

# Configuring the Cisco Access Registrar and LEAP

Document ID: 28901

---

## Introduction

### Prerequisites

Requirements

Components Used

Conventions

### Configuring EAP–Cisco Wireless (Cisco LEAP)

Step-by-Step Instructions

### Enabling EAP–Cisco (Cisco LEAP) on the AP

Step-by-Step Instructions

### Configuring ACU 6.00

Step-by-Step Instructions

### Traces from Cisco AR

### NetPro Discussion Forums – Featured Conversations

### Related Information

---

## Introduction

Cisco Networking Services Access Registrar (AR) 3.0 supports Light Extensible Authentication Protocol (LEAP) (EAP–Cisco Wireless). This document shows how to configure wireless Aironet Client Utilities and Cisco Aironet 340, 350, or 1200 series Access Points (APs) for LEAP authentication to the Cisco AR.

## Prerequisites

### Requirements

There are no specific prerequisites for this document.

### Components Used

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

- Cisco Aironet® 340, 350, or 1200 series Access Points
- AP Firmware 11.21 or later for Cisco LEAP
- Cisco Aironet 340 or 350 series Network Interface Cards (NICs)
- Firmware versions 4.25.30 or later for Cisco LEAP
- Network Driver Interface Specification (NDIS) 8.2.3 or later for Cisco LEAP
- Aironet Client Utilities (ACU) versions 5.02 or later
- Cisco Access Registrar 3.0 or later is required to run and authenticate Cisco LEAP and MAC authentication requests

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.

## Conventions

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

## Configuring EAP–Cisco Wireless (Cisco LEAP)

This section covers the basic configurations of Cisco LEAP on the Cisco AR server, the AP, and various clients.

### Step–by–Step Instructions

Follow these instructions to configure LEAP:

1. Change the port on the Cisco AR server.

The AP sends RADIUS information on User Datagram Protocol (UDP) ports 1812 (authentication) and 1813 (accounting). Since the Cisco AR listens on UDP ports 1645 and 1646 by default, you must configure the Cisco AR to listen on UDP ports 1812 and 1813.

- a. Issue the **cd /radius/advanced/ports** command.
- b. Issue the **add 1812** command to add port 1812.
- c. If you plan to do accounting, issue the **add 1813** command to add port 1813.

Save the configuration, and then restart the services.

2. To add the AP to the Cisco AR server, issue these commands:

- ◆ **cd /Radius/Clients**
- ◆ **add ap350–1**
- ◆ **cd ap350–1**
- ◆ **set ipaddress 171.69.89.1**
- ◆ **set sharedsecret cisco**

3. To configure the Wired Equivalent Privacy (WEP) key session timeout, issue these commands:

**Note:** 802.1x specifies a reauthentication option. The Cisco LEAP algorithm utilizes this option to expire the current WEP session key for the user and issue a new WEP session key.

- ◆ **cd /Radius/Profiles**
- ◆ **add ap–profile**
- ◆ **cd ap–profile**
- ◆ **cd attributes**
- ◆ **set session–timeout 600**

4. To create a user group that uses the profiles added in Step 3, issue these commands:

- ◆ **cd /Radius/Usergroups**
- ◆ **add ap–group**
- ◆ **cd ap–group**
- ◆ **set baseprofile ap–profile**

Users in this user group inherit the profile and in turn receive the session timeout.

5. To create users in a user list and to add the users to the user group defined in Step 4, issue these commands:

- ◆ **cd /Radius/Userlists**
- ◆ **add ap–users**
- ◆ **cd ap–users**

- ◆ **add user1**
  - ◆ **cd user1**
  - ◆ **set password Cisco**
  - ◆ **set group ap-group**
6. To create a local authentication and authorization service to use UserService "ap-userservice" and to set service type to "eap-leap", issue these commands:
- ◆ **cd /Radius/Services**
  - ◆ **add ap-localservice**
  - ◆ **cd ap-localservice**
  - ◆ **set type eap-leap**
  - ◆ **set UserService ap-userservice**
7. To create a user service "ap-userservice" to use the user list defined in Step 5, issue these commands:
- ◆ **cd /Radius/Services**
  - ◆ **add ap-userservice**
  - ◆ **cd ap-localservice**
  - ◆ **set type local**
  - ◆ **set userlist ap-users**
8. To set the default authentication and authorization service that Cisco AR uses to the service defined in Step 6, issue these commands:
- ◆ **cd /radius**
  - ◆ **set defaultauthenticationservice ap-localservice**
  - ◆ **set defaultauthorizationservice ap-localservice**
9. To save and reload the configuration, issue these commands:
- ◆ **save**
  - ◆ **reload**

## Enabling EAP-Cisco (Cisco LEAP) on the AP

### Step-by-Step Instructions

Follow these steps to enable Cisco LEAP on the AP:

1. Browse to the AP.
2. From the Summary Status page, click **SETUP**.
3. In the Services menu, click **Security > Authentication Server**.
4. Select the version of 802.1x to run on this AP in the 802.1x Protocol Version drop-down menu.
5. Configure the IP address of the Cisco AR in the Server Name/IP text box.
6. Verify the Server Type drop-down menu is set to **RADIUS**.
7. Change the Port text box to **1812**. This is the correct IP port number to use with the Cisco AR.
8. Configure the Shared Secret text box with the value used on the Cisco AR.
9. Select the **EAP Authentication** check box.
10. Modify the Timeout text box if so desired. This is the timeout value for an authentication request for the Cisco AR.
11. Click **OK** to return to the Security Setup screen.

If you are also doing RADIUS accounting, verify that the port on the Accounting Setup Page agrees with the port configured in the Cisco AR (set for 1813).

12. Click **Radio Data Encryption (WEP)**.
13. Configure a broadcast WEP key by typing in a 40- or 128-bit key value in the WEP Key 1 text box.

14. Select the authentication types to use. Make sure that, at a minimum, the **Network–EAP** check box is selected.
15. Verify the Use of Data Encryption drop–down menu is set to **Optional** or **Full Encryption**. Optional allows the use of non–WEP and WEP clients on the same AP. Be aware that this is an insecure mode of operation. Use Full Encryption when possible.
16. Click **OK** to finish.

## Configuring ACU 6.00

### Step–by–Step Instructions

Follow these steps to configure the ACU:

1. Open the ACU.
2. Click **Profile Manager** on the toolbar.
3. Click **Add** to create a new profile.
4. Enter the profile name in the text box, and then click **OK**.
5. Enter in the appropriate Service Set Identifier (SSID) in the SSID1 text box.
6. Click **Network Security**.
7. Select **LEAP** from the Network Security Type drop–down menu.
8. Click **Configure**.
9. Configure the password settings as needed.
10. Click **OK**.
11. Click **OK** on the Network Security screen.

## Traces from Cisco AR

Issue the **trace /r 5** to obtain trace output on the Cisco AR. If you need AP debug, you can connect to the AP via Telnet and issue the **eap\_diag1\_on** and **eap\_diag2\_on** commands.

```
06/28/2004 16:31:49: P1121: Packet received from 10.48.86.230
06/28/2004 16:31:49: P1121: Checking Message-Authenticator
06/28/2004 16:31:49: P1121: Trace of Access-Request packet
06/28/2004 16:31:49: P1121: identifier = 5
06/28/2004 16:31:49: P1121: length = 146
06/28/2004 16:31:49: P1121:
    reqauth = e5:4f:91:27:0a:91:82:6b:a4:81:c1:cc:c8:11:86:0b
06/28/2004 16:31:49: P1121: User-Name = user1
06/28/2004 16:31:49: P1121: NAS-IP-Address = 10.48.86.230
06/28/2004 16:31:49: P1121: NAS-Port = 37
06/28/2004 16:31:49: P1121: Service-Type = Login
06/28/2004 16:31:49: P1121: Framed-MTU = 1400
06/28/2004 16:31:49: P1121: Called-Station-Id = 000d29e160f2
06/28/2004 16:31:49: P1121: Calling-Station-Id = 00028adc8f2e
06/28/2004 16:31:49: P1121: NAS-Identifier = frinket
06/28/2004 16:31:49: P1121: NAS-Port-Type = Wireless - IEEE 802.11
06/28/2004 16:31:49: P1121: EAP-Message = 02:02:00:0a:01:75:73:65:72:31
06/28/2004 16:31:49: P1121:
    Message-Authenticator = f8:44:b9:3b:0f:33:34:a6:ed:7f:46:2d:83:62:40:30
06/28/2004 16:31:49: P1121: Cisco-AVPair = ssid=blackbird
06/28/2004 16:31:49: P1121: Using Client: ap1200-1 (10.48.86.230)
06/28/2004 16:31:49: P1121: Using Client ap1200-1 (10.48.86.230) as the NAS
06/28/2004 16:31:49: P1121: Authenticating and Authorizing with
    Service ap-localservice
06/28/2004 16:31:49: P1121: Response Type is Access-Challenge,
    skipping Remote Session Management.
06/28/2004 16:31:49: P1121: Response Type is Access-Challenge,
    skipping Local Session Management.
```

06/28/2004 16:31:49: P1121: Adding Message-Authenticator to response  
06/28/2004 16:31:49: P1121: Trace of Access-Challenge packet  
06/28/2004 16:31:49: P1121: identifier = 5  
06/28/2004 16:31:49: P1121: length = 61  
06/28/2004 16:31:49: P1121:  
    reqauth = 60:ae:19:8d:41:5e:a8:dc:4c:25:1b:8d:49:a3:47:c4  
06/28/2004 16:31:49: P1121: EAP-Message =  
    01:02:00:15:11:01:00:08:66:27:c3:47:d6:be:b3:67:75:73:65:72:31  
06/28/2004 16:31:49: P1121: Message-Authenticator =  
    59:d2:bc:ec:8d:85:36:0b:3a:98:b4:90:cc:af:16:2f  
06/28/2004 16:31:49: P1121: Sending response to 10.48.86.230  
06/28/2004 16:31:49: P1123: Packet received from 10.48.86.230  
06/28/2004 16:31:49: P1123: Checking Message-Authenticator  
06/28/2004 16:31:49: P1123: Trace of Access-Request packet  
06/28/2004 16:31:49: P1123: identifier = 6  
06/28/2004 16:31:49: P1123: length = 173  
06/28/2004 16:31:49: P1123:  
    reqauth = ab:f1:0f:2d:ab:6e:b7:49:9e:9e:99:00:28:0f:08:80  
06/28/2004 16:31:49: P1123: User-Name = user1  
06/28/2004 16:31:49: P1123: NAS-IP-Address = 10.48.86.230  
06/28/2004 16:31:49: P1123: NAS-Port = 37  
06/28/2004 16:31:49: P1123: Service-Type = Login  
06/28/2004 16:31:49: P1123: Framed-MTU = 1400  
06/28/2004 16:31:49: P1123: Called-Station-Id = 000d29e160f2  
06/28/2004 16:31:49: P1123: Calling-Station-Id = 00028adc8f2e  
06/28/2004 16:31:49: P1123: NAS-Identifier = frinket  
06/28/2004 16:31:49: P1123: NAS-Port-Type = Wireless - IEEE 802.11  
06/28/2004 16:31:49: P1123: EAP-Message =  
    02:02:00:25:11:01:00:18:5e:26:d6:ab:3f:56:f7:db:21:96:f3:b0:fb:ec:6b:  
    a7:58:6f:af:2c:60:f1:e3:3c:75:73:65:72:31  
06/28/2004 16:31:49: P1123: Message-Authenticator =  
    21:da:35:89:30:1e:e1:d6:18:0a:4f:3b:96:f4:f8:eb  
06/28/2004 16:31:49: P1123: Cisco-AVPair = ssid=blackbird  
06/28/2004 16:31:49: P1123: Using Client: ap1200-1 (10.48.86.230)  
06/28/2004 16:31:49: P1123: Using Client ap1200-1 (10.48.86.230) as the NAS  
06/28/2004 16:31:49: P1123: Authenticating and Authorizing  
    with Service ap-localservice  
06/28/2004 16:31:49: P1123: Calling external service ap-userservice  
    for authentication and authorization  
06/28/2004 16:31:49: P1123: Getting User user1's UserRecord  
    from UserList ap-users  
06/28/2004 16:31:49: P1123: User user1's MS-CHAP password matches  
06/28/2004 16:31:49: P1123: Processing UserGroup ap-group's check items  
06/28/2004 16:31:49: P1123: User user1 is part of UserGroup ap-group  
06/28/2004 16:31:49: P1123: Merging UserGroup ap-group's BaseProfiles  
    into response dictionary  
06/28/2004 16:31:49: P1123: Merging BaseProfile ap-profile  
    into response dictionary  
06/28/2004 16:31:49: P1123: Merging attributes into the Response Dictionary:  
06/28/2004 16:31:49: P1123: Adding attribute Session-Timeout, value = 600  
06/28/2004 16:31:49: P1123: Merging UserGroup ap-group's Attributes  
    into response Dictionary  
06/28/2004 16:31:49: P1123: Merging attributes into the Response Dictionary:  
06/28/2004 16:31:49: P1123: Removing all attributes except for  
    EAP-Message from response - they will be sent back in the Access-Accept  
06/28/2004 16:31:49: P1123: Response Type is Access-Challenge,  
    skipping Remote Session Management.  
06/28/2004 16:31:49: P1123: Response Type is Access-Challenge,  
    skipping Local Session Management.  
06/28/2004 16:31:49: P1123: Adding Message-Authenticator to response  
06/28/2004 16:31:49: P1123: Trace of Access-Challenge packet  
06/28/2004 16:31:49: P1123: identifier = 6  
06/28/2004 16:31:49: P1123: length = 44  
06/28/2004 16:31:49: P1123:  
    reqauth = 28:2e:a3:27:c6:44:9e:13:8d:b3:60:01:7f:da:8b:62  
06/28/2004 16:31:49: P1123: EAP-Message = 03:02:00:04

```

06/28/2004 16:31:49: P1123: Message-Authenticator =
    2d:63:6a:12:fd:91:9e:7d:71:9d:8b:40:04:56:2e:90
06/28/2004 16:31:49: P1123: Sending response to 10.48.86.230
06/28/2004 16:31:49: P1125: Packet received from 10.48.86.230
06/28/2004 16:31:49: P1125: Checking Message-Authenticator
06/28/2004 16:31:49: P1125: Trace of Access-Request packet
06/28/2004 16:31:49: P1125: identifier = 7
06/28/2004 16:31:49: P1125: length = 157
06/28/2004 16:31:49: P1125:
    reqauth = 72:94:8c:34:4c:4a:ed:27:98:ba:71:33:88:0d:8a:f4
06/28/2004 16:31:49: P1125: User-Name = user1
06/28/2004 16:31:49: P1125: NAS-IP-Address = 10.48.86.230
06/28/2004 16:31:49: P1125: NAS-Port = 37
06/28/2004 16:31:49: P1125: Service-Type = Login
06/28/2004 16:31:49: P1125: Framed-MTU = 1400
06/28/2004 16:31:49: P1125: Called-Station-Id = 000d29e160f2
06/28/2004 16:31:49: P1125: Calling-Station-Id = 00028adc8f2e
06/28/2004 16:31:49: P1125: NAS-Identifier = frinket
06/28/2004 16:31:49: P1125: NAS-Port-Type = Wireless - IEEE 802.11
06/28/2004 16:31:49: P1125: EAP-Message =
    01:02:00:15:11:01:00:08:3e:b9:91:18:a8:dd:98:ee:75:73:65:72:31
06/28/2004 16:31:49: P1125: Message-Authenticator =
    8e:73:2b:a6:54:c6:f5:d9:ed:6d:f0:ce:bd:4f:fl:d6
06/28/2004 16:31:49: P1125: Cisco-AVPair = ssid=blackbird
06/28/2004 16:31:49: P1125: Using Client: ap1200-1 (10.48.86.230)
06/28/2004 16:31:49: P1125: Using Client ap1200-1 (10.48.86.230) as the NAS
06/28/2004 16:31:49: P1125: Authenticating and Authorizing
    with Service ap-localservice
06/28/2004 16:31:49: P1125: Merging attributes into the Response Dictionary:
06/28/2004 16:31:49: P1125: Adding attribute Session-Timeout, value = 600
06/28/2004 16:31:49: P1125: Restoring all attributes to response
    that were removed in the last Access-Challenge
06/28/2004 16:31:49: P1125: No default Remote Session Service defined.
06/28/2004 16:31:49: P1125: Adding Message-Authenticator to response
06/28/2004 16:31:49: P1125: Trace of Access-Accept packet
06/28/2004 16:31:49: P1125: identifier = 7
06/28/2004 16:31:49: P1125: length = 142
06/28/2004 16:31:49: P1125:
    reqauth = 71:f1:ef:b4:e6:e0:c2:4b:0a:d0:95:47:35:3d:a5:84
06/28/2004 16:31:49: P1125: Session-Timeout = 600
06/28/2004 16:31:49: P1125: EAP-Message =
    02:02:00:25:11:01:00:18:86:5c:78:3d:82:f7:69:c7:96:70:35:31:bb:51:a7:ba:f8:48:8c:
    45:66:00:e8:3c:75:73:65:72:31
06/28/2004 16:31:49: P1125: Message-Authenticator = 7b:48:c3:17:53:67:44:f3:af:5e:17:27:3d
06/28/2004 16:31:49: P1125: Cisco-AVPair = 6c:65:61:70:3a:73:65:73:73:69:6f:6e:2d:6b:65:79
    :b8:1b:e9:2c:f9:9a:3e:83:55:ff:ae:54:57:4b:60:e1:03:05:fd:22:95:4c:b4:62
06/28/2004 16:31:49: P1125: Sending response to 10.48.86.230

```

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

## Related Information

- [Cisco Access Registrar Support Page](#)
  - [Documentation for Cisco Access Registrar](#)
  - [Fixed and Mobile Wireless Solution](#)
  - [Cisco Aironet Support Page](#)
  - [Technical Support – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jan 19, 2006

Document ID: 28901

---