

Configurações de autenticação de usuário cliente Secure Shell (SSH) em switches empilháveis Sx500 Series

Objetivo

O recurso de servidor Secure Shell (SSH) permite estabelecer uma sessão SSH com os Switches empilháveis Sx500 Series. Uma sessão SSH é como uma sessão telnet, mas é mais segura. A segurança é obtida pelo dispositivo quando ele gera as chaves pública e privada automaticamente. Essas chaves também podem ser alteradas pelo usuário. Uma sessão SSH pode ser aberta com o uso do aplicativo PuTTY.

Este artigo fornece informações sobre como selecionar o método de autenticação para um cliente SSH. Ele também explica como configurar um nome de usuário e uma senha para o cliente SSH em Switches empilháveis Sx500 Series.

Dispositivos aplicáveis

Switches Empilháveis Sx500 Series

Versão de software

•1.3.0.62

Configuração de autenticação de usuário SSH cliente

Esta seção explica como configurar a autenticação de usuário nos Switches empilháveis Sx500 Series.

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Security > SSH Client > SSH User Authentication**. A página *Autenticação de usuário SSH* é aberta:

SSH User Authentication

Global Configuration

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

Credentials

Username: (Default Username: anonymous)

Password: Encrypted
 Plaintext (Default Password: anonymous)

SSH User Key Table

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input type="checkbox"/>	RSA	User Defined	b4:47:70:4f:4d:50:fd:f2:a0:f0:ba:c8:80:cc:c8:c6
<input type="checkbox"/>	DSA	Auto Generated	c5:ec:15:a7:3d:a3:b9:c5:9b:4f:56:5a:f8:2b:3a:b0

Etapa 2. Na área Configuração global, clique no botão de opção para o Método de autenticação de usuário SSH desejado. As opções disponíveis são:

Por senha — Esta opção permite configurar uma senha para autenticação de usuário

Por chave pública RSA — Essa opção permite que você use uma chave pública RSA para autenticação de usuário. RSA é usado para criptografia e assinatura.

Por chave pública DSA — Esta opção permite que você use uma chave pública DSA para autenticação do usuário. DSA é apenas para assinatura.

Etapa 3. Na área Credenciais, no campo Nome de usuário, digite o nome de usuário.

Etapa 4. Se você escolher Por senha na etapa 2, no campo Senha, clique no método para inserir a senha. As opções disponíveis são:

Encriptado — Esta opção permite introduzir uma senha encriptada.

Texto sem formatação — Esta opção permite inserir uma senha em texto simples. O texto simples é inserido para que você possa fazer login no dispositivo e exibir a senha caso tenha esquecido.

Etapa 5. Clique em **Apply** para salvar sua configuração de autenticação.

Etapa 6. (Opcional) Para restaurar o nome de usuário e a senha padrão, clique em **Restaurar credenciais padrão**.

Passo 7. (Opcional) Para mostrar os dados confidenciais da página em formato de texto simples, clique em **Exibir dados confidenciais como texto simples**.

Tabela de chave de usuário SSH

Esta seção explica como gerenciar a tabela de usuários SSH nos switches empilháveis Sx500 Series.

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Security > SSH Client > SSH User Authentication**. A página *Autenticação de usuário SSH* é aberta:

SSH User Authentication

Global Configuration

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

Credentials

Username: (Default Username: anonymous)

Password: Encrypted
 Plaintext (Default Password: anonymous)

SSH User Key Table

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	b4:47:70:4f:4d:50:fd:f2:a0:f0:ba:c8:80:cc:c8:c6
<input type="checkbox"/>	DSA	Auto Generated	c5:ec:15:a7:3d:a3:b9:c5:9b:4f:56:5a:f8:2b:3a:b0

Etapa 2. Marque a caixa de seleção da chave que deseja gerenciar.

Etapa 3. (Opcional) Para gerar uma nova chave, clique em **Gerar**. A nova chave substitui a chave verificada.

Etapa 4. (Opcional) Para editar uma chave atual, clique em **Editar**. A janela *Editar configurações de autenticação do cliente SSH* é exibida.

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

Key Type:

Public Key:

```
--- BEGIN SSH2 PUBLIC KEY ---  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAABIwAAAIEA79zGK7S5RD5JShWUvOPVFFDnwRyD+cVxuSUn06AHbjxNBP  
Dwgd18Jl4Bu3yK0zW5Rn0k79uLzdfKLLcHNGx+r5dJY4ihc+aXfHZKrpzHb33nHQzSdyNpGfME+J9J  
HiD+pleJawnliuGJdKBUEIWgxYbSGC6hko9A9BOe9oAPU=  
--- END SSH2 PUBLIC KEY ---
```

Private Key: Encrypted Plaintext

```
---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----  
Comment: RSA Private Key  
EZ2eLdVg4K7h1icrGG/jbLqFarPl65f3Neki5NmmAbMRwNDpvNDWgjWc+WkI1Un5Sq2aTyuW  
Zja8heVQY7ZT8h0VFI9mJ6GYaXKyMjzXxao9MGE3aPYirmPu0m6ZciefLsrj8qill7QkII+T3KpAg  
tgPBBf0nwYZR1FYsFzbybJl20oK  
/rugVCP7ejdgeaXQfTMkrmfTaXFHxDzd32Cwa3wJHKjel9eNhill5o35E1WXuMopnUtorcDSevZTI  
Di0JzZpwAMZbbS5rWmwewVl+gFMXqWxMrnfp+Mv6zPuXZ5OyN4MWTgpwtyrfmceDqOUI7sHq9
```

As opções que você pode editar são:

Tipo de chave — Essa opção permite escolher na lista suspensa Tipo de chave o tipo de chave de sua preferência. Você pode escolher RSA ou DSA como o tipo de chave. RSA é usado para criptografia e assinatura, enquanto DSA é apenas para assinatura.

Chave pública — Nesse campo, você pode editar a chave pública atual.

Chave privada — Neste campo, você pode editar a chave privada e clicar em **Criptografado** para ver a chave privada atual como um texto criptografado ou **Texto simples** para ver a chave privada atual em texto simples.

Etapa 5. Clique em **Apply** para salvar suas alterações.

SSH User Authentication

Global Configuration

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

Credentials

Username: example (Default Username: anonymous)

Password: Encrypted AUy3Nne84DHjTuVuzd1
 Plaintext (Default Password: anonymous)

Apply Cancel Restore Default Credentials Display Sensitive Data As Plaintext

SSH User Key Table

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	44:ad:6e:b4:bd:9e:c9:e9:ff:9c:09:37:29:63:0e:9d
<input type="checkbox"/>	DSA	Auto Generated	49:fa:5b:6c:37:c2:fd:10:45:0f:2d:d2:01:f8:01:4b

Generate Edit... Delete Details...

Etapa 6. (Opcional) Para excluir a chave selecionada, clique em **Excluir**.

Passo 7. (Opcional) Para visualizar os detalhes da chave selecionada, clique em **Detalhes**. Abaixo está uma imagem dos detalhes da chave do usuário.

SSH User Key Details

SSH Server Key Type: RSA

Public Key: --- BEGIN SSH2 PUBLIC KEY ---
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAIEAzzGyPuoBcoaNa32Pk2ELNnt7UaGR5xFEPoH7
JdGj3Lto7UfkRAM9Xlvai9Xua/B4pU1fCL
/I2ZFjGVgTs7UUsNOjjuOTRSopHR8udhUGqgdzA4hHQyovCGy8OIuRYNIU0q6UHWW7
6NX+jnD4WphJxeYCKx2AIWzmsu14p6GQ2Eo=
--- END SSH2 PUBLIC KEY ---

Private Key (Encrypted): --- BEGIN SSH2 ENCRYPTED PRIVATE KEY ---
Comment: RSA Private Key
mF32KmMsoyqrru/46gXYvYHa8i4GpPchdlzh7fQDyx5+zAXxJ6skn3bAo
/brX7Nshms5zf0SPgbRGmdWXAfo3o0AZUaE/pHcPfpTE3Ilyu6Qtjfo64S
/kJKYwfvZhrvU4g6hIBfZnCDXz0H1mgXvzoYBpkqxq8ZldTdYOIRW+3W25z8+ez2r
/LycEtNyEziv0RGhCfSZat3PGCpNX9IH1DY9asfNAnIKDcRvqOnIO4hcBY+aCirtSs3wS
xtYPS1m3rBUdhUBOX4m/bzH1qJJP6dLuxZAVsrNRY1XmK3WGjxsyNGsUgC
/2dEmPZodIstKtV4xg13hux78rzd3u072ofCSRmEuO166S2JNNR1IRLeVOI
/PKVv1pfuuZUDDm0qmeqr8sDvWFXkDbeWPisOvRQXO3Yk2D94TiW1sFpW0B4zB9nN
QMsO4/dQnl/Qa5ofk/ObzwVNmmaNhXdK
/TYPXRQGJEz9McLc641VNYmKWpBELTqS
/vujygonYqDpgUw2XJlxZ9nmhp1mYteqINTUNVv4QNnssc9no5YoffPdyNEuox9L0rmT
LgNaIpdo5R6CP7hyN0Ao9wGgBMwnq8dz2fUSplhu2vqNULmaRgUIKR2bVtmSBWuX
S8CRtDFnt3qB3UMRLouMssWWEuGfCJaAA7zhDbeqDRuct
/EiPWLgzYBqGbCvTB4EZtbbIqebmFphnqxc3X7CuxmU9klwUrkZTVhjoQb7rjySbCypB
w47xpxi5/6u6A6kyhC+/wpWBld6C4UO2u/9C7zDJSnho5w+anL6
/1tl6p06lkwn+hCsQzJA9kphmaq5NjUscQadZqQtz4w5s8kvpjT3lfy5NZr2KB030Qi9ICsP
O+ao1vhnfBSPfu8Rt/8fPXVQyfhXvYG
/RI6aDIho3+pL7VUdqZ7u4CyYB+pnrZ5psX9I6qRuGfqiTDMsSiZyWY
/p+J6lhLfYwKfI3Lj2wpeggRwl4HUUiZpGr+0S5O51ot8+1ItlkFhoqA1+Z3C9Sh7TvNyBGI
gbLqLPsXxz2xAHlzH8
/NK7EquMs0Ob52DPJ79vNeJjtjNAvPjwDkCunkEzjoo3LYxliE3DtMCBAcVPUeGndcK
hCA==
--- END SSH2 PRIVATE KEY ---

Back

Display Sensitive Data As Plaintext