

LEAP/MAC Authentication Configuration Guide

Document ID: 64066

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Configure

- LEAP Authentication

- MAC Authentication

Verify

Troubleshoot

Related Information

Introduction

This document provides a sample configuration for LEAP or MAC authentication.

Note: This guide assumes the most basic configuration. It does not cover configuration of more advanced encryption modes such as Cisco Key Integrity Protocol (CKIP) and Cisco Centralized Key Management (CCKM).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

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

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

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

LEAP Authentication

Configure Global Authentication Settings

Complete these steps:

1. On the ACS server, click **System Configuration** on the left.
2. Click **Global Authentication Setup**.
3. Check **Allow LEAP**.

Set Up the AP on the ACS

Complete these steps to set up the AP on the ACS:

1. On the ACS server, click **Network Configuration** on the left.
2. To add a AAA client, click **Add Entry**.
3. Enter these values in the boxes:
 - ◆ AAA Client IP Address IP_of_your_AP
 - ◆ Key Make up a key (make sure the key matches the AP shared secret key)
 - ◆ Authenticate Using RADIUS (Cisco Aironet)
4. Click **Submit**.
5. Restart.

Configure the AP

If you are using broadcast key rotation, you do not need to set a key as the key should already be set. If not, choose **Setup > Radio Advance**, and set a value for the broadcast key rotation. You do not need to set this any lower than five minutes (300 secs). Once the value is set, click **OK** and return to the radio data encryption page.

VxWorks

Complete these steps:

1. Open the AP.
2. Choose **Setup > Security > Authentication Server**.
3. Enter the ACS IP address.
4. Enter the shared secret (must match the ACS key).
5. Check the **EAP Authentication** box.
6. Click **Ok**.
7. Choose **Setup > Security > Radio Data Encryption**.
8. Check the **Open** box.
9. If you are not using broadcast key rotation, select WEP key 1 and 128.
10. Change the Use of Data Encryption by Stations to full Encryption (if you cannot change this, click **apply**).
11. Click **Ok**.

IOS AP Web Interface

Complete these steps:

1. Choose **Security > Server Manager**.
2. From the Current Server List drop-down list, choose RADIUS.

3. Enter the ACS IP address.
4. Enter the shared secret (must match the key in ACS).
5. Click **Apply**.
6. From the EAP Authentication drop-down list, choose the RADIUS server's IP address.
7. Click **Apply**.

SSID Manager (WEP Encryption Only)

Complete these steps for WEP encryption only:

1. Choose the SSID from the Current SSID List, or enter a new SSID in the SSID field.
2. Check the **Open Authentication** box.
3. From the drop-down list, choose with EAP.
4. Check the **Network EAP** box.
5. Click **Apply**.

Encryption Manager (WEP Encryption Only)

Complete these steps for WEP encryption only:

1. Choose **Security > Encryption Manager**.
2. Click the **WEP Encryption** radio button.
3. From the drop-down list, choose Mandatory.
4. Click the **Encryption Key 1** radio button.
5. Enter the key.
6. From the Key Size drop-down list, choose 128.
7. Click **Apply**.

Set Up the Client for LEAP

Complete these steps:

1. Open the ACU.
2. Choose **Manage Profile**.
3. Create a profile (or edit one).
4. Enter the client name and SSID of the AP.
5. Click the **Network Security** tab.
6. For Network Security Type, choose LEAP.
7. For WEP, select Use Dynamic WEP Keys.
8. Click **Ok**.
9. Click **Ok**.
10. Select the profile you created.

MAC Authentication

Add a MAC Address to ACS

Complete these steps:

1. From the ACS main menu, click on the **User Setup** button.
2. In the User text box, enter the MAC address to add to the user database.

Note: The MAC address must be exactly as it is sent by the AP for both the username and the password. If authentication fails, check the failed attempts log to see how the MAC is being reported

- by the AP. Do not cut and paste the MAC address, as this can introduce phantom characters.
3. On the User Setup screen, enter the MAC address in the Secure–PAP password text box.

Note: The MAC address must be exactly as it is sent by the AP for both the username and the password. If authentication fails, check the failed attempts log to see how the MAC is being reported by the AP. Do not cut and paste the MAC address, as this can introduce phantom characters.

4. Check the **Separate** (CHAP/MS–CHAP) box.
5. Enter a password for CHAP/MS–CHAP (this password should be different from the MAC address).
6. Click **Submit**.

Configure the AP

If you are using broadcast key rotation, you do not need to set a key as the key should already be set. If not, choose **Setup > Radio Advance**, and set a value for the broadcast key rotation. You do not need to set this any lower than five minutes (300 secs). Once the value is set, click **OK** and return to the radio data encryption page.

VxWorks

Complete these steps:

1. Open the AP.
2. Choose **Setup > Security > Authentication Server**.
3. Enter the ACS IP address.
4. Enter the shared secret (must match the ACS key).
5. Check the **EAP Authentication** box.
6. Click **Ok**.
7. Choose **Setup > Security > Radio Data Encryption**.
8. Check the **Open** box.
9. If you are not using broadcast key rotation, select WEP key 1 and 128.
10. Change the Use of Data Encryption by Stations to full Encryption (if you cannot change this, click **apply**).
11. Click **Ok**.

IOS AP Web Interface

Complete these steps:

1. Choose **Security > Server Manager**.
2. From the Current Server List drop–down list, choose RADIUS.
3. Enter the ACS IP address.
4. Enter the shared secret (must match the key in ACS).
5. Click **Apply**.
6. From the EAP Authentication drop–down list, choose the RADIUS server's IP address.
7. Click **Apply**.

SSID Manager (WEP Encryption Only)

Complete these steps for WEP encryption only:

1. Choose the SSID from the Current SSID List, or enter a new SSID in the SSID field.
2. Check the **Open Authentication** box.
3. From the drop–down list, choose with EAP.
4. Check the **Network EAP** box.

5. Click **Apply**.

Encryption Manager (WEP Encryption Only)

Complete these steps for WEP encryption only:

1. Choose **Security > Encryption Manager**.
2. Click the **WEP Encryption** radio button.
3. From the drop-down list, choose Mandatory.
4. Click the **Encryption Key 1** radio button.
5. Enter the key.
6. From the Key Size drop-down list, choose 128.
7. Click **Apply**.

Set Up the Client for LEAP

Complete these steps:

1. Open the ACU.
2. Select Manage Profile.
3. Create a profile (or edit one).
4. Enter the client name and SSID of the AP.
5. Click the **Network Security** tab.
6. For Network Security Type, select LEAP.
7. For WEP, select Use Dynamic WEP Keys.
8. Click **Ok**.
9. Click **Ok**.
10. Select the profile you created.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- [Cisco Secure Access Control Server for Unix](#)
- [Cisco Secure Access Control Server for Windows](#)
- [Technical Support – Cisco Systems](#)

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

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 14, 2009

Document ID: 64066
