Troubleshoot LDAP

Who is this article for?
√ Ø Code42 for Enterprise
√ Ø CrashPlan for Small Business

Code42 for Enterprise, yes.
CrashPlan for Small Business, no.

This article applies to on-premises authority servers.

Overview

LDAP (http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol) provides a powerful and flexible way to manage your user base. Its flexibility and features, however, mean that your Code42 environment's LDAP implementation may sometimes experience problems or invalid configurations. This article will help you troubleshoot a number of LDAP issues.

Affects

On-premises authority servers configured with LDAP

Before you begin

This article includes advanced instructions on your Code42 environment's LDAP configuration. Familiarize yourself first with these foundational articles on LDAP and your Code42 environment:

• Integrating With LDAP For User Authentication (https://support.code42.com/Administrator/6/Configuring/Integrate_with_LDAP_for_user_authentication)
• User Management With LDAP Integration (https://support.code42.com/Administrator/6/Monitoring_and_managing/User_management_with_LDAP_integration)
• How LDAP Syncing Works (https://support.code42.com/Administrator/6/Monitoring_and_managing/How_LDAP_sync_works)
• LDAP Connection Problem (https://support.code42.com/Administrator/6/Troubleshooting/Alerts/LDAP_connection_problem)
Considerations

• The Code42 environment's LDAP implementation provides many settings and features (https://support.code42.com/Administrator/6/Code42_console_reference/LDAP_reference). If one of these settings is inadvertently changed, or if the associated Microsoft Active Directory (http://en.wikipedia.org/wiki/Active_Directory), Apple Open Directory (http://en.wikipedia.org/wiki/Apple_Open_Directory), or LDAP server is offline or experiences a configuration change, then your Code42 environment's LDAP functionality may be affected. Network and firewall (https://support.code42.com/Administrator/6/Planning_and_installing/IP_addresses_and_ports_used_by_the_Code42_platform) settings are also common sources of problems.


This article will help you try to determine the source of LDAP issues and suggest solutions for them.

Diagnose problems

Your Code42 environment has a number of ways to alert you to LDAP problems:

• Alerts that appear on the Alerts Overview (https://support.code42.com/Administrator/6/Code42_console_reference/Alerts_reference) page

• Emailed alerts

• Icons on the LDAP configuration page (https://support.code42.com/Administrator/6/Code42_console_reference/LDAP_reference#Add)

• Logs within the Code42 environment

Each of these items is discussed in greater detail below. Keep in mind that LDAP is a complex subject, and that it may take some time, research, and effort to isolate a problem related to LDAP.

Alerts overview page and emailed alerts

The Alerts Overview page contains two alerts relevant to LDAP. The emailed alerts are identical, and are sent to the email addresses configured at Settings > Notifications (https://support.code42.com/Administrator/6/Code42_console_reference/Notifications_settings_reference).

• LDAP Connection Problem (https://support.code42.com/Administrator/6/Troubleshooting/Alerts/LDAP_connection_problem)
• Directory Sync Deactivate (https://support.code42.com/Administrator/6/Troubleshooting/Alerts/Directory_sync_deactivate)

Refer to these alert description articles for more details and possible solutions.
LDAP configuration page

The LDAP configuration pane ([link](https://support.code42.com/Administrator/6/Code42_console_reference/LDAP_reference#LDAP_settings_in_the_administration_console)), located at Settings > Security > LDAP > LDAP Servers contains information on your LDAP configuration and mapping. If values are configured incorrectly, warning icons will appear to indicate an LDAP problem.

**Testing values or options**

In order to force your authority server to test a value or option, and display errors and possible issues, tab through the LDAP configuration fields ([link](https://support.code42.com/Administrator/6/Code42_console_reference/LDAP_reference#LDAP_settings_in_the_administration_console)).

A configuration pane with no visible issues looks like the example below:

![LDAP Server Setup](image)

LDAP activity logs

LDAP activity appears in com_backup42_app.log.[0-9], which is located in the Code42 server log directory:

- **Linux**: `/var/log/proserver`  
  Applies to Code42 servers installed as root on Ubuntu

- **Windows**: `C:\Program Files\CrashPlan PROe Server\logs`

Using your favorite text editor or textual search tool (e.g., `grep` in Linux/Unix), search for the keyword "DIRSYNC".

For example, from a terminal window in the Linux operating system, you could enter the following command to find all LDAP related entries in the latest log file:

```bash
grep "DIRSYNC" com_backup42_app.log.9
```
The actual messages you see in your log files depend on the LDAP settings and activity in your Code42 environment.

**Log files**

Your Code42 environment rotates log files when they reach a certain size. The current application log is `com_backup42_app.log.0`. Older logs are signified by `com_backup42_app.log.1`, and so on.

**Change the logging level**

You can change the logging level for LDAP activity in your authority server in order to gather troubleshooting information.

https://support.code42.com/Administrator/6/Troubleshooting/Troubleshoot_LDAP (https://support.code42.com/Administrator/6…)

Updated: Sat, 01 Aug 2020 15:52:42 GMT

Powered by Mindtouch®
To log the most detailed information, enter the following command in the Code42 console CLI (https://support.code42.com/Administrator/6/Code42_console_reference/Code42_console_command-line_interface_reference):

```
log com.code42.core.ldap trace
```

The logging level returns to the default level (info) when the Code42 server restarts. You can manually change the LDAP logging level back to default with the following command in the Code42 console CLI:

```
log com.code42.core.ldap info
```

For more information on the `log` command, see the Code42 console command-line interface (https://support.code42.com/Administrator/6/Code42_console_reference/Code42_console_command-line_interface_reference#Log) reference.

## LDAP troubleshooting

Each section below describes an LDAP issue, its symptoms, and a solution.

### URL unreachable

If the LDAP server is unreachable for any reason, you will see a warning icon to the right of the URL and search base field. Hover over it to see the tooltip Unreachable:

![LDAP Server Setup](image)

**Solution**

1. Check that you have entered the correct URL or IP address
2. Read [LDAP Connection Problem](https://support.code42.com/Administrator/6/Troubleshooting/Alerts/LDAP_connection_problem) for further troubleshooting

### Bind failure

If your authority server is unable to bind (HTTP://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol#Bind_.28authenticate.29) to the LDAP server, you will see the message "Bind failed" to the right of the Bind DN field. If you hover over the warning icon to the right of the "Bind password field", you will see a tool tip reading "Bind failed":

![Bind failure](image)
False Bind Failed Warnings Possible

Due to a known issue, the Code42 console sometimes displays a **Bind failed** message and/or a warning icon next to the **Bind password** field, even though the values for Bind DN and Bind password are correct.

If you think your **Bind DN** and **Bind password** values are correct and that the warning icon is being displayed in error, you should take the following steps:

1. Confirm that your search base and search filter are correct
2. Check the **Attribute Mapping** section of the LDAP configuration pane. If user information is being returned from your directory server and displayed, then you can safely ignore the **Bind failed** message and/or warning icon.

**Solution**

If the binding process fails, the authority server is unable to authenticate with the LDAP server. This could be caused by a number of issues:

- The Bind DN (distinguished name) is not correct
- The password for the Bind user may not be correct
- The entry for the Bind DN may have changed on the LDAP server
- The password for the Bind DN may have changed on the LDAP server

Confirm that the **Bind DN** and **Bind password** values are correct, and that the Bind user has the privileges needed to read entries from the LDAP server and search base.

If binding still fails, confirm that the Bind DN and password have not been inadvertently changed on the LDAP server. Contact your LDAP administrator, if necessary.

**Search filter issues**

**Search filter invalid**

If the search filter contains syntax errors or formatting errors, you will see the error message "Invalid. Example: (mail=?)" to the right of the search filter field.

**Solution**

Use valid formatting for your search filter. Search filters can contain multiple parameters joined by logical "and" statements. For example, here is a valid filter that looks for entries with the object class **inetOrgPerson**, and returns entries based on email address:

```
(&(objectclass=inetOrgPerson)(mail=?))
```

[https://support.code42.com/Administrator/6/Troubleshooting/Troubleshoot_LDAP](https://support.code42.com/Administrator/6/Troubleshooting/Troubleshoot_LDAP)
Search filter returns multiple results for each username

Search filter must return unique results
In order for your authority server to successfully sync with an LDAP server, the search filter must return unique results for each user entry in the configured search base. For example, if the search filter looks for users based on the uid, then there must be a one-to-one relationship between users and uids.

Because you can create a search filter based on any combination of object classes and attributes, it is possible to create a search filter that returns multiple results for a single combination of attributes and objects. This will cause the authority server to skip the affected user or users during sync.

In the example screenshot below, there are two users with entries in the configured LDAP server who have the same last names:

- Jane Doe
- Joe Doe

If the search filter is set to look for just the last name (using the sn or surname attribute), then one or both of these users are skipped during syncs:

Solution
Choose a search filter that returns unique results. In the example above, changing the search filter to the following search string solves the problem, because each user has a unique email address:

```
(mail=?)
```

https://support.code42.com/Administrator/6/Troubleshooting/Troubleshoot_LDAP
Search filter returns no results

![Search filter example](image)

**Search filter must return results**

If your search filter returns no search results on the LDAP configuration screen, then the search filter is incorrect, or a serious problem has occurred within your LDAP server.

This issue prevents new users from registering (or shunts them into the organization designated for registrants who are not found in the LDAP search). If the search filter on your authority server finds no users, then all active users in the affected organizations could be deactivated, and become unable to backup, restore, or sync.

**Solution**

- Ensure that your search filter uses the appropriate combination of attributes to find unique entries for each user
- Confirm on the LDAP server that users are present and in the appropriate LDAP locations

Search base error

If the search base is not correct or is omitted, no search results will be returned. Your users will be deactivated, and new users will not be added (or will be added to the organization configured to receive non-LDAP users).

This problem may be hard to detect, because the LDAP server will still appear to be reachable as long as the URL is correct. In the screenshot below, the URL is correct, but the search base is incorrect:

![Search base example](image)

If you tab through the "Search filter" field, however, the search will fail, and you will be alerted with the message "Error performing search," to the right of the "Search filter" field:

![Search filter example](image)

**Solution**

Study your LDAP schema with an LDAP browser in order to choose an appropriate search base. See the example LDAP schema below, as displayed by an open source LDAP browser ([JXplorer](http://jxplorer.org/)):
In this example, a valid search base would be "dc=testdomain,dc=c42". The entire URL and search base would be:

```
ldap://ldap:389/dc=testdomain,dc=c42
```

Another valid search base would be:

```
ldap://ldap:389/ou=people,dc=testdomain,dc=c42
```

This is because the desired users are within the "people" container of the LDAP hierarchy. You should have a good understand of your organizations LDAP hierarchy before setting the search base.

Unable to retrieve users

If the LDAP search is unable to retrieve users after you have confirmed that the URL, search base, Bind DN, password, and search filter are correct, you can enable a command-line setting to troubleshoot the user retrieval.

**Solution**

1. Enter the following command in the Code42 console CLI (https://support.code42.com/Administrator/6/Code42_console_reference/Code42_console_command-line_interface_reference):
   - `prop.set b42.ldap.ignore.partialResultException true save`
2. Restart the Code42 server with the following command:
   - `node.restart`

Reactivation of manually deactivated users

If you use the Code42 console to directly deactivate users from an LDAP-enabled organization, these users will be reactivated at the next LDAP sync (https://support.code42.com/Administrator/6/Monitoring_and_managing/How_LDAP_sync_works).

**Solutions**
You may choose one of the following solutions:

- For all users and devices in LDAP-enabled orgs, you must deactivate or remove the users from the LDAP server, rather than directly from the authority server.
- Create a new organization that is not linked to any LDAP servers, and move users to that organization before deactivating them. They will then not be reactivated by LDAP syncs.
- Change the user's username, or whatever attribute is mapped to the LDAP search filter in your authority server. The user will no longer be affected by LDAP syncs.

Move a large number of users

If an LDAP administrator moves large numbers of users at a time from an organization within your Code42 environment (or the LDAP container that corresponds to the organization based on the Org Name script), then your authority server may enter an unresponsive state.

Solution

Contact our Customer Champions for support (https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Get_support_for_CrashPlan_for_Small_Business_or_Code42_CrashPlan).

Referrals to remote LDAP servers

If your LDAP environment refers clients to remote LDAP servers (HTTP://www.zytrax.com/books/LDAP/cH2/index.html#Overview), then you may want to change the following property on your authority server using the Code42 console CLI. Otherwise, clients may not have access to the most current information for an organization or user:

1. Enter the following command in the Code42 console CLI (https://support.code42.com/Administrator/6/Code42_console_reference/Code42_console_command-line_interface_reference):
   - prop.set b42.ldap.referral follow save
2. Restart the Code42 server with the following command:
   - node.restart

Your authority server will now follow LDAP referrals.

User management script problems

The Active (https://support.code42.com/Administrator/6/Monitoring_and_managing/User_management_with_LDAP_integration#Active_script), Org Name (https://support.code42.com/Administrator/6/Monitoring_and_managing/User_management_with_LDAP_integration#Org_name_script), and Role (https://support.code42.com/Administrator/6/Monitoring_and_managing/User_management_with_LDAP_integration#Role_name_script) scripts provide powerful ways to manage users' status, organization membership, and roles. However, if the scripts use incorrect syntax or formatting, unintended results can...
occur during LDAP sync. Read the article User Management With LDAP Integration (https://support.code42.com/Administrator/6/Monitoring_and_managing/User_management_with_LDAP_integration), and verify that your scripts are performing as intended.

External resources

- Wikipedia:
  - Microsoft Active Directory (http://en.wikipedia.org/wiki/Active_Directory)
- Zytrax's open-source LDAP guide (http://www.zytrax.com/books/ldap/)
- Jxplorer (http://jxplorer.org/), software for browsing LDAP hierarchy

Related topics

- LDAP connection problem (https://support.code42.com/Administrator/6/Troubleshooting/Alerts/LDAP_connection_problem)
- How LDAP sync works (https://support.code42.com/Administrator/6/Monitoring_and_managing/How_LDAP_sync_works)
- Integrate your Code42 environment with complex LDAP directory structures (https://support.code42.com/Administrator/6/Monitoring_and_managing/Integrate_your_Code42_environment_with_complex_LDAP_directory_structures)
- Integrate with LDAP for user authentication (https://support.code42.com/Administrator/6/Configuring/Integrate_with_LDAP_for_user_authentication)
- User management with LDAP integration (https://support.code42.com/Administrator/6/Monitoring_and_managing/User_management_with_LDAP_integration)