

Esempio di configurazione dell'autenticazione Web con LDAP sui Wireless LAN Controller (WLC)

Sommario

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Convenzioni](#)

[Processo di autenticazione Web](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurare il server LDAP](#)

[Crea utenti nel controller di dominio](#)

[Creazione di un database utenti in un'unità organizzativa](#)

[Configurare l'utente per l'accesso LDAP](#)

[Binding anonimo](#)

[Abilita funzione di binding anonimo sul server Windows 2012 Essentials](#)

[Concessione all'utente dell'accesso ANONIMO](#)

[Concedi autorizzazione contenuto elenco nell'unità organizzativa](#)

[Binding autenticato](#)

[Concessione dei privilegi di amministratore a WLC-admin](#)

[Utilizzare LDP per identificare gli attributi utente](#)

[Configura WLC per server LDAP](#)

[Configurazione della WLAN per l'autenticazione Web](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare un controller WLC (Wireless LAN Controller) per l'autenticazione Web. Viene illustrato come configurare un server LDAP (Lightweight Directory Access Protocol) come database back-end per l'autenticazione Web in modo da recuperare le credenziali utente e autenticare l'utente.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza della configurazione dei Lightweight Access Point (LAP) e dei Cisco WLC
- Conoscenze di controllo e provisioning del protocollo CAPWAP (Wireless Access Point Protocol)
- Informazioni sull'impostazione e la configurazione di LDAP (Lightweight Directory Access Protocol), Active Directory e dei controller di dominio

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco 5508 WLC con firmware versione 8.2.100.0
- Cisco serie 1142 LAP
- Scheda client wireless Cisco 802.11a/b/g.
- Server Microsoft Windows 2012 Essentials che esegue il ruolo del server LDAP

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Convenzioni


Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.](#)

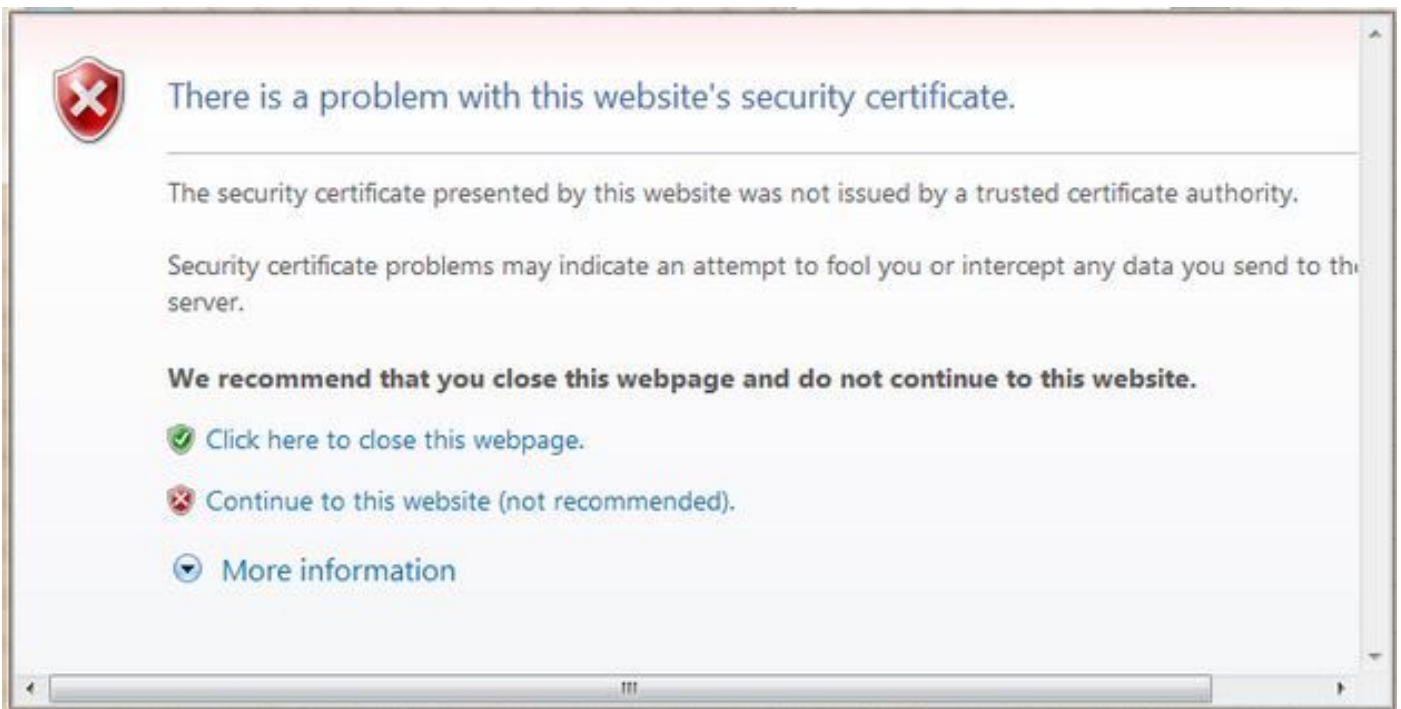
Processo di autenticazione Web

L'autenticazione Web è una funzione di sicurezza di livello 3 che impedisce al controller di autorizzare il traffico IP (ad eccezione dei pacchetti relativi a DHCP e DNS) da un determinato client fino a quando il client non ha fornito correttamente un nome utente e una password validi. Quando si utilizza l'autenticazione Web per autenticare i client, è necessario definire un nome utente e una password per ogni client. Quindi, quando i client tentano di collegarsi alla LAN wireless, devono immettere il nome utente e la password quando richiesto da una pagina di

accesso.

Quando l'autenticazione Web è abilitata (con protezione di livello 3), gli utenti ricevono occasionalmente un avviso di protezione del browser Web la prima volta che tentano di accedere a un URL.

-
-  Suggerimento: per rimuovere questo avviso di certificato, tornare alla guida seguente per installare un certificato attendibile di terze parti
<http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-certificates-wlc-00.html>
-



Dopo aver fatto clic su Sì per procedere (o più precisamente Continua con questo sito Web (non consigliato) per il browser Firefox, ad esempio), o se il browser del client non visualizza un avviso di protezione, il sistema di autenticazione Web reindirizza il client a una pagina di accesso, come mostrato nell'immagine:

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 pagina di accesso predefinita contiene un logo Cisco e un testo specifico per Cisco. È possibile scegliere di visualizzare nel sistema di autenticazione Web uno dei seguenti elementi:

- Pagina di accesso predefinita
- Una versione modificata della pagina di login predefinita
- Pagina di accesso personalizzata configurata su un server Web esterno
- Una pagina di accesso personalizzata che viene scaricata sul controller

Quando si immettono un nome utente e una password validi nella pagina di accesso per l'autenticazione Web e si fa clic su Invia, l'autenticazione viene eseguita in base alle credenziali inviate e all'autenticazione riuscita dal database backend (LDAP in questo caso). Il sistema di autenticazione Web visualizza quindi una pagina di login riuscita e reindirizza il client autenticato all'URL richiesto.

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 pagina di accesso riuscita predefinita contiene un puntatore a un indirizzo di gateway virtuale: <https://1.1.1.1/logout.html>. L'indirizzo IP impostato per l'interfaccia virtuale del controller funge da indirizzo di reindirizzamento per la pagina di accesso.

Questo documento spiega come usare la pagina Web interna sul WLC per l'autenticazione Web. In questo esempio viene utilizzato un server LDAP come database back-end per l'autenticazione Web per recuperare le credenziali utente e autenticare l'utente.

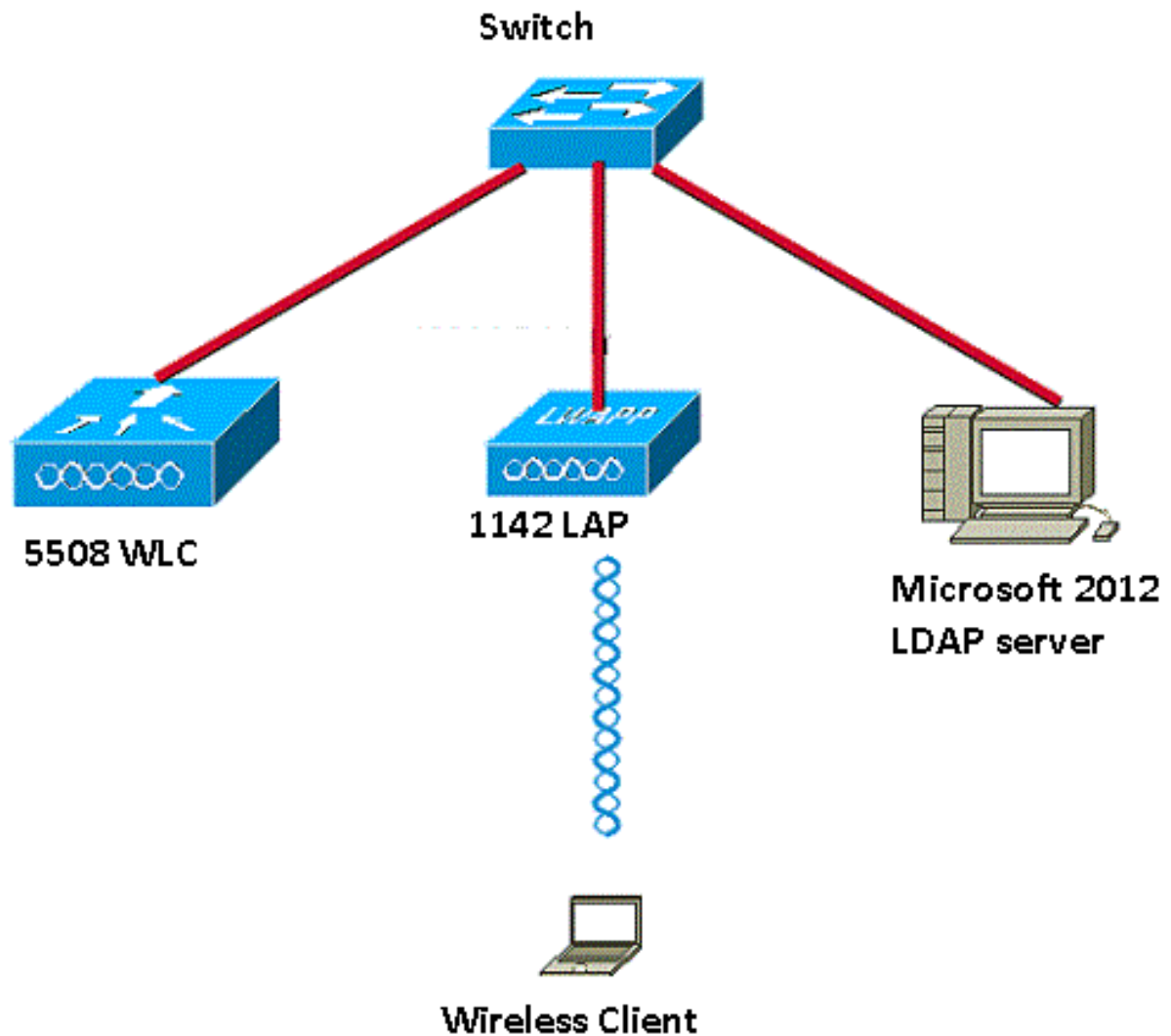
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

 Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

Esempio di rete

Il documento usa la seguente configurazione di rete:



Configurazioni

Per implementare correttamente l'impostazione, completare i seguenti passaggi:

- [Configurare il server LDAP.](#)
- [Configurare WLC per il server LDAP.](#)
- [Configurare la WLAN per l'autenticazione Web.](#)

Configurare il server LDAP

Il primo passaggio consiste nella configurazione del server LDAP, che funge da database back-end per memorizzare le credenziali utente dei client wireless. In questo esempio, il server Microsoft Windows 2012 Essentials viene utilizzato come server LDAP.

Il primo passo nella configurazione del server LDAP consiste nel creare un database utenti sul server LDAP in modo che il WLC possa eseguire una query su questo database per autenticare l'utente.

Crea utenti nel controller di dominio

Un'unità organizzativa (OU, Organizational Unit) contiene più gruppi che contengono riferimenti a voci personali in un profilo persona. Una persona può essere membro di più gruppi. Tutte le definizioni delle classi oggetto e degli attributi sono predefinite dello schema LDAP. Ogni gruppo contiene riferimenti (dn) per ogni persona che vi appartiene.

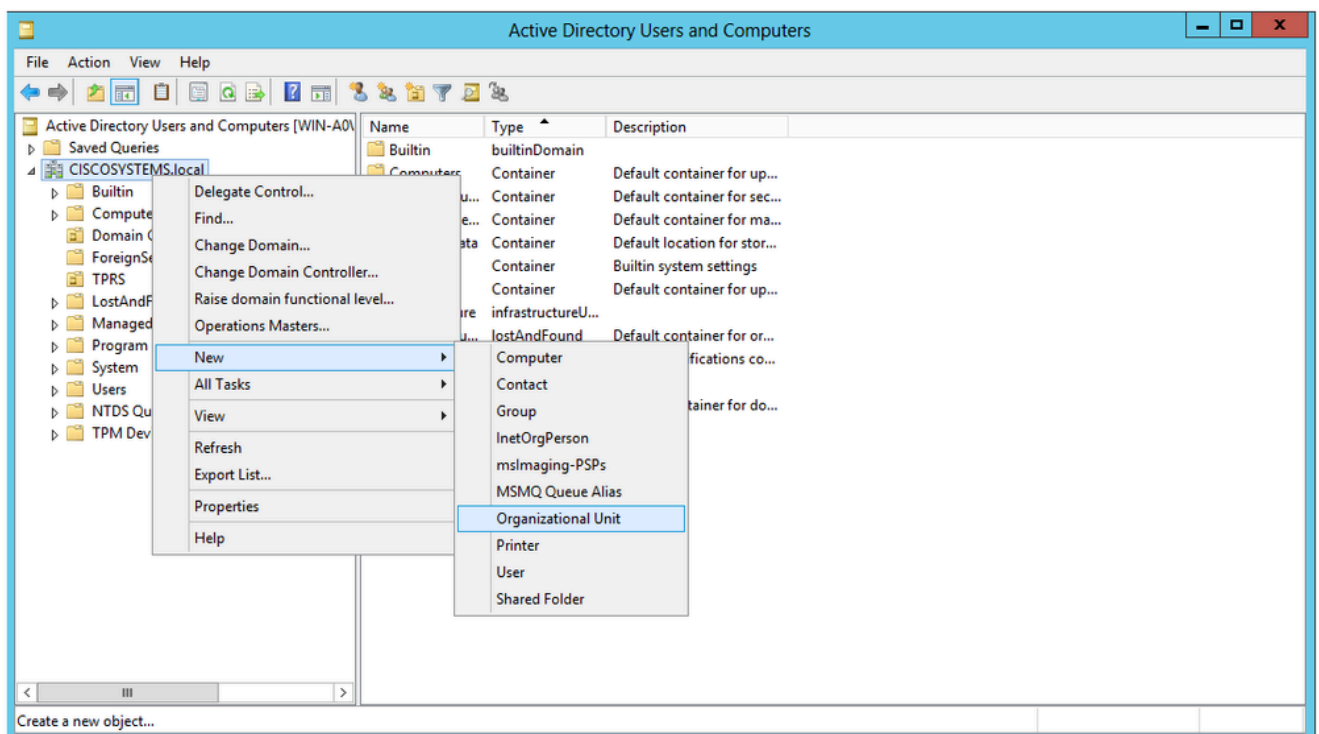
In questo esempio viene creata una nuova unità organizzativa LDAP-USERS e l'utente User1 viene creato in questa unità organizzativa. Quando si configura questo utente per l'accesso LDAP, il WLC può eseguire una query in questo database LDAP per l'autenticazione dell'utente.

Il dominio utilizzato in questo esempio è CISCOSYSTEMS.local.

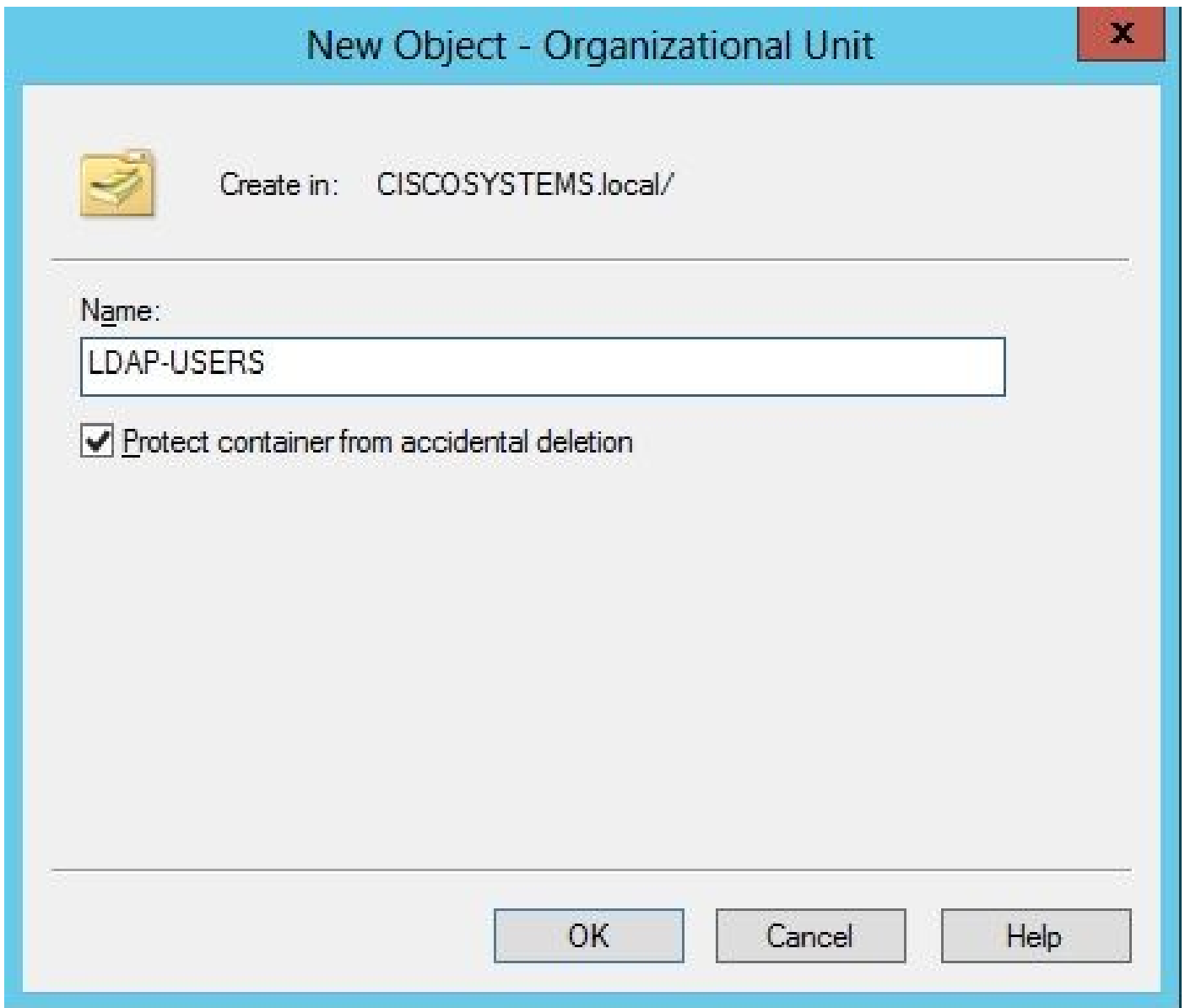
Creazione di un database utenti in un'unità organizzativa

In questa sezione viene illustrato come creare una nuova unità organizzativa nel dominio e creare un nuovo utente in questa unità organizzativa.

1. Aprire Windows PowerShell e digitare servermanager.exe
2. Nella finestra Server Manager fare clic su Servizi di dominio Active Directory. Fare quindi clic con il pulsante destro del mouse sul nome del server per scegliere Utenti e computer di Active Directory.
3. Fare clic con il pulsante destro del mouse sul nome di dominio, che in questo esempio è CISCOSYSTEMS.local, quindi selezionare Nuovo > Unità organizzativa dal menu di scelta rapida per creare una nuova unità organizzativa.

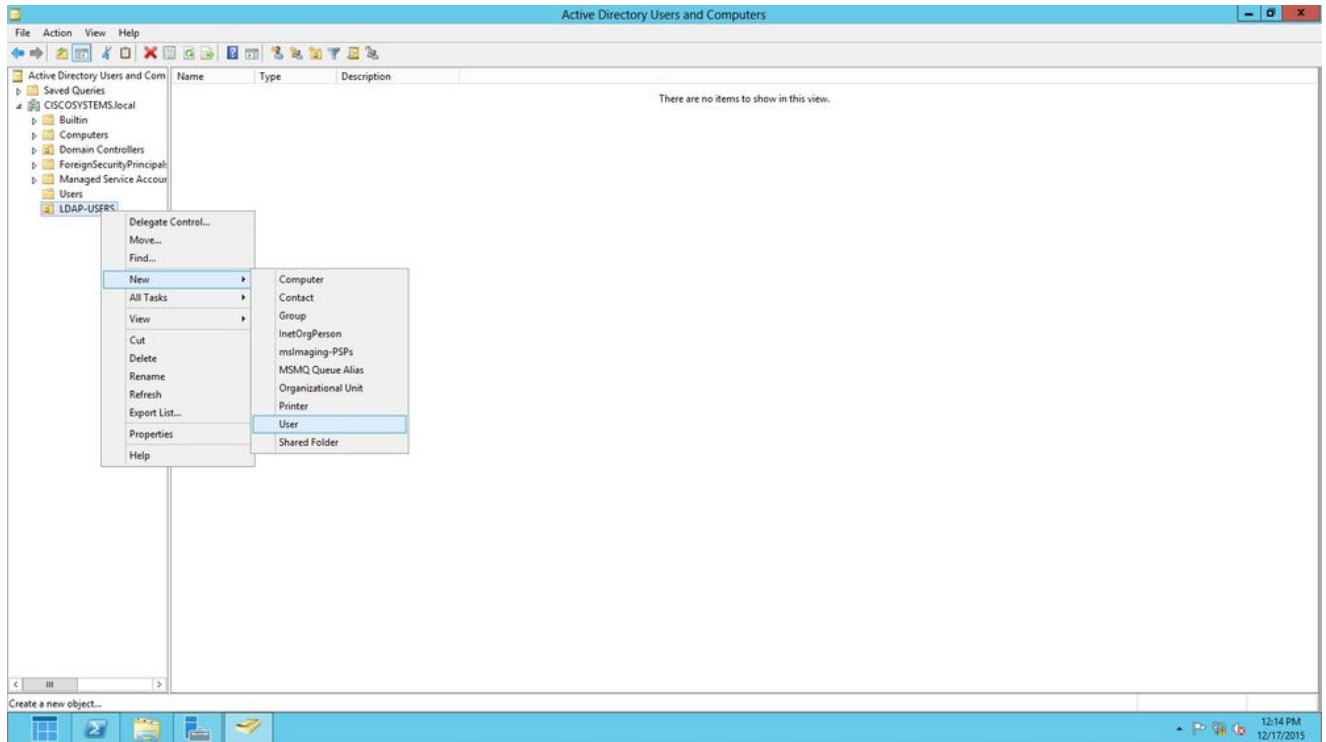


4. Assegnare un nome all'unità organizzativa e fare clic su OK, come mostrato nell'immagine:



Ora che la nuova unità organizzativa LDAP-USERS viene creata sul server LDAP, il passaggio successivo consiste nella creazione dell'utente User1 in questa unità organizzativa. A tale scopo, effettuare i seguenti passaggi:

1. Fare clic con il pulsante destro del mouse sulla nuova unità organizzativa creata. Passare a LDAP-USERS> Nuovo > Utente dai menu di scelta rapida risultanti per creare un nuovo utente, come mostrato nell'immagine:



2. Nella pagina Impostazione utente, compilare i campi obbligatori come illustrato in questo esempio. In questo esempio, il campo Nome di accesso utente contiene User1.

Nome utente verificato nel database LDAP per autenticare il client. In questo esempio viene utilizzato User1 nei campi Nome e Nome completo. Fare clic su Next (Avanti).

New Object - User X

 Create in: CISCO SYSTEMS.local/LDAP-USERS

First name: Initials:

Last name:

Full name:

User logon name:
 ▾

User logon name (pre-Windows 2000):

3. Immettere una password e confermarla. Selezionare l'opzione Nessuna scadenza password e fare clic su Avanti.

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

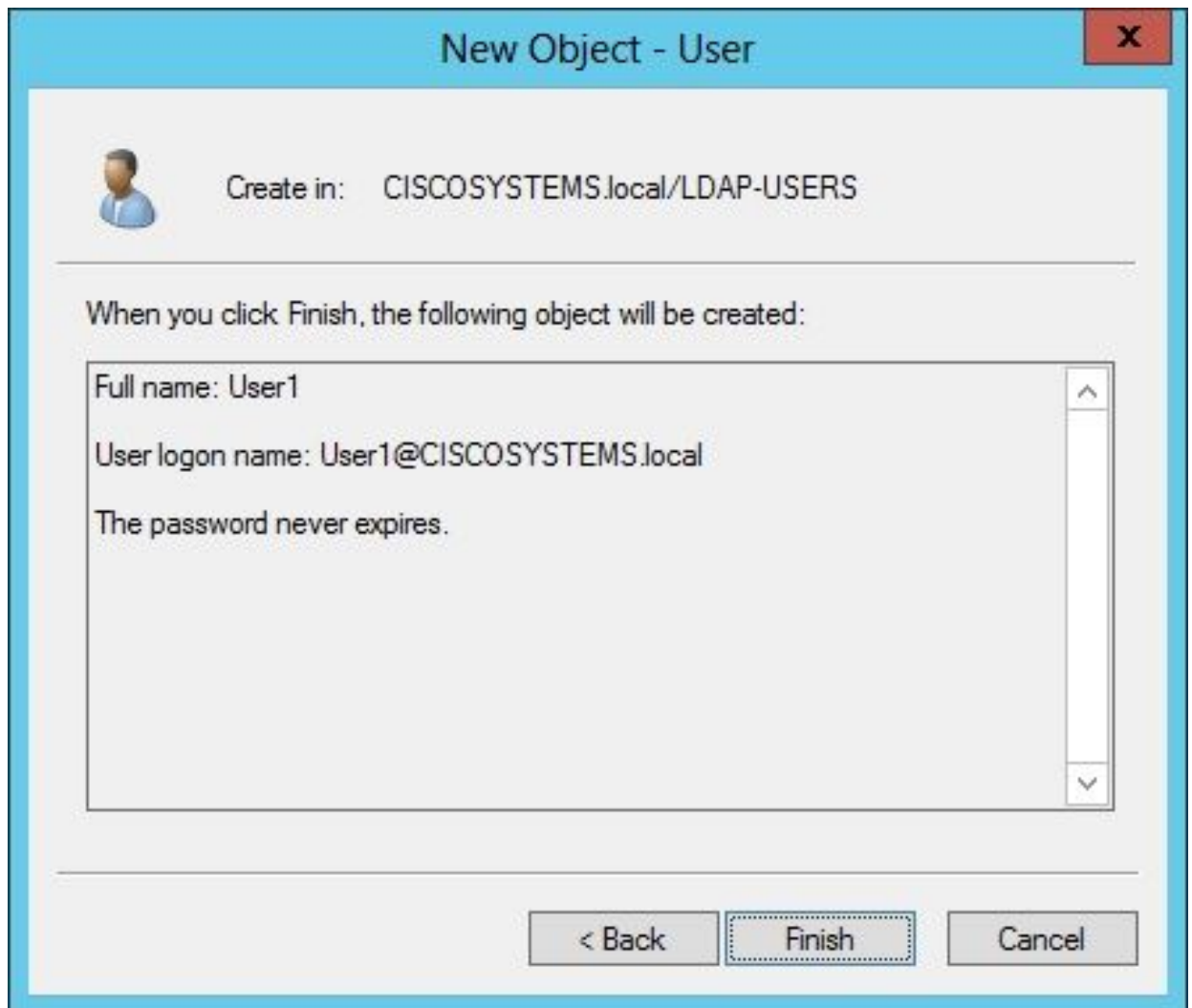
Password never expires

Account is disabled

4. Fare clic su Finish (Fine).

Viene creato un nuovo utente User1 nell'unità organizzativa LDAP-USERS. Credenziali utente:

- nome utente: User1
- password: Portatile123




Ora che l'utente è stato creato in un'unità organizzativa, il passaggio successivo consiste nel configurare l'utente per l'accesso LDAP.

Configurare l'utente per l'accesso LDAP

È possibile scegliere Anonimo o Autenticato per specificare il metodo di associazione dell'autenticazione locale per il server LDAP. Il metodo Anonymous consente l'accesso anonimo al server LDAP. Il metodo Authenticated richiede l'immissione di un nome utente e di una password per l'accesso sicuro. Il valore predefinito è Anonimo.

In questa sezione viene illustrato come configurare i metodi Anonymous e Authenticated.

Binding anonimo

 **Nota:** si consiglia di non utilizzare l'associazione anonima. Un server LDAP che consente il binding anonimo non richiede alcun tipo di autenticazione con credenziali. Un utente non autorizzato potrebbe sfruttare la voce di binding anonimo per visualizzare i file sul director LDAP.

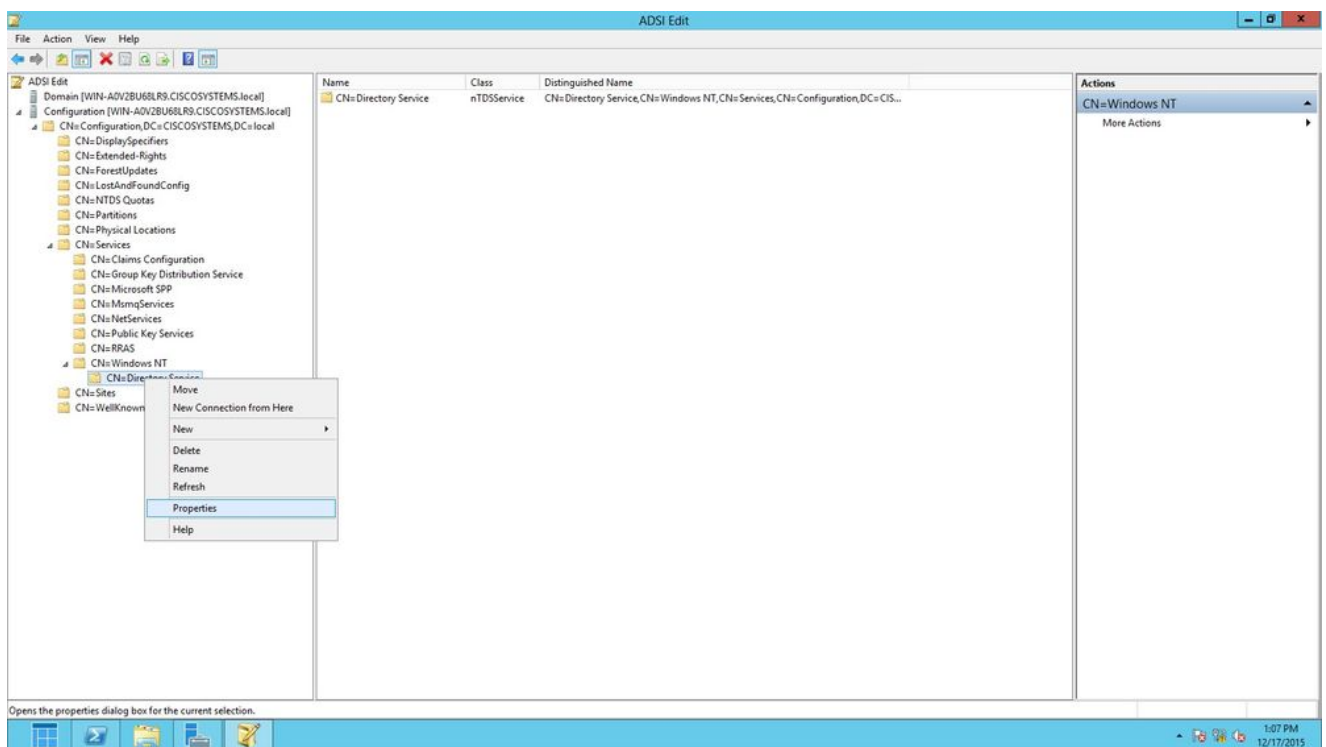
Eseguire la procedura descritta in questa sezione per configurare l'accesso LDAP per l'utente anonimo.

Abilita funzione di binding anonimo sul server Windows 2012 Essentials


Affinché le applicazioni di terze parti (nel nostro caso WLC) possano accedere a Windows 2012 AD su LDAP, è necessario abilitare la funzione di binding anonimo su Windows 2012. Per impostazione predefinita, le operazioni LDAP anonime non sono consentite nei controller di dominio di Windows 2012. Per abilitare la funzione Associazione anonima, effettuare le seguenti operazioni:


1. Avviare lo strumento Modifica ADSI digitando: ADSIEdit.msc in Windows PowerShell. Questo strumento fa parte degli strumenti di supporto di Windows 2012.
2. Nella finestra Modifica ADSI, espandere il dominio radice (Configuration [WIN-A0V2BU68LR9.CISCOSYSTEMS.local]).

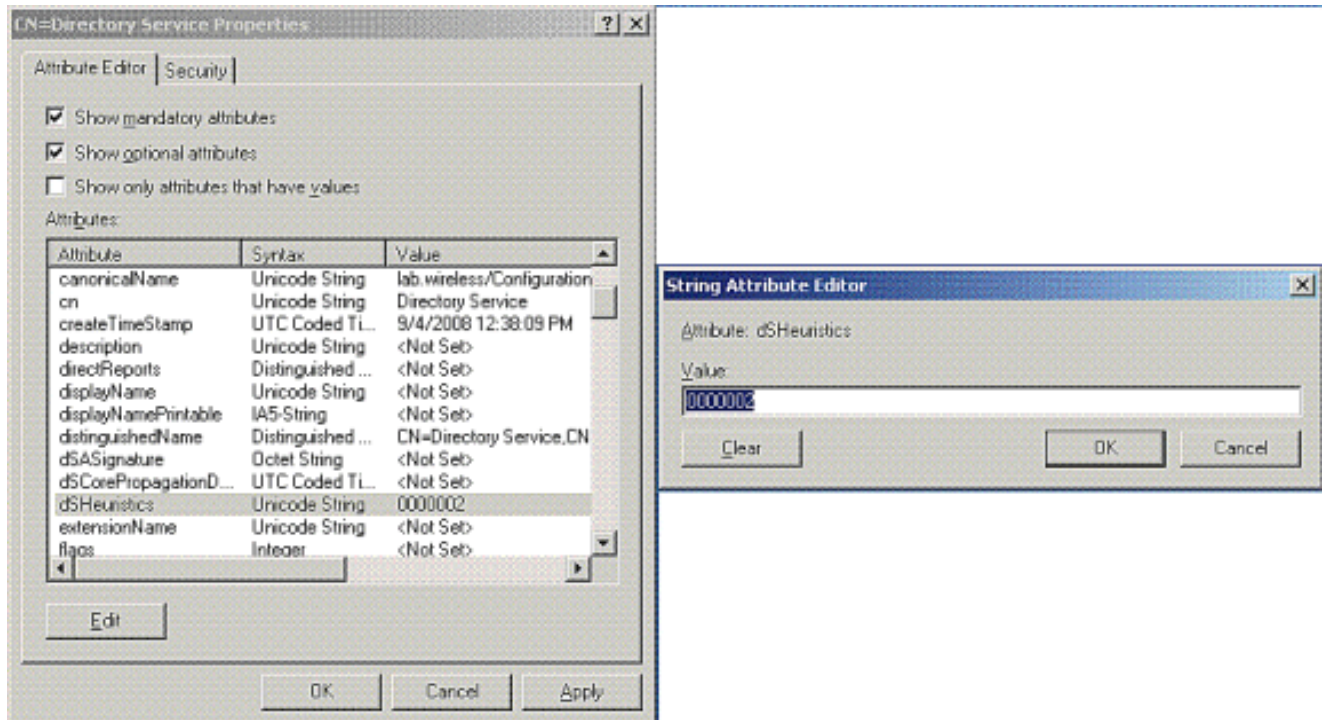
Passare a CN=Servizi > CN=Windows NT > CN=Servizio directory. Fare clic con il pulsante destro del mouse sul contenitore CN=Directory Service e scegliere Proprietà dal menu di scelta rapida, come mostrato nell'immagine:



3. Nella finestra CN=Directory Service Properties, in Attributi, fare clic sull'attributo dsEuristics nel campo Attributo e scegliere Modifica. Nella finestra Editor attributi stringa di questo attributo, immettere il valore 0000002; fare clic su Apply (Applica) e su OK, come mostrato nell'immagine. La funzionalità Binding anonimo è attivata nel server Windows 2012.

 Nota: l'ultimo (settimo) carattere controlla il modo in cui è possibile eseguire l'associazione al servizio LDAP. 0 (zero) o nessun settimo carattere indica che le

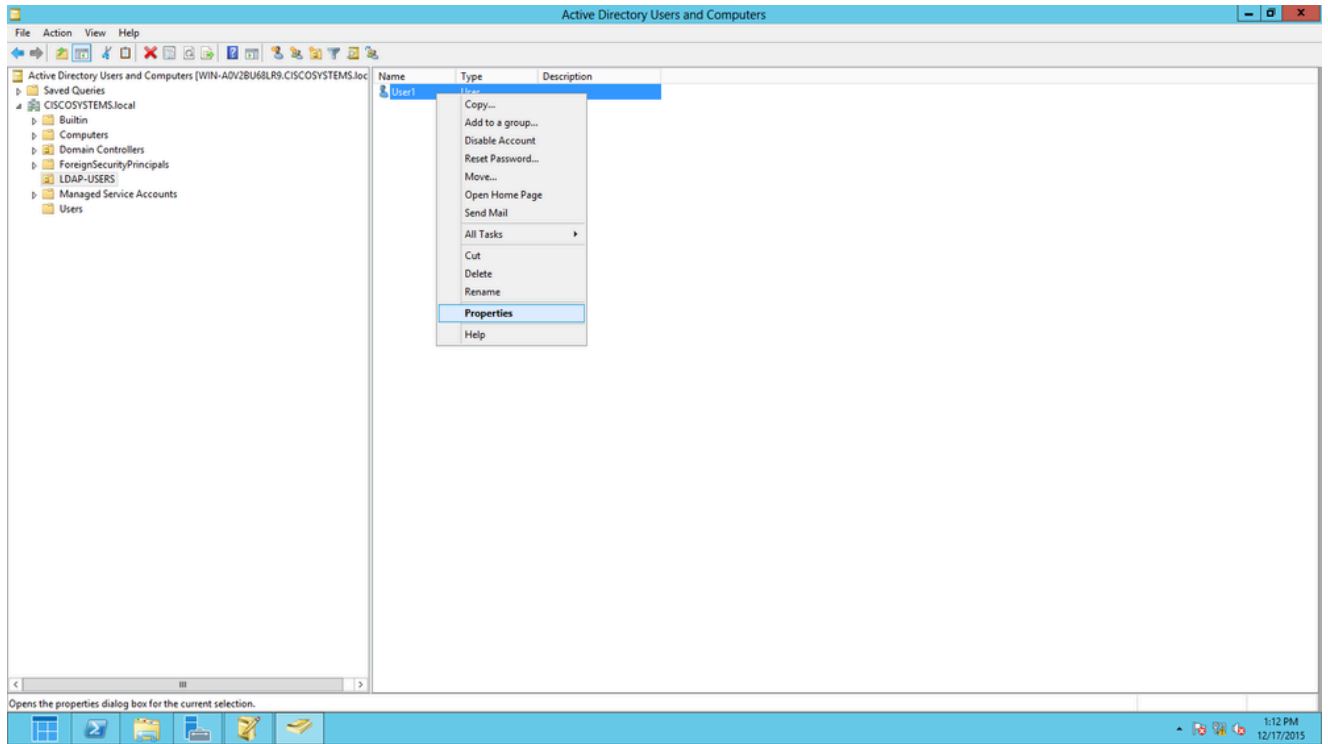
-  operazioni LDAP anonime sono disabilitate. Se si imposta il settimo carattere su 2, viene attivata la funzione Associazione anonima.



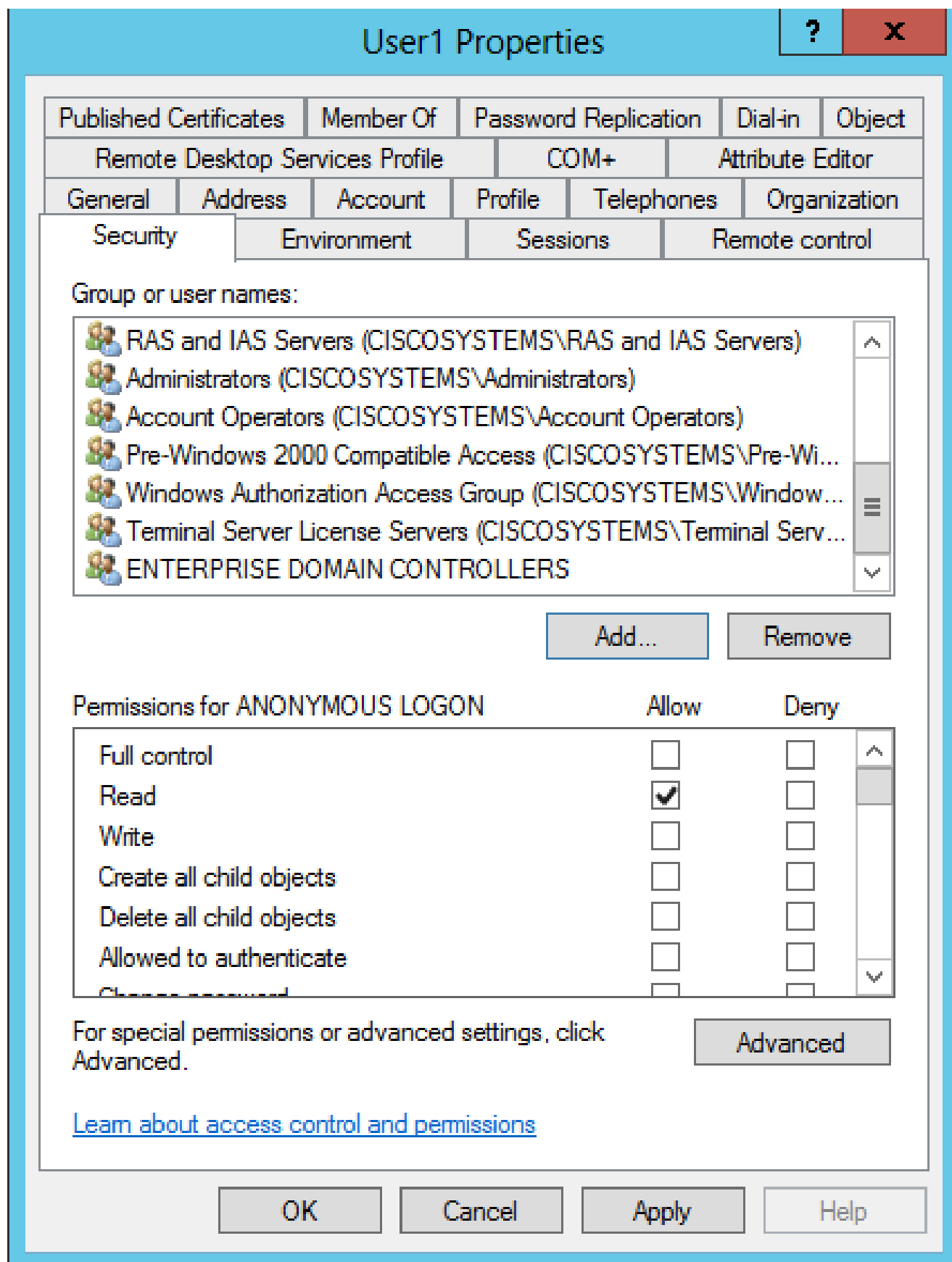
Concessione all'utente dell'accesso ANONIMO

Il passaggio successivo consiste nel concedere l'accesso ANONIMO all'utente User1. A tale scopo, completare i seguenti passaggi:

1. Aprire Utenti e computer di Active Directory.
2. Accertarsi che l'opzione Visualizza gruppi di facce avanzati sia selezionata.
3. Individuare l'utente User1 e fare clic con il pulsante destro del mouse su di esso. Scegliere Proprietà dal menu di scelta rapida. Questo utente è identificato dal nome Utente1.



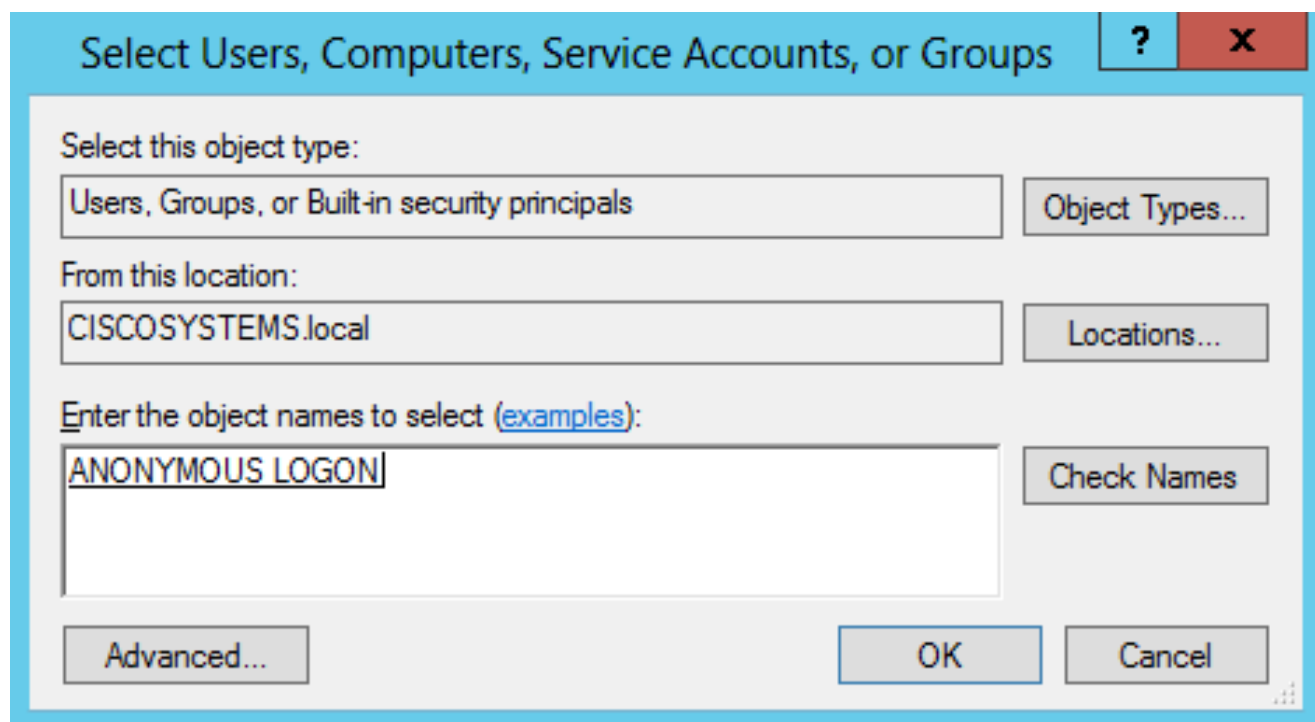
4. Fare clic sulla scheda Protezione, come illustrato nell'immagine:



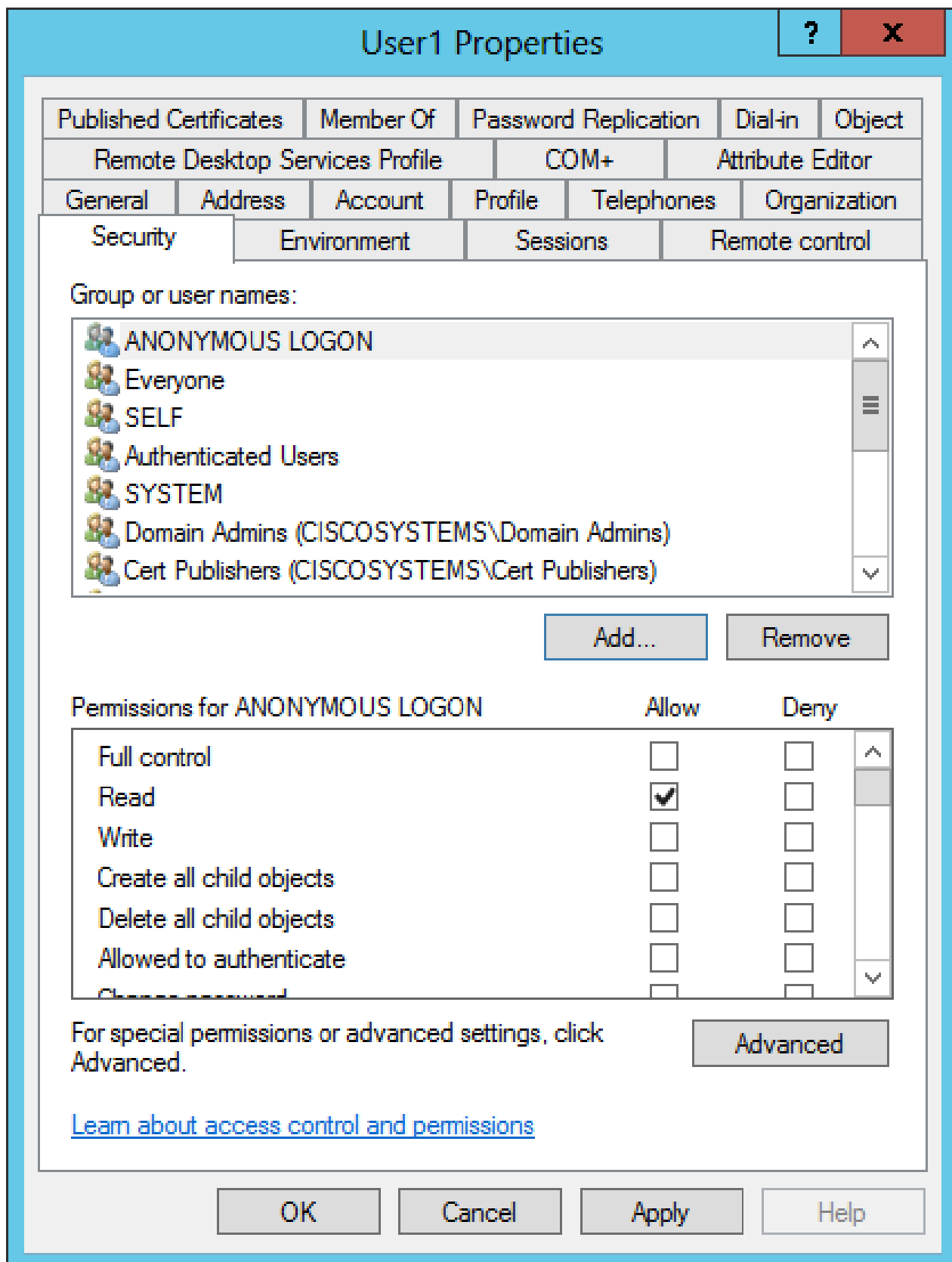
5. Fare clic su Add nella finestra risultante.

6. Immettere ACCESSO ANONIMO nella casella Immettere i nomi degli oggetti da selezionare

e confermare la finestra di dialogo, come mostrato nell'immagine:



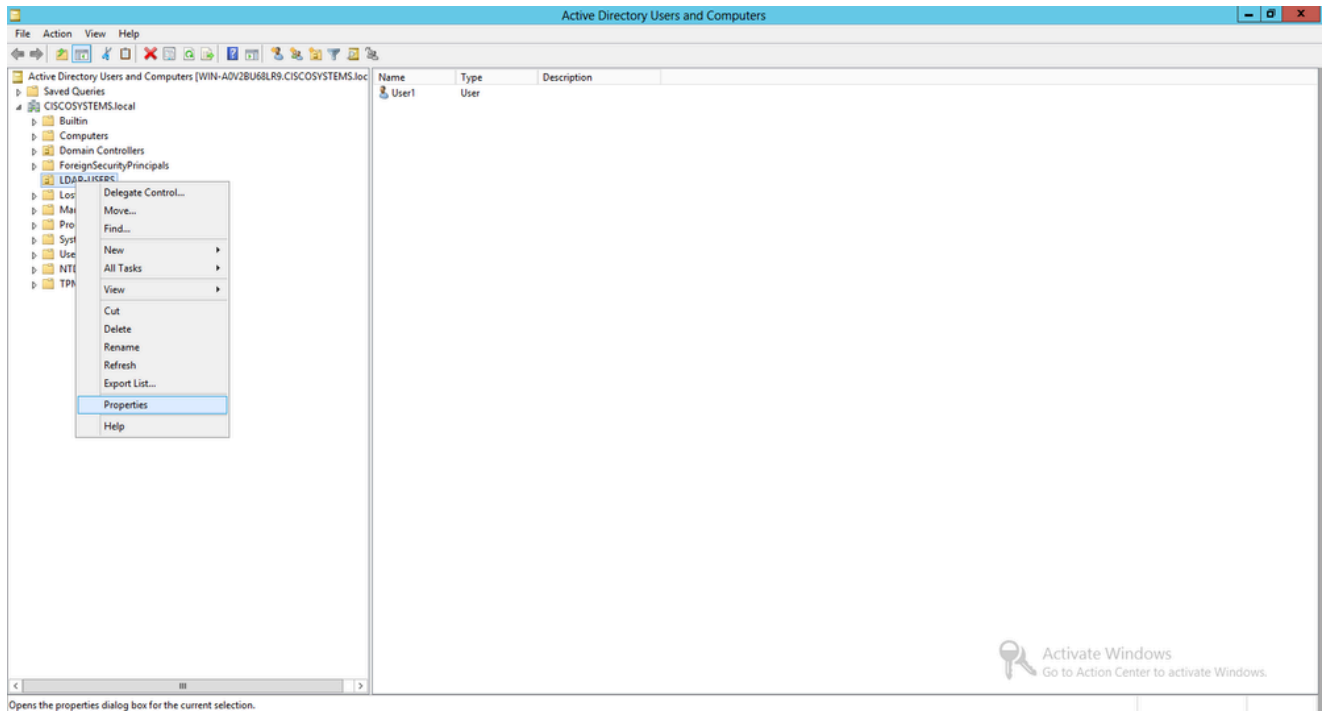
7. Nell'ACL, notare che ACCESSO ANONIMO ha accesso ad alcuni insiemi di proprietà dell'utente. Fare clic su OK. L'accesso ANONIMO è concesso a questo utente, come mostrato nell'immagine:



Concedi autorizzazione contenuto elenco nell'unità organizzativa

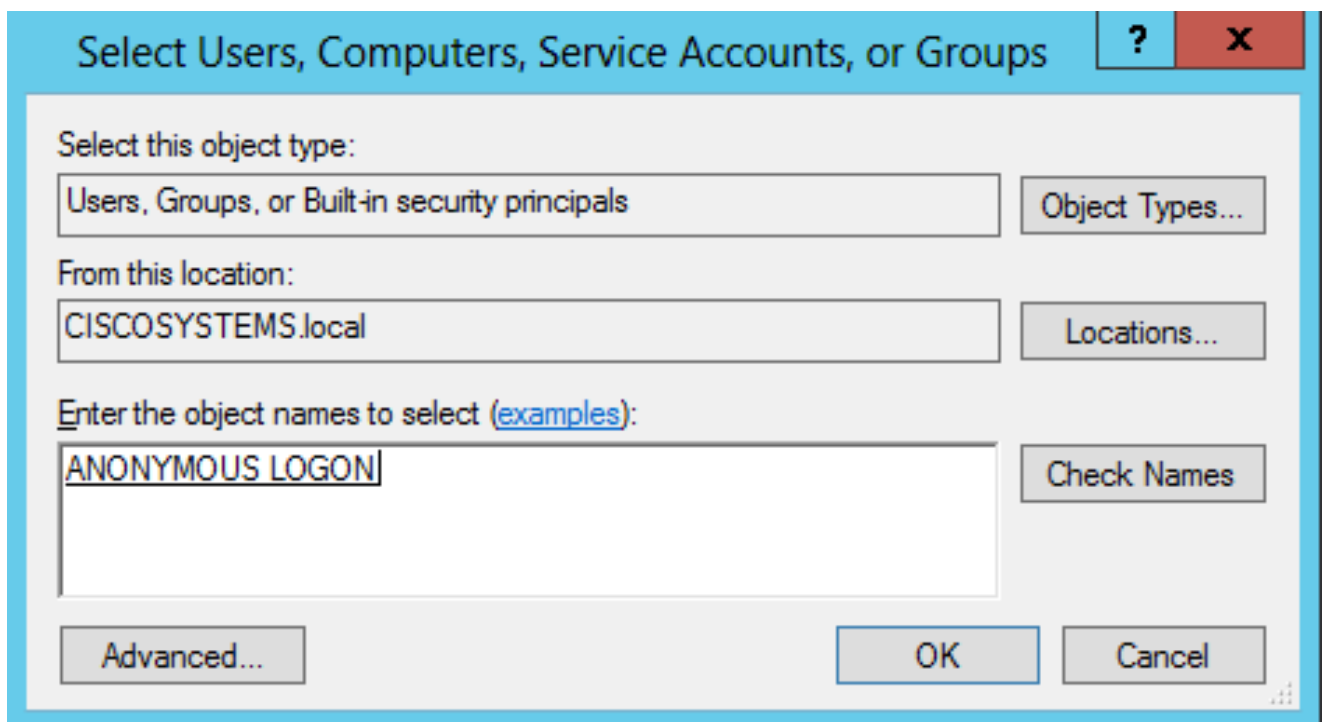
Il passaggio successivo consiste nel concedere almeno l'autorizzazione Elenco contenuti all'accesso ANONIMO all'unità organizzativa in cui si trova l'utente. In questo esempio, User1 si trova nell'unità organizzativa LDAP-USERS. A tale scopo, completare i seguenti passaggi:

1. In Utenti e computer di Active Directory, fare clic con il pulsante destro del mouse su OU LDAP-USERS e scegliere Proprietà, come mostrato nell'immagine:



2. Fare clic su Protezione.

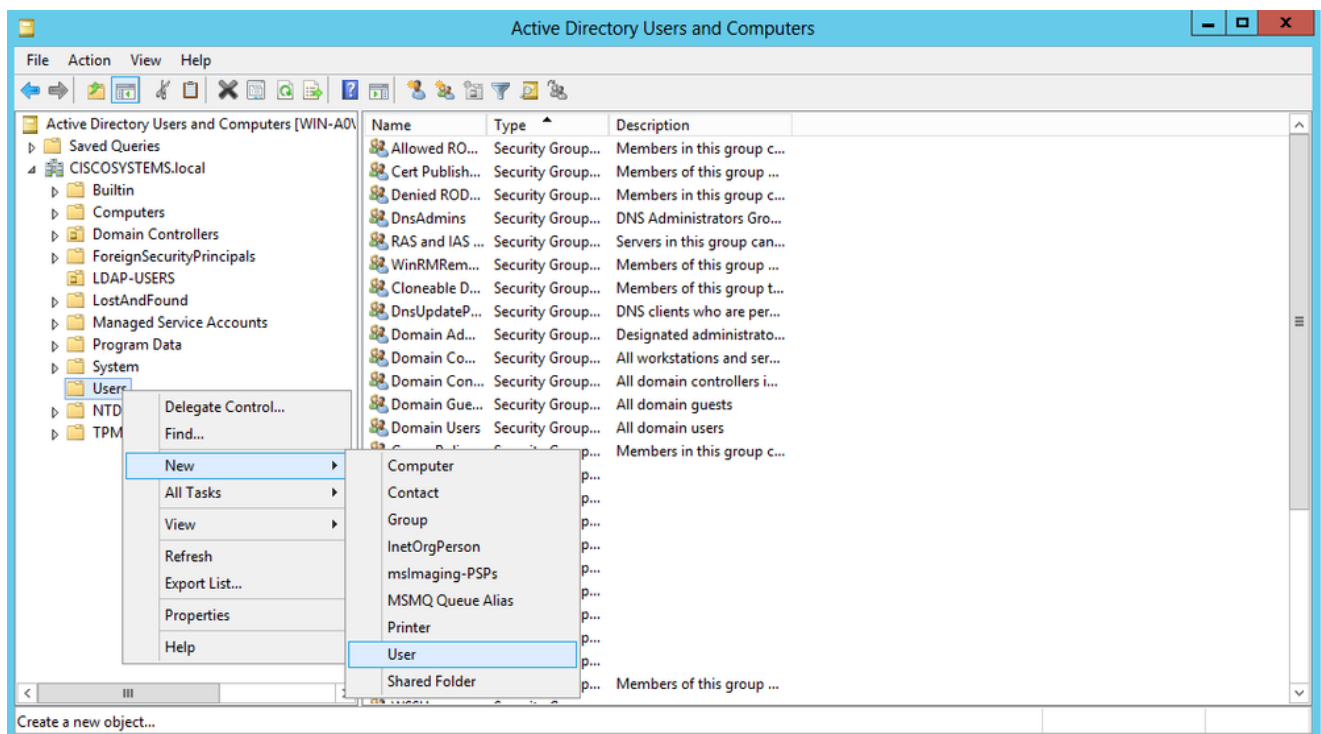
3. Fare clic su Add. Nella finestra di dialogo visualizzata, immettere ANONYMOUS LOGON (ACCESSO ANONIMO) e Confermare la finestra di dialogo, come mostrato nell'immagine:



Binding autenticato

Eseguire la procedura descritta in questa sezione per configurare un utente per l'autenticazione locale sul server LDAP.

1. Aprire Windows PowerShell e digitare servermanager.exe
2. Nella finestra Server Manager fare clic su Servizi di dominio Active Directory. Fare quindi clic con il pulsante destro del mouse sul nome del server per scegliere Utenti e computer di Active Directory.
3. Fare clic con il pulsante destro del mouse su Utenti. Passare a Nuovo > Utente dai menu di scelta rapida risultanti per creare un nuovo utente.



4. Nella pagina Impostazione utente, compilare i campi obbligatori come illustrato in questo esempio. In questo esempio, il campo WLC-admin del nome di accesso dell'utente è. Il nome utente da utilizzare per l'autenticazione locale al server LDAP. Fare clic su Next (Avanti).
5. Immettere una password e confermarla. Selezionare l'opzione Nessuna scadenza password e fare clic su Avanti.
6. Fare clic su Finish (Fine).

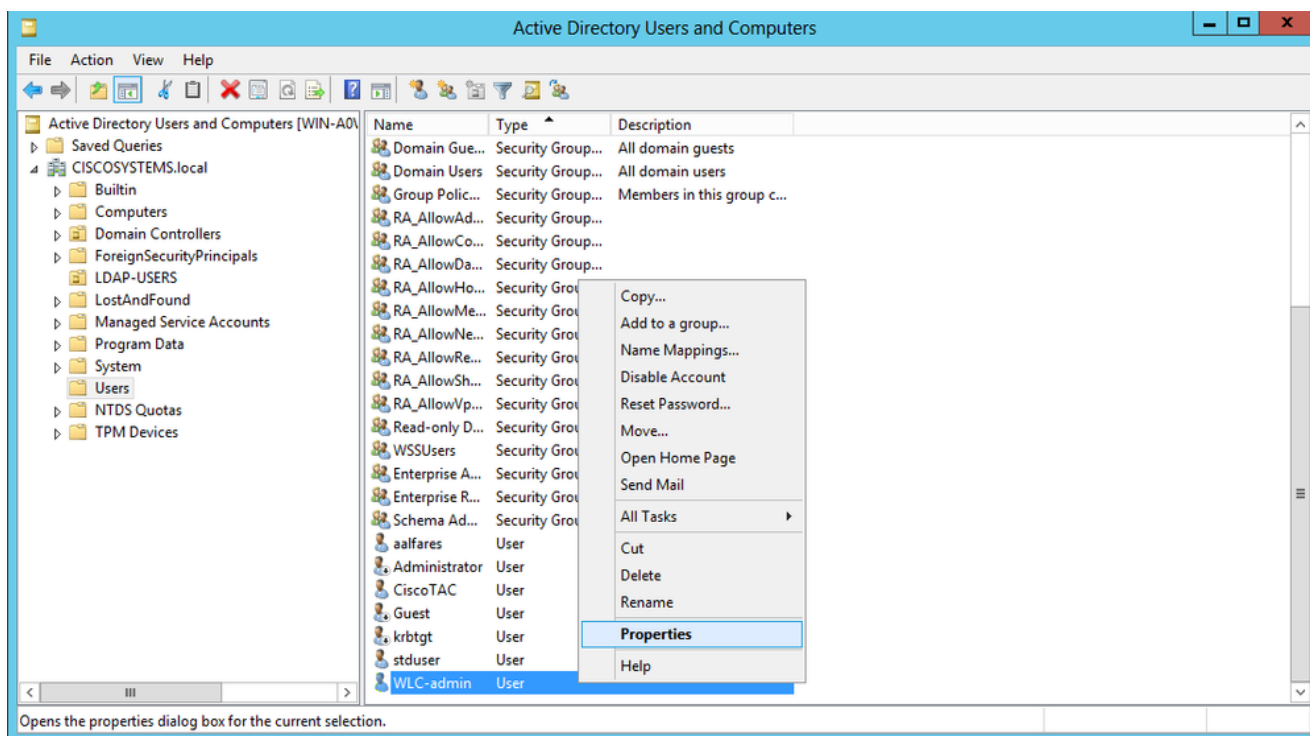
Viene creato un nuovo utente WLC-admin nel contenitore Users. Credenziali utente:

- nome utente: WLC-admin
- password: Admin123

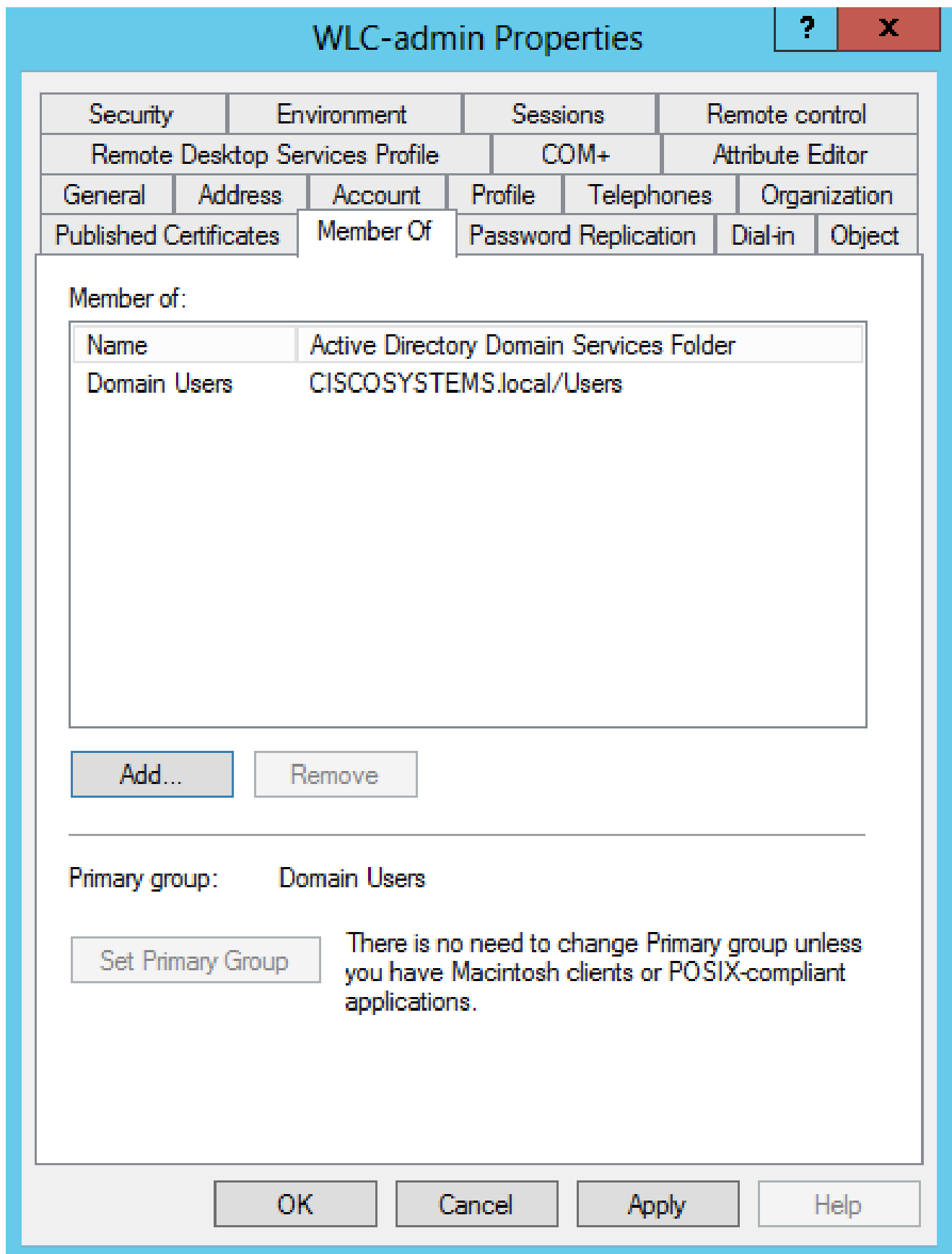
Concessione dei privilegi di amministratore a WLC-admin

Dopo la creazione dell'utente di autenticazione locale, è necessario concedergli i privilegi di amministratore. A tale scopo, completare i seguenti passaggi:

1. Aprire Utenti e computer di Active Directory.
2. Accertarsi che l'opzione Visualizza gruppi di facce avanzati sia selezionata.
3. Passare all'utente WLC-admin e fare clic con il pulsante destro del mouse su di esso. Scegliere Proprietà dal menu di scelta rapida, come illustrato nell'immagine. Questo utente è identificato dal nome WLC-admin.

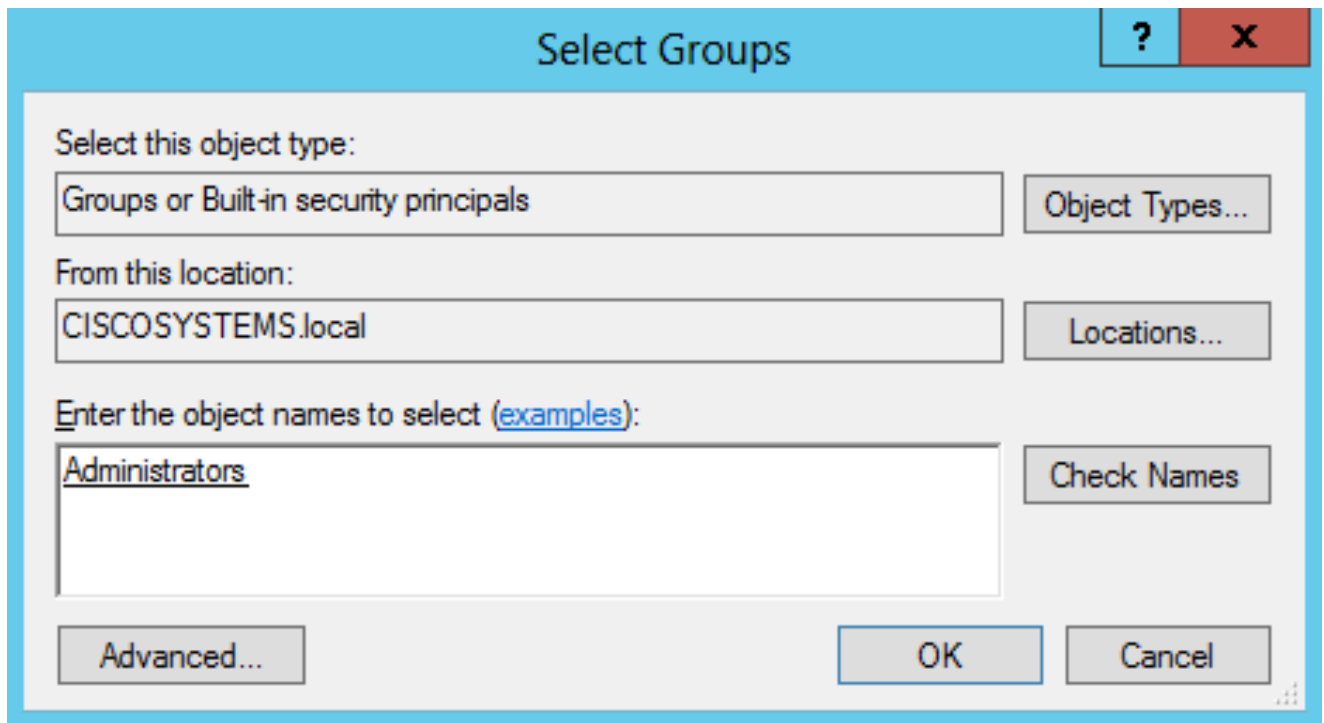


4. Fare clic sulla scheda Member of, come mostrato nell'immagine:



::

5. Fare clic su Add. Nella finestra di dialogo visualizzata, immettere Administrators e fare clic su OK, come mostrato nell'immagine:

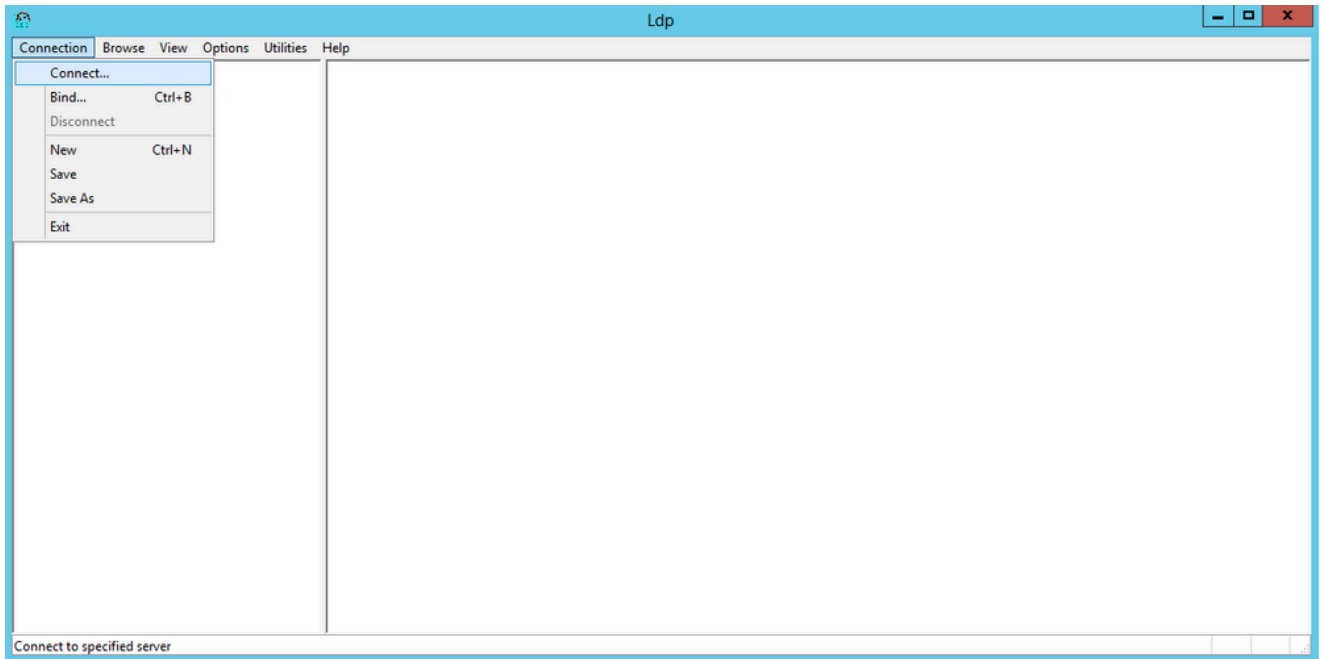


Utilizzare LDP per identificare gli attributi utente

Questo strumento GUI è un client LDAP che consente agli utenti di eseguire operazioni quali la connessione, il binding, la ricerca, la modifica, l'aggiunta o l'eliminazione in qualsiasi directory compatibile con LDAP, ad esempio Active Directory. LDP viene utilizzato per visualizzare gli oggetti archiviati in Active Directory insieme ai relativi metadati, ad esempio i descrittori di protezione e i metadati di replica.

Lo strumento LDP GUI è incluso quando si installano gli strumenti di supporto di Windows Server 2003 dal CD del prodotto. Questa sezione spiega come utilizzare l'utility LDP per identificare gli attributi specifici associati all'utente User1. Alcuni di questi attributi vengono utilizzati per compilare i parametri di configurazione del server LDAP sul WLC, ad esempio il tipo di attributo utente e il tipo di oggetto utente.

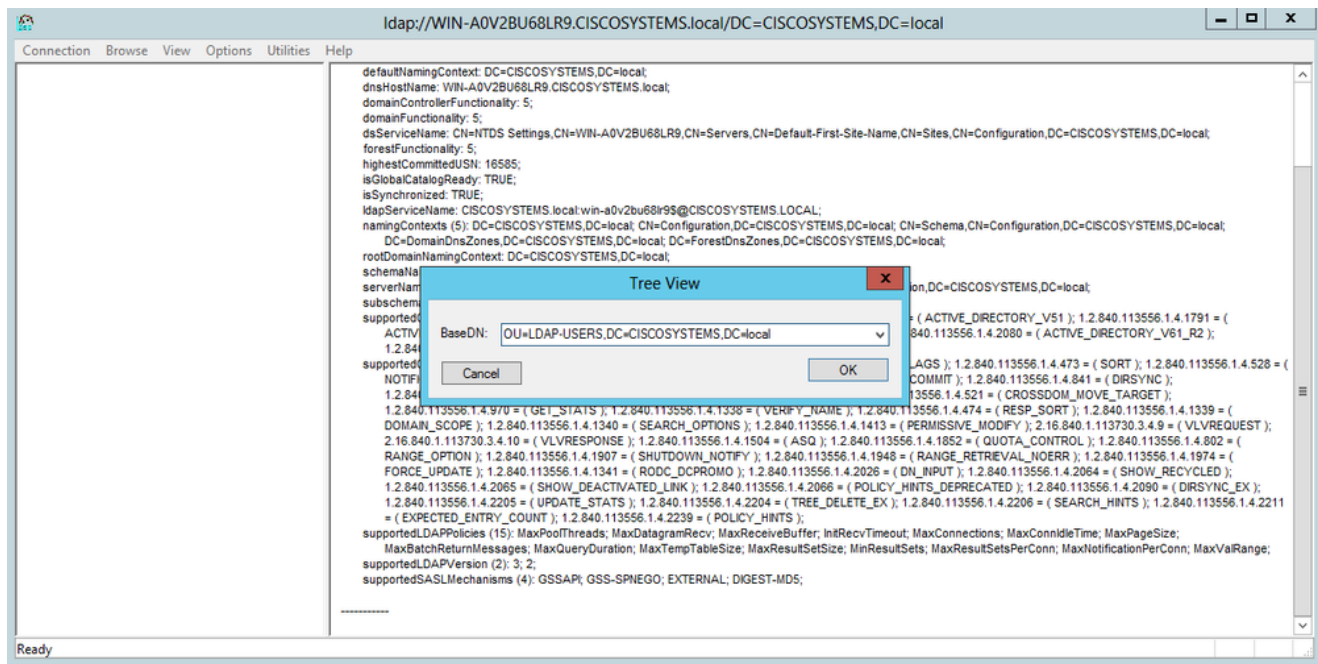
1. Sul server Windows 2012 (anche sullo stesso server LDAP), aprire Windows PowerShell e immettere LDP per accedere al browser LDP.
2. Nella finestra principale di LDP, selezionare Connessione > Connetti e connettersi al server LDAP quando si immette l'indirizzo IP del server LDAP, come mostrato nell'immagine.



3. Una volta connessi al server LDAP, scegliere Visualizza dal menu principale e fare clic su Albero, come mostrato nell'immagine:



4. Nella finestra Visualizzazione struttura risultante, immettere il nome distintoBase dell'utente. In questo esempio, l'utente 1 si trova nell'unità organizzativa "LDAP-USERS" nel dominio CISCOSYSTEMS.local. Fare clic su OK, come mostrato nell'immagine:



5. Sul lato sinistro del browser LDP viene visualizzata l'intera struttura sotto il nome di dominio di base specificato (OU=LDAP-USERS, dc=CISCOYSTEMS, dc=local). Espandere la struttura per individuare l'utente User1. Questo utente può essere identificato con il valore CN che rappresenta il nome dell'utente. In questo esempio, è CN=User1. Fare doppio clic su CN=User1. Nel riquadro a destra del browser LDP, LDP visualizza tutti gli attributi associati a User1, come mostrato nell'immagine:




6. Quando si configura il WLC per il server LDAP, nel campo Attributo utente immettere il nome dell'attributo nel record utente che contiene il nome utente. Da questo output LDP, è possibile vedere che sAMAccountName è un attributo che contiene il nome utente "User1", quindi immettere l'attributo sAMAccountName che corrisponde al campo Attributo utente sul WLC.

7. Quando si configura il WLC per il server LDAP, nel campo Tipo oggetto utente immettere il valore dell'attributo objectType LDAP che identifica il record come utente. I record utente dispongono spesso di diversi valori per l'attributo objectType, alcuni dei quali sono univoci per l'utente e altri sono condivisi con altri tipi di oggetto. Nell'output LDP, CN=Person è un valore che identifica il record come utente, quindi specificare Person come attributo User Object Type sul WLC.

Il passaggio successivo consiste nel configurare il WLC per il server LDAP.

Configura WLC per server LDAP

Una volta configurato il server LDAP, il passaggio successivo consiste nel configurare il WLC con i dettagli del server LDAP. Completare questi passaggi sull'interfaccia utente grafica del WLC:

 Nota: in questo documento si presume che il WLC sia configurato per il funzionamento di base e che i LAP siano registrati sul WLC. Se si è un nuovo utente che desidera configurare il WLC per il funzionamento di base con i LAP, fare riferimento alla [registrazione di un Lightweight AP \(LAP\) su un Wireless LAN Controller \(WLC\)](#).

1. Nella pagina Sicurezza del WLC, scegliere AAA > LDAP dal riquadro attività a sinistra per passare alla pagina di configurazione del server LDAP.



The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'SECURITY' tab is active. On the left, the 'Security' menu is expanded to 'AAA', which is further expanded to 'LDAP'. The main content area is titled 'LDAP Servers' and contains a table with the following data:

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

Per aggiungere un server LDAP, fare clic su Nuovo. Viene visualizzata la pagina Server LDAP > Nuovo.

2. Nella pagina Server LDAP: Modifica, specificare i dettagli del server LDAP, ad esempio l'indirizzo IP del server LDAP, il numero di porta, lo stato Abilita server e così via.

- Scegliere un numero dalla casella a discesa Indice server (priorità) per specificare l'ordine di priorità del server rispetto agli altri server LDAP configurati. È possibile configurare fino a diciassette server. Se il controller non riesce a raggiungere il primo server, proverà con il secondo nell'elenco e così via.
- Immettere l'indirizzo IP del server LDAP nel campo Indirizzo IP server.
- Immettere il numero di porta TCP del server LDAP nel campo Port Number (Numero

porta). L'intervallo valido è compreso tra 1 e 65535 e il valore predefinito è 389.

- per il binding Semplice, è stato utilizzato Autenticato, per il nome utente di binding, ovvero la posizione dell'utente amministratore WLC che verrà utilizzato per accedere al server LDAP e alla relativa password
- Nel campo DN base utente, immettere il nome distinto (DN) della sottostruttura nel server LDAP che contiene un elenco di tutti gli utenti. Ad esempio, ou=unità organizzativa, ou=unità organizzativa successiva e o=corporation.com. Se la struttura che contiene gli utenti è il DN di base, immettere o=corporation.com o dc=corporation, dc=com.

In questo esempio, l'utente si trova sotto l'unità organizzativa LDAP-USERS, che, a sua volta, viene creata come parte del dominio lab.wireless.

Il DN di base dell'utente deve puntare al percorso completo in cui si trovano le informazioni utente (credenziali utente in base al metodo di autenticazione EAP-FAST). In questo esempio, l'utente si trova nel DN di base OU=LDAP-USERS, DC=CISCOSYSTEMS, DC=local.

- Nel campo Attributo utente, immettere il nome dell'attributo nel record utente che contiene il nome utente.

Nel campo Tipo oggetto utente immettere il valore dell'attributo objectType LDAP che identifica il record come utente. I record utente dispongono spesso di diversi valori per l'attributo objectType, alcuni dei quali sono univoci per l'utente e altri sono condivisi con altri tipi di oggetto

È possibile ottenere il valore di questi due campi dal server delle directory con l'utilità del browser LDAP inclusa negli strumenti di supporto di Windows 2012. Questo strumento del browser LDAP Microsoft è denominato LDP. Con l'aiuto di questo strumento, è possibile conoscere i campi DN base utente, Attributo utente e Tipo oggetto utente di questo particolare utente. Per informazioni dettagliate su come utilizzare LDP per conoscere questi attributi specifici dell'utente, vedere la sezione Uso di LDP per identificare gli attributi utente in questo documento.

- Nel campo Timeout server immettere il numero di secondi che devono intercorrere tra le ritrasmissioni. L'intervallo valido è compreso tra 2 e 30 secondi e il valore predefinito è 2 secondi.
- Selezionare la casella di controllo Abilita stato server per abilitare il server LDAP oppure deseleggerla per disabilitarlo. Il valore predefinito è disattivato.
- Fare clic su Applica per eseguire il commit delle modifiche. Questo è un esempio già configurato con queste informazioni:

The screenshot shows the Cisco WLC configuration interface for LDAP Servers. The left sidebar is expanded to 'Security' > 'LDAP'. The main area shows the configuration for 'LDAP Servers > Edit' with the following fields:

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

3. Ora che i dettagli sul server LDAP sono stati configurati sul WLC, il passaggio successivo consiste nel configurare una WLAN per l'autenticazione Web.

Configurazione della WLAN per l'autenticazione Web

Il primo passo è creare una WLAN per gli utenti. Attenersi alla seguente procedura:

1. Per creare una WLAN, fare clic su WLAN dall'interfaccia utente del controller.

Viene visualizzata la finestra WLAN. In questa finestra sono elencate le WLAN configurate sul controller.

2. Per configurare una nuova WLAN, fare clic su New (Nuovo).

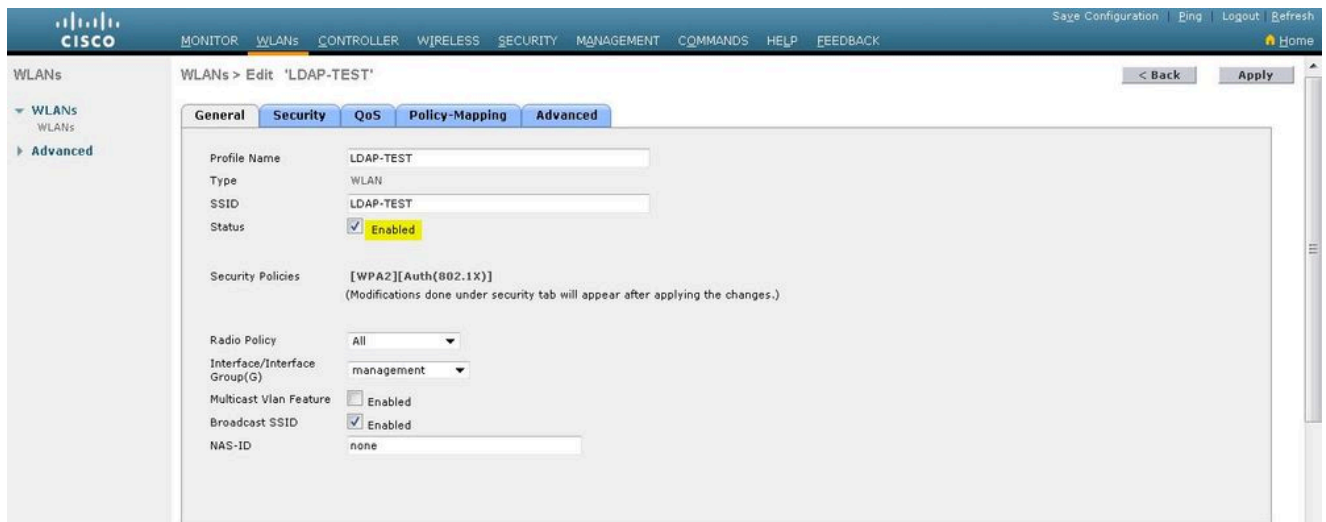
Nell'esempio, il nome della WLAN è Web-Auth.

The screenshot shows the Cisco WLC configuration interface for creating a new WLAN. The left sidebar is expanded to 'WLANs' > 'Advanced'. The main area shows the configuration for 'WLANs > New' with the following fields:

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

3. Fare clic su Apply (Applica).

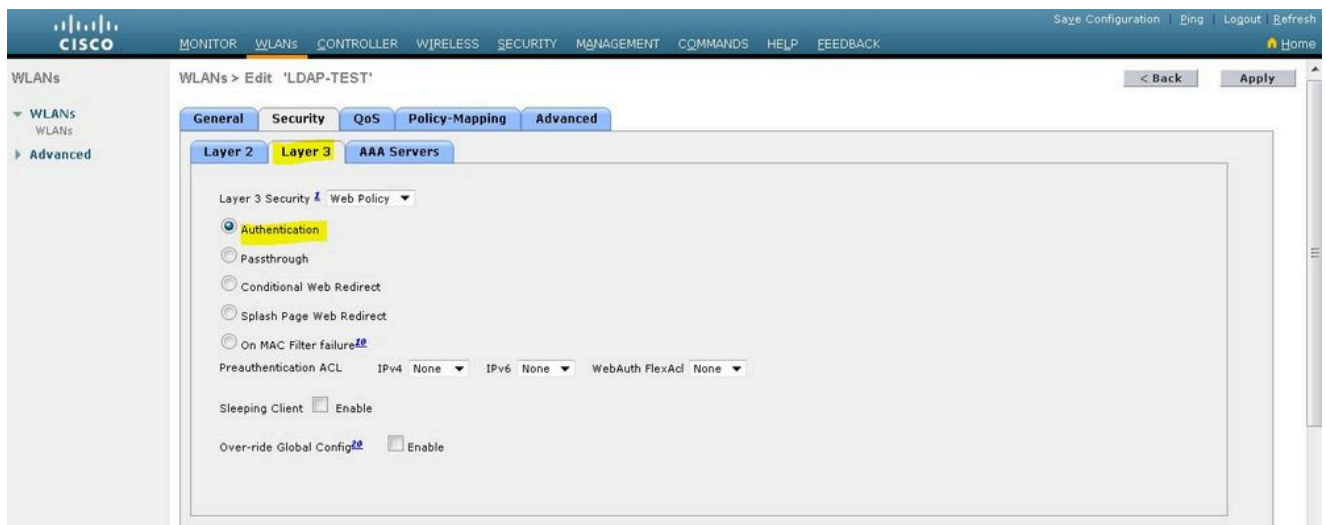
4. Nella finestra WLAN > Modifica, definire i parametri specifici della WLAN.




- Per abilitare la WLAN, selezionare la casella di controllo Status (Stato).
- Per la WLAN, selezionare l'interfaccia appropriata nel campo Interface Name (Nome interfaccia).


In questo esempio viene mappata l'interfaccia di gestione che si connette alla WLAN Web-Auth.

5. Fare clic sulla scheda Protezione. Nel campo Sicurezza di layer 3, selezionare la casella di controllo Criteri Web e scegliere l'opzione Autenticazione.

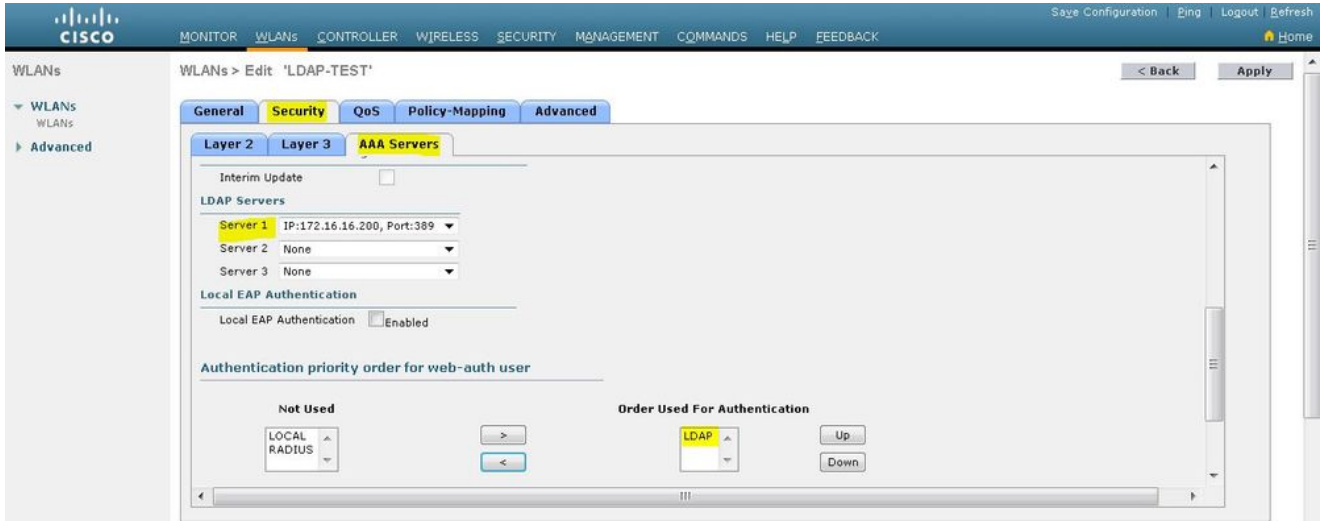


Questa opzione è stata scelta perché per autenticare i client wireless viene utilizzata l'autenticazione Web. Selezionare la casella di controllo Ignora configurazione globale per abilitare la configurazione di autenticazione Web della WLAN. Scegliere il tipo di autenticazione Web appropriato dal menu a discesa Tipo di autenticazione Web. In questo esempio viene utilizzata l'autenticazione Web interna.

 **Nota:** l'autenticazione Web non è supportata con l'autenticazione 802.1x. Ciò significa che non è possibile scegliere 802.1x o WPA/WPA2 con 802.1x come protezione di livello 2 quando si utilizza l'autenticazione Web. L'autenticazione Web è supportata con


 tutti gli altri parametri di protezione di livello 2.

6. Fare clic sulla scheda Server AAA. Scegliere il server LDAP configurato dal menu a discesa Server LDAP. Se si utilizza un database locale o un server RADIUS, è possibile impostare la priorità di autenticazione nel campo Ordine di priorità autenticazione per utente Web-auth.



The screenshot shows the Cisco WLC configuration interface for the 'AAA Servers' tab. The 'LDAP Servers' section is active, showing three servers: Server 1 (IP: 172.16.16.200, Port: 389), Server 2 (None), and Server 3 (None). Below this, the 'Authentication priority order for web-auth user' section is visible, showing a list of authentication methods: 'LOCAL RADIUS' and 'LDAP'. The 'LDAP' method is selected in the 'Order Used For Authentication' list.

7. Fare clic su Apply (Applica).

 Nota: in questo esempio, non vengono utilizzati i metodi di sicurezza di livello 2 per autenticare gli utenti, quindi scegliere Nessuno nel campo Sicurezza di livello 2.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Per verificare questa configurazione, collegare un client wireless e verificare che funzioni come previsto.

Viene visualizzato il client wireless e l'utente immette l'URL, ad esempio www.yahoo.com, nel browser Web. Poiché l'utente non è stato autenticato, il WLC lo reindirizza all'URL di accesso Web interno.

All'utente vengono richieste le credenziali dell'utente. Una volta che l'utente ha inviato il nome utente e la password, la pagina di accesso accetta l'input delle credenziali dell'utente e, al momento dell'invio, invia nuovamente la richiesta all'esempio action_URL, <http://1.1.1.1/login.html>, del server Web WLC. Viene fornito come parametro di input per l'URL di reindirizzamento del cliente, dove 1.1.1.1 è l'indirizzo dell'interfaccia virtuale sullo switch.

Il WLC autentica l'utente rispetto al database utenti LDAP. Una volta completata l'autenticazione, il server Web WLC inoltra l'utente all'URL di reindirizzamento configurato o all'URL con cui il client è stato avviato, ad esempio www.yahoo.com.



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

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

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

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

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



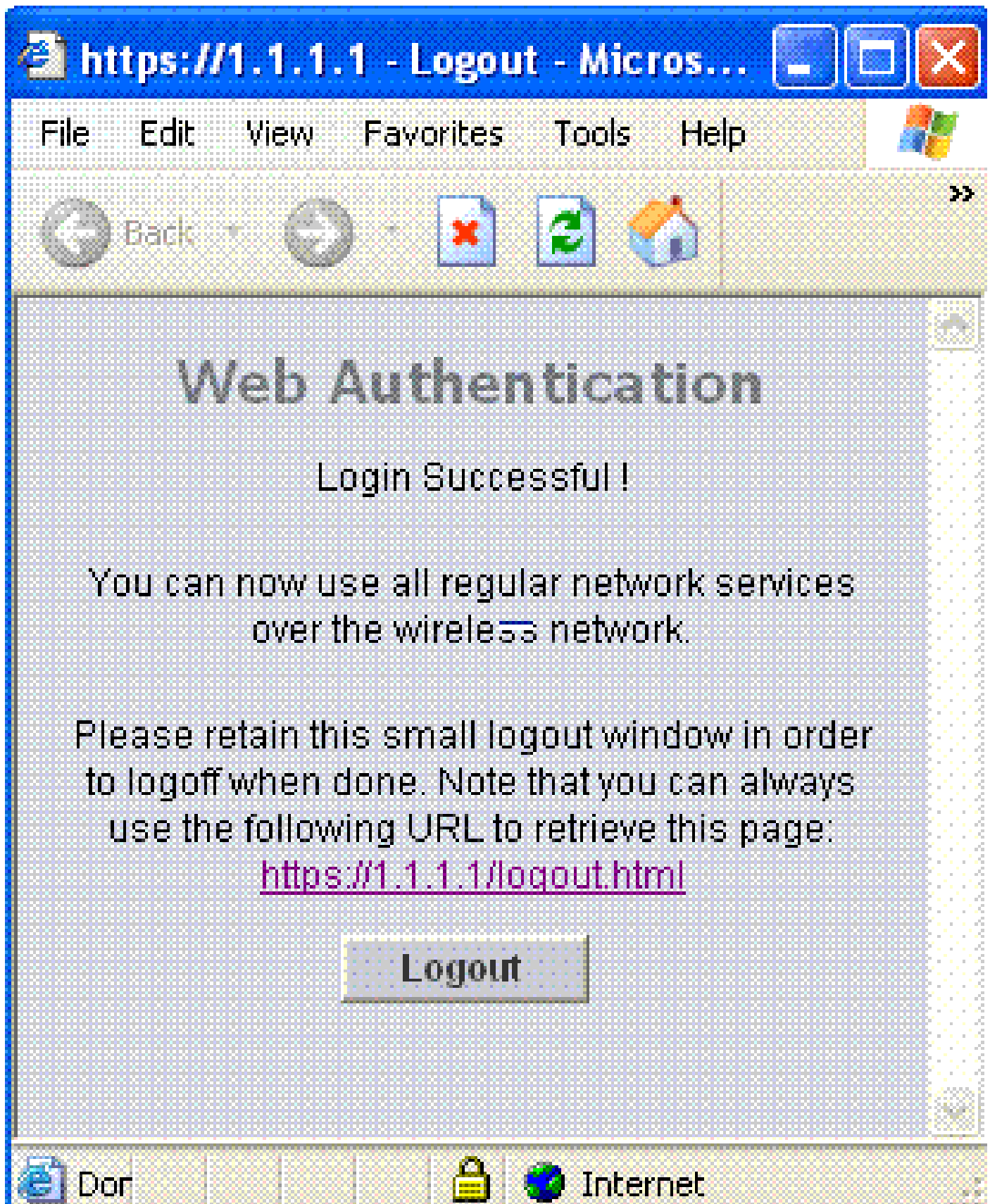
Login



Welcome to the Cisco wireless network

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

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



Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

Utilizzare questi comandi per risolvere i problemi relativi alla configurazione:

- debug mac addr <indirizzo-MAC-client 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

Di seguito viene riportato un esempio di output dei comandi 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 Local

*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 gotSuppRatesElev
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 AID 2 in Assoc Req from flex AP 00:23:eb:e5:04
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfMs1xStateDec
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Change state to

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

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

*pemReceiveTask: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 Removed NPU entry.
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Not Using WMM Compliance code qosCap 00
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4) Plumbed mobil
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4) Change state
```

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) pemApfAddMobile
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Adding Fast Path
type = Airespace AP Client - ACL passthru
on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0
IPv4 ACL I
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Successfully pl
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) pemApfAddMobile
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Replacing Fast
type = Airespace AP Client - ACL passthru
on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0
IPv4 AC
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Successfully pl
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2 (apf_policy.c:359) Changing sta
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2:session timeout forstation cc:f
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Scheduling deletion of Mobile Station: (calle
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Func: apfPemAddUser2, Ms Timeout = 1800, Sessi
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Sending assoc-resp with status 0 station:cc:fa
*apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sending Assoc Response to station on BSSID 00:
*apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 apfProcessAssocReq (apf_80211.c:10187) Changin
*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2, dtlFla
*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sent an XID frame
*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2, dtlFla
*pemReceiveTask: Dec 24 03:45:43.558: cc:fa:00:f7:32:35 Sent an XID frame
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len 322,vla
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype 0xff:ff:ff:ff:
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block settin
dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0,
dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25 VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25 mscbVapLoc
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local a
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block settin
dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0,
dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25 VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block settin
dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25 mscbVapLoc
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local a
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP transmitting DHCP DISCOVER (1)
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP op: BOOTREQUEST, htype: Ethernet, hlen
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 0,
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP chaddr: cc:fa:00:f7:32:35
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0

*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP siaddr: 0.0.0.0, giaddr: 172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block setting
dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE
*DHCP Proxy Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP received op BOOTREPLY (2) (len 572,vlan 0)
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418, port 1, vl
*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
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len 334,vlan
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype 0xff: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 mscbVapLoc
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local a
*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
*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 i
*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, vl
*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
*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created for mobile, leng
*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created in mscb for mobi
*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
*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 PLUMBFASPETH: 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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).