

Configure Secure LDAP on UCS C-Series Servers

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configuration on the UCS C Series Server Side](#)

[Verification](#)

Introduction

This document describes how to configure SecureLDAP on C Series Servers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic understanding of Cisco UCS and CIMC.

Components Used

- Cisco UCS C Series Server in standalone mode.

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, ensure that you understand the potential impact of any command.

Background Information

The example in this guide demonstrates secure LDAP configuration on UCS C Series servers:

- Set up a DNS Server, allowing the use of domain names for the LDAP server instead of an IP address on the UCS Server. Ensure that the appropriate A records have been configured to point to both the LDAP server and the UCS C Series Server IP addresses.
- Configure Windows Certificate Services on the LDAP Server, enabling Certificate Generation for secure LDAP communication. The generated Certificates (Root and Intermediate) are uploaded to the UCS C Series server.

Configuration on the UCS C Series Server Side

To configure UCS C Series Server to interact with a preconfigured DNS server, access the CIMC Interface of the UCS server, then click on the **Navigation Icon** located in the top left corner.



Server Properties

Product Name:

Serial Number:

PID:

UUID:

BIOS Version:

Description:

Asset Tag:

Unknown

Navigate to **Admin** and choose **Networking**.

Chassis



Compute

Networking



Storage



Admin



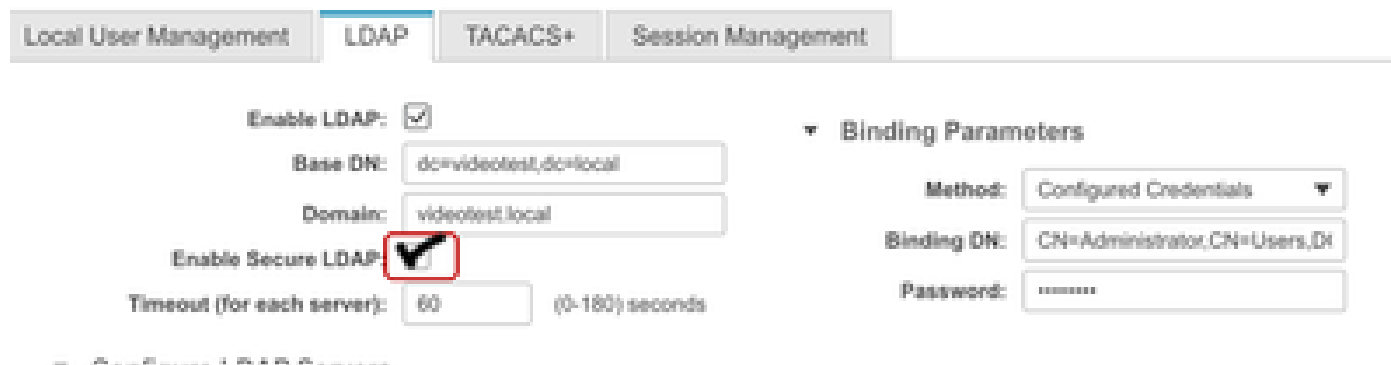
User Management

Networking

Communication Services

section, configure the BaseDN, Domain, Timeout and Bind Parameters in alignment with standard LDAP configuration practices.

Next, check the **Enable Secure LDAP** check box.



The screenshot displays a configuration interface with four tabs: 'Local User Management', 'LDAP' (selected), 'TACACS+', and 'Session Management'. Under the 'LDAP' tab, the 'Enable LDAP' checkbox is checked. Below it, the 'Base DN' is set to 'dc=videotest,dc=local' and the 'Domain' is 'videotest.local'. The 'Enable Secure LDAP' checkbox is checked and highlighted with a red square. The 'Timeout (for each server)' is set to '60' seconds. To the right, the 'Binding Parameters' section shows the 'Method' as 'Configured Credentials', the 'Binding DN' as 'CN=Administrator,CN=Users,DC=videotest,DC=local', and the 'Password' field is masked with dots.

In the pop-up window, select the **Paste Certificate Content** option.

For this demonstration, a Self-Signed Certificate is used, generated from the Windows Server instance running active directory and saved in a text file. This Self-Signed Certificate has also been concatenated with the Root Certificate from the same server to form a Certificate Chain.



Note: Note that the entire contents of the Base64 encoded X.509 (CER) file starting from the -----BEGIN CERTIFICATE----- to the -----END CERTIFICATE----- needs to be copied, then immediately on the next line, must be the next certificate starting from the -----BEGIN CERTIFICATE----- to the -----END CERTIFICATE----- in cases where multiple certificates are used.

Paste the copied content in the **Paste Certificate Content** field and click on **Upload Certificate**.

Upload LDAP CA Certificate

To enable Secure LDAP, Certificate of Signing Authority of the LDAP server has to be uploaded to IMC. Please upload the CA Certificate.

☐ Upload from remote location
☐ Upload through browser Client
☒ Paste certificate content

Paste certificate content:

```

caBhYccZ9b0DTHo8
siQr88arNZ6Oj0E17zYkHilky0oHgtdrjn1wSX86CxKU7wmp
5cig7mdal8PUzE
VGp0HiiHowpsRAnpzZnyMMe9o17ttzwbW9AEFkhGyC9ua
GNzpjS
-----END CERTIFICATE-----

```

Upload Certificate

Close

All other settings in Secure LDAP remain the same as the standard LDAP configuration for C Series Servers, therefore, click on **Save Changes** on the overall LDAP configuration page.

User Management / LDAP

Refresh

Host Power

Launch vMM

Ping

CMC Refresh

Locate USB

Local User Management

LDAP

SAC/CS+

Session Management

LDAP Settings

Enable LDAP

Base DN: dc=redhat,dc=local

Domain: redhat.local

Enable Secure LDAP

Timeout (for each server): 60 (0-180) seconds

Binding Parameters

Method: Configured Credentials

Binding DN: CN=Administrator,CN=Users,DC=

Password: *****

Search Parameters

LDAP CA Certificate Status

Upload Status: COMPLETED

Export Status: NotSet

Configure LDAP Servers

1. 10.10.10.10

2. 10.10.10.10

3. 10.10.10.10

4. 10.10.10.10

5. 10.10.10.10

6. 10.10.10.10

Use (Add) to Configure LDAP Servers

Source: External

Group Authorization

LDAP Group Authorization

Configure

Delete

Index	Group Name	Group Domain	Role
<input type="checkbox"/> 1	IT	redhat.local	read-only
<input type="checkbox"/> 2			
<input type="checkbox"/> 3			
<input type="checkbox"/> 4			
<input type="checkbox"/> 5			

Save Changes

Reset Values

Now secure LDAP has been successfully configured on the UCS C Series Server.

Verification

To verify this, attempt to log into the UCS C Series Server using one of the configured user accounts in Active Directory. Select your domain and proceed to log in.

Cisco Integrated Management Controller

testuser1

password

Language | English

Log In

Test User1 log in is successful over Secure LDAP



testuser1 (LDAP)@



[Refresh](#)



Cisco Integrated Management Controller (Cisco IMC) Information