

# Table of Contents

<b><u>LEAP Authentication with Local RADIUS Server</u></b> .....	<b>1</b>
<u>Introduction</u> .....	1
<u>Before You Begin</u> .....	1
<u>Conventions</u> .....	1
<u>Prerequisites</u> .....	1
<u>Components Used</u> .....	1
<u>Configure</u> .....	2
<u>CLI Configuration</u> .....	2
<u>GUI Configuration</u> .....	4
<u>Verify</u> .....	7
<u>Troubleshoot</u> .....	7
<u>Troubleshooting Procedure</u> .....	7
<u>Troubleshooting Commands</u> .....	8
<u>Related Information</u> .....	8

# LEAP Authentication with Local RADIUS Server

---

## Introduction

### Before You Begin

- Conventions
- Prerequisites
- Components Used

### Configure

- CLI Configuration
- GUI Configuration

### Verify

### Troubleshoot

- Troubleshooting Procedure
- Troubleshooting Commands

### Related Information

---

## Introduction

This document provides a sample configuration for LEAP authentication of wireless users against the Local RADIUS Server database on an IOS based access point running IOS version 12.2(11)JA or later.

## Before You Begin

### Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

### Prerequisites

Before attempting this configuration, please ensure that you meet the following prerequisites:

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

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

### Components Used

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

- Cisco Aironet access point products running IOS
- IOS Release 12.2(11)JA or later
- Assumption of only one VLAN in the network

# Configure

The following configuration describes how to configure LEAP, as well as the Local RADIUS Server database feature. Local RADIUS Server feature was introduced in IOS release 12.2(11)JA. For background information on configuring LEAP, see the document LEAP Authentication with RADIUS Server. To find additional information on the commands used in this document, use the Command Lookup Tool ( registered customers only)

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. Creating a strong password policy is the most effective way to mitigate dictionary attacks. This includes using strong passwords and periodically expiring passwords. For more information about dictionary attacks and how to prevent them, see the Dictionary Attack on Cisco Leap document.

## CLI Configuration

This document uses the configuration shown below.

```
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 192.168.2.108 auth-port 1812 acct-port 1813
!--- a server group for RADIUS is created called "rad_eap"
!--- using the server at 192.168.2.108 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 will use server group "rad_eap"
.
.
.
!
bridge irb
!
interface Dot11Radio0
  no ip address
  no ip route-cache
  !
  encryption key 1 size 128bit 12345678901234567890123456 transmit-key
!--- The value here 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 mode wep mandatory

!--- This defines the policy for the use of WEP. If more than one
!--- VLAN is used, the policy must be set to mandatory for each VLAN.

!
ssid labap1200
    authentication network-eap eap_methods

!--- Expect that users attaching to SSID "labap1200" will be
!--- requesting authentication with the type 128 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 192.168.2.108 255.255.255.0
!--- Address of this unit

no ip route-cache
!
ip default-gateway 192.168.2.1
ip http server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100
ip radius source-interface BVI1
snmp-server community cable RO
snmp-server enable traps tty
radius-server local
!--- Engages Local RADIUS Server feature

    nas 192.168.2.108 key shared_secret
!--- Identifies itself as a RADIUS server, reiterating
!--- "localness" and defining key between server (itself) and AP

!
group testgroup
!--- Groups are optional

!
user user1 nhash password1 group testgroup

```

```

!--- Individual user
    user user2 ntlm password2 group testgroup
!--- Individual user
!
radius-server host 192.168.2.108 auth-port 1812 acct-port 1813 key shared_secret

!--- Defines where RADIUS server is and key between AP (itself) and 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

To configure the Local RADIUS Server feature by the GUI, follow these steps.

1. From the Server Manager tab, define the IP address, ports, and shared secret of the RADIUS server. For Local RADIUS Server, this is the IP address of the AP.

**Note:** The Local RADIUS Server listens on ports 1812 and 1813.

2. From the Encryption Manager tab:

- ◆ Specify that WEP encryption is to be used.
- ◆ Specify that its use is MANDATORY.

- ◆ Initialize the value of WEP key # 1 with any 26 hex–character string .
- ◆ Set the key size to 128–bits.
- ◆ Click Apply.

The screenshot shows the 'Security: Encryption Manager' configuration page. On the left is a navigation sidebar with categories: NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY (selected), SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. Under SECURITY, 'Encryption Manager' is highlighted. The main panel has a teal header 'Security: Encryption Manager'. Below it is the 'Encryption Modes' section with radio buttons for 'None', 'WEP Encryption' (selected), and 'Cipher'. The 'WEP Encryption' mode is set to 'Mandatory'. Below this are checkboxes for 'Cisco Compliant TKIP Features' with options 'Enable MIC' and 'Enable Per Packet Keying'. The 'Cipher' mode is set to 'WEP 128 bit'. The 'Encryption Keys' section contains a table with four rows for 'Encryption Key 1' through 'Encryption Key 4'. Each row has a radio button for 'Transmit Key', a text input field for 'Encryption Key (Hexadecimal)', and a dropdown for 'Key Size' (all set to '128 bit').

3. From the SSID Manager tab, for the desired SSID:

**Note:** Additional features and key management can be added later, once the base configuration is confirmed to be working correctly.

- ◆ Check the box Network–EAP.
- ◆ Click Apply.

The screenshot shows the 'Security: SSID Manager' configuration page. On the left is the same navigation sidebar as in the previous image, with 'SSID Manager' highlighted. The main panel has a teal header 'Security: SSID Manager'. Below it is the 'SSID Properties' section. On the left of this section is a 'Current SSID List' with a table containing three rows: '<NEW>', 'labap1200', and 'vigil'. A 'Delete' button is below the list. To the right of the list are fields for 'SSID:' (containing 'labap1200') and 'VLAN:' (set to '< NONE >'). There is a 'Define VLANs' link. Below these are 'Authentication Methods Accepted' with checkboxes for 'Open Authentication', 'Shared Authentication', and 'Network EAP' (checked). Each has a dropdown menu. Below that is 'Authenticated Key Management' with radio buttons for 'None' (selected), 'CCKM' (set to 'Mandatory'), and 'WPA' (set to 'Optional'). Below this is 'WPA Pre-shared Key' with a text input field and radio buttons for 'ASCII' (selected) and 'Hexadecimal'. At the bottom is 'EAP Client (optional)' with 'Username:' and 'Password:' text input fields.

4. From the Local RADIUS Server tab (General Set–Up subtab):

- ◆ Define the IP address and shared secret of the RADIUS server. For Local RADIUS Server, this is the IP address of the AP.
- ◆ Click Apply.

Hostname ap1200 ap1200 uptime is 2 days, 25 minutes

**Security: Local RADIUS Server - General Set-Up**

**Network Access Server**

**Current Network Access Servers**

< NEW >  
192.168.2.108

Network Access Server: 192.168.2.108 (IP Address)

Shared Secret: [REDACTED]

Delete Apply Cancel

**Individual User**

**Current User List**

< NEW >

Username: [REDACTED]

Password: [REDACTED]  Text  NT Hash

Confirm Password: [REDACTED]

Group Name: < NONE >

Delete Apply Cancel

5. Further down the General Set-Up subtab, individual users are defined.

**Individual User**

**Current User List**

< NEW >  
user1  
user2

Username: user1

Password: [REDACTED]  Text  NT Hash

Confirm Password: [REDACTED]

Group Name: testgroup

Delete Apply Cancel

**User Groups**

**Current User Group**

< NEW >  
testgroup

Group Name: [REDACTED]

Session Timeout (optional): [REDACTED] (1-4294967295 sec)

Failed Authentications before Lockout (optional): [REDACTED] (1-4294967295)

Lockout (optional):  Infinite  Interval [REDACTED] (1-4294967295 sec)

VLAN ID (optional): [REDACTED]

Delete

**Note:** Groups are optional. The group attributes do not pass to Active Directory and are only locally relevant. Groups can be added later, once the base configuration is confirmed to be working correctly.

6. Further down the General Set-Up subtab, user groups can be defined.

The screenshot shows the 'User Groups' configuration window. On the left, under 'Current User Group', there is a dropdown menu with '<NEW>' and 'testgroup' (selected). Below it is a 'Delete' button. To the right, the 'Group Name' field contains 'testgroup'. Below that are fields for 'Session Timeout (optional)' (1-4294967295 sec), 'Failed Authentications before Lockout (optional)' (1-4294967295), and 'Lockout (optional)' with radio buttons for 'Infinite' and 'Interval' (selected, 1-4294967295 sec). There are also fields for 'VLAN ID (optional)' and 'SSID (optional)' with an 'Add' button. At the bottom right are 'Delete', 'Apply', and 'Cancel' buttons.

**Note:** Groups are optional. The group attributes do not pass to Active Directory and are only locally relevant. Groups can be added later, once the base configuration is confirmed to be working correctly.

## Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only), which allows you to view an analysis of **show** command output.

- **show radius local-server statistics** – This command displays statistics collected by the local authenticator.
- **show radius server-group all** – This command displays a list of all configured RADIUS server-groups on the access point.

## Troubleshoot

### Troubleshooting Procedure

Below is troubleshooting information relevant to this configuration.

1. To eliminate the possibility of RF issues preventing successful authentication, temporarily disable authentication by setting the method on the SSID to Open.
  - ◆ 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 is not contributing 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 regarding user groups. Sometimes conflicts can occur



between user groups defined by the AP, and user groups on the underlying domain.

## Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool ( registered customers only) , which allows you to view an analysis of **show** command output.

**Note:** Before issuing **debug** commands, see Important Information on Debug Commands.

- **debug dot11 aaa dot1x all** – This debug shows the various negotiations taken in EAP authentication, and what the results of those negotiations are.
- **debug radius authentication** – This debug shows the RADIUS negotiations between the server and client, both of which, in this case, are the AP.
- **debug radius local-server client** – This debug shows the authentication of the client from the RADIUS server's perspective.
- **debug radius local-server packets** – This debug shows all processing done by the RADIUS server, from it's perspective.

---

## Related Information

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.