

Guía de configuración de la versión 1.02 del EAP-FAST

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Configure el AP en el ACS](#)

[Configure el ACS para el EAP-FAST](#)

[Configure el AP](#)

[Configure al cliente para el EAP-FAST](#)

[Suplemento manual del aprovisionamiento PAC](#)

[Opciones de ACS de la configuración para el EAP-FAST](#)

[Cree el PAC usando CSUtil.exe](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento suministra una configuración de ejemplo para Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) Versión 1.02.

prerrequisitos

Requisitos

Antes de utilizar esta configuración, asegúrese de que cumple con estos requisitos:

- IOS AP 12.2(13)JA3, 350, o cliente CB20A con la versión de firmware 5.40 y la versión del driver 8.5 (cliente del CB21AG a ser 2H soportado CY2004)
- Access Control Server (ACS) 3.2.3, Windows 2000, o XP con ACU 6.3 instalado.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Para obtener más información sobre las convenciones del documento, consulte las [Convenciones de Consejos Técnicos de Cisco](#).

[Configurar](#)

[Configure el AP en el ACS](#)

Complete estos pasos para configurar el punto de acceso en el ACS:

1. En el servidor ACS, haga clic la **configuración de red** a la izquierda.
2. Para agregar a un cliente AAA, el tecleo **agrega la entrada**.
3. Ingrese estos valores en los rectángulos: Dirección IP del cliente AAA — IP_of_your_APClave — Componga un dominante (asegurese la clave hace juego la clave secreta compartida AP)Autentique usando — RADIUS (Cisco Aironet)
4. Haga clic en Submit (Enviar).
5. Reinicio.

[Configure el ACS para el EAP-FAST](#)

Complete estos pasos para configurar el ACS para el EAP-FAST:

1. Elija la **configuración de la configuración del sistema > de la autenticación global**.
2. Marque el cuadro del **EAP-FAST de la permit**.
3. Ingrese un valor en el campo de información ID de la autoridad (los espacios no se soportan).
4. Marque el cuadro **automático del aprovisionamiento de la permit PAC**. **Nota:** El aprovisionamiento automático PAC es un método de arriba bajo de proveer del cliente una en-banda PAC. Hay algunas advertencias al aprovisionamiento automático: el Auto-aprovisionamiento requiere la autenticación inicial del EAP-FAST fallar. Los usuarios LDAP *no pueden* ser auto-aprovisionado y deben ser manualmente aprovisionado. el Auto-aprovisionamiento es susceptible a un ataque MITM durante el aprovisionamiento inicial.
5. Marque el cuadro del **servidor del master del EAP-FAST**.
6. Haga clic en Submit (Enviar).
7. Reinicio.

[Configure el AP](#)

Complete estos pasos para configurar el AP:

1. Elija la **Seguridad > al administrador de servidor**.
2. De la lista desplegable de la lista del servidor actual, elija el RADIUS.

3. Ingrese el IP Address ACS.
4. Ingrese el secreto compartido (debe corresponder con la clave en el ACS).
5. Haga clic en Apply (Aplicar).
6. De la lista desplegable de la autenticación EAP, elija la dirección IP del servidor de RADIUS.
7. Haga clic en Apply (Aplicar).

[Administrador del cifrado \(encriptación WEP solamente\)](#)

Complete estos pasos para la encriptación WEP solamente:

1. Elija **Security > Encryption Manager**.
2. Haga clic el botón de radio de la **encriptación WEP**.
3. De la lista desplegable, elija obligatorio.
4. Haga clic el botón de radio de la **clave de encriptación 1**.
5. Ingrese la clave.
6. De la lista desplegable del tamaño de clave, elija el 128.
7. Haga clic en Apply (Aplicar).

[Administrador del cifrado \(administración de claves WPA\)](#)

Complete estos pasos para la administración de claves WPA:

1. Elija **Security > Encryption Manager**.
2. Haga clic el botón de radio de la **cifra**.
3. De la lista desplegable, elija el TKIP.
4. Haga clic en Apply (Aplicar).

[Administrador SSID \(encriptación WEP solamente\)](#)

Complete estos pasos para la encriptación WEP solamente:

1. Elija el SSID de la lista actual SSID, o ingrese un nuevo SSID en el campo SSID.
2. Marque el cuadro de la **autenticación abierta**.
3. De la lista desplegable, elija con el EAP.
4. Marque el cuadro de la **red EAP**.
5. Haga clic en Apply (Aplicar).

[Administrador SSID \(administración de claves WPA\)](#)

Complete estos pasos para la administración de claves WPA:

1. Elija el SSID de la lista actual SSID, o ingrese un nuevo SSID en el campo SSID.
2. Marque el cuadro de la **autenticación abierta**.
3. De la lista desplegable, elija con el EAP.
4. Marque el cuadro de la **red EAP**.
5. Seleccione la administración de claves autenticada.
6. De la lista desplegable, elija obligatorio.
7. Marque el cuadro **WPA**.

8. Haga clic en Apply (Aplicar).

[Configure al cliente para el EAP-FAST](#)

[Encriptación WEP solamente](#)

Complete estos pasos para la encriptación WEP solamente:

1. Abra el ACU.
2. Selecto maneje el perfil.
3. Cree un perfil (o edite uno).
4. Ingrese el Nombre del cliente y el SSID del AP.
5. Haga clic la **ficha de seguridad de la red**.
6. Seleccione el EAP-FAST.
7. Haga clic en Configure (Configurar).
8. Marque el **aprovisionamiento automático de la permit PAC para este** cuadro del **perfil**.**Nota:** El aprovisionamiento automático PAC es un método de arriba bajo de proveer del cliente una en-banda PAC. Hay algunas advertencias al aprovisionamiento automático:el Auto-aprovisionamiento requiere la autenticación inicial del EAP-FAST fallar.Los usuarios LDAP *no pueden* ser auto-aprovisionado y deben ser manualmente aprovisionado.el Auto-aprovisionamiento es susceptible a un ataque MITM durante el aprovisionamiento inicial.
9. **Autorización del teclado.**
10. **Autorización del teclado.**
11. **Autorización del teclado.**
12. Seleccione el perfil que usted creó.

[Administración de claves WPA](#)

Complete estos pasos para la administración de claves WPA:

1. Abra el ACU.
2. Selecto maneje el perfil.
3. Cree un perfil (o edite uno).
4. Ingrese el Nombre del cliente y el SSID del AP.
5. Haga clic la **ficha de seguridad de la red**.
6. Marque el cuadro **protegido WiFi del acceso (WPA)**.
7. Para el tipo de la seguridad de la red, seleccione el EAP-FAST (WPA).
8. Haga clic en Configure (Configurar).
9. Marque el **aprovisionamiento automático de la permit PAC para este** cuadro del **perfil**.**Nota:** El aprovisionamiento automático PAC es un método de arriba bajo de proveer del cliente una en-banda PAC. Hay algunas advertencias al aprovisionamiento automático:el Auto-aprovisionamiento requiere la autenticación inicial del EAP-FAST fallar.Los usuarios LDAP *no pueden* ser auto-aprovisionado y deben ser manualmente aprovisionado.el Auto-aprovisionamiento es susceptible a un ataque MITM durante el aprovisionamiento inicial.
10. **Autorización del teclado.**
11. **Autorización del teclado.**
12. **Autorización del teclado.**

13. Seleccione el perfil que usted creó.

Suplemento manual del aprovisionamiento PAC

Esta sección incluye los procedimientos que varían de éstos presentados ya para configurar el aprovisionamiento manual PAC.

Nota: La generación de los archivos del EAP-FAST PAC de la opción no está disponible en el ACS para las ventanas y el procedimiento se debe hacer manualmente usando el procedimiento definido en esta sección.

Opciones de ACS de la configuración para el EAP-FAST

Estos pasos son opcionales. Si usted quisiera que algunos clientes utilizaran el aprovisionamiento automático, deje esta opción marcada.

1. Elija la configuración de la configuración del sistema > de la autenticación global.
2. Desmarque el cuadro automático del aprovisionamiento de la permit PAC.

Cree el PAC usando CSUtil.exe

Este procedimiento puede variar grandemente dependiendo de sus requisitos. Refiera al [guía del usuario para el servidor 3.2 del Cisco Secure ACS for Windows](#) para más información.

El sintaxis básico para cortar un PAC con CSUtil.exe es:

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

- el `filepath` es opcional y especifica el directorio para la salida (el directorio debe existir ya). Si están sin especificar, los PAC se colocan en el directorio ACS Utils (que puede conseguir sucio si usted crea muchos PAC).

- el `passwd` es opcional y especifica la contraseña para proteger el PAC. Si está sin especificar, no hay contraseña predeterminada.

Esta área algunos comandos de los ejemplos de creación PAC válida:

- `csutil - t - filepath c:\acspac - el passwd 5p0rk5 - f c:\acspac\pac.txt` — crea el PAC para los usuarios enumerados en un archivo nombrado `pac.txt`.
- `csutil - t - filepath c:\acspac - el passwd 5p0rk5 - g 0` — crea el PAC para los usuarios en el grupo 0 ACS.
- `csutil - t - filepath c:\acspac - el passwd 5p0rk5 - vadablam u` — crea el PAC para el nombre de usuario `vadablam` en el ACS.
- `csutil - t - filepath c:\acspac - el passwd 5p0rk5 - a` — crea el PAC para *todos los* usuarios en el ACS (esto puede tomar muy un rato).

Complete estos pasos para crear un PAC para un único usuario para comprobar:

1. Cree un directorio para hacer salir el PAC a (opcional).
2. Verifique que el usuario exista en el ACS.

3. Abra un comando prompt.
4. Navegue al directorio ACS Utils.
5. Ingrese el **comando csutil -t -filepath <filepath> -passwd <password> -u <user>**.
6. Copie el nuevo archivo .pac al host del usuario.

Complete estos pasos para configurar al cliente para el aprovisionamiento manual PAC:

1. Después de seleccionar el EAP-FAST como su seguridad de la red teclee adentro el ACU, **configuración del tecleo**.
2. Desmarque el **aprovisionamiento automático de la permit PAC para este cuadro del perfil**.
3. Haga clic la **importación**.
4. Hojee al .pac.
5. Seleccione el .pac.
6. Ingrese la contraseña (si está indicado).
7. Haga clic la **autorización**.
8. Haga clic la **autorización**.
9. Haga clic la **autorización**.
10. Haga clic la **autorización**.
11. Seleccione el perfil que usted creó.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Si desea más información, consulte estos documentos:

- [INFO: Códigos de error en la parte 1 del Windows NT de 2 \(artículo 1\)](#)
- [Cómo a los códigos de error en la parte 2 del Windows NT de 2](#)

Información Relacionada

- [Página de soporte de Cisco Secure ACS para Windows](#)
- [Página de soporte de Cisco Secure ACS para Windows](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)