Configuring LDAP

The User Administration module facilitates user authentication and integration with LDAP servers. In this section:

- Accessing User Directories
- Configuring Directory Settings
- Importing Users
- User Administration REST API

> ⓘ **Connecting to an LDAP over SSL**
>
> DTP will reject connections to external servers if the server's certificate is not trusted or unsigned by a trusted certificate authority. See Adding Trusted Certificates for additional information on integrating with LDAP servers and other external systems secured with TLS/SSL.

Accessing User Directories

Choose **User Administration** from the settings menu (gear icon) and click the **User Directories** tab. Existing directory configurations are listed in the table.

You can perform the following actions:

- Click **Create User Directory** and configure the directory settings to add a new user directory configuration (see Configuring Directory Settings).
- Click on an existing directory name or URL to edit the directory configuration (see Configuring Directory Settings).
- Click the import button to add users associated with the directory to DTP (see Importing Users).
- Click the trash button to delete the user directory configuration.
- Click and drag directories into the preferred order. When using the search function in the Users and Groups tabs, DTP checks directories in the order specified in the User Directories tab.

Configuring Directory Settings

Click on a directory to configure existing settings or click **Create User Directory** to set up a new directory. You can configure the following settings.

General Settings

New directories are enabled by default, but you can prevent the directory from syncing with your LDAP server by disabling the **Enable** option.

A name for the directory is required.

Server Settings

This settings specify DTP's connection to the LDAP server. Click **Test Connection** after you've configured the settings to verify that DTP can communicate with your LDAP server.

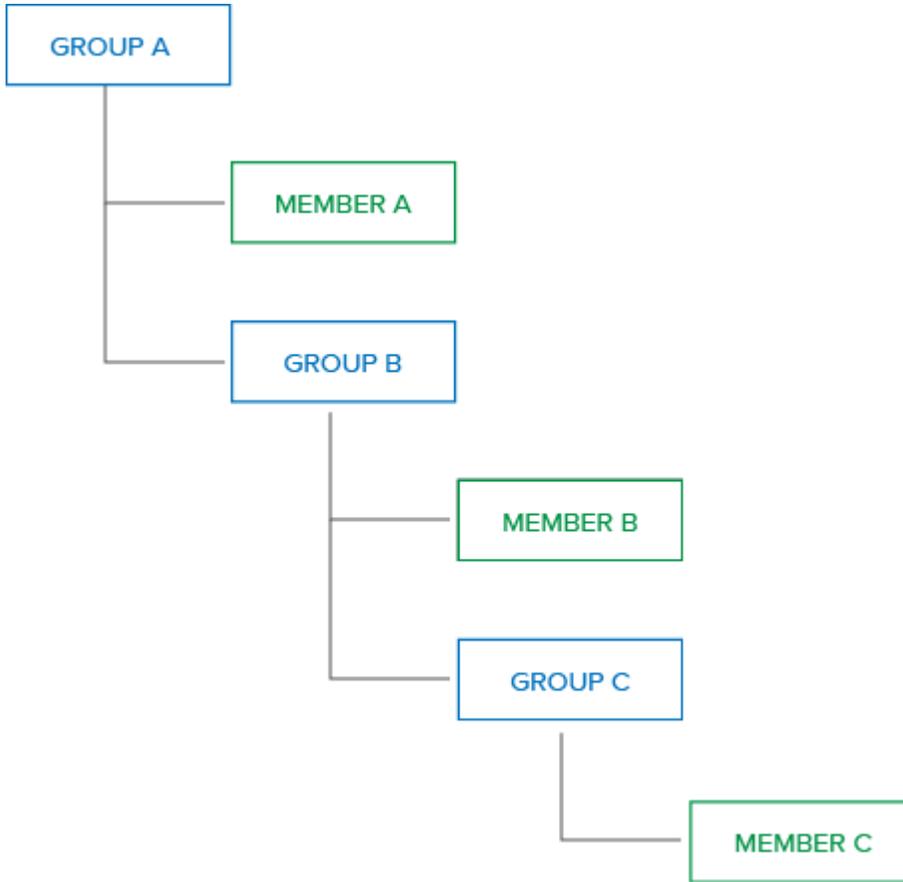|	
Hostname	The LDAP server hostname.
Port	The LDAP server port.
Use SSL	Enable this option to connect to the LDAP server over SSL.
Credentials	
Username	If the LDAP server requires credentials, specify the username in this field.
Password	If the LDAP server requires credentials, specify the password in this field.

User Import Settings

Click **Test User Import Settings** after configuration to verify that they are correct before saving.

Base DN	The base DN is the context DN (distinguished name) where the directory objects reside. If empty, DTP will use the root DN of the directory tree. Organizational units (ou) and domain components (dc) are used to define directory tree structures.
	
	The following example shows how an organization could structure its directory:
	
	`ou=US,ou=People,dc=company,dc=com`
	
	`ou=Europe,ou=People,dc=company,dc=com`
	
	`ou=Asia,ou=People,dc=company,dc=com`
	
	In this example, you would enter the following base DNs to scan users from Europe and Asia only.
	
	`ou=Europe,ou=People,dc=company,dc=com`
	
	`ou=Asia,ou=People,dc=company,dc=com`

Filter	Enter an expression in the Filter field to search on specific parameters. Searches are performed on the base DN(s) and specified scope. The following examples describe some of the ways filters can be used:
	
	Simple filter for users under provided base DN:
	
	`(objectclass=person)`
	
	Find "devel1" and "devel2" users only:
	
	`(objectclass=devel1)(objectclass=devel2)`
	
	Find users that are members of group "Managers":
	
	`(objectclass=person)(memberOf=cn=Managers,cn=Users,ou=company,ou=com))`
	
	ⓘ **About Filter Settings in Previous Versions of DTP**
	
	In versions of DTP prior to 5.4, the LDAP filter configuration included an extra attribute and template: `uid={0}`. This attribute and template has been removed in version 5.4 and later. If you upgraded 5.4 or later from a previous version, though, `the uid={0}` attribute will be set to `uid=*` for compatibility with the current LDAP user import functionality. There should be no impact to your experience as a result of this change, but we recommend verifying that your user and group import settings function as expected.

Restrict To Groups	Enable this option to import only the users that belong to a group specified in the Group Import Settings. Users that do not belong to a group configured in Group Import Settings will not be imported.
Attribute Mappings	
The attributes mapping section defines how DTP user definitions (i.e., DTP user login name, first name, last name, and email) map to directory object attributes (i.e., uid, givenName, sn, and email). You can use the defaults mappings or configure the attributes to align with your LDAP server. Refer to the documentation for your LDAP server	
Username	This field is used in DTP as the users' login name. The the `uid` attribute is commonly used to identify users in LDAP servers. In Active Directory, the `sAMAccountName` attribute is used as the client login name. Default is `uid.`

First Name	This field is used in DTP as the users' first name. The `givenName` attribute is commonly used to specify users' first name in LDAP servers. Default is `givenName`.
Last Name	This field is used in DTP as the users' last name (surname). The `sn` attribute is commonly used to specify users' last name in LDAP servers. Default is `sn`.
Email Address	This field is used in DTP as the users' email address. The `mail` attribute is commonly used to specify users' email address in LDAP servers. Default is `mail`.
Member Of	This field is used in DTP to associate users with LDAP groups. Default is `memberOf`. See Advanced Settings for additional information.

Group Import Settings

Click **Test Group Import Settings** after configuring the settings to verify that they are correct before saving.
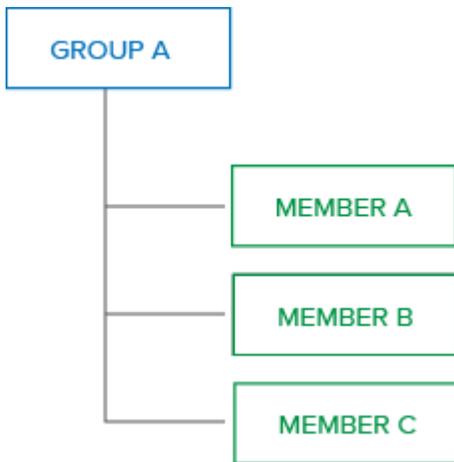
Enable group import	If you want to import groups set in your LDAP, enable the **Enable Group Import** option.
Base DN	See the Base DN setting under User Import Settings.
Filter	See the Filter setting under User Import Settings. ⓘ **About Group Filter Settings in Previous Versions of DTP** In versions of DTP prior to 5.4, the LDAP filter configuration included an extra attribute and template: `cn={0}`. This attribute and template has been removed in version 5.4 and later. If you upgraded 5.4 or later from a previous version, though, `the cn={0}` attribute will be set to `cn=*` for compatibility with the current LDAP user import functionality. There should be no impact to your experience as a result of this change, but we recommend verifying that your user and group import settings function as expected.
Enable nested groups	If groups contain other groups in your directory, you can enable this setting to retain your LDAP server's hierarchical structure.

Ancestor groups only	A nested group may contain users, in addition to other groups. An ancestor is a user that is the immediate member of a group nested inside another group. In the following example, MEMBER B and C are the ancestors within the groups nested within GROUP A.
	You can enable the **Ancestor groups only** option and specify a group name in the **Ancestor group names** field to import only the immediate members associated with the nested groups. Members of the group specified in the **Ancestor group names** field will also be imported.
Ancestor group names	If the Ancestor groups option is enabled, specify the name of the nested group that contains the ancestors you want to import.

Attribute Mappings

The attributes mapping section defines how Parasoft User Administration object attributes map to the connected directory object attributes. You can use the defaults mappings or configure the attributes to meet your specific needs.

Name	Default is `cn`.
Description	Default is `cn`.

Member	Default is `member`. See Advanced Settings for additional information.

Advanced Settings

You can specify the scope of user and group queries User Administration performs in your LDAP.

User search scope	Choose one of the following options from the drop-menu to set the user search scope: • Object: Restricts search to the base DN. The maximum number of objects returned is always one. • One Level: Restricts search to the immediate children of the base DN. The base DN object is also excluded. • Subtree: All child objects, as well as the base DN, are searched. You can request the LDAP provider to chase referrals to other LDAP directory services, including other directory domains or forests.
Group search scope	Choose one of the following options from the drop-menu to set the group search scope: • Object: Restricts search to the base DN. The maximum number of objects returned is always one. • One Level: Restricts search to the immediate children of the base DN. The base DN object is also excluded. • Subtree: All child objects, as well as the base DN, are searched. You can request the LDAP provider to chase referrals to other LDAP directory services, including other directory domains or forests.
Referral	Choose **Follow** from the drop-down menu to enable JNDI lookup. Choose this option for Active Directory servers configured without a DNS. Choose **Ignore** from the drop-down menu to ignore communication errors when Active Directory returns domain names for referrals other than the name specified in the server.
Page size	This setting specifies the number of record requests per page. Setting a page size allows the server to send the data in pages as the pages are being built. Default is `1000`.
Membership strategy	This setting specifies how group membership is correlated when importing users from LDAP. DTP can correlate users based on their `member` or `memberOf` attribute from the LDAP server. • Choose **Use "Member" Attribute** from the drop-down menu and DTP will associate groups to users based on the group Member attribute. The Group Import Settings must be enabled to use this membership strategy. • Choose **User "Member Of" Attribute** from the drop-down menu and DTP will associate users to groups based on the user Member Of attribute. You can set the Member Of attribute in the User Import Settings.
Sync group membership	Enable this option to update user attributes and permissions based on group membership from LDAP. If enabled, DTP will refer to LDAP as the system of record for user membership. Any user/group associations made in DTP that differ from the membership associations in LDAP will be removed or overwritten by the associations stored in LDAP. DTP applies directory configurations in reverse sequence as they appear in the User Directories page. As a result, the directory at the top of the list takes precedence and should be the directory with Sync Group Membership enabled. Default is disabled.
Use DNs for membership	Enable this setting if DTP should expect distinguished names (DN) from your LDAP server to set user and group associations. Disable this setting to associate users and groups based on usernames and/or group attributes. Default is enabled.
User primary groups	Enable this settings to determine user group membership information using basic and Primary Groups defined in Active Directory. Default is disabled.
Read timeout (ms)	Specify how long DTP should wait when attempting to read data from the LDAP server before timing out. Default is `120000`
Connection timeout (ms)	Specify how long DTP should wait when attempting to connect to the LDAP server before timing out. Default is `10000`

Importing Users

You can import users from your user directories after configuring your LDAP connection.

1. Open Choose **User Administration** from the settings menu and click the **User Directories** tab.

2. Click the import button for the directory you want to import.

3. Review the users to be imported and click **Next** to proceed or **Cancel** to exit without importing.

> (i) Attributes associated with existing users will be overwritten with data from the LDAP server.

4. Review the user groups to be imported. Click on the disclosure triangle to view the users within a group.

5. Click **Next** to review the import settings.
6. Click **Import** to begin importing users.

A summary of the results will appear after the import completes.

User Administration REST API

The User Administration module includes a dedicated API that you can use to automate user administration tasks. Choose **API Documentation** from the help menu on the User Administration page. The documentation describes the available endpoints. *The API is only accessible from the User Administration page in DTP.*

Automating LDAP Synchronization

The simplest method for automating LDAP synchronization is to set up a nightly job using an automation tool, such as Jenkins. You can trigger LDAP synchronization by using a cURL command, for example, to call the User Administration REST API (/pstsec/api) endpoint:

```
curl -u username:password -X POST "https://hostname:port/pstsec/api/v1.0/ldap/import/configurationName" -H
"accept: application/json"
```

In this example, replace `username`, `password`, `hostname`, `port`, and `configurationName` with your specific information.