# ACS 5.X: Konfigurationsbeispiel für sicheren LDAP-Server

## Inhalt



## Einführung

Lightweight Directory Access Protocol (LDAP) ist ein Netzwerkprotokoll zum Abfragen und Ändern von Verzeichnisdiensten, die auf TCP/IP und UDP ausgeführt werden. LDAP ist ein einfacher Mechanismus für den Zugriff auf einen x.500-basierten Verzeichnisserver. RFC 2251 definiert LDAP.

ACS 5.x (Access Control Server) kann mithilfe des LDAP-Protokolls in eine externe LDAP-Datenbank integriert werden, die auch als Identitätsspeicher bezeichnet wird. Es gibt zwei Methoden, um eine Verbindung zum LDAP-Server herzustellen: Klartext (einfach) und SSL (verschlüsselt) Verbindung. ACS 5.x kann für die Verbindung mit dem LDAP-Server mit beiden Methoden konfiguriert werden. In diesem Dokument wird ACS 5.x für die Verbindung mit einem LDAP-Server über eine verschlüsselte Verbindung konfiguriert.

## Voraussetzungen

### Anforderungen

In diesem Dokument wird davon ausgegangen, dass ACS 5.x über eine IP-Verbindung zum LDAP-Server verfügt und der Port TCP 636 offen ist.

Der Microsoft® Active Directory-LDAP-Server muss so konfiguriert werden, dass er sichere LDAP-Verbindungen am Port TCP 636 akzeptiert. In diesem Dokument wird davon ausgegangen, dass Sie das Stammzertifikat der Zertifizierungsstelle (CA) besitzen, die das Serverzertifikat an den Microsoft LDAP-Server ausgegeben hat. Weitere Informationen zum Konfigurieren des LDAP-

Servers finden Sie unter Aktivieren von LDAP über SSL mit einer Zertifizierungsstelle eines Drittanbieters.

## Verwendete Komponenten

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

- Cisco Secure ACS 5.x
- Microsoft Active Directory LDAP-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.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

# Hintergrundinformationen

### Verzeichnisdienst

Der Verzeichnisdienst ist eine Softwareanwendung oder eine Gruppe von Anwendungen zum Speichern und Organisieren von Informationen über die Benutzer und Netzwerkressourcen eines Computernetzwerks. Sie können den Verzeichnisdienst verwenden, um den Benutzerzugriff auf diese Ressourcen zu verwalten.

Der LDAP-Verzeichnisdienst basiert auf einem Client-Server-Modell. Ein Client startet eine LDAP-Sitzung, indem er eine Verbindung zu einem LDAP-Server herstellt und betriebliche Anforderungen an den Server sendet. Der Server sendet dann seine Antworten. Ein oder mehrere LDAP-Server enthalten Daten aus der LDAP-Verzeichnisstruktur oder der LDAP-Backend-Datenbank.

Der Verzeichnisdienst verwaltet das Verzeichnis, d. h. die Datenbank, in der die Informationen gespeichert sind. Verzeichnisdienste verwenden ein verteiltes Modell zum Speichern von Informationen, und diese Informationen werden in der Regel zwischen Verzeichnisservern repliziert.

Ein LDAP-Verzeichnis ist in einer einfachen Baumhierarchie organisiert und kann auf viele Server verteilt werden. Jeder Server kann über eine replizierte Version des Gesamtverzeichnisses verfügen, die regelmäßig synchronisiert wird.

Ein Eintrag in der Struktur enthält eine Reihe von Attributen, bei denen jedes Attribut einen Namen (einen Attributtyp oder eine Attributbeschreibung) und einen oder mehrere Werte hat. Die Attribute werden in einem Schema definiert.

Jeder Eintrag hat eine eindeutige Kennung: Distinguished Name (DN): Dieser Name enthält den RDN (Relative Distinguished Name), der aus Attributen im Eintrag erstellt wurde, gefolgt von der DN des übergeordneten Eintrags. Sie können sich den DN als vollständigen Dateinamen und den

RDN als relativen Dateinamen in einem Ordner vorstellen.

### Authentifizierung über LDAP

ACS 5.x kann einen Principal für einen LDAP-Identitätsspeicher authentifizieren, indem er eine Bindungsoperation auf dem Verzeichnisserver durchführt, um den Principal zu finden und zu authentifizieren. Wenn die Authentifizierung erfolgreich ist, kann der ACS Gruppen und Attribute abrufen, die dem Principal angehören. Die abzurufenden Attribute können in der ACS-Webschnittstelle (LDAP-Seiten) konfiguriert werden. Diese Gruppen und Attribute können vom ACS verwendet werden, um den Principal zu autorisieren.

Um einen Benutzer zu authentifizieren oder den LDAP-Identitätsspeicher abzufragen, stellt der ACS eine Verbindung zum LDAP-Server her und verwaltet einen Verbindungspool.

### LDAP-Verbindungsmanagement

ACS 5.x unterstützt mehrere gleichzeitige LDAP-Verbindungen. Verbindungen werden bei Bedarf zum Zeitpunkt der ersten LDAP-Authentifizierung geöffnet. Die maximale Anzahl von Verbindungen wird für jeden LDAP-Server konfiguriert. Das Öffnen von Verbindungen im Voraus verkürzt die Authentifizierungszeit.

Sie können die maximale Anzahl von Verbindungen festlegen, die für gleichzeitige Bindungsverbindungen verwendet werden sollen. Die Anzahl der geöffneten Verbindungen kann für jeden LDAP-Server (primär oder sekundär) unterschiedlich sein und wird anhand der maximalen Anzahl der für jeden Server konfigurierten Administrationsverbindungen bestimmt.

ACS behält eine Liste offener LDAP-Verbindungen (einschließlich der binden Informationen) für jeden LDAP-Server bei, der in ACS konfiguriert ist. Während des Authentifizierungsprozesses versucht der Verbindungs-Manager, eine offene Verbindung aus dem Pool zu finden.

Wenn keine offene Verbindung vorhanden ist, wird eine neue geöffnet. Wenn der LDAP-Server die Verbindung geschlossen hat, meldet der Verbindungs-Manager während des ersten Anrufs einen Fehler, um das Verzeichnis zu durchsuchen, und versucht, die Verbindung zu erneuern.

Wenn der Authentifizierungsprozess abgeschlossen ist, gibt der Connection Manager die Verbindung zum Connection Manager frei. Weitere Informationen finden Sie im ACS 5.X-Benutzerhandbuch.

# Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

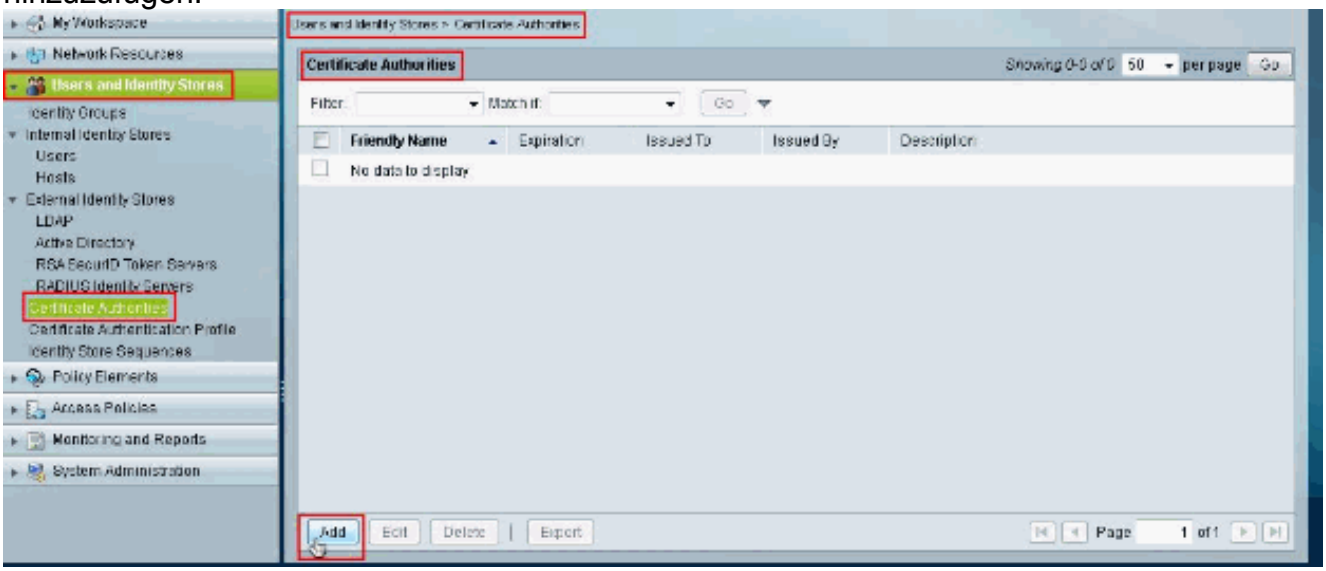
## Installation des Root CA-Zertifikats auf ACS 5.x

Führen Sie die folgenden Schritte aus, um ein Zertifikat der Stammzertifizierungsstelle auf Cisco Secure ACS 5.x zu installieren:

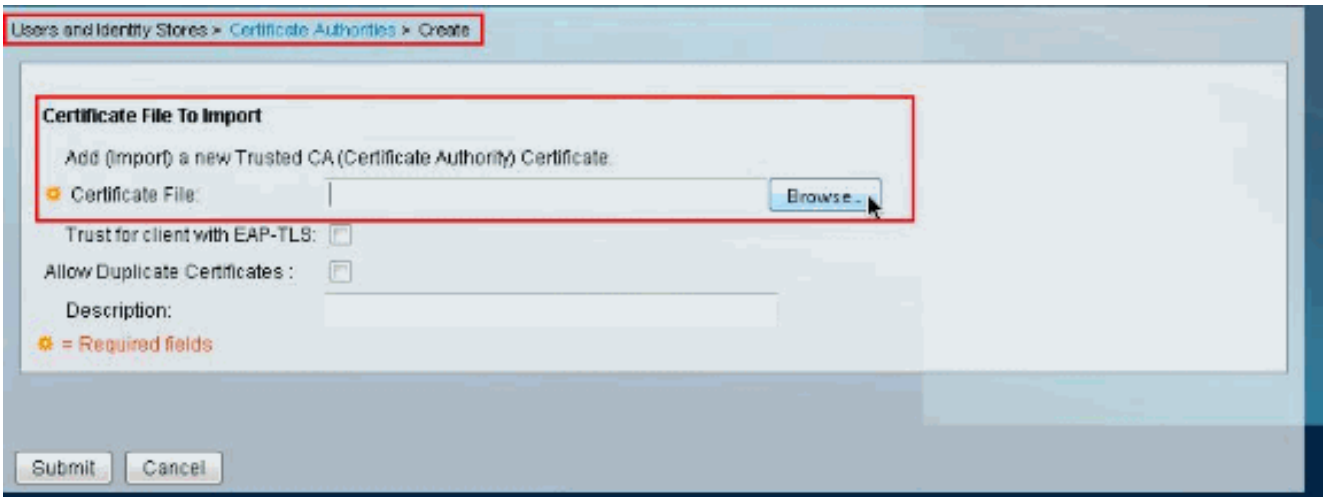
**Hinweis:** Stellen Sie sicher, dass der LDAP-Server vorkonfiguriert ist, um verschlüsselte Verbindungen auf Port TCP 636 zu akzeptieren. Weitere Informationen zum Konfigurieren des Microsoft LDAP-Servers finden Sie unter Aktivieren von LDAP über SSL mit einer

Zertifizierungsstelle eines Drittanbieters.

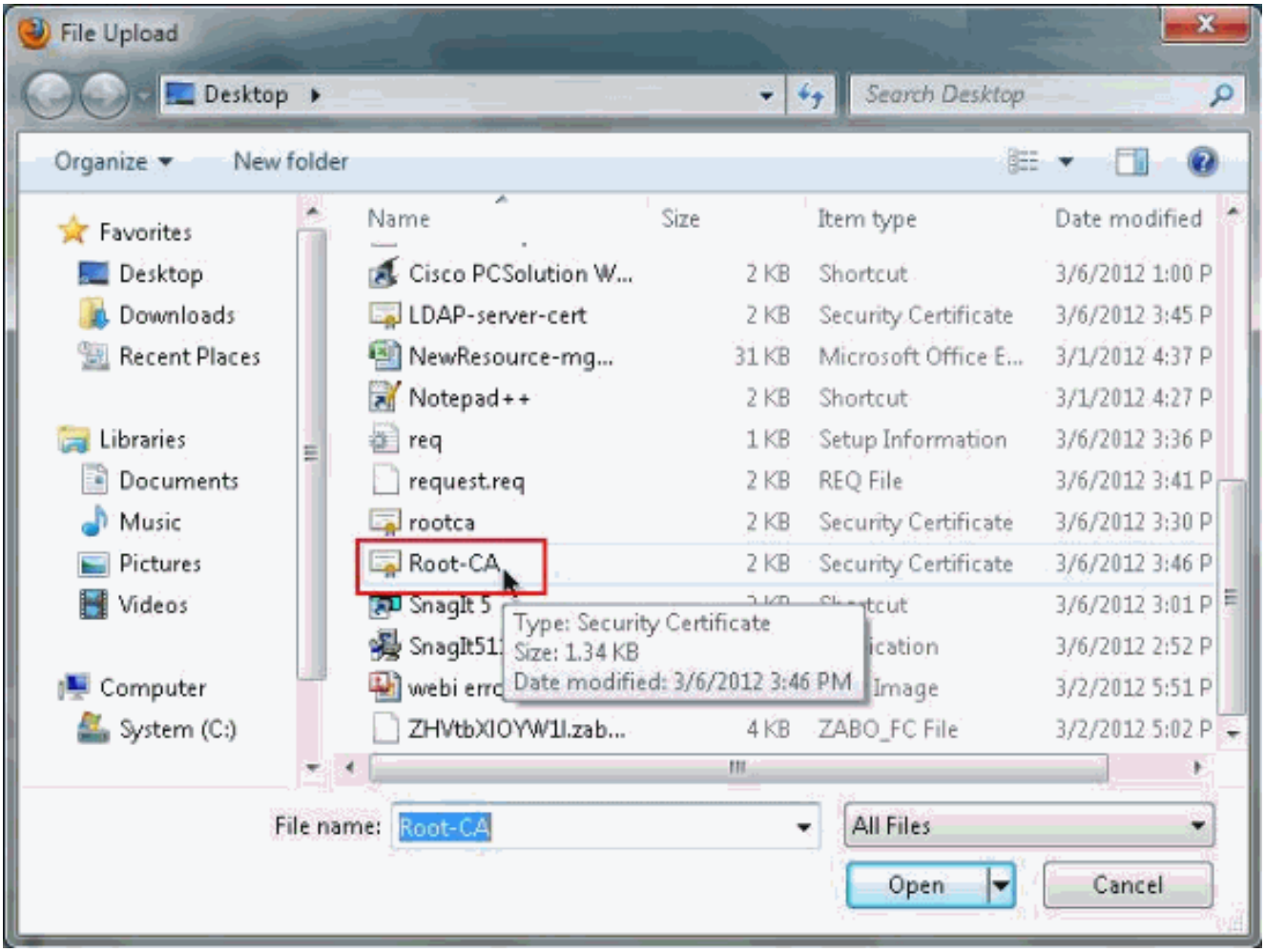
1. Wählen Sie **Benutzer und Identity Stores > Certificate Authorities aus**, und klicken Sie dann auf **Add**, um das Stammzertifikat der CA, die das Serverzertifikat ausgestellt hat, zum Microsoft LDAP-Server hinzuzufügen.



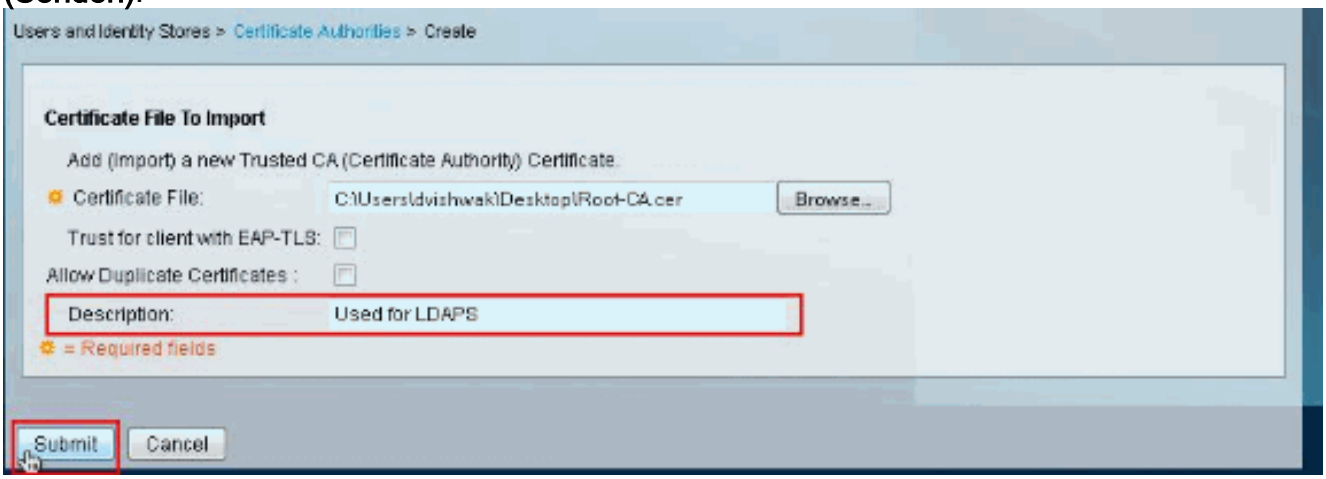

2. Klicken Sie im Abschnitt **Zertifikatsdatei zum Importieren** auf **Durchsuchen** neben **Zertifikatsdatei**, um nach der Zertifikatsdatei zu suchen.



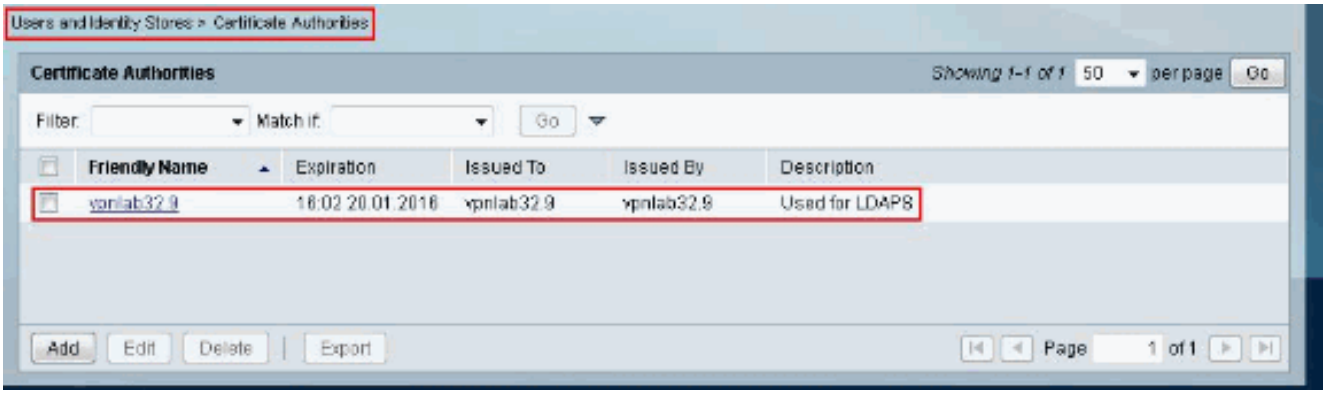

3. Wählen Sie die erforderliche **Zertifikatsdatei** (das Stammzertifikat der CA, die das Serverzertifikat an den Microsoft LDAP-Server ausgegeben hat), und klicken Sie auf **Öffnen**.




4. Geben Sie eine **Beschreibung** im Feld neben Description (Beschreibung) ein, und klicken Sie auf **Submit (Senden)**.



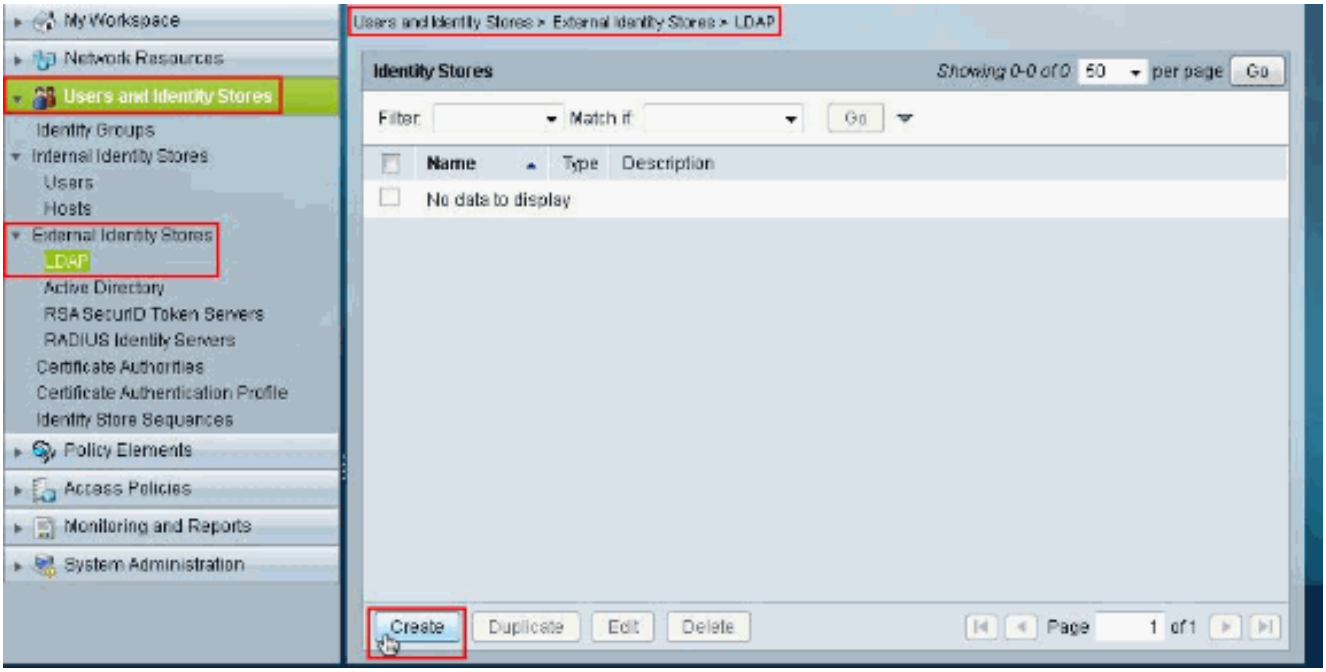

Dieses Bild zeigt, dass das Stammzertifikat ordnungsgemäß installiert wurde:



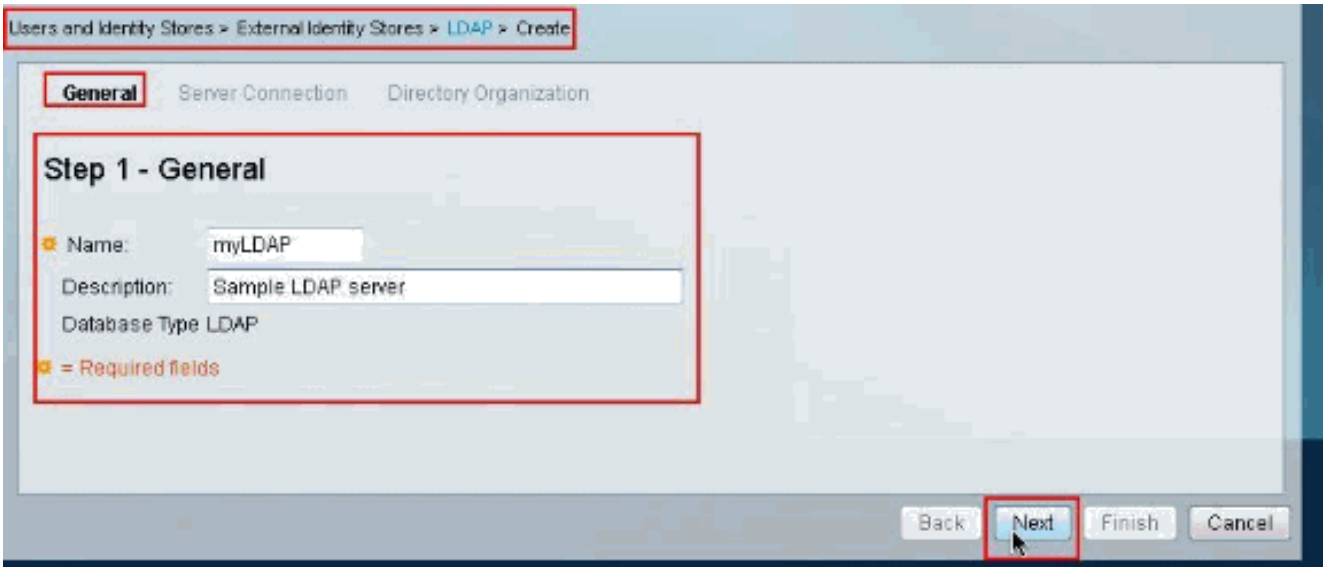

## Konfigurieren von ACS 5.X für sichere LDAP

Gehen Sie wie folgt vor, um ACS 5.x für sicheres LDAP zu konfigurieren:

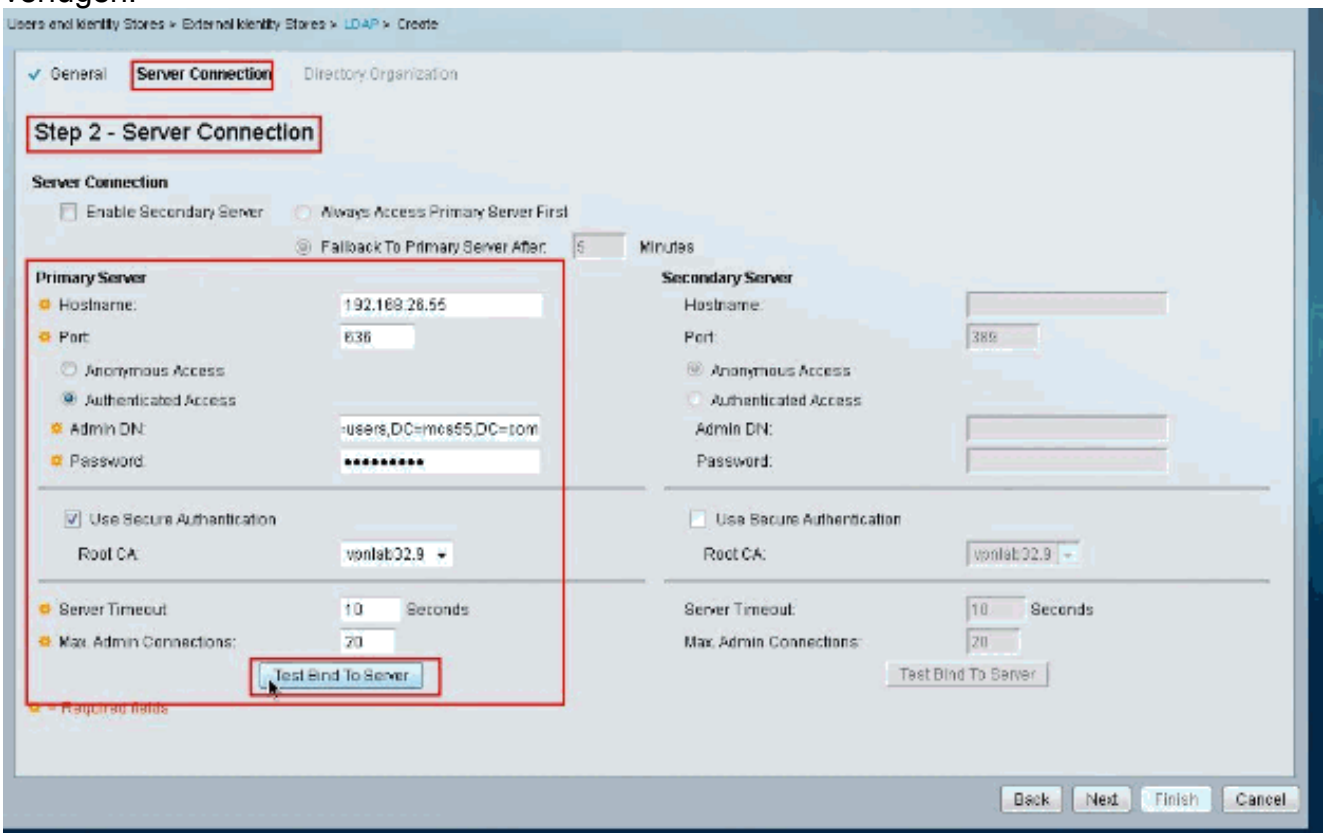
1. Wählen Sie **Benutzer und Identitätsdaten > Externe Identitätsdaten > LDAP aus,** und klicken Sie auf **Erstellen**, um eine neue LDAP-Verbindung zu erstellen.



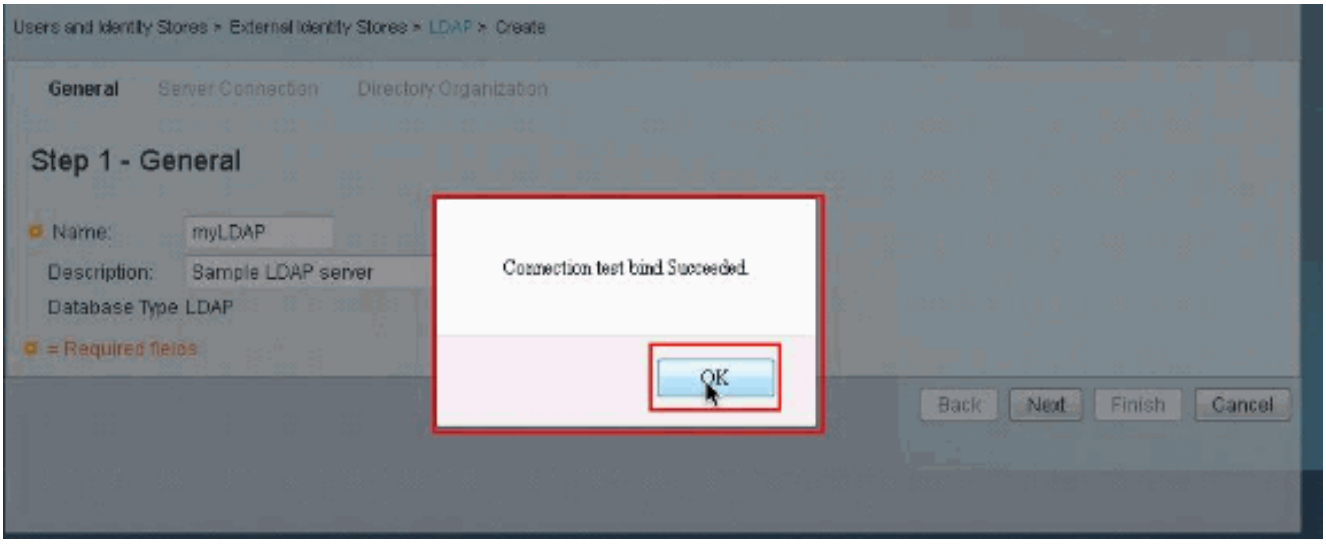

2. Geben Sie auf der **Registerkarte Allgemein** den **Namen** und die **Beschreibung** (optional) für das neue LDAP an, und klicken Sie dann auf **Weiter**.



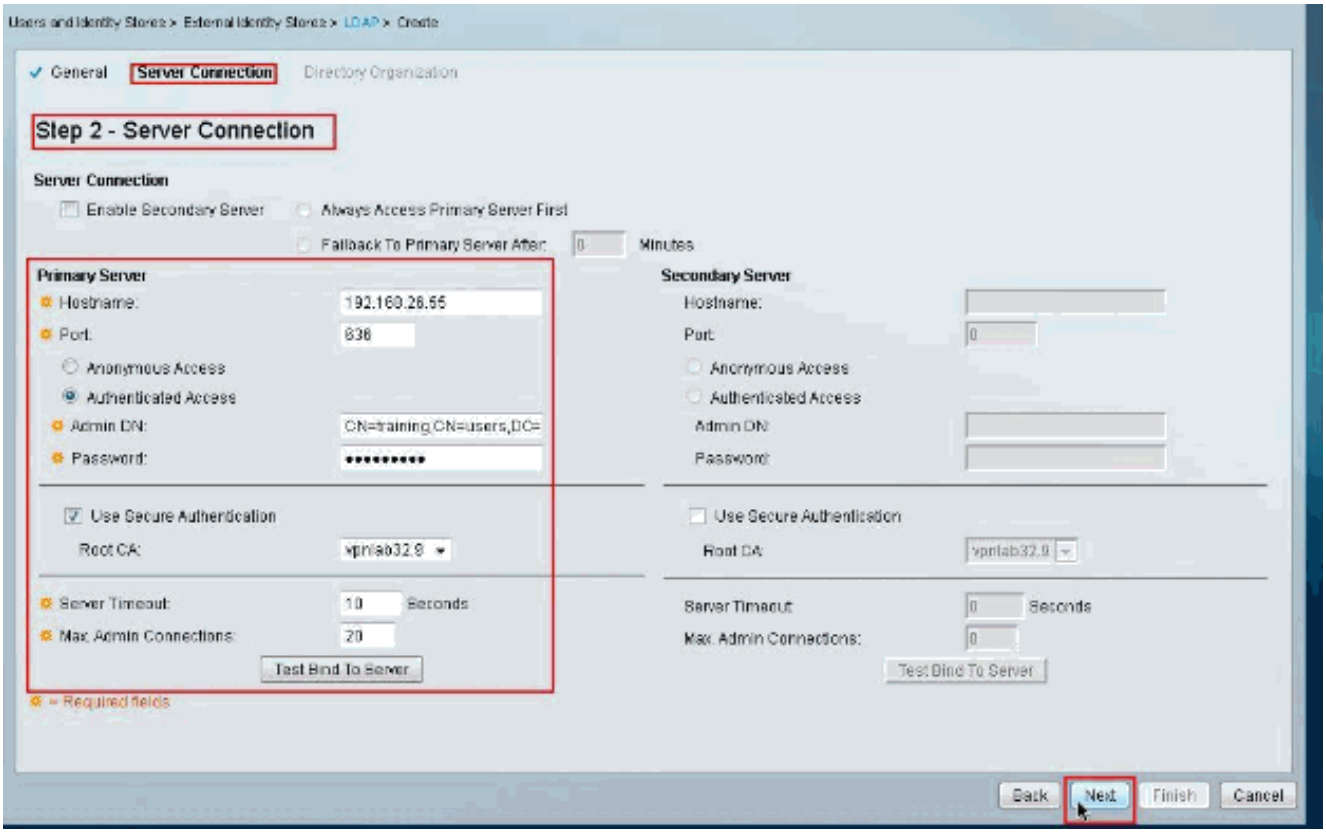

3. Geben Sie auf der Registerkarte **Server Connection** im Abschnitt **Primary Server (Primärer Server)** den **Hostnamen, den Port, die Admin-DN und das Kennwort ein**. Stellen Sie sicher, dass das Kontrollkästchen neben **Sichere Authentifizierung verwenden** aktiviert ist, und wählen Sie das kürzlich installierte **Root CA-Zertifikat aus**. Klicken Sie auf **Testbindung an Server**.**Hinweis: Die** IANA-zugewiesene Portnummer für sicheres LDAP ist TCP 636. Bestätigen Sie jedoch die Portnummer, die Ihr LDAP-Server verwendet, vom LDAP-Administrator.**Hinweis:** Die Admin-DN und das Kennwort sollten Ihnen vom LDAP-Administrator bereitgestellt werden. Der Admin-DN muss über alle Berechtigungen für alle OUs auf dem LDAP-Server
verfügen.



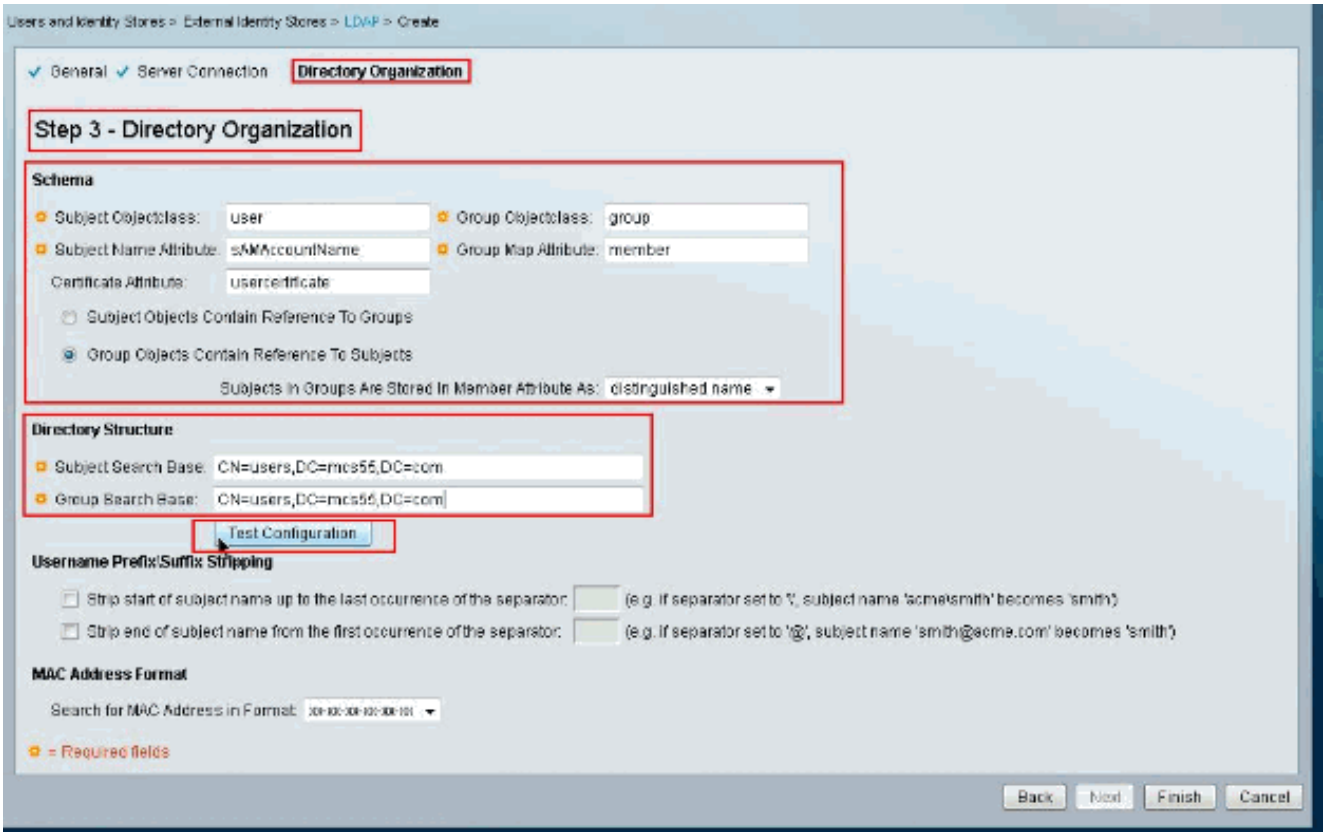

Das nächste Bild zeigt, dass das **Verbindungstestbind zum Server** erfolgreich war.**Hinweis:** Wenn die Testbindung nicht erfolgreich ist, überprüfen Sie den **Hostnamen, die Portnummer, die Admin-DN, das Kennwort** und die **Root-CA** von Ihrem LDAP-Administrator.



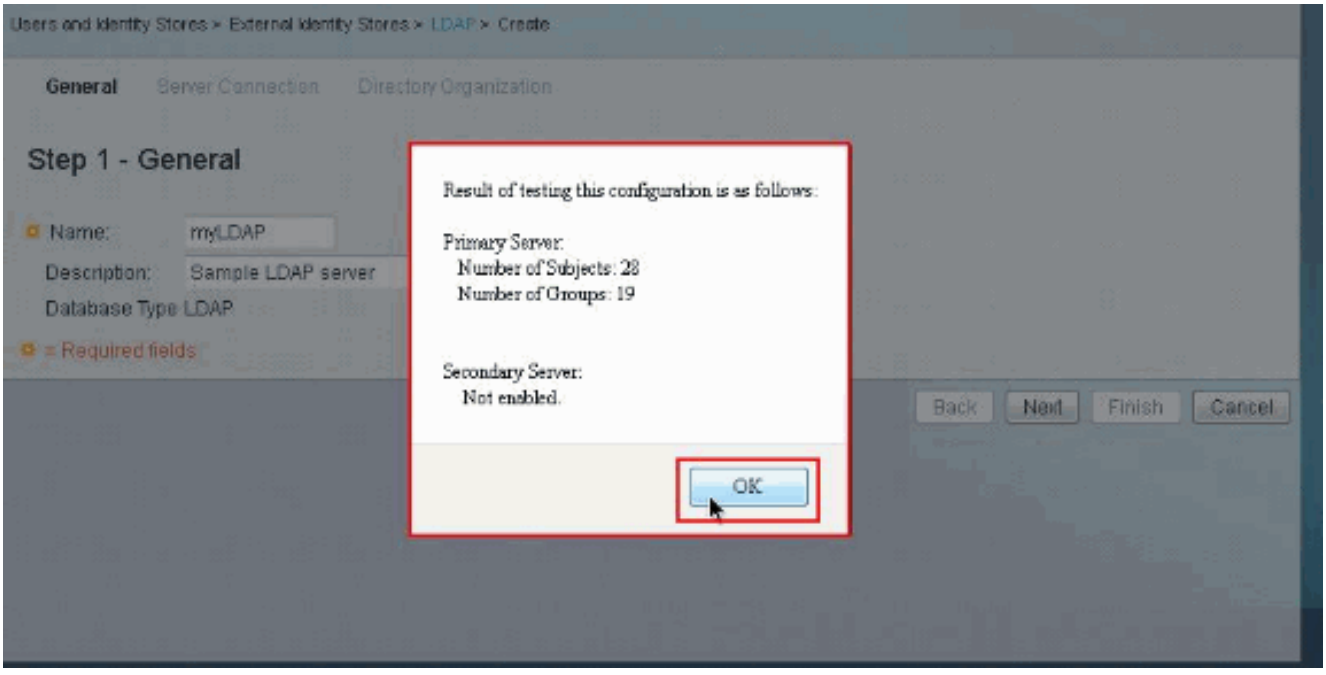

4. Klicken Sie auf **Weiter**.



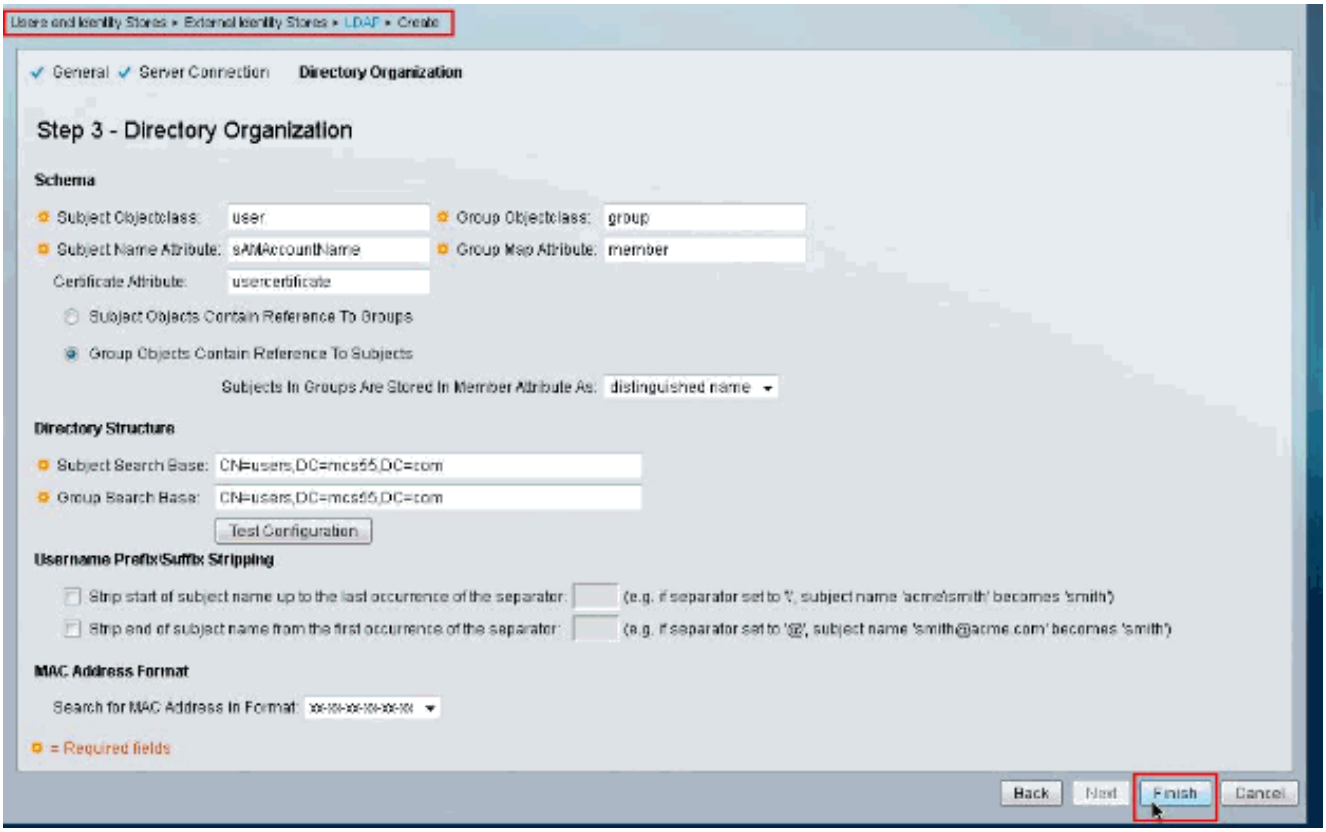

5. Geben Sie auf der Registerkarte **Verzeichnisorganisation** im Abschnitt **Schema** die erforderlichen Details an. Geben Sie entsprechend die erforderlichen Informationen im Abschnitt **Verzeichnisstruktur** an, wie vom LDAP-Administrator bereitgestellt. Klicken Sie auf **Testkonfiguration**.



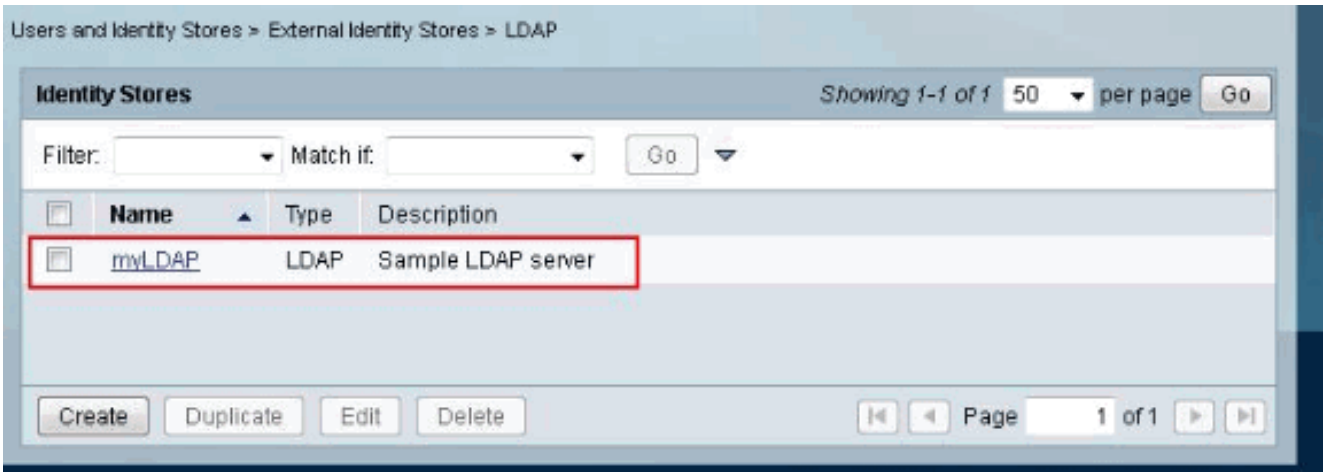

Das nächste Bild zeigt, dass der **Konfigurationstest** erfolgreich durchgeführt wurde.**Hinweis:** Wenn der Konfigurationstest nicht erfolgreich ist, überprüfen Sie die Parameter im **Schema** und in der **Verzeichnisstruktur** erneut von Ihrem LDAP-Administrator.




6. Klicken Sie auf **Fertig stellen**.



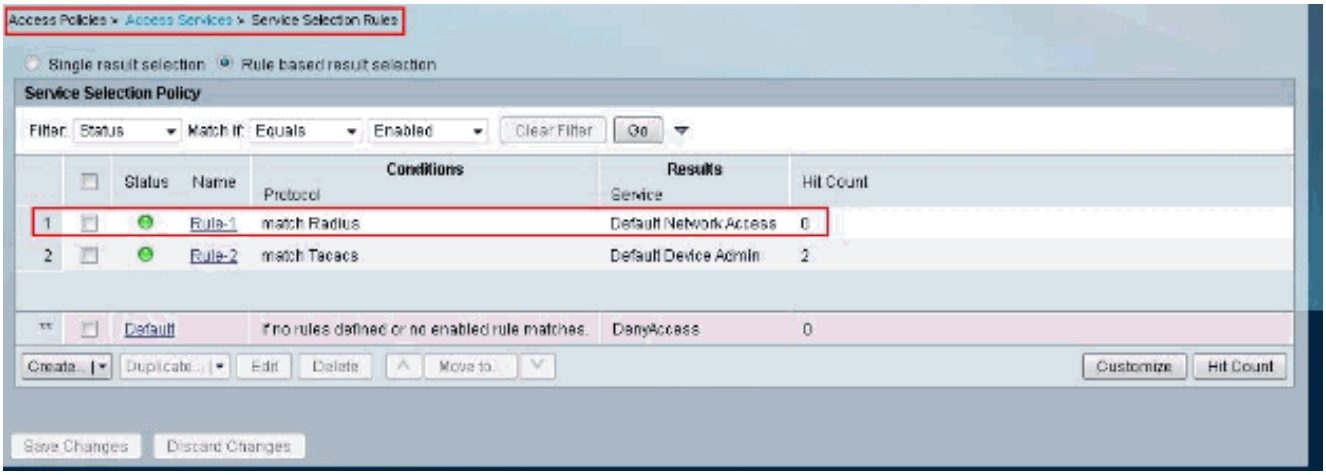

Der **LDAP-Server** wurde erfolgreich erstellt.



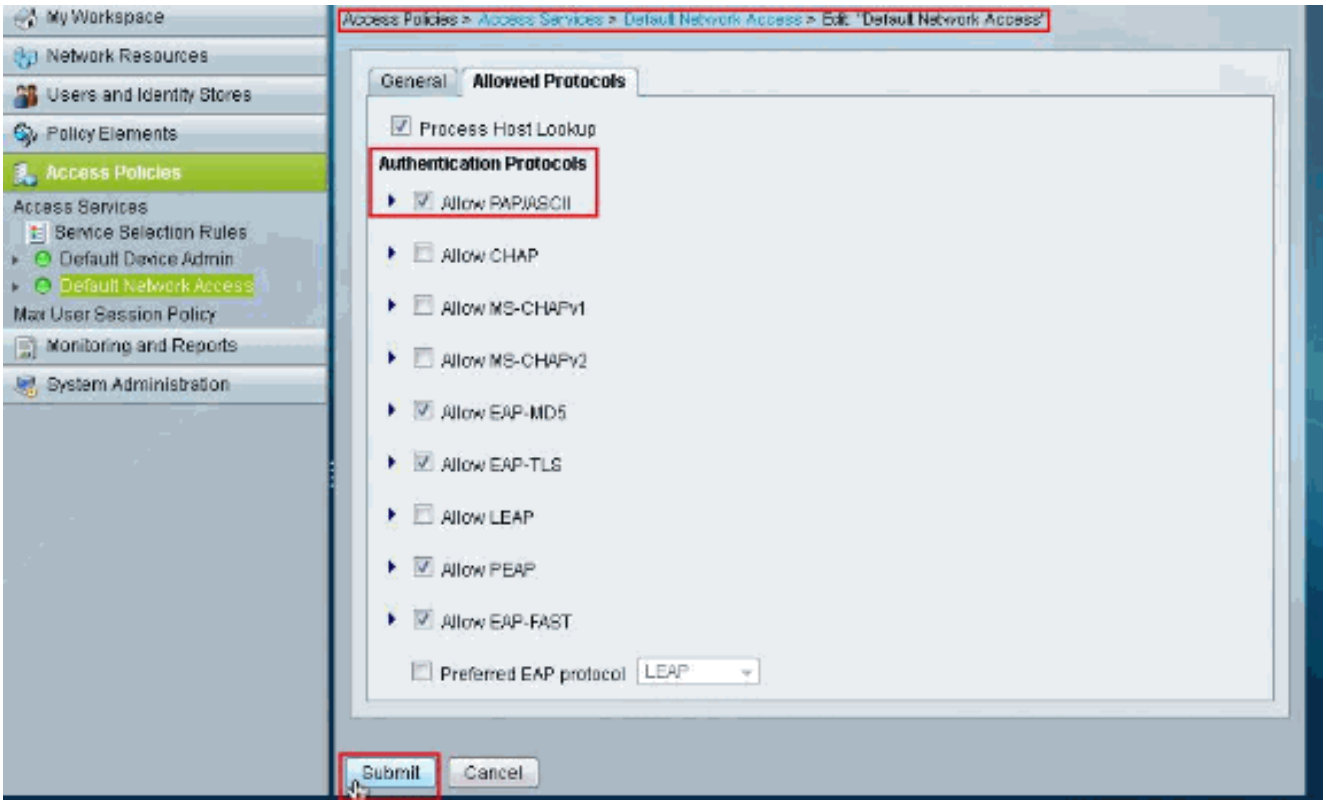

## Konfigurieren des Identitätsspeichers

Gehen Sie wie folgt vor, um den Identity Store zu konfigurieren:

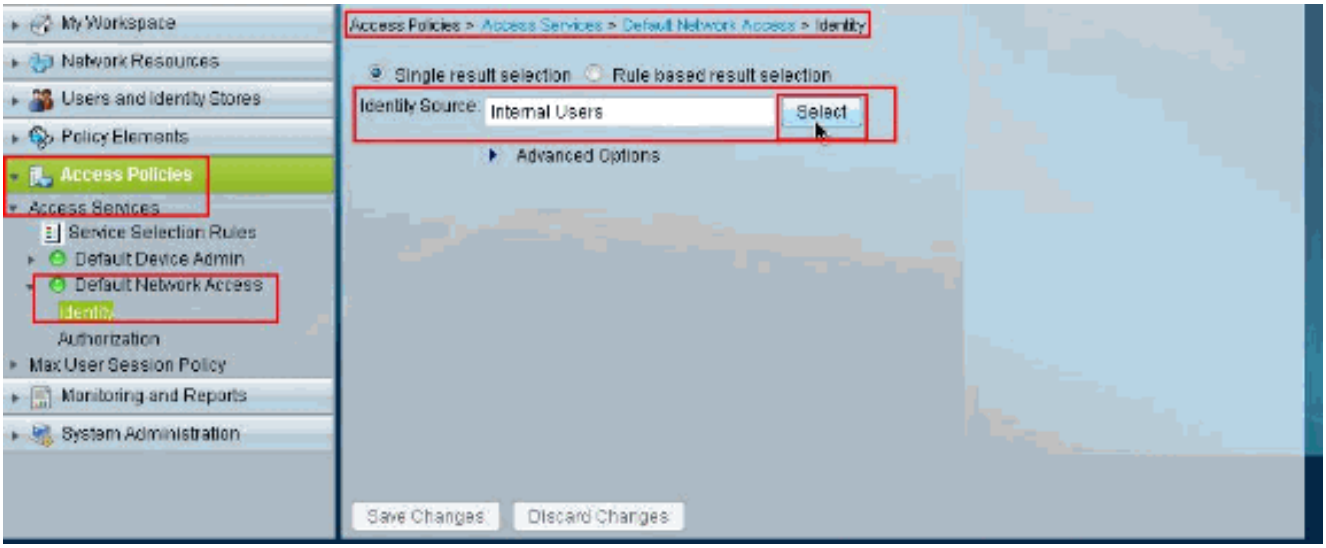
1. Wählen Sie **Zugriffsrichtlinien > Zugriffsdienste > Dienstauswahlregeln** aus, und überprüfen Sie, welcher Dienst den sicheren LDAP-Server für die Authentifizierung verwendet. In diesem Beispiel ist der Dienst **Standard-Netzwerkzugriff**.



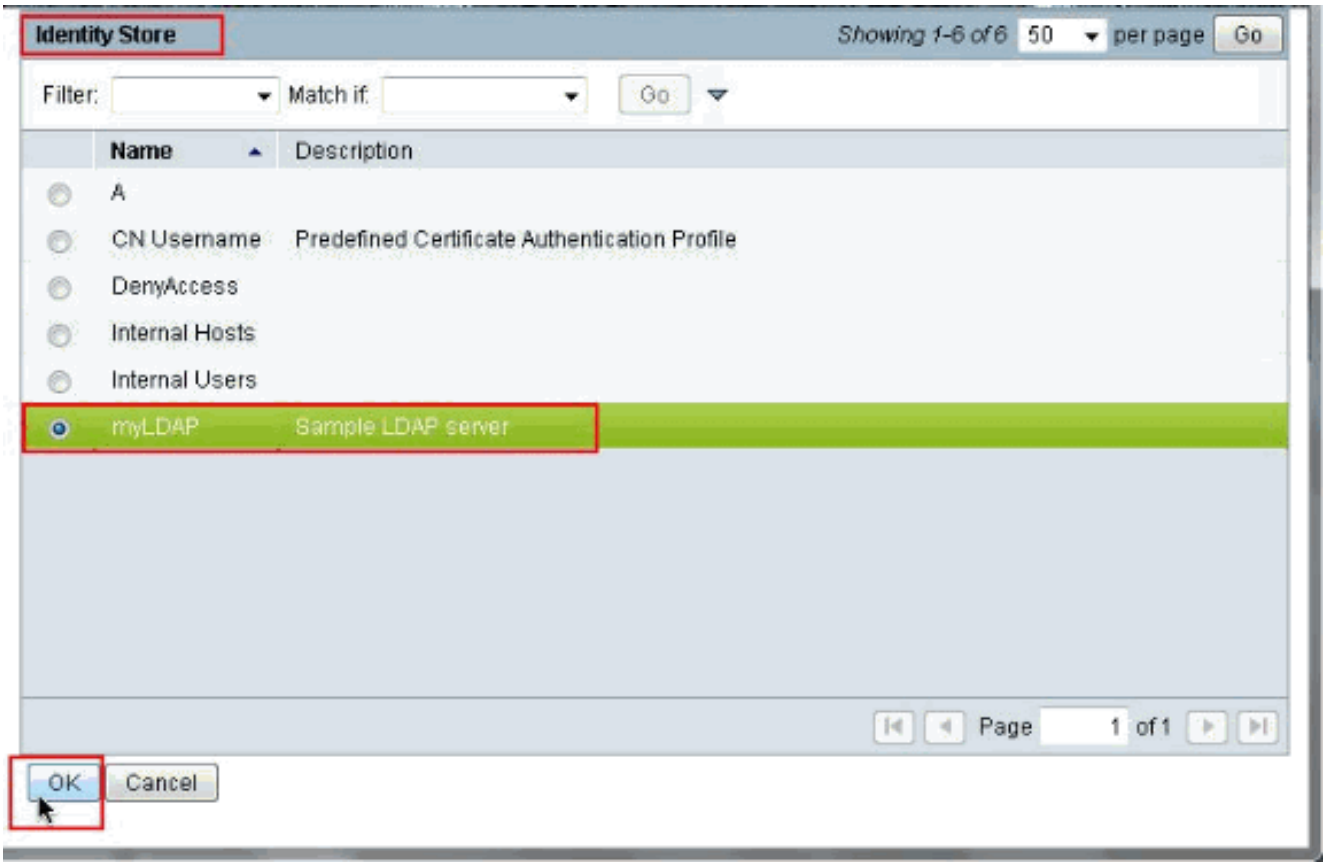

2. Nachdem Sie den Dienst in Schritt 1 überprüft haben, gehen Sie zum jeweiligen Dienst, und klicken Sie auf **Zulässige Protokolle**. Stellen Sie sicher, dass **PAP/ASCII zulassen** aktiviert ist, und klicken Sie dann auf **Senden**.**Hinweis:** Sie können andere Authentifizierungsprotokolle mit PAP/ASCII zulassen auswählen.



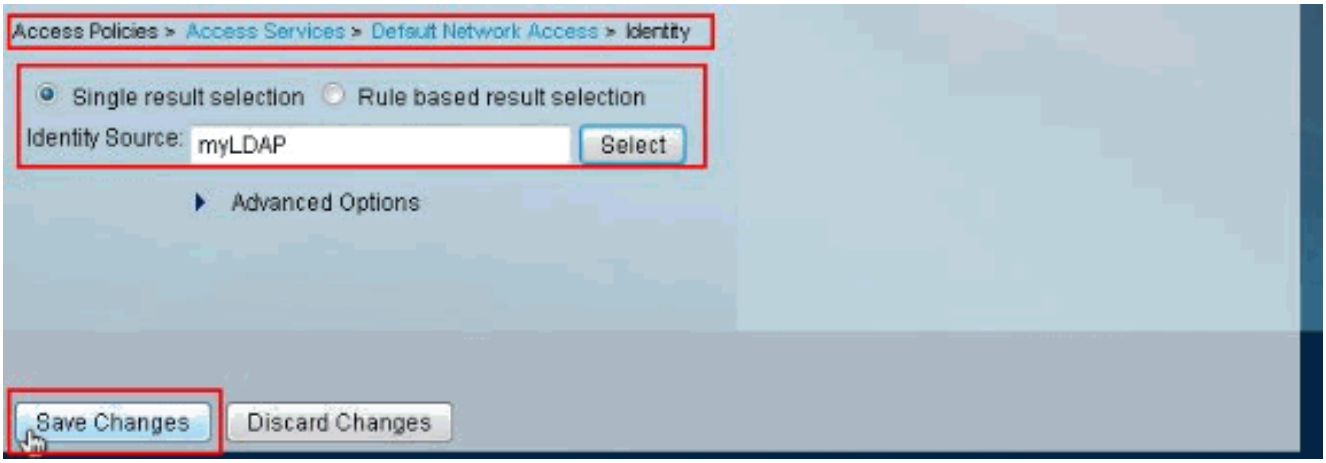

3. Klicken Sie auf den in Schritt 1 identifizierten Service und anschließend auf **Identität**. Klicken Sie neben **Identitätsquelle auf Auswählen**.



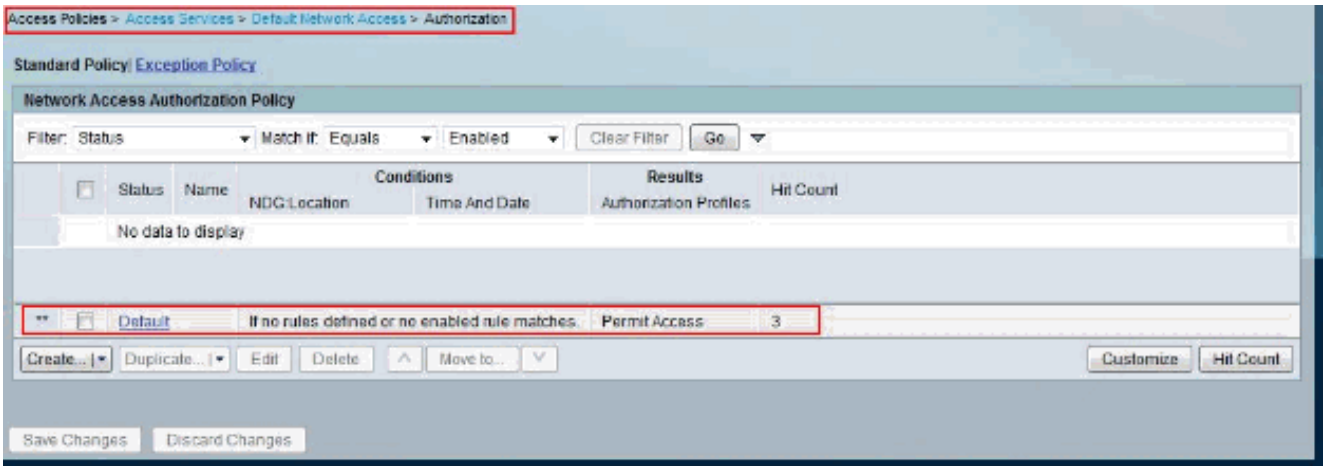

4. Wählen Sie den neu erstellten **sicheren LDAP-Server** (**myLDAP** in diesem Beispiel) aus, und klicken Sie dann auf **OK**.




5. Klicken Sie auf **Änderungen speichern**.




6. Gehen Sie zum Abschnitt **Autorisierung** des in **Schritt 1** identifizierten Dienstes, und stellen Sie sicher, dass mindestens eine Regel für die **Authentifizierung** vorhanden ist.




## Fehlerbehebung

Der ACS sendet eine Verbindungsanforderung zur Authentifizierung des Benutzers über einen LDAP-Server. Die Bindungsanforderung enthält die DN und das Benutzerkennwort des Benutzers in Klartext. Ein Benutzer wird authentifiziert, wenn die DN und das Kennwort des Benutzers mit dem Benutzernamen und Kennwort im LDAP-Verzeichnis übereinstimmen.

- **Authentifizierungsfehler**: ACS protokolliert Authentifizierungsfehler in den ACS-Protokolldateien.
- **Initialisierungsfehler** - Verwenden Sie die Zeitüberschreitungseinstellungen des LDAP-Servers, um die Anzahl der Sekunden zu konfigurieren, die der ACS auf eine Antwort von einem LDAP-Server wartet, bevor festgestellt wird, dass die Verbindung oder Authentifizierung auf diesem Server fehlgeschlagen ist. Mögliche Gründe, warum ein LDAP-Server einen Initialisierungsfehler zurückgibt, sind:LDAP wird nicht unterstütztDer Server ist ausgefallen.Der Server ist nicht ausgelastet.Der Benutzer hat keine Berechtigungen.Falsche Administratoranmeldeinformationen werden konfiguriert.
- **Bind Errors** (Bind-Fehler): Möglicherweise gibt ein LDAP-Server Bind- (Authentifizierungs-) Fehler zurück:FilterfehlerEine Suche mithilfe von Filterkriterien schlägt fehlParameterfehlerUngültige Parameter wurden eingegeben.Das Benutzerkonto ist eingeschränkt (deaktiviert, gesperrt, abgelaufen, Kennwort abgelaufen usw.)

Diese Fehler werden als Fehler externer Ressourcen protokolliert, was auf ein mögliches Problem mit dem LDAP-Server hinweist:

- Es ist ein Verbindungsfehler aufgetreten
- Das Timeout ist abgelaufen
- Der Server ist ausgefallen.
- Der Server ist nicht ausgelastet.

Dieser Fehler wird als Fehler "Unbekannter Benutzer" protokolliert: `Ein Benutzer ist nicht in der Datenbank vorhanden.`

Dieser Fehler wird als Fehler "Ungültiges Kennwort" protokolliert, wenn der Benutzer zwar vorhanden ist, das gesendete Kennwort jedoch ungültig ist: `Ein ungültiges Kennwort wurde eingegeben.`

## Zugehörige Informationen

- Cisco Secure Access Control System
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems