# Ejemplo de Configuración de Generación PuTTYgen de Claves Autorizadas SSH y Autenticación RSA en Cisco Secure IDS

## Contenido



## Introducción

Este documento explica cómo utilizar el generador de claves para PuTTY (PuTTYgen) para generar claves autorizadas de Secure Shell (SSH) y la autenticación RSA para su uso en el Sistema Seguro de Detección de Intrusos (IDS) de Cisco. El problema principal cuando establece claves autorizadas de SSH es que solamente es aceptable el formato de clave RSA1 más antiguo. Esto significa que necesita indicar al generador de claves que cree una clave RSA1 y debe restringir el cliente SSH para que use el protocolo SSH1.

## Prerequisites

### Requirements

No hay requisitos específicos para este documento.

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- PuTTY reciente - 7 de febrero de 2004
- Cisco Secure IDS

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). If your network is live, make sure that you understand the potential impact of any command.

### Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

## Configurar

En esta sección se presenta información para configurar las características que este documento describe.

Nota: Utilice la Command Lookup Tool (sólo clientes registrados) para encontrar información adicional sobre los comandos que utiliza este documento.

### Configurar PuTTYgen

Complete estos pasos para configurar PuTTYgen.

1. Inicie PuTTYgen.
2. Haga clic en el tipo de clave SSH1 y establezca el número de bits en la clave generada en 2048 en el grupo Parámetros en la parte inferior del cuadro de diálogo.
3. Haga clic en Generar y siga las instrucciones.

   La información clave se muestra en la sección superior del cuadro de diálogo.
4. Desactive el cuadro de edición Comentario de clave.
5. Seleccione todo el texto de la clave pública para pegarlo en el archivo authorized_keys y presione Ctrl-C.
6. Escriba una frase de paso en los cuadros Key passphrase (Frase de paso clave) y Confirm passphrase edit (Confirmar frase de paso).
7. Haga clic en Guardar clave privada.
8. Guarde el archivo de clave privada PuTTY en un directorio privado para iniciar sesión en Windows (en el subárbol Documents and Settings/(userid)/My Documents de Windows 2000/XP).
9. Lanza PuTTY.
10. Cree una nueva sesión PuTTY como se muestra a continuación:

- Sesión:
- Dirección IP: dirección IP del sensor IDS
- Protocolo: SSH
- Puerto: 22
- Conexión:
- Nombre de usuario de inicio de sesión automático: cisco (también puede ser el nombre de usuario que utiliza en el sensor)
- Conexión/SSH:
- Versión SSH preferida: 1 solamente
- Connection/SSH/Auth:
- Archivo de clave privada para la autenticación: busque el archivo .PPK almacenado en el paso 8.
- Sesión: (volver al principio)
- Sesiones guardadas: (introduzca el nombre del sensor y haga clic en Guardar)

11. Haga clic en Open y utilice la autenticación de contraseña para conectarse a la CLI del sensor, ya que la clave pública aún no está en el sensor.
12. Ingrese el comando configure terminal CLI y presione Enter.
13. Ingrese el comando ssh authorized-key mykey CLI, pero no presione Enter en este momento. Asegúrese de escribir un espacio al final.
14. Haga clic con el botón derecho en la ventana de terminal PuTTY.

    El material del portapapeles copiado en el paso 5 se escribe en la CLI.
15. Press Enter.
16. Ingrese el comando exit y presione Enter.
17. Confirme que la clave autorizada se ha introducido correctamente. Ingrese el comando show ssh authorized-keys mykey y presione Enter.
18. Ingrese el comando exit para salir de la CLI de IDS y presione Enter.

# Verificación

## Autenticación RSA

Complete los siguientes pasos.

1. Lanza PuTTY.
2. Busque la sesión guardada creada en el paso 10 y haga doble clic en ella. Se abre una ventana de terminal PuTTY y aparece este texto:

```
Sent username "cisco"
Trying public key authentication.
Passphrase for key "":
```

3. Escriba la frase de contraseña de clave privada que ha creado en el paso 6 y pulse Intro.

   La sesión se iniciará automáticamente.

## Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

## Información Relacionada

- Páginas de soporte técnico de Network Intrusion Detection
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).