

Autenticación de usuario del Secure Shell (SSH) del cliente para el Switches SG350XG y SG550XG

Objetivo

El Secure Shell (SSH) es un protocolo que proporciona una conexión remota segura a un dispositivo específico. El Switches manejado las 350XG y 550XG Series le dejó autenticar y manejar a los usuarios para conectar con el dispositivo vía SSH. La autenticación ocurre vía una clave pública, así que el usuario puede utilizar esta clave para establecer una conexión SSH a un dispositivo específico. Las conexiones SSH son útiles para resolver problemas una red remotamente, en caso de que el administrador de la red no esté en el sitio de red.

Este artículo explica cómo configurar la autenticación de usuario de cliente en el Switches manejado serie SG350XG y SG550XG.

Dispositivos aplicables

- SG350XG
- SG550XG

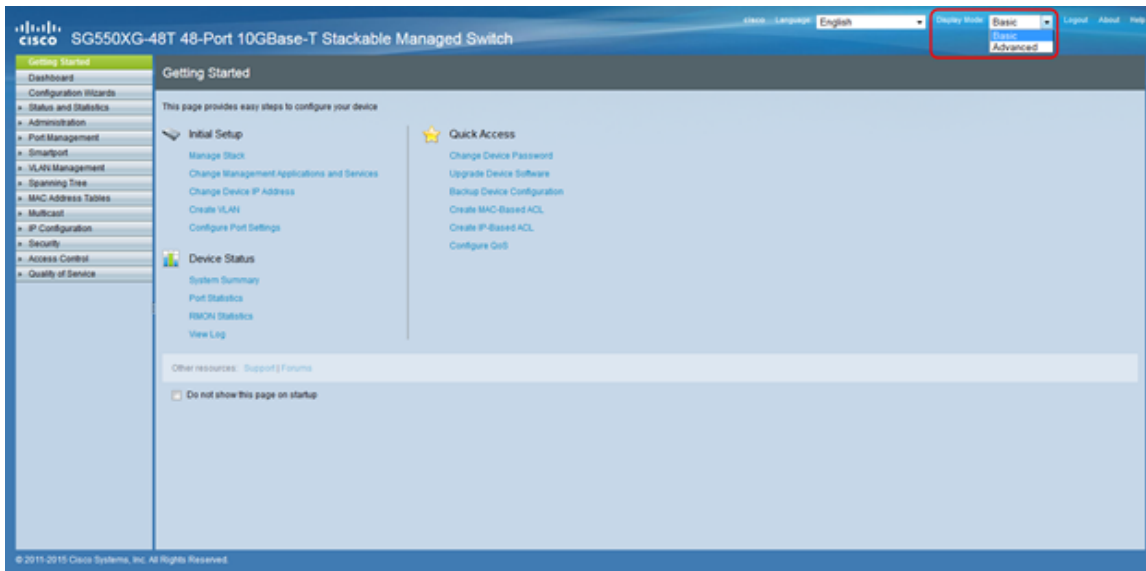
Versión del software

- v2.0.0.73

Autenticación de cliente SSH de la configuración

Configuración global

Nota: El screenshots siguiente es de la visualización avanzada. Esto puede ser conectada haciendo clic la lista desplegable del *modo de visualización* situada en la esquina superior derecha de la pantalla



Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **Seguridad > el cliente SSH > la autenticación de usuario de SSH**. La página de la *autenticación de usuario de SSH* se abre:

SSH User Authentication

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

✦ Username: (0/70 characters used)

✦ Password: Encrypted
 Plaintext (Default Password: anonymous)

SSH User Key Table

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input type="checkbox"/>	RSA	Auto Generated	6f:bf:d8:12:60:74:ea:4c:68:a1:76:91:e5:8f:a4:d1
<input type="checkbox"/>	DSA	Auto Generated	24:31:b0:3c:5c:94:74:35:ba:d1:ce:c6:f7:16:84:48

Paso 2. En el campo del *método de autenticación de usuario SSH*, haga clic en el botón de radio para el método de autenticación global deseado.

SSH User Authentication

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

✦ Username: (0/70 characters used)

✦ Password: Encrypted
 Plaintext (Default Password: anonymous)

Las opciones disponibles son como sigue:

- Por la contraseña – Esta opción le deja configurar una autenticación de contraseña para el usuario. Ingrese una contraseña o conserve el valor por defecto, “anónimo”.
- Por la clave pública RSA – Esta opción le deja utilizar una clave pública RSA para la autenticación de usuario. El RSA se utiliza para el cifrado y firmar. Si se selecciona esto, cree una clave pública y privada RSA en el bloque de la tabla de la clave del usuario de SSH.
- Por la clave pública DSA – Esta opción le deja utilizar una clave pública DSA para la autenticación de usuario. El DSA se utiliza para firmar solamente. Si se selecciona esto, cree un público/la clave privada DSA en el bloque de la tabla de la clave del usuario de SSH.

Paso 3. Localice el área de las *credenciales*. En el *campo de nombre de usuario*, ingrese el nombre de usuario.

SSH User Authentication

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

Username: (0/70 characters used)

Password: Encrypted AUy3Nne84DHjTuVuzd1
 Plaintext (Default Password: anonymous)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

Paso 4. Si **por la contraseña** fue seleccionado en el [paso 2](#), hacen clic el botón de radio para el método de clave deseado en el campo de *contraseña*. La contraseña predeterminada es “anónima”.

SSH User Authentication

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

Username: (0/70 characters used)

Password: Encrypted AUy3Nne84DHjTuVuzd1
 Plaintext (Default Password: anonymous)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

Se describen las opciones disponibles como sigue:

- Cifrado – Ingrese una contraseña encriptada.
- Plaintext – Ingrese una contraseña como sólo texto.

Paso 5. El tecleo **se aplica** para salvar la configuración de autenticación.

SSH User Authentication

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

Username: (0/70 characters used)

Password: Encrypted
 Plaintext (Default Password: anonymous)

Apply **Cancel** **Restore Default Credentials** **Display Sensitive Data as Plaintext**

Paso 6. (opcional) para restablecer el nombre de usuario predeterminado y la contraseña, **credenciales del valor por defecto del Restore del teclado**. El valor por defecto la contraseña es “anónimo”.

SSH User Authentication

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

Username: (0/70 characters used)

Password: Encrypted
 Plaintext (Default Password: anonymous)

Apply **Cancel** **Restore Default Credentials** **Display Sensitive Data as Plaintext**

Paso 7. (opcional) para ver los datos vulnerables como texto simple o como texto cifrado, **datos vulnerables de la visualización del teclado como el texto simple/cifrado**.

SSH User Authentication

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

Username: (0/70 characters used)

Password: Encrypted
 Plaintext (Default Password: anonymous)

Apply **Cancel** **Restore Default Credentials** **Display Sensitive Data as Plaintext**

Nota: El nombre del botón alterará dependiendo de la configuración actual. El botón conectará siempre la visualización de los datos.

Tabla de la clave del usuario de SSH

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

Paso 1. Navegue a la *tabla de la clave del usuario de SSH*. En la lista visualizada, seleccione los checkbox dejados a la clave que usted desea manejar.

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

Generate Edit... Delete Details

El tecleo (opcional) del paso 2. **genera** para generar una nueva clave. La nueva clave reemplaza la clave seleccionada. Una ventana de confirmación surgirá. Para continuar, haga clic en OK (Aceptar).

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

Generate Edit... Delete Details

Cancelación (opcional) del tecleo del paso 3. para borrar la clave seleccionada. Una ventana de confirmación surgirá. Para continuar, haga clic en OK (Aceptar).

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

Generate Edit... Delete Details

Detalles (opcionales) del tecleo del paso 4. para ver los detalles de la clave seleccionada.

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

Generate Edit... Delete Details

La página de los detalles de la clave del usuario de SSH aparece. Haga clic **de nuevo a la vuelta** a la tabla de la clave del usuario de SSH.

SSH User Key Details

SSH Server Key Type: RSA

Public Key:

```
---- BEGIN SSH2 PUBLIC KEY ----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxb  
XRqFXeMQ2LNyUTCK8hcu0zVSipsQ8AFRZmpnaVkEgSunFK5YYJ2AckP9NyMikihWfRWm  
UXT6SBOK/Bjk7GPXhcs0JE6II3uPCyiC50vzGRBGHWSH/oGBxMqkavDGpcToaDyKQ==  
---- END SSH2 PUBLIC KEY ----
```

Private Key (Encrypted):

```
---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
```

```
Comment: RSA Private Key
```

```
-----
```

```
---- END SSH2 PRIVATE KEY ----
```

Back

Display Sensitive Data as Plaintext

Paso 5. El tecleo **edita** para editar la clave elegida.

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

Generate Edit... Delete Details

La ventana de configuración de la autenticación de cliente SSH del editar se abre:

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type: RSA

Public Key:

```
---- BEGIN SSH2 PUBLIC KEY ----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF'  
---- END SSH2 PUBLIC KEY ----
```

Private Key: Encrypted Plaintext

Apply Close Display Sensitive Data as Plaintext

Paso 6. Seleccione el tipo dominante deseado de la lista desplegable *dominante del tipo*.

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type: RSA

Public Key:

```

---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF'
---- END SSH2 PUBLIC KEY ----

```

Private Key: Encrypted

Plaintext

Apply Close Display Sensitive Data as Plaintext

Las opciones disponibles son como sigue:

- RSA – El RSA se utiliza para el cifrado y firmar.
- DSA – El DSA se utiliza para firmar solamente.

Paso 7. En el campo de *clave pública*, usted puede editar la clave pública actual.

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type: RSA

Public Key:

```

---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF'
---- END SSH2 PUBLIC KEY ----

```

Private Key: Encrypted

Plaintext

Apply Close Display Sensitive Data as Plaintext

Paso 8. En el campo de *clave privada*, usted puede editar la clave privada actual. Haga clic

Botón de radio **cifrado** para ver la clave privada actual según lo cifrado. Si no, haga clic el botón de radio del **texto simple** para ver la clave privada actual como sólo texto.

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type: RSA

Public Key:

```
-----BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;  
-----END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted Plaintext

Apply Close Display Sensitive Data as Plaintext

Paso 9. El teclado **se aplica** para salvar sus cambios.

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type: RSA

Public Key:

```
-----BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;  
-----END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted Plaintext

Apply Close Display Sensitive Data as Plaintext