SANGFOR

Endpoint Secure

Quick Start Guide

Change Log

Date	Change Description
September 4, 2019	Quick Start Guide release.

CONTENT

Chapter 1 Introduction of Endpoint Secure

Endpoint Secure is a set of terminal security solutions provided by Sangfor, consisting of lightweight endpoint security software and management platform software.

The Endpoint Secure management platform is able to perform the unified terminal asset management, terminal virus detection and killing, terminal compliance check, unified management of micro-isolation access control policies, one-click isolation and handling for the security events, and IOC-based network-wide threats location for hot events.

Endpoint security software supports such functions as antivirus, intrusion prevention, firewall isolation, data collection and reporting, and one-click processing. Sangfor Endpoint Secure also supports collaboration with the NGAF and IAM, constituting a new generation of the security protection system.

1.1 Endpoint Secure Features and Values

Comprehensive management of terminal assets: It enables a comprehensive inventory of the network-wide terminal assets, including the terminals of the service servers and the terminals of user PCs. The inventory indicates the name, IP address, MAC address, organization, owner, asset number, and asset location of each terminal device. The asset information on each terminal shall be clear, and each security event shall be addressed by the specific employee so that security management can be put in place.

Compliance review on terminal security: Each organization has its unique compliance requirements for terminal security, specifically the compliance requirements for grade protection and the security requirements for the host. The terminal security compliance review is designed according to the host security requirements based on grade protection. It performs the compliance review on the policies about identity authentication, access control, security audit, intrusion prevention and malicious code prevention, aiming to meet the host security requirements based on grade protection for enterprises.

Real-time protection against ransomware: Ransomware is a type of malware that encrypts files of a victim. Then the attacker demands a ransom from the victim to restore access to the files upon payment. This type of malware is becoming more and more popular and

happens to our customers almost every day. Sangfor Endpoint Secure can accurately differentiate various families of ransomware, and identify various infection behaviors and encryption features of ransomware based on professional analysis. In this way, Sangfor Endpoint Secure effectively detects and kills the latest ransomware, protecting users from the latest ransomware.

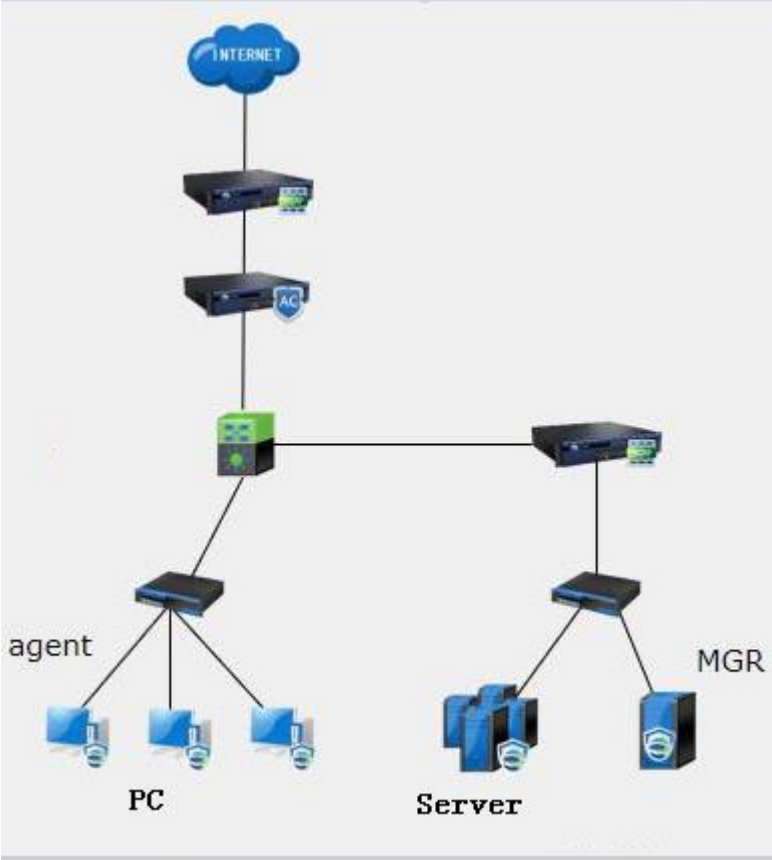
Proactive detection of intrusion attacks: Most of the terminal hosts infected with ransomware or mining viruses are hacked through the brute force against weak passwords. Sangfor Endpoint Secure proactively detects the brute force behaviors and blocks the IPs starting such attacks. Besides, Sangfor Endpoint Secure proactively detects the Web backdoor files to protect against Web security attacks.

Quick response to hot events: Sangfor Neural-X provides the IOC intelligence about hot events based on the global security analysis using the big data, and sends the intelligence data to the Endpoint Secure. The Endpoint Secure can quickly perform the location analysis on network-wide threats based on the IOC intelligence data, and detect and respond to the latest hot events on time. Also, the Endpoint Secure performs root cause analysis based on the historical behavior data to protect the organizations from security events.

1.2 Deployment Introduction

The Endpoint Secure is deployed on local users and the Agent is installed on each server. The Endpoint Secure is linked with the Sangfor Security Cloud through the public network. The Agent on each server in the LAN is linked with the Endpoint Secure. In this way, the local terminal users are provided with accurate security intelligence and solutions. All data is encrypted in the communication process. The servers do not require permission to access the public network, thereby achieving security isolation.

Applicable scenario: servers isolated from the Internet. The networking diagram is as follows:



- Install the Endpoint Secure management platform (MGR) on a Linux server at the local end.

- Install the Agent program on terminals (Windows and Linux) for terminal security detection.

- The MGR delivers the security policy to the Agent to perform threat detection and security protection for terminals.

- The MGR is linked with the Sangfor Security Cloud through the public network. The Agent on each terminal in the LAN is linked with the MGR. In this way, the local terminal users are provided with accurate security intelligence and solutions.

Chapter 2 Installation Conditions

This chapter describes the installation conditions for the central management end of Endpoint Secure (hereinafter referred to as MGR) as well as the client (hereinafter referred to as Agent). The Endpoint Secure does not involve hardware products.

2.1 Central Management End (MGR)

The **MGR** where the Linux system is installed must be configured as follows:

CPU: > = 4 cores

Memory: > = 8 GB

Hard drive: > = 500 GB

System requirements: **64-bit Ubuntu (recommended Ubuntu16) or Centos (Centos7)**. The 32-bit operating systems or the Windows systems are not supported. The above conditions must also be met if the virtual machine is adopted (virtual machine platform Sangfor HCI and VMware additionally supported).

***Note: Incompatibility may occur if the system requirements are not met.**

Network Connectivity:

- The Agent communicates with the MGR over the ports 443, 8083, and 54120 (port 443 for downloading the Agent, port 8083 for services, and port 54120 for management).
- Port 443 is used for the management platform access. Please allow the corresponding firewall policy to ensure connectivity.

  The management platform needs to communicate with the upgrade server (121.46.26.113). Please ensure connectivity. The cloud search engine for malicious file detection needs to access https://analysis.sangfor.com.cn and https://auth.sangfor.com.cn/v1/auth. Please ensure connectivity between the management platform and https://analysis.sangfor.com.cn and https://auth.sangfor.com.cn/v1/auth. (Lack of network connectivity does not have impact on the use of product but may affect the effectiveness of virus detection.)

- To improve Endpoint Secure products, customers who voluntarily join the cloud security program need to allow https://cloud.sangfor.com.cn for virus data reporting.

Note: The Centos system turns on the firewall denying access to all ports in default settings. Please allow the corresponding port to be accessed by the console.

Run the following commands to allow ports 443, 54120, and 8083:

- firewall-cmd --permanent --zone=public --add-port=8083/tcp
- firewall-cmd --permanent --zone=public --add-port=54120/tcp
- firewall-cmd --permanent --zone=public --add-port=443/tcp firewall-cmd --reload

2.2 Endpoint Secure Software (Agent)

The **endpoint secure software (Agent)** can be installed in common 32-bit/64-bit Windows and 32-bit/64-bit Linux systems. See the following table for details. Unpredictable problems may occur if a system not listed in the table is installed.

Windows (64bit & 32 bit)		Linux (64 bit & 32 bit)
Server	Pc	Server
Windows Server 2003 SP2	Windows XP SP3	Centos 5,6,7
Windows Server 2008	Windows Vista	Ubuntu 10,11,12,13,14,16,17,18
Windows Server 2018 R2	Windows 7	Debian 6,7,8,9
Windows Server 2012	Windows 8	RHEL 5,6,7
Windows Server 2012 R2	Windows 8.1	SUSE 11,12,16

Windows Server 2016	Windows 10	Oracle Linux5,6,7
Windows Server 2019		

2.3 Precautions

- If the Linux system is installed with the Agent of Endpoint Secure and enables micro-isolation, it will take over the iptables rules (micro-isolation function: the customer-configured iptables rules are backed up and then deleted). If the iptables rules have been configured, please communicate with the customer first and then use the micro-isolation function. Uninstalling or disabling the Agent will restore the original firewall state and retrieve the iptables rules.
- When the Agent is installed on Linux, the ping command will be used to detect connectivity with the MGR. If the ping command returns a failure or the ping command is banned, the Agent installation will fail.
- If the Windows system is installed with the Agent of Endpoint Secure and enables micro-isolation, the original firewall rules will continue to take effect and micro-isolation configuration will be added to the firewall.

Chapter 3 Endpoint Secure Installation and Deployment

3.1 Central Management End (MGR) Fresh Installation

3.1.1 Central Management End (MGR) Installation using pkg

The terminal security detection and response management platform provides the offline installation package.

Download the installation package from: https://community.sangfor.com

Select **[Self-service] - [Software Download] - [Endpoint Secure] - [Endpoint Secure Upgrade Package]**. Download the latest package for installation.

For offline package installation, the customer only needs to provide a qualified Linux server (see Section 2.1 Central Management End (MGR)).

Installation Steps:

- Download the **manager_deploy.sh** script for fresh installation, and download the latest installation package. In this step, the Endpoint Secure3.2.8R1 package in the above figure is used as an example.
- Upload **manager_deploy.sh** and **Endpoint Secure3.2.8_offline_20181019035239_Build379.pkg** to any directory of the MGR background.
- Run the **chmod u+x manager_deploy.sh** command to modify the permission to manager_deploy.sh.
- Run the command to install the offline package:

  ./manager_deploy.sh Endpoint Secure3.2.8_offline_20181019035239_Build379.pkg 121.46.26.113

  Wait for about 5 minutes until the installation succeeds.

3.1.1.1 Modifications of Platform Network Settings

After the installation is complete, modify the MGR's IP address, routing and DNS settings in the background so that the Agent can connect to the platform and the platform can connect to the cloud search and upgrade servers via the Internet.

The steps are as follows with CentOS used as an example:

- Run the ifconfig command to view network ports.
- Run the **vi /etc/sysconfig/network-scripts/ifcfg-eth0** command to modify the network configuration.
- Run the **vi /etc/resolv.conf** command to modify DNS settings.
- Run the service network restart command to restart network services.
- Run the **cat /sf/edr/manager/config/server.ini** command to check whether the cloud address is 121.46.26.113. If not, manually modify the address to ensure consistency. Then, run the **sh /sf/edr/manager/bin/eps_services** restart command to restart the Endpoint Secure service.
- Run the **iptables –nv -L** command to check whether the firewall configuration allows ports 443, 8083, and 54120. If not, allow these ports.

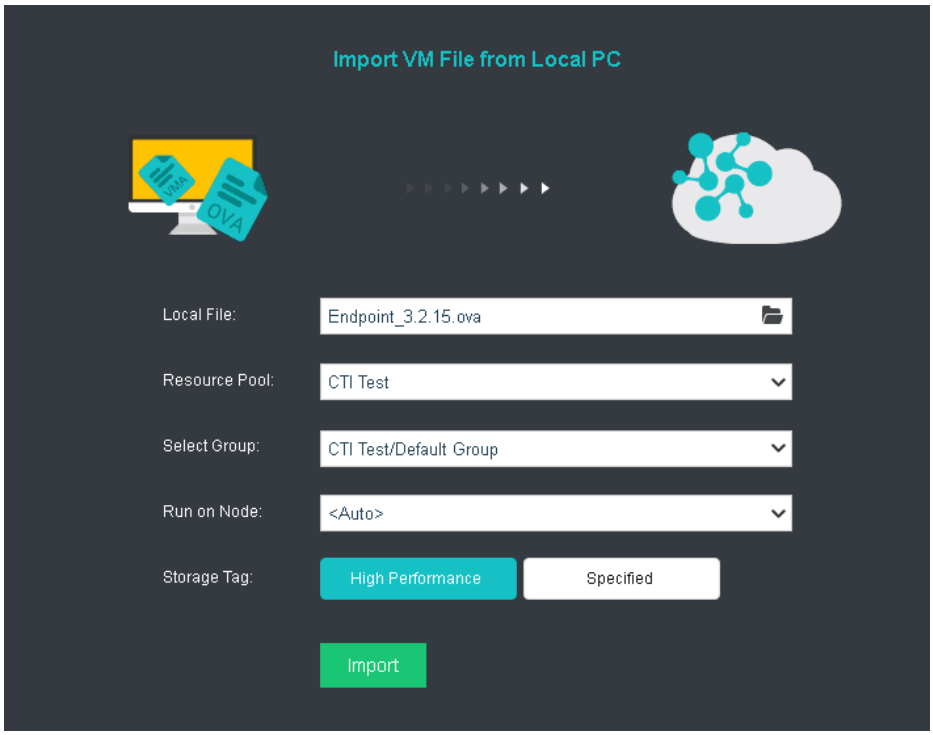
For other Linux distributions, locate the corresponding files and modify them.

3.1.2 Central Management End (MGR) Installation using ova

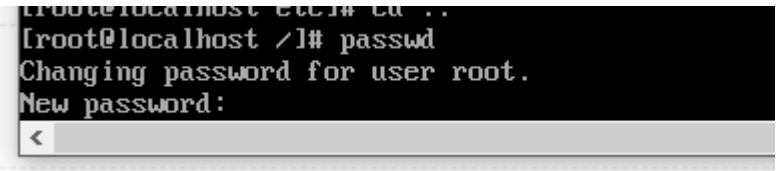
OVA template deployment for deploying MGR in VMWARE and HCI virtualized environments.

Step 1: Import an OVA template

Import the OVA template from the virtualization environment, as shown in the following figure (using aCloud as an example).



The password of root is recommended to change (using the command passwd) after successfully import the template, as shown in the figure.



Note: To enter backend of linux, root password is needed.

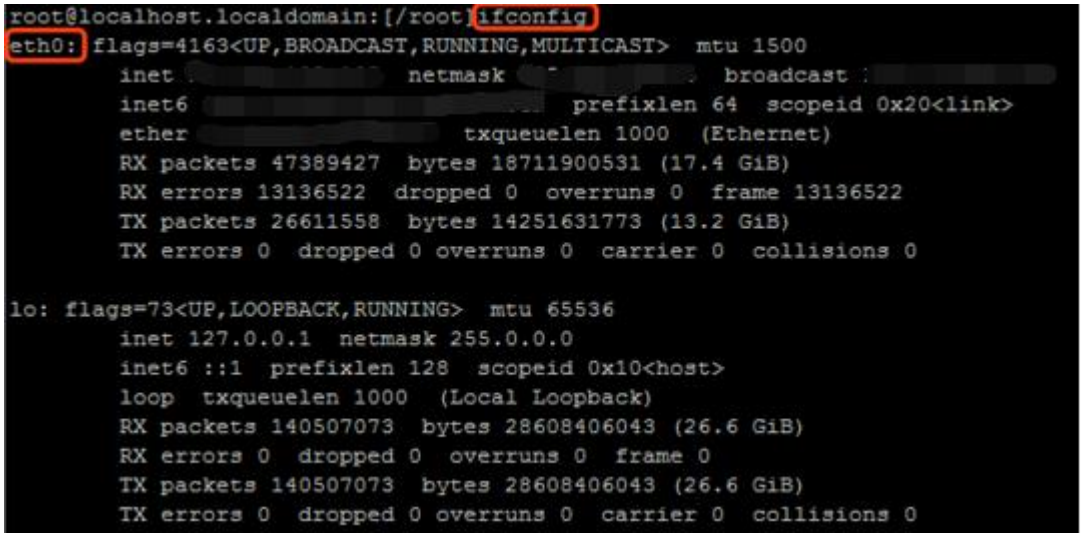
Step 2: Network configuration

Modify the OVA template's IP address and DNS address that is compatible to client's network.

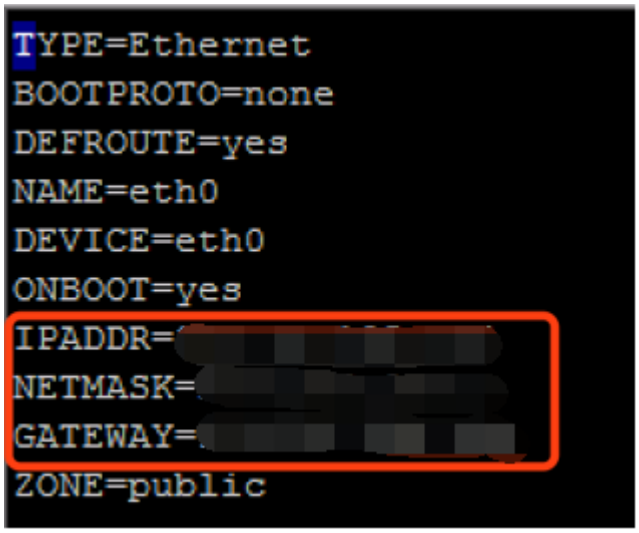
The following example is using centos, the following is only act as a guide to configure.

- Modify the network interface IP address:

ifconfig or ip addr to check the information of the interface, as shown in figure:



Configure the interface's IP address, netmask and gateway as shown in the figure:



When the configuration is done, press Esc and execute the following command to save and quit (:wq!)

- Modify DNS confiuration:

Change the DNS configuration to ensure that the following domain name can be resolve and it is function properly.

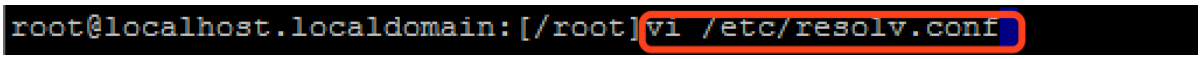
(Cloud) Vulnerability related patch: https://upd.sangfor.com.cn

(Cloud) Authorization to access cloud: https://auth.sangfor.com.cn

(Cloud) Cloud analysis server: https://analysis.sangfor.com.cn

(Cloud) Cloud security plan: https://clt.sangfor.com.cn

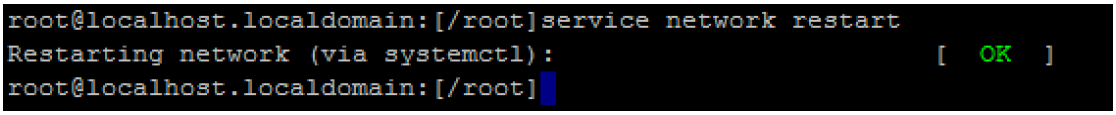
Execute: vi /etc/resolv.conf, configure the DNS IP address at the nameserver IP address, as shown in the figure:



When the configuration is done, press Esc and execute the following command to save and quit (:wq!)

Step 3: Restart the services in order for the configuration to take effect

Execute (service network restart) to restart the network in order for the configuration to take effect.



From MGR server to test the stated domain name can be resolved and the connectivity to port 443.

3.1.3 Central Management End (MGR) Installation using iso

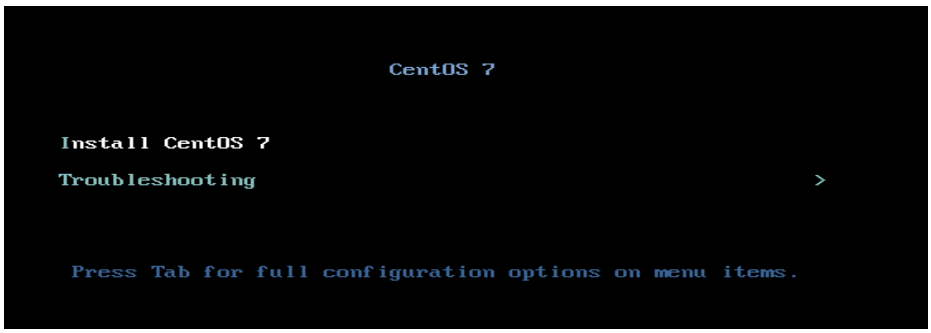
The deployment of ISO template is suitable for both virtual environment and physical server when install MGR.

Step 1: Preparation for intallation

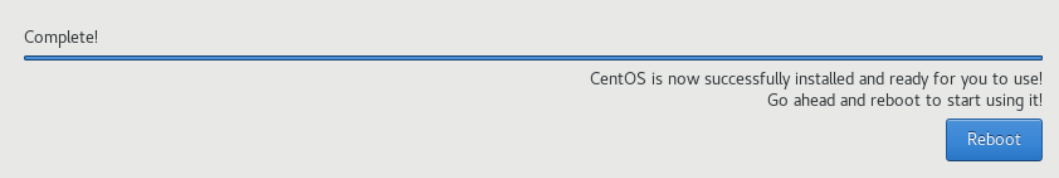
The ISO file should be ready before hand, then burn the ISO image file to a DVD or a USB.

Step 2: Installation process

CD-ROM and USB should be set as the server's first boot order. The following is an example of the startup page.



Choose "Install CentOS 7", click Enter to install (the installation process will be automated), wait until the installation is completed.



The figure above shows that the installation is completed, click "reboot" to restart into the server.

Note: To enter backend of linux, root password is needed.

Step 3: Network configuration

The network configuration include IP configuration, DNS configuration, the configuration guide can refer to "3.1.2 Central Management End (MGR) Installation using ova"

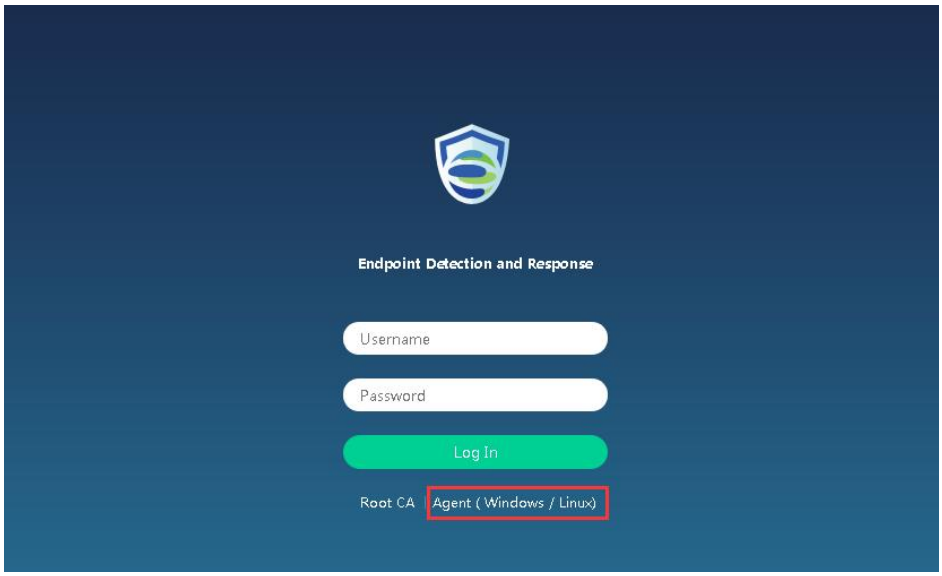
3.2 Endpoint Protection Software (Agent) Installation

3.2.1 Downloading and Deploying the Installation Package

3.2.1.1 Installing the Agent in Windows

- Download the installation script from the MGR console page (https://Manager_IP). There are two available console entries for downloading the installation script.

  1) The login page, as shown in the following figure.



  2) The system management page, as shown in the following figure.

- Upload the installation package to the terminal device to be installed, retaining the file names. Directly run the EXE file for installation. The installation path of software: %ProgramFiles%\Sangfor\Endpoint Secure
- The Agent will get online at the MGR within 2 minutes after the installation is complete.

3.2.1.2 Installing the Agent in Linux

- Download the installation script. There are two download methods, which are console download and Linux host download by command. For details about console download, see Step 1 in Section 3.2.1.1 installing the Agent in Windows.

- Download the installation script directly on the Linux host by running the following command:

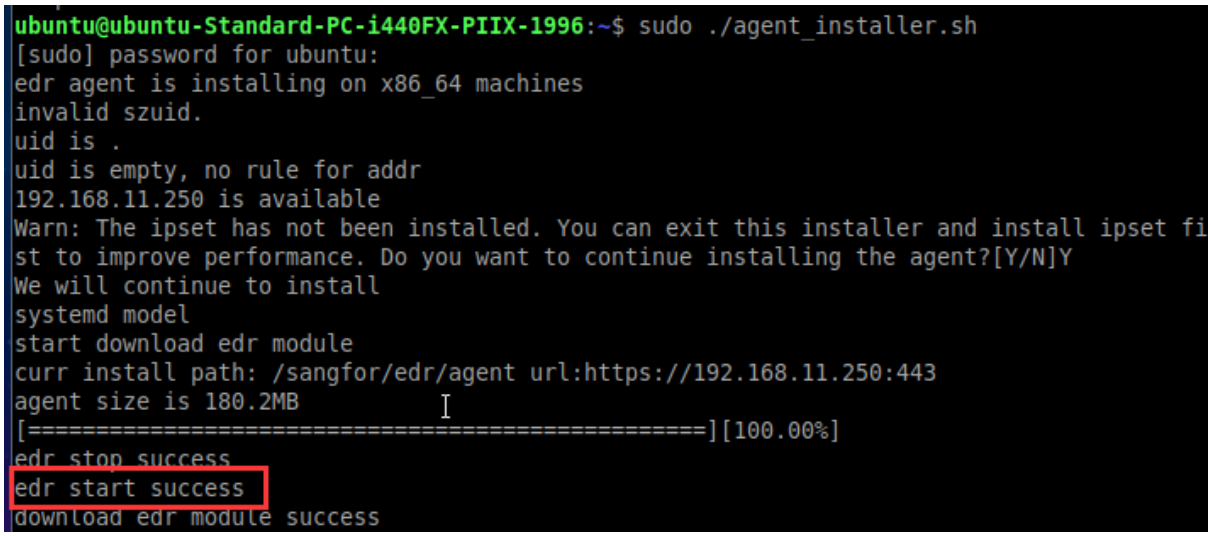
  wget --no-check-certificate https://Manager_IP/html/linux_Endpoint Secure_installer.tar.gz. In this command, Manager_IP indicates the actual IP address of the management platform.

```
ubuntu@ubuntu-Standard-PC-i440FX-PIIX-1996:~$ wget --no-check-certificate https://192.168
.11.250/html/linux_edr_installer.tar.gz
--2019-09-03 11:01:25--  https://192.168.11.250/html/linux_edr_installer.tar.gz
Connecting to 192.168.11.250:443... connected.
WARNING: cannot verify 192.168.11.250's certificate, issued by 'CN=WEBUI,O=INFOSEC,C=CN':
  Unable to locally verify the issuer's authority.
    WARNING: certificate common name '222.222.222.0' doesn't match requested host name '1
92.168.11.250'.
HTTP request sent, awaiting response... 200 OK
Length: 2806414 (2.7M) [application/octet-stream]
Saving to: 'linux_edr_installer.tar.gz'

linux_edr_installer 100%[===================>]   2.68M  2.63MB/s    in 1.0s

2019-09-03 11:01:26 (2.63 MB/s) - 'linux_edr_installer.tar.gz' saved [2806414/2806414]
```

- Upload the installation script to the terminal device on which the Agent is to be installed (Skip this step if you run commands to download the installation script). Then, run the command **tar -xzvf linux_Endpoint Secure_installer.tar.gz** to decompress the file.

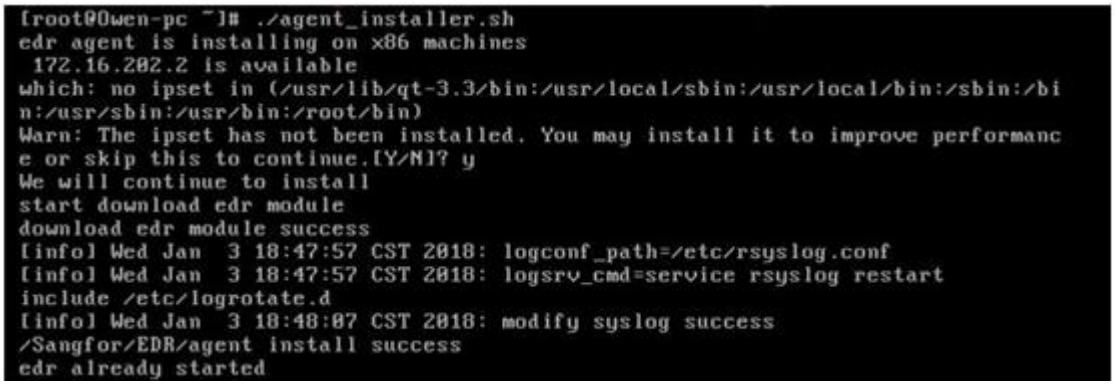
```
ubuntu@ubuntu-Standard-PC-i440FX-PIIX-1996:~$ tar -zxvf linux_edr_installer.tar.gz
agent_installer.sh
manager_info.txt
readme.txt
sfupdate32.bin
sfupdate64.bin
```

- Run the install command. That is, run the ./agent_installer.sh command in the decompressed directory to install the Agent. By default, the installation path is /Sangfor/Endpoint Secure/agent.



The customer can also designate an installation path. For example, run the **./agent_installer.sh 10.251.251.251 /home/Endpoint Secure/** command to install the Agent in /home/Endpoint Secure/. In this command, **10.251.251.251 indicates the IP address of the management platform, which needs to be modified on the basis of actual situations**.

The installation process will recommend the installation of ipset. You may choose to ignore ipset and continue to install Agent. If you choose n, you will start installing ipset manually, and then reinstall Agent after ipset is installed.



1. **If the Linux system is installed with the Agent of Endpoint Secure and enables micro-isolation, it will take over the iptables rules of Linux (micro-isolation function: the customer-configured iptables rules are backed up and then deleted). If the iptables rules have been configured, please communicate with the customer first and then use the micro-isolation function. Uninstalling or disabling the Agent will restore the original firewall state and retrieve the iptables rules.**
2. **The Agent will get online in the terminal online list at the MGR within 2 minutes after the installation is successful.**

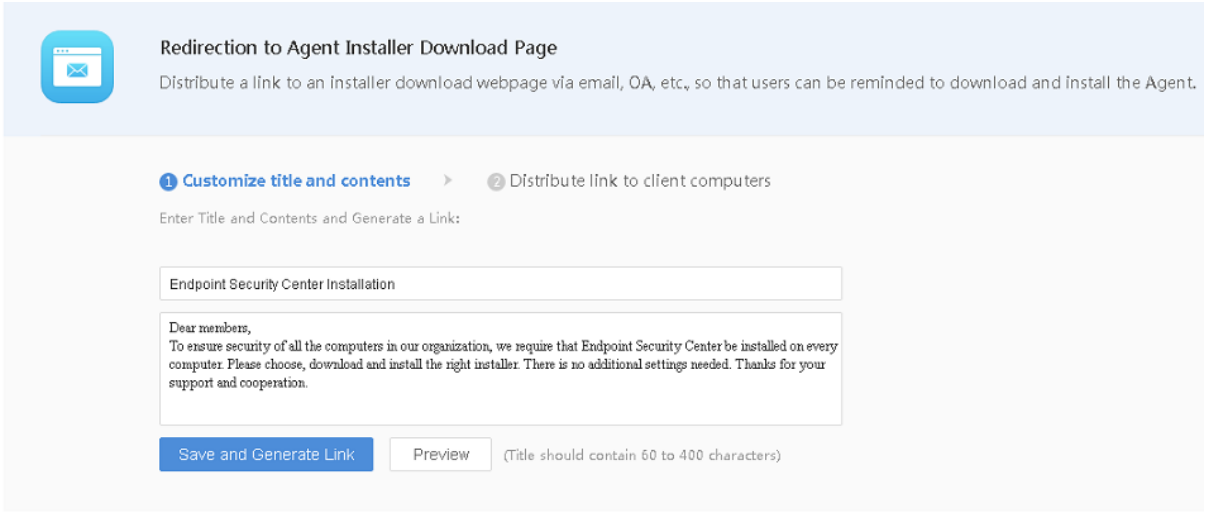
3.2.2 Installing and Deploying the Agent in Batch Mode

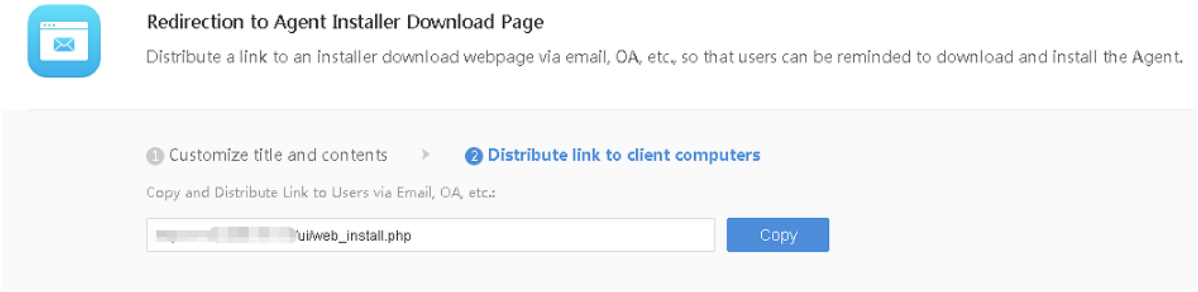
3.2.2.1 Webpage Promotion Deployment

The administrator releases the deployment notice webpage and sends the webpage link to terminals using email, OA, etc.

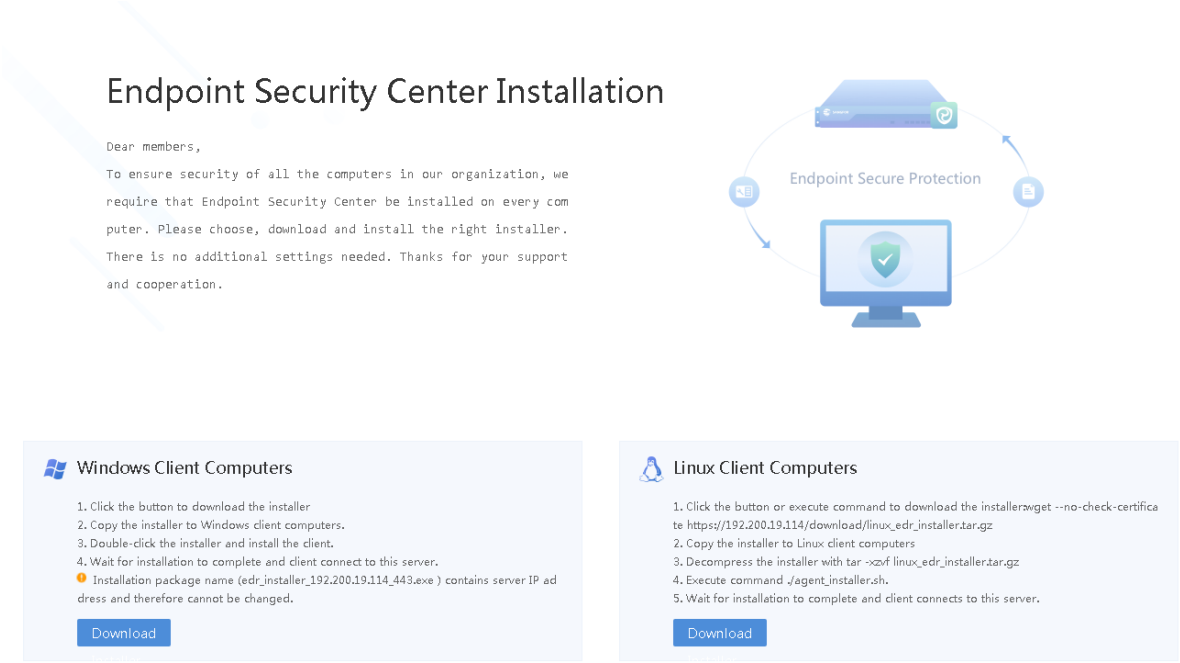
Terminal users download the Agent installation package for installation and deployment.

Log in to the console and select [System] - [Clinet Enforcement] – [Redirection to Agent Installer Download Page]. Fill out the title and content of the deployment notice. Click Save and Generate Link.


Redirection to Agent Installer Download Page
Distribute a link to an installer download webpage via email, OA, etc., so that users can be reminded to download and install the Agent.
1 Customize title and contents
2 Distribute link to client computers
Enter Title and Contents and Generate a Link:
Endpoint Security Center Installation
Dear members,
To ensure security of all the computers in our organization, we require that Endpoint Security Center be installed on every computer. Please choose, download and install the right installer. There is no additional settings needed. Thanks for your support and cooperation.
Save and Generate Link
Preview
(Title should contain 60 to 400 characters)


Redirection to Agent Installer Download Page
Distribute a link to an installer download webpage via email, OA, etc., so that users can be reminded to download and install the Agent.
1 Customize title and contents
2 Distribute link to client computers
Copy and Distribute Link to Users via Email, OA, etc.:
ui/web_install.php
Copy

The promotion webpage is shown as follows:



- Download the Agent installation package. For details, see Section 3.2.1 Downloading and Deploying the Installation Package.

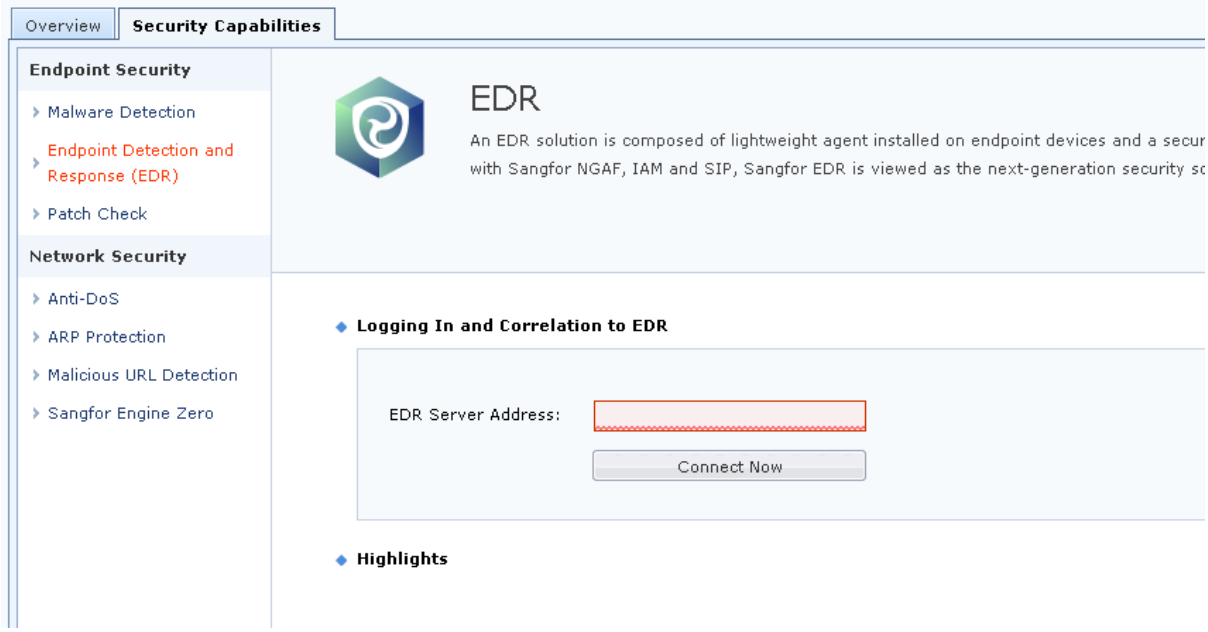
1. The terminal to be installed with the Agent requires port 443 to access the MGR for downloading the Agent program.

3.2.2.2 Internet Access Management (IAM) Correlation Deployment

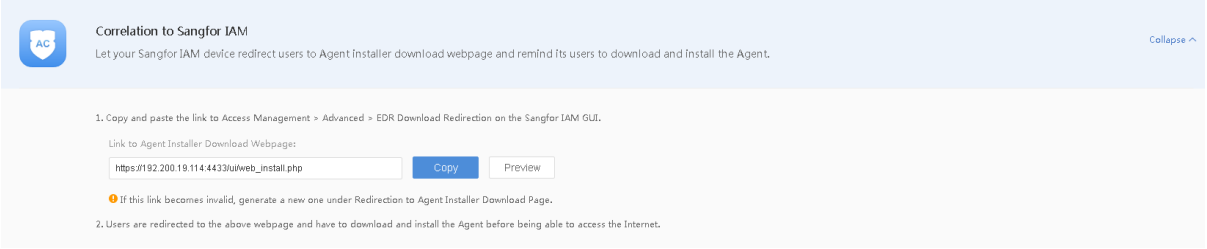
Agent deployment can be correlated with the Internet Access Management (IAM) system of Sangfor. If a terminal has not been installed with the Agent of Endpoint Secure and requires Internet access, the Endpoint Secure promotion configuration of the IAM system will redirect the terminal to the deployment notice webpage.

- Log in to the Endpoint Secure console. Select [System] - [Correlation], and view the connected IAM devices.

- If no IAM device is connected. Login to IAM WebUI then select [Security] – [Security Cappbilities] – [Security Capabilities] – [Endpoint Detection and Response (EDR)].



  - Select **[System] - [Client Enforcement] - [Correlation to Sangfor IAM]**.

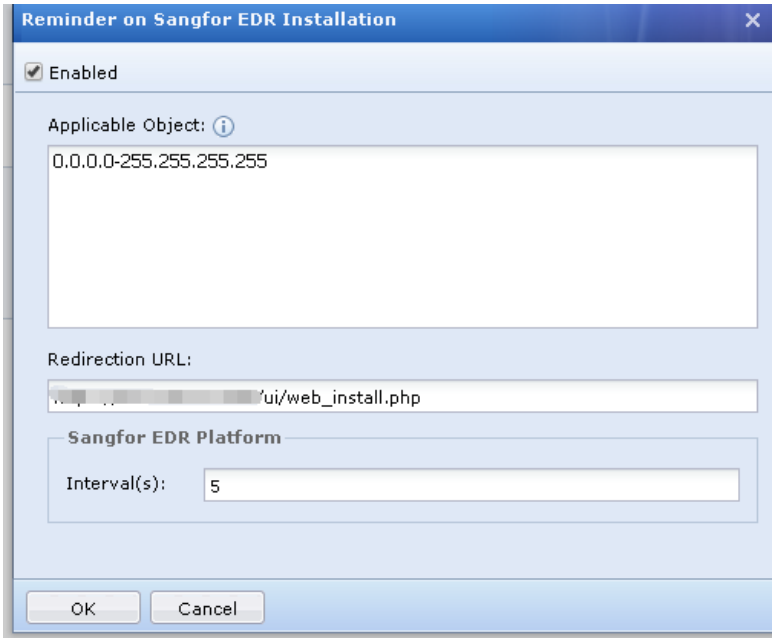


- Log in to the IAM device console connected with MGR. Select **[Security Capabilitiies] - [Security Capabilities] - [Endpoint Detection and Response (EDR)]** for parameter settings.

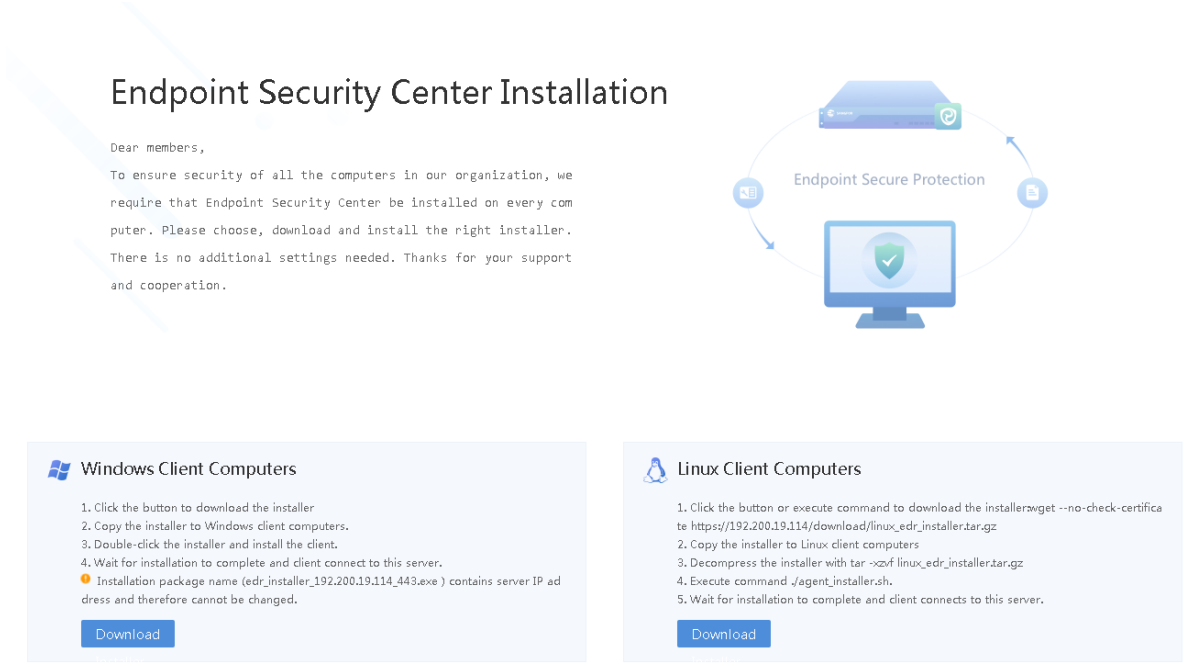
  1) In the Applicable Scope of the Policy text box, fill in the terminal IP address or IP address segment for promotion configuration.

  2) In the Redirect Address text box, fill in the link generated in step 3.

  3) In the Push Time Interval text box, specify a value, which indicates the time interval between two successive pushes of the download webpage. During this time interval, terminals can **access the Internet normally.**



- On the terminal to be deployed, click the browser to access the Internet.

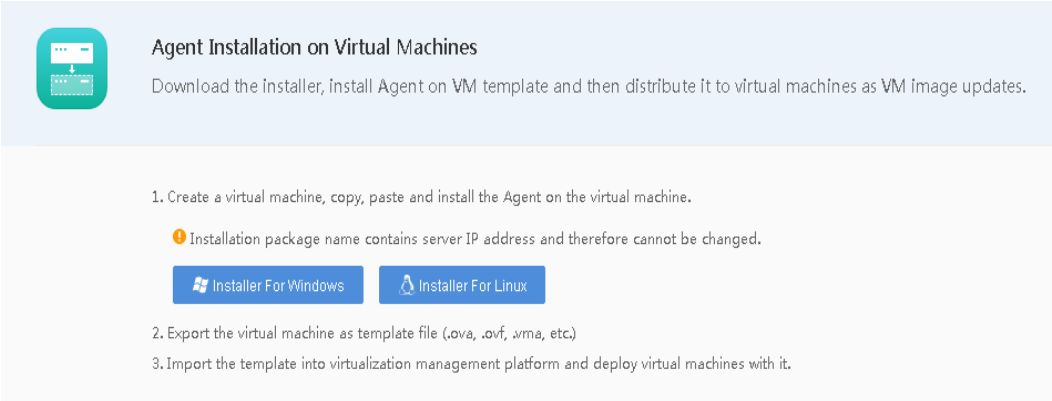


- Download the Agent installation package. For details, see Section 3.2.1 Downloading and Deploying the Installation Package.

1. **Minimum IAM version requirement: AC12.0.14**

3.2.2.3 Virtual Machine Template-based Deployment

This deployment model applies to virtualization scenarios. The administrator performs the mirror deployment of virtual machines using a virtual machine template on the virtualization platform.

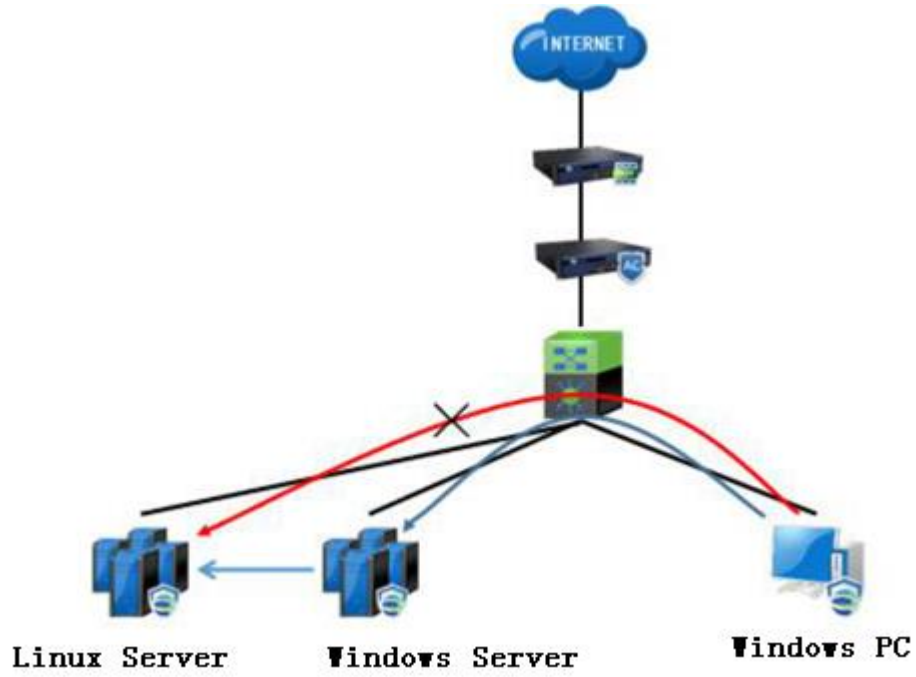


- Create a new virtual machine. Install and deploy the Agent on the virtual machine by using the Agent installation package.
- Export the virtual machine as a mirror file in ova, ovf, vma or other formats. Import the template file (mirror file) on the virtualization platform, and deploy other virtual machines.
- Alternatively, convert a virtual machine to a template that can be used to derive virtual machines in batches on the platform when new virtual machines are required.

1. The procedure for downloading the Agent program in this section is the same as that in Section 3.2.1.

Chapter 4: Micro-isolation Scenario

In the routine office scenario, office terminals have the permission to access the webserver of OA, and the webmserver has the permission to access the database server, while office terminals do not have the permission to access the database server.



Instructions:

A PC serving as Terminal A (installed with or without the Agent), a Windows server serving as Terminal B, and a Linux server serving as Terminal C (installed with the Agent and keeping normal communication with the MGR)

Network interworking is normal between Terminals A, B, and C. You can run the ping command to verify it.

Expected Result:

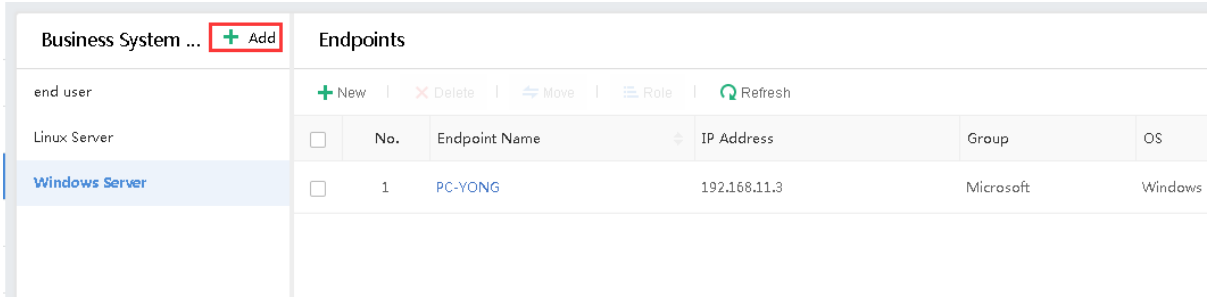
Terminal A (PC) can access port 80 of Windows Server but cannot access other ports.

Terminal A (PC) cannot access Linux Server.

Terminal B can access port 3306 of Terminal C but cannot access other ports.

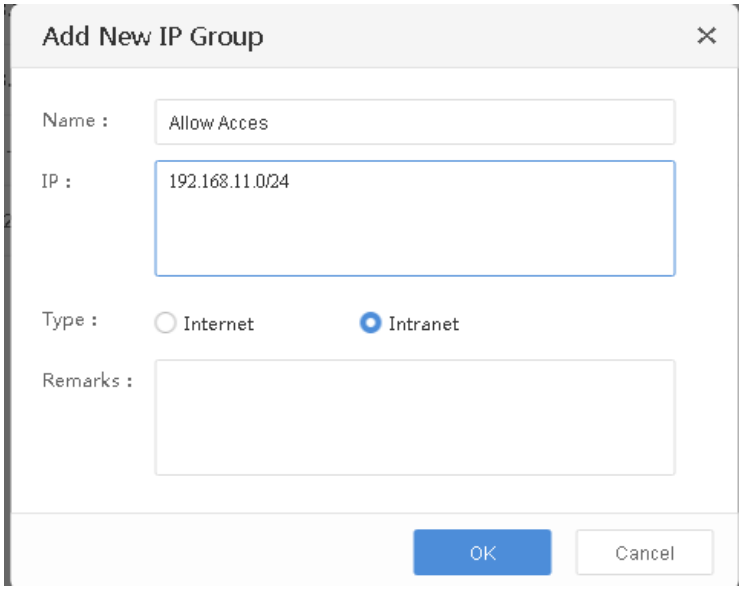
Configuration Steps:

- Log in to the MGR. Select [Micro-Segmentation] - [Business System] and click Add to create a new business system group. Add the Terminal B server to the OA Windows Server. Add the Terminal C to the Linux server system.



- Select [Micro-Segmentation] - [IP Group]. Set the IP address range for the office terminals that can access the web

- Server, with the name defined as "Allow Access". Note that the specified IP address range should include the IP address of Terminal A. Select Intranet.



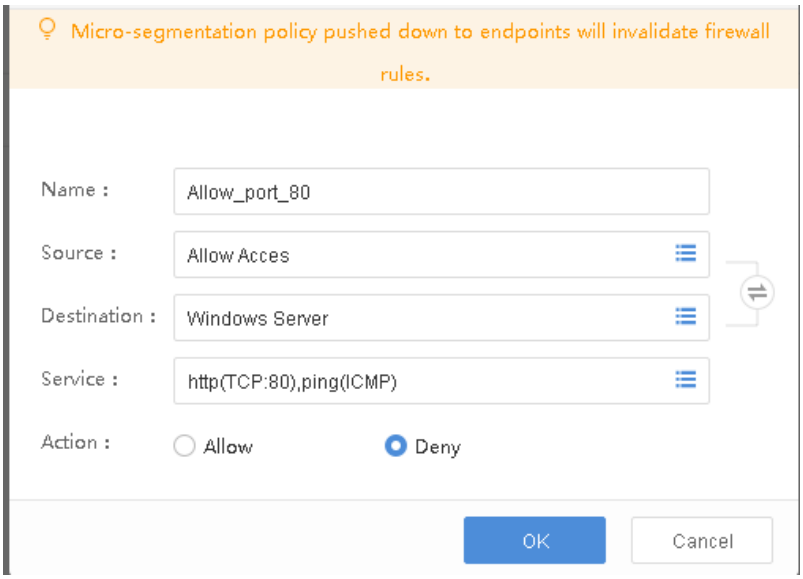
- Select [Micro-Segmentation] - [Service]. You can see that port 80 of the webserver is a built-in service.

No.	Service Name	Protocol	Port	Traffic Type
1	http	TCP	80	Business Traffic

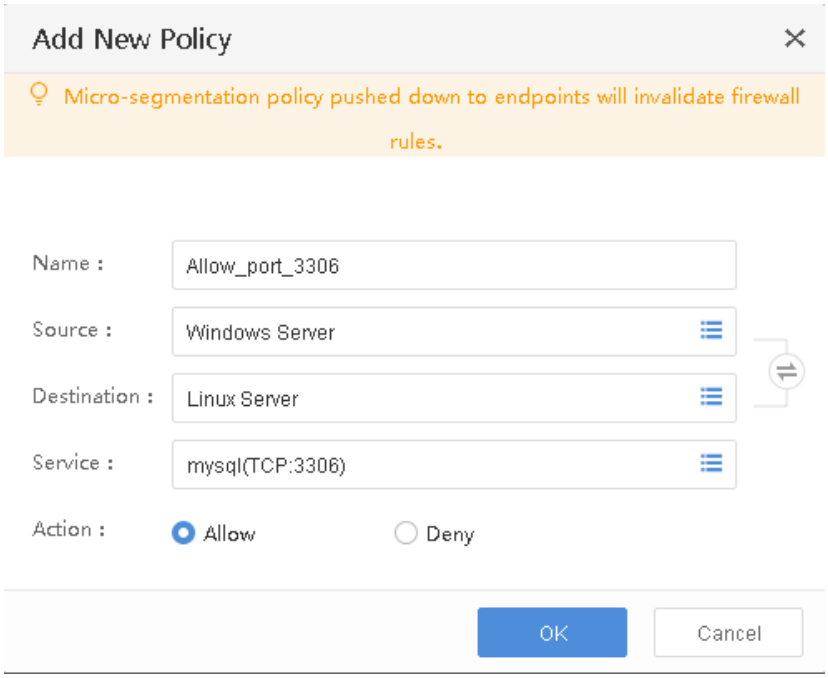
- The MYSQL database uses port 3306 as a built-in service for testing.

No.	Service Name	Protocol	Port	Traffic Type
1	mysql	TCP	3306	Business Traffic

- Configure [Micro-Segmentation Policy] with the above configuration items specified. Select **Allow** so that the Terminal A has the permission to access Terminal B



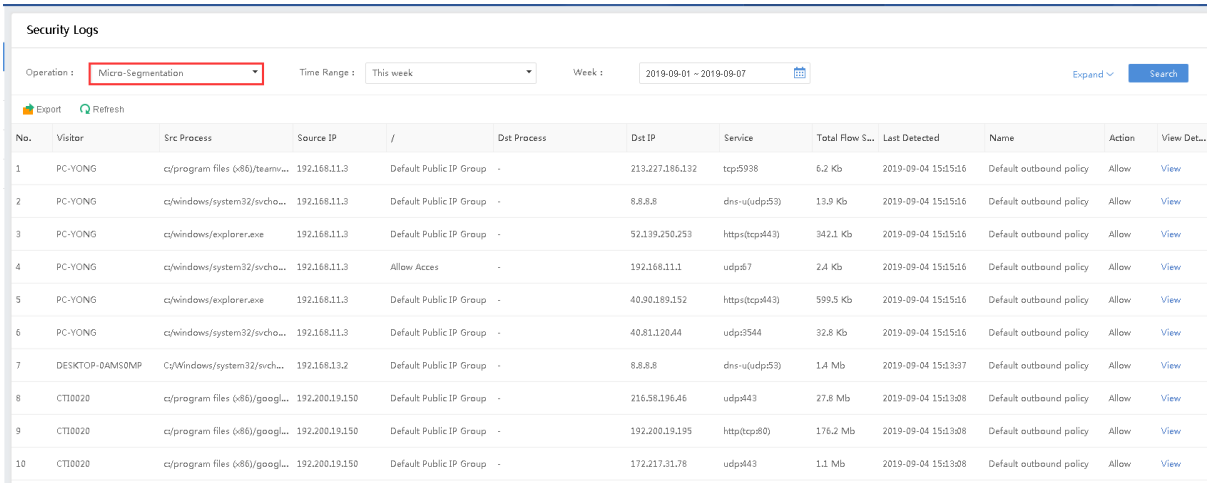
- Select **Allow** in the following dialog box so that the Terminal B has the permission to access port 3306 of the Terminal C.



- View the delivery status of policies.

Policy-matching priority: added allow policy > added reject policy > default policy

- Select **[Log] - [Security Log]**. Select **Micro-Segmentation** in **Log Type** to view the micro-Segmenttaion log.

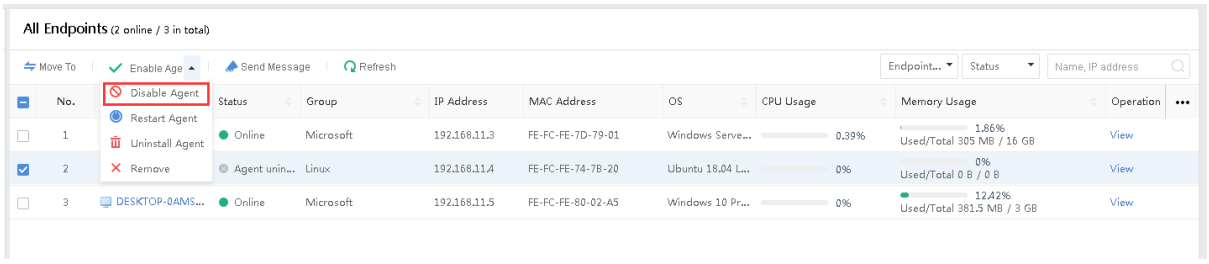


Chapter 5 How to Determine Whether Agent Impacts System Services

Perform the following steps to troubleshoot the terminals if terminal system services are impacted after the Agent is installed:

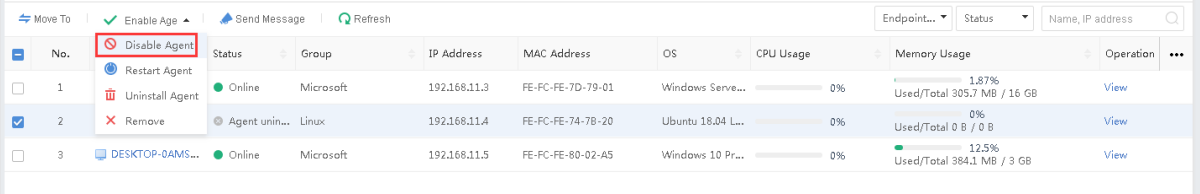
1. Log in to the MGR. Display the [Micro-Segmentation] page and check whether the corresponding terminals have enabled the micro-segmentation policies. If so, remove or disable all the micro-segmentation policies of terminals from the business system, and then check whether the terminal system services return to normal. If the services are still abnormal, go to Step 2. If the services return to normal, check whether the micro-segmentation policies sent to the terminals block some ports or flows that may affect the normal operations of terminal services.

2. Log in to the MGR. Display the [Endpoint] page, select the corresponding terminals, and disable the Agent function for the selected terminals. Then check the terminal system services. If the services are still abnormal, skip to Step 3. If the services return to normal, skip to Step 4.



3. If the terminal system services are still abnormal after the Agent is disabled, the Agent process is not the cause for abnormality. You are not advised to rush to uninstall the Agent. You may contact the Endpoint Secure technical support or call the service hotline (+6012-7117129) of Sangfor for troubleshooting. If the terminal system fails to work normally, you are advised to firstly back up the logs in the Agent installation

directory\Program Files\Sangfor\EDR\agent\var\, and then uninstall the Agent. After that, restart your computer. If the terminal system services return to normal after your computer is restarted, you may contact the Endpoint Secure technical support or call the service hotline (+6012-7117129) of Sangfor for troubleshooting. If the terminal system services are still abnormal after the Agent is uninstalled and the computer is restarted, it indicates that the Agent is not the cause for abnormality.



4. If the terminal system services return to normal after the Agent is disabled, you are not advised to rush to uninstall the Agent. You may contact the Endpoint Secure technical support or call the service hotline (+6012-7117129) of Sangfor for troubleshooting. If the Agent has to be uninstalled from the terminal, you are advised to firstly back up the logs in the Agent installation directory\Program Files\sangfor\EDR\agent\var\, and then uninstall the Agent. You may contact the Endpoint Secure technical support or call the service hotline (+6012-7117129) of Sangfor to submit the logs to R&D personnel of Sangfor for further analysis and troubleshooting.

SANGFOR