



SANGFOR

NGAF

Release Note

Version 8.0.26

Change Log

Date	Change Description
10/9/2020	Version 8.0.26 Release Note.

Contents

Chapter 1 What is New?	1
Chapter 2 Upgrade Instructions for Customer Service or Distributors	2
Confirmation Before Upgrade	2
Upgrade Limitations	3
Immediate Upgrade of Configurations, Logs and Data	4
Impacts on Functions After Upgrade	4
Reboot Required After Upgrade	4
Time Taken	4
Upgrade Recommendations	5
Chapter 3 Upgrade Procedure	5
Handling of Upgrade Failure	5
Upgrade Instructions for Beta Customers (Upgrade to official version before the official release)	6
Upgrade Instructions for Customers	6
Chapter 4 Others	6
Chapter 5 Notes	7

Chapter 1 What is New?

[New] Endpoint Secure on NGAF

1. It adds Endpoint Secure on NGAF for endpoint protection, and supports accessing Endpoint Secure manager and managing endpoints from NGAF manager.

[New] Licensing

1. It updates licensing methods, and licensing is managed by Sangfor licensing server.

[Enhanced] File Restoring Capability Enhancement

1. It supports uploading file via HTTP/HTTPS, FTP and SMBv3.
2. It enhances engines to reduce file antivirus bypass.

[Enhanced] File Type Identification Capability Enhancement

1. It adopts new identification methods to support identifying frequently attacked file types.

[Enhanced] File Antivirus Stability Enhancement

1. It enhances stability of email proxy.

[Enhanced] Web Application Protection Enhancement

1. It adds XML parsing function to enhance XML block.
2. It supports HTTP charset decoding to solve most problems of charset encoding bypass NGAF detection.
3. It adds XXE attack prevention to enhance XXE attack block.

Chapter 2 Upgrade Instructions for Customer Service or Distributors

Confirmation Before Upgrade

For Chinese version of NGAF, it supports upgrade from the following earlier versions by loading the upgrade package AF8.0.26(20201107).ssu:

NGAF7.1 official version, NGAF7.2 official version, NGAF7.3 official version, NGAF7.3.0R1 official version, NGAF7.4 official version, NGAF7.5.0 official version, NGAF7.5.1 official version, NGAF8.0.2 official version, NGAF8.0.5 official version, NGAF8.0.6 official version, NGAF8.0.6 R1 beta version, NGAF8.0.7 official version, NGAF8.0.7R2 official version, NGAF8.0.8 official version, NGAF8.0.9 official version, NGAF8.0.10 official version, NGAF8.0.13 official version, NGAF8.0.16 beta version, NGAF8.0.17 official version, NGAF8.0.18 beta version, NGAF8.0.19 official version, NGAF8.0.23 official version and NGAF8.0.26 beta version(268 or 328).

For English version of NGAF, it supports upgrade from the following earlier versions by loading the upgrade package AF8.0.26.335(20201107).ssu:

NGAF7.1 official version, NGAF7.1 R1 official version, NGAF7.2 official version, NGAF7.3 official version, NGAF7.3.0 R1 official version, NGAF7.4 official version, NGAF7.5.1 official version, NGAF8.0.2 official version, NGAF8.0.5 official version, NGAF8.0.6 official version, NGAF8.0.7 official version, NGAF8.0.7 R2 official version, NGAF8.0.8 official version, NGAF8.0.9 official version, NGAF8.0.10 official version, NGAF8.0.13 official version, NGAF8.0.16 beta version, NGAF8.0.17 official version, NGAF8.0.18 beta version, NGAF8.0.19 official version, NGAF8.0.23 official version and NGAF8.0.26 beta version(268 or 328).

For Chinese version of vNGAF in HCI, it supports upgrade from vNGAF7.1 R3 official version, vNGAF8.0.8 official version, vNGAF8.0.9 official version, vNGAF8.0.13 official version, vNGAF8.0.17 official version, vNGAF8.0.18 beta version, vNGAF8.0.19 official version, vNGAF8.0.23 official version and vNGAF8.0.26 beta version to vNGAF8.0.26 version by loading the upgrade package AF8.0.26(20201107).ssu.

For English version of vNGAF in HCI, it supports upgrade from vNGAF7.1 R3 official version, vNGAF8.0.8 official version, vNGAF8.0.9 official version, vNGAF8.0.13 official version, vNGAF8.0.17 official version, vNGAF8.0.18 beta version, vNGAF8.0.19 official version, vNGAF8.0.23 official version and vNGAF8.0.26 beta version to vNGAF8.0.26 version by loading the upgrade package AF8.0.26(20201107).ssu.

For Chinese version of vNGAF in aBOS, it supports upgrade from vNGAF7.5.3 official version, vNGAF8.0.8 official version, vNGAF8.0.9 official version, vNGAF8.0.13 official version and vNGAF8.0.17 official version, vNGAF8.0.18 beta version, vNGAF8.0.19 official version, vNGAF8.0.23

official version and vNGAF8.0.26 beta version to vNGAF8.0.26 version by loading the upgrade package AF8.0.26(20201107).ssu.

For English version of vNGAF in aBOS, it supports upgrade from vNGAF8.0.8 official version, vNGAF8.0.9 official version, vNGAF8.0.13 official version, vNGAF8.0.17 official version, vNGAF8.0.18 beta version, vNGAF8.0.19 official version, vNGAF8.0.23 official version and vNGAF8.0.26 beta version to vNGAF8.0.26 version by loading the upgrade package AF8.0.26(20201107).ssu.

Upgrade Limitations

1. Not support upgrade from custom version.
2. Not support upgrade from version installed KB package.
3. If "Always detect data packets that traverse repeatedly" is enabled, immediate upgrade is not supported. You need to disable it manually first and upgrade. After upgrading, you may go to System > General > System > Second-passthrough Traffic to enable it.
4. For upgrade from earlier version, high availability and configuration sync should be disabled first.
5. Earlier NGAF device cannot be upgraded to version 8.0.26 and its configurations cannot be imported to the device (version 8.0.26) if it has any of the following configurations:
 - 1) **Mobile user or virtual IP pool is configured.**
Solution: Delete mobile user(s) or virtual IP pool(s).
 - 2) **Dynamic routing is configured for VPN.**
Solution: Disable routing information protocol (RIP) in Network > IPsec VPN > Advanced > Dynamic Routing.
 - 3) **Default user is configured with local password-based authentication method enabled.**
Solution: Disable the default user in Network > IPsec VPN > Local Users.
 - 4) **Multicast or broadcast is enabled for VPN.**
Solution: Disable multicast and broadcast in Network > IPsec VPN > Basics > Advanced.
 - 5) **MTU in Basic settings under Sangfor VPN is not within the range 576-1500.**
Solution: Change MTU in Network > IPsec VPN > Basics.
 - 6) **IPsec VPN is used in earlier versions but its lines have not been added in multiple lines.**
Solution: Enable multiline (gateway) and add a line for IPsec VPN connection in Network > IPsec VPN > Multiline Options.
 - 7) **IPsec VPN is used in earlier versions and there are lines, but multiline is not enabled.**
Solution: Enable multiline (gateway) in Network > IPsec VPN > Multiline Options.
 - 8) **Indirect Internet connection is chosen for IPsec VPN basic settings.**
Solution: Choose direct Internet connection for IPsec VPN basic settings
 - 9) **Indirect Internet connection is chosen for IPsec VPN multiline options.**
Solution: Choose direct Internet connection for IPsec VPN multiline options in Network > IPsec VPN > Multiline Options.
 - 10) **For earlier versions, IPsec VPN outgoing line option is not selected for WAN interface of Sangfor VPN (in single line scenario)**
Solution: Follow instructions to fix it.

- 11) When the product number between local IP address and peer IP address is over 64 in third-party connection of IPsec VPN, please merge or delete the addresses of local or peer device. You may add them back after upgrade.
Solution: Follow the tips on the manager.
 - 12) Phase I or Phase II are disabled or unassociated settings when connecting to third-party device in lower NGAF versions.
Solution: Delete or enable the settings and make them corresponding to Phase I or Phase II separately and then upgrade the device.
 - 13) Not support upgrading devices to this version for earlier versions with memory size smaller than 4 GB (not inclusive of 4GB) and SSL VPN is licensed.
Solution: Remove the SSL VPN license and then upgrade the device to this version.
 - 14) Not support upgrading devices to this version for vNGAF (vAF-100) with 1 core and 2 GB memory.
Solution: Shut down the vNGAF device and edit its settings to 2 cores and 4 GB memory or higher settings. Restart the device and then upgrade to this version.
6. Not support upgrade for devices with External Report Center enabled. If you have any problems, please contact Sangfor Customer Service.
 7. Upgrade is not allowed if database service encountered error. In this case, please check the status of database service.

Immediate Upgrade of Configurations, Logs and Data

Yes

Impacts on Functions After Upgrade

1. The port detection of Web application protection and intrusion prevention is enabled by default after upgrade.
2. PHP code injection prevention, Java code injection prevention, command injection prevention and WebShell upload prevention are added in all templates of Web application prevention after upgrade.

Reboot Required After Upgrade

Yes. Device will restart automatically upon upgrade completion.

Time Taken

Upgrade process may take about 10 minutes under normal circumstance (at least 40% of the total CPU and memory are available, and network is connected).

Upgrade Recommendations

1. Back up configurations before upgrade.
2. Before upgrade, make sure network connection is OK.
3. After upgrade completes, make sure network is not impacted and NGAF manager can be accessed.
4. If you encounter any problem, contact Customer Service to turn to developer for help.

Chapter 3 Upgrade Procedure

● To upgrade standalone device, do the following:

1. Check whether the current version is a custom version, since upgrade from custom version is not supported. Check whether that version has been installed KB package. If KB package has been installed, contact developer to confirm whether the issues brought about by the KB package can be fixed. Check whether that version is an official version. If it is a Beta version (Labeled B), upgrade it to its corresponding official version first. Make sure free space is sufficient.
2. Get update package and the corresponding MD5 file, and make sure that the MD5 is correct.
3. Back up configurations and import configuration files.
4. Check the version first. For upgrade from NGAF7.1 or later versions, launch Sangfor Firmware Updater and load the update package AF8.0.26.335(20201107).ssu.
5. After upgrade completion, check network connection and whether NGAF manager can be accessed properly.

● To upgrade device in high availability environment, do the following:

1. Disable high availability and configuration sync, and then follow the upgrade steps (step 1-5 illustrated for standalone device).
2. After active and standby devices are upgraded, enable HA.

Handling of Upgrade Failure

Scenario 1: Memory is insufficient.

Solution: If memory is insufficient but customer insists on upgrading, contact Customer Service to turn to developer for help.

Scenario 2: Error parsing update package.

Solution: Get update package and MD5 hash file and make sure the MD5 is correct.

Scenario 3: appre execution failed message occurs, prompting that upgrade from the current version is not supported.

Solution: Check whether the current version is a custom version, since upgrade from custom version is not supported. If it is a Beta version (Labeled B), upgrade it to its corresponding official version first.

Scenario 4: appsh execution failed message occurs, prompting that upgrade is not supported in high availability environment.

Solution: Disable HA and configuration sync before upgrade and then perform upgrade again.

Scenario 5: System upgrade is successful but enhancement package update failed. In order to enhance system security, please update the package again or contact Sangfor technical support representative.

Solution: Contact Customer Service to turn to developers for help.

Scenario 6: Other error occurs.

Solution: Contact Customer Service to turn to developers for help.

Upgrade Instructions for Beta Customers (Upgrade to official version before the official release)

None

Upgrade Instructions for Customers

Update Procedure

1. Contact customer service or distributors to upgrade device.
2. Obtain offline update package and launch Sangfor Firmware Updater 6.0 to load the update package

Upgrade Procedure for Customers

Refer to Upgrade Instructions for Customer Service or Distributors section.

Chapter 4 Others

1. Support upgrade with Sangfor Firmware Updater 6.0 only.
2. Internal Database
 - a) Databases can be updated online. Please log in to NGAF manager and go to System > Security Capability Update to update databases.
 - b) Obtain update package from database servers for offline update.
3. Central management (CM) is not supported, but Sangfor BBC is supported.
4. Support pass-through. Enabling pass-through does not require a restart of device.
5. HA module update: Disable HA and configuration sync before upgrading earlier version to this version.
6. Downgrade is not supported.

Chapter 5 Notes

1. For versions earlier than NGAF8.0.7 (exclusive of NGAF8.0.7), when IPsec VPN connection is established but multiline options are not specified:

IPsec VPN will be disconnected but upgrade will succeed if your device is upgraded to NGAF8.0.7 first and then to NGAF8.0.26 (solution: enable multiline and add a IPsec VPN line to multiple line).

2. For earlier versions, IPsec VPN outgoing line is not selected for all WAN interfaces for Sangfor VPN (in multiple line scenario):

VPN will be disconnected for those IPsec VPN outgoing line is not selected after upgrade to NGAF8.0.26.

3. LAN service schedule in IPsec VPN is removed in this version.

If LAN service schedule is configured in earlier versions, the schedule will be all day after upgrade to NGAF8.0.26 and previous disconnected period will be connected for all day.

4. The default value of security proposal in phase II are modified from ESP+MD5+3DES to ESP+AES+SHA1.

When connecting to lower version NGAF with default configurations, disconnection may occur due to inconsistency.

5. For earlier NGAF versions, there is no ID type in main mode. ID type can be left empty when IPv4 is selected for IP type, and in this case, IPsec VPN connection can be established between NGAF of lower version and this version.

6. If NGAF is correlated to Cyber Command, Cyber Command should also be upgraded to 3.0.37 after NGAF is upgraded to 8.0.26 version.

7. It takes about one and half hours to firstly convert logs during the last 7 days after upgrade to 8.0.26 under normal circumstance (at least 40% of the total CPU and memory are available, and network is connected).

8. Not support upgrade for devices with External Report Center enabled.

9. When upgrading via NGAF manager, the available space of fwlog must be over 3 GB. If its space is or lower than 3 GB, upgrade is not allowed.

10. Unable to upgrade to this version if fwlib space is less than 400 MB.

11. For NGAF devices with 2 GB memory size and activated and valid SSL VPN and Engine Zero Model Update licenses, unable to upgrade to this version. And the following error message shows: Unable to upgrade to the new version due to device memory size. To upgrade, please contact Sangfor Customer Service.

12. To upgrade to this version, enable SSH port first because SSH port is for connecting Sangfor Firmware Updater to NGAF devices. SSH port is disabled by default. Once it is enabled, it will be disabled automatically in eight hours. Every time NGAF device restarts, SSH port will be disabled.

13. SSL VPN on NGAF8.0.26 is not supported by Windows XP. Windows XP users cannot use SSL VPN after upgrade to NGAF8.0.26.

14. NGAF8.0.26 supports offline licensing only.



Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

The information in this document is subject to change without notice.

To obtain the latest version, contact the international service center of SANGFOR Technologies Inc