# Secure LDAP Problems After an Upgrade to CUCM 10.5(2)SU2

## Contents



## Introduction

This document describes problems with secure Lightweight Directory Access Protocol (LDAP) after upgrading to Cisco Unified Communications Manager (CUCM) 10.5(2)SU2, or 9.1(2)SU3 and the steps that can be taken to resolve the issue.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on CUCM version 10.5(2)SU2.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Background Information

CUCM can be configured to use either IP address or Fully Qualified Domain Name (FQDN) for secure LDAP authentication. FQDN is preffered. The default behavior of CUCM is to use FQDN. If

the use of IP address is desired the **utils ldap config ipaddr** command can be run from the Command Line Interface (CLI) of the CUCM Publisher.

Prior to the fix for CSCun63825 which is introduced in 10.5(2)SU2 and 9.1(2)SU3, CUCM did not strictly enforce FQDN validation for Transport Layer Security (TLS) connections to LDAP. FQDN validation involves a comparison of the hostname configured in CUCM (**CUCM Admin > System > LDAP > LDAP Authentication)**, and the Common Name (CN) or Subject Alternative Name (SAN) field of the LDAP certificate presented by the LDAP server during the TLS connection from CUCM to the LDAP server. So, if LDAP Authentication is enabled (check **use SSL)** and the LDAP server/servers are defined by IP address, authentication will succeed even if the **utils ldap config ipaddr** command is not issued.

After a CUCM upgrade to 10.5(2)SU2, 9.1(2)SU3, or later versions, FQDN validation is enforced and any changes using **utils ldap config** are reverted to the default behavior, which is to use FQDN. The result of this change was the opening of CSCux83666. Also, the CLI command **utils ldap config status** is added to show if IP address or FQDN is being used.

**Scenario 1**

Before the upgrade LDAP Authentication is enabled, server/servers are defined by IP address, the **utils ldap config ipaddr** command is configured on the CLI of the CUCM Publisher.

After the upgrade LDAP Authentication fails, and the **utils ldap config status** command on the CLI of the CUCM Publisher shows that FQDN is used for authentication.

**Scenario 2**

Before the upgrade LDAP Authentication is enabled, server/servers are defined by IP address, the **utils ldap config ipaddr** command is not configured on the CLI of the CUCM Publisher.

After the upgrade LDAP Authentication fails, and the **utils ldap config status** command on the CLI of the CUCM Publisher shows that FQDN is used for authentication.

# Problem

Secure LDAP authentication fails if LDAP authentication is configured to use Secure Sockets Layer (SSL) on CUCM and the LDAP server/servers were configured using IP address prior to the upgrade.

In order to confirm the LDAP authentication settings navigate to the **CUCM Admin page > System > LDAP > LDAP Authentication** and verify that the LDAP servers are defined by IP address, not FQDN. If your LDAP server is defined by FQDN and the CUCM is configured to use FQDN (see command below for verification) it is unlikely that this is your issue.


In order to verify if CUCM (after an upgrade) is configured to use IP address or FQDN use

the **utils ldap config status** command from the CLI of the CUCM publisher.

```
admin:utils ldap config status utils ldap config fqdn configured
```

In order to verify that you are experiencing this problem you can check the CUCM DirSync logs for this error. This error indicates that the LDAP server is configured using an IP Address on the LDAP Authentication configuration page in CUCM and it does not match the CN field in the LDAP certificate.

```
2016-02-09 14:08:32,718 DEBUG [http-bio-443-exec-1] impl.AuthenticationLDAP -
URL contains IP Address
```

# Solution

Navigate to The **CUCM Admin > System > LDAP > LDAP Authentication** page and change the LDAP server configuration from the IP address of the LDAP server to the FQDN of the LDAP server. If you must use the IP Address of the LDAP server use this command from the CLI of the CUCM Publisher

```
admin:utils ldap config ipaddr Now configured to use IP address admin:
```

Other reasons that can can result in FQDN validation failure not related to this particular isuse :

1. The LDAP hostname configured in CUCM does not match the CN field in the LDAP certificate (hostname of the LDAP server).

In order to address this issue navigate to The **CUCM Admin > System > LDAP > LDAP Authentication** page and modify the **LDAP Server Information** to use the hostname/FQDN from the CN Field in the LDAP certificate. Also, verify that the name used is routable and can be reached from CUCM using **utils network ping** from the CLI of the CUCM publisher.

2. A DNS Load Balancer is deployed in the network and the LDAP server configured in CUCM uses the DNS Load Balancer. For example, the configuration points to adaccess.example.com, which then load balances between several LDAP servers based on geography, or other factors. The LDAP server that answers the request can have a FQDN other than adaccess.example.com. This results in a validation failure since there is a hostname mismatch.

```
2016-02-06 09:19:51,702 ERROR [http-bio-443-exec-23] impl.AuthenticationLDAP -
verifyHostName:Exception.javax.net .ssl.SSLPeerUnverifiedException: hostname of the server
'adlab.testing.cisco.local' does not match the hostname in the server's certificate.
```

In order to address this issue change the LDAP loadbalancer scheme such that the TLS connection terminates at the loadbalancer, rather than the LDAP server itself. If this is not possible the only option is to disable FQDN validation and instead validate using IP address.