在無線LAN控制器(WLC)上使用LDAP的Web驗證組態範例

目錄

簡介

本文說明如何設定無線LAN控制器(WLC)以進行Web驗證。本章介紹如何將輕量級目錄訪問協定(LDAP)伺服器配置為用於Web身份驗證的後端資料庫，以檢索使用者憑據並對使用者進行身份驗證。

必要條件

需求

思科建議您瞭解以下主題：

- 輕量型存取點(LAP)和Cisco WLC的組態資訊
- 無線存取點通訊協定(CAPWAP)的控制和布建知識
- 瞭解如何設定和配置輕量級目錄訪問協定(LDAP)、Active Directory和域控制器

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 5508 WLC（執行韌體版本8.2.100.0）
- 思科1142系列LAP
- 思科802.11a/b/g無線客戶端介面卡。
- 執行LDAP伺服器角色的Microsoft Windows 2012 Essentials伺服器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

慣例

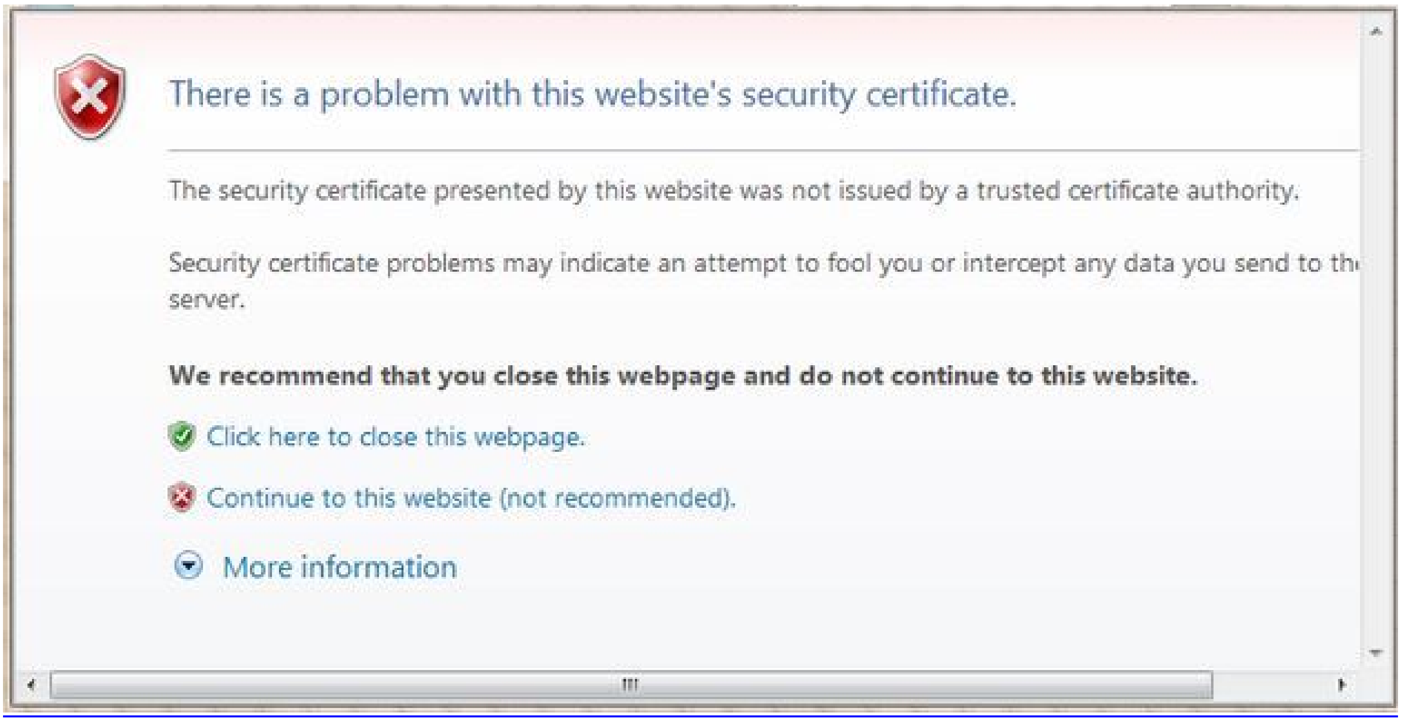
請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

Web驗證程式

Web驗證是第3層安全功能，會導致控制器禁止來自特定使用者端的IP流量（DHCP和DNS相關封包除外），直到該使用者端正確提供了有效的使用者名稱和密碼。使用Web驗證來驗證使用者端時，必須為每個使用者端定義使用者名稱和密碼。然後，當客戶端嘗試加入無線LAN時，必須在登入頁面提示時輸入使用者名稱和密碼。

啟用Web驗證後（在第3層安全下），使用者在第一次嘗試存取URL時，偶爾會收到Web瀏覽器安全警告。

> **提示**：要刪除此證書警告，請返回以下有關如何安裝第三方受信任證書的指南 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.

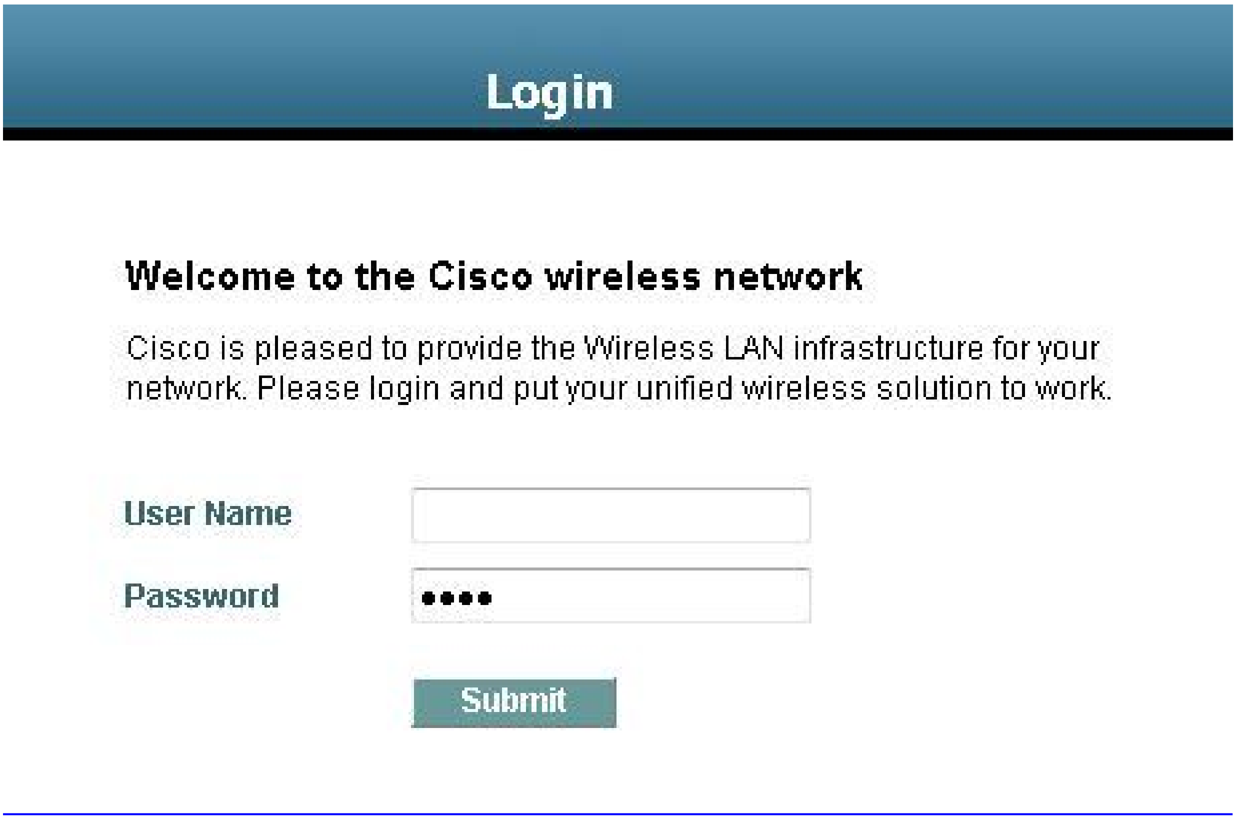
The security certificate presented by this website was not issued by a trusted certificate authority.

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

按一下**Yes**以繼續(或更準確地說，**Continue to this website（不推薦）**（例如，對於Firefox瀏覽器 ））後，或者如果使用者端的瀏覽器不顯示安全警報，Web驗證系統會將使用者端重新導向到登入頁面，如下圖所示：



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

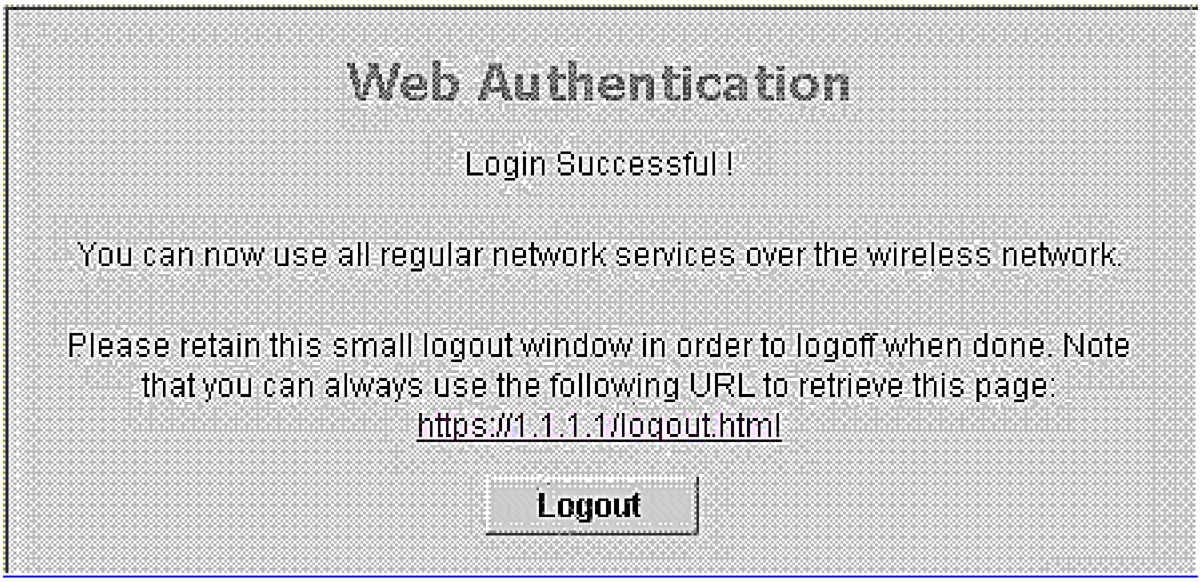
Password ●●●●

預設登入頁面包含思科徽標和思科特定文本。您可以選擇讓Web驗證系統顯示以下其中一項：

- 預設登入頁面
- 修改後的預設登入頁面
- 在外部Web伺服器上設定的自訂登入頁面
- 下載到控制器的自訂登入頁面

在Web驗證登入頁面中輸入有效的使用者名稱和密碼並點選**Submit**時，將根據提交的憑證和來自後

端資料庫（本例中為LDAP）的成功驗證進行驗證。然後，Web驗證系統顯示一個成功的登入頁面，並將已驗證使用者端重新導向到所請求的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

預設成功登入頁面包含指向虛擬網關地址URL的指標:https://1.1.1.1/logout.html。為控制器虛擬介面設定的IP位址會用作登入頁面的重新導向位址。

本檔案介紹如何使用WLC上的內部網頁進行Web驗證。此示例使用LDAP伺服器作為Web身份驗證的後端資料庫來檢索使用者憑據並對使用者進行身份驗證。

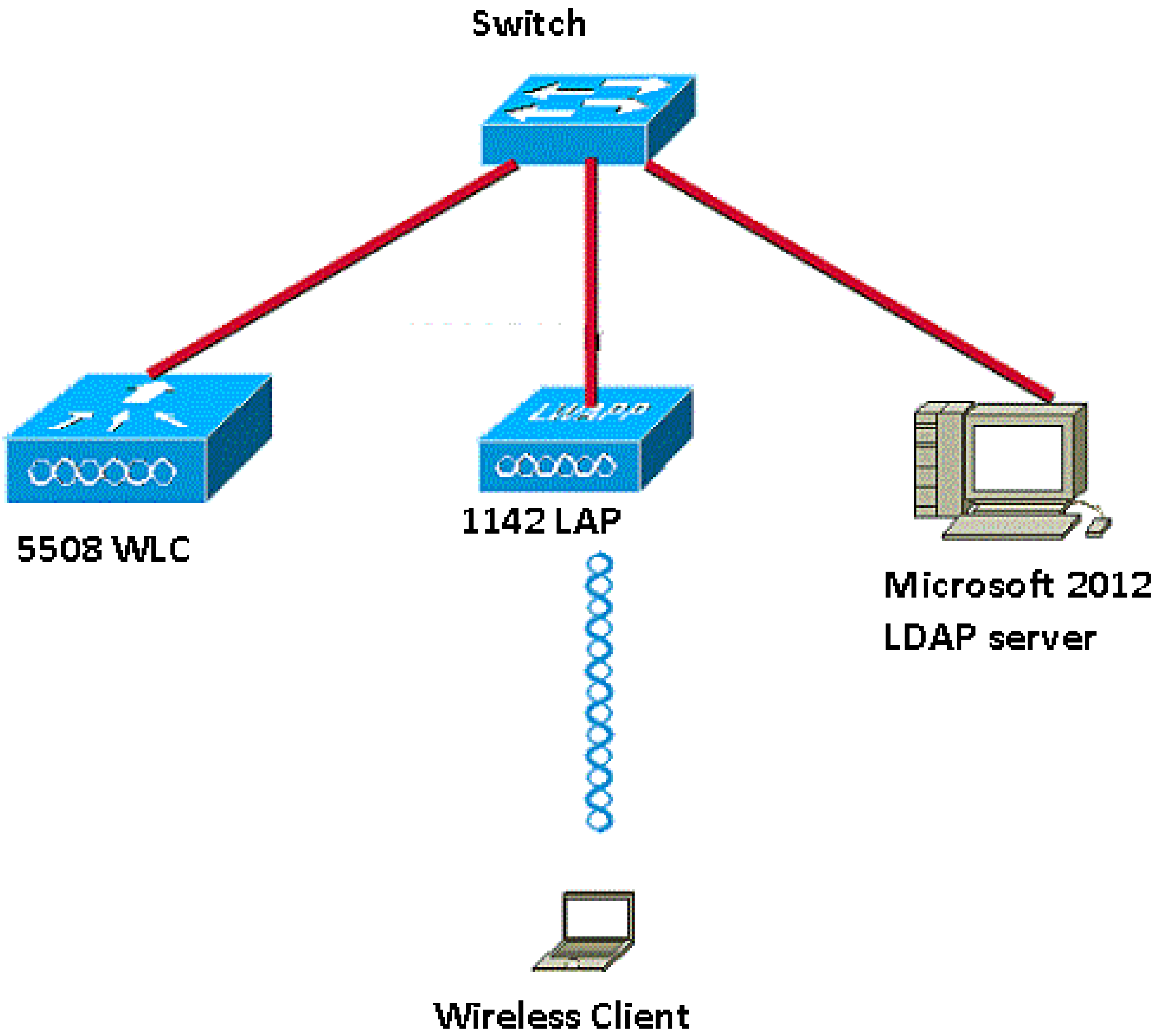
設定

本節提供用於設定本文件中所述功能的資訊。

注意：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



組態

完成以下步驟以成功實施此設定：

- 配置LDAP伺服器。
- 為LDAP伺服器配置WLC。
- 為Web驗證設定WLAN。

配置LDAP伺服器

第一步是配置LDAP伺服器，該伺服器用作儲存無線客戶端的使用者憑據的後端資料庫。在本示例中，Microsoft Windows 2012 Essentials伺服器用作LDAP伺服器。

LDAP伺服器配置的第一步是在LDAP伺服器上建立使用者資料庫，以便WLC可以查詢此資料庫以驗證使用者。

在域控制器上建立使用者

組織單位(OU)包含多個在PersonProfile中引用個人條目的組。個人可以是多個組的成員。所有對象類和屬性定義均為LDAP架構預設值。每個組都包含屬於它的每個人的引用(dn)。

在此示例中，將建立一個新的OU LDAP-USERS，並在此OU下建立使用者User1。配置此使用者進

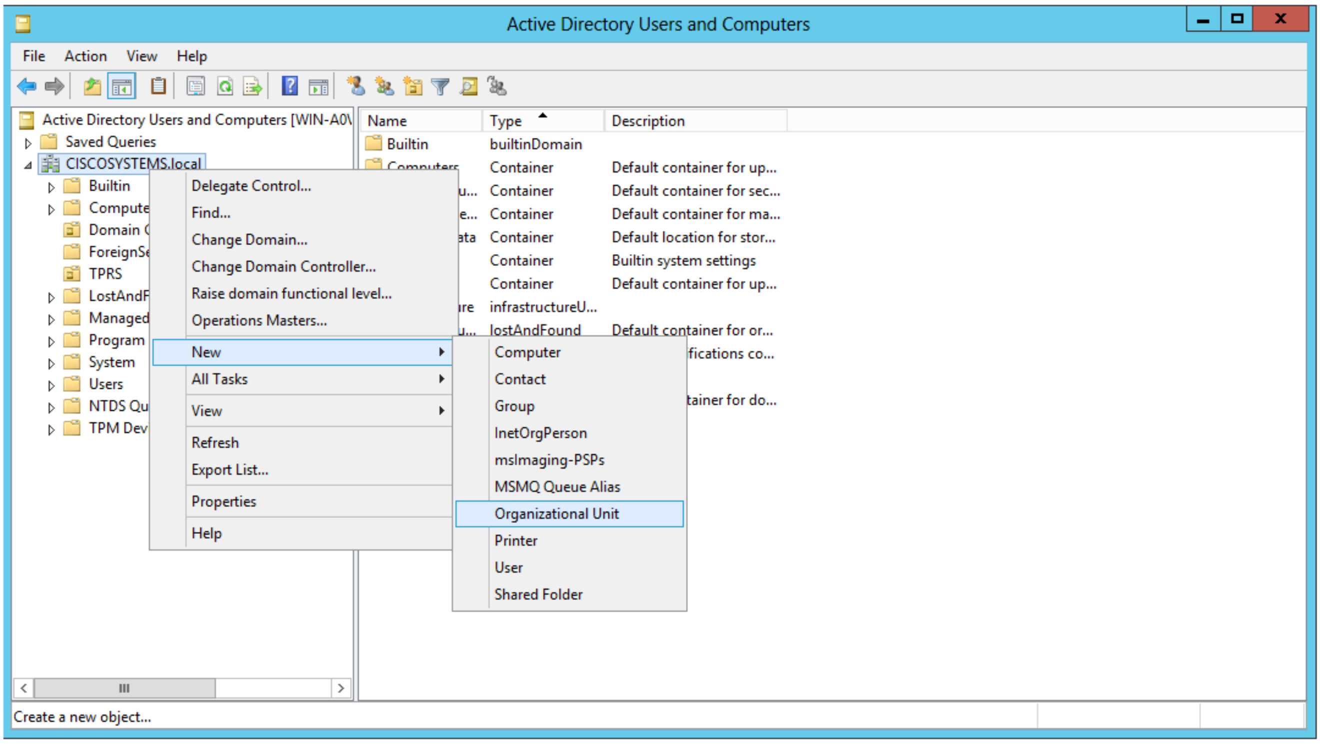
行LDAP訪問時，WLC可以查詢此LDAP資料庫進行使用者身份驗證。

本示例中使用的域是**CISCOSYSTEMS.local**。

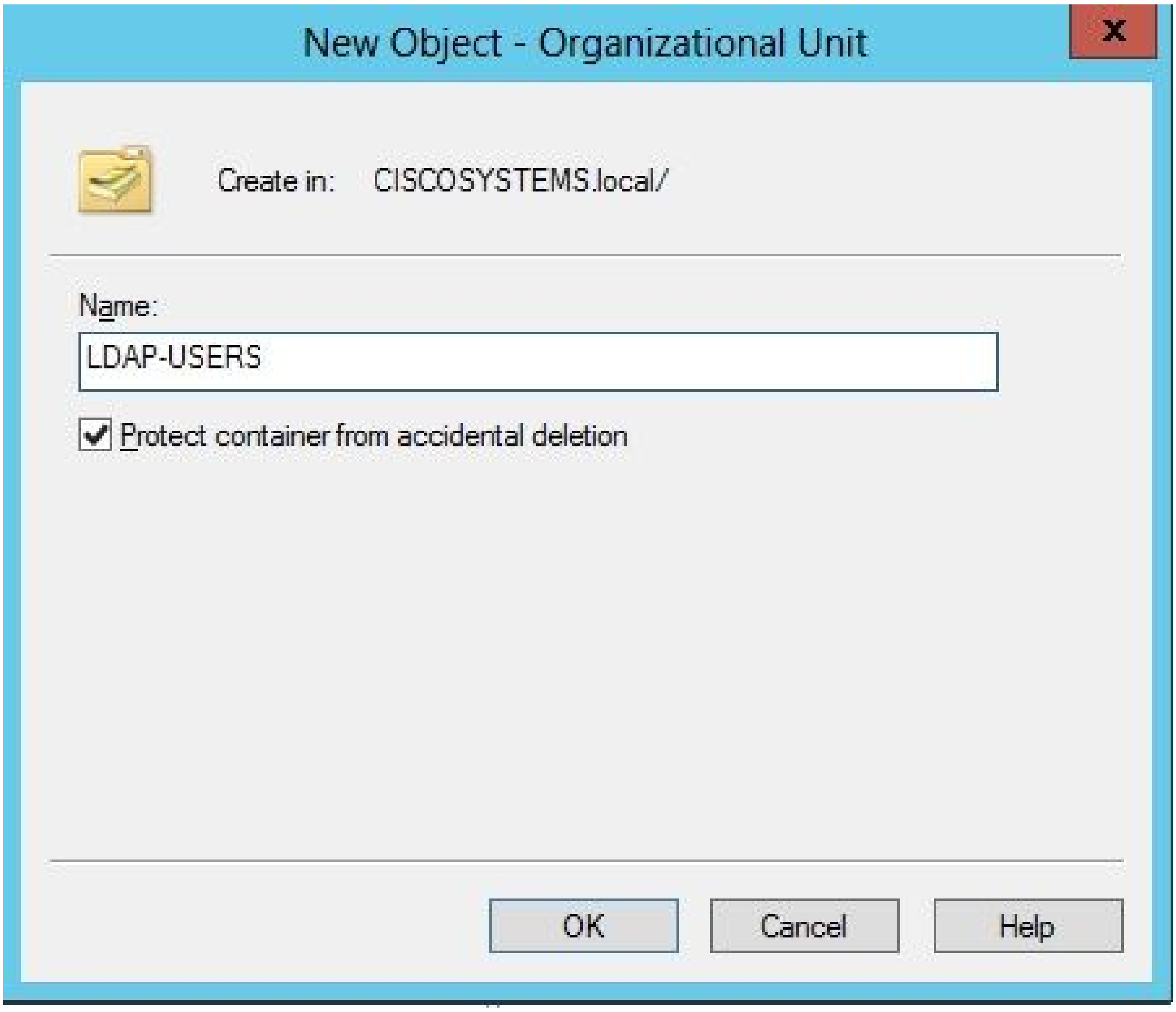
在OU下建立使用者資料庫

本節介紹如何在您的域中建立新的OU並在此OU上建立新使用者。

1. 開啟Windows PowerShell並鍵入**servermanager.exe**
2. 在「伺服器管理器」(Server Manager)視窗中，按一下**AD DS。**然後按一下右鍵您的伺服器名稱，以選擇**Active Directory使用者和電腦。**
3. 按一下右鍵您的域名(在本示例中為**CISCOSYSTEMS.local**)，然後從上下文選單導航到**New > Organizational Unit**以建立新的OU。



4. 為此OU分配名稱並按一下**OK**，如下圖所示：



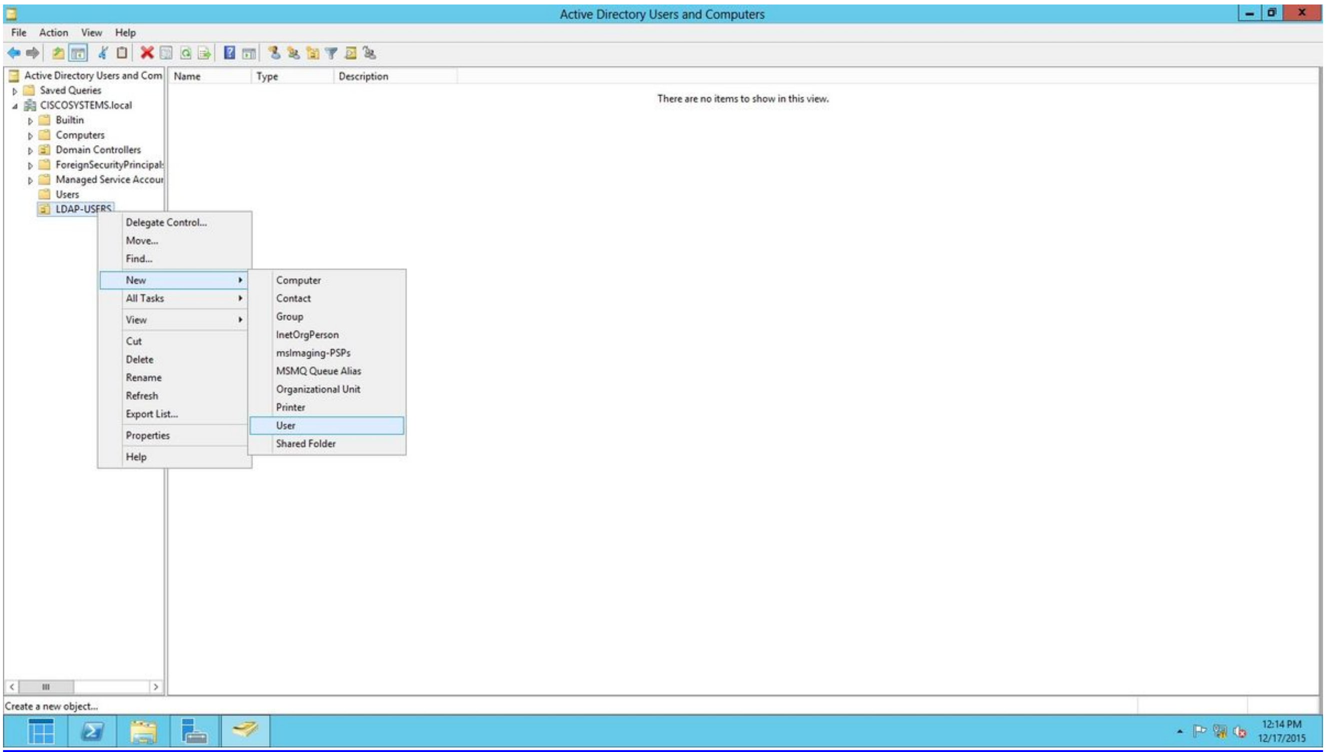
Create in: CISCOSYSTEMS.local/

Name:
LDAP-USERS

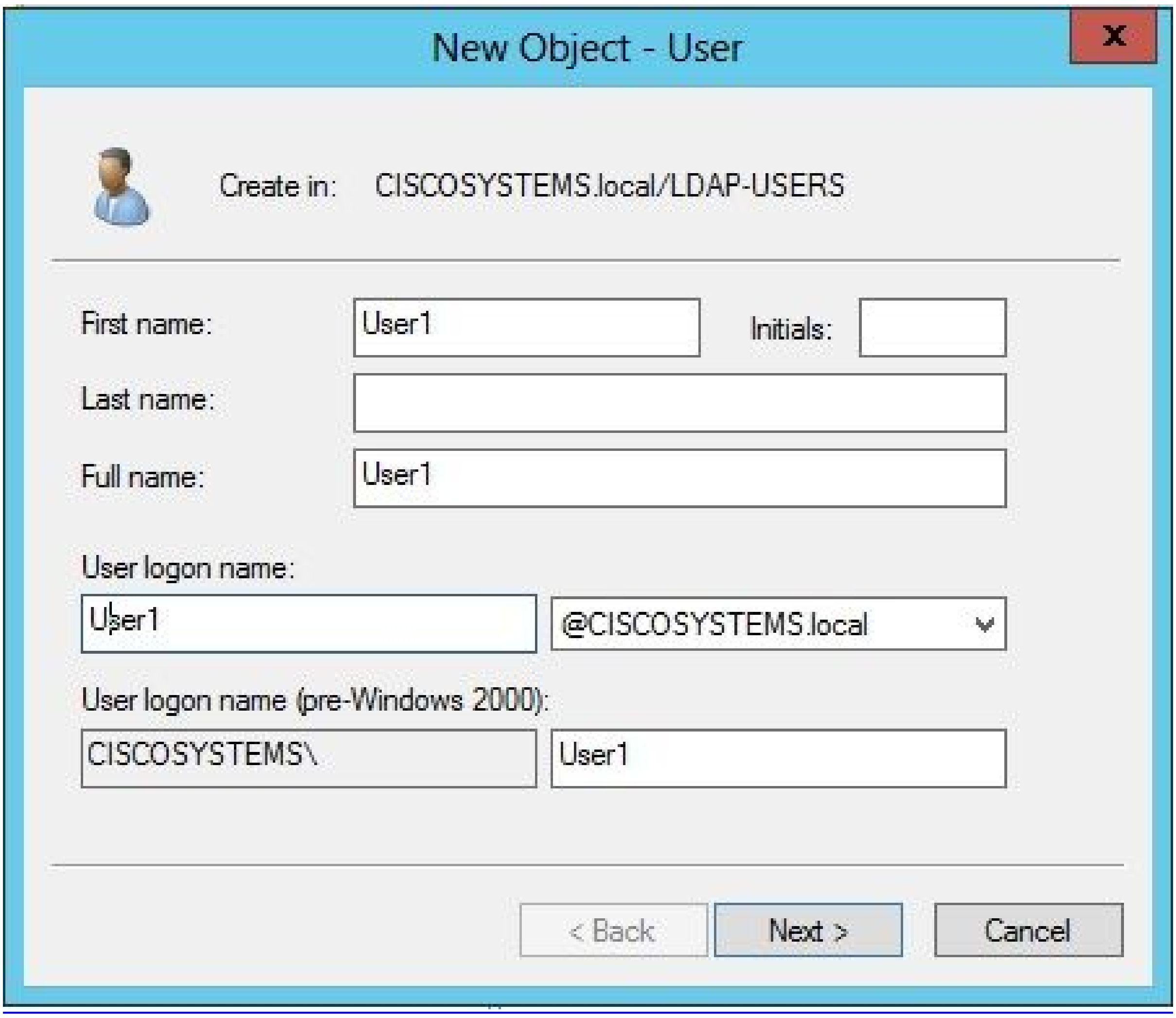
☑ Protect container from accidental deletion

現在在LDAP伺服器上建立了新的OU LDAP-USERS，下一步是在此OU下建立使用者**User1**。為了達成此目的，請完成以下步驟：

1. 按一下右鍵建立的新OU。從生成的上下文選單導航到**LDAP-USERS> New > User**，以建立新使用者，如下圖所示：



2. 在「使用者設定」頁面中，填寫所需欄位，如本例所示。此示例在**User logon name**欄位中包含**User1**。這是在LDAP資料庫中驗證以對客戶端進行身份驗證的使用者名稱。此示例在First name和Full Name欄位中使用User1。按「**Next**」（下一步）。


New Object - User

Create in: CISCOSYSTEMS.local/LDAP-USERS

First name: User1

Initials:

Last name:

Full name: User1

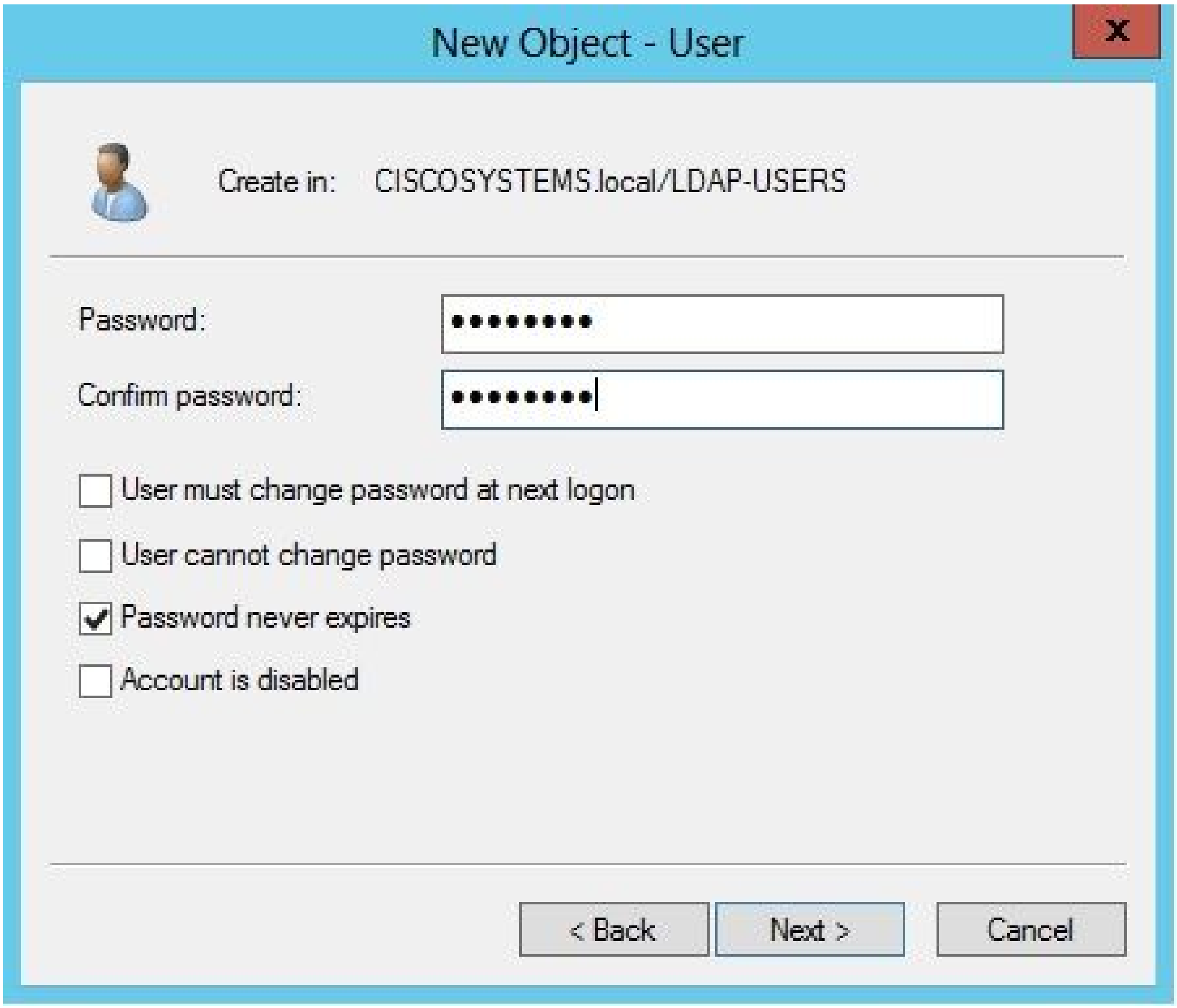
User logon name:

User1 @CISCOSYSTEMS.local

User logon name (pre-Windows 2000):

CISCOSYSTEMS\ User1

3. 輸入密碼並確認密碼。選擇**Password never expires**選項，然後按一下**Next**。



Create in: CISCOSYSTEMS.local/LDAP-USERS

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

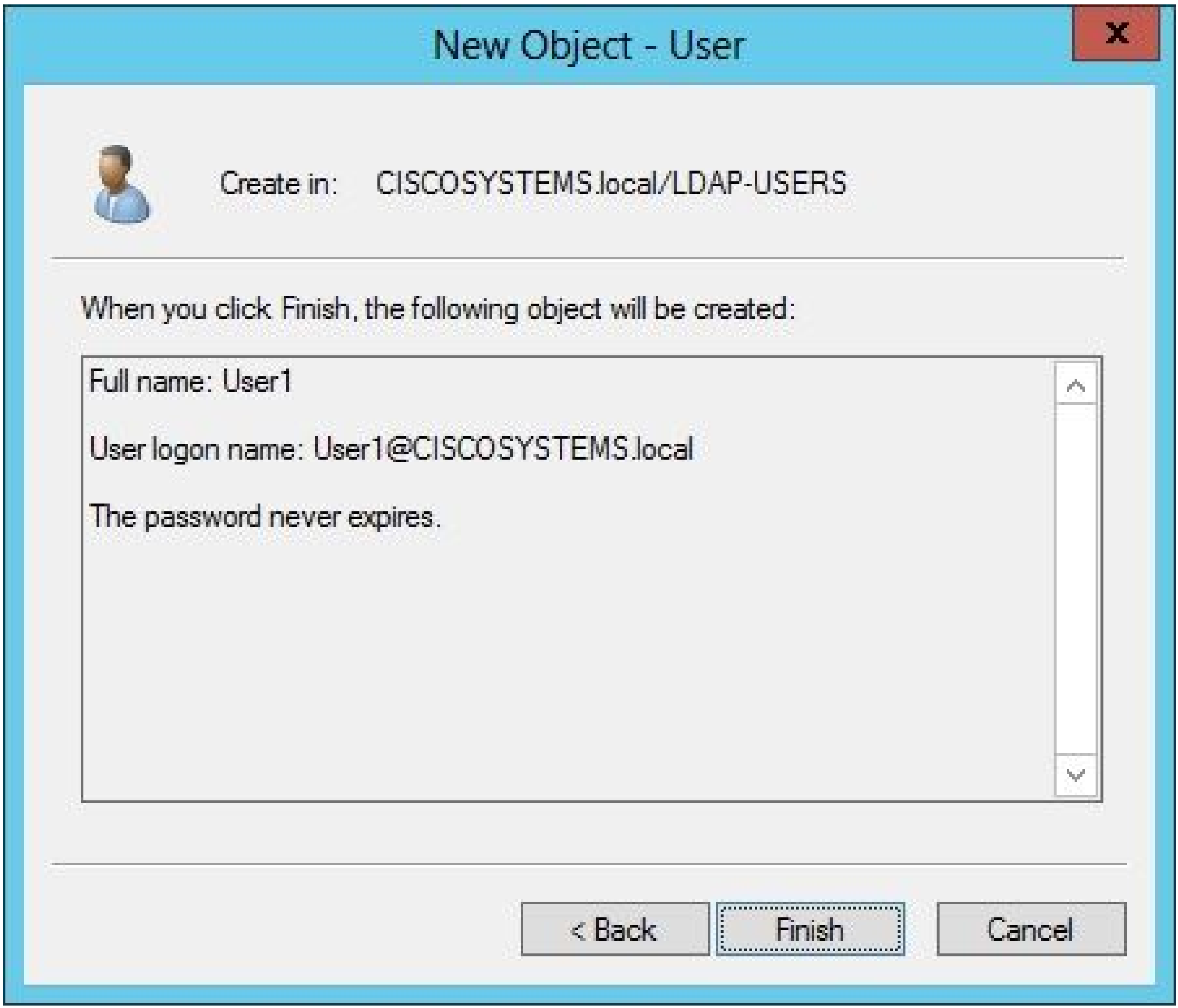
□ User must change password at next logon

□ User cannot change password

☑ Password never expires

□ Account is disabled

4. 按一下「**Finish**」（結束）。在OU LDAP-USERS下建立新的使用者User1。以下是使用者憑據：使用者名稱**:User1**密碼： **筆記型電腦123**


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.

現在使用者是在OU下建立的，下一步是配置此使用者以進行LDAP訪問。

配置使用者的LDAP訪問

您可以選擇**Anonymous**或**Authenticated**來指定LDAP伺服器的本地身份驗證繫結方法。Anonymous方法允許匿名訪問LDAP伺服器。Authenticated方法要求輸入使用者名稱和密碼來保護訪問。預設值為Anonymous。

本節介紹如何配置匿名方法和已驗證方法。

匿名繫結

注意：不建議使用匿名繫結。LDAPLDAP

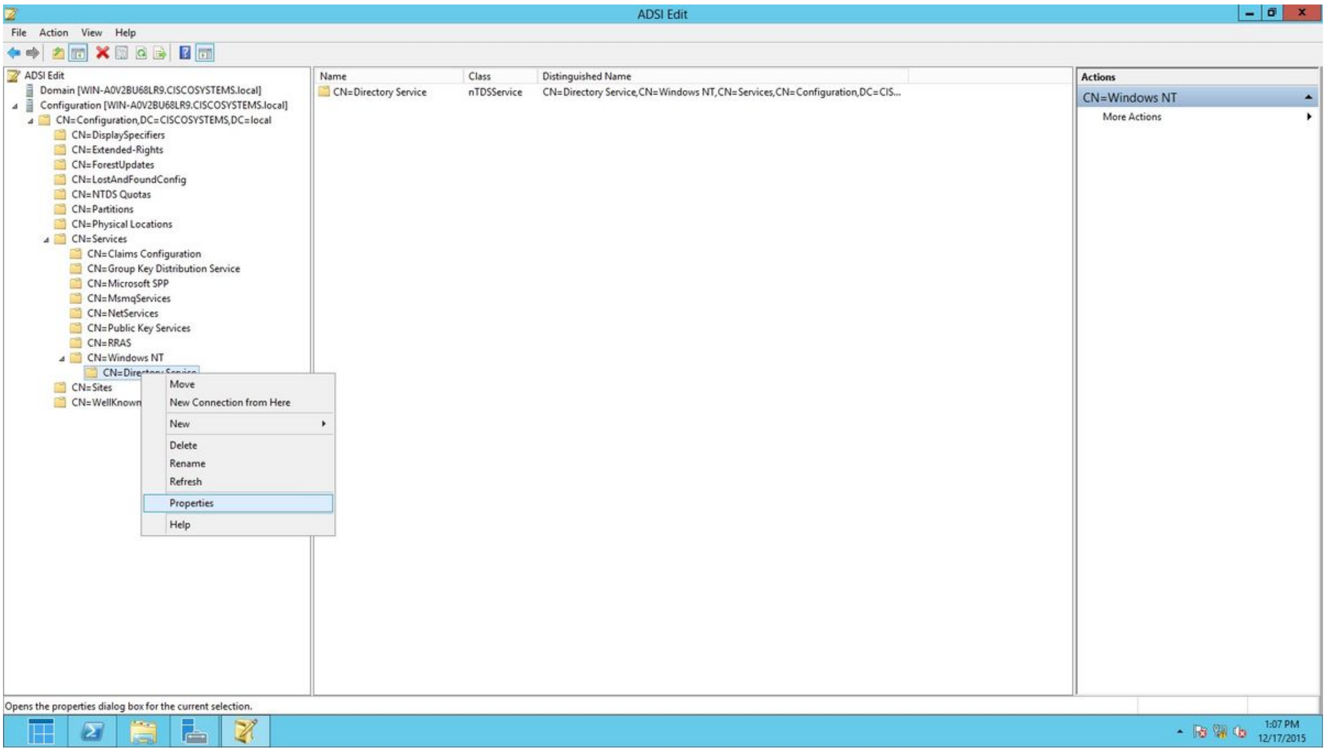
執行本節中的步驟，為LDAP訪問配置匿名使用者。

在Windows 2012 Essentials Server上啟用匿名繫結功能

對於要在LDAP上訪問Windows 2012 AD的任何第三方應用程式（在本例中為WLC），必須在Windows 2012上啟用匿名繫結功能。預設情況下，在Windows 2012域控制器上不允許匿名LDAP操作。執行以下步驟以啟用匿名繫結功能：

1. 在Windows PowerShell中鍵入ADSIEdit.msc，**啟動ADSI** Edit工具。此工具是Windows 2012支援工具的一部分。

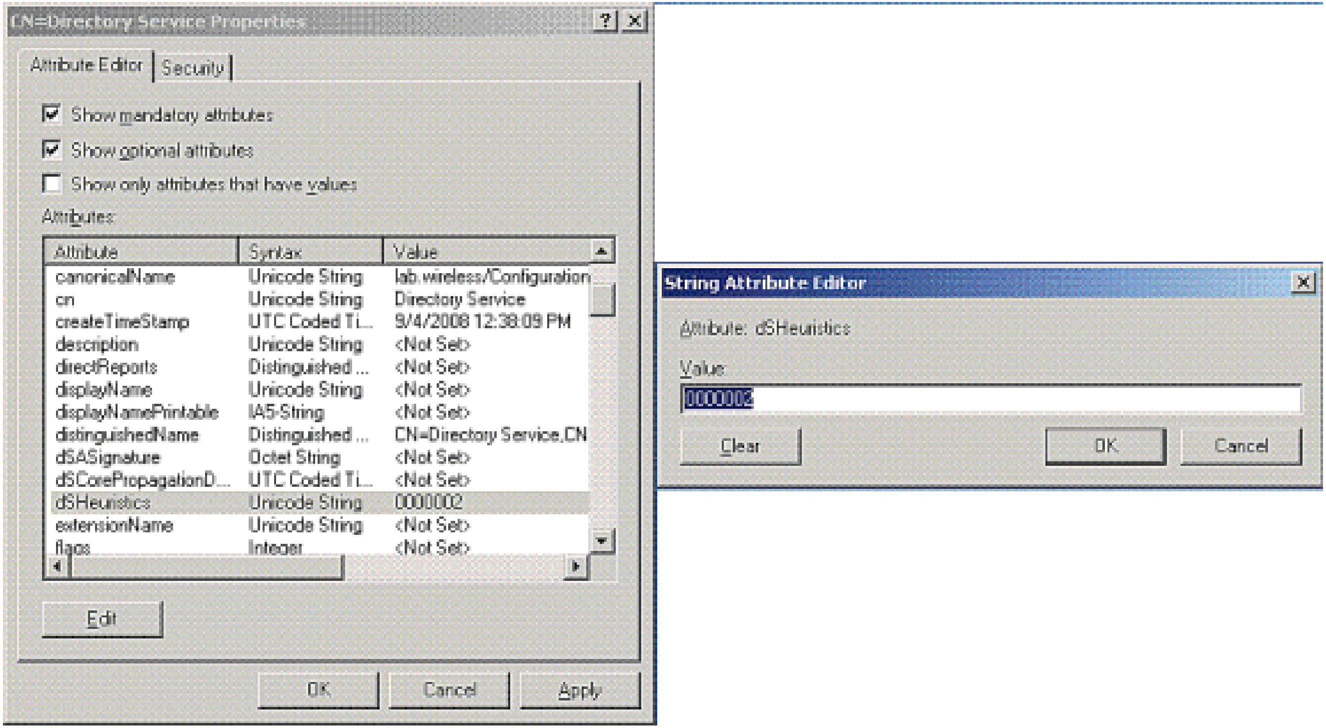
2. 在ADSI Edit視窗中，展開根域（配置[WIN-A0V2BU68LR9.CISCOSYSTEMS.local]）。導航到**CN=Services > CN=Windows NT > CN=Directory Service**。按一下右鍵**CN=Directory Service**容器，然後從上下文選單中選擇**Properties**，如下圖所示：



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. 在CN=Directory Service Properties視窗的**Attributes**下，按一下Attribute欄位下的**dsHeuristics**屬性，然後選擇**Edit**。在此屬性的「字串屬性編輯器」視窗中，輸入值**0000002**；按一下**Apply**和**OK**，如下圖所示。Windows 2012伺服器上啟用了匿名繫結功能。**註**：最後（第七）個字元用於控制繫結到LDAP服務的方式。0（零）或無第七個字元表示已禁用匿名LDAP操作。如果將第七個字元設定為2，則會啟用匿名繫結功能。



☑ 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>

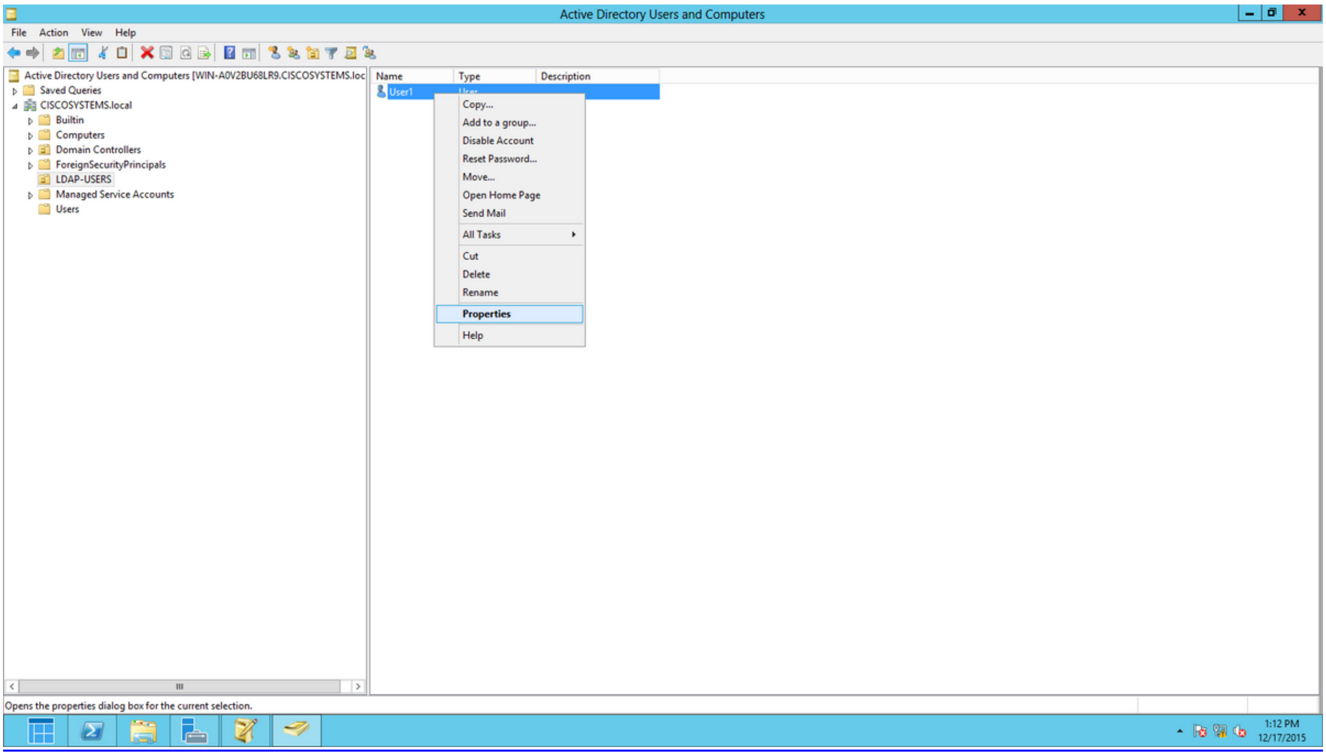
Attribute: dSHeuristics

Value: 0000002

向使用者授予ANONYMOUS登入訪問許可權

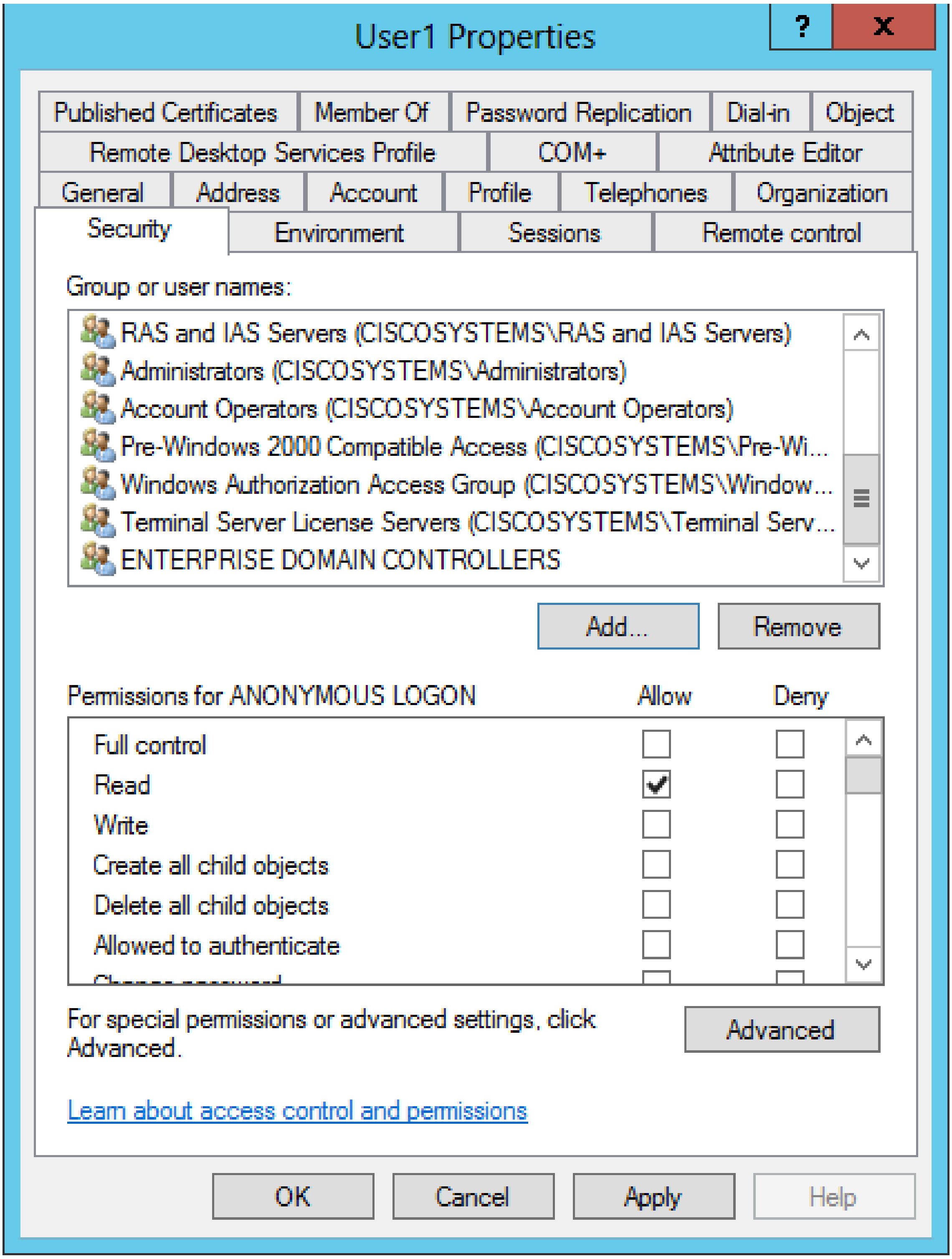
下一步是向使用者User1授予ANONYMOUS LOGON訪問許可權。完成以下步驟即可完成以下操作：

1. 開啟**Active Directory使用者和電腦**。
2. 確保選中**View Advanced Features**。
3. 導航到使用者User1，然後按一下右鍵該使用者。從上下文選單中選擇**屬性**。此使用者使用名字User1標識。



Opens the properties dialog box for the current selection.

4. 按一下**Security**索引標籤，如下圖所示：



Group or user names:

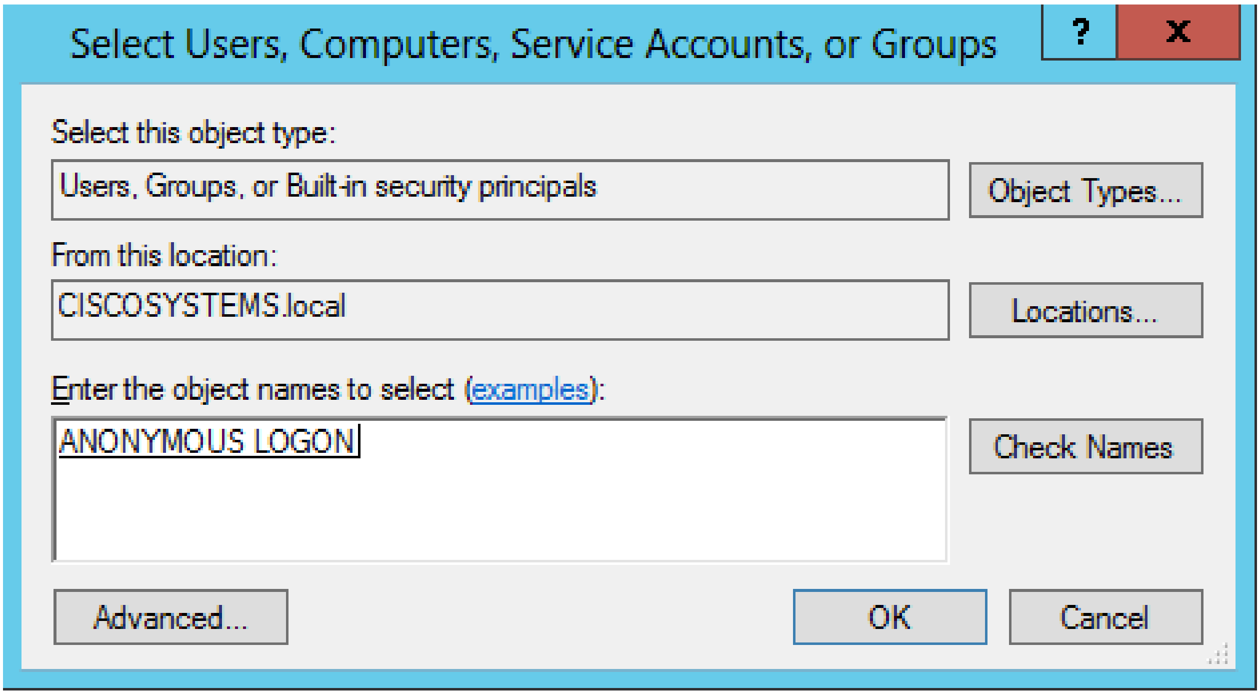
- RAS and IAS Servers (CISCOSYSTEMS\RAS and IAS Servers)
- Administrators (CISCOSYSTEMS\Administrators)
- Account Operators (CISCOSYSTEMS\Account Operators)
- Pre-Windows 2000 Compatible Access (CISCOSYSTEMS\Pre-Wi...
- Windows Authorization Access Group (CISCOSYSTEMS\Window...
- Terminal Server License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

5. 在生成的視窗中按一下**Add**。

6. 在「*Enter the object names to select*」框下輸入**ANONYMOUS LOGON**並確認對話方塊，如下圖所示：



Select Users, Computers, Service Accounts, or Groups

Select this object type:

Users, Groups, or Built-in security principals

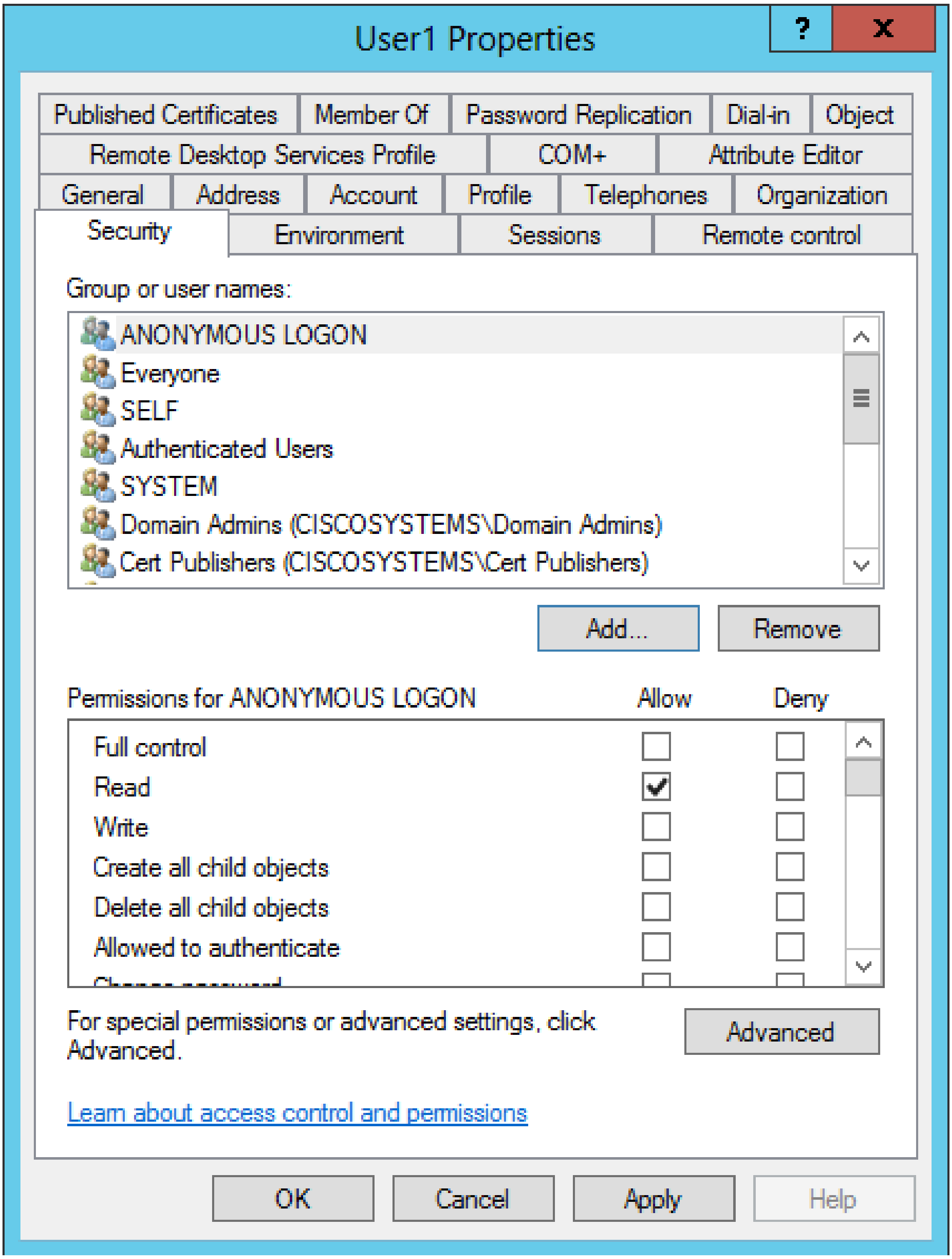
From this location:

CISCOSYSTEMS.local

Enter the object names to select (examples):

ANONYMOUS LOGON

7. 在ACL中，請注意ANONYMOUS LOGON有權訪問使用者的一些屬性集。按一下「**OK**」（確定）。已授予此使用者匿名登入訪問許可權，如下圖所示：



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	□	□

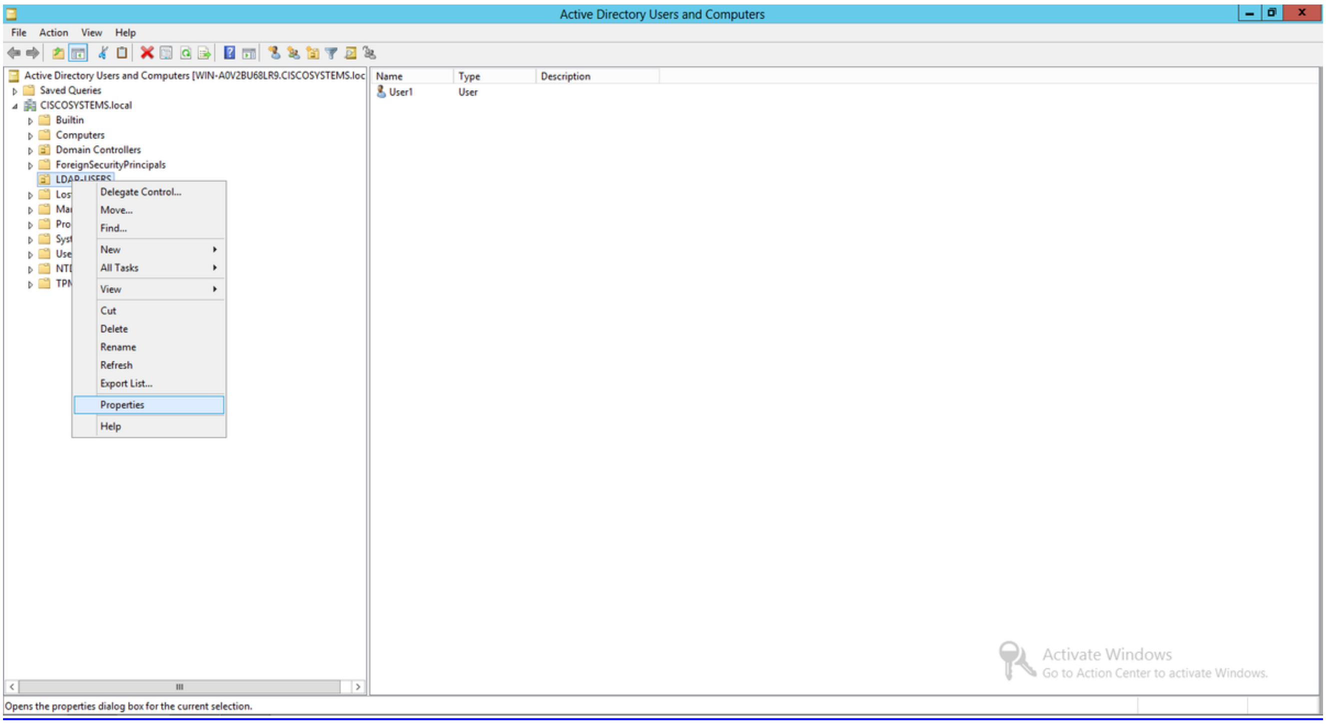
For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

對OU授予清單內容許可權

下一步是至少向使用者所在的OU上的ANONYMOUS LOGON授予List Contents許可權。在本示例中，User1位於OU LDAP-USERS上。完成以下步驟即可完成以下操作：

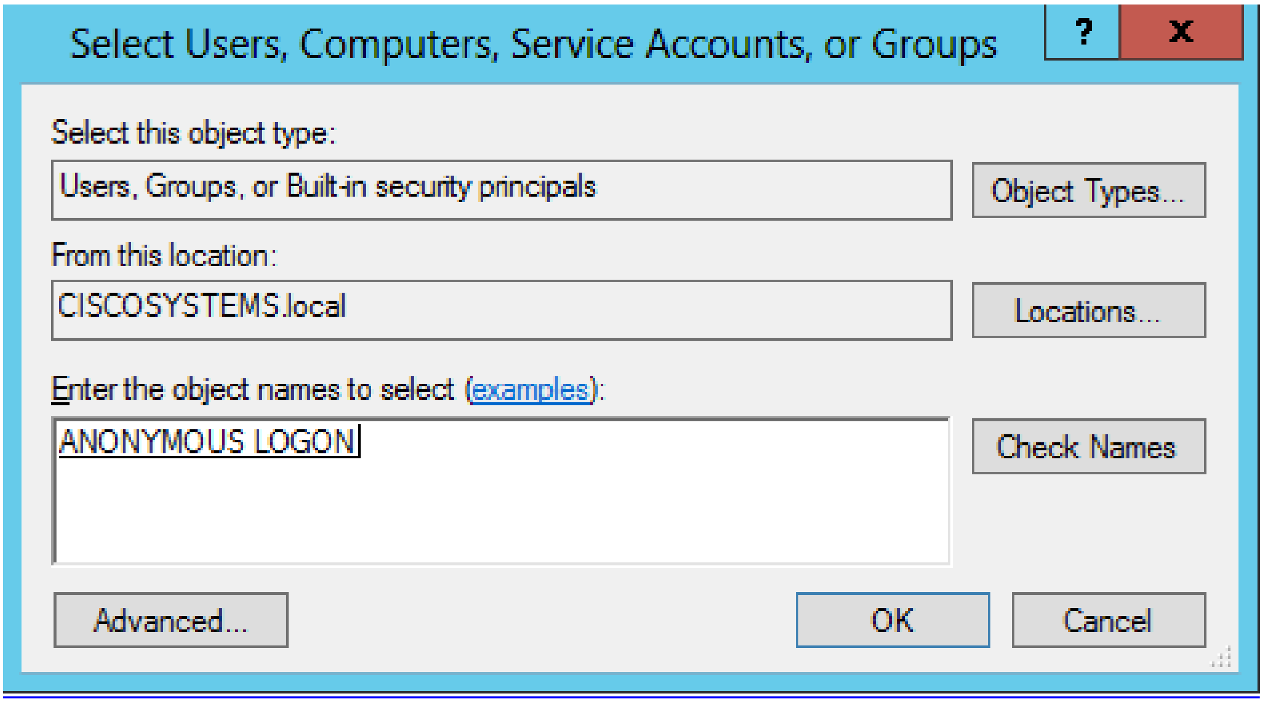
1. 在**Active Directory Users and Computers**中，按一下右鍵**OU LDAP-USERS**，然後選擇**Properties**，如下圖所示：



Opens the properties dialog box for the current selection.

2. 按一下「**Security**」。

3. 按一下「**Add**」。在開啟的對話方塊中，輸入**ANONYMOUS LOGON**並確認對話方塊，如下圖所示：



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

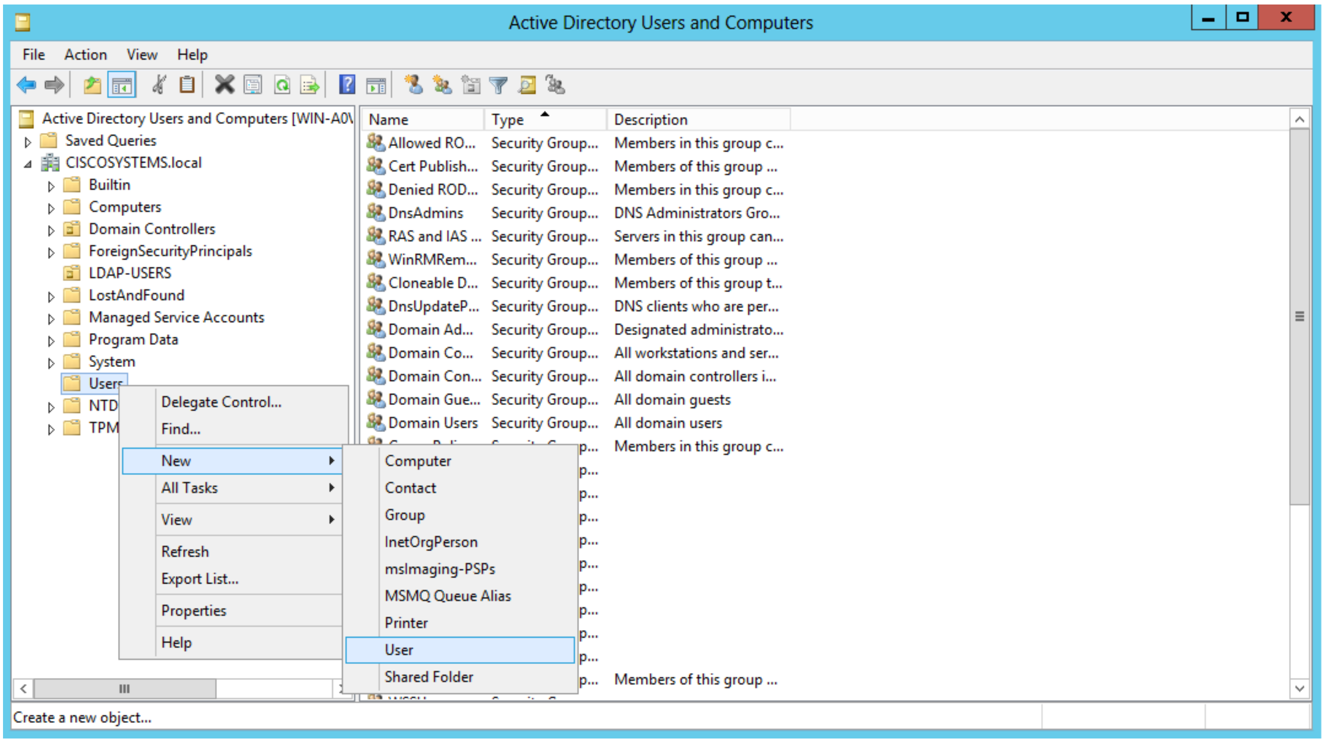
已驗證的繫結

執行本節中的步驟以配置對LDAP伺服器進行本地身份驗證的使用者。

1. 開啟Windows PowerShell並鍵入 **servermanager.exe**

2. 在「伺服器管理器」(Server Manager)視窗中，按一下**AD DS。**然後按一下右鍵您的伺服器名稱以選擇 **Active Directory使用者和電腦。**

3. 按一下右鍵**Users**。從生成的上下文選單中導航到**New** > **User**，以建立新使用者。



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
	p...	Members in this group c...
	p...	
	p...	
	p...	
	p...	
	p...	
	p...	
	p...	
	p...	
	p...	
	p...	Members of this group ...

4. 在「使用者設定」頁面中，填寫所需欄位，如本例所示。此範例在**User logon name**欄位中具有**WLC-admin**。這是用於對LDAP伺服器進行本地身份驗證的使用者名稱。按「**Next**」（下一步）。

5. 輸入密碼並確認密碼。選擇**Password never expires**選項，然後按一下**Next**。

6. 按一下「**Finish**」（結束）。在**Users**容器下建立新的使用者WLC-admin。以下是使用者憑據：使用者名稱:**WLC-admin**密碼：**Admin123**

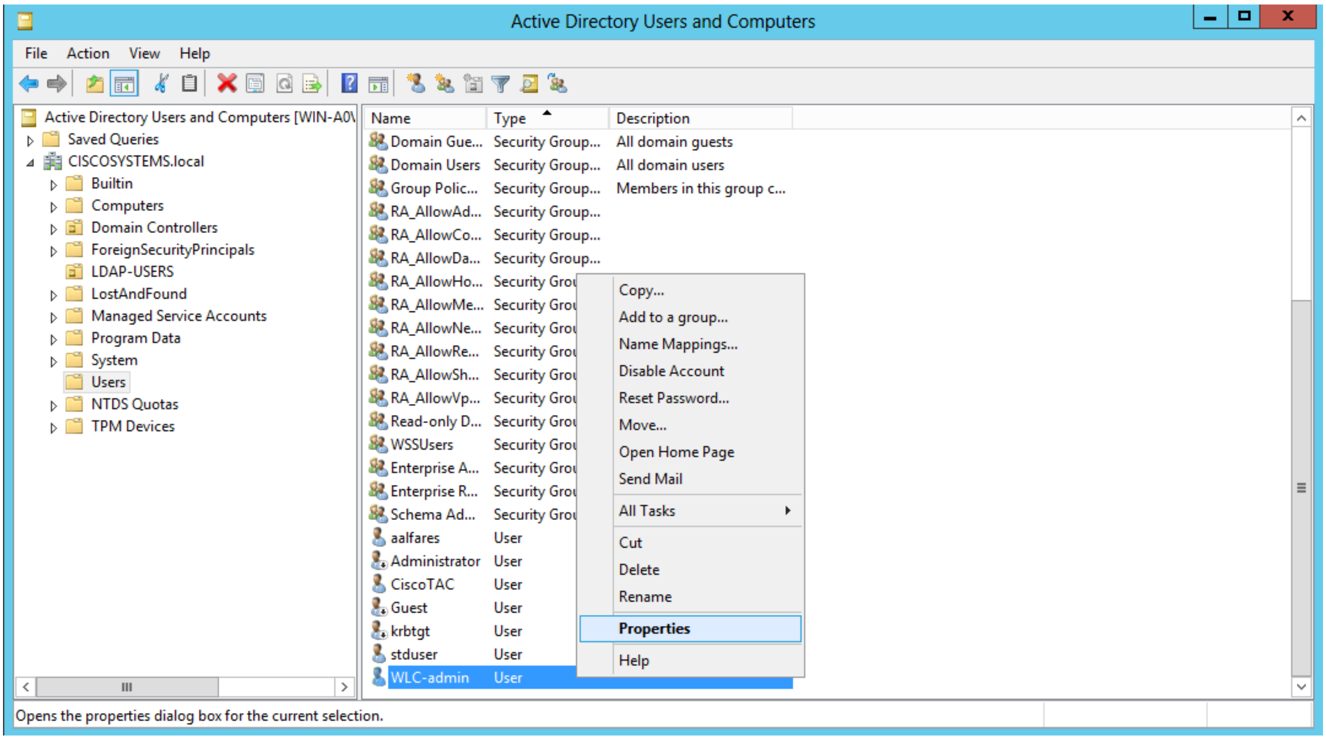
向WLC-admin授予管理員許可權

建立本地身份驗證使用者後，我們需要授予其管理員許可權。完成以下步驟即可完成以下操作：

1. 開啟**Active Directory使用者和電腦**。

2. 確保選中**View Advanced Features**。

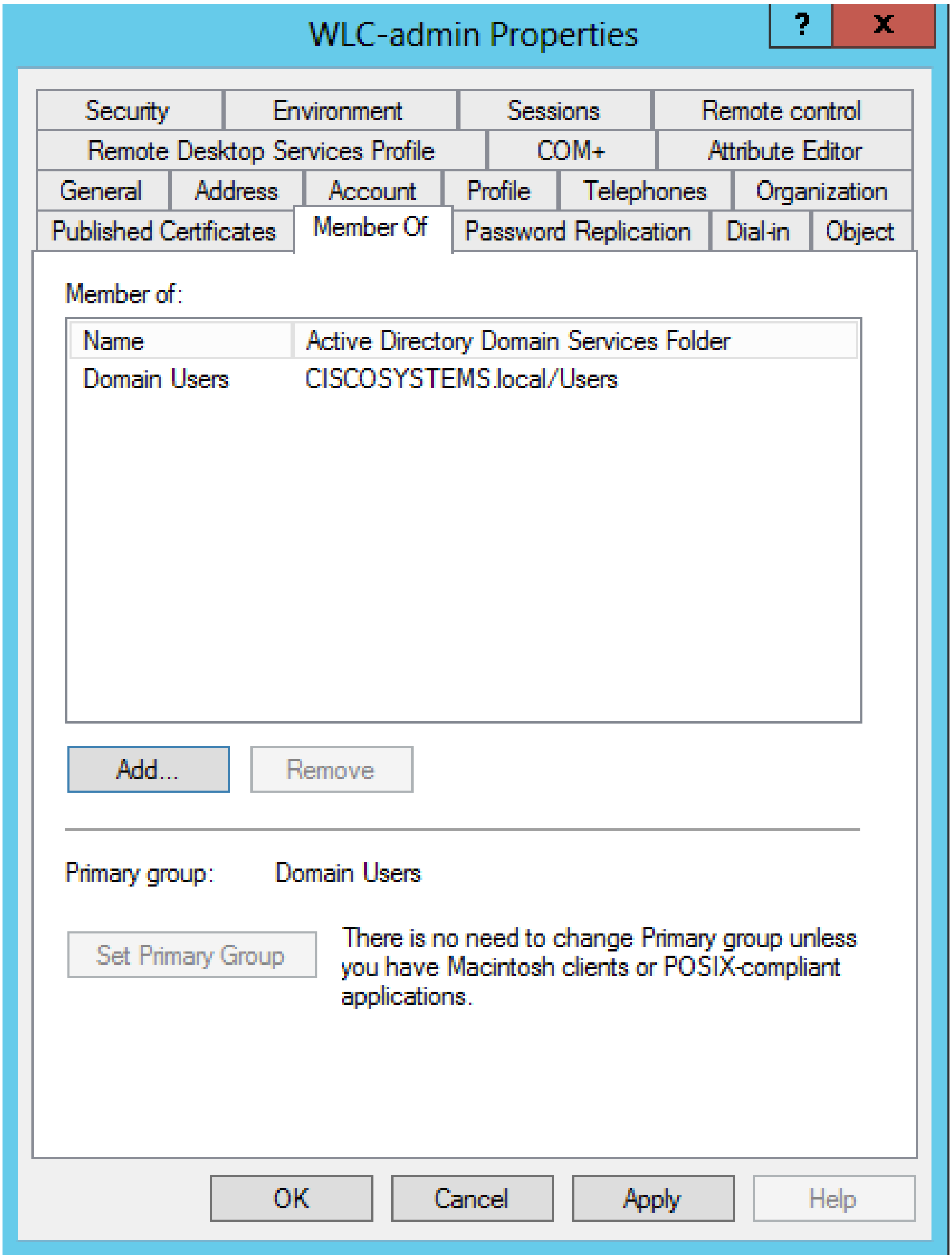
3. 導航到使用者**WLC-admin**，然後按一下右鍵該使用者。從上下文選單中選擇**屬性**，如下圖所示。此使用者使用名字WLC-admin進行標識。



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. 按一下「**Member Of**」索引標籤，如下圖所示：



Member of:

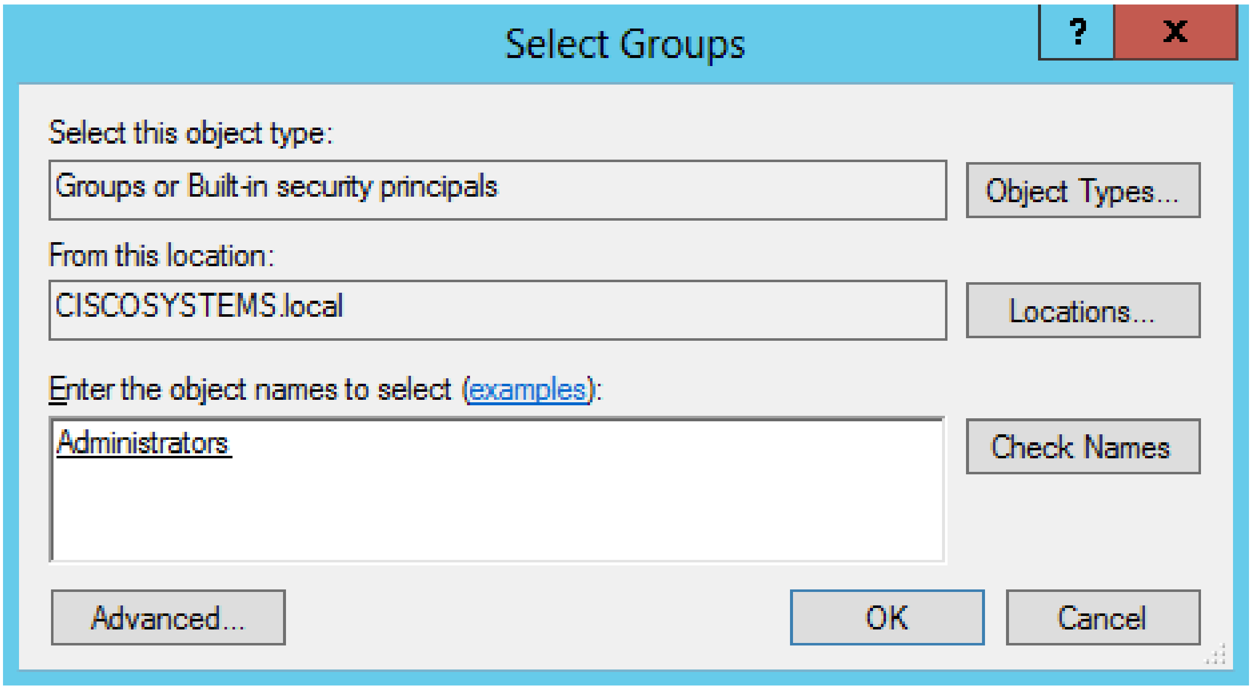
Name	Active Directory Domain Services Folder
Domain Users	CISCOSYSTEMS.local/Users

Primary group: Domain Users

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

::

5. 按一下「**Add**」。在開啟的對話方塊中，輸入**Administrators**，然後按一下**OK**，如下圖所示：

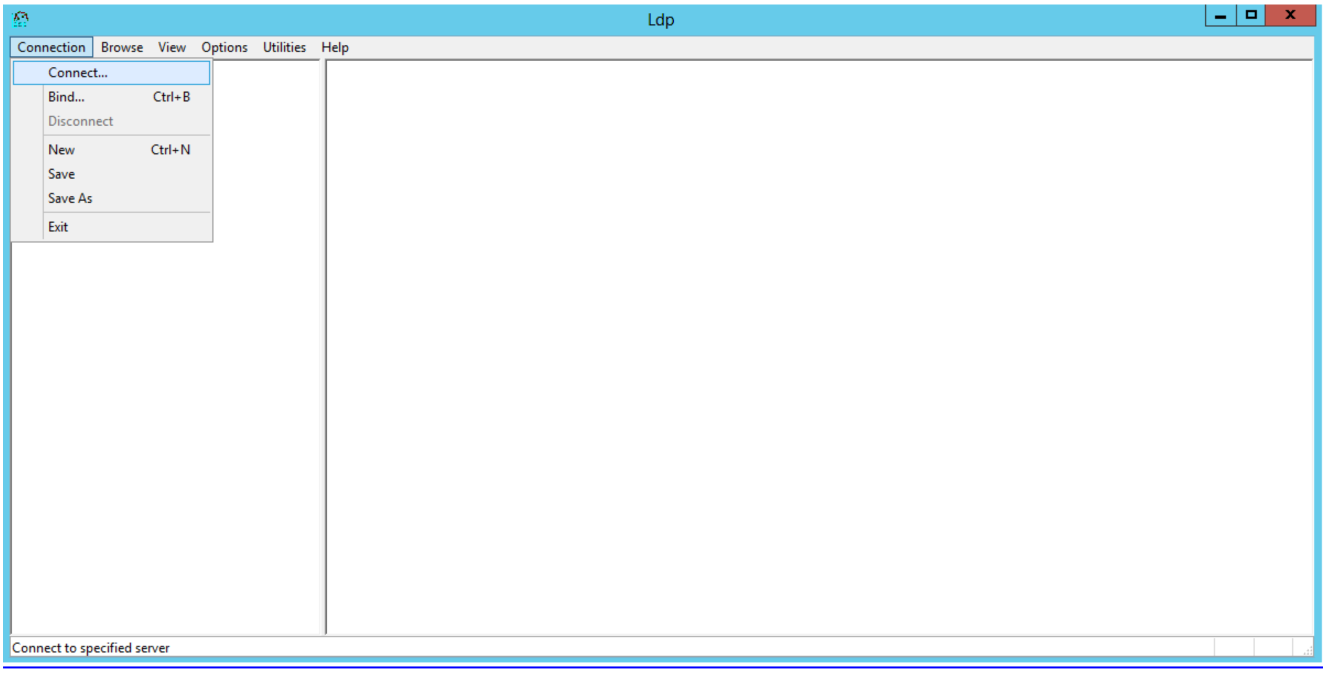


使用LDP標識使用者屬性

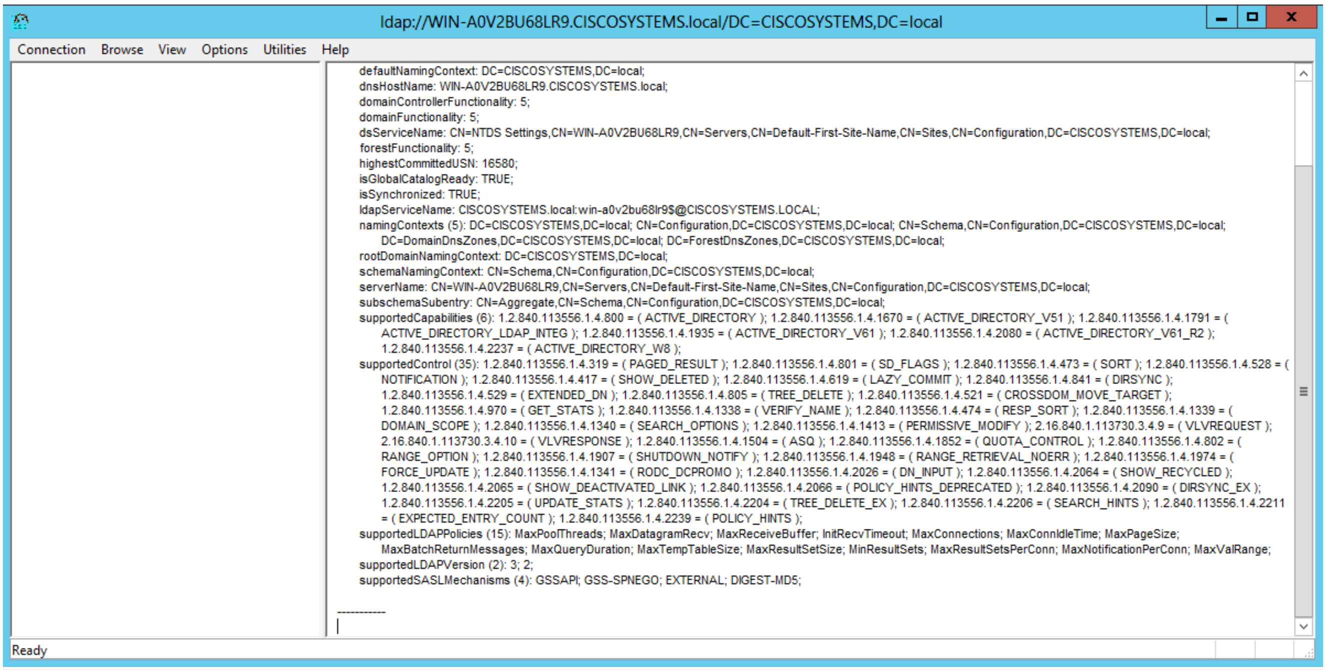
此GUI工具是一個LDAP客戶端，允許使用者針對任何與LDAP相容的目錄（如Active Directory）執行操作，如連線、繫結、搜尋、修改、新增或刪除。LDP用於檢視儲存在Active Directory中的對象及其後設資料，如安全描述符和複製後設資料。

從產品CD安裝Windows Server 2003支援工具時，會包括LDP GUI工具。本節介紹如何使用LDP實用程式標識與使用者User1關聯的特定屬性。其中有些屬性用於填寫WLC上的LDAP伺服器配置引數，例如「使用者屬性」型別和「使用者對象」型別。

1. 在Windows 2012伺服器上（即使在同一個LDAP伺服器上），開啟Windows PowerShell並輸入**LDP**以訪問LDP瀏覽器.
2. 在LDP主視窗中，當您輸入LDAP伺服器的IP地址時，導航到**Connection > Connect**並連線到LDAP伺服器，如下圖所示。



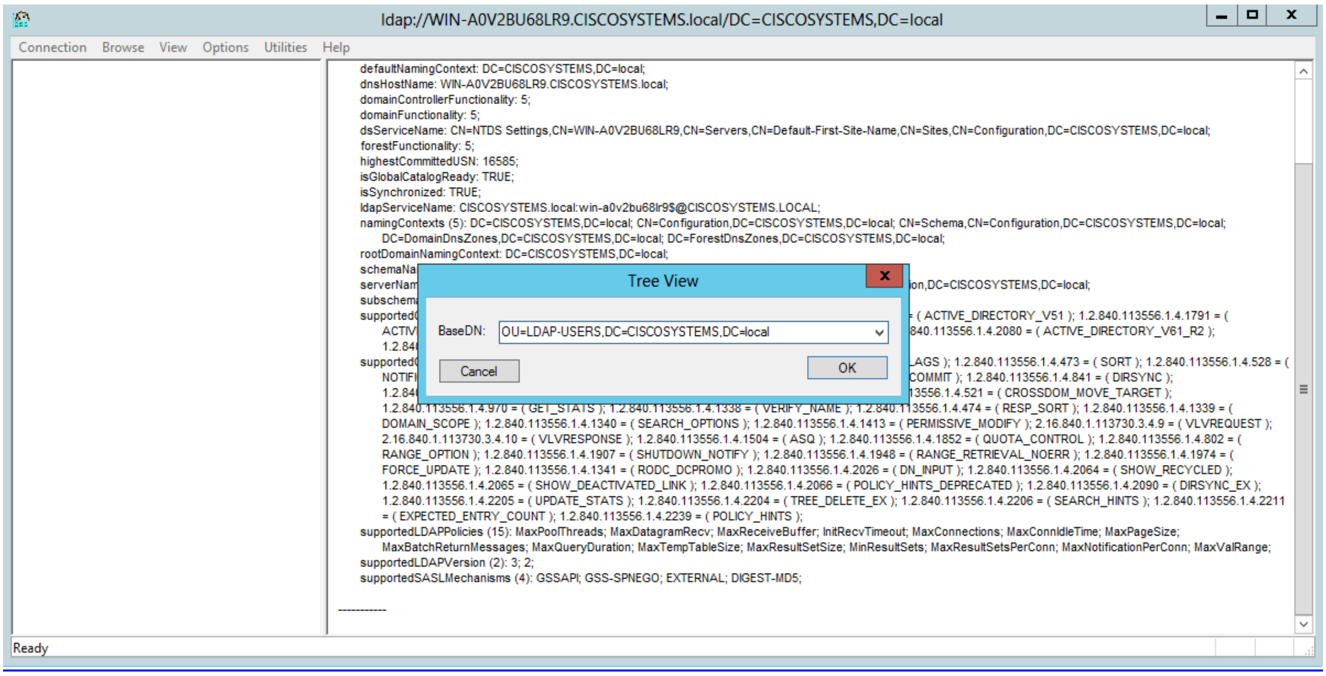
3. 連線到LDAP伺服器後，從主選單中選擇**View**，然後按一下**Tree**，如下圖所示：


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. 在生成的「樹檢視」視窗中，輸入使用者的**BaseDN**。在本示例中，User1位於域CISCOSYSTEMS.local下的OU "LDAP-USERS"下。按一下「**OK**」，如下圖所示：

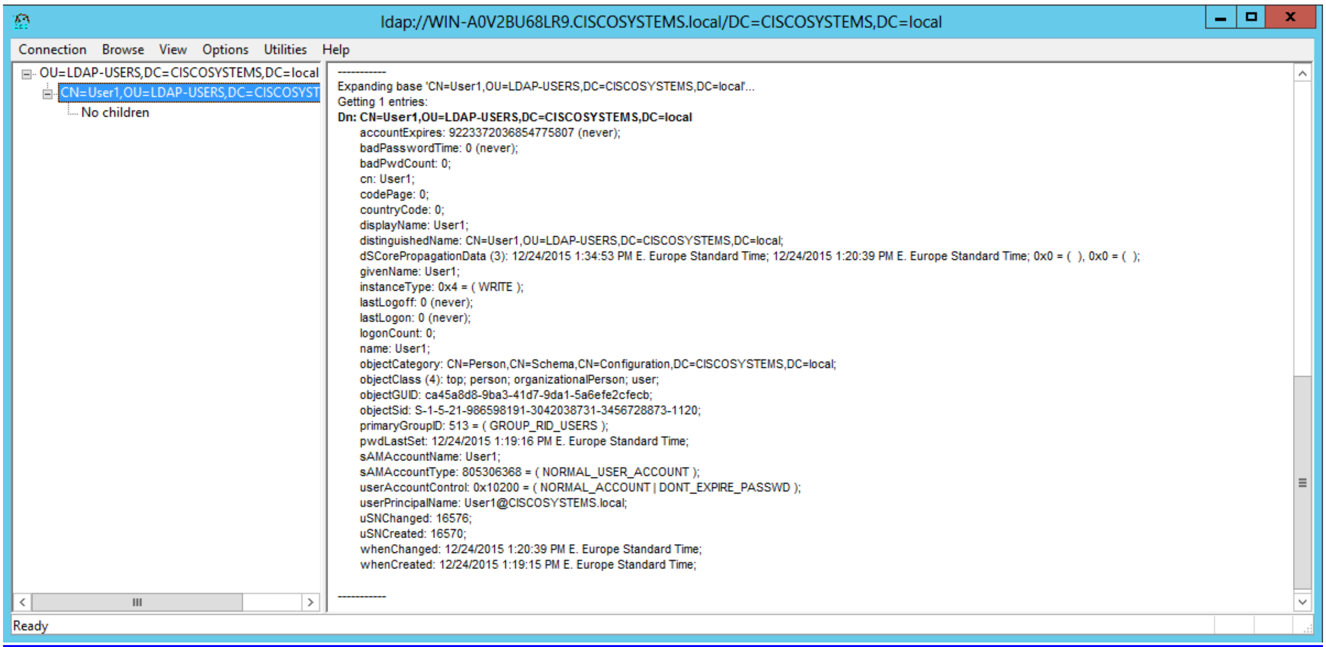

ldap://WIN-A0V2BU68LR9.CISCOSYSTEMS.local/DC=CISCOSYSTEMS,DC=local
Connection
Browse
View
Options
Utilities
Help
Tree View
Cancel
OK
Ready

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                                                        AGS ); 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. LDP瀏覽器的左側顯示出現在指定BaseDN(OU=LDAP-USERS， dc=CISCOSYSTEMS，dc=local)下的整個樹。展開樹以找到使用者User1。此使用者可以使用代表該使用者名稱字的CN值進行標識。在本例中，它是CN=User1。按兩下**CN=User1**。在LDP瀏覽器的右側窗格中，LDP顯示與User1關聯的所有屬性，如下圖所示：


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. 為LDAP伺服器配置WLC時，在*User Attribute*欄位中，在包含使用者名稱的使用者記錄中輸入屬性的名稱。從此LDP輸出中，您可以看到sAMAccountName是包含使用者名稱「User1」的一個屬性，因此請輸入與WLC上的「User Attribute」欄位對應的sAMAccountName屬性。

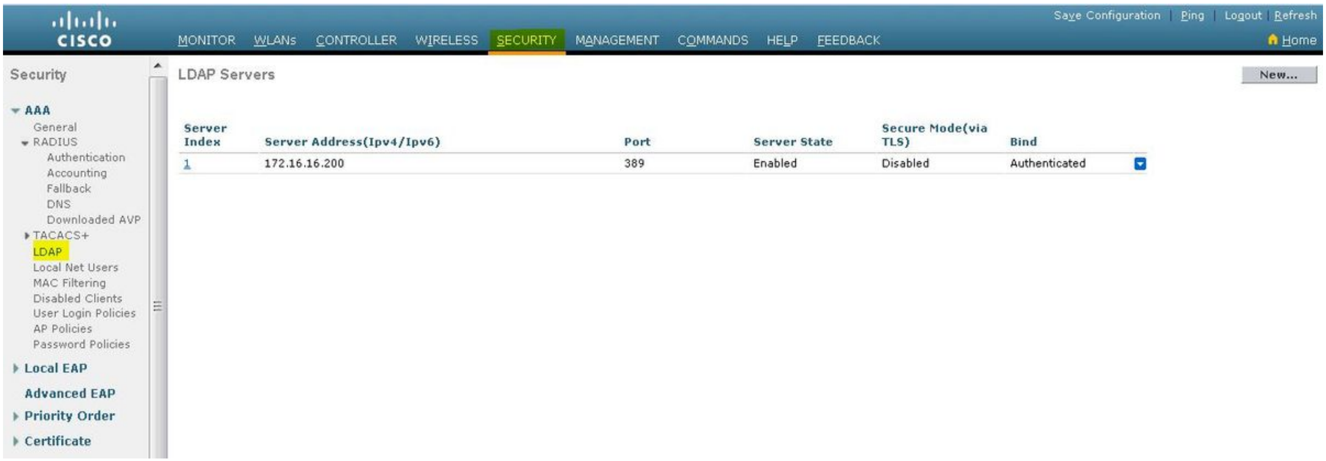
7. 為LDAP伺服器配置WLC時，在*User Object Type*欄位中輸入將記錄標識為使用者的LDAP objectType屬性的值。通常，使用者記錄有若干objectType屬性值，其中某些值對於使用者是唯一的，而某些值則與其他對象型別共用。在LDP輸出中，CN=Person是將記錄標識為使用者的值，因此請將**Person**指定為WLC上的「使用者對象型別」屬性。下一步是為LDAP伺服器配置WLC。

為LDAP伺服器配置WLC

現在已配置LDAP伺服器，下一步是使用LDAP伺服器的詳細資訊配置WLC。在WLC GUI上完成以下步驟：

> **註**：本檔案假設WLC已設定為基本操作，且LAP已註冊到WLC。如果您是新使用者，希望設定WLC以對LAP執行基本操作，請參閱向無線LAN控制器(WLC)註冊輕量AP(LAP)。

1. 在WLC的Security頁面中，從左側任務窗格中選擇**AAA > LDAP**，以轉到LDAP伺服器配置頁面。



LDAP Servers

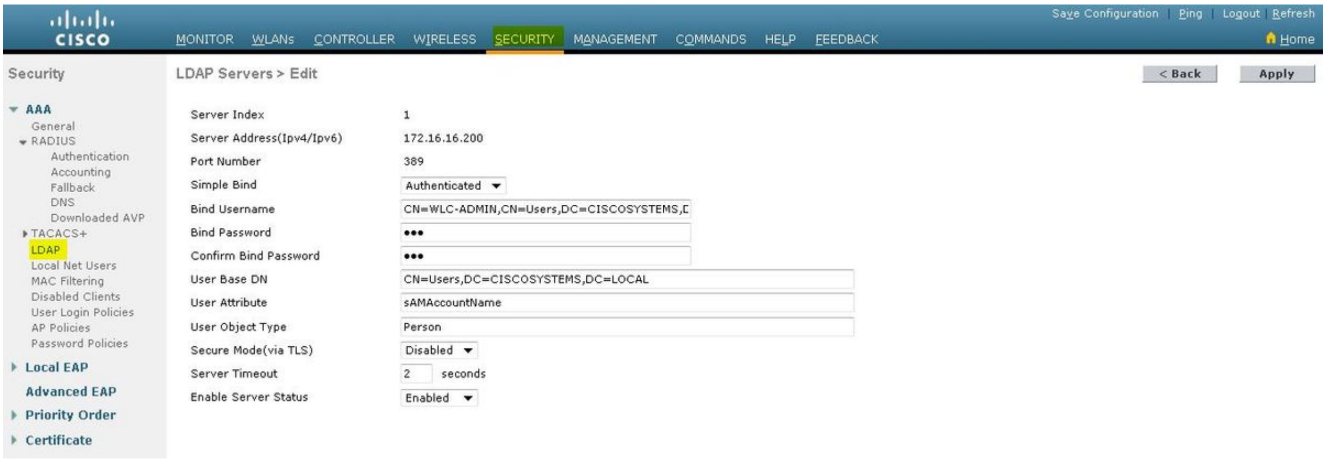
Server Index	Server Address(Ipv4/Ipv6)	Port	Server State	Secure Mode(via TLS)	Bind
1	172.16.16.200	389	Enabled	Disabled	Authenticated

要新增LDAP伺服器，請按一下**New**。系統將顯示LDAP Servers > New頁面。

2. 在「LDAP伺服器編輯」頁中，指定LDAP伺服器的詳細資訊，例如LDAP伺服器的IP地址、埠

號、啟用伺服器狀態等。從Server Index(Priority)下拉框中選擇一個數字，以指定此伺服器相對於任何其他已配置的LDAP伺服器的優先順序順序。最多可以配置17台伺服器。如果控制器無法連線到第一個伺服器，便會嘗試清單中的第二個伺服器，以此類推。在Server IP Address欄位中輸入LDAP伺服器的**IP地址**。在Port Number欄位中輸入LDAP伺服器的**TCP埠號**。有效範圍為1至65535，預設值為389。對於Simple繫結，我們使用Authenticated作為繫結使用者名稱，該使用者名稱是WLC管理員使用者用於訪問LDAP伺服器及其密碼的位置在User Base DN欄位中，輸入包含所有使用者清單的LDAP伺服器中子樹的**可分辨名稱(DN)**。例如，ou=組織單位、.ou=next organizational unit和o=corporation.com。如果包含使用者的樹是基本DN，請輸入o=corporation.com或dc=corporation， dc=com。在本示例中，使用者位於Organizational Unit(OU)LDAP-USERS下，而組織單元LDAP-USERS又作為lab.wireless域的一部分建立。使用者基礎DN必須指向使用者資訊（根據EAP-FAST身份驗證方法的使用者憑據）所在的完整路徑。在本示例中，使用者位於基本DN OU=LDAP-USERS，DC=CISCOSYSTEMS， DC=local下。在「使用者屬性」欄位中，輸入包含使用者名稱的使用者記錄中的屬性名稱。在User Object Type欄位中，輸入將記錄標識為使用者的LDAP objectType屬性值。通常，使用者記錄有若干objectType屬性值，其中某些值對於使用者是唯一的，而某些值則與其他對象型別共用您可以使用作為Windows 2012支援工具一部分的LDAP瀏覽器實用程式從目錄伺服器獲取這兩個欄位的值。此Microsoft LDAP瀏覽器工具稱為LDP。藉助此工具，您可以瞭解此特定使用者的「使用者基礎DN」、「使用者屬性」和「使用者對象型別」欄位。有關如何使用LDP瞭解這些使用者特定屬性的詳細資訊，請參閱本文檔的*使用LDP識別使用者屬性*部分。在Server Timeout欄位中，輸入重新傳輸之間的秒數。有效範圍為2到30秒，預設值為2秒。選中**Enable Server Status**覈取方塊以啟用此LDAP伺服器，或取消選中以禁用它。預設值已停用。按一下**Apply**提交更改。以下是已使用以下資訊設定的範例

：



LDAP Servers > Edit

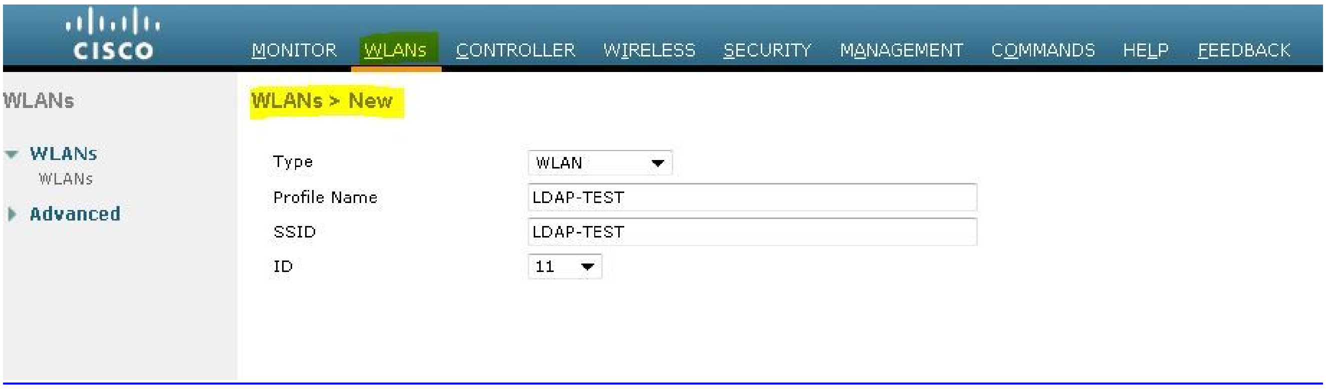
Server Index 1
Server Address(Ipv4/Ipv6) 172.16.16.200
Port Number 389
Simple Bind Authenticated
Bind Username CN=WLC-ADMIN,CN=Users,DC=CISCOSYSTEMS,D
Bind Password •••
Confirm Bind Password •••
User Base DN CN=Users,DC=CISCOSYSTEMS,DC=LOCAL
User Attribute sAMAccountName
User Object Type Person
Secure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

3. 現在已在WLC上配置有關LDAP伺服器的詳細資訊，下一步是配置用於Web身份驗證的WLAN。

為Web驗證設定WLAN

第一步是為使用者建立WLAN。請完成以下步驟：

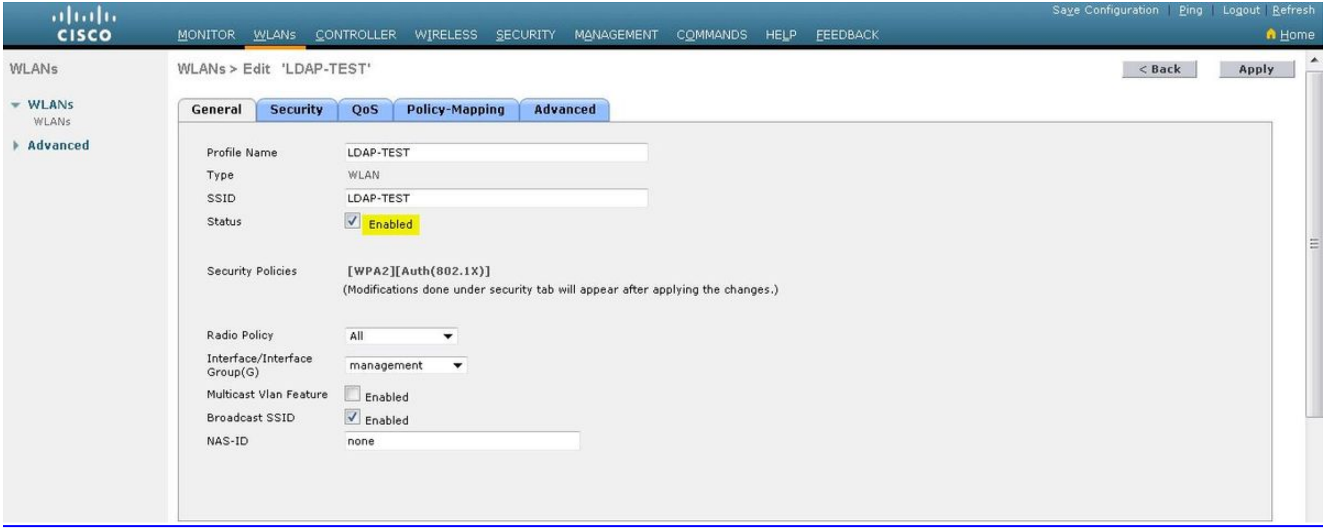
1. 在控制器GUI上按一下「**WLANs**」以建立WLAN。出現WLANs視窗。此視窗列出控制器上設定的WLAN。
2. 按一下**New**以設定新的WLAN。在本範例中，WLAN命名為Web-Auth。



WLANs > New

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

3. 按一下「**Apply**」。
4. 在WLAN > Edit視窗中，定義特定於WLAN的引數。



WLANs > Edit 'LDAP-TEST'

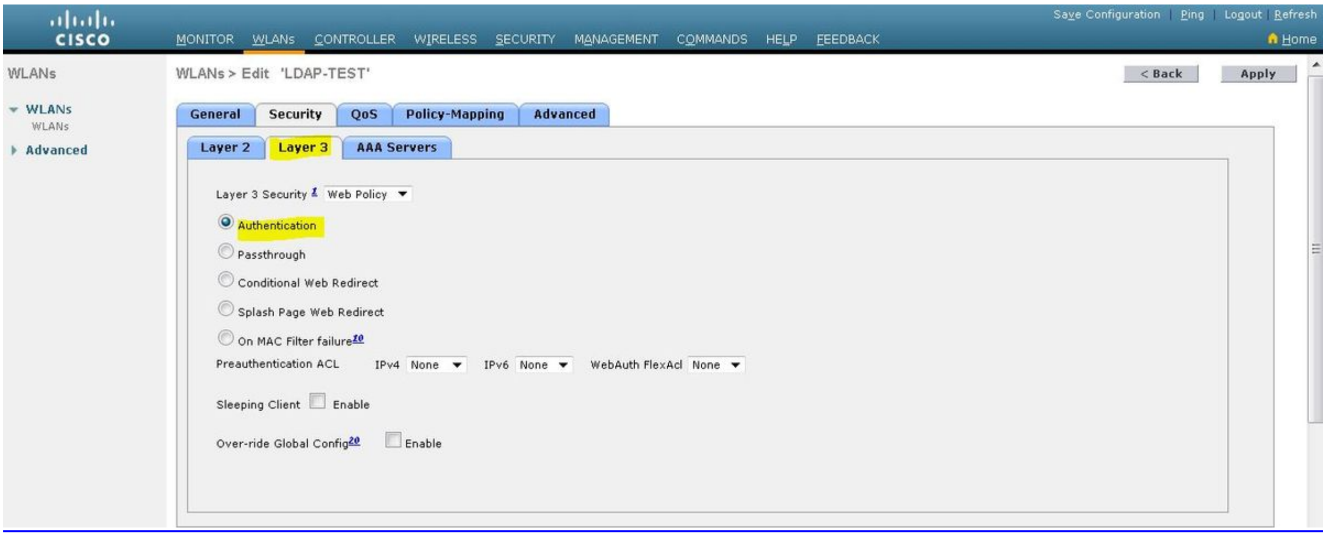
Profile Name: LDAP-TEST
Type: WLAN
SSID: LDAP-TEST
Status: ☑ Enabled

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

選中Status覈取方塊以啟用WLAN。對於WLAN，從Interface Name欄位中選擇適當的介面。此範例將對應連線到WLAN Web-Auth的管理介面。

5. 按一下**Security**頁籤。在第3層安全欄位中，選中**Web Policy**覈取方塊，然後選擇**Authentication**選項。



WLANs > Edit 'LDAP-TEST'

Layer 3 Security: Web Policy

● Authentication
○ Passthrough
○ Conditional Web Redirect
○ Splash Page Web Redirect
○ On MAC Filter failure

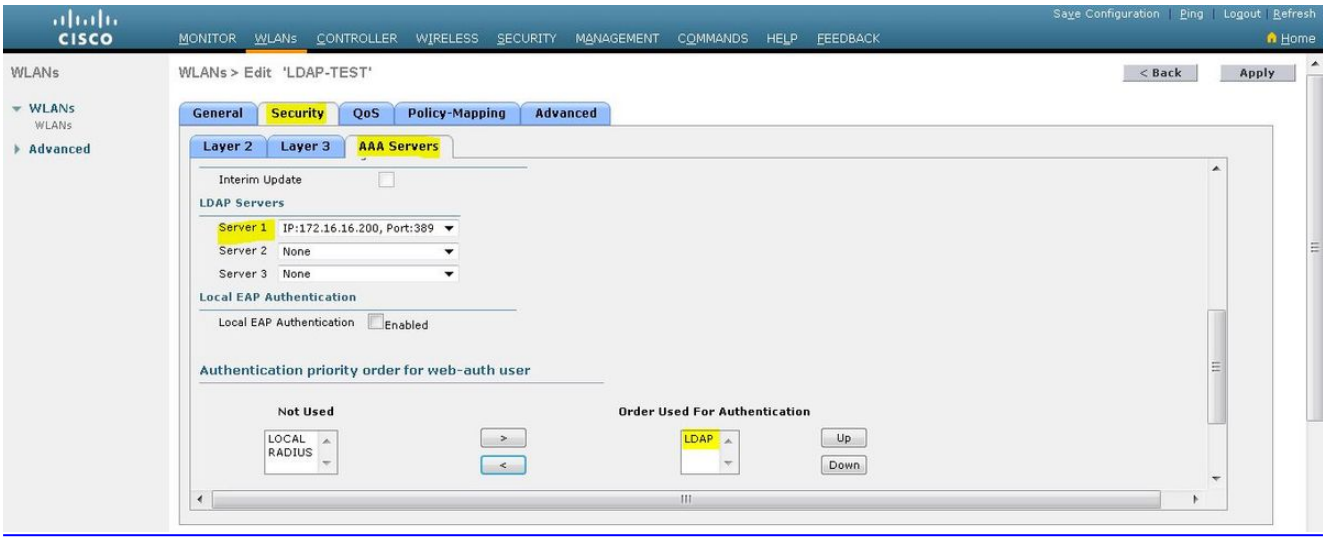
Preauthentication ACL: IPv4 None IPv6 None WebAuth FlexAcl None

Sleeping Client: □ Enable

Over-ride Global Config: □ Enable

之所以選擇此選項，是因為使用Web驗證來驗證無線客戶端。選中**Override Global Config**覈取方塊以根據WLAN Web身份驗證配置啟用。從Web Auth type下拉選單中選擇適當的Web驗證型別。此範例使用內部Web驗證。**註**:802.1x身份驗證不支援Web身份驗證。這表示使用Web驗證時，不能選擇802.1x或具有802.1x的WPA/WPA2作為第2層安全性。所有其他第2層安全引數都支援Web驗證。

6. 按一下**AAA Servers**頁籤。從LDAP伺服器下拉選單中選擇配置的LDAP伺服器。如果您使用本地資料庫或RADIUS伺服器，則可以在*Authentication priority order for web-auth userfield*下設定身份驗證優先順序。


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

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	Order Used For Authentication
LOCAL RADIUS	LDAP

7. 按一下「**Apply**」。**注意**：在此示例中，未使用驗證使用者身份的第2層安全方法，因此在第2層安全欄位中選擇**None。**

驗證

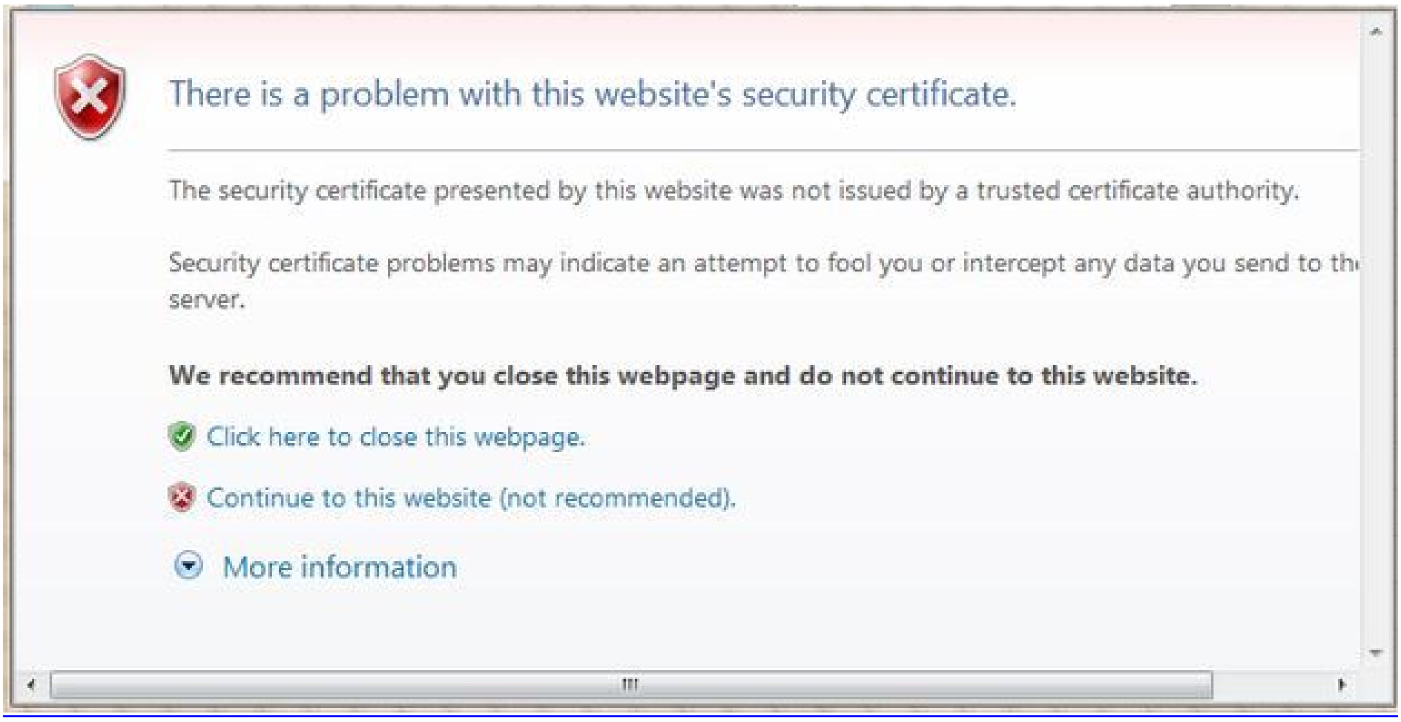
使用本節內容，確認您的組態是否正常運作。

若要驗證此設定，請連線無線客戶端並檢查配置是否按預期工作。

無線客戶端開啟，使用者在Web瀏覽器中輸入URL，例如www.yahoo.com。由於使用者尚未通過驗證，因此WLC會將使用者重新導向到內部Web登入URL。

系統將提示使用者輸入使用者憑證。使用者提交使用者名稱和密碼後，登入頁面取得使用者憑證輸入，並在提交時將要求傳回WLC Web伺服器的action_URL範例http://1.1.1.1/login.html。提供此項目是要作為客戶重新導向 URL 的輸入參數，其中 1.1.1.1 是交換器上的虛擬介面位址。

WLC根據LDAP使用者資料庫對使用者進行身份驗證。驗證成功後，WLC Web伺服器會將使用者轉送到已設定的重新導向URL或使用者端啟動的URL，例如 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

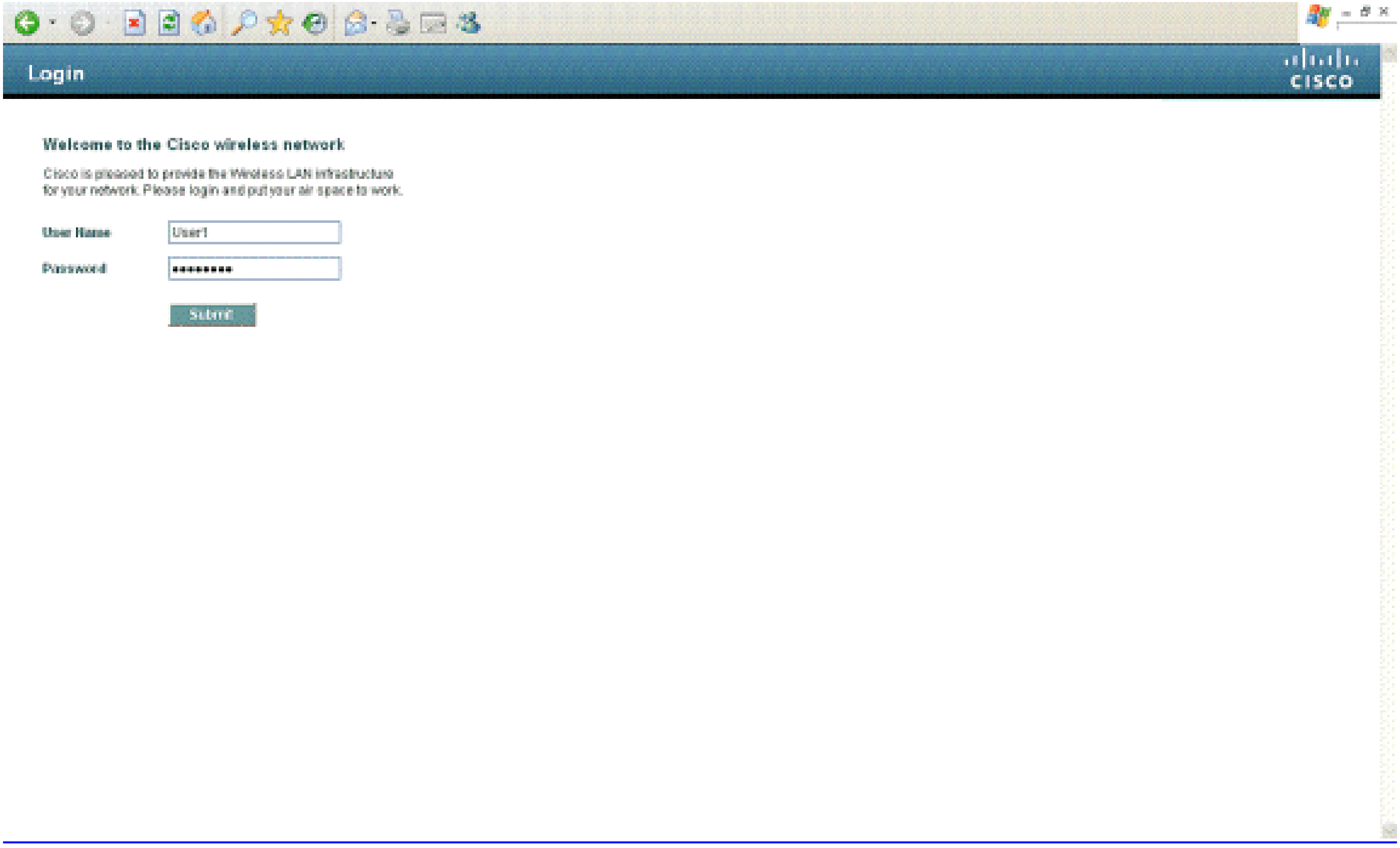
server.

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



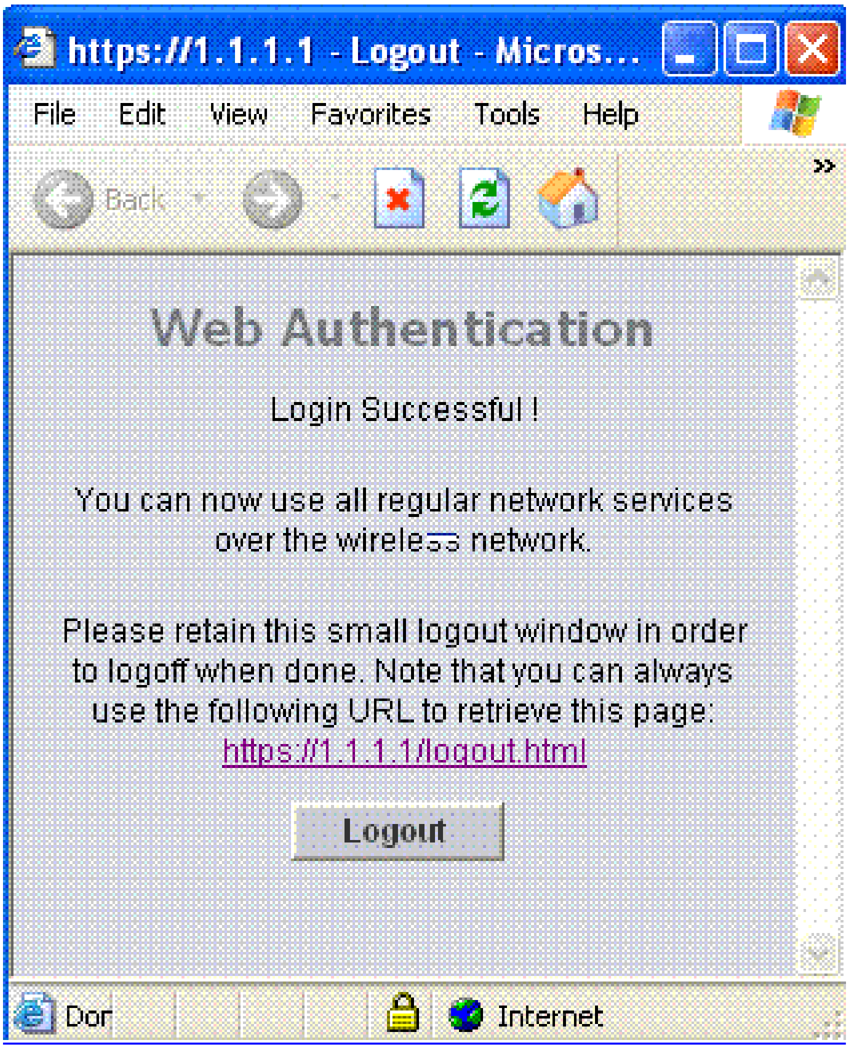
Login

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

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

使用以下命令對組態進行疑難排解：

- **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**

以下是**debug mac addr cc:fa:00:f7:32:35**命令的輸出示例

debug aaa ldap enable

```
(Cisco_Controller) >*pemReceiveTask: Dec 24 03:45:23.089: cc:fa:00:f7:32:35 Sent an XID frame
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Processing assoc-req
station:cc:fa:00:f7:32:35 AP:00:23:eb:e5:04:10-01 thread:18ec9330
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Association received from mobile on
BSSID 00:23:eb:e5:04:1f AP AP1142-1
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Global 200 Clients are allowed to AP
radio

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

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

*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 override for default ap group, marking
intgrp NULL
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Interface policy on Mobile,
role Local. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 16

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

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Changing
IPv4 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2699)
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Changing
IPv6 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2720)
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfApplyWlanPolicy: Apply WLAN Policy
over PMIPv6 Client Mobility Type, Tunnel User - 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6246 setting Central
switched to TRUE
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6249 apVapId = 1 and
Split Acl Id = 65535
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying site-specific Local Bridging
override for station cc:fa:00:f7:32:35 - vapId 1, site 'default-group', interface 'management'
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Local Bridging Interface
Policy for station cc:fa:00:f7:32:35 - vlan 16, interface id 0, interface 'management'
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE  statusCode is 0 and
status is 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE  ssid_done_flag is 0
finish_flag is 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 STA - rates (3): 24 164 48 0 0 0 0 0 0
0 0 0 0 0 0 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 suppRates  statusCode is 0 and
```

```
gotSuppRatesElement is 1
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 AID 2 in Assoc Req from flex AP
00:23:eb:e5:04:10 is same as in mscb cc:fa:00:f7:32:35
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfMs1xStateDec
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Change
state to START (0) last state WEBAUTH_REQD (8)

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 pemApfAddMobileStation2:
APF_MS_PEM_WAIT_L2_AUTH_COMPLETE = 0.
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Initializing
policy
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Change state to
AUTHCHECK (2) last state START (0)

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

*pemReceiveTask: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 Removed NPU entry.
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Not Using WMM Compliance code qosCap 00
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4)
Plumbed mobile LWAPP rule on AP 00:23:eb:e5:04:10 vapId 1 apVapId 1 flex-acl-name:
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4) Change
state to WEBAUTH_REQD (8) last state L2AUTHCOMPLETE (4)

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
pemApfAddMobileStation2 3802, Adding TMP rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Adding
Fast Path rule
 type = Airespace AP Client - ACL passthru
 on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0
 IPv4 ACL I
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, IntfId = 0  Local Bridging Vlan =
16, Local Bridging intf id = 0
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
pemApfAddMobileStation2 3911, Adding TMP rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
Replacing Fast Path rule
 type = Airespace AP Client - ACL passthru
 on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0
 IPv4 AC
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, IntfId = 0  Local Bridging Vlan =
16, Local Bridging intf id = 0
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2 (apf_policy.c:359)
Changing state for mobile cc:fa:00:f7:32:35 on AP 00:23:eb:e5:04:10 from Associated to
Associated

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2:session timeout
forstation cc:fa:00:f7:32:35 - Session Tout 1800, apfMsTimeOut '1800' and sessionTimerRunning
flag is  1
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Scheduling deletion of Mobile Station:
(callerId: 49) in 1800 seconds
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Func: apfPemAddUser2, Ms Timeout =
1800, Session Timeout = 1800

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Sending assoc-resp with status 0
station:cc:fa:00:f7:32:35 AP:00:23:eb:e5:04:10-01 on apVapId 1
*apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sending Assoc Response to station on
BSSID 00:23:eb:e5:04:1f (status 0) ApVapId 1 Slot 1
*apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 apfProcessAssocReq (apf_80211.c:10187)
Changing state for mobile cc:fa:00:f7:32:35 on AP 00:23:eb:e5:04:10 from Associated to
Associated

*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2,
dtlFlags 0x0
*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sent an XID frame
*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2,
dtlFlags 0x0
*pemReceiveTask: Dec 24 03:45:43.558: cc:fa:00:f7:32:35 Sent an XID frame
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len
322,vlan 16, port 1, encap 0xec03, xid 0x62743488)
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype
0ff:ff:ff:ff:ff:ff
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block
settings:
                       dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0,
                       dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25
mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25
(local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1)
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block
settings:
                       dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0,
                       dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block
settings:
                       dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                       dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25
mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25
(local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1)
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP transmitting DHCP DISCOVER (1)
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   op: BOOTREQUEST, htype:
Ethernet, hlen: 6, hops: 1
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792),
secs: 0, flags: 0
```

```
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   chaddr: cc:fa:00:f7:32:35
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   ciaddr: 0.0.0.0,  yiaddr:
0.0.0.0
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   siaddr: 0.0.0.0,  giaddr:
172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block
settings:
                       dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                       dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE
*DHCP Proxy Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP received op BOOTREPLY (2) (len
572,vlan 0, port 0, encap 0x0, xid 0x62743488)
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418,
port 1, vlan 16)
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP transmitting DHCP OFFER (2)
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   op: BOOTREPLY, htype: Ethernet,
hlen: 6, hops: 0
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792),
secs: 0, flags: 0
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   chaddr: cc:fa:00:f7:32:35
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   ciaddr: 0.0.0.0,  yiaddr:
172.16.16.122
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   siaddr: 0.0.0.0,  giaddr:
0.0.0.0
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   server id: 1.1.1.1  rcvd server
id: 172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len
334,vlan 16, port 1, encap 0xec03, xid 0x62743488)
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype
0ff:ff:ff:ff:ff:ff
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block
settings:
                       dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                       dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25
mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25
(local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1)
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP transmitting DHCP REQUEST (3)
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP   op: BOOTREQUEST, htype:
Ethernet, hlen: 6, hops: 1
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792),
secs: 0, flags: 0
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP   chaddr: cc:fa:00:f7:32:35
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   ciaddr: 0.0.0.0,  yiaddr:
0.0.0.0
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   siaddr: 0.0.0.0,  giaddr:
172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   requested ip: 172.16.16.122
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   server id: 172.16.16.25  rcvd
server id: 1.1.1.1
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block
settings:
                       dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                       dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP received op BOOTREPLY (2) (len
572,vlan 0, port 0, encap 0x0, xid 0x62743488)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP setting server from ACK
(mscb=0x40e64b88 ip=0xac10107a)(server 172.16.16.25, yiaddr 172.16.16.122)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418,
port 1, vlan 16)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP transmitting DHCP ACK (5)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   op: BOOTREPLY, htype: Ethernet,
hlen: 6, hops: 0
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792),
secs: 0, flags: 0
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   chaddr: cc:fa:00:f7:32:35
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   ciaddr: 0.0.0.0,  yiaddr:
172.16.16.122
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   siaddr: 0.0.0.0,  giaddr:
0.0.0.0
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   server id: 1.1.1.1  rcvd server
id: 172.16.16.25
*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created for
mobile, length = 7
*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created in mscb
for mobile, length = 7
*aaaQueueReader: Dec 24 03:46:01.222: AuthenticationRequest: 0x2b6bdc3c


*aaaQueueReader: Dec 24 03:46:01.222:   Callback.....................................0x12088c50

*aaaQueueReader: Dec 24 03:46:01.222:   protocolType.................................0x00000002

*aaaQueueReader: Dec 24 03:46:01.222:
proxyState..................................CC:FA:00:F7:32:35-00:00

*aaaQueueReader: Dec 24 03:46:01.222:   Packet contains 15 AVPs (not shown)

*LDAP DB Task 1: Dec 24 03:46:01.222: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE'
(1)
*LDAP DB Task 1: Dec 24 03:46:01.222: LDAP server 1 changed state to INIT
*LDAP DB Task 1: Dec 24 03:46:01.223: LDAP_OPT_REFERRALS = -1

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

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

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

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

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

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate = 0,
BurstRate = 0

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate = 0,
BurstRate = 0

*ewmwebWebauth1: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 1,
dtlFlags 0x0


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

--More or (q)uit current module or <ctrl-z> to abort
Session Timeout.................................. 1800
Client CCX version............................... No CCX support
QoS Level........................................ Silver
Avg data Rate.................................... 0
Burst data Rate.................................. 0
Avg Real time data Rate.......................... 0
```

```
Burst Real Time data Rate........................ 0
802.1P Priority Tag.............................. disabled
CTS Security Group Tag........................... Not Applicable
KTS CAC Capability............................... No
Qos Map Capability............................... No
WMM Support...................................... Enabled
 APSD ACs.......................................  BK  BE  VI  VO
Current Rate..................................... m7
Supported Rates.................................. 12.0,18.0,24.0
Mobility State................................... Local
Mobility Move Count.............................. 0
Security Policy Completed........................ Yes
Policy Manager State............................. RUN
Audit Session ID................................. ac10101900000005567b69f8
AAA Role Type.................................... none
Local Policy Applied............................. none
IPv4 ACL Name.................................... none

--More or (q)uit current module or <ctrl-z> to abort
FlexConnect ACL Applied Status................... Unavailable
IPv4 ACL Applied Status.......................... Unavailable
IPv6 ACL Name.................................... none
IPv6 ACL Applied Status.......................... Unavailable
Layer2 ACL Name.................................. none
Layer2 ACL Applied Status........................ Unavailable
Client Type...................................... SimpleIP
mDNS Status...................................... Enabled
mDNS Profile Name................................ default-mdns-profile
No. of mDNS Services Advertised.................. 0
Policy Type...................................... N/A
Encryption Cipher................................ None
Protected Management Frame ...................... No
Management Frame Protection...................... No
EAP Type......................................... Unknown
FlexConnect Data Switching....................... Central
FlexConnect Dhcp Status.......................... Central
FlexConnect Vlan Based Central Switching......... No
FlexConnect Authentication....................... Central
FlexConnect Central Association.................. No
Interface........................................ management
VLAN............................................. 16
Quarantine VLAN.................................. 0

--More or (q)uit current module or <ctrl-z> to abort
Access VLAN...................................... 16
Local Bridging VLAN.............................. 16
Client Capabilities:
     CF Pollable................................ Not implemented
     CF Poll Request............................ Not implemented
     Short Preamble............................. Not implemented
     PBCC....................................... Not implemented
     Channel Agility............................ Not implemented
     Listen Interval............................ 10
     Fast BSS Transition........................ Not implemented
     11v BSS Transition......................... Not implemented
Client Wifi Direct Capabilities:
     WFD capable................................ No
     Manged WFD capable......................... No
     Cross Connection Capable................... No
     Support Concurrent Operation............... No
Fast BSS Transition Details:
Client Statistics:
     Number of Bytes Received................... 16853
     Number of Bytes Sent....................... 31839
     Total Number of Bytes Sent................ 31839
     Total Number of Bytes Recv................ 16853
     Number of Bytes Sent (last 90s)........... 31839

--More or (q)uit current module or <ctrl-z> to abort
     Number of Bytes Recv (last 90s)........... 16853
     Number of Packets Received................ 146
     Number of Packets Sent.................... 92
     Number of Interim-Update Sent............. 0
     Number of EAP Id Request Msg Timeouts...... 0
     Number of EAP Id Request Msg Failures...... 0
     Number of EAP Request Msg Timeouts......... 0
     Number of EAP Request Msg Failures......... 0
     Number of EAP Key Msg Timeouts............. 0
     Number of EAP Key Msg Failures............. 0
     Number of Data Retries.................... 2
     Number of RTS Retries..................... 0
     Number of Duplicate Received Packets....... 0
     Number of Decrypt Failed Packets........... 0
     Number of Mic 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
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。