

Web-Authentifizierung mithilfe von LDAP auf Wireless LAN Controllern (WLCs) - Konfigurationsbeispiel

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konventionen](#)

[Webauthentifizierungsprozess](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Konfigurieren des LDAP-Servers](#)

[Erstellen von Benutzern auf dem Domänencontroller](#)

[Erstellen einer Benutzerdatenbank unter einer Organisationseinheit](#)

[Konfigurieren des Benutzers für den LDAP-Zugriff](#)

[Anonyme Bindung](#)

[Aktivieren der Funktion für anonyme Bindung auf dem Windows 2012 Essentials Server](#)

[Gewähren des Zugriffs auf ANONYME ANMELDUNG für den Benutzer](#)

[Inhaltsberechtigung der Gewährungsliste für Organisationseinheit](#)

[Authentifizierte Bindung](#)

[Administratorberechtigungen für WLC-Administrator erteilen](#)

[Verwenden von LDP zum Identifizieren der Benutzerattribute](#)

[WLC für LDAP-Server konfigurieren](#)

[WLAN für die Webauthentifizierung konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird die Einrichtung eines Wireless LAN Controllers (WLC) für die Webauthentifizierung beschrieben. Es wird erläutert, wie Sie einen LDAP-Server (Lightweight Directory Access Protocol) als Backend-Datenbank für die Webauthentifizierung konfigurieren, um Benutzeranmeldeinformationen abzurufen und den Benutzer zu authentifizieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse der Konfiguration von Lightweight Access Points (LAPs) und Cisco WLCs
- Kenntnisse des CAPWAP-Protokolls (Control And Provisioning of Wireless Access Point Protocol)
- Kenntnisse zum Einrichten und Konfigurieren von LDAP (Lightweight Directory Access Protocol), Active Directory und Domänencontrollern

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco 5508 WLC mit Firmware-Version 8.2.100.0
- Cisco Serie 1142 - LAP
- Cisco 802.11a/b/g Wireless Client Adapter
- Microsoft Windows 2012 Essentials Server, der die Rolle des LDAP-Servers übernimmt

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Konventionen

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

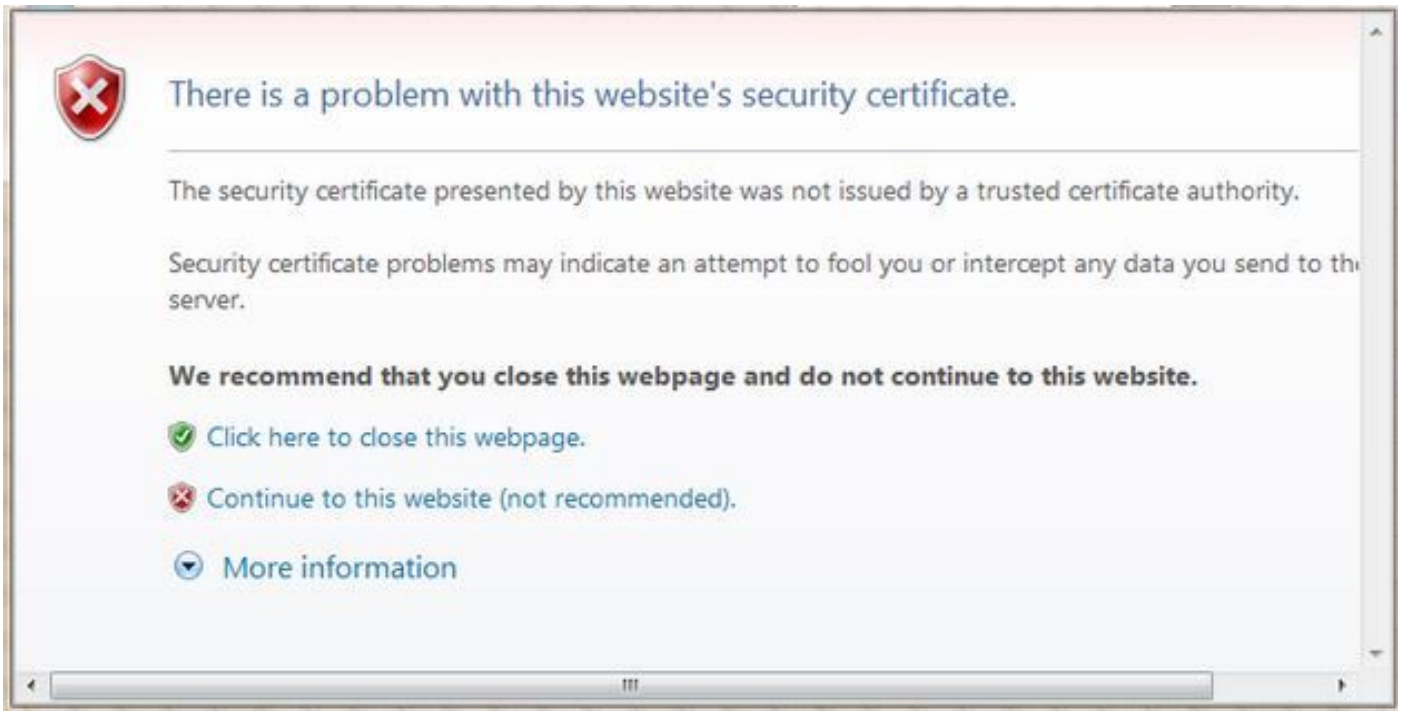
Webauthentifizierungsprozess

Die Webauthentifizierung ist eine Sicherheitsfunktion auf Layer 3, die den Controller veranlasst, den IP-Datenverkehr (mit Ausnahme von DHCP und DNS-bezogenen Paketen) von einem bestimmten Client zu unterbinden, bis dieser Client einen gültigen Benutzernamen und ein gültiges Kennwort eingegeben hat. Wenn Sie die Webauthentifizierung zur Authentifizierung von Clients verwenden, müssen Sie für jeden Client einen Benutzernamen und ein Kennwort definieren. Wenn die Clients dann versuchen, dem WLAN beizutreten, müssen sie den Benutzernamen und das Passwort eingeben, wenn sie von einer Anmeldeseite dazu aufgefordert werden.

Wenn die Webauthentifizierung aktiviert ist (unter Layer-3-Sicherheit), erhalten Benutzer gelegentlich eine Sicherheitswarnung für den Webbrowser, wenn sie zum ersten Mal versuchen, auf eine URL zuzugreifen.

Tipp: Kehren Sie zum Entfernen dieser Zertifikatswarnung zur folgenden Anleitung zurück, um ein vertrauenswürdigen Zertifikat eines Drittanbieters zu installieren:

<http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan->



Nachdem Sie zum Beispiel für Firefox-Browser auf **Ja** klicken, **um** fortzufahren (oder genauer gesagt, **diese Website fortsetzen (nicht empfohlen)**) oder wenn der Browser des Clients keine Sicherheitswarnung anzeigt, leitet das Web-Authentifizierungssystem den Client auf eine Anmeldeseite um, wie im Bild gezeigt:

Login

Welcome to the Cisco wireless network

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

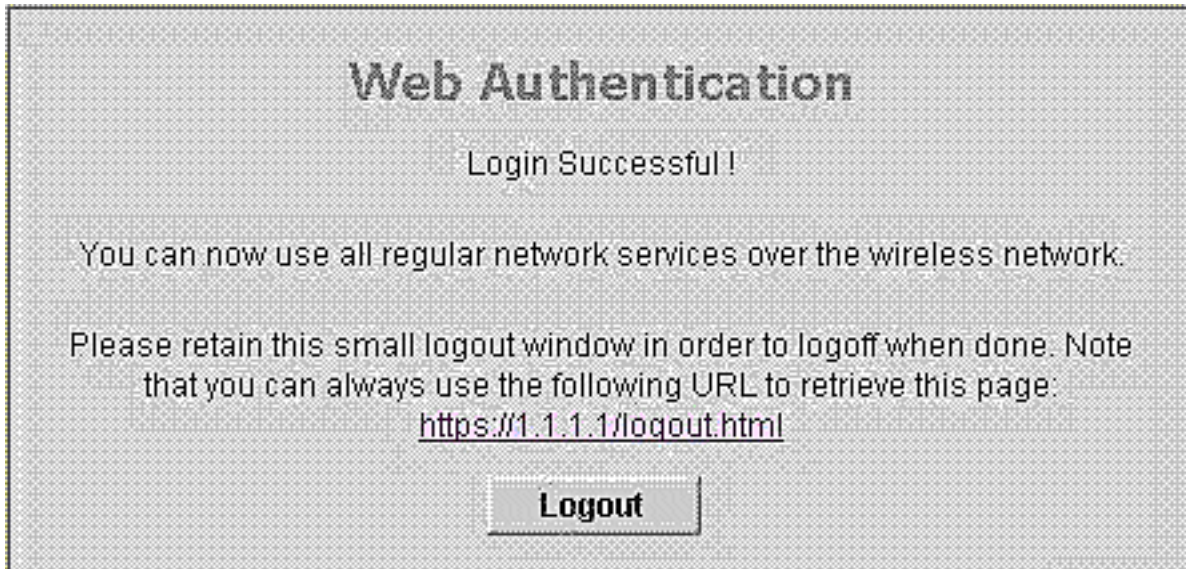
| | |
|---------------------------------------|--------------------------|
| User Name | <input type="text"/> |
| Password | <input type="password"/> |
| <input type="submit" value="Submit"/> | |

Die Standard-Anmeldeseite enthält ein Cisco Logo und einen speziellen Text von Cisco. Sie können wählen, ob das Web-Authentifizierungssystem eine der folgenden Optionen anzeigen soll:

- Die Standardanmeldeseite

- Eine geänderte Version der Standardanmeldeseite
- Eine benutzerdefinierte Anmeldeseite, die Sie auf einem externen Webserver konfigurieren
- Eine benutzerdefinierte Anmeldeseite, die Sie auf den Controller herunterladen

Wenn Sie auf der Anmeldeseite für die Webauthentifizierung einen gültigen Benutzernamen und ein gültiges Kennwort eingeben und auf **Senden** klicken, werden Sie anhand der übermittelten Anmeldeinformationen und einer erfolgreichen Authentifizierung aus der Backend-Datenbank (in diesem Fall LDAP) authentifiziert. Das Web-Authentifizierungssystem zeigt dann eine erfolgreiche Anmeldeseite an und leitet den authentifizierten Client an die angeforderte URL weiter.



Die standardmäßig erfolgreiche Anmeldeseite enthält einen Verweis auf die URL eines virtuellen Gateways: <https://1.1.1.1/logout.html>. Die IP-Adresse, die Sie für die virtuelle Controller-Schnittstelle festlegen, dient als Umleitungsadresse für die Anmeldeseite.

In diesem Dokument wird erläutert, wie Sie die interne Webseite des WLC für die Webauthentifizierung verwenden. In diesem Beispiel wird ein LDAP-Server als Backend-Datenbank für die Webauthentifizierung verwendet, um Benutzeranmeldeinformationen abzurufen und den Benutzer zu authentifizieren.

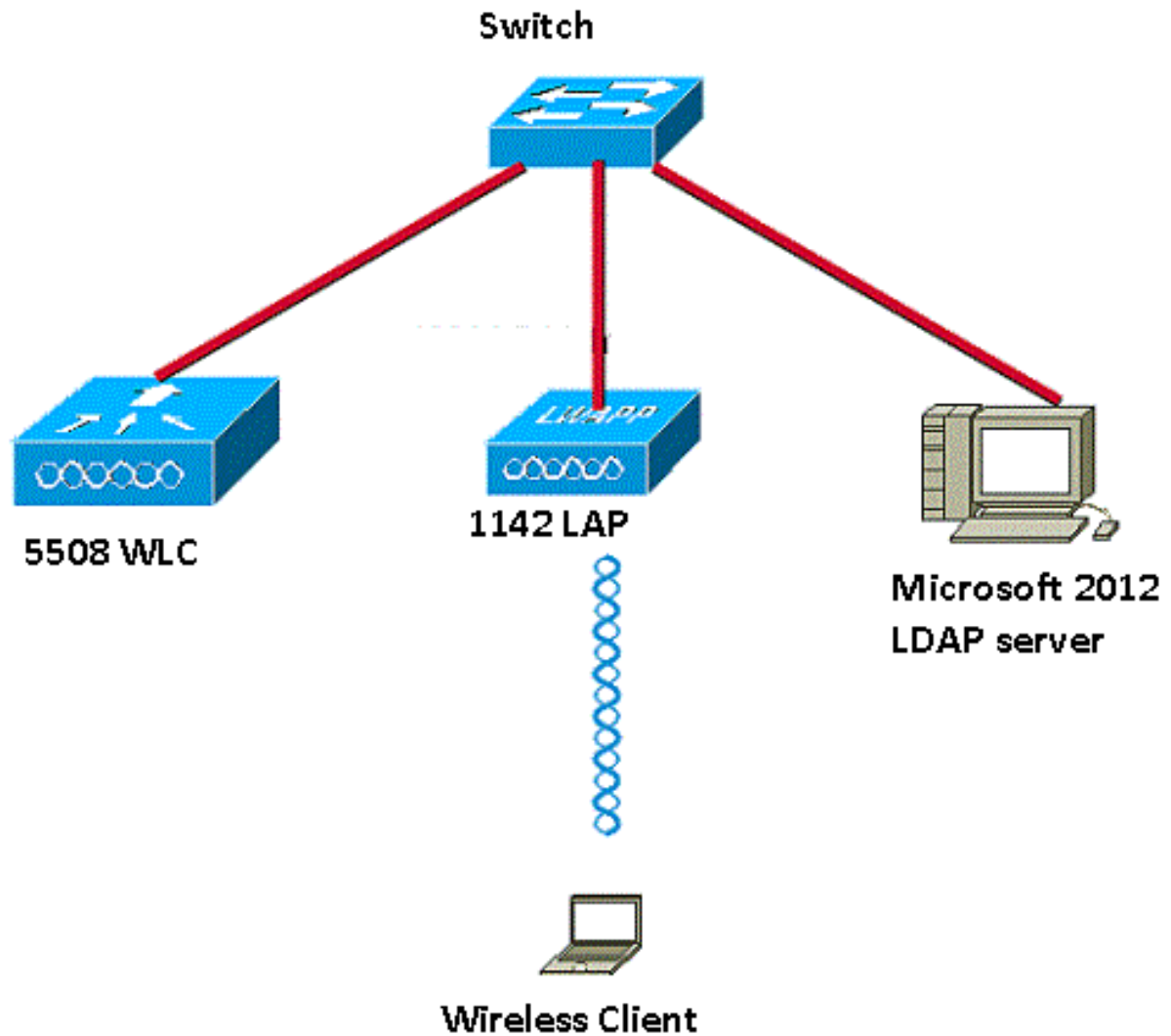
Konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Hinweis: Verwenden Sie das Tool für die Suche nach Befehlen ([nur registrierte Kunden](#)), um [weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten](#).

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

Gehen Sie wie folgt vor, um diese Konfiguration erfolgreich zu implementieren:

- [Konfigurieren Sie den LDAP-Server.](#)
- [WLC für LDAP-Server konfigurieren.](#)
- [Konfigurieren Sie das WLAN für die Webauthentifizierung.](#)

Konfigurieren des LDAP-Servers

Der erste Schritt besteht in der Konfiguration des LDAP-Servers, der als Backend-Datenbank zum Speichern der Benutzeranmeldeinformationen der Wireless-Clients dient. In diesem Beispiel wird der Microsoft Windows 2012 Essentials-Server als LDAP-Server verwendet.

Der erste Schritt bei der Konfiguration des LDAP-Servers besteht darin, eine Benutzerdatenbank auf dem LDAP-Server zu erstellen, sodass der WLC diese Datenbank abfragen kann, um den Benutzer zu authentifizieren.

Erstellen von Benutzern auf dem Domänencontroller

Eine Organisationseinheit (OU) enthält mehrere Gruppen, die Verweise auf persönliche Einträge in einem Personenprofil enthalten. Eine Person kann Mitglied mehrerer Gruppen sein. Alle

Objektklassen- und Attributdefinitionen sind standardmäßig im LDAP-Schema definiert. Jede Gruppe enthält Referenzen (dn) für jede Person, die zu ihr gehört.

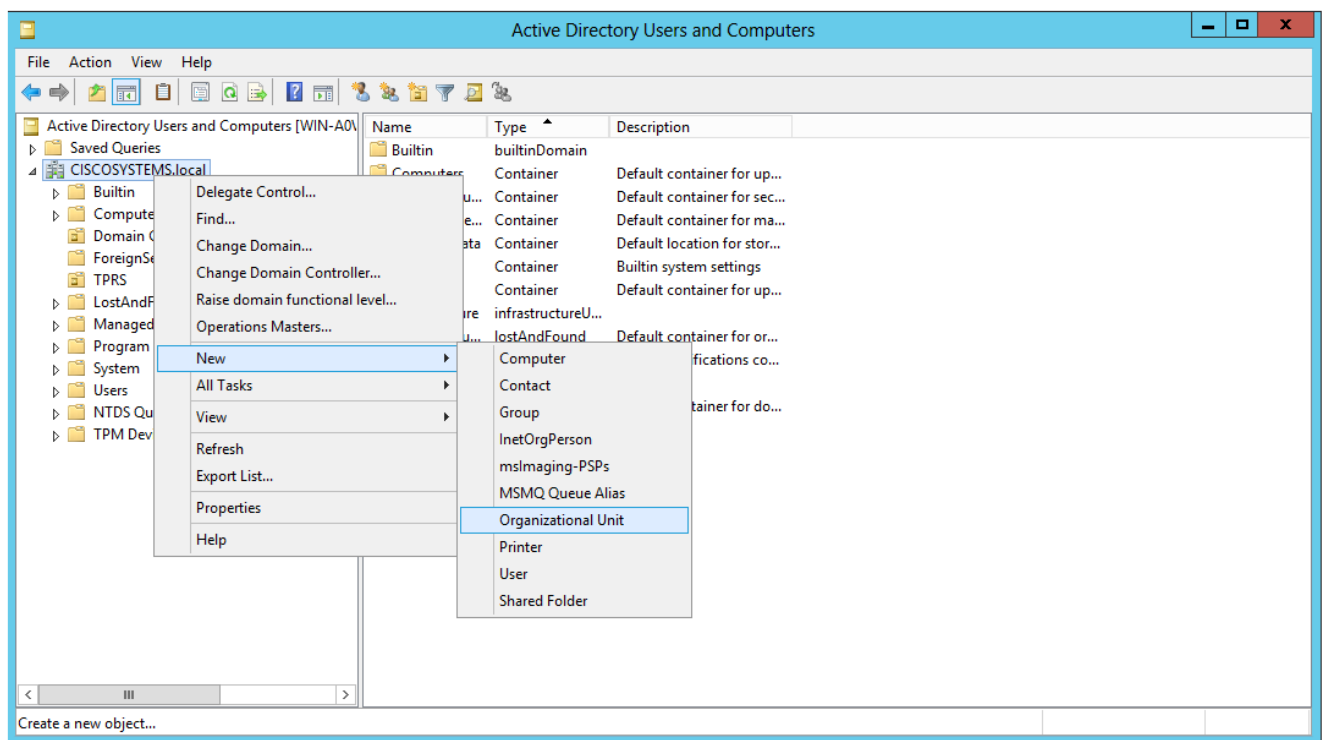
In diesem Beispiel wird eine neue OU LDAP-USERS erstellt, und der Benutzer User1 wird unter dieser OU erstellt. Wenn Sie diesen Benutzer für den LDAP-Zugriff konfigurieren, kann der WLC diese LDAP-Datenbank zur Benutzerauthentifizierung abfragen.

Die in diesem Beispiel verwendete Domäne ist **CISCOSYSTEMS.local**.

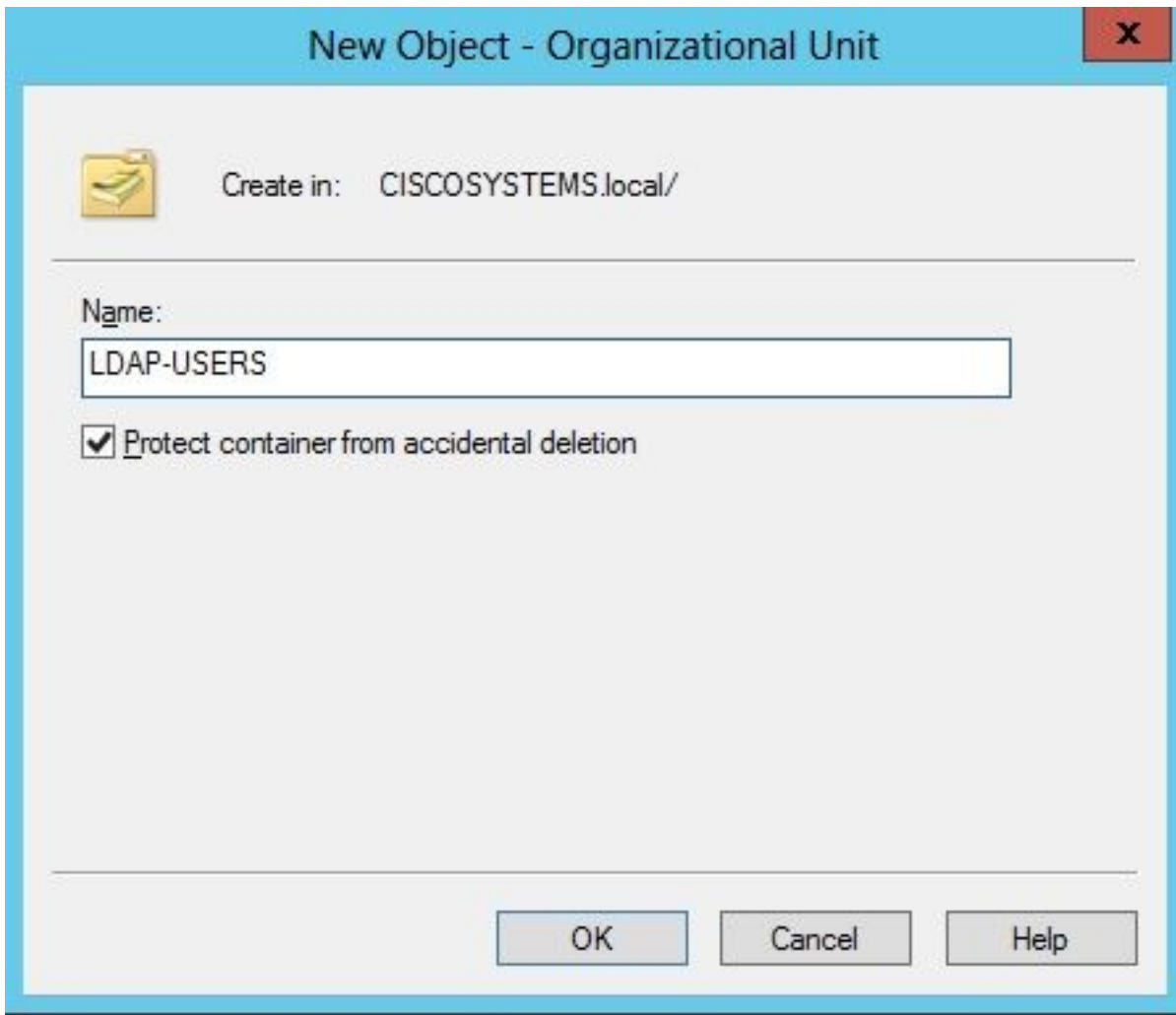
Erstellen einer Benutzerdatenbank unter einer Organisationseinheit

In diesem Abschnitt wird erläutert, wie Sie eine neue OU in Ihrer Domäne erstellen und einen neuen Benutzer auf dieser OU erstellen.

1. Öffnen Sie Windows PowerShell, und geben Sie **servermanager.exe** ein.
2. Klicken Sie im Fenster Server Manager auf **AD DS**. Klicken Sie dann mit der rechten Maustaste auf den Servernamen, um **Active Directory-Benutzer und -Computer** auszuwählen.
3. Klicken Sie mit der rechten Maustaste auf den Domännennamen, der in diesem Beispiel **CISCOSYSTEMS.local** lautet, und navigieren Sie dann im Kontextmenü zu **Neu > Organisationseinheit**, um eine neue Organisationseinheit zu erstellen.

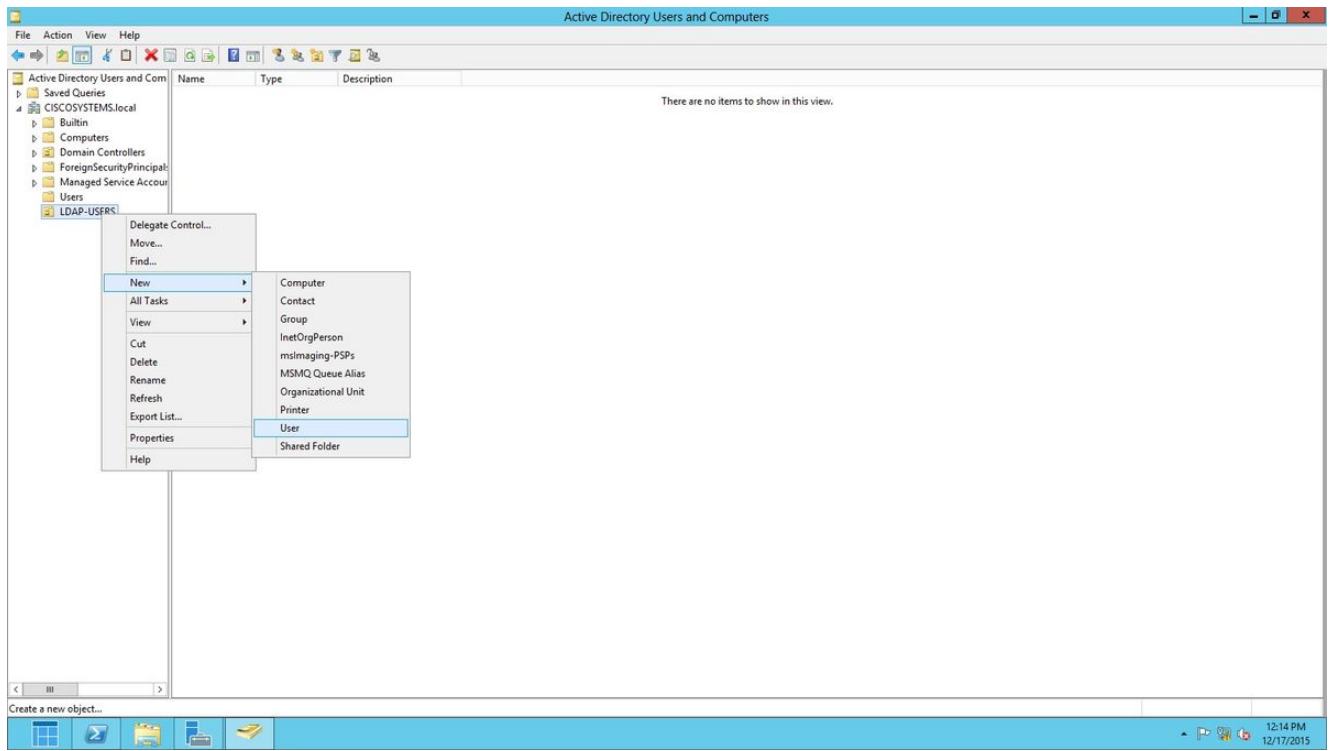


4. Weisen Sie dieser OU einen Namen zu, und klicken Sie auf **OK**, wie in der Abbildung dargestellt:



Nachdem die neuen OU LDAP-BENUTZER auf dem LDAP-Server erstellt wurden, besteht der nächste Schritt darin, **User1** unter dieser OU zu erstellen. Gehen Sie wie folgt vor, um dieses Ziel zu erreichen:

1. Klicken Sie mit der rechten Maustaste auf die neu erstellte Organisationseinheit. Navigieren Sie zu **LDAP-USERS > New > User** aus den resultierenden Kontextmenüs, um einen neuen Benutzer zu erstellen, wie im Bild gezeigt:



2. Füllen Sie auf der Seite für die Benutzereinrichtung die erforderlichen Felder aus, wie in diesem Beispiel gezeigt. In diesem Beispiel befindet sich **User1** im Feld **Benutzername**. Dies ist der Benutzername, der in der LDAP-Datenbank zur Authentifizierung des Clients überprüft wird. In diesem Beispiel wird User1 in den Feldern Vorname und Vollständiger Name verwendet. Klicken Sie auf **Next** (Weiter).

The screenshot shows the 'New Object - User' wizard. At the top, it says 'Create in: CISCO SYSTEMS.local/LDAP-USERS'. Below this are several input fields:

- 'First name:' with the value 'User1' and an empty 'Initials:' field.
- 'Last name:' with an empty field.
- 'Full name:' with the value 'User1'.
- 'User logon name:' with a text field containing 'User1' and a dropdown menu showing '@CISCO SYSTEMS.local'.
- 'User logon name (pre-Windows 2000):' with a text field containing 'CISCO SYSTEMS\'\' and another text field containing 'User1'.

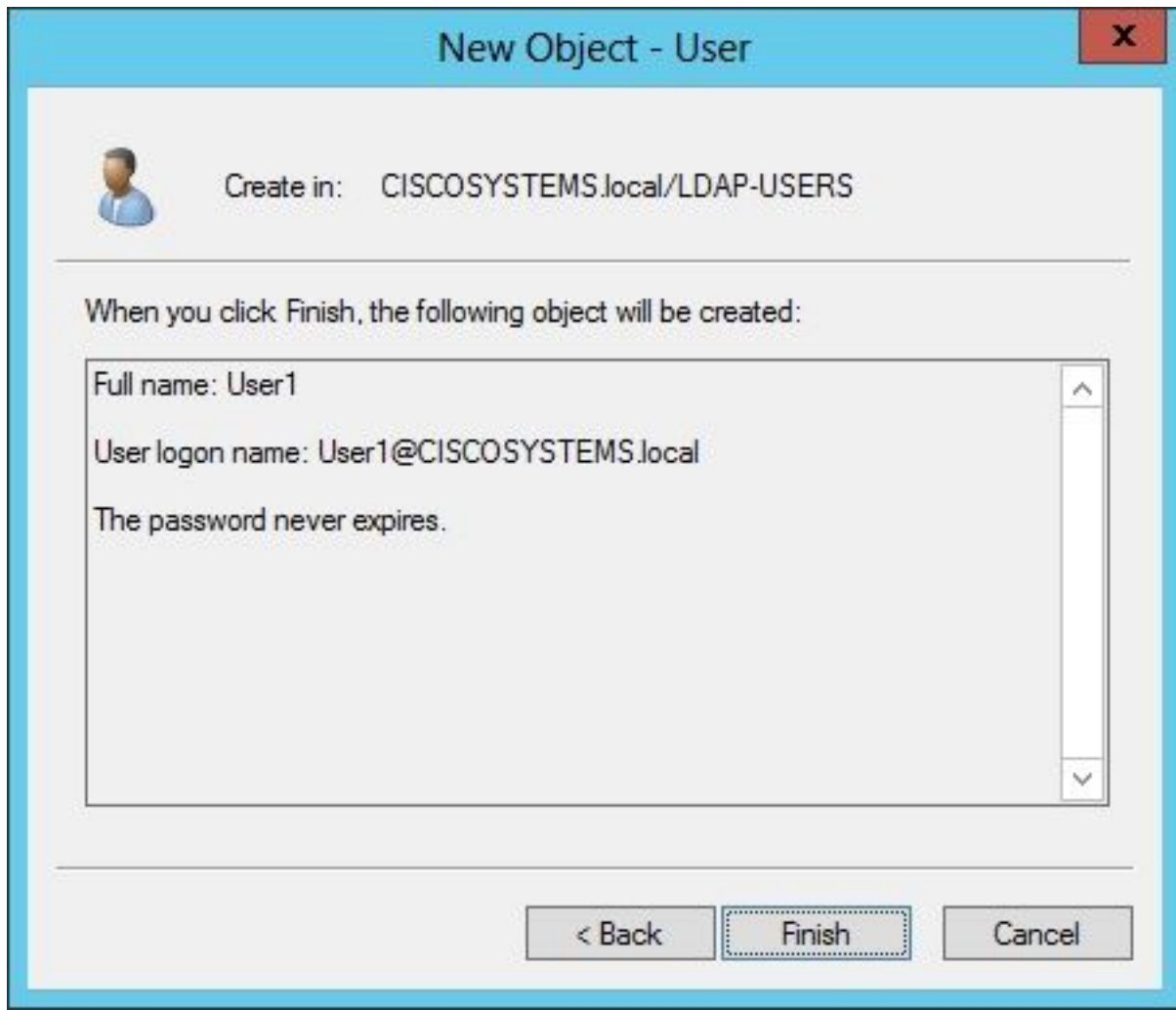
At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

3. Geben Sie ein Kennwort ein, und bestätigen Sie es. Wählen Sie die Option **Kennwort läuft nie ab**, und klicken Sie auf **Weiter**.



The screenshot shows a dialog box titled "New Object - User" with a close button (X) in the top right corner. Below the title bar, there is a user icon and the text "Create in: CISCO SYSTEMS.local/LDAP-USERS". The main area contains two password input fields: "Password:" and "Confirm password:", both filled with black dots. Below these fields are four checkboxes with the following labels: "User must change password at next logon", "User cannot change password", "Password never expires" (which is checked), and "Account is disabled". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

4. Klicken Sie auf **Beenden**. Unter der Organisationseinheit LDAP-BENUTZER wird ein neuer Benutzer Benutzer Benutzer1 erstellt. Dies sind die Benutzeranmeldeinformationen: Benutzername: **Benutzer1** Kennwort: **Notebook123**



Nachdem der Benutzer unter einer Organisationseinheit erstellt wurde, besteht der nächste Schritt darin, diesen Benutzer für den LDAP-Zugriff zu konfigurieren.

Konfigurieren des Benutzers für den LDAP-Zugriff

Sie können entweder **Anonym** oder **Authentifiziert** auswählen, um die lokale Authentifizierungsanbindungsmethode für den LDAP-Server anzugeben. Die Anonymous-Methode ermöglicht den anonymen Zugriff auf den LDAP-Server. Bei der Authenticated-Methode müssen ein Benutzername und ein Kennwort eingegeben werden, um den Zugriff zu sichern. Der Standardwert ist "Anonymous".

In diesem Abschnitt wird erläutert, wie Sie sowohl anonyme als auch authentifizierte Methoden konfigurieren.

Anonyme Bindung

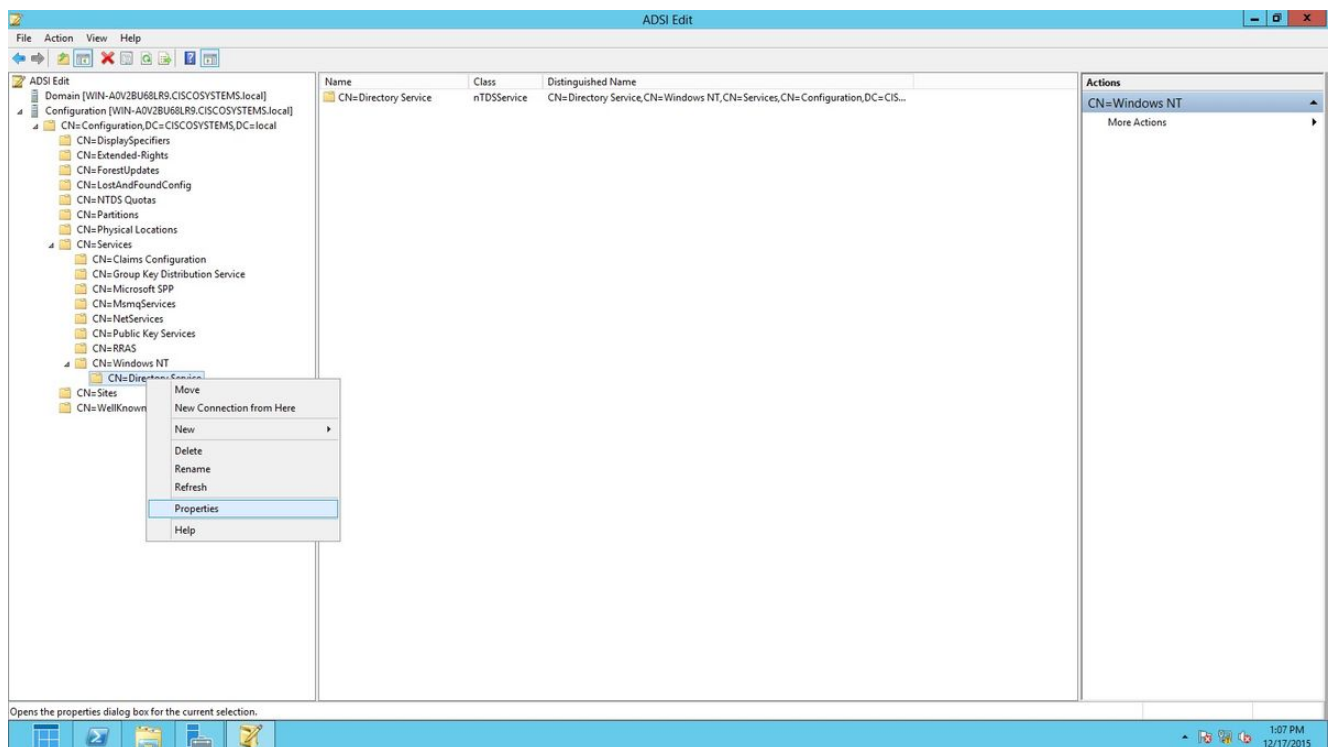
Hinweis: Die Verwendung von Anonymous Bind wird nicht empfohlen. Ein LDAP-Server, der anonyme Bindungen zulässt, erfordert keine Art von authentifizierter Authentifizierung. Ein Angreifer könnte den Eintrag Anonymous bind nutzen, um Dateien auf dem LDAP-Director anzuzeigen.

Führen Sie die Schritte in diesem Abschnitt aus, um den anonymen Benutzer für den LDAP-Zugriff zu konfigurieren.

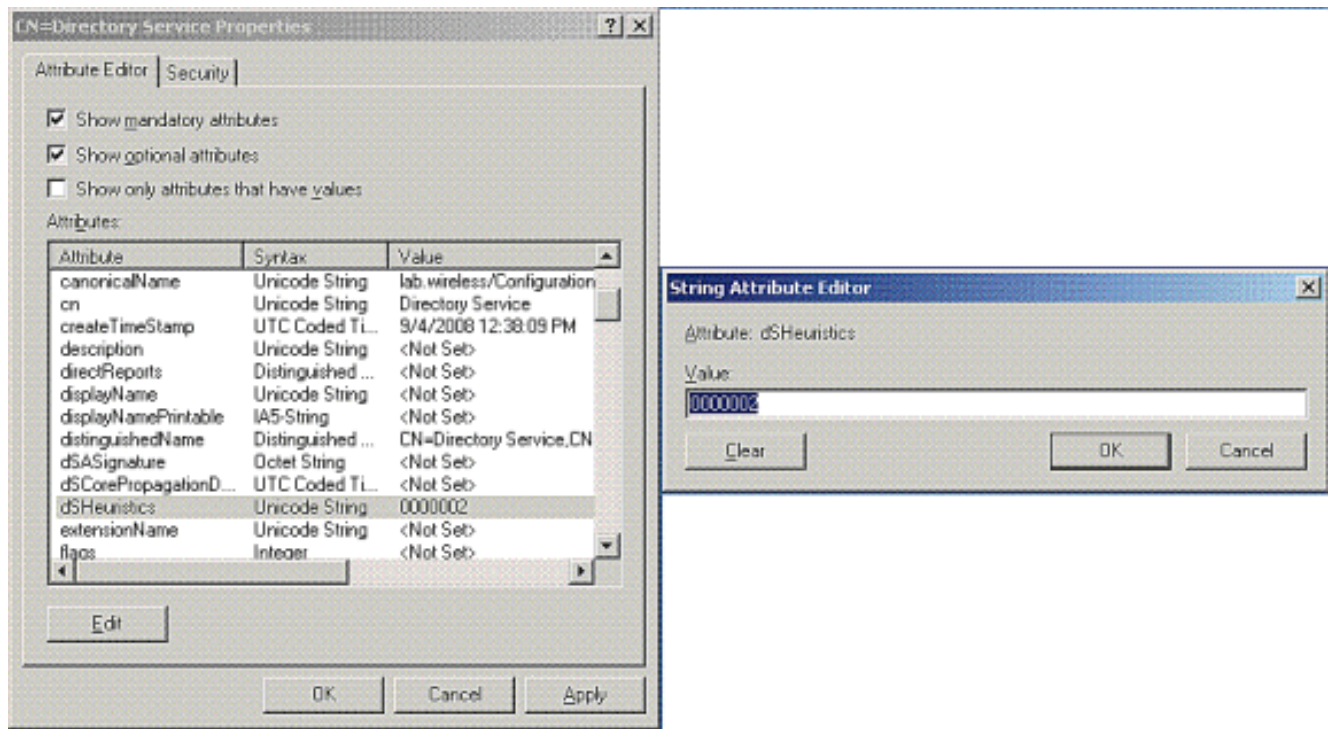
Aktivieren der Funktion für anonyme Bindung auf dem Windows 2012 Essentials Server

Damit Anwendungen von Drittanbietern (im vorliegenden Fall WLC) auf Windows 2012 AD über das LDAP zugreifen können, muss die Funktion "Anonyme Bindung" unter Windows 2012 aktiviert sein. Standardmäßig sind anonyme LDAP-Vorgänge auf Windows 2012-Domänencontrollern nicht zulässig. Führen Sie die folgenden Schritte aus, um die Funktion "Anonyme Bindung" zu aktivieren:

1. Starten Sie das ADSI-Bearbeitungstool, indem Sie **ADSIEdit.msc** in Windows PowerShell eingeben. Dieses Tool ist Teil der Windows 2012 Support-Tools.
2. Erweitern Sie im Fenster ADSI Edit (ADSI-Bearbeitung) die Stammdomäne (Configuration [WIN-A0V2BU68LR9.CISCOSYSTEMS.local]). Navigieren Sie zu **CN=Services > CN=Windows NT > CN=Directory Service**. Klicken Sie mit der rechten Maustaste auf den Container **CN=Directory Service**, und wählen Sie im Kontextmenü die Option **Eigenschaften** aus, wie in der Abbildung dargestellt:



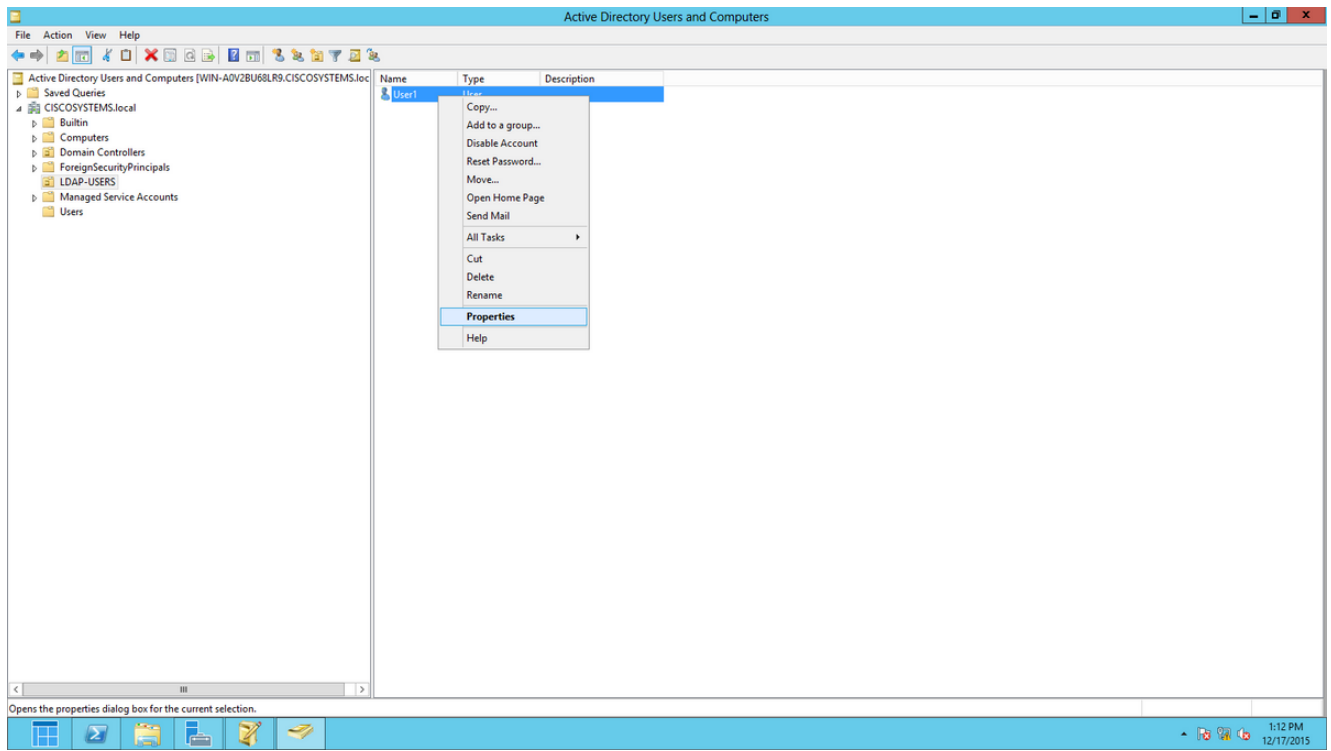
3. Klicken Sie im Fenster CN=Directory Service Properties (Eigenschaften von Verzeichnisdienst) unter **Attributes (Attribute)** auf das **dsHeuristics**-Attribut im Feld Attribute (Attribut), und wählen Sie **Edit (Bearbeiten)**. Geben Sie im Fenster Zeichenfolgenattribut-Editor dieses Attributs den Wert **000002** ein, klicken Sie auf **Anwenden** und **OK**, wie im Bild dargestellt. Die Funktion "Anonyme Bindung" ist auf dem Windows 2012-Server aktiviert. **Hinweis:** Das letzte (siebte) Zeichen steuert die Art der Anbindung an den LDAP-Dienst. 0 (Null) oder kein siebtes Zeichen bedeutet, dass anonyme LDAP-Vorgänge deaktiviert sind. Wenn Sie das siebte Zeichen auf 2 setzen, wird die Funktion Anonyme Bindung aktiviert.



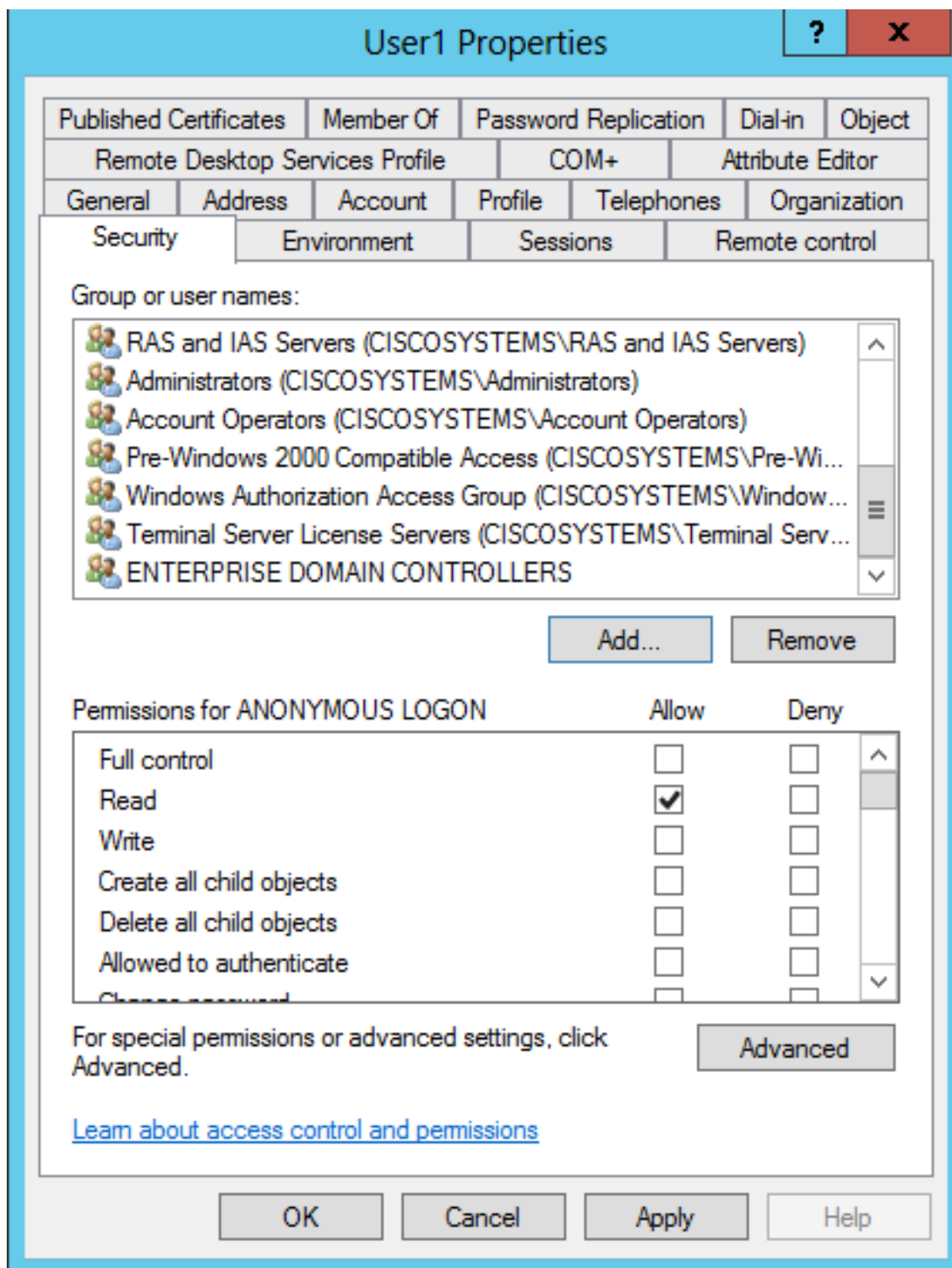
Gewähren des Zugriffs auf ANONYME ANMELDUNG für den Benutzer

Der nächste Schritt besteht darin, dem Benutzer User1 ANONYMOUS LOGON-Zugriff zu gewähren. Gehen Sie wie folgt vor, um dieses Ziel zu erreichen:

1. Öffnen Sie **Active Directory-Benutzer und -Computer**.
2. Stellen Sie sicher, dass die Option **Erweiterte Funktionen anzeigen** aktiviert ist.
3. Navigieren Sie zum Benutzer User1, und klicken Sie mit der rechten Maustaste darauf. Wählen Sie im Kontextmenü die Option **Eigenschaften**. Dieser Benutzer ist mit dem Vornamen User1 gekennzeichnet.

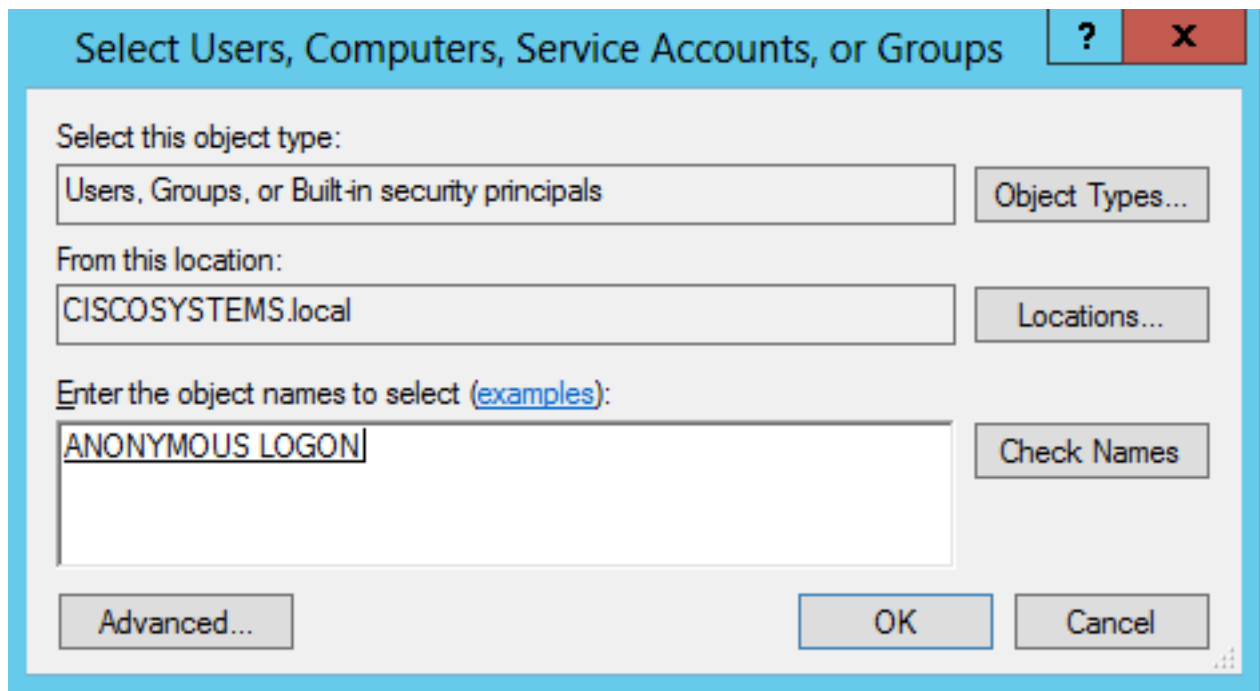


4. Klicken Sie auf die Registerkarte **Sicherheit**, wie in der Abbildung dargestellt:

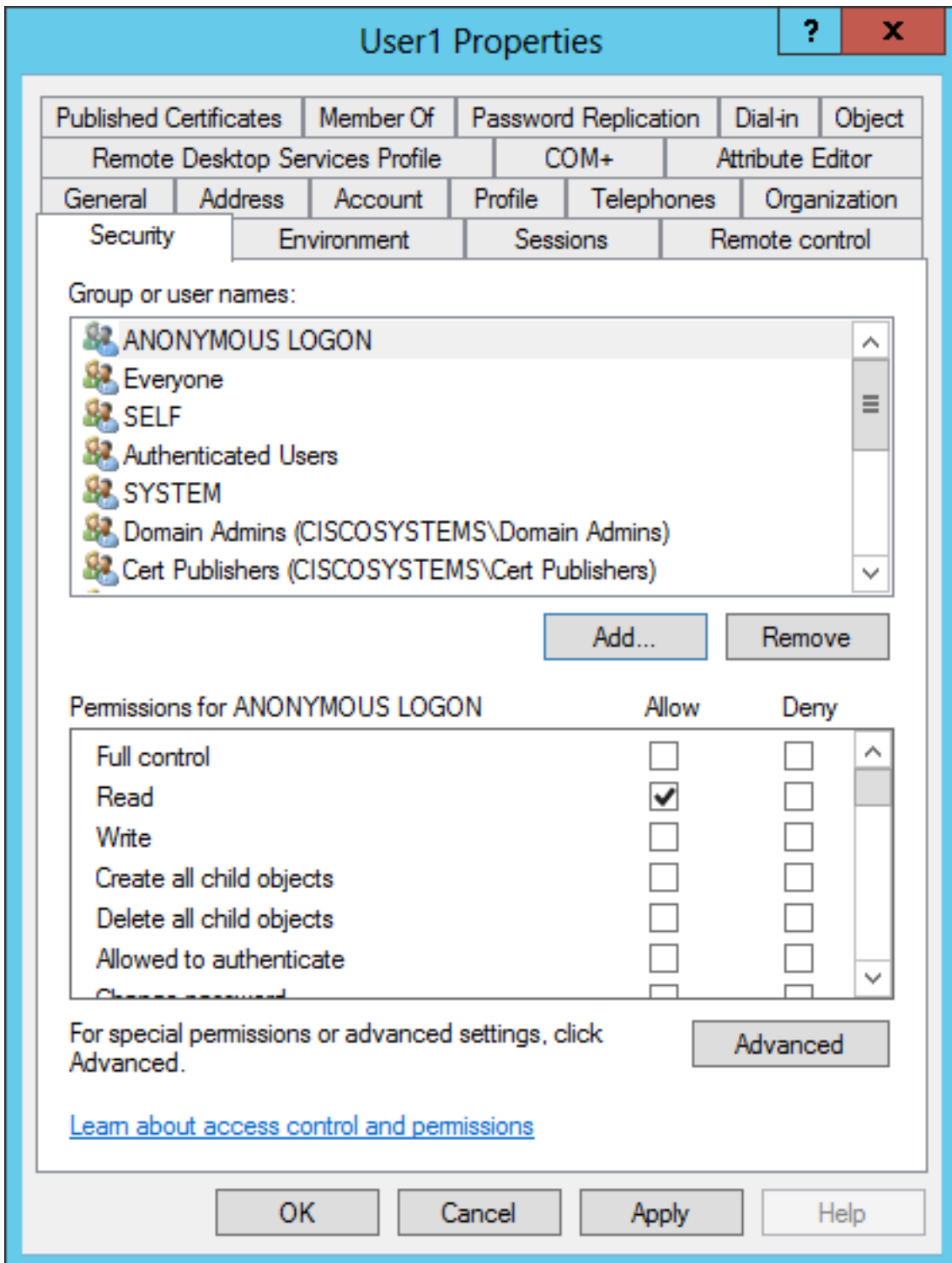


5. Klicken Sie im resultierenden Fenster auf **Hinzufügen**.

6. Geben Sie im Feld *Geben Sie die zu verwendenden Objektnamen ein* und bestätigen Sie den Dialog, wie in der Abbildung dargestellt:



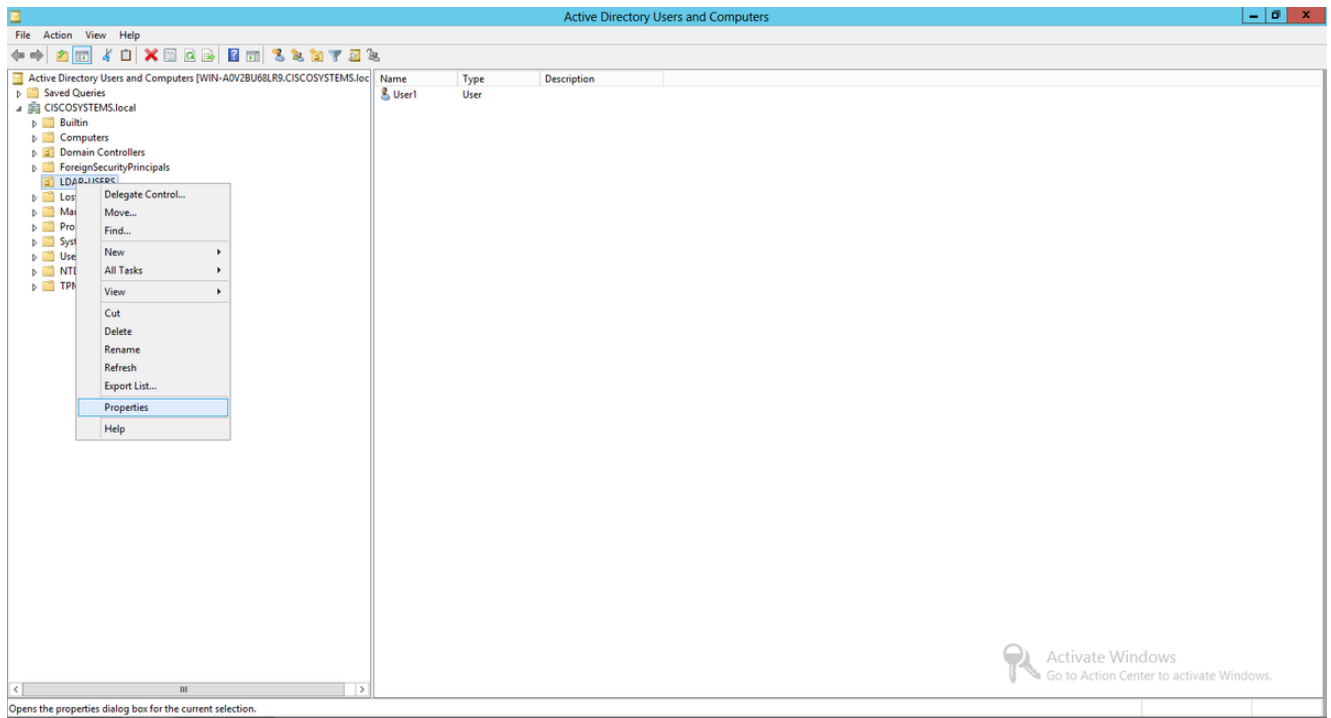
7. Beachten Sie, dass ANONYME LOGON in der ACL Zugriff auf einige Eigenschaftensätze des Benutzers hat. Klicken Sie auf **OK**. Der ANONYME LOGON-Zugriff wird diesem Benutzer gewährt, wie im Bild gezeigt:



Inhaltsberechtigung der Gewährungsliste für Organisationseinheit

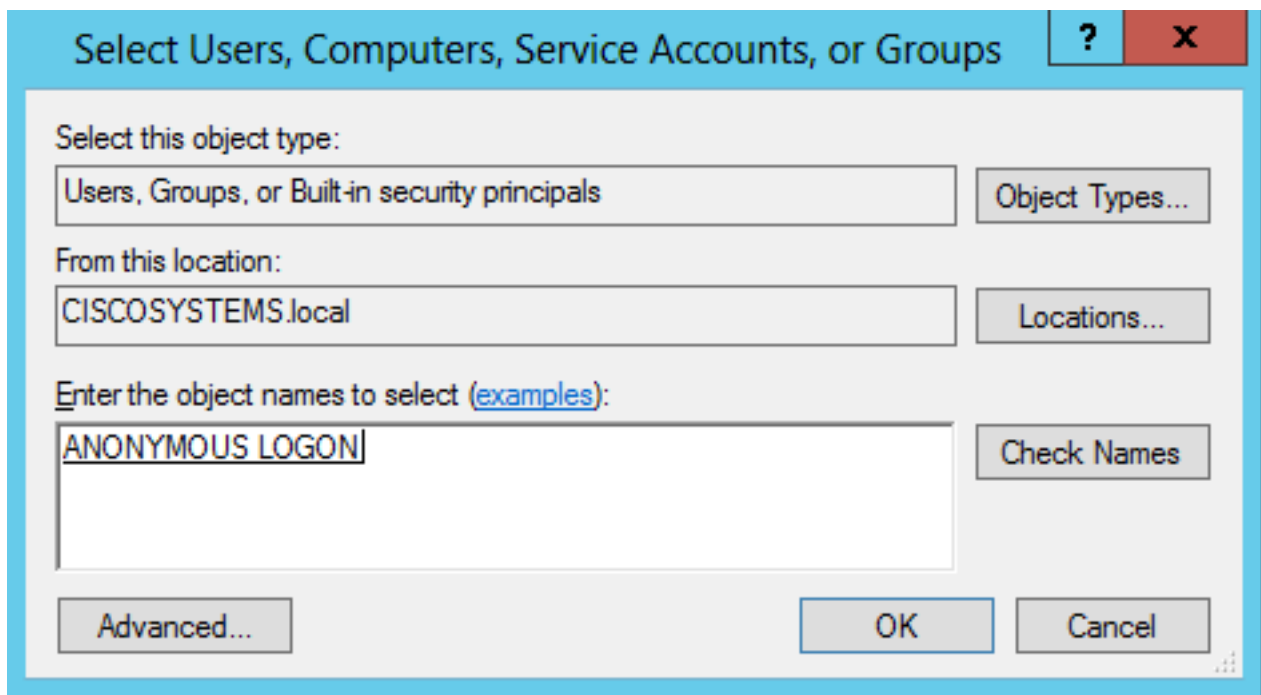
Der nächste Schritt besteht darin, der ANONYMEN ANMELDUNG in der OU, in der sich der Benutzer befindet, mindestens die Berechtigung zum Auflisten des Inhalts zu gewähren. In diesem Beispiel befindet sich User1 in der Organisationseinheit LDAP-USERS. Gehen Sie wie folgt vor, um dieses Ziel zu erreichen:

1. Klicken Sie in **Active Directory Users and Computers** mit der rechten Maustaste auf die OU **LDAP-USERS**, und wählen Sie **Eigenschaften** aus, wie im Bild gezeigt:



2. Klicken Sie auf **Sicherheit**.

3. Klicken Sie auf **Hinzufügen**. Geben Sie im daraufhin geöffneten Dialogfeld **ANONYME LOGON** ein, und bestätigen Sie das Dialogfeld, wie in der Abbildung dargestellt:



Authentifizierte Bindung

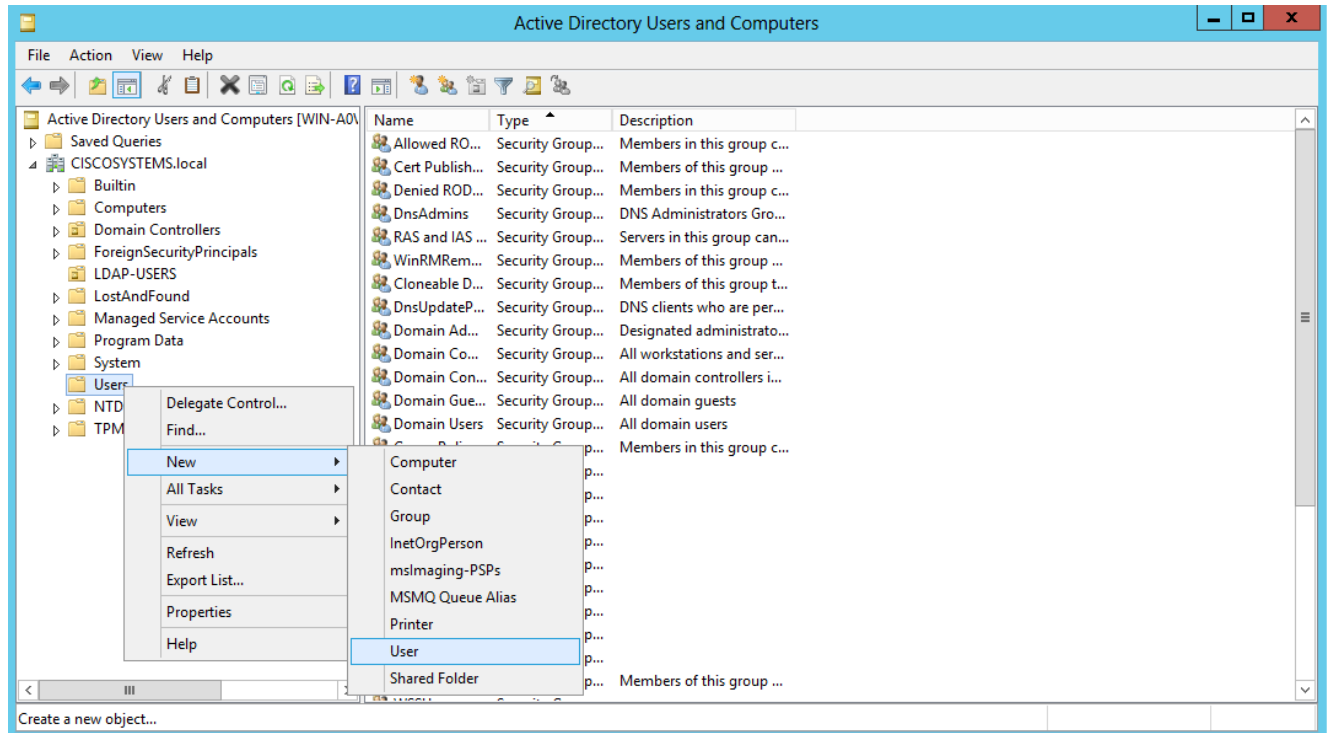
Führen Sie die Schritte in diesem Abschnitt aus, um einen Benutzer für die lokale Authentifizierung beim LDAP-Server zu konfigurieren.

1. Windows PowerShell öffnen und Folgendes eingeben **Servermanager.exe**

2. Klicken Sie im Fenster Server Manager auf **AD DS**. Klicken Sie dann mit der rechten Maustaste auf den Servernamen, um ihn auszuwählen. **Active Directory-Benutzer und -**

Computer.

3. Klicken Sie mit der rechten Maustaste auf **Benutzer**. Navigieren Sie aus den resultierenden Kontextmenüs zu **Neu > Benutzer**, um einen neuen Benutzer zu erstellen.

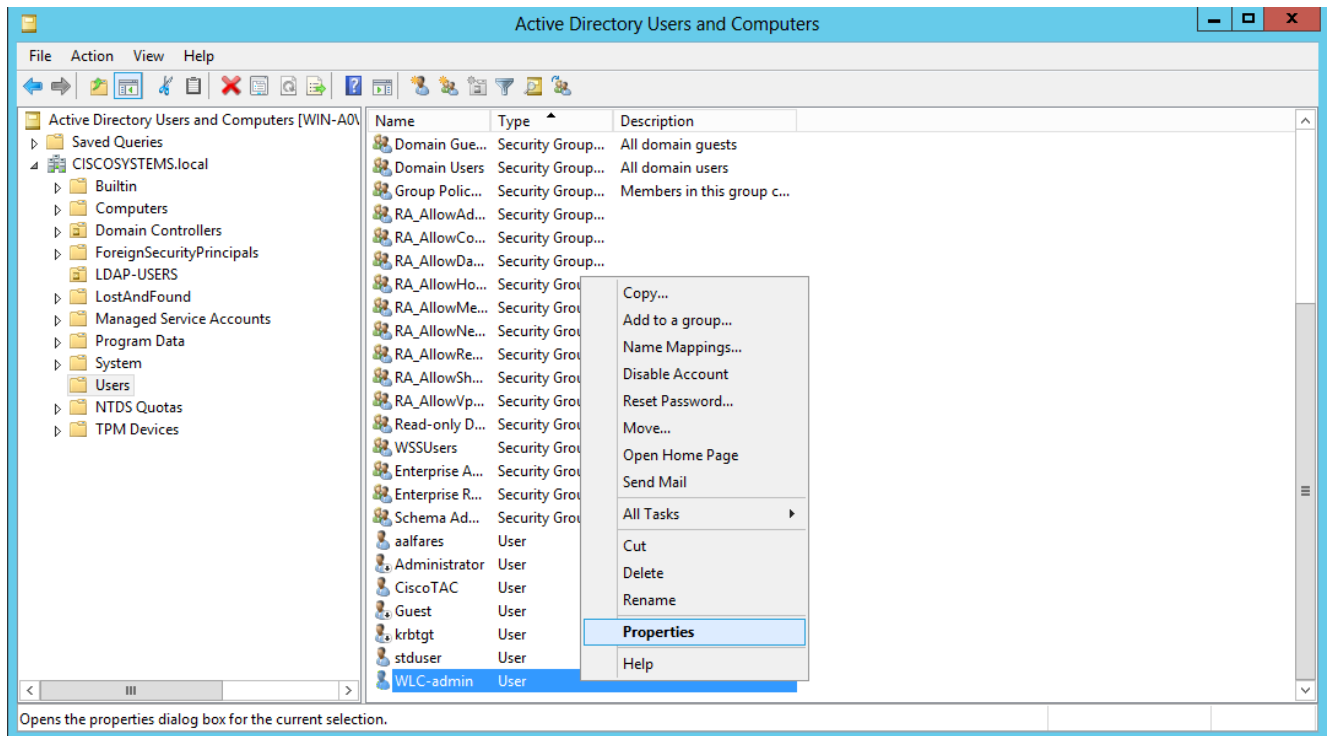


4. Füllen Sie auf der Seite für die Benutzereinrichtung die erforderlichen Felder aus, wie in diesem Beispiel gezeigt. In diesem Beispiel ist **WLC-admin** im Feld **Benutzername** angegeben. Dies ist der Benutzername, der für die lokale Authentifizierung beim LDAP-Server verwendet wird. Klicken Sie auf **Next** (Weiter).
5. Geben Sie ein Kennwort ein, und bestätigen Sie es. Wählen Sie die Option **Kennwort läuft nie ab**, und klicken Sie auf **Weiter**.
6. Klicken Sie auf **Beenden**. Unter dem Container **Users** wird ein neuer Benutzer **WLC-admin** erstellt. Dies sind die Benutzeranmeldeinformationen: Benutzername: **WLC-admin** Kennwort: **Admin123**

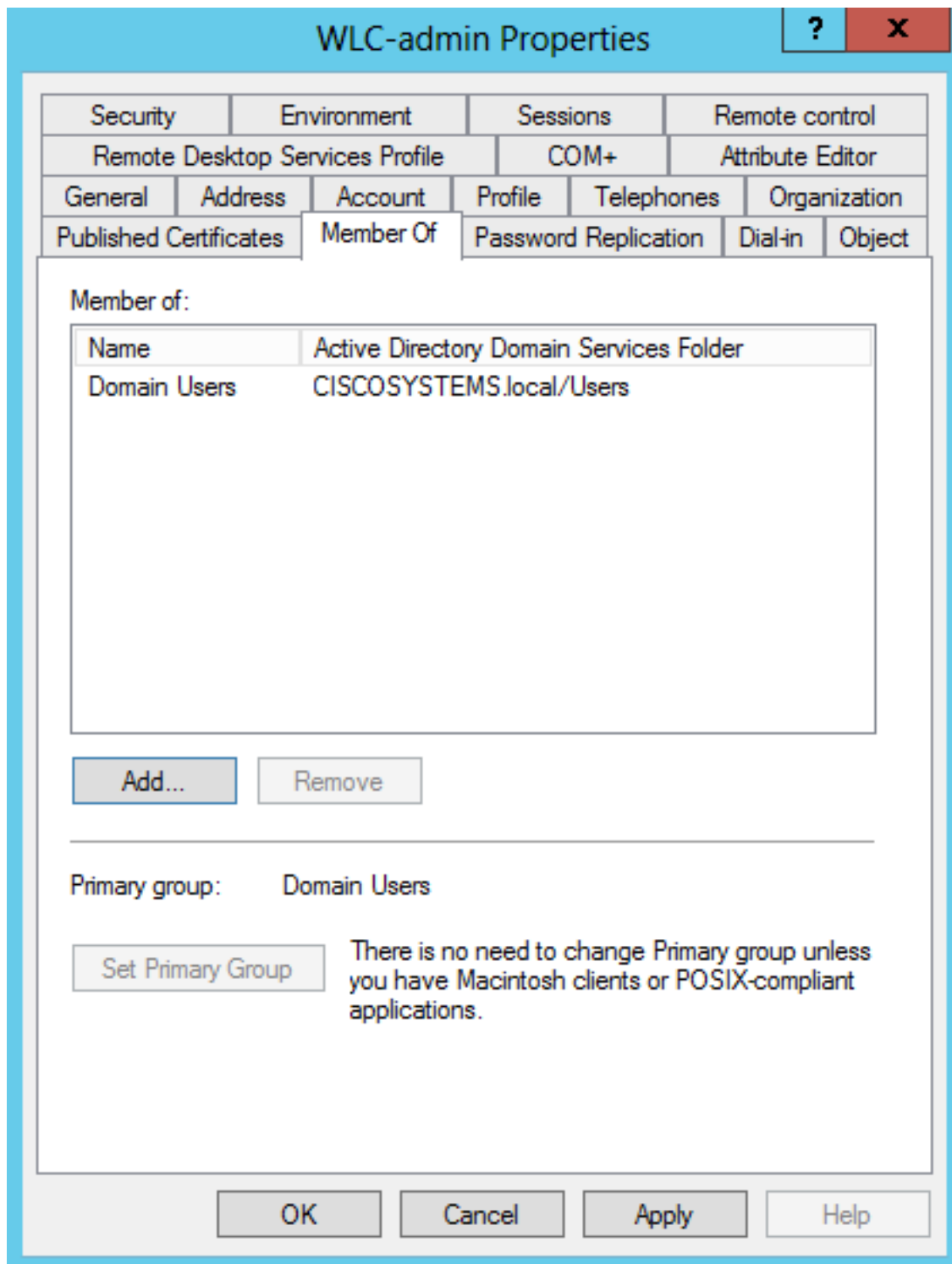
Administratorberechtigungen für WLC-Administrator erteilen

Nachdem der lokale Authentifizierungsbenutzer erstellt wurde, müssen ihm nun Administratorberechtigungen erteilt werden. Gehen Sie wie folgt vor, um dieses Ziel zu erreichen:

1. Öffnen Sie **Active Directory-Benutzer und -Computer**.
2. Stellen Sie sicher, dass die Option **Erweiterte Funktionen anzeigen** aktiviert ist.
3. Navigieren Sie zum Benutzer **WLC-admin**, und klicken Sie mit der rechten Maustaste darauf. Wählen Sie **Eigenschaften** aus dem Kontextmenü, wie im Bild dargestellt. Dieser Benutzer ist mit dem Vornamen **WLC-admin** gekennzeichnet.

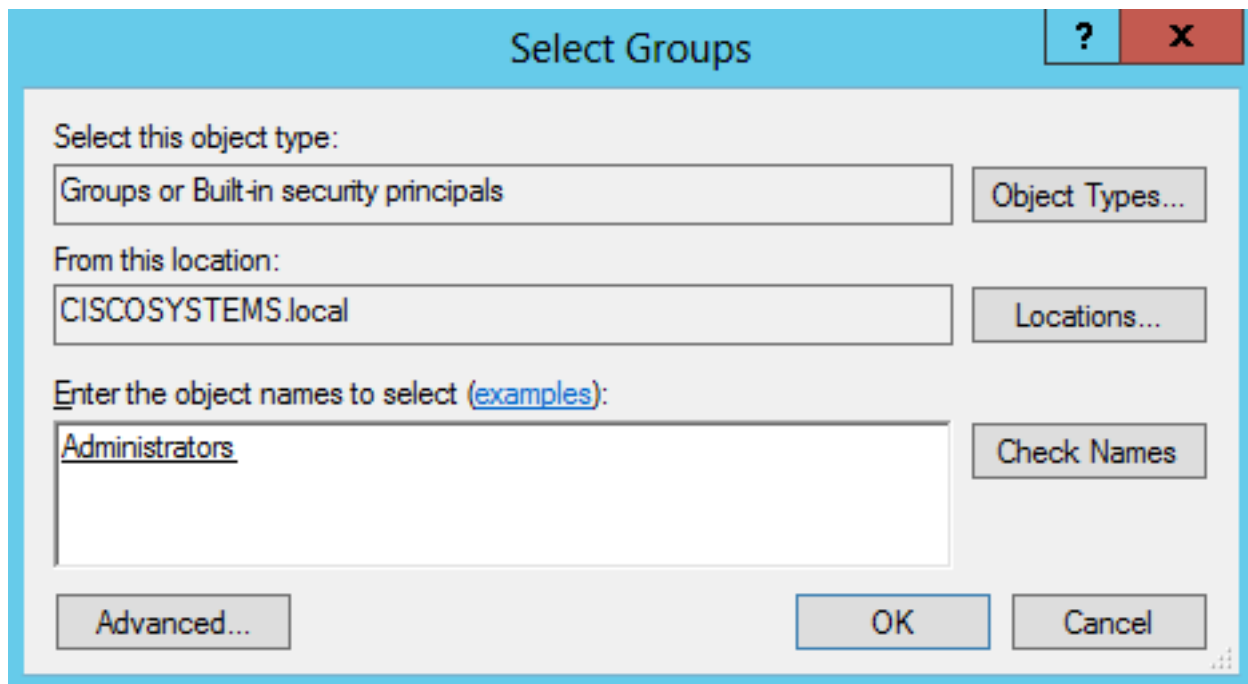


4. Klicken Sie auf die Registerkarte Mitglied von, wie in der Abbildung dargestellt:



::

5. Klicken Sie auf **Hinzufügen**. Geben Sie im daraufhin geöffneten Dialogfeld **Administratoren** ein, und klicken Sie auf **OK**, wie in der Abbildung dargestellt:

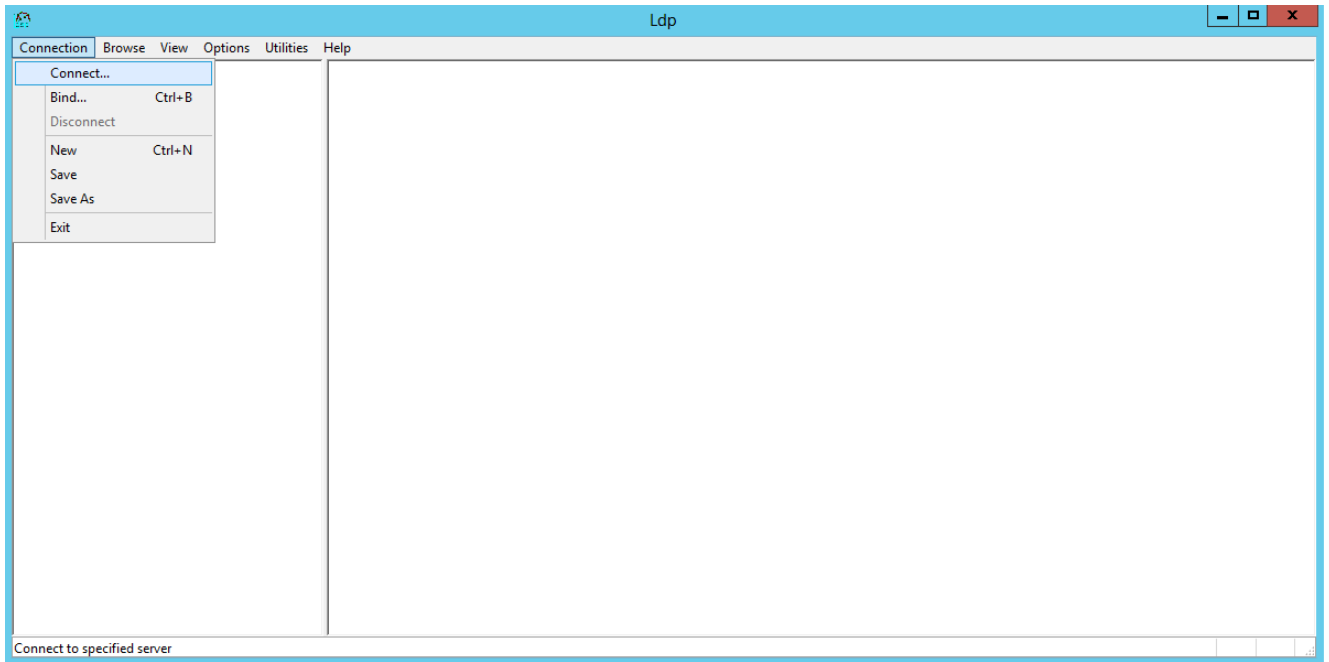


Verwenden von LDP zum Identifizieren der Benutzerattribute

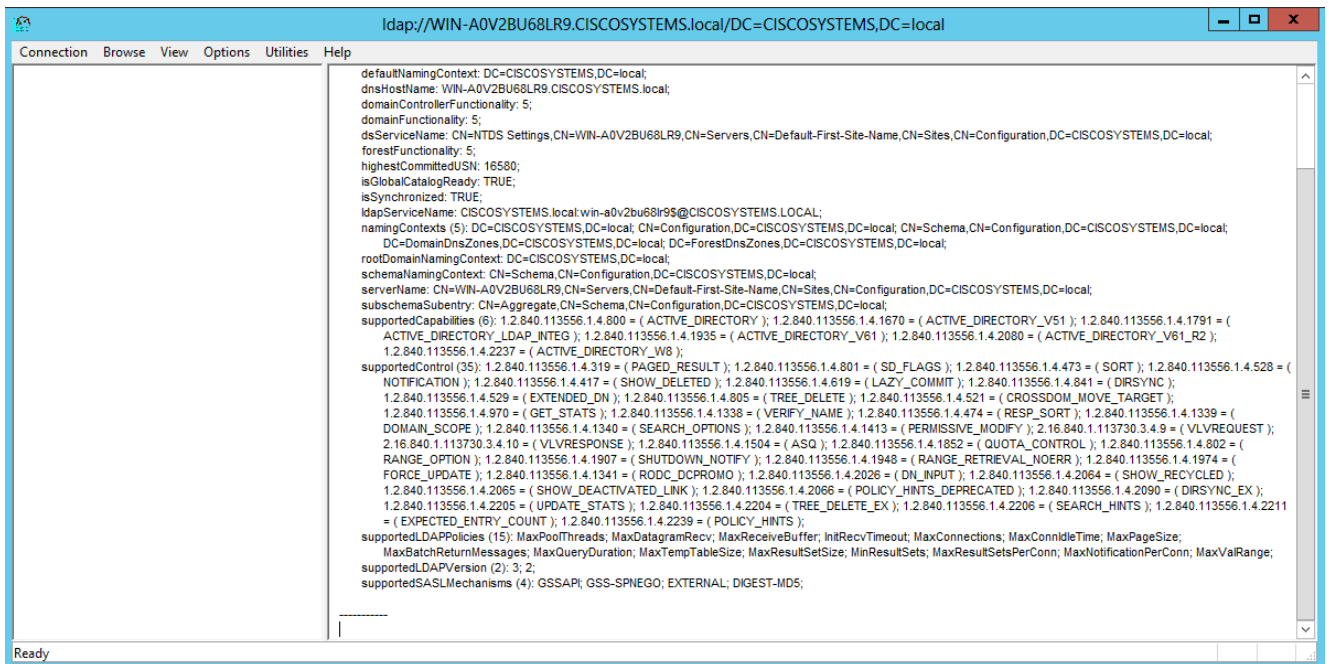
Dieses GUI-Tool ist ein LDAP-Client, mit dem Benutzer Vorgänge wie Verbinden, Binden, Suchen, Ändern, Hinzufügen oder Löschen in einem beliebigen LDAP-kompatiblen Verzeichnis (z. B. Active Directory) ausführen können. LDP wird verwendet, um Objekte anzuzeigen, die zusammen mit ihren Metadaten in Active Directory gespeichert sind, z. B. Sicherheitsbeschreibungen und Replikationsmetadaten.

Das LDP GUI-Tool ist enthalten, wenn Sie die Windows Server 2003 Support Tools von der Produkt-CD installieren. In diesem Abschnitt wird erläutert, wie Sie mit dem LDP-Dienstprogramm die spezifischen Attribute identifizieren, die Benutzer User1 zugeordnet sind. Einige dieser Attribute werden verwendet, um die LDAP-Serverkonfigurationsparameter für den WLC auszufüllen, z. B. Benutzerattribut-Typ und Benutzerobjekttyp.

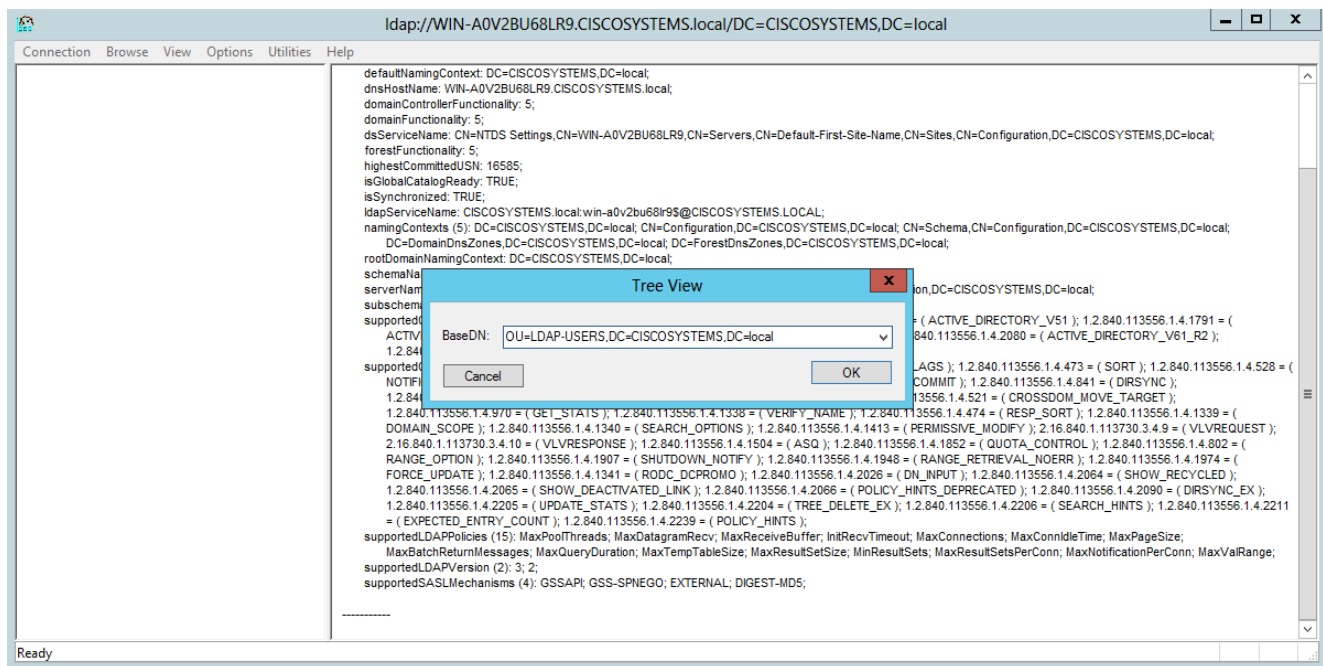
1. Öffnen Sie auf dem Windows 2012-Server (auch auf demselben LDAP-Server) Windows PowerShell, und geben Sie **LDP ein**, um auf den LDP-Browser zuzugreifen..
2. Navigieren Sie im LDP-Hauptfenster zu **Verbindung > Verbinden**, und stellen Sie eine Verbindung mit dem LDAP-Server her, wenn Sie die IP-Adresse des LDAP-Servers eingeben, wie im Bild dargestellt.



3. Wenn Sie mit dem LDAP-Server verbunden sind, wählen Sie im Hauptmenü die Option **Anzeigen**, und klicken Sie auf **Struktur**, wie in der Abbildung dargestellt:



4. Geben Sie im resultierenden Fenster Baumansicht die **BaseDN** des Benutzers ein. In diesem Beispiel befindet sich User1 unter der OU "LDAP-USERS" unter der Domäne CISCOSYSTEMS.local. Klicken Sie auf **OK**, wie in der Abbildung dargestellt:



5. Auf der linken Seite des LDP-Browsers wird die gesamte Baumstruktur angezeigt, die unter der angegebenen BaseDN angezeigt wird (OU=LDAP-USERS, dc=CISCOYSTEMS, dc=local). Erweitern Sie die Struktur, um den Benutzer User1 zu suchen. Dieser Benutzer kann mit dem CN-Wert identifiziert werden, der den Vornamen des Benutzers darstellt. In diesem Beispiel ist dies CN=User1. Doppelklicken Sie auf **CN=User1**. Im rechten Fensterbereich des LDP-Browsers zeigt LDP alle mit User1 verknüpften Attribute an, wie in der Abbildung dargestellt:



6. Wenn Sie den WLC für den LDAP-Server konfigurieren, geben Sie im Feld *Benutzerattribut* den Namen des Attributs in den Benutzerdatensatz ein, der den Benutzernamen enthält. Aus dieser LDP-Ausgabe geht hervor, dass sAMAccountName ein Attribut ist, das den Benutzernamen "User1" enthält. Geben Sie daher das Attribut sAMAccountName ein, das dem Feld "User Attribute" auf dem WLC entspricht.
7. Wenn Sie den WLC für den LDAP-Server konfigurieren, geben Sie im Feld *User Object Type* (*Benutzerobjekttyp*) den Wert des LDAP objectType-Attributs ein, das den Datensatz als Benutzer identifiziert. Benutzerdatensätze verfügen häufig über mehrere Werte für das

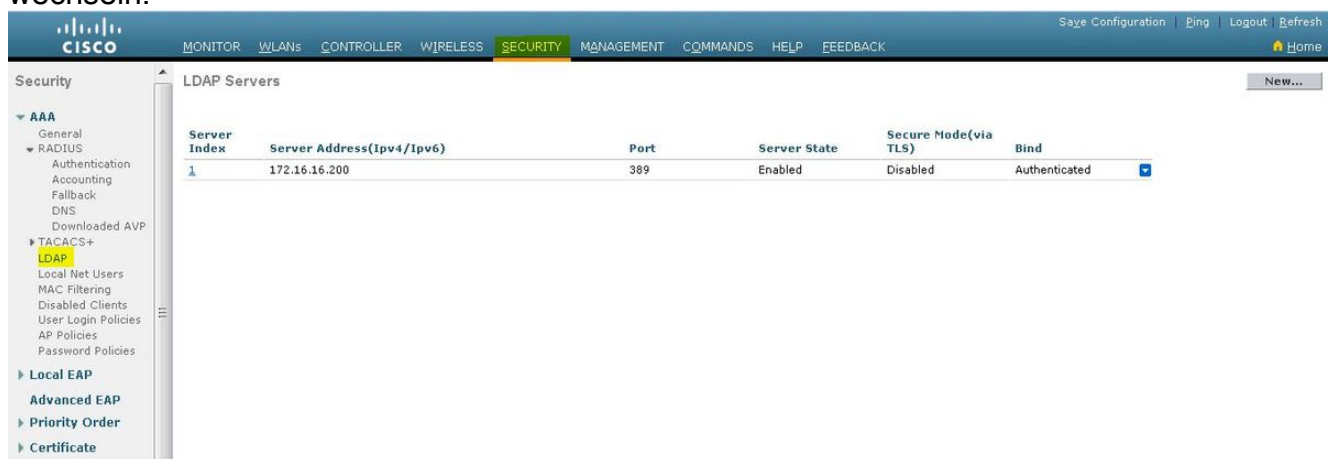
objectType-Attribut, von denen einige für den Benutzer eindeutig sind und von denen einige für andere Objekttypen freigegeben sind. In der LDP-Ausgabe ist CN=Person ein Wert, der den Datensatz als Benutzer identifiziert. Geben Sie **Person** also als Attribut "User Object Type" auf dem WLC an. Im nächsten Schritt wird der WLC für den LDAP-Server konfiguriert.

WLC für LDAP-Server konfigurieren

Nachdem der LDAP-Server konfiguriert wurde, besteht der nächste Schritt darin, den WLC mit Details zum LDAP-Server zu konfigurieren. Führen Sie in der WLC-Benutzeroberfläche die folgenden Schritte aus:

Hinweis: In diesem Dokument wird davon ausgegangen, dass der WLC für den Basisbetrieb konfiguriert ist und dass die LAPs beim WLC registriert sind. Wenn Sie ein neuer Benutzer sind, der den WLC für den Basisbetrieb mit LAPs einrichten möchte, finden Sie weitere Informationen unter [Lightweight AP \(LAP\) Registration to a Wireless LAN Controller \(WLC\)](#).

1. Wählen Sie auf der Seite Sicherheit des WLC im linken Aufgabenbereich **AAA > LDAP** aus, um zur LDAP-Serverkonfigurationsseite zu wechseln.



The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'SECURITY' tab is active. On the left, the 'AAA' menu is expanded to 'LDAP'. The main content area displays a table titled 'LDAP Servers' with the following data:

| Server Index | Server Address(Ipv4/Ipv6) | Port | Server State | Secure Mode(via TLS) | Bind |
|--------------|---------------------------|------|--------------|----------------------|---------------|
| 1 | 172.16.16.200 | 389 | Enabled | Disabled | Authenticated |

Um einen LDAP-Server hinzuzufügen, klicken Sie auf **Neu**. Die Seite LDAP-Server > Neu wird angezeigt.

2. Geben Sie auf der Seite "LDAP Servers Edit" (LDAP-Server bearbeiten) Details zum LDAP-Server an, z. B. die IP-Adresse des LDAP-Servers, die Portnummer, den Status Enable Server usw. Wählen Sie im Dropdown-Feld "Serverindex (Priorität)" eine Zahl aus, um die Prioritätsreihenfolge dieses Servers in Bezug auf andere konfigurierte LDAP-Server anzugeben. Sie können bis zu siebzehn Server konfigurieren. Wenn der Controller den ersten Server nicht erreichen kann, versucht er den zweiten Server in der Liste und so weiter. Geben Sie die **IP-Adresse** des LDAP-Servers in das Feld Server-IP-Adresse ein. Geben Sie die **TCP-Portnummer** des LDAP-Servers in das Feld Port Number (Portnummer) ein. Der gültige Bereich liegt zwischen 1 und 65535, und der Standardwert ist 389. Für die einfache Bindung verwenden wir Authentifiziert, für den Benutzernamen "bind", der den Speicherort des WLC-Admin-Benutzers darstellt, der für den Zugriff auf den LDAP-Server und dessen Kennwort verwendet wird. Geben Sie im Feld User Base DN (Benutzerbasis-DN) den **Distinguished Name (DN)** der Unterstruktur des LDAP-Servers ein, der eine Liste aller Benutzer enthält. Beispielsweise ou=Organisationseinheit, .ou=nächste Organisationseinheit und o=corporation.com. Wenn die Struktur, die Benutzer enthält, die Basis-DN ist, geben Sie o=corporation.com oder dc=corporation, dc=com ein. In diesem

Beispiel befindet sich der Benutzer unter der Organisationseinheit (OU) LDAP-USERS, die wiederum als Teil der Lab.Wireless-Domäne erstellt wird. Der Basis-DN des Benutzers muss auf den vollständigen Pfad verweisen, in dem sich die Benutzerinformationen (Benutzeranmeldeinformationen gemäß der EAP-FAST-Authentifizierungsmethode) befinden. In diesem Beispiel befindet sich der Benutzer unter der Basis-DN OU=LDAP-USERS, DC=CISCOYSTEMS, DC=local. Geben Sie im Feld Benutzerattribut den Namen des Attributs in den Benutzerdatensatz ein, der den Benutzernamen enthält. Geben Sie im Feld User Object Type (Benutzerobjekttyp) den Wert des LDAP objectType-Attributs ein, das den Datensatz als Benutzer identifiziert. Benutzerdatensätze enthalten häufig mehrere Werte für das objectType-Attribut, von denen einige für den Benutzer eindeutig sind und von denen einige für andere Objekttypen freigegeben sind. Sie können den Wert dieser beiden Felder vom Verzeichnisserver mit dem LDAP-Browserdienstprogramm abrufen, das Teil der Windows 2012-Supporttools ist. Dieses Microsoft LDAP-Browsertool heißt LDP. Mithilfe dieses Tools können Sie die Felder Benutzerbasis-DN, Benutzerattribut und Benutzerobjekttyp dieses Benutzers kennen. Ausführliche Informationen zur Verwendung von LDP zum Erkennen dieser benutzerspezifischen Attribute finden Sie im Abschnitt *Using LDP to Identify the User Attributes (Verwenden von LDP zum Identifizieren von Benutzerattributen)* dieses Dokuments. Geben Sie im Feld Server Timeout (Serverzeitüberschreitung) die Anzahl der Sekunden zwischen erneuten Übertragungen ein. Der gültige Bereich liegt zwischen 2 und 30 Sekunden, und der Standardwert ist 2 Sekunden. Aktivieren Sie das Kontrollkästchen **Serverstatus aktivieren**, um diesen LDAP-Server zu aktivieren, oder deaktivieren Sie ihn, um ihn zu deaktivieren. Der Standardwert ist deaktiviert. Klicken Sie auf **Anwenden**, um die Änderungen zu übernehmen. Dies ist ein Beispiel, das bereits mit diesen Informationen konfiguriert

wurde:

The screenshot shows the Cisco WLC configuration interface for an LDAP server. The page title is "LDAP Servers > Edit". The configuration details are as follows:

| | |
|---------------------------|--|
| Server Index | 1 |
| Server Address(Ipv4/Ipv6) | 172.16.16.200 |
| Port Number | 389 |
| Simple Bind | Authenticated |
| Bind Username | CN=WLC-ADMIN,CN=Users,DC=CISCOYSTEMS,E |
| Bind Password | ••• |
| Confirm Bind Password | ••• |
| User Base DN | CN=Users,DC=CISCOYSTEMS,DC=LOCAL |
| User Attribute | sAMAccountName |
| User Object Type | Person |
| Secure Mode(via TLS) | Disabled |
| Server Timeout | 2 seconds |
| Enable Server Status | Enabled |

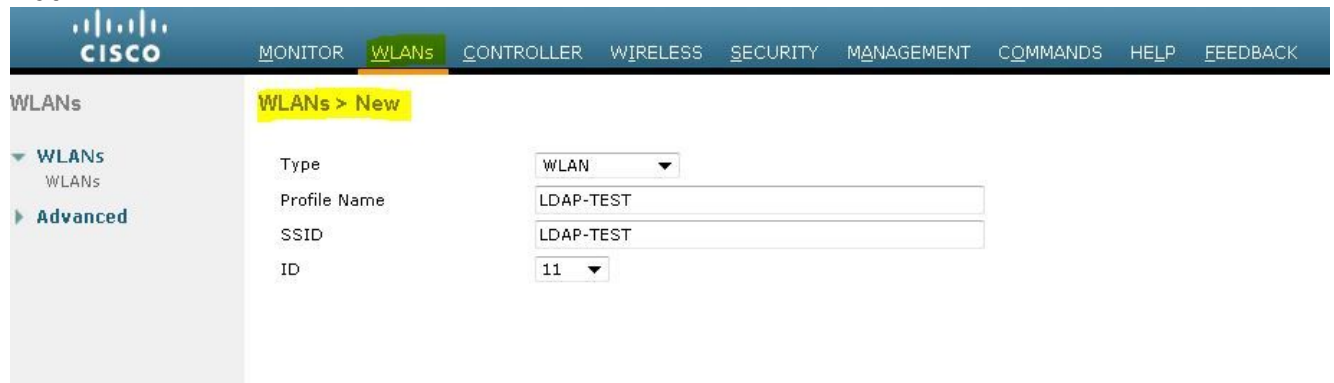
3. Nachdem nun Details zum LDAP-Server auf dem WLC konfiguriert sind, besteht der nächste Schritt darin, ein WLAN für die Webauthentifizierung zu konfigurieren.

WLAN für die Webauthentifizierung konfigurieren

Der erste Schritt besteht darin, ein WLAN für die Benutzer zu erstellen. Führen Sie diese Schritte aus:

1. Klicken Sie in der Controller-GUI auf **WLANs**, um ein WLAN zu erstellen. Das Fenster WLANs wird angezeigt. In diesem Fenster werden die auf dem Controller konfigurierten WLANs aufgeführt.
2. Klicken Sie auf **Neu**, um ein neues WLAN zu konfigurieren. In diesem Beispiel heißt das

WLAN Web-Auth.

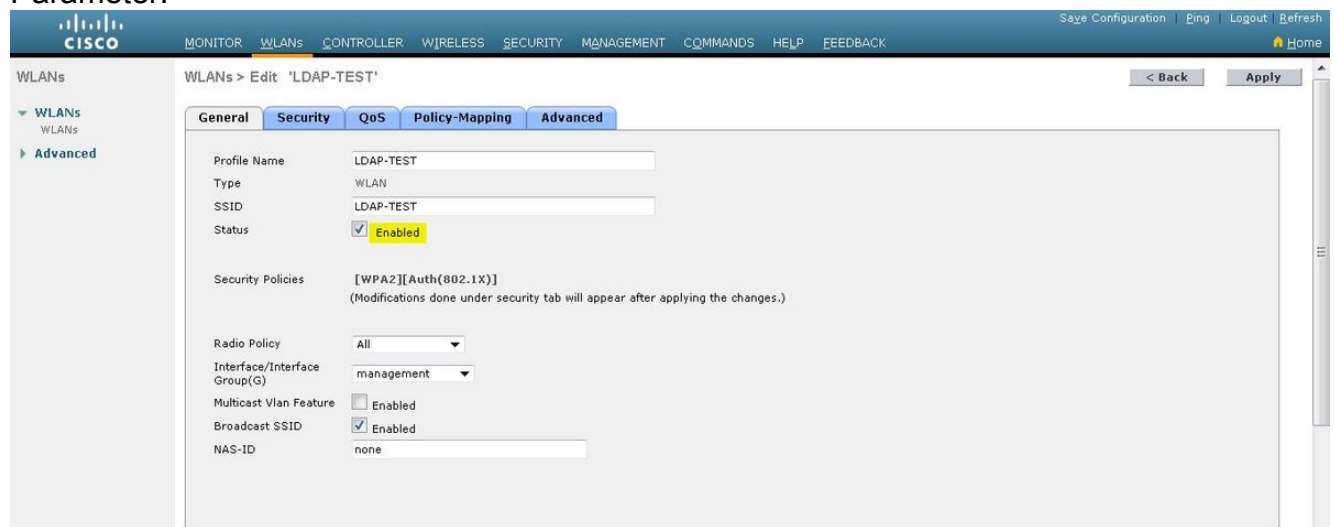


The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows 'WLANs' with a sub-menu 'Advanced'. The main content area is titled 'WLANs > New' and contains the following fields:

| | |
|--------------|-----------|
| Type | WLAN |
| Profile Name | LDAP-TEST |
| SSID | LDAP-TEST |
| ID | 11 |

3. Klicken Sie auf **Apply** (Anwenden).

4. Definieren Sie im Fenster WLAN > Edit (WLAN > Bearbeiten) die WLAN-spezifischen Parameter.

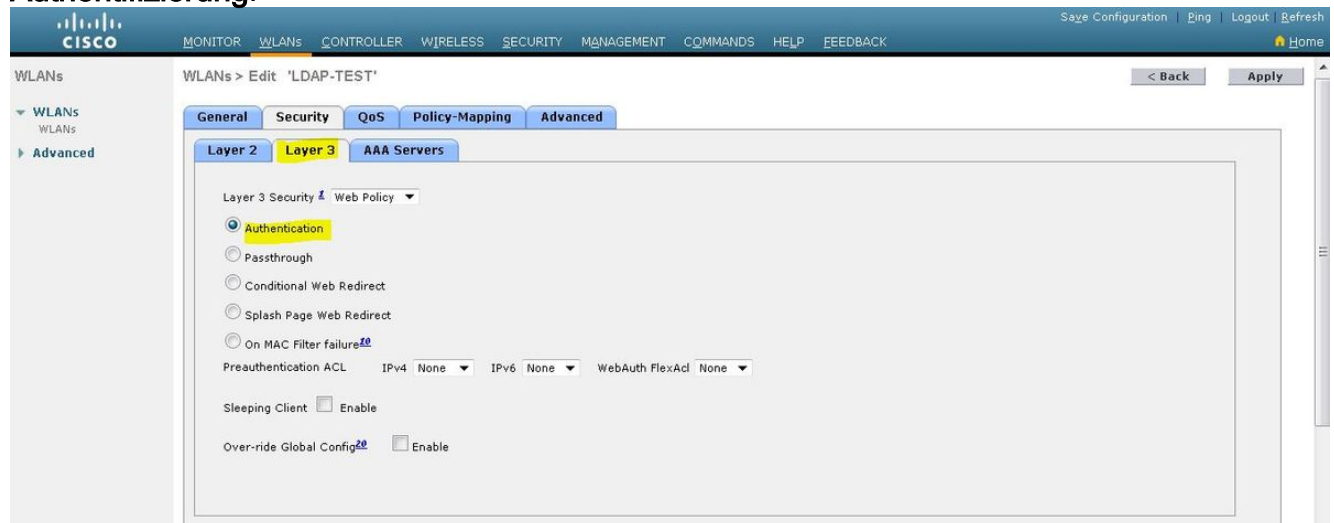


The screenshot shows the Cisco WLAN configuration interface for editing the 'LDAP-TEST' WLAN. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', 'FEEDBACK', 'Save Configuration', 'Eng', 'Logout', 'Refresh', and 'Home'. The left sidebar shows 'WLANs' with a sub-menu 'Advanced'. The main content area is titled 'WLANs > Edit 'LDAP-TEST'' and contains the following fields:

| | |
|------------------------------|---|
| Profile Name | LDAP-TEST |
| Type | WLAN |
| SSID | LDAP-TEST |
| Status | <input checked="" type="checkbox"/> Enabled |
| Security Policies | [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) |
| Radio Policy | All |
| Interface/Interface Group(G) | management |
| Multicast Vlan Feature | <input type="checkbox"/> Enabled |
| Broadcast SSID | <input checked="" type="checkbox"/> Enabled |
| NAS-ID | none |

Aktivieren Sie das Kontrollkästchen Status, um das WLAN zu aktivieren. Wählen Sie im Feld "Interface Name" (Schnittstellennamen) die entsprechende Schnittstelle für das WLAN aus. In diesem Beispiel wird die Verwaltungsschnittstelle zugeordnet, die mit der WLAN-Web-Auth verbunden ist.

5. Klicken Sie auf die Registerkarte **Sicherheit**. Aktivieren Sie im Feld Layer 3-Sicherheit das Kontrollkästchen **Webrichtlinie**, und wählen Sie die Option **Authentifizierung**.



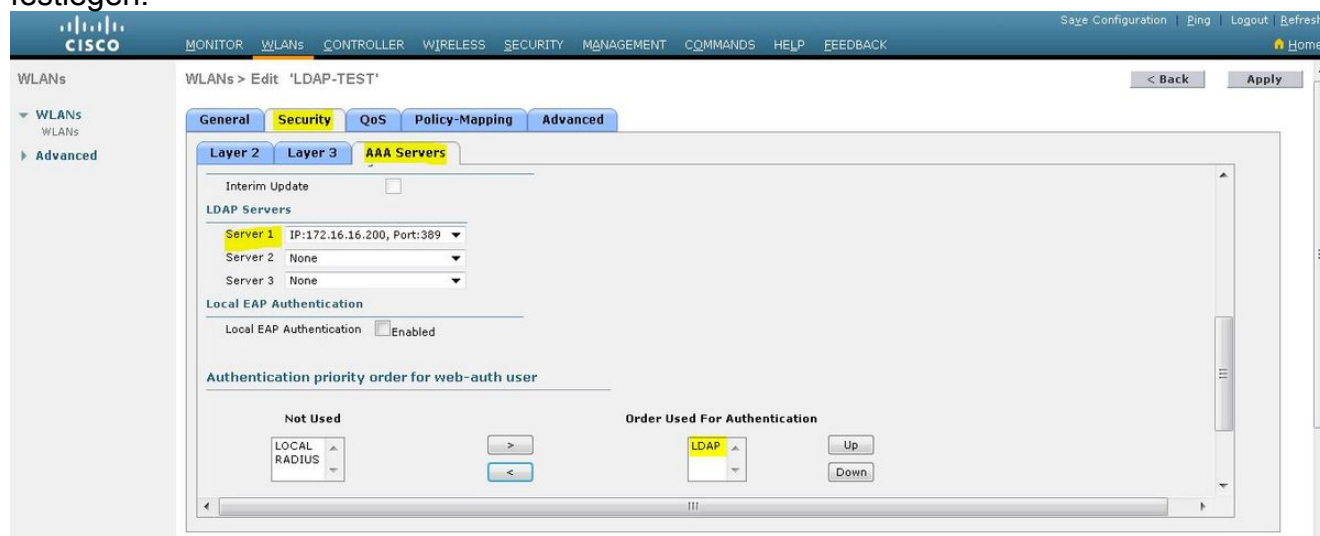
The screenshot shows the Cisco WLAN configuration interface for editing the 'LDAP-TEST' WLAN, specifically the 'Security' tab. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', 'FEEDBACK', 'Save Configuration', 'Ping', 'Logout', 'Refresh', and 'Home'. The left sidebar shows 'WLANs' with a sub-menu 'Advanced'. The main content area is titled 'WLANs > Edit 'LDAP-TEST'' and contains the following fields:

| | |
|--------------------------|--|
| Layer 3 Security | Web Policy |
| Authentication | <input checked="" type="radio"/> |
| Passthrough | <input type="radio"/> |
| Conditional Web Redirect | <input type="radio"/> |
| Splash Page Web Redirect | <input type="radio"/> |
| On MAC Filter failure | <input type="radio"/> |
| Preauthentication ACL | IPv4 None IPv6 None WebAuth FlexAct None |
| Sleeping Client | <input type="checkbox"/> Enable |
| Over-ride Global Config | <input type="checkbox"/> Enable |

Diese Option wird gewählt, da die Wireless-Clients mithilfe der Webauthentifizierung authentifiziert werden. Aktivieren Sie das Kontrollkästchen **Globale Konfiguration**

überschreiben", um die Konfiguration für die WLAN-Webauthentifizierung zu aktivieren. Wählen Sie im Dropdown-Menü Web Auth Type (Web Auth-Typ) den entsprechenden Web-Authentifizierungstyp aus. In diesem Beispiel wird die interne Webauthentifizierung verwendet. **Hinweis:** Die Webauthentifizierung wird für die 802.1x-Authentifizierung nicht unterstützt. Das bedeutet, dass Sie bei der Webauthentifizierung nicht 802.1x oder WPA/WPA2 mit 802.1x als Layer-2-Sicherheit auswählen können. Die Webauthentifizierung wird mit allen anderen Sicherheitsparametern auf Layer 2 unterstützt.

6. Klicken Sie auf die Registerkarte **AAA-Server**. Wählen Sie den konfigurierten LDAP-Server aus dem Dropdown-Menü LDAP-Server aus. Wenn Sie eine lokale Datenbank oder einen RADIUS-Server verwenden, können Sie die Authentifizierungspriorität im Feld *Authentifizierungspriorität für Web-Authentifizierungsbenutzer* festlegen.



7. Klicken Sie auf **Apply** (Anwenden). **Hinweis:** In diesem Beispiel werden keine Layer-2-Sicherheitsmethoden zum Authentifizieren von Benutzern verwendet. Wählen Sie daher im Feld "Layer-2-Sicherheit" die Option **Keine aus**.

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

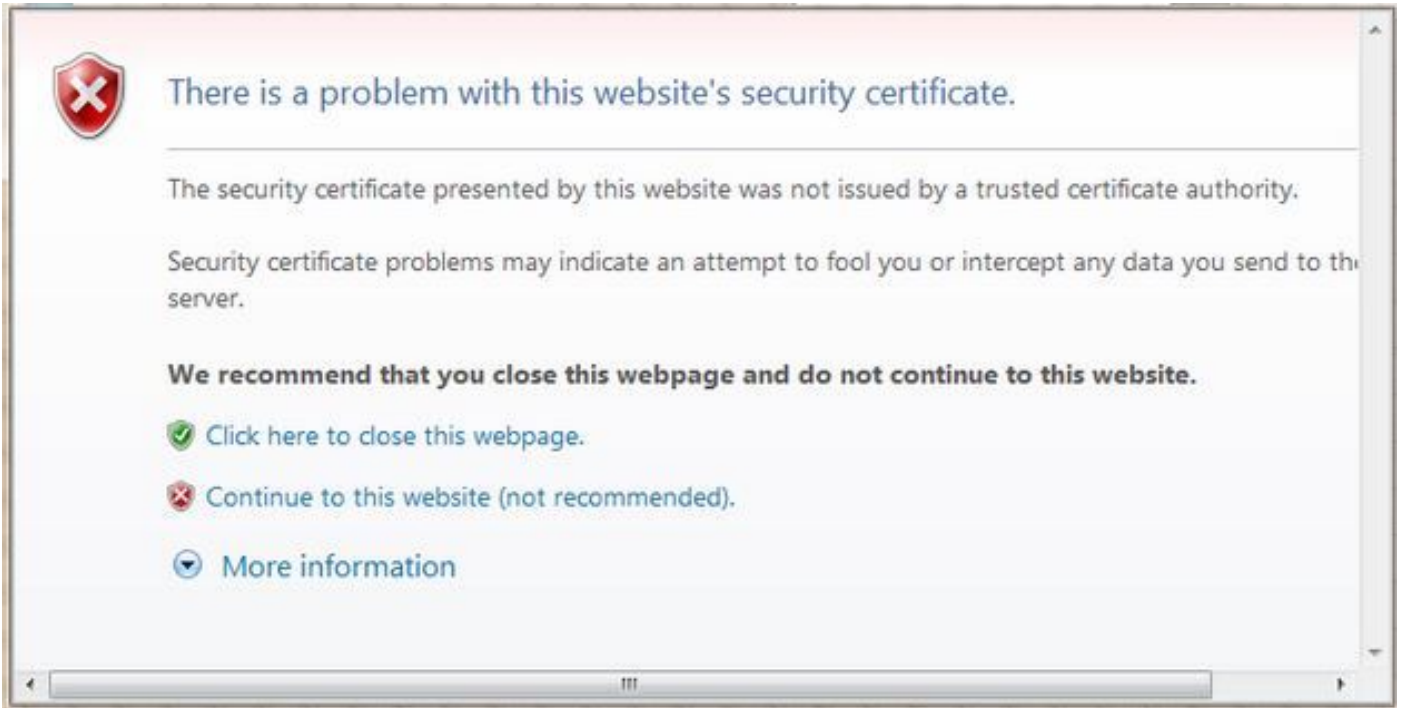
Um diese Konfiguration zu überprüfen, verbinden Sie einen Wireless-Client, und überprüfen Sie, ob die Konfiguration wie erwartet funktioniert.

Der Wireless-Client wird geöffnet, und der Benutzer gibt die URL wie www.yahoo.com in den Webbrowser ein. Da der Benutzer nicht authentifiziert wurde, leitet der WLC den Benutzer an die interne Web-Anmelde-URL um.

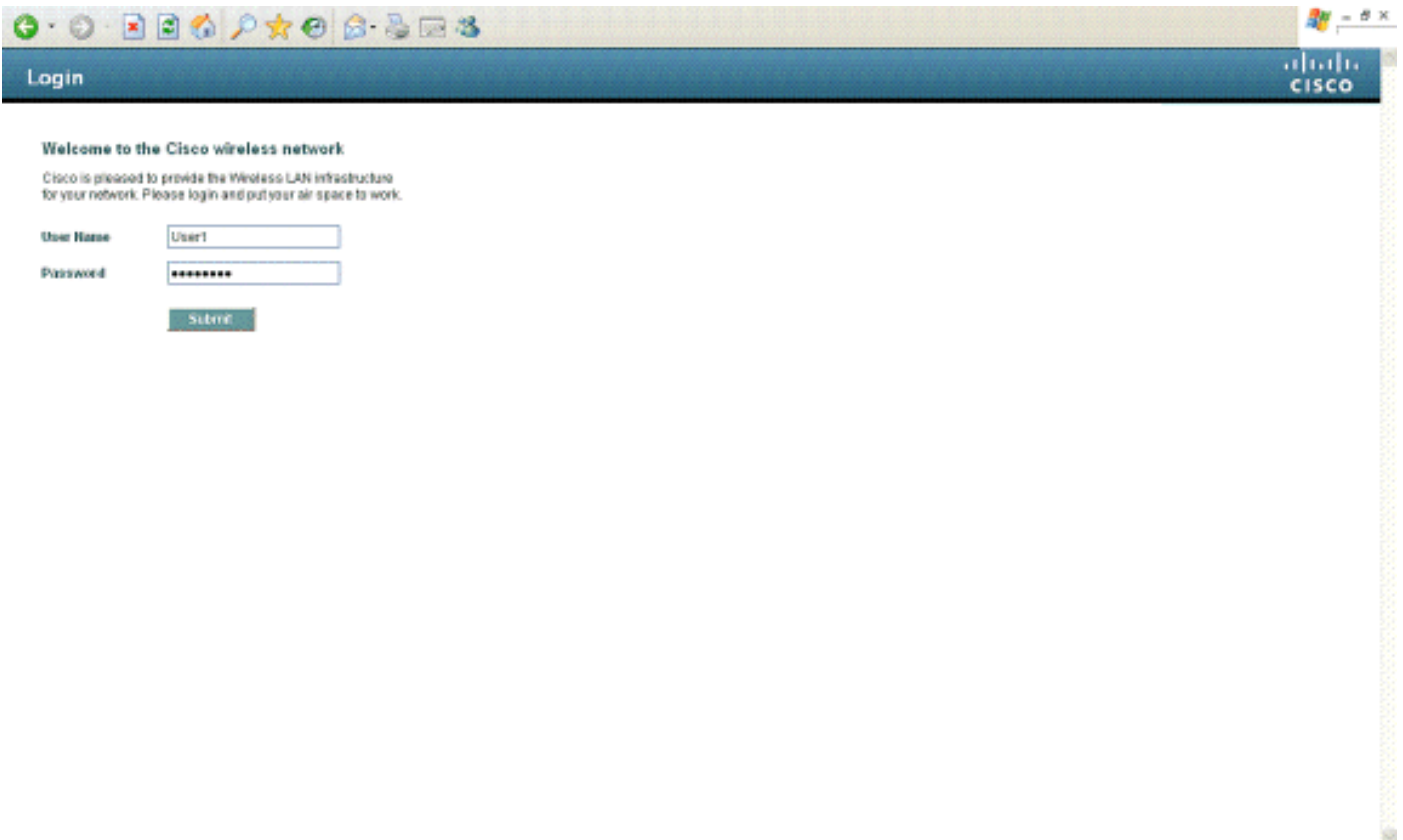
Der Benutzer wird zur Eingabe der Anmeldeinformationen aufgefordert. Nachdem der Benutzer den Benutzernamen und das Kennwort eingegeben hat, nimmt die Anmeldeseite die Eingabe der Benutzeranmeldeinformationen vor und sendet die Anforderung nach dem Absenden an das action_URL-Beispiel <http://1.1.1.1/login.html> des WLC-Webservers zurück. Dieser wird als Eingabeparameter für die Kundenumleitungs-URL bereitgestellt, wobei 1.1.1.1 die virtuelle Schnittstellenadresse auf dem Switch ist.

Der WLC authentifiziert den Benutzer anhand der LDAP-Benutzerdatenbank. Nach erfolgreicher

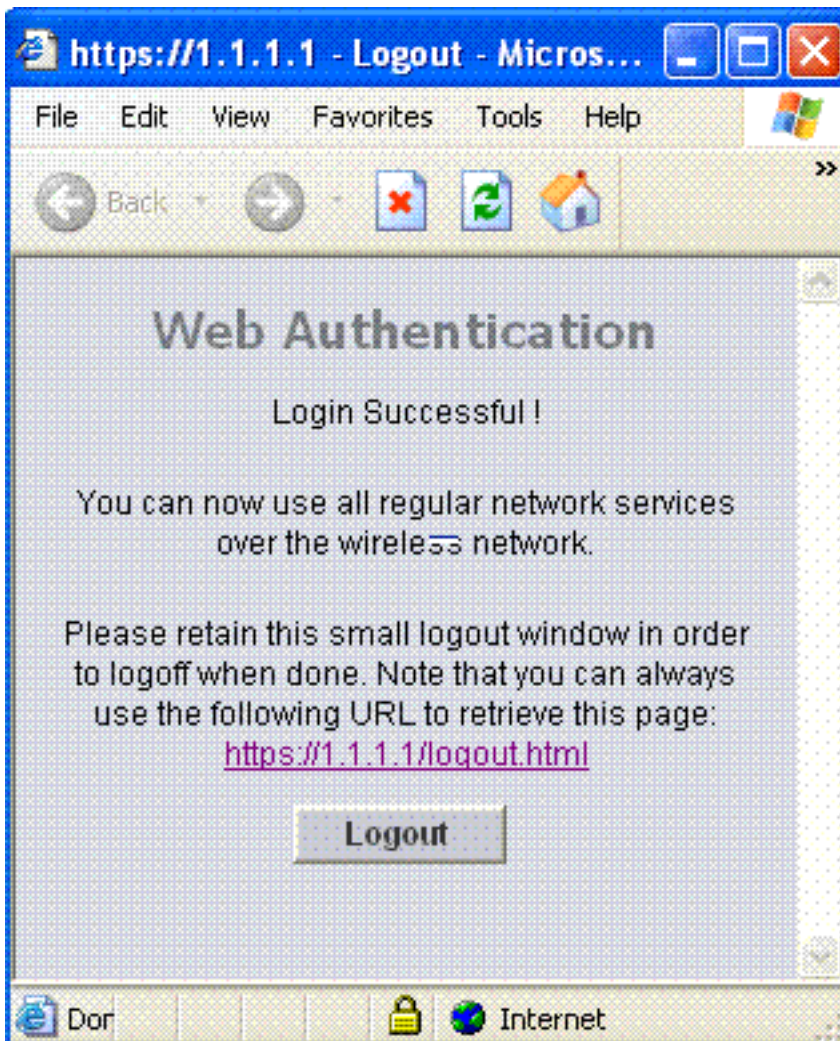
Authentifizierung leitet der WLC-Webserver den Benutzer entweder an die konfigurierte Umleitungs-URL oder an die URL weiter, mit der der Client gestartet wurde, z. B. www.yahoo.com



The image shows a security warning dialog box from a web browser. At the top left is a red shield icon with a white 'X'. The main heading reads "There is a problem with this website's security certificate." Below this, the text explains: "The security certificate presented by this website was not issued by a trusted certificate authority. Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server." A bold recommendation follows: "We recommend that you close this webpage and do not continue to this website." Three options are listed: "Click here to close this webpage." (with a green checkmark icon), "Continue to this website (not recommended)." (with a red 'X' icon), and "More information" (with a blue downward arrow icon). The dialog box has a scroll bar on the right and a close button in the top right corner.



The image shows a login page for a Cisco wireless network. The page has a dark blue header with the word "Login" on the left and the Cisco logo on the right. Below the header, the text reads: "Welcome to the Cisco wireless network. Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work." There are two input fields: "User Name" with the text "User1" and "Password" with a masked password of "*****". A green "Submit" button is located below the password field. The page is displayed in a browser window with a taskbar at the bottom showing various application icons.



Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Verwenden Sie die folgenden Befehle, um eine Fehlerbehebung für Ihre Konfiguration durchzuführen:

- **debug mac addr <client-MAC-Adresse xx:xx:xx:xx:xx:xx>**
- **debug aaa all enable**
- **debug pem state enable**
- **debug pem events enable**
- **debug dhcp message enable**
- **debug dhcp packet enable**

Dies ist eine Beispielausgabe der Befehle **debug mac addr cc:fa:00:f7:32:35**

debug aaa ldap enable

```
(Cisco_Controller) >*pemReceiveTask: Dec 24 03:45:23.089: cc:fa:00:f7:32:35 Sent an XID frame
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Processing assoc-req
station:cc:fa:00:f7:32:35 AP:00:23:eb:e5:04:10-01 thread:18ec9330
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Association received from mobile on
BSSID 00:23:eb:e5:04:1f AP AP1142-1
```

*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Global 200 Clients are allowed to AP radio

*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Max Client Trap Threshold: 0 cur: 1

*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Rf profile 600 Clients are allowed to AP wlan

*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 override for default ap group, marking intgrp NULL

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Interface policy on Mobile, role Local. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 16

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Re-applying interface policy for client

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Changing IPv4 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2699)

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Changing IPv6 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2720)

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfApplyWlanPolicy: Apply WLAN Policy over PMIPv6 Client Mobility Type, Tunnel User - 0

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6246 setting Central switched to TRUE

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6249 apVapId = 1 and Split Acl Id = 65535

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying site-specific Local Bridging override for station cc:fa:00:f7:32:35 - vapId 1, site 'default-group', interface 'management'

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Local Bridging Interface Policy for station cc:fa:00:f7:32:35 - vlan 16, interface id 0, interface 'management'

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE statusCode is 0 and status is 0

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE ssid_done_flag is 0 finish_flag is 0

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 STA - rates (3): 24 164 48 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 suppRates statusCode is 0 and gotSuppRatesElement is 1

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 AID 2 in Assoc Req from flex AP 00:23:eb:e5:04:10 is same as in mscb cc:fa:00:f7:32:35

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfMslxStateDec

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Change state to START (0) last state WEBAUTH_REQD (8)

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 pemApfAddMobileStation2: APF_MS_PEM_WAIT_L2_AUTH_COMPLETE = 0.

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Initializing policy

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Change state to AUTHCHECK (2) last state START (0)

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) last state AUTHCHECK (2)

*pemReceiveTask: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 Removed NPU entry.

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Not Using WMM Compliance code qosCap 00

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:23:eb:e5:04:10 vapId 1 apVapId 1 flex-acl-name:

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4) Change state to WEBAUTH_REQD (8) last state L2AUTHCOMPLETE (4)

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) pemApfAddMobileStation2 3802, Adding TMP rule

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Adding Fast Path rule

```
type = Airespace AP Client - ACL passthru
on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0
IPv4 ACL I
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, IntfId = 0 Local Bridging Vlan =
16, Local Bridging intf id = 0
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit: AppID = 0 ,AppAction = 4, AppToken = 15206 AverageRate =
0, BurstRate = 0
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit: AppID = 0 ,AppAction = 4, AppToken = 15206 AverageRate =
0, BurstRate = 0
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit: AppID = 0 ,AppAction = 4, AppToken = 15206 AverageRate =
0, BurstRate = 0
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
pemApfAddMobileStation2 3911, Adding TMP rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
Replacing Fast Path rule
type = Airespace AP Client - ACL passthru
on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0
IPv4 AC
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, IntfId = 0 Local Bridging Vlan =
16, Local Bridging intf id = 0
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit: AppID = 0 ,AppAction = 4, AppToken = 15206 AverageRate =
0, BurstRate = 0
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit: AppID = 0 ,AppAction = 4, AppToken = 15206 AverageRate =
0, BurstRate = 0
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit: AppID = 0 ,AppAction = 4, AppToken = 15206 AverageRate =
0, BurstRate = 0
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2 (apf_policy.c:359)
Changing state for mobile cc:fa:00:f7:32:35 on AP 00:23:eb:e5:04:10 from Associated to
Associated
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2:session timeout
forstation cc:fa:00:f7:32:35 - Session Tout 1800, apfMsTimeOut '1800' and sessionTimerRunning
flag is 1
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Scheduling deletion of Mobile Station:
(callerId: 49) in 1800 seconds
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Func: apfPemAddUser2, Ms Timeout =
1800, Session Timeout = 1800
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Sending assoc-resp with status 0
station:cc:fa:00:f7:32:35 AP:00:23:eb:e5:04:10-01 on apVapId 1
*apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sending Assoc Response to station on
BSSID 00:23:eb:e5:04:1f (status 0) ApVapId 1 Slot 1
*apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 apfProcessAssocReq (apf_80211.c:10187)
Changing state for mobile cc:fa:00:f7:32:35 on AP 00:23:eb:e5:04:10 from Associated to
Associated
```

*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2, dtlFlags 0x0

*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sent an XID frame

*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2, dtlFlags 0x0

*pemReceiveTask: Dec 24 03:45:43.558: cc:fa:00:f7:32:35 Sent an XID frame

*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len 322,vlan 16, port 1, encap 0xec03, xid 0x62743488)

*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype 0ff:ff:ff:ff:ff:ff

*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block settings:

dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0,
dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25 VLAN: 16

*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25 mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25

*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1)

*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block settings:

dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0,
dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25 VLAN: 16

*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE

*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block settings:

dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16

*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25 mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25

*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1)

*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP transmitting DHCP DISCOVER (1)

*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1

*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 0, flags: 0

*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP chaddr: cc:fa:00:f7:32:35

*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0

*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP siaddr: 0.0.0.0, giaddr: 172.16.16.25

*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block settings:

dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16

*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE

*DHCP Proxy Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP received op BOOTREPLY (2) (len 572,vlan 0, port 0, encap 0x0, xid 0x62743488)

*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418, port 1, vlan 16)

*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP transmitting DHCP OFFER (2)

*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0

*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 0, flags: 0

*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP chaddr: cc:fa:00:f7:32:35

*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP ciaddr: 0.0.0.0, yiaddr: 172.16.16.122

*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0

*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP server id: 1.1.1.1 rcvd server id: 172.16.16.25

*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len 334,vlan 16, port 1, encap 0xec03, xid 0x62743488)


```
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype
Off:ff:ff:ff:ff:ff
*Dhcp Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block
settings:
                dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16
*Dhcp Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25
mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25
*Dhcp Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25
(local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1)
*Dhcp Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP transmitting DHCP REQUEST (3)
*Dhcp Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP op: BOOTREQUEST, htype:
Ethernet, hlen: 6, hops: 1
*Dhcp Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792),
secs: 0, flags: 0
*Dhcp Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP chaddr: cc:fa:00:f7:32:35
*Dhcp Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP ciaddr: 0.0.0.0, yiaddr:
0.0.0.0
*Dhcp Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP siaddr: 0.0.0.0, giaddr:
172.16.16.25
*Dhcp Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP requested ip: 172.16.16.122
*Dhcp Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP server id: 172.16.16.25 rcvd
server id: 1.1.1.1
*Dhcp Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block
settings:
                dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16
*Dhcp Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE
*Dhcp Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP received op BOOTREPLY (2) (len
572,vlan 0, port 0, encap 0x0, xid 0x62743488)
*Dhcp Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP setting server from ACK
(mscb=0x40e64b88 ip=0xac10107a)(server 172.16.16.25, yiaddr 172.16.16.122)
*Dhcp Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418,
port 1, vlan 16)
*Dhcp Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP transmitting DHCP ACK (5)
*Dhcp Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP op: BOOTREPLY, htype: Ethernet,
hlen: 6, hops: 0
*Dhcp Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792),
secs: 0, flags: 0
*Dhcp Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP chaddr: cc:fa:00:f7:32:35
*Dhcp Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP ciaddr: 0.0.0.0, yiaddr:
172.16.16.122
*Dhcp Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP siaddr: 0.0.0.0, giaddr:
0.0.0.0
*Dhcp Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP server id: 1.1.1.1 rcvd server
id: 172.16.16.25
*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created for
mobile, length = 7
*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created in mscb
for mobile, length = 7
*aaaQueueReader: Dec 24 03:46:01.222: AuthenticationRequest: 0x2b6bdc3c

*aaaQueueReader: Dec 24 03:46:01.222: Callback.....0x12088c50
*aaaQueueReader: Dec 24 03:46:01.222: protocolType.....0x00000002
*aaaQueueReader: Dec 24 03:46:01.222:
proxyState.....CC:FA:00:F7:32:35-00:00
*aaaQueueReader: Dec 24 03:46:01.222: Packet contains 15 AVPs (not shown)
*LDAP DB Task 1: Dec 24 03:46:01.222: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE'
(1)
```

*LDAP DB Task 1: Dec 24 03:46:01.222: LDAP server 1 changed state to INIT
*LDAP DB Task 1: Dec 24 03:46:01.223: LDAP_OPT_REFERRALS = -1

*LDAP DB Task 1: Dec 24 03:46:01.223: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success)
*LDAP DB Task 1: Dec 24 03:46:01.225: ldapInitAndBind [1] configured Method Authenticated
lcapi_bind (rc = 0 - Success)
*LDAP DB Task 1: Dec 24 03:46:01.225: LDAP server 1 changed state to CONNECTED
*LDAP DB Task 1: Dec 24 03:46:01.225: disabled LDAP_OPT_REFERRALS

*LDAP DB Task 1: Dec 24 03:46:01.225: LDAP_CLIENT: UID Search
(base=CN=Users,DC=CISCO SYSTEMS,DC=local, pattern=(&(objectclass=Person)(sAMAccountName=User1)))
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: ldap_search_ext_s returns 0 -5
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Returned 2 msgs including 0 references
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Returned msg 1 type 0x64
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Received 1 attributes in search entry msg
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Returned msg 2 type 0x65
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT : No matched DN
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT : Check result error 0 rc 1013
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Received no referrals in search result msg
*LDAP DB Task 1: Dec 24 03:46:01.226: ldapAuthRequest [1] 172.16.16.200 - 389 called lcapi_query
base="CN=Users,DC=CISCO SYSTEMS,DC=local" type="Person" attr="sAMAccountName" user="User1" (rc =
0 - Success)
*LDAP DB Task 1: Dec 24 03:46:01.226: Attempting user bind with username
CN=User1,CN=Users,DC=CISCO SYSTEMS,DC=local
*LDAP DB Task 1: Dec 24 03:46:01.228: LDAP ATTR> dn = CN=User1,CN=Users,DC=CISCO SYSTEMS,DC=local
(size 45)
*LDAP DB Task 1: Dec 24 03:46:01.228: Handling LDAP response Success
*LDAP DB Task 1: Dec 24 03:46:01.228: Authenticated bind : Closing the binded session

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Change
state to WEBAUTH_NOL3SEC (14) last state WEBAUTH_REQD (8)

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 apfMsRunStateInc
*LDAP DB Task 1: Dec 24 03:46:01.228: ldapClose [1] called lcapi_close (rc = 0 - Success)
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_NOL3SEC (14)
Change state to RUN (20) last state WEBAUTH_NOL3SEC (14)

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Stopping deletion of Mobile Station:
(callerId: 74)
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Setting Session Timeout to 1800 sec -
starting session timer for the mobile
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Reached
PLUMBFASPATH: from line 6972
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Replacing Fast
Path rule
type = Airespace AP Client
on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255, IPv6 ACL ID
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, IntfId = 0 Local Bridging Vlan = 16, Local
Bridging intf id = 0
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) AVC Ratelimit: AppID = 0 ,AppAction = 4, AppToken = 15206 AverageRate = 0,
BurstRate = 0
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) AVC Ratelimit: AppID = 0 ,AppAction = 4, AppToken = 15206 AverageRate = 0,
BurstRate = 0
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) AVC Ratelimit: AppID = 0 ,AppAction = 4, AppToken = 15206 AverageRate = 0,
BurstRate = 0
*ewmwebWebauth1: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Successfully

plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 1,
dtlFlags 0x0

```
(Cisco_Controller) >show client detail cc:fa:00:f7:32:35
Client MAC Address..... cc:fa:00:f7:32:35
Client Username ..... User1
AP MAC Address..... 00:23:eb:e5:04:10
AP Name..... AP1142-1
AP radio slot Id..... 1
Client State..... Associated
Client User Group..... User1
Client NAC OOB State..... Access
Wireless LAN Id..... 1
Wireless LAN Network Name (SSID)..... LDAP-TEST
Wireless LAN Profile Name..... LDAP-TEST
Hotspot (802.11u)..... Not Supported
BSSID..... 00:23:eb:e5:04:1f
Connected For ..... 37 secs
Channel..... 36
IP Address..... 172.16.16.122
Gateway Address..... 172.16.16.1
Netmask..... 255.255.254.0
Association Id..... 2
Authentication Algorithm..... Open System
Reason Code..... 1
Status Code..... 0
```

```
--More or (q)uit current module or <ctrl-z> to abort
Session Timeout..... 1800
Client CCX version..... No CCX support
QoS Level..... Silver
Avg data Rate..... 0
Burst data Rate..... 0
Avg Real time data Rate..... 0
Burst Real Time data Rate..... 0
802.1P Priority Tag..... disabled
CTS Security Group Tag..... Not Applicable
KTS CAC Capability..... No
Qos Map Capability..... No
WMM Support..... Enabled
  APSD ACs..... BK BE VI VO
Current Rate..... m7
Supported Rates..... 12.0,18.0,24.0
Mobility State..... Local
Mobility Move Count..... 0
Security Policy Completed..... Yes
Policy Manager State..... RUN
Audit Session ID..... ac10101900000005567b69f8
AAA Role Type..... none
Local Policy Applied..... none
IPv4 ACL Name..... none
```

```
--More or (q)uit current module or <ctrl-z> to abort
FlexConnect ACL Applied Status..... Unavailable
IPv4 ACL Applied Status..... Unavailable
IPv6 ACL Name..... none
IPv6 ACL Applied Status..... Unavailable
Layer2 ACL Name..... none
Layer2 ACL Applied Status..... Unavailable
Client Type..... SimpleIP
mDNS Status..... Enabled
mDNS Profile Name..... default-mdns-profile
```

No. of mDNS Services Advertised..... 0
Policy Type..... N/A
Encryption Cipher..... None
Protected Management Frame No
Management Frame Protection..... No
EAP Type..... Unknown
FlexConnect Data Switching..... Central
FlexConnect Dhcp Status..... Central
FlexConnect Vlan Based Central Switching..... No
FlexConnect Authentication..... Central
FlexConnect Central Association..... No
Interface..... management
VLAN..... 16
Quarantine VLAN..... 0

--More or (q)uit current module or <ctrl-z> to abort

Access VLAN..... 16
Local Bridging VLAN..... 16

Client Capabilities:

CF Pollable..... Not implemented
CF Poll Request..... Not implemented
Short Preamble..... Not implemented
PBCC..... Not implemented
Channel Agility..... Not implemented
Listen Interval..... 10
Fast BSS Transition..... Not implemented
11v BSS Transition..... Not implemented

Client Wifi Direct Capabilities:

WFD capable..... No
Manged WFD capable..... No
Cross Connection Capable..... No
Support Concurrent Operation..... No

Fast BSS Transition Details:

Client Statistics:

Number of Bytes Received..... 16853
Number of Bytes Sent..... 31839
Total Number of Bytes Sent..... 31839
Total Number of Bytes Recv..... 16853
Number of Bytes Sent (last 90s)..... 31839

--More or (q)uit current module or <ctrl-z> to abort

Number of Bytes Recv (last 90s)..... 16853
Number of Packets Received..... 146
Number of Packets Sent..... 92
Number of Interim-Update Sent..... 0
Number of EAP Id Request Msg Timeouts..... 0
Number of EAP Id Request Msg Failures..... 0
Number of EAP Request Msg Timeouts..... 0
Number of EAP Request Msg Failures..... 0
Number of EAP Key Msg Timeouts..... 0
Number of EAP Key Msg Failures..... 0
Number of Data Retries..... 2
Number of RTS Retries..... 0
Number of Duplicate Received Packets..... 0
Number of Decrypt Failed Packets..... 0
Number of Mic Failed Packets..... 0
Number of Mic Missing Packets..... 0
Number of RA Packets Dropped..... 0
Number of Policy Errors..... 0
Radio Signal Strength Indicator..... -48 dBm
Signal to Noise Ratio..... 41 dB

Client Rate Limiting Statistics:

Number of Data Packets Received..... 0
Number of Data Rx Packets Dropped..... 0

--More or (q)uit current module or <ctrl-z> to abort

Number of Data Bytes Received..... 0
Number of Data Rx Bytes Dropped..... 0
Number of Realtime Packets Received..... 0
Number of Realtime Rx Packets Dropped..... 0
Number of Realtime Bytes Received..... 0
Number of Realtime Rx Bytes Dropped..... 0
Number of Data Packets Sent..... 0
Number of Data Tx Packets Dropped..... 0
Number of Data Bytes Sent..... 0
Number of Data Tx Bytes Dropped..... 0
Number of Realtime Packets Sent..... 0
Number of Realtime Tx Packets Dropped..... 0
Number of Realtime Bytes Sent..... 0
Number of Realtime Tx Bytes Dropped..... 0

Nearby AP Statistics:

AP1142-1(slot 0)
 antenna0: 25 secs ago..... -37 dBm
 antennal: 25 secs ago..... -37 dBm
AP1142-1(slot 1)
 antenna0: 25 secs ago..... -44 dBm
 antennal: 25 secs ago..... -57 dBm

DNS Server details:

DNS server IP 0.0.0.0

--More or (q)uit current module or <ctrl-z> to abort

DNS server IP 0.0.0.0

Assisted Roaming Prediction List details:

Client Dhcp Required: False

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.