Configurar ajustes da autenticação de usuário do Shell Seguro (ssh) em um interruptor

Objetivo

O Shell Seguro (ssh) é um protocolo que forneça uma conexão remota segura aos dispositivos de rede específicos. Esta conexão fornece a funcionalidade que é similar a uma conexão Telnet, salvo que é cifrada. O SSH permite que o administrador configure o interruptor através do comando line interface(cli) com um programa da terceira parte.

No modo de CLI através do SSH, o administrador pode executar mais configurações avançadas em uma conexão segura. As conexões de SSH são úteis em pesquisar defeitos uma rede remotamente, nos casos onde o administrador de rede não está fisicamente atual na site de rede. O interruptor deixa o administrador autenticar e controlar usuários conectar à rede através do SSH. A autenticação ocorre através de uma chave pública que o usuário pode se usar para estabelecer uma conexão de SSH a uma rede específica.

A característica do cliente SSH é um aplicativo que execute sobre o protocolo SSH para fornecer a autenticação e a criptografia do dispositivo. Permite um dispositivo de fazer um seguro e uma conexão criptografada a um outro dispositivo que execute o servidor de SSH. Com autenticação e criptografia, o cliente SSH permite uma comunicação segura sobre uma conexão Telnet inseguro.

Este artigo fornece instruções em como configurar a autenticação de usuário cliente em um interruptor controlado.

Dispositivos aplicáveis

- Sx200 Series
- Sx300 Series
- Sx350 Series
- Série SG350X
- Sx500 Series
- Série Sx550X

Versão de software

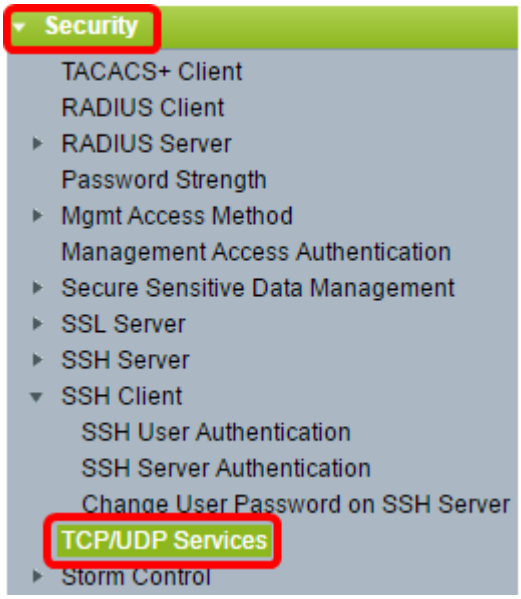
- 1.4.5.02 – Sx200 Series, Sx300 Series, Sx500 Series
- 2.2.0.66 – Sx350 Series, série SG350X, série Sx550X

Configurar ajustes da autenticação de usuário do cliente SSH

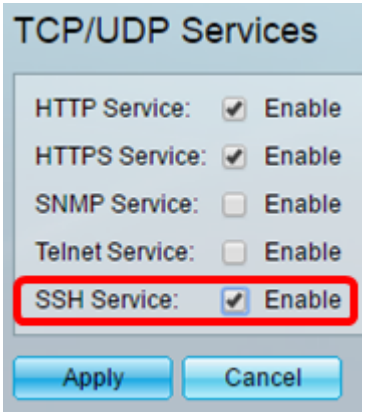
Permita o serviço SSH

Nota: A fim apoiar a configuração automática de um dispositivo da para fora--caixa (dispositivo com configuração padrão de fábrica), a autenticação de servidor de SSH é desabilitada à revelia.

Etapa 1. Entre à utilidade com base na Web e escolha a **Segurança > os serviços TCP/UDP**



Etapa 2. Verifique a caixa de verificação do **serviço SSH** para permitir o acesso do comando prompt do Switches com o SSH.



Etapa 3. O clique **aplica-se** para permitir o serviço SSH.

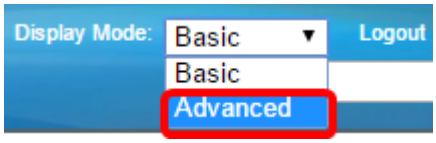
Configurar ajustes da autenticação de usuário SSH

Use esta página para escolher um método de autenticação de usuário SSH. Você pode ajustar um nome de usuário e senha no dispositivo se o método de senha é escolhido. Você pode igualmente gerar uma chave de Ron Rivest, DDA Shamir e de Leonard Adleman (RSA) ou de Digital Signature Algorithm (DSA) se o público ou método da chave privada é selecionada.

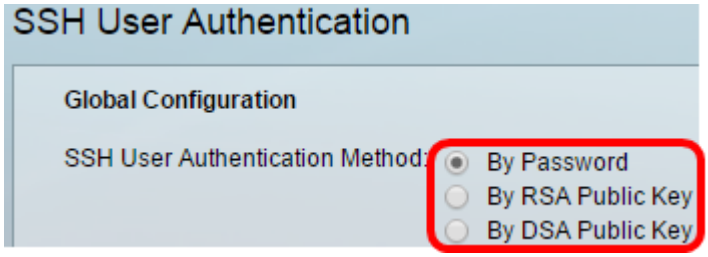
Os pares de chave padrão RSA e DSA estão gerados para o dispositivo quando é carreg. Uma destas chaves é para cifrado os dados que estão sendo transferidos do servidor de SSH. A chave RSA é usada à revelia. Se o usuário suprime de uma ou both of these chave, estão regenerados.

Etapa 1. Entre à utilidade com base na Web e escolha a **Segurança > o cliente SSH > a autenticação de usuário SSH**.

Nota: Se você tem um Sx350, um SG300X, ou um Sx500X, interruptor a modo avançado escolhendo **avançado da** lista de drop-down do modo de exibição.



Etapa 2. Sob a configuração global, clique o método de autenticação de usuário desejado SSH.

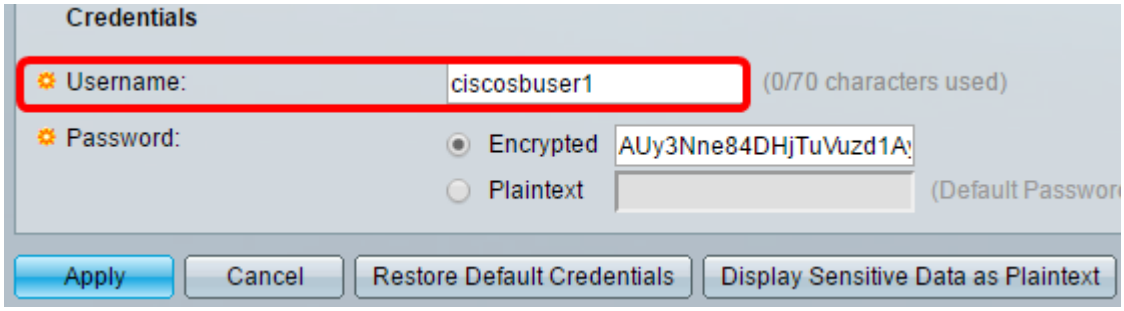


Nota: Quando um dispositivo (cliente SSH) tenta estabelecer uma sessão SSH ao servidor de SSH, o servidor de SSH usa um dos seguintes métodos para a authenticação do cliente:

- Pela senha — Esta opção deixa-o configurar uma senha para a autenticação de usuário. Esta é a configuração padrão e a senha padrão é anônima. Se esta opção é escolhida, certifique-se de que as credenciais do nome de usuário e senha estiveram estabelecidas no servidor de SSH.
- Pela chave pública RSA — Esta opção deixa-o usar a chave pública RSA para a autenticação de usuário. Uma chave RSA é uma chave cifrada baseada no factorization de grandes inteiros. Esta chave é a maioria de tipo comum de chave usado para a autenticação de usuário SSH.
- Pela chave pública DSA — Esta opção deixa-o usar uma chave pública DSA para a autenticação de usuário. Uma chave DSA é uma chave cifrada baseada no algoritmo discreto de ElGamal. Esta chave não é de uso geral para a autenticação de usuário SSH porque toma mais tempo no processo de autenticação.

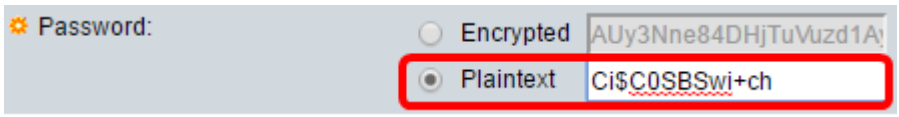
Nota: Neste exemplo, pela senha é escolhido.

Etapa 3. Na área das credenciais, dê entrada com o nome de usuário no *campo de nome de usuário*.



Nota: Neste exemplo, ciscosbuser1 é usado.

Etapa 4. (opcional) se você escolheu pela senha em etapa 2, clica o método a seguir incorpora a senha ao campo *cifrada* ou do *texto simples*.



As opções são:

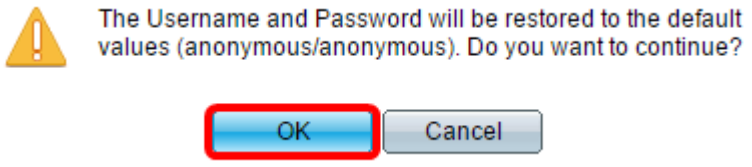
- Cifrado — Esta opção deixa-o incorporar uma versão cifrada da senha.
- Texto simples — Esta opção deixa-o incorporar uma senha do texto simples.

Nota: Neste exemplo, o texto simples é escolhido e uma senha do texto simples é incorporada.

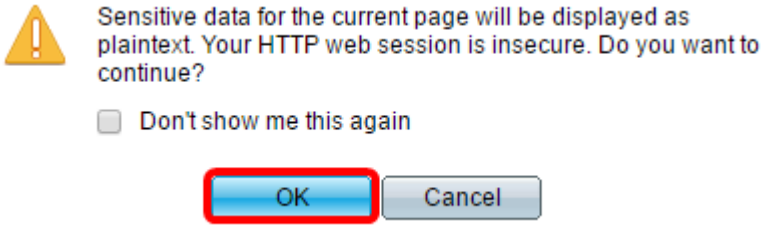
Etapa 5. O clique **aplica-se** para salvar sua configuração de autenticação.

As credenciais (opcionais) do **padrão da restauração do** clique de etapa 6. para restaurar o nome de usuário padrão e a senha clicam então a **APROVAÇÃO** para continuar.

Nota: O nome de usuário e senha será restaurado aos valores padrão: anônimo/anônimo.

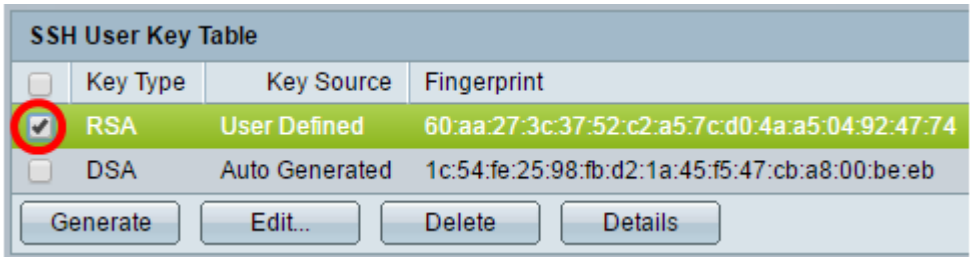


Dados sensíveis (opcionais) do **indicador do** clique de etapa 7. **como o texto simples** para mostrar os dados sensíveis da página no formato em texto simples clica então a **APROVAÇÃO** para continuar.



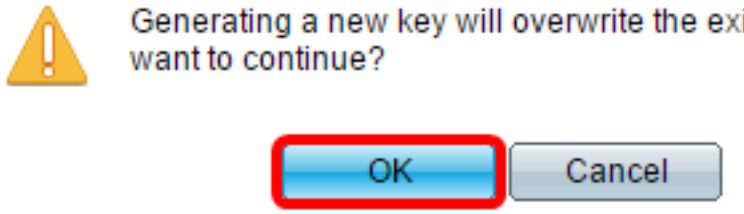
Configurar a tabela da chave do usuário SSH

Etapa 8. Verifique a caixa de verificação da chave que você deseja controlar.

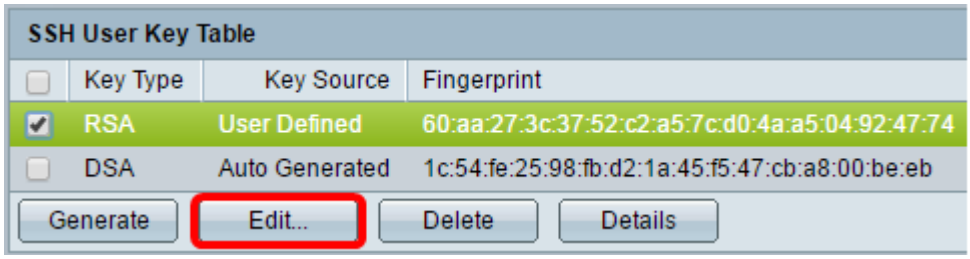


Nota: Neste exemplo, o RSA é escolhido.

O clique (opcional) de etapa 9. **gerencie** para gerar uma chave nova. A chave nova cancelará a chave verificada a seguir clica a **APROVAÇÃO** para continuar.



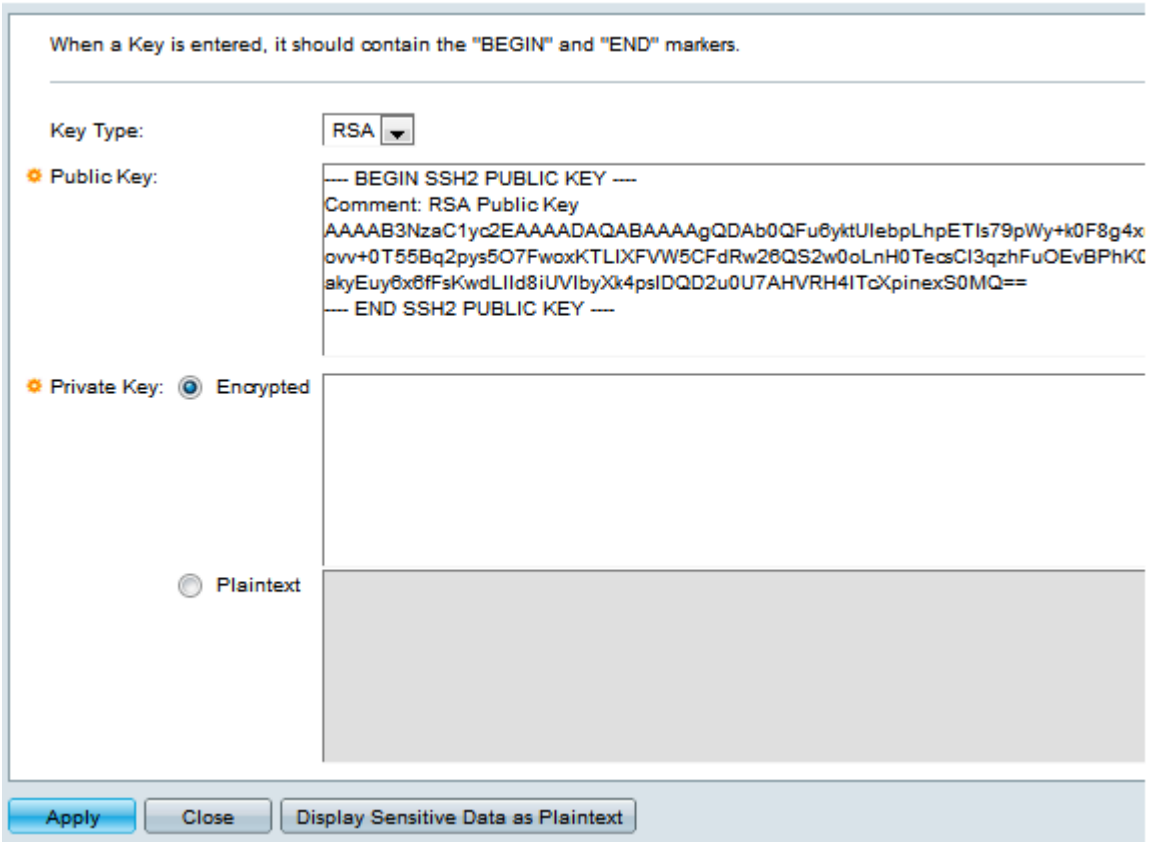
O clique (opcional) de etapa 10. **edita** para editar uma chave atual.



Etapa 11. (opcional) escolhe um tipo chave do tipo chave lista de drop-down.

Nota: Neste exemplo, o RSA é escolhido.

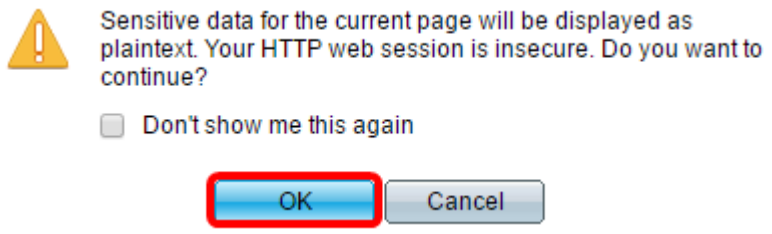
Etapa 12. (Opcional) incorpore a chave pública nova ao campo de *chave pública*.



Etapa 13. (Opcional) incorpore a chave privada nova ao campo de *chave privada*.

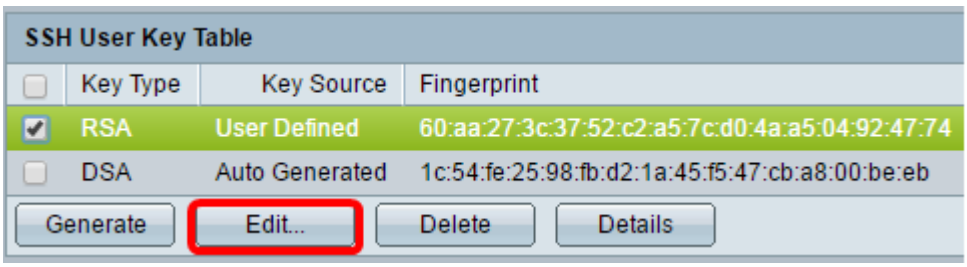
Nota: Você pode editar a chave privada e você pode clicar cifrado para ver a chave privada atual enquanto um texto cifrado, ou o texto simples para ver a chave privada atual no texto simples.

Etapa 14. (Opcional) clique **dados sensíveis do indicador enquanto o texto simples** para mostrar os dados criptografados da página no formato em texto simples a seguir clica a **APROVAÇÃO** para continuar.

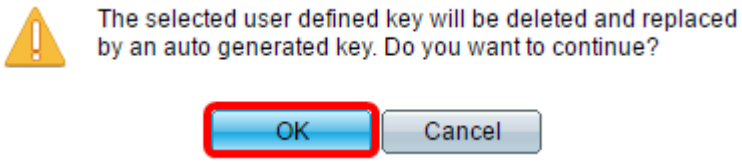


Etapa 15. O clique **aplica-se** para salvar suas mudanças a seguir clica-se **perto**.

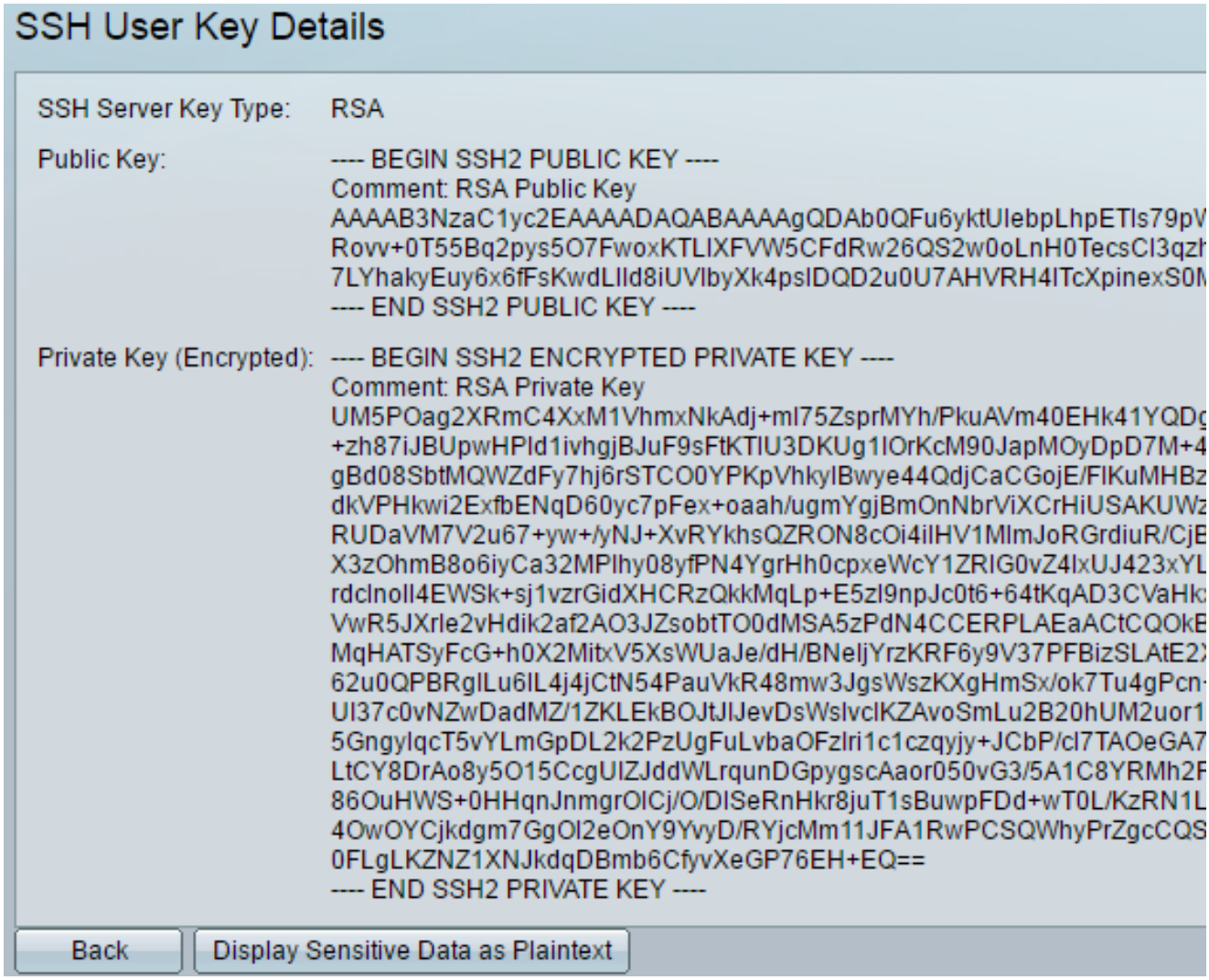
Etapa 16. (Opcional) clique a **supressão** para suprimir da chave verificada.



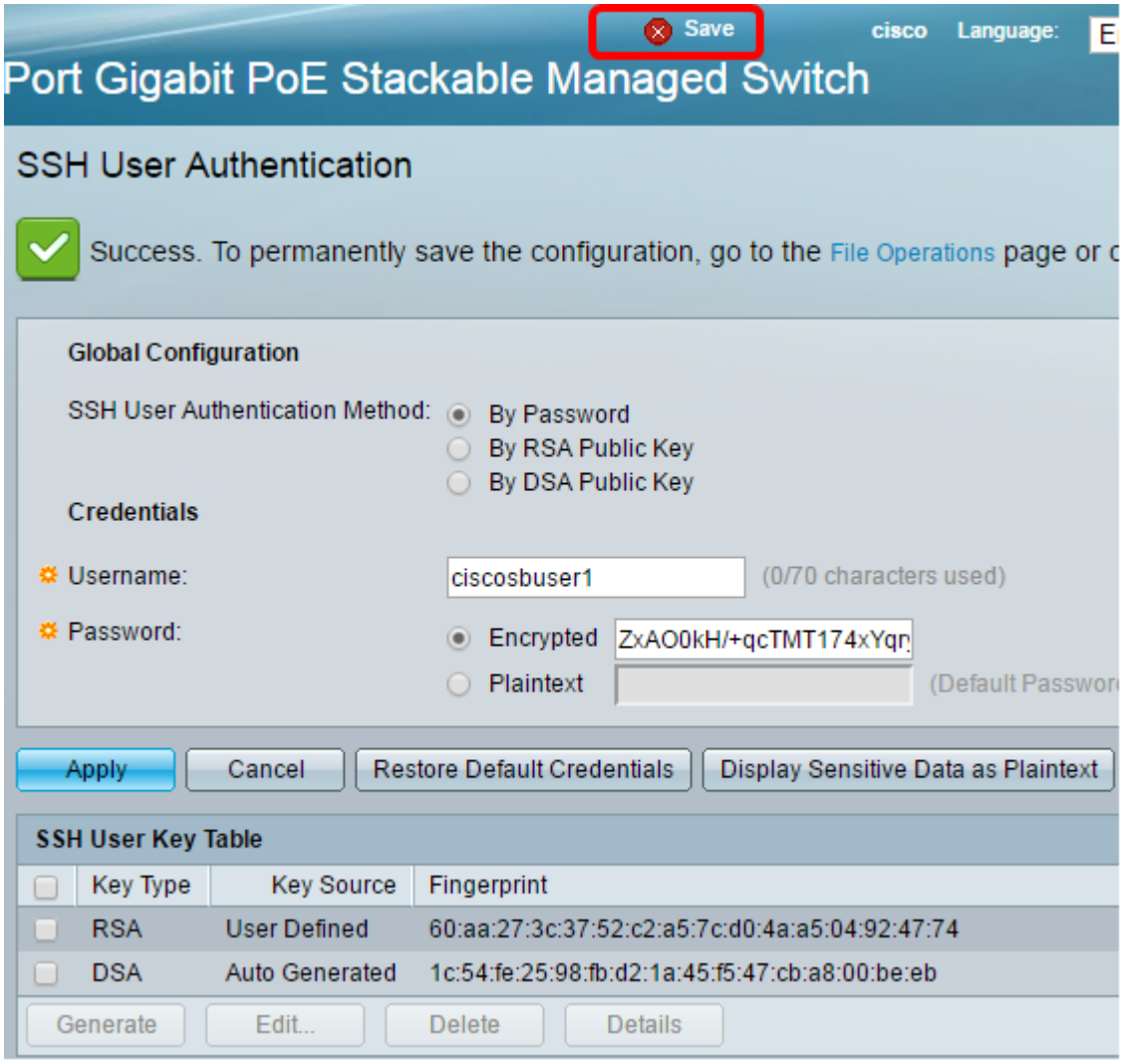
Etapa 17. (Opcional) alertou uma vez por um mensagem de confirmação como mostrado abaixo, **APROVAÇÃO do** clique para suprimir da chave.



Etapa 18. (Opcional) clique **detalhes** para ver os detalhes da chave verificada.



Etapa 19. (Opcional) clique o **botão Save Button na** parcela superior da página para salvar as mudanças ao arquivo de configuração de inicialização.



Você deve agora ter configurado os ajustes da autenticação de usuário cliente em seu interruptor controlado.