Autenticación de usuario de Shell seguro de cliente (SSH) para los switches SG350XG y SG550XG

Objetivo

Secure Shell (SSH) es un protocolo que proporciona una conexión remota segura a un dispositivo específico. Los switches gestionados serie 350XG y 550XG le permiten autenticar y administrar usuarios para conectarse al dispositivo a través de SSH. La autenticación se produce a través de una clave pública, de modo que el usuario puede utilizar esta clave para establecer una conexión SSH a un dispositivo específico. Las conexiones SSH son útiles para resolver problemas de una red de forma remota, en el caso de que el administrador de red no se encuentre en el sitio de red.

En este artículo se explica cómo configurar la autenticación de usuario del cliente en los switches gestionados SG350XG y SG550XG Series.

Dispositivos aplicables

- SG350XG
- SG550XG

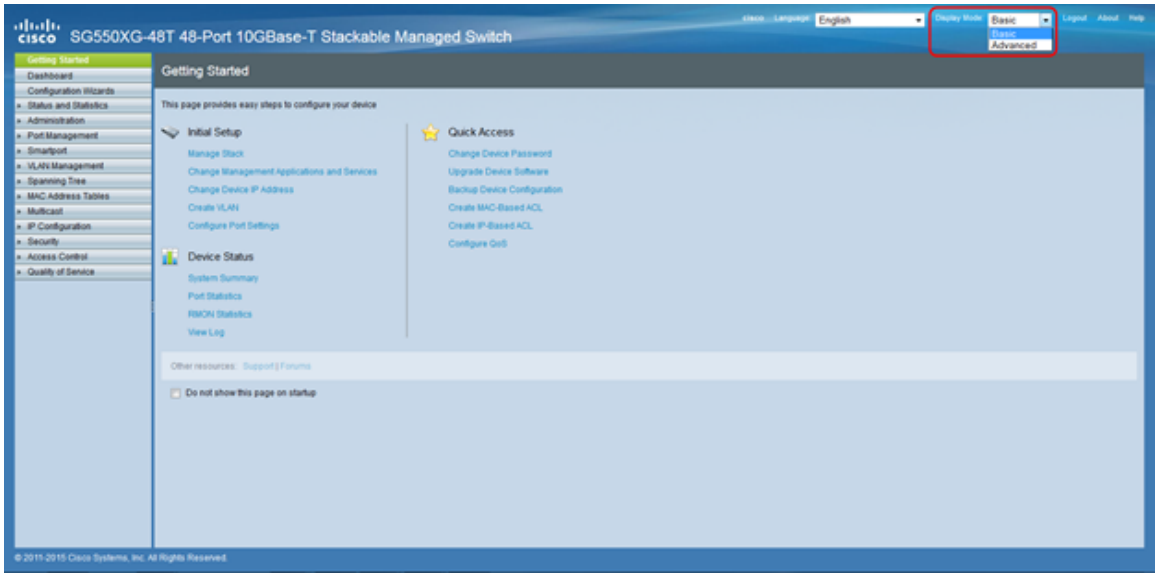
Versión del software

- v2.0.0.73

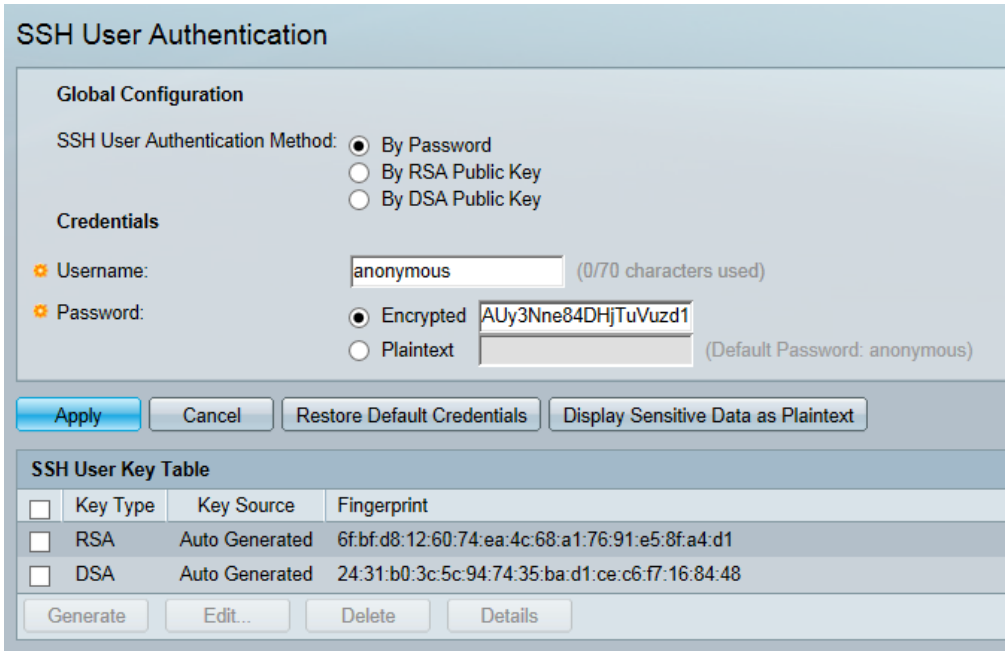
Configurar SSH Cliente Autenticación

Configuración global

Nota: Las siguientes capturas de pantalla pertenecen a la pantalla avanzada. Esto se puede cambiar haciendo clic en la lista desplegable *Modo de visualización* situada en la parte superior derecha de la pantalla



Paso 1. Inicie sesión en la utilidad de configuración web y elija **Security > SSH Client > SSH User Authentication**. Se abre la página *Autenticación de Usuario SSH*:



Paso 2. En el campo *SSH User Authentication Method*, haga clic en el botón de opción del método de autenticación global deseado.

Las opciones disponibles son las siguientes:

- By Password (Por contraseña): Esta opción le permite configurar una contraseña para la autenticación de usuario. Introduzca una contraseña o conserve el valor predeterminado, "anonymous" (anónimo).
- By RSA Public Key - Esta opción le permite utilizar una clave pública RSA para la autenticación de usuario. RSA se utiliza para el cifrado y la firma. Si selecciona esta opción, cree una clave pública y privada RSA en el bloque Tabla de claves de usuario SSH.
- By DSA Public Key (Clave pública DSA): Esta opción permite utilizar una clave pública DSA para la autenticación de usuario. DSA se utiliza sólo para firmar. Si selecciona esta opción, cree una clave pública/privada de DSA en el bloque Tabla de claves de usuario de SSH.

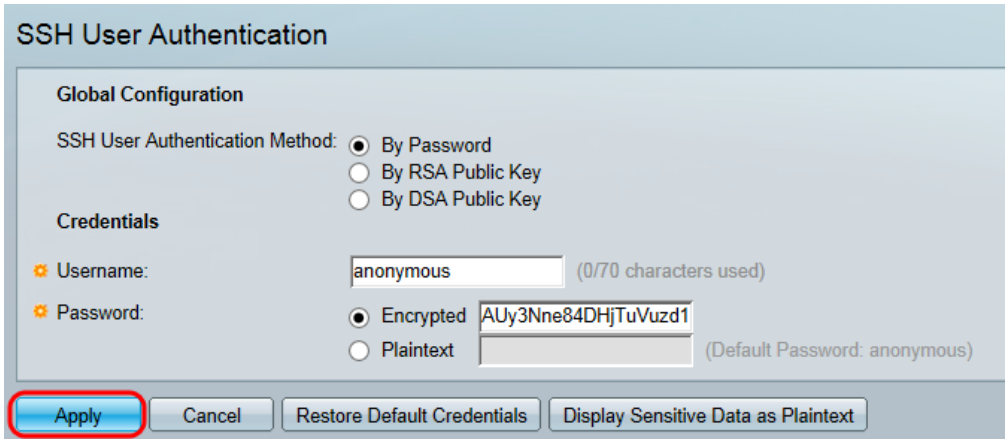
Paso 3. Localice el área *Credenciales*. En el campo *Username*, ingrese el nombre de usuario.

Paso 4. Si **By Password** fue seleccionado en el Paso 2, haga clic en el botón de opción del método de contraseña deseado en el campo *Password* . La contraseña predeterminada es "anonymous".

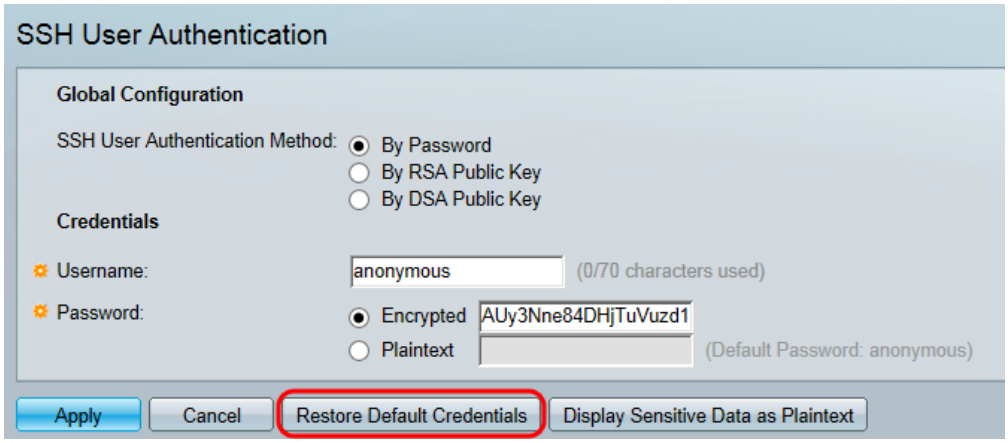
Las opciones disponibles se describen a continuación:

- Cifrado: introduzca una contraseña cifrada.
- Texto sin formato: introduzca una contraseña como texto sin formato.

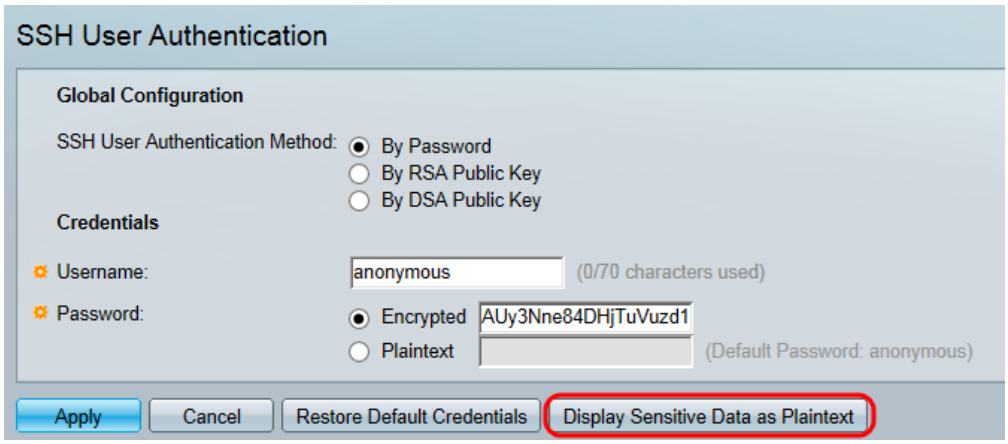
Paso 5. Haga clic en **Aplicar** para guardar la configuración de autenticación.



Paso 6. (Opcional) Para restaurar el nombre de usuario y la contraseña predeterminados, haga clic en **Restaurar credenciales predeterminadas**. La contraseña predeterminada es "anonymous" (anónima).



Paso 7. (Opcional) Para ver los datos confidenciales como texto sin formato o como texto cifrado, haga clic en **Mostrar datos confidenciales como texto sin formato/cifrado.**

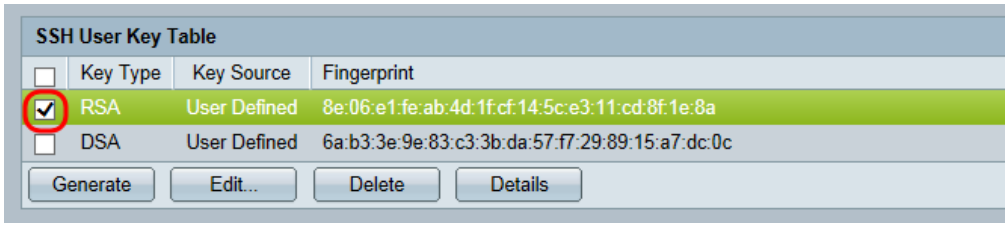


Nota: El nombre del botón cambiará en función de la configuración actual. El botón siempre cambiará la visualización de los datos.

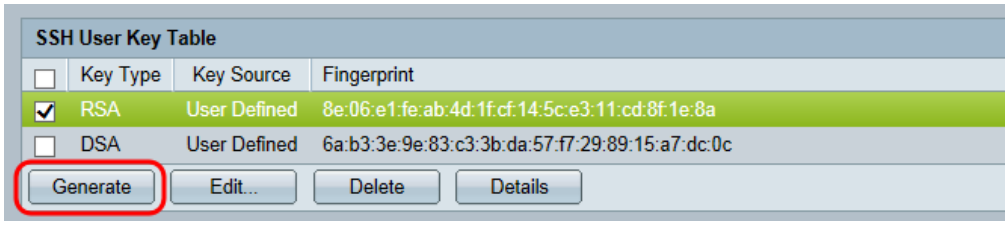
Tabla de claves de usuario SSH

Esta sección explica cómo administrar la tabla de usuario de SSH.

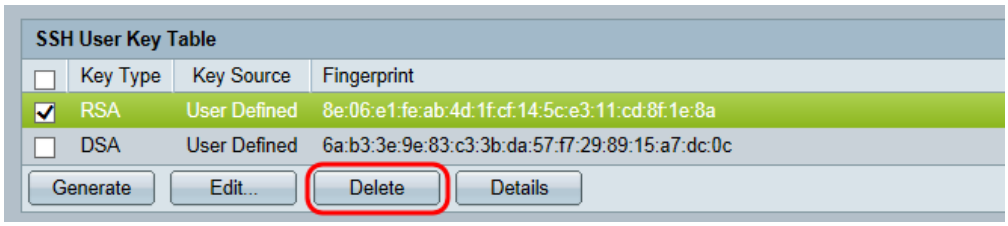
Paso 1. Navegue hasta la *Tabla de claves de usuario de SSH*. En la lista mostrada, seleccione las casillas de verificación que quedan a la clave que desea administrar .



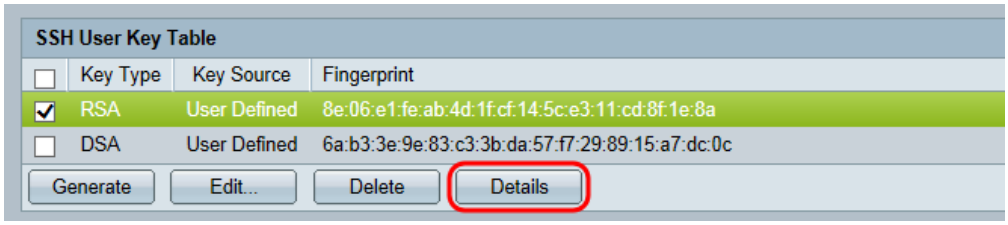
Paso 2. (Opcional) Haga clic en **Generar** para generar una nueva clave. La nueva clave reemplaza la clave seleccionada. Aparecerá una ventana de confirmación. Para continuar, haga clic en OK (Aceptar).



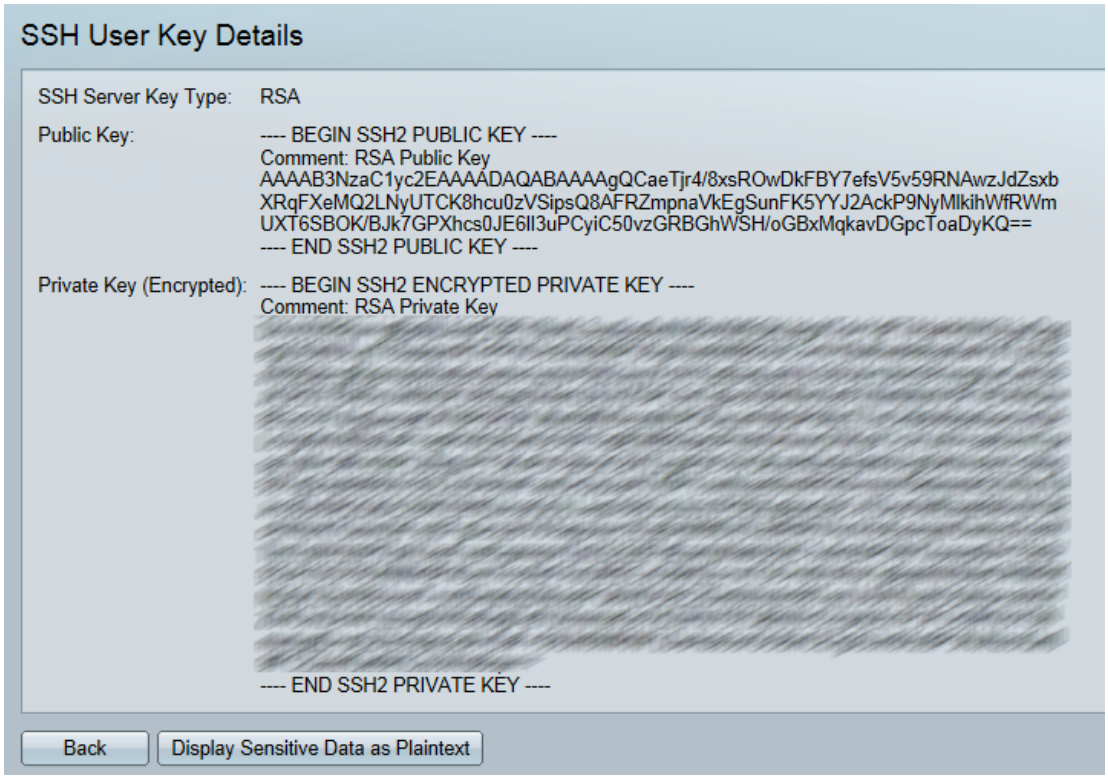
Paso 3. (Opcional) Haga clic en **Eliminar** para eliminar la clave seleccionada. Aparecerá una ventana de confirmación. Para continuar, haga clic en OK (Aceptar).



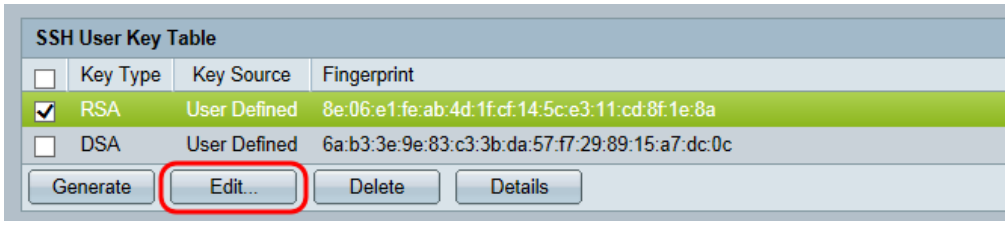
Paso 4. (Opcional) Haga clic en **Detalles** para ver los detalles de la clave seleccionada.



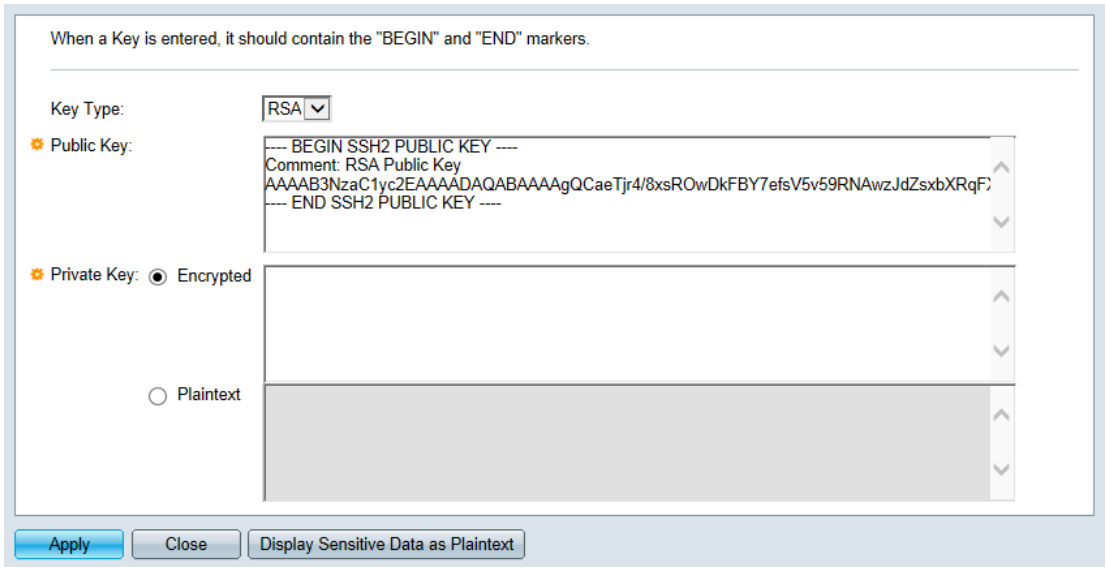
Aparecerá la página Detalles de la clave de usuario SSH. Haga clic en **Atrás** para volver a la tabla de claves de usuario SSH.



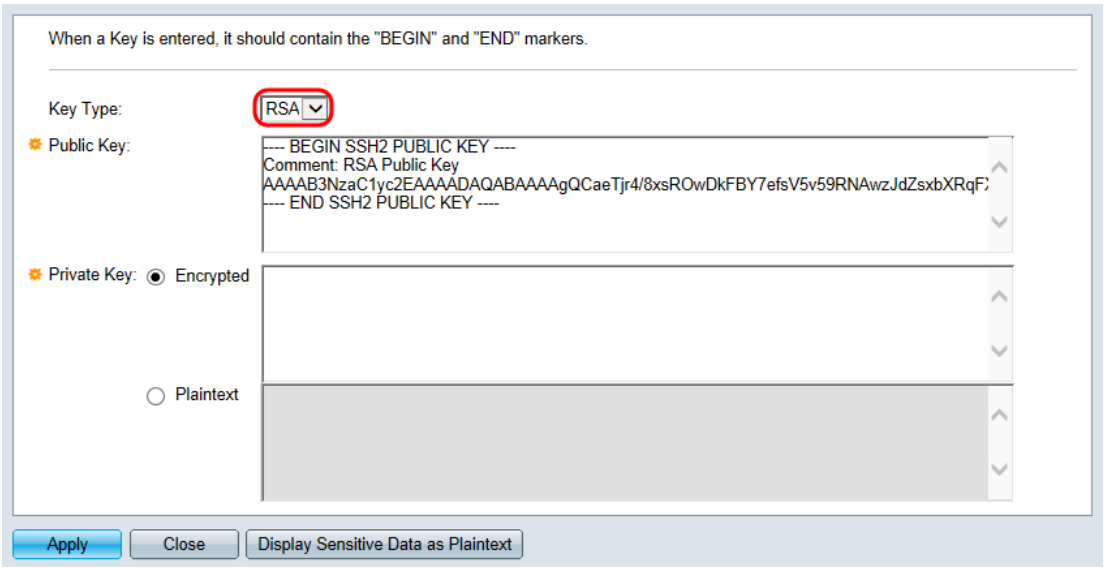
Paso 5. Haga clic en **Editar** para editar la clave elegida.



Se abre la ventana *Edit SSH Client Authentication Settings*:



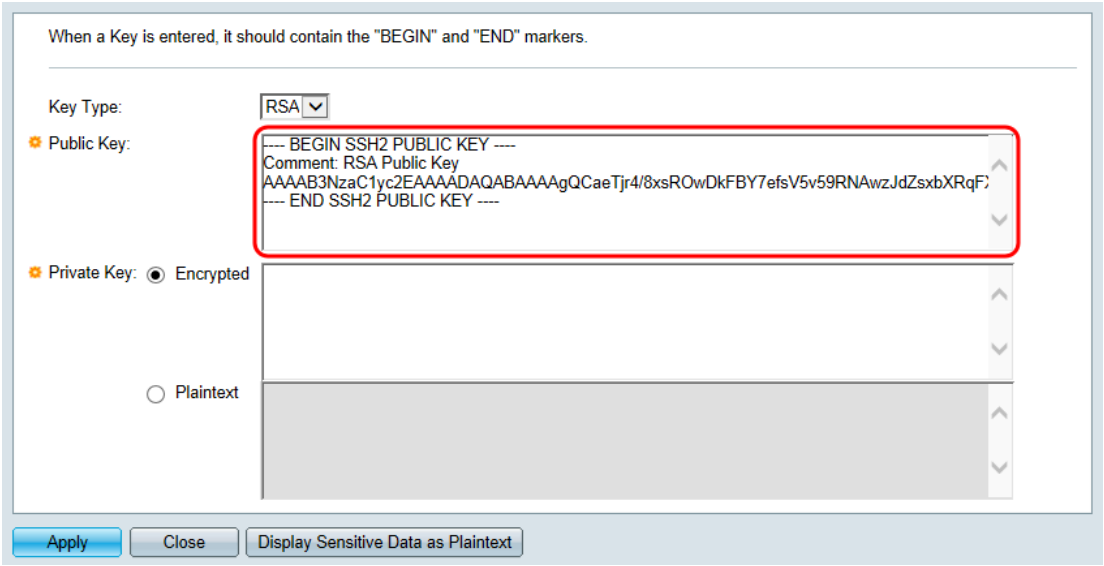
Paso 6. Seleccione el tipo de clave deseado en la lista desplegable *Tipo de clave*.



Las opciones disponibles son las siguientes:

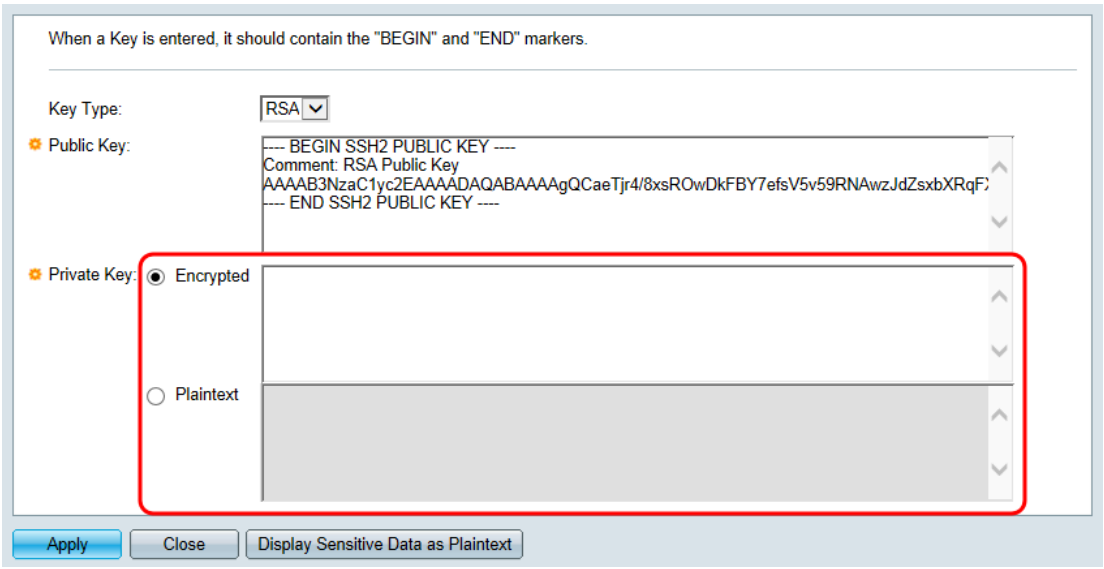
- RSA: RSA se utiliza para el cifrado y la firma.
- DSA: DSA se utiliza sólo para firmar.

Paso 7. En el campo *Public Key*, puede editar la clave pública actual.



Paso 8. En el campo *Private Key*, puede editar la clave privada actual. Haga clic en el

Botón de opción **Cifrado** para ver la clave privada actual como cifrada. De lo contrario, haga clic en el botón de opción **Texto sin formato** para ver la clave privada actual como texto sin formato.



Paso 9. Haga clic en **Aplicar** para guardar los cambios.