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

Document ID: 108008

Introduction
Prerequisites
Requirements
Components Used
Conventions
Web Authentication Process
Configure
Network Diagram
Configurations
Configure LDAP Server
Configure WLC for LDAP Server
Configure the WLAN for Web Authentication
Verify
Troubleshoot
NetPro Discussion Forums − Featured Conversations
Related Information

Introduction

This document explains how to setup a wireless LAN controller (WLC) for web authentication. This document also 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

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of the configuration of Lightweight Access Points (LAPs) and Cisco WLCs
- Knowledge of Lightweight Access Point Protocol (LWAPP)
- Knowledge of how to set up and configure LDAP, Active Directory and domain controllers

Components Used

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

- Cisco 4400 WLC that runs firmware release 5.1
- Cisco 1232 Series LAP
- Cisco 802.11a/b/g Wireless Client Adapter that runs firmware release 4.2
- Microsoft Windows 2003 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.

Conventions

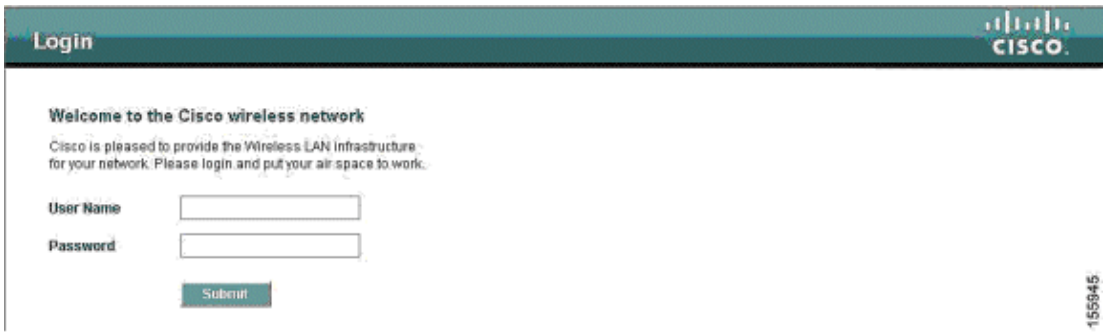
Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Web Authentication Process

Web authentication is a Layer 3 security feature that causes the controller to disallow IP traffic (except DHCP−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, their users 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.

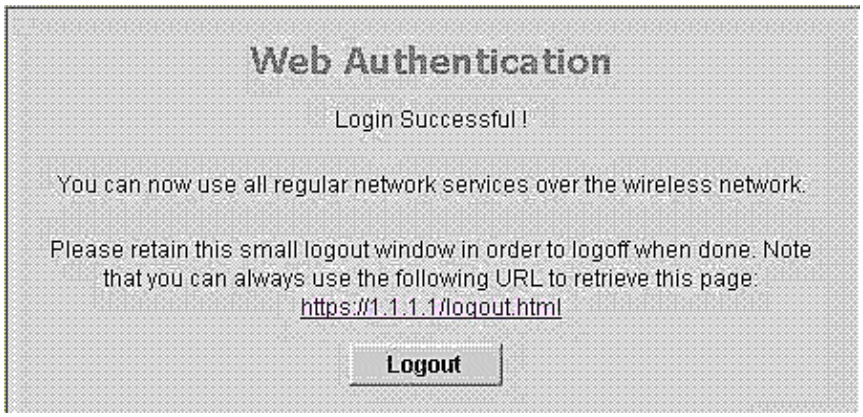
After the user clicks **Yes** to proceed, or if the browser of theclient does not display a security alert, the web authentication system redirects the client to a login page



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 the user enters a valid username and password on the web authentication login page and clicks **Submit**, the user is authenticated based upon the credentials submitted and a successful authentication. The web authentication system then displays a successful login page and redirects the authenticated client to the requested URL.



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 Lightweight Directory Access Protocol (LDAP) server as the backend database for web authentication to retrieve user credentials and authenticate the user.

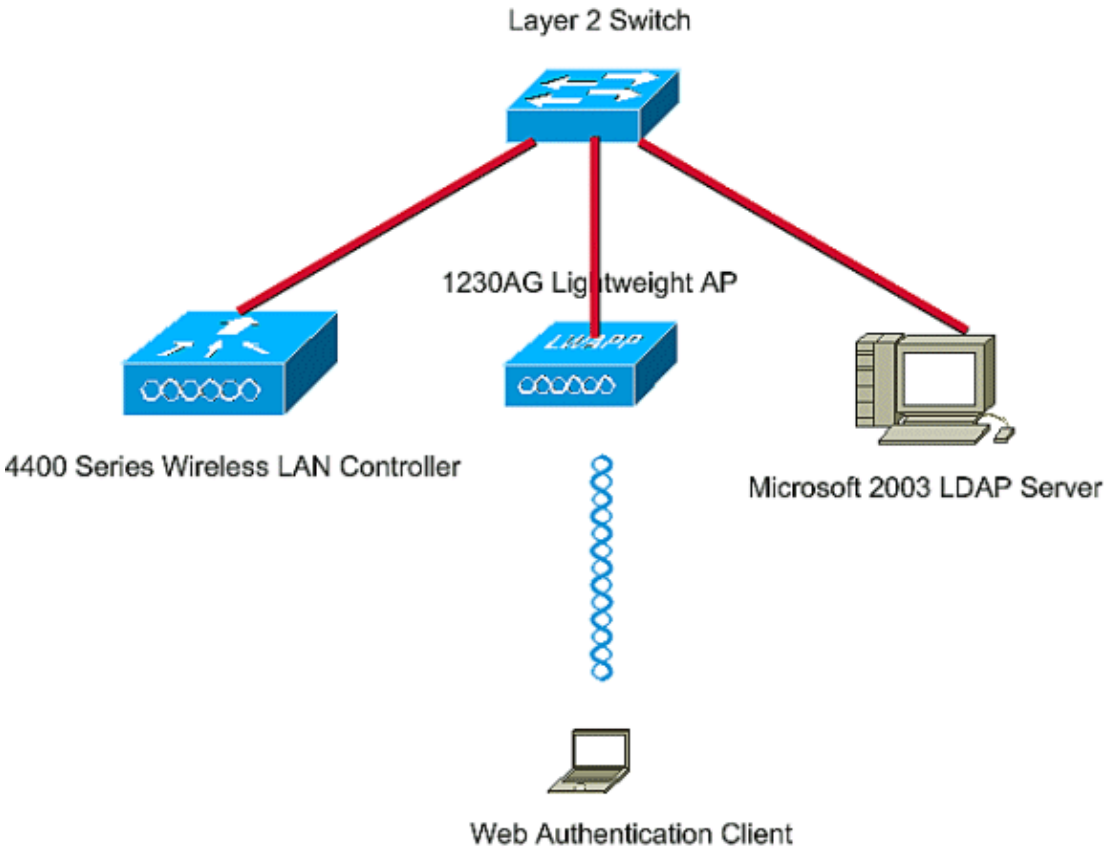
Configure

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 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 2003 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.

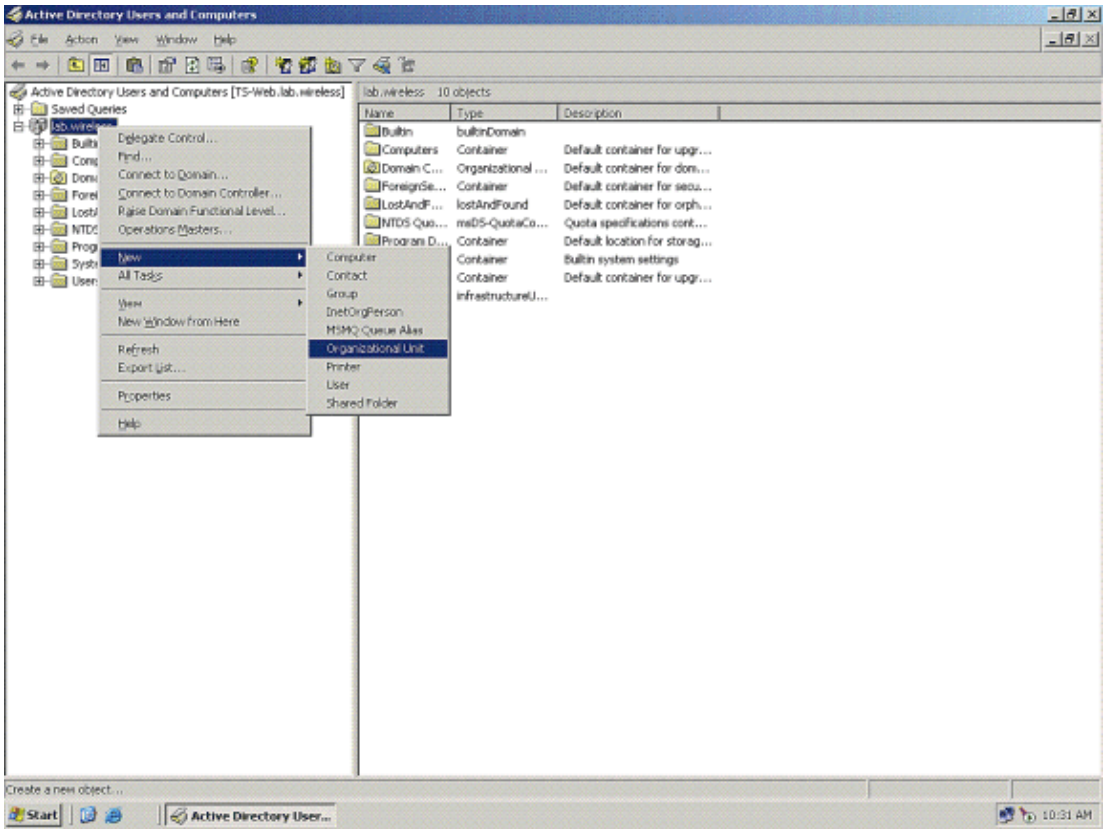
In this example, a new OU LDAP−USERS is created, and the user User1 is created under this OU. When you configure this user for LDAP access, the WLC can query this LDAP database for user authentication.

The domain used in this example is **lab.wireless**.

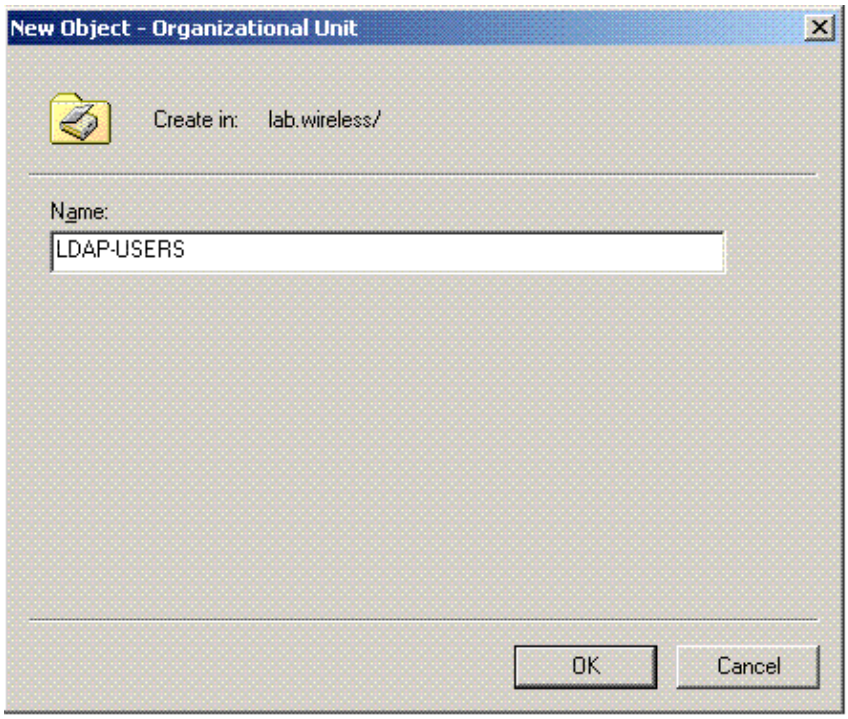
Create a User Database Under an OU

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

1. In the domain controller, click **Start > Programs > Administrative Tools > Active Directory Users and Computers** in order to launch the Active Directory Users and Computers management console.
2. Right−click your domain name, which is **lab.wireless** in this example, and then choose **New > Organizational Unit** from the context menu in order to create a new OU.

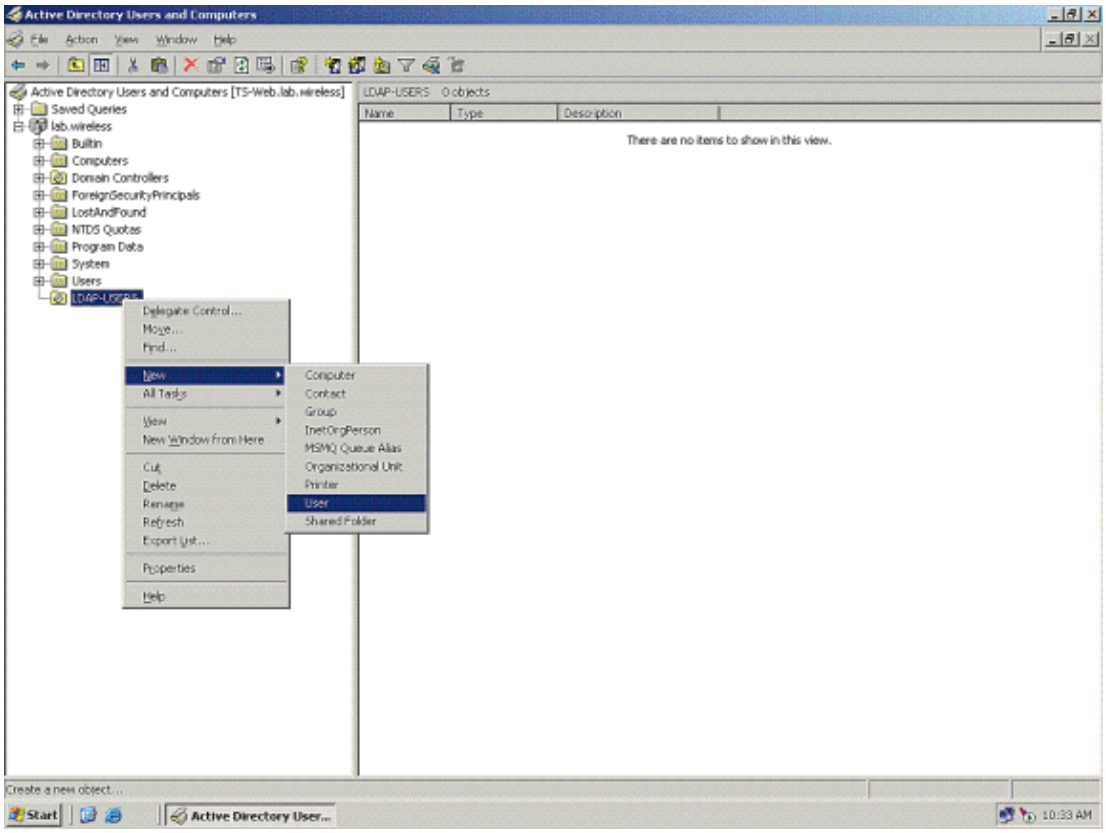


3. Assign a name to this OU and click **OK**.



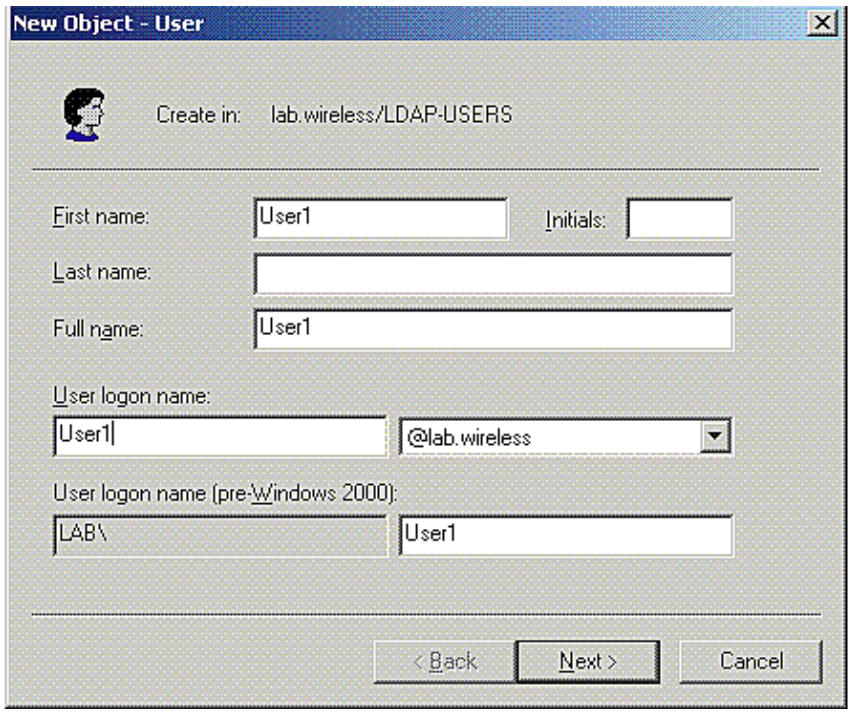
Now that the new OU LDAP−USERS is created on the LDAP server, the next step is to create user **User1** under this OU. In order to achieve this, complete these steps:

1. Right−click the new OU created. Choose **New > User** from the resultant context menus in order to create a new user.

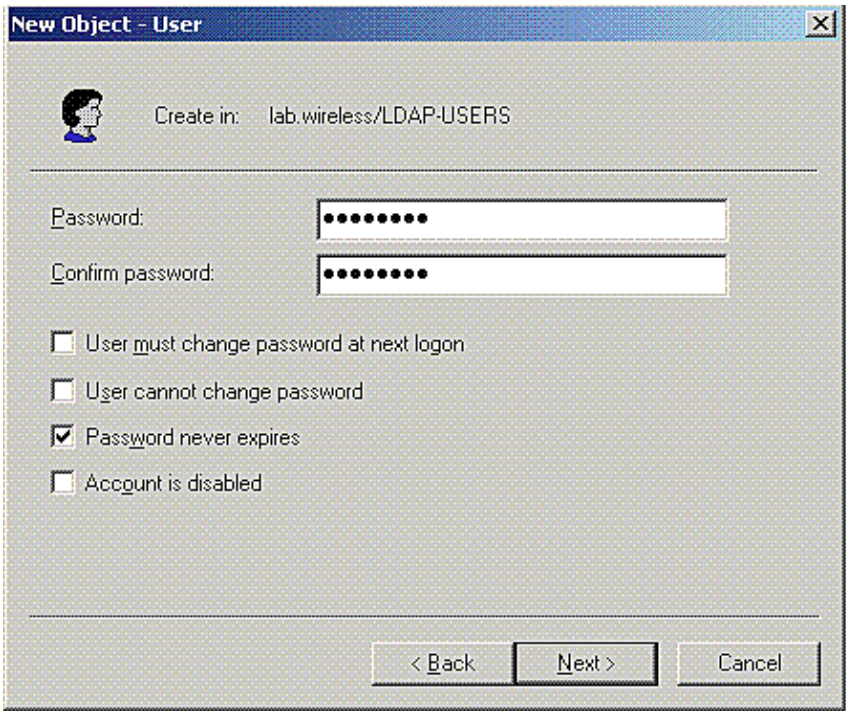


2. In the User setup page, fill in the required fields as shown in this example. This example has **User1** in the **User logon name** field.

   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**.



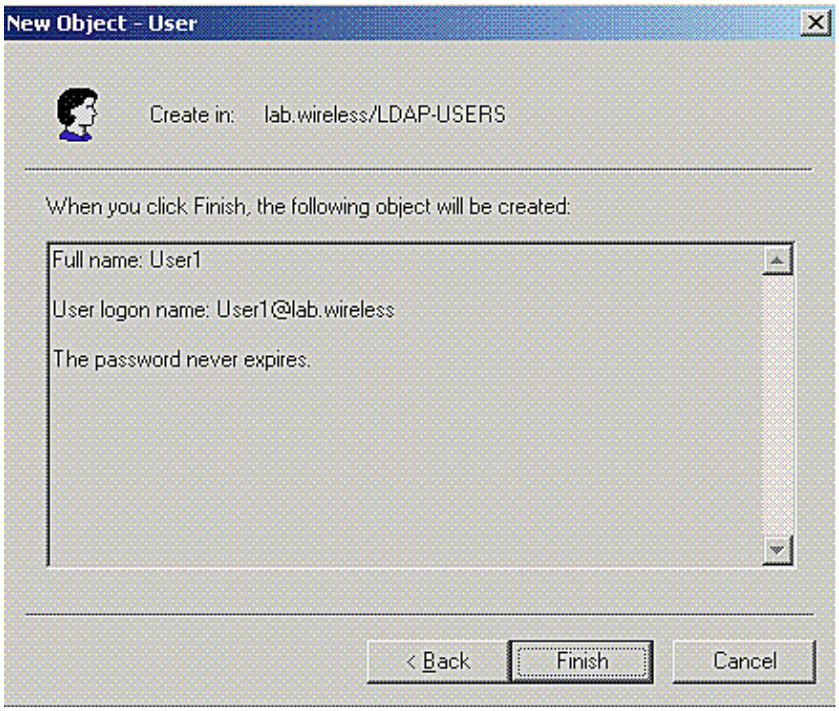
3. Enter a password and confirm the password. Choose the **Password never expires** option and click **Next**.



4. Click **Finish**.

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

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



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

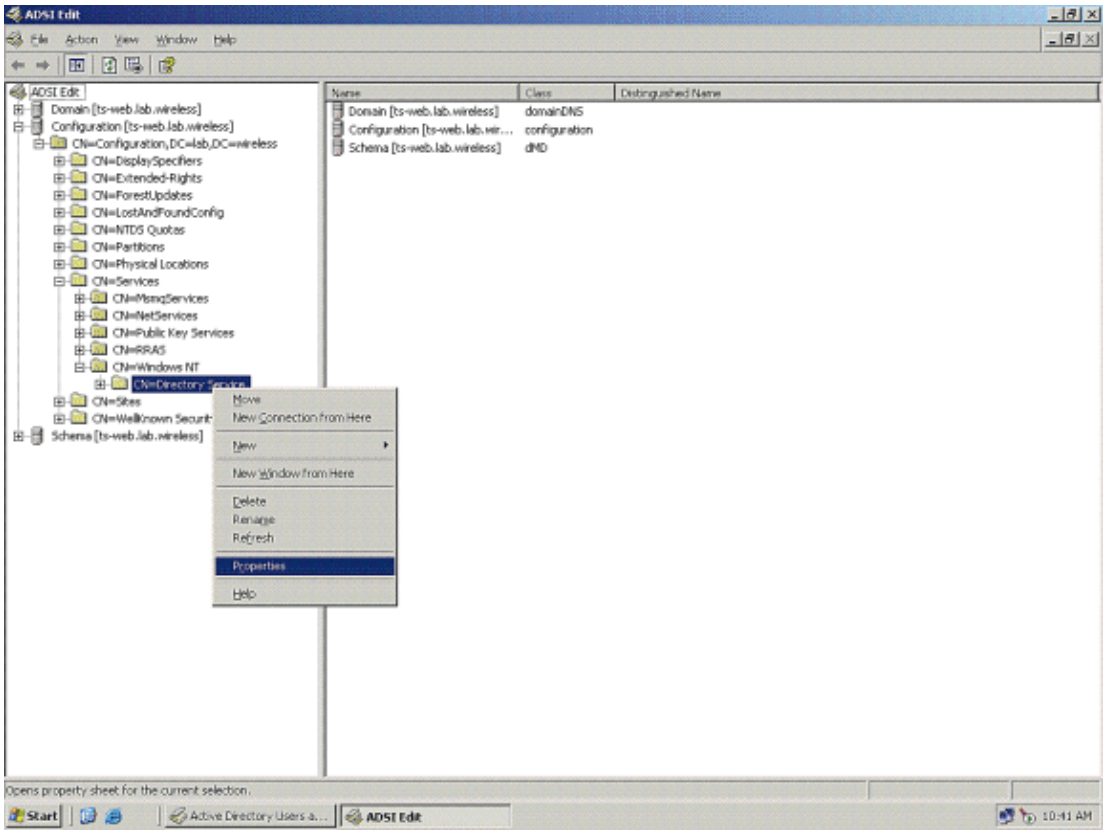
Perform the steps in this section in order to configure a user for LDAP access.

Enable Anonymous Bind Feature on the Windows 2003 Server

For any third−party applications (in our case WLC) to access Windows 2003 AD on the LDAP, the Anonymous Bind feature must be enabled on Windows 2003. By default, anonymous LDAP operations are not permitted on Windows 2003 domain controllers. Perform these steps in order to enable the Anonymous Bind feature:

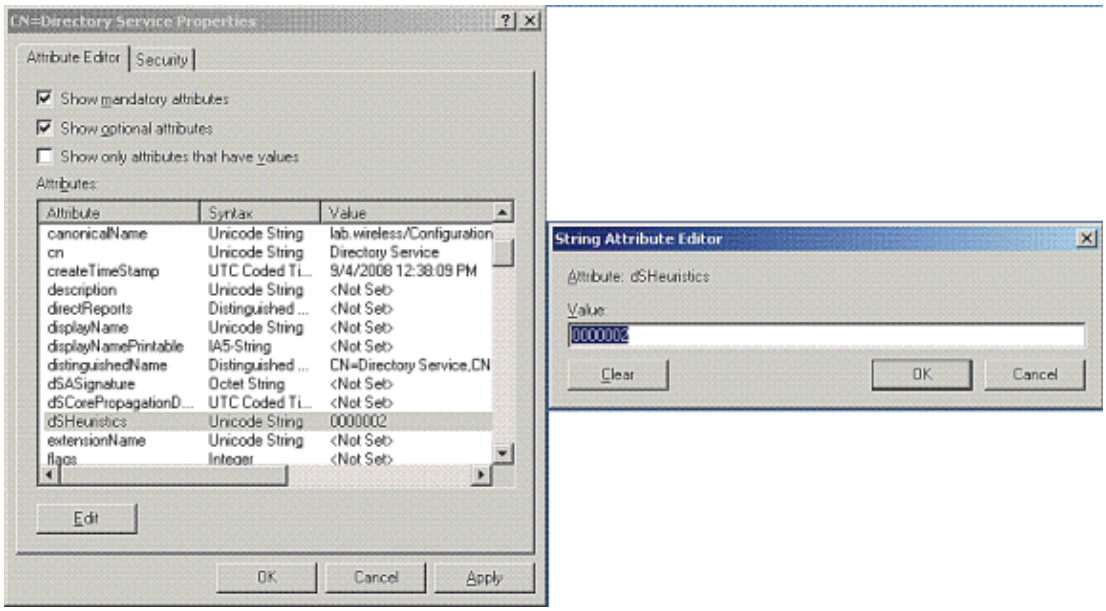
1. Launch the ADSI Edit tool from the location **Start > Run > Type: ADSI Edit.msc**. This tool is part of the Windows 2003 support tools.
2. In the ADSI Edit window, expand the root domain (Configuration [tsweb.lab.wireless]).

   Expand **CN=Services > CN=Windows NT > CN=Directory Service**. Right−click the **CN=Directory Service** container, and choose **Properties** from the context menu.



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**. The Anonymous Bind feature is enabled on the Windows 2003 server.

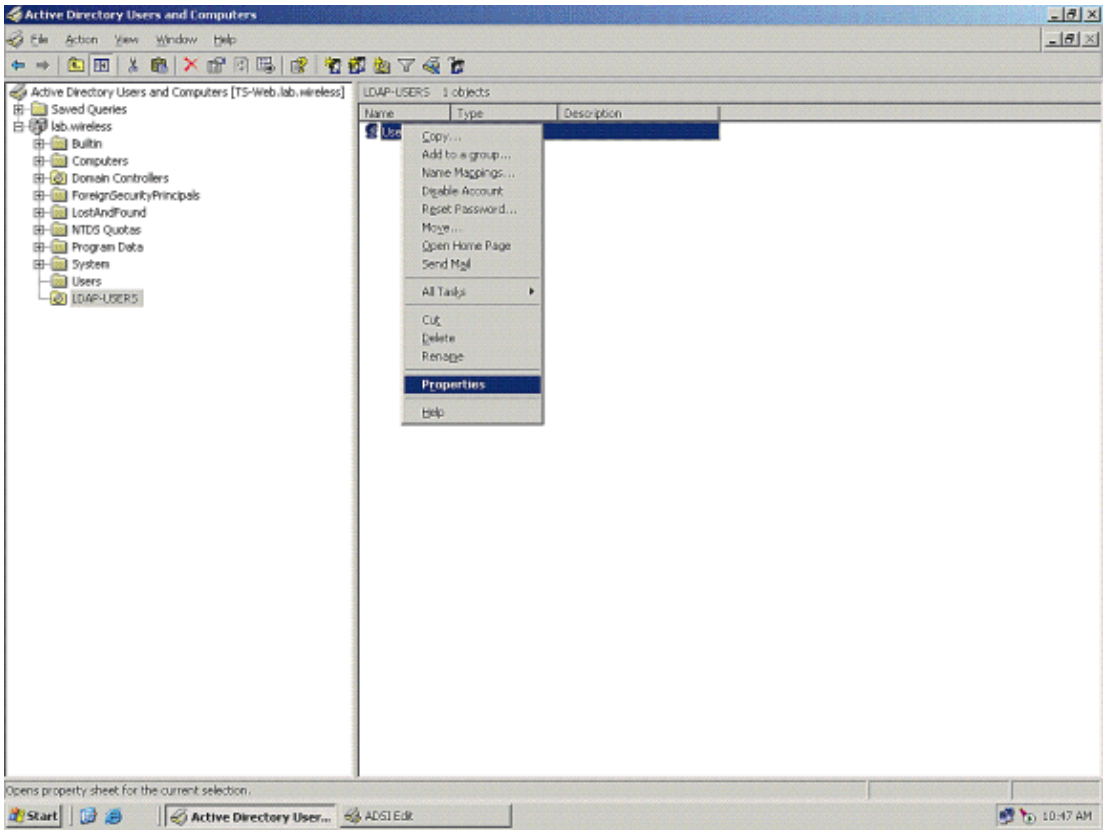
   Note: The last (seventh) character is the one that controls the way you can bind to LDAP service. "0" or no seventh character means that anonymous LDAP operations are disabled. If you set the seventh character to "2," it enables the Anonymous Bind feature.



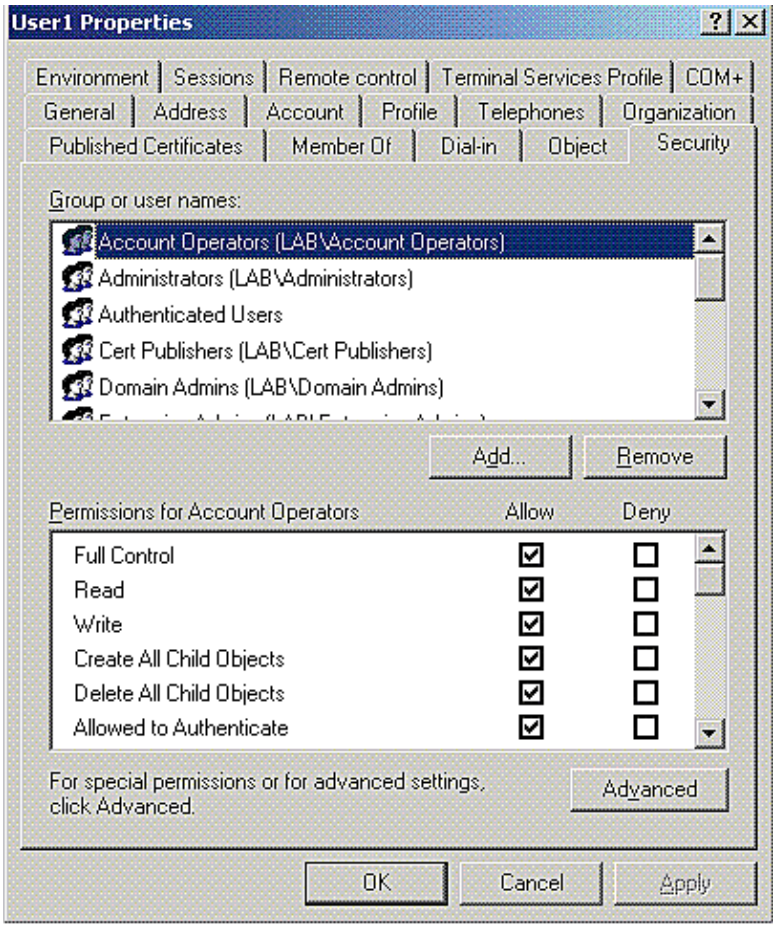
Granting ANONYMOUS LOGON Access to the User "User1"

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

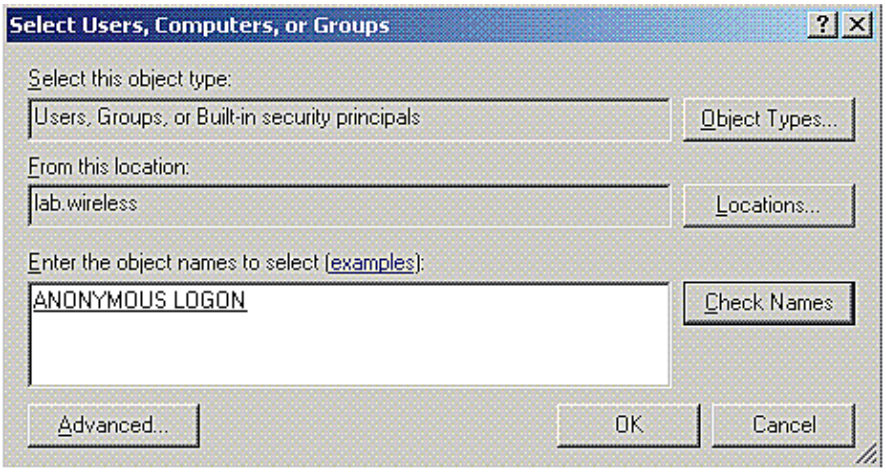
1. Open **Active Directory Users and Computers**.
2. Make sure that the **View Advanced Features** is checked.
3. Navigate to the user User1 and right−click it. Choose **Properties** from the context menu. This user is identified with the first name "User1."



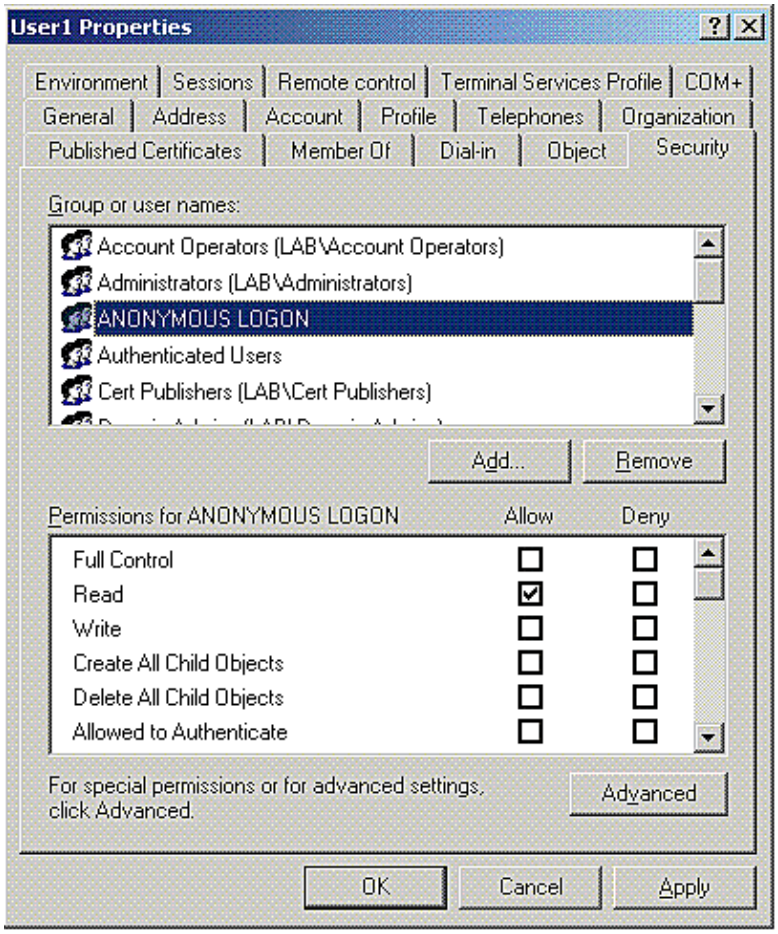
4. Click the **Security** tab.



5. Click **Add** in the resultant window.
6. Enter **ANONYMOUS LOGON** under the *Enter the object names to select* box and acknowledge the dialog.



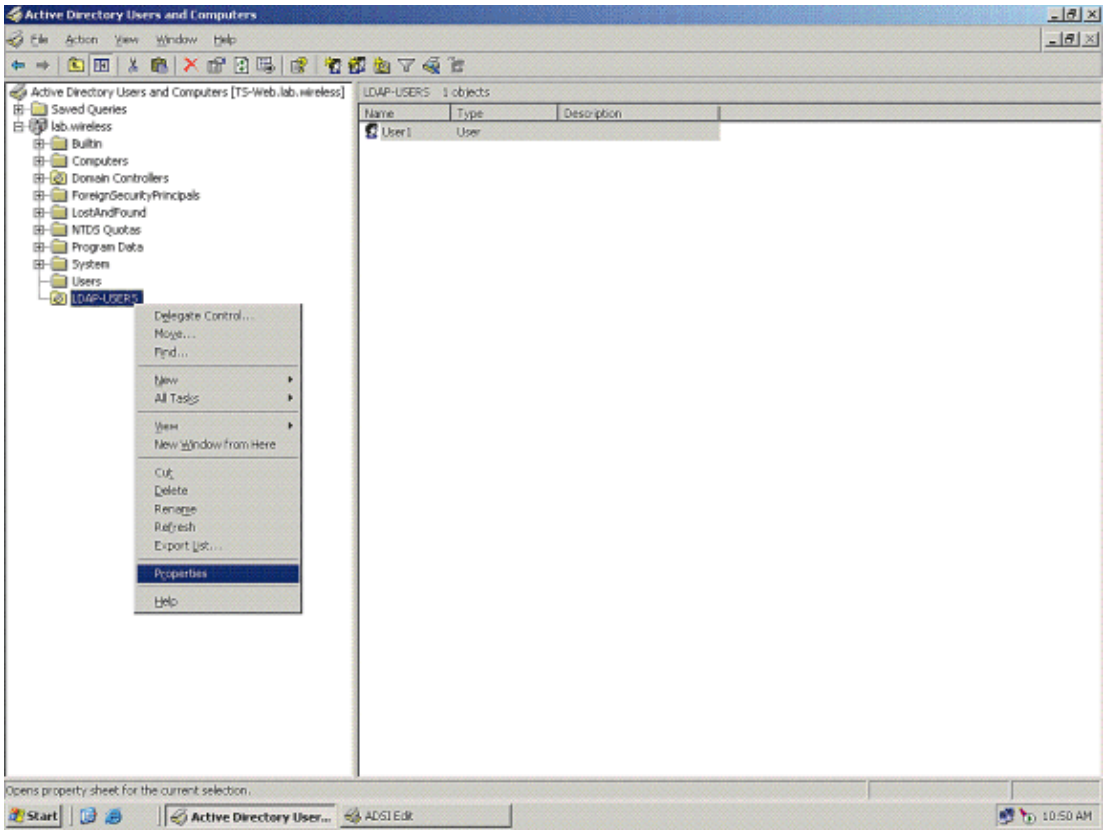
7. In the ACL, notice that ANONYMOUS LOGON has access to some property sets of the user. Click **OK**. The ANONYMOUS LOGON access is granted to this user.



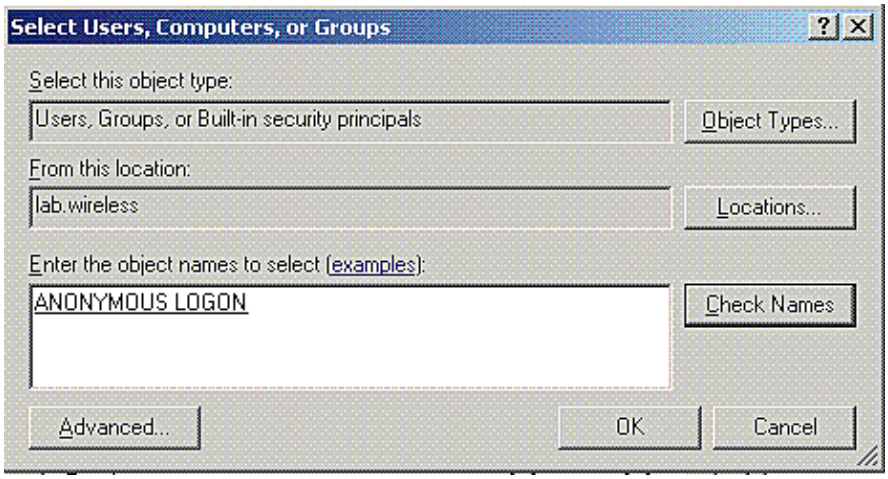
Grant List Contents Permission on the OU

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:

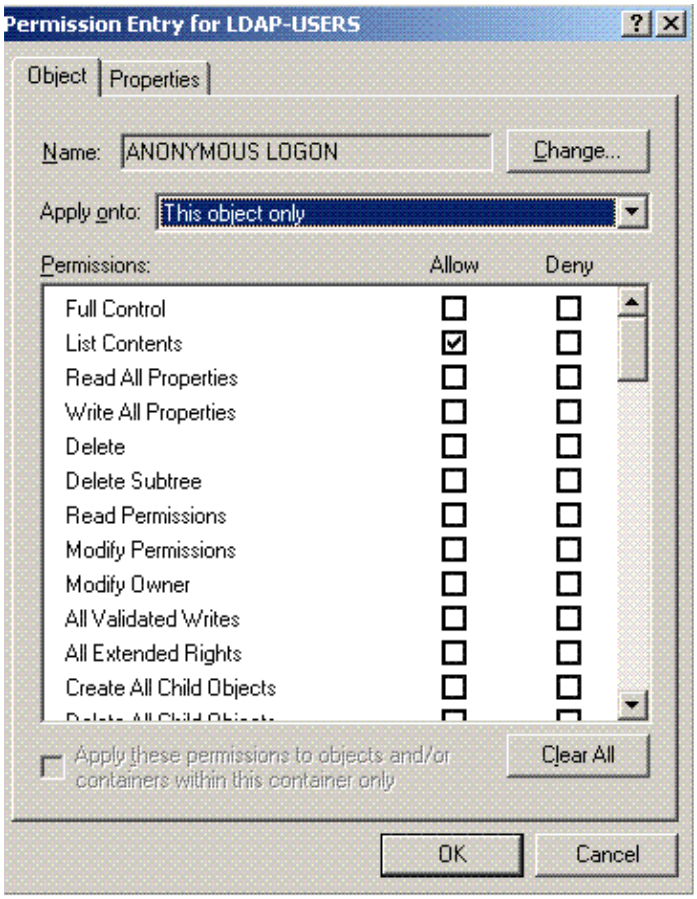
1. In **Active Directory Users and Computers**, right−click the OU LDAP−USERS and choose **Properties**.



2. Click **Security** and then **Advanced**.
3. Click **Add**. In the dialog that opens, enter **ANONYMOUS LOGON**.



4. Acknowledge the dialog. This opens a new dialog window.
5. In the *Apply onto* drop−down box, choose **This object only**. Enable the **List Contents** *Allow* check box.

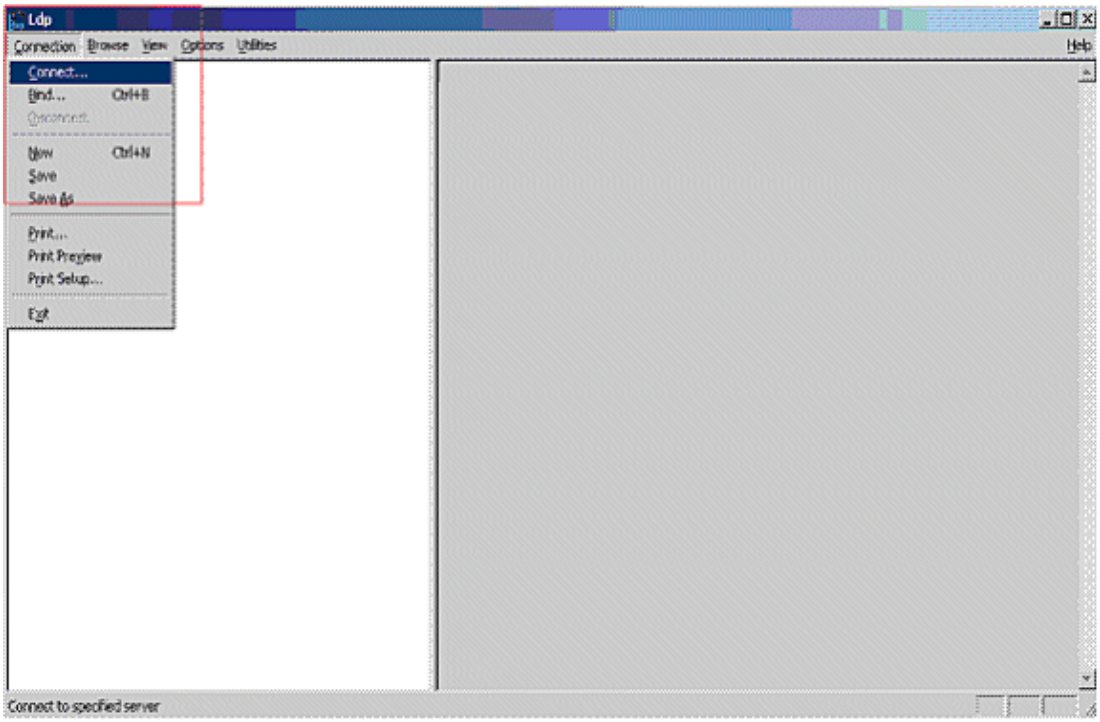


Use LDP to Identify the User Attributes

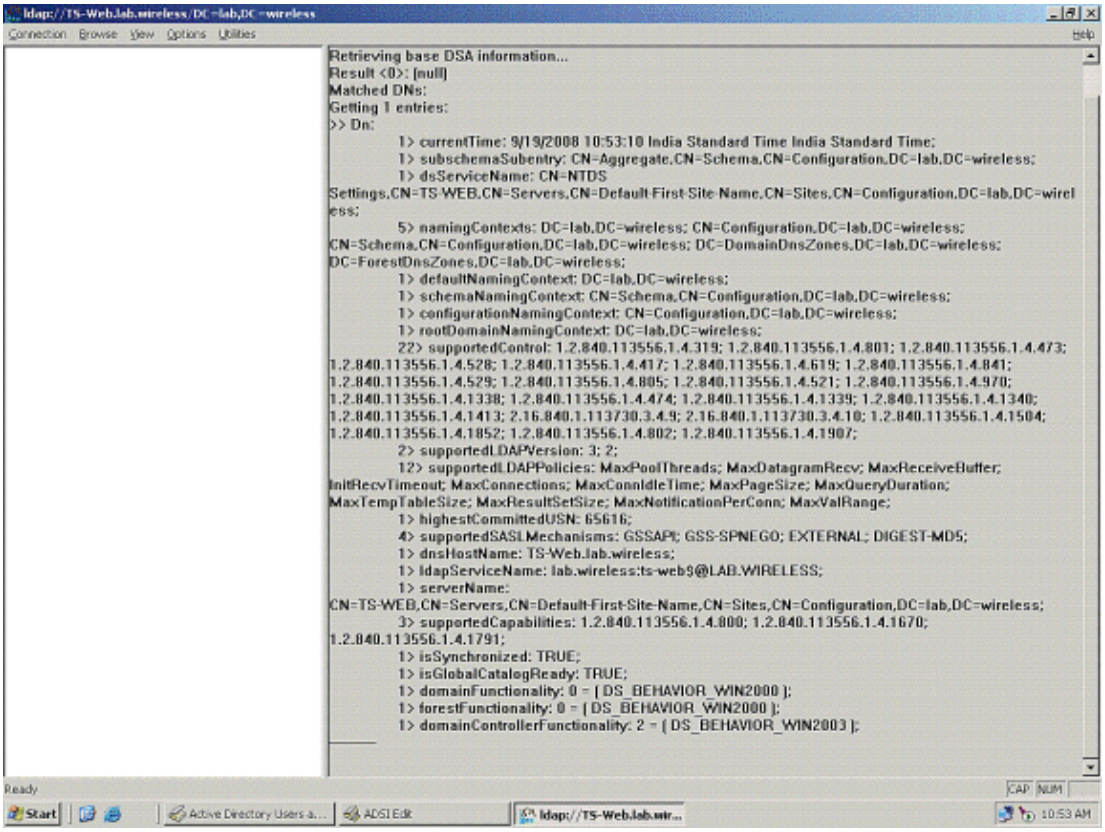
This GUI tool is a LDAP client that allows users to perform operations, such as connect, bind, search, modify, add, or delete, against any LDAP−compatible directory, such as Active Directory. LDP is used to view objects that are stored in Active Directory along with their metadata, such as security descriptors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

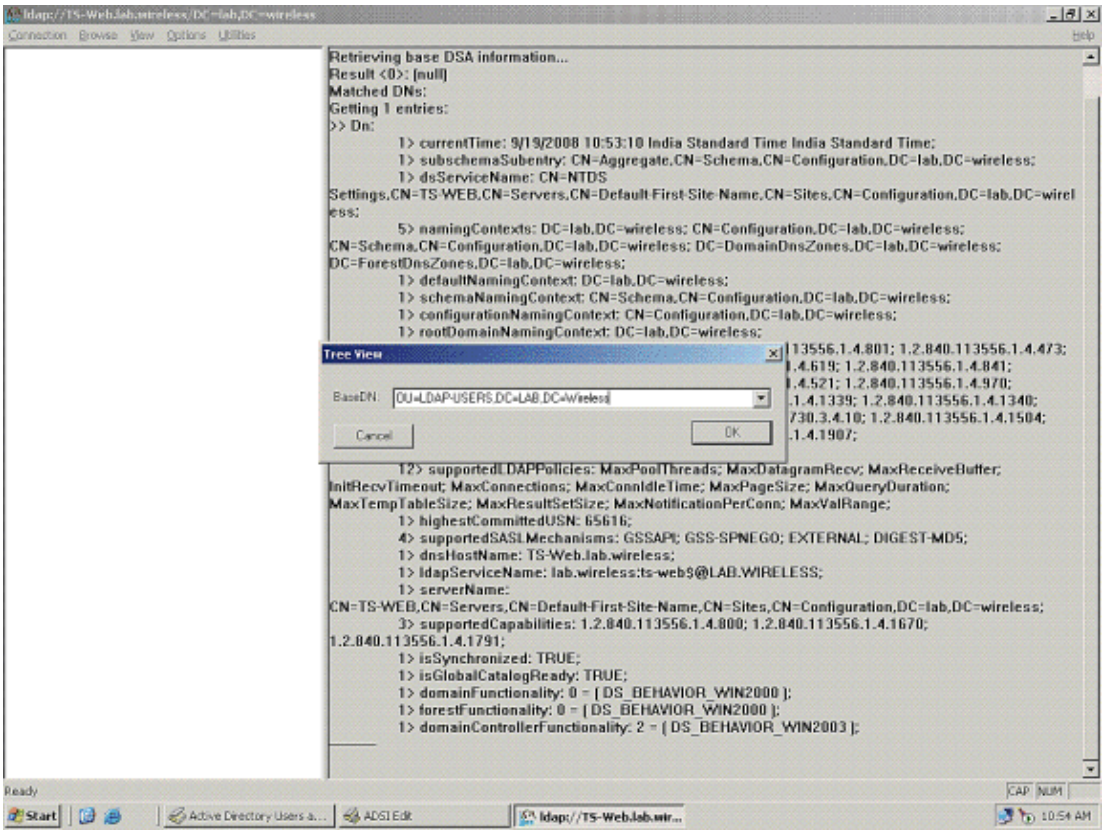
1. On the Windows 2003 server (even on the same LDAP server), click **Start > Run** and enter **LDP** in order to access the LDP browser.
2. In the LDP main window, click **Connection > Connect** and connect to the LDAP server when you enter the IP address of the LDAP server.



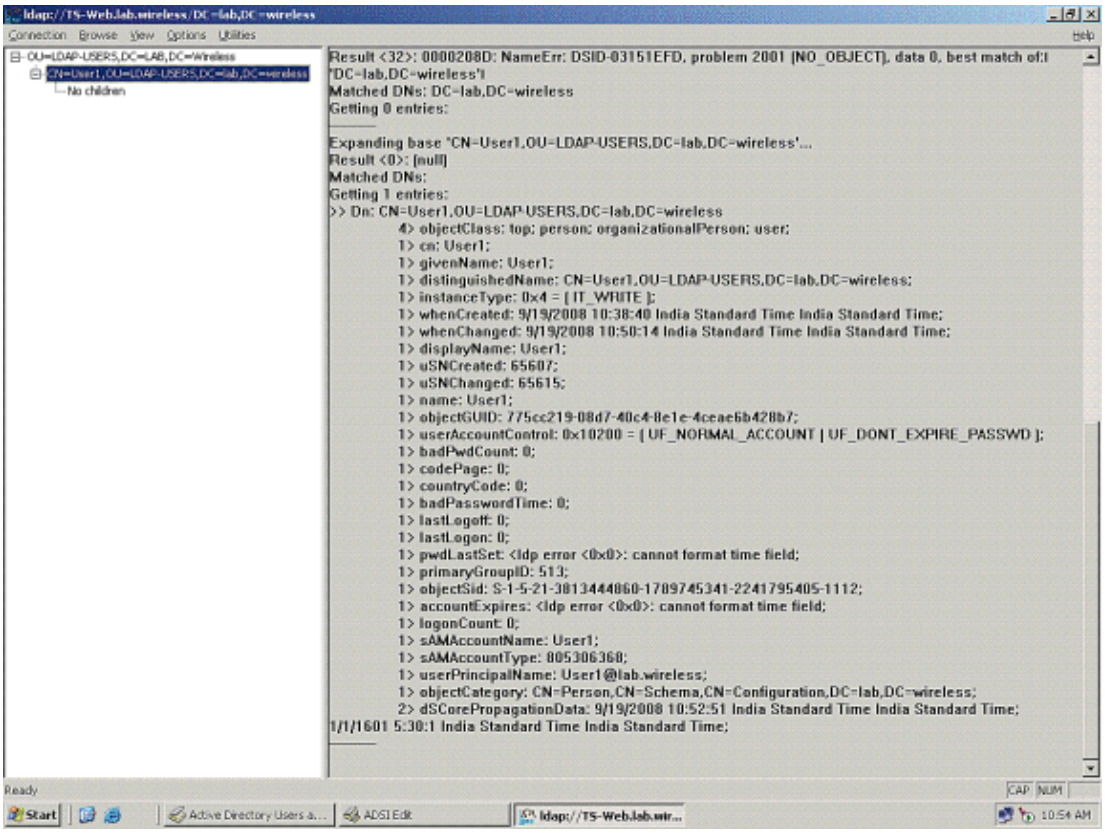
3. Once connected to the LDAP server, choose **View** from the main menu and click **Tree**.



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 LAB.wireless. Click **OK**.



5. The left side of the LDP browser displays the entire tree that appears under the specified BaseDN (OU=LDAP−USERS, dc=LAB, dc=Wireless). 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. This example explains this step:



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.

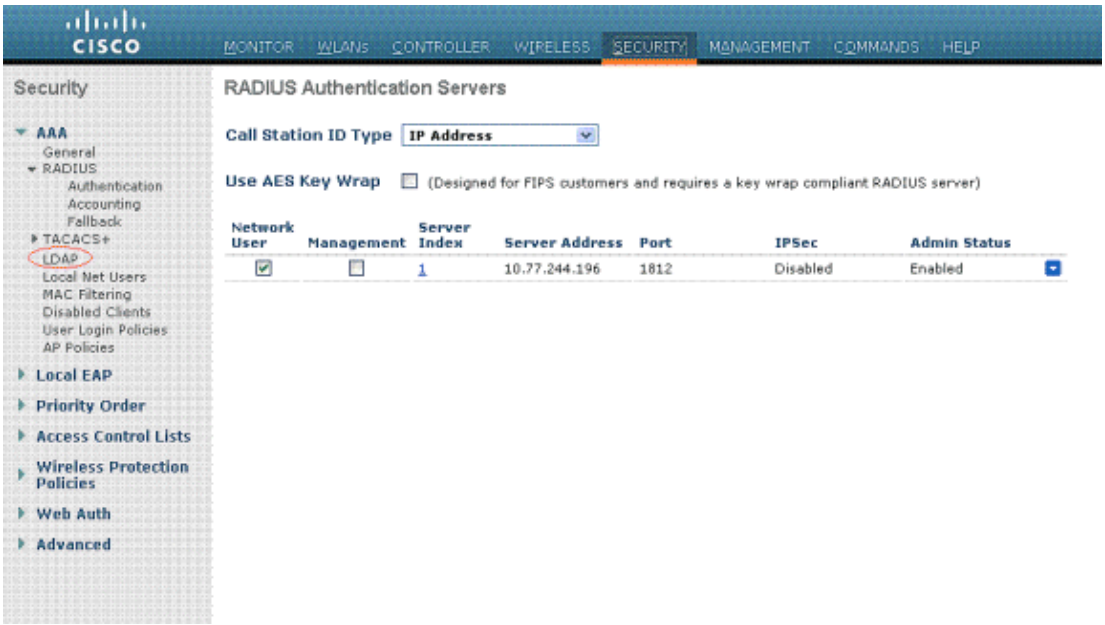
   The next step is to configure the WLC for the LDAP server.

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.



   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.
   - 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=lab, DC=Wireless.

- 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 2003 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:

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

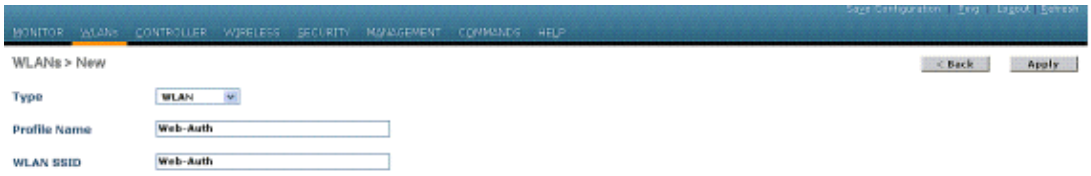
Configure the WLAN for Web Authentication

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.

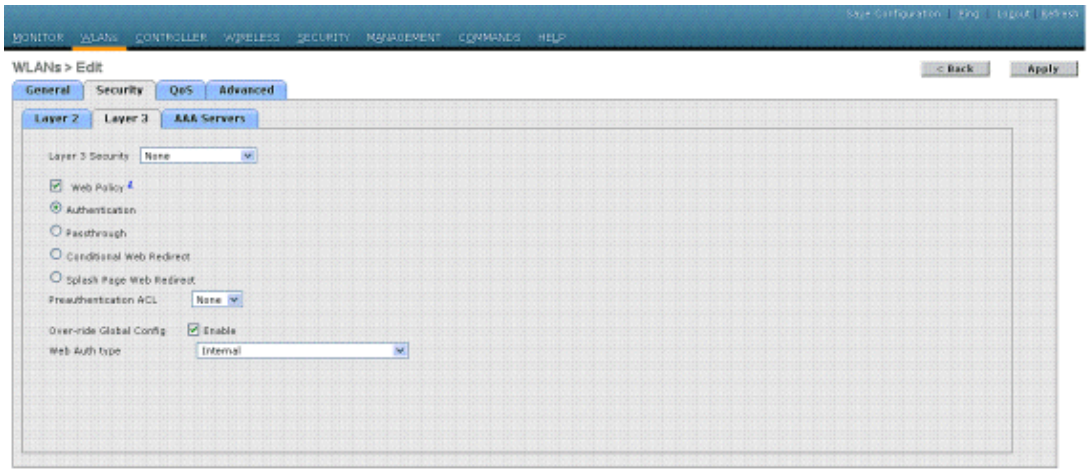


3. Click **Apply**.
4. In the WLAN > Edit window, define the parameters specific to the WLAN.

- 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.

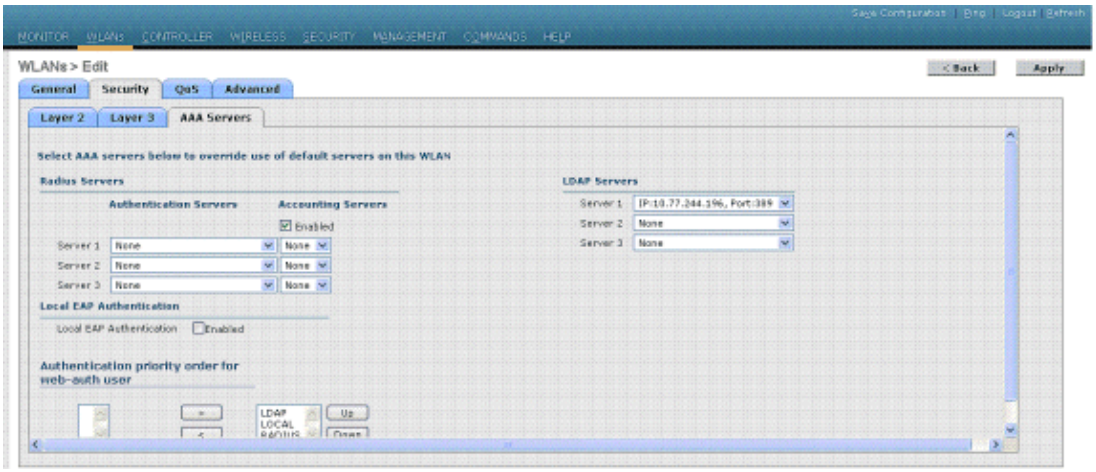
5. Click the **Security** tab. In the Layer 3 Security field, check the **Web Policy** check box, and choose the **Authentication** option.



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.



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.

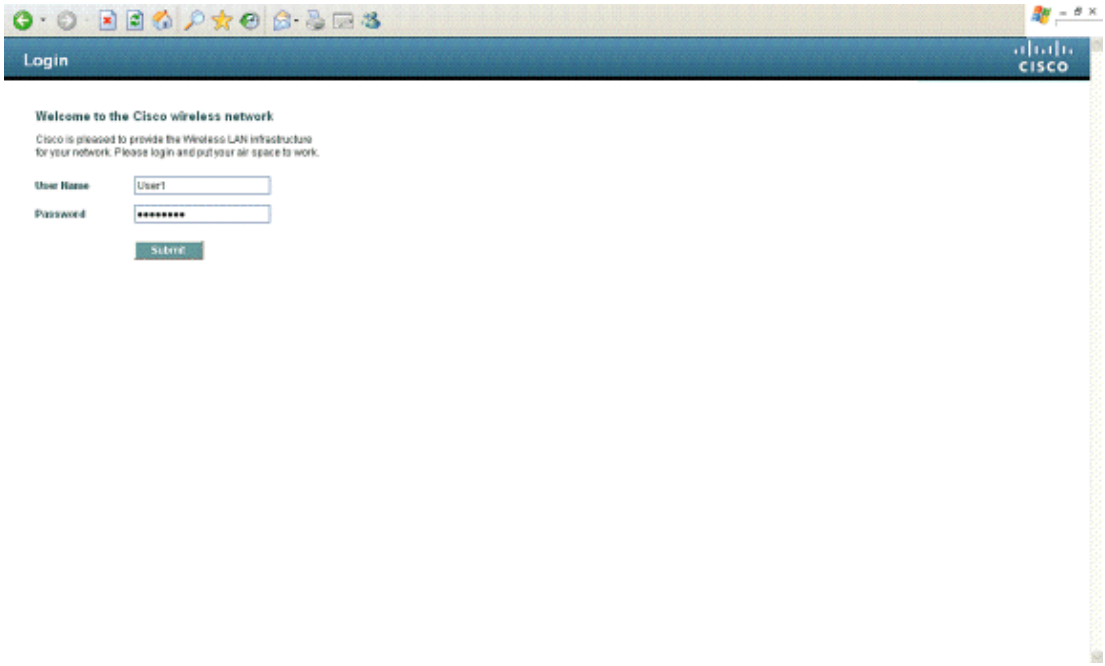
Verify

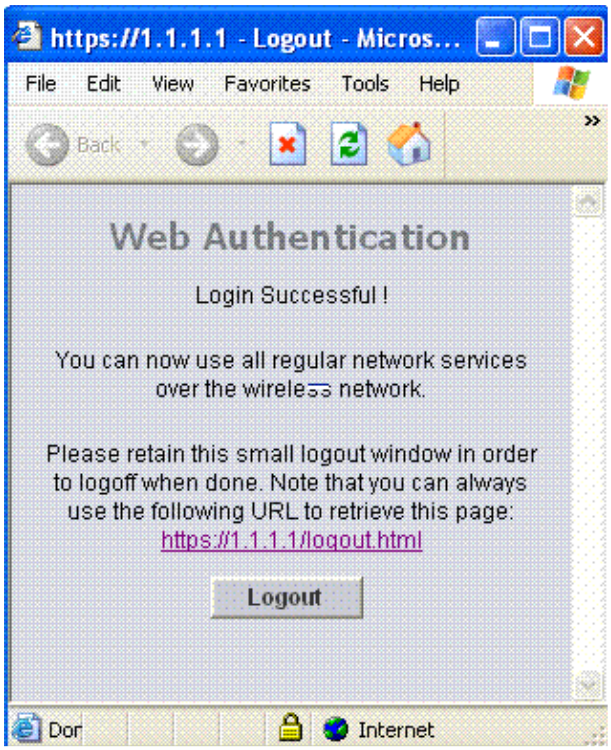
In order to verify this setup, connect a Wireless client and check if the configuration works as expected.

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.





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 **debug aaa all enable** command.

```
*Sep 19 15:16:10.286: AuthenticationRequest: 0x152c8e78


*Sep 19 15:16:10.286:
   Callback.....................................0x10567ae0

*Sep 19 15:16:10.286:
   protocolType.................................0x00000002

*Sep 19 15:16:10.286:
   proxyState...................................00:40:96:AF:3E:93-00:00

*Sep 19 15:16:10.286:   Packet contains 8 AVPs (not shown)

*Sep 19 15:16:10.287:
   ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE' (1)
*Sep 19 15:16:10.287:
   LDAP server 1 changed state to INIT
*Sep 19 15:16:10.287:
   ldapInitAndBind [1] called lcapi_init (rc = 0 - Success)
*Sep 19 15:16:10.296:
   ldapInitAndBind [1] configured Method Anonymous
   lcapi_bind (rc = 0 - Success)
*Sep 19 15:16:10.297: LDAP server 1 changed state to CONNECTED
*Sep 19 15:16:10.297: LDAP_CLIENT: UID Search (base=OU=LDAP-USERS,
   DC=LAB,DC=WIRELESS, pattern=(&(objectclass=Person)
   (sAMAccountName=User1)))
*Sep 19 15:16:10.308: LDAP_CLIENT: Returned 2 msgs
*Sep 19 15:16:10.308: LDAP_CLIENT: Returned msg 1 type 0x64
*Sep 19 15:16:10.308: LDAP_CLIENT:
   Received 1 attributes in search entry msg
*Sep 19 15:16:10.308: LDAP_CLIENT: Returned msg 2 type 0x65
*Sep 19 15:16:10.308: LDAP_CLIENT : No matched DN
*Sep 19 15:16:10.308: LDAP_CLIENT : Check result error 0 rc 1013
*Sep 19 15:16:10.309: ldapAuthRequest [1] called lcapi_query base=
   "OU=LDAP-USERS,DC=LAB,DC=WIRELESS" type="Person" attr="sAMAccountName"
   user="User1" (rc = 0 - Success)
*Sep 19 15:16:10.309: Attempting user bind with username
   CN=User1,OU=LDAP-USERS,DC=lab,DC=wireless
*Sep 19 15:16:10.335: LDAP ATTR> dn = CN=User1,OU=LDAP-USERS,
   DC=lab,DC=wireless (size 41)
*Sep 19 15:16:10.335: Handling LDAP response Success
*Sep 19 15:16:10.335: 00:40:96:af:3e:93 Returning AAA
   Success for mobile 00:40:96:af:3e:93
*Sep 19 15:16:10.335: AuthorizationResponse: 0x3fbf7b40


*Sep 19 15:16:10.336:   structureSize.........................137

*Sep 19 15:16:10.336:   resultCode............................0

*Sep 19 15:16:10.336:   protocolUsed..........................0x00000002

*Sep 19 15:16:10.336:   proxyState.............................
   00:40:96:AF:3E:93-00:00

*Sep 19 15:16:10.336:   Packet contains 3 AVPs:

*Sep 19 15:16:10.336:       AVP[01] Unknown Attribute 0.........
   CN=User1,OU=LDAP-USERS,DC=lab,DC=wireless (41 bytes)

*Sep 19 15:16:10.336:         AVP[02] User-Name.............
   User1 (5 bytes)
```

```
*Sep 19 15:16:10.336:          AVP[03] User−Password....[...]

*Sep 19 15:16:10.336: Authentication failed for User1,
   Service Type: 0
*Sep 19 15:16:10.336: 00:40:96:af:3e:93 Applying new AAA
   override for station 00:40:96:af:3e:93
*Sep 19 15:16:10.336: 00:40:96:af:3e:93
   Override values for station 00:40:96:af:3e:93
        source: 48, valid bits: 0x1
        qosLevel: −1, dscp: 0xffffffff, dot1pTag:
   0xffffffff, sessionTimeout: −1
        dataAvgC: −1, rTAvg
*Sep 19 15:16:10.337: 00:40:96:af:3e:93 Unable to apply
   override policy for station 00:40:96:af:3e:93 −
   VapAllowRadiusOverride is FALSE
*Sep 19 15:16:10.339: 00:40:96:af:3e:93 Sending
   Accounting request (0) for station 00:40:96:af:3e:93
*Sep 19 15:16:10.339: AccountingMessage
   Accounting Start: 0x152d9778

*Sep 19 15:16:10.339:   Packet contains 11 AVPs:

*Sep 19 15:16:10.339:
   AVP[01] User−Name.....................User1 (5 bytes)

*Sep 19 15:16:10.339:
   AVP[02] Nas−Port.....................0x00000002
   (2) (4 bytes)

*Sep 19 15:16:10.339:
   AVP[03] Nas−Ip−Address.................0x0a4df4cc
   (172881100) (4 bytes)

*Sep 19 15:16:10.339:
   AVP[04] Framed−IP−Address..............0x0a4df4c6
   (172881094) (4 bytes)

*Sep 19 15:16:10.339:
   AVP[05] NAS−Identifier.................WLC−4400 (8 bytes)

*Sep 19 15:16:10.339:
   AVP[06] Airespace / WLAN−Identifier.....0x00000001 (1)
   (4 bytes)

*Sep 19 15:16:10.340:
   AVP[07] Acct−Session−Id.................
   48d3c23a/00:40:96:af:3e:93/162 (30 bytes)

*Sep 19 15:16:10.340:
   AVP[08] Acct−Authentic.................0x00000003 (3)
   (4 bytes)

*Sep 19 15:16:10.340:
   AVP[09] Acct−Status−Type...............0x00000001 (1)
   (4 bytes)

*Sep 19 15:16:10.340:
   AVP[10] Calling−Station−Id.............10.77.244.198
   (13 bytes)

*Sep 19 15:16:10.340:
   AVP[11] Called−Station−Id..............10.77.244.204
   (13 bytes)
```

NetPro Discussion Forums − Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums − Featured Conversations for Wireless
Wireless − Mobility: WLAN Radio Standards
Wireless − Mobility: Security and Network Management
Wireless − Mobility: Getting Started with Wireless
Wireless − Mobility: General

Related Information

- **Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC)**
- **Wireless LAN Controller Web Authentication Configuration Example**
- **External Web Authentication with Wireless LAN Controllers Configuration Example**
- **Technical Support & Documentation − Cisco Systems**

Updated: Sep 26, 2008 Document ID: 108008