2014/04/15 16:13:28 EDT.
- **Internal Job ID:** This id can be used to link individual tasks together. This id will be 0 (zero) if there is no associated job. In the example above, the internal job ID is “0”.
- **Internal Task ID:** In the example above the internal task ID is “0”.
- **Name of internal service that generated the entry:** In the example above, the name of the internal service is Configuration Service.
- **Event Type:** Examples of possible event types include: Information, Warning, Success Audit, Failure Audit, Success Provenance, or Failure Provenance. In the example above, the event type is Information.
- **Event ID:** In the example above, the event ID is “37”.
- **Event Name:** In the example above, the event name is Remove Access Role from Resource.
- **ID of user that initiated action (if applicable):** In the example above, the ID of the user that initiated the action is “otadmin@otds.admin”.
- **Name of Directory Services node that generated the event:** In the example above, the name of the OTDS node is “opentext.ot.com”.
- **Further event details (free form):** In the example above, the free form display of further event details is: Access Role 'cn=psmith,ou=AccessRoles,dc=identity,dc=opentext,dc=net' removed from Resource 'cn=opentext.ot.com,ou=Resources,dc=identity,dc=opentext,dc=net'

---

#### How do I enable Directory Services C library logging with LOG4CXX?

**To enable C library logging with LOG4CXX:**

1. Create the otds.c.library.logging.xml configuration file. For example:

**Example:**

```
<?xml version="1.0" encoding="UTF-8" ?>
<log4j:configuration xmlns:log4j="https://jakarta.apache.org/log4j/">

<!-- Output the log message to system console. -->

    <appender name="otds.c.library.console.appenders"
class="org.apache.log4j.ConsoleAppender">
        <param name="Target" value="System.out"/>
```

```

<layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern" value="%-5p %c{3} - %m%n" />
</layout>
</appender>

<!-- Output the log message to a log file named otds.c.library.log -->

<appender name="otds.c.library.normal.appenden"
class="org.apache.log4j.FileAppender">
    <param name="file" value="otds.c.library.log" />
    <param name="append" value="true" />
    <layout class="org.apache.log4j.PatternLayout">
        <param name="ConversionPattern" value="%d %5p %c{3} - %m%n" />
    </layout>
</appender>

<!-- the following appender creates a logfile in log4j XML format, suitable to
viewing with
    XML log viewer such as Chainsaw (https://logging.apache.org/chainsaw/2.x/) -->

<appender name="otds.c.library.xml.appenden"
class="org.apache.log4j.RollingFileAppender">
    <param name="file" value="otds.c.library.xml" />
    <param name="append" value="true" />
    <param name="ImmediateFlush" value="true" />
    <layout class="org.apache.log4j.xml.XMLLayout" />
</appender>

<!-- Setup the logger category, add the appenders and set the default level
    5 level of logging, ALL < DEBUG < INFO < WARN < ERROR < FATAL -->

<logger name="otds">
    <level value="ALL" />
    <appender-ref ref="otds.c.library.console.appenden" />
    <appender-ref ref="otds.c.library.xml.appenden" />
    <appender-ref ref="otds.c.library.normal.appenden" />
</logger>

</log4j:configuration>

```

2. Modify appender in order to redirect the log file to an accessible directory.  
For example:

**Example:**

```

<appender name="otds.c.library.normal.appenden"
class="org.apache.log4j.FileAppender">
    <param name="file" value="c:\temp\otds.c.library.log" />
    <param name="append" value="true" />
    <layout class="org.apache.log4j.PatternLayout">
        <param name="ConversionPattern" value="%d %5p %c{3} - %m%n" />
    </layout>
</appender>

```

3. For UNIX, move the otds.c.library.logging.xml configuration file to the /tmp/config directory.
4. For Windows, move the otds.c.library.logging.xml configuration file to the same location as the otdsclient.dll file.
5. Restart your system or OpenText Content Management process and capture the otds.c.library log file.

---

If you intend making major changes to your synchronized user partition

---

You may want to stop monitoring your identity provider before making major changes to your synchronized user partition. To stop monitoring changes, see [step 12](#).

## 25.3 Enterprise sync issues

Enterprise Sync imports and synchronizes users from Active Directory and LDAP. Here are some common issues:

---

### I am unable to connect to Active Directory through SSL

---

To resolve this issue, use a fully qualified domain name for the domain controller.

---

### Limited import / sync failures

---

Some user or group entries exist in Active Directory, but do not make it to OTDS. This can occur because OTDS has stricter syntax checking than Active Directory for some types, for example, `telephoneNumber`.

To resolve this issue, consult the “[directory-provenance.log](#)” on page 376 for individual import or sync failure entries and correct the appropriate entry in Active Directory. You can also choose to map the attribute that is not importing to a string-valued OTDS attribute. If you choose this option, you will need to consolidate after making mapping changes.

---

### Password expiry

---

OTDS can use read-only accounts with which to sync. OTDS read-only accounts tend to have passwords that expire.

---

### Some user and group types are not imported

---

The default import filter includes:

- Domain Users
- Domain Local Groups
- Domain Global Groups
- Universal Groups

The default import filter excludes:

- Active Directory Built-in Users
- Active Directory Built-in Groups
- Groups of type Distribution

The default filter can be changed to include or exclude your desired object types. The Domain Users group is not supported, and therefore is not imported.

---

**What does “Person Error: ALREADY\_EXISTS” in the logs mean?**

---

The default synchronized partition user mapping is from OTDS CN to LDAP CN. If your environment is structured to allow users with duplicate CNs, and you leave the default user mapping, you will see the following error messages in the logs:

```
Person Error: ALREADY_EXISTS  
<user> cannot be added because an entry with that name already exists
```

You must ensure that your Directory Services CN user mapping is unique in OU. Identify a unique user attribute that can be mapped, and then edit your user mappings accordingly. For more information, see [“Defining user attributes” on page 70](#).

## 25.4 OpenText Content Management issues

Here are details and suggestions when dealing with OpenText Content Management issues:

---

**What are the OTDS client library error codes?**

---

When trying to resolve difficulties with OTDS, always check the OTDS log files. For more information, see [“Log Files” on page 375](#).

| OTDS client library error code number | Description                                                                                                                                                                                                                                               |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2                                     | The network call to OTDS failed.                                                                                                                                                                                                                          |
| 3                                     | OTDS server error. See the <a href="#">“otds.log” on page 375</a> file for more information.                                                                                                                                                              |
| 9 / 10 / 11                           | Failure to parse OTDS ticket. For more information, see <a href="#">“What does “Error validating a ticket. OTDS client library error code: -11” mean? on page 398</a> .                                                                                   |
| 12                                    | The OTDS ticket is a single-use type ticket which has already been used and cannot be used again.                                                                                                                                                         |
| 13                                    | Clock skew error. Verify that the time and time zone on OTDS and OpenText Content Management is correct and in sync.                                                                                                                                      |
| 19                                    | The OpenText Content Management resource has not been activated in OTDS. For more information, see <a href="#">“What does “Error activating OpenText Content Management as an OTDS resource. OTDS client library error code: -19” mean? on page 399</a> . |

---

**What does “Error validating a ticket. OTDS client library error code: -11” mean?**

---

This error indicates that the user is seeing a ticket mismatch between OpenText Content Management and OTDS. There are three possible options to resolve this issue:

1. The first option is to deactivate the resource from the OTDS side, and then reactivate from OpenText Content Management:
  - a. Sign in to Directory Services, and deactivated the resource.
  - b. Sign in to OpenText Content Management. On the **Directory Services Integration Administration** page, change the integration information, and then restart the OpenText Content Management admin servers.
  - c. In OpenText Content Management, change the Directory Services integration settings to the correct settings and then restart the OpenText Content Management admin servers again.
2. A second option to resolve this issue is to ensure that you set your maxHttpHeaderSize to 65536. For more information, see "[Configuring Tomcat for OTDS](#)" on page 14.
3. The final option to resolve this issue is to check to see if a client / server mismatch has occurred:
  - Content Server was using a resource ID that was activated with 10.5, and then switched back to Content Server 10.0.
  - If Content Server 10.0, as opposed to 10.5, is being used in an OTAG/ AppWorks environment.
  - If somebody put a 10.2.1 client library, maybe from a hotfix, onto a Content Server 10.5 server.

---

**What does "Error activating OpenText Content Management as an OTDS resource. OTDS client library error code: -19" mean?**

---

This error indicates that the user must deactivate the resource from the OTDS side, and then reactivate from OpenText Content Management:

1. Sign in to Directory Services, and deactivated the resource.
2. Sign in to OpenText Content Management. On the **Directory Services Integration Administration** page, change the integration information, and then restart the OpenText Content Management admin servers.
3. In OpenText Content Management, change the Directory Services integration settings to the correct settings and then restart the OpenText Content Management admin servers again.

---

**How do I access OpenText Content Management if OTDS is unavailable?**

---

If OTDS is not available, OpenText Content Management will still be accessible by:

- The Admin user. The password must be maintained using OpenText Content Management.
- Any users created from OpenText Content Management with Administration privileges, whose password is maintained using OpenText Content Management.

Access OpenText Content Management directly using this URL:

`https://<server>/<OpenText Content Management_name>/cs.exe?  
func=admin.adminuserlogin`

---

**What ports must the administrator ensure are open on OTDS and OpenText Content Management?**

---

The port used by the web application server, Tomcat, needs to be open.

If you are running consolidation from a server that is not the master host, you also need to ensure that the port that you defined in [Synchronization Master Host on page 312](#) is open.

---

**When I perform an OTDS migration, why are my OpenText Content Management internal groups not migrated?**

---

The exact reasons for migration failures are shown in the log which is displayed on the OpenText Content Management **Migration Status** page.

One common reason for “unauthorized” errors is that resources do not have administration rights in OTDS and OpenText Content Management cannot create a partition. You must do the following:

- Make sure the OpenText Content Management access role in OTDS has been created correctly. The OpenText Content Management Members partition needs to be added to the OpenText Content Management access role.
- Make sure that the **Include groups** option has been selected on this OpenText Content Management access role.

---

**Why can I not reset the password for a user in the otds.admin partition?**

---

To reset the password for any user in the `otds.admin` partition, the OpenText Content Management resource principal must be given administration rights in OTDS.

To do this, you can add the resource principal user to the `otdsadmins@otds.admin` group.

The `otds.admin` partition includes the OpenText Content Management Admin account. By default, the `otadmin@otds.admin` account is mapped to the OpenText Content Management Admin account.

## 25.5 Resource configuration issues

Directory Services displays the message: There was a problem with your request. Please contact your administrator if this persists. The DNS domains for the request and response differ or cannot be determined.

---

Directory Services may need to use a domain-level cookie to pass the user's authentication token to resources, depending on the functionality implemented by the resource. The resource must be configured with a fully qualified DNS domain name for the Directory Services URL, and the browser must use a fully qualified DNS domain name in order to access Directory Services. Moreover, Directory Services and the resource must reside in the same top-level domain.

As an example, the cookie from Directory Services *will* make it to the resource if:

- Directory Services is in .opentext.net and the resource is in .opentext.net
- Directory Services is in .opentext.net and the resource is in .cs.opentext.net

The cookie from Directory Services *will not* make it to the resource if:

- Directory Services is in .opentext.net and the resource is in .opentext.com

In this case, Directory Services will display the error above. Ensure that both OTDS and the resource are accessed using the same top level DNS domain. This may require a DNS alias, a reverse proxy, or another network-level solution.

Directory Services will issue the cookie to the narrowest scope domain that matches the Directory Services URL and the resource's URL. For example, if OpenText Content Management is cs.dev.opentext.net and Directory Services is otds.dev.opentext.net, Directory Services will issue the cookie to the .dev.opentext.net domain.

However, the Directory Services configuration property **Default HTTP Cookie Domain** can be used to force the cookie domain to a wider scope, for example .opentext.net, if this is desired.

---

OpenText Content Management displays a message informing you that the request came from a referring website that is not trusted

---

To resolve this issue, add the Directory Services URL to the **Trusted Referring Websites** box.

**To add the Directory Services URL to the Trusted Referring Websites box:**

1. In the OpenText Content Management administration page, under **Core System - Security Configuration**, click **Security Parameters**.
2. On the **Configure Security Parameters** page, scroll down to the **Referring Websites** box in the **Trusted Relationships** area.

3. In the **Trusted websites** box, type your Directory Services URL. For example: `http://opentext-otds.opentext.net:8080`

For more information, see “[Configuring Directory Services integration administration in OpenText Content Management](#)” on page 219.



**Note:** This occurs automatically in OpenText Content Management Update 7.

---

#### One or more users cannot access a resource

---

A log entry similar to the following may appear:

**Example:**

```
OtdsException: cannot map Otds user: user@domain to resource:  
c7f7d5b9-19be-4134-96ac-37fc4f34e31e
```

This occurs when Directory Services has successfully authenticated the user, but Directory Services has not been configured to allow this user access to the requested resource.

If you are certain the user should have access to the resource, perform the following steps, stopping when you have resolution.

**To resolve user access to a resource:**

1. Double check all access roles for that resource, and ensure that there is a route from the user to at least one access role where:
  - Organizational unit hierarchy is traversed.
  - Group membership is traversed, double check group membership for user.
2. Updates may have been missed, attempt consolidation against the user, user's groups, organizational units, and partitions.
3. Try removing and re-adding members to the access role.
4. Double check that your resource is configured with the correct resource identifier. You do this from the web administration menu, from the **Resources** page.
5. Verify that the user has a value for `oTGroupOfResources` for the resource in question.

---

```
User jsmith@otag does not have access to resource <x>. Please contact  
your administrator.
```

---

Could mean that the user has not yet been added to the access role. Check that the user is in OpenText Content Management, and was created or pushed by OTDS. You also need to ensure that user `jsmith@otag` is in the OpenText Content Management access role in OTDS.

Why, when I select delete users/groups on consolidate, are my users or groups not removed?

When you choose to consolidate your resource, you have the option of selecting **Delete users/groups that are not consolidated**. The consolidation must first succeed without errors in order for OTDS to begin deleting unknown users and/or groups. You can check for consolidation errors in “[otds.log](#)” on page 375 and “[directory-provenance.log](#)” on page 376.

What does “The URL `http://mymachine.opentext.net:8080/` is not a trusted referral site. Please contact your administrator.” mean?

After you have set up a resource in OTDS, and if that resource is physically located on a different system than OTDS, you need to add the URL that accesses that resource to the trusted sites in OTDS. For more information, see “[Trusted Sites](#)” on page 327.

What can I use in the **Format** column of my synchronized resource's **User Attribute Mappings** and **Group Attribute Mappings** pages?

In general, you can use the Java Formatter syntax in addition to specific options available in OTDS. For more information, see “[OTDS resource Format options](#)” on page 183 and “[Support for javascript and multi-valued javascript in the Format column](#)” on page 183. For more information, see the reference to the Java Formatter document in “[References to external websites](#)” on page 385.



**Note:** There is a format column available in user partitions and resources. This section applies to the **Attribute Mappings Format** column for resources only.

For information about the format column in user partitions, see “[User partitions](#)” on page 65.

## 25.6 Single sign on issues

---

### Issues with Directory Services Service Principal Names

---

Use `setspn.exe` to associate your Directory Services installation to the following Active Directory Service Principal Names:

- `HTTP/<Fully Qualified Domain name of Directory Services Server>`.
- `HTTP/<NetBIOS Name of Directory Services Server>`.



**Note:** If Tomcat is running under the Local System Account (default), you must set SPN against the Computer Object.

If Tomcat is running under a named account, you must set SPN against the Account Object.



#### Important

Do not set SPN against multiple objects because this causes instability and intermittent authentication faults.

For more information, see [Authentication Service Principal Name on page 290](#).

---

#### Single sign on from desktop does not work with Firefox on Windows

This occurs because Firefox permits negotiated authentication only with named servers.

#### To configure single sign on with Firefox:

1. Launch Firefox.
2. In the address box, enter “about:config”.
3. Add this setting: network.negotiate-auth.trusted-uris = otdsServer, where otdsServer is the DNS name or IP address of the Directory Services server.

---

#### Single sign on from Internet Explorer does not work

When your browser gets redirected to the ECM Suite sign in page, it displays a login window from Internet Explorer.

This occurs because the Directory Services server may not be deployed on a site trusted by your Internet Explorer, or Integrated Windows Authentication may not be enabled on your Internet Explorer.

To resolve this issue, add your Directory Services server as a trusted site using **Tools > Internet Options > Security > Local Intranet > Sites > Advanced**.

Alternately, make sure Integrated Windows Authentication is enabled using **Tools > Internet Options > Advanced > Security > Enable Integrated Windows Authentication**. This requires a restart.

---

#### Single sign on is not recognizing the local intranet

On Windows 7 if the environment within which the web browser is running is not recognized as a part of the intranet, it will not even attempt IWA (Integrated Windows Authentication). This problem should be confined to environments where the local networks are not fully trusted by the local domain.

To resolve this issue, the settings in the security or intranet zone must be modified to include the server as a proper intranet site.



**Tip:** This issue could apply to all recent versions of Windows. When in doubt, check to see what your browser shows in the status bar for the zone in which it has put the site. If it is not the Local Intranet then this may resolve your single sign on issue.

#### To create trusted intranet zones for single sign on with a Windows browser:

1. Start a browser session.
2. In the Windows Control Panel, open **Internet Options**.
3. Select the **Security** tab.

4. Select the **Local Intranet** zone.
5. Click **Sites**.
6. In the next window, click the **Advanced** button.
7. Add the fully qualified name of the server in the format `http://<server>`
8. Click **OK** to close all the Windows.

**To create trusted intranet zones for single sign on in Firefox:**

1. Open a Firefox browser window.
2. In the address box, enter “about:config”.
3. In each of the following configuration parameters add the fully qualified name of the trusted server:
  - `network.automatic-ntlm-auth.trusted-uris`
  - `network.negotiate-auth.delegation-uris`
  - `network.negotiate-auth.trusted-uris`

---

A third-party authentication product prompts for sign in with  
OpenText Content Management

---

Usually, your third-party authentication product's agent will already be deployed on OpenText Content Management, therefore, accessing OpenText Content Management will result in a sign in prompt by the third-party product. You must have the third-party authentication product's agent deployed on the Directory Services server. However, the policy server must be configured to protect only `/otdswebs/login*`, that is, `/otdswebs/login` and all subpaths. No other paths belonging to Directory Services should be protected.

These other paths can be seen through the Tomcat Manager:

- `/otds-usergroup*`
- `/ot-auth*`
- `/ot-authws*`
- `/otds-v2*`
- `/otds-system-configuration*`
- `/ot-universaladmin*`
- `/ot-trigger*`
- `/ot-transfer*`
- `/ot-reg*`

These are web service URLs and, if they are blocked by an authentication prompt, OpenText Content Management will not be able to reach Directory Services through web service calls.

## 25.7 Performance issues

If you are using Oracle Directory Server, the default OTDS search method may timeout if there are over 200,000 objects in the server.

When adding a user partition to connect to an Oracle Directory Server, the default search method used by OTDS is VLV (virtual list view) because Oracle Directory Server does not support paged search.

If the Oracle Directory Server contains over 200,000 objects, any search call that spans the 200,000 objects in the server can stop responding for a long time before timing out. This prevents users or groups from being imported.

To work around this problem, when you create the user partition, you need to ensure that the **Start import** box is cleared at the end. After creating the user partition, edit the **Notification/Search** tab. Change the **Search Method** to unlimited. You can now start the import process. For more information, see “[Editing a synchronized user partition](#)” on page 97 and “[Importing users and groups](#)” on page 86.

! **Important**

The user running the search must have the proper rights to run an unlimited search.

## 25.8 General issues

**Cannot accept ticket. Clock skewed too much.**

Your clock is not synchronized across the domain. The domain controller's clock and your server's clock are more than ten minutes apart.

To resolve this issue, synchronize time throughout your entire network. For more information, see the synchronize time reference in “[References to external websites](#)” on page 385.

**How can I monitor the consolidation process and what do I do if users and groups are not synched to my resource?**

You can check for consolidation messages on the **Jobs** tab in the OTDS administration page. You can also check in the “[otds.log](#)” on page 375 and “[directory-provenance.log](#)” on page 376 log files.

➔ **Example 25-1: An example of a consolidation message:**

```
2014-04-16 14:05:03.464 INFO - ,2014/04/16 14:05:03 EDT,0,0,,Enterprise Sync  
Processor,Success Provenance,3,Object Modify,punisherTestScheduler  
IMPORTED,,setPartitionConsolidationStatus()  
  
2014-04-16 14:05:03.465 INFO - ,2014/04/16 14:05:03 EDT,0,0,,Enterprise Sync  
Processor,Success Provenance,3,Object Modify,punisherTestScheduler 16/4/2014:2h:5m:  
3s PM,,setPartitionConsolidationEndTime()
```



In the consolidation message you will find `oTConsolidationStatus` attributes that will tell you what is going on.

---

**What should I do when I see “null.null.null:...error validating ticket” in the SAP UI?**

---

Perform the following checks:

1. Check the logs to see whether the SAPlogon ticket has been successfully validated:

For example, check for:

```
2012-06-22 14:34:30,201 INFO [http-8080-5] otx.OTDS :
com.opentext.otds.as.drivers.sapsoext.SAPSSOEXTAuthHandler - User verified in
SAP token
[AjQxMDMBABhLAEsATwBMAFUAUwBVACAAIAgACAAIAACAY4ADAAMAADABBEADYATgAgACAAIAAgAC
AABAAYMgAwADEAMgAwADYAMgAyADEAMgAzADQABwAEAAAAAgAAQEJAAJFAP8BCTCCAQUGCSqGSIB3D
QEHAqCB9zCB9zIBATELMakGBSs0AwIaBQAwCwYJKoZIhvCNQcBMYHUMIHRAgEBMCYwGzELMAKGa1UE
BhMCREUXDDAKBgNVBAMTA0Q2TgIHIBEJQ1I0DAJBgUrDgMCggUAoFOwGAYJKoZIhvCNQkDMQsGCSq
GSIB3DQEHEATAcBgkqhkiG9w0BCQUxDcNMTIwNjIyMTIzNDI2WjAjBgkqhkiG9w0BCQQQxFgQUuP91IE
PyTLaqhaqgnKxBJSpqPUwCQYHKoZIZjgEAwQvMCOCFHJEQ7W2sC8RLPYpo1AEBW3jirWHAhUAgm8zU
WLZY7Ln/a7gikFVawSzp3w=] is: KKOLUSU
```

If the SAPlogon ticket authentication does not work, check the following:

2. If you see an “Unsatisfied Link error” message in the `otds.log` file, it may be because the SAPSSO libraries cannot be found by the application server.  
To enable tracing of the SAPSSO library, see the information about the environment variables `SAP_EXT_TRC=mytracefile.txt` and `SAP_EXT_TRL=3` in the SAP documentation.
3. Check to see if there are any SAP return value numbers, then check the SAP documentation for an explanation of the return codes.
4. Check to see whether the SAP user is mapped correctly to OTDS and to OpenText Content Management. To check, see the `directory-access.log` file.
5. Check to see whether the users are assigned to OpenText Content Management.

---

**How do I resolve “MULTIPLE\_IDENTITIES\_FOR\_USER\_NAME” errors when different users are registered with the same email account in OTDS?**

---

If you have more than one user sharing the **Login User Name Attributes** system attribute, you need to change the configuration of this system attribute to remove those attributes that cause the conflict.

For example, if multiple accounts can have the same email address, and users do not sign in with their email address, you can remove “mail” from the **Login User Names Attributes** system attribute.

For more information, see [Login User Name Attributes on page 305](#).

---

**Why are my Global Help Server URLs not resolving properly?**

---

There are three OTDS system attributes that need to be set correctly in order for the Global Help Server URLs to resolve properly. If you cannot open the OpenText Global Help Server:

- Ensure that the [help.config.HelpTenant](#) on page 301 system attribute's value is: 1
- Ensure that the [help.config.HelpType](#) on page 301 system attribute's value is: ofh1
- Ensure that the [help.config.HelpURL](#) on page 302 system attribute's value is: <http://docsapi.opentext.com/mapperpi>



**Note:** Another, related, issue you may experience has do with your browser's cache. For example, if you upgrade OTDS from 16.0.2 to 16.0.3 and then open the online help, you might see the 16.0.2 online help appearing. If this happens, you will need to clear your browser's cache and then open the online help.

---

**What happens with my email customizations after I patch or update OTDS?**

---

You have the opportunity to customize the emails that OTDS sends out, as documented in ["Customizing OTDS emails"](#) on page 356.

- If you are using OTDS 10.5 SP1 Patch 9 or previous, and, after customizing OTDS emails, you applied an OTDS patch or update, that update overwrote any customizations to the `ot_email_header.png` file, the XSLT stylesheet files, and the variables stylesheet.

You will need to implement your email customizations again.

- If you are using OTDS 16.0.1 or previous, and, after customizing OTDS emails, you applied an OTDS patch or update, that update overwrote any customizations to the `ot_email_header.png` file, the XSLT stylesheet files, and the variables stylesheet.

You will need to implement your email customizations again.

- If you are using OTDS 10.5 SP1 Patch 10 and forward, or version 16.0.2 and forward, your email customizations will remain in place during subsequent patches and updates.
- Beginning with OTDS 16.4.2, the direction is to create a new `email-custom` directory. When you patch or update OTDS, your `email-custom` files will not be updated. Only the files in the `email` directory will be updated.

---

**How do I remove the availability of a certain language in OTDS?**

---

If you do not want a certain language to be available in OTDS, you can delete the corresponding `login_<langcode>.properties` translation file in the `<OTDS_install_dir>/otdsws/WEB-INF/classes` directory.



**Important**

You must not delete the English language file, `login.properties`.

Before making changes to a synchronized user partition, can I save my configuration?

If you want to test changes to a synchronized user partition's configuration, you can duplicate the partition in order to save the original configuration. For more information, see "[Duplicating a synchronized user partition](#)" on page 100.

---

Why do I experience issues with the OTDS UI when using IE?

In Internet Explorer you might experience several UI issues if you have Compatibility View enabled. You should disable Compatibility View by selecting **Tools > Compatibility View settings**. In the **Compatibility View Settings** box, clear **Display intranet sites in Compatibility View**.

---

Why am I experiencing issues with SAML and Chrome?

SAML-based authentication typically involves cross-site POST requests to deliver SAML payloads. OTDS uses cookies to maintain authentication-related state. Depending on the version of the Chrome browser you are using, and due to changes in Chrome's default security settings, SAML-based authentication with OTDS might only work over a secure, https, connection.

You should ensure that the OTDS system attribute, [Want Secure Cookies on page 314](#), is set to the default "True".

OTDS authentication is frequently performed in a framed environment, *<iframe>*, with integrated applications. A framed environment is treated as a third-party context by the browser. For such scenarios, the following system attribute must also be enabled in order for OTDS to set SameSite=None on all its cookies: `otds.as.SameSiteCookieVal = None`

For more information, see [SameSite Cookie Attribute on page 308](#).

