

# Ejemplo de Configuración de Autenticación Web Usando LDAP en Controladores LAN Inalámbricos (WLCs)

## Contenido

---

### Table Of Contents

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Convenciones](#)

[Proceso de Autenticación Web](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración del servidor LDAP](#)

[Crear usuarios en el controlador de dominio](#)

[Crear una base de datos de usuarios en una unidad organizativa](#)

[Configuración del usuario para el acceso LDAP](#)

[Enlace anónimo](#)

[Habilitar la característica de enlace anónimo en Windows 2012 Essentials Server](#)

[Concesión de acceso de INICIO DE SESIÓN ANÓNIMO al usuario](#)

[Conceder permiso de contenido de lista en la unidad organizativa](#)

[Enlace autenticado](#)

[Concesión de privilegios de administrador a WLC-admin](#)

[Uso de LDP para Identificar los Atributos de Usuario](#)

[Configuración de WLC para servidor LDAP](#)

[Configuración de la WLAN para la autenticación Web](#)

[Verificación](#)

[Troubleshoot](#)

## Introducción

Este documento describe cómo configurar un Wireless LAN Controller (WLC) para la autenticación Web. Explica cómo configurar un servidor LDAP (Protocolo ligero de acceso a directorios) como base de datos back-end para la autenticación Web con el fin de recuperar credenciales de usuario y autenticar al usuario.

# Prerequisites

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de la configuración de Lightweight Access Points (LAP) y Cisco WLC
- Conocimiento del control y el aprovisionamiento del protocolo de punto de acceso inalámbrico (CAPWAP)
- Conocimientos sobre cómo configurar y configurar el protocolo ligero de acceso a directorios (LDAP), Active Directory y controladores de dominio

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 5508 WLC que ejecuta la versión 8.2.100.0 del firmware
- LAP de la serie 1142 de Cisco
- Adaptador de cliente inalámbrico 802.11a/b/g de Cisco.
- Servidor Essentials de Microsoft Windows 2012 que desempeña la función de servidor LDAP

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

## Antecedentes

### Convenciones


Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

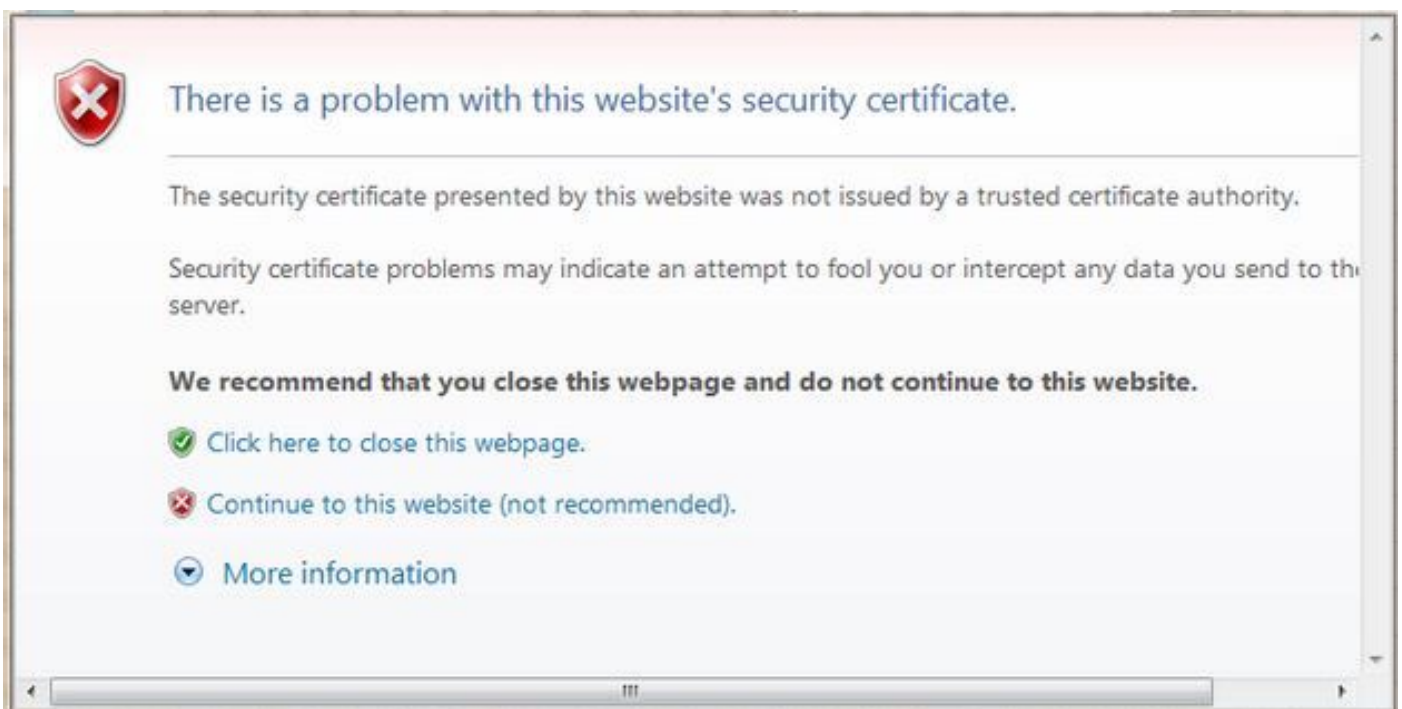
## Proceso de Autenticación Web

La autenticación Web es una función de seguridad de Capa 3 que hace que el controlador no permita el tráfico IP (excepto los paquetes relacionados con DHCP y DNS) de un cliente determinado hasta que ese cliente haya proporcionado correctamente un nombre de usuario y una contraseña válidos. Cuando utiliza la autenticación Web para autenticar clientes, debe definir un nombre de usuario y una contraseña para cada cliente. A continuación, cuando los clientes

intenten conectarse a la LAN inalámbrica, deben introducir el nombre de usuario y la contraseña cuando se les solicite en una página de inicio de sesión.

Cuando la autenticación web está activada (en Seguridad de capa 3), los usuarios reciben ocasionalmente una alerta de seguridad del navegador web la primera vez que intentan acceder a una URL.

 Sugerencia: para eliminar esta advertencia de certificado, vuelva a la siguiente guía sobre cómo instalar un certificado de confianza de terceros  
<http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-certificates-wlc-00.html>



Después de hacer clic en Sí para continuar (o más precisamente Continuar a este sitio web (no recomendado) para el navegador Firefox, por ejemplo), o si el navegador del cliente no muestra una alerta de seguridad, el sistema de autenticación web redirige al cliente a una página de inicio de sesión, como se muestra en la imagen:

# Login

## Welcome to the Cisco wireless network

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

User Name

Password

Submit

La página de inicio de sesión predeterminada contiene un logotipo de Cisco y un texto específico de Cisco. Puede optar por que el sistema de autenticación Web muestre uno de estos elementos:

- La página de inicio de sesión predeterminada
- Una versión modificada de la página de inicio de sesión predeterminada
- Una página de inicio de sesión personalizada que se configura en un servidor Web externo
- Una página de inicio de sesión personalizada que se descarga en el controlador

Cuando ingresa un nombre de usuario y una contraseña válidos en la página de login de autenticación web y hace clic en Enviar, se le autentica según las credenciales enviadas y una autenticación exitosa de la base de datos backend (LDAP en este caso). A continuación, el sistema de autenticación web muestra una página de inicio de sesión correcta y redirige el cliente autenticado a la URL solicitada.

# Web Authentication

Login Successful !

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

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

<https://1.1.1.1/logout.html>

**Logout**


La página de inicio de sesión correcta predeterminada contiene un puntero a una dirección URL de gateway virtual: <https://1.1.1.1/logout.html>. La dirección IP que configure para la interfaz virtual del controlador sirve como dirección de redirección para la página de inicio de sesión.

Este documento explica cómo utilizar la página Web interna en el WLC para la autenticación Web. En este ejemplo se utiliza un servidor LDAP como base de datos backend para la autenticación Web con el fin de recuperar las credenciales de usuario y autenticar al usuario.

## Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

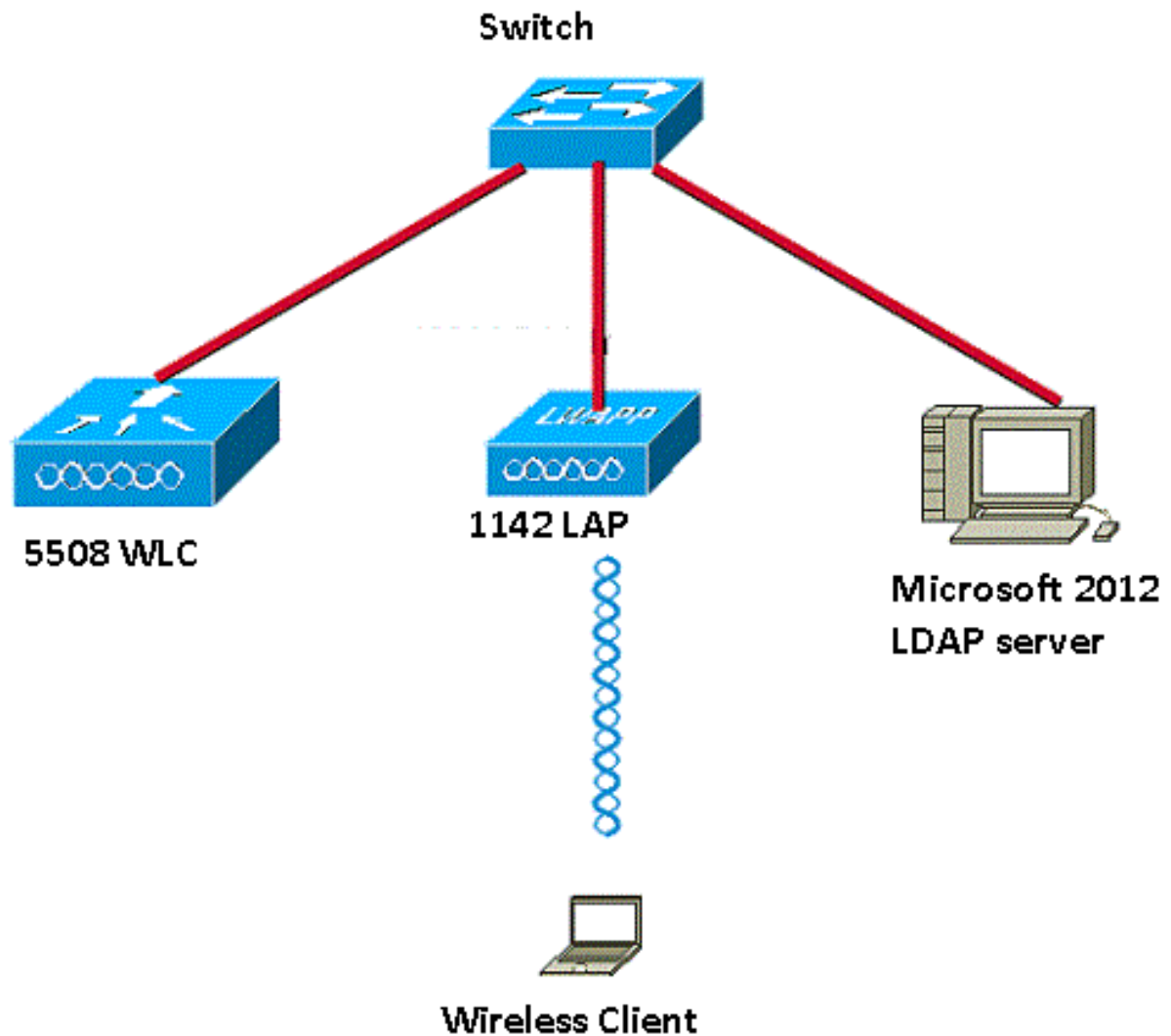
---

 Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

---

## Diagrama de la red

En este documento, se utiliza esta configuración de red:



## Configuraciones

Complete estos pasos para implementar con éxito esta configuración:

- [Configure el servidor LDAP.](#)
- [Configure el WLC para el servidor LDAP.](#)
- [Configure la WLAN para la autenticación Web.](#)

## Configuración del servidor LDAP

El primer paso es configurar el servidor LDAP, que sirve como base de datos backend para almacenar las credenciales de usuario de los clientes inalámbricos. En este ejemplo, el servidor Essentials de Microsoft Windows 2012 se utiliza como servidor LDAP.

El primer paso en la configuración del servidor LDAP es crear una base de datos de usuario en el servidor LDAP para que el WLC pueda consultar esta base de datos para autenticar al usuario.

Crear usuarios en el controlador de dominio

Una unidad organizativa (OU) contiene varios grupos que llevan referencias a entradas personales en un perfil de persona. Una persona puede ser miembro de varios grupos. Todas las definiciones de clase de objeto y atributo son valores predeterminados de esquema LDAP. Cada grupo contiene referencias (dn) para cada persona que le pertenece.

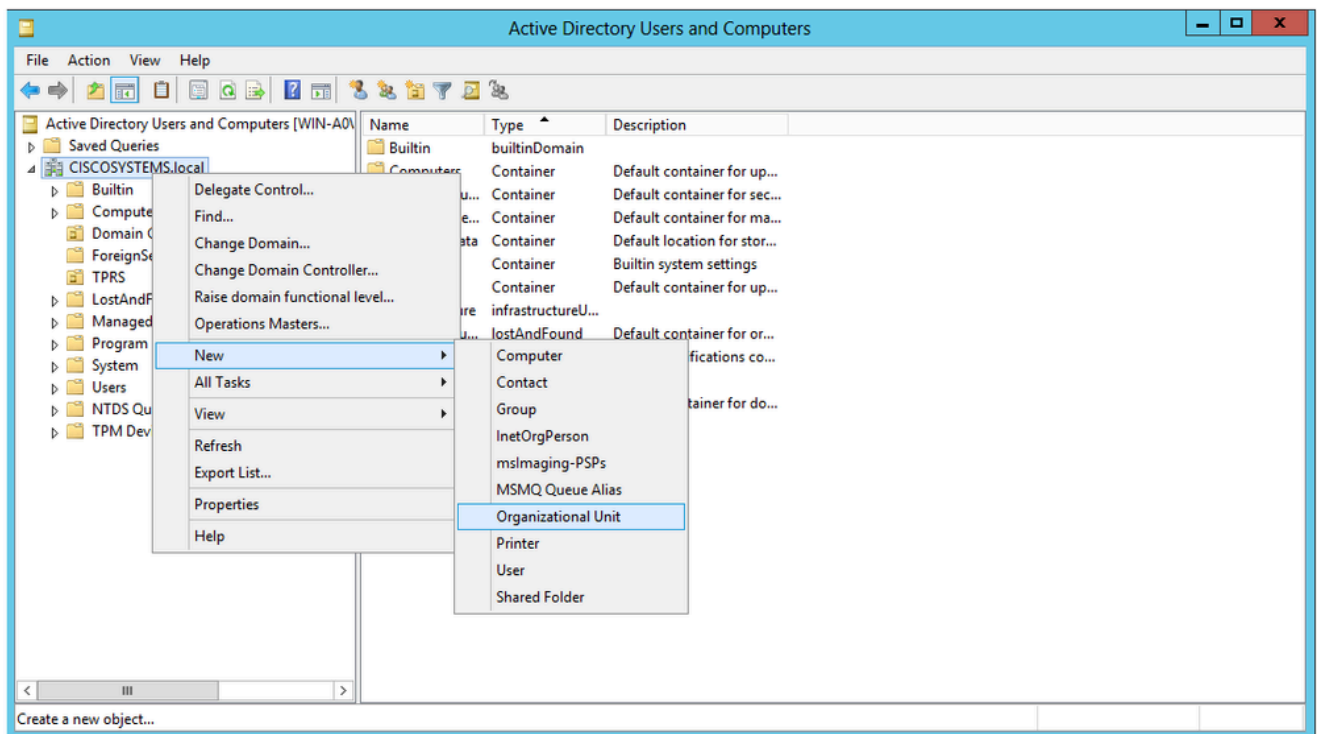
En este ejemplo, se crea un nuevo OU LDAP-USERS, y el usuario User1 se crea bajo este OU. Cuando configura este usuario para el acceso LDAP, el WLC puede consultar esta base de datos LDAP para la autenticación del usuario.

El dominio utilizado en este ejemplo es CISCOSYSTEMS.local.

Crear una base de datos de usuarios en una unidad organizativa

Esta sección explica cómo crear una nueva OU en su dominio y crear un nuevo usuario en esta OU.

1. Abra Windows PowerShell y escriba servermanager.exe
2. En la ventana Administrador del servidor, haga clic en AD DS. A continuación, haga clic con el botón secundario en el nombre del servidor para elegir Usuarios y equipos de Active Directory.
3. Haga clic con el botón derecho en su nombre de dominio, que es CISCOSYSTEMS.local en este ejemplo, y luego navegue hasta Nuevo > Unidad organizativa desde el menú contextual para crear una nueva OU.



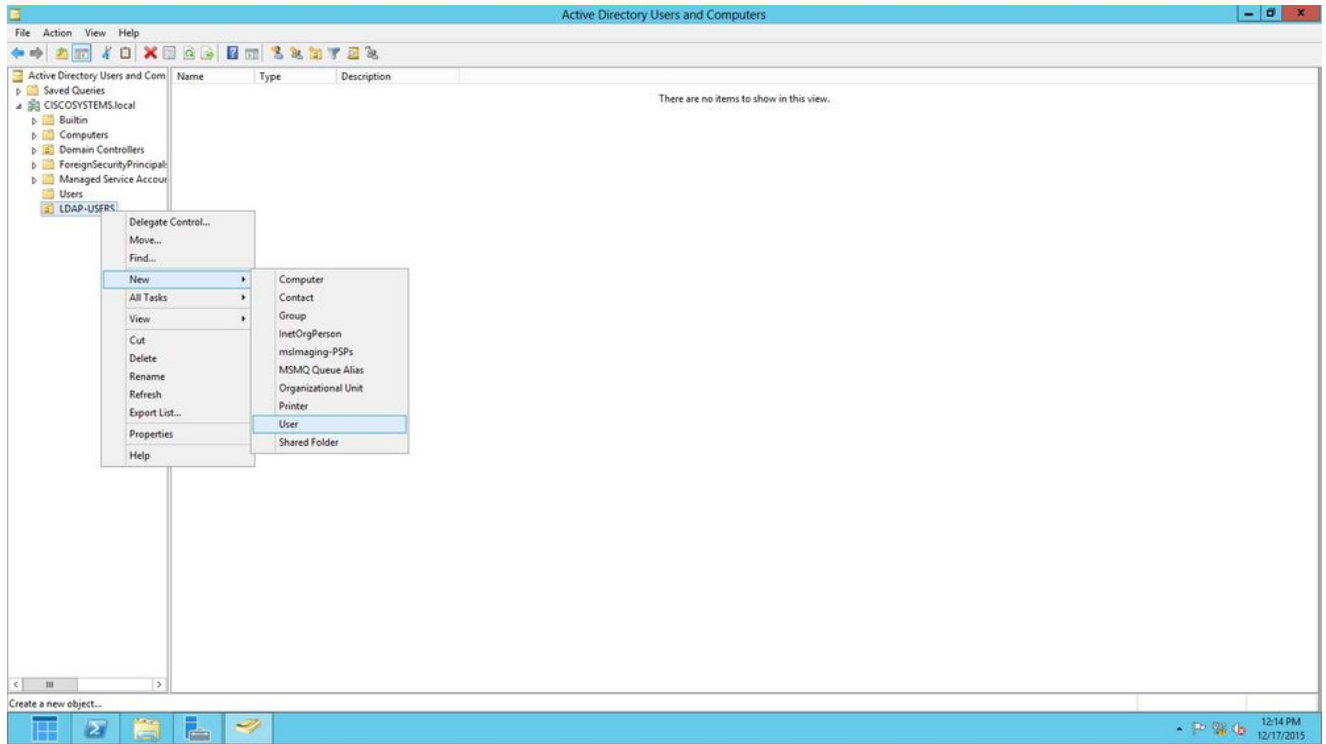
4. Asigne un nombre a esta unidad organizativa y haga clic en Aceptar, como se muestra en la imagen:



Ahora que se crea el nuevo OU LDAP-USERS en el servidor LDAP, el siguiente paso es crear el usuario User1 bajo este OU. Para lograr esto, complete estos pasos:

1. Haga clic con el botón secundario en la unidad organizativa nueva creada. Navegue hasta LDAP-USERS> New > User desde los menús contextuales resultantes para crear un nuevo usuario, como se muestra en la imagen:





2. En la página Configuración de usuario, rellene los campos obligatorios como se muestra en este ejemplo. Este ejemplo tiene User1 en el campo Nombre de inicio de sesión de usuario.

Este es el nombre de usuario que se verifica en la base de datos LDAP para autenticar al cliente. En este ejemplo se utiliza User1 en los campos First name y Full Name. Haga clic en Next (Siguiente).

**New Object - User** X

 Create in: CISCOSYSTEMS.local/LDAP-USERS

---

First name:  Initials:

Last name:

Full name:

User logon name:  
  ▾

User logon name (pre-Windows 2000):

---

3. Introduzca una contraseña y confírmela. Elija la opción Password never expires y haga clic en Next.

**New Object - User** X

---

 Create in: CISCO SYSTEMS.local/LDAP-USERS

---

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

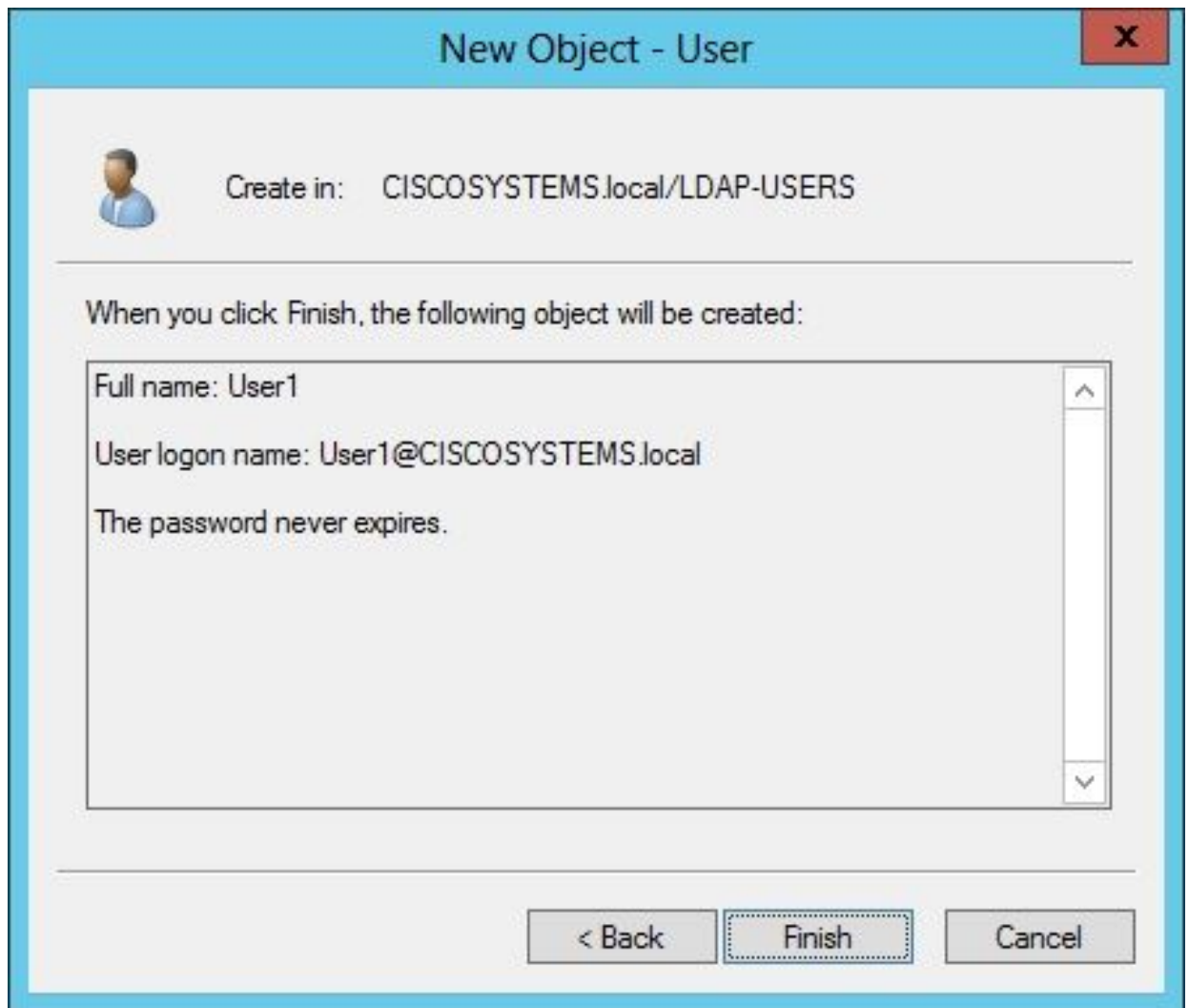
Account is disabled

---

4. Haga clic en Finish (Finalizar).

Se crea un nuevo usuario User1 bajo OU LDAP-USERS. Estas son las credenciales de usuario:

- nombre de usuario: Usuario1
- password: Portátil123




Ahora que el usuario se ha creado en una OU, el siguiente paso es configurar este usuario para el acceso LDAP.

### Configuración del usuario para el acceso LDAP

Puede elegir Anonymous o Authenticated para especificar el método de enlace de autenticación local para el servidor LDAP. El método Anonymous permite el acceso anónimo al servidor LDAP. El método Authenticated requiere que se especifique un nombre de usuario y una contraseña para proteger el acceso. El valor predeterminado es Anonymous.

En esta sección se explica cómo configurar los métodos Anonymous y Authenticated.

#### Enlace anónimo

 **Nota:** no se recomienda el uso de enlace anónimo. Un servidor LDAP que permite el enlace anónimo no requiere ningún tipo de autenticación con credenciales. Un atacante podría aprovechar la entrada de enlace anónimo para ver los archivos en el director LDAP.

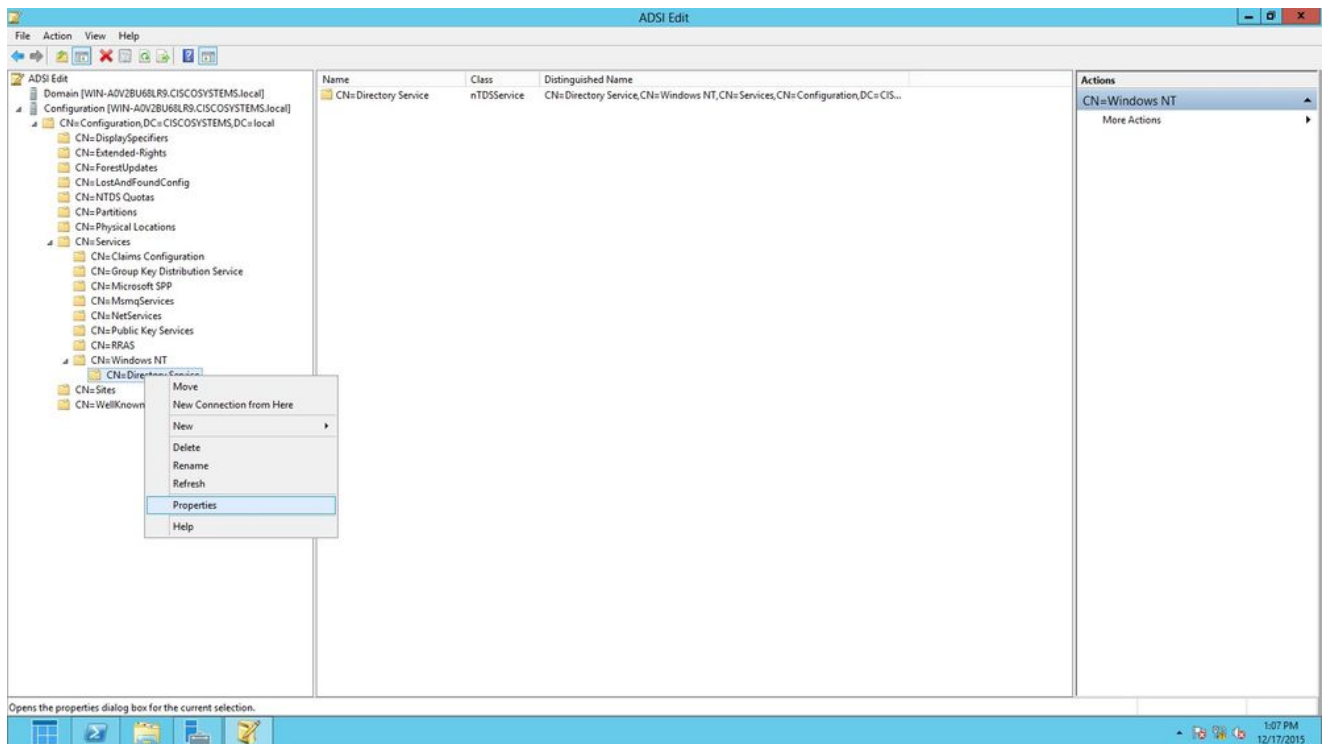
Realice los pasos de esta sección para configurar el usuario anónimo para el acceso LDAP.

## Habilitar la característica de enlace anónimo en Windows 2012 Essentials Server


Para que cualquier aplicación de terceros (en nuestro caso WLC) acceda a Windows 2012 AD en LDAP, la función Anonymous Bind debe estar habilitada en Windows 2012. De forma predeterminada, las operaciones LDAP anónimas no están permitidas en los controladores de dominio de Windows 2012. Realice estos pasos para habilitar la función Anonymous Bind:


1. Inicie la herramienta de edición ADSI escribiendo: ADSIEdit.msc en Windows PowerShell. Esta herramienta forma parte de las herramientas de soporte de Windows 2012.
2. En la ventana Editar ADSI, expanda el dominio raíz (Configuración [WIN-A0V2BU68LR9.CISCOSYSTEMS.local]).

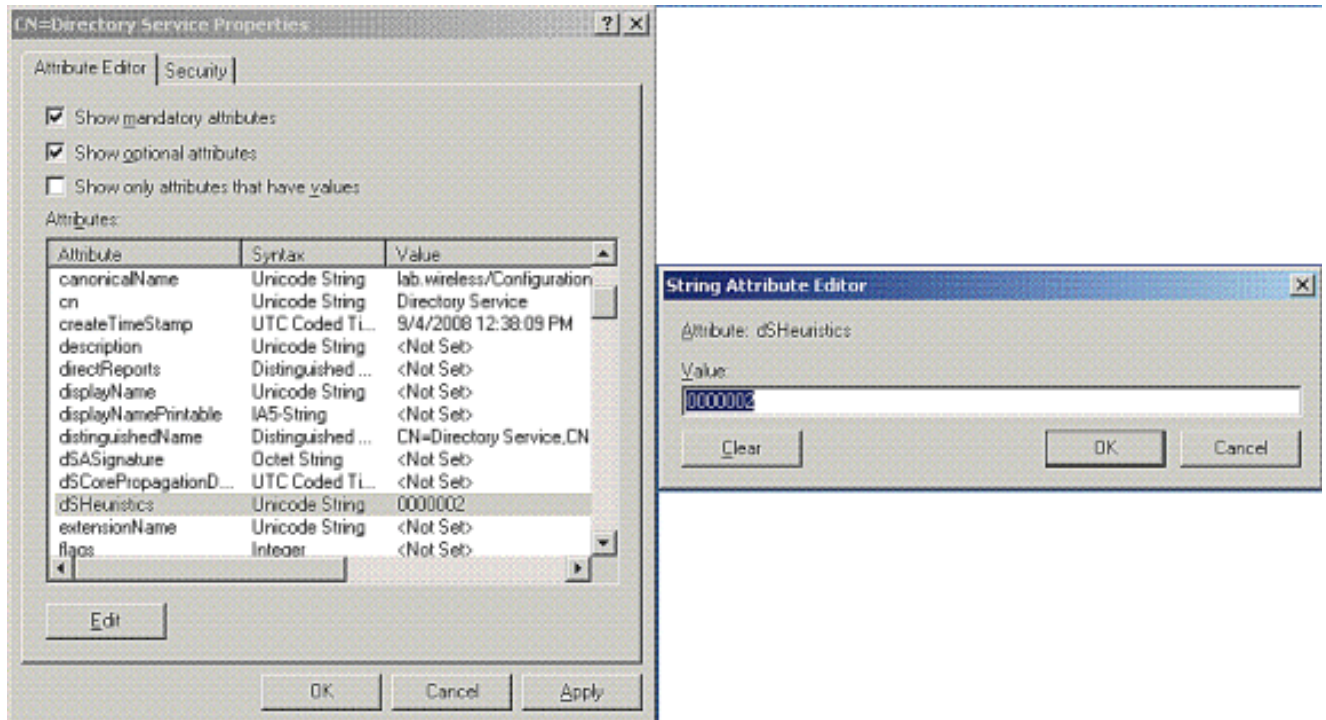
Navegue hasta CN=Services > CN=Windows NT > CN=Directory Service. Haga clic con el botón derecho del mouse en el contenedor CN=Directory Service y elija Properties en el menú contextual, como se muestra en la imagen:



3. En la ventana CN=Directory Service Properties, en Attributes, haga clic en el atributo dsHeuristics en el campo Attribute y elija Edit. En la ventana Editor de atributos de cadena de este atributo, introduzca el valor 0000002; haga clic en Aplicar y en Aceptar, como se muestra en la imagen. La característica Enlace anónimo está habilitada en el servidor de Windows 2012.

 Nota: El último (séptimo) carácter es el que controla la forma en que se puede enlazar con el servicio LDAP. 0 (cero) o ningún séptimo carácter significa que las operaciones

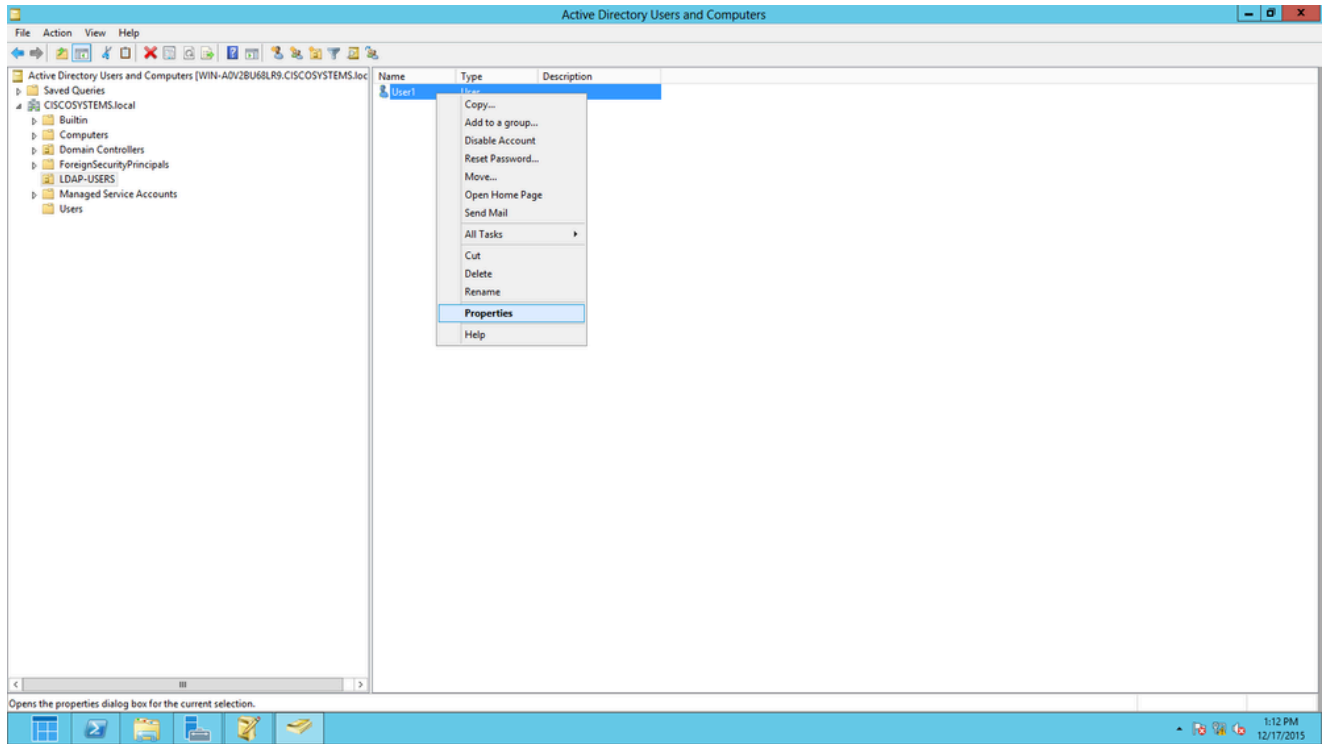
-  LDAP anónimas están inhabilitadas. Si establece el séptimo carácter en 2, se habilita la característica Enlace anónimo.



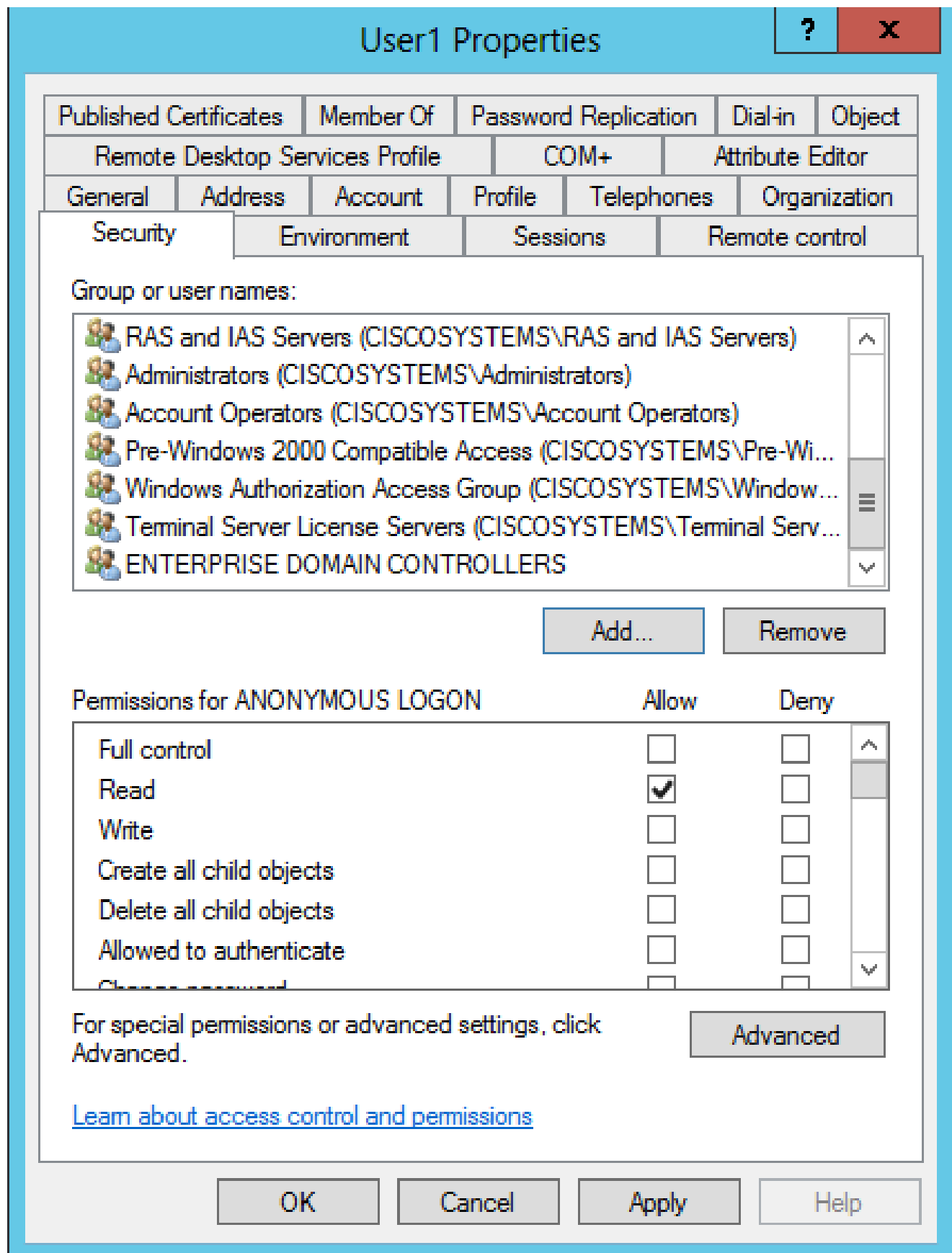
Concesión de acceso de INICIO DE SESIÓN ANÓNIMO al usuario

El siguiente paso consiste en conceder acceso de INICIO DE SESIÓN ANÓNIMO al usuario User1. Complete estos pasos para lograr esto:

1. Abra Usuarios y equipos de Active Directory.
2. Asegúrese de que la opción Ver funciones avanzadas esté activada.
3. Desplácese hasta el usuario User1 y haga clic con el botón secundario en él. Elija Properties en el menú contextual. Este usuario se identifica con el nombre User1.



4. Haga clic en la pestaña Security, como se muestra en la imagen:

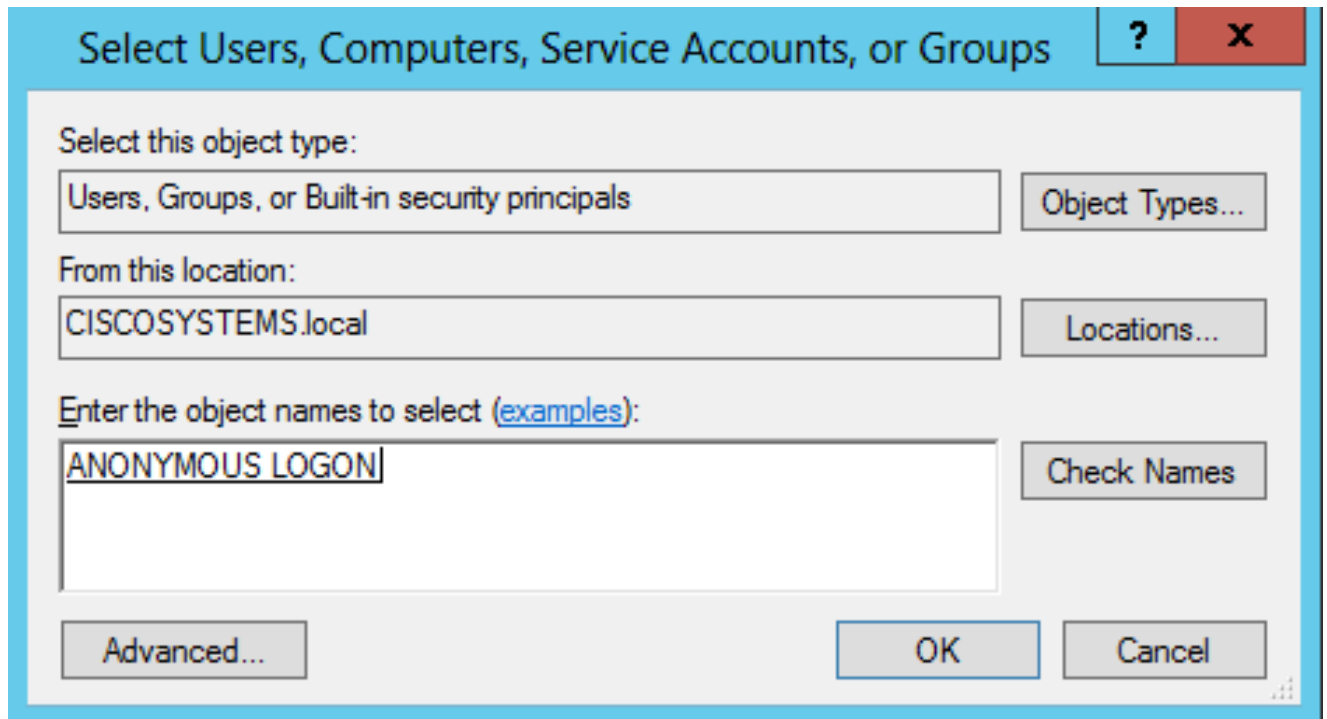


5. Haga clic en Agregar en la ventana resultante.

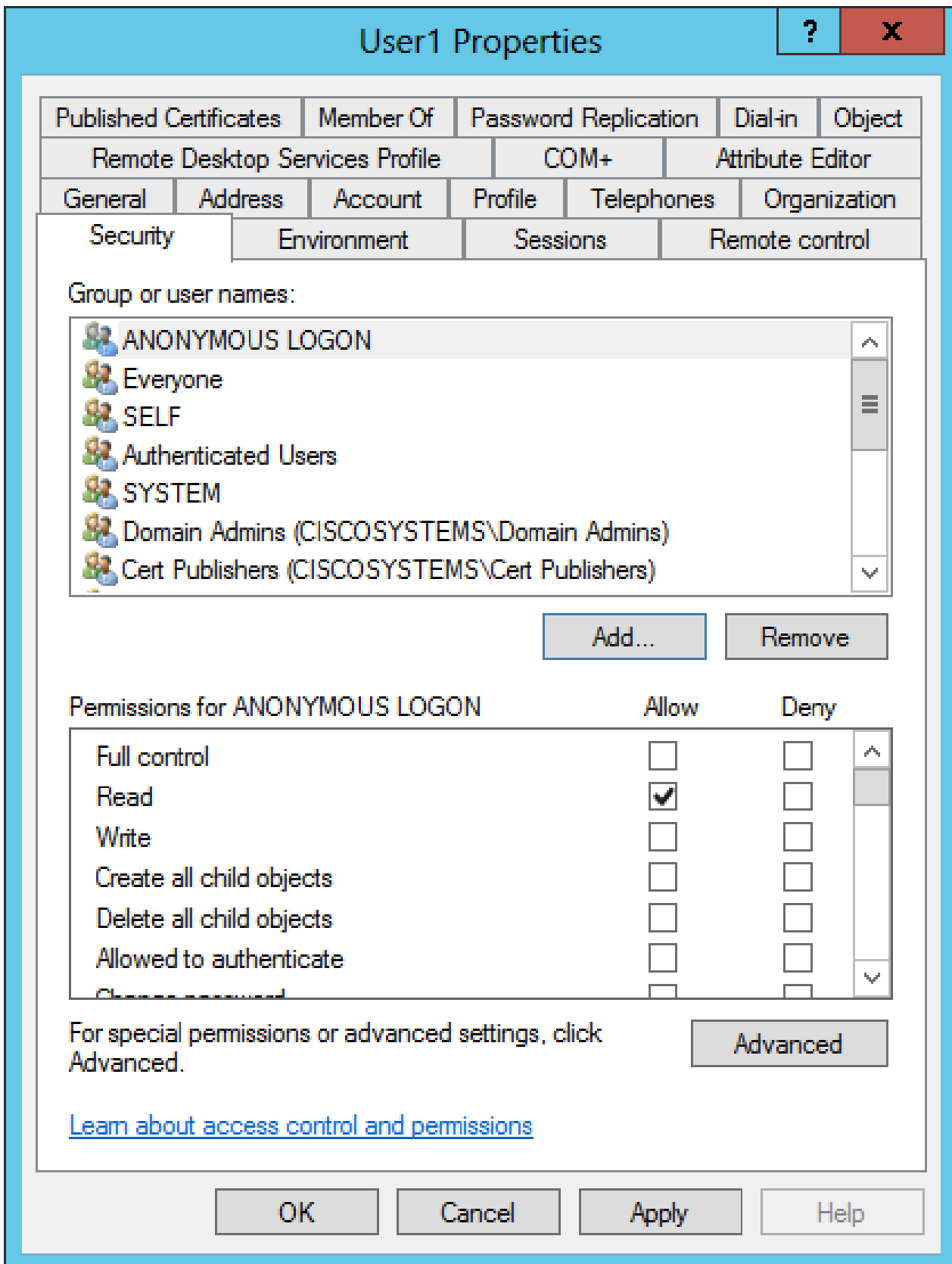
6. Ingrese ANONYMOUS LOGON bajo el cuadro Ingrese los nombres de objeto a seleccionar



y acepte el diálogo, como se muestra en la imagen:



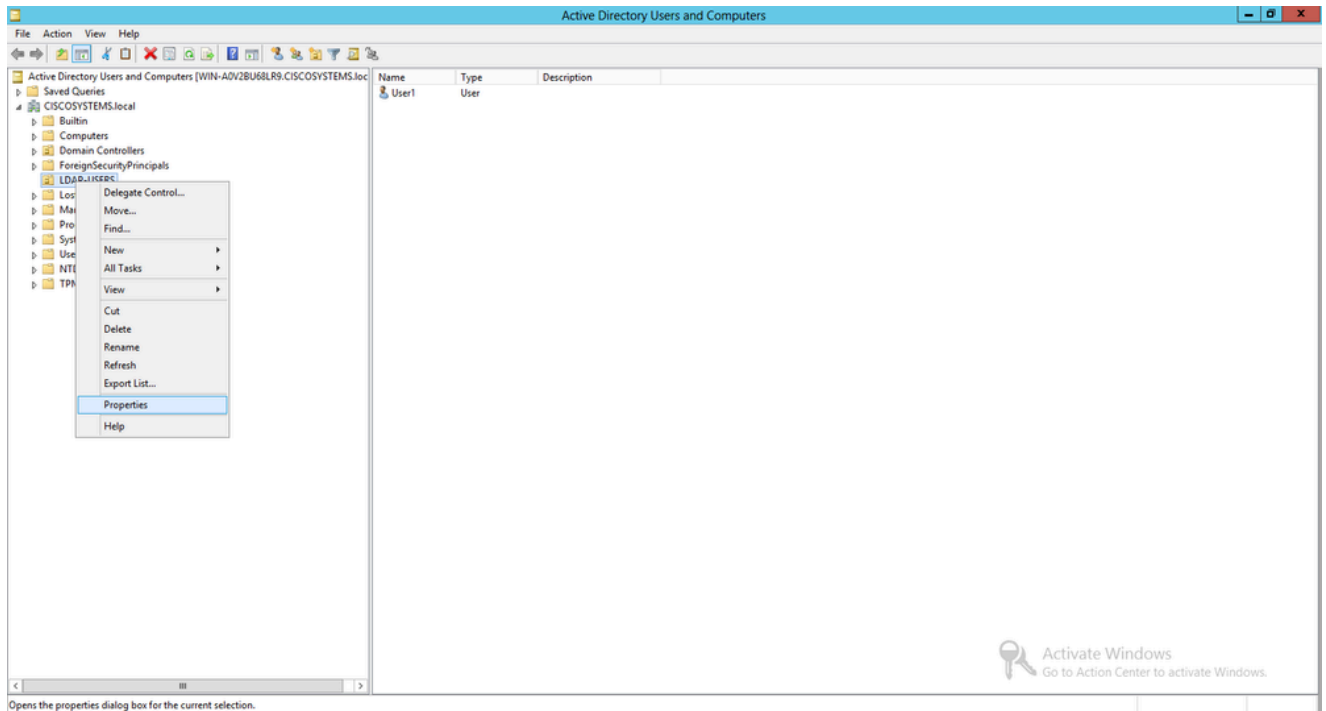
7. En la ACL, observe que ANONYMOUS LOGON tiene acceso a algunos conjuntos de propiedades del usuario. Click OK. El acceso de INICIO DE SESIÓN ANÓNIMO se concede a este usuario, como se muestra en la imagen:



Conceder permiso de contenido de lista en la unidad organizativa

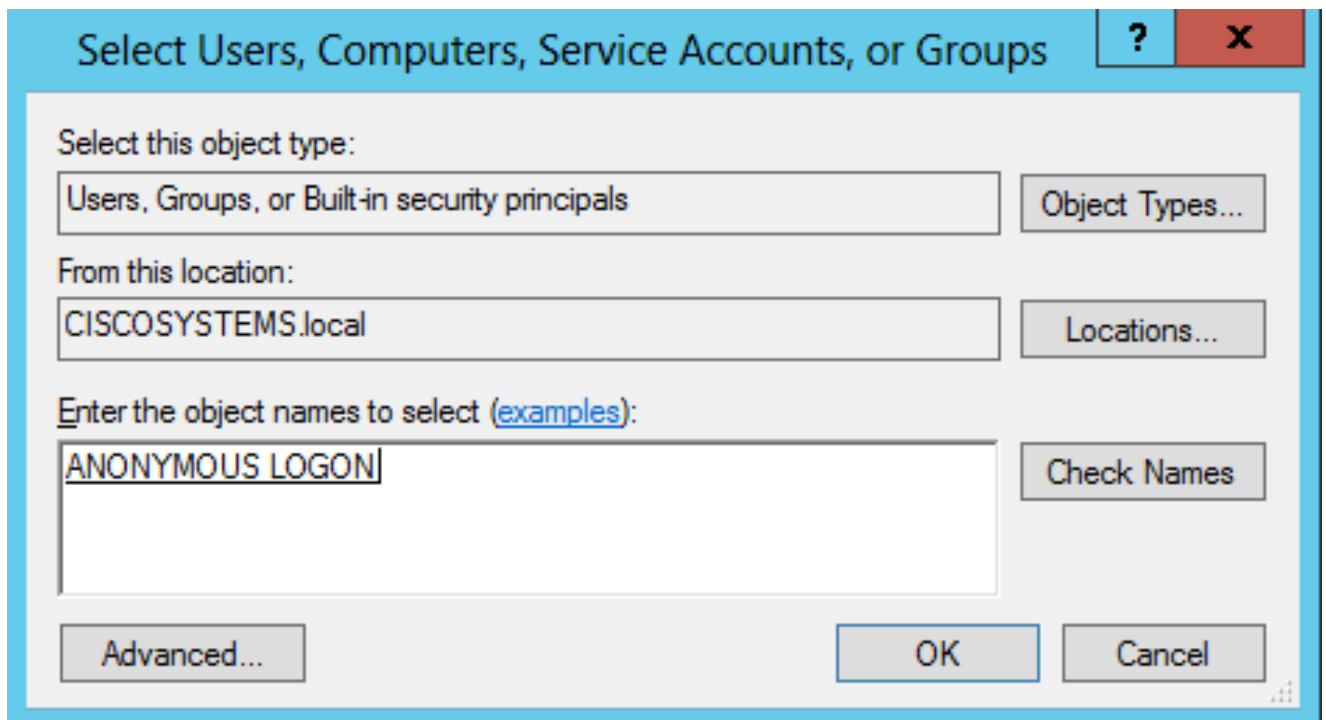
El siguiente paso consiste en conceder al menos el permiso Contenido de la lista al INICIO DE SESIÓN ANÓNIMO en la unidad organizativa en la que se encuentra el usuario. En este ejemplo, User1 se encuentra en OU LDAP-USERS. Complete estos pasos para lograr esto:

1. En Active Directory Users and Computers, haga clic con el botón derecho en OU LDAP-USERS y elija Properties, como se muestra en la imagen:



2. Haga clic en Seguridad.

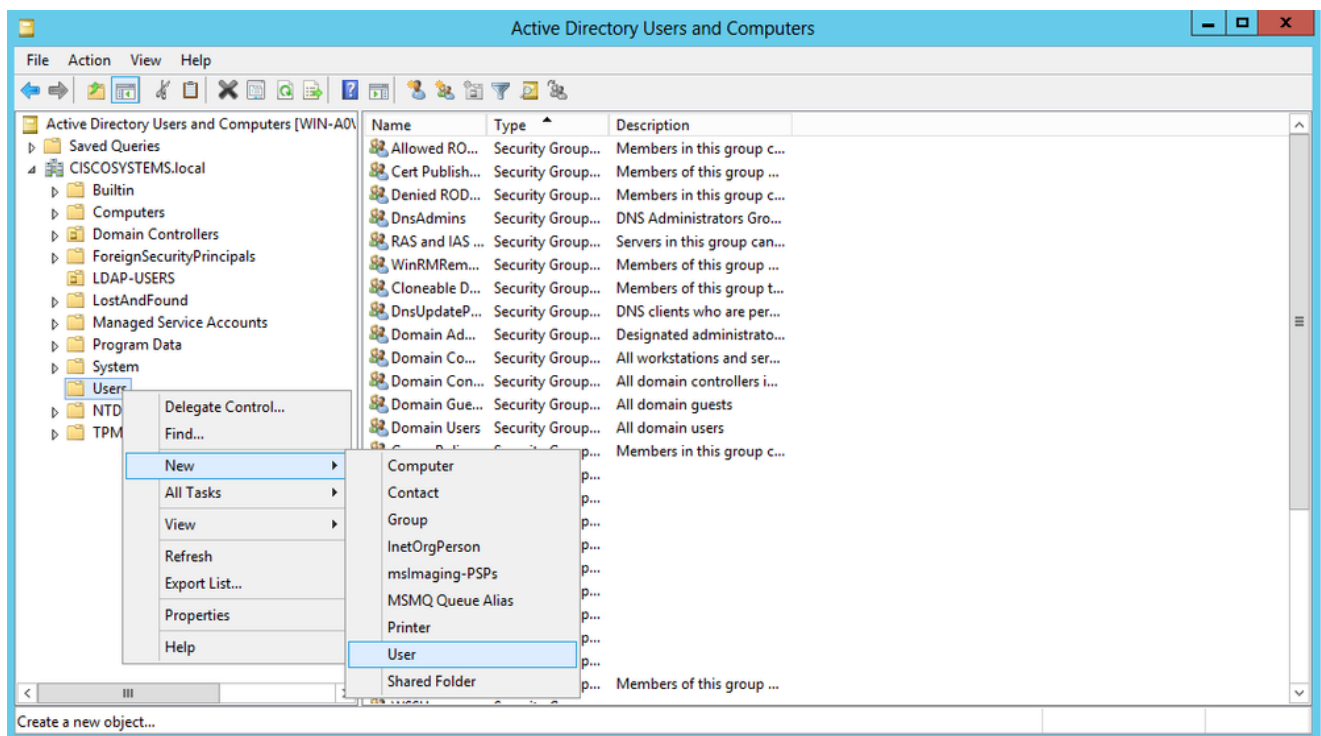
3. Haga clic en Add (Agregar). En el diálogo que se abre, ingrese ANONYMOUS LOGON y Acknowledge the dialog, como se muestra en la imagen:



## Enlace autenticado

Realice los pasos de esta sección para configurar un usuario para la autenticación local al servidor LDAP.

1. Abra Windows PowerShell y escriba `servermanager.exe`
2. En la ventana Administrador del servidor, haga clic en AD DS. A continuación, haga clic con el botón derecho del ratón en el nombre del servidor para elegir Usuarios y equipos de Active Directory.
3. Haga clic con el botón secundario en Usuarios. Navegue hasta Nuevo > Usuario desde los menús contextuales resultantes para crear un nuevo usuario.



4. En la página Configuración de usuario, rellene los campos obligatorios como se muestra en este ejemplo. Este ejemplo tiene WLC-admin en el campo Nombre de inicio de sesión de usuario. Este es el nombre de usuario que se utilizará para la autenticación local en el servidor LDAP. Haga clic en Next (Siguiente).
5. Introduzca una contraseña y confírmela. Elija la opción Password never expires y haga clic en Next.
6. Haga clic en Finish (Finalizar).

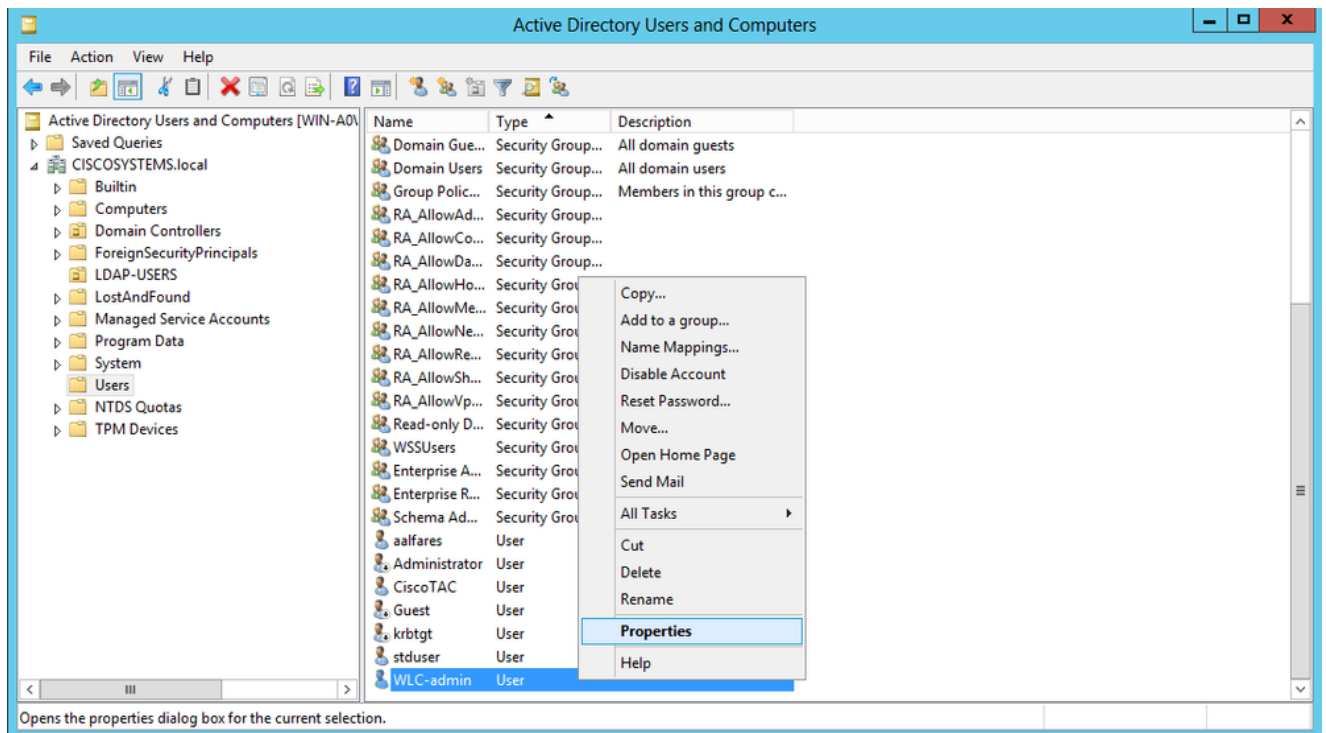
Se crea un nuevo usuario WLC-admin bajo el contenedor Users. Estas son las credenciales de usuario:

- nombre de usuario: WLC-admin
- contraseña: Admin123

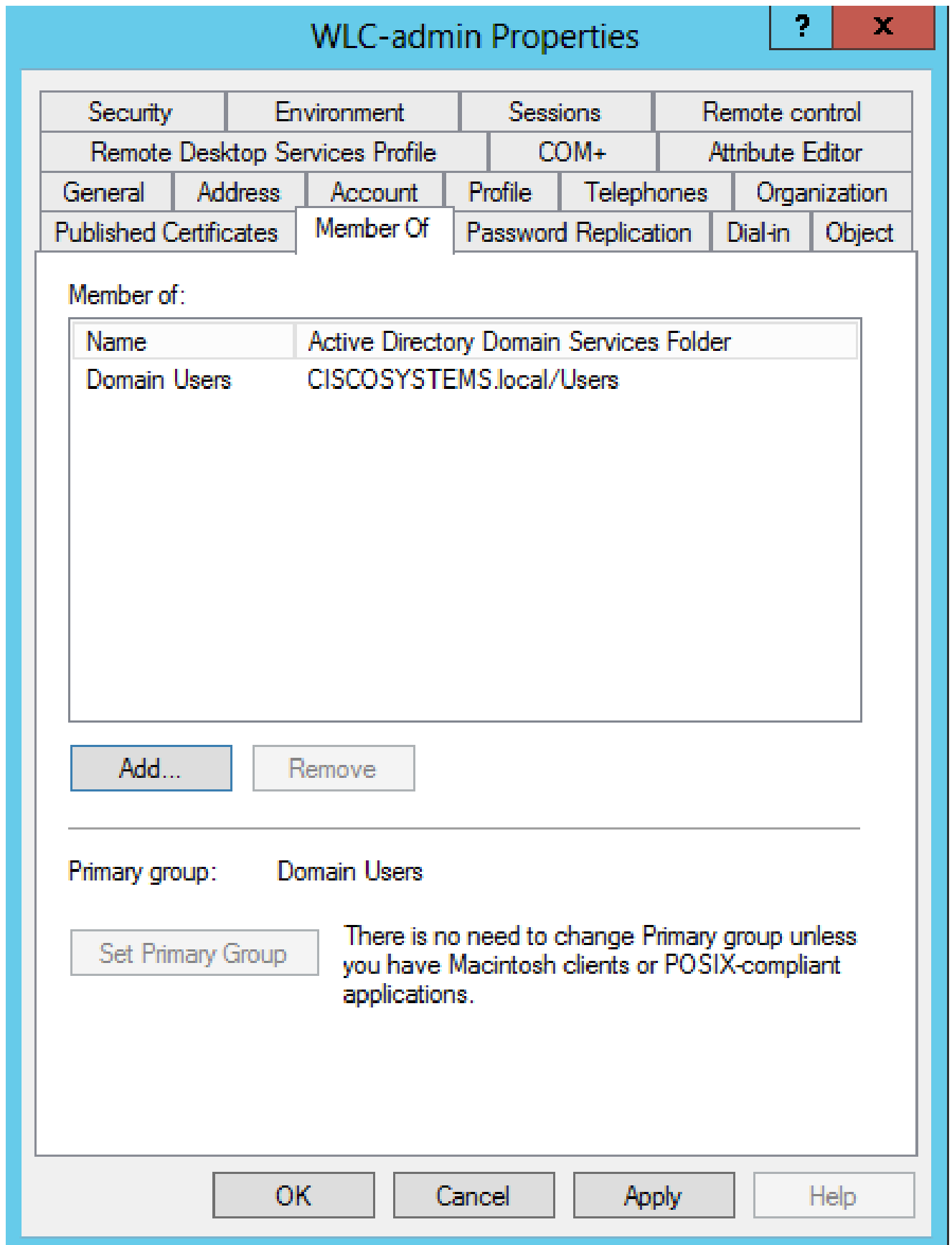
### Concesión de privilegios de administrador a WLC-admin

Ahora que se ha creado el usuario de autenticación local, debemos concederle privilegios de administrador. Complete estos pasos para lograr esto:

1. Abra Usuarios y equipos de Active Directory.
2. Asegúrese de que la opción Ver funciones avanzadas esté activada.
3. Navegue hasta el usuario WLC-admin y haga clic con el botón derecho en él. Elija Properties en el menú contextual, como se muestra en la imagen. Este usuario se identifica con el nombre WLC-admin.

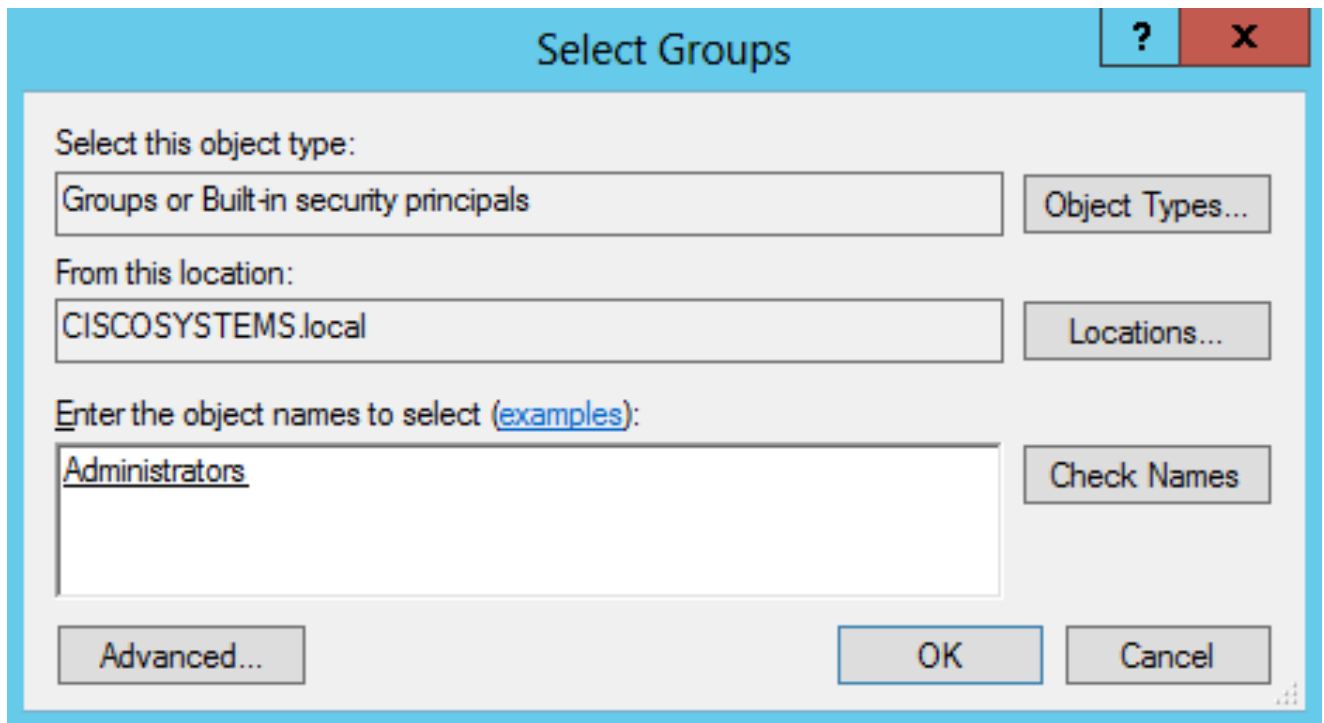


4. Haga clic en la pestaña Member Of, como se muestra en la imagen:



::

5. Haga clic en Add (Agregar). En el cuadro de diálogo que se abre, ingrese Administradores y haga clic en Aceptar, Como se muestra en la imagen:

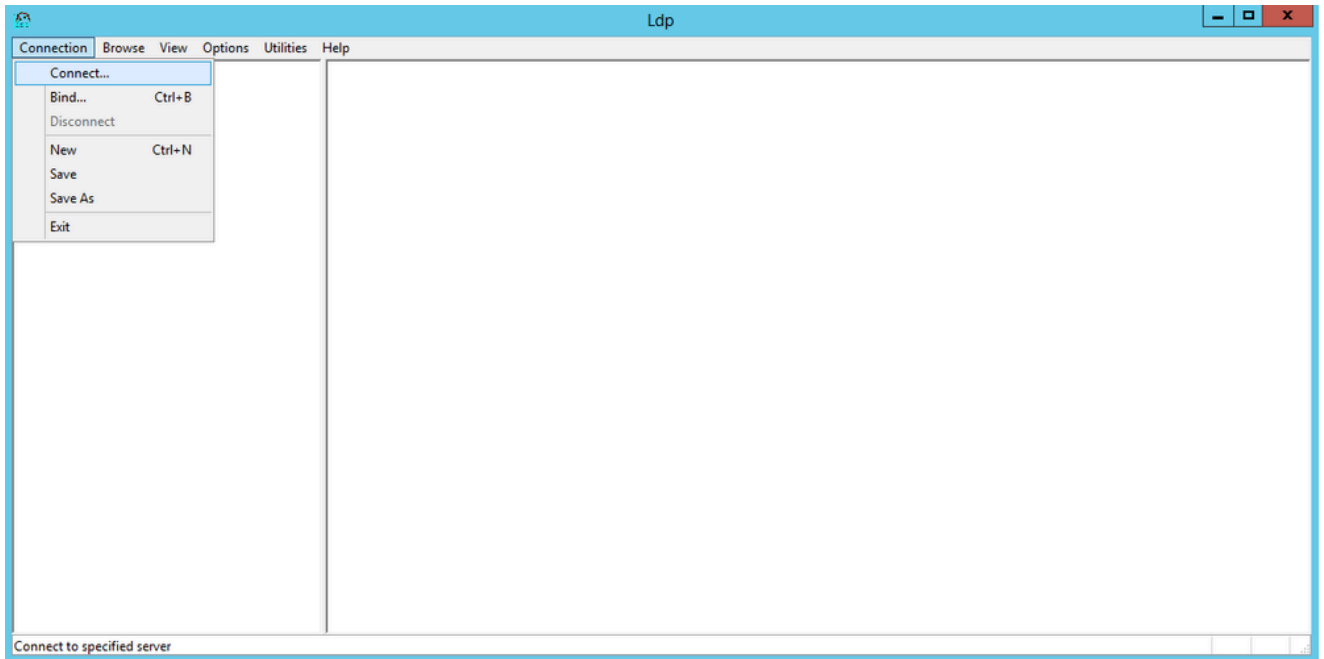


### Uso de LDP para Identificar los Atributos de Usuario

Esta herramienta GUI es un cliente LDAP que permite a los usuarios realizar operaciones, como conectar, enlazar, buscar, modificar, agregar o eliminar, en cualquier directorio compatible con LDAP, como Active Directory. LDP se utiliza para ver objetos almacenados en Active Directory junto con sus metadatos, como los descriptores de seguridad y los metadatos de replicación.

La herramienta GUI de LDP se incluye al instalar las herramientas de soporte técnico de Windows Server 2003 desde el CD del producto. Esta sección explica cómo utilizar la utilidad LDP para identificar los atributos específicos asociados al usuario User1. Algunos de estos atributos se utilizan para rellenar los parámetros de configuración del servidor LDAP en el WLC, como el tipo de atributo de usuario y el tipo de objeto de usuario.

1. En el servidor de Windows 2012 (incluso en el mismo servidor LDAP), abra Windows PowerShell e ingrese LDP para acceder al explorador LDP.
2. En la ventana principal de LDP, Navegue hasta Conexión > Conectar y conéctese al servidor LDAP cuando ingrese la dirección IP del servidor LDAP, como se muestra en la imagen.

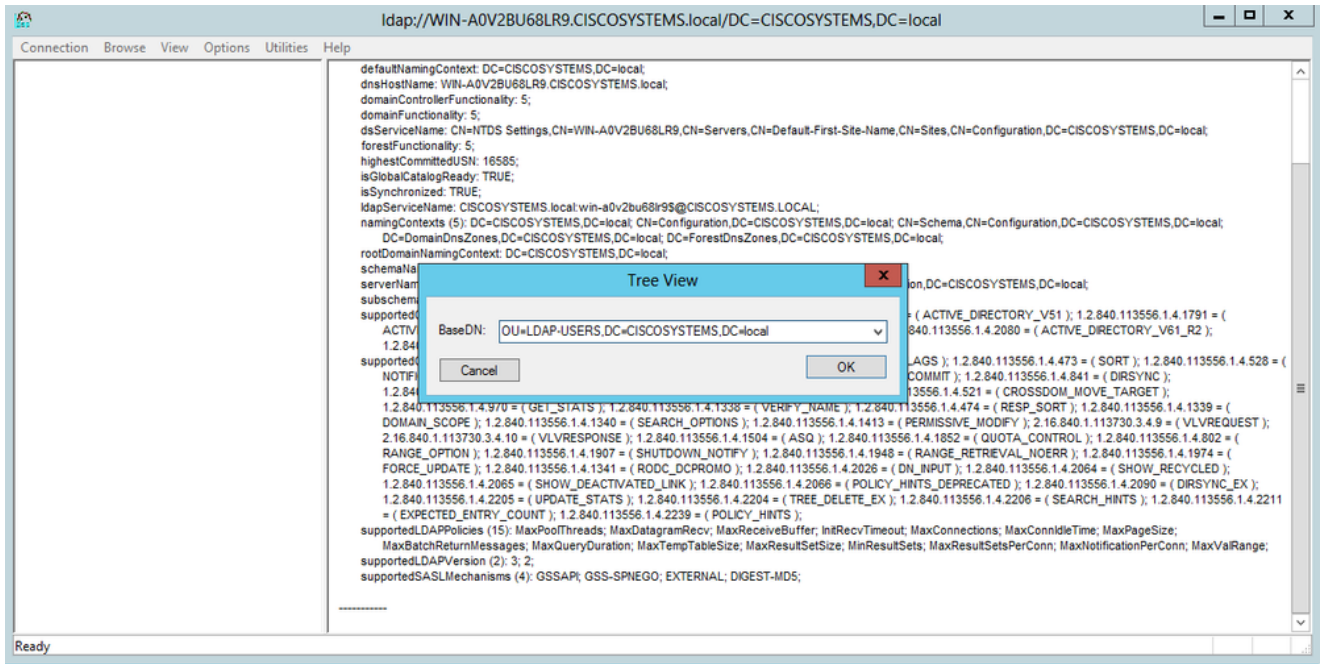


3. Una vez conectado al servidor LDAP, elija View en el menú principal y haga clic en Tree, como se muestra en la imagen:



4. En la ventana Vista de árbol resultante, introduzca el DNbase del usuario. En este ejemplo, Usuario1 se encuentra en la unidad organizativa "LDAP-USERS" bajo el dominio CISCOSYSTEMS.local. Haga clic en OK, como se muestra en la imagen:





5. El lado izquierdo del navegador LDP muestra el árbol completo que aparece bajo el DN base especificado (OU=LDAP-USERS, dc=CISCOYSTEMS, dc=local). Expanda el árbol para localizar al usuario User1. Este usuario se puede identificar con el valor CN que representa el nombre del usuario. En este ejemplo, es CN=User1. Haga doble clic en CN=User1. En el panel derecho del navegador LDP, LDP muestra todos los atributos asociados con User1, como se muestra en la imagen:




6. Cuando configure el WLC para el servidor LDAP, en el campo User Attribute, ingrese el nombre del atributo en el registro de usuario que contiene el nombre de usuario. En esta salida LDP, puede ver que sAMAccountName es un atributo que contiene el nombre de usuario "User1", así que ingrese el atributo sAMAccountName que corresponde al campo User Attribute en el WLC.

7. Cuando configure el WLC para el servidor LDAP, en el campo User Object Type, ingrese el valor del atributo objectType de LDAP que identifica el registro como usuario. A menudo, los registros de usuario tienen varios valores para el atributo objectType, algunos de los cuales son únicos al usuario y otros son compartidos con otros tipos de objeto. En la salida LDP, CN=Person es un valor que identifica el registro como usuario, así que especifique Person como el atributo User Object Type en el WLC.

El siguiente paso es configurar el WLC para el servidor LDAP.

## Configuración de WLC para servidor LDAP

Ahora que el servidor LDAP está configurado, el siguiente paso es configurar el WLC con los detalles del servidor LDAP. Complete estos pasos en la GUI del WLC:

 Nota: Este documento asume que el WLC se configura para el funcionamiento básico y que los LAPs se registran al WLC. Si usted es un nuevo usuario que desea configurar el WLC para el funcionamiento básico con los LAPs, consulte [Registro ligero del AP \(LAP\) a un controlador del Wireless LAN \(WLC\)](#).

1. En la página Security del WLC, elija AAA > LDAP del panel de tareas del lado izquierdo para moverse a la página de configuración del servidor LDAP.



Server Index	Server Address (IPv4/IPv6)	Port	Server State	Secure Mode (via TLS)	Bind
1	172.16.16.200	389	Enabled	Disabled	Authenticated

Para agregar un servidor LDAP, haga clic en New. Se abrirá la ventana LDAP Servers > New.

2. En la página LDAP Servers Edit (Editar servidores LDAP), especifique los detalles del servidor LDAP, como la dirección IP del servidor LDAP, el número de puerto, el estado del servidor Enable (Activar servidor), etc.
  - Elija un número en el cuadro desplegable Server Index (Priority) para especificar el orden de prioridad de este servidor en relación con cualquier otro servidor LDAP configurado. Puede configurar hasta diecisiete servidores. Si el controlador no puede alcanzar el primer servidor, intenta el segundo en la lista y así sucesivamente.
  - Ingrese la dirección IP del servidor LDAP en el campo Dirección IP del servidor.

- Ingrese el número de puerto TCP del servidor LDAP en el campo Número de puerto. El intervalo válido es 1 a 65535, y el valor predeterminado es 389.
- para el enlace simple, utilizamos Authenticated, para el nombre de usuario de enlace que es la ubicación del usuario administrador del WLC que se utilizará para acceder al servidor LDAP y su contraseña
- En el campo User Base DN, ingrese el nombre distintivo (DN) de la sub-estructura en el servidor LDAP que contiene una lista de todos los usuarios. Por ejemplo, ou=organizational unit, .ou=next organizational unit o o=corporation.com. Si el árbol que contiene usuarios es el DN base, introduzca o=corporation.com o dc=corporation, dc=com.

En este ejemplo, el usuario se encuentra bajo la unidad organizativa (OU) LDAP-USERS, que, a su vez, se crea como parte del dominio lab.wireless.

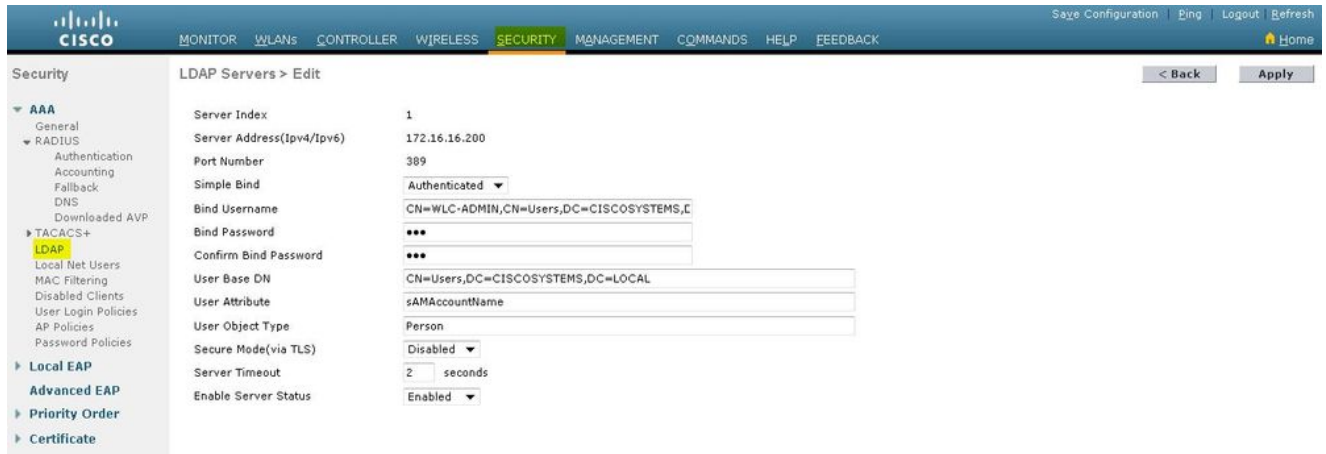
El DN base de usuario debe indicar la ruta completa en la que se encuentra la información de usuario (credencial de usuario según el método de autenticación EAP-FAST). En este ejemplo, el usuario se encuentra en el DN base OU=LDAP-USERS, DC=CISCOYSTEMS, DC=local.

- En el campo User Attribute, ingrese el nombre del atributo en el registro de usuarios que contiene el nombre de usuario.

En el campo User Object Type, ingrese el valor del atributo objectType del LDAP que identifica el registro como usuario. A menudo, los registros de usuario tienen varios valores para el atributo objectType, algunos de los cuales son únicos al usuario y otros son compartidos con otros tipos de objeto

Puede obtener el valor de estos dos campos desde el servidor de directorios con la utilidad de explorador LDAP que se incluye como parte de las herramientas de soporte de Windows 2012. Esta herramienta del navegador LDAP de Microsoft se llama LDP. Con la ayuda de esta herramienta, puede conocer los campos User Base DN, User Attribute y User Object Type de este usuario en particular. En la sección Uso de LDP para Identificar los Atributos de Usuario de este documento se trata información detallada sobre cómo utilizar LDP para conocer estos atributos específicos de Usuario.

- En el campo Server Timeout (Tiempo de espera del servidor), introduzca el número de segundos entre retransmisiones. El intervalo válido es de 2 a 30 segundos, y el valor predeterminado es 2 segundos.
- Marque el cuadro Enable Server Status para habilitar este servidor LDAP, o desmárquelo para inhabilitarlo. Se inhabilitará el valor predeterminado.
- Haga clic en Apply para aplicar sus cambios. Este es un ejemplo ya configurado con esta información:



3. Ahora que los detalles sobre el servidor LDAP se configuran en el WLC, el siguiente paso es configurar un WLAN para la autenticación Web.

## Configuración de la WLAN para la autenticación Web

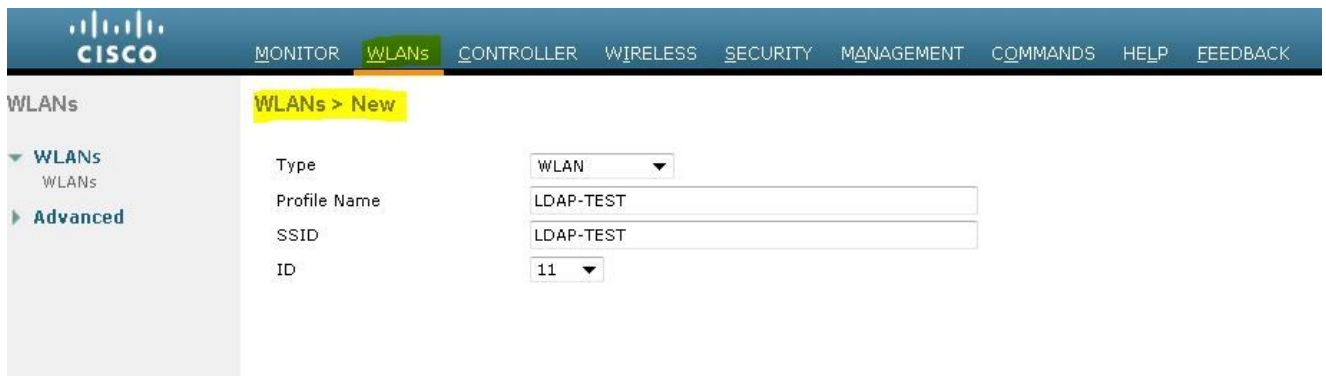
El primer paso es crear una WLAN para los usuarios. Complete estos pasos:

1. Haga clic en WLAN en la GUI para crear una WLAN.

Aparece la ventana WLAN. Esta ventana enumera las WLAN configuradas en el controlador.

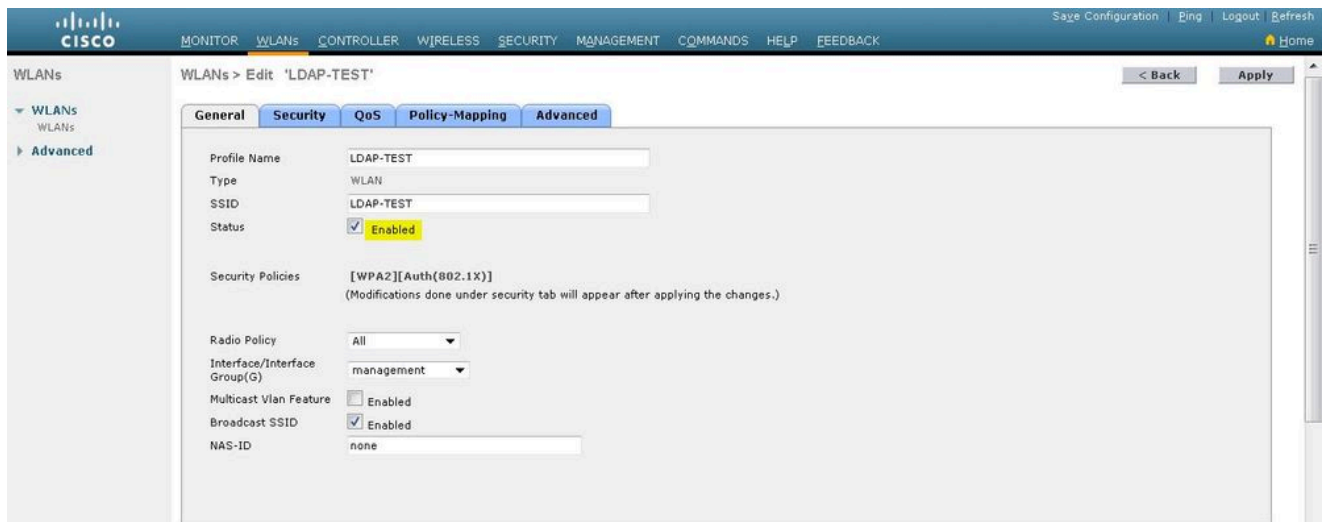
2. Haga clic en Nuevo para configurar una WLAN nueva.

En este ejemplo, la WLAN se llama Web-Auth.



3. Haga clic en Apply (Aplicar).

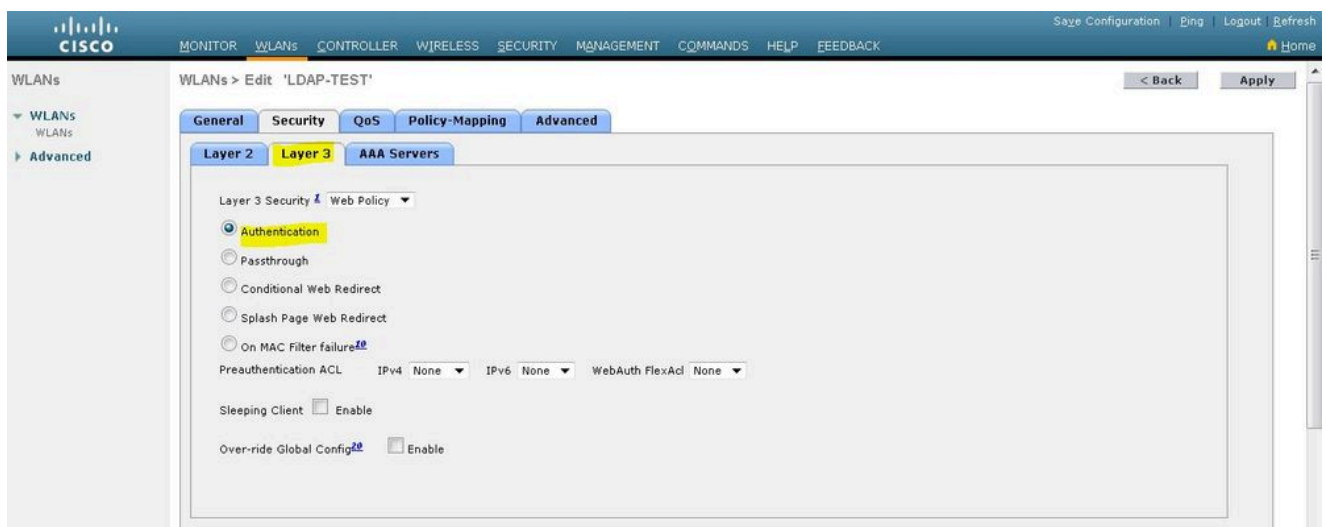
4. En la ventana WLAN > Edit , defina los parámetros específicos de la WLAN.




- Marque la casilla de verificación Status (Estado) para activar la WLAN.
- Para la WLAN, elija la interfaz apropiada del campo Interface Name (Nombre de la interfaz).

En este ejemplo se asigna la interfaz de administración que se conecta a la autenticación Web WLAN.

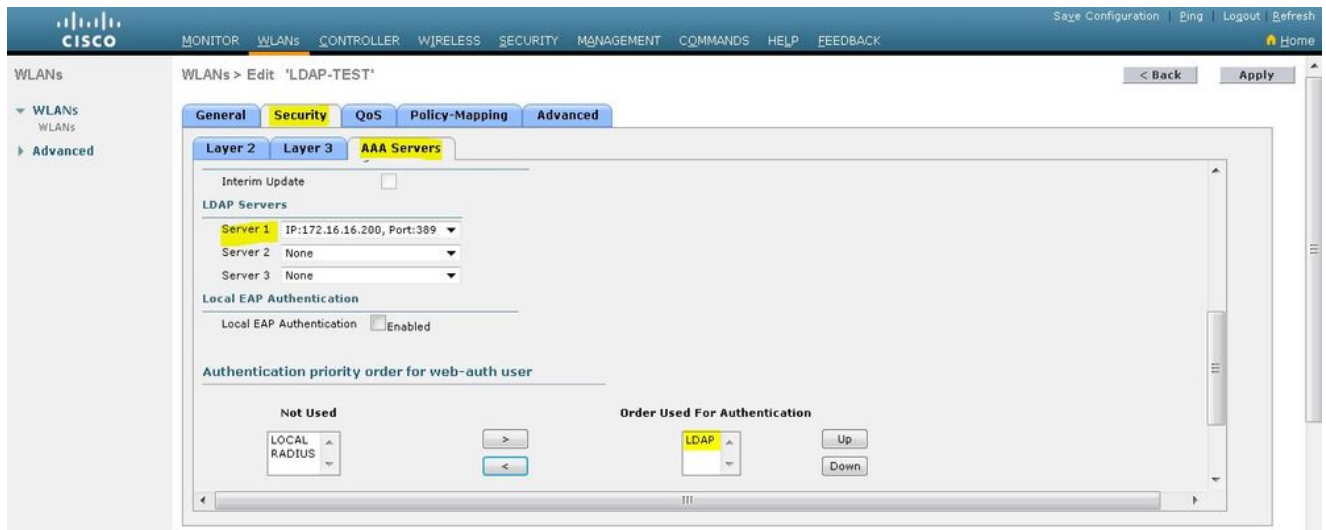
5. Haga clic en la ficha Security (Seguridad). En el campo Layer 3 Security, marque la casilla de verificación Web Policy y elija la opción Authentication.



Esta opción se elige porque la autenticación Web se utiliza para autenticar los clientes inalámbricos. Marque la casilla de verificación Override Global Config para habilitar por la configuración de autenticación web WLAN. Elija el tipo de autenticación web adecuado en el menú desplegable Web Auth type . Este ejemplo utiliza la autenticación Web interna.

 Nota: la autenticación Web no es compatible con la autenticación 802.1x. Esto significa que no puede elegir 802.1x o un WPA/WPA2 con 802.1x como seguridad de capa 2 cuando utiliza la autenticación Web. La autenticación Web es compatible con todos los demás parámetros de seguridad de capa 2.

6. Haga clic en la pestaña AAA Servers. Elija el servidor LDAP configurado en el menú desplegable del servidor LDAP. Si utiliza una base de datos local o un servidor RADIUS, puede establecer la prioridad de autenticación en el campo de usuario Orden de prioridad de autenticación para Web-auth.



7. Haga clic en Apply (Aplicar).



Nota: En este ejemplo, no se utilizan los métodos de seguridad de capa 2 para autenticar a los usuarios, por lo que debe elegir None (Ninguno) en el campo Layer 2 Security (Seguridad de capa 2).

## Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Para verificar esta configuración, conecte un cliente inalámbrico y verifique si la configuración funciona según lo esperado.

El cliente inalámbrico se activa y el usuario introduce la URL, como [www.yahoo.com](http://www.yahoo.com), en el navegador web. Debido a que el usuario no ha sido autenticado, el WLC redirige al usuario a la URL de login web interna.

Se le solicitarán al usuario las credenciales de usuario. Una vez que el usuario envía el nombre de usuario y la contraseña, la página de login toma la entrada de las credenciales del usuario y, al enviar, envía la solicitud de nuevo al ejemplo action\_URL, <http://1.1.1.1/login.html>, del servidor web del WLC. Esto se proporciona como un parámetro de entrada a la URL de redirección del cliente, donde 1.1.1.1 es la dirección de la interfaz virtual en el switch.

El WLC autentica al usuario contra la base de datos de usuarios LDAP. Después de la autenticación exitosa, el servidor web del WLC reenvía al usuario a la URL de redireccionamiento configurada o a la URL con la que el cliente comenzó, tal como [www.yahoo.com](http://www.yahoo.com).





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

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

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

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

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



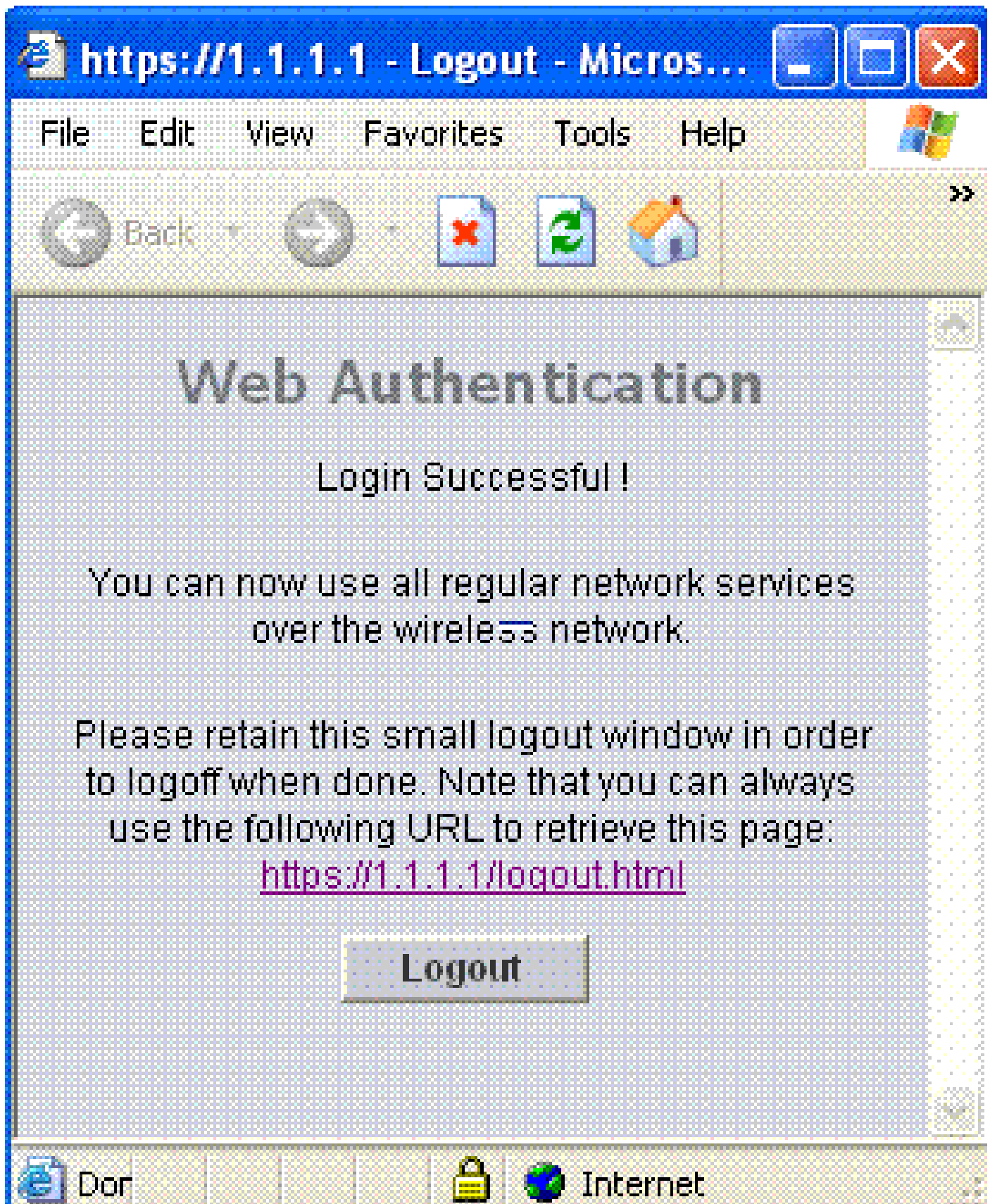
Login



### Welcome to the Cisco wireless network

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.

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



## Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de



configuración.

Utilice estos comandos para resolver problemas de configuración:

- 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

Este es un ejemplo de salida de los comandos debug mac addr cc:fa:00:f7:32:35

debug aaa ldap enable

```
(Cisco_Controller) >*pemReceiveTask: Dec 24 03:45:23.089: cc:fa:00:f7:32:35 Sent an XID frame
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Processing assoc-req station:cc:fa:00:f7:32:35
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Association received from mobile on BSSID 00:2
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Global 200 Clients are allowed to AP radio

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

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

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

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

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Changing IPv4 A
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Changing IPv6 A
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfApplyWlanPolicy: Apply WLAN Policy over PMI
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6246 setting Central switched
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6249 apVapId = 1 and Split Ac
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying site-specific Local Bridging override
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Local Bridging Interface Policy for s
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE statusCode is 0 and status is 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE ssid_done_flag is 0 finish_flag
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 STA - rates (3): 24 164 48 0 0 0 0 0 0 0 0 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 suppRates statusCode is 0 and gotSuppRatesEle
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 AID 2 in Assoc Req from flex AP 00:23:eb:e5:04
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfMs1xStateDec
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Change state to

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 pemApfAddMobileStation2: APF_MS_PEM_WAIT_L2_AU
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Initializing policy
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Change state to AUTHCH

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

*pemReceiveTask: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 Removed NPU entry.
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Not Using WMM Compliance code qosCap 00
```

\*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4) Plumbed mobile  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4) Change state  
  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) pemApfAddMobile  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Adding Fast Path  
type = Airespace AP Client - ACL passthru  
on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0  
IPv4 ACL I  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Fast Path rule  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Fast Path rule  
  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Fast Path rule  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Fast Path rule  
  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Successfully pl  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) pemApfAddMobile  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Replacing Fast  
type = Airespace AP Client - ACL passthru  
on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0  
IPv4 AC  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Fast Path rule  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Fast Path rule  
  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Fast Path rule  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Fast Path rule  
  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Successfully pl  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2 (apf\_policy.c:359) Changing sta  
  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2:session timeout for station cc:fa  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Scheduling deletion of Mobile Station: (calle  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Func: apfPemAddUser2, Ms Timeout = 1800, Sessi  
  
\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Sending assoc-resp with status 0 station:cc:fa  
\*apfMsConnTask\_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sending Assoc Response to station on BSSID 00:  
\*apfMsConnTask\_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 apfProcessAssocReq (apf\_80211.c:10187) Changin  
  
\*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2, dtlFla  
\*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sent an XID frame  
\*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2, dtlFla  
\*pemReceiveTask: Dec 24 03:45:43.558: cc:fa:00:f7:32:35 Sent an XID frame  
\*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len 322,vla  
\*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype 0xff:ff:ff:ff:  
\*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block settin  
dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0,  
dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25 VLAN: 16  
\*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25 mscbVapLoc  
\*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local a  
\*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block settin  
dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0,  
dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25 VLAN: 16  
\*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE  
\*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block settin  
dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,  
dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16  
\*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25 mscbVapLoc  
\*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local a  
\*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP transmitting DHCP DISCOVER (1)  
\*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP op: BOOTREQUEST, htype: Ethernet, hlen  
\*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 0,

```

*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP chaddr: cc:fa:00:f7:32:35
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP siaddr: 0.0.0.0, giaddr: 172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block setting
    dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
    dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE
*DHCP Proxy Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP received op BOOTREPLY (2) (len 572,vlan 0)
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418, port 1, vlan 0)
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP transmitting DHCP OFFER (2)
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 0,
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP chaddr: cc:fa:00:f7:32:35
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP ciaddr: 0.0.0.0, yiaddr: 172.16.16.122
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP server id: 1.1.1.1 rcvd server id: 172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len 334,vlan 0)
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype 0xff:ff:ff:ff:ff:ff
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block setting
    dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
    dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25 mscbVapLocalMac=00:00:00:00:00:00
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local address)
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP transmitting DHCP REQUEST (3)
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 0,
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP chaddr: cc:fa:00:f7:32:35
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP siaddr: 0.0.0.0, giaddr: 172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP requested ip: 172.16.16.122
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP server id: 172.16.16.25 rcvd server id: 172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block setting
    dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
    dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP received op BOOTREPLY (2) (len 572,vlan 0)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP setting server from ACK (mscb=0x40e64b88)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418, port 1, vlan 0)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP transmitting DHCP ACK (5)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 0,
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP chaddr: cc:fa:00:f7:32:35
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP ciaddr: 0.0.0.0, yiaddr: 172.16.16.122
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP server id: 1.1.1.1 rcvd server id: 172.16.16.25
*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created for mobile, length 10
*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created in mscb for mobile, length 10
*aaaQueueReader: Dec 24 03:46:01.222: AuthenticationRequest: 0x2b6bdc3c

*aaaQueueReader: Dec 24 03:46:01.222: Callback.....0x12088c50
*aaaQueueReader: Dec 24 03:46:01.222: protocolType.....0x00000002
*aaaQueueReader: Dec 24 03:46:01.222: proxyState.....CC:FA:00:F7:32:35-
*aaaQueueReader: Dec 24 03:46:01.222: Packet contains 15 AVPs (not shown)

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

```

```

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

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

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Change state to V
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 apfMsRunStateInc
*LDAP DB Task 1: Dec 24 03:46:01.228: ldapClose [1] called lcapi_close (rc = 0 - Success)
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_NOL3SEC (14) Change state

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Stopping deletion of Mobile Station: (callerId:
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Setting Session Timeout to 1800 sec - starting
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Reached PLUMBFASPATH: f
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Replacing Fast Path rule
    type = Airespace AP Client
    on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0
    IPv4 ACL ID = 255, IPv6 ACL ID
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule (contd...
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule (contd...

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

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

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

```

```

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

```

Netmask..... 255.255.254.0  
Association Id..... 2  
Authentication Algorithm..... Open System  
Reason Code..... 1  
Status Code..... 0

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

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

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

FlexConnect ACL Applied Status..... Unavailable  
IPv4 ACL Applied Status..... Unavailable  
IPv6 ACL Name..... none  
IPv6 ACL Applied Status..... Unavailable  
Layer2 ACL Name..... none  
Layer2 ACL Applied Status..... Unavailable  
Client Type..... SimpleIP  
mDNS Status..... Enabled  
mDNS Profile Name..... default-mdns-profile  
No. of mDNS Services Advertised..... 0  
Policy Type..... N/A  
Encryption Cipher..... None  
Protected Management Frame ..... No  
Management Frame Protection..... No  
EAP Type..... Unknown  
FlexConnect Data Switching..... Central  
FlexConnect Dhcp Status..... Central  
FlexConnect Vlan Based Central Switching..... No  
FlexConnect Authentication..... Central  
FlexConnect Central Association..... No  
Interface..... management  
VLAN..... 16  
Quarantine VLAN..... 0

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

Access VLAN..... 16  
Local Bridging VLAN..... 16  
Client Capabilities:  
    CF Pollable..... Not implemented  
    CF Poll Request..... Not implemented

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

Client Wifi Direct Capabilities:

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

Fast BSS Transition Details:

Client Statistics:

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

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

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

Client Rate Limiting Statistics:

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

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

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

Nearby AP Statistics:

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

antenna1: 25 secs ago..... -37 dBm  
AP1142-1(slot 1)  
antenna0: 25 secs ago..... -44 dBm  
antenna1: 25 secs ago..... -57 dBm  
DNS Server details:  
DNS server IP ..... 0.0.0.0

--More or (q)uit current module or <ctrl-z> to abort  
DNS server IP ..... 0.0.0.0

Assisted Roaming Prediction List details:

Client Dhcp Required: False

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).