



Sangfor Endpoint Secure

Network Access Address Requirements Guide

Product Version	General
Document Version	01
Released on	Nov. 11, 2024



Copyright © Sangfor Technologies 2024. All rights reserved.

Unless otherwise stated or authorized, Sangfor Technologies (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 required network access addresses for Sangfor Endpoint Secure.

Intended Audience

This document is intended for:

- All Users.

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
Nov. 11, 2024	This is the first release of this document.

Contents

Technical Support	1
Change Log	2
1 Addresses Requirements for On-Premises Endpoint Secure.....	4
2 Default Ports for On-Premises Endpoint Secure Manager	5
3 Addresses Requirements for SaaS Endpoint Secure	7

1 Addresses Requirements for On-Premises Endpoint Secure

For On-Premises Endpoint Secure, please allow the network traffic of the corresponding addresses according to the actual usage scenario.

It should be noted that when allowing the traffic of the corresponding domain name port, the upper-layer protocol must be allowed. For example, if only the traffic of port 443 is allowed but HTTPS traffic is not allowed, communication will fail.

Manager Type	Domain or IP	Port	Description
On Premises	license.sangfor.com	TCP: 443	Used to connect to the Online License Center to obtain license information.
	x.sangfor.com	TCP: 443	
	upd.sangfor.com	TCP: 443, 80	Used to obtain version information of rule databases such as vulnerability databases.
	download.sangfor.com	TCP: 443, 80	Used to obtain commonly used signature databases, such as vulnerability databases, virus databases, IOC, IOA, etc.
	update1.sangfor.net update2.sangfor.net update3.sangfor.net	TCP: 443, 80	Used to update SP patches.
	sp.sangfor.com sp1.sangfor.com sp2.sangfor.com sp3.sangfor.com	TCP: 443	
	device.sangfor.com	TCP: 443, 80	Used to connect to the Platform-X platform and integrate with SaaS Omni Command/Cyber Guardian.
	device.scloud.sangfor.com	TCP: 443, 80	
	dlauth.sangfor.com	TCP: 443	Used to integrate with SaaS Omni Command and upload data to the data lake.
	datalake.sangfor.com	TCP: 443	
	analysis.sangfor.com	TCP: 443	Cloud-based threat analysis
	intelligence.sangfor.com	TCP: 443	Used to obtain IOC popular

		threat information.
	download.windowsupdate.com	TCP: 443, 80 Microsoft's official server for storing operating system vulnerability patches.
	auth.sangfor.com	TCP: 443 When integrated with Neural-X, used for authentication of Neural-X.
	auth.sea.sangfor.com	TCP: 443 When integrated with Neural-X, used for authentication of Neural-X. This domain is only used when integrating with the Cyber Guardian platform.
	clt.sangfor.com	TCP: 443, 80 After you accept the Data Processing Agreement and End User License Agreement, Endpoint Secure will collect suspicious files to the cloud for analysis purposes, to provide better security services. We are committed to protecting your privacy.
	clt.sea.sangfor.com	TCP: 443, 80 After you accept the Data Processing Agreement and End User License Agreement, Endpoint Secure will collect suspicious files to the cloud for analysis purposes, to provide better security services. We are committed to protecting your privacy. This domain is only used when integrating with the Cyber Guardian platform.

2 Default Ports for On-Premises Endpoint Secure Manager

The following ports need to be allowed between the Endpoint Secure Agent and the on-premises manager:

Destination Address	Port	Functionality
---------------------	------	---------------

On-premises manager IP	TCP: 443	WebUI access.
	TCP: 4430	For Endpoint Secure Agent upgrade. 4430 is the default port in use, you can change it to other ports if needed.
	TCP: 8083	Endpoint Secure Agent's communication channel with the manager.
	TCP: 54120	
	TCP: 22345	For advanced troubleshooting. This port is closed by default, you can enable it via WebUI when needed.
	TCP: 4460	Only used when integrating with Sangfor Network Secure, Cyber Command, etc. If you do not have Sangfor Network Secure, Cyber Command yet, it is not necessary to allow this port.



The ports listed in the table above are the default fixed ports. The ports that the manager uses to connect to services such as cloud servers, proxy servers, mail servers, and syslog servers are random, and not fixed.

3 Addresses Requirements for SaaS Endpoint Secure

For SaaS Endpoint Secure, please allow the network traffic of the corresponding addresses according to the actual usage scenario.

It should be noted that when allowing traffic of the corresponding domain name port, the upper-layer protocol must be allowed. For example, if only the traffic of port 443 is allowed but HTTPS traffic is not allowed, communication will fail.

Manager Type	Domain or IP	Ports	Description
SaaS	upd.sangfor.com	TCP: 443, 80	Used to obtain version information of rule databases such as vulnerability databases.
	download.sangfor.com	TCP: 443, 80	Used to obtain commonly used signature databases, such as vulnerability databases, virus databases, IOC, IOA, etc.
	download.sangfor.com.cn	TCP: 443, 80	Used to obtain commonly used signature databases, such as vulnerability databases, virus databases, IOC, IOA, etc. This domain name is no longer used from Endpoint Secure 6.0.4 and later versions.
	edrsaas.sangfor.com	TCP: 8083, 443, 54120, 80	One of the addresses of SaaS Endpoint Secure Manager.
	edragent.sangfor.com	TCP: 8083, 443, 54120, 80	Used for communication between SaaS Endpoint Secure Manager and Agent.
	edrlinkage.sangfor.com	TCP: 443,	For SaaS Endpoint Secure integration with on-premises security appliances.
	13.94.16.103	ALL	The fixed address of SaaS Endpoint Secure, is used to provide syslog services.
	download.windowsupdate.com	TCP: 443, 80	Microsoft's official server for storing operating system

			vulnerability patches.
	update1.sangfor.net update2.sangfor.net update3.sangfor.net	TCP: 443, 80	
	sp.sangfor.com sp1.sangfor.com sp2.sangfor.com sp3.sangfor.com	TCP: 443	Used to update SP patches.



SANGFOR

