

Konfigurieren der Einstellungen für die Secure Shell (SSH)-Benutzerauthentifizierung auf einem Switch

Ziel

Secure Shell (SSH) ist ein Protokoll, das eine sichere Remoteverbindung zu bestimmten Netzwerkgeräten bereitstellt. Diese Verbindung stellt Funktionen bereit, die einer Telnet-Verbindung ähneln, nur dass sie verschlüsselt ist. SSH ermöglicht dem Administrator, den Switch über die Befehlszeilenschnittstelle (CLI) eines Drittanbieterprogramms zu konfigurieren.

Im CLI-Modus über SSH kann der Administrator erweiterte Konfigurationen in einer sicheren Verbindung ausführen. SSH-Verbindungen sind bei der Remote-Behebung von Netzwerkfehlern hilfreich, wenn der Netzwerkadministrator nicht physisch am Netzwerkstandort anwesend ist. Der Switch ermöglicht dem Administrator, Benutzer zu authentifizieren und zu verwalten, um eine Verbindung zum Netzwerk über SSH herzustellen. Die Authentifizierung erfolgt über einen öffentlichen Schlüssel, mit dem der Benutzer eine SSH-Verbindung zu einem bestimmten Netzwerk herstellen kann.

Die SSH-Client-Funktion ist eine Anwendung, die über das SSH-Protokoll ausgeführt wird, um Geräteauthentifizierung und -verschlüsselung zu ermöglichen. Es ermöglicht einem Gerät, eine sichere und verschlüsselte Verbindung mit einem anderen Gerät herzustellen, auf dem der SSH-Server ausgeführt wird. Mit Authentifizierung und Verschlüsselung ermöglicht der SSH-Client eine sichere Kommunikation über eine unsichere Telnet-Verbindung.

Dieser Artikel enthält Anweisungen zum Konfigurieren der Clientbenutzerauthentifizierung auf einem verwalteten Switch.

Unterstützte Geräte

- Sx200-Serie
- Sx300-Serie
- Sx350-Serie
- SG350X-Serie
- Sx500-Serie
- Sx550X-Serie

Software-Version

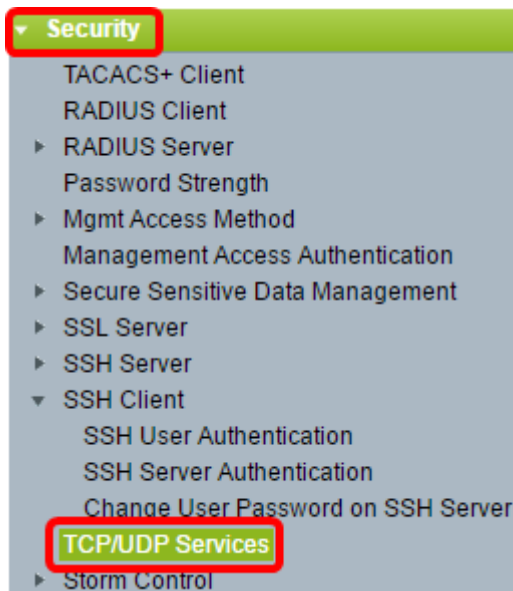
- 1.4.5.02 - Serie Sx200, Serie Sx300, Serie Sx500
- 2.2.0.66 - Serie Sx350, Serie SG350X, Serie Sx550X

Authentifizierungseinstellungen für den SSH-Client konfigurieren

SSH-Dienst aktivieren

Hinweis: Um die automatische Konfiguration eines Out-of-Box-Geräts (Gerät mit werkseitiger Standardkonfiguration) zu unterstützen, ist die SSH-Serverauthentifizierung standardmäßig deaktiviert.

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Security > TCP/UDP Services** aus.



Schritt 2: Aktivieren Sie das Kontrollkästchen **SSH-Dienst**, um den Zugriff auf die Switch-Eingabeaufforderung über SSH zu aktivieren.



Schritt 3: Klicken Sie auf **Apply**, um den SSH-Dienst zu aktivieren.

Einstellungen für die SSH-Benutzerauthentifizierung konfigurieren

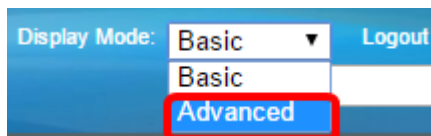
Auf dieser Seite können Sie eine SSH-Benutzerauthentifizierungsmethode auswählen. Sie können einen Benutzernamen und ein Kennwort auf dem Gerät festlegen, wenn Sie die Kennwortmethode auswählen. Sie können auch einen Ron Rivest-, Adi Shamir- und Leonard Adleman- (RSA) oder Digital Signature Algorithm- (DSA)-Schlüssel generieren, wenn die öffentliche oder private Schlüsselmethod ausgewählt ist.

RSA- und DSA-Standardschlüsselpaare werden beim Booten des Geräts generiert. Einer dieser Schlüssel wird verwendet, um die vom SSH-Server heruntergeladenen Daten zu verschlüsseln. Der RSA-Schlüssel wird standardmäßig verwendet. Wenn der Benutzer einen oder beide Schlüssel löscht, werden sie neu generiert.

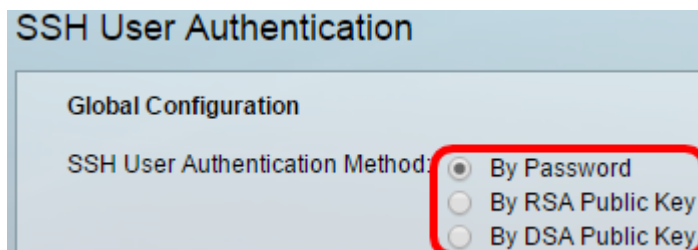
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Security > SSH Client > SSH User Authentication** aus.



Hinweis: Wenn Sie über einen Sx350, SG300X oder Sx500X verfügen, wechseln Sie in den erweiterten Modus, indem Sie **Erweitert** aus der Dropdown-Liste Anzeigemodus auswählen.



Schritt 2: Klicken Sie unter Global Configuration (Globale Konfiguration) auf die gewünschte SSH-Benutzerauthentifizierungsmethode.



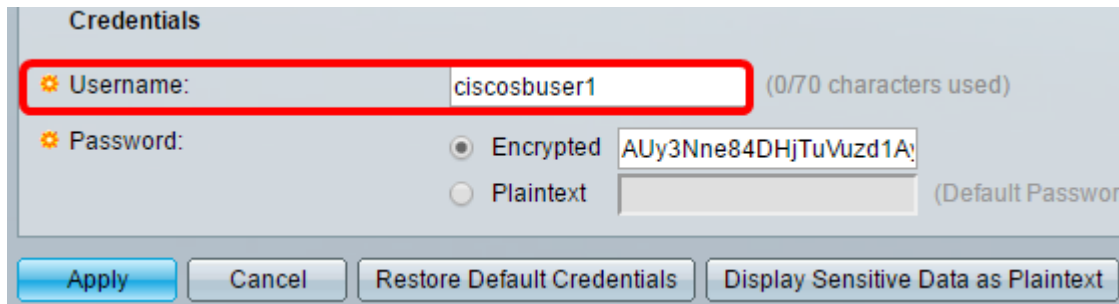
Hinweis: Wenn ein Gerät (SSH-Client) versucht, eine SSH-Sitzung mit dem SSH-Server herzustellen, verwendet der SSH-Server eine der folgenden Methoden für die Client-Authentifizierung:

- By Password (Nach Kennwort) - Mit dieser Option können Sie ein Kennwort für die Benutzerauthentifizierung konfigurieren. Dies ist die Standardeinstellung, und das Standardkennwort ist anonym. Wenn Sie diese Option auswählen, stellen Sie sicher, dass der Benutzername und das Kennwort auf dem SSH-Server eingerichtet wurden.
- By RSA Public Key (Nach öffentlichem RSA-Schlüssel) - Mit dieser Option können Sie den öffentlichen RSA-Schlüssel für die Benutzerauthentifizierung verwenden. Ein RSA-Schlüssel ist ein verschlüsselter Schlüssel, der auf der Faktorisierung großer Zahlen basiert. Dieser Schlüssel ist der gängigste Schlüsseltyp für die SSH-Benutzerauthentifizierung.
- By DSA Public Key (Nach öffentlichem DSA-Schlüssel) - Mit dieser Option können Sie einen öffentlichen DSA-Schlüssel für die Benutzerauthentifizierung verwenden. Ein DSA-Schlüssel ist ein verschlüsselter Schlüssel, der auf einem diskreten ElGamal-Algorithmus basiert. Dieser Schlüssel wird normalerweise nicht für die SSH-Benutzerauthentifizierung verwendet, da der

Authentifizierungsprozess länger dauert.

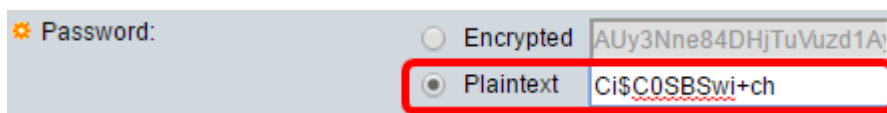
Hinweis: In diesem Beispiel wird By Password (Nach Kennwort) ausgewählt.

Schritt 3: Geben Sie im Bereich Anmeldeinformationen den Benutzernamen in das Feld *Benutzername* ein.



Hinweis: In diesem Beispiel wird ciscosbuser1 verwendet.

Schritt 4. (Optional) Wenn Sie In Schritt 2 Nach Kennwort ausgewählt haben, klicken Sie auf die Methode, und geben Sie dann das Kennwort in das Feld *Verschlüsselt* oder *Nur-Text* ein



Folgende Optionen sind verfügbar:

- Verschlüsselt - Über diese Option können Sie eine verschlüsselte Version des Kennworts eingeben.
- Plaintext - Mit dieser Option können Sie ein Nur-Text-Passwort eingeben.

Hinweis: In diesem Beispiel wird Nur-Text ausgewählt, und es wird ein Nur-Text-Passwort eingegeben.

Schritt 5: Klicken Sie auf **Apply**, um die Authentifizierungskonfiguration zu speichern.

Schritt 6. (Optional) Klicken Sie auf **Standard-Anmeldedaten wiederherstellen**, um den Standard-Benutzernamen und das Standard-Kennwort wiederherzustellen. Klicken Sie anschließend auf **OK**, um fortzufahren.

Hinweis: Benutzername und Kennwort werden auf die Standardwerte zurückgesetzt: anonymous/anonymous.



The Username and Password will be restored to the default values (anonymous/anonymous). Do you want to continue?



Schritt 7. (Optional) Klicken Sie auf **Vertrauliche Daten als Klartext anzeigen**, um die vertraulichen Daten der Seite im Nur-Text-Format anzuzeigen. Klicken Sie dann auf **OK**, um fortzufahren.



Sensitive data for the current page will be displayed as plaintext. Your HTTP web session is insecure. Do you want to continue?

Don't show me this again



SSH-Benutzerschlüsseltabelle konfigurieren

Schritt 8: Aktivieren Sie das Kontrollkästchen des Schlüssels, den Sie verwalten möchten.

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb

Buttons: Generate, Edit..., Delete, Details

Hinweis: In diesem Beispiel wird RSA ausgewählt.

Schritt 9. (Optional) Klicken Sie auf **Generate (Generieren)**, um einen neuen Schlüssel zu generieren. Der neue Schlüssel überschreibt den markierten Schlüssel und klickt dann auf **OK**, um fortzufahren.



Generating a new key will overwrite the existing key. Do you want to continue?



Schritt 10. (Optional) Klicken Sie auf **Bearbeiten**, um einen aktuellen Schlüssel zu bearbeiten.

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb

Buttons: Generate, Edit... (highlighted with a red box), Delete, Details

Schritt 11. (Optional) Wählen Sie in der Dropdown-Liste "Key Type" (Schlüsseltyp) einen Schlüsseltyp aus.

Key Type: RSA ▼
Public Key: RSA
Comment:

Hinweis: In diesem Beispiel wird RSA ausgewählt.

Schritt 12. (Optional) Geben Sie den neuen öffentlichen Schlüssel in das Feld *Öffentlicher Schlüssel* ein.

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
AAAAB3NzaC1yc2EAAAADAQABAAQDAQDAb0QFu6yktUlebpLhpETIs79pWY+k0F8g4x
ovv+0T55Bq2pys5O7FwoxKTLIXFVW5CFdRw26QS2w0oLnH0TecsC13qzhFuOEVBPhKC
akyEuy6x8fFsKwdLIld8iUVIbyXk4psIDQD2u0U7AHVRH4ITcXpinexS0MQ==
--- END SSH2 PUBLIC KEY ---

```

Private Key: Encrypted

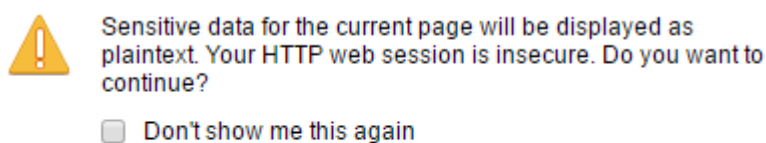
Plaintext

Apply Close Display Sensitive Data as Plaintext

Schritt 13. (Optional) Geben Sie den neuen privaten Schlüssel in das Feld *Privater Schlüssel* ein.

Hinweis: Sie können den privaten Schlüssel bearbeiten und auf **Verschlüsselt** klicken, um den aktuellen privaten Schlüssel als verschlüsselten Text anzuzeigen, oder auf **Nur-Text**, um den aktuellen privaten Schlüssel im Nur-Text-Format anzuzeigen.

Schritt 14. (Optional) Klicken Sie auf **Vertrauliche Daten als Klartext anzeigen**, um die verschlüsselten Daten der Seite im Nur-Text-Format anzuzeigen. Klicken Sie dann auf **OK**, um fortzufahren.



Schritt 15: Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, und klicken Sie dann auf **Schließen**.

Schritt 16. (Optional) Klicken Sie auf **Löschen**, um den markierten Schlüssel zu löschen.

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb

Generate Edit... Delete Details

Schritt 17. (Optional) Wenn Sie wie unten dargestellt von einer Bestätigungsmeldung dazu aufgefordert werden, klicken Sie auf **OK**, um den Schlüssel zu löschen.



The selected user defined key will be deleted and replaced by an auto generated key. Do you want to continue?



Schritt 18. (Optional) Klicken Sie auf **Details**, um die Details des geprüften Schlüssels anzuzeigen.

SSH User Key Details

SSH Server Key Type: RSA

Public Key: ---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAQgQDAb0QFu6yktUlebpLhpETIs79pV
Rovv+0T55Bq2pys5O7FwoxKTLIXFW5CFdRw26QS2w0oLnH0TecsCI3qzF
7LYhakyEuy6x6fFsKwdLlId8iUVlbyXk4psIDQD2u0U7AHVRH4ITcXpinexS0M
---- END SSH2 PUBLIC KEY ----

Private Key (Encrypted): ---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
Comment: RSA Private Key
UM5POag2XRmC4XxM1VhmxNkAdj+ml75ZsprMYh/PkuAVm40EHk41YQDg
+zh87iJBUpwHPId1ivhgjBJuF9sFtKTIU3DKUg1lOrKcM90JapMOyDpD7M+4
gBd08SbtMQWZdFy7hj6rSTCO0YPKpVhkylBwye44QdjCaCGojE/FIKuMHBz
dkVPHkwi2ExfbENqD60yc7pFex+oaah/ugmYgjBmOnNbrViXCrHiUSAKUWz
RUDaVM7V2u67+yw+/yNJ+XvRYkhsQZRON8cOi4ilHV1MImJoRGrdiuR/CjE
X3zOhmB8o6iyCa32MPlhy08yfPN4YgrHh0cpxeWcY1ZRIG0vZ4lxUJ423xYL
rdclnoll4EWSk+sj1vzrGidXHCRzQkkMqLp+E5zl9npJc0t6+64tKqAD3CVaHk
VwR5JXrle2vHdik2af2AO3JZsobtTO0dMSA5zPdN4CCERPLAEaACTCQOkE
MqHATSyFcG+h0X2MitxV5XsWUaJe/dH/BNeljYrzKRF6y9V37PFBizSLAtE2
62u0QPBRglLu6lL4j4jCtN54PauVkr48mw3JgsWszKXgHmSx/ok7Tu4gPcn
UI37c0vNZwDadMZ/1ZKLEkBOJtJIJevDsWslvclKZAvoSmLu2B20hUM2uor1
5GngylqcT5vYLMGpDL2k2PzUgFuLvbaOFzIri1c1czqjy+JCbP/cl7TAOeGA7
LtCY8DrAo8y5O15CcgUIZJddWLRqunDGpygscAaor050vG3/5A1C8YRMh2F
86OuHWS+0HHqnJnmgrOICj/O/DiSeRnHkr8juT1sBuwpFDd+wT0L/KzRN1L
4OwOYCjkdgm7GgOI2eOnY9YvyD/RyjCmM11JFA1RwPCSQWhyPrZgcCQS
0FLgLKZNZ1XNjkdqDBmb6CfyvXeGP76EH+EQ==
---- END SSH2 PRIVATE KEY ----

Back Display Sensitive Data as Plaintext

Schritt 19. (Optional) Klicken Sie oben auf der Seite auf die Schaltfläche **Speichern**, um die Änderungen in der Startkonfigurationsdatei zu speichern.

cisco Language: E

Port Gigabit PoE Stackable Managed Switch

SSH User Authentication

 Success. To permanently save the configuration, go to the [File Operations](#) page or c

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)

SSH User Key Table

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb

Sie sollten jetzt die Authentifizierungseinstellungen für den Client-Benutzer auf dem verwalteten Switch konfiguriert haben.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.