StoneOS Upgrade Guide

Version 5.5R11



TechDocs | docs.hillstonenet.com

Copyright 2024 Hillstone Networks. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Hillstone Networks.

Hillstone Networks

Contact Information:

US Headquarters:

Hillstone Networks

5201 Great America Pkwy, #420

Santa Clara, CA 95054

Phone: 1-408-508-6750

http://www.hillstonenet.com/about-us/contact/

About this Guide:

This guide gives you comprehensive configuration instructions of Hillstone Networks StoneOS .

For more information, refer to the documentation site: https://docs.hillstonenet.com.

To provide feedback on the documentation, please write to us at:

TechDocs@hillstonenet.com

Hillstone Networks

TWNO: TW-Upgrade-UNI-5.5R11-EN-V1.0-2024-07-05

Contents

Contents 1

About This Guide 6

Procedure 7

Procedure for Upgrade 7

Overview of Upgrade Steps 8

Preparations 9

Upgrade Notes 12

Upgrade Notes for Each Series of Platforms 13

Upgrade Notes for CloudEdge 13

Upgrading Notes for Each Module 16

Upgrading Notes for HSM & HSA Matching Version 18

Upgrading Notes for SSL VPN/ZTNA Function 18

Upgrading Notes for IPSec VPN Function 19

Upgrading Notes for Log Server Function 20

Upgrading Notes for Link Status Monitor Function 20

Upgrading Notes for IPS Signature Database 20

Upgrading Notes for Web Authentication Function 20

Upgrading Notes for IM Audit Function 21

Upgrading Notes for File Filtering Function 21

Upgrading Notes for Share Access Detect Function 21

Upgrading Notes for AD Agent Function 21
Upgrading Notes for SSO Monitor Function 21
Upgrading Notes for the SSL Proxy Function 22
Upgrading Notes for Link Load Balancing Function 22
Upgrading Notes for iQos Function 22
Upgrade Operations 23
Upgrading StoneOS via WebUI 24
Upgrading StoneOS via CLI 27
Upgrading StoneOS via FTP Server 27
Upgrading StoneOS via TFTP/FTPS/SFTP Server 30
Upgrading StoneOS via USB Drive 31
Upgrading StoneOS via Sysloader 32
Introduction to the Boot System 32
Physical Connection Requirements for the Device 32
PC Directly Connected to the Firewall via the Console Port 33
PC Connected to the Firewall via a Serial Server 33
Upgrade Procedure 33
Upgrading StoneOS via TFTP Server in Sysloader 34
Upgrading StoneOS via FTP Server in Sysloader 41
Upgrading StoneOS via USB Port in Sysloader 42
Introduction to the Sysloader Menu 43
Upgrading StoneOS in HA Environment 46

Environment 46
Upgrade Operations 46
Upgrading A/X/K Platform From 5.5 Versions to 5.5R11 46
Before You Start 46
Upgrading Device B 47
HA Synchronization and Switchover 47
Upgrading Device A 48
HA Synchronization 48
Completing the Upgrade 49
Upgrading StoneOS by Using Hotfix 50
Importing a Patch File 51
Loading/Activating/Running/Deleting a Patch 53
Viewing the Patch Status 54
Verification 55
Checking Whether the System Version is the Target Version 55
Checking Whether the Patch is Running/Activated Successfully 56
Checking Whether the Device Temperature, Power Supply, and Fan are Normal 56
Checking Whether the CPU Utilization and Memory Utilization of the Device are Normal 58
Checking Whether the Status of Each Expansion Module is Normal after the Upgrade 58
Checking Whether the Status of the Master and Backup Devices is Normal in an HA Scenario 59
Checking Whether the Configuration Takes Effect 61
Checking Whether Basic Services Can be Used Normally. 61

Upgrade Troubleshooting 62
Device Login Failure 62
Failure Description 62
Possible Causes 62
Processing Steps 63
Version File Import Failure 64
Failure Description 64
Possible Causes 64
Processing Steps 64
Device Reboot Failure after Upgrade 65
Failure Description 65
Possible Causes 65
Processing Steps 65
Software Version Rollback 67
Version Rollback Procedure 67
Version Rollback Operations 67
Verifying Whether the Rollback is Successful 68
Rolling Back Your Version via WebUI 69
Rolling Back to the Backup Version 69
Rolling Back to Other Versions 69
Rolling Back Your Version via CLI 70
Rolling Back to the Backup Version 70

Rolling Back to Other Versions 70
Rolling Back Your Version in Sysloader 71
Rolling Back to the Backup Version 71
Rolling Back to Other Versions 72

About This Guide

StoneOS Upgrade Guide provides instructions for upgrading the firmware version of StoneOS.

This guide covers the following topics: upgrade notes, preparations, procedure for upgrade, upgrade operations, verification after the upgrade, troubleshooting, and StoneOS version rollback.



Notes: This guide is applicable for upgrading devices to StoneOS 5.5R11. To upgrade to other versions, please refer to the corresponding upgrade guide.

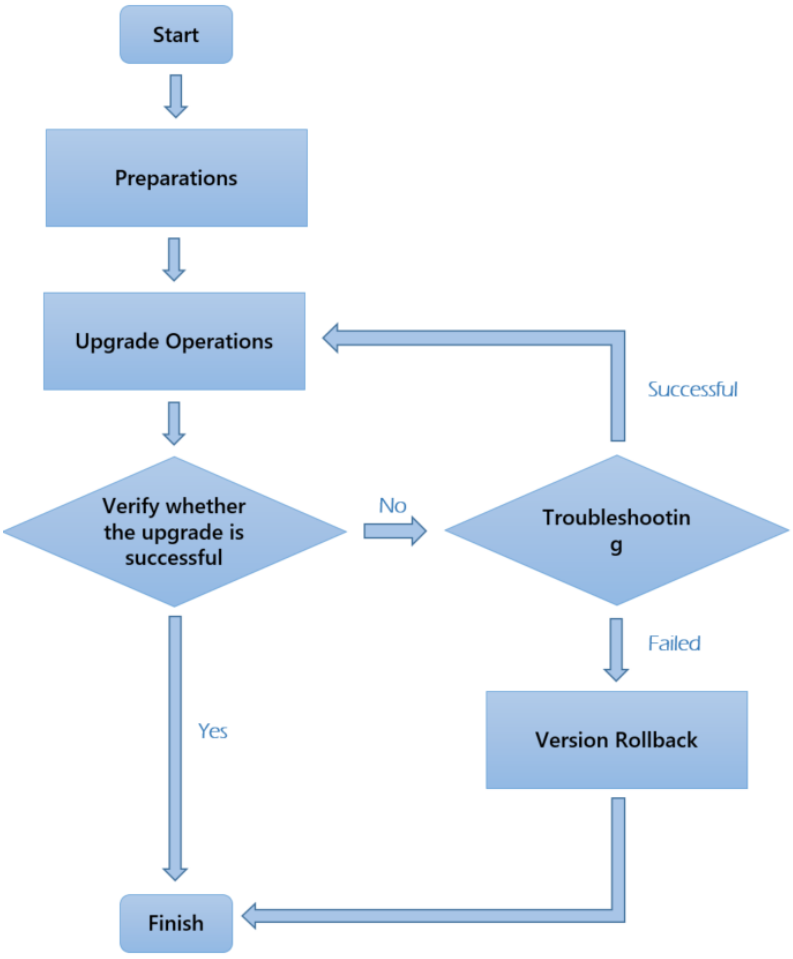
References:

- "Procedure" on Page 7
- "Preparations" on Page 9
- "Upgrade Notes" on Page 12
- "Upgrade Operations" on Page 23
- "Verification" on Page 55
- "Upgrade Troubleshooting" on Page 62
- "Software Version Rollback" on Page 67

Procedure

This chapter describes the system upgrade procedure and provides an overview of the steps involved.

Procedure for Upgrade



Overview of Upgrade Steps

1. Preparations before the upgrade. For more information, see "Preparations" on Page 9.
2. Perform system upgrade. To do this, select an appropriate upgrade method based on the current scenario and perform system upgrade based on the selected method. For more information, see "Upgrade Operations" on Page 23.
3. Verify whether the upgrade is successful. Perform necessary checks after the upgrade. If the upgrade is successful, the upgrade process is completed. For more information, see "Verification" on Page 55.
4. If the upgrade fails, check whether the upgrade steps are incorrect and perform troubleshooting. For more information, see "Upgrade Troubleshooting" on Page 62.
    - If troubleshooting is successful, repeat steps 2 and 3.
    - 若If troubleshooting fails, perform version rollback.
5. (Optional) Perform system version rollback. For more information, see "Software Version Rollback" on Page 67.

Preparations

To upgrade the version, complete the following processes step by step:

Preparations > "Upgrade Notes" on Page 12 > "Upgrade Operations" on Page 23 > "Verification" on Page 55

This chapter describes preparations required before performing the upgrade.

Please check the items in the following table in order.

No.	Check Item	Details
1	Prepare Upgrade Tools	Before upgrading, prepare the following tools: • operator terminal • network cable, serial cable • FTP/TFTP/FTPS/SFTP server/USB drive • terminal emulation program
2	Prepare New-Version System Software	Based on your device model, find the system file used by the model in *ReleaseNotes for StoneOS 5.5R11* and download it locally. You can also contact customer service at 1-800-889-9860 to obtain the corresponding system file. If the device model cannot be found in *ReleaseNotes for StoneOS 5.5R11*, it indicates that the model does not support the upgrade to 5.5R11. **Note**: If the platform license of the device has not expired, the device can be upgraded to the latest software version. If the platform license has expired, the device can only be upgraded to the software version released before the license expiration. The expiration date of the platform license can be viewed on the **System** > **License** page of the WebUI.

No.	Check Item	Details
3	Prepare Upgrade Reference Documents	Visit the Hillstone Networks Documents Center website at https://www.hillstonenet.com to obtain the latest version of the manuals. Ensure that the documents needed for reference during the upgrade process are printed and carried with you or stored on your computer.
4	Check Current Software Version	Based on the precautions of the product model and software version, select an appropriate upgrade method. To view the current software version, use one of the following methods: • WebUI: On the **System** > **System and Signature Database** page, view the current software version. • CLI: Use the **show version** command to view the current software version.
5	Check Device Operating Status	Ensure that the device is operating normally (device indicator status), and CPU and memory utilization are normal. To check CPU and memory utilization, use the **show cpu** and **show memory** commands. • For X-series devices and K9180 devices, use the **show module** command to check the operating status of each expansion module before and after the upgrade, to facilitate post-upgrade status check and troubleshooting in case of upgrade failure. • For HA devices, check the status of the master and backup devices and the HA control link status before the upgrade. For more information, see Checking

No.	Check Item	Details
		Whether the Status of Master and Backup Devices and the Status of HA Control Link are Normal.
6	Set Up Upgrade Environment	Requirements for setting up the upgrade environment: • Connect the PC's serial port to the device's CON port by using a serial cable. • Ensure network connectivity between the PC and the device.
7	Backup Current System Configuration	You can back up the configuration file within the system or export the configuration file. **Note:** You can back up the configuration file by clicking **Backup Restore** on the **System** > **Configuration File Management** > **Configuration File List** page of the WebUI, or export the configuration file from the **System** > **Configuration File Management** > **Current Configurations** page.

Upgrade Notes

To upgrade the version, complete the following processes step by step:

"Preparations" on Page 9 > **Upgrade Notes** > "Upgrade Operations" on Page 23 > "Verification" on Page 55

This chapter describes the notes for upgrading various series of firewall devices and the instructions for upgrading system functional modules.

Notes: It's strongly recommended that you upgrade to a neighbor version instead of upgrading across several versions. If you upgrade across several versions, please compare the configurations before and after the upgrade carefully. For more information, you can contact 1-800-889-9860.

- "Upgrade Notes for Each Series of Platforms" on Page 13
- "Upgrading Notes for Each Module " on Page 16

Upgrade Notes for Each Series of Platforms

Notes:

- Make sure that the current device is operating normally before the upgrade, including the indicators for power supply, fan, and pluggable modules such as expansion modules.
- Maintain a stable device status during the upgrade process. Do not power off, restart, or plug/unplug any pluggable modules.
- If you upgrade StoneOS via USB, do not remove the USB flash drive when restarting the device, as this may cause the device to fail to start properly.
- Make sure that the CPU utilization of the device is not too high before the upgrade.
- SG-6000-X9180/X10800 does not support an upgrade to StoneOS 5.5R11. If you want to upgrade your version, please contact 1-800-889-9860.

Upgrade Notes for CloudEdge

- StoneOS 5.5R11 only releases the firmware of CloudEdge. To upgrade CloudEdge to 5.5R11, take note of the following items:
  - 5.5R8P12/5.5R9P5/5.5R9F4 and later can be directly upgraded to 5.5R11;
  - For all R/F/M/P versions earlier than 5.5R8P12 and all R/F/M/P versions earlier than 5.5R9P5, upgrade to 5.5R8P12/5.5R9P5/5.5R9F4 and later first based on the instructions of related guide, and then upgrade to 5.5R11.
  - To obtain the upgrade file in the 5.5R11.img format, contact 1-800-889-9860.

- To upgrade 5.5R2 or lower versions to 5.5R11, we recommend you first upgrade to 5.5R6P12.2 based on related guidebooks, and then upgrade to 5.5R9P5/5.5R9F4 and later, and finally upgrade to 5.5R11.

  Upgrading system from 5.5R2 or lower versions to 5.5R9 and later is not supported. The reasons are as follows:

  - The default license in 5.5R1/5.5R2 is valid permanently, but only supports part of functions. However, the default license in 5.5R7 or higher versions is only valid for 30 days and supports all functions. Therefore, errors may occur when upgrading to 5.5R9 is performed.
  - Due to the default license is not pre-installed in the .img system file, it may not be valid for 30 days after upgrade.

- From 5.5R6, after the upgrade of CloudEdge, the licenses applied through the old SN code will be invalid because the SN code is changed. You need to apply and install the licenses with the new SN code, while the licenses distributed through LMS and vLMS system do not need to be reapplied. **We strongly recommend that you back up current configuration files before upgrading.**

- From 5.5R6, the firmware of CloudEdge will be unified into one type. System will automatically identify the platform model based on the CPU license and the resource configurations of VM. After system upgrades from the versions lower than 5.5R6 to 5.5R11, take note of the following items:

  - After upgrading, install the corresponding CPU license and configure VM resources (vCPU and memory) of the platform model as soon as possible. Otherwise, system may fail to display the corresponding platform model or start up.

    - When CPU license is installed, restart the device. If the right platform model can be displayed via the command **show version**, it indicates that CPU license has been installed successfully.
    - Configure the VM as the required resources of CloudEdge platforms: VM01 (2vCPU/2G memory) / VM02 (2vCPU/4G memory) / VM04 (4vCPU/8G memory)/VM08 (8vCPU/16G memory). If the minimum resources are not met before the upgrade, the system may fail to display the corresponding platform model or start up.
- From 5.5R4, the .img system files can be adapted to virtualization platforms automatically.
- From 5.5R4, the virtual MAC prefix of HA can be configured on CloudEdge, but the virtual MAC address will be changed after reboot.
- From 5.5R3, the system files are divided into IPv4 and IPv6 versions.
- From 5.5R1P15/5.5R2P8/5.5R3P6/5.5R4P4 and later P release, you're strongly recommended to use the 2vCPU/2GB memory to deploy CloudEdge VM01.
- From 5.5R5, at least 2vCPU/2G memory is required to deploy CloudEdge.

Upgrading Notes for Each Module



Notes:

- Before the upgrade, back up important data such as the current version of system file and login password to avoid data loss due to exceptions such as storage media damage.
- Confirm the compatibility between the system software version and the device model, as well as between the patch and the software version, as the upgrade will not be successful if the software package or patch is not matched. Compatibility between system software versions and device models can be found in *ReleaseNotes for StoneOS 5.5R11*; For compatibility between patches and software versions, please contact 1-800-889-9860.
- In the system, only one patch can be active or running. Before upgrading a new patch, ensure that no other patches are active or running. If there is a running patch, you need to unload the patch before proceeding with the upgrade.
- It is recommended to enable the logging function of terminal tool during the upgrade and collect print information.
- The device needs to restart during the upgrade, which may cause service interruptions. The interruption duration will be the time it takes for the device to restart.
- The returned information in the upgrade guide examples may vary based on devices.



- View the upgrade instructions for the corresponding functional modules in this chapter to confirm the differences between the command lines of the new and old versions. Changes in command lines may make some configurations unavailable.

If your device uses the following functional modules, pay attention to the upgrade instructions for the corresponding functional modules before the upgrade:

- Connecting to HSM&HSA
- SSL VPN/ZTNA function
- IPSec VPN function
- Log Server function
- Link Status Monitor function
- IPS Signature Database
- Web Authentication function
- IM Audit function
- File Filtering function
- Share Access Detect function
- AD Agent function
- SSO Monitor function
- SSL Proxy function

- Link Load Balancing function
- QoS function

Upgrading Notes for HSM & HSA Matching Version

When connecting 5.5R11 devices to HSA or HSM, you need to first upgrade HSA to 2.11.0 or later, or upgrade HSM to 4.15 or later.

Upgrading Notes for SSL VPN/ZTNA Function

1. From 5.5R9, the client supports to configure the TCP data tunnel port. The Windows client supports to configure communication stability optimization in version 1.4.9.1281 and later so that TCP data tunnels can be used. The macOS, Linux, iOS, Android, and ChineseOS client support to configure communication stability optimization in version 5.0.0 so that TCP data tunnels can be used.

    - If you use the Hillstone Secure Connect client (version 1.4.9.1281 and later), take note of the following items:

        - If the server enables the TCP port, the SSL VPN client can successfully connect to the server regardless of whether **Communication stability optimization** is selected.

        - If the server disables the TCP port, an error will occur when the SSL VPN client with **Communication stability optimization** selected starts a connection attempt. The connection can be successfully established after this option is deselected.

    - If you use the Hillstone Secure Connect client v5.0.0 or later, "Automatic" is added to the configuration of **Communication stability optimization**. If **Auto** is selected, the

system automatically selects the connection mode based on whether the TCP port is enabled on the server.

2. From 5.5R9, SSL VPN no longer supports RSA SecurID Token authentication by using the RSA server. When the system is upgraded from an earlier version to 5.5R9 or later, use other authentication methods.

3. From 5.5R10, it is necessary to use the new Hillstone Secure Connect client, which supports Windows, macOS, Linux, Android, iOS, and ChineseOS operating systems.

4. From 5.5R10, the SSL VPN Address Pool function has been changed to the Access Address Pool function. Changes have been made on the CLI and WebUI, for example: The command **scvpn pool** *pool-name* is replaced with access-address-pool pool-name. You can select **Object** > **Access Address Pool** on the WebUI. When the system is upgraded from an earlier version to 5.5R10 or later, the original configuration is retained and can be used normally.

5. From 5.5R11, when configuring ZTNA endpoint tag information items, the ChineseOS client needs to configure the operating system type as ChineseOS to match ZTNA policies. In StoneOS 5.5R10 and earlier versions, the ChineseOS client can match ZTNA policies just by configuring the operating system type as Linux.

Upgrading Notes for IPSec VPN Function

From 5.5R11, the CLI configuration of IKEv2 has been adjusted. When upgrading from a version earlier than 5.5R11 to 5.5R11 or later, the IKEv2 configuration will automatically be converted, and the IKEv2 tunnel instance will forcefully enable check-id. The names of IKEv2 P1 proposal, P2 proposal, ISAKMP gateway, and tunnel instance will be converted to "name_ikev2".

If the names of IKEv1 and IKEv2 are the same and have the maximum character length in versions earlier than 5.5R11, upgrading to 5.5R11 or later may cause IKEv2 configuration loss.
Solution: It is recommended to reconfigure this function.

Upgrading Notes for Log Server Function

From 5.5R11, the commands for configuring the log server have been adjusted, and when you create a log server, you need to specify the server name.

If a log server is configured before the upgrade, the corresponding server name field (composed of Syslog Server address/hostname, protocol type, destination port number, binding method, and binding name) will be automatically generated during the upgrade. The original log server configuration will be automatically split into the configuration commands of multiple parameters. For more information, refer to *StoneOS CLI User Guide*.

Upgrading Notes for Link Status Monitor Function

From 5.5R11, in WebUI, the "Detection Destination" configuration item on the Link Status Monitor page has been moved to the Link Detection page. After entering the Link Detection page, you can configure the detection destination in the upper-right corner of the page.

Upgrading Notes for IPS Signature Database

From 5.5R8P2, IPS signature database 3.0 is supported. You can update your IPS signature database to the latest version with improved protection capability based on your requirements. The original IPS signature database 2.0 can still be used after the system is upgraded. To update IPS Signature Database, go to **System** > **Upgrade Management** > **Signature Database Update** and update it online, or download IPS signature database 3.0 for offline update.

Upgrading Notes for Web Authentication Function

From 5.5R5, Web authentication function is adjusted. When the system is upgraded from versions lower than 5.5R5 to 5.5R11, the custom files (such as Web authentication background images, web redirection background images) uploaded by the old version will not take effect, you need to configure it again.

Upgrading Notes for IM Audit Function

From 5.5R5, IM audit function is adjusted. When the system is upgraded from versions lower than 5.5R5 to 5.5R11, the old configurations will be lost, you need to configure it again.

Solution: Reconfigure this function via WebUI after upgrade.

Upgrading Notes for File Filtering Function

From 5.5R5, the function of file filtering will no longer support filtering through file name and file size. When the system is upgraded from versions lower than 5.5R5 to 5.5R11, the old configurations will be lost.

Solution: Reconfigure this function

Upgrading Notes for Share Access Detect Function

From 5.5R6, share access function is adjusted, the command **host share-access detect enable** of share access detect function will no longer be supported. When the system is upgraded from versions lower than 5.5R6 to 5.5R11, the old configurations will be lost, you need to configure the share access function again.

Upgrading Notes for AD Agent Function

To use AD Agent software to obtain user information in version earlier than StoneOS 5.5R10, you can connect the AD agent by using SSO Monitor or configure the security agent in Active-Directory server configuration mode. In StoneOS 5.5R10 and later, the system no longer supports the security agent function. When the version is upgraded to StoneOS 5.5R11, the configured security agent function is automatically converted to the SSO Monitor function to connect to the AD Agent software configuration. You can run the **show user-sso client sso-monitor** *profile-name* command to view the configuration. The converted name of SSO Monitor Profile is the same as that of the AD server.

Upgrading Notes for SSO Monitor Function

From StoneOS 5.5R10, SSO Monitor can connect to multiple external servers to implement redundant backup. Therefore, the configured **host x.x.x.x** of SSO Monitor will be automatically

converted to **host1 x.x.x.x** after the system is upgraded to StoneOS 5.5R11. You can run the **show user-sso client sso-monitor** *profile-name* command to view the converted configuration.

Upgrading Notes for the SSL Proxy Function

From 5.5R9, the system changes the default value of the **Unsupported version**, **Unsupported encryption algorithms**, **Unknown Error**, and **Client verification** parameters in the SSL Proxy configuration from **Block** to **Bypass**. After the system is upgraded to 5.5R9 and later, related configurations will change. If you still want to use the **Bypass** value, manually change the configurations.

Upgrading Notes for Link Load Balancing Function

From 5.5R4, **llb outbound** related command is no longer supported, with the new command **llb rule** instead. When the system is upgraded from versions lower than 5.5R4 to 5.5R7 or later, the old configurations will be lost, you must configure it again.

Upgrading Notes for iQos Function

Intelligent Quality of Service (iQos) is added from version 5.5R1, and the function is enabled automatically from 5.5R2. When system with QoS configured is upgraded to 5.5R7 or higher versions, use the **exec iqos enable** command to enable iQoS (iQoS can only be configured via CLI). After iQoS is enabled, the QoS configurations will be saved but become invalid and cannot be edited. If you need to enable QoS, use the **exec iqos disable** command to disable iQoS and reactivate QoS.

From 5.5R6, iQoS can be obtained via IOM module on the X platform. Before obtaining the iQoS function via IOM module, make sure the iQoS license has been installed.

Upgrade Operations

To upgrade the version, complete the following processes step by step:

"Preparations" on Page 9 > "Upgrade Notes" on Page 12 > **Upgrade Operations** > "Verification" on Page 55

This chapter describes the methods for upgrading the version of the device, the operations for upgrading the version in an HA environment, and the operations for applying patches to the current software version.

- "Upgrading StoneOS via WebUI" on Page 24
- "Upgrading StoneOS via CLI" on Page 27
- "Upgrade Procedure" on Page 33
- "Upgrading StoneOS in HA Environment" on Page 46
- "Upgrading StoneOS by Using Hotfix" on Page 50

Upgrading StoneOS via WebUI



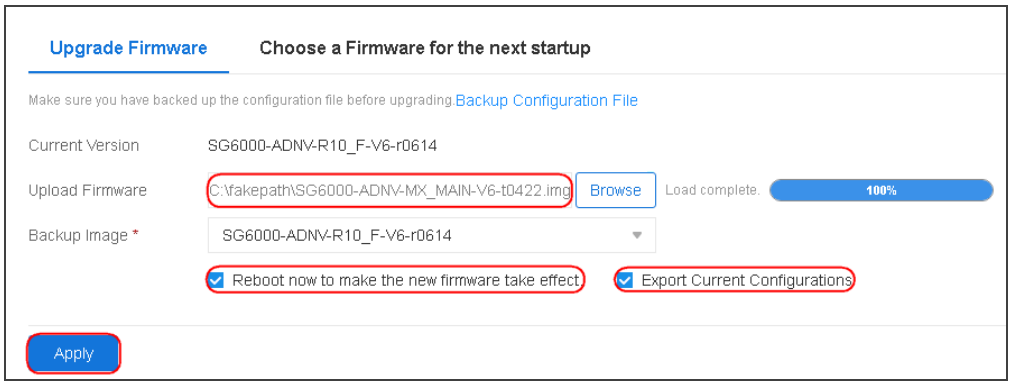
Notes:

- When you upgrade StoneOS via WebUI, prepare the software version file to be upgraded on your local computer first.
- When you upgrade StoneOS via WebUI, the system will use the startup file for reboot by default. During the upgrade process, the system will pop up a tips message to ask if you want to save the current configuration of the device, please click **OK**, the system will save the current configuration of the system to the startup file.

To upgrade the software version via WebUI, take the following steps:

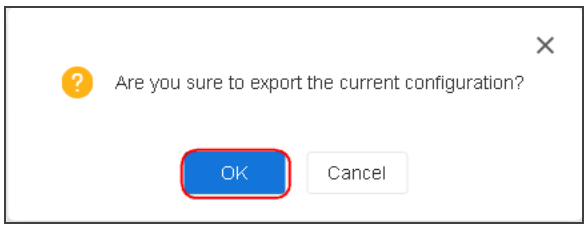
1. Log into the WebUI of the device.
2. Select **System** > **Upgrade Management** > **Upgrade Firmware**.
3. On the **Upgrade Firmware** page, click the **Upgrade Firmware** tab.
4. Upload the version file. To do this, click **Browse** and select a software version file from your computer.
5. After you upload the version file, the **Export Current Configuration** checkbox is selected by default. Do not select this checkbox if the configuration file is not backed up before the upgrade.

6. Select **Reboot now to make the new firmware take effect** and click **Apply**.

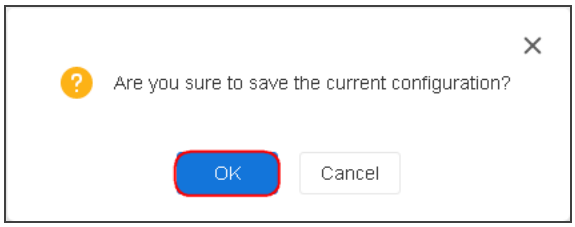


Note: If you do not select **Reboot now to make the new firmware take effect**, you can also click Apply to save the configuration. The new version will take effect after the next reboot.

7. A message pops up asking if you want to export the current configuration. Click **OK**, and the configuration file will be exported in .DAT format to your local computer.



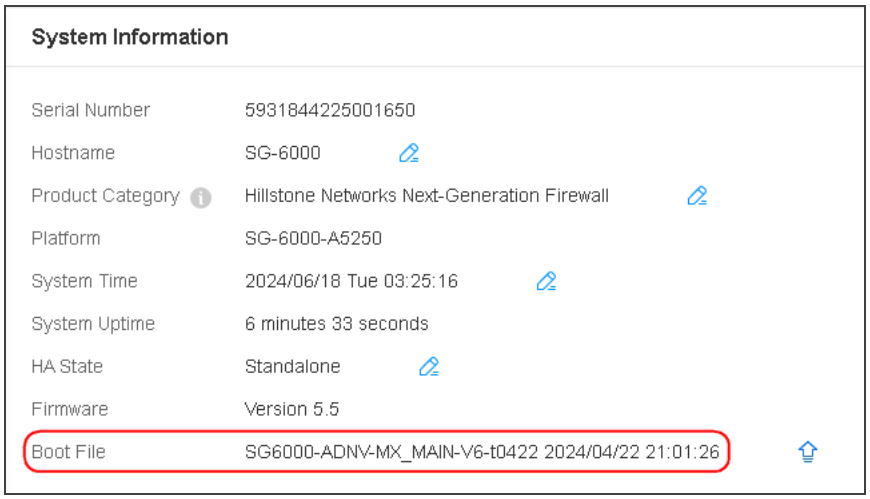
8. During the system reboot, a message pops up asking if you want to save the current configuration of the device. Click **OK**.



9. Wait for a period of time during the upgrade process, and do not perform any operations. After the upgrade is completed, a message pops up saying "Login time out. Please login

again." Click **OK**. The login page of the WebUI will appear. Then, enter your username and password to log in to the new version.

10. Verify whether the system version is the target version. To do this, select **System** > **System and Signature Database** to check if the "Boot File" is consistent with the target new version. If so, the upgrade is successful.



Upgrading StoneOS via CLI

You can upgrade StoneOS via CLI by using an FTP server, TFTP server, FTPS server, SFTP server, or USB drive.

Upgrading StoneOS via FTP Server

1. After logging into the CLI, in execution mode, use the following command to import the version file to be upgraded via the FTP server:

   import image from ftp server *ip-address* [**user** *user-name* **password** *password*] [**vrouter** *vrouter-name*] *file-name*

   Take SG-6000-A7600 as an example:

```
hostname# import image from ftp server 10.10.10.2 vrouter trust-vr user admin password test123 test/5.5R11/SG6000-ADNV-MX_MAIN-V6-r0516.img
```

Variable	Description
ip-address	Specifies the IP address of the FTP server.
user *user-name* **password** *password*	Specifies the username and password of the FTP server.
vrouter-name	Specifies the Vrouter corresponding to the device interface used to access the FTP server.
file-name	Specifies the name of the file of the version to be upgraded. If the version file is in the root directory of the FTP server, enter the version file name directly. If the version file is in a subdirectory, enter the "full path + version file name".

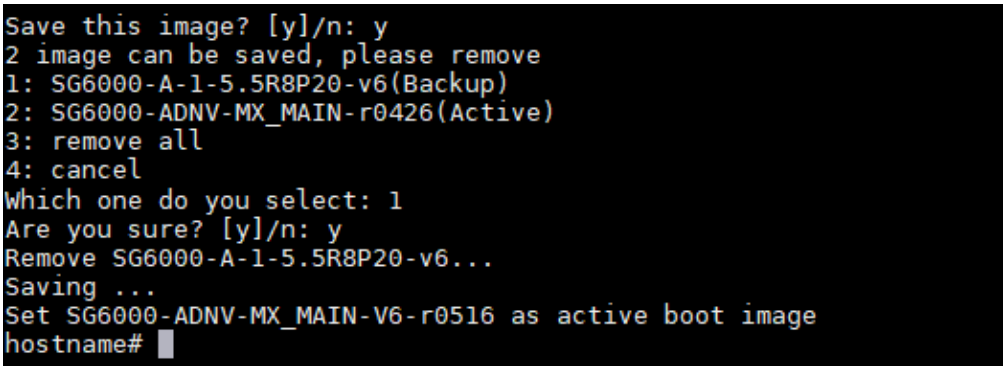
Variable	Description
	For example, if SG6000-ADNV-MX_MAIN-V6-r0516.img is in the test/5.5R11 directory on the FTP server, enter test/5.5R11/SG6000-ADNV-MX_MAIN-V6-r0516.img as the file name.

2. After importing the version file, save the version file to be upgraded as follows:

    1. The system prompts "Save this image?". Select 'y' to save the current version file to be upgraded.

    2. Delete any excess version files in the system. The device's Flash can store up to two version files. If Flash already contains two version files, delete one of the stored version files as prompted.
       For example, if the system prompts "Which one do you select:", select '1' to delete the currently backed-up version file.

    3. The system prompts "Are you sure?". Select 'y' to confirm the deletion of the currently backed-up version file.



3. In execution mode, enter the **reboot** command to restart the system and apply the new StoneOS version.

    1. Enter the **reboot** command and press Enter.

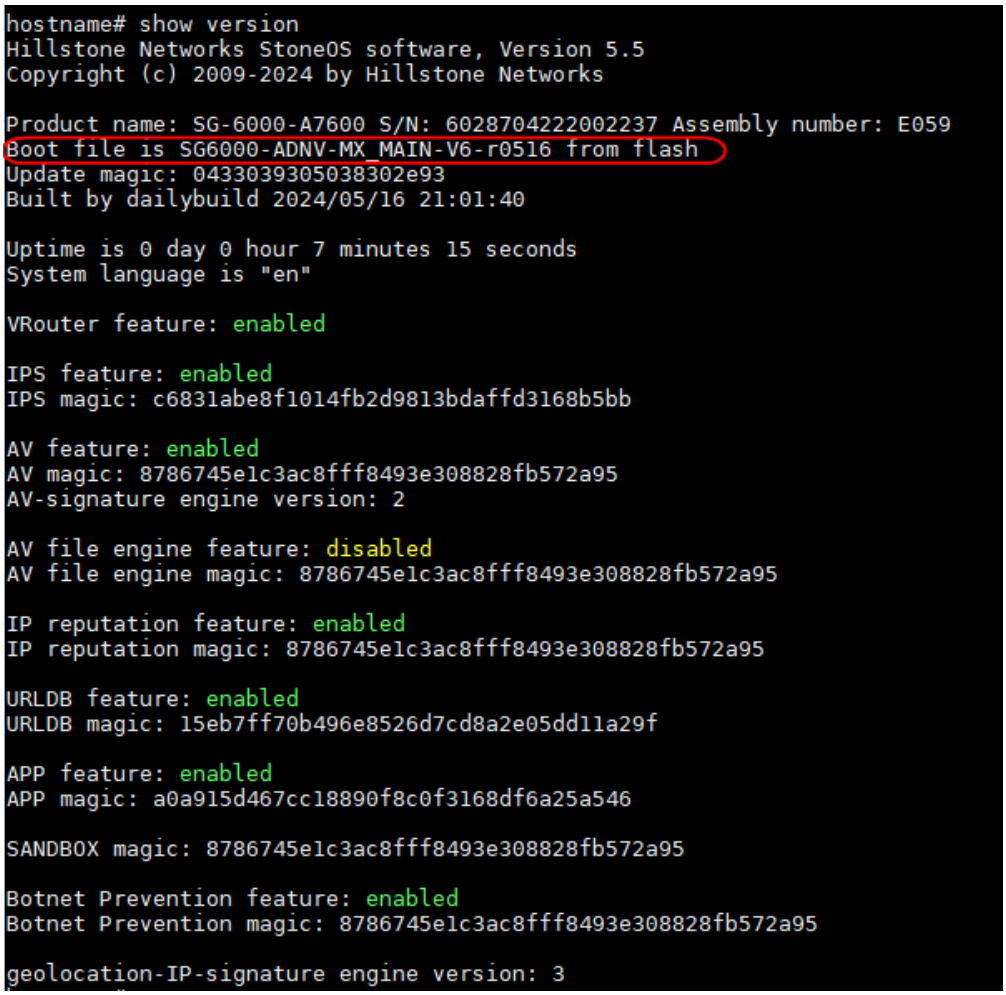
    2. The system prompts "System reboot, are you sure?". Select 'y' to confirm the device reboot.

    3. Select a configuration file in the system as the startup file when the device restarts. For example, if the system prompts "Please choose one:", select "a" startup file as the device's startup file.

```
hostname# reboot
System reboot, are you sure? y/[n]: y
3 configuration in system, please choose one to be loaded.
=========================================================================
        Name      Version        Save Time           Size (bytes)
-------------------------------------------------------------------------
    [a]: Startup   5.5R11         2024-05-21 10:57:33 45738
    [b]: Backup 1  5.5R11         2024-04-03 16:03:22 45686
    [c]: Backup 0  5.5R10         2024-02-19 14:49:54 39046
=========================================================================
Press enter to use system current setting
Please choose one: a
```

4. Wait for the upgrade to complete without performing any operations. After the upgrade is completed, log into the CLI again, and enter the **show version** command to verify if the system has been successfully upgraded to the new version. As shown in the following figure,

SG-6000-A7600 has already been upgraded to the target version.



Upgrading StoneOS via TFTP/FTPS/SFTP Server

You can also upgrade StoneOS via a TFTP, FTPS, or SFTP server. The upgrade method is similar to upgrading via an FTP server. You can refer to Upgrading StoneOS via FTP Server.

Commands for importing a version file:

- TFTP server: **import image from tftp server** *ip-address* [**vrouter** *vrouter-name*] *file-name*
- FTPS server: **import image from ftps server** *ip-address* [**user** *user-name* **password** *password*] [**vrouter** *vrouter-name*] *file-name*

- SFTP server: **import image from sftp server** *ip-address* [**user** *user-name* **password** *password*] [**vrouter** *vrouter-name*] *file-name*

Upgrading StoneOS via USB Drive



Notes: To upgrade StoneOS via USB drive, save the version file to be upgraded in the root directory of the USB drive.

1. Copy the version file to the root directory of the USB drive.
2. Insert the USB drive into the USB port of the device.
3. After logging into the CLI, upgrade StoneOS via USB drive by using the following command in execution mode:

   import image from {**usb0** | **usb1**} *file-name*

   - **usb0** | **usb1** – Specifies the USB port of the device used for the upgrade.
   - *file-name* – Specifies the name of the version file to be upgraded. Example: SG6000-ADNV-MX_MAIN-r0401.img.
4. After importing the version file, follow the prompts in the CLI to save the version file to be upgraded and delete the previous version file as needed. You can refer to Step 2 of Upgrading StoneOS via FTP Server.
5. In execution mode, enter the **reboot** command to restart the system and apply the new StoneOS version. You can refer to Step 3 of Upgrading StoneOS via FTP Server.
6. During the upgrade process, do not perform any operations. After the upgrade is completed, log into the CLI and enter the **show version** command to verify whether the system is successfully upgraded to the new version.
7. Remove the USB drive promptly after the upgrade is completed.

Upgrading StoneOS via Sysloader

When the device fails and cannot boot into the StoneOS system, you can upgrade StoneOS via Sysloader by using an FTP server, TFTP server, or USB drive.

Introduction to the Boot System

Hillstone Networks firewall devices have a boot system divided into three parts: Bootloader, Sysloader, and StoneOS. Some devices only include Sysloader and StoneOS. Their functions are as follows:

- Bootloader – The first program that runs when the device is powered on. Bootloader loads and executes StoneOS or Sysloader.
- Sysloader - Used to upgrade StoneOS.
- StoneOS – The operating system of the device.

When the device starts, you can press the "ESC" key as prompted, and the Bootloader will attempt to start Sysloader. StoneOS is the OS of the device. Sysloader allows for updating and selecting StoneOS and supports upgrade via FTP, TFTP, and directly via USB Host port.

During device startup, some devices require pressing "Ctrl+W" to enter Sysloader, and it may prompt for a password or username and password. The actual device prevails. If you need a username and password, contact 1-800-889-9860.



Notes: Only A200, A200W, A200G4B, A1600, A1800, A2200, and X8180 devices need to enter Sysloader via Bootloader.

Physical Connection Requirements for the Device

When you upgrade StoneOS via Sysloader, the PC needs to be directly connected to the firewall via the Console port or connected by using a serial server.

PC Directly Connected to the Firewall via the Console Port

Upgrade personnel in a data center environment can connect the Console port of the firewall directly to the PC by using an RS-232 cable to perform the upgrade operation.

PC Connected to the Firewall via a Serial Server

If the data center has a serial server and the serial port of the server is connected to the Console port of the firewall via an RS-232 cable, the upgrade personnel can connect to the firewall remotely by using the serial server, thus performing the upgrade operation.

Run a terminal emulation program on the PC of the user, connect to the firewall by using the serial server, and enter the following command:
telnet *ip-address port*

- *ip-address* – Specifies the IP address of the serial server.
- *port* – Specifies the server port number of the serial server connected to the firewall.

Upgrade Procedure

In Sysloader, you can upgrade StoneOS by using an FTP server, TFTP server, FTPS server, SFTP server, or a USB drive.

Notes: Before upgrading StoneOS via Sysloader, complete the following steps:

1. The Console port (CON port) of the firewall is connected to the serial port of PC via a standard RS-232 cable. If the firewall is connected to a serial server, the PC of the user can be connected to the firewall through remote access to the serial server.
2. Obtain the baud rate of the Console port of the firewall in advance. Ensure that the baud rate of the terminal emulation program matches the baud rate of the device when running terminal emulation program on the PC to

establishing a connection with the firewall. Use the **show console** command to view the baud rate of the Console port of the device. If the device does not change the baud rate, you can refer to **Hardware Reference Guide** to obtain the default baud rate of the device.

3. Connect the MGT port of the device to the FTP/TFTP server. If there is no MGT port, use the eth0/0 interface.
4. After completing the above steps, restart the device and enter the boot system of the device.

Upgrading StoneOS via TFTP Server in Sysloader

Sysloader can obtain the version file to be upgraded from a TFTP server, allowing you to quickly upgrade StoneOS through the network. To do this, take the following steps:

1. After the CON port of the device is connected to the serial port of the PC via an RS-232 cable, restart the device and enter Sysloader during the reboot process. If Sysloader cannot be selected by using the up and down arrow keys, press "Ctrl+W" first and then enter Sysloader. For example, the SG-6000-K6580 device requires pressing "Ctrl+W" to enter Sysloader. The returned information may vary based on devices.

   Take SG-6000-X25803 as an example:

```
                GNU GRUB version 2.02
SG6000-XN-5.5R11B5-v6
SG6000-XN-5.5R11B8-v6
*SYSLOADER( Select Sysloader by using the up and
down arrow keys and press Enter to enter Sys-
loader)
```

```
Loading Sysloader
[ 7.253642]
[ 7.255125] Arbitrating
[ 7.373235] -> Master
Sysloader 2.0.4 Jul 19 2023 - 11:40:32
Enter the password to stop autoboot: 3( Enter the
password that is used to log into Sysloder within 5
seconds and press Enter. To obtain the password,
contact 1-800-889-9860.)
sysloader(M)#
1 Load firmware via TFTP
2 Load firmware via FTP
3 Load firmware from USB disks (not available)
4 Select backup firmware as active
5 Show on-board firmware
6 Reset
7 Reset Administrator password
8 Load sysloader via TFTP
```

Take SG-6000-A2000 as an example:

```
                        GNU GRUB version 2.02
SG6000-ADNV-MX_MAIN-V6-t0419
SG6000-ADNV-MX_MAIN-r0420
*SYSLOADER( Select Sysloader by using the up and
down arrow keys and press Enter to enter Sys-
loader)
Sysloader 1.0.5 Sep 23 2020 - 16:09:24
```

```
sysloader#
1 Load firmware via TFTP
2 Load firmware via FTP
3 Load firmware from USB disks (available)
4 Select backup firmware as active
5 Show on-board firmware
6 Reset
7 Reset Administrator password
8 Load sysloader via TFTP
```

For devices that need to enter Sysloader via Bootloader, follow these prompts (using SG-6000-A200 as an example):

```
Press ESC to stop autoboot: 2( Press "ESC" to enter the interactive mode of Bootloader)
load sysloader from USB? [y]/n: n( Type "n" for not upgrading Sysloader via USB)
Run on-board sysloader? [y]/n: y( Type "y" to enter Sysloader)
Loading: #
Starting kernel ...
Sysloader 8.0.10 Feb 2 2023 - 09:16:23
sysloader#
1 Load firmware via TFTP
2 Load firmware via FTP
3 Load firmware from USB disks (not available)
4 Select backup firmware as active
5 Show on-board firmware
```

```
6 Reset

7 Reset Administrator password
```

For SG-6000-K6580, press "Ctrl+W" and then select Sysloader. Follow these prompts:

```
                          GNU GRUB version 2.06

SG6000-HYGON-MX_MAIN-V6-r0420

SG6000-HYGON-R10_F-V6-r0409

*SYSLOADER( Select Sysloader by using the up and
down arrow keys and press Enter to enter Sys-
loader)

Enter username:(Enter the username used to log into
Sysloder and press Enter. To obtain the username,
contact 1-800-889-9860.)

Enter password:(Enter the password used to log into
Sysloder and press Enter. To obtain the password,
contact 1-800-889-9860.)

Loading Sysloader

▒

Sysloader 8.0.12 May 22 2023 - 01:52:42

sysloader#

1 Load firmware via TFTP

2 Load firmware via FTP

3 Load firmware from USB disks (not available)

4 Select backup firmware as active

5 Show on-board firmware

6 Reset

7 Reset Administrator password
```

```
8 Clear button
9 Load sysloader via FTP
```

2. From the Operation Selection menu of Sysloader, select Upgrade StoneOS via TFTP Server. Follow these prompts (using SG-6000-A2000 as an example):

   Note: The startup option of Sysloader may vary based on platforms. For more information, see Introduction to the Sysloader Menu.

```
Sysloader 1.0.5 Sep 23 2020 - 16:09:24
sysloader#
1 Load firmware via TFTP
2 Load firmware via FTP
3 Load firmware from USB disks (available)
4 Select backup firmware as active
5 Show on-board firmware
6 Reset
7 Reset Administrator password
8 Load sysloader via TFTP
sysloader# 1( Enter "1" here and press Enter)
```

3. Configure the IP address of Sysloader, the IP address of TFTP server, the gateway IP address, and the version file name to be upgraded. Follow these prompts (using SG-6000-A2000 as an example):

```
Local ip address [ ]: 192.168.1.1/16 ( Enter the IP address of Sys-
loader and press Enter)
  Server ip address [ ]: 192.168.1.20 ( Enter the IP address of the
  TFTP server and press Enter)
  Gateway ip address [ ]: 192.168.1.2 ( If the IP addresses of Sys-
```

```
loader and the TFTP server do not belong to the
same CIDR block, enter the IP address of the gate-
way and press Enter; otherwise, just press Enter)

File name : SG6000-ADNV-MX_MAIN-r0401.img( Enter the version
file name to be upgraded and press Enter. The sys-
tem will start to obtain the version file to be
upgraded via TFTP. If the version file is not in
the root directory of the TFTP server, you need to
enter "full path + version file name". For example,
if SG6000-ADNV-MX_MAIN-r0401.img is in the
test/5.5R11 path on the TFTP server, enter
test/5.5R11/SG6000-ADNV-MX_MAIN-r0401.img as the
file name.)

SG6000-ADNV-MX_MAIN- 100%
|*****************************| 327M 0:00:00 ETA
```

4. Save the version file to be upgraded. Follow these prompts (using SG-6000-A2000 as an example):

```
Save this image? [y]/n: y( Type "y" or press Enter to save
the obtained version file)

Only 2 image can be saved, please remove( A maximum
of two version files can be stored in the Flash of
the device. If two version files are already stored
in the Flash, follow the prompts to delete the
stored version file.)

1: SG6000-ADNV-MX_MAIN-r0420(Backup)( Delete the
currently backed-up version file)

2: SG6000-ADNV-MX_MAIN-V6-t0419(Active)( Delete the
current system version file)

3: remove all( Delete all version files except for
```

```
the one to be upgraded)
4: cancel( Do not delete any files, select 4 to
exit the upgrade)
Which one do you select: 2
Are you sure? [y]/n: y
Remove SG6000-ADNV-MX_MAIN-V6-t0419...
Saving
.................................................-
.........
Checking saved firmware
.............................................. OK
Set SG6000-ADNV-MX_MAIN-r0401 as active boot image
```

5. Restart the system. The system will start with the new version file. Follow these prompts (using SG-6000-A2000 as an example):

```
1 Load firmware via TFTP
2 Load firmware via FTP
3 Load firmware from USB disks (not available)
4 Select backup firmware as active
5 Show on-board firmware
6 Reset
7 Reset Administrator password
8 Load sysloader via TFTP
sysloader# 6( Enter "6" here and press Enter, the
system will restart)
```

6. During the upgrade process, do not perform any operations. After the upgrade is completed, log into the CLI and enter the **show version** command to verify whether the system is successfully upgraded to the new version.

Upgrading StoneOS via FTP Server in Sysloader

The device support to obtain the version file to be upgraded from an FTP server. To upgrade StoneOS via FTP in Sysloader, take the following steps:

1. Enter Sysloader, select "2" from the Operation Selection menu of Sysloader, and press Enter. For more information about how to enter Sysloader, refer to Step 1 of Upgrading StoneOS via TFTP Server in Sysloader.
2. Configure the IP address of Sysloader. Enter the IP address configured for the Sysloader after "*Local ip address [ ]:*" and press Enter.
3. Configure the IP address of the FTP server. Enter the IP address of the FTP server after "*Server ip address [ ]:*" and press Enter.
4. If the IP addresses of Sysloader and the FTP server do not belong to the same CIDR block, configure the Sysloader's gateway IP address. Enter the gateway IP address after "*Gateway ip address [ ]:*" and press Enter.
5. Enter the FTP username after "*User Name [anonymous]:*" and press Enter.
6. Enter the corresponding password for the username after "*Password :*" and press Enter.
7. Enter the version file name to be upgraded after "*File name :*" and press Enter. The system will start to obtain the specified StoneOS via FTP. If the version file is not in the root directory of the FTP server, you need to enter "full path + version file name". For example, if SG6000-ADNV-MX_MAIN-r0401.img is in the test/5.5R11 path on the FTP server, enter test/5.5R11/SG6000-ADNV-MX_MAIN-r0401.img as the file name.

8. After the version file is transferred, the system will ask if you want to save the version file. Type "y" and the system will save the version file to the Flash of the device.
   Note: A maximum of two version files can be stored in the Flash of the device. If two version files are already stored in the Flash, follow the prompts to delete the stored version file.
9. After the version file is saved, press Enter, the Operation Selection menu of Sysloader will appear again. Select "6" and press Enter. The system will restart with the new version file.
10. During the upgrade process, do not perform any operations. After the upgrade is completed, log into the CLI and enter the **show version** command to verify whether the system is successfully upgraded to the new version.



Tips: For anonymous FTP servers, directly press Enter after "*User Name* [*anonymous*]:" and "*Password* :" (Step 5 and Step 6).

Upgrading StoneOS via USB Port in Sysloader

You can also upgrade StoneOS via the USB Host port of the device by saving the version file to be upgraded in a USB flash drive.



Notes: To upgrade StoneOS via USB, you need to save the version file to be upgraded in the root directory of the USB flash drive.

Take the following steps:

1. Copy the version file to be upgraded to the root directory of the USB flash drive.
2. Insert the USB flash drive into the USB port of the device.
3. Enter Sysloader and select "3" from the Operation Selection menu of Sysloader, and press Enter.

4. Enter "y" after the version file to be upgraded, and the system will start to obtain the version file from the USB flash drive. The returned information may vary based on devices. Follow these prompts:

```
sysloader# 3( Enter "3" here and press Enter)
Please select firmware
1 SG6000-ADNV-MX_MAIN-r0401.img (usb0) [y]/n: n
2 SG6000-ADNV-MX_MAIN-V6-t0422.img (usb0) [y]/n: y
```

   Note: If two USB flash drives are inserted into the device, and the version file to be upgraded is on USB1, first type "n" for the version file on USB0.

5. After the version file is transferred, the system will ask if you want to save the version file. Type "y" and the system will save the version file to the Flash of the device.
   Note: A maximum of two version files can be stored in the Flash of the device. If two version files are already stored in the Flash, follow the prompts to delete the stored version file.

6. After the version file is saved, press Enter, the Operation Selection menu of Sysloader will appear again. Select "6" and press Enter. The system will restart with the new version file.

7. During the upgrade process, do not perform any operations. After the upgrade is completed, log into the CLI and enter the **show version** command to verify whether the system is successfully upgraded to the new version.

8. Remove the USB drive promptly after the upgrade is completed.

Introduction to the Sysloader Menu

Sysloader uses menu prompts to help you complete specified operations. This section introduces the functions of each menu option in Sysloader, as described in the following table.

Menu Option	Function
1 Load firmware via TFTP	Upgrade StoneOS via TFTP.
2 Load firmware via FTP	Upgrade StoneOS via FTP.
3 Load firmware from USB disks	Upgrade StoneOS via USB flash drive.
4 Select backup firmware as active	Select the backup version file saved in the system as the current StoneOS startup system.
5 Show on-board firmware	Display the name and status of version files saved in the system.
6 Reset	Restart the system.
7 Clear button	Delete all configurations and restore to factory settings. **Note**: The SG-6000 A/X/K9180 platform does not support this option. The sequence number of this option may vary based on devices.
7 Reset administrator password	Reset the password of the default administrator (hillstone). The reset password is randomly generated and is only effective for the first reboot. Change the password promptly after the first reboot. **Note**: The sequence number of this option may vary based on devices.
8 Load sysloader via TFTP	Upgrade Sysloader via TFTP. **Note**: The SG-6000 A/X/K platform supports this option. SG-6000-

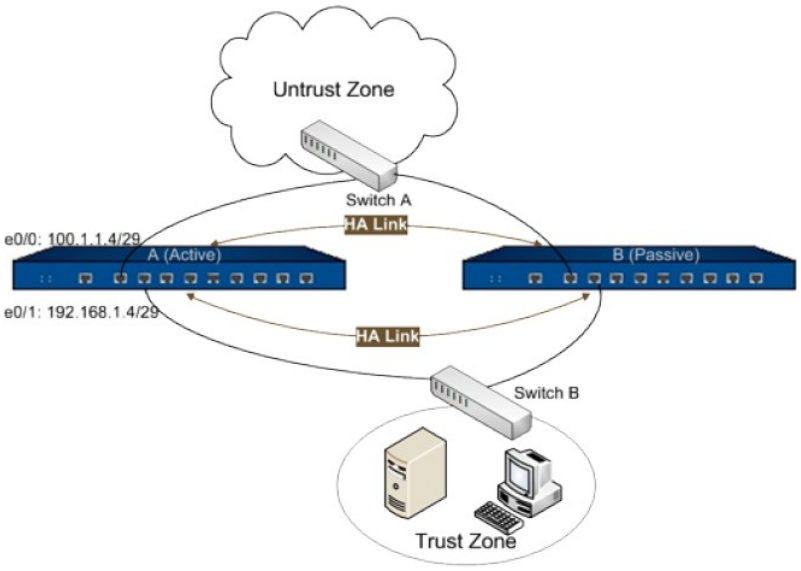
Menu Option	Function
	A200/A200W/A200G4B also supports to upgrade Sysloader via USB. After enter the Bootloader interaction mode, enter "y" after the "load sysloader from USB?" prompt to upgrade Sysloader via USB.
9 Load sysloader via FTP	Upgrade Sysloader via FTP. **Note**: SG-6000-K6580 supports this option.

Follow the menu prompts and enter the corresponding number of the menu option after "sys-loader#", then press Enter.

Upgrading StoneOS in HA Environment

Environment

The following is the topology of HA:



Upgrade Operations

It's strongly recommended that you upgrade to a neighbor version instead of upgrading across several versions. If you upgrade across several versions, please compare the configurations before and after the upgrade carefully. For more information, see Verifying the Configurations. If needed, call 1-800-889-9860.

Upgrading A/X/K Platform From 5.5 Versions to 5.5R11

Before You Start

1. Back up the current configurations of devices A and B to your PC.
2. Check the configurations of the master and backup devices to ensure they are consistent before the upgrade.

3. Make sure that the current business is normal.
4. Import the system files of version 5.5R11 into devices A and B respectively.
5. If the devices have the preempt mode enabled, disable it before the upgrade and re-enable it after the upgrade is completed. If there are track objects of the HA group bound to the devices, unbind them before the upgrade and restore them after the upgrade.

Upgrading Device B

1. Remove the service line of Device B, and then remove its HA heartbeat line to take device B offline.
2. Run the **save** command on device B to save the configuration, and then reboot device B to start the upgrade. After a successful reboot, check if the version and HA-related configurations on device B are correct.
3. Export the configuration of device B and compare it with the pre-upgrade configuration to check there are any exceptions such as configuration loss.
4. Run the **show ha group config** command on both device B and device A to check their priority values. Ensure that the priority value of device A is less than that of device B, which indicates that device A has a higher priority. If device A's priority value is higher than that of device B, adjust device B's priority value to be higher than that of device A.
5. Reconnect device B's HA heartbeat line, wait for the successful negotiation between devices B and A (device A is the master device), and then reconnect device B's service line.

HA Synchronization and Switchover

1. Run the **exec ha sync all** command on the master device A to manually synchronize the configurations of devices A and B.

2. Run the **show arp** and **show session generic** command on both devices A and B to check whether ARP tables and session information have been synchronized.

3. Run the **show logging alarm** command on the master device A and confirm that the message "Admin batch synchronization of HA group 0 has completed." appears, indicating that the configuration synchronization is completed.

4. Run the **exec ha master switch-over** command on the master device A to manually perform switchover. After a successful switchover, device B becomes the master device.

Upgrading Device A

1. Remove the service line of Device A, and then remove its HA heartbeat line to take device A offline. At this point, ensure that the user business on device B is normal.

2. Run the **save** command on device A to save the configuration, and then reboot device A to start the upgrade. After a successful reboot, check if the version and HA-related configurations on device A are correct.

3. Export the configuration of device A and compare it with the pre-upgrade configuration to check there are any exceptions such as configuration loss.

4. Run the **show ha group config** command on both device A and device B to check their priority values. Ensure that the priority value of device A is greater than that of device B, which indicates that device A has a lower priority.

5. Reconnect device A's HA heartbeat line, wait for the successful negotiation between devices A and B (device B is the master device), and then reconnect device A's service line.

HA Synchronization

1. Run the **exec ha sync all** command on device B to manually synchronize the configurations of devices A and B.

2. Run the **show arp** and **show session generic** commands on both devices A and B to check if ARP tables and session information have been synchronized.

3. Run the **show logging alarm** command on device B and confirm that the message "Admin batch synchronization of HA group 0 has completed." appears, indicating that the configuration synchronization is completed.

Completing the Upgrade

1. (Optional) Run the **exec ha master switch-over** command on device B to manually perform switchover, making device A the master device again.

2. The upgrade is completed.

Upgrading StoneOS by Using Hotfix

Hotfix upgrade allows the system to fix issues of the current software version without interrupting ongoing services. You can upload a patch file via an FTP server, TFTP server, FTPS server, or SFTP server, load the patch into the process, and then activate/run the patch to make it take effect.



Notes:

- The patch upgrade can only be performed via CLI.
- By default, the imported patch file is in the UNLOAD state and needs to be loaded into the system before being activated/run.
- The difference between **activate** and **run** in the **exec patch** *patch-name* {**activate** | **run**} command is as follows: **activate** activates the loaded patch to make it take effect, and it will automatically change to **RUNNING** after 48 hours. **run** directly runs the loaded patch, and the patch remains in the running state even after a device reboot. If the device with an **ACTIVE** patch is rebooted, the patch will revert to the UNLOAD state.
- The patch upgrade takes effect without needing to reboot the device.
- Patches are version-specific. After a version upgrade, previously running patches will become invalid.

To upgrade hotfix, take the following steps:

1. Import the patch file from the FTP/TFTP/FTPS/SFTP server to the device. For more information, see Importing a Patch File.
2. Use the **exec patch** *patch-name* **load** command to load the imported patch file into the StoneOS system. For more information, see Loading/Activating/Running/Deleting a Patch.

3. Use the **exec patch** *patch-name* {**activate** | **run**} command to activate or run the patch file to successfully upgrade the patch. For more information, see Loading/Activating/Running/Deleting a Patch.

4. Use the **show patch** command to view the patch status. The **ACTIVE** or **RUNNING** state should be displayed based on the configuration of Step 3. For more information, see Viewing the Patch Status.

To delete hotfix, take the following steps:

1. Use the **exec patch** *patch-name* **unload** command to unload the activated/running patch file.

2. Use the **show patch** command to view the patch status, which is displayed as **UNLOAD**.

3. Use the **exec patch** *patch-name* **delete** command to delete the patch file from the device. Only patches in the **UNLOAD** state can be deleted.

Importing a Patch File

In execution mode, use the following command to import the patch file to the system by using the FTP server:

import patch from ftp server *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name***password** *password*] *filename*

- *ip-address* – Specifies the IP address of the FTP server.
- **user** *user-name* **password** *password* – Specifies the username and password for the FTP server.
- *vrouter-name* - Specifies the Vrouter associated with the device interface used to access the FTP server.
- *filename* – Specifies the name of the patch file to be imported. If the patch file is in the root directory of the FTP server, enter the patch file name directly. If the patch file is in a

subdirectory, enter the "full path + patch file name". For example, if K5680-r0426.patch is in the patch/5.5R11 directory on the FTP server, enter patch/5.5R11/K5680-r0426.patch as the file name.

In execution mode, use the following command to import the patch file to the system by using the TFTP server:

import patch from tftp server *ip-address* [**vrouter** *vrouter*] [*filename*]

- *ip-address* – Specifies the IP address of the TFTP server.
- *vrouter-name* - Specifies the Vrouter associated with the device interface used to access the TFTP server.
- *filename* – Specifies the name of the patch file to be imported. If the patch file is in the root directory of the TFTP server, enter the patch file name directly. If the patch file is in a sub-directory, enter the "full path + patch file name". For example, if K5680-r0426.patch is in the patch/5.5R11 directory on the TFTP server, enter patch/5.5R11/K5680-r0426.patch as the file name.

In execution mode, use the following command to import the patch file to the system by using the FTPS server:

import patch from ftps server *ip-address* [**user** *user-name* **password** *password*] [**vrouter** *vrouter-name*] *file-name*

- *ip-address* – Specifies the IP address of the FTPS server.
- **user** *user-name* **password** *password* – Specifies the username and password for the FTPS server.
- *vrouter-name* - Specifies the Vrouter associated with the device interface used to access the FTPS server.
- *filename* – Specifies the name of the patch file to be imported. If the patch file is in the root directory of the FTPS server, enter the patch file name directly. If the patch file is in a

subdirectory, enter the "full path + patch file name". For example, if K5680-r0426.patch is in the patch/5.5R11 directory on the FTPS server, enter patch/5.5R11/K5680-r0426.patch as the file name.

In execution mode, use the following command to import the patch file to the system by using the SFTP server:

import patch from sftp server *ip-address* [**user** *user-name* **password** *password*] [**vrouter** *vrouter-name*] *file-name*

- *ip-address* – Specifies the IP address of the SFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password for the SFTP server.
- *vrouter-name* - Specifies the Vrouter associated with the device interface used to access the SFTP server.
- *filename* – Specifies the name of the patch file to be imported. If the patch file is in the root directory of the SFTP server, enter the patch file name directly. If the patch file is in a sub-directory, enter the "full path + patch file name". For example, if K5680-r0426.patch is in the patch/5.5R11 directory on the SFTP server, enter patch/5.5R11/K5680-r0426.patch as the file name.

Loading/Activating/Running/Deleting a Patch

To delete, load, activate, or run a patch, in any mode, use the following command:

exec patch *patch-name* {**delete** | **load** | **unload** | **activate** | **deactivate** | **run**}

- *patch-name* – Specifies the name of the patch file on which you want to perform operations.
- **delete** – Deletes the specified patch file. Only patches in the **UNLOAD** state can be deleted.
- **load** – Loads the specified patch file.

- **unload** – Unloads the specified patch file.
- **activate** – Activates the specified patch file to make it take effect. After a device reboot, the patch state will revert to the UNLOAD state.
- **deactivate** – Reverts the specified patch to the deactivated state.
- **run** – Runs the specified patch file. After a device reboot, the patch state remains running.

Viewing the Patch Status

After loading, activating, running, or deleting a patch, you can view the current patch status.

To view the patch status, in any mode, use the following command:

show patch

Verification

To upgrade the version, complete the following processes step by step:

"Preparations" on Page 9 > "Upgrade Notes" on Page 12 > "Upgrade Operations" on Page 23 > **Verification**

After completing the version upgrade, follow these steps to verify the upgrade:

1. Check whether the system version is the target version.
2. Check whether the patch is running/activated successfully. (This step is required only for patch upgrade.)
3. Check whether the device temperature, power supply, and fan are normal.
4. Check whether the CPU utilization and memory utilization of the device are normal.
5. Check whether the status of each expansion module is normal after the upgrade. (This step is required only for distributed devices SG-6000-X series and SG-6000-K9180.)
6. Check whether the status of the master and backup devices is normal in an HA scenario. (This step is required only for upgrade in an HA scenario.)
7. Check whether the configuration takes effect.
8. Check whether basic services can be used normally.

Checking Whether the System Version is the Target Version

You can check whether the system version has been upgraded to the target version via WebUI or CLI.

- WebUI: After you log into the WebUI, go to the **System** > **System and Signature Database** page to view whether the "Boot File" is consistent with the target new version.

- CLI: After you log into the CLI, in any mode, use the **show version** command to verify whether the system has been successfully upgraded to the new version. The software version in the returned information needs to be consistent with the target new version.

Checking Whether the Patch is Running/Activated Successfully



Notes: This section is necessary only when a patch is installed.

After logging into the CLI, use the **show patch** command to view the patch information after the upgrade. If the patch status is **RUNNING** or **ACTIVE**, the patch is installed successfully.

Take the **RUNNING** status of the patch of SG-6000-K5680 as an example:

```
hostname(config)# show patch
patchset: K5680-r0426
- patch: mgd
status: RUNNING
- patch: logd
status: RUNNING
- patch: dnsd
status: RUNNING
```

Checking Whether the Device Temperature, Power Supply, and Fan are Normal

After logging into the CLI, use the **show environment** command to check whether the device's temperature, power supply, and fan are normal.

The returned information may vary based on devices.

Take SG-6000-A5800 as an example:

```
hostname(config)# show environment
```

```
Temperature information(C):
=========================================
Description Temperature Range
-----------------------------------------
CPU 43 0-90
Chassis_Inlet 22 0-90
Chassis_Outlet 24 0-90
TMP464 23 0-90
SW0 34 0-90
SW1 34 0-90
-----------------------------------------
Fan information:
=========================================
Description Status
-----------------------------------------
Fan0 Fine
Fan1 Fine
Fan2 Fine
Fan3 Fine
-----------------------------------------
Power information:
=========================================
Description Status
-----------------------------------------
PS0 Fine
```

```
PS1 Absent
---------------------------------------
```

Checking Whether the CPU Utilization and Memory Utilization of the Device are Normal

- Check CPU: After logging into the CLI, in any mode, use the **show cpu** command to check if the device's CPU utilization is normal after the upgrade.
- Check memory: After logging into the CLI, in any mode, use the **show memory** command to check if the device's memory utilization is normal after the upgrade.

Checking Whether the Status of Each Expansion Module is Normal after the Upgrade



Notes: This section is necessary only when a distributed device is upgraded.

To check the status of expansion modules of SG-6000 X-series devices and SG-6000-K9180, after you log into the CLI, in any mode, use the **show module** command.

Take SG-6000-X25803 as an example:

```
hostname(config)# show module
NO. Name State Module Type Serial Number Work-Mode
--- ------------ ------------ ---------------------- ------------------
--- ----------------
1 slot1/0 Online SIOM-P100-400 6429018232000340 SIOM
slot1/1 Online SIOM-P100-400 6429018232000340 SIOM
slot1/2 Online SIOM-P100-400 6429018232000340 SIOM
2 slot2 Empty
3 slot3 Empty
```

```
4 slot4 Online SCM-D2T-400(M) 6429833222001951
5 slot5 Empty
```

Checking Whether the Status of the Master and Backup Devices is Normal in an HA Scenario

Notes: This section is necessary only when master and backup devices are upgraded in an HA scenario.

After upgrading the software version of the master and backup devices in an HA scenario, you can check if the status of the master and backup devices is normal by using the following commands.

1. After logging into the CLI, in any mode, use the **show ha group** *group-id* command to check the status of the master and backup devices. The master device should display as **Master**, and the backup device should display as **Backup**.
2. In any mode, use the **show ha link ststus** command to check the status of the HA control link **HA link 1**. The **status** should be **UP** and the **quality** should be **10**.

Take SG-6000-K6580 that forms an HA pair as an example:

1. Check the status of the master device:

```
hostname(M)# show ha group 0
HA Group id=0
state Master
priority 100
preempt N/A
monitor
HA total peer number 1
HA peer information:
device id 57199AB6HB410050
ip 6.6.6.7
state Backup
priority 150
hostname(M)#  show ha link ststus
HA link status:
HA link ip=6.6.6.6
HA link 1: HA link if ifid=31 ifname=HA status=UP quality=10
```

2. Check the status of the backup device:

```
hostname(B)# show ha group 0
HA Group id=0
state Backup
priority 150
preempt N/A
monitor
```

```
HA total peer number 1
HA peer information:
device id 57199AB6HB370020
ip 6.6.6.6
state Master
priority 100
hostname(B)# show ha link ststus
HA link status:
HA link ip=6.6.6.7
HA link 1: HA link if ifid=31 ifname=HA status=UP quality=10
```

Checking Whether the Configuration Takes Effect

After the upgrade is completed, export the current configuration file again and compare it with the backup configuration file before the upgrade to check if there is any configuration loss. If there is any loss, confirm if the new version has changed the configuration. If there are changes, reconfigure them in WebUI or CLI.

Checking Whether Basic Services Can be Used Normally.



Notes: Before checking if services are normal, please check if the configuration is restored.

Check if the service traffic and service operation of the current network are normal.

Upgrade Troubleshooting

This chapter describes the possible issues and processing steps during the version upgrade.

If the issue persists, perform "Software Version Rollback" on Page 67, or contact 1-800-889-9860.

Device Login Failure

Failure Description

You cannot log in to the device via the management port or Console port.

Possible Causes

- The baud rate is configured incorrectly in the terminal emulation program.
- The physical port connection is abnormal, such as the indicator not being on or being flickering.
- The Telnet/SSH/HTTP/HTTPS service is not enabled on the device interface (for management port login issues only).
- The login service permissions for the administrator are not enabled (for management port login issues only).
- The IP address of your PC is not within the range of trusted hosts (for management port login issues only).
- The login service for the trusted host corresponding to the IP address of the login PC is not enabled (for management port login issues only).

Processing Steps

1. Use the **show console** command to view the baud rate of the Console port of the device. Check whether the baud rate and data bits are set correctly in the terminal emulation program. If incorrect, set the parameters correctly. For more information, refer to *Hardware Reference Guide*.

2. Check whether the physical connection between the device's Ethernet interface or Console port and the peer device is normal. If the physical connection is abnormal, replace it with the correct physical connection.

3. Log in to the device via the Console port and use the **show interface** *interface-name* command to check whether the Telnet/SSH/HTTP/HTTPS service is enabled. If not, use the **manage** { **ssh** | **telnet** | **http** | **https** } command in the interface configuration mode to enable the corresponding service. For more information, refer to *StoneOS CLI User Guide*.

4. Log in to the device via the Console port and use the **show admin user** *user-name* command to check whether the administrator's login service permissions (access) are enabled. If not, use the **access** { **console** | **http** | **https** | **ssh** | **telnet**} command in the administrator configuration mode to enable the corresponding login service permission. For more information, refer to *StoneOS CLI User Guide*.

5. Log in to the device via the Console port and use the **show admin host** command to check the address configuration of the trusted host. The trusted host needs to include the IP address of your PC.

6. Log in to the device via the Console port and use the **show admin host** command to check the login type for the trusted host. If the corresponding service is not enabled, enable it.

7. If the issue persists, perform software version rollback, or collect the following information and contact technical support.

- The results of the above steps.
- The device configuration file, and operation log information in the terminal tool.

Version File Import Failure

Failure Description

- Transmission is abnormally interrupted during the process of importing the version file.
- The device displays an version file import failure.

Possible Causes

- The remaining space of storage medium of the device is insufficient.
- The transmission link between the device and PC fails or the network is unstable.
- The platform license expires.
- The software version is not compatible with the device model.
- An error occurred on the FTP Server or TFTP Server software.

Processing Steps

1. If the remaining space of storage medium of the device is insufficient, delete redundant version files in the storage medium.
2. Use methods such as ping to check the transmission link or network between the device and the PC. If issues exist, replace the transmission link medium.
3. Check whether the platform license is expired. If it is, renew the license before the upgrade.
4. Use *ReleaseNotes for StoneOS 5.5R11* to check the compatibility between the system software version and the device model. If not compatible, download the correct version file.

5. Check whether the FTP/TFTP/FTPS/SFTP server is running normally and whether the relevant configuration is correct, such as the version file name and the path where the version file is stored on the file server. If issues exist, correctly set up the FTP/TFTP/FTPS/SFTP server or replace it with other server software.
6. If the issue persists, perform software version rollback, or collect the following information and contact technical support.
    - The results of the above steps.
    - The device configuration file, and operation log information in the terminal tool.

Device Reboot Failure after Upgrade

Failure Description

- The version file used for the upgrade cannot start the device.
- After reboot, you cannot log in to the device.

Possible Causes

- The power supply or fan tray fails.
- The version file used for the upgrade is damaged.
- The version span between the pre-upgrade and post-upgrade versions is too large.

Processing Steps

1. Check whether the power supply is normal. To do this, check whether the device's PWR indicator is solid green. If there are power issues, replace the power module. For more information, refer to *Hardware Reference Guide*.

2. Check whether the fan tray is normal. To do this, check whether the device's FAN indicator is solid green, and ensure that there are no obstructions in the device's air inlet/outlet. If there are issues, replace the fan tray or clean the air inlet/outlet. For more information, refer to *Hardware Reference Guide*.

3. The version span between the pre-upgrade and post-upgrade versions should not be too large. For more information, see "Upgrade Notes for Each Series of Platforms" on Page 13.

4. If the issue persists, perform software version rollback, or collect the following information and contact technical support.

   - The results of the above steps.
   - The device configuration file, and operation log information in the terminal tool.

Software Version Rollback

Application scenarios for version rollback:

- Due to your business requirements, the current version needs to be rolled back to an older version.
- After a system upgrade, the device cannot operate normally, requiring the current version to be rolled back to an older version. (This scenario can be addressed only by rolling back via Sysloader)

This chapter describes the process of rolling back the system version of StoneOS.

- Version rollback procedure
- Version rollback operations
- Verify whether the rollback is successful

Version Rollback Procedure

For more information about the version rollback procedure, see "Procedure" on Page 7.

Version Rollback Operations

- To roll back to the backup version, refer to the following topics:
  - "Rolling Back Your Version via WebUI" on Page 69
  - "Rolling Back Your Version via CLI" on Page 70
  - "Rolling Back Your Version in Sysloader" on Page 71
- To roll back to a specified version, the steps are similar with version upgrade operations, so you can refer to the following topics:

- "Upgrading StoneOS via WebUI" on Page 24
- "Upgrading StoneOS via CLI" on Page 27
- "Upgrade Procedure" on Page 33

Verifying Whether the Rollback is Successful

The steps of verifying whether the rollback is successful are similar with the steps of verifying whether the upgrade is successful. For more information, refer to "Verification" on Page 55.

Rolling Back Your Version via WebUI

Rolling Back to the Backup Version

Based on your needs, you can specify the device's next startup version to roll back to the backup version taken during the upgrade. To do this, take the following steps:

1. Log in to the WebUI of the device.
2. Select **System** > **Upgrade Management** > **Upgrade Firmware**.
3. On the **Upgrade Firmware** page, click the **Choose a Firmware for the next startup** tab.
4. Select the next startup version from the drop-down list, that is, the backed up version.
5. Select **Reboot now to make the new firmware take effect** and click **Apply** to immediately reboot the system and enter the specified version, or simply click **Apply** to save the configuration. The selected version will take effect at the next reboot.

Rolling Back to Other Versions

To roll back to a specified version, the steps are similar with version upgrade operations. For more information, refer to "Upgrading StoneOS via WebUI" on Page 24.

Rolling Back Your Version via CLI

Rolling Back to the Backup Version

To roll back to the backup version taken during the upgrade via CLI, take the following steps:

1. After you log into the CLI, in execution mode, use the following command to change the backup version file to the next startup version:
   exec image *image-name* **active**
   - *image-name* - Specifies the current backup version file as the next startup version.
2. In any mode, use the **show image** command to check if the status of the backup version file has changed to **active**.
3. In execution mode, enter the **reboot** command to reboot the system to make the new software version takes effect.

Rolling Back to Other Versions

To roll back to a specified version, the steps are similar with version upgrade operations. For more information, refer to "Upgrading StoneOS via CLI" on Page 27.

Rolling Back Your Version in Sysloader

Rolling Back to the Backup Version

To roll back to the backup version in Sysloader, take the following steps:

1. Connect the device's CON port to the PC's serial port by using an RS-232 cable, and reboot the device. During the reboot process, enter Sysloader. If you cannot select Sysloader by using the arrow keys, first press "Ctrl+W" and then enter Sysloader (e.g., for SG-6000-K6580, press "Ctrl+W" and then enter Sysloader). Note that the returned information may vary by device.

   For more information about prompt examples of operations in Sysloader for different devices, see Upgrade Procedure.

2. After you enter Sysloader, select option "4" from the Sysloader operation selection menu and press Enter. Refer to the following operation prompts (using SG-6000-A2000 as an example):

   Note: The startup option of Sysloader may vary based on platforms. For more information, see Introduction to the Sysloader Menu.

```
Sysloader 1.0.5 Sep 23 2020 - 16:09:24
sysloader#
1 Load firmware via TFTP
2 Load firmware via FTP
3 Load firmware from USB disks (available)
4 Select backup firmware as active
5 Show on-board firmware
6 Reset
7 Reset Administrator password
```

```
8 Load sysloader via TFTP
sysloader# 4( Enter "4" here and press Enter)
```

3. The system will prompt you to confirm if you want to select the backup version file stored in the system as the current StoneOS version file. Type "y" and press Enter.

4. Based on the Sysloader operation selection menu, select option "6" and press Enter. The system will start using the backup version file to reboot.

Rolling Back to Other Versions

To roll back to a specified version, the steps are similar with version upgrade operations. For more information, refer to "Upgrade Procedure" on Page 33.