

ワイヤレス LAN コントローラ (WLC) 上での LDAP を使用した Web 認証の設定例

内容

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[表記法](#)

[Web 認証プロセス](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[LDAP サーバの設定](#)

[ドメイン コントローラでのユーザの作成](#)

[OU でのユーザ データベースの作成](#)

[ユーザの LDAP アクセスの設定](#)

[匿名バインド](#)

[Windows 2012 Essentials Serverで匿名バインド機能を有効にする](#)

[ユーザへのANONYMOUS LOGONアクセス権の付与](#)

[OU での List Contents 権限の付与](#)

[認証されたバインド](#)

[WLC-adminへの管理者権限の付与](#)

[LDAP を使用したユーザ属性の確認](#)

[LDAP サーバの WLC の設定](#)

[Web 認証用の WLAN の設定](#)

[確認](#)

[トラブルシュート](#)

はじめに

このドキュメントでは、Web認証用にワイヤレスLANコントローラ(WLC)を設定する方法について説明します。ユーザクレデンシャルを取得してユーザを認証するために、Lightweight Directory Access Protocol(LDAP)サーバをWeb認証用のバックエンドデータベースとして設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Lightweight アクセス ポイント (LAP) および Cisco WLC の設定に関する知識
- Control And Provisioning of Wireless Access Point Protocol(CAPWAP)に関する知識
- Lightweight Directory Access Protocol(LDAP)、Active Directory、およびドメインコントローラのセットアップ方法と設定方法に関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ファームウェア リリース 8.2.100.0 が稼働している Cisco 5508 WLC
- Cisco 1142 シリーズ LAP
- Cisco 802.11a/b/gワイヤレスクライアントアダプタ
- LDAPサーバの役割を実行するMicrosoft Windows 2012 Essentialsサーバ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

表記法

ドキュメント表記の詳細については、『[シスコテクニカルティップスの表記法](#)』を参照してください。

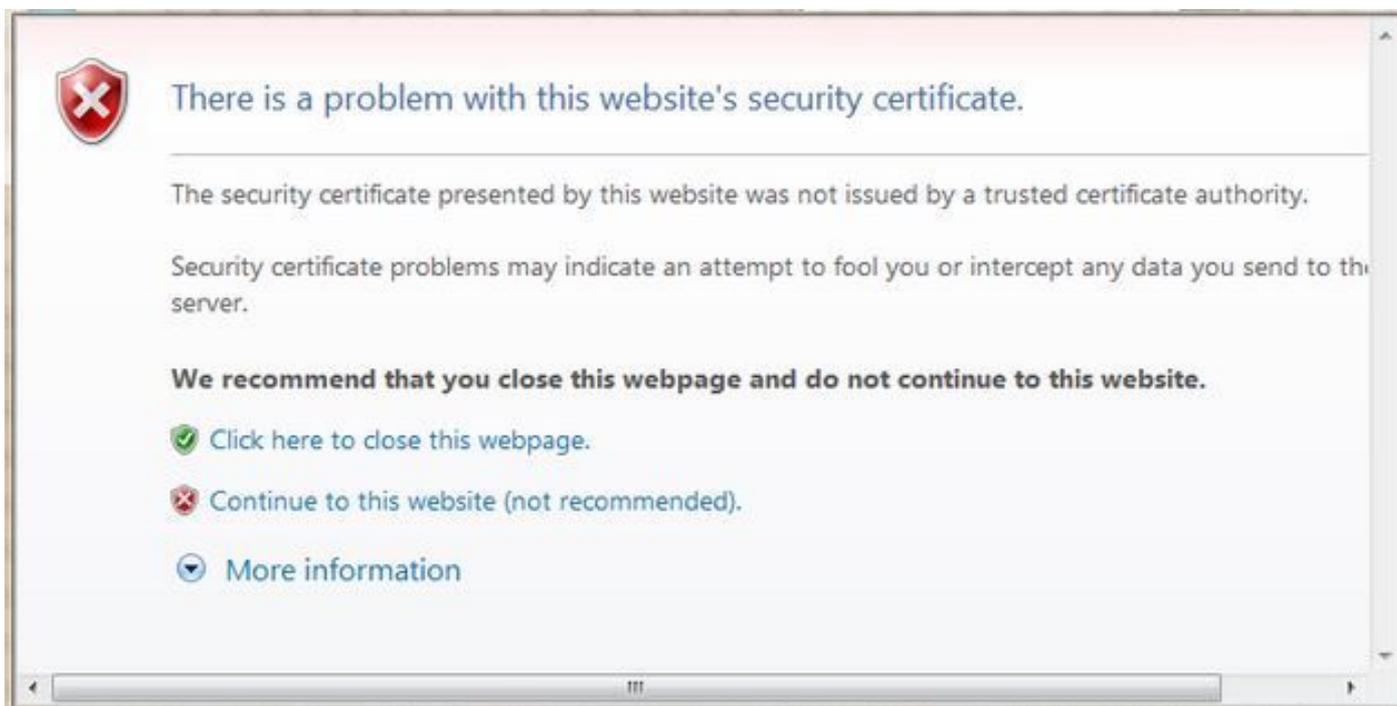
Web 認証プロセス

Web認証は、有効なユーザ名とパスワードが正しく入力されるまで、特定のクライアントからのIPトラフィック (DHCPおよびDNS関連パケットを除く) をコントローラで拒否させるレイヤ3セキュリティ機能です。Web 認証を使用してクライアントを認証する場合は、クライアントごとにユーザ名とパスワードを定義する必要があります。次に、クライアントがワイヤレスLANに参加しようとする、ログインページでプロンプトが表示されたときにユーザ名とパスワードを入力する必要があります。

Web 認証が (レイヤ 3 セキュリティ下で) 有効になっている場合、ユーザが、最初にある URL にアクセスしようとした際に、Web ブラウザにセキュリティ警告が表示されることがあります。

 ヒント：この証明書の警告を削除するには、サードパーティの信頼できる証明書をインストールする方法に関する次のガイドに戻ってください

<http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-certificates-wlc-00.html>



Yesをクリックして続行するか(Firefoxブラウザなどのより正確なContinue to this website (推奨されません))、またはクライアントのブラウザにセキュリティ警告が表示されない場合、Web認証システムは図に示すようにログインページにクライアントをリダイレクトします。

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

Password

Submit

デフォルトのログイン ページには、Cisco ロゴや Cisco 特有のテキストが表示されます。Web 認証システムが次のいずれかを表示するように選択できます。

- デフォルトのログイン ページ
- デフォルトのログイン ページの変更バージョン
- 外部の Web サーバに設定する、カスタマイズされたログイン ページ
- コントローラにダウンロードする、カスタマイズされたログイン ページ

Web認証のログインページで有効なユーザ名とパスワードを入力してSubmitをクリックすると、送信されたクレデンシャル（この場合はLDAP）と、バックエンドデータベースからの正常な認証に基づいて認証されます。その後、Web 認証システムは、ログインに成功したことを示す（ログイン成功）ページを表示し、認証されたクライアントを要求された URL へリダイレクトします。

Web Authentication

Login Successful !

You can now use all regular network services over the wireless network.

Please retain this small logout window in order to logoff when done. Note that you can always use the following URL to retrieve this page:

<https://1.1.1.1/logout.html>

Logout

デフォルトのログイン成功ページには、仮想ゲートウェイアドレス URL(<https://1.1.1.1/logout.html>)へのポインタが含まれます。コントローラの仮想インターフェイスに設定した IP アドレスは、ログイン ページのリダイレクト アドレスとして機能します。

このドキュメントでは、WLC 上の内部 Web ページを Web 認証用に使用する方法を説明します。この例では、LDAPサーバをWeb認証用のバックエンドデータベースとして使用して、ユーザ クレデンシャルを取得し、ユーザを認証します。

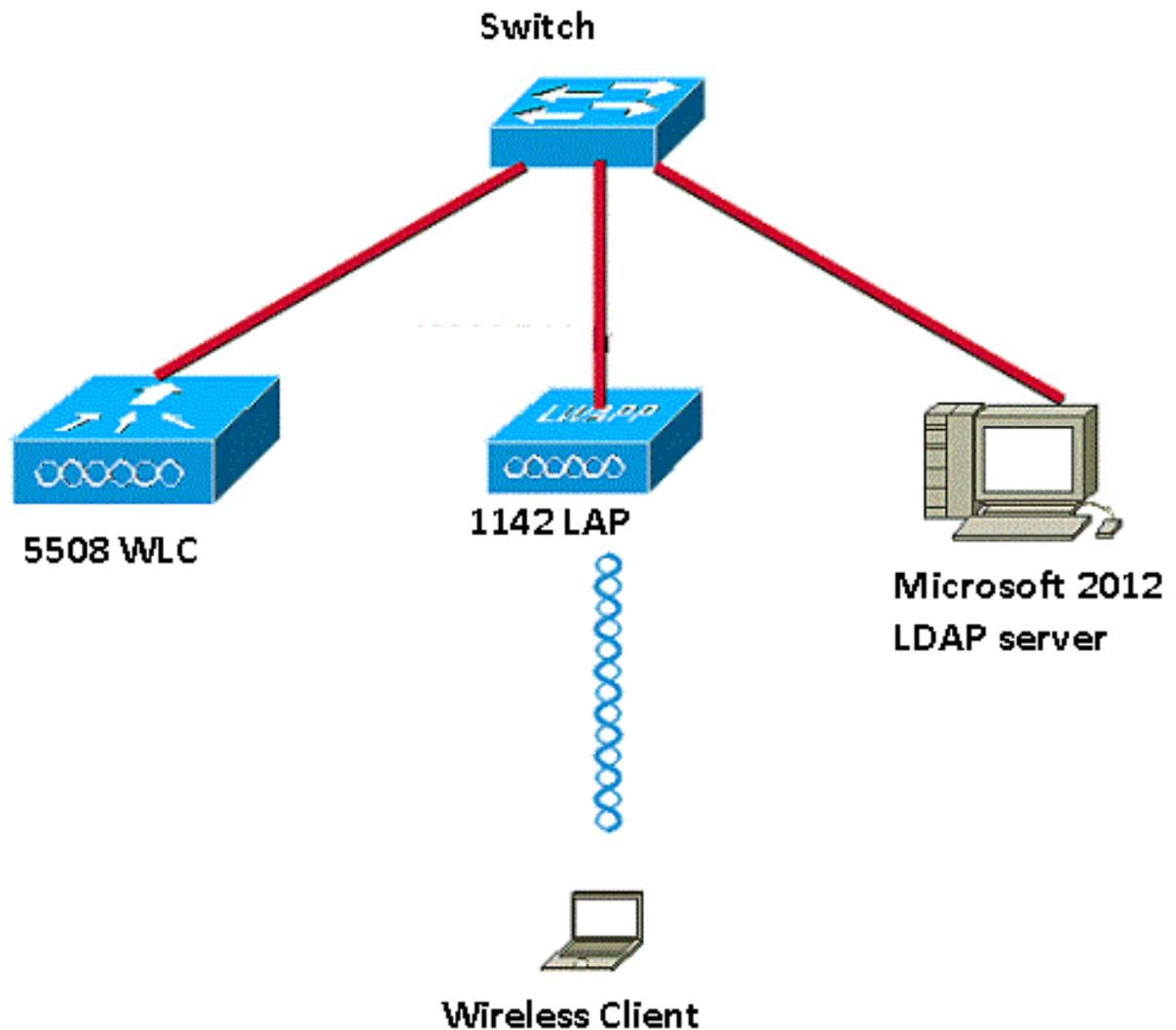
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

 注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool (登録ユーザ専用) を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



コンフィギュレーション

この設定を実装するには、次の作業を実行します。

- [LDAP サーバの設定](#)
- [LDAP サーバの WLC の設定](#)
- [Web 認証用の WLAN の設定](#)

LDAP サーバの設定

最初の手順では、LDAP サーバを設定します。LDAP サーバは、ワイヤレスクライアントのユーザ クレデンシャルを格納するためのバックエンド データベースとして機能します。この例では、LDAPサーバとしてMicrosoft Windows 2012 Essentialsサーバが使用されます。

LDAP サーバを設定する最初の手順として、LDAP サーバでユーザ データベースを作成します。これにより、WLC はユーザ認証時にこのデータベースをクエリできます。

ドメイン コントローラでのユーザの作成

組織単位 (OU) には、PersonProfile のパーソナル エントリへの参照を持つ複数のグループが含まれます。1 人で複数のグループのメンバになることができます。オブジェクト クラスと属性定義はすべて LDAP スキーマのデフォルトです。各グループには、そこに所属する各人への参照 (dn) が含まれます。

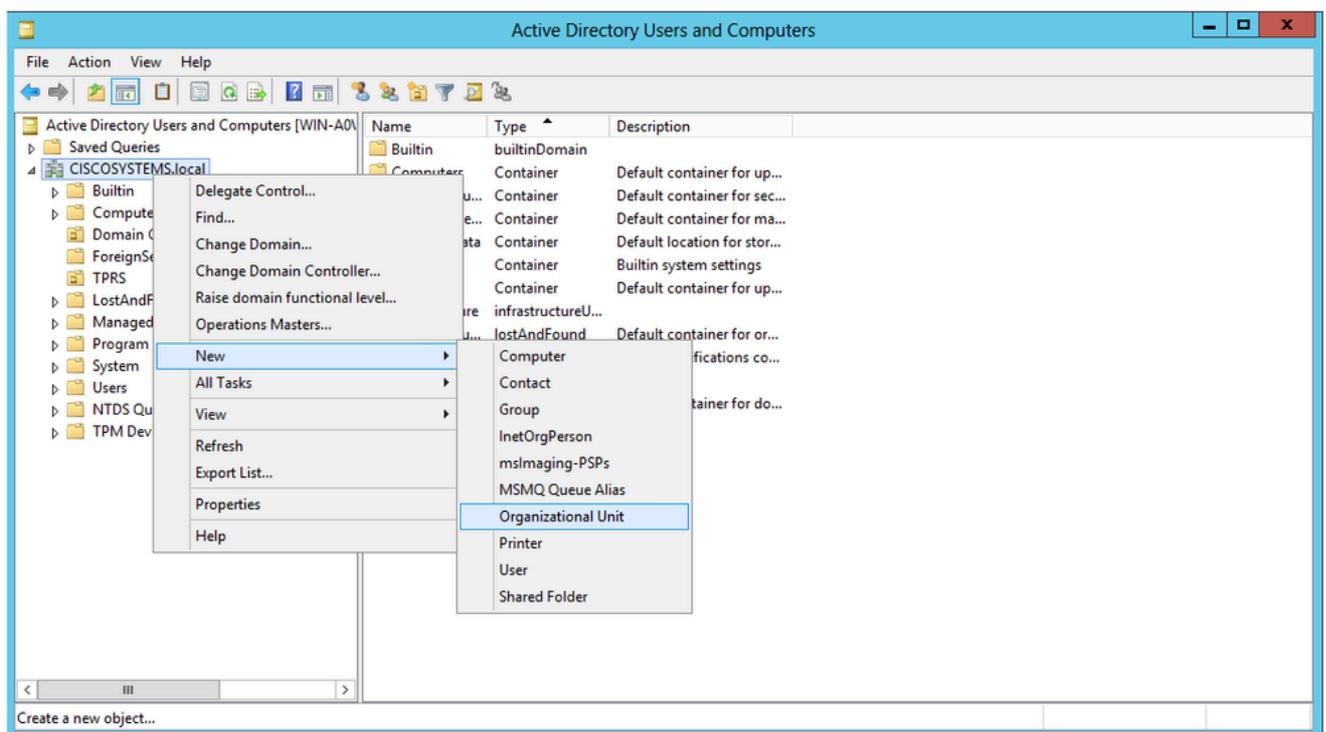
この例では新しい OU LDAP-USERS が作成され、この OU の中にユーザ User1 が作成されました。このユーザに対して LDAP アクセスを設定することで、WLC はユーザ認証でこの LDAP データベースをクエリできます。

この例で使用するドメインはCISCOSYSTEMS.localです。

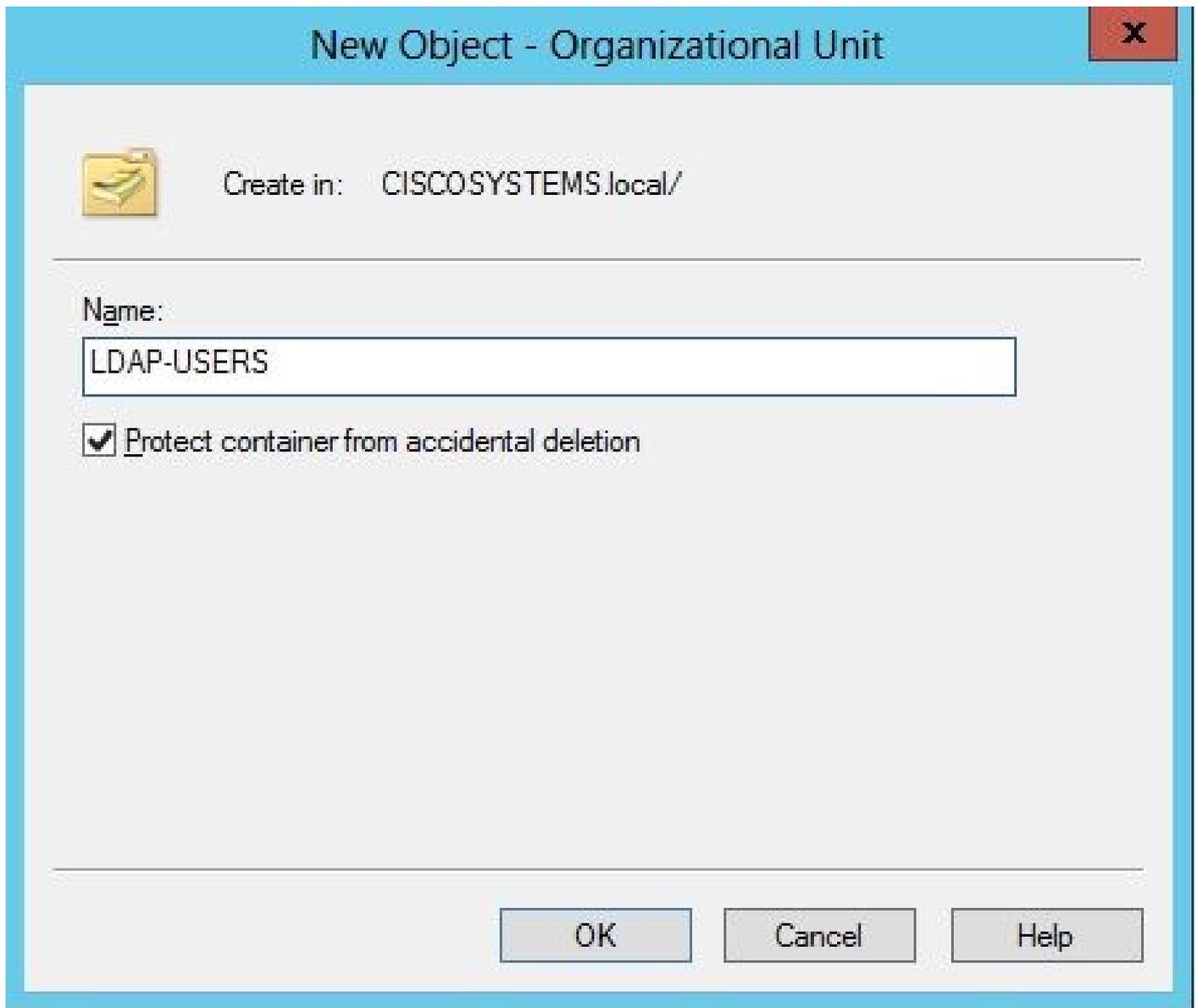
OU でのユーザ データベースの作成

この項では、ドメインに新しい OU を作成し、この OU の中に新しいユーザを作成する手順を説明します。

1. Windows PowerShellを開き、「servermanager.exe」と入力します。
2. Server Managerウィンドウで、AD DSをクリックします。次に、サーバ名を右クリックして、Active Directory Users and Computersを選択します。
3. ドメイン名(この例ではCISCOSYSTEMS.local)を右クリックし、コンテキストメニューから New > Organizational Unitに移動して新しいOUを作成します。

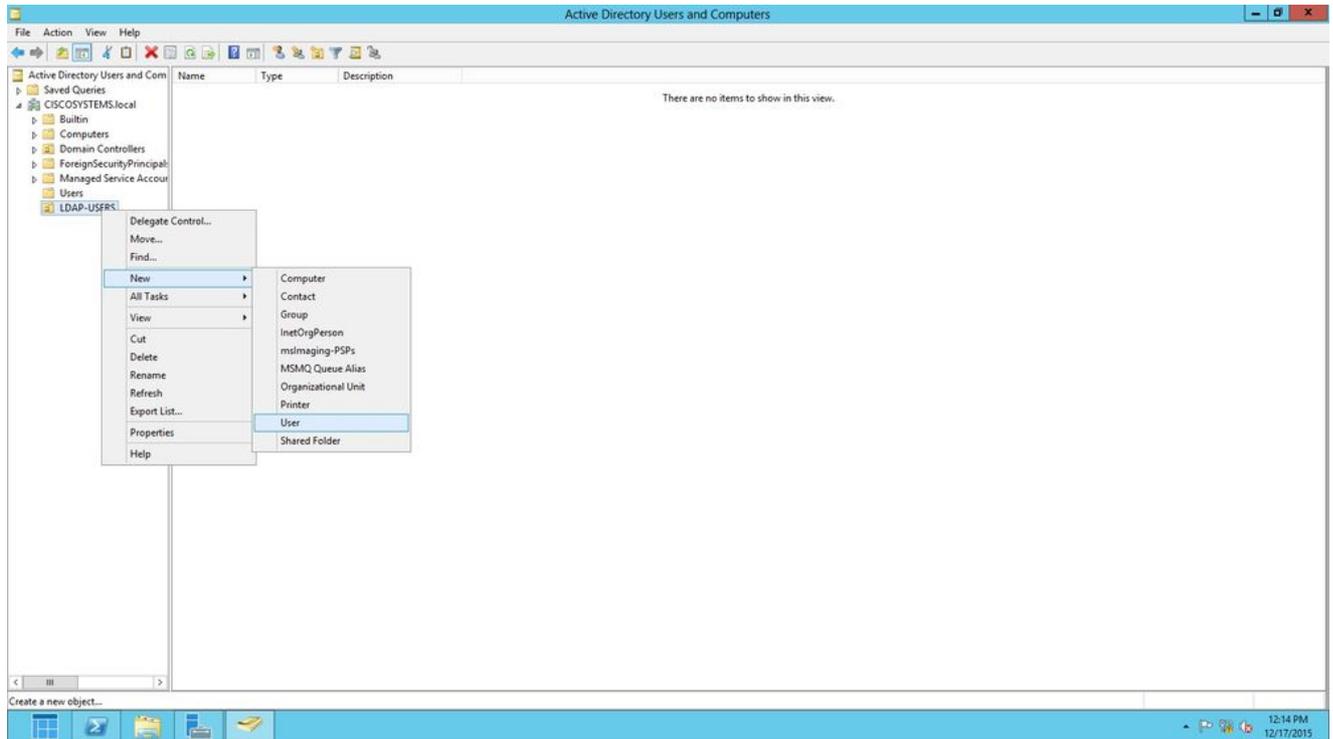


4. 次の図に示すように、このOUに名前を割り当て、OKをクリックします。



これで、LDAP サーバに新しい OU LDAP-USERS が作成されました。次に、この OU にユーザ User1 を作成します。これを行うには、次の手順を実行します。

1. 作成した新しい OU を右クリックします。次の図に示すように、表示されたコンテキストメニューからLDAP-USERS> New > Userに移動して、新しいユーザを作成します。



2. 次の例に示すように、ユーザ設定ページで必須フィールドに情報を入力します。この例では、[User logon name] フィールドに User1 が指定されています。

これは、クライアントを認証するために LDAP データベースで検証されるユーザ名です。この例では、[First name] および [Full Name] フィールドに User1 が指定されています。[Next] をクリックします。

New Object - User X

 Create in: CISCO SYSTEMS.local/LDAP-USERS

First name: Initials:

Last name:

Full name:

User logon name:
 ▾

User logon name (pre-Windows 2000):

3. パスワードを入力し、確認のためのパスワードを入力します。[Password never expires] オプションを選択して [Next] をクリックします。

New Object - User X

 Create in: CISCO SYSTEMS.local/LDAP-USERS

Password:

Confirm password:

User must change password at next logon

User cannot change password

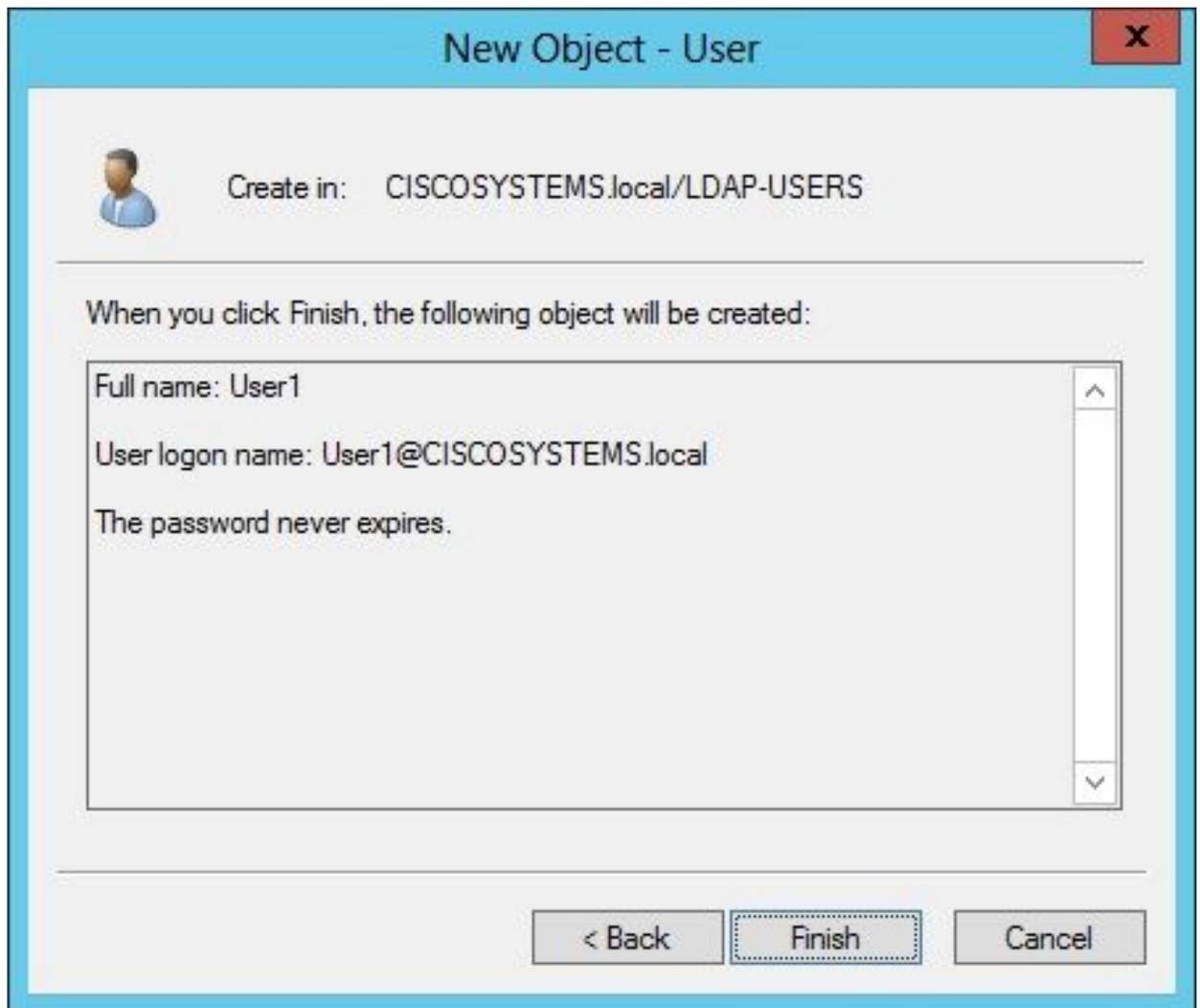
Password never expires

Account is disabled

4. [Finish] をクリックします。

新しいユーザ User1 が OU LDAP-USERS に作成されます。以下は、ユーザ クレデンシャルです。

- ユーザ名 : User1
- パスワード : Laptop123



これで OU の中にユーザが作成されました。次に、このユーザの LDAP アクセスを設定します。

ユーザの LDAP アクセスの設定

AnonymousまたはAuthenticatedのいずれかを選択して、LDAPサーバのローカル認証バインド方式を指定できます。Anonymous方式では、LDAPサーバへの匿名アクセスが許可されます。Authenticated方式では、アクセスを保護するためにユーザ名とパスワードを入力する必要があります。デフォルトでは [Anonymous] になっています。

このセクションでは、匿名方式と認証方式の両方を設定する方法について説明します。

匿名バインド

 注：匿名バインドの使用は推奨されません。匿名バインドを許可するLDAPサーバでは、クレデンシャル認証のタイプは必要ありません。攻撃者は、匿名バインドエントリを利用して、LDAPディレクトリ上のファイルを表示する可能性があります。

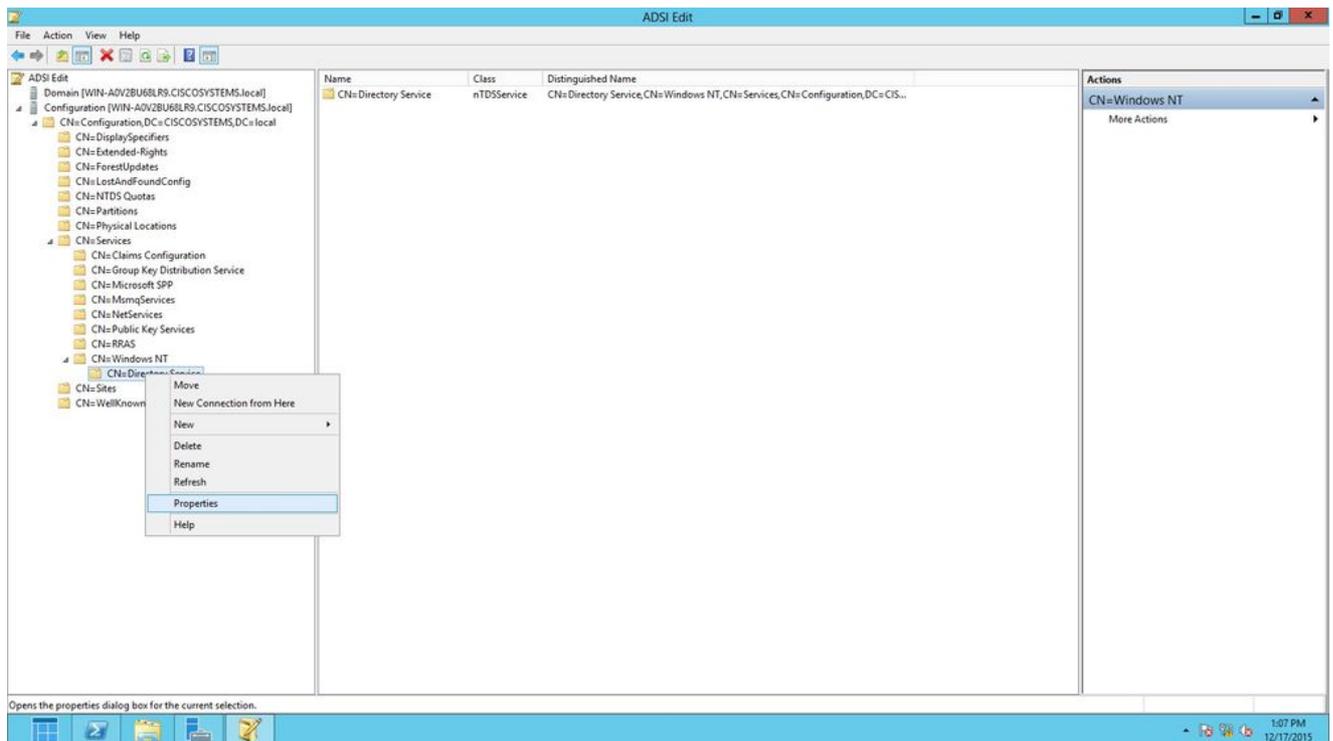
LDAPアクセス用に匿名ユーザを設定するには、このセクションの手順を実行します。

Windows 2012 Essentials Serverで匿名バインド機能を有効にする

サードパーティアプリケーション (この例ではWLC) がLDAP上のWindows 2012 ADにアクセスするには、Windows 2012で匿名バインド機能が有効になっている必要があります。デフォルトでは、Windows 2012 ドメイン コントローラでは匿名 LDAP 操作は許可されていません。匿名バインド機能を有効にするには、次の手順を実行します。

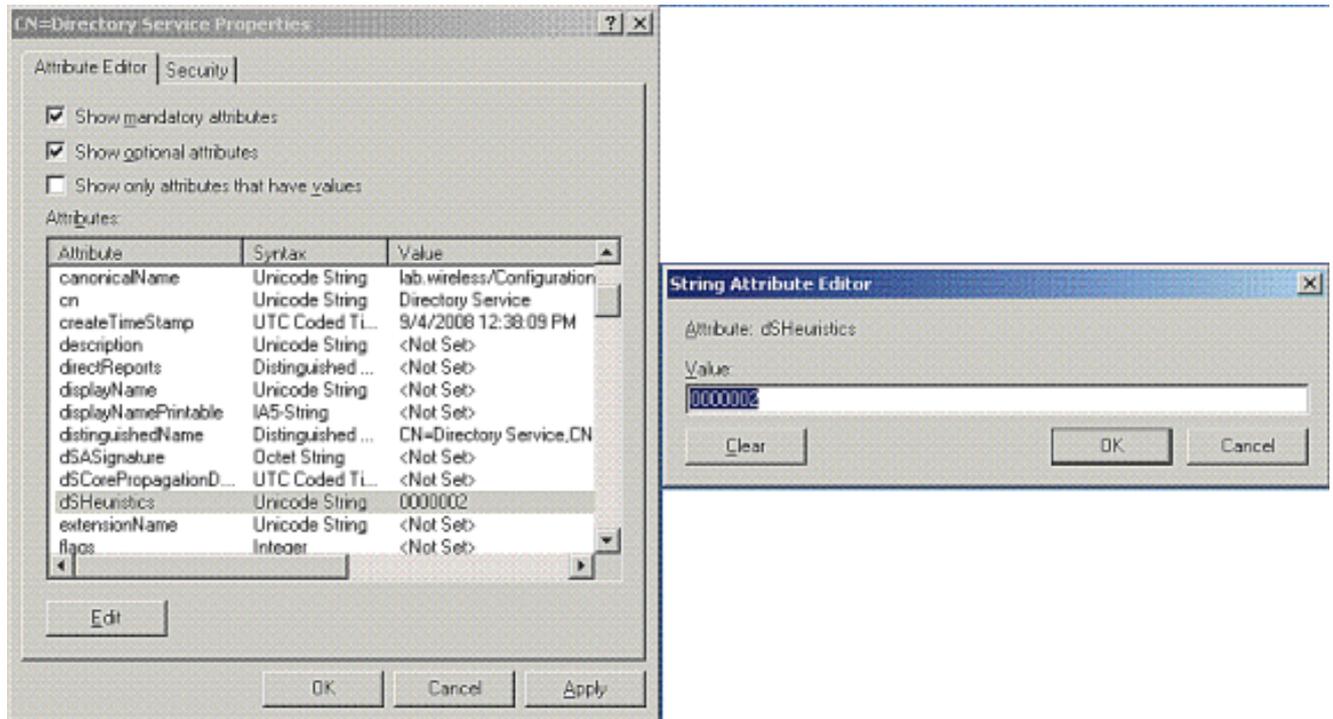
1. Windows PowerShellでADSIEdit.mscと入力して、ADSI編集ツールを起動します。このツールは、Windows 2012サポートツールの一部です。
2. ADSI Editウィンドウで、ルートドメイン(Configuration [WIN-A0V2BU68LR9.CISCOSYSTEMS.local])を展開します。

CN=Services > CN=Windows NT > CN=Directory Serviceの順に移動します。図に示すように、CN=Directory Serviceコンテナを右クリックし、コンテキストメニューからPropertiesを選択します。



3. [CN=Directory Service Properties] ウィンドウで [Attribute] フィールドの下にある [dsHeuristics] 属性をクリックし、[Edit] を選択します。この属性のString Attribute Editorウィンドウで、値0000002を入力し、図に示すようにApplyとOKをクリックします。Windows 2012 サーバで匿名バインド機能が有効になりました。

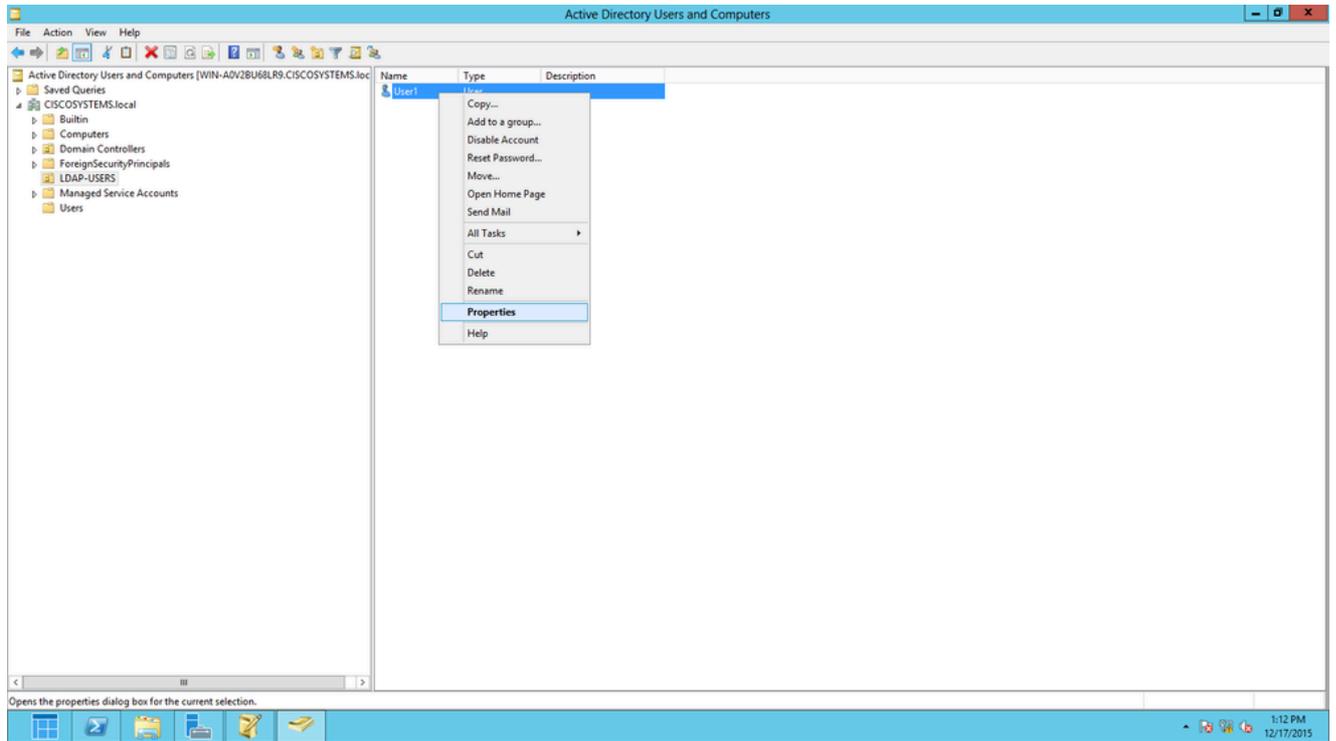
 注：最後 (7番目) の文字は、LDAPサービスへのバインド方法を制御するものです。0 (ゼロ) または7文字目がない場合は、匿名LDAP操作が無効になります。7番目の文字を2に設定すると、匿名バインド機能が有効になります。



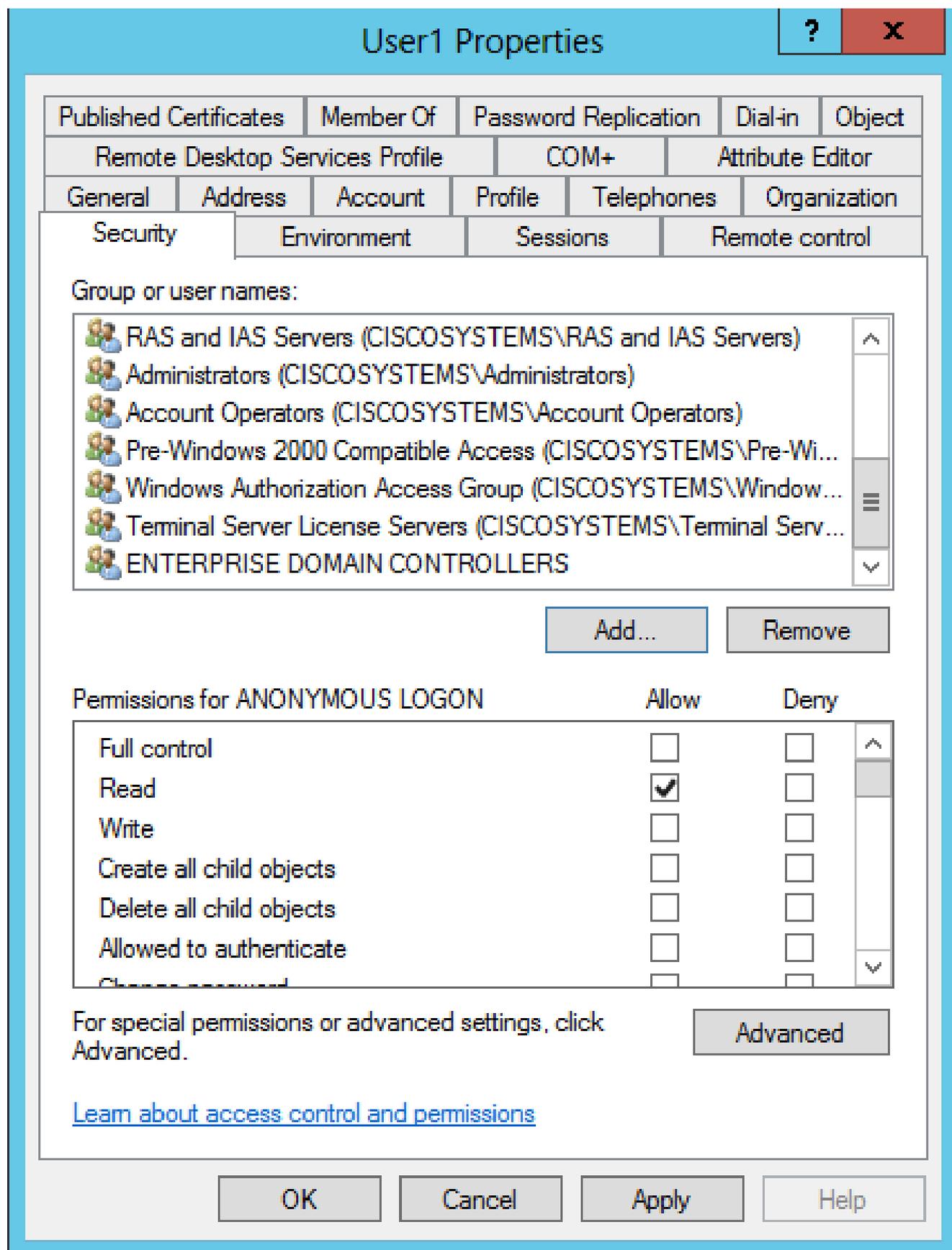
ユーザへのANONYMOUS LOGONアクセス権の付与

次に、ANONYMOUS LOGON アクセス権限をユーザ User1 に付与します。これを行うには、次の手順を実行します。

1. [Active Directory Users and Computers] を開きます。
2. View Advanced Featuresにチェックマークが付いていることを確認します。
3. ユーザ User1 にナビゲートして右クリックします。コンテキストメニューから [Properties] を選択します。このユーザは、名User1で識別されます。



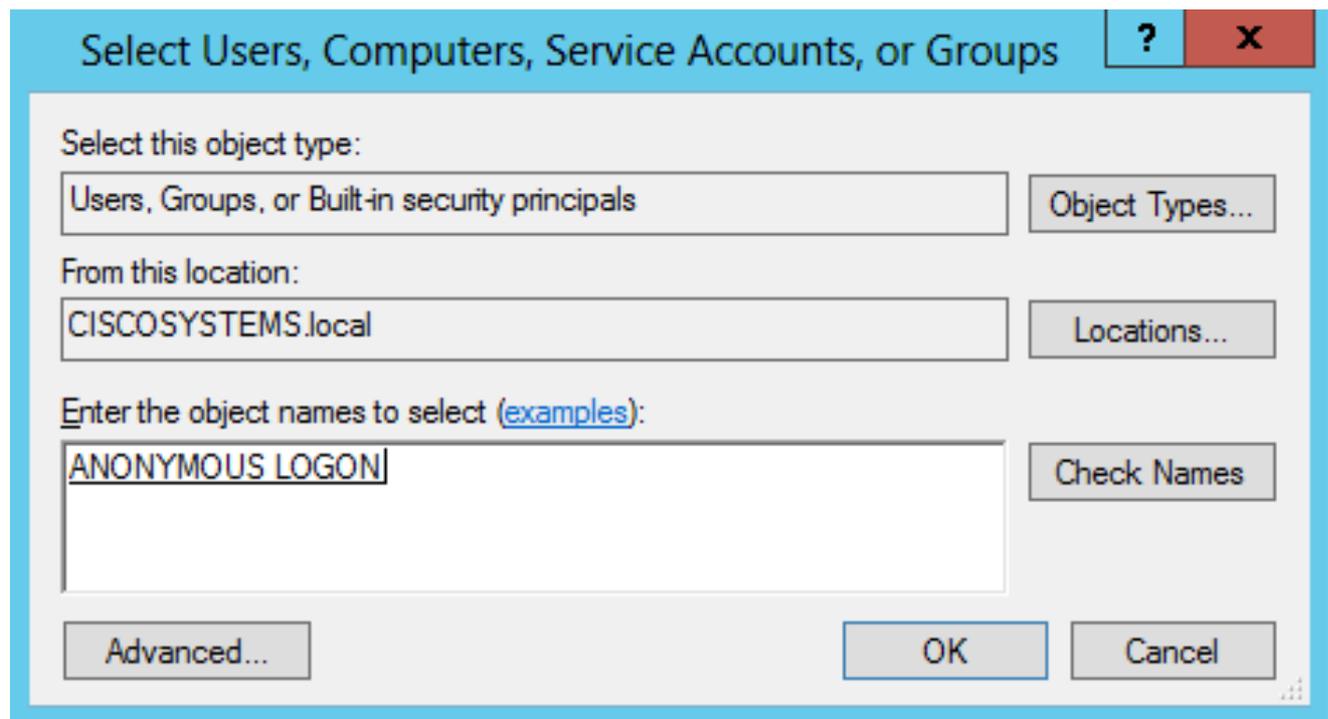
4. 図に示すように、Securityタブをクリックします。



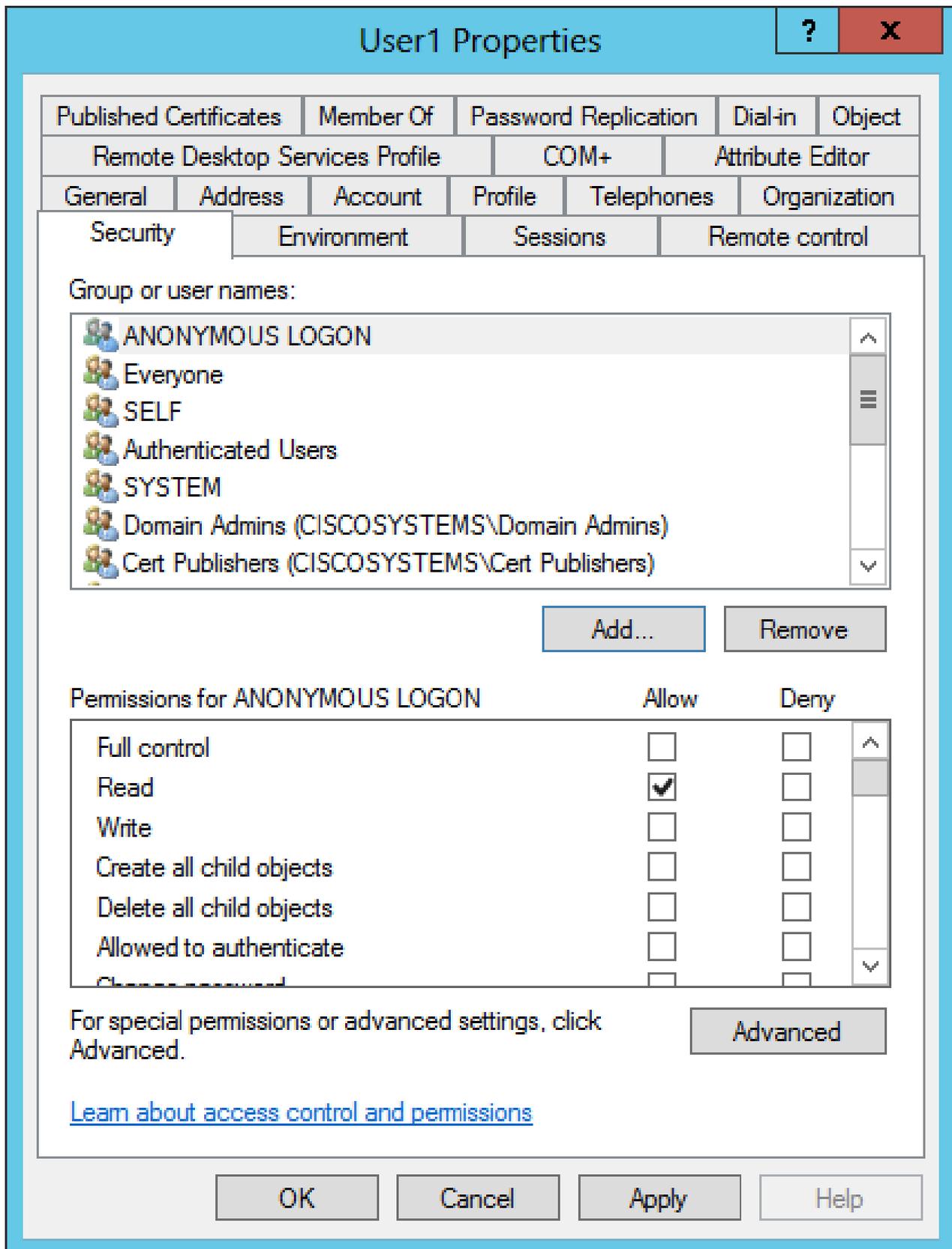
5. 表示されるウィンドウで [Add] をクリックします。

6. 図に示すように、[Enter the object names to select] ボックスにANONYMOUS LOGONと入

かし、ダイアログを確認します。



7. ACL で ANONYMOUS LOGON がユーザの一部のプロパティ セットにアクセスできることがわかります。[OK] をクリックします。図に示すように、ANONYMOUS LOGON アクセス権限がこのユーザに付与されます。

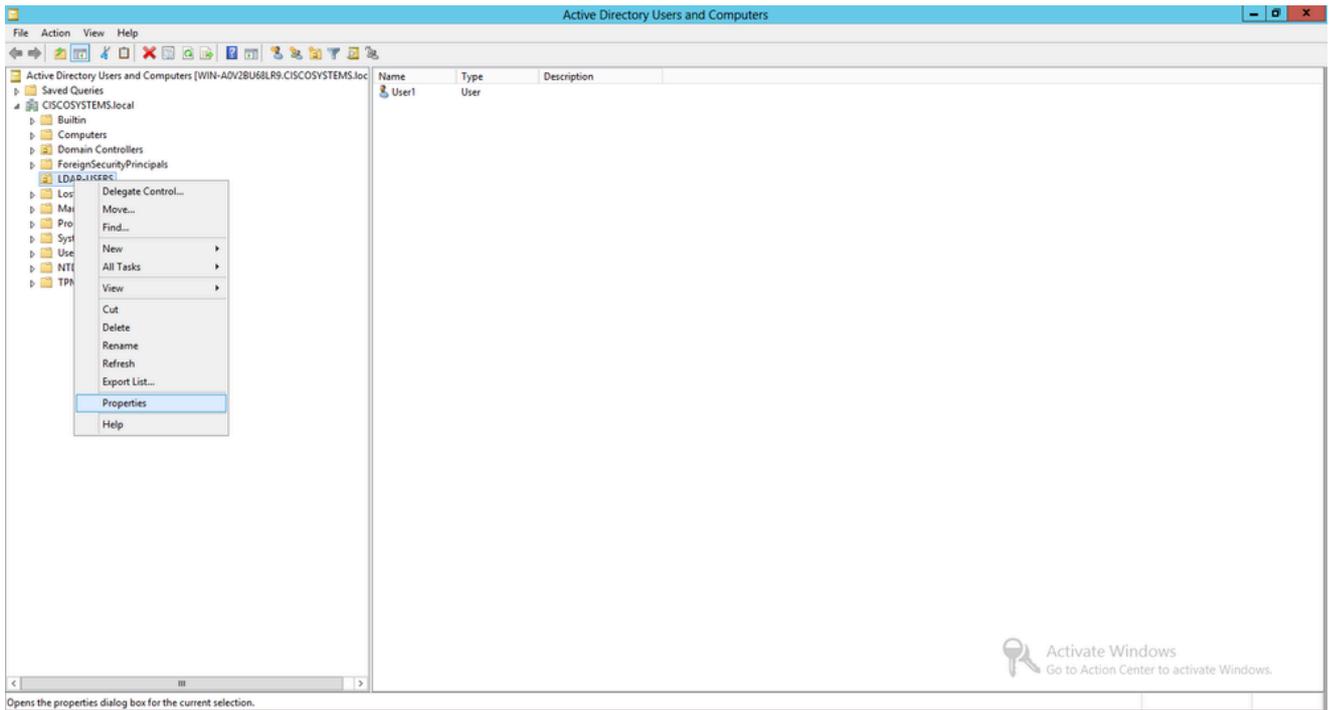


OU での List Contents 権限の付与

次に、ユーザが含まれている OU で ANONYMOUS LOGON に List Contents 権限を付与します。この例では、User1はOU LDAP-USERSにあります。これを行うには、次の手順を実行します。

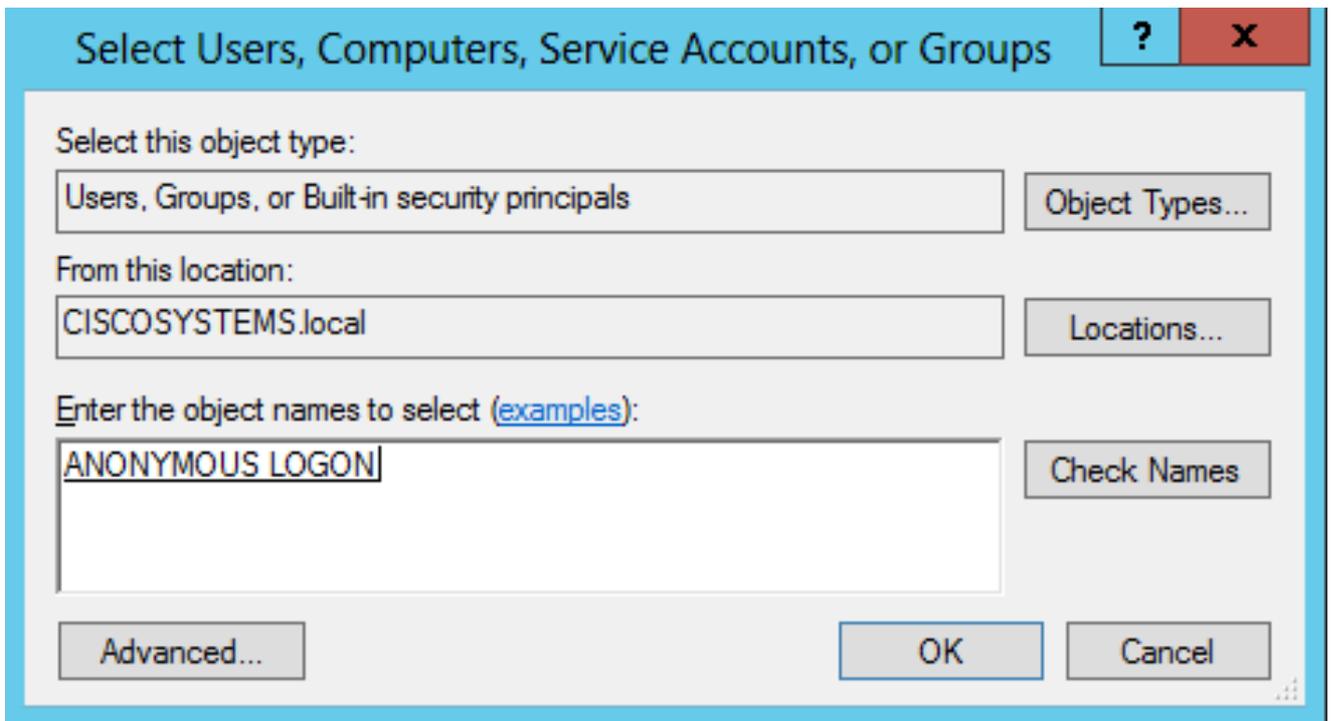
1. 次の図に示すように、Active Directory Users and ComputersでOU LDAP-USERSを右クリ

ックし、Propertiesを選択します。



2. [Security] をクリックします。

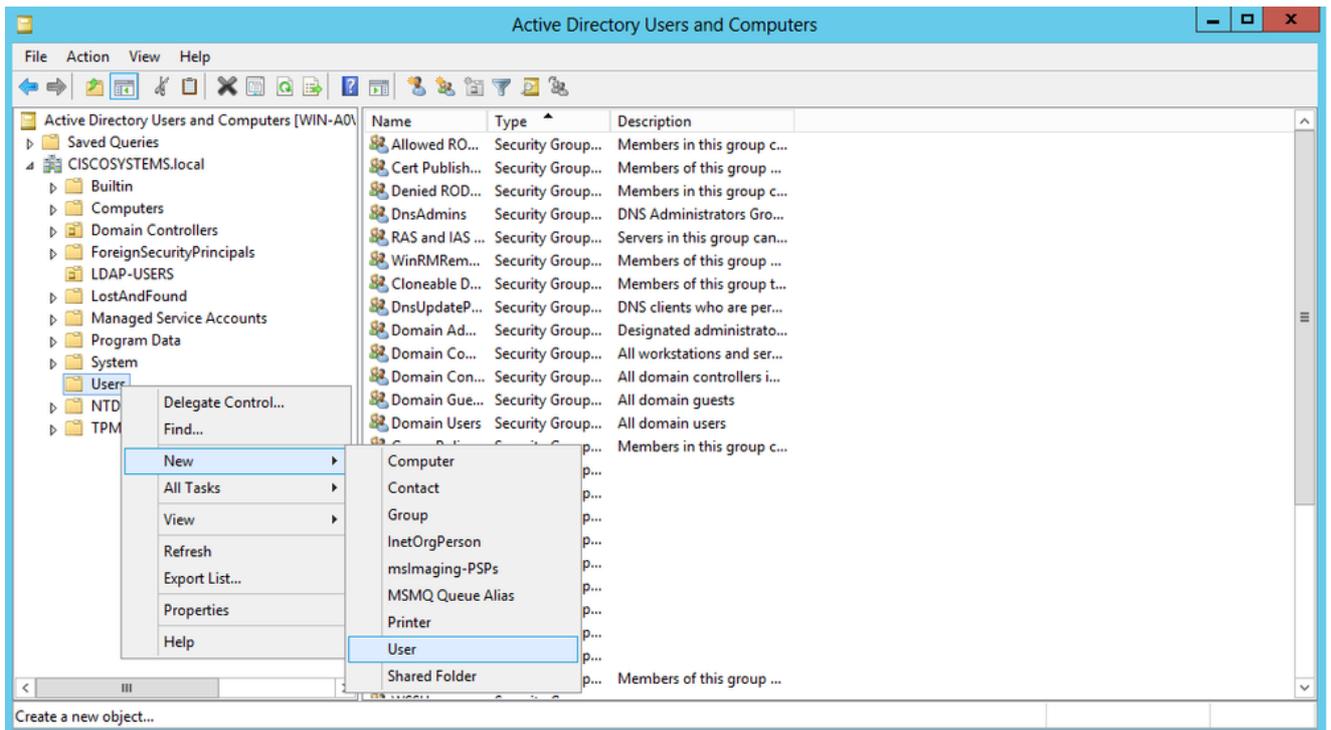
3. [Add] をクリックします。開くダイアログで、ANONYMOUS LOGONと入力し、図に示すようにダイアログを確認します。



認証されたバインド

LDAPサーバへのローカル認証用にユーザを設定するには、この項の手順を実行します。

1. Windows PowerShellを開き、次のように入力します servermanager.exeファイル
2. Server Managerウィンドウで、AD DSをクリックします。サーバ名を右クリックして選択します [Active Directory Users and Computers] の順に選択します。
3. [Users] を右クリックします。表示されたコンテキストメニューからNew > Userの順に移動し、新しいユーザを作成します。



4. 次の例に示すように、ユーザ設定ページで必須フィールドに情報を入力します。この例では、User logon nameフィールドにWLC-adminが設定されています。これは、LDAPサーバへのローカル認証に使用されるユーザ名です。[Next] をクリックします。
5. パスワードを入力し、確認のためのパスワードを入力します。[Password never expires] オプションを選択して [Next] をクリックします。
6. [Finish] をクリックします。

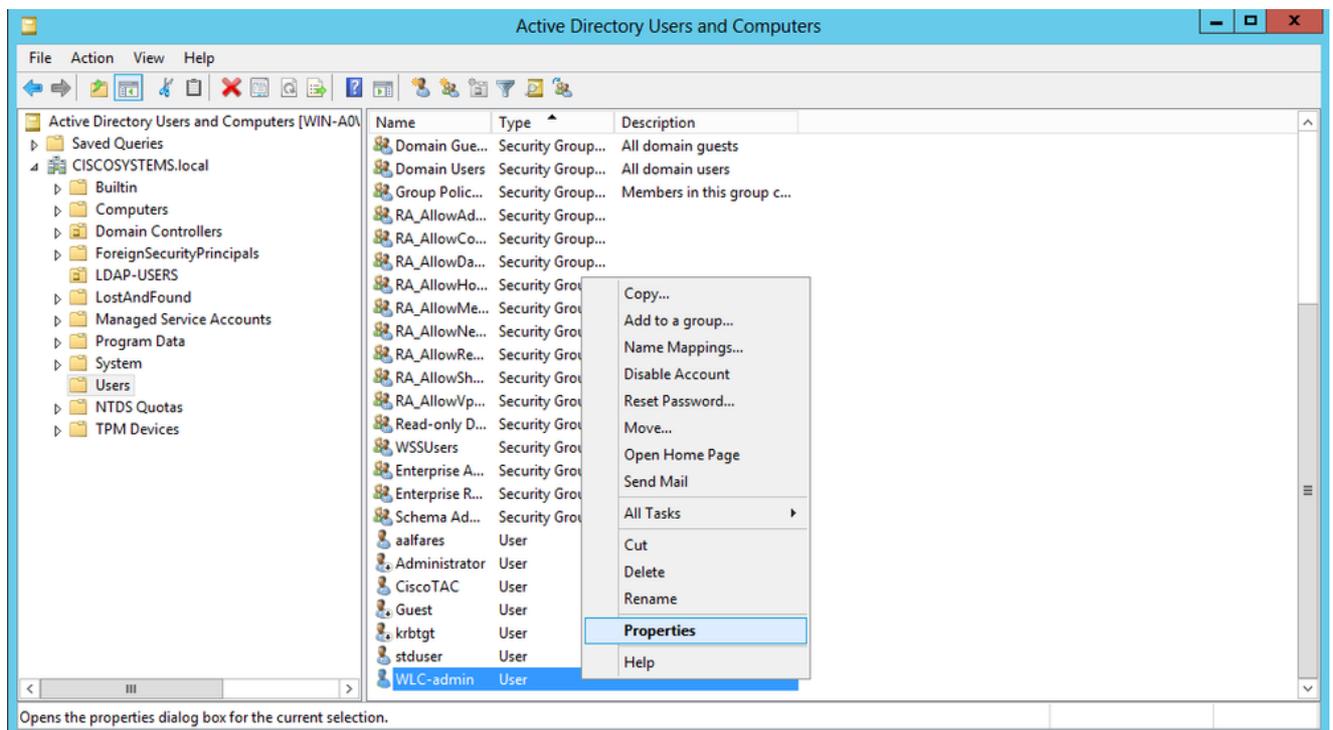
新しいユーザWLC-adminがUsersコンテナの下に作成されます。以下は、ユーザ クレデンシャルです。

- ユーザ名 : WLC-admin
- パスワード : Admin123

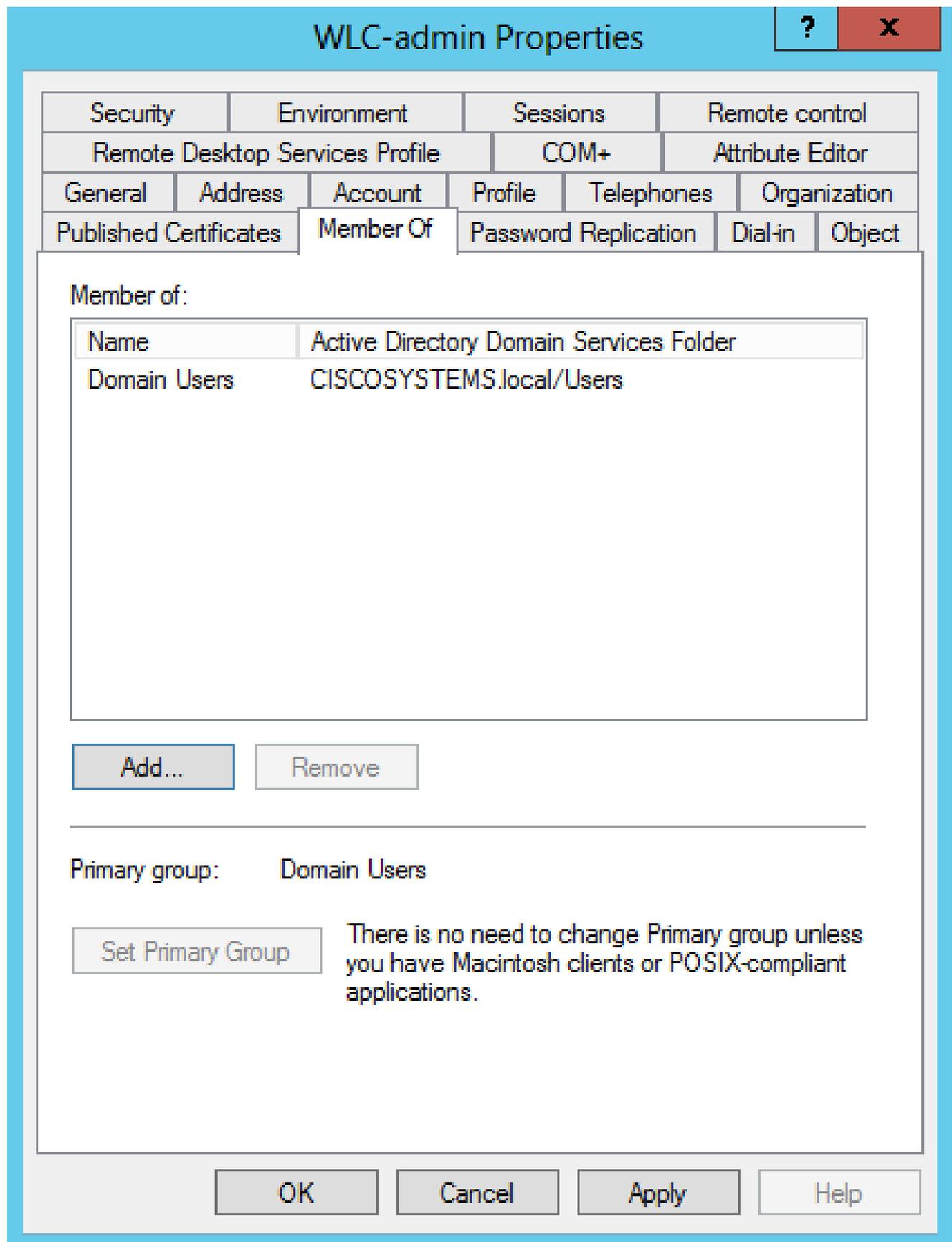
WLC-adminへの管理者権限の付与

ローカル認証ユーザが作成されたので、管理者権限を付与する必要があります。これを行うには、次の手順を実行します。

1. [Active Directory Users and Computers] を開きます。
2. View Advanced Featuresにチェックマークが付いていることを確認します。
3. ユーザWLC-adminに移動して右クリックします。次の図に示すように、コンテキストメニューからPropertiesを選択します。このユーザは、名WLC-adminで識別されます。

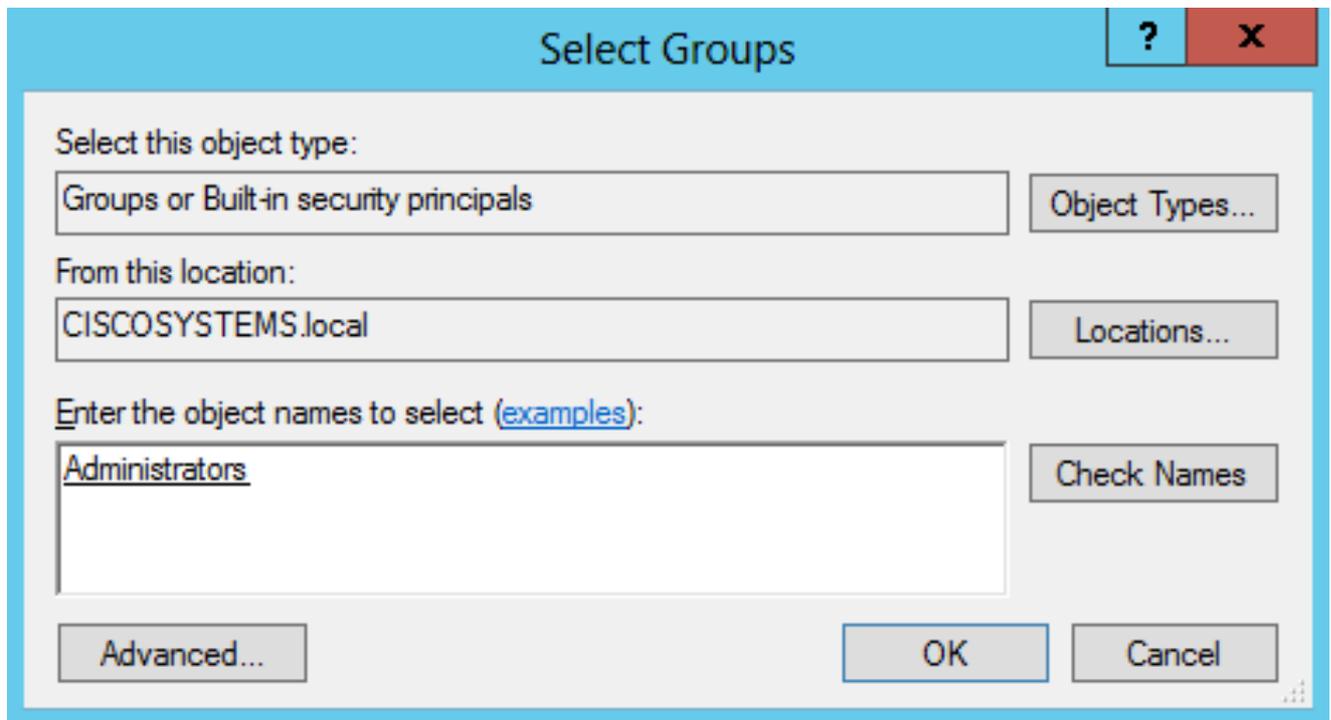


4. 図に示すように、[Member Of] タブをクリックします。



::

5. [Add] をクリックします。開くダイアログで、Administratorsと入力し、次の図に示すようにOKをクリックします。

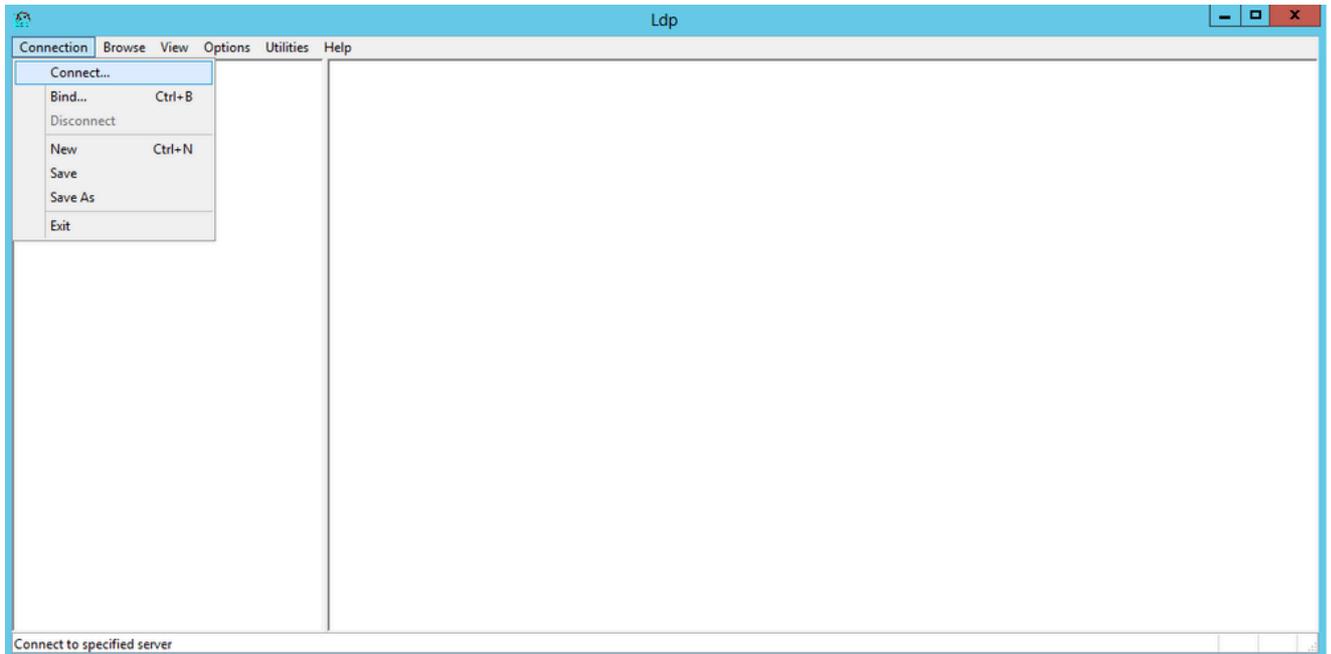


LDP を使用したユーザ属性の確認

この GUI ツールは、ユーザがすべての LDAP 互換ディレクトリ (Active Directory など) に対して接続、バインド、検索、変更、追加、削除などの操作を実行できるようにする LDAP クライアントです。LDP では、Active Directory に格納されているオブジェクトとそのメタデータ (セキュリティ記述子やレプリケーションメタデータなど) を表示できます。

LDP GUI ツールは、製品 CD から Windows Server 2003 Support Tools をインストールするとインストールされます。ここでは、LDP ユーティリティを使用してユーザ User1 に関連付けられている特定の属性を確認する方法について説明します。一部の属性は、WLC で LDAP サーバ設定パラメータ (ユーザ属性タイプ、ユーザ オブジェクトタイプなど) の値を入力するときに使用されます。

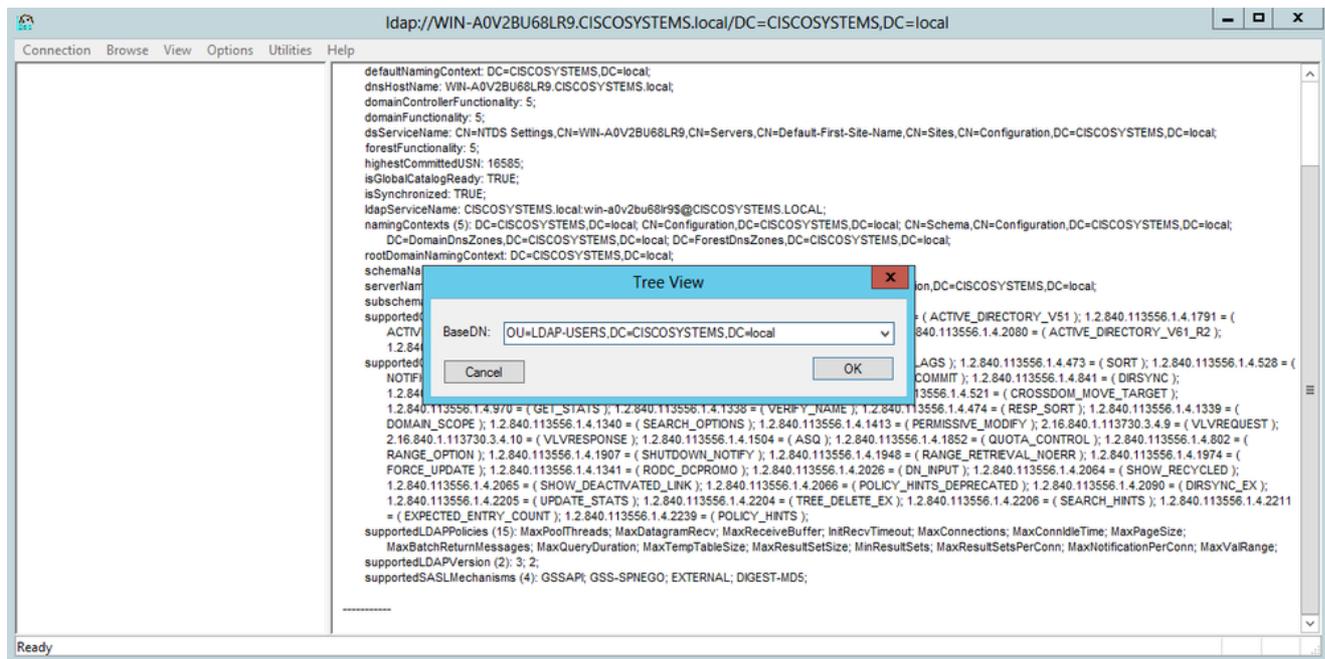
1. Windows 2012サーバ (同じLDAPサーバ上でも) で、Windows PowerShellを開き、LDPと入力してLDPブラウザにアクセスしますを参照。
2. 図に示すように、LDPメインウィンドウでConnection > Connectの順に選択し、LDAPサーバのIPアドレスを入力してLDAPサーバに接続します。



- LDAPサーバに接続したら、次の図に示すように、メインメニューからViewを選択し、Treeをクリックします。



- 表示される [Tree View] ウィンドウで、ユーザの BaseDN を入力します。この例では、User1はドメインCISCOSYSTEMS.localのOU「LDAP-USERS」に含まれています。次の図に示すように、OKをクリックします。



5. LDPブラウザの左側には、指定したBaseDN(OU=LDAP-USERS, dc=CISCOYSTEMS, dc=local)の下にツリー全体が表示されます。ツリーを展開してユーザ User1 を見つけます。このユーザは、ユーザの名前を表す CN 値で識別されます。この例では CN=User1 です。CN=User1 をダブルクリックします。図に示すように、LDPブラウザの右側のペインに、User1に関連付けられているすべての属性が表示されます。



6. LDAP サーバに WLC を設定するときには、[User Attribute] フィールドに、ユーザ名を含むユーザレコードの属性の名前を入力します。この LDP の出力から、sAMAccountName がユーザ名「User1」を含む属性の 1 つであることがわかります。そこで、WLC の [User Attribute] フィールドに対応する sAMAccountName 属性を入力します。

7. LDAP サーバに WLC を設定するときには、[User Object Type] フィールドに、レコードを

ユーザとして識別する LDAP objectType 属性の値を入力します。多くの場合、ユーザレコードには objectType 属性の値が複数あり、そのうちのいくつかはユーザに固有であり、また、いくつかは他のオブジェクトタイプと共有されています。LDAP 出力の CN=Person はレコードをユーザとして識別する値の 1 つです。そこで、WLC の User Object Type 属性として Person を指定します。

次に LDAP サーバの WLC を設定します。

LDAP サーバの WLC の設定

ここまでで LDAP サーバが設定されました。次に LDAP サーバの詳細を使用して WLC を設定します。WLC の GUI から次の手順を実行します。

 注：このドキュメントでは、WLCが基本動作用に設定され、LAPがWLCに登録されていることを前提としています。WLCでLAPとの基本動作を初めて設定する場合は、「[Wireless LAN Controller \(WLC \) への Lightweight AP \(LAP \) の登録](#)」を参照してください。

1. WLC の [Security] ページの左側にあるタスク ペインで [AAA] > [LDAP] を選択し、LDAP サーバ設定ページに進みます。



The screenshot shows the Cisco WLC GUI Security page. The left sidebar has a tree view with 'AAA' expanded and 'LDAP' selected. The main area is titled 'LDAP Servers' and contains a table 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

LDAP サーバを追加するには、[New] をクリックします。[LDAP Servers > New] ページが表示されます。

2. [LDAP Servers Edit] ページで LDAP サーバの詳細 (LDAP サーバの IP アドレス、ポート番号、サーバ有効化ステータスなど) を指定します。
 - [Server Index (Priority)] ドロップダウン ボックスから番号を選択し、その他の設定済みの LDAP サーバに関連したこのサーバの優先順位を指定します。サーバは最大 17 個まで設定できます。コントローラが最初のサーバに接続できない場合、リスト内の 2 番目のサーバへの接続を試行する、というようになります。
 - [Server IP Address] フィールドに LDAP サーバの IP アドレスを入力します。
 - [Port Number] フィールドに LDAP サーバの TCP ポート番号を入力します。有効な範囲は 1 ~ 65535 で、デフォルト値は 389 です。

- 簡易バインドでは、バインドユーザ名にAuthenticatedを使用しました。これは、LDAPサーバとそのパスワードへのアクセスに使用されるWLC管理ユーザの場所です
- [User Base DN] フィールドに、すべてのユーザのリストを含む LDAP サーバ内のサブツリーの識別名 (DN) を入力します。たとえば、ou=organizational unit, .ou=next organizational unit および o=corporation.com などです。ユーザを含むツリーがベース DN である場合、o=corporation.com または dc=corporation、dc=com と入力します。

この例ではユーザは組織単位 (OU) LDAP-USERS に含まれています。この組織単位は lab.wireless ドメインの一部として作成されています。

ユーザベース DN は、ユーザ情報 (EAP-FAST 認証方式に基づくユーザ クレデンシャル) が保存されている場所のフルパスを指している必要があります。この例では、ユーザはベースDN OU=LDAP-USERS, DC=CISCO SYSTEMS, DC=localの下にあります。

- [User Attribute] フィールドに、ユーザ名を含むユーザレコード内の属性の名前を入力します。

[User Object Type] フィールドに、対象のレコードをユーザとして特定する LDAP objectType 属性の値を入力します。多くの場合、ユーザレコードには objectType 属性の値が複数あり、そのうちのいくつかはユーザに固有であり、また、いくつかは他のオブジェクトタイプと共有されています。

これらの2つのフィールドの値は、Windows 2012サポートツールの一部として提供されているLDAPブラウザユーティリティを使用して、ディレクトリサーバから取得できます。この Microsoft LDAP ブラウザ ツールは LDP と呼ばれます。このツールを使用して、特定ユーザの [User Base DN]、[User Attribute]、および [User Object Type] フィールドの値を確認できます。LDP を使用したユーザ固有属性の確認方法の詳細については、このドキュメントの「LDP を使用したユーザ属性の確認」を参照してください。

- [Server Timeout] フィールドに再送信の間隔 (秒数) を入力します。有効な範囲は 2 ~ 30 秒であり、デフォルト値は 2 秒です。
- [Enable Server Status] チェックボックスをオンにしてこの LDAP サーバを有効にするか、チェックマークをオフにして無効にします。デフォルト値は無効です。
- [Apply] をクリックして、変更を確定します。上記の情報を使用した設定の例を次に示します。



- これで LDAP サーバに関する詳細が WLC に設定されました。次に、WLAN を Web 認証用に設定します。

Web 認証用の WLAN の設定

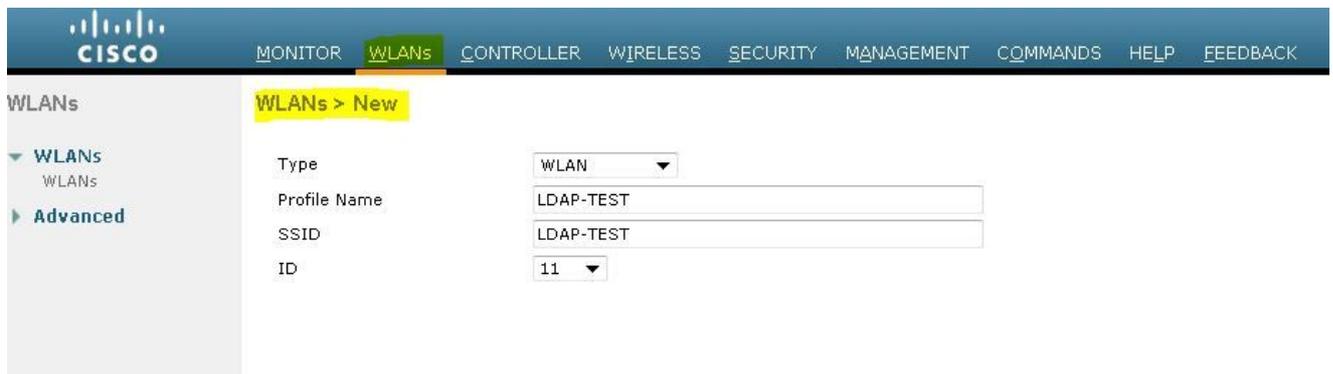
最初の手順では、ユーザの WLAN を作成します。次のステップを実行します。

- WLAN を作成するために、コントローラの GUI で [WLANs] をクリックします。

[WLANs] ウィンドウが表示されます。このウィンドウには、コントローラに設定されている WLAN の一覧が表示されます。

- 新しい WLAN を設定するために [New] をクリックします。

この例では、WLAN の名前を Web-Auth としています。



- [APPLY] をクリックします。
- [WLAN] > [Edit] ウィンドウで、WLAN 固有のパラメータを定義します。

The screenshot shows the Cisco WLAN configuration interface for the 'LDAP-TEST' profile. The 'Security' tab is selected, and the 'Status' checkbox is checked and highlighted in yellow. Other fields include Profile Name (LDAP-TEST), Type (WLAN), SSID (LDAP-TEST), Security Policies ([WPA2][Auth(802.1X)]), Radio Policy (All), Interface/Interface Group (management), Multicast Vlan Feature (Enabled), Broadcast SSID (Enabled), and NAS-ID (none).

- [Status] チェックボックスをオンにしてこの WLAN を有効にします。
- WLAN に対し、[Interface Name] フィールドから適切なインターフェイスを選択します。

この例では、WLAN Web-Auth に接続する管理インターフェイスを割り当てています。

5. [Security] タブをクリックします。[Layer 3 Security] フィールドで、[Web Policy] チェックボックスをオンにして、[Authentication] オプションを選択します。

The screenshot shows the 'Layer 3 Security' configuration page. The 'Web Policy' dropdown is set to 'Authentication', which is highlighted in yellow. Other options include Passthrough, Conditional Web Redirect, Splash Page Web Redirect, and On MAC Filter failure. Below are fields for Preauthentication ACL (IPv4: None, IPv6: None, WebAuth FlexAct: None), Sleeping Client (Enable), and Over-ride Global Config (Enable).

Web 認証を使用してワイヤレス クライアントを認証するため、このオプションを選択します。[Override Global Config] チェックボックスをオンにして、各 WLAN の Web 認証設定を有効にします。[Web Auth type] ドロップダウン メニューから適切な Web 認証の種類を選択します。この例では、内部 Web 認証を使用します。

 注: Web 認証は 802.1x 認証ではサポートされていません。これは、Web 認証を使用する場合、レイヤ 2 セキュリティとして、802.1x または 802.1x を使用する WPA/WPA2 を選択できないことを意味します。その他のすべてのレイヤ 2 セキュリティ パラメータを使用した Web 認証がサポートされます。

6. [AAA Servers] タブを選択します。LDAP サーバのプルダウン メニューから設定した LDAP サーバを選択します。ローカル データベースまたは RADIUS サーバを使用している場合は、[Authentication priority order for web-auth user] フィールドで認証のプライオリティを設定できます。

The screenshot shows the Cisco WLAN configuration page for a WLAN named 'LDAP-TEST'. The 'AAA Servers' tab is selected, and the 'LDAP Servers' section shows three servers: Server 1 (IP: 172.16.16.200, Port: 389), Server 2 (None), and Server 3 (None). The 'Authentication priority order for web-auth user' section shows 'LOCAL RADIUS' in the 'Not Used' list and 'LDAP' in the 'Order Used For Authentication' list.

7. [APPLY] をクリックします。

 注：この例では、ユーザを認証するためのレイヤ2セキュリティ方式は使用されていないため、レイヤ2セキュリティフィールドでNoneを選択します。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

このセットアップを検証するために、ワイヤレス クライアントを接続し、設定が想定どおりに動作するかどうかを確認します。

ワイヤレス クライアントが起動したら、Web ブラウザに URL (www.yahoo.com など) を入力します。ユーザが認証されていないため、WLC はそのユーザを内部 Web ログイン URL にリダイレクトします。

ユーザ クレデンシャルの入力が求められます。ユーザがユーザ名とパスワードを送信すると、ログイン ページ側がユーザ クレデンシャルの入力を受け取り、WLC Web サーバの action_URL (http://1.1.1.1/login.html など) に入力を送信するとともに要求を戻します。これが入力パラメータとしてカスタマーのリダイレクト URL に提供されます。ここで、1.1.1.1 は、スイッチの仮想インターフェイス アドレスです。

WLC は LDAP ユーザ データベースに照合してユーザを認証します。認証が成功すると、WLC Webサーバは、設定されたリダイレクトURLまたはクライアントが開始されたURLにユーザを転送します。次に例を示します [www.yahoo.com にアクセスしてください。](http://www.yahoo.com)



There is a problem with this website's security certificate.

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.

We recommend that you close this webpage and do not continue to this website.

- [Click here to close this webpage.](#)
- [Continue to this website \(not recommended\).](#)
- [More information](#)



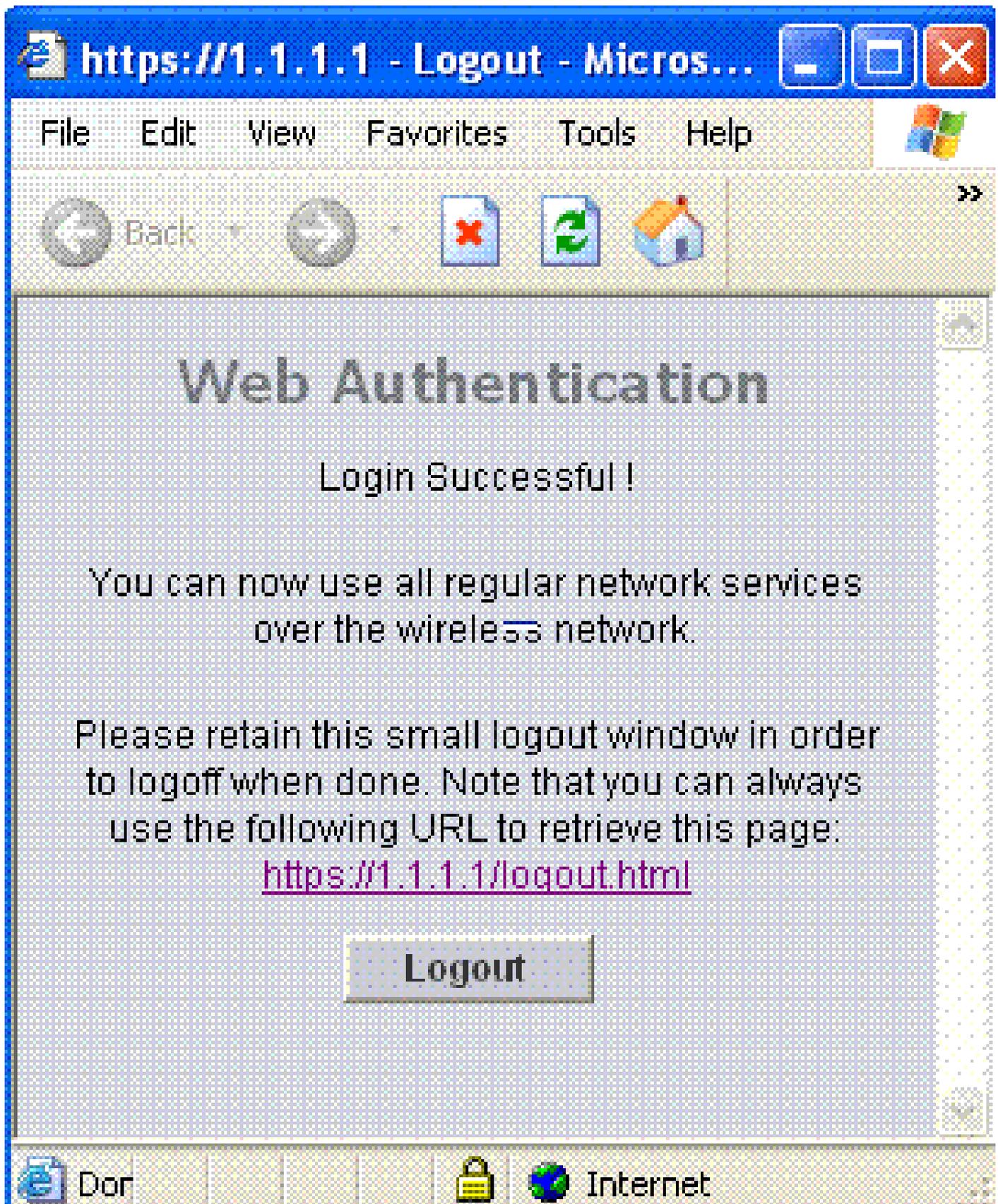
Login



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.

User Name	<input type="text" value="User1"/>
Password	<input type="password" value="*****"/>
<input type="button" value="Submit"/>	



トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

設定のトラブルシューティングを行うために、次のコマンドを使用できます。

- debug mac addr <client-MAC-address 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

次に、debug mac addr cc:fa:00:f7:32:35コマンドの出力例を示します

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
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Association received from mobile on BSSID 00:2
*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 l
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Interface policy on Mobile, role Loca

*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 A
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Changing IPv6 A
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfApplyWlanPolicy: Apply WLAN Policy over PMI
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6246 setting Central switched
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6249 apVapId = 1 and Split Ac
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying site-specific Local Bridging override
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Local Bridging Interface Policy for s
*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
*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
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 suppRates statusCode is 0 and gotSuppRatesEle
*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
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfMs1xStateDec
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Change state to

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 pemApfAddMobileStation2: APF_MS_PEM_WAIT_L2_AU
*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 AUTHCH

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 AUTHCHECK (2) Change state to L2

*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 mobil
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4) Change state
```

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) pemApfAddMobile
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Adding Fast Path
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
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Successfully pl
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) pemApfAddMobile
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Replacing Fast
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
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Successfully pl
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2 (apf_policy.c:359) Changing sta
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2:session timeout forstation cc:f
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Scheduling deletion of Mobile Station: (calle
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Func: apfPemAddUser2, Ms Timeout = 1800, Sessi
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Sending assoc-resp with status 0 station:cc:fa
*apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sending Assoc Response to station on BSSID 00:
*apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 apfProcessAssocReq (apf_80211.c:10187) Changin
*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2, dtlFla
*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, dtlFla
*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,vla
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype 0xff:ff:ff:ff:
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block settin
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 mscbVapLoc
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local a
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block settin
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 settin
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 mscbVapLoc
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local a
*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
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 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 setting
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)
*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 0)
*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
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 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 0)
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype 0xff: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 setting
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 mscbVapLocalMac=00:00:00:00:00:00
*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)
*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
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 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: 172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block setting
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)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP setting server from ACK (mscb=0x40e64b88)
*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 0)
*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
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 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 10
*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created in mscb for mobile, length 10
*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-
*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=CISCOYSTEMS,DC=local,
*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=""
*LDAP DB Task 1: Dec 24 03:46:01.226: Attempting user bind with username CN=User1,CN=Users,DC=CISCOYST
*LDAP DB Task 1: Dec 24 03:46:01.228: LDAP ATTR> dn = CN=User1,CN=Users,DC=CISCOYSTEMS,DC=local (size
*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
*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

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Stopping deletion of Mobile Station: (callerId:
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Setting Session Timeout to 1800 sec - starting
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Reached PLUMBFASPATH: f
*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...
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule (contd...

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule (contd...

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule (contd...

*ewmwebWebauth1: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Successfully plumbed mob
*pemReceiveTask: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 1, dtlFla

```

```

(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
 antenna1: 25 secs ago..... -37 dBm
AP1142-1(slot 1)

antenna0: 25 secs ago..... -44 dBm
antenna1: 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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。