



SANGFOR

Sangfor Cyber Command

Release Notes

Product Version	3.0.64
Document Version	01
Released on	Sept. 5, 2022



Copyright © Sangfor Technologies Inc. 2022. All rights reserved.

Unless otherwise stated or authorized, Sangfor Technologies Inc. (hereinafter referred to as "Sangfor") and its affiliates reserve all intellectual property rights, including but not limited to copyrights, trademarks, patents, and trade secrets, and related rights to text, images, pictures, photographs, audio, videos, charts, colors, and layouts as presented in or concerning this document and content therein. Without prior written consent of Sangfor, this document and content therein must not be reproduced, forwarded, adapted, modified or displayed or distributed by any other means for any purpose.

Disclaimer

Products, services or features described in this document, whether wholly or in part, may be not within your purchase scope or usage scope. The products, services or features you purchase must be subject to the commercial contract and terms as agreed by you and Sangfor. Unless otherwise provided in the contract, Sangfor disclaims warranties of any kind, either express or implied, for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is used for reference only, and all statements, information, and recommendations therein do not constitute any express or implied warranties.

Technical Support

For technical support, please visit: <https://www.sangfor.com/en/about-us/contact-us/technical-support>

Send information about errors or any product related problem to tech.support@sangfor.com.

About This Document






This document describes the Release Notes of Sangfor Cyber Command(CCOM) version 3.0.6.4.

Intended Audience

This document is intended for:

- Network design engineers
- O&M personnel

Note Icons

English Icon	Description
	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
	Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
	Indicates a hazardous situation, which if not avoided, could result in settings failing to take effect, equipment damage, or data loss. NOTICE addresses practices not related to personal injury.
	Calls attention to important information, best practices, and tips. NOTE addresses information not related to personal injury or equipment damage.

Change Log

Date	Change Description
Sep. 9, 2022	This is the first release of this document.
Sep. 21, 2022	Change details in part 4.3.

Contents

Technical Support	1
Change Log	2
1 New Features	4
2 Enhancements	4
3 Resolved Issues	4
4 Upgrade Instruction	4
4.1 Pre-Upgrade Check	4
4.2 Upgrade Limitations	4
4.3 Upgrade Procedure	5
4.4 Handling of Upgrade Failure	8
5 Precautions	8

1 New Features

ATT&CK capability:

1. Custom Intelligence.
2. Cluster expansion.
3. More countries or regions are available for customer locations.
4. Licensing management of third-party integrated devices.
5. Integration with HCI.
6. Threshold settings for the abnormal behavior engine.
7. Audio alert.
8. AKSK added to the connection method between STA and Cyber Command.
9. Access control for source IP addresses.

2 Enhancements

1. Whitelist.
2. Alerts are displayed by details or correlation.
3. Alert or Incident proof optimized.

3 Resolved Issues

1. Some previous versions' known issues were fixed.

4 Upgrade Instruction

4.1 Pre-Upgrade Check

CCOM3.0.64 support upgrade from the following earlier versions:

Cyber Command 3.0.60.

4.2 Upgrade Limitations

Hardware:

1. Memory: None.

2. Disk: None.
3. Disk size: Directory /stmp/ is not smaller than 200 MB.
4. CPU: None.

Software:

Dependent on specific packages:

No. Immediate Upgrade of Configurations, Logs, and Data.

Yes. Impacts on Functions After Upgrade:

1. SSH process function is disabled by default. However, it can be enabled manually and will be disabled automatically 8 hours later.
2. Firmware Updater is disabled by default. However, if an upgrade is required, it can be enabled together with SSH and will be disabled automatically 8 hours later.

Reboot Required After Upgrade:

Yes.

Time Taken:

30 minutes.

4.3 Upgrade Procedure

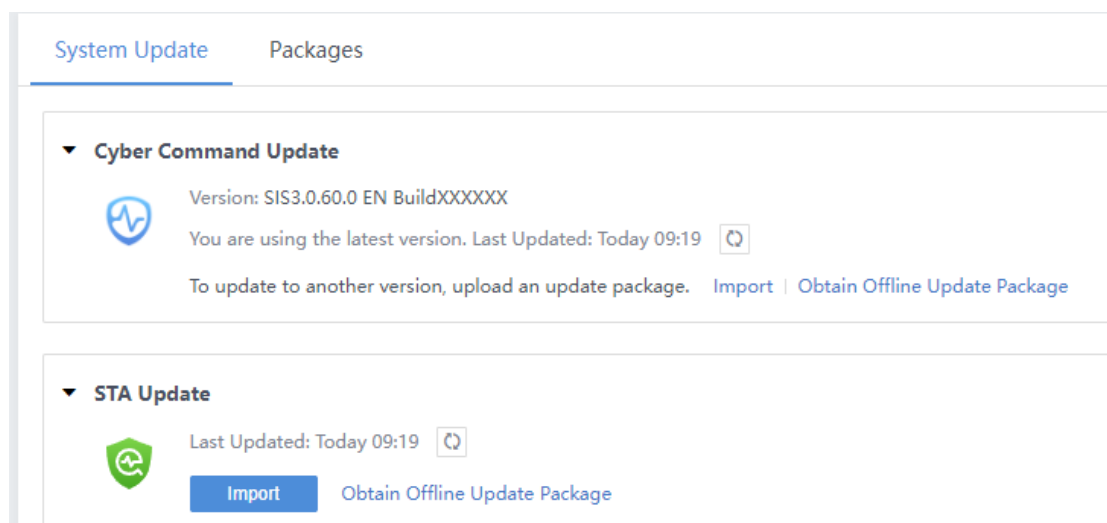
Follow the steps below If you are upgrading from Cyber Command Version 3.0.64.

Before Upgrade:

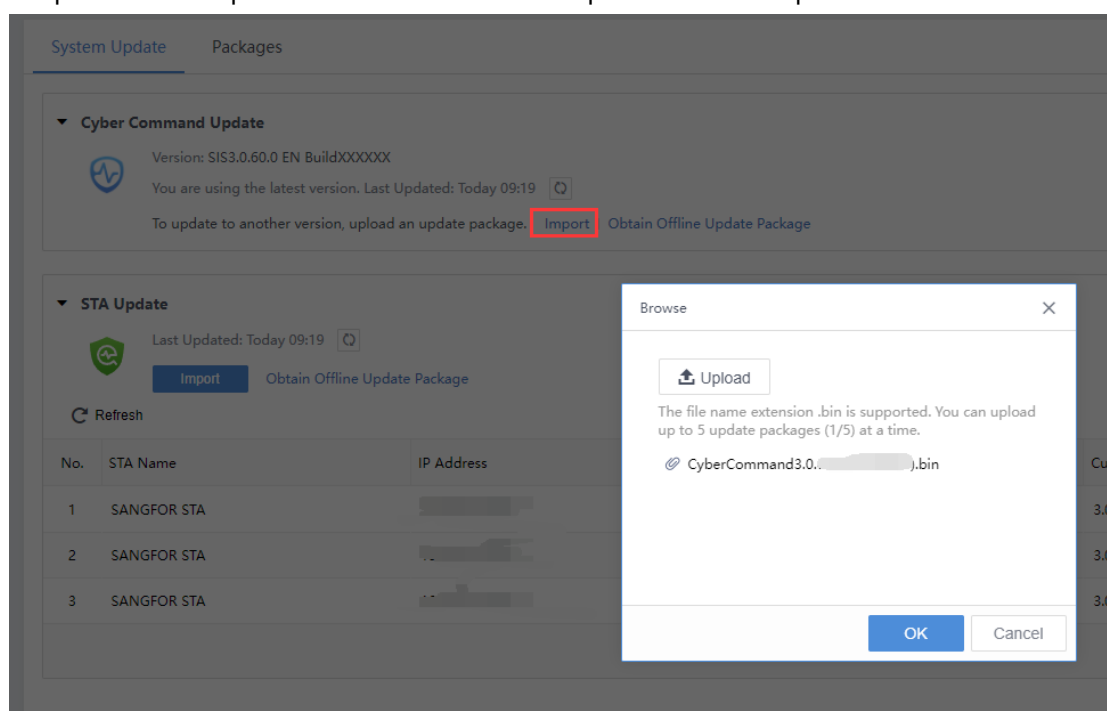
Step 1. Check the MD5 values of all update packages to ensure they are the same as those in the attachments.

Step 1. Check whether the device has been upgraded to version 3.0.64.

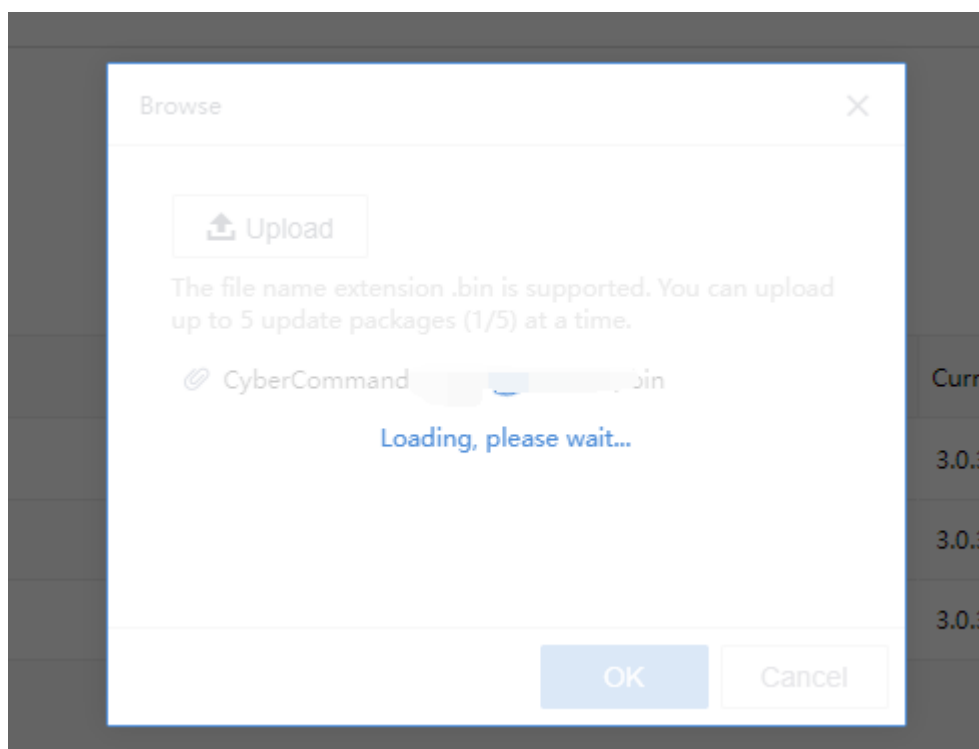
Step 2. Go to System > Update > System Update and click Import to import the .bin package.



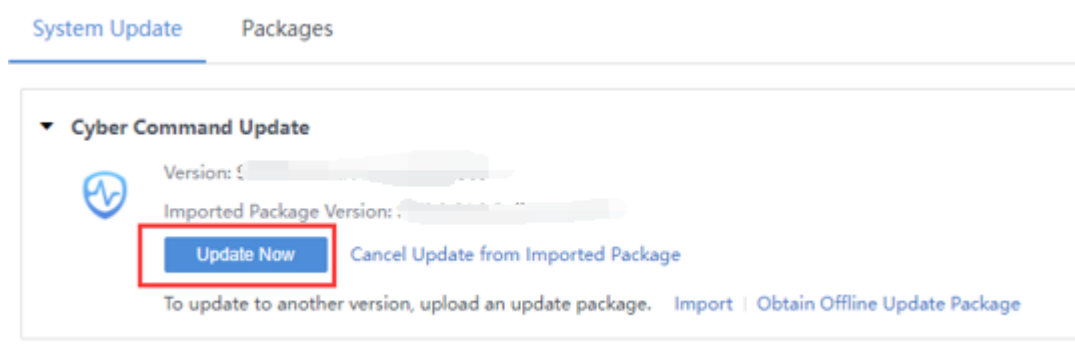
Step 3. Click Import and select the bin to upload to the CC platform.



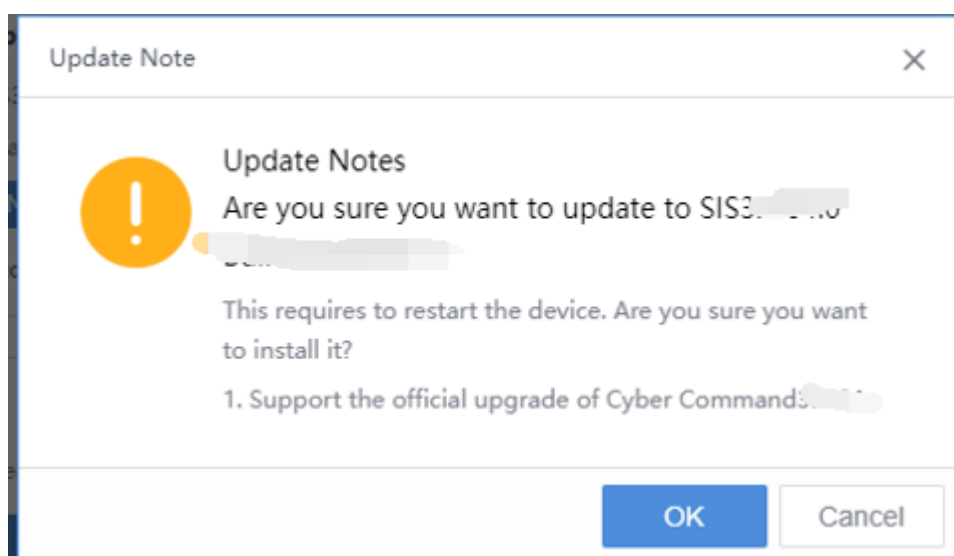
Step 4. Click OK to complete the import process.



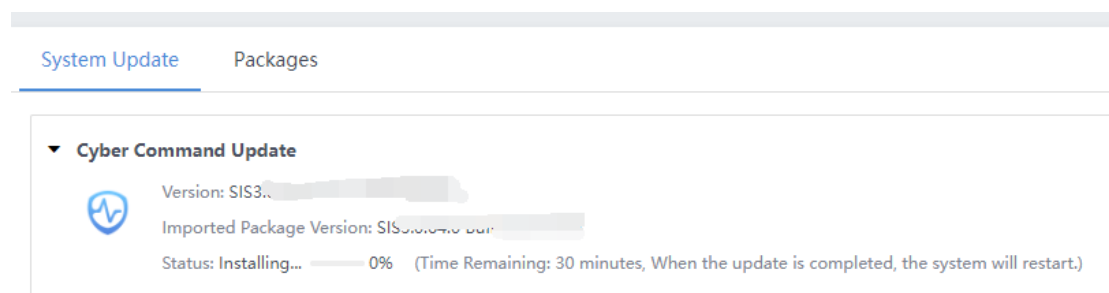
Step 5. Wait for it until it will change the status to update now.



Step 6. Click OK to perform the update.



Step 7. Wait for around 30 minutes until the update process run complete, the CC will restart automatically once it is completed. If the version number has changed to latest version number means the update process is successful.



4.4 Handling of Upgrade Failure

If the upgrade fails, please contact technical support in time.

5 Precautions

1. A downgrade is not supported.
2. Starting from CCOM 3.0.60, only the bin file upgrade package is supported.
3. A CCOM 3.0.60 is required to upgrade to CCOM 3.0.64. Please upgrade to 3.0.60 first if the CCOM firmware is lower than the 3.0.60 version.
4. The CCOM upgrade can only be done via Web Console, and Sangfor Updater is not supported because the upgrade file is large.
5. Do not load the upgrade package in the public network during the upgrade. Instead, it is recommended to use an internal PC to upgrade devices.
6. During the upgrade, avoid manual device restart and accidental power failure.
7. Contact customer service if any problems occur during the upgrade, and do not manually restart the device.

