

# Configuración de ISE SFTP con autenticación basada en certificados

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[1. Configuración del servidor CentOS](#)

[2. Configuración del repositorio de ISE](#)

[3. Generar pares clave en el servidor ISE](#)

[3.1. GUI de ISE](#)

[3.2. CLI de ISE](#)

[4. Integración](#)

[Verificación](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo configurar un servidor Linux con distribución CentOS como servidor de protocolo de transferencia de archivos seguro (SFTP) con autenticación de infraestructura de clave pública (PKI) hacia Identity Services Engine (ISE).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento general de ISE
- configuración del repositorio ISE
- Conocimiento general básico de Linux

### Componentes Utilizados

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

- ISE 2.2
- ISE 2.4
- ISE 2.6

- ISE 2.7
- ISE 3.0
- CentOS Linux versión 8.2.2004 (Core)

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. Si su red está activa, asegúrese de comprender el impacto potencial de cualquier comando.

## Antecedentes

Para aplicar la seguridad para las transferencias de archivos, ISE puede autenticarse a través de certificados PKI a través de SFTP para garantizar una forma más segura de acceder a los archivos de repositorios.

## Configurar

### 1. Configuración del servidor CentOS

#### 1.1 Cree un directorio como usuario raíz.

```
mkdir -p /cisco/engineer
```

#### 1.2. Cree un grupo de usuarios.

```
groupadd tac
```

1.3. Este comando agrega el usuario al directorio principal (archivos), especifica que el usuario pertenece a los **ingenieros** de grupo.

```
useradd -d /cisco/engineer -s /sbin/nologin engineer  
usermod -aG tac engineer
```

**Nota:** La parte **/sbin/nologin** del comando indica que el usuario no podrá iniciar sesión a través de Secure Shell (SSH).

#### 1.4. Proceda a crear el directorio para cargar los archivos.

```
mkdir -p /cisco/engineer/repo
```

##### 1.4.1 Establecer permisos para los archivos de directorio.

```
chown -R engineer:tac /cisco/engineer/repo  
find /cisco/engineer/repo -type d -exec chmod 2775 {} \+  
find /cisco/engineer/repo -type f -exec chmod 664 {} \+
```

1.5. Cree el directorio y el archivo en el que el servidor CentOS realiza la verificación de los certificados.

Directorio:

```
mkdir /cisco/engineer/.ssh
chown engineer:engineer /cisco/engineer/.ssh
chmod 700 /cisco/engineer/.ssh
```

Archivo:

```
touch /cisco/engineer/.ssh/authorized_keys
chown engineer:engineer /cisco/engineer/.ssh/authorized_keys
chmod 600 /cisco/engineer/.ssh/authorized_keys
```

1.6. Cree los permisos de inicio de sesión en el archivo **sshd\_config** del sistema.

Para editar el archivo, puede utilizar la herramienta **vim** Linux con este comando.

```
vim /etc/ssh/sshd_config
```

1.6.1 Agregue las líneas especificadas a continuación.

```
#Subsystem sftp /usr/libexec/openssh/sftp-server
Subsystem sftp internal-sftp
Match Group tac
ChrootDirectory %h
X11Forwarding no
AllowTCPForwarding no
ForceCommand internal-sftp
```

1.7. Ejecute el comando para verificar los sintaxis del archivo del sistema **sshd\_config**.

```
sshd -t
```

**Nota:** Ningún resultado significa que la sintaxis del archivo es correcta.

1.8. Proceda a reiniciar el servicio SSH.

```
systemctl restart sshd
```

**Nota:** Algunos servidores Linux tienen aplicación **selinux**, para confirmar este parámetro, puede utilizar el **comando getenforce**. Como recomendación, si está en modo **de ejecución**, cámbielo a **permisivo**.

1.9. (opcional) Edite el archivo **semanage.conf** para establecer la aplicación en permisiva.

```
vim /etc/selinux/semanage.conf
```

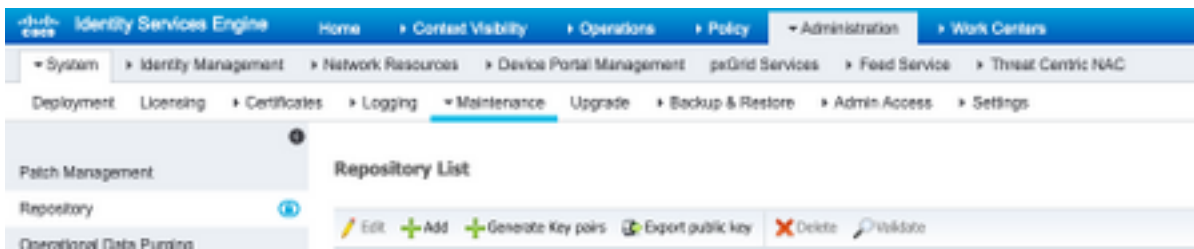
Agregue el comando **setenforce0**.

```
setenforce0
```

## 2. Configuración del repositorio de ISE

2.1. Continúe agregando el repositorio a través de la interfaz gráfica de usuario (GUI) de ISE.

Vaya a **Administración>Mantenimiento del sistema>Repositorio>Agregar**



2.2. Introduzca la configuración adecuada para su repositorio.

[Repository List > Add Repository](#)

### Repository Configuration

\* Repository Name

\* Protocol

**Location**

\* Server Name

\* Path

**Credentials**

\* Enable PKI authentication

\* User Name

\* Password

**Nota:** Si necesita acceder al directorio de repo en lugar del directorio raíz del ingeniero, la ruta de destino debe ser /repo/.

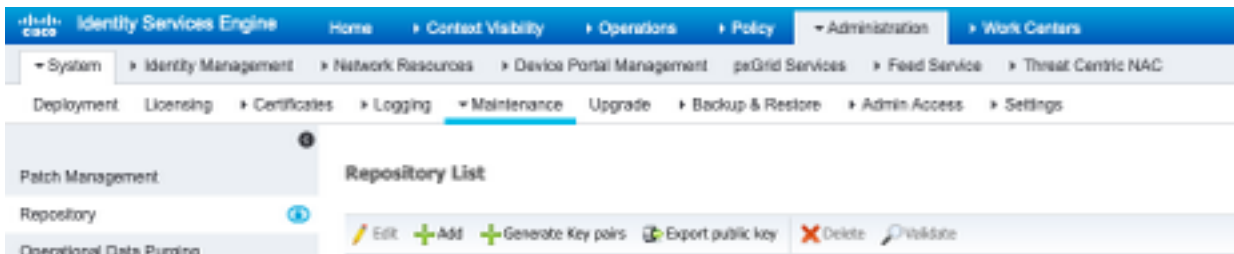


## 3. Generar pares clave en el servidor ISE

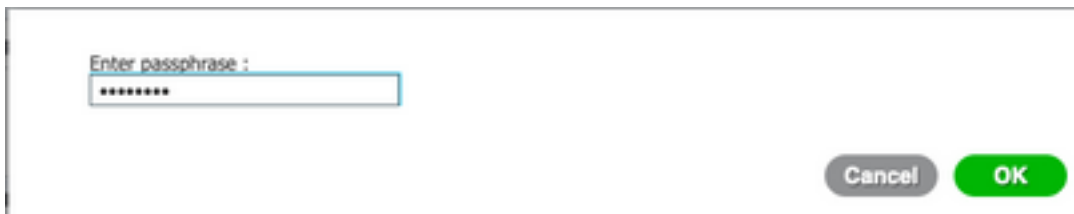
### 3.1. GUI de ISE

Vaya a **Administración>Mantenimiento del sistema>Repositorio>Generar pares de claves**, como se muestra en la imagen.

**Nota:** Debe generar pares clave desde la GUI de ISE y la interfaz de línea de comandos (CLI) para tener acceso bidireccional completo al repositorio.



3.1.1. Introduzca una frase de paso, lo cual es necesario para proteger el par de claves.

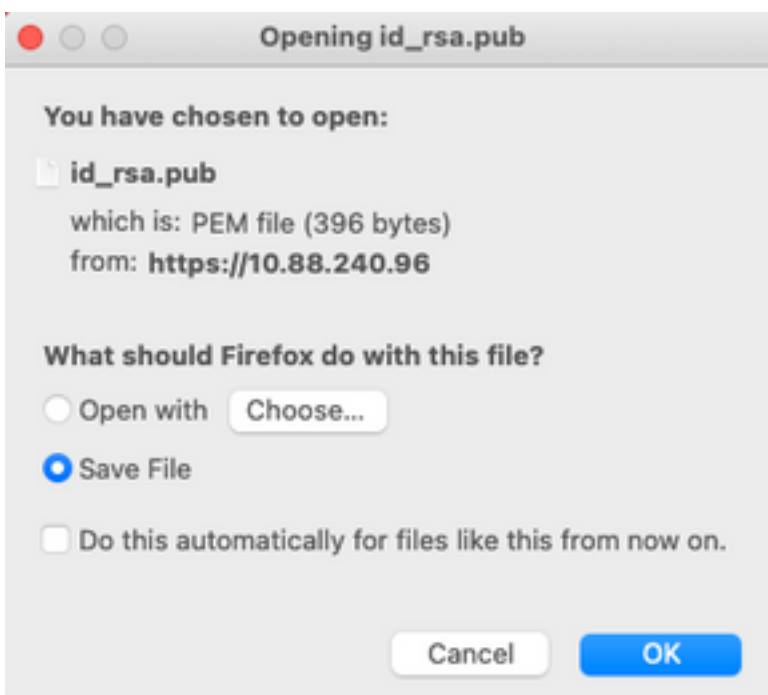


**Nota:** Primero, genere los pares de claves antes de exportar las claves públicas.

3.1.2. Proceda a exportar la clave pública.

Vaya a **Administración>Mantenimiento del sistema>Repositorio>Exportar clave pública**.

Seleccione **Exportar clave pública**. Se genera un archivo con el nombre **id\_rsa.pub** (asegúrese de que se guarda para futuras referencias).



## 3.2. CLI de ISE

3.2.1. Vaya a la CLI del nodo en el que desea finalizar la configuración del repositorio.

**Nota:** A partir de este punto, se necesitarán los siguientes pasos en cada nodo que desee permitir el acceso al repositorio SFTP con el uso de la autenticación PKI.

3.2.2. Ejecute este comando para agregar la IP del servidor Linux al archivo del sistema `host_key`.

```
crypto host key add host <Linux server IP>  
ise24https/admin# crypto host_key add host 10.88.240.102  
host key fingerprint added  
# Host 10.88.240.102 found: line 2  
10.88.240.102 RSA_SHA256:sFA1b+NujB8NxIx4zhS/7Fj1hyHRkJlKyLhJClteSpE
```

3.2.3. Genere una clave pública de CLI.

```
crypto key generate rsa passphrase <passphrase>  
ise24https/admin# crypto key generate rsa passphrase admin123
```

3.2.4. Exporte los archivos de clave pública desde la CLI de ISE con este comando.

```
crypto key export <name of the file> repository <repository name>
```

**Nota:** Debe tener un repositorio al que previamente se haya podido acceder y al que pueda exportar el archivo de clave pública.

```
ise24https/admin# crypto key export public repository FTP
```

## 4. Integración

4.1. Inicie sesión en su servidor CentOS.

Navegue hasta la carpeta en la que configuró previamente el archivo `authorized_key`.


4.2. Edite el archivo de clave autorizado.

Ejecute el comando `vim` para modificar el archivo.

```
vim /cisco/engineer/.ssh/authorized_keys
```

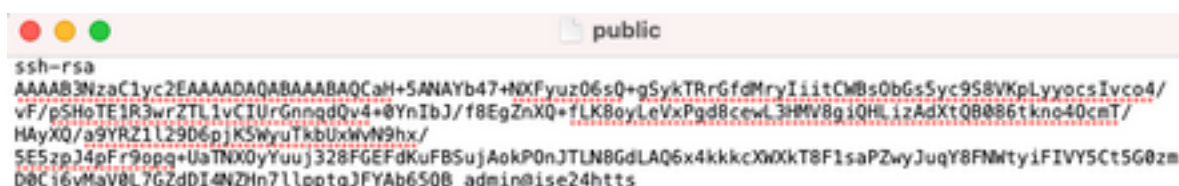
4.3. Copie y pegue el contenido generado en los pasos 4 y 6 de la sección **Generar pares clave**.

Clave pública generada a partir de la GUI de ISE:



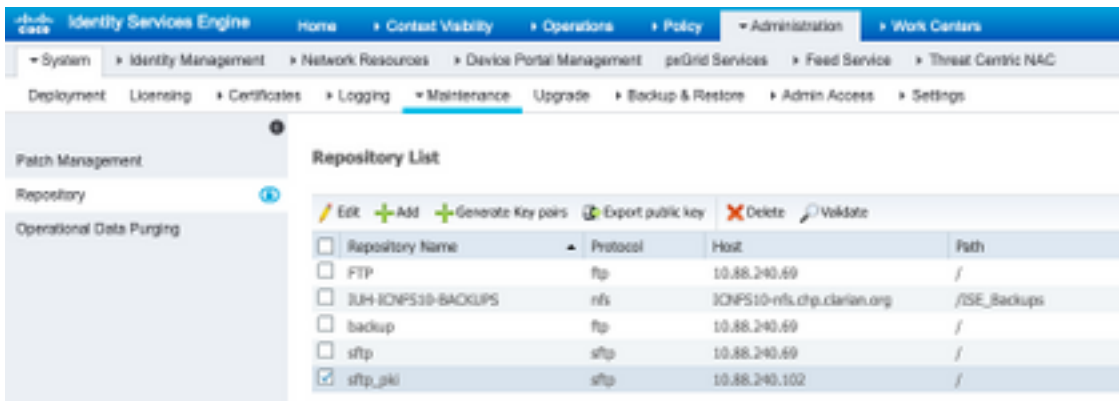
```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAH+5ANAYb47+HXFyuz06s0+gSykTRrGfdMryIiitCMBs0bGs5yc9S8VKpLyyocsIvco4/  
vF/pSHoTE1R3wrZTLlvCIUrGnngdQv4+@YnIbJ/f8EgZnXQ+fLK8oyLeVxPgD8cewL3HMV8giQHLizAdXtQ8086tkno40cmT/  
HAYXQ/a9YRZ1L2906pjK5WyuTkbUxwV9hx/  
SE5zpJ4pFr9opq+UaTNX0yYuuJ328FGEFdkuFBSuJAokP0nJTLN8GdLAQ6x4kkkXwXkT8F1saPZwyJuqY8FNWtyiFIVY5Ct5G0zm  
D0Cj6vMaV0L7GzdDI4NZHn7llpptqJFYAb65QB admin@ise24https
```

Clave pública generada desde la CLI de ISE:

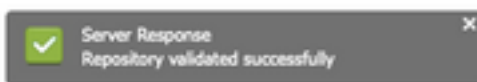


```
ssh-rsa  
AAAAB3NzaC1yc2EAAAADAQABAAQCAH+5ANAYb47+HXFyuz06s0+gSykTRrGfdMryIiitCMBs0bGs5yc9S8VKpLyyocsIvco4/  
vF/pSHoTE1R3wrZTLlvCIUrGnngdQv4+@YnIbJ/f8EgZnXQ+fLK8oyLeVxPgD8cewL3HMV8giQHLizAdXtQ8086tkno40cmT/  
HAYXQ/a9YRZ1L2906pjK5WyuTkbUxwV9hx/  
SE5zpJ4pFr9opq+UaTNX0yYuuJ328FGEFdkuFBSuJAokP0nJTLN8GdLAQ6x4kkkXwXkT8F1saPZwyJuqY8FNWtyiFIVY5Ct5G0zm  
D0Cj6vMaV0L7GzdDI4NZHn7llpptqJFYAb65QB admin@ise24https
```





Debe ver una ventana emergente que indica la **respuesta del servidor** en la esquina inferior derecha de la pantalla.



Desde la CLI, ejecute el comando `show repo sftp_pki` para validar las claves.

```
ise24https/admin# show repo sftp_pki
repo
```

Para seguir depurando ISE, ejecute este comando en CLI:

```
debug transfer 7
```

Se debe mostrar el resultado, como se muestra en la imagen:

```
ise24https/admin# debug transfer 7
ise24https/admin# show repo sftp_pki
6 [16745]:[info] transfer: cars_xfer.c[224] [admin]: sftp dir of repository sftp_pki requested
6 [16745]:[info] transfer: cars_xfer_util.c[2298] [admin]: resolved server to 10.88.240.102
7 [16745]:[debug] transfer: sftp_handler.c[1027] [admin]: Running sftp command: 10.88.240.102 engineer *** /repo/ ls -l /repo/
6 [16745]:[info] transfer: sftp_handler.c[554] [admin]: DEBUG: local user: admin UID: 0 sftp_run_parent FD: 5 remote host: 10.88.240.102 remote user: engineer comm
nd: ls -l /repo/
7 [16747]:[debug] transfer: sftp_handler.c[268] [admin]: Executing SFTP command: 0 admin /usr/bin/sftp -oIdentityFile=/home/admin/.ssh/id_rsa -oUserKnownHostsFile=/
home/admin/.ssh/known_hosts -oPasswordAuthenticationno engineer@10.88.240.102
7 [16745]:[debug] transfer: sftp_handler.c[586] [admin]: fd is 5
7 [16745]:[debug] transfer: sftp_handler.c[461] [admin]: Found sftp prompt; No more data to read
7 [16745]:[debug] transfer: sftp_handler.c[917] [admin]: sftp parent status 0
7 [16745]:[debug] transfer: cars_xfer_util.c[2315] [admin]: ssh_list xfer succeeded
% Repository is empty
```

## Información Relacionada

[https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin\\_guide/b\\_ise\\_admin\\_guide\\_22/b\\_ise\\_admin\\_guide\\_22\\_chapter\\_01011.html](https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_01011.html)