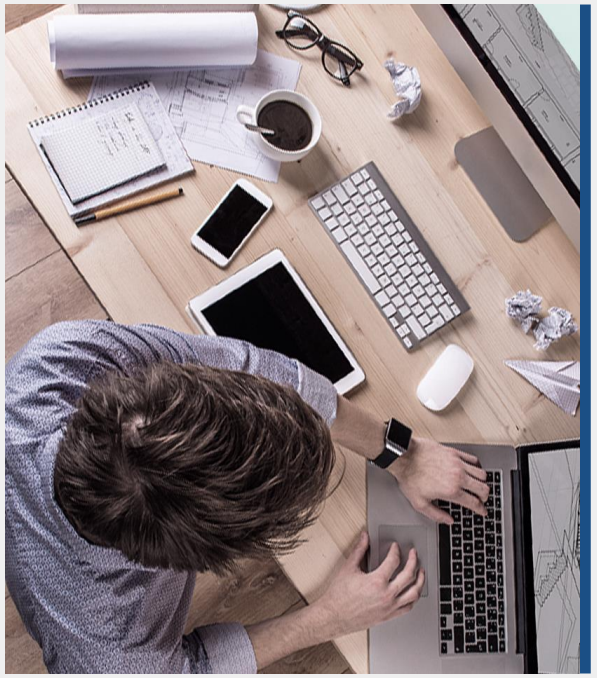
Sangfor Endpoint Secure 3.2.22

Chapter 2 Installation and Deployment

SANGFOR 深信服科技 | SANGFOR SECURITY 深信服智安全



1. Product Architecture
2. Deployment Preparation
3. Management Platform Deployment
4. Agent Deployment
5. Agent Uninstallation

1. Product Architecture

SANGFOR
深信服科技

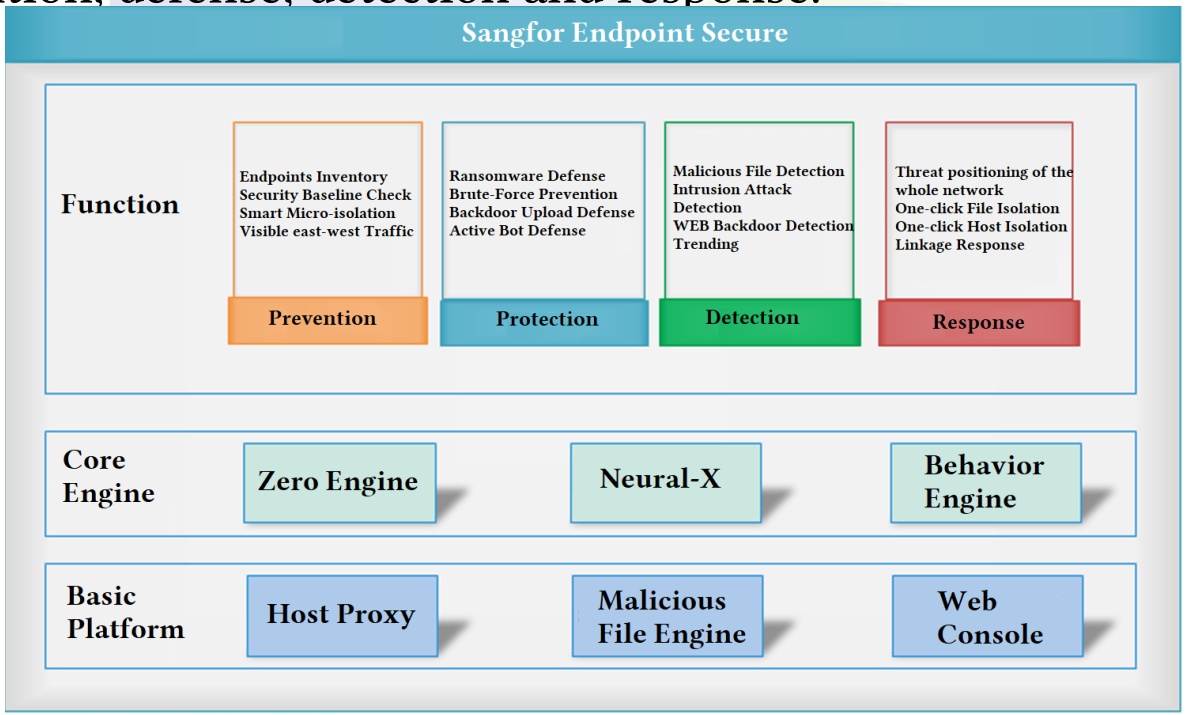
General Architecture

Endpoint Secure is divided into three layers in terms of system architecture: the basic platform layer, the core engine layer and the functional presentation layer.

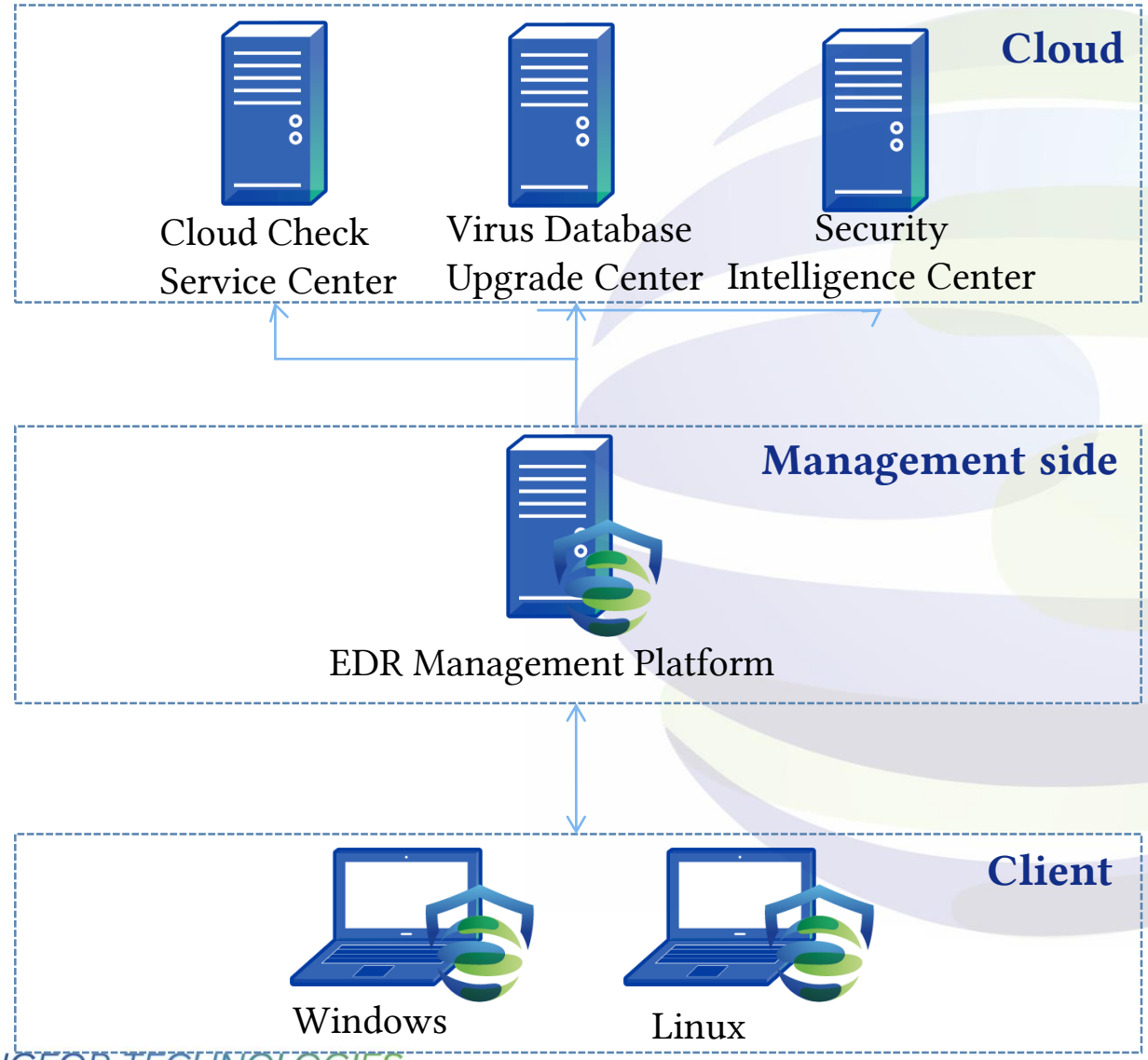
Basic platform layer: responsible for providing centralized control, cloud checking and the basic capability of host agent function.

Core engine layer: responsible for providing virus detection, threat analysis and behavior detection capabilities.

Function presentation layer: It provides a comprehensive security protection system from four aspects, including prevention, defense, detection and response.



Deployment Structure



Endpoint Secure is divided into cloud, management (MGR) and client (Agent) in terms of deployment structure.

Cloud: including virus database upgrade, cloud-based check and kill service center, and security intelligence center.
Console: Responsible for maintaining and managing all Agent clients.
Client: Software installed on the terminal to provide security to the terminal.

2. Deployment Preparation

SANGFOR
深信服科技

Reflections

Scenario: The company leader gives you a software, tells you that this software can achieve certain functions, you need to install on as soon as possible, put into use

Think: what do you need to know to install

Deployment Preparation

Before installing and deploying Endpoint Secure, you need to do

confirmation system compatibility,

confirmation hardware resource environment,

confirmation network connectivity confirmation

System compatibility confirmation

Endpoint Secure

MGR

Browser	Mgr Console
IE10	Y
IE11	Y
Edge	Y
Chrome	Y
Firefox	Y
Safari	Y
360	Y
Search Dog	Y
Operating system (64-bit)	Mgr Console
Centos7+	Y
Ubntul16+	Y

Agent Client

Operating system type	Operating System
User PC terminal	win vista x86
	win vista x64
	win xpSP3
	win7 x86
	win7 x86
	win8 x86
	win8 x64
	win8.1 x86
	win8.1 x64
	win10 x86
	win10 x64
windows server terminal	win server 2003sp2 x86
	win server 2003sp2 x64
	win server 2008sp2 x86
	win server 2008sp2 x64
	win server 2008R2 x64
	win server 2012 x64
	win server 2012R2 X64
	win server 2016 x64
	win server 2019 X64

Operating system type	Operating System
linux server terminal	Debian 6 x86
	Debian 6 x64
	Debian 7 x86
	Debian 7 x64
	Debian 8 x86
	Debian 8 x64
	Debian 9 x86
	Debian 9 x64
	RHEL 5 x86
	RHEL 5 x64
	RHEL 6 x86
	RHEL 6 x64
	RHEL 7 x64
	suse 11
	suse 12
	suse 15
	oracle Linux 5 x86
	oracle Linux 5 x64
	oracle Linux 6 x86
	oracle Linux 6 x64
	oracle Linux 7 x64

System compatibility confirmation

Agent Client

Operating system type	Operating System
linux server terminal	Centos5 x86
	Centos5 x64
	Centos6 x86
	Centos6 x64
	Centos7 x64
	Ubuntu 10 x86
	Ubuntu 10 x64
	Ubuntu 11 x86
	Ubuntu 11 x64
	Ubuntu 12 x86
	Ubuntu 12 x64
	Ubuntu 13 x86
	Ubuntu 13 x64
	Ubuntu 14 x86
	Ubuntu 14 x64
	Ubuntu 16 x86
	Ubuntu 16 x64
	Ubuntu 17 x64
	Ubuntu 18 x64

Operating system type	Operating System
Homemade	Neokylin 5.0x86 (client version)
	Neokylin 6.0x86 (client version)
	Neokylin 7.0x86 (client version)
	Galaxy Kirin 4.0x64 (client version)
	Ubiquitous 18.0

Hardware resource environment confirmation

Both the physical and virtualized environments need to meet the following hardware resource requirements

Number of terminals	CPU (Pentium Dual Core)	Memory	Disks
1 to 50	2 cores	2G	100G
50 to 500	4 cores	4G	250G
500 to 2000	4 cores	8G	500G
Note: If the MGR server is used as a vulnerability patch server, the recommended disk size configuration is 1T			

Network connectivity confirmation

Network connectivity between client and management platform

The client (Agent) uses TCP:443, TCP:8083, and TCP:54120 ports to communicate with the management platform (MGR). Ensure port connectivity.

Port 443: https service port, used for management platform page access, upgrade package patch package download, remote script download.

Port 8083: IPC communication port for end and MGR communication.

Port 54120: Escape port, emergency situation and Agent communication port. Complete Agent restart, uninstall and script execution command issuance.

Network connectivity confirmation

SANGFOR

Management platform and cloud-based network connectivity

(Neural-X) Vulnerability patch related: https://upd.sangfor.com.cn

(Cloud Brain) Access to Cloud Brain License: https://auth.sangfor.com.cn

(Cloud Brain) Cloud Check Server: https://analysis.sangfor.com.cn

(Cloud Brain) Cloud Security Program: https://clt.sangfor.com.cn

(CDN) Vulnerability patches, rules, and virus libraries at http://download.sangfor.com.cn

3. Management Platform Deployment

SANGFOR
深信服科技

Management Platform Deployment

MGR Management Platform Deployment.

Software Deployment

- ISO image deployment
- OVA Template Deployment

ISO image deployment

ISO image deployment is based on CentOS system image with embedded MGR installation package, i.e. MGR is automatically deployed after installing the ISO.

Advantage.

Simplified installation steps. The ISO is customized based on the latest CentOS package with embedded mgr installation package, which can be installed only once, eliminating the need for the original mgr separate deployment process.

Higher security. The ISO has undergone multiple penetration scans prior to release, installing the latest system patches to eliminate security issues introduced by customers using vulnerable third-party systems (older, unmaintained Linux systems).Both physical and virtualized environments support installation

OVA Template Deployment

OVA template deployment is based on CentOS installation image with embedded MGR installation package, which is automatically deployed in virtualized environment by importing OVA template.

Advantage.

- Simplified installation steps. This OVA template is customized based on the latest CentOS package with embedded MGR installation package, which can be installed in just one time, eliminating the need for the original MGR separate deployment process.

- Higher security. The systems in this template have been scanned for multiple penetrations and installed with the latest system patches prior to release, eliminating security issues introduced by customers using vulnerable third-party systems (older, unmaintained Linux systems).

4. Agent Deployment

SANGFOR
深信服科技

Client Agent Deployment

Deployment methods (5 types): installation package deployment, web promotion deployment, IAM(IAG) correlated deployment, virtual machine template deployment, domain control scenario deployment

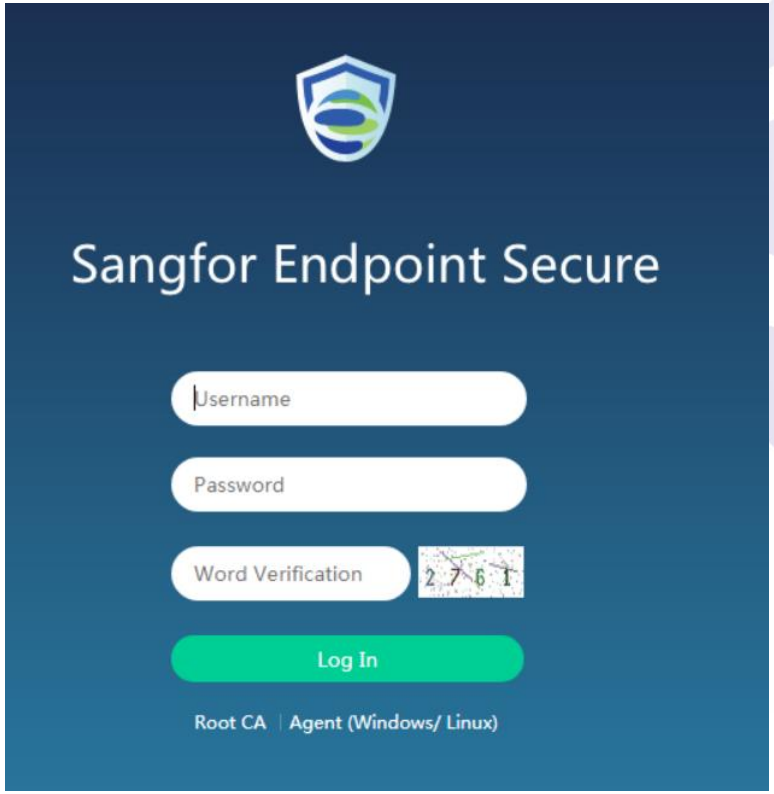
Special Note: Endpoint Secure Agent is fully compatible with the following security software. Computers with security software other than the following are supported to install Endpoint Secure Agent in compatibility mode, but the real-time file monitoring function will not work properly.

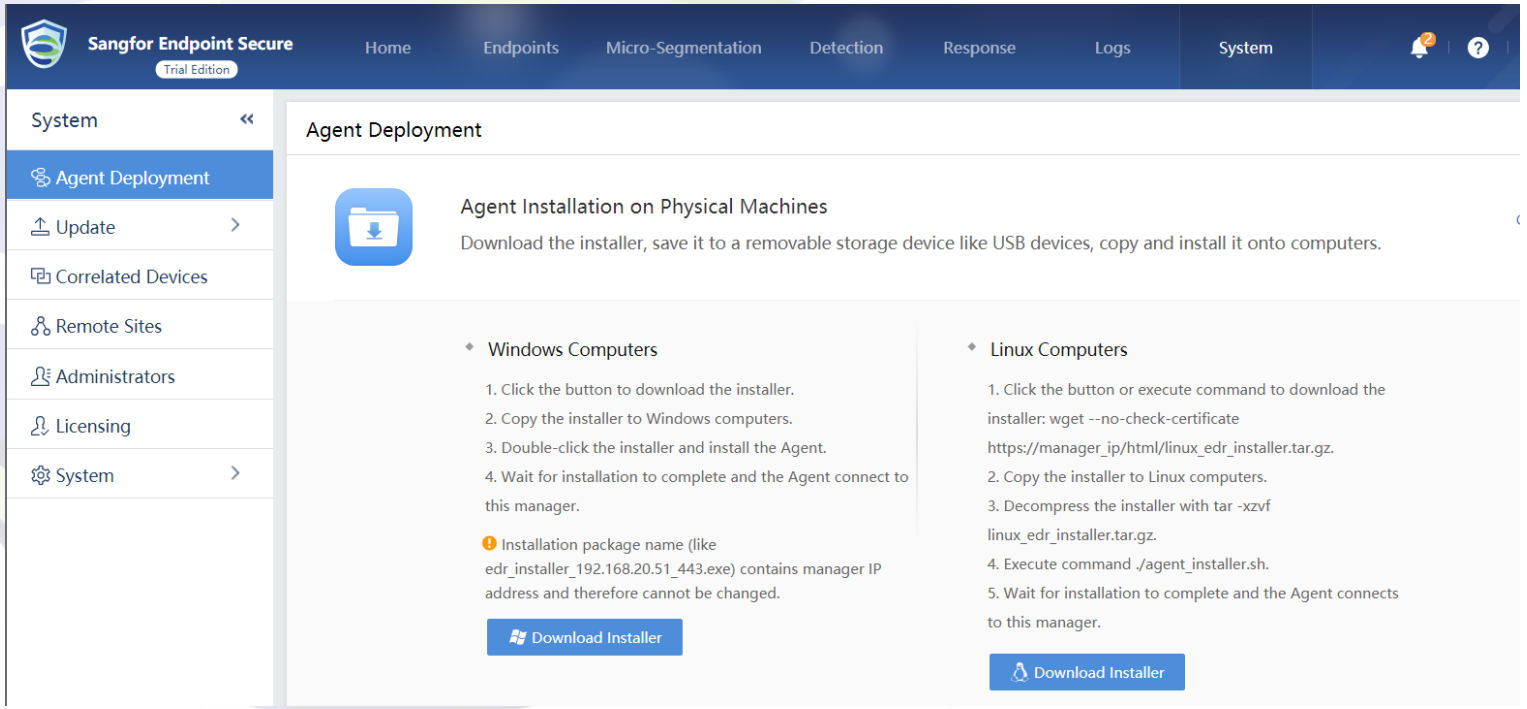
Endpoint Secure Agent supports the installation and use of 10 security software compatible with Kingsoft Antivirus, Flint (Personal Edition), QQ Butler, Rising Star Personal Edition, Qi'anxin Tianquan, 360 Antivirus, 360 Security Guard, Trend Deep Security, Trend office scan, Symantec

Installation package deployment

Applicable scenarios.

The administrator downloads the agent installation package and imports it into the terminal for installation and deployment via mobile media such as USB flash drive, the most direct deployment method

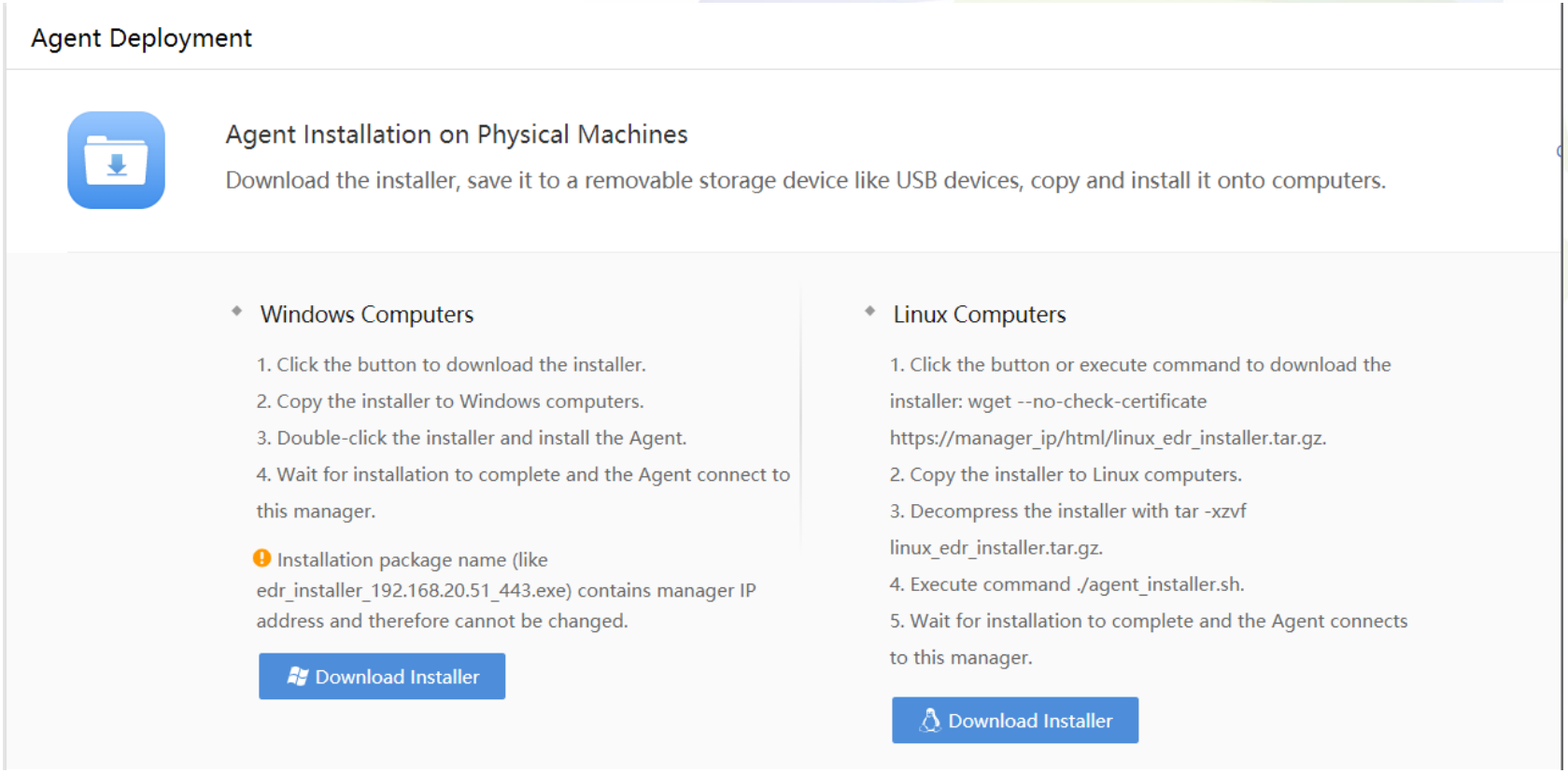




Web Promotion Deployment

Applicable scenarios.

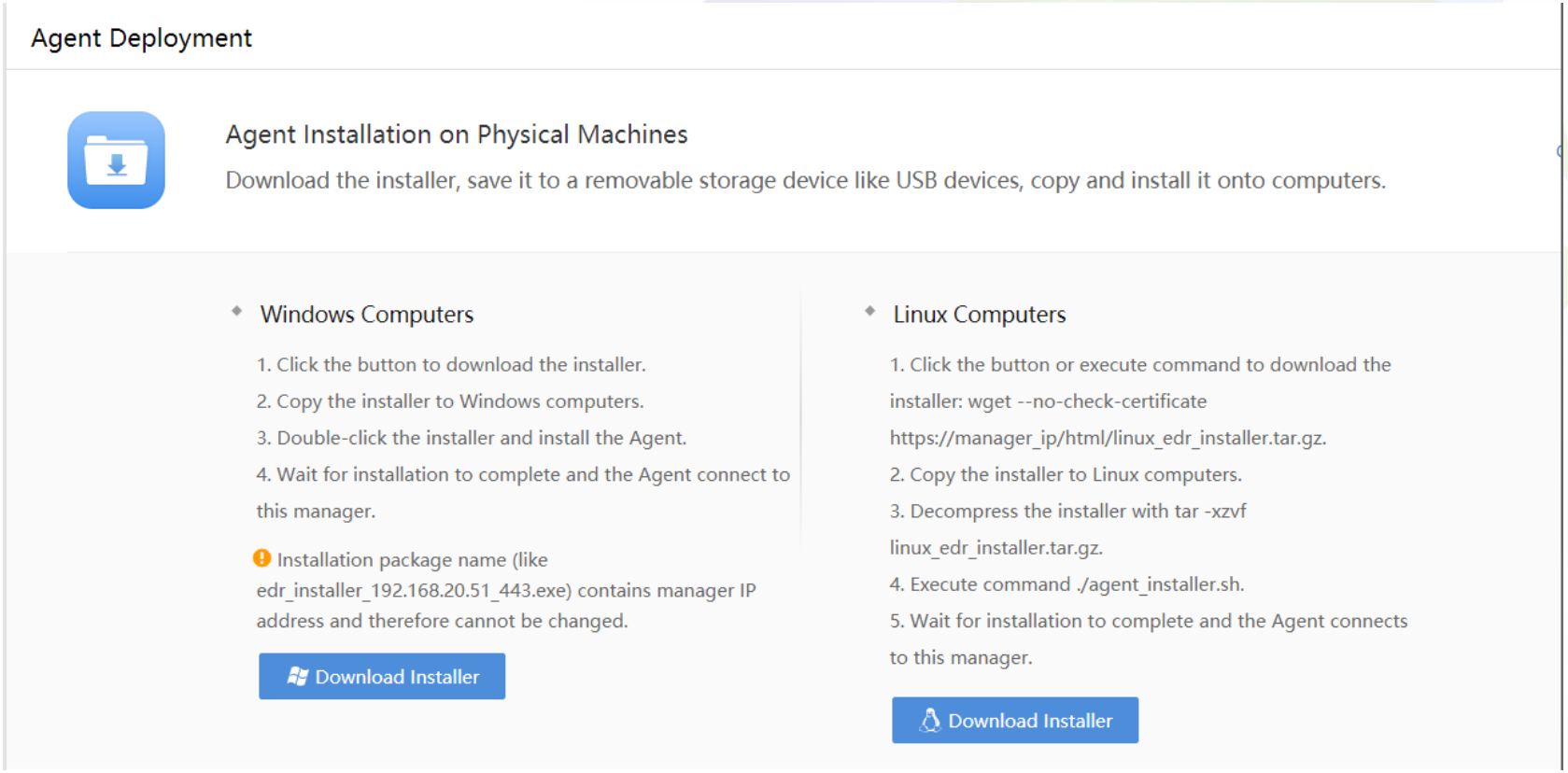
The administrator will publish the web page of the deployment notice, send the link of the publishing page to the terminal via email, OA, etc., and the end user will download the agent installation package for installation and deployment.



IAM(IAG) correlated Deployment

Applicable scenarios.

For customers who have purchased IAM(IAG) at the same time, Endpoint Secure and IAM(IAG) are linked, and when users open the web page, they are redirected by IAM(IAG) to the Agent installation page as shown below, until the Agent is successfully installed on the terminal.



Virtual Machine Template Deployment

Applicable scenarios.

Suitable for desktop office environments or virtualized environments, administrators can prepare virtual machine templates with Endpoint Secure Agent in advance in the virtualization platform, and generate other virtual machines as needed.

Domain Control Scenario Deployment

Applicable scenarios.

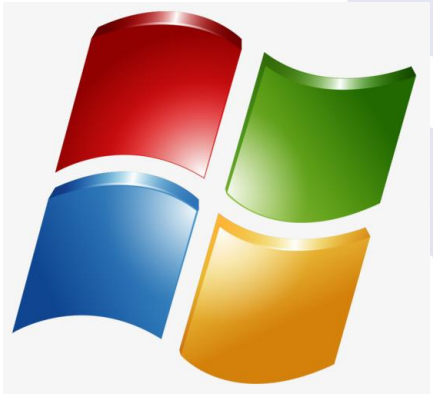
The terminal is unified managed by Windows AD domain control and can deploy software installation package in bulk for silent installation through domain control group policy.

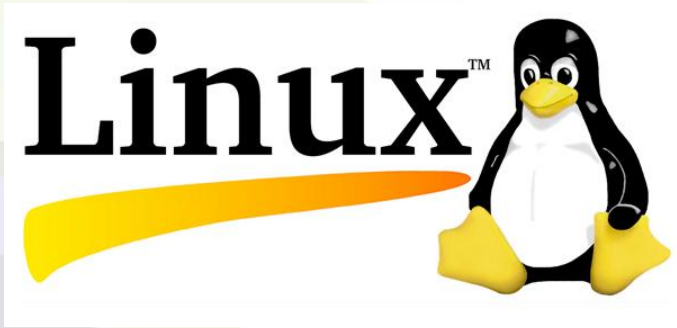
5. Agent Uninstallation

SANGFOR
深信服科技

Client Agent Uninstallation

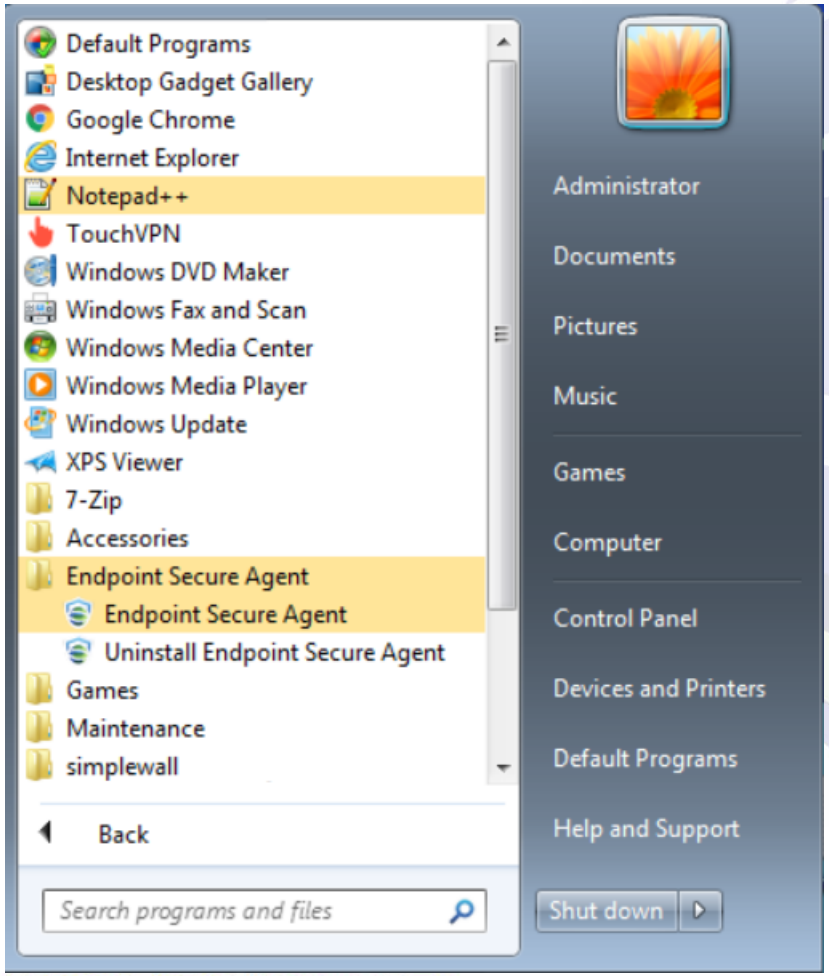
Agent uninstallation includes Windows client uninstallation and Linux client uninstallation

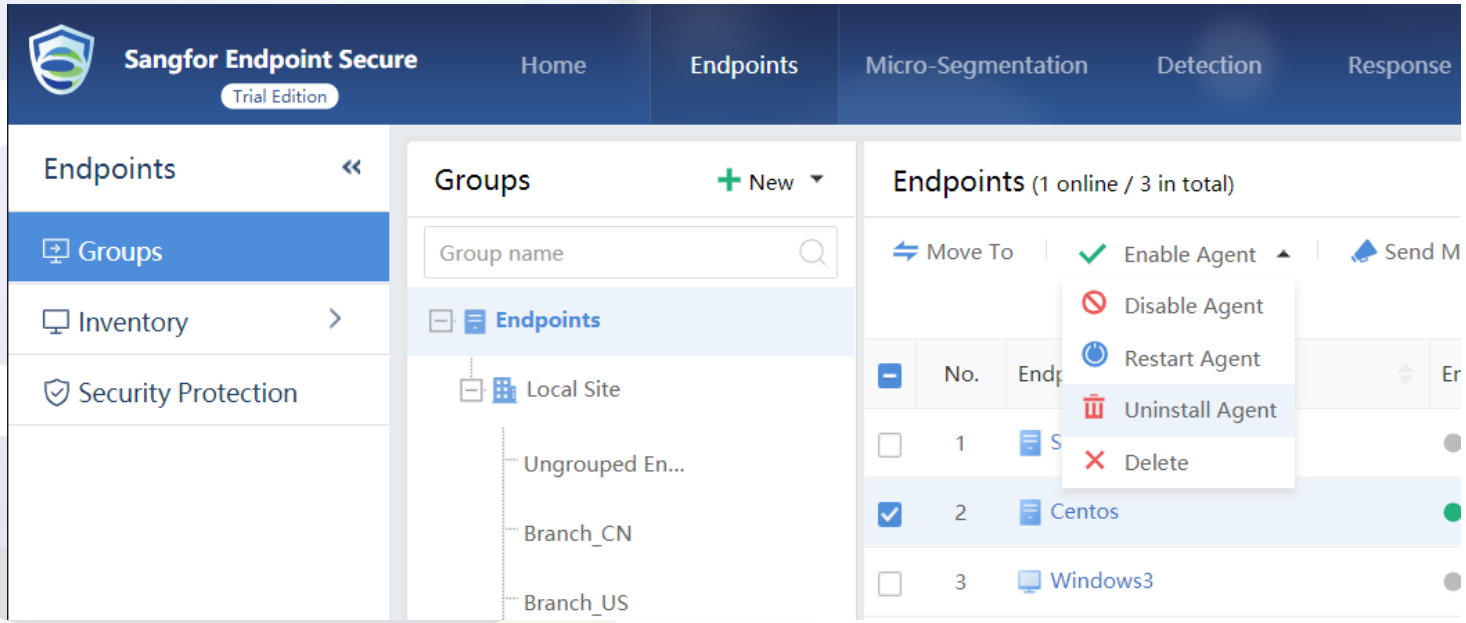




Windows client uninstall

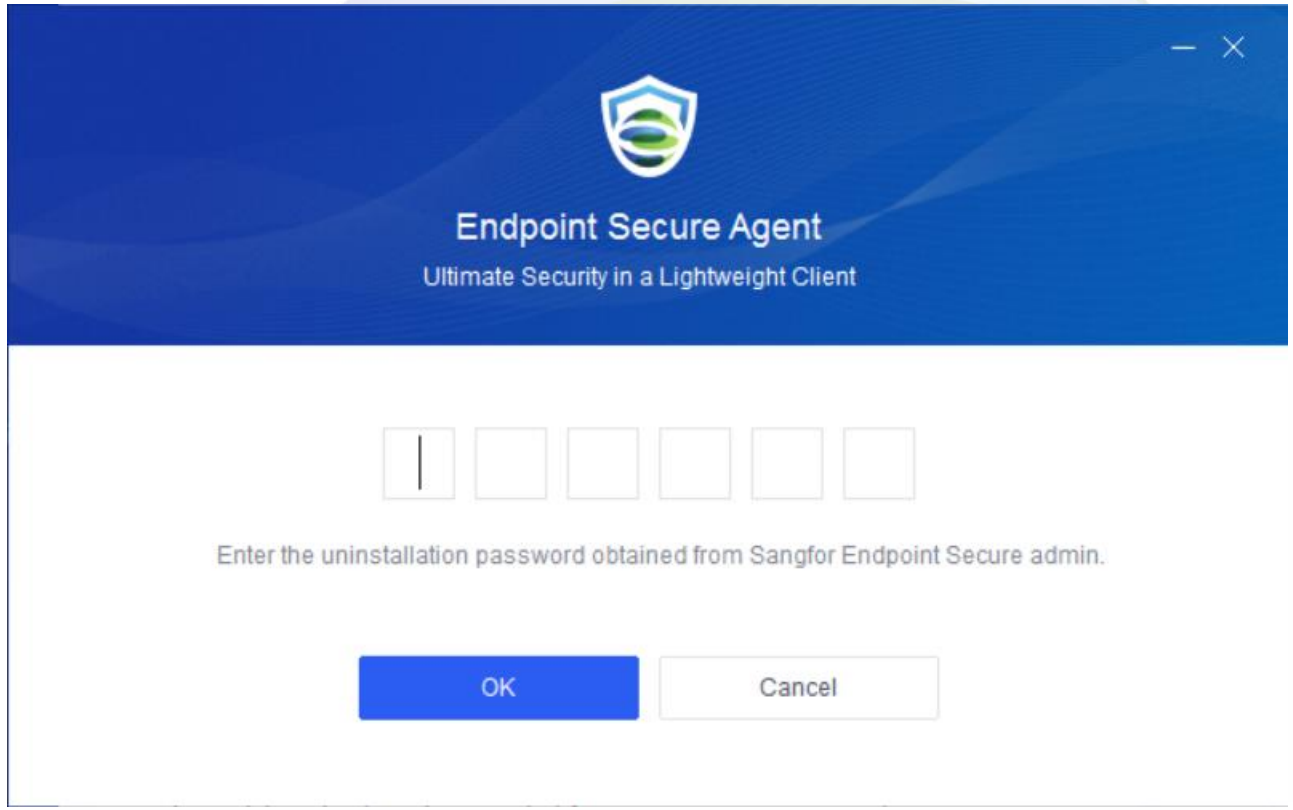
There are two ways to uninstall the Windows client: terminal uninstallation and MGR management platform uninstallation





Windows client uninstall

In order to prevent the terminal from being unsecured due to malicious uninstallation of the client, it is necessary to obtain the anti-uninstallation password when uninstalling the Agent from the terminal (the anti-uninstallation password is set by the administrator in the management platform).



Linux client uninstallation

There are two ways to uninstall the Linux client: terminal uninstallation, MGR management platform uninstallation

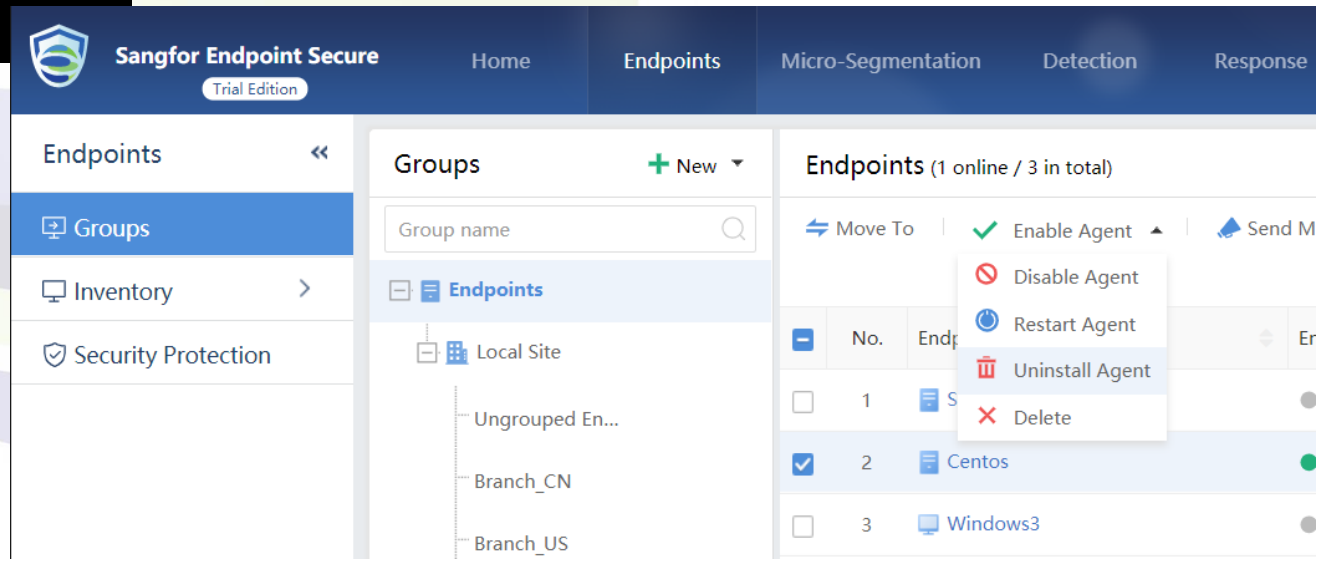
```
[root@hbz ~]# cd /sangfor/edr/agent/bin/
[root@hbz bin]# ls
abs_deployer        edr_agent              eps_uninstall.sh  isolate_area_set    sfavsrv              stop_pre.sh
abs_monitor         edr_monitor            epsxtest          isolate_area_set.l  sfcachecleaner       uninstall_agent_ipc.l
abs_monitor.lock    edr_sec_plan           flux_app          lloader             sf_isolate_encry     webshell_first_scan_flag
agent_list          eps_app                get_appversion    luadbg              sfupdate             wfplog.l
agent_list.l        eps_delay_clean.sh     ipc_probe         post_script         sfupdatemgr
blscan.sh           eps_services           ipc_probe.l       resmon_export.sh    start_post.sh
cfg_dump.lua        eps_services_check.sh  ipc_proxy         rwini               start_pre.sh
cpulimit            eps_services_ctrl      iptables          setsyslog           stop_agent_ipc.l
download_limits.sh  eps_services_ctrl.lock iptables.l        sfavcfg.ini         stop_post.sh
[root@hbz bin]# ./eps_uninstall.sh
start uninstall eps agent
start stop eps_services
uninstall
edr stop success
start clean file
edr agent uninstall success!!

*********************************************
*                                           *
*  [Warning] Please reboot your server now. *
*                                           *
*********************************************

You have new mail in /var/spool/mail/root
[root@hbz bin]#
```

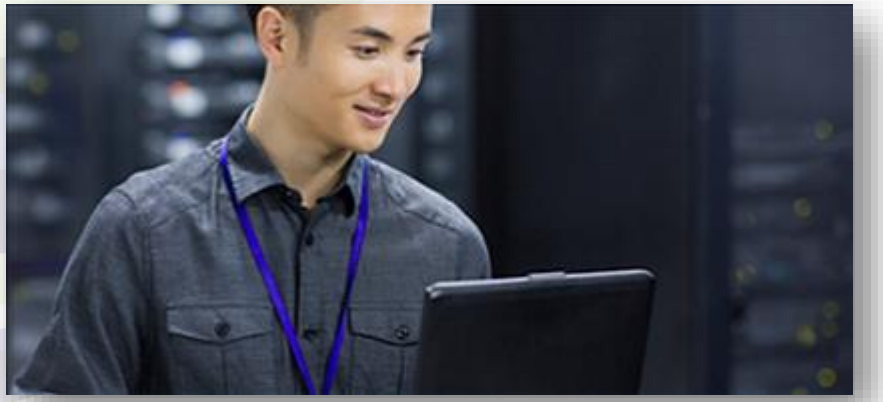
The Linux terminal is GUI-less.

Therefore, no uninstall password is required for uninstallation from the Linux terminal or from the MGR management platform.



Thank you !

tech.support@sangfor.com
community.sangfor.com



Sangfor Technologies (Headquarters)
Block A1, Nanshan iPark, No.1001
Xueyuan Road, Nanshan District,
Shenzhen, Guangdong Province,
P. R. China (518055)