

Configuration Migration Service Tool

Objective

The tool will update interface names to the new interface naming conventions used in the new devices. When converting the settings from the source to the destination, the tool will map the commands from interfaces in the source device to interfaces that would use the same role in the destination device. It will convert commands that are no longer supported to analogous commands from the newer devices. The tool will attempt to keep the same functionality between the original behavior and the behavior in the updated configuration.

The objective of this document is to show you how to use the migration tool to take configuration from a Sx200, Sx300, or Sx500 series switches and convert it to the appropriate Sx250, Sx350, and Sx550.

Applicable Devices

- Sx200
- Sx300
- Sx500

Source Software Version

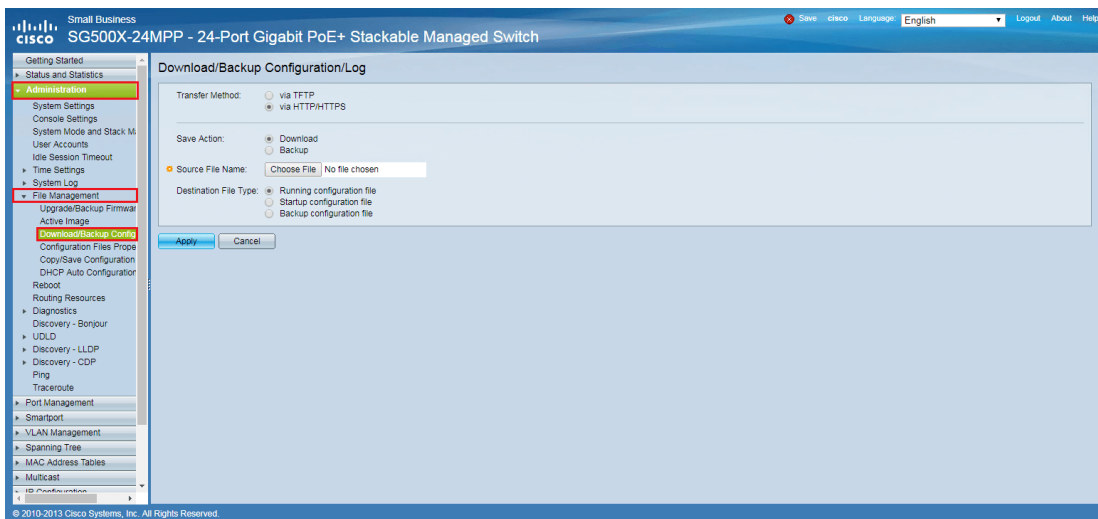
- v1.4 or above

Destination Software Version

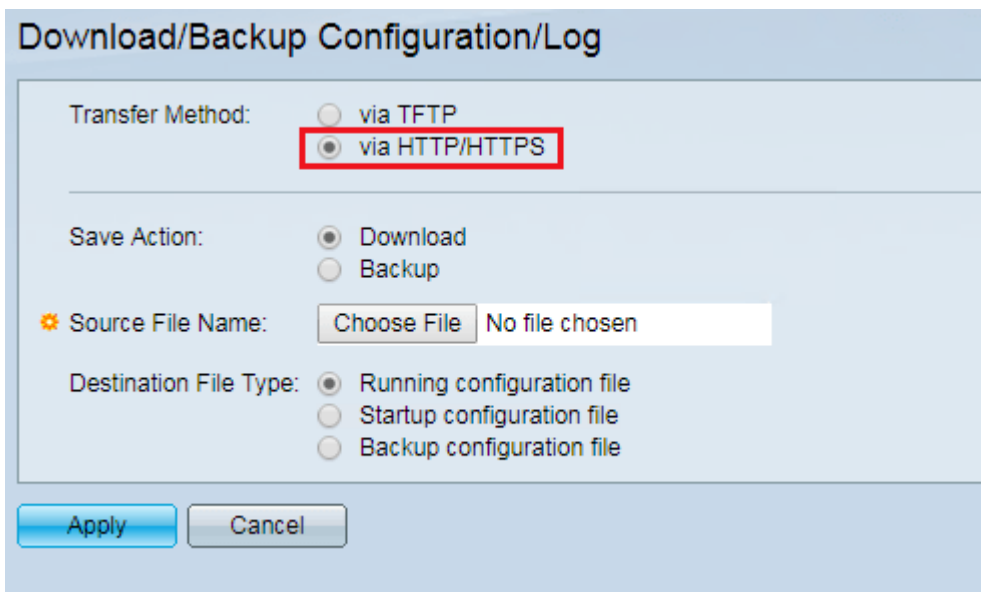
- v2.3 or above

Configuration Migration Overview

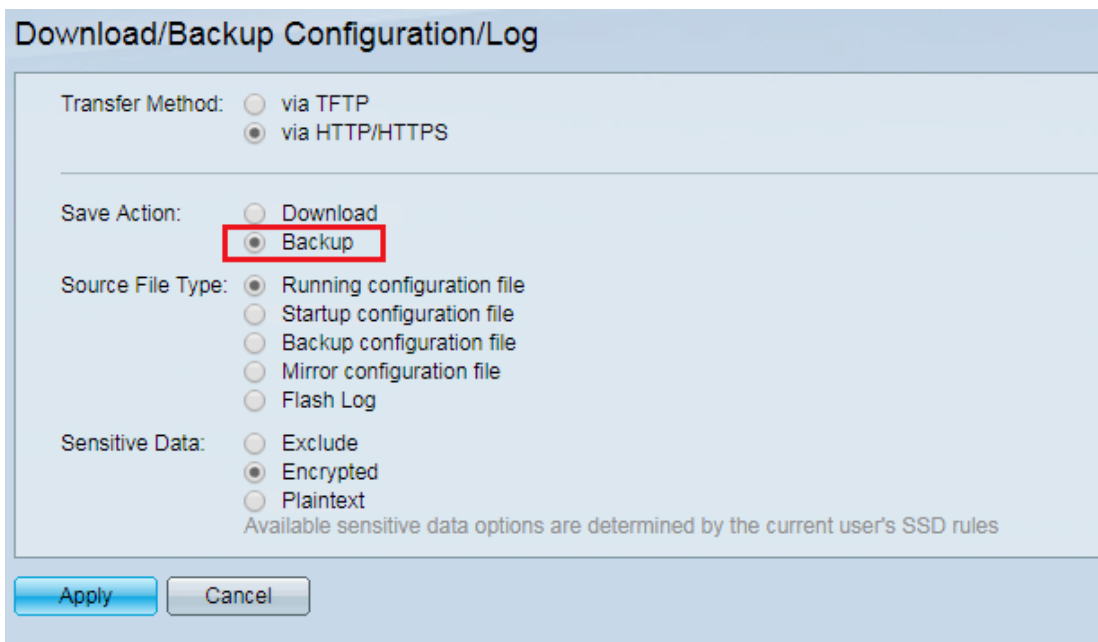
Step 1. In your source switch, log in to the web configuration utility and choose **Administration > File Management > Download/Backup Configuration**. The Download/Backup Configuration/Log page opens.



Step 2. Select the **viaHTTP/HTTPS** in the *Transfer Method* radial button.



Step 3. In the *Save Action* field, select **Backup** to back up the configuration file.



Step 4. Select **Startup configuration file** in the *Source File Type* field as we want to convert the startup configuration file.

Download/Backup Configuration/Log

Transfer Method: ☐ via TFTP
☒ via HTTP/HTTPS

Save Action: ☐ Download
☒ Backup

Source File Type: ☐ Running configuration file
☒ Startup configuration file
☐ Backup configuration file
☐ Mirror configuration file
☐ Flash Log

Sensitive Data: ☐ Exclude
☒ Encrypted
☐ Plaintext

Available sensitive data options are determined by the current user's SSD rules

Step 5. Select **Plaintext** or **Exclude** in the *Sensitive Data* field.

Download/Backup Configuration/Log

Transfer Method: ☐ via TFTP
☒ via HTTP/HTTPS


Save Action: ☐ Download
☒ Backup

Source File Type: ☐ Running configuration file
☒ Startup configuration file
☐ Backup configuration file
☐ Mirror configuration file
☐ Flash Log

Sensitive Data: ☒ Exclude
☐ Encrypted
☒ Plaintext

Available sensitive data options are determined by the current user's SSD rules

Step 6. Open the [Configuration Migration Service Tool](#). The *Configuration Migration Service Tool* page opens.



Configuration Migration Service

Help

Source Configuration

Updated Configuration

Source Device Model: SG500X-24

Destination Device Model: SF550X-24

Convert

Copy to Clipboard

Step 7. In the *Source Configuration* section, select the source device from the *Source Device Model*.

Configuration Migration Service

Source Configuration

Source Device Model:

SG500X-24

SG300-52

SG300-52P

SG300-52MP

ESW2-350G-52

ESW2-350G-52DC

Sx500

SF500-24

SF500-24P

SF500-24MP

SF500-48

SF500-48P

SF500-48MP

SG500-28

SG500-28P

SG500-28MPP

SG500-52

SG500-52P

SG500-52MP

SG500X

SG500X-24

Step 8. Copy the text of the source configuration file to the *Source Configuration* text area.

Note: Ensure the source configuration includes the file full header section.

Configuration Migration Service

Source Configuration

Source Device Model: SG500X-24 ▼

```
config-file-header
Test-1
v1.4.0.00p6 / R750_NIK_1_4_647_335
CLI v1.0
set system queues-mode 4

file SSD indicator plaintext
@
vlan database
vlan 2-3
exit
voice vlan oui-table add 0001e3 Siemens_AG_phone_____
voice vlan oui-table add 00036b Cisco_phone_____
voice vlan oui-table add 00096e Avaya_____
voice vlan oui-table add 000fe2 H3C_Aolynk_____
voice vlan oui-table add 0060b9 Philips_and_NEC_AG_phone_____
voice vlan oui-table add 00d01e Pingtel_phone_____
voice vlan oui-table add 00e075 Polycom/Veritel_phone____
voice vlan oui-table add 00e0bb 3Com_phone_____
bonjour interface range vlan 1
hostname Test-1
username cisco password encrypted
e5df2d8279432f3e35b68b34c30b18f8d0ff8723 privilege 15
ip ssh server
!
interface vlan 2
name test-VLAN
!
interface vlan 3
name test-VLAN-2
shutdown
```

Step 9. Select the model of the destination switch from the *Destination Device Model* dropdown menu.

Updated Configuration

Destination Device Model: SF550X-24 ▼

Sx550X

SF550X-24

SF550X-24P

SF550X-24MP

SF550X-48

SF550X-48P

SF550X-48MP

SG550X-24

SG550X-24P

SG550X-24MP

SG550X-24MPP

SG550X-48

SG550X-48P

SG550X-48MP

Step 10. Click the **Convert** button to convert the source configuration file to the destination configuration file.

Note: Configurations of features that are no longer supported will be removed.

Source Configuration

Source Device Model: SG500X-24 ▼

```
config-file-header
Test-1
v1.4.0.00p6 / R750_NIK_1_4_647_335
CLI v1.0
set system queues-mode 4

file SSD indicator plaintext
@
vlan database
vlan 2-3
exit
voice vlan oui-table add 0001e3 Siemens_AG_phone_____
voice vlan oui-table add 00036b Cisco_phone_____
voice vlan oui-table add 00096e Avaya_____
voice vlan oui-table add 000fe2 H3C_Aolynk_____
voice vlan oui-table add 0060b9 Philips_and_NEC_AG_phone_____
voice vlan oui-table add 00d01e Pingtel_phone_____
voice vlan oui-table add 00e075 Polycom/Veritel_phone_____
voice vlan oui-table add 00e0bb 3Com_phone_____
bonjour interface range vlan 1
hostname Test-1
username cisco password encrypted
e5df2d8279432f3e35b68b34c30b18f8d0ff8723 privilege 15
ip ssh server
!
interface vlan 2
name test-VLAN
!
interface vlan 3
name test-VLAN-2
shutdown
```

Updated Configuration

Destination Device Model: SF550X-24 ▼

Convert

»

Copy to Clipboard

Step 11. Once the conversion is completed, review the results in the *Updated Configuration* text area.

Note: All the rows that were updated will be highlighted in the text area. Comments are added to the configuration to explain all the changes that were made during the conversion.

Updated Configuration

Destination Device Model:

```
! The command "set system" was removed. The system now always works in 8 queues
combined switch and router mode
config-file-header
file SSD indicator plaintext
@
vlan database
vlan 2-3
exit
voice vlan oui-table add 0001e3 Siemens_AG_phone_____
voice vlan oui-table add 00036b Cisco_phone_____
voice vlan oui-table add 00096e Avaya_____
voice vlan oui-table add 000fe2 H3C_Aolynk_____
voice vlan oui-table add 0060b9 Philips_and_NEC_AG_phone
voice vlan oui-table add 00d01e Pingtel_phone_____
voice vlan oui-table add 00e075 Polycom/Veritel_phone____
voice vlan oui-table add 00e0bb 3Com_phone_____
bonjour interface range vlan 1
hostname Test-1
username cisco password encrypted e5df2d8279432f3e35b68b34c30b18f8d0ff8723
privilege 15
ip ssh server
!
interface vlan 2
name test-VLAN
!
interface vlan 3
name test-VLAN-2
shutdown
```

Step 12. Copy the updated configuration and paste it into a new text file.

Updated Configuration

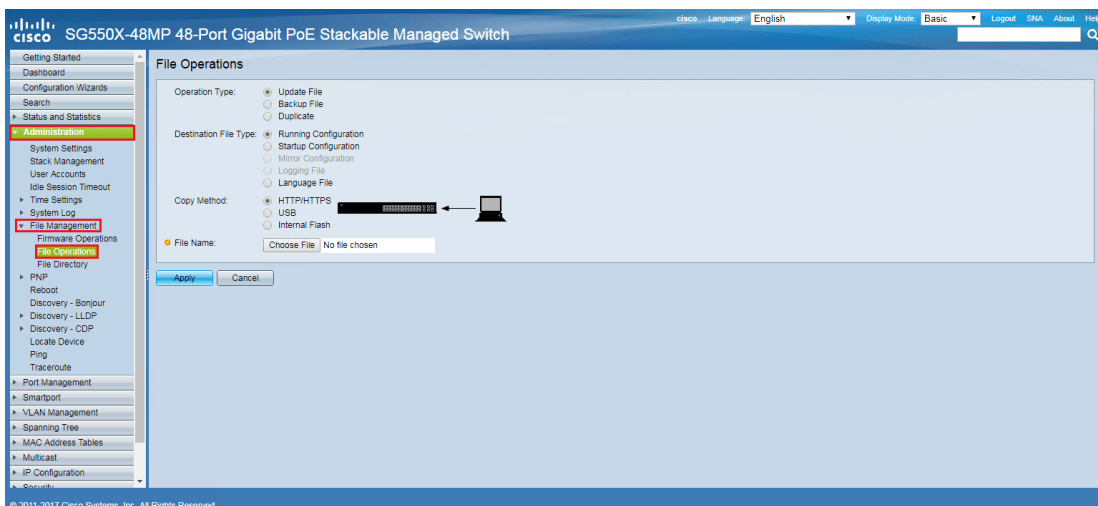
Destination Device Model: SG550X-48MP ▼

! The command "set system" was removed. The system now always works in 8 queues combined switch and router mode

```
config-file-header
file SSD indicator plaintext
@
vlan database
vlan 2-3
exit
voice vlan oui-table add 0001e3 Siemens_AG_phone_____
voice vlan oui-table add 00036b Cisco_phone_____
voice vlan oui-table add 00096e Avaya_____
voice vlan oui-table add 000fe2 H3C_Aolynk_____
voice vlan oui-table add 0060b9 Philips_and_NEC_AG_phone
voice vlan oui-table add 00d01e Pingtel_phone_____
voice vlan oui-table add 00e075 Polycom/Veritel_phone___
voice vlan oui-table add 00e0bb 3Com_phone_____
bonjour interface range vlan 1
hostname Test-1
username cisco password encrypted e5df2d8279432f3e35b68b34c30b18f8d0ff8723
privilege 15
ip ssh server
!
interface vlan 2
name test-VLAN
!
interface vlan 3
name test-VLAN-2
shutdown
no snmp trap link-status
```

Copy to Clipboard

Step 13. Log in to the web configuration utility of the destination switch and choose **Administrator > File Management > File Operations**.



Step 14. In the *Operation Type* field, select **Update File**.

File Operations

Operation Type: ☒ Update File
☐ Backup File
☐ Duplicate

Destination File Type: ☒ Running Configuration
☐ Startup Configuration
☐ Mirror Configuration
☐ Logging File
☐ Language File

Copy Method: ☒ HTTP/HTTPS ☐ USB ☐ Internal Flash

File Name: No file chosen

Step 15. Select **Startup Configuration** in the *Destination File Type* field.

File Operations

Operation Type: ☒ Update File
☐ Backup File
☐ Duplicate

Destination File Type: ☐ Running Configuration
☒ Startup Configuration
☐ Mirror Configuration
☐ Logging File
☐ Language File

Copy Method: ☒ HTTP/HTTPS ☐ USB ☐ Internal Flash

File Name: No file chosen

Step 16. Select **HTTP/HTTPS** in the *Copy Method* field.

File Operations

Operation Type: ☒ Update File
☐ Backup File
☐ Duplicate

Destination File Type: ☐ Running Configuration
☒ Startup Configuration
☐ Mirror Configuration
☐ Logging File
☐ Language File

Copy Method: ☒ HTTP/HTTPS ☐ USB ☐ Internal Flash

File Name: No file chosen

Step 17. In the *File Name* field, select the converted configuration file that was saved in Step 12.

File Operations

Operation Type: ☒ Update File
☐ Backup File
☐ Duplicate

Destination File Type: ☐ Running Configuration
☒ Startup Configuration
☐ Mirror Configuration
☐ Logging File
☐ Language File

Copy Method: ☒ HTTP/HTTPS ☐ USB ☐ Internal Flash

File Name: Tesla Migration.txt

Step 18. Reload the switch to load the new configuration.

Reboot

To reboot the device, click the 'Reboot' button.

Reboot: ☒ Immediate
☐ Date Time HH:MM
☐ In Days Hours Minutes

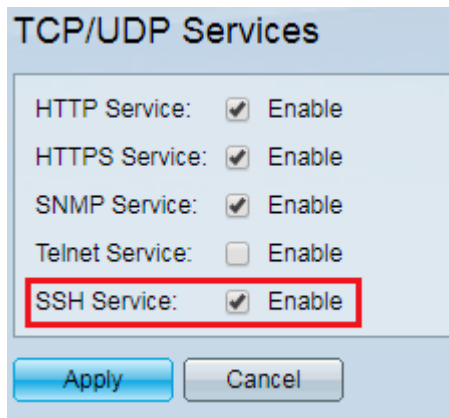
☐ Restore to Factory Defaults
☐ Clear Startup Configuration File

Conclusion

The instructions in this document allows you to convert configuration from a Sx200, Sx300, or Sx500 series switches to a Sx250, Sx350, or Sx550 series switches. To verify the device's successful conversion you can use the command line interface (CLI), following the below steps.

Note: In this example, I will be using SG550X-48MP as the destination switch.

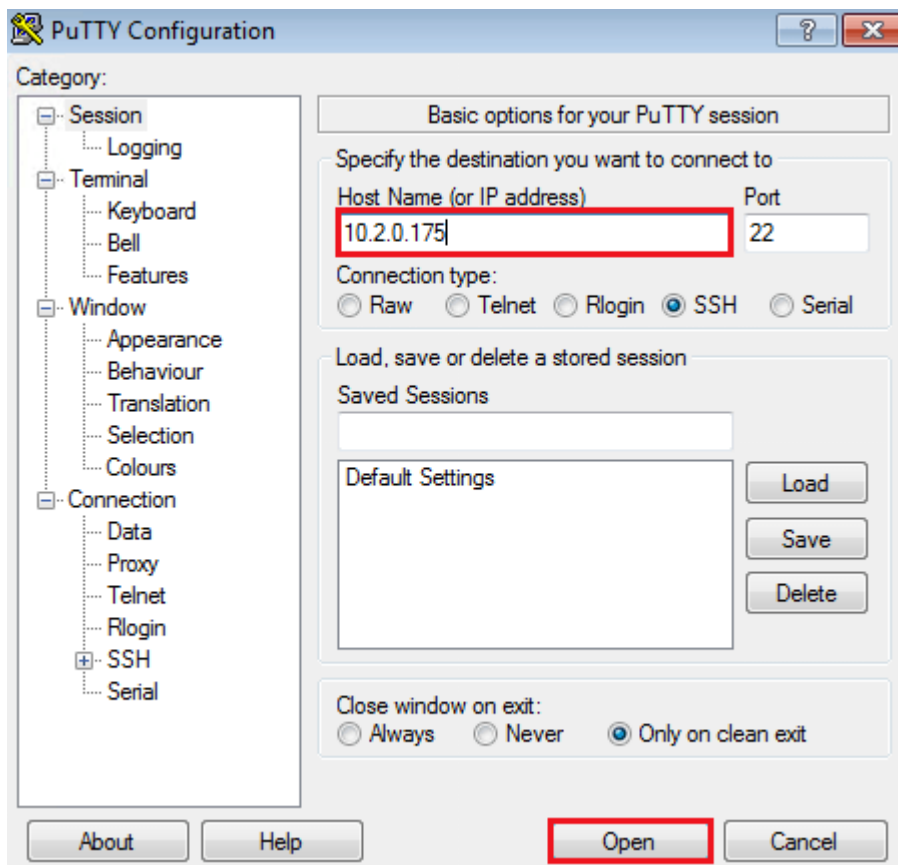
Step 1. Log in to the destination switch (Sx250, Sx350, or Sx550 series switches) and navigate to **Security > TCP/UDP Services**. Check the **SSH Service** check box to enable access of switches command prompt via SSH.



The screenshot shows the 'TCP/UDP Services' configuration window. It contains a list of services with checkboxes and 'Enable' labels: HTTP Service, HTTPS Service, SNMP Service, Telnet Service, and SSH Service. The 'SSH Service' checkbox is checked and highlighted with a red rectangular box. Below the list are 'Apply' and 'Cancel' buttons.

Step 2. You must use an SSH application in order to access the CLI. In this example, we will be using [PuTTY](#) to access the CLI of the switch. Begin by entering the IP address or hostname of the switch you want to access in the *Host Name (or IP address)* field. Then click **Open**.

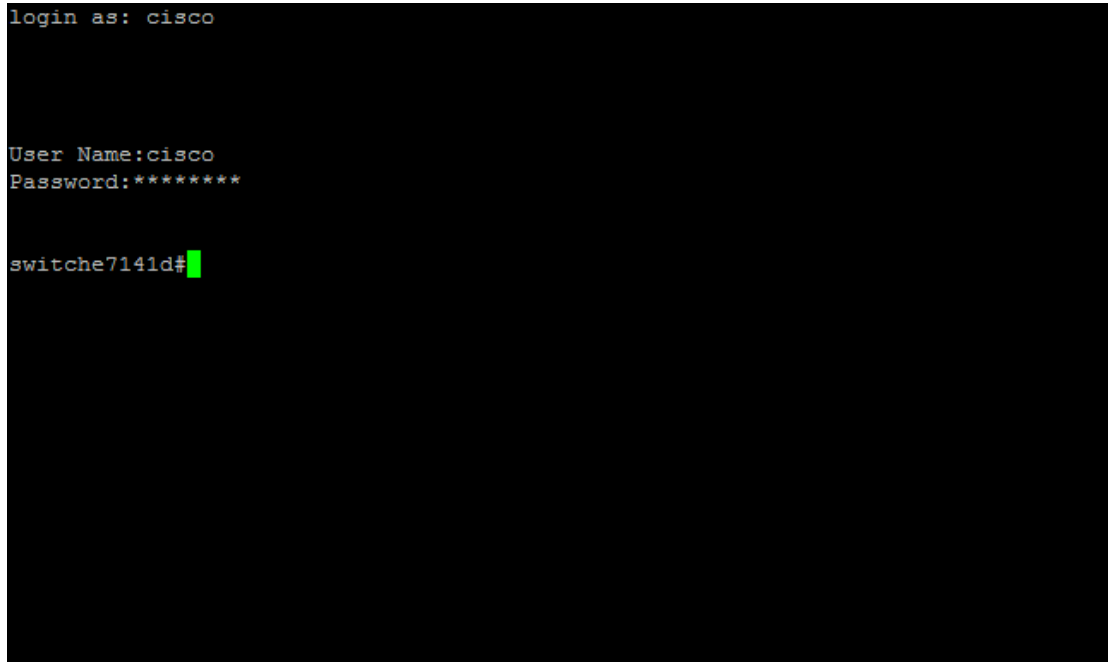
Note: Make sure the port is 22.



The screenshot shows the 'PuTTY Configuration' window. On the left is a tree view with categories: Session, Logging, Terminal, Keyboard, Bell, Features, Window, Appearance, Behaviour, Translation, Selection, Colours, Connection, Data, Proxy, Telnet, Rlogin, SSH, and Serial. The 'SSH' option under the 'Connection' category is selected. The main area is titled 'Basic options for your PuTTY session'. It contains fields for 'Host Name (or IP address)' (filled with '10.2.0.175') and 'Port' (filled with '22'). Below these are radio buttons for 'Connection type': Raw, Telnet, Rlogin, SSH (selected), and Serial. There is a section for 'Load, save or delete a stored session' with a 'Saved Sessions' list (containing 'Default Settings') and 'Load', 'Save', and 'Delete' buttons. At the bottom, there are radio buttons for 'Close window on exit': Always, Never, and Only on clean exit (selected). The 'Open' button at the bottom right is highlighted with a red rectangular box.

Step 3. Once you have established a connection with the switch, you should be prompted to enter your credentials. Enter your log in credentials to the switch.

Note: If you get a PuTTY Security Alert, hit **Yes** to update PuTTY's cache and continue connecting. In the picture below, I have not applied the converted configuration from SG500X-24MPP to SG550X-48MP, you can see that the current hostname is switche7141d.



```
login as: cisco

User Name:cisco
Password:*****

switche7141d#
```

Step 4. Type in the command **show startup-config**. This will display your converted startup-configuration that you have uploaded onto this switch.

Note: In the picture below, I have applied the converted configuration to the SG550X-48MP switch. You can see that the hostname is called Test-1.

```

Test-1#show startup-config
config-file-header
Test-1
v2.3.5.63 / RLINUX_923_093
CLI v1.0
file SSD indicator encrypted
@
ssd-control-start
ssd config
ssd file passphrase control unrestricted
no ssd file integrity control
ssd-control-end cb0a3fdb1f3a1af4e4430033719968c0
!
!
unit-type-control-start
unit-type unit 1 network gi uplink te
unit-type unit 2 network gi uplink te
unit-type unit 3 network gi uplink te
unit-type unit 4 network gi uplink te
unit-type unit 5 network gi uplink te
unit-type unit 6 network gi uplink te
unit-type unit 7 network gi uplink te
unit-type unit 8 network gi uplink te
unit-type-control-end
!
vlan database
vlan 2-3
exit
voice vlan oui-table add 0001e3 Siemens_AG_phone_____
voice vlan oui-table add 00036b Cisco_phone_____
voice vlan oui-table add 00096e Avaya_____
voice vlan oui-table add 000fe2 H3C_Aolynk_____
voice vlan oui-table add 0060b9 Philips_and_NEC_AG_phone_____
voice vlan oui-table add 00d01e Pingtel_phone_____
voice vlan oui-table add 00e075 Polycom/Veritel_phone____
voice vlan oui-table add 00e0bb 3Com_phone_____
bonjour interface range vlan 1
hostname Test-1
username cisco password encrypted e5df2d8279432f3e35b68b34c30b18f8d0ff8723 privilege 15
ip ssh server
!
interface vlan 2
name test-VLAN
!
interface vlan 3
More: <space>, Quit: q or CTRL+Z, One line: <return>

```