Sangfor SCP

Release Notes

Product Version	6.7.30
Document Version	1.0
Released on	July. 14, 2022

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 is the release notes of Sangfor Cloud Platform(SCP) version 6.7.30_EN.

Intended Audience

This document is intended for:

- Network Design Engineer
- Operations Engineer

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
July. 14, 2022	This is the first release of this document.

Contents

1 Overview

1.1 Features

1.1.1 New Features

1. Distributed firewall function is added, which supports protecting the traffic between VMs in the same subnet.
2. Administrators can set bandwidth for shared service networks for tenants.
3. Support third-party KMS server management and use KMS keys to encrypt and decrypt devices (VMs) on SCP(Only support HCI6.7.10).
4. Support creating SQL server.
5. Support automatically generating a policy with the lowest priority that blocks traffic from the Internet for the newly-created subnets in tenant VPC.
6. Support automatically creating VM snapshots.
7. Support upgrading the earlier versions of application instances.
8. Support virtual IP address.

1.1.2 Others

Upgrade from special versions:

SCP6.7.0 to SCP6.7.30

Before the upgrade:

- Check whether there is a managed resource pool of the HCI6.7.0_EN (including HCI6.7.0_R2_EN).
- If the above resource pool exists, check whether it was upgraded from earlier versions under the management of SCP6.7.0_EN.
- After upgraded SCP from 6.7.0 to 6.7.30, contact Sangfor Support for further inspection.

If these conditions are met, contact Sangfor Support for further inspection.

1.1.3 Integration with Third-Party Products

None.

1.2 Upgrade Impacts

Upgrade from the following versions are supported:

- aCMP5.8.6_EN
- aCMP5.8.6R1_EN
- aCMP5.8.8_EN
- aCMP6.0.10R1_EN
- aCMP6.0.10R2_EN
- SCP6.1.0_EN
- SCP6.2.0_EN_B
- SCP6.2.0_EN
- SCP6.2.70_EN_B
- SCP6.2.70_EN
- SCP6.3.0_EN_B
- SCP6.3.0_EN
- SCP6.3.70_EN_B
- SCP6.3.70_EN
- SCP6.3.80_EN_B
- SCP6.3.80_EN
- SCP6.7.0_EN_B
- SCP6.7.0_EN
- SCP6.7.30_EN_B
- SCP6.7.30_EN

- **Upgrade Limitations**

None.

- **Immediate Upgrade of Configurations, Logs, and Data**

Yes.

- **Impacts on Functions After Upgrade**

None.

- **Reboot Required After Upgrade**

Yes. A manual reboot is required.

- **Time Taken**

About 30 minutes.

- **Upgrade Recommendation**

None.

1.2.1 Impacts on Services

None.

1.2.2 Impacts on O&M

None.

1.2.3 Impacts on Customer Network

None.

1.2.4 Other Impacts

None.

1.3 Upgrade Instructions for Customers

1.3.1 Upgrade Preparations

None.

1.3.2 Notes

None.

1.4 Implementation Procedure

Refer to Chapter **2.4 Upgrade Steps.**

1.5 Check the Service Status After Upgrade

1. Check whether the SCP platform can be logged in successfully.
2. Whether all services, including backup and disaster recovery, are working.

1.6 Rollback

None.

2 Upgrade Guide

2.1 Confirmation Before Upgrade

2.1.1 Upgrade Tools

- **Upgrade Client Version**

  None.

- **Database Version**

  None.

- **Impacts of Central Management (CM) on Cluster**

  None.

- **Pass-Through Supported**

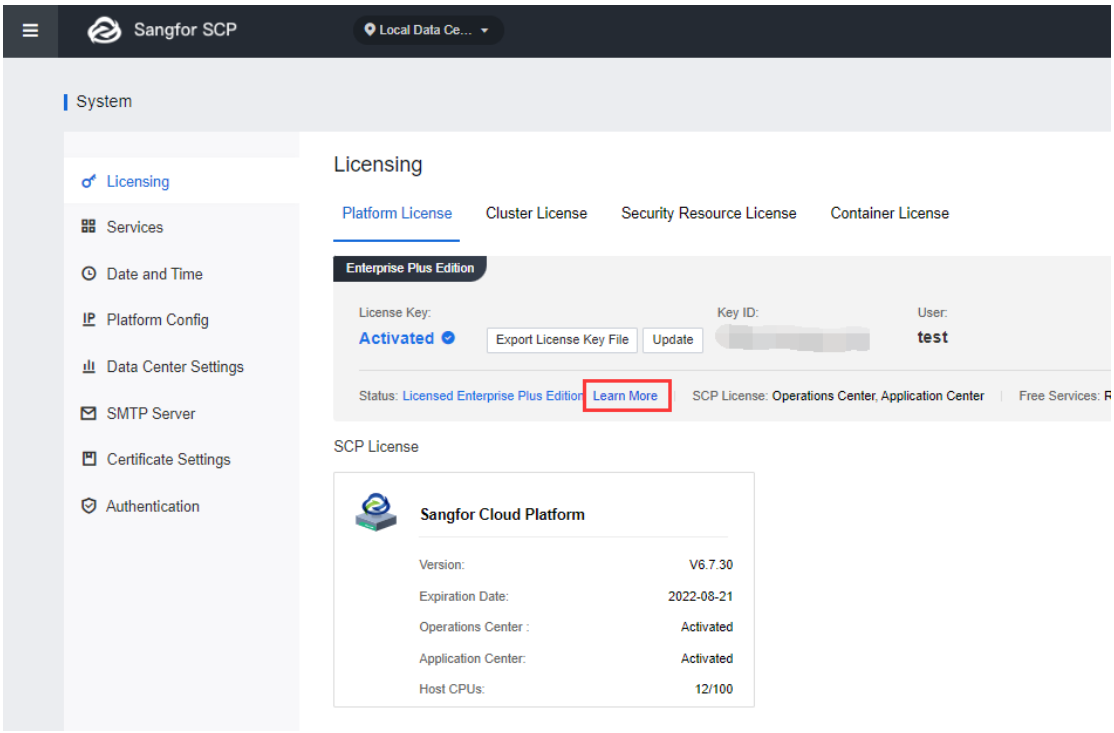
  None.

- **High Availability Supported**

  None.

- **Licensing**

1. The SCP license is still valid.
2. The license of the current SCP version is SCP6.3.70_EN.
   a. Since SCP6.2.0_EN, the original aOC license has changed to the SCP license, categorized into **Advanced Edition, Enterprise Edition,** and **Enterprise Plus Edition.** Each edition comes with different features. You can click **Learn More** on the Licensing page for more details, as shown below.



   b. If the version earlier than SCP6.7.30 contains an aOC license, the license will be converted into an SCP Enterprise Edition license after completing the update.

   c. SCP6.7.30EN and the later versions that contain aHCM license have a quota for licensed physical machines. Therefore, if an aHCM license already exists before the update, a total of 500 licensed physical machines will be available after the update by default.

   d. For versions earlier than SCP6.7.30_EN, only Enterprise Plus Edition customers can use the Application Center. In SCP6.7.30_EN, the

customers who have purchased Advanced Edition or Enterprise Edition can activate aAPP and aHCM license to use the Application Center and AWS Cloud. Additionally, versions earlier than SCP6.7.30_EN with Advanced Edition and Enterprise Edition purchased can use the feature of Physical Machines management. SCP6.7.30_EN with Advanced Edition newly purchased can use this feature after activating the aHCM license.

e. For versions earlier than SCP6.7.30_EN, licensing of AWS Cloud VMs is based on the validity period only. While for SCP6.7.30_EN and later versions, the licensing is based on both the validity period and the number of VMs. In Enterprise Plus Edition, a certain number of AWS Cloud VMs will be given according to the number of host CPUs.

NOTE

If the number of AWS Cloud VMs needed exceeds the number of VMs provided by the platform, you need to renew a license key, and the number of available VMs is the number of licensed VMs. Otherwise, the number of available VMs is the number of VMs provided by the platform.

2.1.2 Environment Information

None.

2.1.3 Customer Resources

None.

2.2 Check Before Upgrade

None.

2.3 Notes

1. **Perform a pre-upgrade check in the disaster recovery scenario.**

   Under the disaster recovery scenario, ensure that no disaster recovery task is in progress before the upgrade. It is recommended to stop disaster

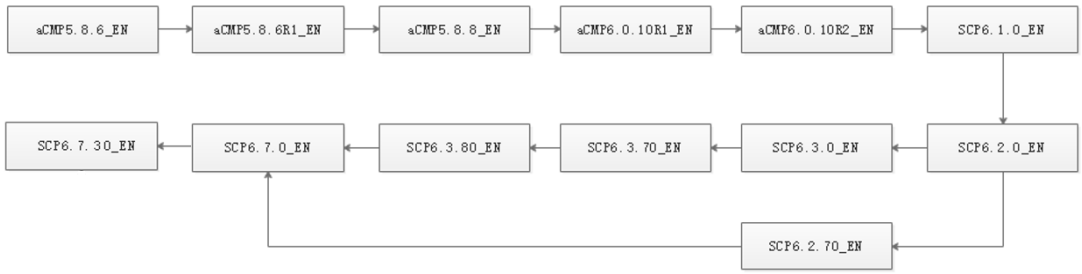
recovery tasks manually and then upgrade the platform. After the upgrade is complete, check the platform to ensure no problems and enable disaster recovery.

2. **Perform a check after the upgrade of active and standby nodes.**

   Upgrade the active and standby nodes and ensure that the versions of the upgraded active and standby nodes are the same.

2.4 Upgrade Steps

2.4.1 Upgrade Path



CAUTION

Each upgrade takes about 30 minutes. Please upgrade during off-peak hours.

All versions can be upgraded to any later version.

2.4.2 Upgrade Steps

CAUTION

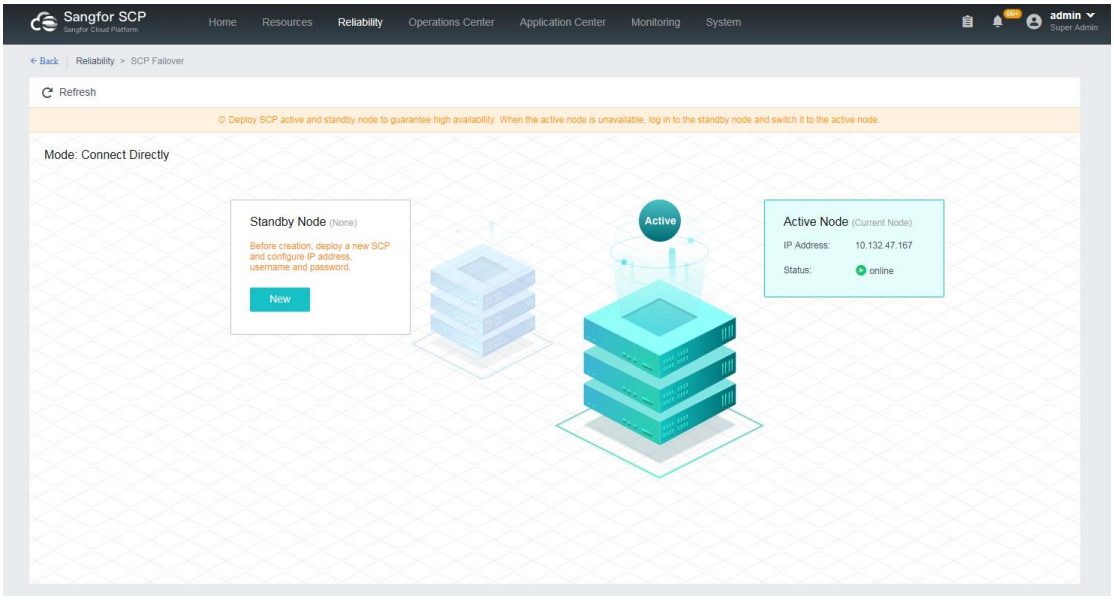
Before Upgrade:

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

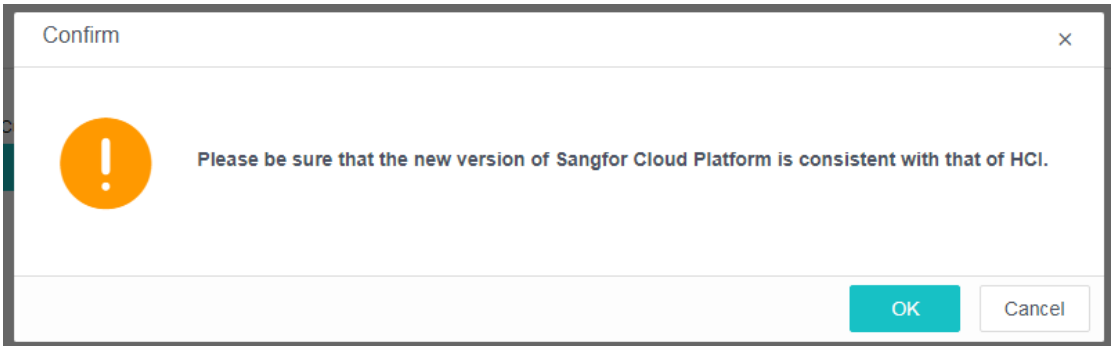
2. Take a snapshot of the SCP that need to be upgraded.

Step 1. Determine whether the SCP platform earlier than SCP6.2.0_EN is

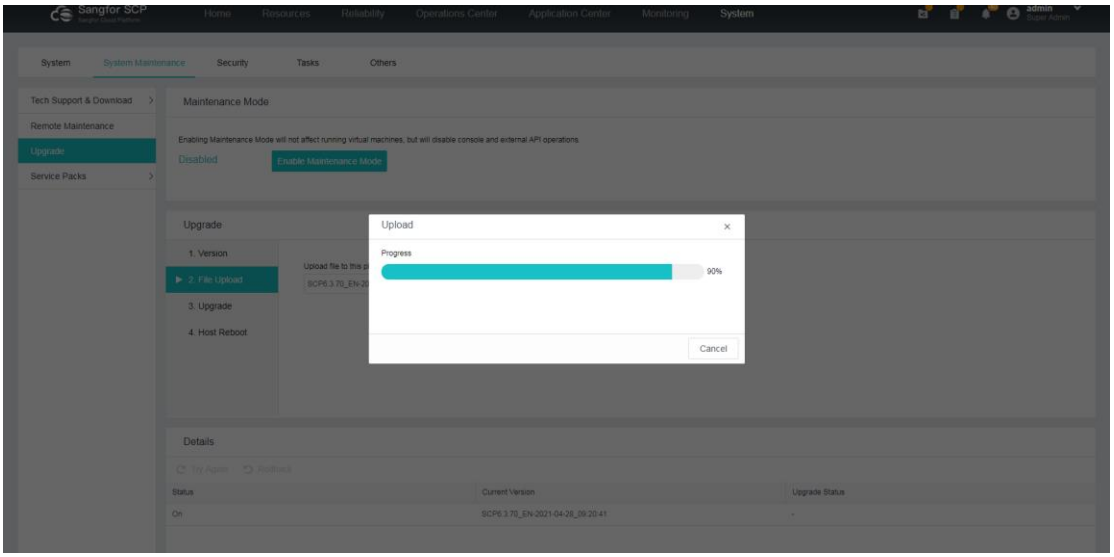
under the failover scenario. Check whether there is a **standby SCP node** in **Reliability** > **SCP Failover**, as shown below. If yes, follow **Step 2** and install the pre-update check package first. For version SCP6.2.0_EN and above, skip to **step 5** and directly update the service pack even with the **standby SCP node**.



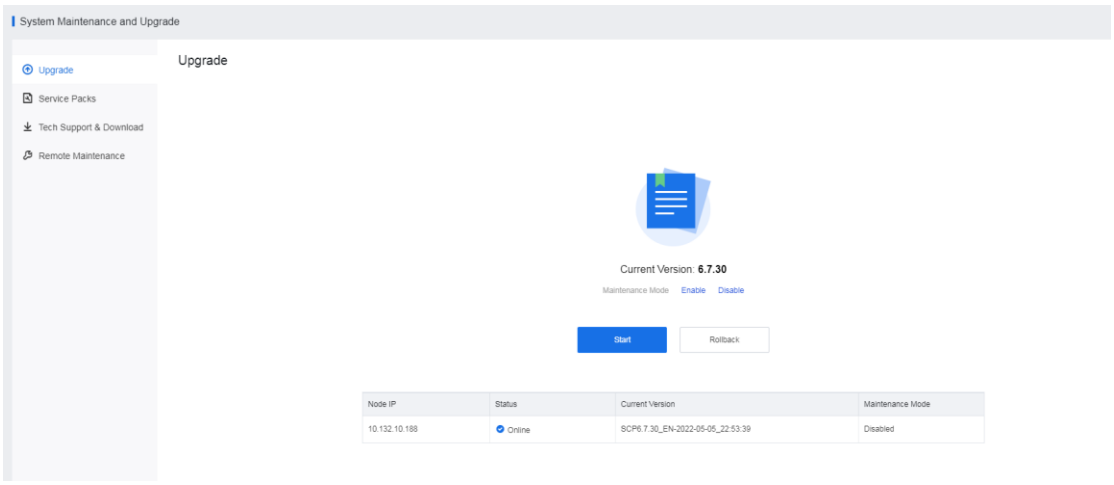
Step 2. Click the **Upgrade** button in **System** > **Upgrade** and click **OK**.



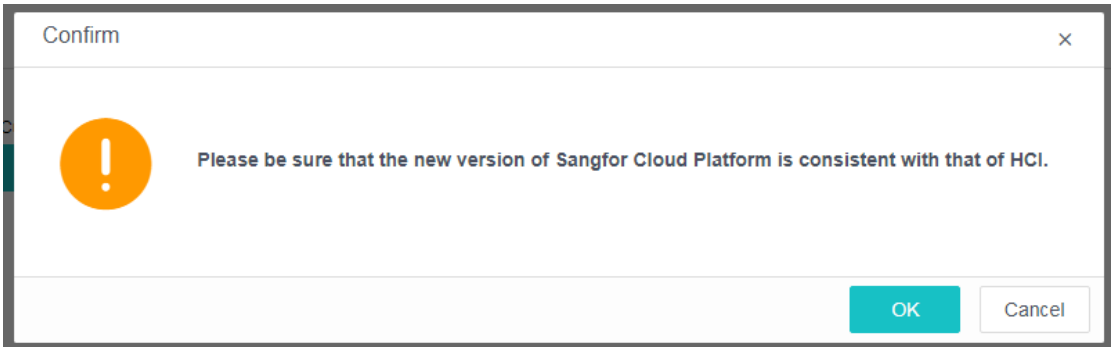
Step 3. Select the pre-update check package and upload it.



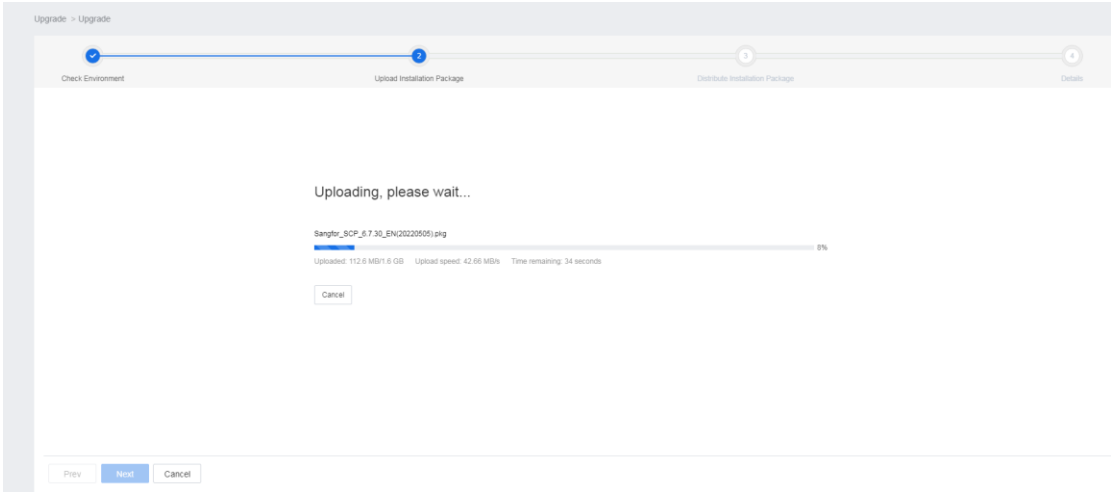
Step 4. Click the **Start** button and wait until the progress bar reaches 100%. No need to restart the VM after the pre-upgrade check package has been successfully installed. You can click the **Disable Maintenance Mode** button to finish the upgrade and view whether the pre-upgrade check package information is included in the **Current Version**.



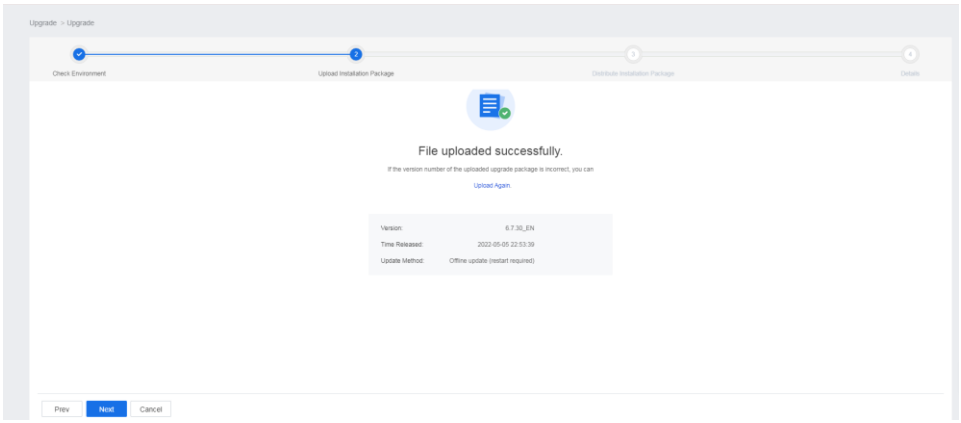
Step 5. Click the **Upgrade** button in **System** > **Upgrade** and click **OK**.



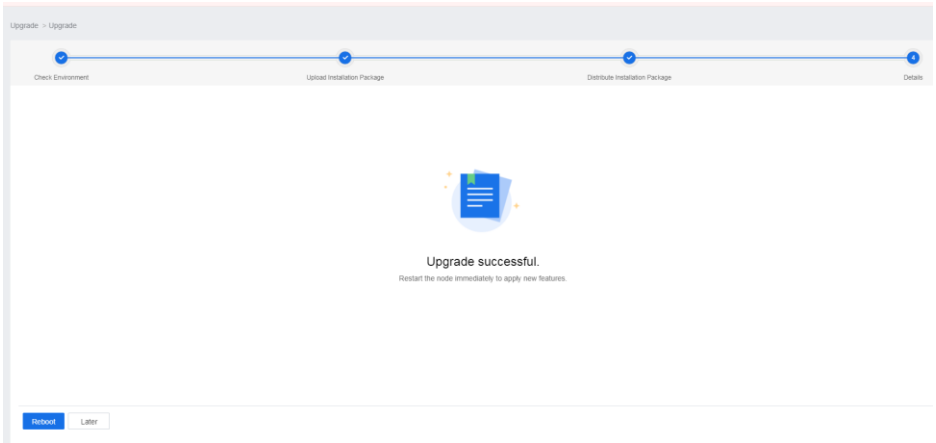
Step 6. Select the **SCP6.7.30_EN upgrade package** and upload it.



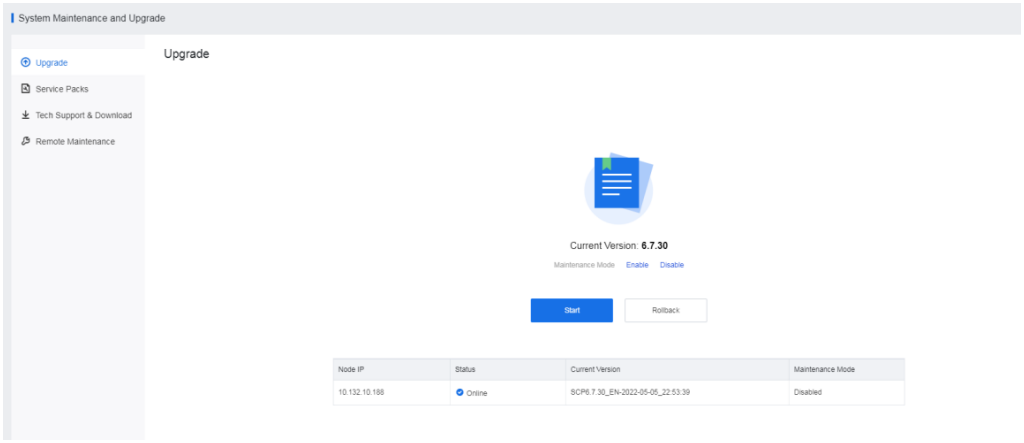
Step 7. Click the **Start** button and wait until the progress bar reaches 100%.



Step 8. Click the **Restart This Platform** after the upgrade is complete.



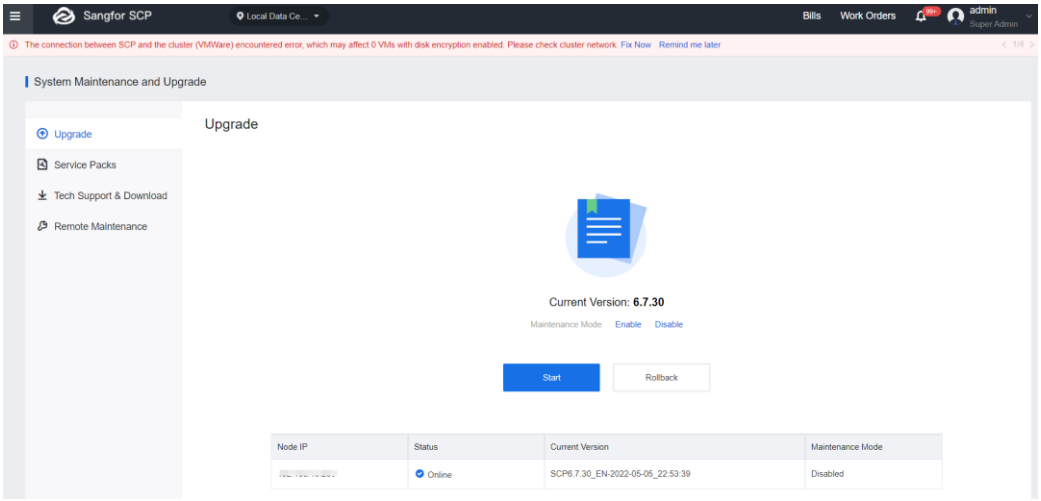
Step 9. After restart, log in to the platform and check whether the current version is SCP6.7.30_EN in **System** > **Upgrade**.



2.5 Post Upgrade Check

2.5.1 Platform

Check whether the current version is SCP6.7.30_EN in **System Maintenance and Upgrade** > **Upgrade**.



2.5.2 Service Status

1. Check whether the SCP platform can be logged in successfully.
2. Check whether all services, including backup and disaster recovery, are working.

2.6 Abnormalities Troubleshooting

Scenario: A task is in progress.

Solution: Go to the task list and cancel the task manually. If it cannot be canceled, update after the task is finished. If it's a disaster recovery task, manually stop the disaster recovery policy and perform the upgrade.

2.7 Rollback

None.

SANGFOR