

EAP-FAST 1.02 Configuration Guide

Document ID: 64063

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Set Up the AP on the ACS
- Set Up the ACS for EAP-FAST
- Configure the AP
- Set Up the Client for EAP-FAST

Manual PAC Provisioning Supplement

- Set Up ACS Options for EAP-FAST
- Create the PAC(s) Using CSUtil.exe

Verify

Troubleshoot

Related Information

Introduction

This document provides a sample configuration for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) Version 1.02.

Prerequisites

Requirements

Before attempting this configuration, ensure that you meet these requirements:

- IOS AP 12.2(13)JA3, 350, or CB20A client with firmware version 5.40 and driver version 8.5 (CB21AG client to be supported 2H CY2004)
- Access Control Server (ACS) 3.2.3, Windows 2000, or XP with ACU 6.3 installed.

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

Set Up the AP on the ACS

Complete these steps to set up the access point (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.

Set Up the ACS for EAP-FAST

Complete these steps to set up the ACS for EAP-FAST:

1. Choose **System Configuration > Global Authentication Setup**.
2. Check the **Allow EAP-FAST** box.
3. Enter a value in the Authority ID Info field (spaces are not supported).
4. Check the **Allow automatic PAC provisioning** box.

Note: Automatic PAC provisioning is a low overhead method of providing the client with a PAC in-band. There are a few caveats to automatic provisioning:

- a. Auto-provisioning requires the initial EAP-FAST authentication to fail.
 - b. LDAP users *cannot* be auto-provisioned and must be manually provisioned.
 - c. Auto-provisioning is susceptible to a MITM attack during initial provisioning.
5. Check the **EAP-FAST master server** box.
 6. Click **Submit**.
 7. Restart.

Configure the AP

Complete these steps to configure the AP:

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**.

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**.

Encryption Manager (WPA Key Management)

Complete these steps for WPA key management:

1. Choose **Security > Encryption Manager**.
2. Click the **Cipher** radio button.
3. From the drop-down list, choose TKIP.
4. 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**.

SSID Manager (WPA Key Management)

Complete these steps for WPA key management:

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. Select Authenticated Key Management.
6. From the drop-down list, choose Mandatory.
7. Check **WPA** box.
8. Click **Apply**.

Set Up the Client for EAP-FAST

WEP Encryption Only

Complete these steps For WEP encryption only:

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. Select EAP-FAST.
7. Click **Configure**.
8. Check the **Allow Automatic PAC Provisioning for This Profile** box.

Note: Automatic PAC provisioning is a low overhead method of providing the client with a PAC in-band. There are a few caveats to automatic provisioning:

- a. Auto-provisioning requires the initial EAP-FAST authentication to fail.
 - b. LDAP users *cannot* be auto-provisioned and must be manually provisioned.
 - c. Auto-provisioning is susceptible to a MITM attack during initial provisioning.
9. Click **Ok**.
 10. Click **Ok**.
 11. Click **Ok**.
 12. Select the profile you created.

WPA Key Management

Complete these steps for WPA key management:

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. Check the **WiFi Protected Access (WPA)** box.
7. For Network Security Type, select EAP-FAST (WPA).
8. Click **Configure**.
9. Check the **Allow Automatic PAC Provisioning for This Profile** box.

Note: Automatic PAC Provisioning is a low overhead method of providing the client with a PAC in-band. There are a few caveats to automatic provisioning:

- a. Auto-provisioning requires the initial EAP-FAST authentication to fail.
 - b. LDAP users *cannot* be auto-provisioned and must be manually provisioned.
 - c. Auto-provisioning is susceptible to a MITM attack during initial provisioning.
10. Click **Ok**.
 11. Click **Ok**.
 12. Click **Ok**.
 13. Select the profile you created.

Manual PAC Provisioning Supplement

This section includes the procedures that vary from those already presented for configuring manual PAC provisioning.

Note: Option **EAP-FAST PAC Files Generation** is not available on ACS for windows and the procedure must be done manually using the procedure defined in this section.

Set Up ACS Options for EAP-FAST

These steps are optional. If you want some clients to use automatic provisioning, leave this option checked.

1. Choose **System Configuration > Global Authentication Setup**.
2. Uncheck the **Allow automatic PAC provisioning** box.

Create the PAC(s) Using CSUtil.exe

This procedure can vary greatly depending on your requirements. Refer to the User Guide for Cisco Secure ACS for Windows Server 3.2 for more information.

The basic syntax for cutting a PAC with CSUtil.exe is:

```
csutil [-t] [-filepath <full filepath>] [-passwd <password>] [[-a] [-g <group number>]  
[-u <user name>] [-f <full filepath>]]
```

`-filepath` is optional and specifies the directory for output (directory must already exist). If unspecified, the PACs are placed in the ACS Utils directory (which can get messy if you create a lot of PACs).

`-passwd` is optional and specifies the password to protect the PAC. If unspecified, there is no default password.

These are a few examples of valid PAC creation commands:

- `csutil -t -filepath c:\acspac -passwd 5p0rk5 -f c:\acspac\pac.txt` Creates PAC for users listed in a file named `pac.txt`.
- `csutil -t -filepath c:\acspac -passwd 5p0rk5 -g 0` Creates PAC for users in ACS group 0.
- `csutil -t -filepath c:\acspac -passwd 5p0rk5 -u vadablam` Creates PAC for username `vadablam` in ACS.
- `csutil -t -filepath c:\acspac -passwd 5p0rk5 -a` Creates PAC for *all* users in ACS (this can take quite awhile).

Complete these steps to create a PAC for a single user for testing purposes:

1. Create a directory to output the PAC to (optional).
2. Verify that the user exists in ACS.
3. Open a command prompt.
4. Navigate to the ACS Utils directory.
5. Enter the `csutil -t -filepath <filepath> -passwd <password> -u <user>` command.
6. Copy the new `.pac` file to the user's host.

Complete these steps to configure the client for manual PAC provisioning:

1. After selecting EAP-FAST as your Network Security Type in the ACU, click **Configure**.
2. Uncheck the **Allow Automatic PAC Provisioning for This Profile** box.
3. Click **Import**.
4. Browse to the `.pac`.
5. Select the `.pac`.
6. Enter the password (if prompted).
7. Click **Ok**.
8. Click **Ok**.
9. Click **Ok**.
10. Click **Ok**.
11. Select the profile you created.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Refer to these documents for more information:

- [INFO: Error Codes in Windows NT Part 1 of 2 \(article I\)](#)
- [How To Error Codes in Windows NT Part 2 of 2](#)

Related Information

- [Cisco Secure ACS for Windows Support Page](#)
 - [Documentation for Cisco Secure ACS for Windows](#)
 - [Cisco Secure ACS for UNIX Support Page](#)
 - [Documentation for Cisco Secure ACS for UNIX](#)
 - [Technical Support & Documentation – 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: 64063
