Web Authentication Using LDAP on Wireless LAN Controllers (WLCs) Configuration Example

Contents

Table of Contents

Introduction

This document describes how to setup a Wireless LAN Controller (WLC) for web authentication. It explains how to configure a Lightweight Directory Access Protocol (LDAP) server as the backend database for web authentication to retrieve user credentials and authenticate the user.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of the configuration of Lightweight Access Points (LAPs) and Cisco WLCs
- Knowledge of Control And Provisioning of Wireless Access Point protocol (CAPWAP)

- Knowledge of how to set up and configure Lightweight Directory Access Protocol (LDAP), Active Directory and domain controllers

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 5508 WLC that runs firmware release 8.2.100.0
- Cisco 1142 Series LAP
- Cisco 802.11a/b/g Wireless Client Adapter.
- Microsoft Windows 2012 Essentials server that performs the role of the LDAP server

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

Conventions

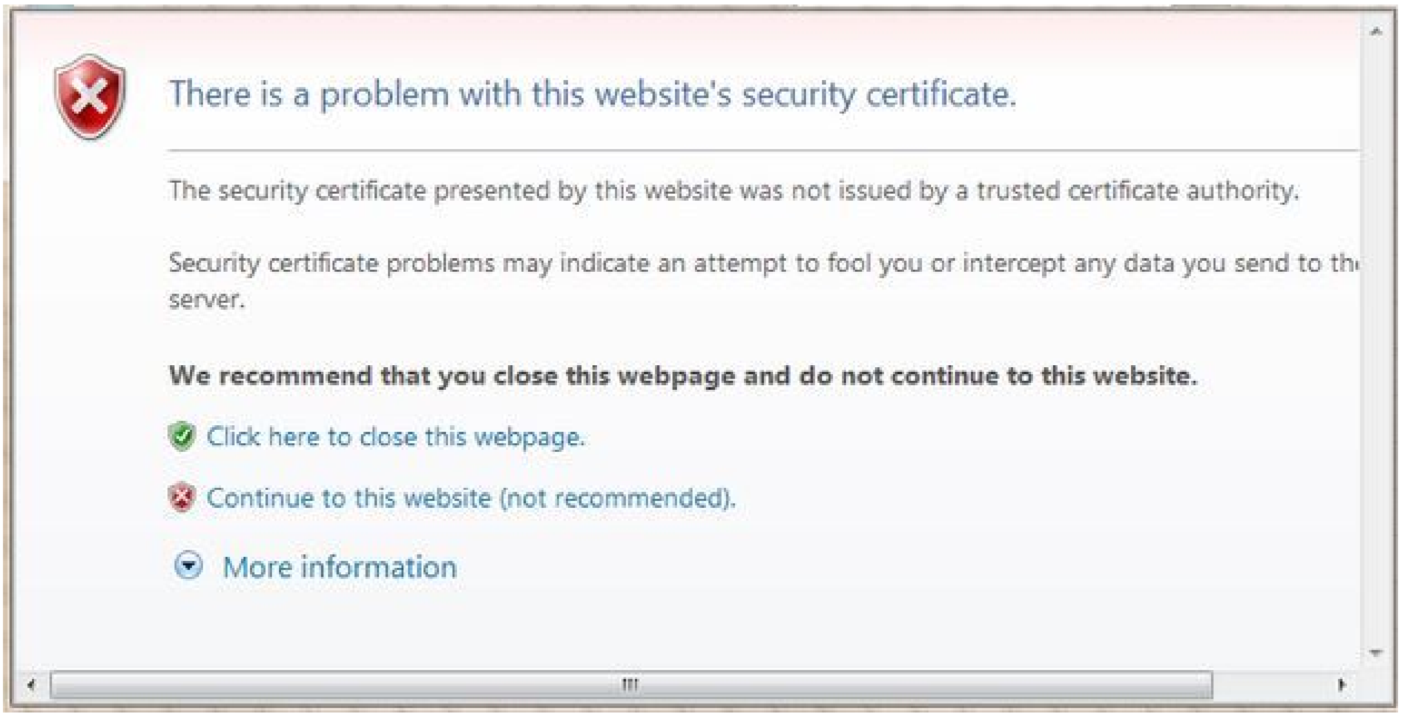
Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Web Authentication Process

Web authentication is a Layer 3 security feature that causes the controller to disallow IP traffic (except DHCP and DNS-related packets) from a particular client until that client has correctly supplied a valid username and password. When you use web authentication to authenticate clients, you must define a username and password for each client. Then, when the clients attempt to join the wireless LAN, they must enter the username and password when prompted by a login page.

When web authentication is enabled (under Layer 3 Security), users occasionally receive a web-browser security alert the first time that they attempt to access a URL.

Tip: To remove this certificate warning, please revert back to the following guide on how to install a 3rd party trusted certificate http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-certificates-wlc-00.html



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 th server.

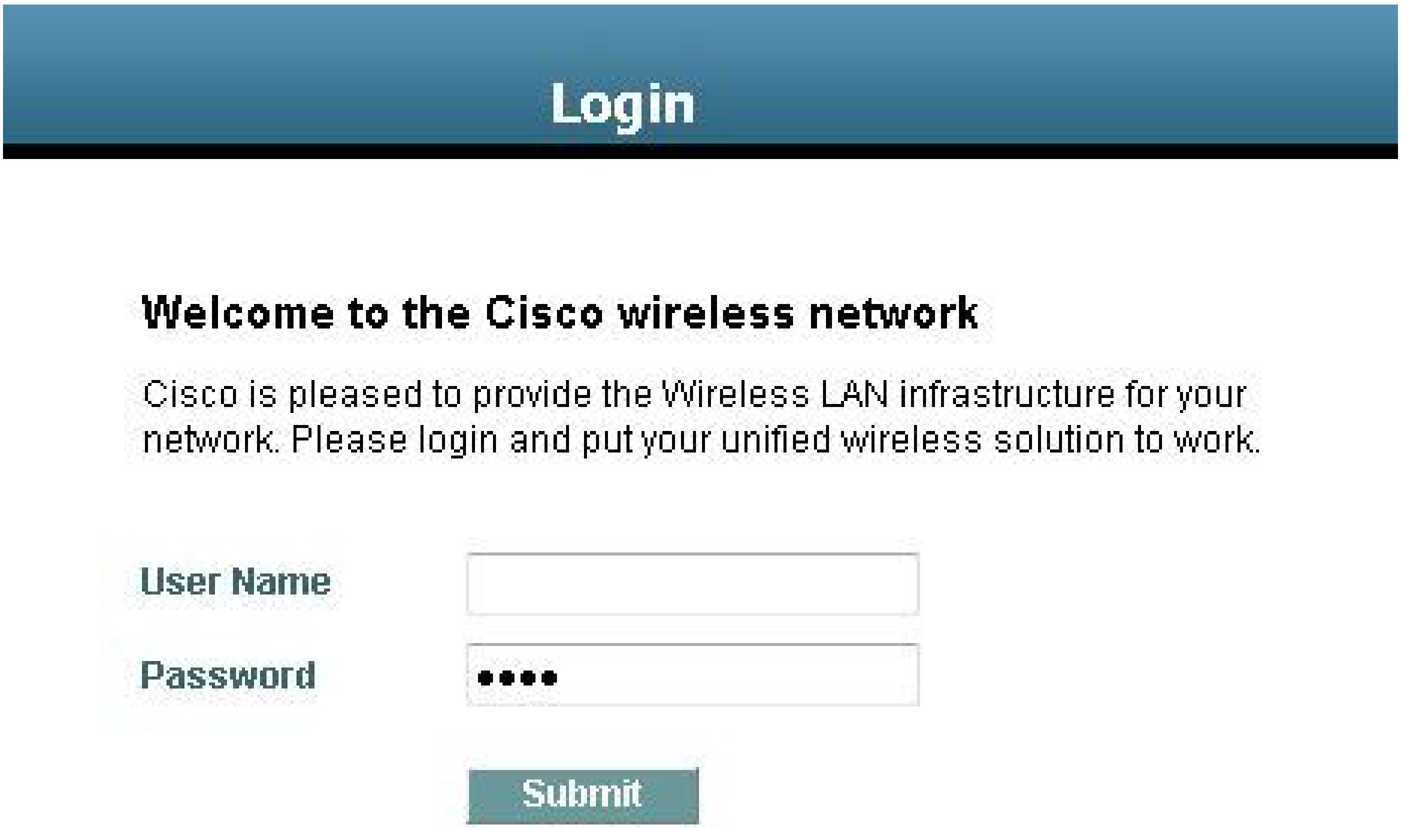
We recommend that you close this webpage and do not continue to this website.

✓ Click here to close this webpage.

✗ Continue to this website (not recommended).

More information

After you click **Yes** to proceed (or more precisely **Continue to this website (not recommended)** for Firefox browser for example), or if the browser of the client does not display a security alert, the web authentication system redirects the client to a login page, as shown in the image:



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

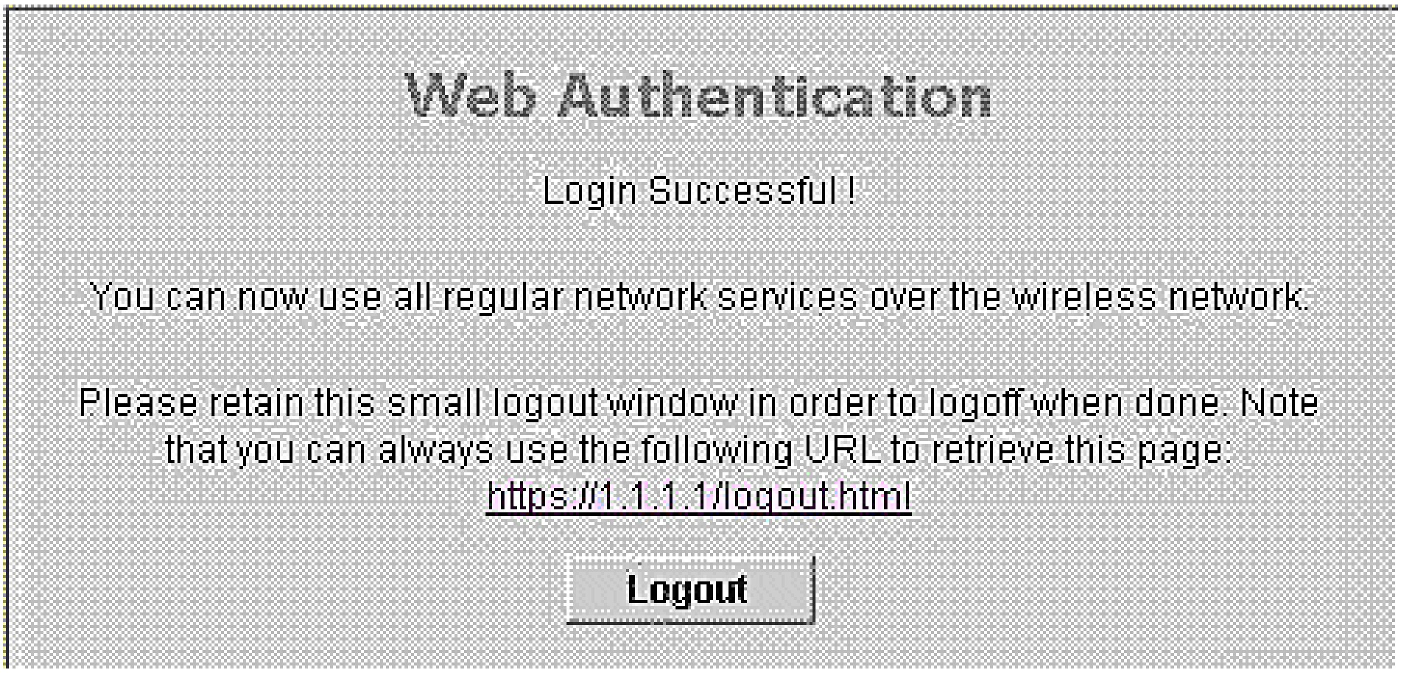
Password ●●●●

The default login page contains a Cisco logo and Cisco-specific text. You can choose to have the web authentication system display one of these:

- The default login page

- A modified version of the default login page
- A customized login page that you configure on an external web server
- A customized login page that you download to the controller

When you enter a valid username and password on the web authentication login page and click **Submit**, you are authenticated based upon the credentials submitted and a successful authentication from the backend database (LDAP in this case). The web authentication system then displays a successful login page and redirects the authenticated client to the requested URL.



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

The default successful login page contains a pointer to a virtual gateway address URL: https://1.1.1.1/logout.html. The IP address that you set for the controller virtual interface serves as the redirect address for the login page.

This document explains how to use the internal web page on the WLC for web authentication. This example uses a LDAP server as the backend database for web authentication to retrieve user credentials and authenticate the user.

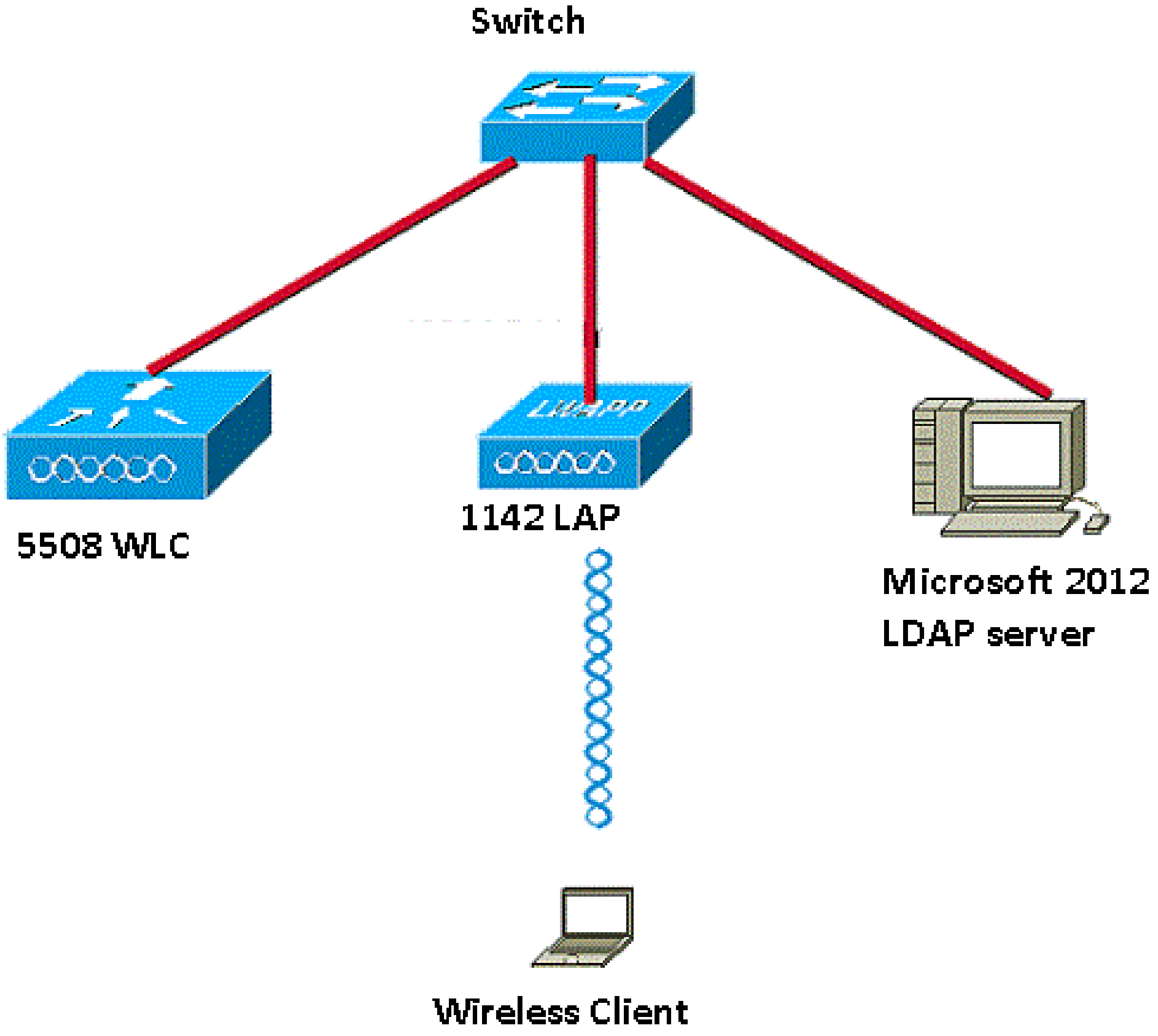
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Configurations

Complete these steps in order to successfully implement this setup:

- Configure LDAP Server.
- Configure WLC for LDAP Server.
- Configure the WLAN for Web Authentication.

Configure the LDAP Server

The first step is to configure the LDAP server, which serves as a backend database to store user credentials of the wireless clients. In this example, the Microsoft Windows 2012 Essentials server is used as the LDAP server.

The first step in the configuration of the LDAP server is to create a user database on the LDAP server so that the WLC can query this database to authenticate the user.

Create Users on the Domain Controller

An Organizational Unit (OU) contains multiple groups that carry references to personal entries in a PersonProfile. A person can be a member of multiple groups. All object class and attribute definitions are

LDAP schema default. Each group contains references (dn) for each person that belongs to it.

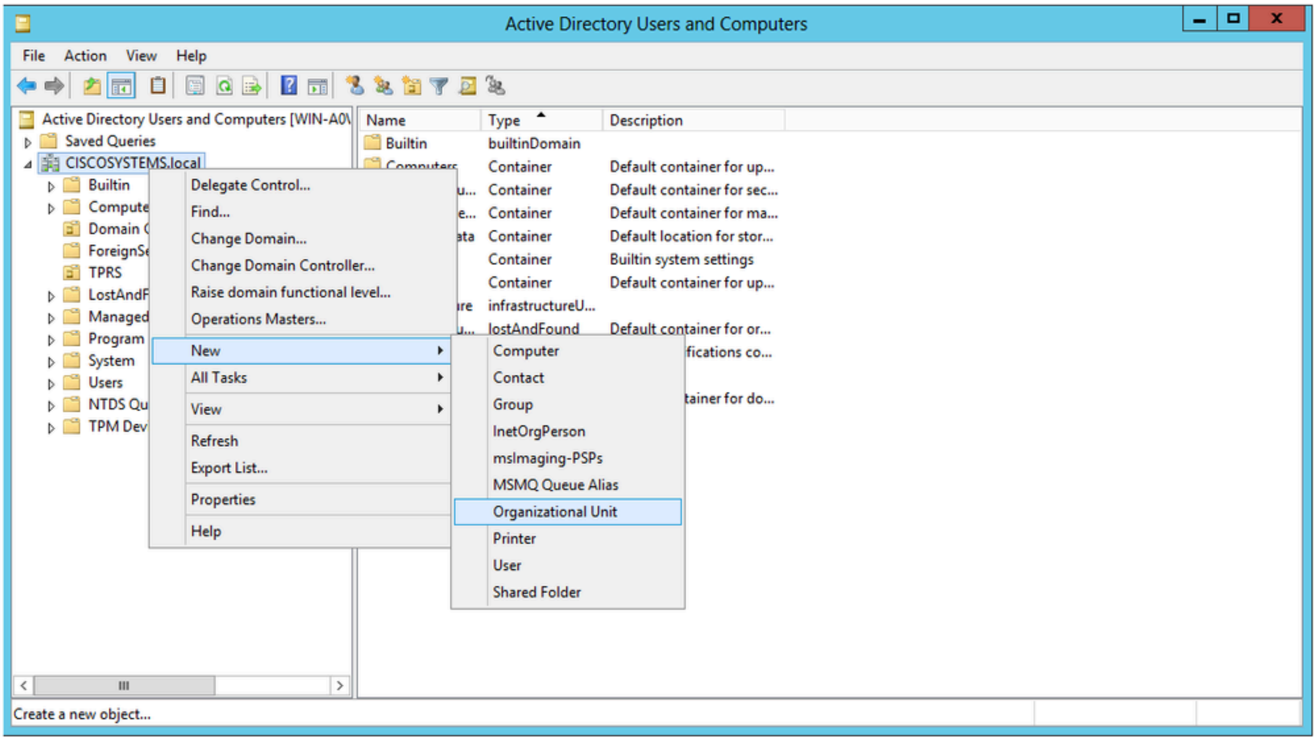
In this example, a new OU LDAP-USERS is created, and the user User1 is created under this OU. When you configure this user for LDAP access, the WLC can query this LDAP database for user authentication.

The domain used in this example is **CISCOSYSTEMS.local**.

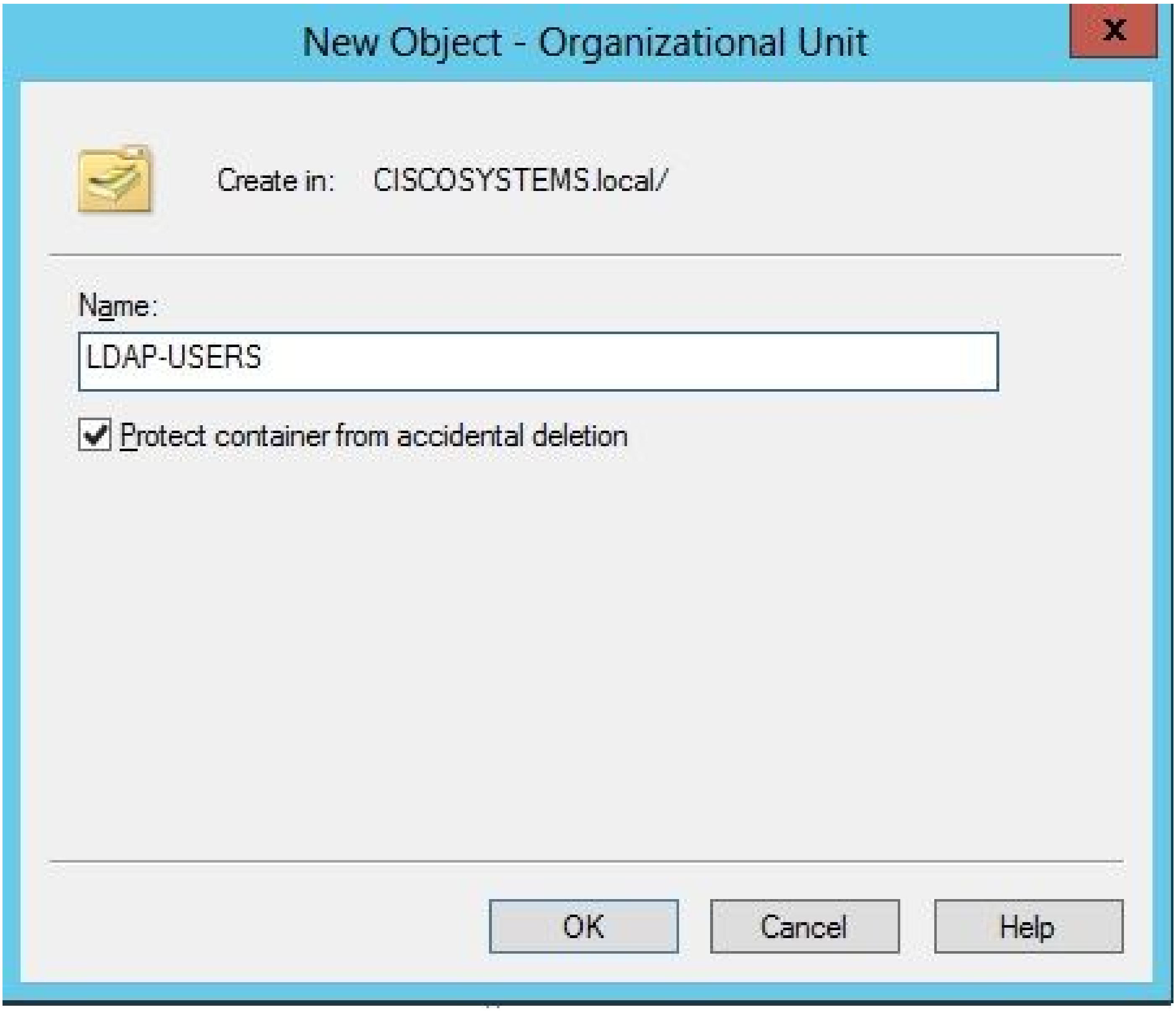
Create a User Database Under an OU

This section explains how to create a new OU in your domain and create a new user on this OU.

1. Open Windows PowerShell and type **servermanager.exe**
2. In the Server Manager window, click on **AD DS.** Then right-click your server name to choose **Active Directory Users and Computers.**
3. Right-click your domain name, which is **CISCOSYSTEMS.local** in this example, and then navigate to **New > Organizational Unit** from the context menu in order to create a new OU.



4. Assign a name to this OU and click **OK**, as shown in the image:



New Object - Organizational Unit

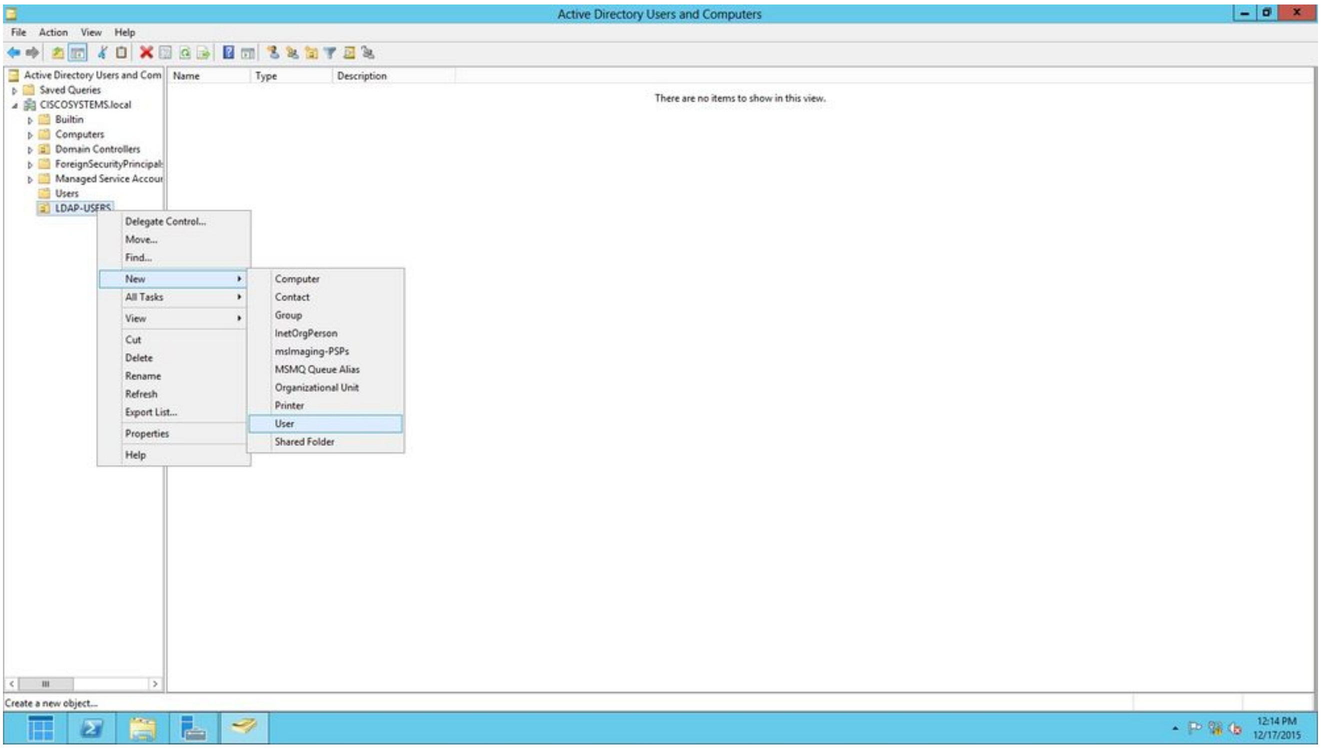
Create in: CISCOSYSTEMS.local/

Name: LDAP-USERS

☑ Protect container from accidental deletion

Now that the new OU LDAP-USERS is created on the LDAP server, the next step is to create user **User1** under this OU. In order to achieve this, complete these steps:

1. Right-click the new OU created. Navigate to **LDAP-USERS> New > User** from the resultant context menus in order to create a new user, as shown in the image:

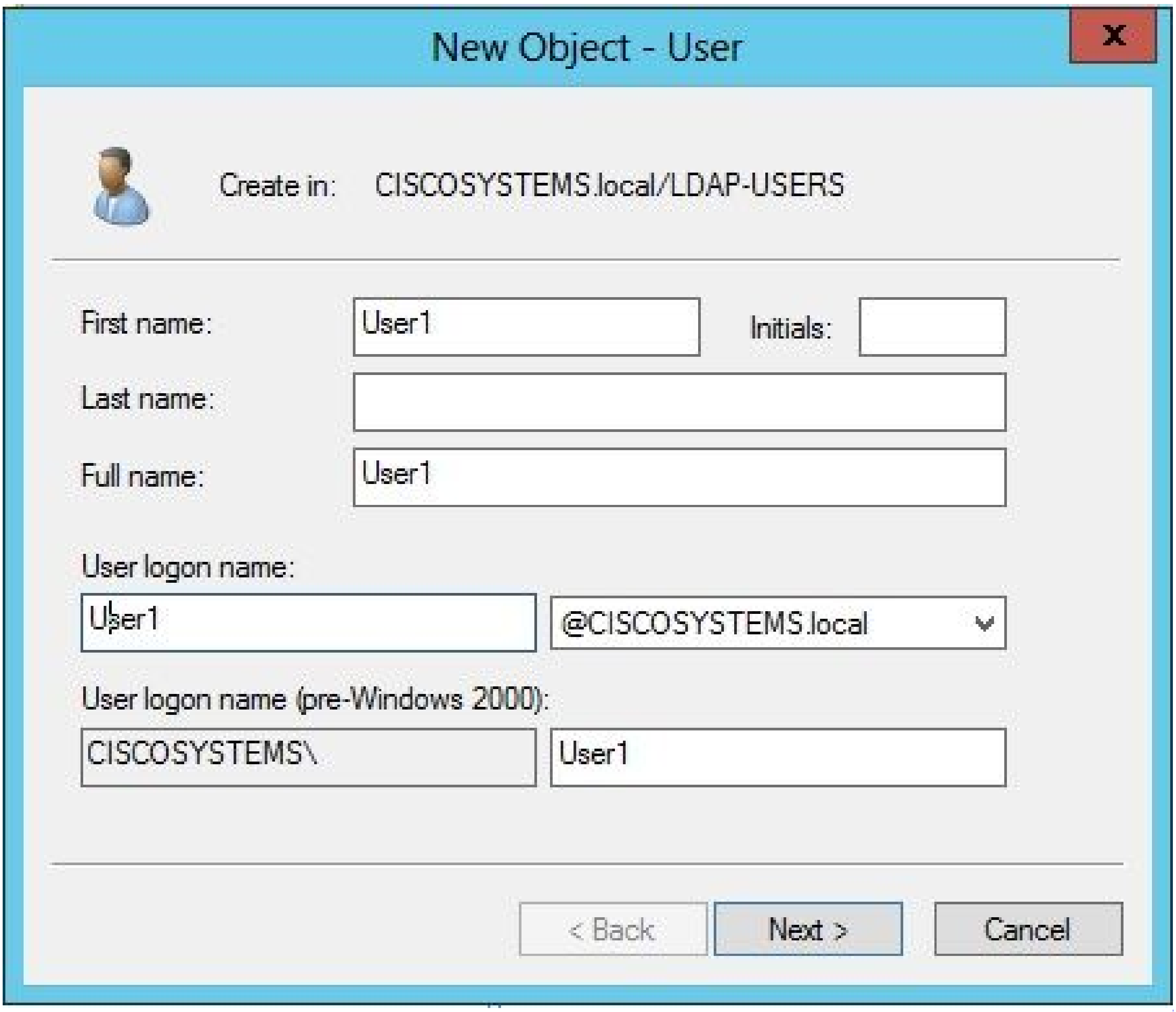


There are no items to show in this view.

Create a new object...

2. In the User setup page, fill in the required fields as shown in this example. This example has **User1** in the **User logon name** field.

   This is the username that is verified in the LDAP database to authenticate the client. This example uses User1 in the First name and Full Name fields. Click **Next**.



New Object - User

Create in: CISCOSYSTEMS.local/LDAP-USERS

First name: User1 Initials:

Last name:

Full name: User1

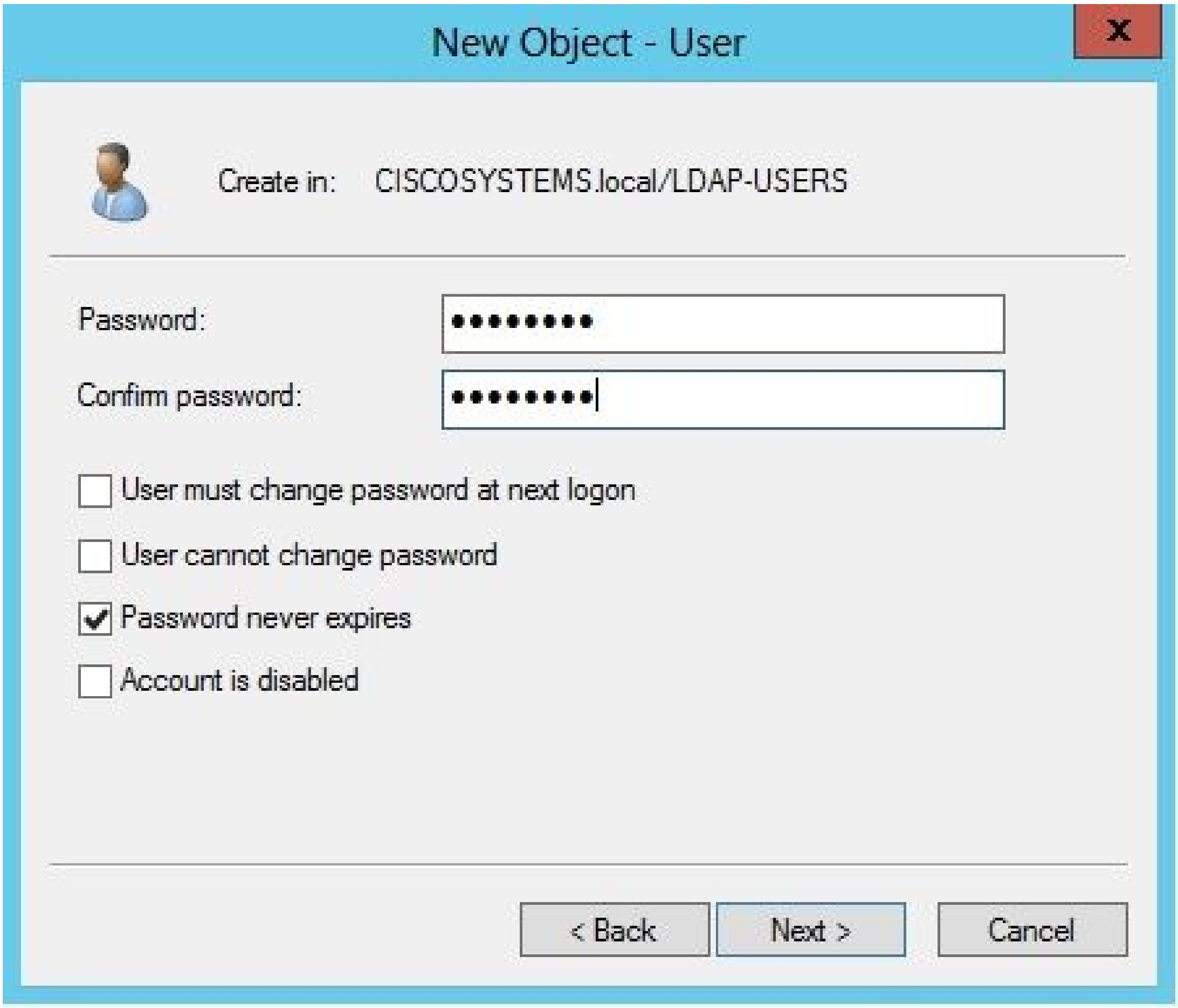
User logon name:

User1 @CISCOSYSTEMS.local

User logon name (pre-Windows 2000):

CISCOSYSTEMS\ User1

3. Enter a password and confirm the password. Choose the **Password never expires** option and click **Next**.



New Object - User

Create in: CISCOSYSTEMS.local/LDAP-USERS

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

□ User must change password at next logon

□ User cannot change password

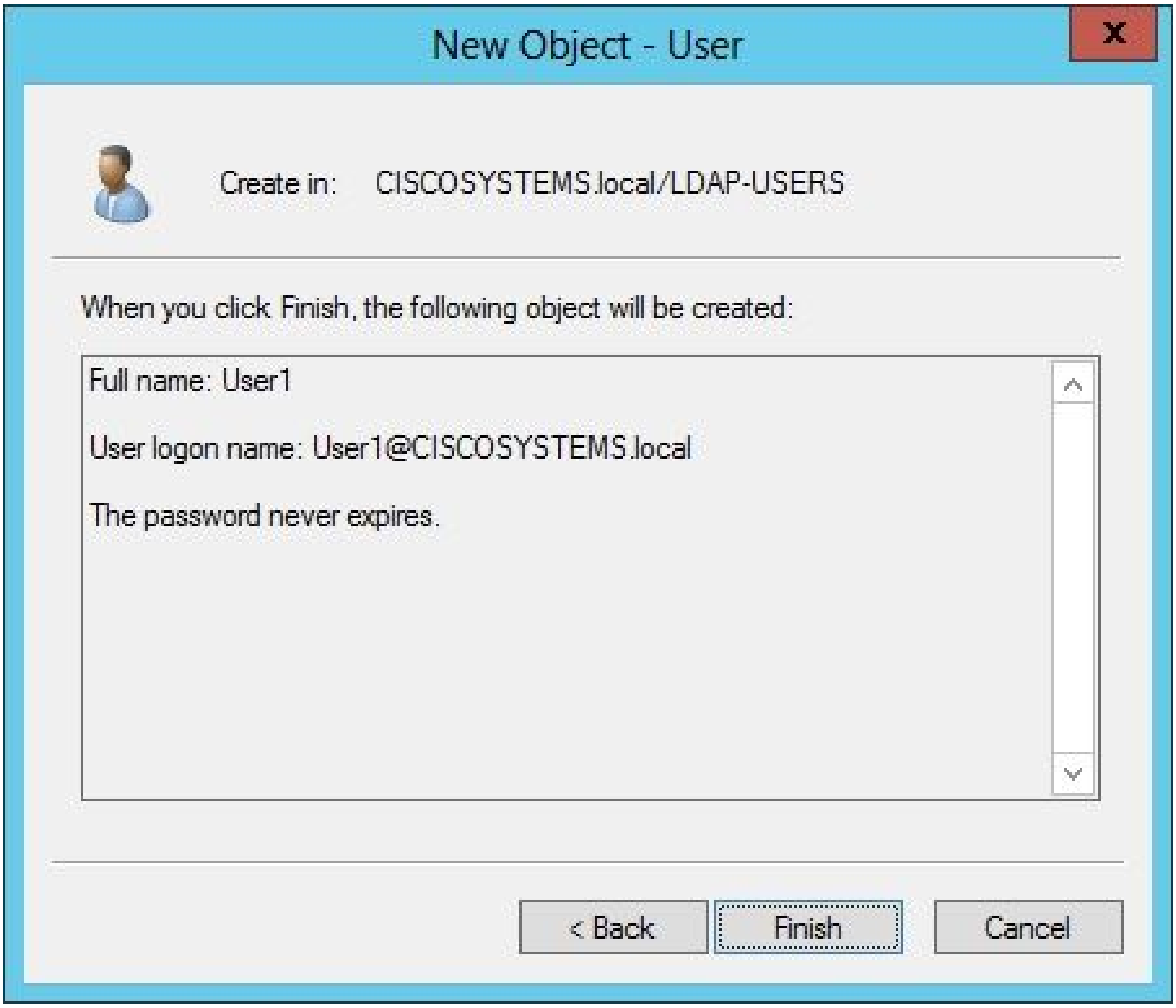
☑ Password never expires

□ Account is disabled

4. Click **Finish**.

A new user User1 is created under the OU LDAP-USERS. These are the user credentials:

- username: **User1**
- password: **Laptop123**



New Object - User

Create in: CISCOSYSTEMS.local/LDAP-USERS

When you click Finish, the following object will be created:

Full name: User1

User logon name: User1@CISCOSYSTEMS.local

The password never expires.

Now that the user is created under an OU, the next step is to configure this user for LDAP access.

Configure the User for LDAP Access

You can choose either **Anonymous** or **Authenticated** to specify the local authentication bind method for the LDAP server. The Anonymous method allows anonymous access to the LDAP server. The Authenticated method requires that a username and password to be entered to secure access. The default value is Anonymous.

This section explains how to configure both Anonymous and Authenticated methods.

Anonymous Bind

Note: Using Anonymous Bind is not recommended. An LDAP server that allows anonymous bind does not require any type of credentialed authentication. An attacker could take advantage of the Anonymous bind entry to view files on the LDAP director.

Perform the steps in this section in order to configure anonymous user for LDAP access.

Enable Anonymous Bind Feature on the Windows 2012 Essentials Server

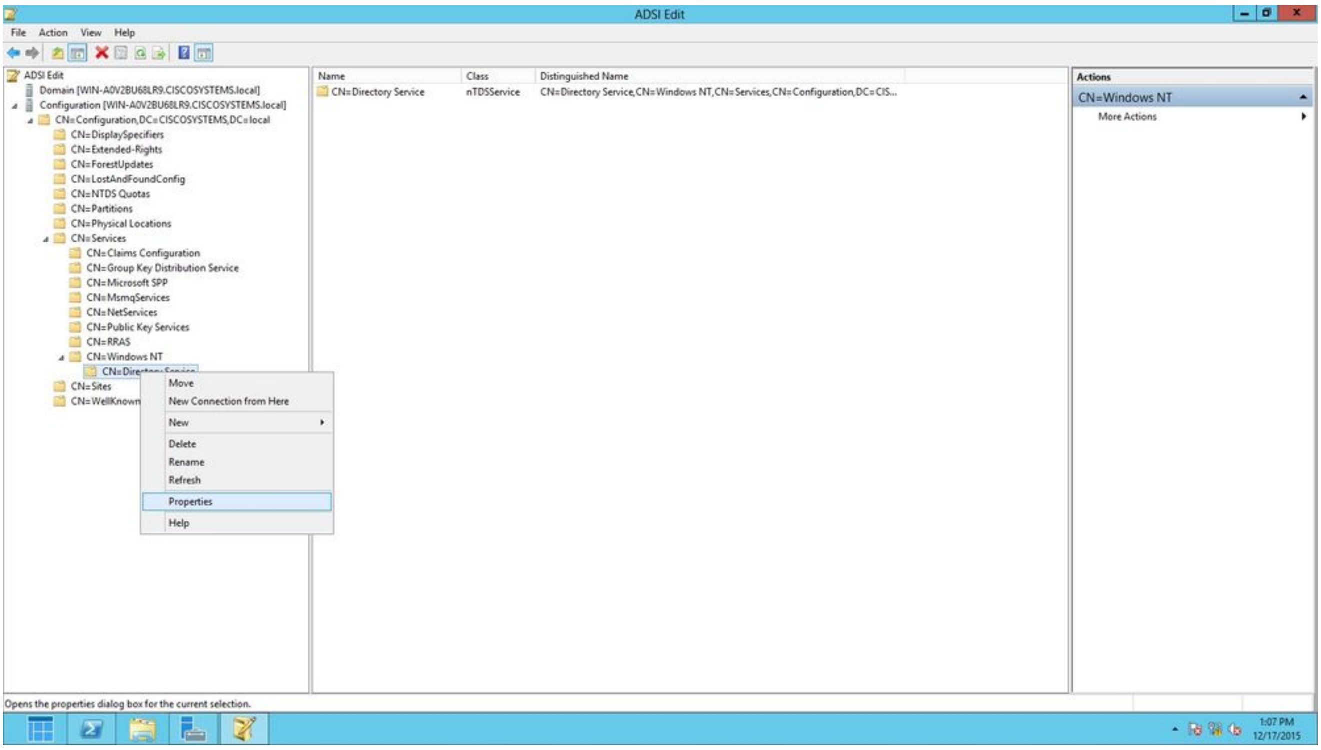
For any third-party applications (in our case WLC) to access Windows 2012 AD on the LDAP, the

Anonymous Bind feature must be enabled on Windows 2012. By default, anonymous LDAP operations are not permitted on Windows 2012 domain controllers. Perform these steps in order to enable the Anonymous Bind feature:

1. Launch the ADSI Edit tool by typing: **ADSIEdit.msc** in Windows PowerShell. This tool is part of the Windows 2012 support tools.

2. In the ADSI Edit window, expand the root domain (Configuration [WIN-A0V2BU68LR9.CISCOSYSTEMS.local]).

   Navigate to **CN=Services > CN=Windows NT > CN=Directory Service**. Right-click the **CN=Directory Service** container, and choose **Properties** from the context menu, as shown in the image:

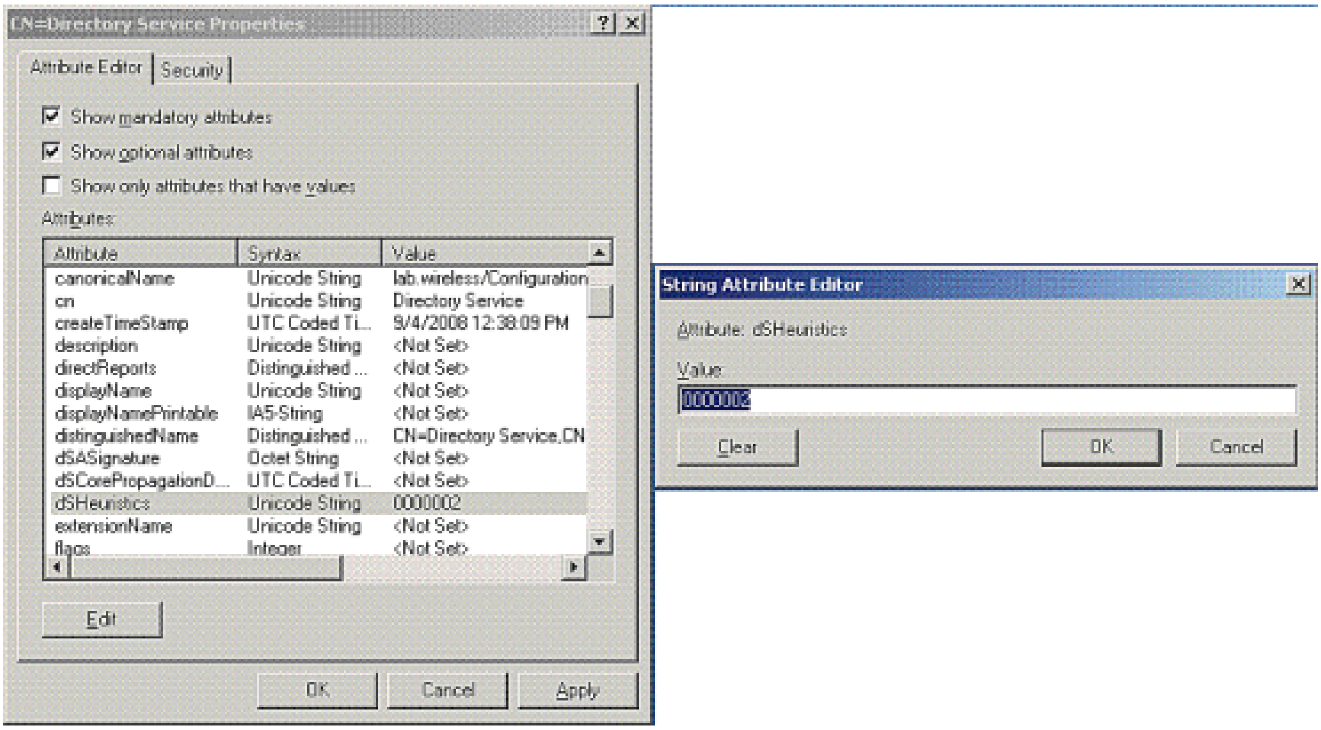


Name	Class	Distinguished Name
CN=Directory Service	nTDSService	CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=CIS...

Opens the properties dialog box for the current selection.

3. In the CN=Directory Service Properties window, under **Attributes**, click the **dsHeuristics** attribute under the Attribute field and choose **Edit**. In the String Attribute Editor window of this attribute, enter the value **0000002**; click **Apply** and **OK**, as shown in the image. The Anonymous Bind feature is enabled on the Windows 2012 server.

   Note: The last (seventh) character is the one that controls the way you can bind to LDAP service. 0 (zero) or no seventh character means that anonymous LDAP operations are disabled. If you set the seventh character to 2, it enables the Anonymous Bind feature.



☑ Show mandatory attributes

☑ Show optional attributes

□ Show only attributes that have values

Attributes:

Attribute	Syntax	Value
canonicalName	Unicode String	lab.wireless/Configuration
cn	Unicode String	Directory Service
createTimeStamp	UTC Coded Ti...	9/4/2008 12:38:09 PM
description	Unicode String	<Not Set>
directReports	Distinguished ...	<Not Set>
displayName	Unicode String	<Not Set>
displayNamePrintable	IA5-String	<Not Set>
distinguishedName	Distinguished ...	CN=Directory Service,CN
dSASignature	Octet String	<Not Set>
dSCorePropagationD...	UTC Coded Ti...	<Not Set>
dSHeuristics	Unicode String	0000002
extensionName	Unicode String	<Not Set>
flags	Integer	<Not Set>

Attribute: dSHeuristics

Value: 0000002

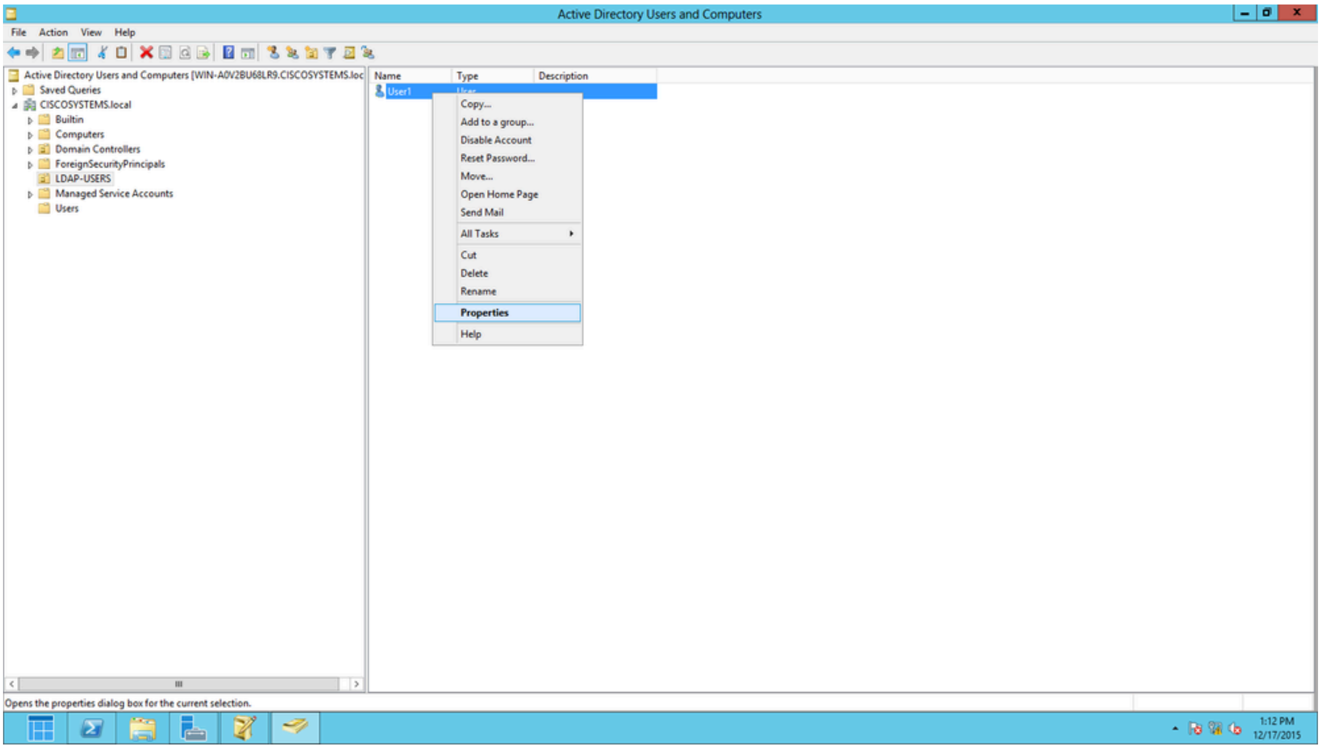
Granting ANONYMOUS LOGON Access to the User

The next step is to grant ANONYMOUS LOGON access to the user User1. Complete these steps in order to achieve this:

1. Open **Active Directory Users and Computers**.

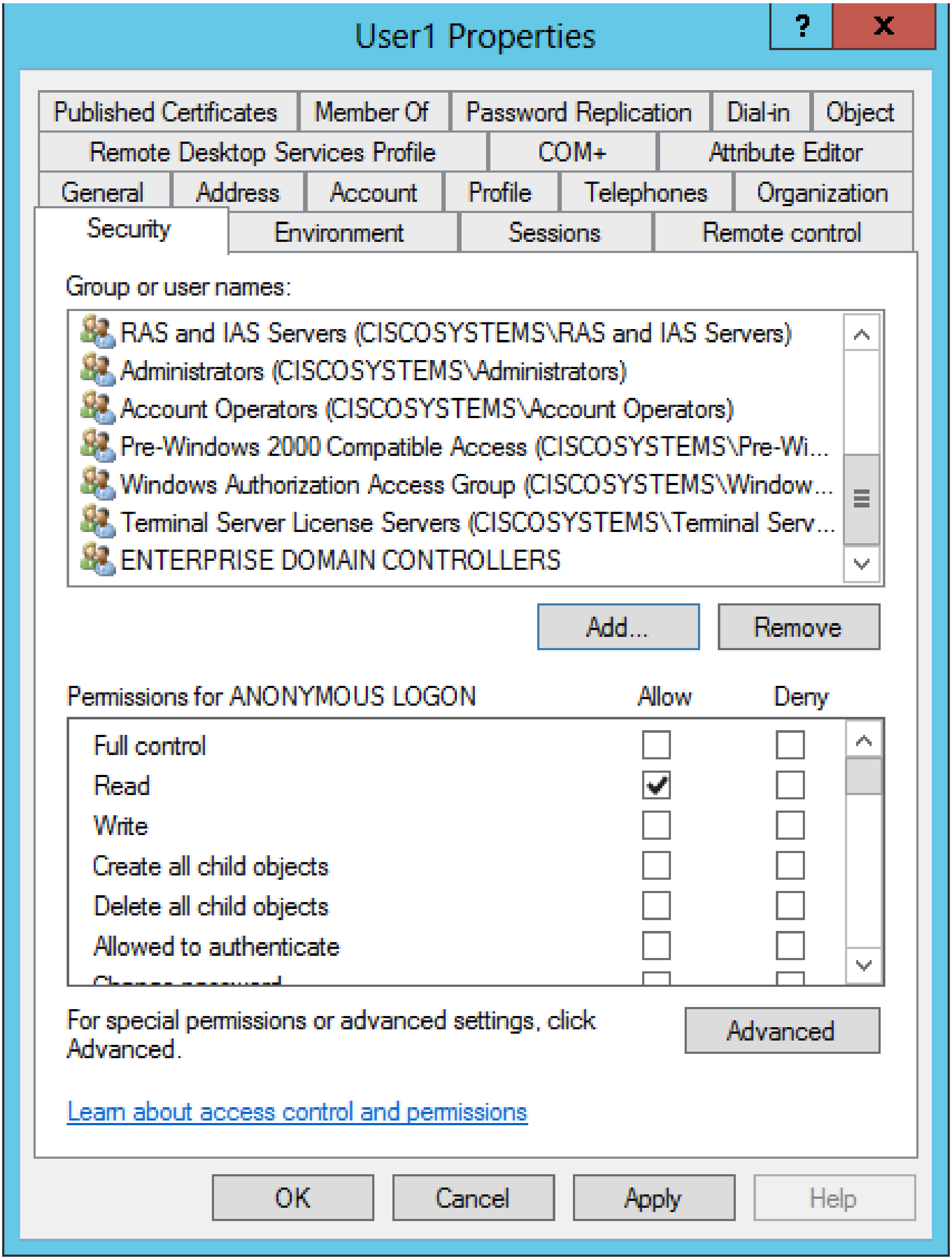
2. Ensure that the **View Advanced Features** is checked.

3. Navigate to the user User1 and right-click it. Choose **Properties** from the context menu. This user is identified with the first name User1.



Opens the properties dialog box for the current selection.

4. Click the **Security** tab, as shown in the image:



Group or user names:

- RAS and IAS Servers (CISCOSYSTEMS\RAS and IAS Servers)
- Administrators (CISCOSYSTEMS\Administrators)
- Account Operators (CISCOSYSTEMS\Account Operators)
- Pre-Windows 2000 Compatible Access (CISCOSYSTEMS\Pre-Wi...
- Windows Authorization Access Group (CISCOSYSTEMS\Window...
- Terminal Server License Servers (CISCOSYSTEMS\Terminal Serv...
- ENTERPRISE DOMAIN CONTROLLERS

Permissions for ANONYMOUS LOGON	Allow	Deny
Full control	□	□
Read	☑	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□
Allowed to authenticate	□	□
Change password	□	□

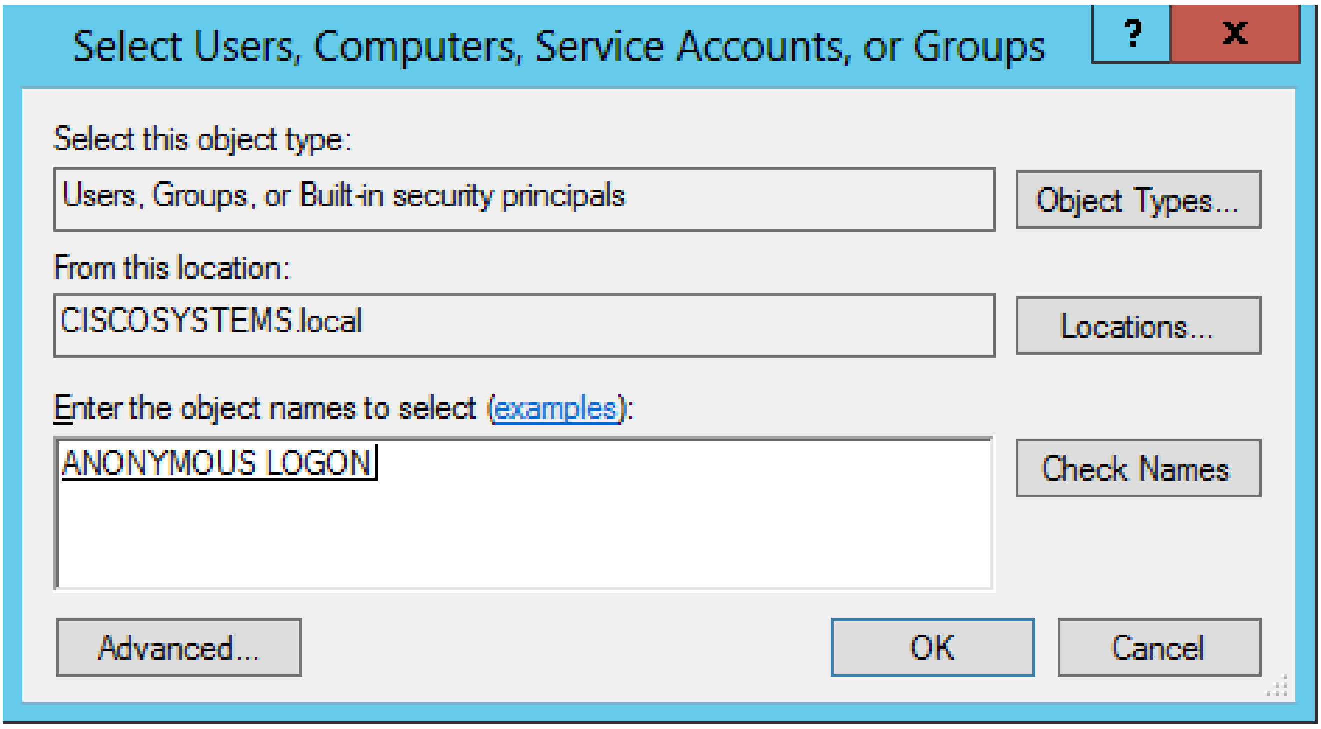
For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

5. Click **Add** in the resultant window.

6. Enter **ANONYMOUS LOGON** under the *Enter the object names to select* box and acknowledge the

dialog, as shown in the image:



Select Users, Computers, Service Accounts, or Groups

Select this object type:

Users, Groups, or Built-in security principals

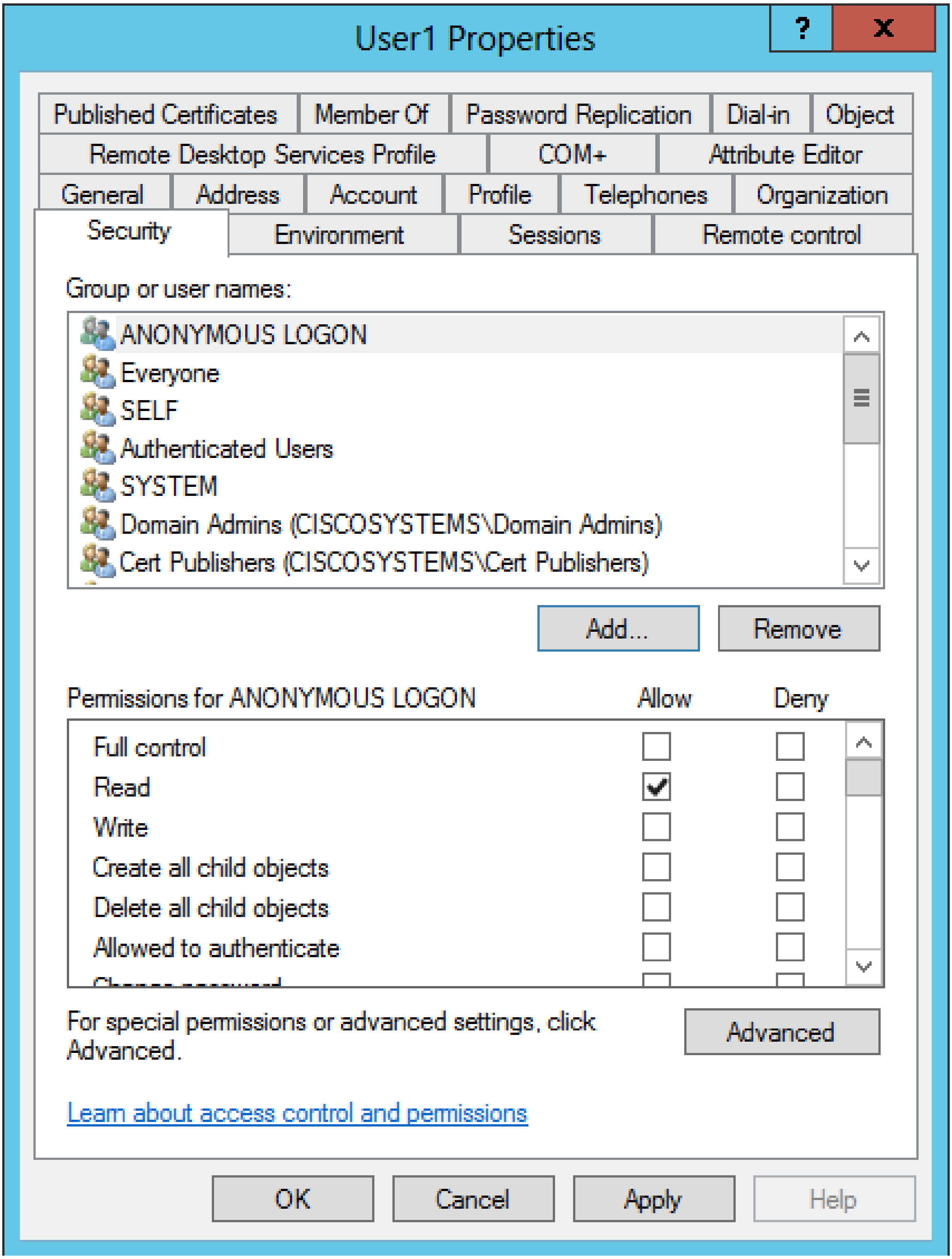
From this location:

CISCOSYSTEMS.local

Enter the object names to select (examples):

ANONYMOUS LOGON

7. In the ACL, notice that ANONYMOUS LOGON has access to some property sets of the user. Click **OK**. The ANONYMOUS LOGON access is granted to this user, as shown in the image:



Group or user names:

- ANONYMOUS LOGON
- Everyone
- SELF
- Authenticated Users
- SYSTEM
- Domain Admins (CISCOSYSTEMS\Domain Admins)
- Cert Publishers (CISCOSYSTEMS\Cert Publishers)

Permissions for ANONYMOUS LOGON	Allow	Deny
Full control	□	□
Read	☑	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□
Allowed to authenticate	□	□
Change password	□	□

For special permissions or advanced settings, click Advanced.

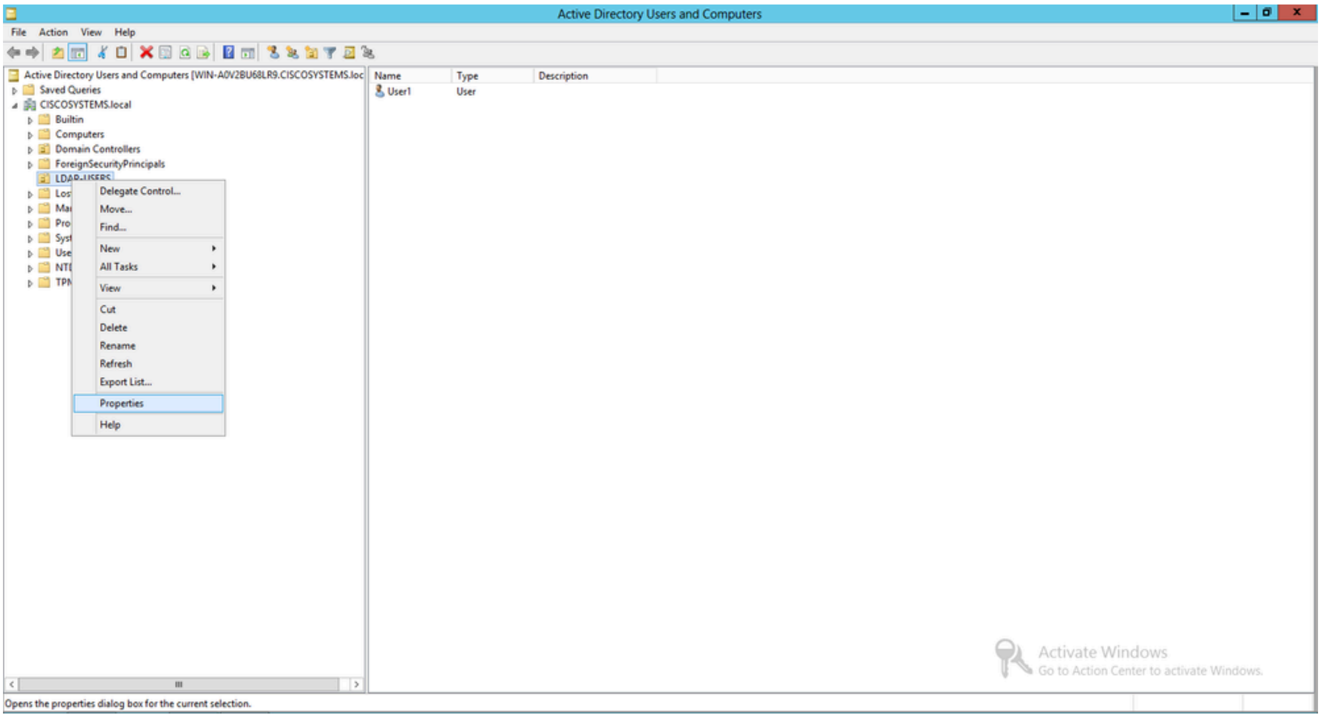
Learn about access control and permissions

Grant List Contents Permission on the OU

The next step is to grant at least List Contents permission to the ANONYMOUS LOGON on the OU in which the user is located. In this example, User1 is located on the OU LDAP-USERS. Complete these steps in order to achieve this:

1. In **Active Directory Users and Computers**, right-click the **OU LDAP-USERS** and choose

Properties, as shown in the image:

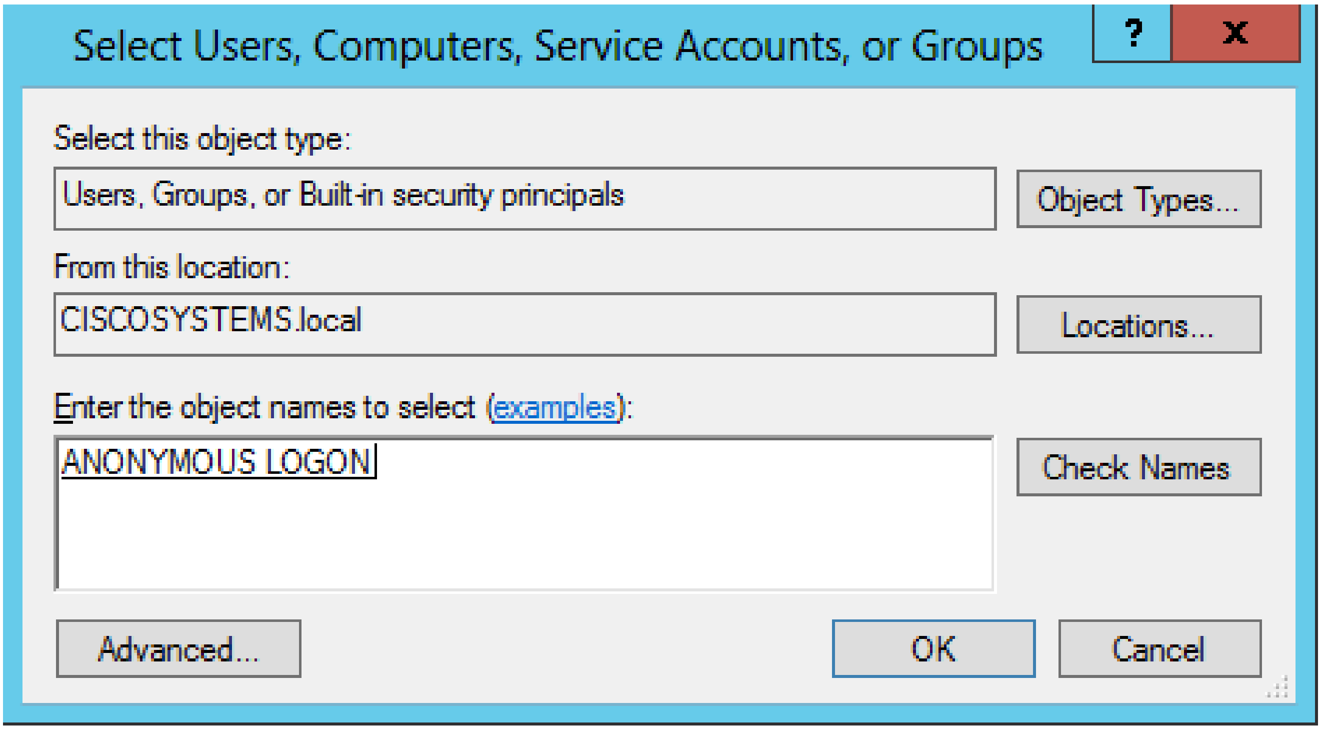


Name	Type	Description
User1	User	

Opens the properties dialog box for the current selection.

2. Click **Security**.

3. Click **Add**. In the dialog that opens, enter **ANONYMOUS LOGON** and Acknowledge the dialog, as shown in the image:



Users, Groups, or Built-in security principals

CISCOSYSTEMS.local

ANONYMOUS LOGON

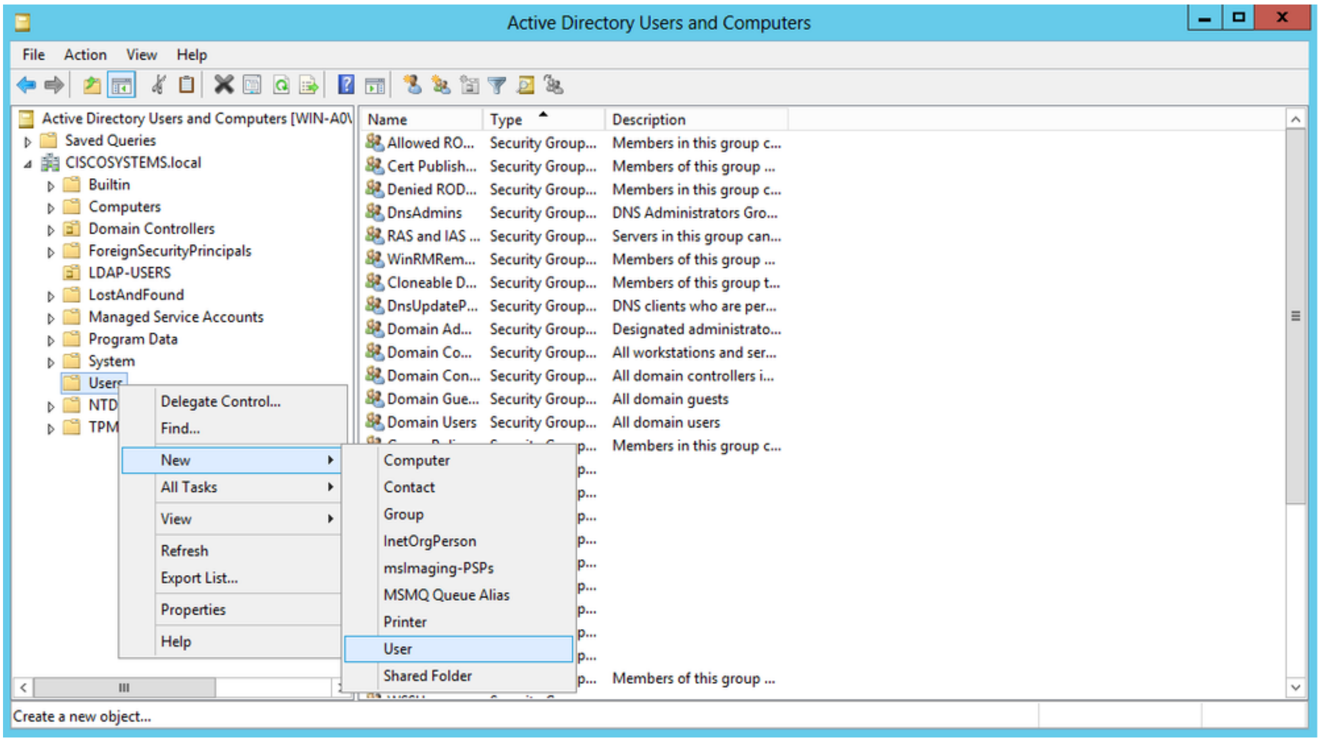
Authenticated Bind

Perform the steps in this section in order to configure a user for local authentication to the LDAP server.

1. Open Windows PowerShell and type **servermanager.exe**

2. In the Server Manager window, click on **AD DS.** Then right-click your server name to choose **Active Directory Users and Computers.**

3. Right-click **Users**. Navigate to **New** > **User** from the resultant context menus in order to create a new user.



Name	Type	Description
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
RAS and IAS ...	Security Group...	Servers in this group can...
WinRMRem...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users

4. In the User setup page, fill in the required fields as shown in this example. This example has **WLC-admin** in the **User logon name** field. This is the username to be used for local authentication to the LDAP server. Click **Next**.

5. Enter a password and confirm the password. Choose the **Password never expires** option and click **Next**.

6. Click **Finish**.

   A new user WLC-admin is created under the **Users** container. These are the user credentials:

   - username: **WLC-admin**
   - password: **Admin123**

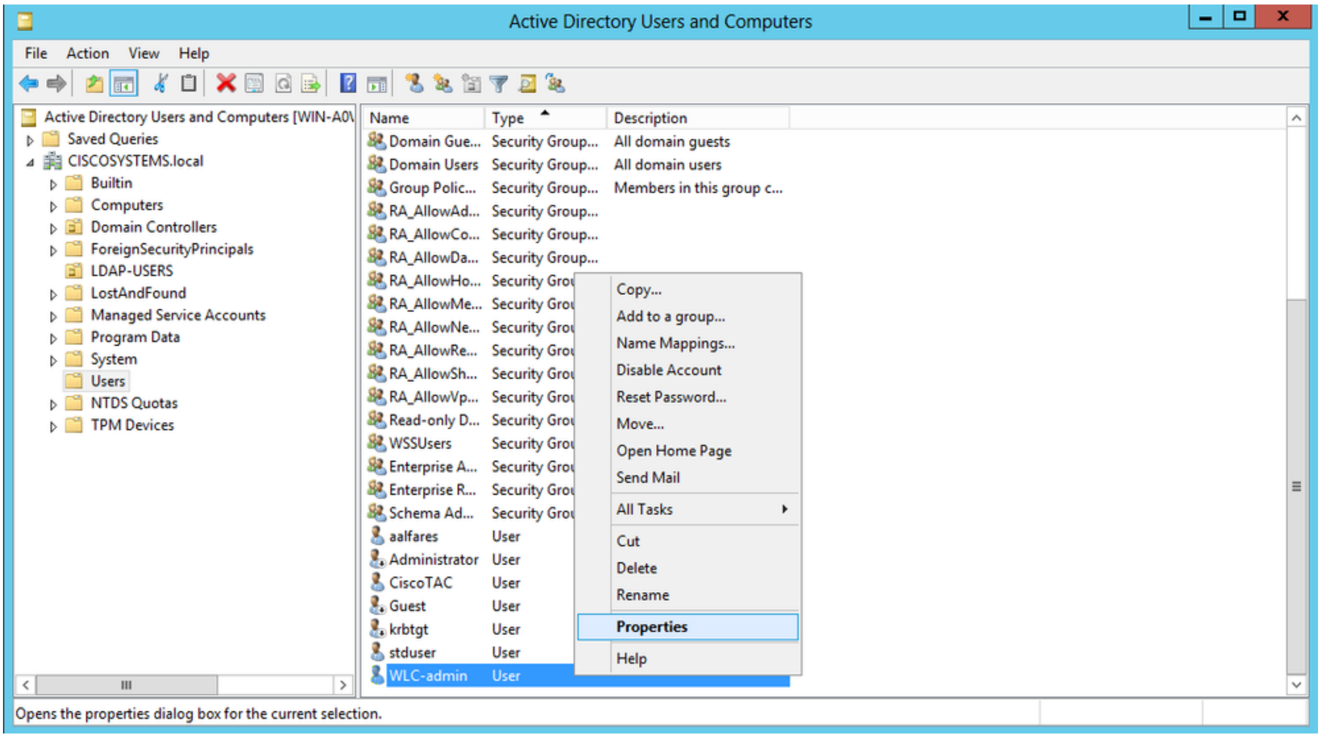
Granting Administrator privilages to WLC-admin

Now that the local authentication user is created, we need to grant it Administrator privilages. Complete these steps in order to achieve this:

1. Open **Active Directory Users and Computers**.

2. Ensure that the **View Advanced Features** is checked.

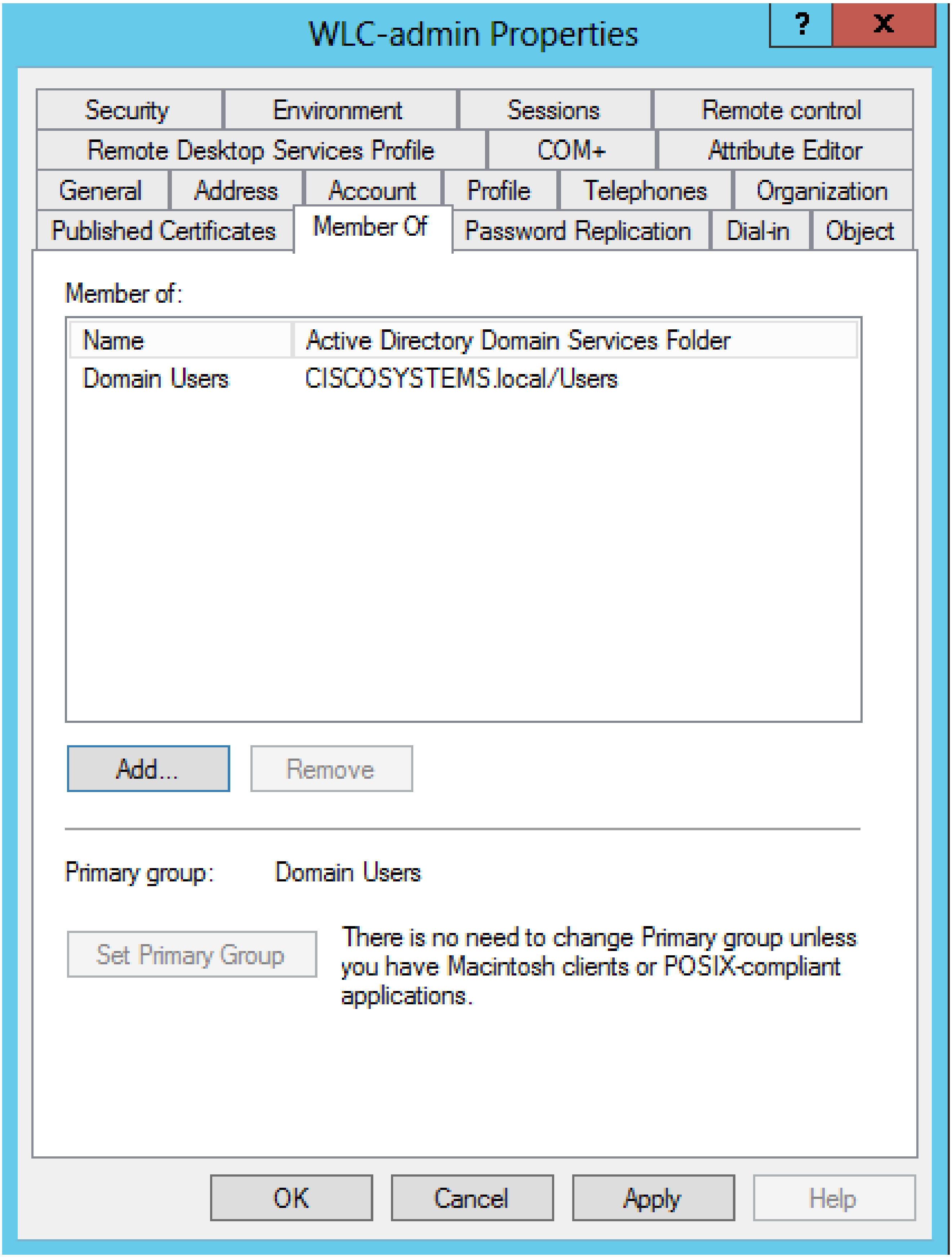
3. Navigate to the user **WLC-admin** and right-click it. Choose **Properties** from the context menu, as shown in the image. This user is identified with the first name WLC-admin.



Name	Type	Description
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Group Polic...	Security Group...	Members in this group c...
RA_AllowAd...	Security Group...	
RA_AllowCo...	Security Group...	
RA_AllowDa...	Security Group...	
RA_AllowHo...	Security Grou	
RA_AllowMe...	Security Grou	
RA_AllowNe...	Security Grou	
RA_AllowRe...	Security Grou	
RA_AllowSh...	Security Grou	
RA_AllowVp...	Security Grou	
Read-only D...	Security Grou	
WSSUsers	Security Grou	
Enterprise A...	Security Grou	
Enterprise R...	Security Grou	
Schema Ad...	Security Grou	
aalfares	User	
Administrator	User	
CiscoTAC	User	
Guest	User	
krbtgt	User	
stduser	User	
WLC-admin	User	

Opens the properties dialog box for the current selection.

4. Click the **Memeber Of** tab, as shown in the image:



Member of:

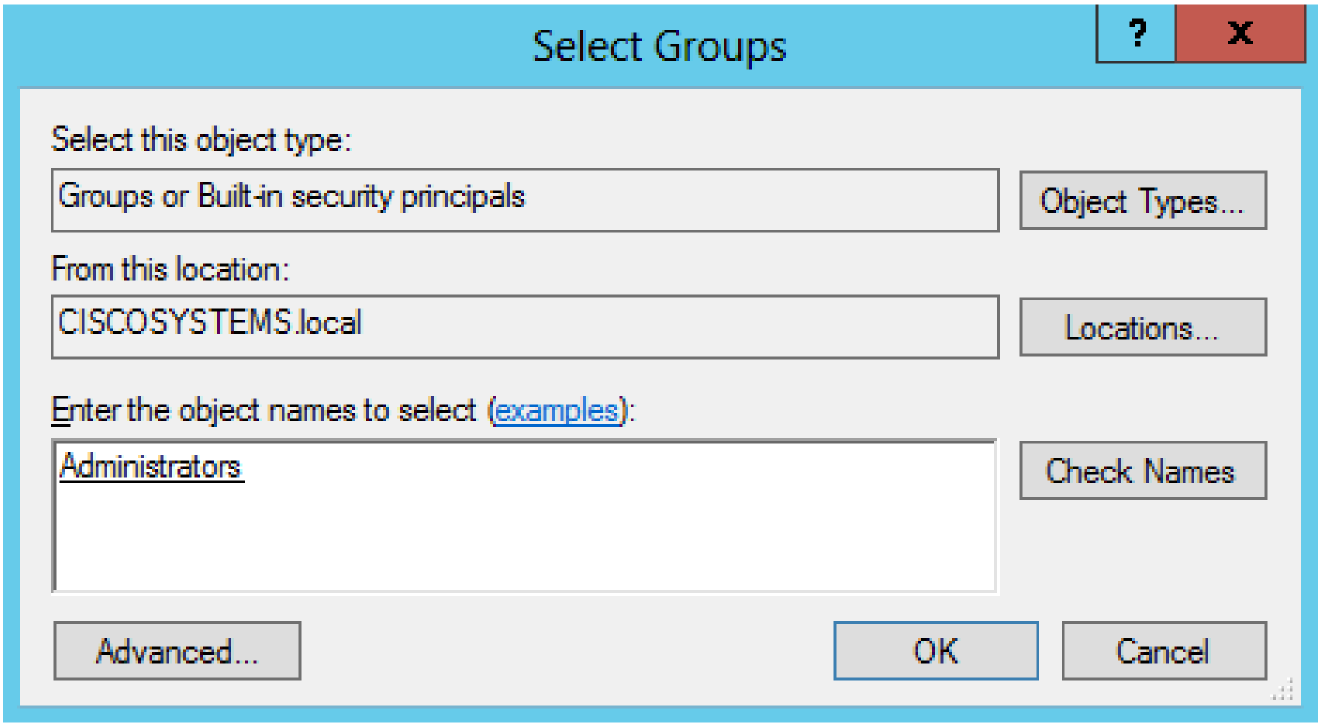
Name	Active Directory Domain Services Folder
Domain Users	CISCOSYSTEMS.local/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

::

5. Click **Add**. In the dialog that opens, enter **Administrators** and click **OK**, As shown in the image:



Select this object type:
Groups or Built-in security principals
From this location:
CISCOSYSTEMS.local
Enter the object names to select (examples):
Administrators

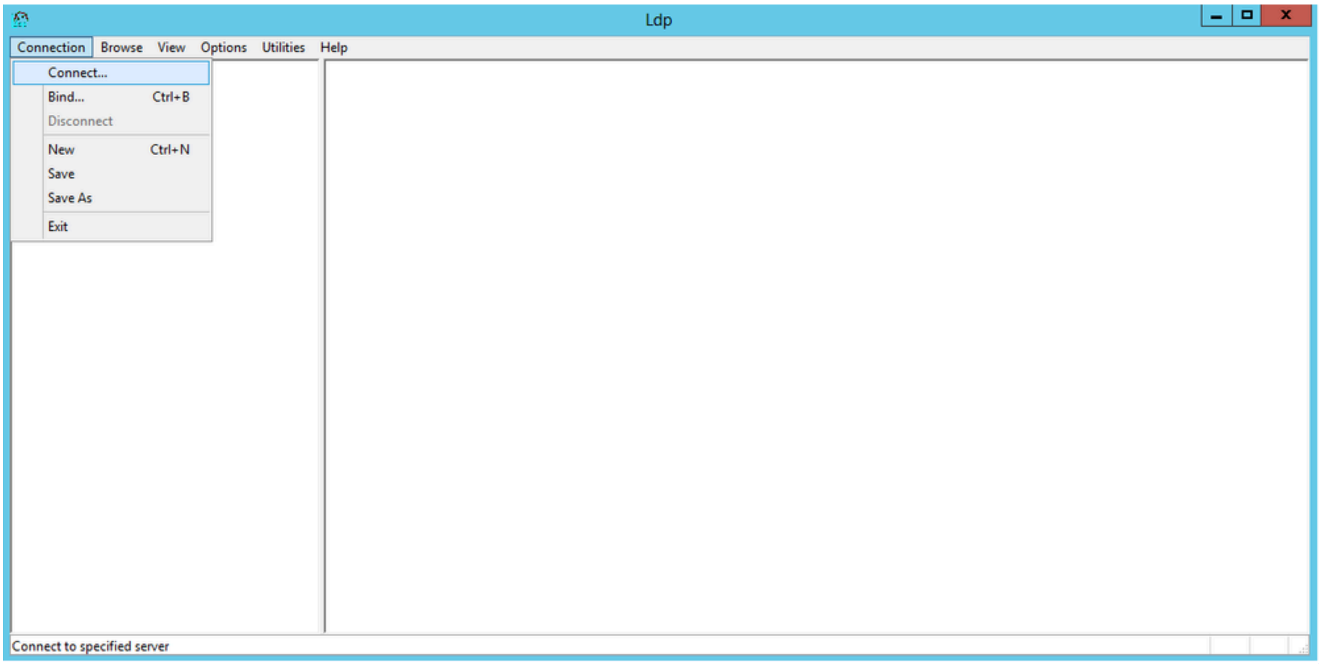
Use LDP to Identify the User Attributes

This GUI tool is a LDAP client that allows users to perform operations, such as connect, bind, search, modify, add, or delete, against any LDAP-compatible directory, such as Active Directory. LDP is used to view objects that are stored in Active Directory along with their metadata, such as security descriptors and replication metadata.

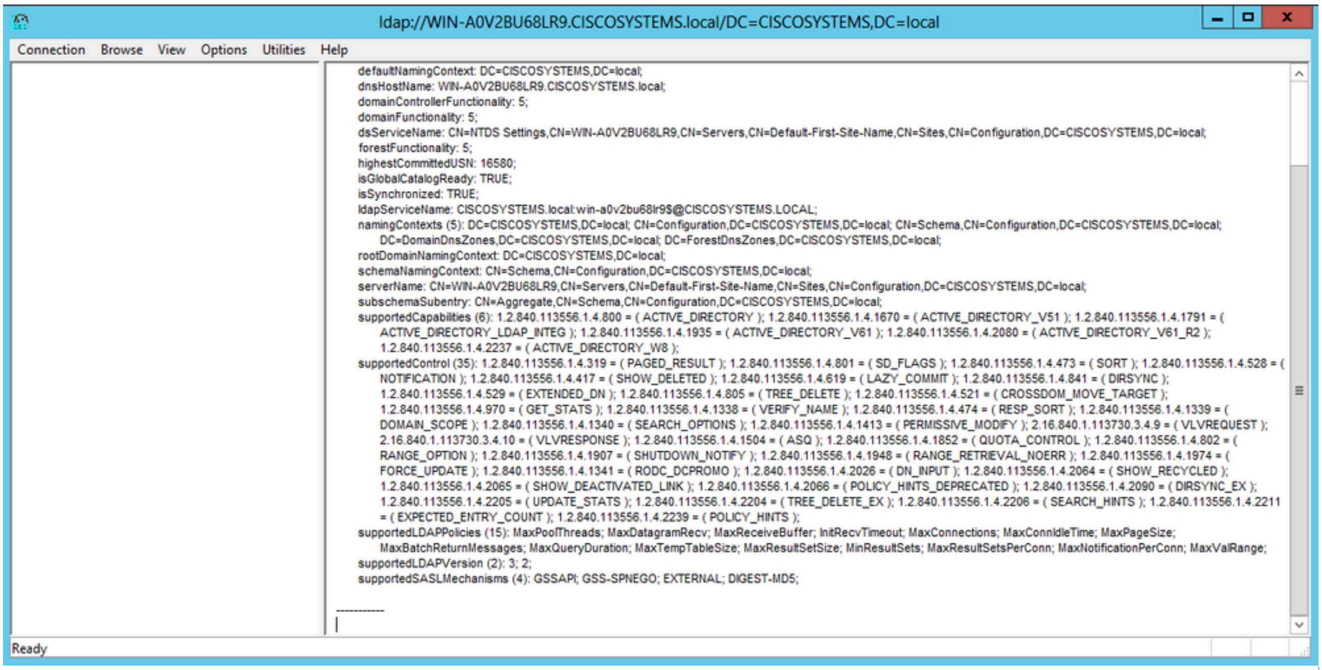
The LDP GUI tool is included when you install the Windows Server 2003 Support Tools from the product CD. This section explains how to use the LDP utility to identify the specific attributes associated to the user User1. Some of these attributes are used to fill in the LDAP server configuration parameters on the WLC, such as User Attribute type and User Object type.

1. On the Windows 2012 server (even on the same LDAP server), open the Windows PowerShell and enter **LDP** in order to access the LDP browser**.**

2. In the LDP main window, Navigate to **Connection** > **Connect** and connect to the LDAP server when you enter the IP address of the LDAP server, as shown in the image.



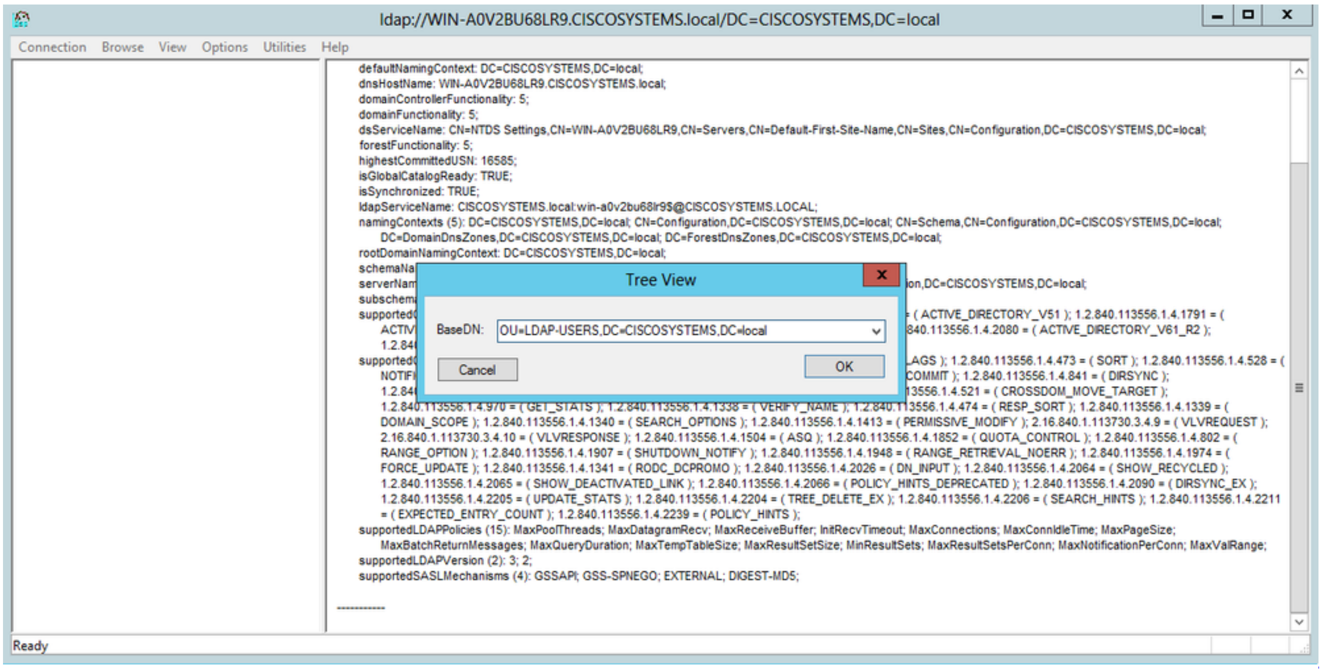
3. Once connected to the LDAP server, choose **View** from the main menu and click **Tree**, as shown in the image:


ldap://WIN-A0V2BU68LR9.CISCOSYSTEMS.local/DC=CISCOSYSTEMS,DC=local
Connection
Browse
View
Options
Utilities
Help
Ready

```
	defaultNamingContext: DC=CISCOSYSTEMS,DC=local;
	dnsHostName: WIN-A0V2BU68LR9.CISCOSYSTEMS.local;
	domainControllerFunctionality: 5;
	domainFunctionality: 5;
	dsServiceName: CN=NTDS Settings,CN=WIN-A0V2BU68LR9,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=CISCOSYSTEMS,DC=local;
	forestFunctionality: 5;
	highestCommittedUSN: 16580;
	isGlobalCatalogReady: TRUE;
	isSynchronized: TRUE;
	ldapServiceName: CISCOSYSTEMS.local:win-a0v2bu68lr9$@CISCOSYSTEMS.LOCAL;
	namingContexts (5): DC=CISCOSYSTEMS,DC=local; CN=Configuration,DC=CISCOSYSTEMS,DC=local; CN=Schema,CN=Configuration,DC=CISCOSYSTEMS,DC=local;
		DC=DomainDnsZones,DC=CISCOSYSTEMS,DC=local; DC=ForestDnsZones,DC=CISCOSYSTEMS,DC=local;
	rootDomainNamingContext: DC=CISCOSYSTEMS,DC=local;
	schemaNamingContext: CN=Schema,CN=Configuration,DC=CISCOSYSTEMS,DC=local;
	serverName: CN=WIN-A0V2BU68LR9,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=CISCOSYSTEMS,DC=local;
	subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=CISCOSYSTEMS,DC=local;
	supportedCapabilities (6): 1.2.840.113556.1.4.800 = ( ACTIVE_DIRECTORY ); 1.2.840.113556.1.4.1670 = ( ACTIVE_DIRECTORY_V51 ); 1.2.840.113556.1.4.1791 = (
		ACTIVE_DIRECTORY_LDAP_INTEG ); 1.2.840.113556.1.4.1935 = ( ACTIVE_DIRECTORY_V61 ); 1.2.840.113556.1.4.2080 = ( ACTIVE_DIRECTORY_V61_R2 );
		1.2.840.113556.1.4.2237 = ( ACTIVE_DIRECTORY_W8 );
	supportedControl (35): 1.2.840.113556.1.4.319 = ( PAGED_RESULT ); 1.2.840.113556.1.4.801 = ( SD_FLAGS ); 1.2.840.113556.1.4.473 = ( SORT ); 1.2.840.113556.1.4.528 = (
		NOTIFICATION ); 1.2.840.113556.1.4.417 = ( SHOW_DELETED ); 1.2.840.113556.1.4.619 = ( LAZY_COMMIT ); 1.2.840.113556.1.4.841 = ( DIRSYNC );
		1.2.840.113556.1.4.529 = ( EXTENDED_DN ); 1.2.840.113556.1.4.805 = ( TREE_DELETE ); 1.2.840.113556.1.4.521 = ( CROSSDOM_MOVE_TARGET );
		1.2.840.113556.1.4.970 = ( GET_STATS ); 1.2.840.113556.1.4.1338 = ( VERIFY_NAME ); 1.2.840.113556.1.4.474 = ( RESP_SORT ); 1.2.840.113556.1.4.1339 = (
		DOMAIN_SCOPE ); 1.2.840.113556.1.4.1340 = ( SEARCH_OPTIONS ); 1.2.840.113556.1.4.1413 = ( PERMISSIVE_MODIFY ); 2.16.840.1.113730.3.4.9 = ( VLVREQUEST );
		2.16.840.1.113730.3.4.10 = ( VLVRESPONSE ); 1.2.840.113556.1.4.1504 = ( ASQ ); 1.2.840.113556.1.4.1852 = ( QUOTA_CONTROL ); 1.2.840.113556.1.4.802 = (
		RANGE_OPTION ); 1.2.840.113556.1.4.1907 = ( SHUTDOWN_NOTIFY ); 1.2.840.113556.1.4.1948 = ( RANGE_RETRIEVAL_NOERR ); 1.2.840.113556.1.4.1974 = (
		FORCE_UPDATE ); 1.2.840.113556.1.4.1341 = ( RODC_DCPROMO ); 1.2.840.113556.1.4.2026 = ( DN_INPUT ); 1.2.840.113556.1.4.2064 = ( SHOW_RECYCLED );
		1.2.840.113556.1.4.2065 = ( SHOW_DEACTIVATED_LINK ); 1.2.840.113556.1.4.2066 = ( POLICY_HINTS_DEPRECATED ); 1.2.840.113556.1.4.2090 = ( DIRSYNC_EX );
		1.2.840.113556.1.4.2205 = ( UPDATE_STATS ); 1.2.840.113556.1.4.2204 = ( TREE_DELETE_EX ); 1.2.840.113556.1.4.2206 = ( SEARCH_HINTS ); 1.2.840.113556.1.4.2211
		= ( EXPECTED_ENTRY_COUNT ); 1.2.840.113556.1.4.2239 = ( POLICY_HINTS );
	supportedLDAPPolicies (15): MaxPoolThreads; MaxDatagramRecv; MaxReceiveBuffer; InitRecvTimeout; MaxConnections; MaxConnIdleTime; MaxPageSize;
		MaxBatchReturnMessages; MaxQueryDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange;
	supportedLDAPVersion (2): 3; 2;
	supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;

-----------
```

4. In the resultant Tree View window, enter the **BaseDN** of the user. In this example, User1 is located under the OU "LDAP-USERS" under the domain CISCOSYSTEMS.local. Click **OK**, as shown in the image:

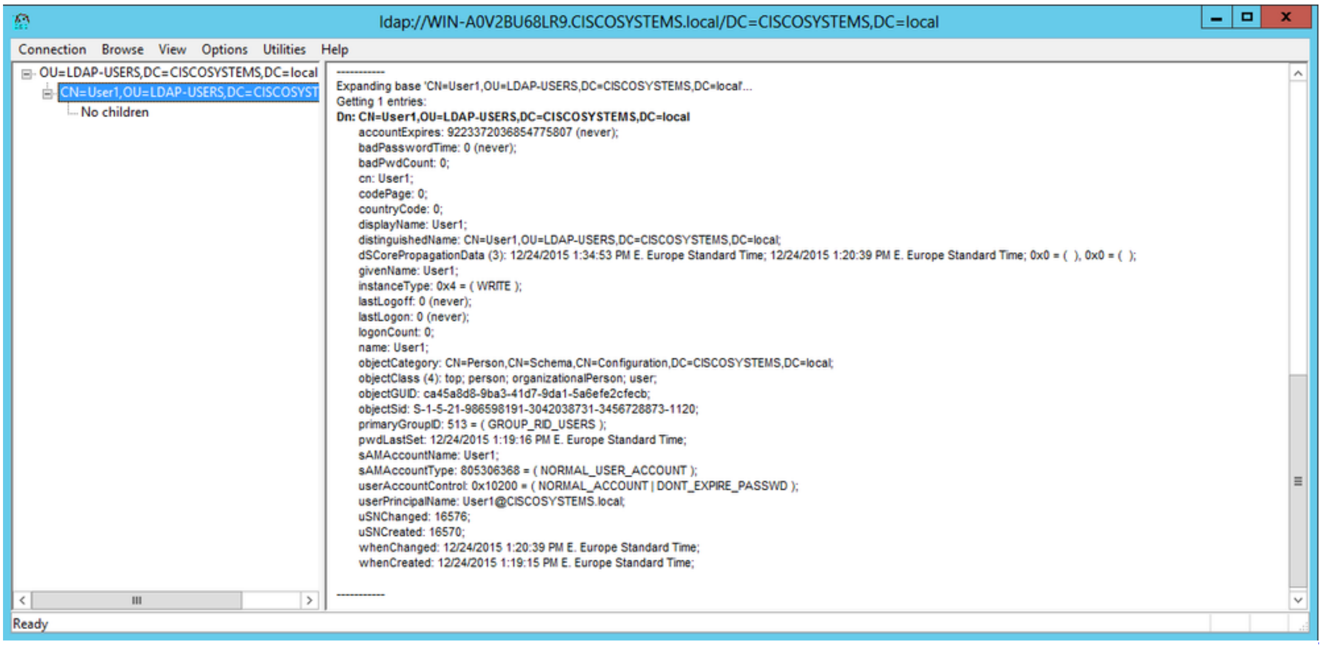

ldap://WIN-A0V2BU68LR9.CISCOSYSTEMS.local/DC=CISCOSYSTEMS,DC=local
Connection
Browse
View
Options
Utilities
Help
Tree View
Cancel
OK
Ready

BaseDN: OU=LDAP-USERS,DC=CISCOSYSTEMS,DC=local

```
    defaultNamingContext: DC=CISCOSYSTEMS,DC=local;
    dnsHostName: WIN-A0V2BU68LR9.CISCOSYSTEMS.local;
    domainControllerFunctionality: 5;
    domainFunctionality: 5;
    dsServiceName: CN=NTDS Settings,CN=WIN-A0V2BU68LR9,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=CISCOSYSTEMS,DC=local;
    forestFunctionality: 5;
    highestCommittedUSN: 16585;
    isGlobalCatalogReady: TRUE;
    isSynchronized: TRUE;
    ldapServiceName: CISCOSYSTEMS.local:win-a0v2bu68lr9$@CISCOSYSTEMS.LOCAL;
    namingContexts (5): DC=CISCOSYSTEMS,DC=local; CN=Configuration,DC=CISCOSYSTEMS,DC=local; CN=Schema,CN=Configuration,DC=CISCOSYSTEMS,DC=local;
        DC=DomainDnsZones,DC=CISCOSYSTEMS,DC=local; DC=ForestDnsZones,DC=CISCOSYSTEMS,DC=local;
    rootDomainNamingContext: DC=CISCOSYSTEMS,DC=local;
    schemaNa
    serverNam                                                  ion,DC=CISCOSYSTEMS,DC=local;
    subschem
    supported                                                  = ( ACTIVE_DIRECTORY_V51 ); 1.2.840.113556.1.4.1791 = (
        ACTIV                                                  840.113556.1.4.2080 = ( ACTIVE_DIRECTORY_V61_R2 );
        1.2.84
    supported                                                  LAGS ); 1.2.840.113556.1.4.473 = ( SORT ); 1.2.840.113556.1.4.528 = (
        NOTIFI                                                 COMMIT ); 1.2.840.113556.1.4.841 = ( DIRSYNC );
        1.2.84                                                 13556.1.4.521 = ( CROSSDOM_MOVE_TARGET );
        1.2.840.113556.1.4.970 = ( GET_STATS ); 1.2.840.113556.1.4.1338 = ( VERIFY_NAME ); 1.2.840.113556.1.4.474 = ( RESP_SORT ); 1.2.840.113556.1.4.1339 = (
        DOMAIN_SCOPE ); 1.2.840.113556.1.4.1340 = ( SEARCH_OPTIONS ); 1.2.840.113556.1.4.1413 = ( PERMISSIVE_MODIFY ); 2.16.840.1.113730.3.4.9 = ( VLVREQUEST );
        2.16.840.1.113730.3.4.10 = ( VLVRESPONSE ); 1.2.840.113556.1.4.1504 = ( ASQ ); 1.2.840.113556.1.4.1852 = ( QUOTA_CONTROL ); 1.2.840.113556.1.4.802 = (
        RANGE_OPTION ); 1.2.840.113556.1.4.1907 = ( SHUTDOWN_NOTIFY ); 1.2.840.113556.1.4.1948 = ( RANGE_RETRIEVAL_NOERR ); 1.2.840.113556.1.4.1974 = (
        FORCE_UPDATE ); 1.2.840.113556.1.4.1341 = ( RODC_DCPROMO ); 1.2.840.113556.1.4.2026 = ( DN_INPUT ); 1.2.840.113556.1.4.2064 = ( SHOW_RECYCLED );
        1.2.840.113556.1.4.2065 = ( SHOW_DEACTIVATED_LINK ); 1.2.840.113556.1.4.2066 = ( POLICY_HINTS_DEPRECATED ); 1.2.840.113556.1.4.2090 = ( DIRSYNC_EX );
        1.2.840.113556.1.4.2205 = ( UPDATE_STATS ); 1.2.840.113556.1.4.2204 = ( TREE_DELETE_EX ); 1.2.840.113556.1.4.2206 = ( SEARCH_HINTS ); 1.2.840.113556.1.4.2211
        = ( EXPECTED_ENTRY_COUNT ); 1.2.840.113556.1.4.2239 = ( POLICY_HINTS );
    supportedLDAPPolicies (15): MaxPoolThreads; MaxDatagramRecv; MaxReceiveBuffer; InitRecvTimeout; MaxConnections; MaxConnIdleTime; MaxPageSize;
        MaxBatchReturnMessages; MaxQueryDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange;
    supportedLDAPVersion (2): 3; 2;
    supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;

-----------
```

5. The left side of the LDP browser displays the entire tree that appears under the specified BaseDN (OU=LDAP-USERS, dc=CISCOSYSTEMS, dc=local). Expand the tree to locate the user User1. This user can be identified with the CN value that represents the first name of the user. In this example, it is CN=User1. Double-click **CN=User1**. In the right-side pane of the LDP browser, LDP displays all the attributes associated with User1, as shown in the image:


ldap://WIN-A0V2BU68LR9.CISCOSYSTEMS.local/DC=CISCOSYSTEMS,DC=local
Connection
Browse
View
Options
Utilities
Help
OU=LDAP-USERS,DC=CISCOSYSTEMS,DC=local
CN=User1,OU=LDAP-USERS,DC=CISCOSYST
No children
Ready

```
-----------
Expanding base 'CN=User1,OU=LDAP-USERS,DC=CISCOSYSTEMS,DC=local'...
Getting 1 entries:
Dn: CN=User1,OU=LDAP-USERS,DC=CISCOSYSTEMS,DC=local
    accountExpires: 9223372036854775807 (never);
    badPasswordTime: 0 (never);
    badPwdCount: 0;
    cn: User1;
    codePage: 0;
    countryCode: 0;
    displayName: User1;
    distinguishedName: CN=User1,OU=LDAP-USERS,DC=CISCOSYSTEMS,DC=local;
    dSCorePropagationData (3): 12/24/2015 1:34:53 PM E. Europe Standard Time; 12/24/2015 1:20:39 PM E. Europe Standard Time; 0x0 = (  ), 0x0 = (  );
    givenName: User1;
    instanceType: 0x4 = ( WRITE );
    lastLogoff: 0 (never);
    lastLogon: 0 (never);
    logonCount: 0;
    name: User1;
    objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=CISCOSYSTEMS,DC=local;
    objectClass (4): top; person; organizationalPerson; user;
    objectGUID: ca45a8d8-9ba3-41d7-9da1-5a6efe2cfecb;
    objectSid: S-1-5-21-986598191-3042038731-3456728873-1120;
    primaryGroupID: 513 = ( GROUP_RID_USERS );
    pwdLastSet: 12/24/2015 1:19:16 PM E. Europe Standard Time;
    sAMAccountName: User1;
    sAMAccountType: 805306368 = ( NORMAL_USER_ACCOUNT );
    userAccountControl: 0x10200 = ( NORMAL_ACCOUNT | DONT_EXPIRE_PASSWD );
    userPrincipalName: User1@CISCOSYSTEMS.local;
    uSNChanged: 16576;
    uSNCreated: 16570;
    whenChanged: 12/24/2015 1:20:39 PM E. Europe Standard Time;
    whenCreated: 12/24/2015 1:19:15 PM E. Europe Standard Time;

-----------
```

6. When you configure the WLC for the LDAP server, in the *User Attribute* field, enter the name of the attribute in the user record that contains the username. From this LDP output, you can see that sAMAccountName is one attribute that contains the username "User1," so enter the sAMAccountName attribute that corresponds to the User Attribute field on the WLC.

7. When you configure the WLC for the LDAP server, in the *User Object Type* field, enter the value of the LDAP objectType attribute that identifies the record as a user. Often, user records have several values for the objectType attribute, some of which are unique to the user and some of which are

shared with other object types. In the LDP output, CN=Person is one value that identifies the record as a user, so specify **Person** as the User Object Type attribute on the WLC.

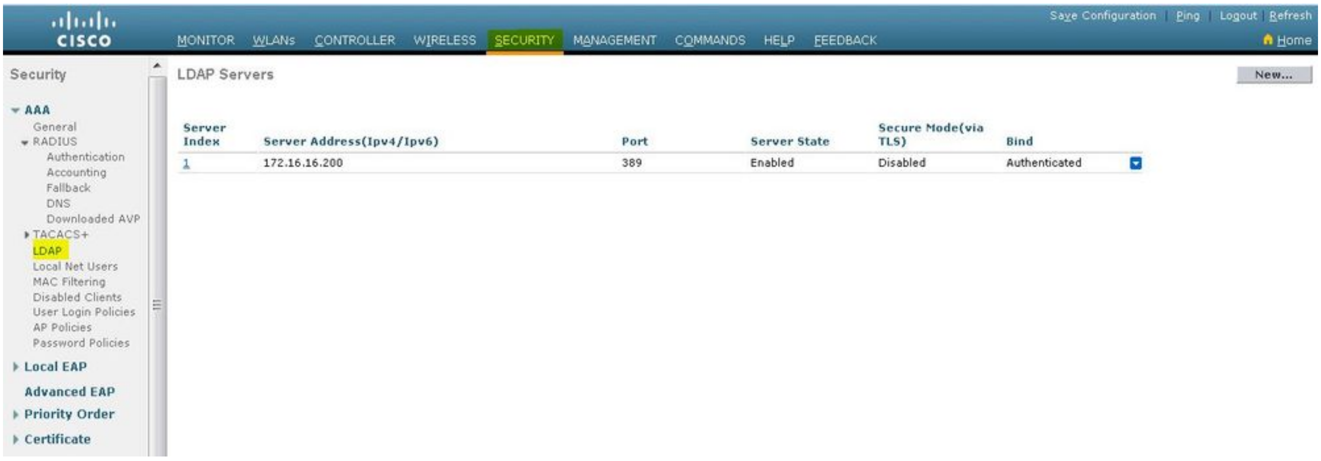
The next step is to configure the WLC for the LDAP server.

Configure WLC for LDAP Server

Now that the LDAP server is configured, the next step is to configure the WLC with details of the LDAP server. Complete these steps on the WLC GUI:

Note:This document assumes that the WLC is configured for basic operation and that the LAPs are registered to the WLC. If you are a new user who wants to setup the WLC for basic operation with LAPs, refer to Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).

1. In the Security page of the WLC, choose **AAA > LDAP** from the left-side task pane in order to move to the LDAP server configuration page.



LDAP Servers

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

In order to add an LDAP server, click **New**. The LDAP Servers > New page appears.

2. In the LDAP Servers Edit page, specify the details of the LDAP server, such as the IP address of LDAP server, Port Number, Enable Server status, and so on.

   - Choose a number from the Server Index (Priority) drop-down box to specify the priority order of this server in relation to any other configured LDAP servers. You can configure up to seventeen servers. If the controller cannot reach the first server, it tries the second one in the list and so on.
   - Enter the **IP address** of the LDAP server in the Server IP Address field.
   - Enter the **TCP port number** of the LDAP server in the Port Number field. The valid range is 1 to 65535, and the default value is 389.
   - for the Simple bind, we used Authenticated, for the bind username which is the location of the WLC admin user that will be used to access the LDAP server and its password
   - In the User Base DN field, enter the **distinguished name (DN)** of the subtree in the LDAP server that contains a list of all the users. For example, ou=organizational unit, .ou=next organizational unit, and o=corporation.com. If the tree that contains users is the base DN, enter o=corporation.com or dc=corporation, dc=com.

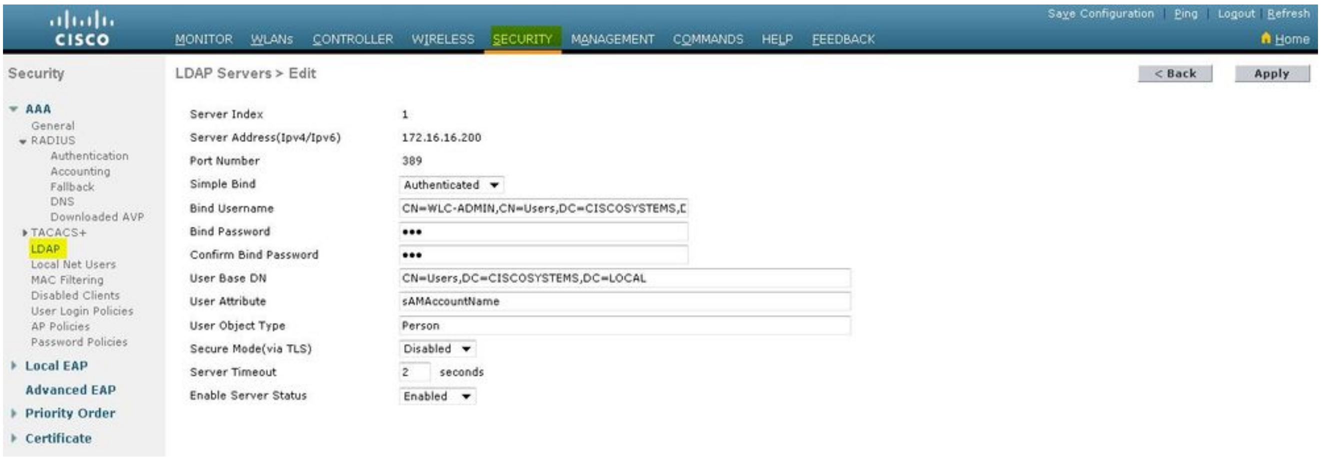
In this example, the user is located under the Organizational Unit (OU) LDAP-USERS, which, in turn, is created as part of the lab.wireless domain.

The User Base DN must point the full path where the user information (user credential as per EAP-FAST authentication method) is located. In this example, the user is located under the base DN OU=LDAP-USERS, DC=CISCOSYSTEMS, DC=local.

- In the User Attribute field, enter the name of the attribute in the user record that contains the username.

  In the User Object Type field, enter the value of the LDAP objectType attribute that identifies the record as a user. Often, user records have several values for the objectType attribute, some of which are unique to the user and some of which are shared with other object types

  You can obtain the value of these two fields from your directory server with the LDAP browser utility that comes as part of the Windows 2012 support tools. This Microsoft LDAP browser tool is called LDP. With the help of this tool, you can know the User Base DN, User Attribute, and User Object Type fields of this particular user. Detailed information on how to use LDP to know these User specific attributes is discussed in the *Using LDP to Identify the User Attributes* section of this document.
- In the Server Timeout field, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.
- Check the **Enable Server Status** check box to enable this LDAP server, or uncheck it to disable it. The default value is disabled.
- Click **Apply** to commit your changes. This is an example already configured with this information:



LDAP Servers > Edit

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=CISCOSYSTEMS,D
Bind Password	•••
Confirm Bind Password	•••
User Base DN	CN=Users,DC=CISCOSYSTEMS,DC=LOCAL
User Attribute	sAMAccountName
User Object Type	Person
Secure Mode(via TLS)	Disabled
Server Timeout	2 seconds
Enable Server Status	Enabled

3. Now that details about the LDAP server are configured on the WLC, the next step is to configure a WLAN for web authentication.

Configure the WLAN for Web Authentication

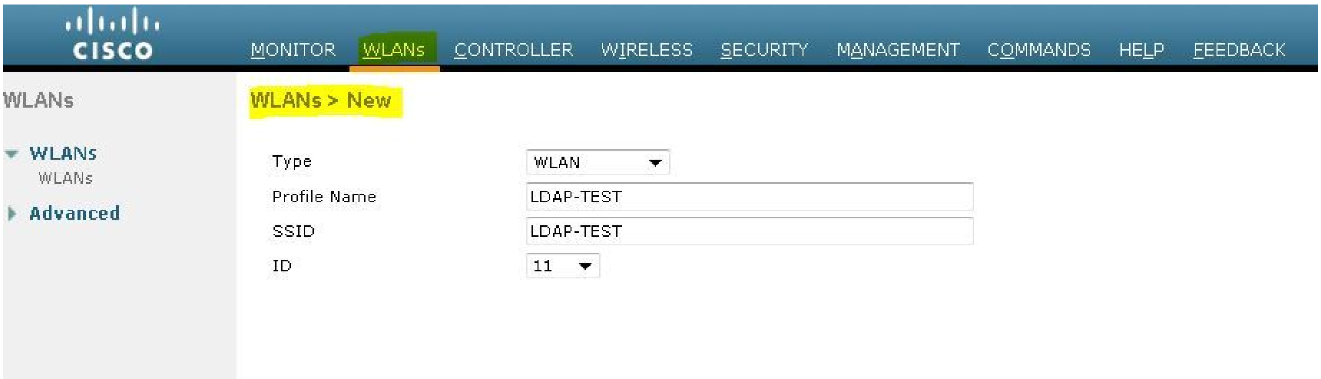
The first step is to create a WLAN for the users. Complete these steps:

1. Click **WLANs** from the controller GUI in order to create a WLAN.

   The WLANs window appears. This window lists the WLANs configured on the controller.

2. Click **New** in order to configure a new WLAN.

   In this example, the WLAN is named Web-Auth.



WLANs > New

Type: WLAN

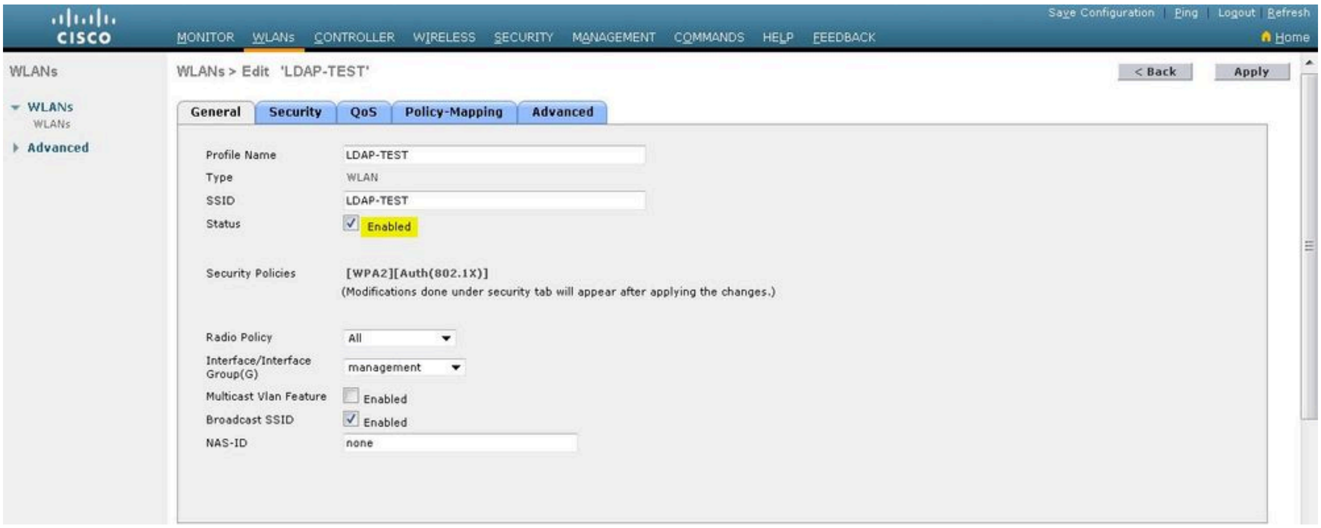
Profile Name: LDAP-TEST

SSID: LDAP-TEST

ID: 11

3. Click **Apply**.

4. In the WLAN > Edit window, define the parameters specific to the WLAN.



WLANs > Edit 'LDAP-TEST'

Profile Name: LDAP-TEST

Type: WLAN

SSID: LDAP-TEST

Status: ☑ 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: □ Enabled

Broadcast SSID: ☑ Enabled

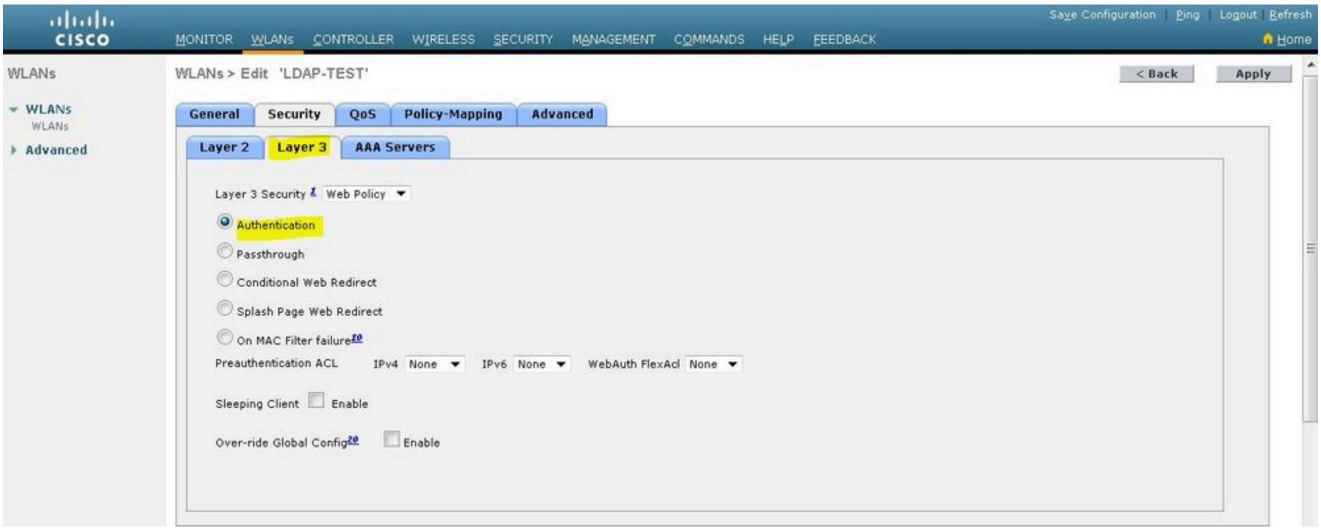
NAS-ID: none

- Check the Status check box to enable the WLAN.

- For the WLAN, choose the appropriate interface from the Interface Name field.

  This example maps the management interface that connects to the WLAN Web-Auth.

5. Click the **Security** tab. In the Layer 3 Security field, check the **Web Policy** check box, and choose the **Authentication** option.


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers

WLANs > Edit 'LDAP-TEST'

Layer 3 Security: Web Policy

● Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

○ On MAC Filter failure[10]

Preauthentication ACL IPv4 None IPv6 None WebAuth FlexAcl None

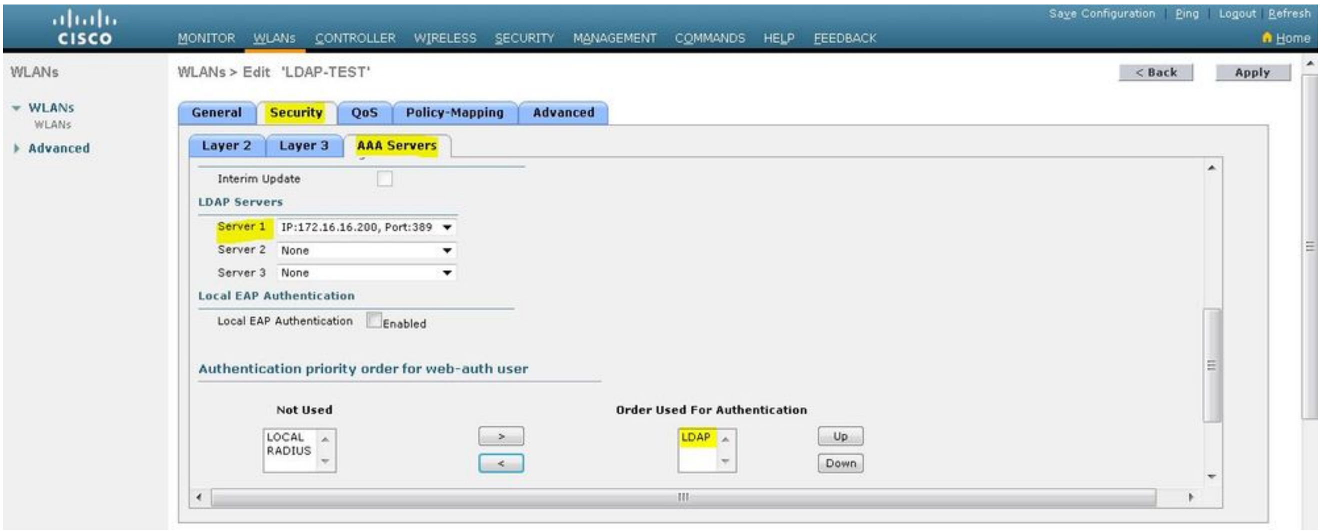
Sleeping Client □ Enable

Over-ride Global Config[20] □ Enable

This option is chosen because web authentication is used to authenticate the wireless clients. Check the **Override Global Config** check box to enable per the WLAN web authentication configuration. Choose the appropriate web authentication type from the Web Auth type drop-down menu. This example uses Internal Web Authentication.

Note: Web authentication is not supported with 802.1x authentication. This means you cannot choose 802.1x or a WPA/WPA2 with 802.1x as the Layer 2 security when you use web authentication. Web authentication is supported with all other Layer 2 security parameters.

6. Click the **AAA Servers** tab. Choose the configured LDAP server from the LDAP server pull-down menu. If you use a local database or RADIUS server, you can set the authentication priority under the *Authentication priority order for web-auth user*field.


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers
>
<
Up
Down

WLANs > Edit 'LDAP-TEST'

Interim Update □

LDAP Servers

Server 1 IP:172.16.16.200, Port:389

Server 2 None

Server 3 None

Local EAP Authentication

Local EAP Authentication □ Enabled

Authentication priority order for web-auth user

Not Used: LOCAL, RADIUS

Order Used For Authentication: LDAP

7. Click **Apply**.

Note: In this example, Layer 2 Security methods to authenticate users are not used, so choose **None** in the Layer 2 Security field.

Verify

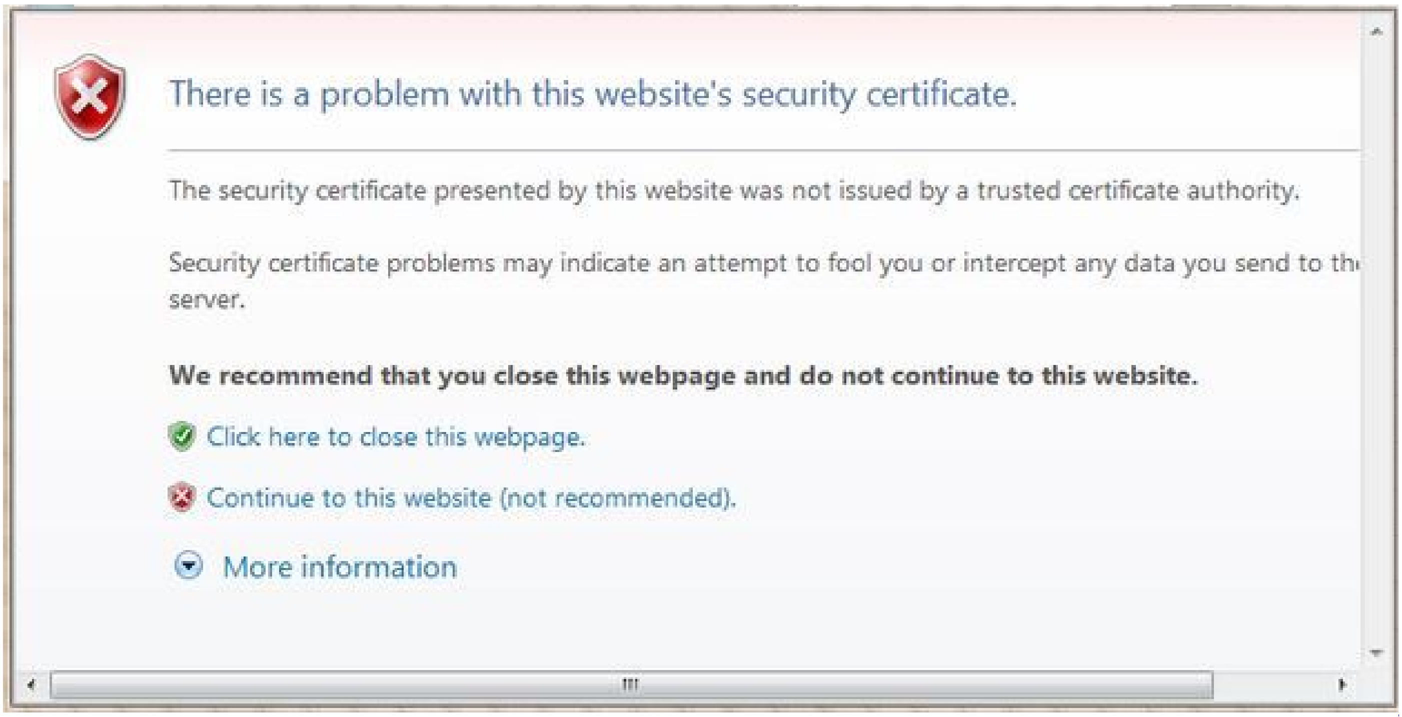
Use this section in order to confirm that your configuration works properly.

In order to verify this setup, connect a Wireless client and check if the configuration works as expected.

The wireless client comes up, and the user enters the URL, such as www.yahoo.com, in the web browser. Because the user has not been authenticated, the WLC redirects the user to the internal web login URL.

The user is prompted for the user credentials. Once the user submits the username and password, the login page takes the user credentials input and, upon submit, sends the request back to the action_URL example, http://1.1.1.1/login.html, of the WLC web server. This is provided as an input parameter to the customer redirect URL, where 1.1.1.1 is the Virtual Interface Address on the switch.

The WLC authenticates the user against the LDAP user database. After successful authentication, the WLC web server either forwards the user to the configured redirect URL or to the URL with which the client started, such as 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.

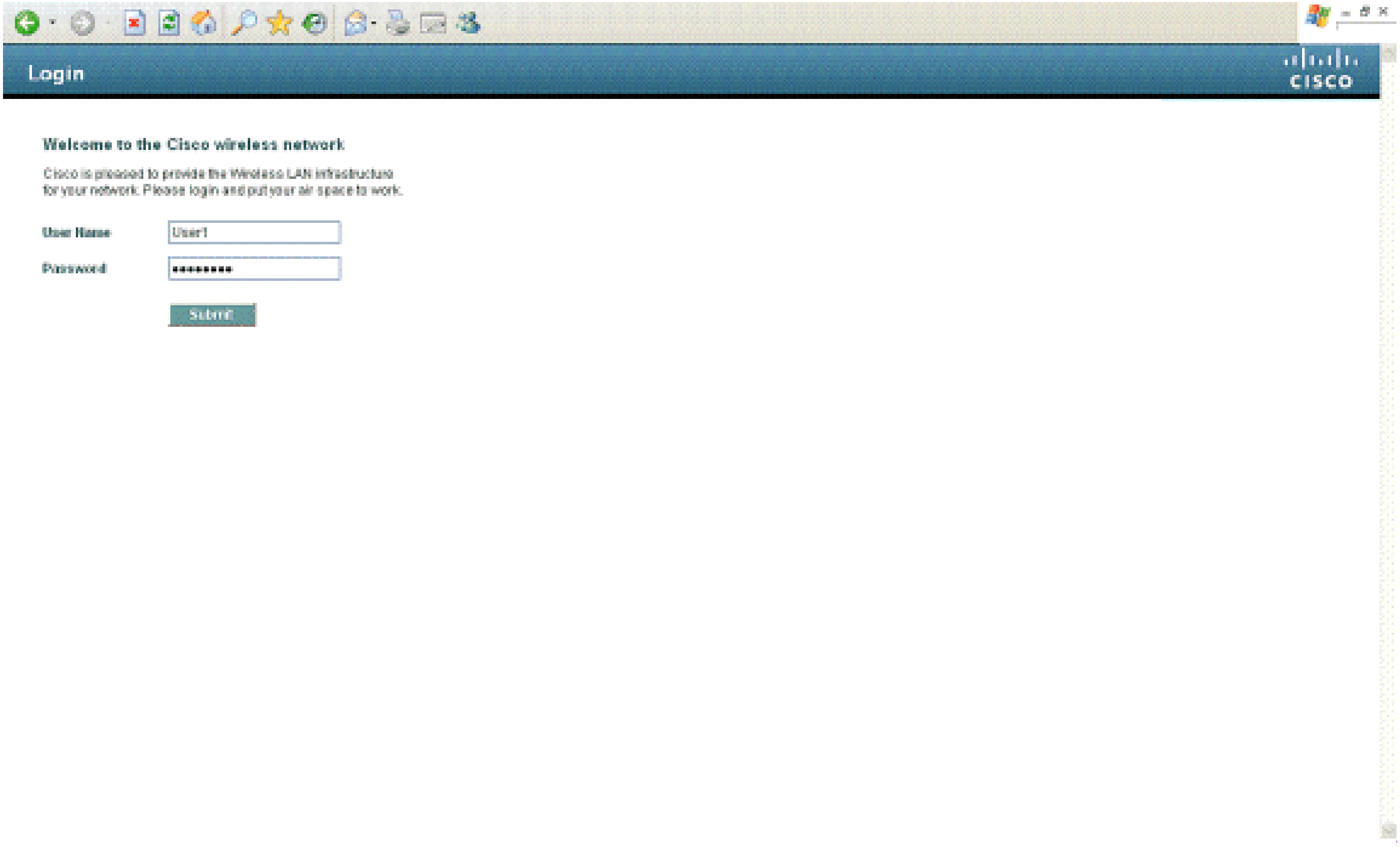
Security certificate problems may indicate an attempt to fool you or intercept any data you send to th server.

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



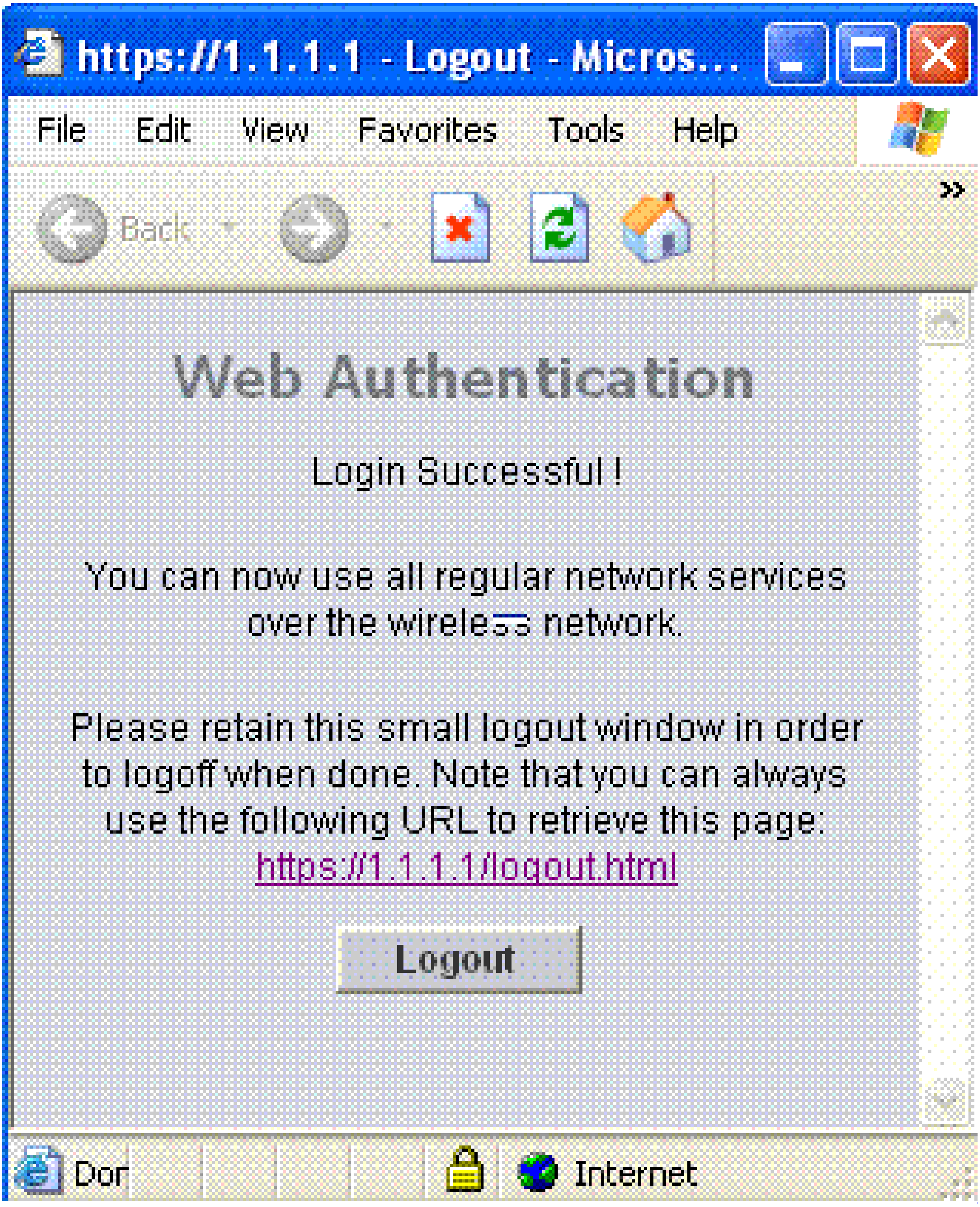
Login

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 User1

Password •••••••••



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

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Use these commands to Troubleshoot your configuration:

- **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**

This is a sample output from the commands **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:
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Association received from mobile on BSSID
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Global 200 Clients are allowed to AP radi

*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

*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 override for default ap group, marking in
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Interface policy on Mobile, role

*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 I
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Changing I
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfApplyWlanPolicy: Apply WLAN Policy ove
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6246 setting Central swi
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6249 apVapId = 1 and Spl
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying site-specific Local Bridging ove
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Local Bridging Interface Policy
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE  statusCode is 0 and status
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE  ssid_done_flag is 0 finish
*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
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 suppRates  statusCode is 0 and gotSuppRat
*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:
*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 sta

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 pemApfAddMobileStation2: APF_MS_PEM_WAIT_
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Initializing poli
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Change state to A

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

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

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) pemApfAddM
```

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

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

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

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

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

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

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Successful
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2 (apf_policy.c:359) Changin

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2:session timeout forstation
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Scheduling deletion of Mobile Station:  (
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Func: apfPemAddUser2, Ms Timeout = 1800,

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Sending assoc-resp with status 0 station:
*apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sending Assoc Response to station on BSSI
*apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 apfProcessAssocReq (apf_80211.c:10187) Ch

*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2, d
*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, d
*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 32
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype 0ff:ff:f
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block s
                        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 mscbV
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (lo
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block s
                        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 s
                        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 mscbV
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (lo
*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,
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792), sec
*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.
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block s
```

```
                        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,v
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418, port
*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, hl
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792), secs
*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: 172.16.1
*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
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len 33
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype 0ff:ff:f
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block s
                        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 mscbV
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (lo
*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,
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792), sec
*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.
*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 ser
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block s
                        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,v
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP setting server from ACK (mscb=0x40e6
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418, port
*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, hl
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792), secs
*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: 172.16.1
*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
*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created for mobile,
*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created in mscb for
*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:F7:3

*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_bi
*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=CISCOSYSTEMS,DC=lc
*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 b
*LDAP DB Task 1: Dec 24 03:46:01.226: Attempting user bind with username CN=User1,CN=Users,DC=CISC
*LDAP DB Task 1: Dec 24 03:46:01.228: LDAP ATTR> dn = CN=User1,CN=Users,DC=CISCOSYSTEMS,DC=local (
*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 stat

*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

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Stopping deletion of Mobile Station: (call
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Setting Session Timeout to 1800 sec - star
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Reached PLUMBFASTPA
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Replacing Fast Path
  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 (cor
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule (cor

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

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

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


(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 Failured 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
```