Autenticazione LEAP su un server RADIUS locale

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per l'autenticazione LEAP (Lightweight Extensible Authentication Protocol) su un punto di accesso basato su IOS®, che serve i client wireless e funge da server RADIUS locale. Ciò è applicabile a un access point IOS con versione 12.2(11)JA o successive.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Familiarità con la GUI o la CLI di IOS
- Familiarità con i concetti alla base dell'autenticazione LEAP

Componenti

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

- Access point Cisco Aironet serie 1240AG
- Software Cisco IOS release 12.3(8)JA2
- Cisco Aironet 802.11 a/b/g/ Adattatore wireless con Aironet Desktop Utility 3.6.0.122
- Si presume che la rete includa una sola VLAN

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.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Panoramica della funzionalità Server RADIUS locale

Per autenticare gli utenti viene in genere utilizzato un server RADIUS esterno. In alcuni casi, questa non è una soluzione fattibile. In questi casi, è possibile impostare un punto di accesso che agisca come server RADIUS. In questo caso, gli utenti vengono autenticati in base al database locale configurato nel punto di accesso. Questa funzionalità è denominata Server RADIUS locale. È inoltre possibile fare in modo che altri punti di accesso nella rete utilizzino la funzionalità Server RADIUS locale in un punto di accesso. Per ulteriori informazioni, consultare il documento sulla configurazione di altri punti di accesso per l'utilizzo dell'autenticatore locale.

Configurazione

La configurazione descrive come configurare le funzionalità LEAP e Server Radius locale su un punto di accesso. La funzionalità Server RADIUS locale è stata introdotta nel software Cisco IOS versione 12.2(11)JA. Per informazioni generali su come configurare LEAP con un server RADIUS esterno, fare riferimento a Autenticazione LEAP con server RADIUS.

Come con la maggior parte degli algoritmi di autenticazione basati su password, Cisco LEAP è vulnerabile agli attacchi dei dizionari. Questo non è un nuovo attacco o una nuova vulnerabilità di Cisco LEAP. È necessario creare criteri per le password complesse per ridurre gli attacchi ai dizionari, che includerebbero password complesse e password nuove frequenti. Per ulteriori informazioni sugli attacchi dei dizionari e su come prevenirli, fare riferimento a Attacco del dizionario su Cisco LEAP.

In questo documento si presume che la configurazione sia per la CLI che per la GUI:

1. L'indirizzo IP del punto di accesso è **10.77.244.194**.
2. L'SSID utilizzato è **cisco**, mappato alla **VLAN 1**.
3. I nomi utente sono **user1** e **user2**, mappati al gruppo **Testuser**.

Configurazione CLI

Access Point
ap#**show running-config**

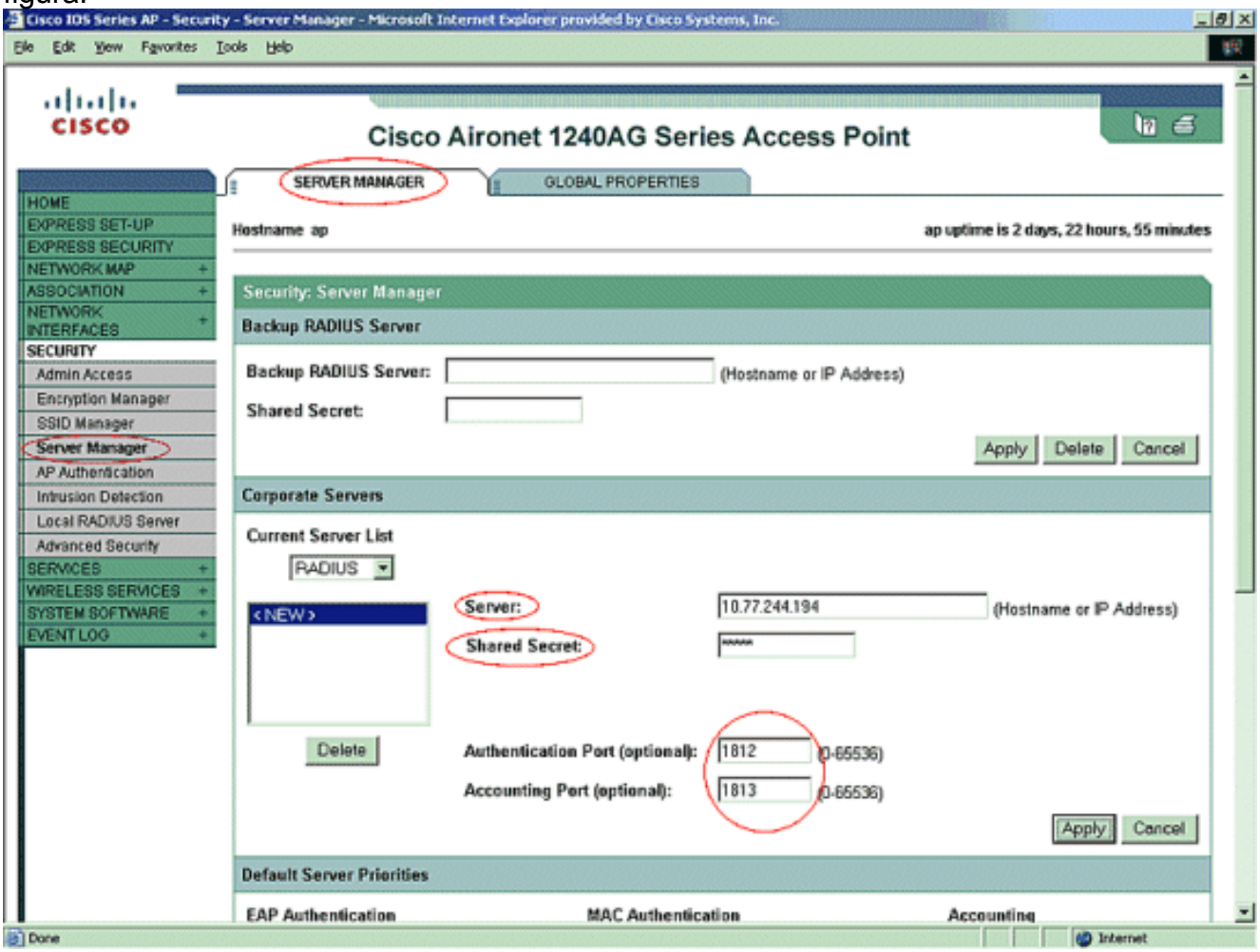
```
Building configuration...
.
.
.
aaa new-model !--- This command reinitializes the
authentication, !--- authorization and accounting
functions. ! ! aaa group server radius rad_eap
 server 10.77.244.194 auth-port 1812 acct-port 1813
!--- A server group for RADIUS is created called
"rad_eap" !--- that uses the server at 10.77.244.194 on
ports 1812 and 1813. . . . aaa authentication login
eap_methods group rad_eap
!--- Authentication [user validation] is to be done for
!--- users in a group called "eap_methods" who use
server group "rad_eap". . . . ! bridge irb ! interface
Dot11Radio0 no ip address no ip route-cache !
encryption vlan 1 key 1 size 128bit
   12345678901234567890123456 transmit-key
!This step is optional----!--- This value seeds the
initial key for use with !--- broadcast
[255.255.255.255] traffic. If more than one VLAN is !---
used, then keys must be set for each VLAN. encryption
vlan 1 mode wep mandatory !--- This defines the policy
for the use of Wired Equivalent Privacy (WEP). !--- If
more than one VLAN is used, !--- the policy must be set
to mandatory for each VLAN. broadcast-key vlan 1 change
300
  !--- You can also enable Broadcast Key Rotation for
each vlan and Specify the time after which Brodacst key
is changed. If it is disabled Broadcast Key is still
used but not changed. ssid cisco
           vlan 1
!--- Create a SSID Assign a vlan to this SSID

            authentication open eap eap_methods
            authentication network-eap eap_methods
 !--- Expect that users who attach to SSID "cisco" !---
request authentication with the type 128 Open EAP and
Network EAP authentication !--- bit set in the headers
of those requests, and group those users into !--- a
group called "eap_methods." ! speed basic-1.0 basic-2.0
basic-5.5 basic-11.0 rts threshold 2312 channel 2437
station-role root bridge-group 1 bridge-group 1
subscriber-loop-control bridge-group 1 block-unknown-
source no bridge-group 1 source-learning no bridge-group
1 unicast-flooding bridge-group 1 spanning-disabled . .
. interface FastEthernet0 no ip address no ip route-
cache duplex auto speed auto bridge-group 1 no bridge-
group 1 source-learning bridge-group 1 spanning-disabled
! interface BVI1 ip address 10.77.244.194 255.255.255.0
!--- The address of this unit. no ip route-cache ! ip
default-gateway 10.77.244.194 ip http server ip http
help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server local !--- Engages the Local RADIUS Server
feature. nas 10.77.244.194 key shared_secret !---
Identifies itself as a RADIUS server, reiterates !---
"localness" and defines the key between the server
(itself) and the access point. ! group testuser !---
Groups are optional. ! user user1 nthash password1 group
testuser !--- Individual user user user2 nthash
password2 group testuser !--- Individual user !--- These
```

```
individual users comprise the Local Database ! radius-
server host 10.77.244.194 auth-port 1812 acct-port
   1813 key shared_secret
!--- Defines where the RADIUS server is and the key
between !--- the access point (itself) and the server.
radius-server retransmit 3 radius-server attribute 32
include-in-access-req format %h radius-server
authorization permit missing Service-Type radius-server
vsa send accounting bridge 1 route ip ! ! line con 0
line vty 5 15 ! end
```

Configurazione GUI

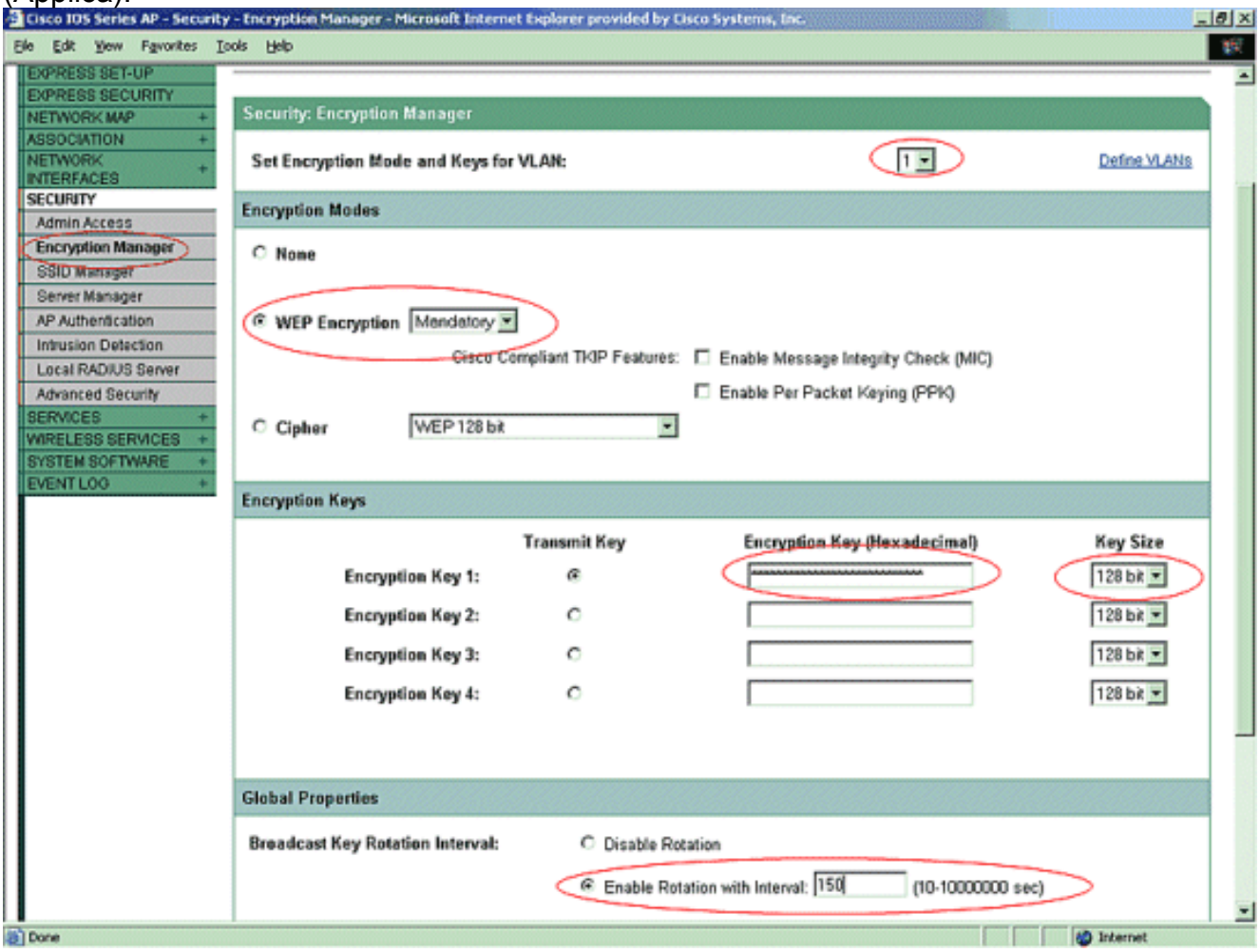
Completare questa procedura per configurare la funzionalità Server RADIUS locale con la GUI:

1. Dal menu a sinistra, scegliere la scheda Server Manager dal menu Security.Configurare il server e indicare l'indirizzo IP del punto di accesso, che nell'esempio è 10.77.244.194.Indicare i numeri di porta 1812 e 1813 su cui il server Radius locale è in ascolto.Specificare il segreto condiviso da utilizzare con il server RADIUS locale, come illustrato nella
figura.

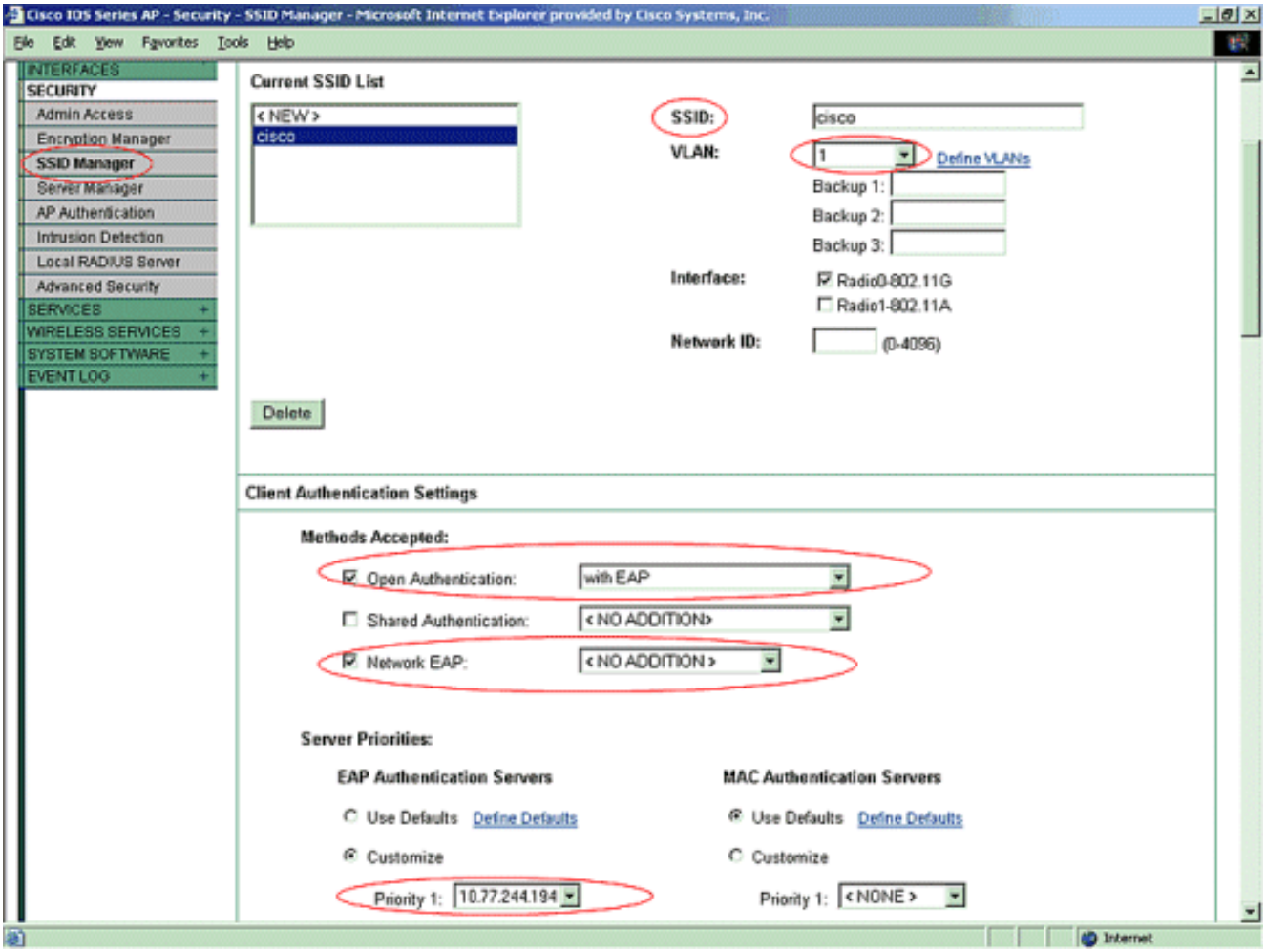


2. Dal menu a sinistra, fare clic sulla scheda Encryption Manager nel menu Security.Specificare la VLAN da applicare.Specificare che deve essere utilizzata la crittografia WEP.Specificare che il suo utilizzo è OBBLIGATORIO.Inizializzare qualsiasi chiave WEP con un carattere esadecimale a 26 cifre. Questa chiave viene utilizzata per crittografare pacchetti broadcast e multicast. Questo passaggio è facoltativo.Impostare la dimensione della chiave su 128 bit. È inoltre possibile scegliere 40 bit. In questo caso, la dimensione della chiave WEP nel

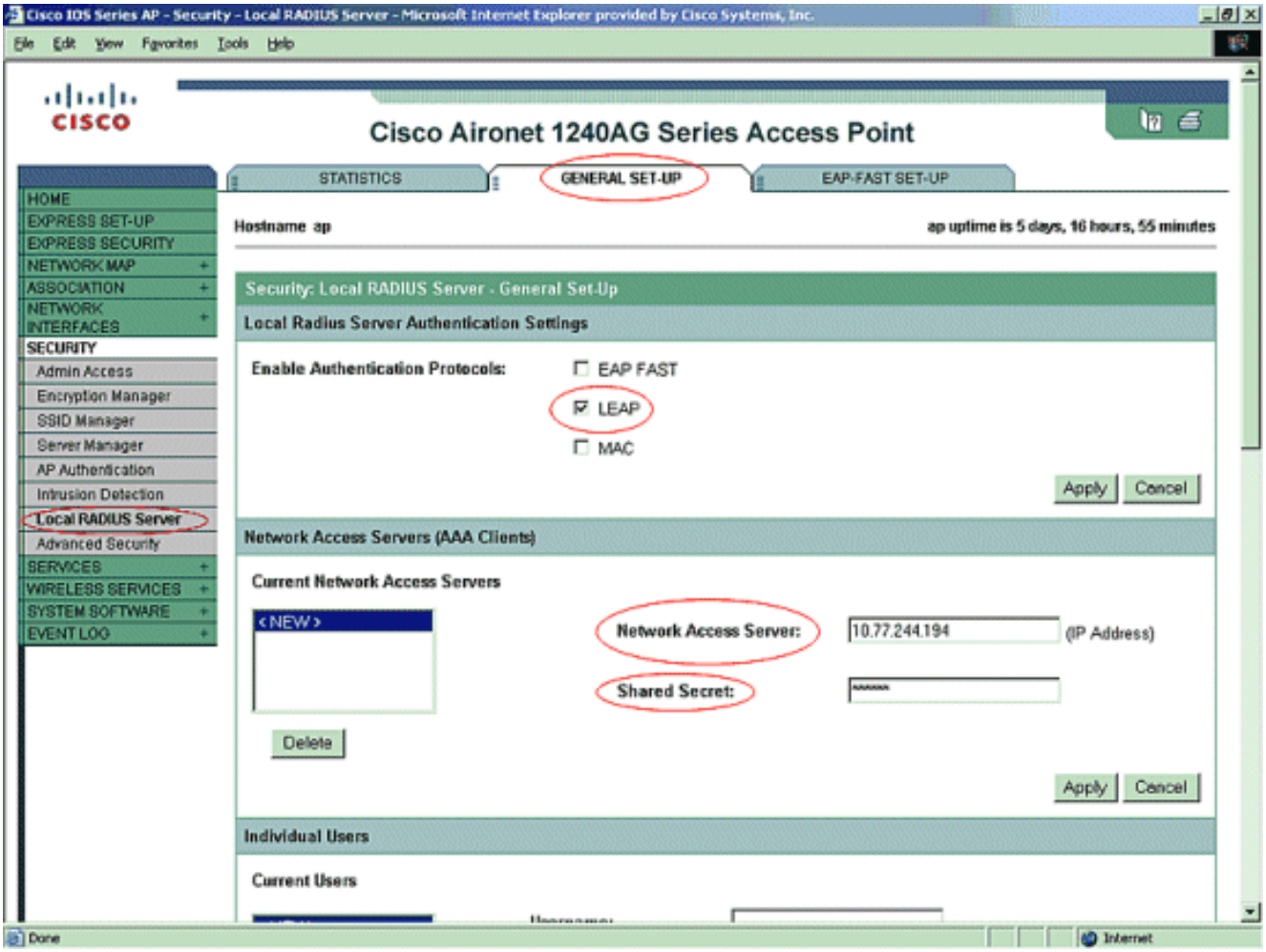
passaggio precedente deve essere un carattere esadecimale a 10 cifre. Questo passaggio è facoltativo.Èinoltre possibile attivare la rotazione della chiave di trasmissione e specificare il periodo di tempo trascorso il quale la chiave di trasmissione viene modificata. Se è disattivata, la chiave di trasmissione è ancora utilizzata ma non modificata. Questo passaggio è facoltativo.**Nota:** Questi passaggi vengono ripetuti per ciascuna VLAN che utilizza l'autenticazione LEAPFare clic su **Apply**
(Applica).



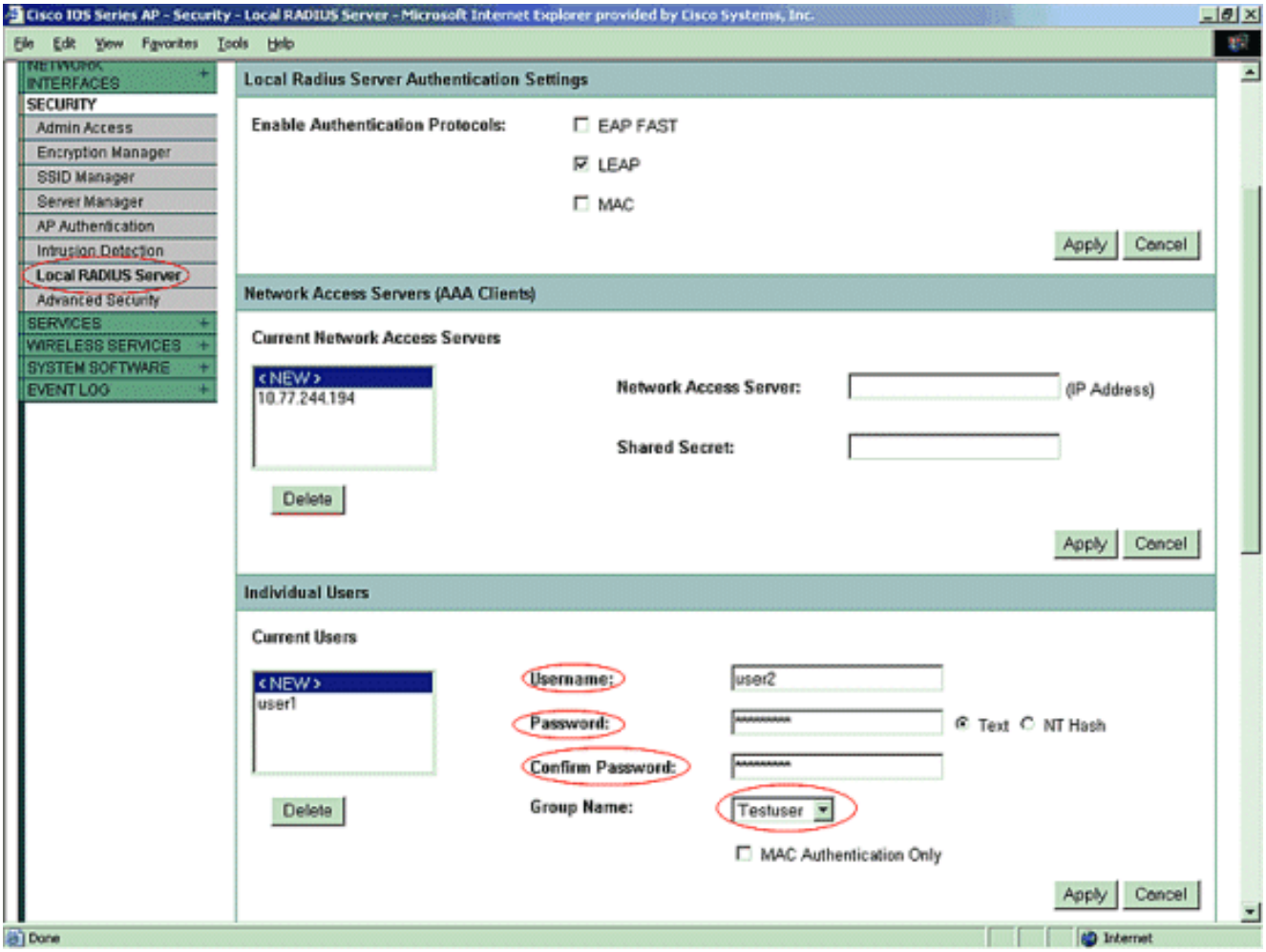
3. Nel menu Protezione della scheda Gestione SSID eseguire le azioni seguenti:**Nota:** è possibile aggiungere ulteriori funzionalità e gestione delle chiavi in un secondo momento, dopo aver verificato che la configurazione di base funziona correttamente.Definire un nuovo SSID e associarlo a una VLAN. Nell'esempio, l'SSID è associato alla VLAN 1.Selezionare **Open Authentication (With EAP)**.Selezionare **Network EAP (No Addition)**.Da **Priorità server > Server di autenticazione EAP**, scegliere **Personalizza**; selezionare l'indirizzo IP di questo punto di accesso **per Priorità 1**.Fare clic su **Apply**
(Applica).



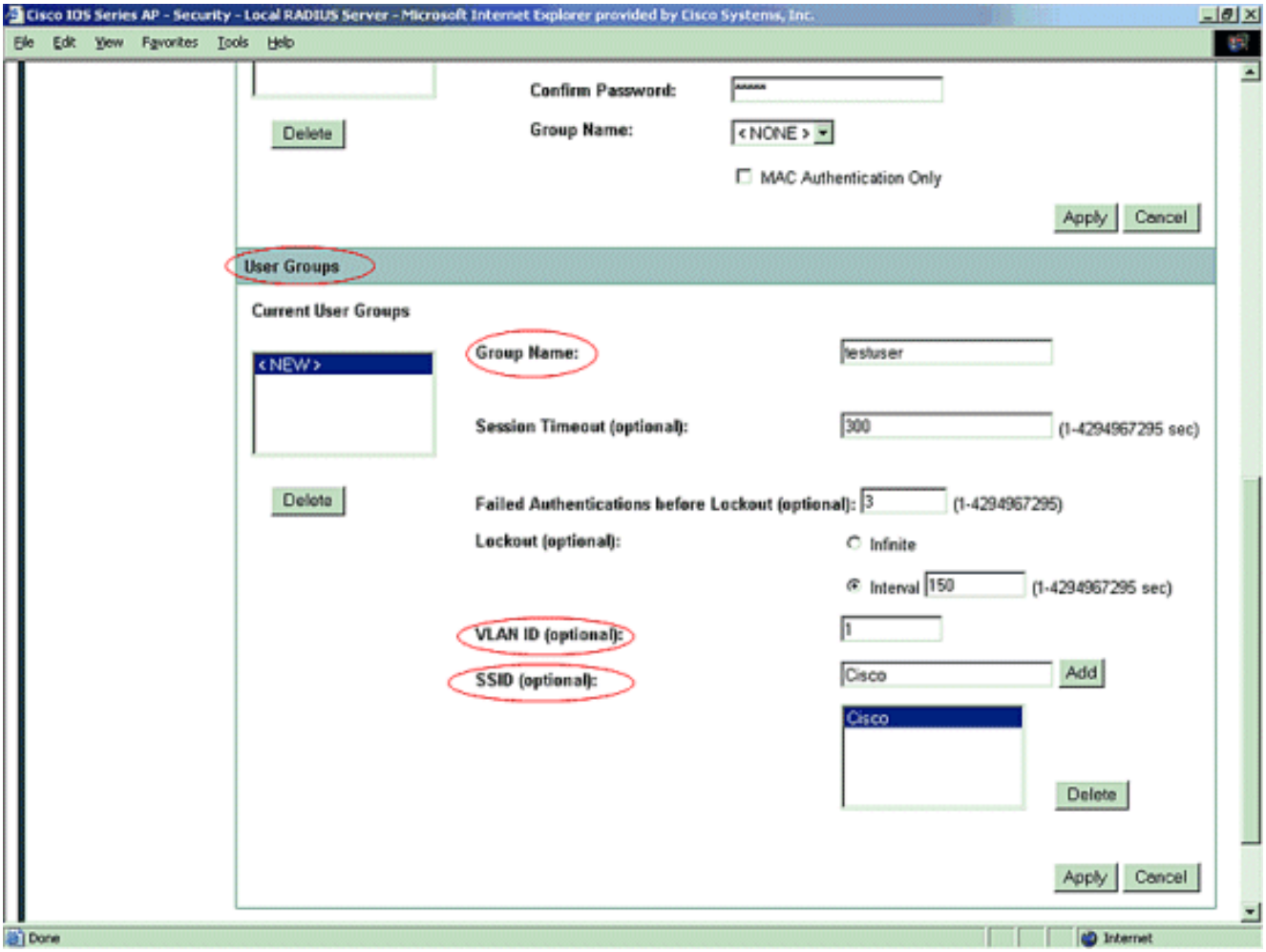
4. In Protezione fare clic su Server RADIUS locale nella scheda Impostazione generaleIn Impostazioni autenticazione server Radius locale, selezionare **LEAP** per assicurarsi che le richieste di autenticazione LEAP vengano accettate.Definire l'indirizzo IP e il segreto condiviso del server RADIUS. Per il server RADIUS locale, questo è l'indirizzo IP del punto di accesso (10.77.244.194).Fare clic su **Apply**
(Applica).



5. Scorrere verso il basso da Server RADIUS locale nella scheda Impostazioni generali e definire i singoli utenti con i relativi nomi utente e password. Se lo si desidera, è possibile associare gli utenti ai gruppi definiti nel passaggio successivo. In questo modo, solo alcuni utenti accedono a un SSID.**Nota:** il database locale RADIUS è costituito da questi nomi utente e password
individuali.



6. Scorrere di nuovo verso il basso nella stessa pagina, dal Server RADIUS locale nella scheda secondaria Configurazione generale fino a Gruppi di utenti; definire i gruppi di utenti e associarli a una VLAN o a un
SSID.



Nota: i gruppi sono facoltativi. Gli attributi del gruppo non vengono passati ad Active Directory e sono rilevanti solo localmente. È possibile aggiungere gruppi in un secondo momento, dopo aver verificato che la configurazione di base funzioni correttamente.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

- **show radius local-server statistics**: questo comando visualizza le statistiche raccolte dall'autenticatore locale.

```
Successes              : 27          Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 0
Unknown NAS            : 0           Invalid packet from NAS: 0

NAS : 10.77.244.194
Successes              : 27          Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 0
Corrupted packet       : 0           Unknown RADIUS message : 0
No username attribute  : 0           Missing auth attribute : 0
Shared key mismatch    : 0           Invalid state attribute: 0
Unknown EAP message    : 0           Unknown EAP auth type  : 0
Auto provision success : 0           Auto provision failure : 0
PAC refresh            : 0           Invalid PAC received   : 0

Username                  Successes  Failures  Blocks
user1                            27         0       0
```

- **show radius server-group all**: questo comando visualizza un elenco di tutti i gruppi di server RADIUS configurati sul punto di accesso.

Risoluzione dei problemi

Procedura di risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere eventuali problemi con questa configurazione.

1. Per evitare problemi di RF che impediscano l'autenticazione, impostare il metodo dell'SSID su **Open** per disabilitare temporaneamente l'autenticazione.Dalla GUI: nella pagina SSID Manager, deselezionare **Network-EAP** e selezionare **Open**.Dalla riga di comando - Utilizzare i comandi **authentication open** e **no authentication network-eap_methods**.Se il client viene associato correttamente, RF non contribuisce al problema di associazione.
2. Verificare che tutte le password segrete condivise siano sincronizzate. Le righe `radius-server host x.x.x.x auth-port x acct-port x key <shared_secret>` e `nas x.x.x key <shared_secret>` devono contenere la stessa password segreta condivisa.
3. Rimuovere tutti i gruppi di utenti e la configurazione relativa ai gruppi di utenti. A volte possono verificarsi conflitti tra i gruppi di utenti definiti dal punto di accesso e i gruppi di utenti del dominio.

Comandi per la risoluzione dei problemi

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug dot11 aaa authenticator all**: questo debug mostra le varie negoziazioni attraverso cui deve passare un client durante l'associazione e l'autenticazione attraverso il processo 802.1x o EAP dal punto di vista di Authenticator (Access Point). Questo debug è stato introdotto nel software Cisco IOS versione 12.2(15)JA. Questo comando rende obsoleto debug dot11 aaa dot1x in questa versione e nelle versioni successive.

```
 *Mar  1 00:26:03.097: dot11_auth_add_client_entry:
   Create new client 0040.96af.3e93 for application 0x1
 *Mar  1 00:26:03.097: dot11_auth_initialize_client:
   0040.96af.3e93 is added to the client list for application 0x1
-----------------------------------------------
   Lines Omitted for simplicity -----------------
*Mar  1 00:26:03.098: dot11_auth_dot1x_start:
   in the dot11_auth_dot1x_start


*Mar  1 00:26:03.132: dot11_auth_dot1x_run_rfsm:
   Executing Action(CLIENT_WAIT,EAP_START) for 0040.96af.3e93
*Mar  1 00:26:03.132: dot11_auth_dot1x_send_id_req_to_client:
   Sending identity request to 0040.96af.3e93(client)
*Mar  1 00:26:03.133: *Mar  1 00:26:03.099:
   dot11_auth_dot1x_send_id_req_to_client:
   Client 0040.96af.3e93 timer started for 30 seconds
*Mar  1 00:26:03.132: dot11_auth_parse_client_pak:
   Received EAPOL packet from 0040.96af.3e93
-----------------------------------------------
```

```
   Lines Omitted----------------------------------
*Mar  1 00:26:03.138: EAP code: 0x2  id: 0x1  length:
   0x000A type: 0x1
01805BF0: 0100000A 0201000A 01757365 7231
   .........user1(User Name of the client)


*Mar1 00:26:03.146: dot11_auth_dot1x_run_rfsm:
   Executing Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96af.3e93
*Mar1 00:26:03.147:dot11_auth_dot1x_send_response_to_server:
   Sending client 0040.96af.3e93 data toserver
*Mar1 00:26:03.147: dot11_auth_dot1x_send_response_to_server:
   Started timer server_timeout 60 seconds
-----------------------------------------------
   Lines Omitted----------------------------------
*Mar1 00:26:03.150: dot11_auth_dot1x_parse_aaa_resp:
   Received server response:GET_CHALLENGE_RESPONSE
*Mar1 00:26:03.150: dot11_auth_dot1x_parse_aaa_resp:
   found session timeout 10 sec


*Mar  1 00:26:03.150: dot11_auth_dot1x_run_rfsm:
   Executing Action(SERVER_WAIT,SERVER_REPLY) for 0040.96af.3e93
*Mar  1 00:26:03.150: dot11_auth_dot1x_send_response_to_client:
   Forwarding server message to client 0040.96af.3e93
-----------------------------------------------
   Lines Omitted----------------------------------
*Mar  1 00:26:03.151: dot11_auth_send_msg:
   Sending EAPOL to requestor
*Mar  1 00:26:03.151: dot11_auth_dot1x_send_response_to_client:
   Started timer client_timeout 10 seconds
*Mar  1 00:26:03.166: dot11_auth_parse_client_pak:
    Received EAPOL packet(User Credentials) from 0040.96af.3e93
*Mar  1 00:26:03.166: EAP code: 0x2  id:
   0x11 length: 0x0025 type: 0x11
01805F90: 01000025 02110025...%...%01805FA0:
   11010018 7B75E719 C5F3575E EFF64B27 ....{ug.EsW^ovK'


Executing Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96af.3e93
*Mar  1 00:26:03.186: dot11_auth_dot1x_send_response_to_server:
   Sending client 0040.96af.3e93 data
   (User Credentials) to server
*Mar  1 00:26:03.186: dot11_auth_dot1x_send_response_to_server:
   Started timer server_timeout 60 seconds
-----------------------------------------------
   Lines Omitted----------------------------------
*Mar  1 00:26:03.196: dot11_auth_dot1x_parse_aaa_resp:
   Received server response: PASS


*Mar1 00:26:03.197: dot11_auth_dot1x_run_rfsm:
   ExecutingAction(SERVER_WAIT,SERVER_PASS) for 0040.96af.3e93
*Mar  1 00:26:03.197: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message(Pass Message) to client
-----------------------------------------------
   Lines Omitted----------------------------------
*Mar  1 00:26:03.198: dot11_auth_send_msg:
   Sending EAPOL to requestor
*Mar  1 00:26:03.199: dot11_auth_dot1x_send_response_to_client:
   Started timer client_timeout 30 second
*Mar  1 00:26:03.199: dot11_auth_send_msg:
   client authenticated 0040.96af.3e93,
   node_type 64 for application 0x1
```

```
*Mar  1 00:26:03.199: dot11_auth_delete_client_entry:
   0040.96af.3e93 is deleted for application 0x1
*Mar  1 00:26:03.200: %DOT11-6-ASSOC:
    Interface Dot11Radio0, Station Station Name 0040.96af.3e93 Associated KEY_MGMT[NONE]
```

- **debug radius authentication**: questo debug visualizza le negoziazioni RADIUS tra il server e il client, che in questo caso sono entrambi il punto di accesso.
- **debug radius local-server client**: questo debug mostra l'autenticazione del client dal punto di vista del server RADIUS.

```
 *Mar 1 00:30:00.742: RADIUS(0000001A):
   SendAccess-Request(Client's User Name) to 10.77.244.194:1812(Local Radius Server)
   id 1645/65, len 128
 *Mar 1 00:30:00.742: RADIUS:
   User-Name [1] 7 "user1"
 *Mar 1 00:30:00.742: RADIUS:
   Called-Station-Id [30] 16 "0019.a956.55c0"
 *Mar 1 00:30:00.743: RADIUS:
   Calling-Station-Id [31] 16 "0040.96af.3e93" (Client)
 *Mar 1 00:30:00.743: RADIUS:
   Service-Type [6] 6 Login [1]
 *Mar 1 00:30:00.743: RADIUS:
   Message-Authenticato[80]
 *Mar  1 00:30:00.743: RADIUS:
   23 2E F4 42 A4 A3 72 4B 28 44 6E 7A 58 CA 8F 7B  [#.?B??rK(DnzX??{]
 *Mar  1 00:30:00.743: RADIUS:
   EAP-Message         [79]  12
 *Mar  1 00:30:00.743:
   RADIUS:   02 02 00 0A 01 75 73 65 72 31
                       [?????user1]
 *Mar  1 00:30:00.744: RADIUS:
   NAS-Port-Type       [61]  6   802.11 wireless
--------------------------------
   Lines Omitted For Simplicity---------------------
 *Mar 1 00:30:00.744: RADIUS:
   NAS-IP-Address [4] 6 10.77.244.194(Access Point IP)
*Mar 1 00:30:00.744: RADIUS: Nas-Identifier [32] 4 "ap"


 ---------------------------------
   Lines Omitted--------------------------------
 *Mar 1 00:30:00.745: RADIUS:
   Received from id 1645/65 10.77.244.194:1812, Access-Challenge, len 117
 *Mar 1 00:30:00.746: RADIUS:
   75 73 65 72 31 [user1]
 *Mar 1 00:30:00.746: RADIUS:
   Session-Timeout [27] 6 10
 *Mar 1 00:30:00.747: RADIUS: State [24] 50
 *Mar 1 00:30:00.747: RADIUS:
   BF 2A A0 7C 8265 76 AA 00 00 00 00 00 00 00 00
   [?*?|?ev?????????]
 ---------------------------------------
   Lines Omitted for simplicity -------------
 *Mar 1 00:30:00.756:
   RADIUS/ENCODE(0000001A):Orig. component type = DOT11
*Mar 1 00:30:00.756: RADIUS: AAA Unsupported Attr: ssid [264] 5
 *Mar 100:30:00.756: RADIUS: 63 69 73 [cis]
 *Mar 1 00:30:00.756: RADIUS: AAA Unsupported Attr: interface [157] 3
 *Mar 1 00:30:00.756: RADIUS: 32 [2]
 *Mar 1 00:30:00.757: RADIUS(0000001A): Config NAS IP: 10.77.244.194
 *Mar 1 00:30:00.757: RADIUS/ENCODE(0000001A): acct_session_id: 26
 *Mar 1 00:30:00.757: RADIUS(0000001A): Config NAS IP: 10.77.244.194
```

```
*Mar 1 00:30:00.779: RADIUS(0000001A):
  Send Access-Request to 10.77.244.194:1812 id 1645/67, len 189
*Mar 1 00:30:00.779: RADIUS:
  authenticator B0 15 3C C1 BC F6 31 85 - 66 5D 41 F9 2E B4 48 7F
*Mar 1 00:30:00.779: RADIUS: User-Name [1] 7 "user1"
*Mar 1 00:30:00.780: RADIUS: Framed-MTU [12] 6 1400
*Mar 1 00:30:00.780: RADIUS: Called-Station-Id [30] 16"0019.a956.55c0"
*Mar 1 00:30:00.780: RADIUS: Calling-Station-Id [31] 16"0040.96af.3e93"
*Mar  1 00:30:00.758: RADIUS:
  92 D4 24 49 04 C2 D2 0A C3 CE E9 00 6B F1 B2 AF  [??$I????????k???]
*Mar  1 00:30:00.759: RADIUS:  EAP-Message         [79]  39
*Mar  1 00:30:00.759: RADIUS:
  02 17 00 25 11 01 00 18 05 98 8B BE 09 E9 45 E2
   [?????????????E?]
*Mar  1 00:30:00.759: RADIUS:
  73 5D 33 1D F0 2F DB 09 50 AF 38 9F F9 3B BD D4
  [s]3??/??P?8??;??]
*Mar  1 00:30:00.759: RADIUS:
  75 73 65 72 31                                  [user1]
----------------------------------------
  Lines Omitted---------------------------
*Mar 1 00:30:00.781: RADIUS: State [24] 50 RADIUS:
  NAS-IP-Address [4] 6 10.77.244.194
*Mar 1 00:30:00.783: RADIUS: Nas-Identifier [32] 4 "ap"


*Mar 1 00:30:00.822: RADIUS:
  Received from id 1645/67 10.77.244.194:1812, Access-Accept, len 214
*Mar 1 00:30:00.822:
  RADIUS: authenticator 10 0C B6 EE 7A 96 3A 46 - 36 49 FC D3 7A F4 42 2A
----------------------------------------
  Lines Omitted---------------------------
*Mar 1 00:30:00.823: RADIUS: 75 73 65 72 31 [user1]
*Mar 1 00:30:00.823: RADIUS: Vendor, Cisco [26] 59
*Mar 1 00:30:00.823: RADIUS:
  Cisco AVpair [1] 53 "leap:session-key=?+*ve=];q,oi[d6|-z."
*Mar 1 00:30:00.823:
  RADIUS: User-Name [1] 28 "user1 *Mar 1 00:30:00.824: RADIUS:
  Message-Authenticato[80] 18
*Mar 1 00:30:00.824: RADIUS:
  06 2D BA 93 10 C0 91 F8 B4 B8 A4 00 82 0E 11 36
  [?-????????????6]
  *Mar 1 00:30:00.826: RADIUS/DECODE: EAP-Message fragments,
37, total 37 bytes
*Mar 1 00:30:00.826: found leap session key
*Mar 1 00:30:00.830: %DOT11-6-ASSOC:
  Interface Dot11Radio0, Station Station Name Associated KEY_MGMT[NONE]
```

- **debug radius local-server packets**: questo debug visualizza tutti i processi eseguiti da e dal punto di vista del server RADIUS.

Informazioni correlate

- Configurazione di un punto di accesso come autenticatore locale
- Configurazione dei tipi di autenticazione
- Configurazione dei server RADIUS e TACACS+
- Documentazione e supporto tecnico – Cisco Systems