Sangfor Endpoint Secure

Release Note

Product Version	3.5.10
Document Version	03
Released on	Jan. 11, 2022

Copyright © Sangfor Technologies Inc. 2021. 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.

Change Log

Date	Change Description
Jun. 22, 2020	This is the first release of this document.
Aug. 08, 2021	Updated version from 3.2.22 document
Jan. 11, 2022	Updated version from 3.5.55 document.

Contents

Change Log 2
1 Overview 4
1.1 Major Features 4
1.1.1 New Features 4
1.1.2 Others 5
1.1.3 Integration with Third-Party Products 5
1.2 Upgrade Impacts 5
1.2.1 Impacts on Services 5
1.2.2 Impacts on O&M 5
1.2.3 Impacts on Customer Network 5
1.2.4 Other Impacts 6
1.3 Customer Upgrade Preparations 6
1.3.1 Upgrade Preparations 6
1.3.2 Notes 6
1.4 Implementation Procedure 6
1.5 Post-Upgrade Service Check 6
1.6 Rollback Instructions 7
1.7 Preparations for Upgrade 8
1.7.1 Upgrade Tools 8
1.7.2 Environment Information 8
1.7.3 Customer Resource Coordination 8
1.8 Pre-Upgrade Check 8
1.9 Notes 8
1.10 Upgrade Procedure 9
1.10.1 Upgrade Path 9
1.10.2 Upgrade Procedure 9
1.11 Post-Upgrade Check 10
1.11.1 Checking the Platform 10
1.11.2 Checking Service Status 10
1.12 Troubleshooting Upgrade Failures 10
1.13 Rollback Instructions 10

1 Overview

1.1 Major Features

1.1.1 New Features

Target Customers

Customers who bought Sangfor Endpoint Secure or have high requirements for antivirus capabilities.

Major Values

1. The Bitdefender engine is used to improve antivirus capabilities, virus detection rate, and fix rate.

2. The memory usage during off-peak hours is further optimized to improve user experience.

3. Multiple agent deployment methods (i.e., agent installer download and others) are provided to improve user experience.

4. Remote support is provided to address the issue of unattended hosts.

5. Management of Mac endpoints is newly added, which supports virus scans and endpoint management.

6. Licensing optimization: Licensing methods are simplified, and the licensing process is optimized so that users can flexibly allocate and manage license resources.

7. WebShell optimization: The wsk 3.0 engine is adopted to improve detection capabilities and the detection supports customized web directories.

8. Special virus scans for Linux endpoints: It supports the detection and fix of crypto mining viruses, improving antivirus capabilities.

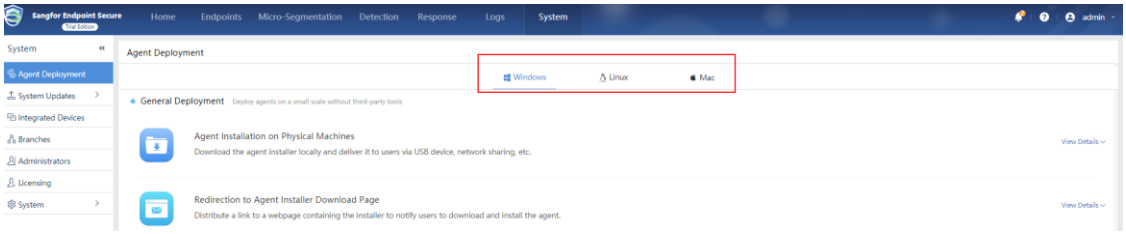
9. RDP Secondary Authentication: It supports secondary authentication of trusting files for Windows endpoints and the use of default passwords as secondary authentication passwords, which greatly improves anti-ransomware capabilities.

1.1.2 Others

1. After the upgrade, integration with Sangfor Platform-X will be unavailable. Contact a Sangfor technical support representative for service packs if necessary.

2. The **Script File** feature under the **Remote Access** module will be unavailable.

3. The method of deploying and installing agents has changed. Agents can only be downloaded in **System** > **Agent Deployment** now.



1.1.3 Integration with Third-Party Products

None.

1.2 Upgrade Impacts

After the update, services will be restarted. There is no need to restart devices.

1.2.1 Impacts on Services

During the upgrade process, events detected on the Endpoint Secure agent cannot be reported to Endpoint Secure Manager.

1.2.2 Impacts on O&M

Endpoint Secure Manager cannot be logged in for 10 minutes.

1.2.3 Impacts on Customer Network

The upgrade of Endpoint Secure Manager may take 10 minutes. The upgrade time of Endpoint Secure agents depends on the number of agents. (Notes: The maximum bandwidth of downloading agents is 2 MB/s, and the maximum number of agents in a download task is 5. It will take 5 minutes to download 5 agents under stable network conditions.)

1.2.4 Other Impacts

None.

1.3 Customer Upgrade Preparations

1.3.1 Upgrade Preparations

The Endpoint Secure Manager is to be upgraded.

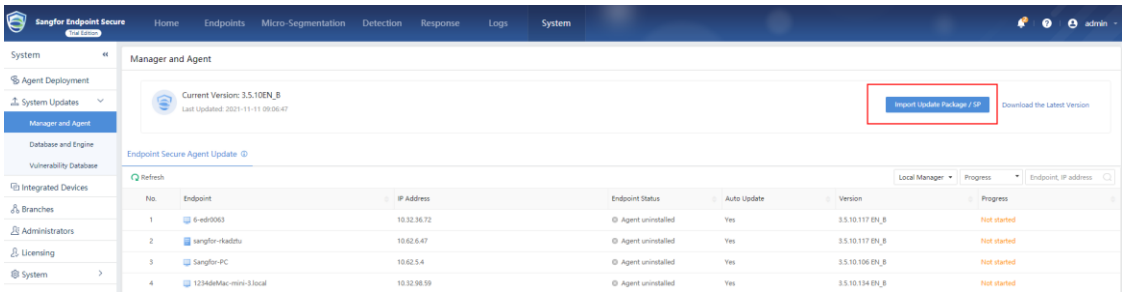
1.3.2 Notes

The upgrade of Endpoint Secure Manager may take 10 minutes. The upgrade time of Endpoint Secure agents depends on the number of agents. (Notes: The maximum bandwidth of downloading agents is 2 MB/s, and the maximum number of agents in a download task is 5. It will take 5 minutes to download 5 agents under stable network conditions.)

1.4 Implementation Procedure

Offline Update:

Step 1. Click **Import Update Package / SP** in **System** > **System Updates** > **Manager and Agent** to import an update package.



Step 2. Perform the update.

The update will be complete in 10 minutes.

1.5 Post-Upgrade Service Check

1. Endpoint Secure Manager can be logged in to.

2. Virus scan tasks sent can be completed.

1.6 Rollback Instructions

Rollback: Not supported.

(Contact a Sangfor technical support representative if the upgrade failed)

Rollback is not supported. You can contact a Sangfor technical support representative to recover the Manager from backups.

Upgrade Guide

1.7 Preparations for Upgrade

1.7.1 Upgrade Tools

EDR3.5.5EN update package: ES3.5.10EN_20220106.pkg

1.7.2 Environment Information

The update requires the IP address, username, and password of the Manager to be updated.

1.7.3 Customer Resource Coordination

The upgrade takes about 10 minutes.

If the upgrade fails, a server background account and password are needed.

1.8 Pre-Upgrade Check

Check whether the current version can be upgraded.

Current Version	Upgrade Path	Notes
3.2.15EN	3.2.15EN>3.2.22EN> ES3.5.10EN_20220106.pkg	3.2.15EN cannot be directly updated to 3.5.10EN. It must be updated to 3.2.22EN first.
3.2.22EN-3.5.5EN	Any version of 3.2.22EN > 3.5.5EN > ES3.5.10EN_20220106.pkg	3.2.22EN, 3.5.1EN, and 3.5.5EN can be updated to 3.5.5EN.

1.9 Notes

- **Upgrade Limitations**

The size of free disk space must be more than three times the size of the upgrade package.

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

Yes.

- **Upgrade Recommendations**

1. During the update, do not restart the device manually and keep the device powered on.
2. If any error message pops up during the update, please do not perform any operations and call us at +6012-7117129 (7511) immediately. Do not manually restart the device.

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

None.

- **Pass-Through Supported**

Not supported.

- **High Availability Supported**

Not supported.

1.10 Upgrade Procedure

1.10.1 Upgrade Path

Upgrade path:

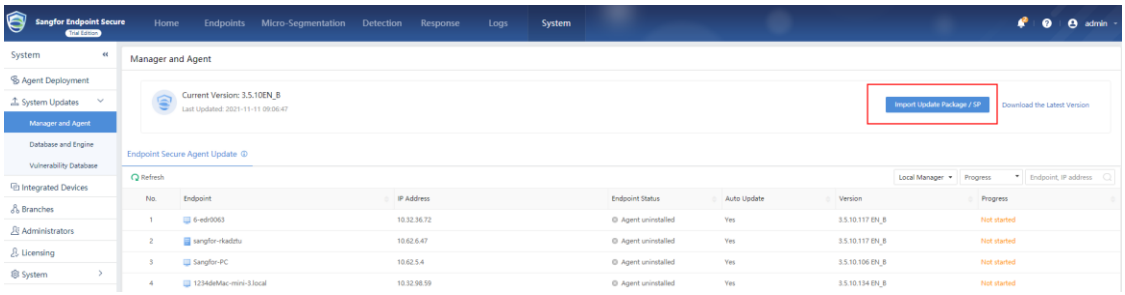
An update may take 15 minutes. Please perform the update during off-peak hours.

Current Version	Upgrade Path	Notes
3.2.15EN	3.2.15EN > 3.2.22EN > ES3.5.10EN_20220106.pkg	3.2.15EN cannot be directly updated to 3.5.10EN. It must be updated to 3.2.22EN first.
3.2.22EN~3.5.5EN	Any version of 3.2.22EN-3.5.5EN > ES3.5.10EN_20220106.pkg	3.2.22EN, 3.5.1EN, and 3.5.5EN can be updated to 3.5.5EN.

Upgrade of custom versions is not supported.

1.10.2 Upgrade Procedure

Step 1. Click **Import Update Package / SP** in **System** > **Update** > **Manager and Agent** to import an update package.



Step 2. Perform the update.

The update will be complete in 10 minutes.

1.11 Post-Upgrade Check

1.11.1 Checking the Platform

Log in to the Manager and check whether the current version is 3.5.10EN in **System** > **System Updates** > **Manager and Agent**.

1.11.2 Checking Service Status

Check if the virus task sent can be completed. If yes, basic functions work properly.

1.12 Troubleshooting Upgrade Failures

Solution 1: Contact a Sangfor technical support representative for troubleshooting.

Solution 2: If the upgrade fails, you can enter the background of Endpoint Secure Manager, enter the command /sf/edr/manager/bin/eps_services restart, and upgrade the manager again.

1.13 Rollback Instructions

Rollback: Not supported.

(Contact a Sangfor technical support representative if the upgrade failed)

Rollback is not supported. You can contact a Sangfor technical support representative to recover the Manager from backups.

SANGFOR