



# NGAF

## NGAF 8.0.17 Version Release Notes

**Version 8.0.17**



## Change Log

Date	Change Description
Dec 2, 2019	NGAF 8.0.17 version release notes.

# CONTENT

Chapter 1 What is New? .....	1
Chapter 2 Resolved Issues .....	1
Chapter 3 Upgrade Instruction.....	1
3.1 Confirmation Before Upgrade .....	1
3.2 Upgrade Limitations.....	2
3.3 Upgrade Recommendations.....	3
3.4 Upgrade Procedure .....	3
3.5 Handling of Upgrade Failure.....	4
Chapter 4 Precautions .....	4

## Chapter 1 What is New?

### [New] Cloud-Based URL Database Detection

- (1) Support dual-engine URL detection, using local database and correlating Neural-X to search the latest unknown URL categories globally in real time.
- (2) Enhance URL category description to offer more accurate classification.

### [New] Ransomware Protection

- (1) Add ransomware protection module to protect your network against ransomware attacks.
- (2) Support scanning for weaknesses in business systems to assess entry point and ransomware attack risk.
- (3) Add Ransomware Protection module in Status > Dashboard to identify and fix risks of ransomware attack.

### [Enhanced] Application Signature Detection Engine

- (1) Expand application signature database from 3500+ to 9500+ rules, offering more comprehensive and accurate application control.
- (2) Support more applications frequently used abroad, such as Google, Facebook, and Office 365.

### [Enhanced] Troubleshooting

- (1) Simpler: Offer three troubleshooting methods (precise traffic analysis, global passthrough and analysis, and L2 packet passthrough), which can be used as required.
- (2) More accurate: Precisely locate faults and misjudgment caused by policies.
- (3) Visualized: Display packet paths in diagrams to make you understand causes easily.

### [Enhanced] Ransomware Intrusion Protection

- (1) Fix 13 high-risk SMB vulnerabilities.
- (2) Enhance detection of SMB medium/low brute-force attacks or SMB distributed brute-force attacks.
- (3) Enhance detection of RDP medium/low brute-force attacks.

## Chapter 2 Resolved Issues

### [Fixed] System

System Health Check results are not displayed properly.

### [Fixed] Configuration Backup

NGAF device failed to download backup configuration, browser prompts failed to download file.

### [Fixed] Business System Security

Public network IP logs appear in business system security under certain circumstances.

### [Fixed] SSL VPN

PC client unable to obtain virtual IP after SSL VPN is disconnected abnormally.

## Chapter 3 Upgrade Instruction

### 3.1 Confirmation Before Upgrade

For Chinese version of NGAF, it supports upgrade from the following earlier versions by loading the upgrade package AF8.0.17(20191125).ssu:

NGAF6.5 official version, NGAF6.6 official version, NGAF6.7 official version, NGAF6.8 official version, NGAF7.0 official version, 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, NGAF8.0.7 R2 official version, NGAF8.0.7 R5 beta version, NGAF8.0.8 official version, NGAF8.0.9 official version, NGAF8.0.9 R2 beta version, NGAF8.0.10 official version, NGAF8.0.12 beta version, AF8.0.13 official version, AF8.0.14 beta version (its appversion is AF8.0.14.3350 B Build20191018) and AF8.0.17 beta version.

For English version of NGAF, it supports upgrade from the following earlier versions by loading the upgrade package AF8.0.17(20191125).ssu:

NGAF7.0 official version, 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, NGAF8.0.9 R2 beta version, NGAF8.0.10 official version, NGAF8.0.13 official version, NGAF8.0.14 beta version (its appversion is AF8.0.14.3350 EN B Build20191018) and NGAF8.0.17 beta version.

For Chinese version of vNGAF in aCloud, it supports upgrade from vNGAF6.9 R4 official version, vNGAF7.1 R3 official version, vNGAF8.0.8 official version, vNGAF8.0.9 official version, vNGAF8.0.13 official version, vNGAF8.0.14 beta version (its appversion is AF8.0.14.3350 B Build20191018) and vNGAF8.0.17 beta version to vNGAF8.0.17 version by loading the upgrade package AF8.0.17(20191125).ssu.

For English version of vNGAF in HCI, it supports upgrade from vNGAF7.1 R3 and vNGAF 8.0.8 official version, vNGAF8.0.9 official version, vNGAF8.0.13 official version, vNGAF8.0.14 beta version (its appversion is AF8.0.14.3350 EN B Build20191018) and vNGAF8.0.17 beta version to vNGAF8.0.17 version by loading the upgrade package AF8.0.17(20191125).ssu (If vNGAF is 1 CPU core 2G memory, upgrade is not supported. )

For Chinese version of vNGAF in aBOS, it supports upgrade from vNGAF6.9R4 official version, vNGAF7.5.3 official version, vNGAF8.0.8 official version, vNGAF8.0.9 official version, vNGAF8.0.13 official version, vNGAF8.0.14 beta version (its appversion is AF8.0.14.3350 B Build20191018) and vNGAF8.0.17 beta version to vNGAF8.0.17 version by loading the upgrade package AF8.0.17(20191125).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, vNGAF 8.0.14 beta version (its appversion is AF8.0.14.3350 EN B Build20191018) and vNGAF8.0.17 beta version to vNGAF 8.0.17 version by loading the upgrade package AF8.0.17(20191125).ssu.

## 3.2 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 8.0.17 and its configurations cannot be imported to the device (version 8.0.17) 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.

## 3.3 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.

## 3.4 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 NGAF6.5, NGAF6.6 or NGAF6.7 version, launch Sangfor Firmware Updater and load the update package AF\_Pre(for 8.0.17).ssu. Reboot is not required after upgrade. Then load the update package AF8.0.17(20191125).ssu with Sangfor Firmware Updater. For upgrade from other versions, launch Sangfor Firmware Updater and load the update package AF8.0.17(20191125).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.

## 3.5 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:** apppre 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.

**Scenario5:** Sangfor Firmware Updater prompts: Update package should be downloaded first from [https://download.sangfor.com/Download/Product/NGAF/NGAF8.0.17/AF\\_Pre\(for 8.0.17\).ssu](https://download.sangfor.com/Download/Product/NGAF/NGAF8.0.17/AF_Pre(for 8.0.17).ssu)

Solution: Launch Sangfor Firmware Updater and load the update package AF\_Pre(for 8.0.17).ssu first. Reboot is not required after upgrade.

**Scenario 6:** Other error occurs.

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

## Chapter 4 Precautions

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.
7. Cloud correlation and Endpoint Secure integration do not support two active units to perform virus scan simultaneously.





**SANGFOR**

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