

LEAP Authentication on a Local RADIUS Server

Document ID: 44100

Introduction

Prerequisites

Requirements

Components

Conventions

Overview of Local RADIUS Server Feature

Configure

CLI Configuration

GUI Configuration

Verify

Troubleshoot

Troubleshooting Procedure

Troubleshooting Commands

Related Information

Introduction

This document provides a sample configuration for Lightweight Extensible Authentication Protocol (LEAP) authentication on an IOS[®]-based access point, which serves the wireless clients, as well as acts as a local RADIUS server. This is applicable to an IOS access point that runs 12.2(11)JA or later.

Prerequisites

Requirements

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

- Familiarity with the IOS GUI or CLI
- Familiarity with the concepts behind LEAP authentication

Components

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

- Cisco Aironet 1240AG Series Access Point
- Cisco IOS Software Release 12.3(8)JA2
- Cisco Aironet 802.11 a/b/g/ Wireless Adapter that runs Aironet Desktop Utility 3.6.0.122
- Assumption of only one VLAN in the network

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Overview of Local RADIUS Server Feature

Usually an external RADIUS Server is used to authenticate users. In some cases, this is not a feasible solution. In these situations, an access point can be made to act as a RADIUS Server. Here, users are authenticated against the local database configured in the access point. This is called a Local RADIUS Server feature. You can also make other access points in the network use the Local RADIUS Server feature on an access point. For more information on this, refer to [Configuring Other Access Points to Use the Local Authenticator](#).

Configure

The configuration describes how to configure LEAP and Local Radius Server Feature on an access point. The Local RADIUS Server feature was introduced in Cisco IOS Software Release 12.2(11)JA. Refer to [LEAP Authentication with RADIUS Server](#) for background information on how to configure LEAP with an external RADIUS Server.

As with most password-based authentication algorithms, Cisco LEAP is vulnerable to dictionary attacks. This is not a new attack or new vulnerability of Cisco LEAP. You must create a strong password policy to mitigate dictionary attacks, that would include strong passwords and frequent new passwords. Refer to [Dictionary Attack on Cisco LEAP](#) for more information about dictionary attacks and how to prevent them.

This document assumes this configuration for both CLI and GUI:

1. The IP address of the access point is **10.77.244.194**.
2. The SSID used is **cisco**, which is mapped to **VLAN 1**.
3. The usernames are **user1** and **user2**, which are mapped to the group **Testuser**.

CLI Configuration

Access Point
<pre>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". . .</pre>

```

.
!
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 Broadcast 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/help/eag/ivory/1100
ip radius source-interface BV11
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 nhash password1 group testuser

/--- Individual user

    user user2 nhash 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

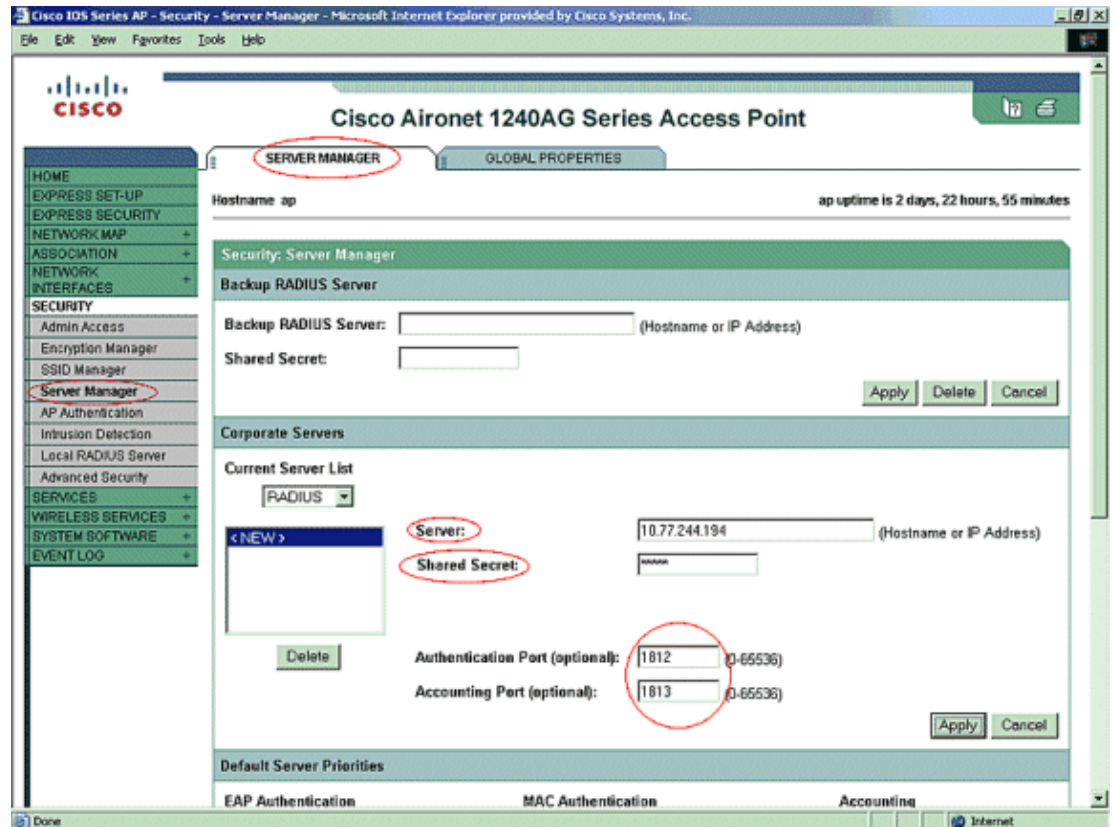
```

GUI Configuration

Complete these steps in order to configure the Local RADIUS Server feature with the GUI:

1. From the menu in the left-hand side , choose the Server Manager tab under the Security menu.

- a. Configure the server and mention the IP address of this access point, which is 10.77.244.194 in this example.
- b. Mention the port numbers 1812 and 1813 on which the Local Radius server listens.
- c. Specify the shared secret to be used with the Local RADIUS Server as shown in the figure.

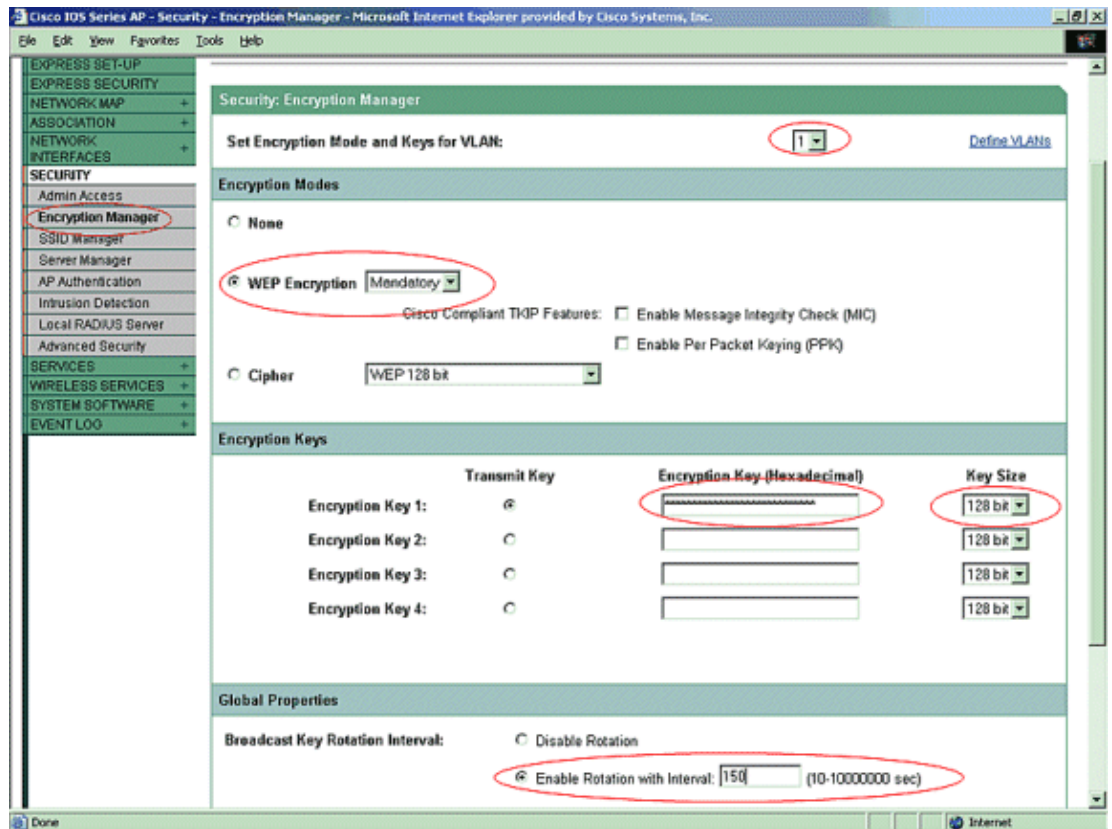


2. From the menu in the left-hand side, click the Encryption Manager tab under the Security menu.

- a. Specify the VLAN to be applied.
- b. Specify that WEP encryption is to be used.
- c. Specify that its use is MANDATORY.
- d. Initialize any WEP key with a 26-digit hexadecimal character. This key is used to encrypt broadcast and multicast packets. This step is optional.
- e. Set the key size to 128 bits. You can also choose 40 bits. In this case, the WEP key size in the previous step must be a 10-digit hexadecimal character. This step is optional.
- f. You can also enable broadcast key rotation and specify the time after which the broadcast key is changed. If it is disabled, the broadcast key is still used but not changed. This step is optional.

Note: These steps are repeated for every VLAN that uses LEAP authentication

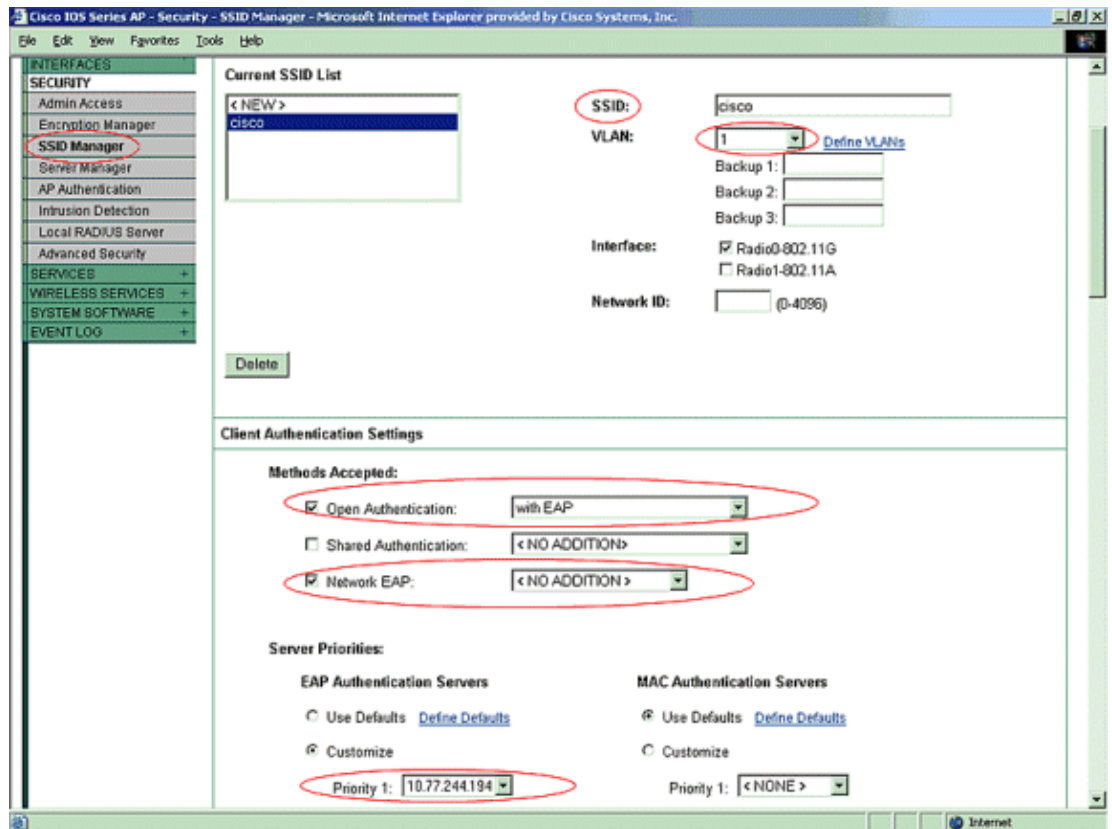
g. Click **Apply**.



3. Under the Security Menu , from the SSID Manager tab, perform these actions:

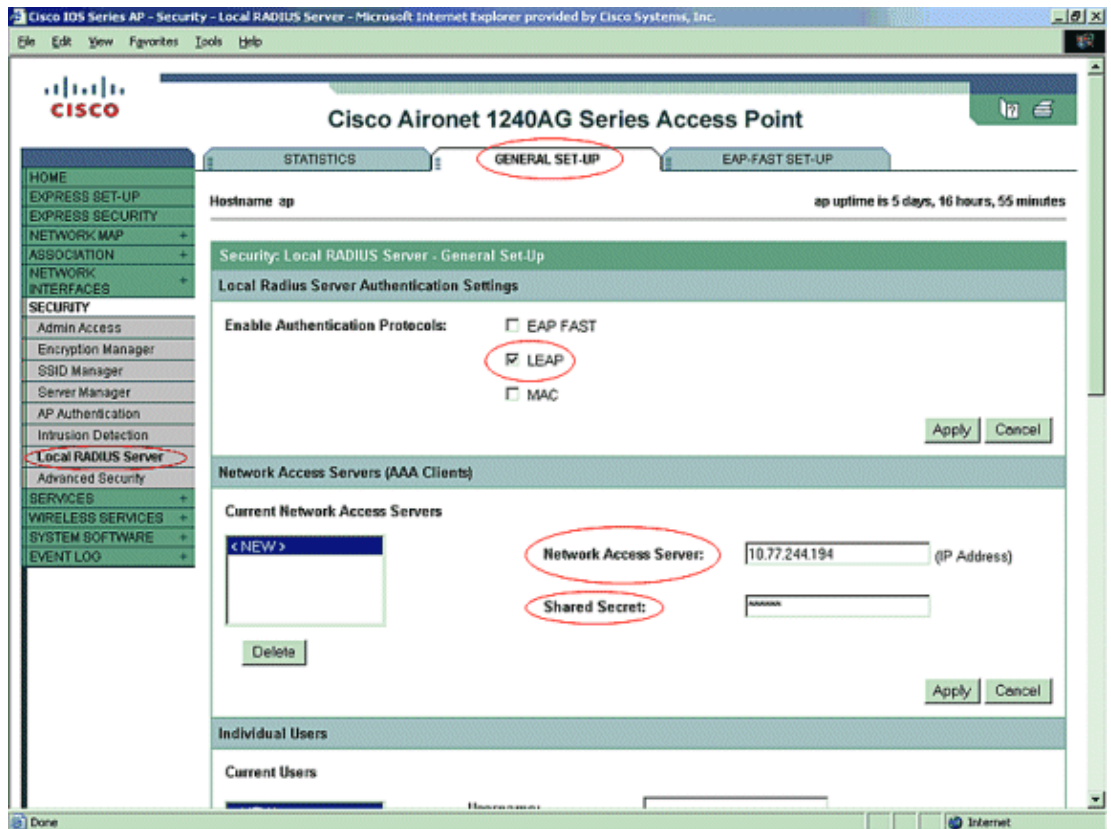
Note: You can add additional features and key management later, once you confirm that the base configuration works correctly.

- a. Define a new SSID and associate it with a VLAN. In this example, the SSID is associated with VLAN 1.
- b. Check **Open Authentication (With EAP)**.
- c. Check **Network EAP (No Addition)**.
- d. From **Server Priorities > EAP Authentication Servers**, choose **Customize**; choose the IP address of this access point for **Priority 1**.
- e. Click **Apply**.



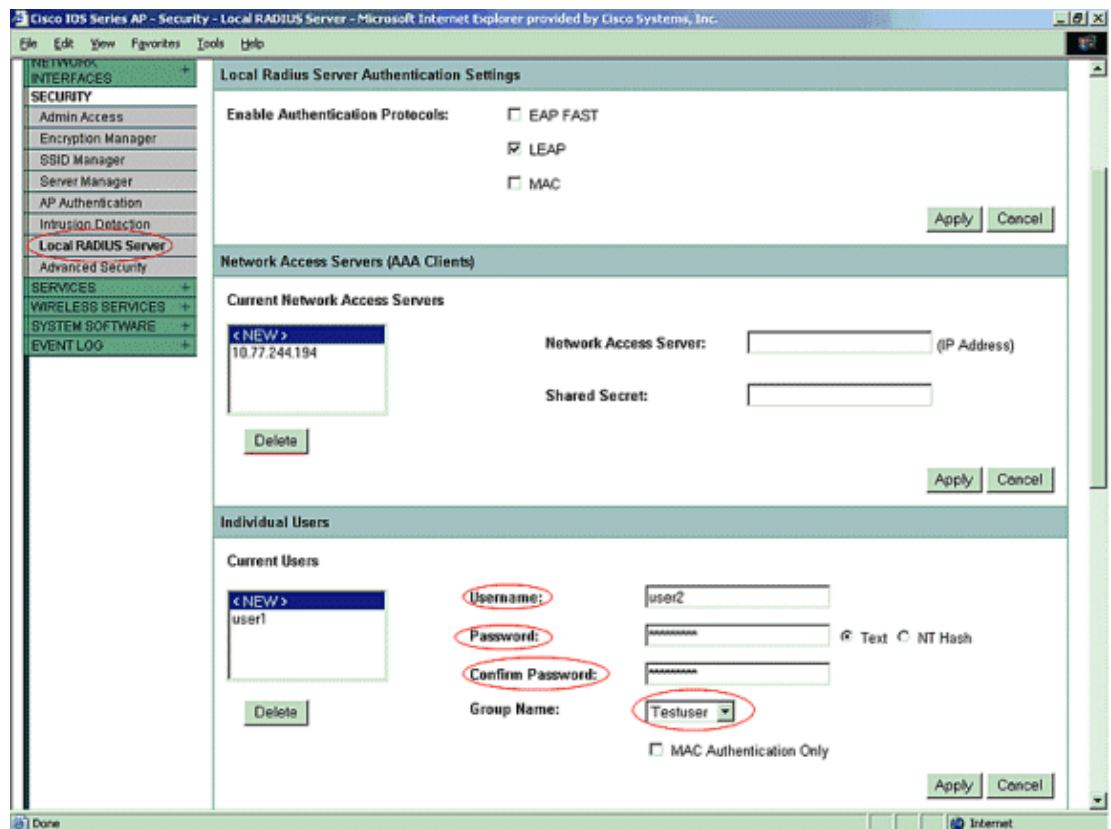
4. Under Security, click Local RADIUS Server from the General Set-UP tab

- a. Under Local Radius Server Authentication Settings, check **LEAP** to make sure that LEAP authentication requests are accepted.
- b. Define the IP address and shared secret of the RADIUS server. For Local RADIUS Server, this is the IP address of this AP (10.77.244.194).
- c. Click **Apply**.



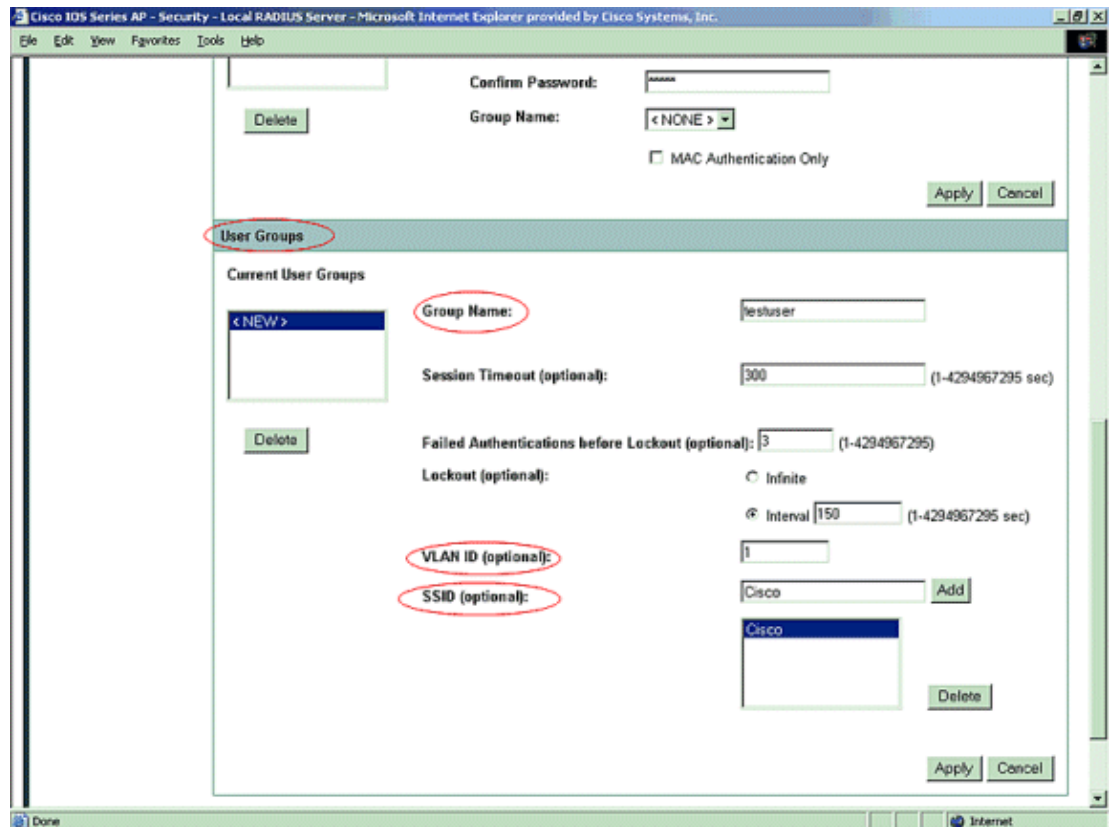
5. Scroll down from Local RADIUS Server under the General Setup tab and define the individual users with their usernames and passwords. Optionally, users can be associated to Groups, which is defined in the next step. This makes sure that only certain users log into a SSID.

Note: The Local RADIUS database is comprised of these individual usernames and passwords.



6. Scroll further down on the same page, again from the Local RADIUS Server under the General

Set-Up sub tab to User Groups; define user groups and associate them to a VLAN or SSID.



Note: Groups are optional. The group attributes do not pass to Active Directory and are only locally relevant. You can add groups later, once you confirm that the base configuration works correctly.

Verify

Use this section to confirm that your configuration works properly.

- **show radius local-server statistics** This command displays statistics collected by the local authenticator.

```

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** This command displays a list of all configured RADIUS server-groups on the access point.

Troubleshoot

Troubleshooting Procedure

This section provides troubleshooting information relevant to this configuration.

1. In order to eliminate the possibility of RF issues preventing successful authentication, set the method on the SSID to **Open** to temporarily disable authentication.
 - ◆ From the GUI On the SSID Manager page, uncheck **Network–EAP** and check **Open**.
 - ◆ From the command line Use the commands **authentication open** and **no authentication network–eap eap_methods**.If the client successfully associates, RF does not contribute to the association problem.
2. Verify that all shared secret passwords are synchronized. The lines `radius-server host x.x.x.x auth-port x acct-port x key <shared_secret>` and `nas x.x.x.x key <shared_secret>` must contain the same shared secret password.
3. Remove any user groups and configuration about user groups. Sometimes conflicts can occur between user groups defined by the access point, and user groups on the domain.

Troubleshooting Commands

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug dot11 aaa authenticator all** This debug shows the various negotiations that a client goes through as the client associates and authenticates through the 802.1x or EAP process from the perspective of Authenticator (Access Point). This debug was introduced in Cisco IOS Software Release 12.2(15)JA. This command obsoletes `debug dot11 aaa dot1x all` in that and later releases.

```
*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 to server
*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

*Mar 1 00:26:03.197: dot11_auth_dot1x_run_rfsm:
    Executing Action(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** This debug shows the RADIUS negotiations between the server and client, both of which, in this case, are the access point.
- **debug radius local-server client** This debug shows the authentication of the client from the perspective of the RADIUS server.

```

*Mar 1 00:30:00.742: RADIUS(0000001A):
  Send Access-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 82 65 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 1 00:30:00.756: 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** This debug shows all processes done by and from the perspective of the RADIUS server.

Related Information

- [Configuring an Access Point as a Local Authenticator](#)
 - [Configuring Authentication Types](#)
 - [Configuring RADIUS and TACACS+ Servers](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-