

# Cisco C880 LDAP-Konfiguration mit Microsoft Active Directory

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[LDAP-Implementierung](#)

[Konfigurieren](#)

[Sonderkonten erstellen](#)

[Verzeichnisdienst](#)

[Benutzergruppe erstellen](#)

[Active Directory](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einführung

Dieses Dokument beschreibt ein Konfigurationsbeispiel, um das Lightweight Directory Access Protocol (LDAP) für den C880 unter Verwendung von Microsoft Active Directory (AD) zu verwenden. Die LDAP-Implementierung des C880 ist so eindeutig, dass der Benutzer im Common Name (CN) = Benutzer sein muss. Es gibt auch einige spezifische Konfigurationsanforderungen, damit diese funktionieren.

## Voraussetzungen

### Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Server: C880-M4
- Firmware: 1.0.5
- Microsoft Active Directory-Server

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

# LDAP-Implementierung

Wenn BenutzerX sich bei MMB anmelden möchte:

Schritt 1: MMB-Firmware fordert AD-Server auf, userX unter CN=Users (hartcodiert) zu durchsuchen.

Schritt 2: Wenn die MMB-Firmware eine Antwort erhält, dass userX im CN=Users vom AD-Server gefunden wird, fordert die MMB-Firmware den AD-Server auf, in der Struktur der Organisationseinheit (OUs) des Verzeichnisinformationsbaums (Directory Information Tree, DIT) von dem Speicherort zu suchen, der vom **Groups-Verzeichnis als Sub-Tree des Basis-DN-Felds** der MMB-Webbenutzeroberfläche angegeben wird.

Schritt 3: Wenn die MMB-Firmware eine Antwort erhält, dass userX in der Struktur der OU vom AD-Server gefunden wird (der Gruppenname, zu dem der BenutzerX gehört, wird auch vom AD-Server gesendet), prüft die MMB-Firmware, ob der empfangene Gruppenname mit dem Gruppennamen übereinstimmt, der auf der Seite **LDAP-Benutzergruppe** in der MMB-Webbenutzeroberfläche registriert ist.

Schritt 4: Wenn der Gruppenname eine Übereinstimmung ist, kann sich UserX anmelden.

Quelle: Fujitsu

## Konfigurieren

### Sonderkonten erstellen

Schritt 1: Secure Shell (SSH) an die IP-Adresse des Servermanagements anhängen und sich als Administrator anmelden.

Schritt 2: Spezielle Admin- und CE-Konten erstellen:

```
Administrator> set special_account spadmin admin
Are you sure you want to add spadmin? [Y/N]: y
Password:xxxxxxxxxx
Confirm Password:xxxxxxxxxx
Administrator>
```

```
Administrator> set special_account spce ce
Are you sure you want to add spce? [Y/N]: y
Password:zzzzzzzzzz
Confirm Password:zzzzzzzzzz
Administrator>
```

### Verzeichnisdienst

Schritt 1: Navigieren Sie zu **Benutzerverwaltung > LDAP-Konfiguration > Verzeichnisdienstkonfiguration**.

Schritt 2: Klicken Sie auf **Aktiviert** für LDAP.

Schritt 3: Wählen Sie aus, ob **LDAP SSL aktiviert/deaktiviert** werden soll.

Schritt 4: Wählen Sie **Active Directory** aus dem Dropdown-Menü für **Verzeichnisservertyp** aus.

Schritt 5: Geben Sie die Details für die Konfiguration **des primären LDAP-Servers** und des **Backup-LDAP-Servers** ein.

Schritt 6: Geben Sie den **Domännennamen** ein.

Schritt 7: Geben Sie das **Groups-Verzeichnis als Sub-Tree von der Basis-DN** ein. Hier muss sich die in der Benutzergruppe erstellte AD-Gruppe befinden.

Schritt 8: Geben Sie den **LDAP-Auth-Benutzernamen** und das **Kennwort** ein. Dieser Benutzer muss in CN=Users, DC=domain, DC=com vorhanden sein.

Schritt 9: Klicken Sie auf **Übernehmen**.

Schritt 10: Klicken Sie auf **LDAP testen**, wie in den Bildern gezeigt.

Global Directory Service Configuration		
LDAP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
LDAP SSL	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Directory Server Type	Active Directory	
Primary LDAP Server	LDAP Server	14.2.26.2
	LDAP Port	389
	LDAP SSL Port	636
Backup LDAP Server	LDAP Server	14.2.26.3
	LDAP Port	389
	LDAP SSL Port	636
Domain Name	vxi.local	
Base DN	DC=vxi,DC=local	
Groups directory as sub-tree from base DN	OU=VXI-TAC-Team,OU=VXI-IT,OU=VXI	
User Search Context	CN=Users,DC=vxi,DC=local	
LDAP Group Scheme	group	
LDAP Member Scheme	member	

#### Directory Service Access Configuration

LDAP Auth UserName	c880bind
LDAP Auth Password	
Confirm Password	
Principal User DN	
Append Base DN to Principal User DN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Bind DN	CN=c880bind,CN=Users,DC=vxi,DC=local
Enhanced User Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
User Login Search Filter	(&(objectclass=person)(sAMAccountName=%s))

Apply Cancel Test LDAP

## Benutzergruppe erstellen

Schritt 1: Navigieren Sie zu **Benutzerverwaltung > LDAP-Konfiguration > LDAP-Benutzergruppenliste**.

Schritt 2: Klicken Sie auf die Schaltfläche **Gruppe hinzufügen**, um eine neue Gruppe hinzuzufügen.

Schritt 3: Geben Sie den **LDAP-Benutzernamen** und die **Berechtigung** ein (z. B. Admin).

Schritt 4: Klicken Sie auf **Übernehmen** wie in den Bildern gezeigt.

System [User Administration](#) [Network Configuration](#) [Maintenance](#) [Logout](#)  
 >User Administration >LDAP Configuration >LDAP User Group List

**LDAP User Group List** [Help](#)

Click the Add Group button to add a new group.  
 Select a group, then click the Edit/Remove Group button to edit or remove the group.

LDAP User Group Name	Privilege	Status
<input type="radio"/> MMBAdmin	Admin	Enabled

System [User Administration](#) [Network Configuration](#) [Maintenance](#) [Logout](#)  
 >User Administration >LDAP Configuration >Add LDAP User Group

**Add LDAP User Group** [Help](#)

Click the Apply Button to apply all changes.

LDAP User Group Name	MMBAdmin
Privilege	<input checked="" type="radio"/> Admin <input type="radio"/> Operator <input type="radio"/> User <input type="radio"/> CE
Status	<input type="radio"/> Enabled <input type="radio"/> Disabled

System [User Administration](#) [Network Configuration](#) [Maintenance](#) [Logout](#)  
 >User Administration >LDAP Configuration >LDAP User Group List

**LDAP User Group List** [Help](#)

Click the Add Group button to add a new group.  
 Select a group, then click the Edit/Remove Group button to edit or remove the group.

LDAP User Group Name	Privilege	Status
<input type="radio"/> MMBAdmin	Admin	Enabled

## Active Directory

Schritt 1: Erstellen Sie **c880bind** User.

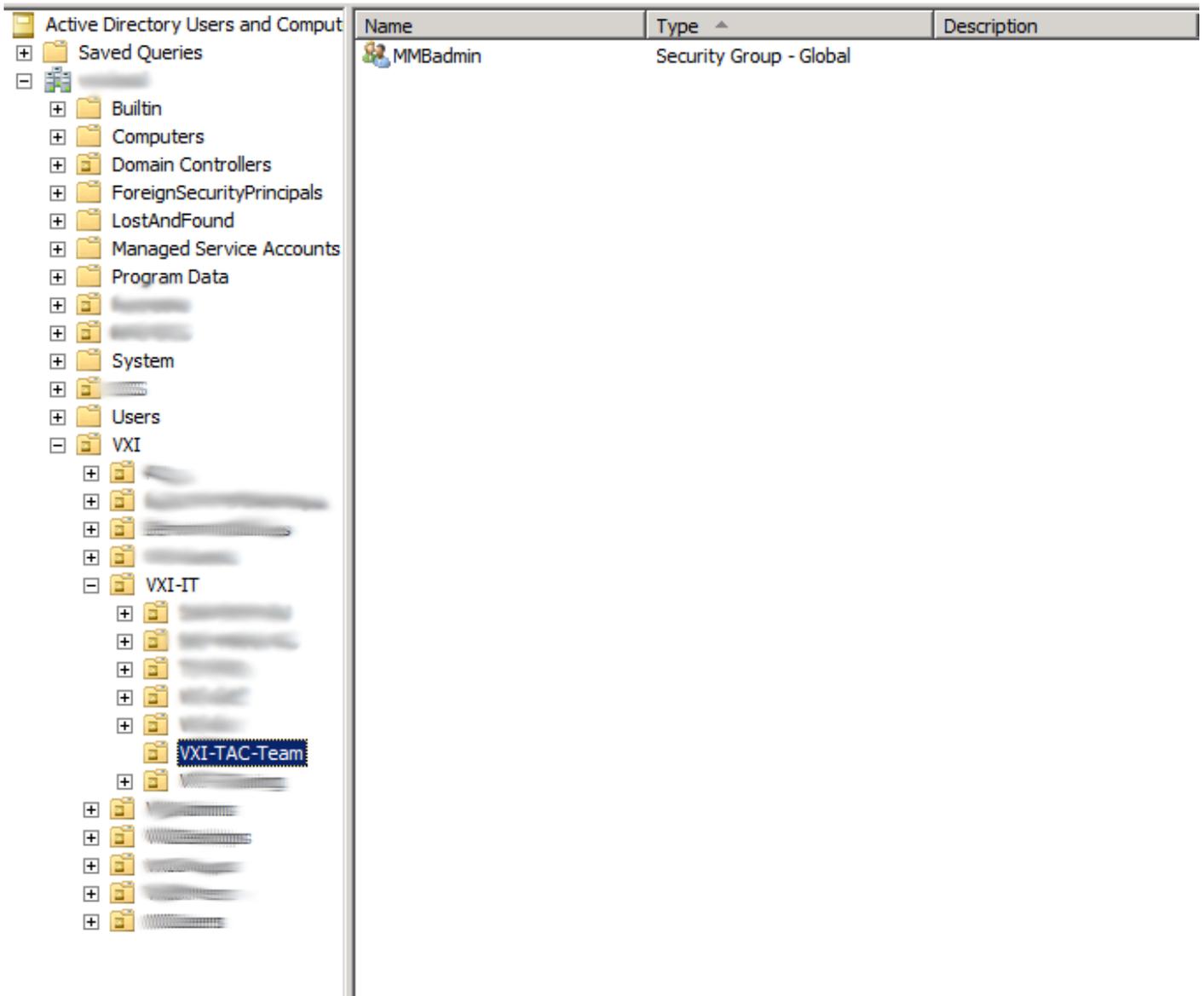
Schritt 2: Erstellen Sie **ldaptest** User wie im Bild gezeigt.

CN=Benutzer, DC=VXI, DC=Lokal:

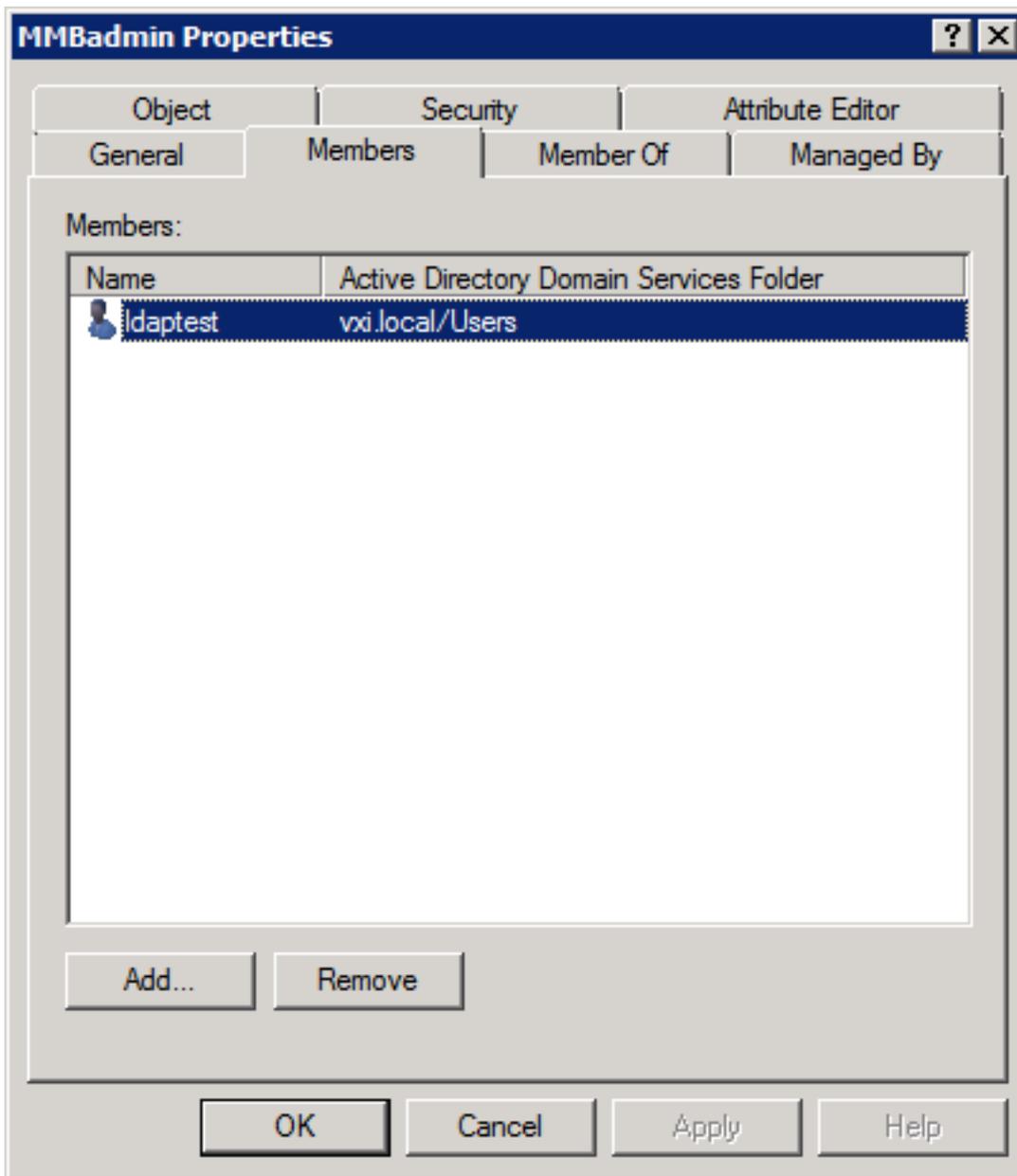
Name	Type	Description
 c880bind	User	
 ldaptest	User	

Schritt 3: Erstellen Sie **MMBAdmin** Security Group in OU, wie im Bild gezeigt.

MMBAdmin group in OU=**VXI-TAC-Team**, OU=**VXI-IT**, OU=**VXI**:



Schritt 4: Fügen Sie **ldaptest** zu MMBAdmin hinzu, wie im Bild gezeigt.



## Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

- **Test-LDAP** muss funktionieren
- Sie müssen sich mit dem **ldaptest**-Konto anmelden können.

## Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

- Überprüfen der Server- und AD-Konfiguration, die der LDAP-Implementierung von Fujitsu entspricht
- Erfassen einer Paketerfassung vom AD-Server

## Zugehörige Informationen

- [PRIMEQUEST Handbücher der Serie 2000](#), die aus Installationshandbuch und Tool-Referenz bestehen
- [Technischer Support und Dokumentation - Cisco Systems](#)