

kaspersky

Kaspersky SD-WAN

© 2024 AO Kaspersky Lab

Contents

[About Kaspersky SD-WAN](#)

[Distribution kit](#)

[Hardware and software requirements](#)

[Ensuring security](#)

[What's new](#)

[Architecture of the solution](#)

[Installing Kaspersky SD-WAN](#)

[Redundancy of central components of the solution](#)

[Logging in and out of the orchestrator web interface](#)

[Licensing of Kaspersky SD-WAN](#)

[About the End User License Agreement](#)

[About data provision](#)

[User interface of the solution](#)

[Setting and resetting the default page](#)

[Switching between light and dark modes of the orchestrator web interface](#)

[Changing the language of the orchestrator web interface](#)

[Managing solution component tables](#)

[Navigating to the orchestrator API](#)

[Managing users and their access permissions](#)

[Managing access permissions](#)

[Creating access permissions](#)

[Editing access permissions](#)

[Cloning access permissions](#)

[Removing an access permission](#)

[Managing LDAP connections](#)

[Creating an LDAP connection](#)

[Editing an LDAP connection](#)

[Changing the password of an LDAP connection](#)

[Deleting an LDAP connection](#)

[Managing users](#)

[Creating a user](#)

[Activating or blocking a user](#)

[Editing a user](#)

[Changing the password of a local user](#)

[Repeated two-factor authentication of a user](#)

[Deleting a user](#)

[Managing LDAP user groups](#)

[Creating an LDAP user group](#)

[Editing an LDAP user group](#)

[Deleting an LDAP user group](#)

[Enabling or disabling two-factor authentication for all users](#)

[Managing confirmation requests](#)

[Limiting the duration of a user session](#)

[Viewing and ending active user sessions](#)

[Managing resources of the organization](#)

[Managing domains](#)

[Creating a domain](#)

[Editing a domain](#)

[Deleting a domain](#)

[Managing data centers](#)

[Creating a data center](#)

[Editing a data center](#)

[Migrating a data center](#)

[Deleting a data center](#)

[Managing management subnets](#)

[Creating a management subnet](#)

[Editing a management subnet](#)

[Deleting a management subnet](#)

[Managing SD-WAN and SDN Controllers](#)

[Editing a Controller](#)

[Opening the controller configuration menu](#)

[Restarting a Controller](#)

[Downloading a file with Controller settings](#)

[Restoring a Controller](#)

[Deleting a Controller](#)

[Managing Controller properties](#)

[Описание изменяемых свойств контроллера](#)

[Editing a Controller property](#)

[Resetting controller properties to default values](#)

[Deleting planning values of Controller properties](#)

[Viewing information about Controller nodes](#)

[Managing a VIM](#)

[Configuring a VIM deployed on location](#)

[Configuring a VIM deployed on a uCPE device](#)

[Editing a VIM](#)

[Viewing VIM usage](#)

[Deleting a VIM](#)

[Multitenancy](#)

[Creating a tenant](#)

[Assigning a user to a tenant](#)

[Assigning a user group to a tenant](#)

[Assigning compute resources to a tenant](#)

[Assigning network service components to a tenant](#)

[Assigning a VIM to a tenant](#)

[Logging in to the tenant self-service portal](#)

[Editing a tenant](#)

[Deleting a tenant](#)

[Managing SD-WAN instances](#)

[Managing SD-WAN instance templates](#)

[Creating an SD-WAN instance template](#)

[Setting the default SD-WAN instance template](#)

[Selecting the number of Controller nodes](#)

[Adding a tenant to an SD-WAN instance template](#)

[Removing a tenant from an SD-WAN instance template](#)

[Deleting an SD-WAN instance template](#)

[Working with SD-WAN instances](#)

[Viewing the usage of an SD-WAN instance](#)

[Opening the configuration menu of the controller deployed for an SD-WAN instance](#)

[Opening the topology of the SD-WAN network service deployed for an instance](#)

[Viewing the topology of a deployed SD-WAN instance](#)

[Adding a tenant to an SD-WAN instance](#)

[Removing a tenant from an SD-WAN instance](#)

[Deleting an SD-WAN instance](#)

[Managing SD-WAN instance pools](#)

[Creating a pool of SD-WAN instances](#)

[Adding an SD-WAN instance to a pool](#)

[Removing an SD-WAN instance from a pool](#)

[Deleting a pool of SD-WAN instances](#)

[Managing CPE devices](#)

[About the interaction of the CPE device and the orchestrator](#)

[About the interaction of the CPE device and the Controller](#)

[Automatic registration of CPE \(ZTP\) devices](#)

[Repeated registration of CPE devices](#)

[Managing CPE templates](#)

[Creating a CPE template](#)

[Exporting a CPE template](#)

[Importing a CPE template](#)

[Cloning a CPE template](#)

[Exporting orchestrator and Controller connection settings and SD-WAN interfaces from a CPE template](#)

[Exporting network interfaces from a CPE template](#)

[Viewing the usage of a CPE template](#)

[Deleting a CPE template](#)

[Managing CPE devices](#)

[Adding a CPE device](#)

[Generating an URL with basic CPE device settings](#)

[Manually registering a CPE device](#)

[Unregistering a CPE device](#)

[Specifying the address of a CPE device](#)

[Enabling and disabling a CPE device](#)

[Restarting a CPE device](#)

[Shutting down a CPE device](#)

[Connecting to the CPE device console](#)

[Viewing the password of a CPE device](#)

[Exporting orchestrator and Controller connection settings and SD-WAN interfaces from a CPE device](#)

[Exporting network interfaces from a CPE device](#)

[Deleting CPE devices](#)

[Two-factor authentication of a CPE device](#)

[Managing certificates](#)

[Uploading a certificate using the orchestrator web interface](#)

[Manually installing certificates on CPE devices](#)

[Scenario: installing certificates on a CPE device with firmware version 23.07](#)

[Exporting a certificate](#)

- [Deleting certificates](#)
- [Automatically deleting and disabling CPE devices](#)
- [Grouping CPE devices using tags](#)
 - [Assigning a tag to CPE devices](#)
 - [Removing a CPE device tag](#)
- [Configuring logs on CPE devices](#)
- [Specifying NTP servers on CPE devices](#)
- [Managing modems](#)
- [Managing firmware](#)
 - [Uploading firmware to the orchestrator web interface](#)
 - [Updating firmware on manually selected CPE devices](#)
 - [Updating firmware on CPE devices with specific tags](#)
 - [Deleting firmware](#)
- [Additional configuration of CPE devices using scripts](#)
 - [Adding a script](#)
 - [Manually running scripts](#)
 - [Scheduling scripts](#)
 - [Editing a script](#)
 - [Deleting a script](#)
- [Managing network interfaces](#)
 - [Creating network interfaces](#)
 - [Creating a network interface with automatic assignment of an IP address via DHCP](#)
 - [Creating a network interface with a static IPv4 address](#)
 - [Creating a network interface with a static IPv6 address](#)
 - [Creating a network interface for connecting to an LTE network](#)
 - [Creating a network interface for connecting to a PPPoE server](#)
 - [Creating a network interface without an IP address](#)
 - [Editing a network interface](#)
 - [Disabling or enabling a network interface](#)
 - [Canceling the application of network interface settings to a CPE device](#)
 - [Deleting a network interface](#)
- [Configuring the connection of a CPE device to the orchestrator and controller](#)
- [Managing SD-WAN interfaces](#)
 - [About sending information about SD-WAN interfaces of the WAN type to the controller](#)
 - [About overriding the IP address and port for connecting an SD-WAN interface of the WAN type to the controller](#)
 - [Package fragmentation](#)
 - [Creating an SD-WAN interface of the WAN type](#)
 - [Editing an SD-WAN interface of the WAN type](#)
 - [Editing an SD-WAN interface of the LAN type](#)
 - [Disabling or enabling an SD-WAN interface](#)
 - [Deleting an SD-WAN interface of the WAN type](#)
- [Managing service interfaces](#)
 - [Creating a service interface](#)
 - [Creating an ACL interface](#)
 - [Viewing the usage of a service interface and an ACL interface](#)
 - [Deleting a service interface and an ACL interface](#)
- [Managing OpenFlow port groups](#)
 - [Creating an OpenFlow port group](#)

- [Editing an OpenFlow port group](#)
- [Deleting an OpenFlow port group](#)
- [Configuring a UNI for connecting CPE devices to network services](#)
 - [Managing UNI templates](#)
 - [Creating a UNI template](#)
 - [Deleting a UNI template](#)
 - [Managing UNIs](#)
 - [Creating a UNI](#)
 - [Viewing UNI usage](#)
 - [Editing a UNI](#)
 - [Deleting a UNI](#)
- [Adding or deleting a static route](#)
- [Filtering routes and traffic packets](#)
 - [Managing access control lists \(ACLs\)](#)
 - [Creating an access-control list](#)
 - [Editing an access control list](#)
 - [Deleting an access control list](#)
 - [Managing prefix lists](#)
 - [Creating a prefix list](#)
 - [Editing a prefix list](#)
 - [Deleting a prefix list](#)
 - [Managing route maps](#)
 - [Creating a route map](#)
 - [Editing a route map](#)
 - [Deleting a route map](#)
- [Route exchange over BGP](#)
 - [Basic BGP settings](#)
 - [Managing BGP peers](#)
 - [Creating a BGP peer](#)
 - [Editing a BGP peer](#)
 - [Deleting a BGP peer](#)
 - [Managing BGP peer groups](#)
 - [Creating a BGP peer group](#)
 - [Editing a BGP peer group](#)
 - [Deleting a BGP peer group](#)
- [Route exchange over OSPF](#)
 - [Basic OSPF settings](#)
 - [Managing OSPF areas](#)
 - [Creating an OSPF area](#)
 - [Editing an OSPF area](#)
 - [Deleting an OSPF area](#)
 - [Managing OSPF interfaces](#)
 - [Creating an OSPF interface](#)
 - [Editing an OSPF interface](#)
 - [Deleting an OSPF interface](#)
- [Using BFD to detect routing failures](#)
 - [Enabling or disabling the BFD protocol](#)
 - [Creating a BFD peer](#)

[Editing a BFD peer](#)

[Deleting a BFD peer](#)

[Ensuring high availability with VRRP](#)

[Enabling or disabling the VRRP protocol](#)

[Managing VRRP instances](#)

[Creating a VRRP instance](#)

[Editing a VRRP instance](#)

[Deleting a VRRP instance](#)

[Managing VRRP instance groups](#)

[Creating a group of VRRP instances](#)

[Editing a VRRP instance group](#)

[Deleting a VRRP instance group](#)

[Transmission of multicast traffic using PIM and IGMP protocols](#)

[Basic PIM settings](#)

[Managing multicast interfaces](#)

[Creating a multicast interface](#)

[Editing a multicast interface](#)

[Deleting a multicast interface](#)

[Managing virtual routing and forwarding \(VRF\) tables](#)

[Creating a virtual routing and forwarding table](#)

[Modifying the virtual routing and forwarding table](#)

[Deleting a virtual routing and forwarding table](#)

[Monitoring traffic packet information using the NetFlow protocol](#)

[Managing NetFlow templates](#)

[Creating a NetFlow template](#)

[Setting a default NetFlow template](#)

[Exporting a NetFlow template](#)

[Importing a NetFlow template](#)

[Cloning a NetFlow template](#)

[Viewing the usage of a NetFlow template](#)

[Deleting a NetFlow template](#)

[Basic NetFlow settings](#)

[Changing the NetFlow template of a CPE Device](#)

[Diagnosing a CPE device](#)

[Requesting diagnostic information](#)

[Enabling interactive mode](#)

[Running the ping utility](#)

[Running the traceroute utility](#)

[Running the tcpdump utility](#)

[Running the iperf utility](#)

[Running the sweep utility](#)

[Managing report files](#)

[Downloading a report file](#)

[Deleting a report file](#)

[IP address and subnet ranges for CPE devices](#)

[Managing IP address ranges](#)

[Creating an IP address range](#)

[Editing an IP address range](#)

[Viewing the usage of an IP address range](#)

[Deleting IP address ranges](#)

[Managing subnet ranges](#)

[Creating a subnet range](#)

[Editing a subnet range](#)

[Viewing the usage of a subnet range](#)

[Deleting subnet ranges](#)

[Managing the firewall](#)

[Managing firewall zones](#)

[Creating a firewall zone](#)

[Editing the name of the firewall common zone](#)

[Cloning a firewall common zone](#)

[Viewing the usage of a firewall common zone](#)

[Editing a firewall zone on a CPE device](#)

[Deleting a firewall zone](#)

[Managing firewall templates](#)

[Creating a firewall template](#)

[Setting the default firewall template](#)

[Exporting a firewall template](#)

[Importing a firewall template](#)

[Cloning a firewall template](#)

[Viewing the usage of a firewall template](#)

[Deleting a firewall template](#)

[Basic firewall settings](#)

[Configuring DPI marking](#)

[Managing firewall rules](#)

[Creating a firewall rule](#)

[Configuring the order of firewall rules](#)

[Editing a firewall rule](#)

[Enabling or disabling a firewall rule](#)

[Deleting a firewall rule](#)

[Managing IP sets](#)

[Creating an IP set](#)

[Editing an IP set](#)

[Disabling or enabling an IP set](#)

[Deleting an IP set](#)

[Managing forwarding](#)

[Creating a forwarding](#)

[Deleting a forwarding](#)

[Managing DNAT rules](#)

[Creating a DNAT rule](#)

[Configuring the order of DNAT rules](#)

[Editing a DNAT rule](#)

[Disabling or enabling a DNAT rule](#)

[Deleting a DNAT rule](#)

[Managing SNAT rules](#)

[Creating a SNAT rule](#)

[Configuring the order of SNAT rules](#)

[Editing a SNAT rule](#)

[Disabling or enabling a SNAT rule](#)

[Deleting a SNAT rule](#)

[Editing a CPE device firewall template](#)

[Managing network services and virtualization of network functions](#)

[Managing VNF and PNF packages](#)

[VNF descriptor](#)

[external_connections block](#)

[internal_connections block](#)

[virtual_links block](#)

[images block](#)

[configurations block](#)

[flavours block](#)

[scaling block](#)

[user_configurations block](#)

[backups block](#)

[Uploading a VNF or PNF package to the orchestrator web interface](#)

[Managing network service templates](#)

[Creating a network service template](#)

[Editing a network service template](#)

[Deleting a network service template](#)

[Managing network services](#)

[Creating a network service](#)

[Editing a network service](#)

[Deploying a network service](#)

[Checking the consistency of a network service](#)

[Redeploying a network service](#)

[Disabling or enabling auto-healing for a network service](#)

[Viewing the network service log](#)

[Deleting a network service](#)

[Specifying a brief description of a shared network service in the topology.](#)

[Managing virtual network functions in the topology.](#)

[Selecting the flavour of a virtual network function](#)

[Configuring external connection points of a virtual network function](#)

[Basic settings of a virtual network function](#)

[Hosting the virtual network function in a data center and on a uCPE device](#)

[Stopping or starting a virtual network function or a VDU that is part of it](#)

[Pausing or unpausing a virtual network function or a VDU that is part of it](#)

[Suspending or unsuspending a virtual network function or a VDU that is part of it](#)

[Soft rebooting a virtual network function or a VDU that is part of it](#)

[Hard rebooting of a virtual network function or a VDU that is part of it](#)

[Redeploying a virtual network function or a VDU that is part of it](#)

[Auto-healing a virtual network function or a VDU that is part of it](#)

[Managing VDU snapshots](#)

[Creating a VDU snapshot](#)

[Restoring VDU settings using a snapshot](#)

[Editing a VDU snapshot](#)

[Deleting a VDU snapshot](#)

[Managing physical network functions in the topology.](#)

[Selecting the flavour of a physical network function](#)

[Basic settings of a physical network function](#)

[Configuring a P2P service in the topology.](#)

[Configuring a P2M service in the topology.](#)

[Configuring a M2M service in the topology.](#)

[Configuring a shared network \(OS 2 SHARED\) in the topology.](#)

[Configuring a virtual router \(OS vRouter\) in the topology.](#)

[Configuring a VLAN in the topology.](#)

[Configuring a VXLAN in the topology.](#)

[Configuring a flat network in the topology.](#)

[Configuring a UNI in the topology.](#)

[Monitoring solution components](#)

[Specifying the Zabbix server](#)

[Specifying the Zabbix proxy server](#)

[Configuring CPE device monitoring](#)

[Viewing monitoring results](#)

[Viewing problems](#)

[Viewing the status of the solution and its components](#)

[Viewing logs](#)

[Viewing and deleting service requests](#)

[Sending CPE device notifications to users](#)

[Specifying the SMTP Server](#)

[Configuring notifications](#)

[Selecting the Docker container log verbosity.](#)

[Monitoring CPE, VNF, and PNF devices using SNMP](#)

[Configuring the connection of the SNMP manager to agents](#)

[Creating a trap](#)

[Editing a trap](#)

[Deleting a trap](#)

[Link monitoring](#)

[Tunnels, segments, and paths](#)

[Redundancy of links between CPE devices](#)

[Configuring paths](#)

[Creating a Manual-TE path](#)

[Editing a Manual-TE path](#)

[Deleting a hop from a Manual-TE path](#)

[Deleting a Manual-TE path](#)

[Specifying the cost of a link](#)

[Enabling Dampening](#)

[Enabling Forward Error Correction](#)

[Determining the effective MTU in a link](#)

[Package fragmentation](#)

[Traffic encryption](#)

[Traffic encryption on a CPE device](#)

[Traffic encryption on a link](#)

[Configuring topology.](#)

[About the Hub-and-Spoke topology.](#)

[About Full-Mesh and Partial-Mesh topologies](#)

[Creating a Hub-and-Spoke topology](#)

[Creating Full-Mesh and Partial-Mesh topologies](#)

[Quality of Service \(QoS\)](#)

[Traffic classes](#)

[Default traffic classes](#)

[Creating or editing traffic classes](#)

[Traffic classifiers](#)

[Creating a traffic classifier](#)

[Editing a traffic classifier](#)

[Deleting a traffic classifier](#)

[QoS rules](#)

[Creating a QoS rule](#)

[Editing a QoS rule](#)

[Deleting a QoS rule](#)

[Constraints](#)

[Creating a Manual-TE constraint](#)

[Editing a Manual-TE constraint](#)

[Deleting a Manual-TE constraint](#)

[Creating a threshold constraint](#)

[Editing a threshold constraint](#)

[Deleting a threshold constraint](#)

[Traffic classification rules](#)

[Creating a traffic classification rule](#)

[Editing a traffic classification rule](#)

[Deleting a traffic classification rule](#)

[Traffic filters](#)

[Creating a traffic filter](#)

[Editing a traffic filter](#)

[Deleting a traffic filter](#)

[Transport services](#)

[Point-to-Point \(P2P\) transport service](#)

[Creating a P2P service](#)

[Editing a P2P service](#)

[Deleting a P2P service](#)

[Viewing statistics of a P2P service](#)

[Configuring the display of devices in a P2P service topology](#)

[Restarting a P2P service](#)

[Point-to-Multipoint \(P2M\) transport service](#)

[Creating a P2M service](#)

[Editing a P2M service](#)

[Deleting a P2M service](#)

[Viewing statistics of a P2M service](#)

[Viewing the MAC table of a P2M service](#)

[Configuring the display of devices in a P2M service topology](#)

[Restarting a P2M service](#)

[Multipoint-to-Multipoint \(M2M\) transport service](#)

[Creating an M2M service](#)

[Editing an M2M service](#)

[Deleting an M2M service](#)

[Viewing statistics of an M2M service](#)

[Viewing the MAC table of an M2M service](#)

[Configuring the display of devices in an M2M service topology.](#)

[Restarting an M2M service](#)

[IP multicast transport service](#)

[Creating an IP multicast service](#)

[Editing an IP multicast service](#)

[Deleting an IP multicast service](#)

[Viewing statistics of an IP multicast service](#)

[L3 VPN transport service](#)

[Creating an L3 VPN service](#)

[Editing an L3 VPN service](#)

[Restarting an L3 VPN service](#)

[Deleting an L3 VPN service](#)

[Viewing the ARP table of an L3 VPN service](#)

[Creating a static record in the ARP table of an L3 VPN service](#)

[Editing a static record in the ARP table of an L3 VPN service](#)

[Deleting a static record in the ARP table of an L3 VPN service](#)

[Viewing the routing table of an L3 VPN service](#)

[Adding a transport service in a CPE template](#)

[Editing a transport service in a CPE template](#)

[Deleting a transport service from a CPE template](#)

[Scenario: Directing application traffic to a transport service](#)

[Traffic mirroring](#)

[Creating a traffic destination](#)

[Deleting a traffic destination](#)

[Creating a TAP service](#)

[Editing a TAP service](#)

[Viewing statistics of a TAP service](#)

[Deleting a TAP service](#)

[Task scheduler](#)

[Creating a delayed task](#)

[Executing a delayed task manually.](#)

[Deleting a delayed task](#)

[Glossary](#)

[Control plane](#)

[Customer Premise Equipment \(CPE\)](#)

[Data plane](#)

[DSCP values](#)

[Orchestrator](#)

[Physical Network Function.\(PNF\)](#)

[PNF package](#)

[Port security.](#)

[SD-WAN Controller](#)

[SD-WAN Gateway.](#)

[SD-WAN instance](#)

[Software-Defined Networking \(SDN\)](#)

[Software-Defined Wide Area Network \(SD-WAN\)](#)

[Tenant](#)

[Transport strategy](#)

[Universal CPE \(uCPE\)](#)

[Virtual Deployment Unit \(VDU\)](#)

[Virtual Infrastructure Manager \(VIM\)](#)

[Virtual Network Function \(VNF\)](#)

[Virtual Network Function Manager \(VNFM\)](#)

[VNF Package](#)

[Contacting Technical Support](#)

[How to obtain Technical Support](#)

[Technical Support via Kaspersky Company Account](#)

[Information about third-party code](#)

[Trademark notices](#)

About Kaspersky SD-WAN

Kaspersky SD-WAN is used to build Software-Defined Wide Area Networks (Software Defined WAN; SD-WAN). In such networks, routes with the lowest latency and the greatest bandwidth are determined automatically. Traffic is routed using the SDN (Software Defined Networking) technology.

The *SDN technology* separates the [control plane](#) from the [data plane](#) and allows managing the network infrastructure using an [orchestrator](#) and the API. Separating the control plane from the data plane makes it possible to *virtualize network functions* (Network Function Virtualization; NFV), wherein network functions such as firewalls, routers, and load balancers are deployed on standard equipment. Network function virtualization in the solution is compliant with the [NFV MANO specification](#) (NFV Management and Network Orchestration) standards of the European Telecommunications Standards Institute (ETSI).

Building an SD-WAN network does not depend on transport technologies. You can also send traffic over multiple tunnels based on application requirements regarding bandwidth and quality of service. The following underlay network links are supported:

- MPLS transport networks
- Broadband links for connecting to the Internet
- Leased communication lines
- Wireless connections including 3G, 4G, and LTE
- Satellite links

The solution is intended for service providers and organizations with a large branch network; it replaces standard routers in distributed networks [with Customer Premise Equipment devices](#) (hereinafter referred to as CPE devices, CPEs, devices).

Kaspersky SD-WAN lets you do the following:

- Intelligent traffic management
- Automatic CPE device configuration
- Central management of solution components using the web interface
- Network monitoring
- Automatically responding to changes in QoS policies to meet requirements of applications

The figure below shows a diagram of an SD-WAN network built using the Kaspersky SD-WAN solution.

 An SD-WAN with two remote locations and one central location, plus a data center and an orchestrator.

SD-WAN network diagram

Distribution kit

To learn more about purchasing the solution, please visit the Kaspersky website (<https://www.kaspersky.com>) or contact partner companies.

The distribution kit includes the following components:

- [Kaspersky SD-WAN Setup Wizard](#).
- Docker containers for deploying Kaspersky SD-WAN components:
 - knaas-ctl
 - knaas-orc
 - knaas-www
 - knass-vnfm
 - knaas-vnfm-proxy
 - mockpnf

You must download the following containers from the [common Docker repository](#):

- mariaDB
- mongo
- redis
- syslog-ng
- zabbix-proxy-mysql
- zabbix-server-mysql
- zabbix-web-nginx-mysql
- CPE device firmware.
- A file with the text of the End User License Agreement, which stipulates the terms and conditions that you must accept to use the solution.
- Kaspersky SD-WAN Online Help files that let you read documentation without an Internet connection.

The content of the distribution kit may differ depending on the region in which the solution is distributed.

Hardware and software requirements

Kaspersky SD-WAN has the following hardware and software requirements:

Hardware requirements

When deploying the solution, you must take into account the hardware requirements for deploying the [orchestrator](#), [SD-WAN controller](#), [VNFM](#), and the monitoring system. Kaspersky SD-WAN uses the Zabbix [monitoring](#) system, versions 5.0.26 and 6.0.0. For detailed information about the hardware requirements of the monitoring system, see the [official documentation of the Zabbix solution](#).

Hardware requirements depend on the number of [CPE devices](#) being managed. If you need to connect more than 250 CPE devices, deploy additional SD-WAN Controller clusters. If you need to calculate hardware requirements for a specific deployment scheme more precisely, we recommend contacting Kaspersky Technical Support.

- [Hardware requirements for up to 50 CPE devices](#)

- To deploy the orchestrator:
 - 8 CPU cores
 - 8 GB of RAM
 - 105 GB of disk space
 - 3 virtual machines
- To deploy the SD-WAN controller:
 - 4 CPU cores
 - 8 GB of RAM
 - 40 GB of disk space
 - 3 containers
- To deploy the VNFM:
 - 4 CPU cores
 - 8 GB of RAM
 - 20 GB of disk space
 - 3 containers
- To deploy the monitoring system:
 - 4 CPU cores
 - 8 GB of RAM
 - 100 GB of disk space
 - 3 containers

- [Hardware requirements for up to 100 CPE devices](#)

- To deploy the orchestrator:
 - 8 CPU cores
 - 10 GB of RAM
 - 110 GB of disk space
 - 3 virtual machines
- To deploy the SD-WAN controller:
 - 6 CPU cores
 - 8 GB of RAM
 - 40 GB of disk space
 - 3 containers
- To deploy the VNFM:
 - 4 CPU cores
 - 8 GB of RAM
 - 20 GB of disk space
 - 3 containers
- To deploy the monitoring system:
 - 4 CPU cores
 - 10 GB of RAM
 - 200 GB of disk space
 - 3 containers

- [Hardware requirements for up to 250 CPE devices](#) 

- To deploy the orchestrator:
 - 8 CPU cores
 - 12 GB of RAM
 - 125 GB of disk space
 - 3 virtual machines
- To deploy the SD-WAN controller:
 - 8 CPU cores
 - 16 GB of RAM
 - 40 GB of disk space
 - 3 containers
- To deploy the VNFM:
 - 4 CPU cores
 - 8 GB of RAM
 - 20 GB of disk space
 - 3 containers
- To deploy the monitoring system:
 - 6 CPU cores
 - 12 GB of RAM
 - 350 GB of disk space
 - 3 containers

- [Hardware requirements for up to 500 CPE devices](#) 

- To deploy the orchestrator:
 - 8 CPU cores
 - 16 GB of RAM
 - 150 GB of disk space
 - 3 virtual machines
- To deploy the SD-WAN controller:
 - 8 CPU cores
 - 16 GB of RAM
 - 40 GB of disk space
 - 6 containers
- To deploy the VNFM:
 - 4 CPU cores
 - 8 GB of RAM
 - 20 GB of disk space
 - 3 containers
- To deploy the monitoring system:
 - 8 CPU cores
 - 24 GB of RAM
 - 600 GB of disk space
 - 3 containers

- [Hardware requirements for up to 1000 CPE devices.](#) 

- To deploy the orchestrator:
 - 10 CPU cores
 - 24 GB of RAM
 - 200 GB of disk space
 - 3 virtual machines
- To deploy the SD-WAN controller:
 - 8 CPU cores
 - 16 GB of RAM
 - 40 GB of disk space
 - 12 containers
- To deploy the VNFM:
 - 4 CPU cores
 - 10 GB of RAM
 - 20 GB of disk space
 - 3 containers
- To deploy the monitoring system:
 - 10 CPU cores
 - 32 GB of RAM
 - 1100 GB of disk space
 - 3 containers

- [Hardware requirements for up to 5000 CPE devices](#) 

- To deploy the orchestrator:
 - 12 CPU cores
 - 32 GB of RAM
 - 600 GB of disk space
 - 3 virtual machines
- To deploy the SD-WAN controller:
 - 8 CPU cores
 - 16 GB of RAM
 - 40 GB of disk space
 - 60 containers
- To deploy the VNFM:
 - 4 CPU cores
 - 12 GB of RAM
 - 20 GB of disk space
 - 3 containers
- To deploy the monitoring system:
 - 12 CPU cores
 - 64 GB of RAM
 - 5100 GB of disk space
 - 3 containers

- [Hardware requirements for up to 10,000 CPE devices](#) 

- To deploy the orchestrator:
 - 16 CPU cores
 - 64 GB of RAM
 - 1100 GB of disk space
 - 5 virtual machines
- To deploy the SD-WAN controller:
 - 8 CPU cores
 - 16 GB of RAM
 - 40 GB of disk space
 - 120 containers
- To deploy the VNFM:
 - 4 CPU cores
 - 16 GB of RAM
 - 20 GB of disk space
 - 3 containers
- To deploy the monitoring system:
 - 16 CPU cores
 - 128 GB of RAM
 - 10,100 GB of disk space
 - 3 containers

Software requirements

Docker 1.5 or later is required. The following 64-bit operating systems are supported:

- Ubuntu 20 LTS or later
- Astra Linux 1.7 or later (security level: "Orel").

The following browsers are supported for managing the orchestrator web interface:

- Google Chrome 100 or later

- Firefox 100 or later
- Microsoft Edge 100 or later
- Opera 90 or later
- Safari 15 or later

In Kaspersky SD-WAN, you can view the network topology overlaid on a geographical map. Maps of the OpenStreetMap service are used for this purpose. If the infrastructure of your organization does not provide for an Internet connection, you can use offline maps. Offline maps take up additional disk space:

- The offline map (central-fed-district-latest.osm.pbf) takes up approximately 100 GB.
- Geocoding data takes up approximately 10 GB.

For detailed information about maps, please refer to the [official documentation of the OpenStreetMap service](#).

CPE device requirements

You can use standard CPE devices and universal CPE devices (uCPE devices; uCPEs). uCPE devices include a hypervisor, which lets you deploy virtual network functions and VIMs.

CPE devices have direct Internet access (DIA) without relaying traffic to the central office.

The following CPE devices are supported:

- KESR-M1-R-5G-2L-W
- KESR-M2-K-5G-1L-W
- KESR-M2-K-5G-1S
- KESR-M3-K-4G-4S
- KESR-M4-K-2X-1CPU
- KESR-M4-K-8G-4X-1CPU
- KESR-M5-K-8G-4X-2CPU
- KESR-M5-K-8X-2CPU

For detailed information about the characteristics of CPE devices, please refer to the [official page of the solution](#).

Kaspersky experts carried out tests to confirm the functionality of CPE devices when providing the L3 VPN service (see the table below). DPI (Deep Packet Inspection) was not used on the tested devices, and [traffic encryption](#) was disabled.

Model	Packet size (bytes)	Bandwidth (Mbps)
KESR-M1	IMIX (417)	30
	Large (1300)	115

KESR-M2	IMIX (417)	165
	Large (1300)	241
KESR-M3	IMIX (417)	805
	Large (1300)	1150
KESR-M4	IMIX (417)	1430
	Large (1300)	2870
KESR-M5	IMIX (417)	2875
	Large (1300)	5750

Shared storage requirements

We recommend using your own shared storage for fault tolerance. The requirements for the storage are as follows:

- Support for simultaneous read and write from multiple hosts.
- The size depends on the size of the files being stored, but at least 40 GB of available protected space that supports further expansion.
- Bandwidth of the communication links between the storage and the orchestrator must be at least 1 Gbps; 10-Gigabit Ethernet or 8-Gigabit FC (Fiber Channel) is recommended.
- The IOPS (input/output operations per second) value must be at least 250, at least 400 IOPS is recommended.
- The following types of shared storage are supported:
 - NFS
 - iSCSI
 - FC
 - CephFS
- The storage must be mounted.
- Must stay available if the host restarts.

Ensuring security

Security in Kaspersky SD-WAN is ensured in the [data plane](#), [control plane](#), and orchestration plane. The security level of the solution as a whole is determined by the security level of each of these planes, as well as the security of their interaction. The following processes take place in each plane:

- User authentication and authorization
- Use of secure management protocols
- [Encryption](#) of control traffic

- Secure connection of [CPE devices](#)

Secure management protocols

We recommend using HTTPS when communicating with the SD-WAN network through the orchestrator web interface or API. You can upload your own certificates to the web interface or use automatically generated self-signed certificates. The solution uses several protocols to transmit control traffic to its components (see the table below).

Interacting components	Protocol	Additional security measures
Orchestrator and SD-WAN Controller	gRPC	TLS is used for authentication and traffic encryption between the client and server.
Orchestrator and CPE device	HTTPS	Certificate verification and a token are used for authentication and traffic encryption between the orchestrator and the CPE device.
SD-WAN Controller and CPE device	OpenFlow 1.3.4	TLS is used for authentication and traffic encryption between the SD-WAN Controller and the CPE device.

Secure connection of CPE devices

The solution uses the following mechanisms for secure connection of CPE devices:

- Discovery of CPE device by DPID.
- Deferred registration. You can select the state of the CPE device after successful registration: *Activated* or *Deactivated*. A deactivated CPE device must be manually [activated](#) after making sure it is installed at the location.
- [Two-factor authentication](#).

Using virtual network functions

You can provide an additional layer of security with virtual network functions deployed in the data center and/or on [uCPEs](#). For example, traffic can be relayed from a CPE device to a virtual network function that acts as a firewall or proxy server. Virtual network functions can perform the following SD-WAN protection functions:

- Next-Generation Firewall (NGFW)
- Protection from DDoS (Distributed Denial of Service) attacks
- Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)
- Anti-Virus
- Anti-Spam
- Content Filtering and URL filtering system
- DLP (Data Loss Prevention) system for preventing confidential information leaks
- Secure Web Proxy

What's new

Kaspersky SD-WAN has the following new and improved functionality:

- Centralized [firewall management](#) with template and DPI support. Now you can disable or enable DPI when [specifying basic firewall settings](#) and [specify DPI marks](#) to apply firewall rules to application traffic packets.
- Now you can create [DNAT](#) and [SNAT](#) rules for firewall management if you want to use the Source Network Address Translation (SNAT), Destination Network Address Translation (DNAT), and Port Address Translation (PAT) mechanisms. You can centrally manage these mechanisms using firewall templates.
- You can use up to 200 [virtual routing and forwarding tables \(VRF\)](#) on CPE devices. You can put BGP routes into one of the virtual routing and forwarding tables.
- Now you can install [certificate](#) chains on CPE devices
- Now you can [monitor traffic packet information using the NetFlow protocol](#) versions 1, 5, and 9. You can centrally manage the protocol using NetFlow templates.
- Information about the following events is now sent to the [Syslog server that you can specify](#):
 - A user logging in or out of the orchestrator web interface.
 - A user entering the password incorrectly when logging in to the orchestrator web interface.
 - A user conducting a brute-force attack.
 - An attempt to log in to the orchestrator web interface using a non-existent account.
- [Two-factor authentication of users is now supported using the Time-based-one-time password \(TOTP\) algorithm](#).
- Support for upgrading Kaspersky SD-WAN from version 2.1.3 to 2.2.0. If you are using a version lower than 2.1.3, you must first upgrade the solution to version 2.1.3, and then to 2.2.0. You must first upgrade the central components of the solution, and then the CPE devices.
- The [Setup Wizard for quick deployment of Kaspersky SD-WAN](#) is now available. The Setup Wizard lets you modify elements of the orchestrator web interface, such as the displayed logo of your organization.
- [Sending notifications about events and problems on CPE devices to user emails](#) is now supported.
- Now you can [diagnose CPE devices](#) using the following utilities:
 - [ping](#)
 - [traceroute](#)
 - [tcpdump](#)
 - [iperf](#)
 - [sweep](#)
- Version 6.0.0 of the Zabbix monitoring system is supported.

- The OVF template for virtual CPE devices is supported. You can use this template to [automatically register CPE devices](#) using the VMware ESXi hypervisor.
- Optimized performance of the SD-WAN Controller and CPE devices.
- Optimized recovery of a failed SD-WAN Controller node.
- Now you can [create IP address and subnet ranges for CPE devices](#) (IPAM). You can use these ranges to centrally assign IPv4 addresses to network interfaces of CPE devices. You can also use IP address ranges to centrally assign IPv4 addresses to CPE router IDs.
- CPE device names are now displayed in Zabbix monitoring system.
- Now you can [place CPE, VNF, and PNF device hosts into automatically created groups on the Zabbix server](#). Groups correspond to tenants to which VNFs, PNFs, and CPE devices belong.
- The RED OS® 8 operating system is supported for central components of the solution.
- [Users with the tenant role can now change the password](#).
- Assigned IPv4 addresses can now be displayed in the [table of network interfaces](#) of a CPE device.
- Now you can [create network interfaces for connecting to a PPPoE server](#).
- [CPE devices can now relay multicast traffic using the PIM and IGMP protocols](#).

Architecture of the solution

Kaspersky SD-WAN includes the following main components:

- The orchestrator controls the solution infrastructure, functions as an NFV orchestrator (NFVO), and manages network services and distributed VNFMs. Can be managed via the web interface or REST API when using external northbound systems.
- The SD-WAN Controller centrally manages the overlay network and network devices in accordance with the service chain topology via the OpenFlow protocol. Deployed as a virtual or physical network function.
- CPE devices relay traffic and form an SDN fabric in the form of an overlay network. Installed at remote locations.
- The VNFM manages the lifecycle of virtual network functions using SSH, Ansible playbooks, scripts, and Cloud-init attributes.

When using virtual network functions, the following additional components may be included in the architecture:

- The SDN controller manages hardware and software switches. This component is optional.
- The VIM -manages computational, networking, and storage resources within the NFV infrastructure. Connects VNFs using virtual links, subnets, and ports. The OpenStack cloud platform is used as the VIM.

Kaspersky SD-WAN has a distributed microservice architecture based on Docker containers (see the figure below). An SD-WAN Controller can include one, three, or five nodes. Controller nodes are separate virtual machines which you can run on different physical servers for fault tolerance.

The figure shows a diagram of the solution: the orchestrator interacts with the controller, VNFM and VIM.

Architecture of Kaspersky SD-WAN

Installing Kaspersky SD-WAN

The KNAAS Setup wizard allows deploying Kaspersky SD-WAN in accordance with the required deployment scheme. The distribution kit includes a TAR.GZ archive named `knaas-installer_<version>`. This archive has the following structure

- The `ansible.cfg` file is a system file with Ansible settings.
- The `CHANGELOG.md` file is the change log for YAML files that are part of the Setup Wizard.
- The `'docs'` directory contains the Setup Wizard documentation.
- The `'images'` directory contains images of the solution components to be deployed.
- The `'inventory'` directory:
 - The `'external'` directory:
 - The `'pnf'` directory contains sample files for typical deployment schemes of the solution with the SD-WAN Controller deployed as physical network functions.
 - The `'vnf'` directory contains example files for typical deployment schemes of the solution with the SD-WAN Controller deployed as virtual network functions.
 - The `'generic'` contains common system files.
- The `'knaas'` directory contains system files with playbooks that are called when the solution is being deployed.
- The `'oem'` directory contains elements of the orchestrator web interface that you can modify. For example, you can use this directory to edit your organization's logo.
- The `'pnfs'` directory contains examples of physical network functions for deploying the SD-WAN Controller.
- The `README.md` file contains instructions for deploying the solution using the Setup Wizard.
- The `requirements.txt` file is a system file with Python requirements.

We do not recommend editing system files because this may cause errors when deploying the solution.

If you experience problems when deploying Kaspersky SD-WAN using the Setup Wizard, we recommend that contacting Kaspersky Technical Support.

Redundancy of central components of the solution

Kaspersky SD-WAN supports two component deployment schemes: N+1 and 2N+1.

In the *N+1 deployment scheme*, you must deploy a backup component along with the active component. If the active component fails, the backup component takes its place.

In the *2N+1 deployment scheme*, you must deploy the active component twice and deploy the backup component alongside it. The components are synchronized with each other, and one can take the place of the other if a malfunction occurs. This redundancy scheme allows components to remain operational even when multiple failures occur in a row.

The table below shows the redundancy schemes and protocols that are used for different components of the solution.

Component	Redundancy scheme	Protocol used
Orchestrator	N+1	REST
Orchestrator web interface	N+1	REST
Orchestrator database	2N+1	MONGODB
SD-WAN Controller and its database	2N+1	OPENFLOW (TLS)
SD-WAN Gateway	N+1	GENEVE

An example of locating solution components in geographically dispersed locations is shown in the figure below. All of the figures below use the following symbols:

- orchestrator – orc
- orchestrator web interface – www
- orchestrator database – orc-dbs
- SD-WAN Controller and its database – ctl
- SD-WAN gateway – GW

For components of the solution that are N+1 redundant, two nodes are deployed in separate locations. Each of the nodes is in the active state. You can use a virtual IP address or DNS service to select the node to which requests are directed.

The diagram shows three interconnected locations with solution components.

Placing solution components in geographically dispersed locations

Components that are 2N+1 redundant form a cluster. This cluster contains one primary node and two nodes providing redundancy. You can designate one of the nodes as an arbiter to economize resources and reduce the requirements for the tunnels.

If a cluster node is designated as an arbiter, it does not contain a database and you cannot make it the primary node. The arbiter node takes part in voting when the primary node is selected and exchanges periodic control packets with other nodes.

The figure below shows an example of a failure at one of the locations and how the solution responds to it. This example shows an accident in which the nodes of the solution component cluster fail at location 1.

The diagram shows three interconnected locations. An accident causes location 1 to fail.

Accident at location 1

If nodes of the solution component cluster at location 1 fail, the following events occur:

1. Node orc-dbs 2 and arbiter node orc-dbs 3 lose contact with node orc-dbs 1, and subsequently vote for a new primary node.
2. Arbiter node orc-dbs 3 cannot be the primary node, therefore orc-dbs 2 becomes the primary node and informs the orchestrator of its role.
3. Node ctl 2 and arbiter node ctl 3 lose contact with node ctl 1, and subsequently vote for a new primary node.
4. Arbiter node ctl 3 cannot be the primary node, therefore ctl 2 becomes the primary node and informs the orchestrator of its role.

The figure below shows an accident in which the nodes of the solution component cluster fail at location 2.

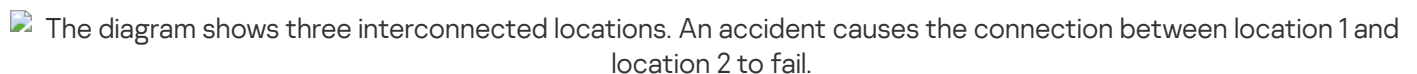
The diagram shows three interconnected locations. An accident causes location 2 to fail.

Accident at location 2

If nodes of the solution component cluster at location 2 fail, the following events occur:

1. Node orc-dbs 1 and arbiter node orc-dbs 3 lose contact with node orc-dbs-2, after which node orc-dbs 1 remains the primary node.
2. Node ctl 1 node and arbiter node ctl 3 lose contact with node ctl 2, after which node ctl 1 remains the primary node.

The figure below shows an example of an accident in which the connection between location 1 and location 2 is severed.

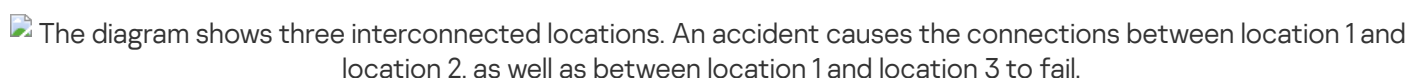
The diagram shows three interconnected locations. An accident causes the connection between location 1 and location 2 to fail.

Connection failure between location 1 and location 2

If cluster nodes of solution components at location 1 and location 2 cannot connect to each other, the following events occur:

1. Node orc-dbs 1 loses contact with node orc-dbs 2.
2. Node orc-dbs 1 node remains the primary node because arbiter node orc-dbs 3 observes both locations operating normally.
3. Node ctl 1 loses contact with node ctl 2.
4. Node ctl 1 remains the primary node because arbiter node ctl 3 observes both locations operating normally.

The figure below shows an example of an accident in which the connection between location 1 and other locations is severed.

The diagram shows three interconnected locations. An accident causes the connections between location 1 and location 2, as well as between location 1 and location 3 to fail.

Failure of connections between location 1 and other locations

If cluster nodes of solution components at location 1 cannot connect to other locations, the following events occur:

1. Node orc-dbs 1 loses contact with node orc-dbs 2.
2. Node orc-dbs 2 becomes the primary node and informs the orchestrator of its role because the arbiter node orc-dbs 3 observes that location 1 is unavailable.
3. Node ctl 1 loses contact with node ctl 2.
4. Node ctl 2 becomes the primary node and informs the orchestrator of its role because arbiter node ctl 3 observes that location 1 is unavailable.

Logging in and out of the orchestrator web interface

Logging in to the orchestrator web interface


To log in to the orchestrator web interface:

1. In the address bar of your browser, enter the IP address or name of the Kaspersky SD-WAN server.
2. This opens the authentication page; on that page, enter a user name and password. The password must contain at least one uppercase character (A–Z), one lowercase character (a–z), a numeral, and a special character. Password length: 8 to 50 characters.
3. Click **Log in**. If [two-factor authentication](#) is enabled for your account:
 - a. Scan the displayed QR code with a physical or software authenticator that supports the [RFC 6238](#) standard.
 - b. Enter and confirm the unique code generated by the authenticator.

After successful authentication, you are taken to the section or subsection that you [set as the default page](#).

Logging out of the orchestrator web interface

To log out of the orchestrator web interface:

1. In the lower part of the window, click the log out button  logout_icon.
2. In the confirmation window, click **OK**.

You are logged out of the orchestrator web interface.

Licensing of Kaspersky SD-WAN

This section covers basic concepts of Kaspersky SD-WAN licensing. If you need to scale the solution, you can purchase additional software and hardware licenses.

About the End User License Agreement

The *End User License Agreement* is a binding agreement between you and AO Kaspersky Lab, stipulating the terms on which you may use the program. The text of the End User License Agreement in supported languages is located in the *license <language code>.rtf* files included in the Kaspersky SD-WAN distribution kit.

Read through the terms of the End User License Agreement carefully before you start using Kaspersky SD-WAN.

By confirming that you agree with the End User License Agreement, you signify your acceptance of the terms of the End User License Agreement. You can do this in one of the following ways:

- Initialize the `KNAAS_EULA_AGREED` environment variable before starting the Kaspersky SD-WAN Docker container:

```
export KNAAS_EULA_AGREED=yes
```

In this case, when starting the Kaspersky SD-WAN Docker container, pass the `KNAAS_EULA_AGREED` environment variable using the `-e` option:

```
docker run -e KNAAS_EULA_AGREED [OPTIONS] IMAGE [COMMAND] [ARG...]
```

- Initialize the `KNAAS_EULA_AGREED` environment variable directly when starting the Kaspersky SD-WAN Docker container:

```
docker run -e KNAAS_EULA_AGREED=yes [OPTIONS] IMAGE [COMMAND] [ARG...]
```

If the `KNAAS_EULA_AGREED` environment variable is not initialized or is initialized with the value `no` (`KNAAS_EULA_AGREED=no`), this means that you do not agree with the terms of the End User License Agreement. In this case, when starting the Kaspersky SD-WAN Docker container, an error message is displayed, and Kaspersky SD-WAN does not start.

About data provision


The following third-party solutions are integrated into Kaspersky SD-WAN:

- Zabbix monitoring system
- OpenStack platform for creating cloud services and storage
- OpenStreetMap geographic maps

Personal information that might be introduced to Zabbix, OpenStack, or OpenStreetMap as a result of integration is not sent outside the perimeter of the organization's infrastructure.

Kaspersky protects received information in accordance with requirements stipulated by applicable law and Kaspersky policies.

User interface of the solution

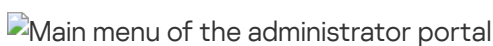
Kaspersky SD-WAN is managed using the orchestrator web interface. You can use the menu sections to configure the components of the solution. When you navigate to a section, an additional menu with subsections is displayed in a collapsed form. To expand the menu, hover your mouse cursor over the icon of one of the subsections. You can click the expand icon  Expanding the navigation pane to disable the automatic minimization of the menu.

Two versions of the orchestrator web interface are supported:

- The *administrator portal* gives administrators full access to managing the solution components.
- The *self-service portal* gives [tenants](#) access to managing the SD-WAN instances that are deployed for them.

Administrators can [log in to the self-service portal of a tenant](#).

Administrator portal

 Main menu of the administrator portal

Main menu of the administrator portal

Dashboard	Information about the current status of solution components such as CPE devices and network functions.
Infrastructure	Resources of the organization . In this section, you can configure the following components: <ul style="list-style-type: none">• Domains• Data centers• Management subnets• Controllers
Catalog	Templates for centralized configuration of network services
SD-WAN	<ul style="list-style-type: none">• CPE – CPE devices for relaying traffic.• CPE templates – CPE templates for centralized configuration of devices.• Firewall templates – firewall templates for centralized configuration of the firewall on CPE devices.• Firewall zones – firewall zones for network interfaces and subnets of CPE devices.• NetFlow templates – NetFlow templates for monitoring traffic packet information on CPE devices.• IPAM – IP address and subnet ranges for CPE devices.• Firmware – CPE device firmware.• Certificates – certificates to be installed on CPE devices.• SD-WAN instances – deployed SD-WAN instances.

	<ul style="list-style-type: none"> • SD-WAN instance templates – SD-WAN instance templates for centralized configuration and deployment of instances. • SD-WAN instance pools – SD-WAN instance pools. • UNI templates – UNI templates for centralized creation of UNIs on CPE devices.
Scheduler	Scheduled tasks .
Monitoring	Zabbix server settings for monitoring solution components .
Notification	Settings for sending email notifications to users .
Logs	Logs of solution components , such as CPE devices, virtual network functions, and physical network functions.
Tenants	Tenants of the solution.
Users	<p>Users of the solution. In this section, you can configure the following components:</p> <ul style="list-style-type: none"> • Users • Access permissions • LDAP user groups • LDAP connections
Confirmation	Confirmation requests for user actions.

Certain components of the solution can be configured in the advanced configuration menu of the Controller.

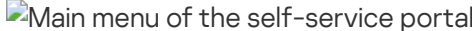
Controller configuration menu

Controller configuration menu on the administrator portal

Controller nodes	Information about the current status of Controller nodes .
Switches	Advanced settings of CPE devices and switches.
Topology	Graphical topology of an SD-WAN instance .
Topology tags	Topology tags for building a topology , for example, Hub-and-Spoke.
Segments	Segments formed from CPE devices and switches.
QoS	<p>Quality of service settings. In this section, you can configure the following components:</p> <ul style="list-style-type: none"> • Traffic classes • Traffic classifiers • QoS rules
P2P services	Point-to-Point transport services .
P2M services	Point-to-Multipoint transport services .
M2M services	Multipoint-to-Multipoint transport services .
IP multicast	IP multicast transport services .

services	
L3 VPN services	L3 VPN transport services.
TAP services	Test Access Point services for traffic mirroring.
Service interfaces	Service interfaces of CPE devices and switches.
Constraints	Threshold constraints for enforcing quality of service.
Traffic filters	Traffic filters for enforcing quality of service.
OpenFlow groups	OpenFlow port groups.
Tunnels	Links between CPE devices and switches, and tunnels between CPE devices.
Logs	Docker container log verbosity level.
SNMP	Settings for monitoring CPE devices, virtual network functions, and physical network functions using SNMP.


Self-service portal

 Main menu of the self-service portal

Main menu of the self-service portal

Dashboard	Information about the current status of solution components such as CPE devices and network functions.
Infrastructure	Resources of the organization. In this section, you can configure Controllers .
Catalog	Network services for traffic transmission and virtualization of network functions.
SD-WAN	<ul style="list-style-type: none"> • CPE – CPE devices for relaying traffic. • CPE templates – CPE templates for centralized configuration of devices. • Firewall templates – firewall templates for centralized configuration of the firewall on CPE devices. • Firewall zones – firewall zones for network interfaces and subnets of CPE devices. • NetFlow templates – NetFlow templates for monitoring traffic packet information on CPE devices. • IPAM – IP address and subnet ranges for CPE devices. • UNI templates – UNI templates for centralized creation of UNIs on CPE devices.
Scheduler	Scheduled tasks.
Notification	Settings for sending email notifications to users.
Logs	Logs of solution components , such as CPE devices, virtual network functions, and physical network functions.
Confirmation	Confirmation requests for user actions.

Certain components of the solution can be configured in the additional menu of the Controller.

 Controller configuration menu on the self-service portal

P2P services	Point-to-Point transport services.
P2M services	Point-to-Multipoint transport services.
M2M services	Multipoint-to-Multipoint transport services.
IP multicast services	IP multicast transport services.
L3 VPN services	L3 VPN transport services.
TAP services	Test Access Point services for traffic mirroring.
Service interfaces	Service interfaces of CPE devices and switches.
Constraints	Threshold constraints for enforcing quality of service.
Traffic filters	Traffic filters for enforcing quality of service.
OpenFlow groups	OpenFlow port groups.

Setting and resetting the default page

The *default page* is a section or subsection of the menu that is automatically displayed after you [log into the orchestrator web interface](#).

To set or reset the default page:

1. In the menu, go to the section or subsection of the orchestrator web interface that you want to set as the default page.
2. In the lower part of the menu, click the settings icon → **Set as default page**.
In the upper part of the page, the Default page is set message is displayed.
3. If you want to reset the default page, click the settings icon → **Reset default page**.
In the upper part of the page, the Default page is reset message is displayed. The **Dashboard** section becomes the default page.

Switching between light and dark modes of the orchestrator web interface

To switch between light and dark modes of the orchestrator web interface:

In the lower part of the menu, click the settings icon → **Dark mode** or **Light mode**.

Changing the language of the orchestrator web interface

The orchestrator web interface supports English and Russian languages.





To change the language of the orchestrator web interface,

in the lower part of the menu, click one of the following buttons:

- **EN** to switch the language of the orchestrator web interface to English.
- **RU** to switch the language of the orchestrator web interface to Russian.


Managing solution component tables

Solution components such as [users](#), [network interfaces](#), and [BGP peers](#) are displayed in tables. You can use the following controls to manage tables:

- The settings icon , which you can use to do the following:
 - Refresh the table by clicking the settings icon → **Reload**. You can also refresh the table using the refresh icon .
 - Restore default widths of table columns by clicking the settings icon → **Reset columns width**.
 - Select which columns are displayed in the table. To do so, click the settings icon  and select the check boxes next to the columns you want to display.
- The search icon  which you can click and enter your search criteria. After entering the search criteria, the table displays the relevant entries.
- Status filters to display entries with the selected status.
- Time filters to display entries for the selected period:
 - **All time**
 - **Last year**
 - **Last month**
 - **Last week**
 - **Last day**


You can manually specify the period using the fields in the upper part of the table.

- The **Actions** button for applying an action simultaneously to all entries with selected check boxes. For example, in the [CPE devices table](#), you can [delete multiple devices](#) at the same time.

You can adjust the width of each column of the table using the three-dot icons  between the names of the columns.

Navigating to the orchestrator API

To navigate to the orchestrator API,

in the lower part of the menu, click the API button question_mark_icon.

This opens a list of API commands that can be used to manage the orchestrator.

Managing users and their access permissions

To restrict access to the administrator portal and self-service portal, as well as to sections, subsections and functions, the solution implements a role-based access control model (Role Based Access Control; RBAC). User accounts can have the following roles:

- An administrator has access to the administrator portal and self-service portal.
- A tenant has access only to the self-service portal.

Deploying the solution creates the **Administrator** user with the administrator role and the **User** user with the tenant role.

You can create local users, LDAP users, and LDAP user groups. The solution does not support creating local user groups. Credentials of local users are stored in the orchestrator database. Credentials of LDAP users and LDAP user groups are stored on a remote server. Supported servers include the remote OpenLDAP server with Simple SSL authentication, as well as Microsoft Active Directory with Kerberos authentication and Kerberos SSL authentication.

You must first create an LDAP connection that the orchestrator uses to connect to the remote server, and then create LDAP users or LDAP user groups. Created LDAP users and LDAP user groups can log in to the orchestrator web interface using their credentials.

Two-factor authentication

To improve the overall security level of the solution, you can require two-factor authentication of users using the Time-based one-time password (TOTP) algorithm. You can enable or disable two-factor authentication for all users. You can also enable or disable two-factor authentication when creating or editing individual local users, LDAP users, and LDAP groups.

If two-factor authentication is enabled for a user, a unique QR code is generated the next time that user logs in to the orchestrator web interface. The user must scan a QR code using a software or hardware [RFC 6238](#) compliant authenticator, such as Kaspersky Password Manager, Google Authenticator, Yandex Key, and Microsoft Authenticator. The authenticator generates a unique code that the user must enter to complete two-factor authentication and log in to the orchestrator web interface. If the user enters the unique code incorrectly more than five times, that user is blocked for 30 minutes.

After completing two-factor authentication, the user must enter a user name, password, and a unique code to log into the orchestrator web interface. If necessary, you can make the user complete two-factor authentication again.

If the time discrepancy between the orchestrator and the authenticator is greater than 30 seconds, two-factor authentication may fail. We recommend synchronizing the time on the orchestrator and the authenticator using an [NTP server](#).

Access permissions

If necessary, you can create access permissions that determine which sections, subsections, and actions are available to which users, and assign these access rights when creating or editing a user or LDAP user group. For example, you can create an access permission that prohibits gaining access to the **Catalog** section and [creating network service templates](#). By default, LDAP users and groups have the **Full Access** permission, which grants full access to all functionality of the solution.

Confirmation requests

When creating a user, you must specify if you want to have a *confirmation request* automatically created whenever this user performs an action. Confirmation requests can be confirmed, denied, or deleted. When a confirmation request is confirmed, the relevant action is applied; denied confirmation requests are saved in the orchestrator web interface.

User sessions

The following functions are used to manage user sessions:

- Limiting the duration of user sessions. If a user remains idle for 3600 seconds (one hour) after logging into the orchestrator web interface, the user session is automatically ended. You can manually specify the period of inactivity that triggers automatic logout.
- Termination of user sessions. If multiple employees use the same user account credentials to log in to the orchestrator web interface, any of these employees can end the sessions of the others.

Managing access permissions

The list of access permissions is displayed in the **Users** section of the **Permissions** tab. By default, the **Full access** permission is created, which grants full access to the orchestrator web interface and is automatically assigned to [users](#) and [LDAP user groups](#) if you do not assign them a different access permission.

The actions you can perform with the list are described in the [Managing solution component tables](#) instructions.

Creating access permissions

To create an access permission:

1. In the menu, go to the **Users** section.
The user management page is displayed. The **Users** tab, which is selected by default, displays the table of users.
2. Select the **Permissions** tab.
The list of access permissions is displayed.
3. In the upper part of the list, click **+ Permission**.
4. In the displayed settings area, in the **Name** field, enter the name of the access permission. Maximum length: 250 characters.
5. In the **Access rights** section next to the sections and subsections of the orchestrator web interface, select one of the following values:
 - **Editing** to allow the users to view the section or subsection and perform all available tasks in it.
 - **Viewing** to allow users only to view the section or subsection.
 - **No access** to prevent users from viewing the section or subsection.

If you want the subsections to inherit the value selected for the section, select the **Apply to subsections** check box. This check box is cleared by default.

6. Click **Create**.

The access permission is created and displayed in the list.

You can assign an access permission when [creating](#) or [editing a user](#), or when [creating](#) or [editing an LDAP user group](#).

Editing access permissions

To edit an access permission:

1. In the menu, go to the **Users** section.

The user management page is displayed. The **Users** tab, which is selected by default, displays the table of users.

2. Select the **Permissions** tab.

The list of access permissions is displayed.

3. Click the access permission that you want to edit.

4. In the displayed settings area, in the **Name** field, enter the name of the access permission. Maximum length: 250 characters.

5. In the **Access rights** section next to the sections and subsections of the orchestrator web interface, select one of the following values:

- **Editing** to allow the users to view the section or subsection and perform all available tasks in it.
- **Viewing** to allow users only to view the section or subsection.
- **No access** to prevent users from viewing the section or subsection.

If you want the subsections to inherit the value selected for the section, select the **Apply to subsections** check box. This check box is cleared by default.

6. Click **Save**.

The access permission is modified and updated in the list.

Cloning access permissions

You can clone an access permission to create an identical access permission with a different name.

To clone an access permission:

1. In the menu, go to the **Users** section.

The user management page is displayed. The **Users** tab, which is selected by default, displays the table of users.

2. Select the **Permissions** tab.

The list of access permissions is displayed.

3. Click the access permission that you want to clone.
4. In the upper part of the displayed settings area, click **Management** → **Clone**.
5. This opens a window; in that window, enter the name of the new access permission.
6. Click **Clone**.

A copy of the access right with the new name is added to the list.

Removing an access permission

Deleted access permissions cannot be restored.

To remove an access permission:

1. In the menu, go to the **Users** section.
The user management page is displayed. The **Users** tab, which is selected by default, displays the table of users.
2. Select the **Permissions** tab.
The list of access permissions is displayed.
3. Click the access permission that you want to delete.
4. In the upper part of the displayed settings area, click **Management** → **Delete**.
5. In the confirmation window, click **Delete**.

The access permission is deleted and is no longer displayed in the list.

Managing LDAP connections

The LDAP connection table is displayed in the **Users** on the **LDAP connection** tab. Information about LDAP connections is displayed in the following table columns:

- **Name** is the name of the LDAP connection.
- **Type** is the type of the connection. This column always displays **LDAP**.
- **Host** is the host name of the remote server.

The actions you can perform with the table are described in the [Managing solution component tables](#) instructions.

Creating an LDAP connection

If you want LDAP users or LDAP user groups to be able to log in to the orchestrator web interface using their credentials, you must first create an LDAP connection that the orchestrator uses to connect to the remote server, and then create your LDAP users or [LDAP user groups](#).

To create an LDAP connection:

1. In the menu, go to the **Users** section.

The user management page is displayed. The **Users** tab, which is selected by default, displays the table of users.

2. Select the **LDAP connection** tab.

A table of LDAP connections is displayed.

3. Click **+ LDAP**.

4. In the displayed settings area, in the **Name** field, enter the name of the LDAP connection.

5. In the **Domain** field, enter the FQDN of the domain of the remote server.

6. In the **Domain alias** field, enter the alias or NETBIOS name of the domain. Users enter the alias, NETBIOS name, or FQDN of the domain when logging into the orchestrator web interface.

For example, if the FQDN of the domain is 'example.com' and the alias is 'example', a user named 'admin' can enter the following credentials when logging into the orchestrator web interface:

- admin@example.com
- admin@example
- example.com\admin
- example\admin

7. In the **LDAP host** field, enter the host name of the remote server. The following host name formats are supported:

- ldap://< host name >:< port number > for a standard LDAP server. The default port is 389.
- ldaps://< host name >:< port number > for an LDAP server with SSL authentication. The default port is 636.

For example, if you enter ldap://example.com:100, the host name of the remote server is 'example.com' and the port number is 100.

8. In the **Base DN** field, enter the base distinguished name to be used by the orchestrator as the starting point for searching user accounts in the remote server directory. The following base distinguished name formats are supported:

- To search in OpenLDAP, enter the base distinguished name in the OU=< value >,OU=< value > format, where OU is the structure of organizational units in the remote server directory. For example, if you enter OU=OU_example1,OU=OU_example2, the starting point for searching user accounts is organizational unit OU_example2, which is nested in OU_example1.
- To search in Microsoft Active Directory, enter the base distinguished name in the DC=< value >,DC=< value >, where DCs are the domain components of the remote server. For example, if you enter DC=example,DC=com, the starting point for searching user accounts is the 'example.com' domain.

9. In the **Search attribute** drop-down list, select the attribute that the orchestrator must use to search for user accounts in the remote server directory:

- **uid (OpenLDAP)** is the UID (user ID) for searching in OpenLDAP. Default value.
- **sAMAccountName (Active Directory)** is the pre-Windows 2000 logon name for searching in Microsoft Active Directory.

10. In the **Bind DN** field, enter the distinguished name for authenticating the orchestrator on the remote server. The following distinguished name formats are supported:

- For authentication in openLDAP, enter a value in the **UID=< value >,OU=< value >** format, where UID is the user ID and OU is the organizational unit structure in the remote server directory where the user is located. For example, if you enter **UID=user_example,OU=OU_example**, user **user_example** from organizational unit **OU_example** is used for authenticating the orchestrator on the remote server.
- For authentication in Microsoft Active Directory, enter a value in the **CN=< value >,OU=< value >,DC=< value >,DC=< value >**, where CN is the common name of the user, OU is the organizational unit structure in the directory of the remote server where the user is located, and the DCs are the user's domain components. For example, if you enter **CN=user_example,OU=OU_example,DC=example,DC=com**, user **user_example** in organizational unit **OU_example** in the **example.com** domain is used for authenticating the orchestrator on the remote server.

11. In the **Bind password** field, enter the remote server password for authenticating the orchestrator on the remote server. To see the entered password, you can click the show icon .

12. To check if the remote server is available, click **Test authentication**.

13. Click **Create**.

The LDAP connection is created and displayed in the table.

Editing an LDAP connection

To edit an LDAP connection:

1. In the menu, go to the **Users** section.

The user management page is displayed. The **Users** tab, which is selected by default, displays the table of users.

2. Select the **LDAP connection** tab.

A table of LDAP connections is displayed.

3. Click the LDAP connection that you want to edit.

4. In the displayed settings area, in the **Name** field, enter the name of the LDAP connection.

5. In the **Domain** field, enter the FQDN of the domain of the remote server.

6. In the **Domain alias** field, enter the alias or NETBIOS name of the domain. Users enter the alias, NETBIOS name, or FQDN of the domain when logging into the orchestrator web interface.

For example, if the FQDN of the domain is 'example.com' and the alias is 'example', a user named 'admin' can enter the following credentials when logging into the orchestrator web interface:

- **admin@example.com**

- admin@example
- example.com\admin
- example\admin

7. In the **LDAP host** field, enter the host name of the remote server. The following host name formats are supported:

- ldap://< host name >:< port number > for a standard LDAP server. The default port is 389.
- ldaps://< host name >:< port number > for an LDAP server with SSL authentication. The default port is 636.

For example, if you enter ldap://example.com:100, the host name of the remote server is 'example.com' and the port number is 100.

8. In the **Base DN** field, enter the base distinguished name to be used by the orchestrator as the starting point for searching user accounts in the remote server directory. The following base distinguished name formats are supported:

- To search in OpenLDAP, enter the base distinguished name in the OU=< value >,OU=< value > format, where OU is the structure of organizational units in the remote server directory. For example, if you enter OU=OU_example1,OU=OU_example2, the starting point for searching user accounts is organizational unit OU_example2, which is nested in OU_example1.
- To search in Microsoft Active Directory, enter the base distinguished name in the DC=< value >,DC=< value >, where DCs are the domain components of the remote server. For example, if you enter DC=example,DC=com, the starting point for searching user accounts is the 'example.com' domain.

9. In the **Search attribute** drop-down list, select the attribute that the orchestrator must use to search for user accounts in the remote server directory:

- **uid (OpenLDAP)** is the UID (user ID) for searching in OpenLDAP. Default value.
- **sAMAccountName (Active Directory)** is the pre-Windows 2000 logon name for searching in Microsoft Active Directory.

10. In the **Bind DN** field, enter the distinguished name for authenticating the orchestrator on the remote server. The following distinguished name formats are supported:

- For authentication in openLDAP, enter a value in the UID=< value >,OU=< value > format, where UID is the user ID and OU is the organizational unit structure in the remote server directory where the user is located. For example, if you enter UID=user_example,OU=OU_example, user user_example from organizational unit OU_example is used for authenticating the orchestrator on the remote server.
- For authentication in Microsoft Active Directory, enter a value in the CN=< value >,OU=< value >,DC=< value >,DC=< value >, where CN is the common name of the user, OU is the organizational unit structure in the directory of the remote server where the user is located, and the DCs are the user's domain components. For example, if you enter CN=user_example,OU=OU_example,DC=example,DC=com, user user_example in organizational unit OU_example in the example.com domain is used for authenticating the orchestrator on the remote server.

11. In the **Bind password** field, enter the remote server password for authenticating the orchestrator on the remote server. To see the entered password, you can click the show icon .

12. To check if the remote server is available, click **Test authentication**.

13. Click **Save**.

The LDAP connection is modified and updated in the table.

Changing the password of an LDAP connection

You can change the remote server password that was specified when the [LDAP connection](#) was created and make the orchestrator use the new password to authenticate with the remote server.

To change the password of an LDAP connection:

1. In the menu, go to the **Users** section.

The user management page is displayed. The **Users** tab, which is selected by default, displays the table of users.

2. Select the **LDAP connection** tab.

A table of LDAP connections is displayed.

3. Click the LDAP connection for which you want to change the password.

4. In the upper part of the displayed settings area, click **Management** → **Change password**.

5. This opens a window; type the new password in the **New password** and **Password confirmation** text boxes.

6. Click **Save**.

The LDAP connection password is changed.

Deleting an LDAP connection

Deleted LDAP connections cannot be restored.

To delete an LDAP connection:

1. In the menu, go to the **Users** section.

The user management page is displayed. The **Users** tab, which is selected by default, displays the table of users.

2. Select the **LDAP connection** tab.

A table of LDAP connections is displayed.

3. Click the LDAP connection that you want to delete.

4. In the upper part of the displayed settings area, click **Management** → **Delete**.

5. In the confirmation window, click **Delete**.

The LDAP connection is deleted and is no longer displayed in the table.

Managing users

The table of users is displayed in the **Users** section. Information about users is displayed in the following columns of the table:

- **Name** is the user name.
- **Tenant** is the [tenant](#) to which the [user](#) is assigned.
- **Role** is the role of the user:
 - **Administrator**
 - **Tenant**
- **Source** is the type of the user:
 - **Local** is a local user.
 - **LDAP** is an LDAP user.
- **Groups** is the group of the user.
- **State** is the status of the user:
 - **Online**
 - **Offline**
 - **Blocked**
- **Two-factor authentication** is the two-factor authentication status of the user:
 - **Enabled** means two-factor authentication is enabled for the user.
 - **Disabled** means two-factor authentication is disabled for the user.
 - **Reinitialization** means [repeated two-factor authentication](#) is performed for the user.

The actions that you can perform with the table are described in the [Managing solution component tables](#) instructions.

Creating a user

You can create local and LDAP users. Credentials of local users are stored in the orchestrator database. LDAP user credentials are stored on the remote server. If you want LDAP users to be able to log in to the orchestrator web interface using their credentials, you must first [create an LDAP connection](#) that the orchestrator uses to connect to the remote server, and then create your LDAP users or LDAP user groups.

To create a user:

1. In the menu, go to the **Users** section.

The user management page is displayed. The **Users** tab, which is selected by default, displays the table of users.

2. Click **+ User**.

3. In the displayed settings area, in the **Source** drop-down list, select the user type:

- **Local** (default) If this value is selected in the **Password** and **Password confirmation** fields, enter the password of the user. The password must contain at least one uppercase character (A–Z), one lowercase character (a–z), a numeral, and a special character. Password length: 8 to 50 characters. To see the entered password, you can click the show icon .
- **LDAP**

4. In the **Username** field, enter the user name of the user. The remote server user name is specified in the user@domain or domain\user format.

5. In the **Role** drop-down list, select the role of the user:

- **Administrator**
- **Tenant**

6. If you want to enable two-factor authentication for the user, select the **Two-step authentication** check box. This check box is cleared by default. The user must complete two-factor authentication the next time the user [logs in to the orchestrator web interface](#).

You cannot enable two-factor authentication for an individual user if two-factor authentication is [disabled for all users](#).

7. If you want to assign an access permission to a user, in the **Permissions** drop-down list, select the previously [created access permission](#). By default, the user gets the **Full access** permission, which grants full access to the orchestrator web interface.

8. If you want to create a [confirmation request](#) every time the user performs an action, select the **Request confirmation is required** check box. By default, the check box is cleared and the user can perform actions without confirmation.

9. In the **First name** field, enter the first name of the employee.

10. In the **Last name** field, enter the last name of the employee.

11. If necessary, enter additional information about the user:

- a. In the **Email** field, enter the email address.
- b. In the **Description** field, enter a brief description of the user.

12. Click **Create**.

The user is created and displayed in the table. By default, the user is blocked.

You must [unblock the user](#) to grant that user access to the orchestrator web interface.

Activating or blocking a user

By default, previously [created users](#) are blocked. You must unblock the user to grant that user access to the orchestrator web interface.

To block or unblock a user:

1. In the menu, go to the **Users** section.

The user management page is displayed. The **Users** tab, which is selected by default, displays the table of users.

2. Click the user that you want to unblock or block.

3. In the upper part of the displayed settings area, click **Management** → **Unblock** or **Block**.

The user is unblocked or blocked.

Editing a user

You cannot change the type and user name of the user. [Separate instructions](#) are given for changing the password of a local user.

To edit a user:

1. In the menu, go to the **Users** section.

The user management page is displayed. The **Users** tab, which is selected by default, displays the table of users.

2. Click the user that you want to edit.

3. In the displayed settings area, in the **Role** drop-down list, select the user role:

- **Administrator**
- **Tenant**

4. Enable or disable two-factor authentication for the user by doing one of the following:

- If you want to enable two-factor authentication for the user, select the **Two-step authentication** check box. The user must complete two-factor authentication the next time the user [logs in to the orchestrator web interface](#).

You cannot enable two-factor authentication for an individual user if two-factor authentication is [disabled for all users](#).

- If you want to disable two-factor authentication for the user, clear the **Two-step authentication** check box.

5. If you want to assign an access permission to a user, in the **Permissions** drop-down list, select the previously [created access permission](#). By default, the user gets the **Full access** permission, which grants full access to the orchestrator web interface.

6. If you want to create a [confirmation request](#) every time the user performs an action, select the **Request confirmation is required** check box. By default, the check box is cleared and the user can perform actions without confirmation.

7. In the **First name** field, enter the first name of the employee.

8. In the **Last name** field, enter the last name of the employee.

9. If necessary, enter additional information about the user:

a. In the **Email** field, enter the email address.

b. In the **Description** field, enter a brief description of the user.

10. Click **Save**.

The user is modified and updated in the table.

Changing the password of a local user

LDAP user passwords are stored on remote servers and cannot be changed in the orchestrator web interface.

To change the password of a local user:

1. Proceed to change the local user password:

- If you have the platform administrator role and want to change the password of a previously [created local user](#), go to the **Users** menu section, click the local user, and in the upper part of the displayed settings area, click **Management** → **Change password**.
- If you have the tenant role and want to change your own password, in the lower part of the menu click the settings icon → **Change password**.

2. This opens a window; type the new password in the **New password** and **Password confirmation** text boxes. The password must contain at least one uppercase character (A–Z), one lowercase character (a–z), a numeral, and a special character. Password length: 8 to 50 characters. To see the entered password, you can click the show icon .

3. Click **Save**.

The password of the local user is changed.

Repeated two-factor authentication of a user

You can have the user repeat the authentication if that user has lost access to the unique code for logging in to the orchestrator web interface that was generated as a result of the previous two-factor authentication.

To repeat user authentication:

1. In the menu, go to the **Users** section.

The user management page is displayed. The **Users** tab, which is selected by default, displays the table of users.

2. Click the user that you want to re-authenticate with two-factor authentication.

3. In the upper part of the displayed settings area, click **Management** → **Reinitialize two-step authentication**.

The user must complete two-factor authentication the next time the user [logs in to the orchestrator web interface](#).

Deleting a user

Deleted users cannot be restored.

To delete a user:

1. In the menu, go to the **Users** section.

The user management page is displayed. The **Users** tab, which is selected by default, displays the table of users.

2. Click the user that you want to delete.

3. In the upper part of the displayed settings area, click **Management** → **Delete**.

4. In the confirmation window, click **Delete**.

The user is deleted and is no longer displayed in the table.

Managing LDAP user groups

The table of LDAP users is displayed in the **Users** section. Information about LDAP user groups is displayed in the following table columns:

- **Name** is the name of the LDAP user group.
- **Tenant** is the [tenant](#) to which the [LDAP user group is assigned](#).
- **Role** is the role of LDAP users in the group.

The actions you can perform with the table are described in the [Managing solution component tables](#) instructions.

Creating an LDAP user group

LDAP user group credentials are stored on the remote server. If you want users in the LDAP user group to be able to log in to the orchestrator web interface using their credentials, you must first [create an LDAP connection](#) that the orchestrator uses to connect to the remote server, and then create your LDAP users or LDAP user groups.

To create an LDAP user group:

1. In the menu, go to the **Users** section.

The user management page is displayed. The **Users** tab, which is selected by default, displays the table of users.

2. Select the **Groups** tab.

A table of LDAP user groups is displayed.

3. Click **+ User group**.

4. In the displayed settings area, in the **Name** field, enter the name of the LDAP user group on the remote server in the user@domain or domain\user format.

5. In the **Role** drop-down list, select the role of LDAP users in the group:

- **Administrator**
- **Tenant**

6. If you want to assign an access permission to an LDAP user group, in the **Permissions** drop-down list, select the previously [created access permission](#). By default, the LDAP user group gets the **Full access** permission, which

grants full access to the orchestrator web interface.

7. If you want to enable two-factor authentication for the LDAP user group, select the **Two-step authentication** check box. This check box is cleared by default. Users in the LDAP user group must complete two-factor authentication the next time they [log in to the orchestrator web interface](#).

When two-factor authentication is enabled for a group of LDAP users, authenticated LDAP users are displayed in the [table of users](#). You can disable two-factor authentication for an LDAP user by [editing the user](#).

You cannot enable two-factor authentication for an LDAP user group if two-factor authentication is [disabled for all users](#).

8. Click **Create**.

The LDAP user group is created and displayed in the table.

Editing an LDAP user group

You cannot change the type and name of the LDAP user group.

To edit a user group:

1. In the menu, go to the **Users** section.
The user management page is displayed. The **Users** tab, which is selected by default, displays the table of users.
2. Select the **Groups** tab.
A table of LDAP user groups is displayed.
3. Click the LDAP user group that you want to edit.
4. In the displayed settings area, in the **Role** drop-down list, select the role of LDAP users in the group:
 - **Administrator**
 - **Tenant**
5. If you want to assign an access permission to an LDAP user group, in the **Permissions** drop-down list, select the previously [created access permission](#). By default, the LDAP user group gets the **Full access** permission, which grants full access to the orchestrator web interface.
6. Enable or disable two-factor authentication for the LDAP user group by doing one of the following:
 - If you want to enable two-factor authentication for the LDAP user group, select the **Two-step authentication** check box. Users in the LDAP user group must complete two-factor authentication the next time they [log in to the orchestrator web interface](#).
When two-factor authentication is enabled for a group of LDAP users, authenticated LDAP users are displayed in the [table of users](#). You can disable two-factor authentication for an LDAP user by [editing the user](#). If you disable two-factor authentication for an LDAP user group, the LDAP users are no longer displayed in the table of users.
You cannot enable two-factor authentication for an LDAP user group if two-factor authentication is [disabled for all users](#).
 - If you want to disable two-factor authentication for an LDAP user group, clear the **Two-step authentication** check box.

7. Click **Save**.

The LDAP user group is modified and updated in the table.

Deleting an LDAP user group

Deleted LDAP user groups cannot be restored.

To delete an LDAP user group:

1. In the menu, go to the **Users** section.

The user management page is displayed. The **Users** tab, which is selected by default, displays the table of users.

2. Select the **Groups** tab.

A table of LDAP user groups is displayed.

3. Click the LDAP user group that you want to delete.

4. In the upper part of the displayed settings area, click **Management** → **Delete**.

5. In the confirmation window, click **Delete**.

The LDAP user group is deleted and is no longer displayed in the table.

Enabling or disabling two-factor authentication for all users

You can enable or disable two-factor authentication for all users. If two-factor authentication is disabled for all users, you cannot enable two-factor authentication for local users, LDAP users, or LDAP groups. Two-factor authentication is disabled by default.

To enable or disable two-factor authentication for all users:

1. In the menu, go to the **Users** section.

The user management page is displayed. The **Users** tab, which is selected by default, displays the table of users.

2. Select the **Authentication security** tab.

3. Do one of the following:

- If you want to enable two-factor authentication for all users, select the **Two-step authentication for all users** check box. All users must complete two-factor authentication the next time a user [logs in to the orchestrator web interface](#).
- If you want to disable two-factor authentication for all users, clear the **Two-step authentication for all users** check box.

This check box is selected by default.

Two-factor authentication is enabled or disabled for all users.

Managing confirmation requests

If when [creating](#) or [editing a user](#), you selected the **Request confirmation is required** check box, a confirmation request is automatically created for each user action. You can confirm, deny, or delete the confirmation request. When a request is confirm, the corresponding action is applied; denied confirmation requests are saved in the orchestrator web interface.

To confirm, deny, or delete a confirmation request:

1. In the menu, go to the **Confirmation** section.

A table of confirmation requests is displayed. Information about confirmation requests is displayed in the following table columns:

- **Method** is the API method that was used to create the confirmation request.
- **URL** is the URL of the API.
- **Note** is a brief description of the confirmation request.
- **User** is the name of the [user](#) whose action resulted in the creation of a confirmation request.
- **Headers** are API headers.
- **Created** is the date and time when the confirmation request was created.
- **Status** is the status of the confirmation request:
 - **Confirmed**
 - **Denied**
 - **Error**
 - **Waiting confirmation**

The actions that you can perform with the table are described in the [Managing solution component tables](#) instructions.

2. Do one of the following:

- To confirm the request, click **Permit** next to it.
- To deny the request, click **Deny** next to it.
- To delete the request, click **Delete** next to it.

If you want to confirm, deny, or delete multiple confirmation requests at the same time, select check boxes next to the requests and select an action by clicking the **Action** button in the upper part of the table.

Confirmation requests are confirmed, denied, or deleted.

Limiting the duration of a user session

By default, if a user remains idle for 3600 seconds (one hour) after logging into the orchestrator web interface, the user session is ended. You can manually specify the maximum inactivity time.

To limit the duration of a user session:

1. In the lower part of the menu, click the settings icon → **Session expiration time**.
2. This opens a window; in that window, enter the time in seconds after which you want to end the session in case of inactivity. Range of values: 60 to 86,400. The default setting is 3600.
3. Click **Save**.

Users are automatically logged out of the orchestrator web interface after remaining idle for the specified amount of time.

Viewing and ending active user sessions

You can view the list of sessions established using your account, and you can end such sessions.

To view or end active user sessions:

1. In the lower part of the menu, click the settings icon → **Active sessions**.

A table of active user sessions is displayed. Information about user sessions is displayed in the following columns of the table:

- **IP address** is the IP address of the user.
- **User agent** is information about the browser and operating system of the user.
- **Date** is the start date of the user session.

The actions that you can perform with the table are described in the [Managing solution component tables](#) instructions.

2. You can end user sessions in one of the following ways:

- If you want to end a specific user session, click **End session** next to it.
- If you want to end multiple user sessions, select the check boxes next to them and in the upper part of the table, click **Actions** → **End session**.

The user sessions are ended.

Managing resources of the organization

For management purposes, the resources of your organization are logically grouped into so-called *data centers*. Data centers are combined into more abstract logical groups called *domains*. You can move data centers between domains.

Kaspersky SD-WAN uses the terms *data center* and *domain* in an unconventional way. The term 'data center' refers to a group of resources instead of a place where computer systems, servers, and equipment are located and maintained. The term 'domain' refers to a group of data centers instead of a group of computers, servers, or resources on the Internet.

The following resources are placed in data centers:

- SD-WAN and SDN Controllers.
- [Virtual infrastructure managers \(VIM\)](#).
- Zabbix proxy servers.
- [Virtual Network Function Managers \(VNFM\)](#).
- CPE device and virtual network function management subnets.

In each data center, you must create at least one management subnet to assign IP addresses to [CPE devices](#) and [virtual network functions](#) (VNFs). You can also specify DNS servers and static routes for virtual network functions.

The figure below shows four logical groups of an organization's resources (Site 1, Site 2, Site 3, and Site 4) combined into two general groups (Domain 1 and Domain 2).

The figure shows two domains, each containing two data centers.

Data centers and domains

Managing domains

The list of domains is displayed in the **Infrastructure** section, in the **Resources** pane. Under the domains, the list displays [data centers](#) added to the domains.

Creating a domain

To create a domain:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. In the upper part of the page, click **+ Domain**.

3. This opens a window; in that window, in the **Name** field, enter the name of the domain. Range of values: 1 to 50 characters.
4. If necessary, in the **Description** field, enter a brief description of the domain. Maximum length: 100 characters.
5. Click **Create**.

The domain is created and displayed in the **Resources** pane.

You can add data centers to a domain when you [create data centers](#).

Editing a domain

To edit a domain:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.
2. In the **Resources** pane, click the settings icon → **Edit** next to the domain that you want to edit.
3. This opens a window; in that window, in the **Name** field, enter the name of the domain. Range of values: 1 to 50 characters.
4. If necessary, in the **Description** field, enter a brief description of the domain. Maximum length: 100 characters.
5. Click **Save**.

The domain is modified and displayed in the **Resources** pane.

Deleting a domain

Deleted domains cannot be restored.

To delete a domain:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.
2. In the **Resources** pane, click the settings icon → **Delete** next to the domain that you want to delete.
3. In the confirmation window, click **Delete**.

The domain is deleted and is no longer displayed in the **Resources** pane.

Managing data centers

Lists of data centers are displayed in the **Infrastructure** in the **Resources** pane under [domains](#).

Creating a data center

To create a data center:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. In the upper part of the page, click **+ Data center**.

3. This opens a window; in that window, in the **Name** field, enter the name of the data center. Range of values: 1 to 50 characters.

4. If necessary, in the **Description** field, enter a brief description of the data center. Maximum length: 100 characters.

5. In the **Domain** drop-down list, select the previously [created domain](#) to which you want to add the data center.

6. If you want to deploy virtual network functions and [run scripts on CPE devices](#), in the **VNFM URL** field, enter the web address of the VNFM to which you want the orchestrator to connect. To verify that the VNFM is available, you can click **Test connection**.

7. If necessary, in the **Location** field, enter the geographical address of the data center.

8. Click **Create**.

The data center is created and displayed in the **Resources** pane.

Editing a data center

To edit a data center:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. In the **Resources** pane, click the settings icon → **Edit** next to the data center you want to edit.

3. This opens a window; in that window, in the **Name** field, enter the name of the data center. Range of values: 1 to 50 characters.

4. If necessary, in the **Description** field, enter a brief description of the data center. Maximum length: 100 characters.

5. If you want to deploy virtual network functions and [run scripts on CPE devices](#), in the **VNFM URL** field, enter the web address of the VNFM to which you want the orchestrator to connect. To verify that the VNFM is available, you can click **Test connection**.

6. If necessary, in the **Location** field, enter the geographical address of the data center.

7. Click **Save**.

The data center is modified and updated in the **Resources** pane.

Migrating a data center

To migrate a data center:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. In the **Resources** pane, click the settings icon → **Migrate** next to the data center you want to migrate.

3. This opens a window; in that window, select the previously [created domain](#) to which you want to migrate the data center.

4. Click **Migrate**.

The data center migration begins; upon completion, the data center is displayed under the new domain in the **Resources** pane.

Deleting a data center

Deleted data centers cannot be restored.

To delete a data center:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. In the **Resources** pane, click the settings icon → **Delete** next to the data center you want to delete.

3. In the confirmation window, click **Delete**.

The data center is deleted and is no longer displayed in the **Resources** pane.

Managing management subnets

To display the table of management subnets, go to the **Infrastructure** menu section, click the previously [created data center](#), and select the **IPAM** → **Subnet** tab. Information about management subnets is displayed in the following columns of the table:

- **Name** is the name of the management subnet.
- **Type** is the type of the subnet. Only management subnets are presently supported.
- **CIDR** is the IPv4 prefix of the management subnet.

- **Gateway** is the IP address of the gateway that the management subnet must assign to virtual network functions.
- **IP range** are the start and end values of the range from which the management subnet must assign IP addresses to CPE devices and virtual network functions.
- **DNS** is the IPv4 address of the DNS server that the management subnet must assign to virtual network functions.
- **Static routes** are the IPv4 addresses of the source and destination of the static route that the management subnet must assign to virtual network functions.
- **Usage** is the number of IP addresses that the management subnet has assigned to CPE devices and virtual network functions.

The table of CPE devices and virtual network functions to which the management subnet has assigned IP addresses is displayed on the **Usage** tab. Information about CPE devices and virtual network functions is displayed in the following table columns:

- **Name** is the name of the management subnet that assigned an IP address to the CPE or virtual network function.
- **IP** is the IP address assigned to the CPE device or virtual network function.
- **Client name** is the name of the CPE device or virtual network function.
- **Client type** is the type of component to which the management subnet assigned an IP address:
 - **VNF**
 - **CPE**
- **Tenant** is the [tenant](#) to which the CPE device or virtual network function is assigned.

The actions you can perform with the tables are described in the [Managing solution component tables](#) instructions.

Creating a management subnet

To create a management subnet:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.
2. In the **Resources** pane, select the previously [created domain](#) and [data center](#) to which you want to add a management subnet.
3. Select the **IPAM** tab.
A table of management subnets is displayed.
4. In the upper part of the page, click **+ Subnet**.

5. In the **Name** field, enter the name of the management subnet.

6. In the **IP version** drop-down list, select the version of IP addresses in the management subnet:

- **IPv4** (default)
- **IPv6**

7. In the **CIDR** field, enter the IPv4 address and prefix of the management subnet.

8. If you want the management subnet to assign a particular gateway to virtual network functions, enter the IPv4 address of the gateway in the **Gateway** field.

9. Specify the range from which the management subnet must assign IP addresses to CPE devices and virtual network functions:

a. Under **IP range**, click **+ Add**.

b. In the fields that are displayed, enter the start and end values for the IP address range.

The range of IP addresses is specified and displayed in the **IP range** section. You can specify multiple ranges of IP addresses; to delete a range, click the delete icon next to it.

10. Specify the DNS server that the management subnet must assign to virtual network functions:

a. Under **DNS**, click **+ Add**.

b. In the field that is displayed, enter the IPv4 address of the DNS server.

The DNS server is specified and displayed in the **DNS** section. You can specify multiple DNS servers; to delete a server, click the delete icon next to it.

11. Specify the static route that the management subnet must assign to virtual network functions:

a. Under **Static routes**, click **+ Add**.

b. In the fields that are displayed, enter the IPv4 addresses of the source and destination of the static route.

The static route is specified and displayed in the **Static routes** section. You can specify multiple static routes; to delete a static route, click the delete icon next to it.

12. Click **Create**.

The management subnet is created and displayed in the table.

Editing a management subnet

You cannot change the domain and data center that you selected when you [created the management subnet](#).

To edit a management subnet:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. In the **Resources** pane, select the previously [created domain](#) and [data center](#) to which you added a management subnet.

3. Select the **IPAM** tab.

A table of management subnets is displayed.

4. Click **Management** → **Edit** next to the management subnet that you want to edit.

5. This opens a window; in that window, in the **Name** field, enter the name of the management subnet.

6. In the **IP version** drop-down list, select the version of IP addresses in the management subnet:

- **IPv4** (default)
- **IPv6**

7. In the **CIDR** field, enter the IPv4 address and prefix of the management subnet.

8. If you want the management subnet to assign a particular gateway to virtual network functions, enter the IPv4 address of the gateway in the **Gateway** field.

9. Specify the range from which the management subnet must assign IP addresses to CPE devices and virtual network functions:

a. Under **IP range**, click **+ Add**.

b. In the fields that are displayed, enter the start and end values for the IP address range.

The range of IP addresses is specified and displayed in the **IP range** section. You can specify multiple ranges of IP addresses; to delete a range, click the delete icon next to it.

10. Specify the DNS server that the management subnet must assign to virtual network functions:

a. Under **DNS**, click **+ Add**.

b. In the field that is displayed, enter the IPv4 address of the DNS server.

The DNS server is specified and displayed in the **DNS** section. You can specify multiple DNS servers; to delete a server, click the delete icon next to it.

11. Specify the static route that the management subnet must assign to virtual network functions:

a. Under **Static routes**, click **+ Add**.

b. In the fields that are displayed, enter the IPv4 addresses of the source and destination of the static route.

The static route is specified and displayed in the **Static routes** section. You can specify multiple static routes; to delete a static route, click the delete icon next to it.

12. Click **Save**.

The subnet is modified and updated in the table.

Deleting a management subnet

Deleted management subnets cannot be restored.

To delete a management subnet:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. In the **Resources** pane, select the previously [created domain](#) and [data center](#) to which you added a management subnet.

3. Select the **IPAM** tab.

The table of management subnets is displayed.

4. Click **Management** → **Delete** next to the management subnet that you want to delete.

5. In the confirmation window, click **Delete**.

The management subnet is deleted and is no longer displayed in the table.

Managing SD-WAN and SDN Controllers

To display the table of Controllers, go to the **Infrastructure** menu section, click the previously [created data center](#), and select the **Network resources** tab. Information about Controllers is displayed in the following columns of the table:

- **Name** is the name of the Controller.
- **Transport/service strategy** is the [transport strategy](#) being used.
- **Controller nodes** are IP addresses of Controller nodes.
- **Connection type** is the type of connection of CPE devices to the Controller:
 - **Unicast**
 - **Multicast**
- **Cluster status** is the status of the cluster of Controller nodes:
 - **Up** means the cluster is operating normally.
 - **DEGRADED** means an error occurred during the operation of the cluster.
 - **Down** means the cluster is not operational.
- **Node statuses** is the status of Controller nodes:
 - **Connected (primary)** means the node is connected to the Controller and is the primary node in the cluster.
 - **Connected (single)** means the node is connected to the Controller and is the only node in the cluster.

- **Connected (secondary)** means the node is connected to the Controller and is a secondary node in the cluster.
- **Disconnected** means the node is not connected to the Controller.
- **Not in cluster** means the node is not added to a cluster.
- **Unavailable** means the node is not available.
- **Unknown** means the status of the node is unknown.

The actions you can perform with the table are described in the [Managing solution component tables](#) instructions.

Editing a Controller

To edit a Controller:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Edit** next to the Controller that you want to edit.

3. This opens a window; in that window, in the **Name** field, enter the name of the Controller. Range of values: 1 to 128 characters.

4. If necessary, in the **Description** field, enter a brief description of the Controller.

5. In the **Controller installation on <1>/<3>/<5> servers** field, select the number of Controller nodes.

6. In the **Connection type** drop-down list, select the type of connection of CPE devices to the Controller:

- **Unicast**
- **Multicast**

7. Configure the Controller node:

- a. In the **Address (IP or hostname)** field, enter the IP address or hostname of the Controller node.

- b. In the **gRPC port** field, enter the gRPC port number of the Controller node.

- c. In the **JGroups port** field, enter the jGroups port number of the Controller node.

- d. If you want to make the Controller node the primary node, select the **Primary** option.

You can configure multiple Controller nodes.

8. Click **Save**.

The Controller is modified and updated in the table.

Opening the controller configuration menu

To go to the configuration menu of the controller:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. Click **Management** → **Configuration menu** next to the controller whose configuration menu you want to manage.

This opens the controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of controller nodes.

Restarting a Controller

The changes you make to the configuration of the Controller may require reprovisioning to take effect. During reprovisioning, [Controller properties](#) are reset to their default values. This may help resolve errors.

To reprovision the Controller:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Reprovision** next to the Controller that you want to reprovision.

3. In the confirmation window, click **Reprovision**.

The controller is reprovisioned.

Downloading a file with Controller settings

You can download a file with Controller settings and [later use the file to recover the Controller](#) if necessary.

To download a file with Controller settings:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Download backup file** next to the Controller whose settings file you want to download.

A YAML file containing the Controller settings is saved to your local device.

Restoring a Controller

To restore a Controller:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Restore** next to the Controller that you want to restore.

3. This opens a window; in that window, specify the path to the previously [downloaded file with Controller settings](#).

4. Click **Restore**.

The Controller settings are modified in accordance with the file.

Deleting a Controller

Deleted Controllers cannot be restored.

To delete a Controller:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Delete** next to the Controller that you want to delete.

3. In the confirmation window, click **Delete**.

The Controller is deleted and is no longer displayed in the table.

Managing Controller properties

Properties regulate the operation of the Controller. Each property has a *change method* that determines whether the property value can be changed and when the change takes effect. The following change methods are available:

- **Read-only** means the property cannot be changed.
- **Reload** means that when a property is changed, the orchestrator commits the new value to the database of the Controller. The new value takes effect after the [Controller is restarted](#).
A property value that is in the database, but has not yet taken effect is called a *planning value*. You can delete a planning value before restarting the Controller to keep the current value.
- **Runtime** means the new value takes effect immediately when the property is modified.

Modifying properties may lead to unstable operation of the Controller, so we recommend contacting Kaspersky Technical Support before managing properties.

You can view the table of all Controller properties of the table of changeable Controller properties:

- To display the table of all Controller properties, navigate to the **Infrastructure** section, click a previously [created data center](#), select the **Network resources** tab, and click **Management** → **Properties** next to the Controller.
- To display the table of changeable properties of the Controller, navigate to the **Infrastructure** section, click a previously [created data center](#), select the **Network resources** tab, click **Management** → **Properties** next to the Controller and on the displayed page, select the **Changeable properties** tab.

Information about Controller properties is displayed in the following columns of the table:

- **Change method** is the change method of the property.
- **Property** is the name of the property.
- **Current value** is the current value of the property.
- **Planned value** is the planning value of the property. This column is displayed only on the **Changeable properties** tab.

The actions you can perform with the table are described in the [Managing solution component tables](#) instructions.

Editing a Controller property

Changes you make to the Controller properties with the Runtime change method take effect immediately. Changes you make to Controller properties with the Reload change method take effect after the [controller is restarted](#).

To change a Controller property:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.
2. Click **Management** → **Properties** next to the Controller for which you want to change a property.
The Controller properties page is displayed. By default, the **All properties** tab is selected, which displays a table of all Controller properties.
3. Select the **Changeable properties** tab.
A table of editable properties of the Controller is displayed.
4. Click **Management** → **Edit** next to the Controller property that you want to edit.
5. This opens a window; in that window, in the **Planned value** field, enter the new value of the Controller property.
6. Click **Save**.

The new value of the property with the Runtime method is displayed in the **Current value** column. The new value of a property with the Reload method is displayed in the **Planned value** column.

Resetting controller properties to default values

To reset controller properties to default values:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. Click **Management** → **Properties** next to the controller whose properties you want to reset to default values.

The controller properties page is displayed. By default, the **All properties** tab is selected, which displays a table of all controller properties.

3. Select the **Changeable properties** tab.

A table of editable properties of the controller is displayed.

4. Reset the controller properties in one of the following ways:

- If you want to reset an individual property of the controller to its default value, click **Management** → **Reset property** next to that property.
- If you want to reset all controller properties to their default values, click the settings icon in the upper part of the table → **Reset all properties**.

5. In the confirmation window, click **Reset**.

The controller properties are reset to their default values.

Deleting planning values of Controller properties

You can delete a planning value to undo a Controller property change. This action is applicable only to properties that have the Reload method.

Deleted planning values of Controller properties cannot be restored.

To delete planning values of Controller properties:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Properties** next to the Controller for which you want to delete planning values of properties.

The Controller properties page is displayed. By default, the **All properties** tab is selected, which displays a table of all Controller properties.

3. Select the **Changeable properties** tab.

A table of editable properties of the Controller is displayed.

4. Delete the planning values of Controller properties in one of the following ways:

- If you want to delete the planning value of an individual property of the Controller, click **Management** → **Delete planned value** next to that property.

- If you want to delete planning values of all Controller properties, in the upper part of the table, click the settings icon → **Delete all planned values**.

5. In the confirmation window, click **Delete**.

The planning values of Controller properties are deleted.

Viewing information about Controller nodes

To view information about Controller nodes:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the Controller for which you want to view information about nodes.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes. Information about Controller nodes is displayed in the following columns of the table:

- **Address** is the IP address of the Controller node.
- **Status** is the status of the Controller node:
 - **Connected (primary)** means the node is connected to the Controller and is the primary node in the cluster.
 - **Connected (single)** means the node is connected to the Controller and is the only node in the cluster.
 - **Connected (secondary)** means the node is connected to the Controller and is a secondary node in the cluster.
 - **Disconnected** means the node is not connected to the Controller.
 - **Not in cluster** means the node is not added to a cluster.
 - **Unavailable** means the node is not available.
 - **Unknown** means the status of the node is unknown.
- **gRPC port** is the number of the gRPC port of the Controller node.
- **JGroups port** is the JGroups port number of the Controller node.
- **Version** is the version of the controller node software.

The actions that you can perform with the table are described in the [Managing solution component tables](#) instructions.

3. If you want to view statistics for a Controller node, click **Management** → **Statistics** next to the node.

4. If you want to view the properties of a Controller node, click **Management** → **Node properties** next to the node.

Managing a VIM

You can deploy a VIM at one of your [locations](#) or on a [uCPE device](#). Deploying the VIM on location implies centralized management of the virtual network function lifecycle. Deploying the VIM on a uCPE device lets you deliver virtual network functions to remote locations and manage them locally.

To display the table of VIMs, go to the **Infrastructure** menu section, click the previously [created data center](#), and select the **IPAM** → **Compute resources** tab. Information about VIMs is displayed in the following columns of the table:

- **Name** is the name of the VIM.
- **Type** is the type of the VIM. Kaspersky SD-WAN uses the VIM from the OpenStack cloud platform.
- **Function** determines if the VIM is deployed in a data center or on a uCPE device.
- **VIM IP** is the IP address of the VIM.
- **Status** is the connection status of the VIM to the OpenStack cloud platform:
 - **Connected**
 - **Disconnected**
- **SDN cluster** is the SDN cluster to which OpenStack is connected.
- **Behind NAT** lets you specify if the VIM is behind NAT (Network Address Translation).

The actions you can perform with the table are described in the [Managing solution component tables](#) instructions.

Configuring a VIM deployed on location

To configure a VIM deployed on location:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.
2. In the **Resources** pane, select the previously [created domain](#) and [data center](#) to which the location belongs.
3. Select the **Compute resources** tab.
A table of VIMs is displayed.
4. In the upper part of the page, click **+ VIM**.
5. This opens a window; in that window, in the **Name** field, enter the name of the VIM.
6. In the **IP** field, enter the IP address or domain name for connecting the orchestrator to the VIM.

7. In the **Port** field, enter the port number for connecting the orchestrator to the VIM identification service. The default setting is 5,000.

8. In the **Protocol** drop-down list, select the protocol for connecting the orchestrator to the VIM:

- **http** (default)
- **https**

9. In the **Login** and **Password** fields, enter the user name and password of an account with administrator privileges to authenticate the orchestrator in the OpenStack cloud platform. If authentication is successful, the orchestrator gains access to managing the virtual infrastructure that is available to the administrator.

10. To specify advanced OpenStack cloud platform authentication settings for the orchestrator, follow these steps:

a. In the **Administrator project** field, enter the name of the administrator project for orchestrator authentication in this project.

b. In the **Domain** field, enter the OpenStack domain name for orchestrator authentication in this domain.

11. In the **Behind NAT** drop-down list, select whether the VIM is behind NAT:

- **Enabled** to indicate that the VIM is behind NAT and network address translation happens when it interacts with the [SD-WAN instance](#).
- **Disabled** to indicate that the VIM is not behind NAT. This is the default.

12. Specify the overcommitment ratios for physical resources:

a. In the **CPU overcommitment** field, enter the CPU core overcommitment ratio. The default setting is 1.

b. In the **RAM overcommitment** field, enter the RAM overcommitment ratio. The default setting is 1.

c. In the **Disk overcommitment** field, enter the disk space overcommitment ratio. The default setting is 1.

Overcommitment ratios let you provision virtual machines with more virtual resources than physically present. This is possible because, as a rule, virtual machines do not simultaneously use all available physical resources to the maximum. For example, if you specify a disk space overcommitment factor of 3, the available virtual disk space can be three times as large as the disk space physically available on the host.

When configuring overcommitment, you must consider how the capabilities of your hardware relate to the requirements of the virtual machines. If you specify a high overcommitment ratio for physical resources and virtual machines happen to use them up, this may lead to the network lagging and/or parts of network becoming completely unavailable.

13. In the **Parallelism** field, enter the maximum number of simultaneous operations between the orchestrator and the VIM. The default setting is 1. This setting lets you reduce the overall processing time for operations, but creates an additional load on the virtual infrastructure.

We recommend not changing the default value unless the overall operation processing speed is critical for you.

14. In the **SDN cluster** drop-down list, select the SDN cluster to which OpenStack is connected, or **None** if OpenStack is not connected to an SDN cluster.
15. In the **Maximum number of VLANs** field, enter the maximum number of VLANs that the VIM may use. This setting lets the orchestrator keep track of the number of segments available for use. Range of values: 0 to 4,094.
16. If the VIM supports SR-IOV, enter the physnet name in the **SR-IOV physical network** field. The orchestrator uses the SR-IOV physical network name to connect virtual machines with the SR-IOV interface type.
17. If you are using a network with the VLAN segmentation type for management, in the **VLAN physical network** field, enter the VLAN tag.
18. If you selected an SDN cluster in the **SDN cluster** drop-down list, configure the connection to that cluster:
 - a. If you want to map the logical networks of the SD-WAN instance to a physical network, enter the physnet name in the **OpenStack physical network** field.
 - b. In the **Interface group** drop-down list, select the port group through which all OpenStack nodes are connected to the SDN cluster.
 - c. In the **Control group** drop-down list, select the port group through which the OpenStack control nodes are connected to the SDN cluster.
 - d. If necessary, in the **Compute group** drop-down list, select the port group through which OpenStack compute nodes are connected to the SDN cluster.
19. If you selected **None** in the **SDN cluster** drop-down list, configure your network:
 - a. If you want to map the flat networks of the SD-WAN instance to a physical network, enter the physnet name in the **Flat physical network** field.
 - b. If you want to map the VXLAN of the SD-WAN instance to a physical network, enter the physnet name in the **VXLAN physical network** field.
 - c. In the **Control network segmentation** drop-down list, select the type of segmentation for isolating and securing [control plane](#) traffic in the SD-WAN structure:
 - **VLAN**
 - **VXLAN**
 - d. In the **Control segment ID** field, enter the segment ID of the management network. The range of values depends on the value selected in the **Control network segmentation** drop-down list:
 - If you selected **VLAN**, the range of values is 0 to 4,095.
 - If you selected **VXLAN**, the range of values is 0 to 16,000,000.
 - e. In the **Port security** drop-down list, select whether you want to enable the Port security function:
 - **Enabled**
 - **Disabled**
 - f. In the **Permit CIDR** field, enter the IPv4 prefix of the allowed subnet for the management network.

20. Click **Create**.

The VIM is created and displayed in the table on the **Compute resources** tab.

Configuring a VIM deployed on a uCPE device

To configure a VIM deployed on a uCPE device, you must specify the settings of the VIM in a [uCPE template](#). When you specify VIM settings in a uCPE template, such settings are propagated to all devices that are using the template.

To configure a VIM deployed on a uCPE device:

1. In the menu, go to the **SD-WAN** → **CPE templates** section.

A table of CPE templates is displayed.

2. Click the uCPE template in which you want to configure a VIM.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. Select the **VIM** tab.

The VIM settings are displayed.

4. In the **Port** field, enter the port number for connecting the orchestrator to the VIM identification service. The default setting is 5,000.

5. In the **Protocol** drop-down list, select the protocol for connecting the orchestrator to the VIM:

- **http** (default)
- **https**

6. In the **Login** and **Password** fields, enter the user name and password of an account with administrator privileges to authenticate the orchestrator in the OpenStack cloud platform. If authentication is successful, the orchestrator gains access to managing the virtual infrastructure that is available to the administrator.

7. To specify advanced OpenStack cloud platform authentication settings for the orchestrator, follow these steps:

a. In the **Administrator project** field, enter the name of the administrator project for orchestrator authentication in this project.

b. In the **Domain** field, enter the OpenStack domain name for orchestrator authentication in this domain.

8. If you are using a network with the VLAN segmentation type for management, in the **VLAN physical network** field, enter the VLAN tag.

9. In the **Behind NAT** drop-down list, select whether the VIM is behind NAT:

- **Enabled** to indicate that the VIM is behind NAT and network address translation happens when it interacts with the SD-WAN instance.
- **Disabled** to indicate that the VIM is not behind NAT. Default value.

10. Specify the overcommitment ratios for physical resources:

- a. In the **CPU overcommitment** field, enter the CPU core overcommitment ratio. The default setting is 1.
- b. In the **RAM overcommitment** field, enter the RAM overcommitment ratio. The default setting is 1.
- c. In the **Disk overcommitment** field, enter the disk space overcommitment ratio. The default setting is 1.

Overcommitment ratios let you provision virtual machines with more virtual resources than physically present. This is possible because, as a rule, virtual machines do not simultaneously use all available physical resources to the maximum. For example, if you specify a disk space overcommitment factor of 3, the available virtual disk space can be three times as large as the disk space physically available on the host.

When configuring overcommitment, you must consider how the capabilities of your hardware relate to the requirements of the virtual machines. If you specify a high overcommitment ratio for physical resources and virtual machines happen to use them up, this may lead to the network lagging and/or parts of network becoming completely unavailable.

11. In the **Maximum number of VLANs** field, enter the maximum number of VLANs that the VIM may use. This setting lets the orchestrator keep track of the number of segments available for use. Range of values: 0 to 4,094.
12. In the upper part of the settings area, click **Save** to save CPE template settings.

Editing a VIM

To edit a VIM:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.
2. In the **Resources** pane, select the previously [created domain](#) and [data center](#) to which the VIM belongs.
3. Select the **Compute resources** tab.
A table of VIMs is displayed.
4. Click **Management** → **Edit** next to the VIM that you want to edit.
5. This opens a window; in that window, in the **Name** field, enter the name of the VIM.
6. In the **IP** field, enter the IP address or domain name for connecting the orchestrator to the VIM.
7. In the **Port** field, enter the port number for connecting the orchestrator to the VIM identification service. The default setting is 5,000.
8. In the **Protocol** drop-down list, select the protocol for connecting the orchestrator to the VIM:
 - **http** (default)
 - **https**

9. In the **Login** and **Password** fields, enter the user name and password of an account with administrator privileges to authenticate the orchestrator in the OpenStack cloud platform. If authentication is successful, the orchestrator gains access to managing the virtual infrastructure that is available to the administrator.
10. To specify advanced OpenStack cloud platform authentication settings for the orchestrator, follow these steps:
 - a. In the **Administrator project** field, enter the name of the administrator project for orchestrator authentication in this project.
 - b. In the **Domain** field, enter the OpenStack domain name for orchestrator authentication in this domain.
11. In the **Behind NAT** drop-down list, select whether the VIM is behind NAT:
 - **Enabled** to indicate that the VIM is behind NAT and network address translation happens when it interacts with the [SD-WAN instance](#).
 - **Disabled** to indicate that the VIM is not behind NAT. This is the default.
12. Specify the overcommitment ratios for physical resources:
 - a. In the **CPU overcommitment** field, enter the CPU core overcommitment ratio. The default setting is **1**.
 - b. In the **RAM overcommitment** field, enter the RAM overcommitment ratio. The default setting is **1**.
 - c. In the **Disk overcommitment** field, enter the disk space overcommitment ratio. The default setting is **1**.

Overcommitment ratios let you provision virtual machines with more virtual resources than physically present. This is possible because, as a rule, virtual machines do not simultaneously use all available physical resources to the maximum. For example, if you specify a disk space overcommitment factor of 3, the available virtual disk space can be three times as large as the disk space physically available on the host.

When configuring overcommitment, you must consider how the capabilities of your hardware relate to the requirements of the virtual machines. If you specify a high overcommitment ratio for physical resources and virtual machines happen to use them up, this may lead to the network lagging and/or parts of network becoming completely unavailable.

13. In the **Parallelism** field, enter the maximum number of simultaneous operations between the orchestrator and the VIM. The default setting is **1**. This setting lets you reduce the overall processing time for operations, but creates an additional load on the virtual infrastructure.

We recommend not changing the default value unless the overall operation processing speed is critical for you.

14. In the **SDN cluster** drop-down list, select the SDN cluster to which OpenStack is connected, or **None** if OpenStack is not connected to an SDN cluster.
15. In the **Maximum number of VLANs** field, enter the maximum number of VLANs that the VIM may use. This setting lets the orchestrator keep track of the number of segments available for use. Range of values: 0 to 4,094.
16. If the VIM supports SR-IOV, enter the physnet name in the **SR-IOV physical network** field. The orchestrator uses the SR-IOV physical network name to connect virtual machines with the SR-IOV interface type.

17. If you are using a network with the VLAN segmentation type for management, in the **VLAN physical network** field, enter the VLAN tag.
18. If you selected an SDN cluster in the **SDN cluster** drop-down list, configure the connection to that cluster:
 - a. If you want to map the logical networks of the SD-WAN instance to a physical network, enter the physnet name in the **OpenStack physical network** field.
 - b. In the **Interface group** drop-down list, select the port group through which all OpenStack nodes are connected to the SDN cluster.
 - c. In the **Control group** drop-down list, select the port group through which the OpenStack control nodes are connected to the SDN cluster.
 - d. If necessary, in the **Compute group** drop-down list, select the port group through which OpenStack compute nodes are connected to the SDN cluster.
19. If you selected **None** in the **SDN cluster** drop-down list, configure your network:
 - a. If you want to map the flat networks of the SD-WAN instance to a physical network, enter the physnet name in the **Flat physical network** field.
 - b. If you want to map the VXLAN of the SD-WAN instance to a physical network, enter the physnet name in the **VXLAN physical network** field.
 - c. In the **Control network segmentation** drop-down list, select the type of segmentation for isolating and securing [control plane](#) traffic in the SD-WAN structure:
 - **VLAN**
 - **VXLAN**
 - d. In the **Control segment ID** field, enter the segment ID of the management network. The range of values depends on the value selected in the **Control network segmentation** drop-down list:
 - If you selected **VLAN**, the range of values is 0 to 4,095.
 - If you selected **VXLAN**, the range of values is 0 to 16,000,000.
 - e. In the **Port security** drop-down list, select whether you want to enable the Port security function:
 - **Enabled**
 - **Disabled**
 - f. In the **Permit CIDR** field, enter the IPv4 prefix of the allowed subnet for the management network.
20. Click **Save**.

The VIM is modified and updated in the table.

Viewing VIM usage

You can view the utilization of the following computing resources by the VIM:

- CPU
- RAM
- Disk space
- Network segments

To view VIM usage:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. In the **Resources** pane, select the previously [created domain](#) and [data center](#) to which the VIM belongs.

3. Select the **Compute resources** tab.

A table of VIMs is displayed.

4. Click **Management** → **Show usage** next to the VIM whose usage you want to view.

This opens a window with information about the usage of computing resources by the VIM.

Deleting a VIM

Deleted VIMs cannot be restored.

To delete a VIM:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. In the **Resources** pane, select the previously [created domain](#) and [data center](#) to which the VIM belongs.

3. Select the **Compute resources** tab.

A table of VIMs is displayed.

4. Click **Management** → **Delete** next to the VIM that you want to delete.

5. In the confirmation window, click **Delete**.

The VIM is deleted and is no longer displayed in the table.

Multitenancy


Kaspersky SD-WAN is a *multi-tenant* solution; its components can be shared among multiple *tenants*, that is, independent customers, offices, or divisions of your organization. Each tenant has its own [SD-WAN instance](#) and a self-service portal. Tenants are isolated and cannot access each other's self-service portals, but can use a shared [management subnet](#).

The list of tenants is displayed in the **Tenants** section. The section also displays the following areas for assigning solution components to a tenant and viewing information about tenants:

- **VIM** for assigning VIMs a tenant.
- **User groups** for assigning [user groups](#) a tenant.
- **Catalog** for assigning [network service](#) components to a tenant.
- **SD-WAN service** for viewing SD-WAN service components of a tenant.
- **Resources** for assigning compute resources to a tenant.
- **Service requests** for [viewing service requests of a tenant](#).
- **Users** for assigning [users](#) to a tenant.
- **CPEs** for [adding CPE devices](#) to a tenant.

Creating a tenant

To create a tenant:

1. In the menu, go to the **Tenants** section.
The tenant management page is displayed.
2. If you are creating the first tenant, under **Tenants**, in the **Name** field, enter the name of the tenant.
3. If you are creating your second or subsequent tenants:
 - a. In the upper part of the **Tenants** section, click **+ Tenant**.
 - b. In the **Name** field, enter the name of the tenant.
4. If necessary, in the relevant area in the lower part of the page, enter a brief description of the tenant.
5. Click the create button  plus button.

The tenant is created and displayed under **Tenants**.

Assigning a user to a tenant

To assign a user to a tenant:

1. In the menu, go to the **Tenants** section.

The tenant management page is displayed.

2. Under **Tenants**, select the tenant to which you want to assign a user.

3. Under **Users**, click **+ Edit**.

4. This opens a window; in that window, under **Users**, select a previously [created user](#) which you want to assign to the tenant.

The user is displayed under **Assign users**.

5. Click **Save**.

The user is assigned to the tenant and displayed under **Users**.

Assigning a user group to a tenant

To assign a user group to a tenant:

1. In the menu, go to the **Tenants** section.

The tenant management page is displayed.

2. Under **Tenants**, select the tenant to which you want to assign a user group.

3. Under **User groups**, click **+ Edit**.

4. This opens a window; in that window, under **Groups**, select a previously [created user group](#) which you want to assign to the tenant.

The user group is displayed under **Assign groups**.

5. Click **Save**.

The user group is assigned to the tenant and displayed under **User groups**.

Assigning compute resources to a tenant

To assign compute resources to a tenant:

1. In the menu, go to the **Tenants** section.

The tenant management page is displayed.

2. Under **Tenants**, select the tenant to which you want to assign compute resources.

3. In the upper part of the **Resources** section, click the settings icon .

4. Click the resize button  next to one of the following computation resources:

- **CPU** – virtual CPU cores
- **RAM** – RAM

- **Disk** — disk space

5. In the displayed field, enter the amount of compute resource that you want to assign to the tenant.

6. Click the save icon checkbox_icon.

The specified amount of compute resources is assigned to the tenant.

Assigning network service components to a tenant

To assign network service components to a tenant:

1. In the menu, go to the **Tenants** section.

The tenant management page is displayed.

2. Under **Tenants**, select the tenant to which you want to assign network service components.

3. Under **Catalog**, select check boxes next to the network service components that you want to assign to the tenant.

The network service components are assigned to the tenant and displayed in the **Catalog** section of the tenant's self-service portal.

Assigning a VIM to a tenant

To assign a VIM to a tenant:

1. In the menu, go to the **Tenants** section.

The tenant management page is displayed.

2. Under **Tenants**, select the tenant to which you want to assign a VIM.

3. Under **VIM**, click **+ Edit**.

4. This opens a window; in that window, under **Domain** and **Data center**, select the previously [created domain](#) and [data center](#) in which the VIM is deployed.

5. Under **VIM**, select the VIM that you want to assign to the tenant.

The VIM is displayed under **Assign VIMs**.

6. Click **Save**.

The VIM is assigned to the tenant and displayed under **VIM**.

Logging in to the tenant self-service portal

To log in to the tenant self-service portal:

1. In the menu, go to the **Tenants** section.


The tenant management page is displayed.

2. Under **Tenants**, select the tenant whose self-service portal you want to log in to.
3. Click **Connect as tenant**.

This opens a new browser tab with the tenant self-service portal and you are logged in.

Editing a tenant

To edit a tenant:

1. In the menu, go to the **Tenants** section.
The tenant management page is displayed.
2. In the **Tenants** section, click the settings icon → **Edit** next to the tenant that you want to edit.
3. In the **Name** field, enter the name of the tenant.
4. In the lower part of the page, enter a brief description of the tenant.
5. Click the save icon checkbox_icon.

The tenant is modified and updated under **Tenants**.

Deleting a tenant

Deleted tenants cannot be restored.

To delete a tenant:

1. In the menu, go to the **Tenants** section.
The tenant management page is displayed.
2. In the **Tenants** section, click the settings icon → **Delete** next to the tenant that you want to delete.
3. In the confirmation window, click **Delete**.

The tenant is deleted and is no longer displayed under **Tenants**.

Managing SD-WAN instances

An *SD-WAN instance* is the Kaspersky SD-WAN solution deployed for one [tenant](#). You can configure the SD-WAN instance to meet your organization's requirements for flexibility, security, and performance when transferring data over the WAN.

To avoid having to configure each instance from scratch, you can specify SD-WAN instance settings in a template and then use the template when deploying SD-WAN instances for your tenants. If you want a tenant to use an SD-WAN instance template, you must add that tenant to the template.

If the settings specified in the SD-WAN instance template do not match the actual settings of the tenant's instance, the solution is not deployed. For example, you may encounter an error when deploying the solution for a tenant if the SD-WAN instance template that is being used specifies the number of Controller nodes that differs from the actual number of nodes that the tenant has.

You can pool SD-WAN instances for scalability and fault tolerance, especially if a great number of CPE devices is used. Each SD-WAN instance pool is a load balancer with CPE devices as the load.

When [adding a CPE device](#), you can assign it to a pool of SD-WAN instances or to individual instances from that pool. If you assign a CPE device to a pool of SD-WAN instances, the orchestrator automatically selects from this pool the SD-WAN instance with the least number of devices and assigns the device to that instance. If the quantities of CPE devices are the same, the SD-WAN instance is selected randomly.

Managing SD-WAN instance templates

The SD-WAN instance templates table is displayed in the **SD-WAN** → **SD-WAN instance templates** section. **Default SD-WAN template** is the SD-WAN instance template that is created by default. If the tenant for which you are deploying the solution is not added to any SD-WAN instance template, that tenant uses the default template. Information about SD-WAN instance templates is displayed in the following table columns:

- **ID** is the ID of the SD-WAN instance template.
- **Name** is the name of the SD-WAN instance template.
- **Used** tells you if the template is used by [SD-WAN instances](#):
 - **Yes**
 - **No**
- **Updated** is the date and time when the SD-WAN instance template settings were last modified.
- **User** is the name of the [user](#) that created the SD-WAN instance template.

The actions that you can perform with the table are described in the [Managing solution component tables](#) instructions.

The SD-WAN instance template settings are displayed on the following tabs:

- **Information** contains basic information about the SD-WAN instance template. You can edit the name of the template in the **Name** field.
- **Traffic classes** contains settings of [traffic classes](#).

- **QoS rules** contains settings of [quality of service rules](#).
- **Transport services** contains settings of [transport services](#).
- **Tenants** contains [tenants](#) added to the SD-WAN instance template.
- **High availability** is the [number of Controller nodes](#) that will be deployed in the SD-WAN instance.
- **Transport/service strategy** is the [transport strategy](#) being used.

Creating an SD-WAN instance template

To create an SD-WAN instance template:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance templates** section.
A table of SD-WAN instance templates is displayed.
2. In the upper part of the page, click **+ SD-WAN instance template**.
3. This opens a window; in that window, enter the name of the SD-WAN instance template.
4. Click **Create**.

The SD-WAN instance template is created and displayed in the table.

Setting the default SD-WAN instance template

To set the default SD-WAN instance template:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance templates** section.
A table of SD-WAN instance templates is displayed.
2. Click the SD-WAN instance template that you want to make the default template.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays the name of the SD-WAN instance template.
3. In the upper part of the settings area, under **Actions**, click **Set as default template**.

The SD-WAN instance template becomes the default template.

Selecting the number of Controller nodes

You can select how many Controller nodes you want to be deployed in the SD-WAN instance.

To select the number of Controller nodes:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance templates** section.
A table of SD-WAN instance templates is displayed.

2. Click the SD-WAN instance template in which you want to select the number of Controller nodes.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays the name of the SD-WAN instance template.

3. Select the **High availability** tab.

4. Select the number of SD-WAN Controller nodes

5. In the upper part of the settings area, click **Save** to save the settings of the SD-WAN instance template.

Adding a tenant to an SD-WAN instance template

To add a tenant to an SD-WAN instance template:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance templates** section.

A table of SD-WAN instance templates is displayed.

2. Click the SD-WAN instance template into which you want to add a tenant.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays the name of the SD-WAN instance template.

3. Select the **Tenants** tab.

A table of tenants is displayed.

4. Click **+ Tenant**.

5. This opens a window; in that window, select the previously [created tenant](#) that you want to add to the SD-WAN instance template.

6. Click **Add**.

The tenant is added to the SD-WAN instance template and is displayed in the table.

7. In the upper part of the settings area, click **Save** to save the settings of the SD-WAN instance template.

Removing a tenant from an SD-WAN instance template

To remove a tenant from an SD-WAN instance template:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance templates** section.

A table of SD-WAN instance templates is displayed.

2. Click the SD-WAN instance template from which you want to remove a tenant.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays the name of the SD-WAN instance template.

3. Select the **Tenants** tab.

A table of tenants is displayed.

4. Click **Delete** next to the tenant that you want to remove from the SD-WAN instance template.

The tenant is removed from the SD-WAN instance template and is no longer displayed in the table.

5. In the upper part of the settings area, click **Save** to save the settings of the SD-WAN instance template.

Deleting an SD-WAN instance template

You cannot delete the default SD-WAN instance template.

Deleted SD-WAN instance templates cannot be restored.

To delete an SD-WAN instance template:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance templates** section.

A table of SD-WAN instance templates is displayed.

2. Click the SD-WAN instance template that you want to delete.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays the name of the SD-WAN instance template.

3. In the upper part of the settings area, under **Actions**, click **Delete**.

4. In the confirmation window, click **Delete**.

The SD-WAN instance template is deleted and is no longer displayed in the table.

Working with SD-WAN instances

The table of SD-WAN instances is displayed in the **SD-WAN** → **SD-WAN instances** section. Information about SD-WAN instances is displayed in the following table columns:

- **ID** is the ID of the SD-WAN instance.
- **Tenant** is the [tenant](#) for which the SD-WAN instance is deployed.
- **Status** is the status of the SD-WAN instance:
 - **Ok** means the SD-WAN instance is operating normally.
 - **Controller is absent** means no Controller is deployed for the SD-WAN instance.
 - **Error** means an error occurred during the operation of the SD-WAN instance.
 - **Deleting** means the SD-WAN instance is in the process of being deleted.
 - **Deleted** means the SD-WAN instance was deleted.

- **# of CPEs** is the number of [CPE devices added to the SD-WAN instance](#).
- **Controllers** are IP addresses and port numbers of Controllers deployed in the SD-WAN instance.
- **DC** is the [data center](#) in which SD-WAN instance is deployed.
- **VIM** is the VIM deployed in the SD-WAN instance.
- **Created** is the date and time when the SD-WAN instance was deployed.

The actions that you can perform with the table are described in the [Managing solution component tables](#) instructions.

The SD-WAN instance settings are displayed on the following tabs:

- **Configuration** contains basic information about the SD-WAN instance.
- **Monitoring** contains [SD-WAN instance monitoring results](#).
- **Service requests** contains [service requests of the SD-WAN instance](#).
- **Tenants** contains tenants added to the SD-WAN instance.

Viewing the usage of an SD-WAN instance

You can view which [CPE devices](#) are added to the SD-WAN instance.

To view the usage of an SD-WAN instance:

1. In the menu, go to the **SD-WAN** → **SD-WAN instances** section.

A table of SD-WAN instances is displayed.

2. Click the SD-WAN instance for which you want to view its usage.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the SD-WAN instance.

3. In the upper part of the settings area, under **Actions**, click **Show associated CPEs**.

This opens the **CPE** section which displays a table of CPE devices added to the SD-WAN instance.

Opening the configuration menu of the controller deployed for an SD-WAN instance

To open the configuration menu of the controller deployed for an SD-WAN instance:

1. In the menu, go to the **SD-WAN** → **SD-WAN instances** section.

A table of SD-WAN instances is displayed.

2. Click the relevant SD-WAN instance.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the SD-WAN instance.

3. In the upper part of the settings area, under **Actions**, click **Manage SD-WAN controller**.

This opens the controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of controller nodes.

Opening the topology of the SD-WAN network service deployed for an instance

To navigate to the topology of the SD-WAN network service deployed for an instance:

1. In the menu, go to the **SD-WAN** → **SD-WAN instances** section.

A table of SD-WAN instances is displayed.

2. Click the relevant SD-WAN instance.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the SD-WAN instance.

3. In the upper part of the settings area, under **Actions**, click **Manage SD-WAN network service**.

The orchestrator web interface of the SD-WAN instance is opened in a new browser tab, and you are automatically logged in and taken to the **Catalog** section. The SD-WAN network service topology is displayed in the graphical design tool.

Viewing the topology of a deployed SD-WAN instance

You can view the topology of a deployed SD-WAN instance. The topology displays tunnels and segments between CPE devices, as well as the paths within the segments.

To view the topology of a deployed SD-WAN instance:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the Controller deployed for the SD-WAN instance.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Topology** section.

The topology of the SD-WAN instance is displayed.

4. If necessary, select the following check boxes:

- Select the **Tunnel utilization** check box to display the utilization of the tunnels. The utilization level of the tunnel is represented by the following colors:

- Green — Low tunnel utilization.
- Yellow — Medium tunnel utilization.
- Red — High tunnel utilization.
- Select the **Segments** check box and in the **Segment switches** drop-down list, select two CPE devices to display all tunnels between those devices.
- Select the **Name** check box to display the names of CPE devices.
- Select the **IP address** check box to display the IP addresses of CPE devices.

By default, all check boxes are cleared.

Adding a tenant to an SD-WAN instance

You can add a tenant to a deployed SD-WAN instance. If tenants are added to the same SD-WAN instance, connectivity is established between the [CPE devices added to those tenants](#).

To add a tenant to an SD-WAN instance:

1. In the menu, go to the **SD-WAN** → **SD-WAN instances** section.

A table of SD-WAN instances is displayed.

2. Click the SD-WAN instance into which you want to add a tenant.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the SD-WAN instance.

3. Select the **Tenants** tab.

A table of tenants is displayed.

4. Click **+ Add**.

5. This opens a window; in that window, select the previously [created tenant](#) that you want to add to the SD-WAN instance.

6. In the **Maximum CPEs** field, enter the maximum number of CPE devices available to the tenant.

7. Click **Add**.

The tenant is added to the SD-WAN instance and is displayed in the table.

Removing a tenant from an SD-WAN instance

To remove a tenant from an SD-WAN instance:

1. In the menu, go to the **SD-WAN** → **SD-WAN instances** section.

A table of SD-WAN instances is displayed.

2. Click the SD-WAN instance from which you want to remove a tenant.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the SD-WAN instance.

3. Select the **Tenant self-service** tab.

A table of tenants is displayed.

4. Click **Delete** next to the tenant that you want to remove from the SD-WAN instance.

5. In the confirmation window, click **Delete**.

The tenant is deleted from the SD-WAN instance and is no longer displayed in the table.

Deleting an SD-WAN instance

When you delete an SD-WAN instance, the [CPE devices that were added to it](#) and the SD-WAN network service deployed for the instance are also automatically deleted. An alternative way of deleting an SD-WAN instance is to delete the SD-WAN [network service](#).

Deleted SD-WAN instances cannot be restored.

To delete an SD-WAN instance:

1. In the menu, go to the **SD-WAN** → **SD-WAN instances** section.

A table of SD-WAN instances is displayed.

2. Click the SD-WAN instance that you want to delete.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the SD-WAN instance.

3. In the upper part of the settings area, under **Actions**, click **Delete**.

4. In the confirmation window, click **Delete**.

The SD-WAN instance is deleted and is no longer displayed in the table.

Managing SD-WAN instance pools

The table of SD-WAN instance pools is displayed in the **SD-WAN** → **SD-WAN instance pools** section. Information about SD-WAN instance pools is displayed in the following table columns:

- **ID** is the ID of the SD-WAN instance pool.
- **Name** is the name of the SD-WAN instance pool.
- **Number of instances** is the number of SD-WAN instances in the pool.
- **# of CPEs** is the number of [CPE devices added to the SD-WAN instances](#).

- **Created** is the date and time when the SD-WAN instance pool was created.

The actions that you can perform with the table are described in the [Managing solution component tables](#) instructions.

The SD-WAN instance pool settings are displayed on the following tabs:

- **Information** contains basic information about the SD-WAN instance pool. You can rename the instance pool in the **Name** field and enter a brief description in the **Description** field.
- **SD-WAN instances** are the SD-WAN instances added to the pool.

Creating a pool of SD-WAN instances

To create a pool of SD-WAN instances:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance pools** section.
A table of SD-WAN instance pools is displayed.
2. In the upper part of the page, click **+ SD-WAN instance pool**.
3. This opens a window; in that window, enter the name of the SD-WAN instance pool.
4. Click **Create**.

The SD-WAN instance pool is created and displayed in the table.

Adding an SD-WAN instance to a pool

To add an SD-WAN instance to the pool:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance pools** section.
A table of SD-WAN instance pools is displayed.
2. Click the pool to which you want to add an SD-WAN instance.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the SD-WAN instance pool.
3. Select the **SD-WAN instances** tab.
A table of SD-WAN instances is displayed.
4. Click **+ SD-WAN instance**.
5. This opens a window; in that window, select the previously deployed SD-WAN instance that you want to add to the pool.
6. Click **Add**.

The SD-WAN instance is added to the pool and displayed in the table.

7. In the upper part of the settings area, click **Save** to save the settings of the SD-WAN instance pool.

Removing an SD-WAN instance from a pool

To remove an SD-WAN instance from a pool:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance pools** section.

A table of SD-WAN instance pools is displayed.

2. Click the pool from which you want to remove an SD-WAN instance.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the SD-WAN instance pool.

3. Select the **SD-WAN instances** tab.

A table of SD-WAN instances is displayed.

4. Click **Delete** next to the SD-WAN instance that you want to remove from the pool.

The SD-WAN instance is removed from the pool and is no longer displayed in the table.

5. In the upper part of the settings area, click **Save** to save the settings of the SD-WAN instance pool.

Deleting a pool of SD-WAN instances

Deleted SD-WAN pools cannot be restored.

To create an SD-WAN instance pool:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance pools** section.

A table of SD-WAN instance pools is displayed.

2. Click the SD-WAN instance pool that you want to delete.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the SD-WAN instance pool.

3. In the upper part of the settings area, under **Actions**, click **Delete**.

4. In the confirmation window, click **Delete**.

The SD-WAN instance pool is deleted and is no longer displayed in the table.

Managing CPE devices

[CPE devices](#) relay traffic between your organization's locations and your customers. You can purchase KESR appliances to use them as CPE devices or deploy CPE devices as virtual machines using an image received from Kaspersky. When using virtual machines, you must make sure that they satisfy the [hardware requirements](#).

For building the SD-WAN network, centralized management and core functionality, an OpenFlow virtual switch (virtual switch; vSwitch) is installed on CPE devices. For example, virtual switch is used to configure traffic streams.

To avoid configuring each device individually, you can specify the settings in the CPE template and then apply the template to devices when [adding](#) or [manually registering](#) them. When you edit a setting in a CPE template, that setting is automatically modified on all devices that are using the template.

When you edit a setting on a CPE device, that setting becomes independent of the template. When the same setting is edited in the CPE template, the change is not propagated to such a device.

Certain CPE device settings can only be specified in a template, for example, the [port number for connecting to the orchestrator](#).

New CPE devices are registered automatically, which is referred to as Zero Touch Provisioning (ZTP). You add the CPE device in the orchestrator web interface, [generate a URL with basic settings](#), and enter that URL on the device. When the CPE device connects to the orchestrator using the received settings, it is mapped to the previously added record and is automatically registered. Registration does not require connecting to Kaspersky cloud services.

You can use *two-factor authentication* to register the CPE device securely. Two-factor authentication records a token (security key) to the orchestrator database; the token is then placed on the CPE device using the URL with basic settings. Registration succeeds if, when the CPE device connects to the orchestrator, the token placed on the device matches the token in the orchestrator database.

When you [remove a CPE device](#) from the orchestrator web interface, the basic settings are retained on the device. If you need to register the device again, you must [restart the CPE device](#) to make it connect to the orchestrator, and when it appears in the orchestrator web interface, you must manually register the device. You cannot use two-factor authentication when re-registering a CPE device.

When adding and registering a CPE device, you can select if you want it to be automatically enabled after registration. When a CPE device is enabled, the CPE template is applied to it and the device becomes available for relaying traffic.

About the interaction of the CPE device and the orchestrator

After registration, the CPE device sends REST API requests to the orchestrator to receive tasks not related to virtual switch management, such as [restarting the device](#) and [updating firmware](#). Requests are sent periodically with a frequency that you can specify when [configuring the connection of the CPE device to the orchestrator and Controller](#).

To display the table of tasks performed by the orchestrator on a CPE device, go to the **SD-WAN** → **CPE** menu section and click the device. Information about tasks is displayed in the following columns of the table:

- **Type** is the type of the task.
- **Status** is the status of the task:

- **Await** means the task is saved in the orchestrator database and is waiting to be received by the CPE device.
- **Executing** means the task is running.
- **Completed** means the task is successfully completed.
- **Error** means an error occurred while running the task.
- **Last update** is the date and time of the last update of the task.

The orchestrator runs tasks on the CPE device in the following way:

1. You run a task, such as modifying [BGP](#) settings, on the CPE device using the orchestrator web interface.
2. The orchestrator saves the task in the database. In the table, the task is displayed with the **Await** status.
3. The CPE device receives the task when it sends a REST API request to the orchestrator. In the table, the task is displayed with the **Executing** status.
4. If the task finishes successfully, the CPE device reports this to the orchestrator. In the table, the task is displayed with the **Completed** status.
5. If the task fails, it is displayed in the table with the **Error** status.

Before running the task, the current settings on the CPE device are saved. If the CPE device cannot send a confirmation message to the orchestrator after successful completion of the task, after 3 attempts the previous settings are restored on the device, and the table displays the task with the **Error** status.

About the interaction of the CPE device and the Controller

After a CPE device is registered, an encrypted or unencrypted management session is established between each of its [SD-WAN interfaces of the WAN type](#) and the available Controllers. One of these sessions is the primary session, and the others are in standby mode.

Through the primary session, the CPE device receives tasks related to managing the virtual switch, for example, modifying path settings. If the primary session is terminated, a new primary session is selected in accordance with the settings that you can specify when [configuring the connection of the CPE device to the orchestrator and Controller](#).

The figure below shows sessions established between three Controllers and a CPE device with two SD-WAN interfaces of the WAN type:

- 10.0.11 → ctl1:6653
- 10.0.21 → ctl1:6654
- 10.0.11 → ctl2:6653
- 10.0.21 → ctl2:6654
- 10.0.11 → ctl3:6653
- 10.0.21 → ctl3:6654

Connection diagram of multiple CPE devices with three Controllers

Sessions between a CPE device and three Controllers

To display the table of CPE devices with information about management sessions, go to the **Infrastructure** menu section, click **Management** → **Configuration menu** next to the SD-WAN Controller to which the devices are connected, and in the displayed controller settings menu, go to the **Switches** section. Information about management sessions is displayed in the following table columns:

- **Name** is the name of the CPE device.
- **ID** is the sequence number of the CPE device. The device with the lowest sequence number was the first to connect to the Controller.
- **Status** is the status of the CPE device in relation to the Controller:
 - **Active** means the device can be used to relay traffic.
 - **Inactive** means the device cannot be used to relay traffic.
- **Connection** is the status of the CPE device connection to the Controller:
 - **Connected** means a management session is established between the device and the Controller.
 - **Disconnected** means no management session is established between the device and the Controller.
- **MAC** is the MAC address of the CPE device.
- **Interface** are SD-WAN interfaces of the WAN type from which management sessions are established with the Controller.
- **Primary session** is the SD-WAN interface of the WAN type from which the primary management session is established with the Controller.
- **IP** is the IP address of the SD-WAN interface of the WAN type from which the management session is established with the Controller.
- **Created** is the date and time when the CPE device was registered.
- **Location** is the address of the CPE device location.
- **Latency (ms.)** is the latency in milliseconds of the management session between the CPE device and the Controller.
- **Description** is a brief description of the CPE device.

Automatic registration of CPE (ZTP) devices

New CPE devices must be automatically registered using an URL with basic settings. The automatic device registration scenario involves the following steps:

1 Switching the CPE device firmware to the initial condition

For automatic registration, the [firmware](#) of the CPE device must be in the initial condition. To reset the firmware to its initial condition, connect to the CPE device console via SSH and execute the following command:

firstboot && reboot

2 Creating a CPE template

[Create a CPE template](#). You can use the created CPE template to configure other devices. This step is optional if already have a CPE template.

3 Adding a CPE device

[Add a CPE device](#). When adding the CPE device, assign a previously created template to it and select whether the device must automatically turn on after registration. The added CPE device has the *Waiting* status.

4 Two-factor authentication

If you want to register your CPE device securely, use [two-factor authentication](#). This step is optional.

5 Generating an URL with basic settings

[Generate an URL with basic CPE device settings](#).

6 Registering the CPE device

Do the following:

1. Connect to the LAN interface of the CPE device and get an IP address via DHCP.
2. Visit the URL with the basic settings of the CPE device or open the HTML file that you saved when generating the URL.
3. On the opened page, click the **Apply configuration** button.
4. Wait until the basic settings are applied and the CPE device is restarted.

If the settings are applied successfully, the CPE device connects to the orchestrator and is matched with the previously added record in the web interface; the CPE device is then registered automatically. A registered device has the *Registered* status and is in the *Activated* or *Deactivated* state.

7 Enabling the CPE device

If, when adding the CPE device, you specified that it must not be enabled automatically, [enable the device](#). An enabled CPE device has the *Registered* status and is in the *Activated* state. This step is optional.

Repeated registration of CPE devices

If you [delete a CPE device](#), the basic settings are kept on it. Such a CPE device can be re-registered without using the basic settings URL.

When re-registering a CPE device, you cannot use [two-factor authentication](#). If you want to use two-factor authentication, [automatically register the CPE device](#).

The CPE device re-registration scenario involves the following steps:

1 Creating a CPE template

[Create a CPE template](#). You can use the created CPE template to configure other devices. This step is optional if already have a CPE template.

2 Connecting the CPE device to the orchestrator

[Restart the CPE device](#) to make it connect to the orchestrator. If the connection is successful, the CPE device is displayed in the orchestrator web interface with the *Unknown* status.

3 Registering the CPE device

[Manually register the CPE device](#). During registration, assign a previously created template to the CPE device and select whether the device must be automatically enabled after registration. A registered device has the *Registered* status and is in the *Activated* or *Deactivated* state.

4 Enabling the CPE device

If, when manually registering the CPE device, you specified that it must not be enabled automatically, [turn on the device](#). An enabled CPE device has the *Registered* status and is in the *Activated* state. This step is optional.

Managing CPE templates

The table of CPE templates is displayed in the **SD-WAN** → **CPE templates** section. Information about CPE templates is displayed in the following columns of the table:

- **ID** is the ID of the CPE template.
- **Name** is the name of the CPE template.
- **Usage** shows whether the template is used by [CPE devices](#).
 - **Yes**
 - **No**
- **Updated** is the date and time when the CPE template settings were last modified.
- **User** is the name of the [user](#) which created the CPE template.
- **Owner** is the [tenant](#) to which the CPE template belongs.

The actions that you can perform with the table are described in the [Managing solution component tables](#) instructions.

CPE template settings are displayed on the following tabs:

- **Information** is the basic information about the CPE template. You can edit the name of the template in the **Name** field.
- **Multipathing** are the path settings.
- **Deactivation** are settings for [automatically removing and disabling the CPE device](#).
- **Encryption** is traffic encryption.
- **Scripts** are [scripts for additional configuration of the CPE device](#).
- The following tabs are displayed on the **SD-WAN settings** tab:
 - **Global settings** contains the [connection settings of a CPE device to the orchestrator and Controller](#).

- **Interfaces** contains [SD-WAN interfaces](#).
- **Topology** contains topology tags for building [tunnels](#) between CPE devices.
- **Network settings** contains [network interfaces](#).
- **BGP settings** is the [BGP protocol](#) for exchanging routes between CPE devices and external network devices. The following tabs are displayed on this tab:
 - **General settings** contains the [basic settings of the BGP protocol](#).
 - **Neighbors** contains [BGP peers](#).
 - **Peer groups** contains [BGP peer groups](#).
- **VRF** contains [virtual routing and forwarding tables](#).
- **OSPF** covers the [OSPF protocol](#) for route exchange between CPE devices and external network devices. The following tabs are displayed on this tab:
 - **General settings** contains [basic settings of the OSPF protocol](#).
 - **OSPF areas** contains [OSPF areas](#).
 - **OSPF interface** contains [OSPF interfaces](#).
- **Routing filters** contains settings for [filtering routes and traffic packets](#) between CPE devices and external network devices. The following tabs are displayed on this tab:
 - **Access control lists** contains [access control lists \(ACLs\)](#).
 - **Prefix lists** contains [prefix lists](#).
 - **Route maps** contains [route maps](#).
- **BFD settings** covers the [BFD protocol](#) for detecting routing failures between CPE devices and external network devices.
- **Static routes** contains [static routes](#).
- **Multicast** contains settings for transmission of multicast traffic between CPE devices and external network devices using the PIM and IGMP protocols. The following tabs are displayed on this tab:
 - **General settings** contains [basic PIM settings](#).
 - **Interfaces** contains [multicast interfaces](#).
- **VRRP** covers the [VRRP protocol](#) for high availability of CPE devices. The following tabs are displayed on this tab:
 - **VRRP instances** contains [VRRP instances](#).
 - **VRRP instance groups** contains [VRRP instance groups](#).
- **Monitoring** contains [CPE device monitoring](#) settings.

- **Transport services** contains transport services.
- **Log files** contains [logging settings](#).
- **NTP** contains [NTP servers](#) for time synchronization.
- **VIM** contains VIM settings. This tab is displayed only if the **uCPE** type is selected when creating the template.

Creating a CPE template

To create a CPE template:

1. In the menu, go to the **SD-WAN** → **CPE templates** section.
A table of CPE templates is displayed.
2. In the upper part of the page, click **+ CPE template**.
3. This opens a window; in that window, in the **Name** field, enter the name of the CPE template.
4. In the **Type** drop-down list, select the CPE template type:
 - **CPE** for a standard CPE device template. Default value.
 - **uCPE** for a uCPE device template. uCPE devices include a hypervisor, which lets you deploy virtual network functions and VIMs.
5. Click **Create**.

The CPE template is created and displayed in the table.

Exporting a CPE template

You can export a CPE template to subsequently [import it into another template](#). When you export a CPE template, an archive with the following data is saved to your local device:

- A file with the description of the CPE template in XML format. The version of the template is indicated in the description.
- [Script](#) files.
- Files required to run scripts, such as SSL certificates

To export a CPE template:

1. In the menu, go to the **SD-WAN** → **CPE templates** section.
A table of CPE templates is displayed.
2. Click the CPE template that you want to export.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. In the upper part of the settings area, under **Actions**, click **Export**.

An archive in the TAR.GZ format is saved on your local device. The archive does not contain information about CPE devices using the template.

Importing a CPE template

You can import a previously [exported template](#) into a CPE template. CPE template settings are specified in accordance with the settings of the imported template. During import, you can select the tabs that you want to leave unchanged.

A CPE template into which another template is imported remains applied to devices, but the settings of those devices are not modified.

To import a CPE template:

1. In the menu, go to the **SD-WAN** → **CPE templates** section.

A table of CPE templates is displayed.

2. Click the CPE template into which you want to import another template.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. In the upper part of the settings area, under **Actions**, click **Import**.

4. This opens a window; in that window, clear the check boxes next to the CPE template tabs that you want to leave unchanged after import.

5. In the **File** field, specify the path to the TAR.GZ archive.

6. Click **Import**.

CPE template settings are modified in accordance with the settings of the imported template.

Cloning a CPE template

You can clone a CPE template to create an identical template with a different name.

To clone a CPE template:

1. In the menu, go to the **SD-WAN** → **CPE templates** section.

A table of CPE templates is displayed.

2. Click the CPE template that you want to clone.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. In the upper part of the settings area, under **Actions**, click **Clone**.

4. This opens a window; in that window, enter the name of the new CPE template.

5. Click **Clone**.

A copy of the CPE template with the new name is created and displayed in the table.

Exporting orchestrator and Controller connection settings and SD-WAN interfaces from a CPE template

To export orchestrator and Controller connection settings and SD-WAN interfaces from a CPE template:

1. In the menu, go to the **SD-WAN → CPE templates** section.

A table of CPE templates is displayed.

2. Click the CPE template from which you want to export orchestrator and Controller connection settings and SD-WAN interfaces.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. In the upper part of the settings area, under **Actions**, click **Export SD-WAN settings**.

A JSON file named <Template name>sdwan-config is saved to your local device.

Exporting network interfaces from a CPE template

To export network interfaces from a CPE template:

1. In the menu, go to the **SD-WAN → CPE templates** section.

A table of CPE templates is displayed.

2. Click the CPE template from which you want to export network interfaces.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. In the upper part of the settings area, under **Actions**, click **Export network interfaces**.

A file in JSON format with the name <Template name>-network-config is saved to your local device.

Viewing the usage of a CPE template

You can see which [CPE devices](#) are using the template. If a CPE template is being used by at least one device, such a template cannot be [deleted](#).

To view CPE template usage:

1. In the menu, go to the **SD-WAN** → **CPE templates** section.

A table of CPE templates is displayed.

2. Click the CPE template for which you want to view the usage.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. In the upper part of the settings area, under **Actions**, click **Show associated CPEs**.

The **CPE** section is displayed with a table of CPE devices that are using the template.

Deleting a CPE template

You cannot delete a CPE template if it is being used by at least one device. You need to [look up the usage of the CPE template](#) and make sure that it is not being used by any device.

Deleted CPE templates cannot be restored.

To delete a CPE template:

1. In the menu, go to the **SD-WAN** → **CPE templates** section.

A table of CPE templates is displayed.

2. Click the CPE template that you want to delete.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. In the upper part of the settings area, under **Actions**, click **Delete**.

4. In the confirmation window, click **Delete**.

The CPE template is deleted and is no longer displayed in the table.

Managing CPE devices

The table of CPE devices is displayed in the **SD-WAN** → **CPE** section. Information about CPE devices is displayed in the following columns of the table:

- **DPID** is the DPID of the CPE device.
- **S/N** is the serial number of the CPE device.
- **Model** is the model of the CPE device.
- **SW version** is the [firmware](#) version of the CPE device. Outdated firmware is highlighted in orange.
- **CPE template** is the [CPE template](#) used by the device.

- **Name** is the name of the CPE device.
- **Role** is the role of the CPE device:
 - CPE
 - Gateway
- **Status** is the status of the CPE device.
 - **Unknown** means the CPE device is connected to the orchestrator but is not registered.
 - **Waiting** means the CPE device has been added in the orchestrator web interface, but it is not connected to the orchestrator.
 - **Registering** means the CPE device is being registered.
 - **Error** means an error occurred while registering the CPE device.
 - **Registered** means the CPE device has been registered successfully.
 - **Configuration** means [scripts](#) are being run on the CPE device.
- **State** is the state of the CPE device:
 - **Activated** means the assigned template has been applied to the CPE device on the orchestrator side. On the Controller side, the CPE device can be used to relay traffic.
 - **Deactivated** (in the **Waiting** status) means the assigned template has not been applied to the CPE device on the orchestrator side. On the Controller side, the CPE device cannot be used to relay traffic.
 - **Deactivated** (in the **Registered** status) means the orchestrator does not respond to REST API requests from the CPE device. On the Controller side, the transmission of traffic through tunnels is blocked for the CPE device.
- **Connection** reflects whether the CPE device is connected to the Controller:
 - Connected
 - Disconnected
- **Topology tags** are topology tags assigned to the CPE device.
- **Fragmentation** is the result of checking for [fragmentation of traffic packets](#) on the CPE device:
 - **Unsupported** means the CPE device cannot transmit fragmented packets.
 - **Unknown** means packet fragmentation cannot be checked on the CPE device.
 - **Supported** means the device can transmit fragmented packets.
- **Usage** reflects whether the [SD-WAN interfaces](#) of the CPE device are being used by transport services:
 - Yes
 - No

- **Transport tenant** is the [tenant](#) to which the CPE device is added.
- **Customer tenant** is the tenant of the customer organization to which the CPE device is added.
- **Location** is the address of the CPE device.
- **Management IP** is the IP address assigned to the CPE device by the [management subnet](#).
- **Controllers** are IP addresses and port number of Controllers to which the CPE device is connected.
- **Gateways** are IP addresses and port numbers of gateways to which the CPE device is connected.
- **Mobile network** is the mobile network to which the CPE device is connected.
- **Registered** is the date and time when the CPE device was registered.
- **Update** is the date and time when the CPE device settings were last modified.
- **User** is the name of the [user](#) which created the CPE device.

The actions that you can perform with the table are described in the [Managing solution component tables](#) instructions.

CPE device settings are displayed on the following tabs:

- **Configuration** is the basic information about the CPE device. You can enter a brief description of the CPE device in the **Description** field and [view the tasks being performed by the orchestrator](#) in the **Out-of-band management** table.
- **Monitoring** are [CPE device monitoring results](#).
- **Problems** are [problems that occurred while the CPE device was operational](#). In case of any problems, a red exclamation mark is displayed next to the tab.
- **Encryption** is traffic encryption.
- **Service requests** are [service requests of the CPE device](#).
- **Tags** are [tags for grouping CPE devices](#).
- **Scripts** are [scripts for additional configuration of the CPE device](#).
- The following tabs are displayed on the **SD-WAN settings** tab:
 - **Global settings** contains the [connection settings of a CPE device to the orchestrator and Controller](#).
 - **Interfaces** contains [SD-WAN interfaces](#).
- **Topology** contains topology tags for building [tunnels](#) between CPE devices.
- **Network settings** contains [network interfaces](#).
- **Firewall settings** are [firewall settings](#).
- **VRF** contains [virtual routing and forwarding tables](#).

- **BGP settings** is the [BGP protocol](#) for exchanging routes between CPE devices and external network devices. The following tabs are displayed on this tab:
 - **General settings** contains the [basic settings of the BGP protocol](#).
 - **Neighbors** contains [BGP peers](#).
 - **Peer groups** contains [BGP peer groups](#).
- **OSPF** covers the [OSPF protocol](#) for route exchange between CPE devices and external network devices. The following tabs are displayed on this tab:
 - **General settings** contains [basic settings of the OSPF protocol](#).
 - **OSPF areas** contains [OSPF areas](#).
 - **OSPF interface** contains [OSPF interfaces](#).
- **Routing filters** contains settings for [filtering routes and traffic packets](#) between CPE devices and external network devices. The following tabs are displayed on this tab:
 - **Access control lists** contains [access control lists \(ACLs\)](#).
 - **Prefix lists** contains [prefix lists](#).
 - **Route maps** contains [route maps](#).
- **BFD settings** covers the [BFD protocol](#) for detecting routing failures between CPE devices and external network devices.
- **Static routes** contains [static routes](#).
- **Multicast** contains settings for transmission of multicast traffic between CPE devices and external network devices using the PIM and IGMP protocols. The following tabs are displayed on this tab:
 - **General settings** contains [basic PIM settings](#).
 - **Interfaces** contains [multicast interfaces](#).
- **VRRP** covers the [VRRP protocol](#) for high availability of CPE devices. The following tabs are displayed on this tab:
 - **VRRP instances** contains [VRRP instances](#).
 - **VRRP instance groups** contains [VRRP instance groups](#).
- **UNIs** are [UNIs](#) on the CPE device.
- **Modems** are [CPE device modem](#) settings.
- **Tunnels** are tunnel settings.
- **Multipathing** are the path settings.
- **Activation** are [two-factor authentication settings of the CPE device](#).

- **Deactivation** are settings for [automatically removing and disabling the CPE device](#).
- **Log files** contains [logging settings](#).
- **NetFlow** contains [basic NetFlow settings](#).
- **NTP** displays [NTP servers](#) used for time synchronization.
- **Diagnostic information** displays [requests for CPE device diagnostic information](#).
- **Utilities** displays utilities for [diagnosing CPE devices](#).

Adding a CPE device

You need to add a CPE device if you are [automatically registering it \(ZTP\)](#). When adding a CPE device, you must specify the DPID so that it can be matched with the connected device. You can add a CPE device to the current [SD-WAN instance](#), a [tenant](#), or a different SD-WAN instance.

To add a CPE device:

1. Begin adding a CPE device in one of the following ways:

- If you want to add a CPE device to the current SD-WAN instance, in the menu, go to the **SD-WAN** → **CPE** section and in the upper part of the page, click **+ CPE**.
- If you want to add a CPE device to a tenant, in the menu, go to the **Tenants** section, under **Tenants**, select the previously [created tenant](#), and under **CPEs**, click **+ CPE**.
- If you want to add a CPE device to a different SD-WAN instance, navigate to the **SD-WAN**→**SD-WAN instances** subsection, click a previously deployed instance and in the upper part of the settings area, in the **Actions** section, click **Create**.

2. This opens a window; in that window, in the **Name** field, enter the name of the CPE device.

3. In the **DPID** field, enter the DPID of the CPE device.

4. In the **State** drop-down list, select the device state after registration:

- **Activated** to apply a CPE template to the device and use it to relay traffic. Default value.
- **Deactivated** to not apply a CPE template to the device.

5. If necessary, enter a brief description of the device in the **Description** field.

6. If you are adding a CPE device to an SD-WAN instance, in the **Tenant** drop-down list, select the tenant to which you want to assign the device. You can select a [pool of SD-WAN instances](#) or an individual instance from the pool.

7. If necessary, in the **Customer tenant** drop-down list, select a tenant for your client's organization.

8. If you want to create a UNI on the CPE device using a UNI template, in the **UNI template** drop-down list, select a previously [created UNI template](#).

9. In the **CPE template** drop-down list, select the previously [created CPE template](#) which you want to use to configure the CPE device.
10. In the **NetFlow template** drop-down list, select the previously [created NetFlow template](#) that you want to use to configure basic NetFlow settings on the CPE device.
11. In the **Firewall template** drop-down list, select the previously [created firewall template](#) which you want to use to configure the firewall of the CPE device.
12. Click **Next** and specify the address of the CPE device location in the **Address** field. As you enter the address, you are prompted to select an address from a drop-down list.
The address is displayed on the map.
13. Click **Add**.

The status of the device changes to *Waiting* and you get one of the following results:

- If you added the CPE device to the current SD-WAN instance, the device is displayed in the table.
- If you added the CPE device to a tenant, the device is displayed under **CPEs**.
- If you added the CPE device to a different SD-WAN instance, the orchestrator web interface of the instance is displayed in a new browser tab, and you are automatically logged in and taken to the **CPE** subsection. The CPE device is added to the table.

Generating an URL with basic CPE device settings

If you are [automatically registering a CPE device](#), you need to generate a URL with basic device settings. You can specify the template of the generated URL when [configuring the connection of the CPE device to the orchestrator and Controller](#). The generated URL contains the following information:

- [Network interfaces](#)
- Settings for connecting the [CPE device to the orchestrator and Controller](#) and [SD-WAN interfaces](#).
- [Certificates](#)
- [BGP](#) settings
- The token if [two-factor authentication](#) is being used
- [Virtual routing and forwarding tables](#).

The maximum size of a URL with basic CPE device settings may not exceed 64 KB.

To generate a URL with basic CPE device settings:

1. In the menu, go to the **SD-WAN** → **CPE** section.
A table of CPE devices is displayed.
2. Click the CPE device for which you want to generate a URL with basic settings.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. In the upper part of the settings area, under **Actions**, click **Get activation URL**.

This opens a window with the basic CPE device settings URL.

4. Save the URL with basic CPE device settings in one of the following ways:

- If you want to copy the URL, click **Copy** next to it.
- If you want to save the URL as an HTML file, click **Save to HTML** next to it.

You need to visit the URL or open the HTML file on the CPE device that you want to automatically register.

5. If you want to [install certificates on a CPE device with firmware version 23.07](#):

- a. In the **Version** drop-down list, select **23.07**.
- b. Click **Copy** next to all generated URLs.
- c. Save the copied web addresses.

You need to visit all of the copied web addresses in sequence on the CPE device where you want to install certificates.

Manually registering a CPE device

You must manually register the CPE device in the web interface when [re-registering the device](#). When registering, you do not need to connect to Kaspersky cloud services.

To manually register a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device that you want to manually register.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. In the upper part of the settings area, under **Actions**, click **Register**.

4. This opens a window; in that window, in the **State** drop-down list, select the device state after registration:

- **Activated** to apply a CPE template to the device and use it to relay traffic. Default value.
- **Deactivated** to not apply a CPE template to the device.

5. If necessary, enter a brief description of the device in the **Description** field.

6. In the **Tenant** drop-down list, select a previously [created tenant](#) to which you want to assign the device. You can select a pool of SD-WAN instances or an individual instance from the pool.
7. If necessary, in the **Customer tenant** drop-down list, select a tenant for your client's organization.
8. If you want to create a UNI on the CPE device using a UNI template, in the **UNI template** drop-down list, select a previously [created UNI template](#).
9. In the **CPE template** drop-down list, select the previously [created CPE template](#) which you want to use to configure the CPE device.
10. In the **NetFlow template** drop-down list, select the previously [created NetFlow template](#) that you want to use to configure basic NetFlow settings on the CPE device.
11. In the **Firewall template** drop-down list, select the previously [created firewall template](#) which you want to use to configure the firewall of the CPE device.
12. Click **Next** and specify the address of the CPE device location in the **Address** field. As you enter the address, you are prompted to select an address from a drop-down list.
The address is displayed on the map.
13. Click **Register**.

The CPE device status changes first to *Registering*, then to *Registered*.

Unregistering a CPE device

To unregister a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.
A table of CPE devices is displayed.
2. Click the CPE device that you want to unregister.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.
3. In the upper part of the settings area, under **Actions**, click **Unregister**.
4. In the confirmation window, click **Unregister**.

The CPE device is unregistered and the device status changes to *Waiting*.

Specifying the address of a CPE device

To specify the address of a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.
A table of CPE devices is displayed.
2. Click the CPE device whose address you want to specify.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. In the upper part of the settings area, under **Actions**, click **Set location**.

4. This opens a window; in that window, enter the address of the CPE device's location. As you enter the address, you are prompted to select an address from a drop-down list.

The address is displayed on the map.

5. Click **Save**.

The address of the CPE device is specified.

Enabling and disabling a CPE device

When a CPE device is enabled, a template is applied to it. Disabled CPE devices cannot be used to relay traffic.

To enable or disable a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device that you want to enable or disable.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. In the upper part of the settings area, under **Actions**, click **Activate** or **Deactivate**.

The CPE device is enabled or disabled.

Restarting a CPE device

To restart a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device that you want to restart.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. In the upper part of the settings area, under **Actions**, click **Reboot**.

4. In the confirmation window, click **Reboot**.

The CPE device is restarted.

Shutting down a CPE device

A CPE device is shut down by sending the `shutdown` command to its operating system.

To shut down a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device that you want to shut down.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. In the upper part of the settings area, under **Actions**, click **Shutdown**.

4. In the confirmation window, click **Shutdown**.

The CPE device is shut down.

Connecting to the CPE device console

To connect to the console of a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device to whose console you want to connect.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. In the upper part of the settings area, under **Actions**, click **Open SSH console**.

This opens the CPE device console window in a new browser tab.

Viewing the password of a CPE device

To view the password of a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device whose password you want to view.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. In the upper part of the settings area, under **Actions**, click **Show password**.

This opens a window with the CPE device password.

Exporting orchestrator and Controller connection settings and SD-WAN interfaces from a CPE device

To export orchestrator and Controller connection settings and SD-WAN interfaces from a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device from which you want to export orchestrator and Controller connection settings and SD-WAN interfaces.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. In the upper part of the settings area, under **Actions**, click **Export SD-WAN settings**.

A JSON file named <Template name>sdwan-config is saved to your local device.

Exporting network interfaces from a CPE device

To export network interfaces from a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device from which you want to export network interfaces.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. In the upper part, under **Actions** click **Export network interfaces**.

A file in JSON format with the name <Template name>-network-config is saved to your local device.

Deleting CPE devices

When you delete a CPE device, all [service interfaces created on it](#) are automatically deleted.

Deleted CPE devices cannot be restored.

To delete CPE devices:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. To delete an individual CPE device:

- a. Click the CPE device that you want to delete.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

- b. In the upper part of the settings area, under **Actions**, click **Delete**.

3. To delete multiple CPE devices:

- a. Select check boxes next to the CPE devices that you want to delete.

- b. In the upper part of the table, click **Actions** → **Delete**.

4. In the confirmation window, click **Delete**.

The CPE devices are deleted and are no longer displayed in the table.

Two-factor authentication of a CPE device

You can use *two-factor authentication* to register the CPE device securely. Two-factor authentication records a token (security key) to the orchestrator database; the token is then placed on the CPE device using the URL with basic settings. Registration succeeds if, when the CPE device connects to the orchestrator, the token placed on the device matches the token in the orchestrator database.

To use two-factor authentication for a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device for which you want to use two-factor authentication.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. Select the **Activation** tab.

Two-factor authentication settings are displayed.

4. In the **Two-factor authentication** drop-down list, select **Enabled**. By default, the **Disabled** option is selected.

5. If you want to generate a new token, click **Generate** under the **Token** field.

6. In the upper part of the settings area, click **Save** to save CPE device settings.

Managing certificates

When communicating with the orchestrator, the CPE device checks whether the orchestrator's certificates can be trusted to prevent MITM attacks. By default, the CPE device trusts public certification authorities.

If the orchestrator uses certificates signed by a custom certification authority, you must upload these certificates in the orchestrator web interface and install them on CPE devices. Standalone root certificates as well as certificate chains consisting of a root certificate and multiple intermediate certificates are supported.

30 days before the certificate expires, a notification is displayed when you log into the orchestrator web interface.

The table of certificates is displayed under **SD-WAN** → **Certificates**. Information about certificates is displayed in the following columns of the table:

- **Common name** is the domain name or host name for which the certificate is issued.
- **Organization** is the name of the organization that issued the certificate.
- **Distribute to CPEs** is the check box for installing the certificate on CPE devices. Certificates that have their check boxes selected are installed on CPE devices in the following cases:
 - [Automatic registration \(ZTP\) of a CPE device](#)
 - [CPE device restart](#)
 - [Manual installation of certificates on the CPE device](#)

Selecting certificates incorrectly may cause the CPE device to stop trusting the certificate of the orchestrator and to disconnect from it.

- **From** is the start date of certificate validity.
- **To** is the certificate expiration date.

The actions you can perform with the table are described in the [Managing solution component tables](#) instructions.

Uploading a certificate using the orchestrator web interface

To upload a certificate in the orchestrator web interface:

1. In the menu, go to the **SD-WAN** → **Certificates** section.
A table of certificates is displayed.
2. In the upper part of the page, click **+ Certificate**.

3. Specify the path to the certificate file in PEM format. Maximum file size: 16 KB.

The certificate is uploaded and displayed in the table. The *Certificate <certificate name> uploaded* message appears.

Manually installing certificates on CPE devices

To install certificates on CPE devices:

1. In the menu, go to the **SD-WAN** → **Certificates** section.

A table of certificates is displayed.

2. Select the **Distribute to CPEs** check boxes next to the previously [uploaded certificates](#) that you want to install on CPE devices.

3. Click **Apply to CPEs**.

The certificates are installed on the CPE devices. The *Certificates are applied to CPEs* message is displayed.

Scenario: installing certificates on a CPE device with firmware version 23.07

You can install a root certificate or a certificate chain signed by a custom certification authority on a CPE device with [firmware](#) version 23.07. Firmware version 23.07 is not fully supported by the current version of the orchestrator, therefore technical issues may occur when using this firmware version. We recommend updating the firmware of all CPE devices to the latest version.

The brief scenario for installing certificates on CPE devices with firmware version 23.07 involves the following steps:

1 Uploading certificates using the orchestrator web interface

[Upload a certificate using the orchestrator web interface.](#)

2 Generating an URL with basic CPE device settings

[Generate a URL with basic CPE device settings](#) and do the following:

1. In the **Version** drop-down list, select **23.07**.
2. Click **Copy** next to all generated URLs.
3. Save the copied web addresses.

3 Installing certificates on a CPE device

Visit each of the copied web address in sequence on the CPE device where you want to install certificates.

The CPE device restarts after installing each certificate.

Exporting a certificate

To export a certificate:

1. In the menu, go to the **SD-WAN** → **Certificates** section.

A table of certificates is displayed.

2. Click the certificate that you want to export.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

3. In the upper part of the settings area, under **Actions**, click **Export**.

An certificate file in the PEM format is saved on your local device.

Deleting certificates

Deleted certificates cannot be restored.

To delete certificates:

1. In the menu, go to the **SD-WAN** → **Certificates** section.

A table of certificates is displayed.

2. To delete an individual certificate:

a. Click the certificate that you want to delete

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

b. In the upper part of the settings area, under **Actions**, click **Delete**.

3. To delete multiple certificates:

a. Select check boxes next to certificates that you want to delete.

b. In the upper part of the table, click **Actions** → **Delete**.

4. In the confirmation window, click **Delete**.

The certificates are deleted and are no longer displayed in the table.

Automatically deleting and disabling CPE devices

In the CPE template or on the CPE device, you can specify the time after which the device must be [deleted](#) or [disabled](#) if the management session with the [controller](#) is terminated. Both functions are used to prevent theft of CPE devices. The automatic deletion function is also used to clean up obsolete entries from the orchestrator web interface. Both functions are disabled by default.

When you specify automatic deletion or disabling time for the CPE template, that time is automatically applied to all devices that are using the template.

To configure automatic deletion and disabling CPE devices:

1. Proceed to configure automatic deletion and disabling in one of the following ways:

- If you want to configure automatic deletion and disabling in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template and in the displayed settings area, select the **Deactivation** tab.
- If you want to configure automatic deletion and disabling on a CPE device, go to the **SD-WAN → CPE** menu section, click the device, and in the displayed settings area, select the **Deactivation** tab and select the **Override** check boxes.

The automatic deletion and disabling settings of the CPE device are displayed.

2. Enable automatic CPE device deletion:

- a. Select the **Enable** check box next to the **Delete timeout (sec.)** field.
- b. In the **Delete timeout (sec.)** field, enter the time in seconds after which the CPE device must be deleted if communication with the controller is not possible. Range of values: 60 to 31,536,000. The entered value may not be lower than the value specified for the automatic disabling.

3. Enable automatic CPE device disabling:

- a. Select the **Enable** check box next to the **Deactivation timeout (sec.)** field.
- b. In the **Deactivation timeout (sec.)** field, enter the time in seconds after which the CPE device must be disabled if communication with the controller is not possible. Range of values: 60 to 31,536,000. The entered value may not be greater than the value specified for the automatic deletion.

4. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Grouping CPE devices using tags

Tags describe CPE device settings such as model, [firmware](#) version, and location address. When you [add a CPE device](#), tags describing the model and [tenant](#) to which it belongs are automatically assigned to the device.

You can use tags to group CPE devices and perform actions on groups. For example, you can assign the same tag to CPE devices located at the same location and then [update firmware on them all](#).

To have a tag assigned, the CPE device must have the *Registered* status. Two identical tags cannot be assigned to the same CPE device.

Assigning a tag to CPE devices

To assign a tag to CPE devices:

1. In the menu, go to the **SD-WAN → CPE** section.

A table of CPE devices is displayed.

2. To assign a tag to an individual CPE device:

- a. Click the CPE device to which you want to assign a tag.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

- b. Select the **Tags** tab.

The assigned tags are displayed.


- c. Enter the tag and click the assign icon  plus button.

- d. In the upper part of the settings area, click **Save** to save CPE device settings.

3. To assign a tag to multiple CPE devices:

- a. Select check boxes next to the CPE devices to which you want to assign a tag.

- b. In the upper part of the table, click **Actions** → **Add tags**.

- c. This opens a window; in that window, enter the tag and click the assign icon  plus button.

- d. Click **Add**.

The tag is assigned to the CPE devices.

Removing a CPE device tag

To remove a tag from CPE devices:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. To remove a tag from an individual CPE device:

- a. Click the CPE device from which you want to remove a tag.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

- b. Select the **Tags** tab.

The assigned tags are displayed.

- c. Click the remove icon  next to the tag you want to remove.

- d. In the upper part of the settings area, click **Save** to save CPE device settings.

3. To remove a tag from multiple CPE devices:

- a. Select check boxes next to the CPE devices from which you want to remove a tag.

- b. In the upper part of the table, click **Actions** → **Delete tags**.

- c. This opens a window; in that window, remove the tags in one of the following ways:

- Click the remove icon next to the tag you want to remove.
- Enter the tag you want to remove and select it from the drop-down list.

d. Click **Delete**.

The CPE device tag is removed.

Configuring logs on CPE devices

Logs generated on CPE devices are stored locally or sent to an external Syslog server. When storing logs locally, you can specify a maximum size. You can specify a prefix to be assigned to logs before they are sent to the external Syslog server.

To view the local log on the CPE device, you need to [request diagnostic information](#).

You can specify log settings in a CPE template or on the device. When you specify log settings in a CPE template, such settings are automatically propagated to all devices that are using the template.

To configure logs on CPE devices:

1. Configure logs in one of the following ways:

- If you want to configure logs in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **Log files** tab.
- If you want to configure logs on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Log files** tab and select the **Override** check box.

The log settings are displayed.

2. In the **Log files size (KB)** field, enter the size of the logs on the CPE device in kilobytes. Range of values: 64 to 2048. The default setting is 64. If the maximum log size is exceeded, new logs overwrite the oldest logs.

3. If you want the CPE device to send logs to an external Syslog server, specify the Syslog server:

- a. In the **Syslog server IP/FQDN** field, enter the IP address of the Syslog server.
- b. In the **Syslog server port** field, enter the port number of the Syslog server. Range of values: 0 to 65,353.
- c. In the **Syslog server protocol** drop-down list, select the protocol for sending logs to the Syslog server:
 - **UDP** (default)
 - **TCP**

d. In the **Log files prefix** field, enter the prefix that you want the CPE device to assign to the logs. Maximum length: 256 characters.

4. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Specifying NTP servers on CPE devices

You must specify an internal or external NTP server, or a pool of servers for CPE devices to make sure accurate time is displayed on these devices. If you need to accurately display the time on network devices that are connected to a CPE device, you can use such a device as an NTP server.

You can specify the NTP server in a CPE template or on the device. When you specify an NTP server in a CPE template, this server is automatically specified on all devices that are using the template.

To specify the NTP server on CPE devices:

1. Specify the NTP server in one of the following ways:

- If you want to specify an NTP server in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **NTP** tab.
- If you want to specify an NTP server on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **NTP** tab and select the **Override** check box.

The NTP server connection settings are displayed.

2. If you do not want to specify the NTP server for the CPE device, clear the **Connect to NTP server** check box. This check box is selected by default.

3. If you want to use the CPE device as an NTP server, select the **Use CPE as NTP server** check box. This check box is cleared by default.

4. Specify an NTP server or pool of servers:

a. Under **NTP servers**, click **+ Add**.

b. In the field that is displayed, enter the IP address or FQDN of the NTP server or pool of servers. The following IP address and FQDN formats are supported:

- To specify an NTP server, enter the IP address or FQDN in the `server <IP address or FQDN>` format, for example, `server 0.pool.ntp.org`.
- To specify a pool of NTP servers, enter the IP address or FQDN in the `pool <IP address or FQDN>` format, for example, `pool pool.ntp.org`.

The NTP server is specified and displayed in the **NTP servers** section. You can specify multiple NTP servers; to delete a server, click the delete icon next to it.

5. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

You can view the time synchronization settings on the CPE device by [requesting diagnostic information](#).

Managing modems

A CPE device can have up to four modems for connecting to the cellular network. To display the table of modems, go to the **SD-WAN** → **CPE** section, click the CPE device, and in the displayed settings area, select the **Modems** tab. Information about modems is displayed in the following columns of the table:

- **Name** is the name of the modem.
- **IP** is the IP address of the modem.

- **Subnet** is the subnet to which the modem is connected.
- **Gateway** is the gateway to which the modem is connected.
- **DNS1, DNS2** are DNS servers used by the modem.
- **Signal** is the signal strength of the modem.
- **Data format** is the data transfer protocol of the modem.
- **Registration** is the registration status of the modem.
- **Network** is the network to which the modem is connected.
- **Country** is the country in which the modem is registered.
- **PLMN MCC** is the Mobile Country Code.
- **PLMN MNC** is the Mobile Network Code.
- **Roaming** whether roaming is used on the modem:
 - Yes
 - No
- **HTTP check** is the result of the modem using HTTP to check the availability of the Internet.

The actions that you can perform with the table are described in the [Managing solution component tables](#) instructions.

Managing firmware

New versions of CPE device software are distributed by Kaspersky in the form of firmware. You receive a TAR.GZ archive containing the firmware and settings files in YAML format. You must upload the firmware to the orchestrator web interface and update it on your devices.

Obsolete firmware is highlighted in orange in the **SW version** column of the [table of CPE devices](#). You can also find obsolete firmware using the **Need update** filter that is displayed in the upper part of the table.

You can update the firmware on manually selected CPE devices or devices with specified [tags](#). If you update the firmware on manually selected CPE devices, an update task is automatically created in the [task scheduler](#). If you are updating the firmware on CPE devices with the specified tags, you must manually create an update task in the task scheduler. The CPE device restarts during the firmware update process.

The table of firmware is displayed under **SD-WAN** → **Firmware**. Information about firmware is displayed in the following columns of the table:

- **Version** is the firmware version.
- **Size (MB)** is the size of the firmware archive in megabytes.
- **SHA256** is the hash of the firmware.
- **Architecture** is the instruction set architecture (ISA) of the firmware.

- **Release date** is the firmware release date.
- **Model** is the model of CPE devices with which the firmware is compatible.

The actions you can perform with the table are described in the [Managing solution component tables](#) instructions.

Uploading firmware to the orchestrator web interface

To upload firmware in the orchestrator web interface:

1. In the menu, go to the **SD-WAN** → **Firmware** section.
A table of firmware is displayed.
2. In the upper part of the page, click **+ Firmware**.
3. Enter the path to the archive with the firmware. When specifying a path, you can select multiple archives at the same time.

The firmware is uploaded and displayed in the table.

Updating firmware on manually selected CPE devices

To update the firmware on manually selected CPE devices:

1. In the menu, go to the **SD-WAN** → **CPE** section.
A table of CPE devices is displayed.
2. Select the check boxes next to the CPE devices on which you want to update the firmware.
3. In the upper part of the table, click **Actions** → **Update firmware**.
4. This opens a window; in that window, in the **Name** field, enter the name of the scheduled task.
5. In the **Version** drop-down list, select the previously [uploaded firmware](#).
6. In the **Completion date and time** field, enter the date and time when you want to run the scheduled task. By default, the date and time specified is the date and time when you started creating the scheduled task.
7. If you want to reset the CPE device to factory settings after updating the firmware, clear the **Save configuration** check box. If the check box is selected, your existing CPE device settings are not modified after a firmware update. This check box is selected by default.

When a CPE device is reset to factory settings, it is disconnected from the orchestrator. To reconnect the CPE device to the orchestrator, you must perform [automatic registration \(ZTP\)](#).

8. The **Force update** check box lets you force the firmware update, even if the CPE's internal check shows that the new firmware is incompatible with the old one. This check box is cleared by default.
9. Click **Next**.

Two tables of CPE devices are displayed. Firmware of CPE devices in the upper table is updated. Firmware of CPE devices in the lower table is not updated. Information about devices is displayed in the following columns:

- **DPID** is the DPID of the CPE device.
- **Model** is the model of the CPE device.
- **Name** is the name of the CPE device.
- **SW version** is the firmware version of the CPE device.
- **Transport tenant** is the [tenant](#) to which the CPE device is added.
- **Reason** is the reason why the firmware cannot be updated. This column is displayed only in the lower table.

If you find that the lower table includes CPE devices on which you do not want to update the firmware, you can move these devices to the upper table.

10. Click **Schedule**.

The scheduled task for updating the firmware is created and displayed in the **Scheduler** section. The firmware update on the CPE device starts at the configured time.

Updating firmware on CPE devices with specific tags

To update firmware on CPE devices with specific tags:

1. In the menu, go to the **Scheduler** section.
The table of scheduled tasks is displayed.
2. In the upper part of the page, click **+ Delayed task**.
3. This opens a window; in that window, in the **Type** drop-down list, select **Delayed firmware update**.
4. In the **Name** field, enter the name of the scheduled task.
5. In the **Version** drop-down list, select the previously [uploaded firmware](#).
6. In the **Completion date and time** field, enter the date and time when you want to run the scheduled task. By default, the date and time specified is the date and time when you started creating the scheduled task.
7. If you want to reset the CPE device to factory settings after updating the firmware, clear the **Save configuration** check box. If the check box is selected, your existing CPE device settings are not modified after a firmware update. This check box is selected by default.

When a CPE device is reset to factory settings, it is disconnected from the orchestrator. To reconnect the CPE device to the orchestrator, you must perform [automatic registration \(ZTP\)](#).

8. The **Force update** check box lets you force the firmware update, even if the CPE's internal check shows that the new firmware is incompatible with the old one. This check box is cleared by default.
9. In the **Tags** field, enter the tags of CPE devices on which you want to update the firmware.

10. Click **Next**.

Two tables of CPE devices are displayed. Firmware of CPE devices in the upper table is updated. Firmware of CPE devices in the lower table is not updated. Information about devices is displayed in the following columns:

- **DPID** is the DPID of the CPE device.
- **Model** is the model of the CPE device.
- **Name** is the name of the CPE device.
- **SW version** is the firmware version of the CPE device.
- **Transport tenant** is the [tenant](#) to which the CPE device is added.
- **Reason** is the reason why the firmware cannot be updated. This column is displayed only in the lower table.

If you find that the lower table includes CPE devices on which you do not want to update the firmware, you can move these devices to the upper table.

11. Click **Create**.

The scheduled task for updating the firmware is created and displayed in the table. The firmware update on the CPE device starts at the configured time.

Deleting firmware

You cannot delete firmware that is being used in a scheduled task.

Deleted firmware cannot be restored.

To delete firmware:

1. In the menu, go to the **SD-WAN** → **Firmware** section.
A table of firmware is displayed.
2. Select check boxes next to firmware that you want to delete.
3. In the upper part of the table, click **Actions** → **Delete**.
4. In the confirmation window, click **Delete**.

The firmware is deleted and is no longer displayed in the table.

Additional configuration of CPE devices using scripts

You can use scripts for additional configuration of CPE devices. To have a script automatically added to all devices that use a CPE template, you can add the script to the template. Added scripts can be run automatically or manually. Scripts are run automatically when the conditions specified in the script settings are satisfied, for example, when a CPE device is registered.

Running scripts is the responsibility of VNFM, so network connectivity between VNFM and CPE devices must be ensured before you begin working with scripts. By default, the CPE template specifies the port number that VNFM uses to connect to the device and the name of the user on whose behalf VNFM must run scripts. You can change the port number and user name if necessary.

The table of scripts is displayed in the CPE template and on the device:

- To display the table of scripts in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template, and in the displayed settings area, select the **Scripts** tab.
- To display the table of scripts on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Scripts** tab.

Information about scripts is displayed in the following columns of the table:

- **Name** is the script name.
- **Executor** is the interpreter.
- **Authentication** is the type of VNFM authentication in the CPE device.
- **Custom executor** is the path to the custom interpreter.
- **Timeout (sec.)** is the time in seconds after which VNFM stops attempting to run a script that could not run the first time.
- **Repeat execution** specifies whether or not the script must be run again:
 - **Yes**
 - **No**
- **Stage** is the stage of the CPE device operation at which VNFM must run the script.
- **Script** is name of the script file or the Ansible playbook file.
- **File** is the name of the archive with additional files that the script requires to run.
- **Actions** contains the actions that can be performed with the script.

Adding a script

You can add a script to a CPE template. When you add a script to a CPE template, the script is automatically added on all devices that are using the template.

To add a script:

1. In the menu, go to the **SD-WAN** → **CPE templates** section.
A table of CPE templates is displayed.
2. Click the CPE template to which you want to add a script.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. Select the **Scripts** tab.

This displays the port number that VNFM uses to connect to the CPE device, credentials of the user for running scripts, and the table of script if at least one script has been added.

4. Click **+ Script**.

5. This opens a window; in that window, in the **Name** field, enter the name of the script. Maximum length: 255 characters.

6. In the **Timeout (sec.)** field, enter the time in seconds after which the VNFM must stop attempting to run a script that could not run the first time. The default setting is 360.

7. In the **Executor** drop-down list, select one of the following values:

- **Ansible** (default)
- **Shell**
- **Expect**
- **Custom** to use an interpreter on the CPE device. If you select this value, enter the path to the interpreter in the **Custom executor** field.

8. In the **Stage** drop-down list, select the stage of CPE device operation at which VNFM must run the script:

- **Registration** (default).
- **Deletion**
- **Manually** to run the script only manually

9. If you need to run the script again, select the **Repeat execution** check box. This check box is cleared by default. Consider the following special considerations for re-running a script:

- If in the **Stage** drop-down list, you selected **Registration**, the script is re-run in cases of registration, powering on, and [restart of the CPE device](#).
- If in the **Stage** drop-down list, you selected **Deletion**, the script does not run again.
- If in the **Stage** drop-down list, you selected **Manually**, the script is re-run in cases of powering on and restart of the CPE device.

10. In the **Script** field, enter the path to the script file or to the Ansible playbook script file.

11. If necessary, in the **File** field, specify the path to the archive with additional files required to run the script. Supported formats of archives with files: TAR.GZ and ZIP.

12. Click **Save**.

The script is created and displayed in the table.

13. In the upper part of the settings area, click **Save** to save CPE template settings.

Manually running scripts

You can manually run an individual script or all scripts in a CPE template or on a device. When you run scripts in a CPE template, these scripts are automatically run on all devices that are using the template or on devices with the specified [tags](#).

Manually running scripts in a CPE template

To manually run scripts in a CPE template:

1. In the menu, go to the **SD-WAN** → **CPE templates** section.

A table of CPE templates is displayed.

2. Click the CPE template in which you want to run scripts.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. Select the **Scripts** tab.

This displays the port number that VNFMs use to connect to the CPE device, credentials of the user for running scripts, and the table of script if at least one script has been added.

4. To run an individual script:

- a. Click **Run** next to the script that you want to run.

- b. This opens a window; in that window, select the CPE devices on which you want to run the script:

- **Run the script <script name> on all related CPEs** to run the script on all devices that are using the CPE template. Default value.
- **Run the script <script name> on all related CPEs with specified tags** to run the script on devices that are using the CPE template and have specific tags. If you select this value, specify the tags in the lower part of the window.

5. To run all scripts:

- a. In the upper part of the settings area, under **Actions**, click **Run scripts**.

- b. This opens a window; in that window, select the CPE devices on which you want to run scripts:

- **Run all scripts on related CPEs** to run the scripts on all devices that are using the CPE template. Default value.
- **Run all scripts on related CPEs with specified tags** to run the scripts on devices that are using the CPE template and have the specified tags. If you select this value, specify the tags in the lower part of the window.

6. Click **Run**.

The scripts are run.

Manually running scripts on CPE devices.

To manually run scripts on a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device on which you want to run scripts.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. Select the **Scripts** tab.

This displays the port number that VNFM uses to connect to the CPE device, credentials of the user for running scripts, and the table of script if at least one script has been added.

4. Do one of the following:

- If you want to run an individual script, click **Run** next to the relevant script.
- If you want to run all scripts, in the upper part of the settings area, under **Actions**, click **Run scripts**.

5. This opens a window; in that window, click **Run**.

The scripts are run.

Scheduling scripts

Scheduled tasks for running scripts on CPE devices can be created in the [task scheduler](#). When creating a scheduled task, you must select a CPE template, scripts, and devices on which you want to run the scripts.

You can run scripts on all devices that are using the CPE template or on a subset of devices by specifying [tags](#) or manually selecting the devices.

To create a scheduled script task:

1. In the menu, go to the **Scheduler** section.

The table of scheduled tasks is displayed.

2. In the upper part of the page, click **+ Delayed task**.

3. This opens a window; in that window, in the **Type** drop-down list select **Script execution**.

4. In the **Name** field, enter the name of the scheduled task.

5. In the **CPEs to run script on** drop-down list, select the CPE devices on which you want to run the scripts:

- **All CPEs with selected template** to run the scripts on all devices that are using the CPE template.
- **All CPEs with selected template and specific tags** to run the scripts on devices that are using the CPE template and have the specified tags. If you select this value, specify the CPE device tags in the **Tags** field.

- **Specific CPEs with selected template** to run scripts for manually selected devices using the CPE template. If you select this value, select the CPE devices under **CPEs**.

6. Under **CPE template**, select the CPE template that contains the scripts that you want to run.

7. Under **Scripts**, select the scripts that you want to run.

8. In the **Completion date and time** field, enter the date and time when you want to run the scheduled task. By default, the date and time specified is the date and time when you started creating the scheduled task.

9. Click **Create**.

A scheduled task for running the script is created and displayed in the table.

Editing a script

You can only edit a script in the CPE template. When you edit a script in a CPE template, the script is automatically modified on all devices that are using the template.

To edit a script:

1. In the menu, go to the **SD-WAN** → **CPE templates** section.

A table of CPE templates is displayed.

2. Click the CPE template in which you want to edit a script.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. Select the **Scripts** tab.

This displays the port number that VNFMs use to connect to the CPE device, credentials of the user for running scripts, and the table of script if at least one script has been added.

4. Click **Edit** next to the script that you want to edit.

5. This opens a window; in that window, in the **Name** field, enter the name of the script. Maximum length: 255 characters.

6. In the **Timeout (sec.)** field, enter the time in seconds after which the VNFMs must stop attempting to run a script that could not run the first time. The default setting is 360.

7. In the **Executor** drop-down list, select one of the following values:

- **Ansible** (default)
- **Shell**
- **Expect**
- **Custom** to use an interpreter on the CPE device. If you select this value, enter the path to the interpreter in the **Custom executor** field.

8. In the **Stage** drop-down list, select the stage of CPE device operation at which VNFMs must run the script:

- **Registration** (default).
 - **Deletion**
 - **Manually** to run the script only manually.
9. If you need to run the script again, select the **Repeat execution** check box. This check box is cleared by default. Consider the following special considerations for re-running a script:
- If in the **Stage** drop-down list, you selected **Registration**, the script is re-run in cases of registration, powering on, and [restart of the CPE device](#).
 - If in the **Stage** drop-down list, you selected **Deletion**, the script does not run again.
 - If in the **Stage** drop-down list, you selected **Manually**, the script is re-run in cases of powering on and restart of the CPE device.
10. In the **Script** field, enter the path to the script file or to the Ansible playbook script file.
11. If necessary, in the **File** field, specify the path to the archive with additional files required to run the script. Supported formats of archives with files: TAR.GZ and ZIP.
12. Click **Save**.
The script is modified and updated in the table.
13. In the upper part of the settings area, click **Save** to save CPE template settings.

Deleting a script

You can only delete a script in the CPE template. When you delete a script in a CPE template, the script is automatically deleted on all devices that are using the template.

Deleted scripts cannot be restored.

To delete a script:

1. In the menu, go to the **SD-WAN** → **CPE templates** subsection.
A table of CPE templates is displayed.
2. Click the CPE template.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.
3. Select the **Scripts** tab.
This displays the port number that VNFMs use to connect to the CPE device, credentials of the user for running scripts, and the table of script if at least one script has been added.
4. Click **Delete** next to the script that you want to delete.
The script is deleted and is no longer displayed in the table.

5. In the upper part of the settings area, click **Save** to save CPE template settings.

Managing network interfaces

Network interfaces correspond to physical ports and virtual interfaces of the CPE device's operating system that connect to the WAN or the LAN. You must map the network interfaces of the CPE device to the OpenFlow ports of the virtual switch using [SD-WAN interfaces](#).

The table of network interfaces is displayed in the CPE template and on the device:

- To display the table of network interfaces in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **Network settings** tab.
- To display the table of network interfaces on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Network settings** tab.

Information about network interfaces is displayed in the following columns of the table:

- **Alias** is the name of the network interface for mapping the network interface to an OpenFlow port. You specify this name when [creating an SD-WAN interface of the WAN type](#).
- **Inherited** specifies whether the network interface is inherited from the CPE template:
 - **Yes**
 - **No**

This column is displayed only on the CPE device.

- **Interface name** is the name of the physical port or virtual interface of the operating system of the CPE device.
- **Protocol** is the method of assigning an IP address to the network interface:
 - **DHCP client** means the IP address is automatically assigned by DHCP.
 - **Static IPv4 address** means an IPv4 address is statically assigned.
 - **Static IPv6 address** means an IPv6 address is statically assigned.
 - **QMI** means LTE network connection settings are specified manually.
 - **PPPoE** means the PPPoE server connection settings are specified manually.
 - **None** means an IP address is not assigned.
- **IP/mask** are the IP address, mask, and default gateway of the network interface.
- **Enable automatically** specifies whether the network interface must be automatically enabled when the CPE device is powered on:
 - **Yes**
 - **No**

Creating network interfaces

You can create a network interface in a CPE template or on a device. When you create a network interface in a CPE template, the interface is automatically created on all devices that are using the template.

Creating a network interface with automatic assignment of an IP address via DHCP

To create a network interface with automatic assignment of an IP address via DHCP:

1. Create a network interface in one of the following ways:

- If you want to create a network interface in a CPE template, go to the **SD-WAN** → **CPE templates** section, click the template and in the displayed settings area, select the **Network settings** tab.
- If you want to create a network interface on a CPE device, go to the **SD-WAN** → **CPE** section, click the device and in the displayed settings area, select the **Network settings** tab.

The table of network interfaces is displayed.

2. Click **+ Network interface**.

3. This opens a window; in that window, in the **Alias** field, enter the name of the network interface for mapping the network interface to an OpenFlow port. You must specify this alias when [creating an SD-WAN interface of the WAN type](#). Maximum length: 15 characters.

4. If you want to add a network interface to a firewall zone, in the **Zone** drop-down list, select a previously [created firewall zone](#).

5. In the **Interface name** field, enter the name of the physical port or virtual interface of the operating system of the CPE device. Maximum length: 256 characters. For example, you can enter eth0, eth1, eth2, or tun0. To create a bridge from multiple interfaces, enter their names separated by spaces.

If you want to assign an outer VLAN tag to a network interface, enter a period (.) after the physical port or virtual interface name of the operating system, and then enter the outer VLAN tag. For example, you can enter eth2.150.

6. If you want to create a bridge from physical or virtual interfaces whose names are specified in the **Interface name** field:

- a. Select the **Bridge** check box. This check box is cleared by default.
- b. If you want to use STP on the bridge to prevent routing loops, select the **STP** check box. This check box is cleared by default.
- c. In the **Age (sec.)** field, enter the duration in seconds for which you want dynamic records to be stored in the MAC table of the bridge. If you want to use the bridge as a hub, enter 0 in this field. Range of values: 0 to 86,400.

7. If you want to enable the [NetFlow protocol](#) on the network interface, select the **NetFlow** check box. This check box is cleared by default.

8. In the **Protocol** drop-down list, select **DHCP client**.
9. If you do not want the network interface to be automatically enabled when the CPE device is enabled, clear the **Enable automatically** check box. This check box is selected by default.
10. If you want an IP address, route, and default gateway automatically assigned to the network interface, select the **Force IP, route, and gateway** check box. This check box is cleared by default.
11. If you do not want the route obtained via DHCP to be used by network interface by default, clear the **Use default route** check box. This check box is selected by default.
12. If necessary, specify a DNS server for the network interface:
 - a. Under **DNS servers**, click **+ Add**.
 - b. In the field that is displayed, enter the IP address of the DNS server.

The DNS server is specified and displayed in the **DNS servers** section. You can specify multiple DNS servers; to delete a server, click the delete icon next to it.
13. In the **Override MAC** field, enter the MAC address of the network interface. The entered value replaces the actual MAC address of the network interface.
14. In the **Override MTU** field, enter the MTU for the network interface. The entered value overrides the default MTU.
15. If you are creating the first network interface to be mapped to the SD-WAN interface of the WAN type, in the **Route metric** field, enter **100**. For each subsequent network interface that will be mapped to the SD-WAN interface of the WAN type, increment this value by 1. For example, for the second network interface, enter **101**.
16. Click **Create**.

The network interface is created and displayed in the table.
17. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Creating a network interface with a static IPv4 address

To create a network interface with a static IPv4 address:

1. Create a network interface in one of the following ways:
 - If you want to create a network interface in a CPE template, go to the **SD-WAN → CPE templates** section, click the template and in the displayed settings area, select the **Network settings** tab.
 - If you want to create a network interface on a CPE device, go to the **SD-WAN → CPE** section, click the device and in the displayed settings area, select the **Network settings** tab.

The table of network interfaces is displayed.

2. Click **+ Network interface**.
3. This opens a window; in that window, in the **Alias** field, enter the name of the network interface for mapping the network interface to an OpenFlow port. You must specify this alias when [creating an SD-WAN interface of the WAN type](#). Maximum length: 15 characters.

4. If you want to add a network interface to a firewall zone, in the **Zone** drop-down list, select a previously [created firewall zone](#).
5. In the **Interface name** field, enter the name of the physical port or virtual interface of the operating system of the CPE device. Maximum length: 256 characters. For example, you can enter eth0, eth1, eth2, or tun0. To create a bridge from multiple interfaces, enter their names separated by spaces.

If you want to assign an outer VLAN tag to a network interface, enter a period (.) after the physical port or virtual interface name of the operating system, and then enter the outer VLAN tag. For example, you can enter eth2.150.
6. If you want to create a bridge from physical or virtual interfaces whose names are specified in the **Interface name** field:
 - a. Select the **Bridge** check box. This check box is cleared by default.
 - b. If you want to use STP on the bridge to prevent routing loops, select the **STP** check box. This check box is cleared by default.
 - c. In the **Age (sec.)** field, enter the duration in seconds for which you want dynamic records to be stored in the MAC table of the bridge. If you want to use the bridge as a hub, enter 0 in this field. Range of values: 0 to 86,400.
7. If you want to enable the [NetFlow protocol](#) on the network interface, select the **NetFlow** check box. This check box is cleared by default.
8. In the **Protocol** drop-down list, select **Static IPv4 address**.
9. If you do not want the network interface to be automatically enabled when the CPE device is enabled, clear the **Enable automatically** check box. This check box is selected by default.
10. If you want an IP address, route, and default gateway automatically assigned to the network interface, select the **Force IP, route, and gateway** check box. This check box is cleared by default.
11. In the **IPv4 address and subnet mask input type** drop-down list, select the method for assigning an IPv4 address to the network interface:
 - **Manually** to manually assign an IPv4 address. If you select this option, do the following:
 - a. In the **IPv4 address** field, enter the IPv4 address of the network interface.
 - b. In the **IPv4 netmask** field, enter the subnet mask of the network interface.
 - **From IP pool** to assign an IPv4 address from the specified range of IP addresses. If you select this value, in the **IP Pool** drop-down list, select a previously [created range of IP addresses](#).
 - **From subnet pool** to assign an IPv4 address from the specified range of subnets. If you select this value, in the **Subnet Pool** drop-down list, select a previously [created range of subnets](#).
12. In the **IPv4 gateway** field, enter the IPv4 address of the default gateway.
13. In the **IPv4 broadcast** field, enter the broadcast address of the network interface. If you do not specify a value for this setting, it is generated automatically.
14. If necessary, specify a DNS server for the network interface:
 - a. Under **DNS servers**, click **+ Add**.

b. In the field that is displayed, enter the IP address of the DNS server.

The DNS server is specified and displayed in the **DNS servers** section. You can specify multiple DNS servers; to delete a server, click the delete icon next to it.

15. In the **Override MAC** field, enter the MAC address of the network interface. The entered value replaces the actual MAC address of the network interface.
16. In the **Override MTU** field, enter the MTU for the network interface. The entered value overrides the default MTU.
17. If you are creating the first network interface to be mapped to the SD-WAN interface of the WAN type, in the **Route metric** field, enter **100**. For each subsequent network interface that will be mapped to the SD-WAN interface of the WAN type, increment this value by 1. For example, for the second network interface, enter **101**.
18. Under **DHCP server**, in the **Type** drop-down list, select the operating mode of the DHCP server for the network interface:
 - **Disabled** (default)
 - **Relay** If you select this value, enter the IP address of the DHCP server in the **DHCP server IP** field.
 - **Server**
19. If the **Type** drop-down list, you selected **Server**, specify the DHCP server settings:

a. In the **First IP** field, enter the offset from the base IP address of the network interface for deriving the lowest IP address that can be leased to clients. The default setting is **100**. You can enter a value greater than 255 for large subnets.

b. In the **Limit** field, enter the maximum number of IP addresses that can be leased to clients. Range of values: 1 to 250. The default setting is **150**.

c. In the **Lease time** field, enter the maximum time, in hours, for which an individual IP address can be leased to a client. Range of values: 1 to 250. The value is specified in the following format: < number of hours >h. For example, if you want the maximum lease time to be 5 hours, enter 5h. The default setting is 12h.

d. If necessary, specify the DHCP option:

1. Under **DHCP options**, click **+ Add**.

2. In the field that is displayed, enter the number of the DHCP option in accordance with the [RFC 1533](#) standard. Maximum length: 250 characters.

The DHCP option is specified and displayed under **DHCP options**. You can specify multiple DHCP options; to delete an option, click the delete icon next to it.

20. Click **Create**.

The network interface is created and displayed in the table.

21. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Creating a network interface with a static IPv6 address

To create a network interface with a static IPv6 address:

1. Create a network interface in one of the following ways:

- If you want to create a network interface in a CPE template, go to the **SD-WAN** → **CPE templates** section, click the template and in the displayed settings area, select the **Network settings** tab.
- If you want to create a network interface on a CPE device, go to the **SD-WAN** → **CPE** section, click the device and in the displayed settings area, select the **Network settings** tab.

The table of network interfaces is displayed.

2. Click **+ Network interface**.

3. This opens a window; in that window, in the **Alias** field, enter the name of the network interface for mapping the network interface to an OpenFlow port. You must specify this alias when [creating an SD-WAN interface of the WAN type](#). Maximum length: 15 characters.

4. If you want to add a network interface to a firewall zone, in the **Zone** drop-down list, select a previously [created firewall zone](#).

5. In the **Interface name** field, enter the name of the physical port or virtual interface of the operating system of the CPE device. Maximum length: 256 characters. For example, you can enter `eth0`, `eth1`, `eth2`, or `tun0`. To create a bridge from multiple interfaces, enter their names separated by spaces.

If you want to assign an outer VLAN tag to a network interface, enter a period (.) after the physical port or virtual interface name of the operating system, and then enter the outer VLAN tag. For example, you can enter `eth2.150`.

6. If you want to create a bridge from physical or virtual interfaces whose names are specified in the **Interface name** field:

- a. Select the **Bridge** check box. This check box is cleared by default.
- b. If you want to use STP on the bridge to prevent routing loops, select the **STP** check box. This check box is cleared by default.
- c. In the **Age (sec.)** field, enter the duration in seconds for which you want dynamic records to be stored in the MAC table of the bridge. If you want to use the bridge as a hub, enter `0` in this field. Range of values: 0 to 86,400.

7. If you want to enable the [NetFlow protocol](#) on the network interface, select the **NetFlow** check box. This check box is cleared by default.

8. In the **Protocol** drop-down list, select **Static IPv6 address**.

9. If you do not want the network interface to be automatically enabled when the CPE device is enabled, clear the **Enable automatically** check box. This check box is selected by default.

10. If you want an IP address, route, and default gateway automatically assigned to the network interface, select the **Force IP, route, and gateway** check box. This check box is cleared by default.

11. In the **IPv6 address** field, enter the IPv6 address of the network interface. You can specify multiple addresses, separating them with spaces.

12. In the **IPv6 suffix** field, enter the IPv6 suffix of the network interface. Maximum length: 30 characters.

13. In the **IPv6 gateway** field, enter the IPv6 address of the default gateway.

14. In the **Prefix length** field, enter the length of the IPv6 prefix of the network interface. Range of values: 12 to 127.
15. In the **DHCPv6 sub-prefix length** field, enter the size of the DHCPv6 sub-prefix of the network interface. Maximum length: 256 characters.
16. In the **IPv6 prefix** field, enter the IPv6 prefix of the network interface. Maximum length: 30 characters.
17. If you want the network interface to accept the specified IPv6 prefix class, do the following:
 - a. Under **IPv6 class**, click **+ Add**.
 - b. Enter the name of the IPv6 prefix class in the field that is displayed. Maximum length: 256 characters.

The IPv6 prefix class is specified and displayed under **IPv6 class**. You can specify multiple IPv6 prefix classes; to delete a class, click the delete icon next to it.
18. If necessary, specify a DNS server for the network interface:
 - a. Under **DNS servers**, click **+ Add**.
 - b. In the field that is displayed, enter the IP address of the DNS server.

The DNS server is specified and displayed in the **DNS servers** section. You can specify multiple DNS servers; to delete a server, click the delete icon next to it.
19. In the **Override MAC** field, enter the MAC address of the network interface. The entered value replaces the actual MAC address of the network interface.
20. In the **Override MTU** field, enter the MTU for the network interface. The entered value overrides the default MTU.
21. If you are creating the first network interface to be mapped to the SD-WAN interface of the WAN type, in the **Route metric** field, enter **100**. For each subsequent network interface that will be mapped to the SD-WAN interface of the WAN type, increment this value by 1. For example, for the second network interface, enter **101**.
22. Under **DHCP server**, in the **Type** drop-down list, select the operating mode of the DHCP server for the network interface:
 - **Disabled** (default)
 - **Relay** If you select this value, enter the IP address of the DHCP server in the **DHCP server IP** field.
 - **Server**
23. If the **Type** drop-down list, you selected **Server**, specify the DHCP server settings:
 - a. In the **First IP** field, enter the offset from the base IP address of the network interface for deriving the lowest IP address that can be leased to clients. The default setting is **100**. You can enter a value greater than 255 for large subnets.
 - b. In the **Limit** field, enter the maximum number of IP addresses that can be leased to clients. Range of values: 1 to 250. The default setting is **150**.
 - c. In the **Lease time** field, enter the maximum time, in hours, for which an individual IP address can be leased to a client. Range of values: 1 to 250. The value is specified in the following format: < number of hours >h. For example, if you want the maximum lease time to be 5 hours, enter **5h**. The default setting is **12h**.

d. If necessary, specify the DHCP option:

1. Under **DHCP options**, click **+ Add**.
2. In the field that is displayed, enter the number of the DHCP option in accordance with the [RFC 1533](#) standard. Maximum length: 250 characters.

The DHCP option is specified and displayed under **DHCP options**. You can specify multiple DHCP options; to delete an option, click the delete icon next to it.

24. Click **Create**.

The network interface is created and displayed in the table.

25. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Creating a network interface for connecting to an LTE network

To create a network interface for connecting to an LTE network:

1. Create a network interface in one of the following ways:

- If you want to create a network interface in a CPE template, go to the **SD-WAN** → **CPE templates** section, click the template and in the displayed settings area, select the **Network settings** tab.
- If you want to create a network interface on a CPE device, go to the **SD-WAN** → **CPE** section, click the device and in the displayed settings area, select the **Network settings** tab.

The table of network interfaces is displayed.

2. Click **+ Network interface**.

3. This opens a window; in that window, in the **Alias** field, enter the name of the network interface for mapping the network interface to a [logical WAN interface](#). Maximum length: 15 characters. The default setting is eth1.

4. In the **Zone** drop-down list, select a previously [created firewall zone](#) to which you want to add the network interface.

5. In the **Protocol** drop-down list, select **QMI**.

6. In the **QMI name** field, enter the path to the modem on the CPE device. Maximum length: 30 characters. For example, you can enter `/dev/cdc-wdm0`.

7. In the **APN** field, enter the APN ID of the service provider that issued the SIM card installed in the modem. Maximum length: 30 characters.

8. In the **Authentication type** drop-down list, select the authentication type on the network interface:

- **PAP** (Password Authentication Protocol).
- **CHAP** (Challenge-Handshake Authentication Protocol).
- **PAP and CHAP** means that both types of authentication are used on the network interface.

- **None** means that authentication is not used on the network interface.
9. In the **Username for PAP/CHAP authentication** field, enter the user name for PAP/CHAP authentication. Maximum length: 30 characters. If you do not want to use authentication, do not specify a value for this setting.
 10. In the **Password for PAP/CHAP authentication** field, enter the password for PAP/CHAP authentication. Maximum length: 30 characters. If you do not want to use authentication, do not specify a value for this setting.
 11. In the **PIN code** field, enter the PIN code of the SIM card installed in the modem. Maximum length: 4 digits.
 12. In the **Delay** field, enter the time in seconds after which the network interface must begin to communicate with the modem. Maximum value: 30. This setting is used when the modem takes too long to start.
 13. If necessary, specify the network mode for the network interface:
 - a. Under **Modes**, click **+ Add**.
 - b. In the drop-down list, select one of the following values:
 - **All** (use all available network modes).
 - **LTE**.
 - **UMTS**.
 - **GSM**.
 - **CDMA**.
 - **TD-SCDMA**.

The network mode is specified and displayed under **Modes**. You can specify multiple network modes; to delete a mode, click the delete icon next to it.

14. In the **Connection profile** field, enter the connection profile index that the network interface must use instead of the APN ID. Maximum length: 30 characters.
15. In the **IP stack** drop-down list, select the IP stack that you want to be used on the network interface:
 - **IPv4** to use the IPv4 protocol stack on the network interface. Default value.
 - **IPv6** to use the IPv6 protocol stack on the network interface.
 - **Dual stack (IPv4 and IPv6)** to use IPv4 and IPv6 dual stack on the network interface.
16. Clear the **IPv4 over DHCP** check box if you do not want to assign an IPv4 address to the network interface via DHCP. To select this check box simultaneously with the **IPv6 over DHCP** check box, select **Dual stack (IPv4 and IPv6)** (for dual stack) in the **IP stack** drop-down list. This check box is selected by default.
17. Select the **IPv6 over DHCP** check box to assign an IPv6 address to the network interface via DHCP. To select this check box simultaneously with the **IPv4 over DHCP** check box, select **Dual stack (IPv4 and IPv6)** in the **IP stack** drop-down list. This check box is cleared by default.
18. Clear the **Autoconnect** check box if you do not want the modem to automatically connect to the network. This check box is selected by default.

19. In the **PLMN** field, enter the PLMN ID of the service provider. The first three digits of the PLMN ID are the country code, and the next three digits are the mobile network code.
20. In the **Timeout** field, enter the time in seconds for the network interface to wait for the completion of the SIM card operations on the modem. Maximum value: 20. The default setting is 10.
21. In the **Serial** field, enter the serial port of the modem. Maximum length: 50 characters.
22. If you are creating the first network interface to be mapped to the SD-WAN interface of the WAN type, in the **Route metric** field, enter 100. For each subsequent network interface that will be mapped to the SD-WAN interface of the WAN type, increment this value by 1. For example, for the second network interface, enter 101.
23. Click **Create**.

The network interface is created and displayed in the table.
24. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Creating a network interface for connecting to a PPPoE server

To create a network interface for connecting to a PPPoE server:

1. Create a network interface in one of the following ways:
 - If you want to create a network interface in a CPE template, go to the **SD-WAN** → **CPE templates** section, click the template and in the displayed settings area, select the **Network settings** tab.
 - If you want to create a network interface on a CPE device, go to the **SD-WAN** → **CPE** section, click the device and in the displayed settings area, select the **Network settings** tab.

The table of network interfaces is displayed.

2. Click **+ Network interface**.
3. This opens a window; in that window, in the **Alias** field, enter the name of the network interface for mapping the network interface to an OpenFlow port. You must specify this alias when [creating an SD-WAN interface of the WAN type](#). Maximum length: 15 characters.
4. If you want to add a network interface to a firewall zone, in the **Zone** drop-down list, select a previously [created firewall zone](#).
5. In the **Interface name** field, enter the name of the physical port or virtual interface of the operating system of the CPE device. Maximum length: 256 characters. For example, you can enter eth0, eth1, eth2, or tun0. To create a bridge from multiple interfaces, enter their names separated by spaces.

If you want to assign an outer VLAN tag to a network interface, enter a period (.) after the physical port or virtual interface name of the operating system, and then enter the outer VLAN tag. For example, you can enter eth2.150.
6. In the **Protocol** drop-down list, select **PPPoE**.
7. In the **Access concentrator** field, enter the IP address or host name of the access concentrator to which you want the network interface to connect. Maximum length: 30 characters. If you do not enter a value in this field, the Point-to-Point Protocol Daemon (PPPD) uses the first access concentrator it detects.

8. In the **Service** field, enter the name of the PPPoE service to which you want the network interface to connect. Maximum length: 30 characters. If you do not enter a value in this field, PPPD uses the first service it detects.
 9. In the **Authentication type** drop-down list, select which authentication is used on the network interface:
 - **PAP and CHAP** if PAP and CHAP authentication is used on the network interface. If you select this option, do the following:
 - a. In the **Username for PAP/CHAP authentication** field, enter the user name for PAP/CHAP authentication. Maximum length: 30 characters.
 - b. In the **Password for PAP/CHAP authentication** field, enter the password for PAP/CHAP authentication. Maximum length: 30 characters.
 - **None** means that authentication is not used on the network interface.
 10. In the **Failed pings maximum** field, enter the number of unsuccessful ICMP requests before the network interface considers the PPPoE server unavailable. Range of values: 1 to 3600. The default setting is 5.
 11. In the **Ping interval (sec.)** field, enter the interval in seconds that the network interface must wait for before sending ICMP requests to the PPPoE server. Range of values: 1 to 3600. The default setting is 1.
 12. If you want the network interface to terminate an inactive PPPoE connection after the specified time, in the **Timeout (sec.)** field, enter the time in seconds. Range of values: 1 to 3600.
 13. If necessary, in the **Host-Uniq** field, enter the Host-Uniq tag for the PPPoE connection. Maximum length: 30 characters. If you do not enter a value in this field, the value of the Host-Uniq tag is the same as the PPPD process identifier.
 14. In the **Override MTU** field, enter the MTU for the network interface. The entered value overrides the default MTU.
 15. If you are creating the first network interface to be mapped to the SD-WAN interface of the WAN type, in the **Route metric** field, enter **100**. For each subsequent network interface that will be mapped to the SD-WAN interface of the WAN type, increment this value by 1. For example, for the second network interface, enter **101**.
 16. If necessary, clear the following check boxes:
 - Clear the check box **Keepalive adaptive** if you want the network interface that has not received Link Control Protocol (LCP) control packets from the PPPoE server to terminate the PPPoE connection, even if traffic has arrived from the server.
 - Clear the **Use default route** check box if you do not want to use the route obtained from the PPPoE server as the default route on the network interface.
 - Clear the **Peer-assigned DNS server** check box if you do not want the network interface to use DNS servers assigned to its neighbors.
- By default, the check boxes are selected.
17. If you want to pass additional command line arguments to PPPD (Point-to-Point Protocol Daemon) at startup, in the **Pppd** field, enter the command line arguments. For example, you can pass authentication parameters, IP addresses, and scripts to PPPD.
 18. If necessary, specify a DNS server for the network interface:
 - a. Under **DNS servers**, click **+ Add**.

b. In the field that is displayed, enter the IP address of the DNS server.

The DNS server is specified and displayed in the **DNS servers** section. You can specify multiple DNS servers; to delete a server, click the delete icon next to it.

19. Click **Create**.

The network interface is created and displayed in the table.

20. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Creating a network interface without an IP address

To create a network interface without an IP address:

1. Create a network interface in one of the following ways:

- If you want to create a network interface in a CPE template, go to the **SD-WAN** → **CPE templates** section, click the template and in the displayed settings area, select the **Network settings** tab.
- If you want to create a network interface on a CPE device, go to the **SD-WAN** → **CPE** section, click the device and in the displayed settings area, select the **Network settings** tab.

The table of network interfaces is displayed.

2. Click **+ Network interface**.

3. This opens a window; in that window, in the **Alias** field, enter the name of the network interface for mapping the network interface to an OpenFlow port. You must specify this alias when [creating an SD-WAN interface of the WAN type](#). Maximum length: 15 characters.

4. If you want to add a network interface to a firewall zone, in the **Zone** drop-down list, select a previously [created firewall zone](#).

5. In the **Interface name** field, enter the name of the physical port or virtual interface of the operating system of the CPE device. Maximum length: 256 characters. For example, you can enter eth0, eth1, eth2, or tun0. To create a bridge from multiple interfaces, enter their names separated by spaces.

If you want to assign an outer VLAN tag to a network interface, enter a period (.) after the physical port or virtual interface name of the operating system, and then enter the outer VLAN tag. For example, you can enter eth2.150.

6. If you want to create a bridge from physical or virtual interfaces whose names are specified in the **Interface name** field:

- a. Select the **Bridge** check box. This check box is cleared by default.
- b. If you want to use STP on the bridge to prevent routing loops, select the **STP** check box. This check box is cleared by default.
- c. In the **Age (sec.)** field, enter the duration in seconds for which you want dynamic records to be stored in the MAC table of the bridge. If you want to use the bridge as a hub, enter 0 in this field. Range of values: 0 to 86,400.

7. If you want to enable the [NetFlow protocol](#) on the network interface, select the **NetFlow** check box. This check box is cleared by default.
8. In the **Protocol** drop-down list, select **None**.
9. If you want the network interface to be automatically enabled when the CPE device is enabled, select the **Enable automatically** check box. This check box is cleared by default.
10. If you want an IP address, route, and default gateway automatically assigned to the network interface, select the **Force IP, route, and gateway** check box. This check box is cleared by default.
11. In the **Override MAC** field, enter the MAC address of the network interface. The entered value replaces the actual MAC address of the network interface.
12. In the **Override MTU** field, enter the MTU for the network interface. The entered value overrides the default MTU.
13. Click **Create**.
The network interface is created and displayed in the table.
14. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Editing a network interface

You can edit a network interface in a CPE template or on a device. When you edit a network interface in a CPE template, the interface is automatically modified on all devices that are using the template. For a description of the settings, see the [instructions for creating a network interface](#).

To edit a network interface:

1. Edit a network interface in one of the following ways:
 - If you want to edit a network interface in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template and in the displayed settings area, select the **Network settings** tab.
 - If you want to edit a network interface on a CPE device, go to the **SD-WAN → CPE** menu section, click the device and in the displayed settings area, select the **Network settings** tab. If you want to edit a network interface inherited from the CPE template, select the **Override** check box next to the network interface.

The table of network interfaces is displayed.

2. Click **Edit** next to the network interface that you want to edit.
3. This opens a window; in that window, edit network interface settings.
4. Click **Save**.
The network interface is modified and updated in the table.
5. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Disabling or enabling a network interface

You can disable or enable a network interface in a CPE template or on a device. When you disable or enable a network interface in a CPE template, that network interface is automatically disabled or enabled on all devices that are using the template.

To disable or enable a network interface:

1. Disable or enable a network interface in one of the following ways:
 - If you want to disable or enable a network interface in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template and in the displayed settings area, select the **Network settings** tab.
 - If you want to disable or enable a network interface on a CPE device, go to the **SD-WAN** menu section, click the device and in the displayed settings area, select the **Network settings** tab. If you want to disable or enable a network interface inherited from the CPE template, select the **Override** check box next to the network interface.

The table of network interfaces is displayed.

2. Click **Disable** or **Enable** next to the network interface that you want to disable or enable.

The network interface is disabled or enabled.

3. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Canceling the application of network interface settings to a CPE device

If you do not want to apply network interface settings to a CPE device:

1. In the menu, go to the **SD-WAN → CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device to which you do not want to apply network interface settings.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. Select the **Network settings** tab.

The table of network interfaces is displayed.

4. Select the **Ignore network settings** check box. This check box is cleared by default.

5. In the upper part of the settings area, click **Save** to save CPE device settings.

Network interface settings are not applied to the CPE device.

If you want to apply network interface settings to the CPE device, clear the **Ignore network settings** check box.

Deleting a network interface

You can delete a network interface in a CPE template or on a device. When you delete a network interface in a CPE template, the interface is automatically deleted on all devices that are using the template. You cannot delete a network interface that is inherited from a template on a CPE device.

Deleted network interfaces cannot be restored.

To delete a network interface:

1. Delete a network interface in one of the following ways:

- If you want to delete a network interface in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template and in the displayed settings area, select the **Network settings** tab.
- If you want to delete a network interface on a CPE device, go to the **SD-WAN → CPE** menu section, click the device and in the displayed settings area, select the **Network settings** tab.

The table of network interfaces is displayed.

2. Click **Delete** next to the network interface that you want to delete.

3. In the confirmation window, click **Delete**.

The network interface is deleted and is no longer displayed in the table.

4. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Configuring the connection of a CPE device to the orchestrator and controller

When a CPE device is being registered, it connects to the orchestrator and controller. You can configure the connection in the CPE template. When you configure the connection in a CPE template, the settings are automatically propagated to all devices that are using the template.

Certain connection settings can also be configured on the CPE device, for example, you can enable automatic restart when the [management session with the controller](#) is terminated.

To configure the connection of a CPE device to the orchestrator and controller:

1. Configure the connection in one of the following ways:

- If you want to configure automatic connection to the orchestrator and controller in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template and in the displayed settings area, select the **SD-WAN settings → General settings** tab.
- If you want to configure automatic connection to the orchestrator and controller in a CPE device, go to the **SD-WAN → CPE** menu section, click the device and in the displayed settings area, select the **SD-WAN settings → General settings** tab and select the **Override** check box.

This displays settings for connecting to the orchestrator and controller.

2. If you are configuring a connection to the orchestrator and controller in a CPE template:

- a. In the **Orchestrator IP/FQDN** field, enter the IP address or FQDN of the orchestrator. Maximum length: 50 characters.
- b. In the **Orchestrator protocol** drop-down list, select the protocol for connecting the CPE device to the orchestrator:
 - **http**
 - **https** (default).
- c. In the **Orchestrator port** field, enter the port number of the orchestrator. Range of values: 0 to 65,535.
- d. In the **OpenFlow transport** drop-down list, select whether the management session between the CPE device and the controller must be encrypted:
 - **TCP** for an unencrypted management session.
 - **SSL** for an encrypted management session. Default value.

These settings can only be specified in the CPE template. The rest of the settings in these instructions can be configured both in the CPE template and on the device.

3. In the **Auto-reboot** drop-down list, select whether you want to automatically restart the CPE device whenever the connection with the controller is lost.
 - **Yes** If you select this option, in the **Reboot timeout (sec.)** field, enter the time in seconds after which the CPE device must be restarted when connection with the controller is lost. Range of values: 60 to 2,073,600.
 - **No** (default).
4. In the **Prioritized control plane interface** drop-down list, select how a new primary management session is determined between the CPE device and the controller when the previous session is terminated:
 - **Random** – a randomly selected session established from a [SD-WAN interface of the WAN type](#) on the CPE device becomes the new primary management session. Default value.
 - **<SD-WAN interface>** – the session established from the specified SD-WAN interface of the WAN type on the CPE device becomes the new primary management session. If the interface is not available, a session established from a randomly chosen interface becomes the new primary management session.
When this value is selected, if you want the previous primary management session to become the primary session again upon restoration:
 - a. Select the **Preemption** check box. This check box is cleared by default.
 - b. In the **Timeout** field, enter the time, in seconds, after which a restored management session must become the primary session. Range of values: 0 to 86,400.
5. In the **Update interval (sec.)** field, enter the period in seconds for [sending REST API requests from the CPE device to the orchestrator](#). Range of values: 5 to 300. The default setting is 30.
6. In the **URL ZTP** field, enter the [URL template for the basic settings of the CPE device](#). When entering a template, consider the following limitations:
 - `{config}` is a mandatory part which is replaced with settings for the CPE device when a link is generated from the template.

- Maximum length: 128 characters.
- You must specify http or https.

By default, the following URL template is used: `http://192.168.7.1/cgi-bin/config?payload={config}`.

7. In the **Interactive update interval (sec.)** field, enter the period in seconds for sending REST API requests from the CPE device to the orchestrator in interactive mode. Range of values: 1 to 10. You can [enable interactive mode](#) for [CPE device diagnostics](#).
8. In the **Interactive mode timeout (sec.)** field, enter the time in seconds after which interactive must should be automatically disabled on the CPE device. Range of values: 30 to 180.
9. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Managing SD-WAN interfaces

SD-WAN interfaces are logical interfaces on top of the [network interfaces](#) of the CPE device and OpenFlow ports of the virtual switch, which form an additional level of abstraction. Each SD-WAN interface is mapped to a network interface by the network interface name and an OpenFlow port by the OpenFlow port number. The following types of SD-WAN interfaces are possible:

- SD-WAN interfaces of the LAN type are SD-WAN interfaces mapped to network interfaces that are connected to the LAN. These interfaces are created by default and you cannot create or delete them. You can edit SD-WAN interfaces of the LAN type to specify the maximum speed and configure traffic queues.
- SD-WAN interfaces of the WAN type are SD-WAN interfaces mapped to network interfaces that are connected to the WAN.
- An SD-WAN interface of the management type is an SD-WAN interface mapped to a network interface that is used by the Zabbix [monitoring](#) system for passive monitoring of the CPE device, as well as by the orchestrator for connecting to the CPE device via SSH. This interface is created by default and you cannot delete it or create new interfaces. If you do not want to use the SD-WAN interface of the management type, you can disable it.

The table of SD-WAN interfaces is displayed in the CPE template and on the device:

- To display the table of SD-WAN interfaces in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template, and in the displayed settings area, select the **SD-WAN settings → Interfaces** tab.
- To display the table of SD-WAN interfaces on a CPE device, go to the **SD-WAN → CPE** menu section, click the device, and in the displayed settings area, select the **SD-WAN settings → Interfaces** tab.

Information about SD-WAN interfaces is displayed in the following columns of the table:

- **Type** is the type of the SD-WAN interface:
 - **WAN**
 - **LAN**
 - **Management**

- **Inherited** indicates whether the SD-WAN interface is inherited from the CPE template:
 - Yes
 - No

This column is displayed only on the CPE device.

- **Port** is the OpenFlow port number.
- **Alias** is the name of the network interface.
- **Maximum rate** is the maximum speed of the SD-WAN interface in Mbps.

Additional information about WAN checks to which SD-WAN interfaces of the WAN type are connected is displayed in the following columns of the table:

- **IP for tracking** are the IP addresses of hosts for checking WAN availability.
- **Reliability** is the minimum number of successful checks that makes the WAN available.
- **Count** is the number of requests to hosts within one WAN check.
- **Timeout** is time to wait for a response from hosts, in milliseconds.
- **Interval** is the WAN check interval in seconds.
- **Down** is the number of unsuccessful checks that makes the WAN unavailable.
- **Up** is the number of successful checks that makes the WAN available.
- **Speed monitoring** indicates whether the speed of the SD-WAN interface of the WAN type is being measured:
 - Yes
 - No

About sending information about SD-WAN interfaces of the WAN type to the controller

When [creating](#) or [editing SD-WAN interfaces of the WAN type](#), you can specify what information must be sent to the controller.


Sending public IP addresses and UDP ports of SD-WAN interfaces to the controller

To build GENEVE tunnels between CPE devices, the controller must obtain information about the public IP addresses of SD-WAN interfaces of the WAN type. By default, the controller obtains this information through a [management session](#). In that case, the source IP address is used as the public IP address.

You can manually specify the IP addresses and UDP ports of SD-WAN interface of the WAN type. In the figure below, CPE 1 and the controller are on the same local network and gain access to the Internet through the same firewall that does IP address forwarding.

When establishing a session between the SD-WAN interface of the WAN type of CPE 1 and the public IP address of the controller (1.1.1.2), if the firewall cannot be configured in a way that would involve the Controller forwarding the private IP address to the public IP address (10.0.1.1 > 1.1.1.1), the Controller is unable to obtain information about the public IP address of the interface and provide it to other devices in the topology (CPE 2).

As a result, a GENEVE tunnel cannot be created between CPE 1 and CPE 2; CPE 1 becomes isolated and cannot be added to the common [control plane](#).

 In the diagram, CPE 1 and the controller are connected to CPE 2 through a firewall and the Internet, and NAT is used.

CPE 1 and the controller are behind NAT and are connected to CPE 2

Sending IP addresses of SD-WAN interfaces of the WAN type located in an isolated network to the controller

SD-WAN interfaces of the WAN type may be on an isolated network without the possibility of establishing a management session with the controller, but they can be used to build GENEVE tunnels. In this case, the controller cannot obtain information about the IP addresses of isolated interfaces and use it to build GENEVE tunnels between CPE devices.

In the figure below, CPE 1 and CPE 2 have two SD-WAN interface of the WAN type each, but they can establish a management session with the controller only through their wan0 interfaces because the wan1 interfaces are on an isolated network (MPLS) that does not have access to the Controller. However, both wan1 interfaces can be used to build GENEVE tunnels.

If the link used to interact with the controller fails for one of the CPE devices, all other links also cannot be used, even if they remain operational, because the Controller eliminates the device from the topology.


The IP addresses of isolated SD-WAN interfaces of the WAN type are sent to the controller through the orchestrator.

 CPE 1 and CPE 2 are connected with each other through MPLS and with the controller through the Internet.

CPE 1 and CPE 2 are connected with each other through MPLS and with the controller through the Internet.

About overriding the IP address and port for connecting an SD-WAN interface of the WAN type to the controller

You can connect SD-WAN interfaces of the WAN type to the controller even if they use different types of links, for example, the Internet vs a private MPLS network (see the figure below). You must manually override the IP addresses and ports for connecting to the controller when [creating](#) or [editing an SD-WAN interface of the WAN type](#).

 In the diagram, the CPE device is connected to the controller through ports sdwan0, 1, and 2. The connection goes through the Internet and MPLS.

Connecting the CPE device to the controller via two different communication channels

If your SD-WAN instance uses multiple controller nodes, you must override IP addresses for all nodes. If the number of controller nodes does not match the number of specified IP addresses, an error occurs and the values stay the same.

You must [restart the CPE device](#) after overriding the IP address and port for connecting an SD-WAN interface of the WAN type to the controller

Package fragmentation

Kaspersky SD-WAN checks whether fragmentation of traffic packets is supported on CPE devices. A packet fragmentation test is started automatically. When each CPE device is enabled, it sends two ICMP requests to the IP addresses that you specified when [creating](#) or [editing](#) SD-WAN interfaces of the WAN type or in the configuration file of the controller.

The ICMP requests have a packet size of 1600 bytes. If at least one of these requests receives a response, a conclusion is made that the CPE device supports packet fragmentation. You can view the result of the fragmentation test result in the **Fragmentation** column of the [table of CPE devices](#) or the link table.

Creating an SD-WAN interface of the WAN type

You can create an SD-WAN interface of the WAN type in a CPE template or on a device. When you create an SD-WAN interface of the WAN type in a CPE template, the interface is automatically created on all devices that are using the template.

To create an SD-WAN interface of the WAN type:

1. Create an SD-WAN interface of the WAN type in one of the following ways:
 - If you want to create an SD-WAN interface of the WAN type in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template and in the displayed settings area, select the **SD-WAN settings → Interfaces** tab.
 - If you want to create an SD-WAN interface of the WAN type on a CPE device, go to the **SD-WAN → CPE** menu section, click the device and in the displayed settings area, select the **SD-WAN settings → Interfaces** tab.

A table of SD-WAN interfaces is displayed.

2. Click **+ SD-WAN interface**.
3. This opens a window; in that window, in the **OpenFlow interface** field, enter the number of the OpenFlow port that must be created on the virtual switch.
4. In the **Interface (alias)** field, enter the name of the previously [created network interface](#), which the SD-WAN interface of the WAN type must be mapped to.
5. In the **Maximum rate** field, enter the maximum speed of the SD-WAN interface of the WAN type in Mbps. Range of values: 1 to 100,000. The default setting is **1000**.
6. Configure the availability check of the WAN to which the SD-WAN interface of the WAN type is connected:
 - a. Specify the host for checking WAN availability:
 1. Under **IP for tracking**, enter the IP address of the host.

2. Click **+ Add**.

The host is specified and displayed under **IP for tracking**. You can specify multiple hosts; to delete a host, click the delete icon next to it.

- b. In the **IP for fragmentation check** field, enter the IPv4 address of the host up to which you want to check for [fragmentation](#) support. Default value: 1.1.1.1.
- c. In the **Reliability** field, enter the minimum number of successful checks that makes the WAN available. The default setting is **1**.

Make sure that the number of hosts does not exceed the number of IP addresses specified under **IP for tracking**. Otherwise, the WAN will always be considered unavailable.

- d. In the **Interval** field, enter the WAN check interval in seconds. Range of values: 1 to 600. The default setting is **2**.
- e. In the **Count** field, enter the number of requests to hosts within one WAN check. Range of values: 1 to 600. The default setting is **2**.
- f. In the **Timeout** field, enter the time to wait for a response from hosts, in milliseconds. Range of values: 1 to 100,000. The default setting is **2000**.
- g. In the **Down** field, enter the number of unsuccessful checks that makes the WAN unavailable. Range of values: 1 to 600. The default setting is **3**.
- h. In the **Up** field, enter the number of successful checks that makes the WAN available. Range of values: 1 to 600. The default setting is **2**.
- i. In the **Speed monitoring** drop-down list, select whether you want the speed of the SD-WAN interface of the WAN type to be measured:
- **Yes**
 - **No** (default).

7. If you want to configure traffic queues on the SD-WAN interface of the WAN type:

- a. Select the **QoS** tab.
A table of traffic queues is displayed.
- b. In the **Remap ToS** column, select the Type of Service value of external headers of traffic packets for each queue.
- c. In the **Minimum rate (%)** column, specify the minimum traffic bandwidth for the queue as a percentage of the maximum speed of the SD-WAN interface of the WAN type. The sum total in a column may not exceed 100.
- d. In the **Maximum rate (%)** column, specify the maximum traffic bandwidth for the queue as a percentage of the maximum speed of the SD-WAN interface of the WAN type. This setting is used to prevent traffic of high-priority queues from indefinitely preempting traffic of low-priority queues.

The maximum speed of the SD-WAN interface of the WAN type is specified at step 5 of these instructions.

8. If you want to configure the [sending of information about the SD-WAN interface of the WAN type](#) to the controller:

a. Select the **NAT and disjoint WAN underlay** tab.

b. In the **State** drop-down list, select one of the following values:

- **Disabled** if you do not want information about the SD-WAN interface of the WAN type to be sent to the controller.
- **NAT/PAT** if the SD-WAN interface of the WAN type is behind NAT or PAT and needs to be assigned a public IP address and UDP port number, which must be sent to the controller.
- **Disjoint WAN underlay** if the SD-WAN interface of the WAN type is connected to an isolated network and its IP address must be communicated to the controller.

c. If in the **State** drop-down list, you selected **NAT/PAT**, follow these steps:

1. In the **Real IP** field, enter the public IPv4 address of the SD-WAN interface of the WAN type.

2. In the **Real GENEVE UDP port** field, enter the UDP port number of the SD-WAN interface of the WAN type. Range of values: 1 to 65,535.

d. If in the **State** drop-down list you selected **Disjoint WAN underlay**, enter the IPv4 address of the SD-WAN interface of the WAN type in the **IP address** field.

9. If you want to [override the IP address and port for connecting the SD-WAN interface of the WAN type to the controller](#):

a. Select the **Controllers** tab.

b. Select the **Rewrite controllers IP/port** check box. This check box is cleared by default.

c. In the **Number of controllers** drop-down list, select the number of controller nodes in the SD-WAN instance.

You must override the IP address for connecting the SD-WAN interface of the WAN type to each node of the controller. Otherwise, an error occurs and the settings remain unchanged.

d. In the **IP address** field, enter the IPv4 address for connecting the SD-WAN interface of the WAN type to the controller. The number of fields corresponds to the value that you selected in the **Number of controllers** drop-down list.

e. In the **Port** field, enter the starting port number for connecting the SD-WAN interface of the WAN type to the controller. The number of fields corresponds to the value that you selected in the **Number of controllers** drop-down list. Range of values: 1 to 65,535. The default setting is 6653.

The number of configured ports depends on the number of SD-WAN interfaces of the WAN type on the CPE device. For example, if you enter 6653 as the starting port number and the device has four SD-WAN interfaces of the WAN type, port numbers 6654, 6655, and 6656 are derived from that port.

You must [restart the CPE device](#) after overriding the IP address and port for connecting an SD-WAN interface of the WAN type to the controller

10. Click **Create**.

The SD-WAN interface of the WAN type is created and displayed in the table.

11. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Editing an SD-WAN interface of the WAN type

You can edit an SD-WAN interface of the WAN type in a CPE template or on a device. You cannot edit the name of an SD-WAN interface of the WAN type. When you edit an SD-WAN interface of the WAN type in a CPE template, the interface is automatically modified on all devices that are using the template.

To edit an SD-WAN interface of the WAN type:

1. Edit an SD-WAN interface of the WAN type in one of the following ways:

- If you want to edit an SD-WAN interface of the WAN type in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template and in the displayed settings area, select the **SD-WAN settings → Interfaces** tab.
- If you want to edit an SD-WAN interface of the WAN type on a CPE device, go to the **SD-WAN → CPE** menu section, click the device and in the displayed settings area, select the **SD-WAN settings → Interfaces** tab. If you want to edit an SD-WAN interface of the WAN type inherited from the CPE template, select the **Override** check box next to that interface.

A table of SD-WAN interfaces is displayed.

2. Click **Edit** button next to the SD-WAN interface of the WAN type that you want to edit.

3. This opens a window; in that window, in the **OpenFlow interface** field, enter the number of the OpenFlow port that must be created on the virtual switch.

4. In the **Maximum rate** field, enter the maximum speed of the SD-WAN interface of the WAN type in Mbps. Range of values: 1 to 100,000. The default setting is **1000**.

5. Configure the availability check of the WAN to which the SD-WAN interface of the WAN type is connected:

a. Specify the host for checking WAN availability:

1. Under **IP for tracking**, enter the IP address of the host.

2. Click **+ Add**.

The host is specified and displayed under **IP for tracking**. You can specify multiple hosts; to delete a host, click the delete icon next to it.

b. In the **IP for fragmentation check** field, enter the IPv4 address of the host up to which you want to check for [fragmentation](#) support. Default value: 1.1.1.1.

c. In the **Reliability** field, enter the minimum number of successful checks that makes the WAN available. The default setting is **1**.

Make sure that the number of hosts does not exceed the number of IP addresses specified under **IP for tracking**. Otherwise, the WAN will always be considered unavailable.

- d. In the **Interval** field, enter the WAN check interval in seconds. Range of values: 1 to 600. The default setting is 2.
 - e. In the **Count** field, enter the number of requests to hosts within one WAN check. Range of values: 1 to 600. The default setting is 2.
 - f. In the **Timeout** field, enter the time to wait for a response from hosts, in milliseconds. Range of values: 1 to 100,000. The default setting is 2000.
 - g. In the **Down** field, enter the number of unsuccessful checks that makes the WAN unavailable. Range of values: 1 to 600. The default setting is 3.
 - h. In the **Up** field, enter the number of successful checks that makes the WAN available. Range of values: 1 to 600. The default setting is 2.
 - i. In the **Speed monitoring** drop-down list, select whether you want the speed of the SD-WAN interface of the WAN type to be measured:
 - **Yes**
 - **No** (default).
6. If you want to configure traffic queues on the SD-WAN interface of the WAN type:
- a. Select the **QoS** tab.
A table of traffic queues is displayed.
 - b. In the **Remap ToS** column, select the Type of Service value of external headers of traffic packets for each queue.
 - c. In the **Minimum rate (%)** column, specify the minimum traffic bandwidth for the queue as a percentage of the maximum speed of the SD-WAN interface of the WAN type. The sum total in a column may not exceed 100.
 - d. In the **Maximum rate (%)** column, specify the maximum traffic bandwidth for the queue as a percentage of the maximum speed of the SD-WAN interface of the WAN type. This setting is used to prevent traffic of high-priority queues from indefinitely preempting traffic of low-priority queues.
- The maximum speed of the SD-WAN interface of the WAN type is specified at step 5 of these instructions.
7. If you want to configure the [sending of information about the SD-WAN interface of the WAN type](#) to the controller:
- a. Select the **NAT and disjoint WAN underlay** tab.
 - b. In the **State** drop-down list, select one of the following values:
 - **Disabled** if you do not want information about the SD-WAN interface of the WAN type to be sent to the controller.
 - **NAT/PAT** if the SD-WAN interface of the WAN type is behind NAT or PAT and needs to be assigned a public IP address and UDP port number, which must be sent to the controller.

- **Disjoint WAN underlay** if the SD-WAN interface of the WAN type is connected to an isolated network and its IP address must be communicated to the controller.

c. If in the **State** drop-down list, you selected **NAT/PAT**, follow these steps:

1. In the **Real IP** field, enter the public IPv4 address of the SD-WAN interface of the WAN type.
2. In the **Real GENEVE UDP port** field, enter the UDP port number of the SD-WAN interface of the WAN type. Range of values: 1 to 65,535.

d. If in the **State** drop-down list you selected **Disjoint WAN underlay**, enter the IPv4 address of the SD-WAN interface of the WAN type in the **IP address** field.

8. If you want to [override the IP address and port for connecting the SD-WAN interface of the WAN type to the controller](#):

- a. Select the **Controllers** tab.
- b. Select the **Rewrite controllers IP/port** check box. This check box is cleared by default.
- c. In the **Number of controllers** drop-down list, select the number of controller nodes in the SD-WAN instance.

You must override the IP address for connecting the SD-WAN interface of the WAN type to each node of the controller. Otherwise, an error occurs and the settings remain unchanged.

d. In the **IP address** field, enter the IPv4 address for connecting the SD-WAN interface of the WAN type to the controller. The number of fields corresponds to the value that you selected in the **Number of controllers** drop-down list.

e. In the **Port** field, enter the starting port number for connecting the SD-WAN interface of the WAN type to the controller. The number of fields corresponds to the value that you selected in the **Number of controllers** drop-down list. Range of values: 1 to 65,535. The default setting is 6653.

The number of configured ports depends on the number of SD-WAN interfaces of the WAN type on the CPE device. For example, if you enter 6653 as the starting port number and the device has four SD-WAN interfaces of the WAN type, port numbers 6654, 6655, and 6656 are derived from that port.

You must [restart the CPE device](#) after overriding the IP address and port for connecting an SD-WAN interface of the WAN type to the controller

9. Click **Save**.

The SD-WAN interface of the WAN type is modified and displayed in the table.

10. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Editing an SD-WAN interface of the LAN type

You can edit an SD-WAN interface of the LAN type in a CPE template or on a device. When you edit an SD-WAN interface of the LAN type in a CPE template, the interface is automatically modified on all devices that are using the template. When editing an SD-WAN interface of the LAN type, you can only configure the maximum speed and traffic queues.

To edit an SD-WAN interface of the LAN type:

1. Edit an SD-WAN interface of the LAN type in one of the following ways:

- If you want to edit an SD-WAN interface of the LAN type in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template and in the displayed settings area, select the **SD-WAN settings → Interfaces** tab.
- If you want to edit an SD-WAN interface of the LAN type on a CPE device, go to the **SD-WAN → CPE** menu section, click the device and in the displayed settings area, select the **SD-WAN settings → Interfaces** tab. If you want to edit an SD-WAN interface of the LAN type inherited from the CPE template, select the **Override** check box next to that interface.

A table of SD-WAN interfaces is displayed.

2. Click **Edit** button next to the SD-WAN interface of the LAN type that you want to edit.

3. This opens a window; in that window, in the **Maximum rate** field, enter the maximum speed of the SD-WAN interface in Mbps. Range of values: 1 to 100,000. The default setting is **1000**.

4. If you want to configure traffic queues on the SD-WAN interface of the LAN type:

a. Select the **QoS** tab.

A table of traffic queues is displayed.

b. In the **Minimum rate (%)** column, specify the minimum traffic bandwidth for the queue as a percentage of the maximum speed of the SD-WAN interface of the LAN type. The sum total in a column may not exceed 100.

c. In the **Maximum rate (%)** column, specify the maximum traffic bandwidth for the queue as a percentage of the maximum speed of the SD-WAN interface of the LAN type. This setting is used to prevent traffic of high-priority queues from indefinitely preempting traffic of low-priority queues.

The maximum speed of the SD-WAN interface of the LAN type is specified at step 3 of these instructions.

5. Click **Save**.

The SD-WAN interface of the LAN type is modified and displayed in the table.

6. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Disabling or enabling an SD-WAN interface

You can disable or enable an SD-WAN interface in a CPE template or on a device. When you disable or enable an SD-WAN interface in a CPE template, that interface is automatically disabled or enabled on all devices that are using the template.

To disable or enable an SD-WAN interface:

1. Disable or enable an SD-WAN interface in one of the following ways:

- If you want to disable or enable an SD-WAN interface in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template and in the displayed settings area, select the **SD-WAN settings → Interfaces** tab.

- If you want to disable or enable an SD-WAN interface on a CPE device, go to the **SD-WAN → CPE** menu section, click the device and in the displayed settings area, select the **SD-WAN settings → Interfaces** tab. If you want to disable or enable an SD-WAN interface inherited from the CPE template, select the **Override** check box next to that interface.

A table of SD-WAN interfaces is displayed.

2. Click **Disable** or **Enable** next to the SD-WAN interface that you want to disable or enable.

The SD-WAN interface is disabled or enabled and updated in the table.

3. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Deleting an SD-WAN interface of the WAN type

You can delete an SD-WAN interface of the WAN type in a CPE template or on a device. When you delete an SD-WAN interface of a WAN type in a CPE template, the interface is automatically deleted on all devices using the template. You cannot delete an SD-WAN interface that is inherited from a template on a CPE device.

SD-WAN interfaces of the LAN type cannot be deleted.

Deleted SD-WAN interfaces of the WAN type cannot be restored.

To delete an SD-WAN interface of the WAN type:

1. Delete an SD-WAN interface of the WAN type in one of the following ways:

- If you want to delete an SD-WAN interface of the WAN type in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template and in the displayed settings area, select the **SD-WAN settings → Interfaces** tab.
- If you want to delete an SD-WAN interface of the WAN type on a CPE device, go to the **SD-WAN → CPE** menu section, click the device and in the displayed settings area, select the **SD-WAN settings → Interfaces** tab.

A table of SD-WAN interfaces is displayed.

2. Click **Delete** next to the SD-WAN interface of the WAN type that you want to delete.

3. In the confirmation window, click **Delete**.

The SD-WAN interface of the WAN type is deleted and is no longer displayed in the table.

4. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Managing service interfaces

Service interfaces are mapped to OpenFlow ports and are used to connect a CPE device to [transport services](#). A service interface cannot be mapped to an OpenFlow port that is already mapped to an [SD-WAN interface of the WAN type](#).

If you want to filter traffic packets on a service interface, you can create an Access Control List (ACL) interface that is mapped to this service interface. The ACL interface applies the specified [traffic filter](#) to the service interface. A single service interface can be mapped to at most four ACL interfaces.

To display the table of service interfaces, go to the **Infrastructure** menu section, click **Management** → **Configuration menu** next to the controller to which the device is connected, and in the displayed controller settings menu, go to the **Service interfaces** section. Information about service interfaces is displayed in the following columns of the table:

- **Port** is the number of the OpenFlow port to which the service interface is mapped to.
- **Type** is the traffic encapsulation type on the service interface.
 - **Access**
 - **VLAN**
 - **Q-in-Q**
 - **ACL**
- **Description** is a brief description of the service interface.
- **VLAN** is the outer VLAN tag of the service interface. The value in this column is only displayed for service interfaces with encapsulation types **VLAN** and **Q-in-Q**.
- **Inner VLAN** is the inner VLAN tag of the service interface. The value in this column is only displayed for service interfaces with encapsulation type **Q-in-Q**.
- **Filter** is the traffic filter for the ACL interface. The value in this column is only displayed for service interfaces with encapsulation type **ACL**.
- **Name** is the name of the service interface.

The actions you can perform with the table are described in the [Managing solution component tables](#) instructions.

Creating a service interface

To create a service interface:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.
2. Click **Management** → **Configuration menu** next to the controller to which the CPE device is connected.
This opens the controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of controller nodes.
3. Go to the **Service interfaces** section.
A table of service interfaces and ACL interfaces is displayed.
4. In the **Switch** and **Port** drop-down lists, select the CPE device and the OpenFlow port to which you want to map the service interface.

5. Click **Create service interface**.

6. This opens a window; in that window, in the **Type** drop-down list, select the type of traffic classification on the service interface:

- **Access** (default).
- **VLAN** If you select this option, in the **VLAN ID** field, enter the outer VLAN tag of the service interface. Range of values: 1 to 4094.
- **Q-in-Q** If you select this option, do the following:
 - a. In the **VLAN ID** field, enter the outer VLAN tag of the service interface. Range of values: 1 to 4094.
 - b. In the **Inner VLAN ID** field, enter the inner VLAN tag of the service interface. Range of values: 1 to 4094.
- **ACL** is used when [creating an ACL interface](#).

7. If necessary, enter a brief description of the service interface in the **Description** field.

8. Click **Create**.

The service interface is created and displayed in the table.

Creating an ACL interface

To create an ACL interface:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. Click **Management** → **Configuration menu** next to the controller to which the CPE device is connected.

This opens the controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of controller nodes.

3. Go to the **Service interfaces** section.

A table of service interfaces and ACL interfaces is displayed.

4. In the **Switch** and **Port** drop-down lists, select the CPE device and the OpenFlow port to which the previously [created service interface](#) is mapped.

5. Click **+ Create service interface**.

6. This opens a window; in that window, in the **Type** drop-down list, select **ACL**.

7. In the **Service interface** drop-down list, select the service interface to which you want to map the ACL interface.

8. In the **Traffic filter** drop-down list, select the previously [created traffic filter](#) for the ACL interface. You can use the same traffic filter for multiple ACL interfaces.

9. In the **Sequence** drop-down list, select the sequential number of the ACL interface. Traffic is directed first to the ACL interface with the lowest number. If the filter used on an ACL interface does not take in the traffic, the

traffic is sent to the second ACL interface, and so on.

Range of values: 1 to 4. Two ACL interfaces with the same serial number cannot be mapped to the same service interface.

10. If necessary, enter a brief description of the ACL interface in the **Description** field.

11. Click **Create**.

The ACL interface is created and displayed in the table.

Viewing the usage of a service interface and an ACL interface

You can view which [transport services](#) are using a service interface or an ACL interface. If a service interface or an ACL interface is used by at least one transport service, such an interface cannot be [deleted](#).

To view the usage of a service interface or ACL interface:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. Click **Management** → **Configuration menu** next to the controller to which the CPE device is connected.

This opens the controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of controller nodes.

3. Go to the **Service interfaces** section.

A table of service interfaces and ACL interfaces is displayed.

4. Click **Management** → **Show usage** next to the service interface or ACL interface for which you want to view usage information.

This opens a window with a table of transport services that are using the service interface or ACL interface.

Deleting a service interface and an ACL interface

You cannot delete a service interface or an ACL interface if it is being used by at least one transport service. You must [view the usage of a service interface or ACL interface](#) and make sure that it is not being used by any transport service.

Deleted service interfaces and ACL interfaces cannot be restored.

To delete a service interface or an ACL interface:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. Click **Management** → **Configuration menu** next to the controller to which the CPE device is connected.

This opens the controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of controller nodes.

3. Go to the **Service interfaces** section.

A table of service interfaces and ACL interfaces is displayed.

4. Click **Management** → **Delete** next to the service interface or ACL interface that you want to delete.

5. In the confirmation window, click **Delete**.

The service interface or ACL interface is deleted and is no longer displayed in the table.

Managing OpenFlow port groups

OpenFlow ports are interfaces of the overlay SDN that are automatically created at the same time as the [SD-WAN interfaces](#). The SD-WAN Controller uses OpenFlow ports to control network traffic. [Service interfaces and UNIs](#) can be created on top of OpenFlow ports.

You can group OpenFlow ports and use the groups when creating [M2M](#) and [P2M](#) transport services. When you add a group of OpenFlow ports to a transport service, a service interface is automatically created on top of each port in the group, which in turn is used by the transport service. Using groups of OpenFlow ports eliminates the need to manually create service interfaces and add them to transport services.

To display the table of OpenFlow port groups, go to the **Infrastructure** menu section, click **Management** → **Configuration menu** next to the controller to which the device is connected, and in the displayed controller settings menu, go to the **OpenFlow groups** section. Information about groups of OpenFlow ports is displayed in the following columns of the table:

- **Name** is the name of the OpenFlow port group.
- **Ports** are the OpenFlow ports added to the group.

The actions you can perform with the table are described in the [Managing solution component tables](#) instructions.

Creating an OpenFlow port group

To create a group of OpenFlow ports:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. Click **Management** → **Configuration menu** next to the controller to which the CPE device is connected.

This opens the controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of controller nodes.

3. Go to the **OpenFlow groups** section.

A table of groups of OpenFlow ports is displayed.

4. In the upper part of the page, click **+ OpenFlow group**.

5. This opens a window; in that window, in the **Name** field, enter the name of the OpenFlow port group.
6. In the **Switch** and **Port** drop-down lists, select the CPE device and OpenFlow port that you want to add to the group. You can add multiple OpenFlow ports to a group.
7. Click **Create**.

The group of OpenFlow interfaces is created and displayed in the table.

Editing an OpenFlow port group

To edit a group of OpenFlow ports:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.
2. Click **Management** → **Configuration menu** next to the controller to which the CPE device is connected.
This opens the controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of controller nodes.
3. Go to the **OpenFlow groups** section.
A table of groups of OpenFlow ports is displayed.
4. Click **Management** → **Edit** next to the group of OpenFlow ports that you want to edit.
5. This opens a window; in that window, in the **Name** field, enter the name of the OpenFlow interface group.
6. If necessary, in the **Switch** and **Port** drop-down lists, select the CPE device and OpenFlow port that you want to add to the group. You can add multiple OpenFlow ports to a group.
7. Click **Save**.

The OpenFlow port group is modified and updated in the table.

Deleting an OpenFlow port group

Deleted groups of OpenFlow ports cannot be restored.

To delete a group of OpenFlow ports:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.
2. Click **Management** → **Configuration menu** next to the controller to which the CPE device is connected.
This opens the controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of controller nodes.
3. Go to the **OpenFlow groups** section.

A table of groups of OpenFlow ports is displayed.

4. Click **Management** → **Delete** next to the group of OpenFlow ports that you want to delete.
5. In the confirmation window, click **Delete**.

The group of OpenFlow ports is deleted and is no longer displayed in the table.

Configuring a UNI for connecting CPE devices to network services

UNIs are mapped to OpenFlow ports and are used to connect a CPE device to [network services](#). A UNI cannot be mapped to an OpenFlow port that is already mapped to an [SD-WAN interface of the WAN type](#).

To avoid creating a UNI on each device individually, you can create a UNI in a CPE template and then apply the template to devices when [adding](#) or [manually registering](#) them. If you edit a UNI in a template, that UNI is automatically modified on all CPE devices that are using the template.

When creating a UNI, a [service interface](#) is automatically created for it.

Managing UNI templates

The table of UNI templates is displayed in the **SD-WAN** → **UNI templates** section. Information about UNI templates is displayed in the following columns of the table:

- **ID** is the ID of the UNI template.
- **Name** is the name of the UNI template.
- **Used** shows whether the UNI template is used by CPE devices.
 - **Yes**
 - **No**
- **Updated** is the date and time when the UNI template settings were last modified.
- **User** is the name of the [user](#) which created the UNI template.
- **Owner** is the [tenant](#) to which the UNI template belongs.

The actions that you can perform with the table are described in the [Managing solution component tables](#) instructions.

UNI template settings are displayed on the following tabs:

- **Information** is the basic information about the UNI template. You can edit the name of the template in the **Name** field.
- **UNIs** are [UNIs created in the template](#).

Creating a UNI template

To create a UNI template:

1. In the menu, go to the **SD-WAN** → **UNI templates** subsection.
A table of UNI templates is displayed.
2. In the upper part of the page, click **+ UNI template**.
3. This opens a window; in that window, enter the name of the UNI template.
4. Click **Create**.

The UNI template is created and displayed in the table.

Deleting a UNI template

Deleted UNI templates cannot be restored.

To delete a UNI template:

1. In the menu, go to the **SD-WAN** → **UNI templates** subsection.
A table of UNI templates is displayed.
2. Click the UNI template that you want to delete.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays the UNI template name and the tenant to which the UNI template is assigned.
3. In the upper part of the settings area, under **Actions**, click **Delete**.
4. In the confirmation window, click **Delete**.

The UNI template is deleted and is no longer displayed in the table.

Managing UNIs

Managing UNIs in a UNI template

To display the table of UNIs in a UNI template, go to the **SD-WAN** → **UNI templates** menu section, click the UNI template, and in the displayed settings area, select the **UNIs** tab. Information about UNIs is displayed in the following columns of the table:

- **Name** is the name of the UNI.
- **OpenFlow interface** is the number of the OpenFlow port mapped to the UNI.

- **Encapsulation** is the traffic classification type on the UNI:
 - **Access**
 - **VLAN**
 - **Q-in-Q**
- **Actions** contains the actions can be performed with the UNI.

Managing UNIs on a CPE device

To display the list of UNIs on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **UNIs** tab.

Creating a UNI

You can create a UNI in a UNI template or on a CPE device. When you create a UNI in a UNI template, that UNI is automatically created on all CPE devices that are using the template.

To create a UNI:

1. Create a UNI in one of the following ways:

- If you want to create a UNI in a UNI template, go to the **SD-WAN** → **UNI templates** menu section, click the template and in the displayed settings area, select the **UNIs** tab.
- If you want to create a UNI on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device and in the displayed settings area, select the **UNIs** tab.

A table or list of UNIs is displayed.

2. Click **+ UNI**.

3. This opens a window; in that window, in the **Name** field, enter the name of the UNI.

4. Specify the OpenFlow port to which you want to map the UNI in one of the following ways:

- If you are creating a UNI in a UNI template, enter the OpenFlow port number in the **OpenFlow interface** field.
- If you are creating a UNI on a CPE device, select the OpenFlow port in the **Port** drop-down list.

5. In the **Encapsulation** drop-down list, select the traffic classification type on the UNI:

- **Access** (default).
- **VLAN** If you select this option, in the **VLAN ID** field, enter the outer VLAN tag of the UNI. Range of values: 1 to 4094.
- **Q-in-Q** If you select this option, do the following:
 - a. In the **VLAN ID** field, enter the outer VLAN tag of the UNI. Range of values: 1 to 4094.

b. In the **Inner VLAN ID** field, enter the inner VLAN tag of the UNI. Range of values: 1 to 4094.

6. If you are creating a UNI on a CPE device, in the **QoS** drop-down list, select a previously [created quality of service rule](#) for the UNI.
7. Click **Create**.
The UNI is created and displayed in the table or list.
8. In the upper part of the settings area, click **Save** to save the settings of the UNI template or CPE device.

Viewing UNI usage

You can view which [network services](#) are using the UNI on a CPE device. If a UNI is being used by at least one network service, such a UNI cannot be [deleted](#).

To view UNI usage:

1. In the menu, go to the **SD-WAN** → **CPE** section.
A table of CPE devices is displayed.
2. Click the CPE device on which you want to view UNI usage.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.
3. Select the **UNIs** tab.
A list of UNIs is displayed.
4. Click **Management** → **Show usage** next to the UNI whose usage you want to view.

This opens a window with a table of network services that are using the UNI.

Editing a UNI

You can edit a UNI in a UNI template. When you edit a UNI in a UNI template, that UNI is modified on all CPE devices that are using the template.

To edit a UNI:

1. In the menu, go to the **SD-WAN** → **UNI templates** subsection.
A table of UNI templates is displayed.
2. Click the UNI template in which you want to edit a UNI.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays the UNI template name and the tenant to which the UNI template is assigned.
3. Select the **UNI** tab.
A table of UNIs is displayed.

4. Click **Edit** next to the UNI that you want to edit.
5. This opens a window; in that window, in the **Name** field, enter the name of the UNI.
6. In the **OpenFlow interface** field, enter the OpenFlow port number to which you want to map the UNI.
7. In the **Encapsulation** drop-down list, select the UNI encapsulation type:
 - **Access** (default).
 - **VLAN** If you select this option, in the **VLAN ID** field, enter the outer VLAN tag of the UNI. Range of values: 1 to 4094.
 - **Q-in-Q** If you select this option, do the following:
 - a. In the **VLAN ID** field, enter the outer VLAN tag of the UNI. Range of values: 1 to 4094.
 - b. In the **Inner VLAN ID** field, enter the inner VLAN tag of the UNI. Range of values: 1 to 4094.
8. Click **Save**.

The UNI is modified and updated in the table.
9. In the upper part of the settings area, click **Save** to save UNI template settings.

Deleting a UNI

You can delete a UNI in a UNI template or on a CPE device. When you delete a UNI in a UNI template, that UNI is automatically delete on all CPE devices that are using the template.

Deleted UNIs cannot be restored.

Deleting a UNI in a UNI template

To delete a UNI in a UNI template:

1. In the menu, go to the **SD-WAN** → **UNI templates** subsection.

A table of UNI templates is displayed.
2. Click the UNI template in which you want to delete a UNI.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays the UNI template name and the tenant to which the UNI template is assigned.
3. Select the **UNIs** tab.

A table of UNIs is displayed.
4. Click **Delete** next to the UNI that you want to delete.

The UNI is deleted and is no longer displayed in the table.

5. In the upper part of the settings area, click **Save** to save UNI template settings.

Deleting an UNI on a CPE device

You cannot delete a UNI if it is being used by at least one [network service](#). You need to [look up the usage of the UNI](#) and make sure that it is not being used by any network service.

To delete a UNI on a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device on which you want to delete a UNI.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon. By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. Select the **UNIs** tab.

A list of UNIs is displayed.

4. Click **Management** → **Delete** next to the UNI that you want to delete.

5. In the confirmation window, click **Delete**.

The UNI is deleted and is no longer displayed in the table.

6. In the upper part of the settings area, click **Save** to save CPE device settings.

Adding or deleting a static route

In addition to dynamic route exchange between CPE devices and external network devices via [BGP](#) and [OSPF](#) protocols, Kaspersky SD-WAN supports static IPv4 routes.

Adding a static route


You can add a static route in a CPE template or on an device. When you add a static route to a CPE template, the static route is automatically added on all devices that are using the template.

To add a static route:

1. Add a static route in one of the following ways:

- If you want to add a static route in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **Static routes** tab.
- If you want to add a static route on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Static routes** tab and select the **Override** check box.

A table of static routes is displayed.

2. Click the add static route icon  plus button.
3. In the **Interface** drop-down list, select the previously [created source network interface of the static route](#).
4. In the **Target** field, enter the destination IPv4 address of the static route.
5. If necessary, in the **IPv4 netmask** field, enter the IPv4 address of the destination subnet of the static route.
6. In the **Gateway** field, enter the IP address of the gateway of the static route.
7. In the **Metric** field, enter a metric for the static route. The default setting is 0.
8. In the **MTU** field, enter the MTU value for the static route.
9. In the **Type** drop-down list, select the type of the static route:
 - **unicast** (default)
 - **local**
 - **broadcast**
 - **multicast**
 - **unreachable**
 - **prohibit**
 - **blackhole**
 - **anycast**
10. If you want to put a static route in a virtual routing and forwarding table, in the **VRF** drop-down list, select a previously [created virtual routing and forwarding table](#). You must place the static route in the virtual routing table that contains the network interface of the source of the static route.

The static route is added and displayed in the table.
11. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Deleting a static route

You can delete a static route in a CPE template or on an device. When you delete a static route in a CPE template, the static route is automatically deleted on all devices that are using the template.


Deleted static routes cannot be restored.

To delete a static route:

1. Delete a static route in one of the following ways:
 - If you want to delete a static route in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **Static routes** tab.

- If you want to delete a static route on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Static routes** tab and select the **Override** check box.

A table of static routes is displayed.

2. Click the delete icon  next to the static route that you want to delete.

The static route is deleted and is no longer displayed in the table.

3. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Filtering routes and traffic packets

You can use the following components for route filtering when working with the [BGP](#) and [OSPF](#) protocols, and for filtering traffic packets when working with the [PIM](#) protocol:

- *Access control lists* (ACL) allow or deny the specified IPv4 prefixes.
- *Prefix lists* are an extended version of access control lists. Prefix lists additionally allow or deny subnet mask ranges. You can use prefix lists in route maps.
- *Route maps* are an extended version of prefix lists. Route maps additionally modify attribute values.

You can create rules in access control lists, prefix lists, and route maps. Each rule is numbered. The rule with the lowest sequence number is the first to be applied to an IPv4 prefix. If none of the rules can be applied, the IPv4 prefix is denied.

Managing access control lists (ACLs)

The table of access control lists is displayed in the CPE template and on the device:

- To display the table of access control lists in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template, and in the displayed settings area, select the **Routing filters** → **Access control lists** tab.
- To display the table of access control lists on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Routing filters** → **Access control lists** tab.

Information about access control lists is displayed in the following columns of the table:

- **Name** is the name of the access control list.
- **Inherited** specifies whether the access control list is inherited from the CPE template:
 - **Yes**
 - **No**

This column is displayed only on the CPE device.

- **Sequence** is the sequence number of the rule in the access control list. The rule with the lowest sequence number is the first to be applied to the IPv4 prefix by the access control list.

- **Network** is the IPv4 prefix to which the access control list must apply the rule.
- **Action** is the action that the rule performs on an IPv4 prefix:
 - **Permit** – allow the IPv4 prefix.
 - **Deny** – deny the IPv4 prefix.
- **Management** contains the actions that can be performed on the access control list.

Creating an access-control list

You can create an access control list in a CPE template or on a device. When you create an access control list in a CPE template, the access control list is automatically created on all devices that are using the template.

To create an access control list:

1. Create an access control list in one of the following ways:

- If you want to create an access control list in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template and in the displayed settings area, select the **Routing filters → Access control lists** tab.
- If you want to create an access control list on a CPE device, go to the **SD-WAN → CPE** menu section, click the device, and in the displayed settings area, select the **Routing filters → Access control lists** tab and select the **Override** check box.

A table of access control lists is displayed.

2. Click **+ Access control list**.

3. This opens a window; in that window, in the **Name** field, enter the name of the access control list. Maximum length: 50 characters. Do not use spaces in this field.

4. Create a rule in the access control list:

a. Click **+ Rule**.

b. In the **Sequence** field, enter the sequential number of the rule. The rule with the lowest sequence number is the first to be applied to the IPv4 prefix by the access control list. Range of values: 1 to 4,294,967,295.

c. In the **Network** drop-down list, select the type of the rule:

- **Any network** for a rule that allows or denies all IPv4 prefixes.
- **IP/mask** for a rule that allows or denies the specified IPv4 prefix. Default value. If you select this value, enter the IPv4 prefix in the field that is displayed.

d. In the **Action** drop-down list, select the action that the rule performs on the IPv4 prefix:

- **Permit** – allow the IPv4 prefix. Default value.
- **Deny** – deny the IPv4 prefix.

The rule is created. You can add multiple rules; to delete a rule, click the delete icon next to it.

5. Click **Create**.

The access control list is created and displayed in the table.

6. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Editing an access control list

You can edit an access control list in a CPE template or on a device. When you edit an access control list in a CPE template, the access control list is automatically modified on all devices that are using the template.

To edit an access control list:

1. Edit an access control list in one of the following ways:

- If you want to edit an access control list in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template and in the displayed settings area, select the **Routing filters → Access control lists** tab.
- If you want to edit an access control list on a CPE device, go to the **SD-WAN → CPE** menu section, click the device, and in the displayed settings area, select the **Routing filters → Access control lists** tab and select the **Override** check box.

A table of access control lists is displayed.

2. Click **Edit** next to the access control list that you want to edit.

3. This opens a window; in that window, in the **Name** field, enter the name of the access control list. Maximum length: 50 characters. Do not use spaces in this field.

4. Edit the rule in the access control list:

a. In the **Sequence** field, enter the sequential number of the rule. The rule with the lowest sequence number is the first to be applied to the IPv4 prefix by the access control list. Range of values: 1 to 4,294,967,295.

b. In the **Network** drop-down list, select the type of the rule:

- **Any network** for a rule that allows or denies all IPv4 prefixes.
- **IP/mask** for a rule that allows or denies the specified IPv4 prefix. Default value. If you select this value, enter the IPv4 prefix in the field that is displayed.

c. In the **Action** drop-down list, select the action that the rule performs on the IPv4 prefix:

- **Permit** — allow the IPv4 prefix. Default value.
- **Deny** — deny the IPv4 prefix.

5. If you want to create a rule in an access control list:

a. Click **+ Rule**.

b. Specify rule settings. The rule settings are described at step 4 of these instructions.

The rule is created. You can add multiple rules; to delete a rule, click the delete icon next to it.

6. Click **Save**.

The access control list is modified and updated in the table.

7. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Deleting an access control list

You can delete an access control list in a CPE template or on a device. When you delete an access control list in a CPE template, the access control list is automatically deleted on all devices that are using the template.

Deleted access control lists cannot be restored.

To delete an access control list:

1. Delete an access control list in one of the following ways:

- If you want to delete an access control list in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template and in the displayed settings area, select the **Routing filters → Access control lists** tab.
- If you want to delete an access control list on a CPE device, go to the **SD-WAN → CPE** menu section, click the device, and in the displayed settings area, select the **Routing filters → Access control lists** tab and select the **Override** check box.

A table of access control lists is displayed.

2. Click **Delete** next to the access control list that you want to delete.

3. In the confirmation window, click **Delete**.

The access control list is deleted and is no longer displayed in the table.

4. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Managing prefix lists

The table of prefix lists is displayed in the CPE template and on the device:

- To display the table of prefix lists in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template, and in the displayed settings area, select the **Routing filters → Prefix lists** tab.
- To display the table of prefix lists on a CPE device, go to the **SD-WAN → CPE** menu section, click the device, and in the displayed settings area, select the **Routing filters → Prefix lists** tab.

Information about prefix lists is displayed in the following columns of the table:

- **Name** is the name of the prefix list.
- **Inherited** specifies whether the prefix list is inherited from the CPE template:
 - **Yes**
 - **No**

This column is displayed only on the CPE device.

- **Sequence** is the sequence number of the rule in the prefix list. The rule with the lowest sequence number is the first to be applied to the IPv4 prefix by the prefix list.
- **Network** is the IPv4 prefix to which the prefix list must apply the rule.
- **Action** is the action that the rule performs on an IPv4 prefix:
 - **Permit** allows the IPv4 prefix.
 - **Deny** denies the IPv4 prefix.
- **Greater or equal** is the start value of the range of subnet masks to which the prefix list must apply the rule.
- **Less or equal** is the end value of the range of subnet masks to which the prefix list must apply the rule.
- **Management** contains the actions that can be performed on the prefix list.

Creating a prefix list

You can create a prefix list in a CPE template or on a device. When you create a prefix list in a CPE template, the prefix list is automatically created on all devices that are using the template.

To create a prefix list:

1. Create a prefix list in one of the following ways:

- If you want to create a prefix list in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **Routing filters** → **Prefix lists** tab.
- If you want to create a prefix list on a CPE device, go to the **SD-WAN** menu section, click the device, and in the displayed settings area, select the **Routing filters** → **Prefix lists** tab and select the **Override** check box.

A table of prefix lists is displayed.

2. Click **+ Prefix list**.

3. This opens a window; in that window, in the **Name** field, enter the name of the prefix list. Maximum length: 50 characters. Do not use spaces in this field.

4. Create a rule in the prefix list:

- a. Click **+ Rule**.

b. In the **Sequence** field, enter the sequential number of the rule. The rule with the lowest sequence number is the first to be applied to the IPv4 prefix by the prefix list. Range of values: 1 to 4,294,967,295.

c. In the **Network** drop-down list, select the type of the rule:

- **Any network** for a rule that allows or denies all IPv4 prefixes.
- **IP/mask** for a rule that allows or denies the specified IPv4 prefix. Default value. If you select this value, enter the IPv4 prefix in the field that is displayed.

d. In the **Action** drop-down list, select the action that the rule performs on the IPv4 prefix:

- **Permit** allows the IPv4 prefix. Default value.
- **Deny** denies the IPv4 prefix.

e. In the **Greater or equal** field, enter the start value of the subnet mask range. Range of values: 0 to 32.

f. In the **Less or equal** field, enter the end value of the subnet mask range. Range of values: 0 to 32.

The rule is created. You can add multiple rules; to delete a rule, click the delete icon next to it.

5. Click **Create**.

The prefix list is created and displayed in the table.

6. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Editing a prefix list

You can edit a prefix list in a CPE template or on a device. When you edit a prefix list in a CPE template, the prefix list is automatically modified on all devices that are using the template.

To edit a prefix list:

1. Edit a prefix list in one of the following ways:

- If you want to edit a prefix list in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **Routing filters** → **Prefix lists** tab.
- If you want to edit a prefix list on a CPE device, go to the **SD-WAN** menu section, click the device, and in the displayed settings area, select the **Routing filters** → **Prefix lists** tab and select the **Override** check box.

A table of prefix lists is displayed.

2. Click **Edit** next to the prefix list that you want to edit.

3. This opens a window; in that window, in the **Name** field, enter the name of the prefix list. Maximum length: 50 characters. Do not use spaces in this field.

4. Edit a rule in the prefix list:

a. In the **Sequence** field, enter the sequential number of the rule. The rule with the lowest sequence number is the first to be applied to the IPv4 prefix by the prefix list. Range of values: 1 to 4,294,967,295.

b. In the **Network** drop-down list, select the type of the rule:

- **Any network** for a rule that allows or denies all IPv4 prefixes.
- **IP/mask** for a rule that allows or denies the specified IPv4 prefix. Default value. If you select this value, enter the IPv4 prefix in the field that is displayed.

c. In the **Action** drop-down list, select the action that the rule performs on the IPv4 prefix:

- **Permit** allows the IPv4 prefix. Default value.
- **Deny** denies the IPv4 prefix.

d. In the **Greater or equal** field, enter the start value of the subnet mask range. Range of values: 0 to 32.

e. In the **Less or equal** field, enter the end value of the subnet mask range. Range of values: 0 to 32.

5. If you want to create a rule in the prefix list:

a. Click **+ Rule**.

b. Specify rule settings. The rule settings are described at step 4 of these instructions.

The rule is created. You can add multiple rules; to delete a rule, click the delete icon next to it.

6. Click **Save**.

The prefix list is modified and updated in the table.

7. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Deleting a prefix list

You can delete a prefix list in a CPE template or on a device. When you delete a prefix list in a CPE template, the prefix list is automatically deleted on all devices that are using the template.

Deleted prefix lists cannot be restored.

To delete a prefix list:

1. Delete a prefix list in one of the following ways:

- If you want to delete a prefix list in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **Routing filters** → **Prefix lists** tab.
- If you want to delete a prefix list on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Routing filters** → **Prefix lists** tab and select the **Override** check box.

A table of prefix lists is displayed.

2. Click **Delete** next to the prefix list that you want to delete.

3. In the confirmation window, click **Delete**.

The prefix list is deleted and is no longer displayed in the table.

4. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Managing route maps

The table of route maps is displayed in the CPE template and on the device:

- To display the table of route maps in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template, and in the displayed settings area, select the **Routing filters** → **Route maps** tab.
- To display the table of route maps on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Routing filters** → **Route maps** tab.

Information about route maps is displayed in the following columns of the table:

- **Name** is the name of the route map.
- **Inherited** specifies whether the route map is inherited from the CPE template:
 - **Yes**
 - **No**

This column is displayed only on the CPE device.

- **Sequence** is the sequence number of the rule in the route map. The rule with the lowest sequence number is the first to be applied to the IPv4 prefix by the route map.
- **Action** is the action that the rule performs on an IPv4 prefix:
 - **Permit** allows the IPv4 prefix.
 - **Deny** denies the IPv4 prefix.
- **Match type** is the criterion that makes the route map apply the rule to the IPv4 prefix:
 - **None** applies the rule to all IPv4 prefixes.
 - **Prefix-List** applies the rule to IPv4 prefixes allowed by the specified prefix list.
- **Value** is a prefix list that must allow the IPv4 prefix to let the route map apply the rule to this IPv4 prefix.
- **Change attribute** is the attribute whose value the rule modifies.
- **New value** is the value that the rule must set for the attribute.
- **Management** contains the actions that can be performed with the route map.

Creating a route map

You can create a route map in a CPE template or on a device. When you create a route map in a CPE template, the route map is automatically created on all devices that are using the template.

To create a route map:

1. Create a route map in one of the following ways:

- If you want to create a route map in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **Routing filters** → **Route maps** tab.
- If you want to create a route map on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Routing filters** → **Route maps** tab and select the **Override** check box.

A table of route maps is displayed.

2. Click **+ Route map**.

3. This opens a window; in that window, in the **Name** field, enter the name of the route map. Maximum length: 50 characters. Do not use spaces in this field.

4. Create a rule in the route map:

a. Click **+ Rule**.

b. In the **Sequence** field, enter the sequential number of the rule. The rule with the lowest sequence number is the first to be applied to the IPv4 prefix by the route map. Range of values: 1 to 4,294,967,295.

c. In the **Action** drop-down list, select the action that the rule performs on the IPv4 prefix:

- **Permit** allows the IPv4 prefix. Default value.
- **Deny** denies the IPv4 prefix.

d. In the **Match type** drop-down list, select the criterion that makes the route map apply the rule to the IPv4 prefix:

- **None** applies the rule to all IPv4 prefixes. Default value.
- **Prefix-List** applies the rule to IPv4 prefixes allowed by the specified prefix list. If you select this value, select a previously **created prefix list** from the [Prefix list](#) drop-down list.

e. If in the **Match type** drop-down list, you selected **Prefix-List**, in the **Change attribute** drop-down list, select the attribute that you want the rule to modify:

- **None** if you do not want to modify attribute values. Default value.
- **IP next-hop** if you want to change the value of the 'next hop' attribute to the specified IPv4 address. If you select this value, enter an IPv4 address in the **New value** field.
- **Local Preference** if you want to change the value of the 'local preference' attribute to the specified value. If you select this value, in the **New value** field, enter a value for the 'local preference' attribute.

Range of values: 0 to 4,294,967,295.

- **Metric** if you want to change the value of the MED attribute to the specified value. If you select this value, in the **New value** field, enter a value for the MED attribute. Range of values: 0 to 4,294,967,295.
- **AS Path Prepend** — Add the number of the autonomous system to the 'as path' attribute. If you select this value, enter the autonomous system number in the **New value** field. You may enter multiple numbers separated by spaces. Range of values: 0 to 4,294,967,295.

The rule is created. You can add multiple rules; to delete a rule, click the delete icon next to it.

5. Click **Create**.

The route map is created and displayed in the table.

6. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Editing a route map

You can edit a route map in a CPE template or on a device. When you edit a route map in a CPE template, the route map is automatically modified on all devices that are using the template.

To edit a route map:

1. Edit a route map in one of the following ways:

- If you want to edit a route map in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **Routing filters** → **Route maps** tab.
- If you want to edit a route map on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Routing filters** → **Route maps** tab and select the **Override** check box.

A table of route maps is displayed.

2. Click **Edit** next to the route map that you want to edit.

3. This opens a window; in that window, in the **Name** field, enter the name of the route map. Maximum length: 50 characters. Do not use spaces in this field.

4. Edit a rule in the route map:

a. In the **Sequence** field, enter the sequential number of the rule. The rule with the lowest sequence number is the first to be applied to the IPv4 prefix by the route map. Range of values: 1 to 4,294,967,295.

b. In the **Action** drop-down list, select the action that the rule performs on the IPv4 prefix:

- **Permit** allows the IPv4 prefix. Default value.
- **Deny** denies the IPv4 prefix.

c. In the **Match type** drop-down list, select the criterion that makes the route map apply the rule to the IPv4 prefix:

- **None** applies the rule to all IPv4 prefixes. Default value.
- **Prefix-List** applies the rule to IPv4 prefixes allowed by the specified prefix list. If you select this value, select a previously **created prefix list** from the [Prefix list](#) drop-down list.

d. If in the **Match type** drop-down list, you selected **Prefix-List**, in the **Change attribute** drop-down list, select the attribute that you want the rule to modify:

- **None** if you do not want to modify attribute values. Default value.
- **IP next-hop** if you want to change the value of the 'next hop' attribute to the specified IPv4 address. If you select this value, enter an IPv4 address in the **New value** field.
- **Local Preference** if you want to change the value of the 'local preference' attribute to the specified value. If you select this value, in the **New value** field, enter a value for the 'local preference' attribute. Range of values: 0 to 4,294,967,295.
- **Metric** if you want to change the value of the MED attribute to the specified value. If you select this value, in the **New value** field, enter a value for the MED attribute. Range of values: 0 to 4,294,967,295.
- **AS Path Prepend** — Add the number of the autonomous system to the 'as path' attribute. If you select this value, enter the autonomous system number in the **New value** field. You may enter multiple numbers separated by spaces. Range of values: 0 to 4,294,967,295.

5. If you want to create a rule in the route map:

- Click **+ Rule**.
- Specify rule settings. The rule settings are described at step 4 of these instructions.

The rule is created. You can add multiple rules; to delete a rule, click the delete icon next to it.

6. Click **Save**.

The route map is modified and updated in the table.

7. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Deleting a route map

You can delete a route map in a CPE template or on a device. When you delete a route map in a CPE template, the route map is automatically deleted on all devices that are using the template.

Deleted route maps cannot be restored.

To delete a route map:

1. Delete a route map in one of the following ways:

- If you want to delete a route map in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **Routing filters** → **Route maps** tab.

- If you want to delete a route map on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Routing filters** → **Route maps** tab and select the **Override** check box.

A table of route maps is displayed.

2. Click **Delete** next to the route map that you want to delete.

3. In the confirmation window, click **Delete**.

The route map is deleted and is no longer displayed in the table.

4. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Route exchange over BGP

Kaspersky SD-WAN supports the BGP (Border Gateway Protocol) dynamic routing protocol for exchanging routing information between CPE devices and external network devices. You can establish internal iBGP (internal BGP) sessions as well as external eBGP (external BGP) sessions.

Dynamic TCP sessions with BGP peer groups are supported, which lets you avoid creating separate BGP peers.

The figures below show examples of BGP being used in the solution:

- Connecting multiple client locations to the L3 SD-WAN network via BGP.

Diagram showing two switches connected to CPE devices via BGP. CPE devices, in turn, are connected via an overlay SD-WAN network.

- Connecting CPE devices to the service provider's IP/MPLS network via BGP.

Diagram showing two CPE devices connected to PE routers via BGP. The PE routers, in turn, are connected via an IP/MPLS underlay network.

- Using BGP to configure the connectivity of CPE devices within the domain.

Diagram showing CPE device connectivity configured using BGP through an SD-WAN gateway over an overlay SD-WAN network.

Basic BGP settings

You can specify basic BGP settings in a CPE template or on the device. When you specify BGP settings in a CPE template, such settings are automatically propagated to all devices that are using the template.

To modify the basic BGP settings:

1. Specify basic BGP settings in one of the following ways:

- If you want to edit the basic BGP settings in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **BGP settings** → **General settings** tab.
- If you want to edit the basic BGP settings on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **BGP settings** → **General settings** tab and select

the **Override** check box.

Basic BGP settings are displayed.

2. In the **BGP** drop-down list, select **Enabled**. By default, the **Disabled** option is selected.
3. If you want to put BGP routes on a CPE device in the specified virtual routing and forwarding table, in the **VRF** drop-down list, select a previously [created virtual routing and forwarding table](#).
4. In the **AS** field, enter the autonomous system number of the CPE device. Range of values: 1 to 4,294,967,295.
5. In the **Router ID** field, enter the IPv4 address that you want to assign to the router ID of the CPE device. If you want to assign an IPv4 address from a specified range of IP addresses:
 - a. Select the **Get router ID from IP pool** check box. This check box is cleared by default.
 - b. In the **IP Pool** drop-down list, select a previously [created range of IP addresses](#).
6. If necessary, in the **Maximum paths** field, enter the maximum number of entries in the routing and forwarding table of the CPE device. Range of values: 1 to 8.
7. If necessary, select the following check boxes:
 - Select the **Always compare MED** check box. This check box allows the CPE device to compare the multi-exit discriminator (MED) of routes advertised from different autonomous systems.

You must make sure that this check box is selected on all CPE devices in your autonomous system. Otherwise, exchange of routing information may result in routing loops.

- Select the **Graceful restart (helper mode)** check box to enable Graceful restart on the CPE device.

These check boxes are cleared by default.

8. If you do not want the CPE device to exchange IPv4 routes with BGP peers by default, clear the **Use default IPv4 unicast routes** check box. This check box is selected by default.
9. If you want to configure BGP timers:
 - a. Select the **BGP timers** check box. This check box is cleared by default.
 - b. In the **Keepalive** field, enter the interval in seconds that the CPE device uses to send control packets to BGP peers. Range of values: 0 to 65,535.
 - c. In the **Holdtime** field, enter the interval in seconds that the CPE device uses when receiving control packets from BGP peers. If no control packets are received from the BGP peer within the specified time, the CPE device considers the peer unavailable. Range of values: 0 to 65,535.
10. If you want to configure route redistribution in BGP, in the **Route redistribution**:
 - a. Select the check boxes next to the route types:
 - **Kernel** to redistribute Kernel routes generated by the operating system of the CPE device.
 - **Connected** to redistribute routes directly connected to [network interfaces](#) of CPE device.

- **Static** to redistribute [static routes](#).
- **OSPF** to redistribute [OSPF routes](#).

These check boxes are cleared by default.

- In the **Route map** drop-down list, select a previously [created route map](#) for redistributed routes.
- In the **Metric** field, enter a metric of redistributed routes. Range of values: 0 to 16,777,214.

11. If you want the CPE device to advertise the specified network to BGP peers:

- Under **Networks**, click **+ Network**.
- In the **Network** field, enter the IPv4 prefix of the subnet.
- In the **Route map** drop-down list, select a previously created route map for the subnet.

The subnet is specified and displayed under **Networks**. You can specify multiple subnets; to delete a subnet, click the delete icon next to it.

12. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Managing BGP peers

The table of BGP peers is displayed in the CPE template and on the device:

- To display the table of BGP peers in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template, and in the displayed settings area, select the **BGP settings** → **Neighbors** tab.
- To display the table of BGP peers on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **BGP settings** → **Neighbors** tab.

Information about BGP peers is displayed in the following columns of the table:

- **Neighbor IP** is the IPv4 address of the BGP peer.
- **Name** is the name of the BGP peer.
- **Description** is a brief description of the BGP peer.
- **Inherited** specifies whether the BGP peer is inherited from the CPE template:
 - **Yes**
 - **No**

This column is displayed only on the CPE device.

- **Remote AS** is the autonomous system number of the BGP peer.
- **Shutdown** indicates whether the BGP peer is disabled and whether a TCP session is established with it:

- **Yes** means the BGP peer is disabled and no TCP session is established with it.
- **No** means the BGP peer is enabled and a TCP session is established with it.
- **Weight** is the weight of routes advertised by the BGP peer.
- **Management** contains the actions that can be performed with the BGP peer.

Creating a BGP peer

You can create a BGP peer in a CPE template or on a device. When you create a BGP peer in a CPE template, the BGP peer is automatically created on all devices that are using the template. The maximum number of dynamic BGP peers is 512.

To create a BGP peer:

1. Create a BGP peer in one of the following ways:

- If you want to create a BGP peer in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **BGP settings** → **Neighbors** tab.
- If you want to create a BGP peer on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **BGP settings** → **Neighbors** tab and select the **Override** check box.

A table of BGP peers is displayed.

2. Click **+ BGP neighbor**.

3. This opens a window; in that window, in the **Name** field, enter the name of the BGP peer. Maximum length: 50 characters.

4. If you want to disable a BGP peer and prevent establishing a TCP session with it, select the **Disable BGP peer** check box. This check box is cleared by default.

5. In the **Neighbor IP** field, enter the IPv4 address of the BGP peer.

6. In the **Remote AS** field, enter the autonomous system number of the BGP peer. Range of values: 1 to 4,294,967,295.

7. If necessary, enter a brief description of the BGP peer in the **Description** field.

8. If you want the CPE device to use a password when establishing a TCP session with the BGP peer, in the **Password** field, enter the password. For a TCP session to be successfully established between two BGP peers, they must use the same password. To see the entered password, you can click the show icon .

9. If necessary, in the **Loopback interface** field, enter the IPv4 address of the loopback interface that the CPE device must send to the BGP peer when establishing a TCP session.

10. If the TCP session is not established directly between the CPE device and the BGP peer, in the **eBGP hops** field, enter the number of hops between the CPE device and the BGP peer. Range of values: 1 to 255.

11. If you want to configure BGP timers:

- a. Select the **Custom BGP timers** check box. This check box is cleared by default.
 - b. In the **Keepalive** field, enter the time interval in seconds that the CPE device uses to send control packets to BGP peers. Range of values: 0 to 65,535.
 - c. In the **Holdtime** field, enter the time interval in seconds that the CPE device uses when receiving control packets from BGP peers. If no control packets are received from the BGP peer within the specified time, the device considers the peer unavailable. Range of values: 0 to 65,535.
12. If you want to use the [BFD protocol](#) to detect loss of connectivity, select the **BFD** check box. This check box is cleared by default.

13. If you want to specify advanced settings for the BGP peer:

- a. Select the **Advanced settings** tab.

Advanced settings of the BGP peer are displayed.

- b. If necessary, select the following check boxes:

- Select the **Soft-reconfiguration inbound** check box to store routes advertised by the BGP peer locally on the CPE device. Using this feature reduces the amount of memory available on the CPE device.
- Select the **Attribute unchanged AS path** check box to prevent modifying the 'AS path' attribute of routes that the CPE device advertises to the BGP peer.
- Select the **Allow AS in** check box to let BGP peers advertise routes to the CPE device with the 'AS path' attribute, whose value is the autonomous system number of the device.
- Select the **Attribute unchanged next-hop** check box to prevent modifying the 'next hop' attribute of routes that the CPE device advertises to the BGP peer.
- Select the **Next-hop self** check box to use the IPv4 address of the CPE device as the 'next-hop' attribute value when advertising routes to the BGP peer.
- Select the **Attribute unchanged MED** check box to prevent modifying the 'MED' attribute of routes that the CPE device advertises to the BGP peer.
- Select the **Route reflector client** check box to assign the *Route Reflector* role to the CPE device and the *Route Reflector Client* role to the BGP peer. You can only select this check box for a BGP peer that is in the same autonomous system as the CPE device.

These check boxes are cleared by default.

- c. In the **Local AS** field, enter the number of the local autonomous system that the CPE device must send to the BGP peer. Range of values: 1 to 4,294,967,295.
- d. In the **Weight** field, enter the weight of the routes advertised by the BGP peer. The greater the weight of a route, the higher its priority. Range of values: 0 to 65,535.
- e. In the **Maximum prefix** field, enter the maximum number of routes that the BGP peer can advertise to a CPE device. Range of values: 1 to 4,294,967,295.
- f. If you want a CPE device to advertise routes with the 'community' attribute to its BGP peer, select the **Send community** check box and select the type of the attribute in the drop-down list:
 - **All** covers all available types of the 'community' attribute.

- **Standard and extended community.**
- **Extended community.**
- **Large community.**
- **Standard community.**

This check box is cleared by default.

g. If you want the CPE device to advertise the default 0.0.0.0/0 route to the BGP peer, select the **Default originate** check box. This check box is cleared by default. You can select the **Set route map** check box and in the drop-down list that is displayed, select a previously [created route map](#) for the 0.0.0.0/0 default route.

14. If you want to configure route filtering for the BGP peer:

a. Select the **Filtering** tab.

The route filtering options are displayed.

b. Under **Route map**, select previously [created route maps](#):

1. In the **Inbound** drop-down list, select a route map for the routes that the BGP peer advertises to the CPE device.
2. In the **Outbound** drop-down list, select a route map for the routes that the CPE device advertises to the BGP peer.

c. Under **Prefix list**, select previously [created prefix lists](#):

1. In the **Inbound** drop-down list, select a prefix list for the routes that the BGP peer advertises to the CPE device.
2. In the **Outbound** drop-down list, select a prefix list for the routes that the CPE device advertises to the BGP peer.

d. Under **Access control list**, select previously [created access control lists](#):

1. In the **Inbound** drop-down list, select an access control list for the routes that the BGP peer advertises to the CPE device.
2. In the **Outbound** drop-down list, select an access control list for the routes that the CPE device advertises to the BGP peer.

15. Click **Create**.

The BGP peer is created and displayed in the table.

16. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Editing a BGP peer

You can edit a BGP peer in a CPE template or on a device. When you edit a BGP peer in a CPE template, the BGP peer is automatically modified on all devices that are using the template. You cannot edit a BGP peer that is inherited from a template on a CPE device.

To edit a BGP peer:

1. Edit a BGP peer in one of the following ways:

- If you want to edit a BGP peer in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **BGP settings** → **Neighbors** tab.
- If you want to edit a BGP peer on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **BGP settings** → **Neighbors** tab and select the **Override** check box.

A table of BGP peers is displayed.

2. Click **Edit** next to the BGP peer that you want to edit.

3. This opens a window; in that window, in the **Name** field, enter the name of the BGP peer. Maximum length: 50 characters.

4. If you want to disable a BGP peer and prevent establishing a TCP session with it, select the **Disable BGP peer** check box. This check box is cleared by default.

5. In the **Neighbor IP** field, enter the IPv4 address of the BGP peer.

6. In the **Remote AS** field, enter the autonomous system number of the BGP peer. Range of values: 1 to 4,294,967,295.

7. If necessary, enter a brief description of the BGP peer in the **Description** field.

8. If you want the CPE device to use a password when establishing a TCP session with the BGP peer, in the **Password** field, enter the password. For a TCP session to be successfully established between two BGP peers, they must use the same password. To see the entered password, you can click the show icon .

9. If necessary, in the **Loopback interface** field, enter the IPv4 address of the loopback interface that the CPE device must send to the BGP peer when establishing a TCP session.

10. If the TCP session is not established directly between the CPE device and the BGP peer, in the **eBGP hops** field, enter the number of hops between the CPE device and the BGP peer. Range of values: 1 to 255.

11. If you want to configure BGP timers:

a. Select the **Custom BGP timers** check box. This check box is cleared by default.

b. In the **Keepalive** field, enter the time interval in seconds that the CPE device uses to send control packets to BGP peers. Range of values: 0 to 65,535.

c. In the **Holdtime** field, enter the time interval in seconds that the CPE device uses when receiving control packets from BGP peers. If no control packets are received from the BGP peer within the specified time, the device considers the peer unavailable. Range of values: 0 to 65,535.

12. If you want to use the [BFD protocol](#) to detect loss of connectivity, select the **BFD** check box. This check box is cleared by default.

13. If you want to specify advanced settings for the BGP peer:

a. Select the **Advanced settings** tab.

Advanced settings of the BGP peer are displayed.

b. If necessary, select the following check boxes:

- Select the **Soft-reconfiguration inbound** check box to store routes advertised by the BGP peer locally on the CPE device. Using this feature reduces the amount of memory available on the CPE device.
- Select the **Attribute unchanged AS path** check box to prevent modifying the 'AS path' attribute of routes that the CPE device advertises to the BGP peer.
- Select the **Allow AS in** check box to let BGP peers advertise routes to the CPE device with the 'AS path' attribute, whose value is the autonomous system number of the device.
- Select the **Attribute unchanged next-hop** check box to prevent modifying the 'next hop' attribute of routes that the CPE device advertises to the BGP peer.
- Select the **Next-hop self** check box to use the IPv4 address of the CPE device as the 'next-hop' attribute value when advertising routes to the BGP peer.
- Select the **Attribute unchanged MED** check box to prevent modifying the 'MED' attribute of routes that the CPE device advertises to the BGP peer.
- Select the **Route reflector client** check box to assign the *Route Reflector* role to the CPE device and the *Route Reflector Client* role to the BGP peer. You can only select this check box for a BGP peer that is in the same autonomous system as the CPE device.

These check boxes are cleared by default.

c. In the **Local AS** field, enter the number of the local autonomous system that the CPE device must send to the BGP peer. Range of values: 1 to 4,294,967,295.

d. In the **Weight** field, enter the weight of the routes advertised by the BGP peer. The greater the weight of a route, the higher its priority. Range of values: 0 to 65,535.

e. In the **Maximum prefix** field, enter the maximum number of routes that the BGP peer can advertise to a CPE device. Range of values: 1 to 4,294,967,295.

f. If you want a CPE device to advertise routes with the 'community' attribute to its BGP peer, select the **Send community** check box and select the type of the attribute in the drop-down list:

- **All** covers all available types of the 'community' attribute.
- **Standard and extended community.**
- **Extended community.**
- **Large community.**
- **Standard community.**

This check box is cleared by default.

g. If you want the CPE device to advertise the default 0.0.0.0/0 route to the BGP peer, select the **Default originate** check box. This check box is cleared by default. You can select the **Set route map** check box and in the drop-down list that is displayed, select a previously [created route map](#) for the 0.0.0.0/0 default route.

14. If you want to configure route filtering for the BGP peer:

a. Select the **Filtering** tab.

The route filtering options are displayed.

b. Under **Route map**, select previously [created route maps](#):

1. In the **Inbound** drop-down list, select a route map for the routes that the BGP peer advertises to the CPE device.
2. In the **Outbound** drop-down list, select a route map for the routes that the CPE device advertises to the BGP peer.

c. Under **Prefix list**, select previously [created prefix lists](#):

1. In the **Inbound** drop-down list, select a prefix list for the routes that the BGP peer advertises to the CPE device.
2. In the **Outbound** drop-down list, select a prefix list for the routes that the CPE device advertises to the BGP peer.

d. Under **Access control list**, select previously [created access control lists](#):

1. In the **Inbound** drop-down list, select an access control list for the routes that the BGP peer advertises to the CPE device.
2. In the **Outbound** drop-down list, select an access control list for the routes that the CPE device advertises to the BGP peer.

15. Click **Save**.

The BGP peer is modified and updated in the table.

16. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Deleting a BGP peer

You can delete a BGP peer in a CPE template or on a device. When you delete a BGP peer in a CPE template, the BGP peer is automatically deleted on all devices that are using the template. You cannot delete a BGP peer that is inherited from a template on a CPE device.

Deleted BGP peers cannot be restored.

To delete a BGP peer:

1. Delete a BGP peer in one of the following ways:

- If you want to delete a BGP peer in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **BGP settings** → **Neighbors** tab.
- If you want to delete a BGP peer on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **BGP settings** → **Neighbors** tab and select the **Override** check box.

A table of BGP peers is displayed.

2. Click **Delete** next to the BGP peer that you want to delete.
3. In the confirmation window, click **Delete**.
The BGP peer is deleted and is no longer displayed in the table.
4. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Managing BGP peer groups

The table of BGP peer groups is displayed in the CPE template and on the device:

- To display the table of BGP peer groups in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template, and in the displayed settings area, select the **BGP settings** → **Peer groups** tab.
- To display the table of BGP peer groups on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **BGP settings** → **Peer groups** tab and select the **Override** check box.

Information about BGP peer groups is displayed in the following columns of the table:

- **Name** is the name of the BGP peer group.
- **BGP range** is the IPv4 prefix of the BGP peer group.
- **Description** is a brief description of the BGP peer group.
- **Inherited** specifies whether the BGP peer group is inherited from the CPE template:
 - **Yes**
 - **No**

This column is displayed only on the CPE device.

- **Remote AS** is the autonomous system number of the BGP peer group.
- **Shutdown** indicates whether the BGP peer group is disabled and whether a TCP session is established with it:
 - **Yes** means the BGP peer group is disabled and no TCP session is established with it.
 - **No** means the BGP peer is enabled and a TCP session is established with it.
- **Weight** is the weight of routes advertised by the BGP peer group.
- **Management** contains the actions that can be performed with the BGP peer group.

Creating a BGP peer group

You can create a BGP peer group in a CPE template or on a device. When you create a BGP peer group in a CPE template, the group is automatically created on all devices that are using the template.

To create a BGP peer group:

1. Create a BGP peer group in one of the following ways:

- If you want to create a BGP peer group in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **BGP settings** → **Peer groups** tab.
- If you want to create a BGP peer group on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **BGP settings** → **Peer groups** tab and select the **Override** check box.

A table of BGP peer groups is displayed.

2. Click **+ Peer group**.

3. This opens a window; in that window, in the **Name** field, enter the name of the BGP peer group. Maximum length: 50 characters.

4. If you want to disable a BGP peer group and prevent establishing a TCP session with it, select the **Disable BGP peer group** check box. This check box is cleared by default.

5. In the **BGP range** field, enter the IPv4 prefix of the BGP peer group.

6. In the **Remote AS** field, enter the autonomous system number of the BGP peer group. Range of values: 1 to 4,294,967,295.

7. If necessary, enter a brief description of the BGP peer group in the **Description** field.

8. If you want the CPE device to use a password when establishing a TCP session with the BGP peer group, in the **Password** field, enter the password. For a TCP session to be successfully established between two BGP peers, they must use the same password. To see the entered password, you can click the show icon .

9. In the **Loopback interface** field, enter the IPv4 address of the loopback interface that the CPE device must send to the BGP peer group when establishing a TCP session.

10. If the TCP session is not established directly between the CPE device and the BGP peer group, in the **eBGP hops** field, enter the number of hops between the CPE device and the BGP peer group. Range of values: 1 to 255.

11. If you want to configure BGP timers:

a. Select the **Custom BGP timers** check box. This check box is cleared by default.

b. In the **Keepalive** field, enter the time interval in seconds that the CPE device uses to send control packets to the BGP peer group. Range of values: 0 to 65,535.

c. In the **Holdtime** field, enter the time interval in seconds that the CPE device uses when receiving control packets from the BGP peer group. If no control packets are received from the BGP peer within the specified time, the CPE device considers the peer unavailable. Range of values: 0 to 65,535.

12. If you want to use the [BFD protocol](#) to detect loss of connectivity, select the **BFD** check box. This check box is cleared by default.

13. If you want to specify advanced settings for the BGP peer group:

a. Select the **Advanced settings** tab.

Advanced settings of the BGP peer group are displayed.

b. If necessary, select the following check boxes:

- Select the **Soft-reconfiguration inbound** check box to store routes advertised by the BGP peer group locally on the CPE device. Using this feature reduces the amount of memory available on the CPE device.
- Select the **Attribute unchanged AS path** check box to prevent modifying the 'AS path' attribute of routes that the CPE device advertises to the BGP peer group.
- Select the **Allow AS in** check box to let the BGP peer group advertise routes to the CPE device with the 'AS path' attribute, whose value is the autonomous system number of the device.
- Select the **Attribute unchanged next-hop** check box to prevent modifying the 'next hop' attribute of routes that the CPE device advertises to the BGP peer group.
- Select the **Next-hop self** check box to use the IPv4 address of the CPE device as the 'next-hop' attribute value when advertising routes to the BGP peer group.
- Select the **Attribute unchanged MED** check box to prevent modifying the 'MED' attribute of routes that the CPE device advertises to the BGP peer group.
- Select the **Route reflector client** check box to assign the *Route Reflector* role to the CPE device and the *Route Reflector Client* role to the BGP peer group. You can only select this check box for a BGP peer group that is in the same autonomous system as the CPE device.

These check boxes are cleared by default.

c. In the **Local AS** field, enter the number of the local autonomous system that the CPE device must send to the BGP peer group. Range of values: 1 to 4,294,967,295.

d. In the **Weight** field, enter the weight of the routes advertised by the BGP peer group. The greater the weight of a route, the higher its priority. Range of values: 0 to 65,535.

e. In the **Maximum prefix** field, enter the maximum number of routes that the BGP peer group can advertise to a CPE device. Range of values: 1 to 4,294,967,295.

f. If you want a CPE device to advertise routes with the 'community' attribute to the BGP peer group, select the **Send community** check box and select the type of attribute to be sent in the drop-down list:

- **All** covers all available types of the 'community' attribute.
- **Standard and extended community.**
- **Extended community.**
- **Large community.**
- **Standard community.**

This check box is cleared by default.

g. If you want the CPE device to advertise the default 0.0.0.0/0 route to the BGP peer group, select the **Default originate** check box. This check box is cleared by default. You can select the **Set route map** check box and in the drop-down list that is displayed, select a previously [created route map](#) for the 0.0.0.0/0 default route.

14. If you want to configure route filtering for the BGP peer group:

a. Select the **Filtering** tab.

The route filtering settings are displayed.

b. Under **Route map**, select previously [created route maps](#):

1. In the **Inbound** drop-down list, select a route map for the routes that the BGP peer group advertises to the CPE device.
2. In the **Outbound** drop-down list, select a route map for the routes that the CPE device advertises to the BGP peer group.

c. Under **Prefix list**, select previously [created prefix lists](#):

1. In the **Inbound** drop-down list, select a list of prefixes that the BGP peer group advertises to the CPE device.
2. In the **Outbound** drop-down list, select a prefix list for the routes that the CPE device advertises to the BGP peer group.

d. Under **Access control list**, select previously [created access control lists](#):

1. In the **Inbound** drop-down list, select an access control list for the routes that the BGP peer group advertises to the CPE device.
2. In the **Outbound** drop-down list, select an access control list for the routes that the CPE device advertises to the BGP peer group.

15. Click **Create**.

The BGP peer group is created and displayed in the table.

16. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Editing a BGP peer group

You can edit a BGP peer group in a CPE template or on a device. When you edit a BGP peer group in a CPE template, the group is automatically modified on all devices that are using the template. You cannot edit a BGP peer group that is inherited from a template on a CPE device.

To edit a BGP peer group:

1. Edit a BGP peer group in one of the following ways:

- If you want to edit a BGP peer group in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **BGP settings** → **Peer groups** tab.
- If you want to edit a BGP peer group on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **BGP settings** → **Peer groups** tab and select the **Override** check box.

A table of BGP peer groups is displayed.

2. Click **Edit** next to the BGP peer group that you want to edit.

3. This opens a window; in that window, in the **Name** field, enter the name of the BGP peer group. Maximum length: 50 characters.
4. If you want to disable a BGP peer group and prevent establishing a TCP session with it, select the **Disable BGP peer group** check box. This check box is cleared by default.
5. In the **BGP range** field, enter the IPv4 prefix of the BGP peer group.
6. In the **Remote AS** field, enter the autonomous system number of the BGP peer group. Range of values: 1 to 4,294,967,295.
7. If necessary, enter a brief description of the BGP peer group in the **Description** field.
8. If you want the CPE device to use a password when establishing a TCP session with the BGP peer group, in the **Password** field, enter the password. For a TCP session to be successfully established between two BGP peers, they must use the same password. To see the entered password, you can click the show icon .
9. In the **Loopback interface** field, enter the IPv4 address of the loopback interface that the CPE device must send to the BGP peer group when establishing a TCP session.
10. If the TCP session is not established directly between the CPE device and the BGP peer group, in the **eBGP hops** field, enter the number of hops between the CPE device and the BGP peer group. Range of values: 1 to 255.
11. If you want to configure BGP timers:
 - a. Select the **Custom BGP timers** check box. This check box is cleared by default.
 - b. In the **Keepalive** field, enter the time interval in seconds that the CPE device uses to send control packets to the BGP peer group. Range of values: 0 to 65,535.
 - c. In the **Holdtime** field, enter the time interval in seconds that the CPE device uses when receiving control packets from the BGP peer group. If no control packets are received from the BGP peer within the specified time, the CPE device considers the peer unavailable. Range of values: 0 to 65,535.
12. If you want to use the [BFD protocol](#) to detect loss of connectivity, select the **BFD** check box. This check box is cleared by default.
13. If you want to specify advanced settings for the BGP peer group:
 - a. Select the **Advanced settings** tab.
Advanced settings of the BGP peer group are displayed.
 - b. If necessary, select the following check boxes:
 - Select the **Soft-reconfiguration inbound** check box to store routes advertised by the BGP peer group locally on the CPE device. Using this feature reduces the amount of memory available on the CPE device.
 - Select the **Attribute unchanged AS path** check box to prevent modifying the 'AS path' attribute of routes that the CPE device advertises to the BGP peer group.
 - Select the **Allow AS in** check box to let the BGP peer group advertise routes to the CPE device with the 'AS path' attribute, whose value is the autonomous system number of the device.
 - Select the **Attribute unchanged next-hop** check box to prevent modifying the 'next hop' attribute of routes that the CPE device advertises to the BGP peer group.

- Select the **Next-hop self** check box to use the IPv4 address of the CPE device as the 'next-hop' attribute value when advertising routes to the BGP peer group.
- Select the **Attribute unchanged MED** check box to prevent modifying the 'MED' attribute of routes that the CPE device advertises to the BGP peer group.
- Select the **Route reflector client** check box to assign the *Route Reflector* role to the CPE device and the *Route Reflector Client* role to the BGP peer group. You can only select this check box for a BGP peer group that is in the same autonomous system as the CPE device.

These check boxes are cleared by default.

- In the **Local AS** field, enter the number of the local autonomous system that the CPE device must send to the BGP peer group. Range of values: 1 to 4,294,967,295.
- In the **Weight** field, enter the weight of the routes advertised by the BGP peer group. The greater the weight of a route, the higher its priority. Range of values: 0 to 65,535.
- In the **Maximum prefix** field, enter the maximum number of routes that the BGP peer group can advertise to a CPE device. Range of values: 1 to 4,294,967,295.
- If you want a CPE device to advertise routes with the 'community' attribute to the BGP peer group, select the **Send community** check box and select the type of attribute to be sent in the drop-down list:

- **All** covers all available types of the 'community' attribute.
- **Standard and extended community.**
- **Extended community.**
- **Large community.**
- **Standard community.**

This check box is cleared by default.

- If you want the CPE device to advertise the default 0.0.0.0/0 route to the BGP peer group, select the **Default originate** check box. This check box is cleared by default. You can select the **Set route map** check box and in the drop-down list that is displayed, select a previously [created route map](#) for the 0.0.0.0/0 default route.

14. If you want to configure route filtering for the BGP peer group:

- Select the **Filtering** tab.

The route filtering settings are displayed.

- Under **Route map**, select previously [created route maps](#):

- In the **Inbound** drop-down list, select a route map for the routes that the BGP peer group advertises to the CPE device.
- In the **Outbound** drop-down list, select a route map for the routes that the CPE device advertises to the BGP peer group.

- Under **Prefix list**, select previously [created prefix lists](#):

1. In the **Inbound** drop-down list, select a list of prefixes that the BGP peer group advertises to the CPE device.
2. In the **Outbound** drop-down list, select a prefix list for the routes that the CPE device advertises to the BGP peer group.

d. Under **Access control list**, select previously [created access control lists](#):

1. In the **Inbound** drop-down list, select an access control list for the routes that the BGP peer group advertises to the CPE device.
2. In the **Outbound** drop-down list, select an access control list for the routes that the CPE device advertises to the BGP peer group.

15. Click **Save**.

The BGP peer group is modified and updated in the table.

16. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Deleting a BGP peer group

You can delete a BGP peer group in a CPE template or on a device. When you delete a BGP peer group in a CPE template, the group is automatically deleted on all devices that are using the template. You cannot delete a BGP peer group that is inherited from a template on a CPE device.

Deleted BGP peer groups cannot be restored.

To delete a BGP peer group:

1. Delete a BGP peer group in one of the following ways:

- If you want to delete a BGP peer group in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **BGP settings** → **Peer groups** tab.
- If you want to delete a BGP peer group on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **BGP settings** → **Peer groups** tab and select the **Override** check box.

A table of BGP peer groups is displayed.

2. Click **Delete** next to the BGP peer group that you want to delete.

3. In the confirmation window, click **Delete**.

The BGP peer group is deleted and is no longer displayed in the table.

4. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Route exchange over OSPF

Kaspersky SD-WAN supports the OSPF (Open Shortest Path First) dynamic routing protocol for exchanging routing information between CPE devices and external network devices. When configuring the protocol, you can create OSPF areas and OSPF interfaces.

Basic OSPF settings

You can specify basic OSPF settings in a CPE template or on the device. When you specify OSPF settings in a CPE template, such settings are automatically propagated to all devices that are using the template.

To modify the basic OSPF settings:

1. Specify basic OSPF settings in one of the following ways:

- If you want to edit the basic OSPF settings in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **OSPF** → **General settings** tab.
- If you want to edit the basic OSPF settings on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **OSPF** → **General settings** tab and select the **Override** check box.

The OSPF settings are displayed.

2. In the **OSPF** drop-down list, select **Enabled**. By default, the **Disabled** option is selected.

3. In the **Router ID** field, enter the IPv4 address that you want to assign to the router ID of the CPE device.

4. In the **Maximum paths** field, enter the maximum number of entries in the routing and forwarding table of the CPE device. Range of values: 1 to 16.

5. If you want to use the CPE device as an Area Border Router (ABR), in the **ABR type** drop-down list, select one of the following implementations:

- **IBM** (default implementation)
- **CISCO**
- **SHORTCUT**
- **STANDARD**

6. In the **Auto cost reference bandwidth** field, enter the reference bandwidth for calculating the cost of links on the CPE device. Range of values: 1 to 4,294,967.

7. If you want to switch all OSPF interfaces of the CPE device to passive mode, select the **Passive interface default** check box. In passive mode, OSPF interfaces do not exchange traffic packets. This check box is cleared by default.

8. If you want to keep an OSPF log, select the **Log adjacency changes** check box. You can select the **Log adjacency changes** check box to keep a more verbose OSPF log. These check boxes are cleared by default.

9. If you want to configure route redistribution in OSPF, under **Route redistribution**, do the following:

- a. Select the check boxes next to the route types:

- **BGP** to redistribute [BGP routes](#).
- **Connected** to redistribute routes directly connected to [network interfaces](#) of CPE device.
- **Kernel** to redistribute Kernel routes generated by the operating system of the CPE device.
- **Static** to redistribute [static routes](#).

These check boxes are cleared by default.

- In the **Route map** drop-down list, select a previously [created route map](#) for redistributed routes.
 - In the **Metric** field, enter a metric of redistributed routes. Range of values: 0 to 16,777,214.
 - In the **Metric type** drop-down list, select the type of the metric:
 - **Type 1** (or "internal metric")
 - **Type 2** (or "external metric")
 - Select the **Filtering** check box and in the **Access control list** drop-down list, select a previously [created access control list](#) for reallocated routes. This check box is cleared by default.
- In the **Default metric** field, enter the default metric of OSPF routes. Range of values: 0 to 16,777,214.
 - If you want to configure the CPE device to advertise the default route 0.0.0.0/0 to OSPF peers:
 - Select the **Default originate** check box. This check box is cleared by default.
 - Select the **Always** check box to always advertise the default 0.0.0.0/0 route, even if it is not present in the route table of the CPE device. This check box is cleared by default.
 - In the **Metric type** drop-down list, select the type of metric for the 0.0.0.0/0 default route:
 - **Type 1**
 - **Type 2**
 - In the **Metric** field, enter a metric for the 0.0.0.0/0 default route. Range of values: 0 to 16,777,214.
 - In the **Route map** drop-down list, select a previously [created route map](#) for the 0.0.0.0/0 default route.
 - In the **Distance** field, enter the administrative distance for all OSPF routes. The lower the administrative distance specified for a protocol, the higher the priority its route have. For example, if you want OSPF routes to always be preferred over BGP routes, specify the administrative distance of 1 for OSPF and 2 for BGP. Range of values: 1 to 255.
 - If you want to configure administrative distances for individual OSPF routes:
 - Select the **Distance OSPF** check box. This check box is cleared by default.
 - In the **External** field, enter the administrative distance for routes from external OSPF domains or routing protocols. Range of values: 1 to 255.
 - In the **Inter-area** field, enter the administrative distance for routes from different areas of the same OSPF domain. Range of values: 1 to 255.

- d. In the **Intra-area** field, enter the administrative distance for routes from the same area. Range of values: 1 to 255.
14. If you want to enable Graceful restart on the CPE device:
- Select the **Graceful restart** check box. This check box is cleared by default.
 - In the **Grace period (sec.)** field, enter the length of time, in seconds, during which the CPE device must announce its intention to restart to OSPF peers. Range of values: 1 to 1800.
15. If you want to configure timers for the Shortest Path First (SPF) algorithm calculations:
- Select the **Timers throttle SPF** check box. This check box is cleared by default.
 - In the **Delay (sec.)** field, enter the length in seconds of the delay before starting the calculations of the SPF algorithm. Range of values: 0 to 600,000.
 - In the **Initial hold-time (ms.)** field, enter the minimum retention time in milliseconds between two calculations of the SPF algorithm. Range of values: 0 to 600,000.
 - In the **Maximum hold-time (ms.)** field, enter the maximum retention time in milliseconds between two calculations of the SPF algorithm. Range of values: 0 to 600,000.
16. If you want to configure Link State Advertisement (LSA) to OSPF peers for the CPE device:
- Select the **Administrative** check box to have the CPE device use the maximum metric in link state advertisements to OSPF peers.
 - If you want to specify the time during which the CPE device must use the maximum metric in link state advertisement to OSPF peers when the OSPF protocol is started or restarted:
 - Select the **On startup** check box. This check box is cleared by default.
 - In the **Timer (sec.)** field, enter the time in seconds. Range of values: 5 to 86,400.
 - If you want to specify the time during which the CPE device must use the maximum metric in link state advertisement to OSPF peers when the OSPF protocol is disabled:
 - Select the **On shutdown** check box. This check box is cleared by default.
 - In the **Timer (sec.)** field, enter the time in seconds. Range of values: 5 to 100.
17. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Managing OSPF areas

The table of OSPF areas is displayed in the CPE template and on the device:

- To display the table of OSPF areas in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template, and in the displayed settings area, select the **OSPF** → **OSPF areas** tab.
- To display the table of OSPF areas on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **OSPF** → **OSPF areas** tab.

Information about OSPF areas is displayed in the following columns of the table:

- **OSPF area** is the ID of the OSPF area in IPv4 address format or an integer.
- **Area type** is the type of the OSPF stub area:
 - **Stub**
 - **Stub NO-SUMMARY**
 - **NSSA**
 - **NSSA NO-SUMMARY**

This value is displayed only for stub areas.

- **OSPF ranges** specifies OSPF ranges.
- **Management** contains the actions that can be performed with the OSPF area.

Creating an OSPF area

You can create an OSPF area in a CPE template or on a device. When you create an OSPF area in a CPE template, the OSPF area is automatically created on all devices that are using the template.

To create an OSPF area:

1. Create an OSPF area in one of the following ways:

- If you want to create an OSPF area in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **OSPF** → **OSPF areas** tab.
- If you want to create an OSPF area on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **OSPF** → **OSPF areas** tab and select the **Override** check box.

A table of OSPF areas is displayed.

2. Click **+ OSPF area**.

3. This opens a window; in that window, in the **OSPF area** field, enter the OSPF area ID as an IPv4 address or an integer number.

4. If you want to make the OSPF area a stub area:

a. Select the **Stub** check box. This check box is cleared by default.

b. In the **Area type** drop-down list, select a stub area type:

- **Stub**
- **Stub NO-SUMMARY**

- **NSSA**
- **NSSA NO-SUMMARY**

c. If the **Area type** drop-down list, you selected **NSSA** or **NSSA NO-SUMMARY**, if you need to prevent the advertisement of the 0.0.0.0/0 default route to the NSSA area, select the **NSSA suppress FA** check box. This check box is cleared by default.

d. In the **Default cost** field, enter a metric for the default route or for summary routes. Range of values: 0 to 16,777,215.

5. If you want to use the shortcut method for SPF calculations, select the **Shortcut** check box. This check box is cleared by default.

6. In the **Authentication** drop-down list, select the OSPF authentication method:

- **Message digest** to use the MD5 algorithm.
- **Simple password** to use an unencrypted password. This authentication method is less secure than MD5 algorithm, however, it can provide authentication when used in a trusted network environment.

7. If you want to specify OSPF ranges:

a. Under **OSPF ranges**, click **+ Range**.

b. In the **Range** field, enter the IPv4 prefix of the routes.

c. In the **Action** drop-down list, select the action to perform with routes:

- **Advertise** if you want to advertise routes over the OSPF protocol. Default value.
- **Not announce** if you do not want to advertise routes over the OSPF protocol.
- **Substitute** to replace the IPv4 prefix of the routes with the specified IPv4 prefix, and then advertise these over the OSPF protocol. If you select this value, in the **Substitute** field, enter the IPv4 prefix.

d. If in the **Action** drop-down list, you selected **Advertise** or **Substitute**, in the **Cost** field, enter a metric for routes. Range of values: 0 to 16,777,215.

The OSPF range is specified and displayed under **OSPF ranges**. You can specify multiple OSPF ranges; to delete a range, click the delete icon next to it.

8. If you want to connect the OSPF area to another area through a transit area, specify a virtual link:

a. Under **Virtual links**, click **+ Virtual link**.

b. In the **Address** field, enter the IPv4 address of the network interface of the router in the transit area.

The virtual link is specified and displayed under **OSPF ranges**. You can specify multiple virtual links; to delete a link, click the delete icon next to it.

9. If you want to configure route filtering for the OSPF area, under **Filtering**, do the following:

a. Select previously [created access control lists](#):

1. In the **Export list** drop-down list, select an access control list for routes that are advertised from the OSPF area to other areas.
 2. In the **Import list** drop-down list, select an access control list for routes that are advertised from other OSPF area to the given area.
- b. Select previously [created prefix lists](#):
1. In the **Outbound filter list** drop-down list, select a prefix list for routes that are advertised from the OSPF area to other areas.
 2. In the **Inbound filter list** drop-down list, select a prefix list for routes that are advertised from other OSPF area to the given area.
10. Click **Save**.
- The OSPF area is created and displayed in the table.
11. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Editing an OSPF area

You can edit an OSPF area in a CPE template or on a device. When you edit an OSPF area in a CPE template, the OSPF area is automatically modified on all devices that are using the template.

To edit an OSPF area:

1. Edit an OSPF area in one of the following ways:
 - If you want to edit an OSPF area in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **OSPF** → **OSPF areas** tab.
 - If you want to edit an OSPF area on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **OSPF** → **OSPF areas** tab and select the **Override** check box.

A table of OSPF areas is displayed.

2. Click **Edit** next to the OSPF area that you want to edit.
3. This opens a window; in that window, in the **OSPF area** field, enter the OSPF area ID as an IPv4 address or an integer number.
4. If you want to make the OSPF area a stub area:
 - a. Select the **Stub** check box. This check box is cleared by default.
 - b. In the **Area type** drop-down list, select a stub area type:
 - **Stub**
 - **Stub NO-SUMMARY**
 - **NSSA**

- **NSSA NO-SUMMARY**

c. If the **Area type** drop-down list, you selected **NSSA** or **NSSA NO-SUMMARY**, if you need to prevent the advertisement of the 0.0.0.0/0 default route to the NSSA area, select the **NSSA suppress FA** check box. This check box is cleared by default.

d. In the **Default cost** field, enter a metric for the default route or for summary routes. Range of values: 0 to 16,777,215.

5. If you want to use the shortcut method for SPF calculations, select the **Shortcut** check box. This check box is cleared by default.

6. In the **Authentication** drop-down list, select the OSPF authentication method:

- **Message digest** to use the MD5 algorithm.
- **Simple password** to use an unencrypted password. This authentication method is less secure than MD5 algorithm, however, it can provide authentication when used in a trusted network environment.

7. If you want to specify OSPF ranges:

a. Under **OSPF ranges**, click **+ Range**.

b. In the **Range** field, enter the IPv4 prefix of the routes.

c. In the **Action** drop-down list, select the action to perform with routes:

- **Advertise** if you want to advertise routes over the OSPF protocol. Default value.
- **Not announce** if you do not want to advertise routes over the OSPF protocol.
- **Substitute** to replace the IPv4 prefix of the routes with the specified IPv4 prefix, and then advertise these over the OSPF protocol. If you select this value, in the **Substitute** field, enter the IPv4 prefix.

d. If in the **Action** drop-down list, you selected **Advertise** or **Substitute**, in the **Cost** field, enter a metric for routes. Range of values: 0 to 16,777,215.

The OSPF range is specified and displayed under **OSPF ranges**. You can specify multiple OSPF ranges; to delete a range, click the delete icon next to it.

8. If you want to connect the OSPF area to another area through a transit area, specify a virtual link:

a. Under **Virtual links**, click **+ Virtual link**.

b. In the **Address** field, enter the IPv4 address of the network interface of the router in the transit area.

The virtual link is specified and displayed under **OSPF ranges**. You can specify multiple virtual links; to delete a link, click the delete icon next to it.

9. If you want to configure route filtering for the OSPF area, under **Filtering**, do the following:

a. Select previously [created access control lists](#):

1. In the **Export list** drop-down list, select an access control list for routes that are advertised from the OSPF area to other areas.

2. In the **Import list** drop-down list, select an access control list for routes that are advertised from other OSPF area to the given area.

b. Select previously [created prefix lists](#):

1. In the **Outbound filter list** drop-down list, select a prefix list for routes that are advertised from the OSPF area to other areas.

2. In the **Inbound filter list** drop-down list, select a prefix list for routes that are advertised from other OSPF area to the given area.

10. Click **Save**.

The OSPF area is modified and updated in the table.

11. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Deleting an OSPF area

You can delete an OSPF area in a CPE template or on a device. When you delete an OSPF area in a CPE template, the OSPF area is automatically deleted on all devices that are using the template.

Deleted OSPF areas cannot be restored.

To delete an OSPF area:

1. Delete an OSPF area in one of the following ways:

- If you want to delete an OSPF area in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template and in the displayed settings area, select the **OSPF → OSPF areas** tab.
- If you want to delete an OSPF area on a CPE device, go to the **SD-WAN → CPE** menu section, click the device, and in the displayed settings area, select the **OSPF → OSPF areas** tab and select the **Override** check box.

A table of OSPF areas is displayed.

2. Click **Delete** next to the OSPF area that you want to delete.

3. In the confirmation window, click **Delete**.

The OSPF area is deleted and is no longer displayed in the table.

4. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Managing OSPF interfaces

The table of OSPF interfaces is displayed in the CPE template and on the device:

- To display the table of OSPF interfaces in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template, and in the displayed settings area, select the **OSPF → OSPF interface** tab.

- To display the table of OSPF interfaces on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **OSPF** → **OSPF interface** tab.

Information about OSPF interfaces is displayed in the following columns of the table:

- **Interface** is the [network interface](#) used as an OSPF interface.
- **OSPF area** is the ID of the [OSPF area](#) to which the OSPF interface belongs.
- **Authentication** is the authentication method.
- **Network type** is the type of network to which the OSPF interface is connected.
- **Management** contains the actions that can be performed with the OSPF interface.

Creating an OSPF interface

You can create an OSPF interface in a CPE template or on an individual device. When you create an OSPF interface in a CPE template, the interface is automatically created on all devices that are using the template.

To create an OSPF interface:

1. Create an OSPF interface in one of the following ways:

- If you want to create an OSPF interface in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **OSPF** → **OSPF interface** tab.
- If you want to create an OSPF interface on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **OSPF** → **OSPF interface** tab and select the **Override** check box.

A table of OSPF interfaces is displayed.

2. Click **+ OSPF interface**.

3. This opens a window, in that window, in the **Interface** drop-down list, select a previously [created network interface](#) which you want to use as an OSPF interface.

4. In the **OSPF area** field, enter the ID of the OSPF area to which the OSPF interface belongs, as an IPv4 address or an integer number.

5. If you want to specify OSPF authentication:

a. In the **Authentication** drop-down list, select an authentication method:

- **Message digest** to use the MD5 algorithm.
- **Simple password** to use an unencrypted password. This authentication method is less secure than MD5 algorithm, however, it can provide authentication when used in a trusted network environment. If you select this option, enter the authentication password in the **Password** field.

b. If in the **Authentication** drop-down list, you selected **Message digest**, follow these steps:

1. In the **Key ID** field, enter the MD5 hash. Range of values: 1 to 255.

2. In the **Key** field, enter the MD5 key.
6. In the **Cost** field, enter the metric of the OSPF interface. Range of values: 1 to 65,535.
7. In the **Network type** drop-down list, select the type of network to which the OSPF interface is connected:
 - **Broadcast**
 - **Non-broadcast**
 - **Point-to-multipoint**
 - **Point-to-point**
8. In the **Priority** field, enter the priority of the OSPF interface. The greater the value, the higher the priority of the OSPF interface.

The highest-priority OSPF interface becomes the designated router of the network segment. The OSPF interface with the second highest priority becomes the backup designated router.
9. If you want to switch the OSPF interface to passive mode, select the **Passive interface** check box. In passive mode, OSPF interfaces do not exchange traffic packets.
10. If you want to use the [BFD protocol](#) to detect loss of connectivity, select the **BFD** check box. This check box is cleared by default.
11. If you want to configure OSPF timers:
 - a. Select the **OSPF timers** check box. This check box is cleared by default.
 - b. In the **Hello (sec.)** field, enter the time interval in seconds that the OSPF interface uses to send control packets to OSPF peers. Range of values: 1 to 65,535.
 - c. In the **Dead (sec.)** field, enter the time interval in seconds that the OSPF interface uses to receive control packets from OSPF peers. If no control packets are received from an OSPF peer within the specified time, the OSPF interface considers the peer unavailable. Range of values: 1 to 65,535.
12. In the **Retransmit interval (sec.)** field, enter the time after which the OSPF resends lost traffic packets. Range of values: 1 to 65,535.
13. In the **Transmit delay (sec.)** field, enter the delay in seconds before the OSPF interface sends the first traffic packet. Range of values: 1 to 65,535.
14. Click **Create**.

The OSPF interface is created and displayed in the table.
15. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Editing an OSPF interface

You can edit an OSPF interface in a CPE template or on an individual device. When you edit an OSPF interface in a CPE template, the interface is automatically modified on all devices that are using the template.

To edit an OSPF interface:

1. Edit an OSPF interface in one of the following ways:

- If you want to edit an OSPF interface in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **OSPF** → **OSPF interface** tab.
- If you want to edit an OSPF interface on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **OSPF** → **OSPF interface** tab and select the **Override** check box.

A table of OSPF interfaces is displayed.

2. Click **Edit** next to the OSPF interface that you want to edit.

3. This opens a window, in that window, in the **Interface** drop-down list, select a previously [created network interface](#) which you want to use as an OSPF interface.

4. In the **OSPF area** field, enter the ID of the OSPF area to which the OSPF interface belongs, as an IPv4 address or an integer number.

5. If you want to specify OSPF authentication:

a. In the **Authentication** drop-down list, select an authentication method:

- **Message digest** to use the MD5 algorithm.
- **Simple password** to use an unencrypted password. This authentication method is less secure than MD5 algorithm, however, it can provide authentication when used in a trusted network environment. If you select this option, enter the authentication password in the **Password** field.

b. If in the **Authentication** drop-down list, you selected **Message digest**, follow these steps:

1. In the **Key ID** field, enter the MD5 hash. Range of values: 1 to 255.

2. In the **Key** field, enter the MD5 key.

6. In the **Cost** field, enter the metric of the OSPF interface. Range of values: 1 to 65,535.

7. In the **Network type** drop-down list, select the type of network to which the OSPF interface is connected:

- **Broadcast**
- **Non-broadcast**
- **Point-to-multipoint**
- **Point-to-point**

8. In the **Priority** field, enter the priority of the OSPF interface. The greater the value, the higher the priority of the OSPF interface.

The highest-priority OSPF interface becomes the designated router of the network segment. The OSPF interface with the second highest priority becomes the backup designated router.

9. If you want to switch the OSPF interface to passive mode, select the **Passive interface** check box. In passive mode, OSPF interfaces do not exchange traffic packets.

10. If you want to use the [BFD protocol](#) to detect loss of connectivity, select the **BFD** check box. This check box is cleared by default.
11. If you want to configure OSPF timers:
 - a. Select the **OSPF timers** check box. This check box is cleared by default.
 - b. In the **Hello (sec.)** field, enter the time interval in seconds that the OSPF interface uses to send control packets to OSPF peers. Range of values: 1 to 65,535.
 - c. In the **Dead (sec.)** field, enter the time interval in seconds that the OSPF interface uses to receive control packets from OSPF peers. If no control packets are received from an OSPF peer within the specified time, the OSPF interface considers the peer unavailable. Range of values: 1 to 65,535.
12. In the **Retransmit interval (sec.)** field, enter the time after which the OSPF resends lost traffic packets. Range of values: 1 to 65,535.
13. In the **Transmit delay (sec.)** field, enter the delay in seconds before the OSPF interface sends the first traffic packet. Range of values: 1 to 65,535.
14. Click **Save**.

The OSPF interface is modified and updated in the table.
15. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Deleting an OSPF interface

You can delete an OSPF interface in a CPE template or on an individual device. When you delete an OSPF interface in a CPE template, the interface is automatically deleted on all devices that are using the template.

Deleted interfaces cannot be restored.

To delete an OSPF interface:

1. Delete an OSPF interface in one of the following ways:
 - If you want to delete an OSPF interface in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **OSPF** → **OSPF interface** tab.
 - If you want to delete an OSPF interface on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **OSPF** → **OSPF interface** tab and select the **Override** check box.

A table of OSPF interfaces is displayed.

2. Click **Delete** next to the OSPF interface that you want to delete.
3. In the confirmation window, click **Delete**.

The OSPF interface is deleted and is no longer displayed in the table.
4. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Using BFD to detect routing failures

Kaspersky SD-WAN supports the Bidirectional Forwarding Detection (BFD) protocol for fast (within one second) detection of network connectivity problems on links and tunnels. When a problem is detected, BFD relays information about the problem from the [data plane](#) to the [control plane](#).

Between BFD peers, a BFD session is established, as part of which they exchange control packets to detect network connectivity problems. If problems with network connectivity occur, the BFD session on the [SD-WAN interface](#) of the CPE device is terminated, after which route tables are rebuilt.

The table of BFD peers is displayed in the CPE template and on the device:

- To display the table of BFD peers in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template, and in the displayed settings area, select the **BFD settings** tab.
- To display the table of BFD peers on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **BFD settings** tab.

Information about BFD peers is displayed in the following columns of the table:

- **Name** is the name of the BFD peer.
- **IP address** is the IPv4 address of the BFD peer.
- **Transmit interval (msec.)** is the interval in milliseconds for sending control packets from the CPE device to the BFD peer.
- **Receive interval (msec.)** is the interval in milliseconds for receiving control packets from the BFD peer on the CPE device. If no control packets are received from the BFD peer within the specified time, the CPE device considers the peer unavailable.
- **Multiplier** is the multiplier of the time interval for sending control packets specified in the BFD peer settings. This multiplier determines the number of milliseconds for which the CPE device must wait for receipt of control packets from the BFD peer. If no control packets are received from the BFD peer within this time, the device announces a network connectivity problem.
- **Management** contains the actions that can be performed with the BFD peer.

Enabling or disabling the BFD protocol

You can enable or disable the BFD protocol in the configuration of the CPE template or on a device. When you enable or disable the BFD protocol in a CPE template, the protocol enabled or disabled on all devices that are using that template.

To enable or disable the BFD protocol:

1. Enable or disable the BFD protocol in one of the following ways:
 - If you want to enable or disable the BFD protocol in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **BFD settings** tab.

- If you want to enable or disable the BFD protocol on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **BFD settings** tab and select the **Override** check box.

A table of BFD peers is displayed.

2. In the **BFD** drop-down list, select one of the following values:

- **Enabled**
- **Disabled** (default).

3. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Creating a BFD peer

You can create a BFD peer in a CPE template or on a device. When you create a BFD peer in a CPE template, the peer is automatically created on all devices that are using the template. Before creating a BFD peer, you must [enable the BFD protocol](#).

To create a BFD peer:

1. Create a BFD peer in one of the following ways:

- If you want to create a BFD peer in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **BFD settings** tab.
- If you want to create a BFD peer on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **BFD settings** tab and select the **Override** check box.

A table of BFD peers is displayed.

2. Click **+ BFD peer**.

3. This opens a window; in that window, in the **Name** field, enter the name of the BFD peer. Maximum length: 255 characters.

4. In the **IP address** field, enter the IPv4 address of the BFD peer.

5. In the **Transmit interval (msec.)** field, enter the time interval in milliseconds for sending control packets from the CPE device to the BFD peer. Range of values: 60 to 10,000.

6. In the **Receive interval (msec.)** field, enter the time interval in milliseconds for receiving control packets from the BFD peer on the CPE device. If no control packets are received from the BFD peer within the specified time, the CPE device considers the peer unavailable. Range of values: 60 to 10,000.

7. In the **Multiplier** enter the multiplier of the time interval for sending control packets specified in the BFD peer settings. This multiplier determines the number of milliseconds for which the CPE device must wait for receipt of control packets from the BFD peer. If no control packets are received from the BFD peer within this time, the device announces a network connectivity problem. Range of values: 2 to 255.

For example, if the time interval for sending control packets in the BFD peer settings is 200 milliseconds, and you specify a multiplier of 2, then if after 400 milliseconds, the CPE device does not receive a single control packet from that BFD peer, the CPE device announces a network connectivity problem.

8. Click **Create**.

The BFD peer is created and displayed in the table.

9. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Editing a BFD peer

You can edit a BFD peer in a CPE template or on a device. When you edit a BFD peer in a CPE template, the BFD peer is automatically modified on all devices that are using the template.

To edit a BFD peer:

1. Edit a BFD peer in one of the following ways:

- If you want to edit a BFD peer in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **BFD settings** tab.
- If you want to edit a BFD peer on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **BFD settings** tab and select the **Override** check box.

A table of BFD peers is displayed.

2. Click **Edit** next to the BFD peer that you want to edit.

3. This opens a window; in that window, in the **Name** field, enter the name of the BFD peer. Maximum length: 255 characters.

4. In the **IP address** field, enter the IPv4 address of the BFD peer.

5. In the **Transmit interval (msec.)** field, enter the time interval in milliseconds for sending control packets from the CPE device to the BFD peer. Range of values: 60 to 10,000.

6. In the **Receive interval (msec.)** field, enter the time interval in milliseconds for receiving control packets from the BFD peer on the CPE device. If no control packets are received from the BFD peer within the specified time, the CPE device considers the peer unavailable. Range of values: 60 to 10,000.

7. In the **Multiplier** enter the multiplier of the time interval for sending control packets specified in the BFD peer settings. This multiplier determines the number of milliseconds for which the CPE device must wait for receipt of control packets from the BFD peer. If no control packets are received from the BFD peer within this time, the device announces a network connectivity problem. Range of values: 2 to 255.

For example, if the time interval for sending control packets in the BFD peer settings is 200 milliseconds, and you specify a multiplier of 2, then if after 400 milliseconds, the CPE device does not receive a single control packet from that BFD peer, the CPE device announces a network connectivity problem.

8. Click **Save**.

The BFD peer is modified and updated in the table.

9. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Deleting a BFD peer

You can delete a BFD peer in a CPE template or on a device. When you delete a BFD peer in a CPE template, the BFD peer is automatically deleted on all devices that are using the template.

Deleted BFD peers cannot be restored.

To delete a BFD peer:

1. Delete a BFD peer in one of the following ways:

- If you want to delete a BFD peer in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **BFD settings** tab.
- If you want to delete a BFD peer on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **BFD settings** tab and select the **Override** check box.

A table of BFD peers is displayed.

2. Click **Delete** next to the BFD peer that you want to delete.

3. This opens a window; in that window, click **Delete**.

The BFD peer is deleted and is no longer displayed in the table.

4. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Ensuring high availability with VRRP

Kaspersky SD-WAN supports the Virtual Router Redundancy Protocol (VRRP) for combining [network interfaces](#) of multiple CPE devices into virtual routers. When network interfaces are combined into a virtual router, they share a virtual IP address. One network interface is primary and the others are secondary. A virtual IP address is assigned to the primary network interface.

Network interfaces in a virtual router exchange control packets to determine which network interfaces have failed. If a primary network interface fails, a new primary network interface is elected and the virtual IP address is assigned to that network interface. Traffic that was relayed to the virtual IP address through the failed network interface is automatically taken over by the new primary network interface.

You can create VRRP instances to combine network interfaces into virtual routers. When creating a VRRP instance, you must select a network interface and specify the Virtual Router ID (VRID) and virtual IP address. Network interfaces are combined into a virtual router if the same virtual router ID and virtual IP address are specified in the VRRP instances created for them.

If you need to synchronously change the primary network interface in multiple virtual routers, you can create groups of VRRP instances. If the primary network interface changes in one of the instances in the group, in all other instances in the group this change also occurs.

Enabling or disabling the VRRP protocol

You can enable or disable the VRRP protocol in the configuration of the CPE template or on a device. When you enable or disable the VRRP protocol in a CPE template, the protocol enabled or disabled on all devices that are using that template.

To enable or disable the VRRP protocol:

1. Enable or disable the VRRP protocol in one of the following ways:

- If you want to enable or disable the VRRP protocol in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template and in the displayed settings area, select the **VRRP → VRRP instances** tab.
- If you want to enable or disable the VRRP protocol on a CPE device, go to the **SD-WAN → CPE** menu section, click the device, and in the displayed settings area, select the **VRRP → VRRP instances** tab and select the **Override** check box.

A table of VRRP instances is displayed.

2. In the **VRRP** drop-down list, select one of the following values:

- **Enabled**
- **Disabled** (default).

When enabling VRRP, you must [create at least one VRRP instance](#).

3. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Managing VRRP instances

The table of VRRP instances is displayed in the CPE template and on the device:

- To display the table of VRRP instances in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template, and in the displayed settings area, select the **VRRP → VRRP instances** tab.
- To display the table of VRRP instances on a CPE device, go to the **SD-WAN → CPE** menu section, click the device, and in the displayed settings area, select the **VRRP → VRRP instances** tab.

Information about VRRP instances is displayed in the following table columns:

- **Name** is the name of the VRRP instance.
- **VRID** is the virtual router ID.
- **Interface** is the [network interface](#) added to the virtual router.
- **VIP** is the virtual IP address assigned to the network interface.
- **State** is the role of the network interface:
 - **Backup** is the backup network interface.
 - **Master** is the primary network interface.
- **Priority** is the priority of the network interface. The greater the value, the higher the priority. When the primary network interface fails, it is replaced by the backup network interface with the highest priority. If, when selecting the new primary network interface, all backup network interfaces have the same priority, the new primary network interface is selected at random.

- **Advertise interval (sec.)** is the interval in seconds for sending control packets from a network interface to other network interfaces.
- **Nopreempt** specifies whether the role of the network interface that became the primary network interface must be changed if the previous primary network interface recovers:
 - **Yes**
 - **No**
- **Management** contains the actions that can be performed with the VRRP instance.

Creating a VRRP instance

You can create a VRRP instance in a CPE template or on a device. When you create a VRRP instance in a CPE template, the instance is automatically created on all devices that are using the template.

To create a VRRP instance:

1. Create a VRRP instance in one of the following ways:

- If you want to create a VRRP instances in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **VRRP** → **VRRP instances** tab.
- If you want to create a VRRP instance on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **VRRP** → **VRRP instances** tab and select the **Override** check box.

A table of VRPP instances is displayed.

2. Click **+ VRRP instance**.

3. This opens a window; in that window, in the **Name** field, enter the name of the VRRP instance. Maximum length: 16 characters.

4. In the **VRID** field, enter the ID of the virtual router. You must specify the same ID when creating VRRP instances for all network interfaces that you want to combine into a virtual router. Range of values: 1 to 255.

5. In the **Interface** drop-down list, select a previously [created network interface](#) that you want to add to the virtual router.

6. In the **VIP** field, enter the virtual IP address that you want to assign to this network interface. You must assign the same virtual IP address to all network interfaces that you want to combine into a virtual router.

7. In the **State** drop-down list, select the role of the network interface:

- **Backup** is the backup network interface. Default value.
- **Master** is the primary network interface.

8. In the **Priority** field, enter the priority of the network interface. The greater the value, the higher the priority. When the primary network interface fails, it is replaced by the backup network interface with the highest priority. If, when selecting the new primary network interface, all backup network interfaces have the same

priority, the new primary network interface is selected at random. Range of values: 1 to 1000. The default setting is 100.

9. In the **Advertise interval (sec.)** field, enter the time interval in seconds for sending control packets from a network interface to other network interfaces. Range of values: 1 to 60. The default setting is 5.
10. If you do not want to change the role of the backup network interface that has become the primary router, even if the old primary network interface becomes operational again, select the **Nopreempt** check box. This check box is cleared by default.
11. If you want to configure unicast sending of control packets by the network interface:
 - a. Select the **Unicast** check box. This check box is cleared by default.
 - b. In the **Main VRRP router IP** field, enter the IP address of the network interface from which you want to send control packets.
 - c. In the **Backup VRRP router IP** field, enter the IP address of the network interface to which you want to send control packets.

By default, the network interface uses multicast to send control packets.

12. If you want to use a password for authentication of control packets on the network interface:
 - a. Select the **Authentication** check box. This check box is cleared by default.
 - b. Enter a password in the field that is displayed. Maximum length of the password: 16 characters. You must specify the same password for all network interfaces that you want to combine into a virtual router. To see the entered password, you can click the show icon .

13. Click **Create**.

The VRRP instance is created and displayed in the table.

14. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Editing a VRRP instance

You can edit a VRRP instance in a CPE template or on a device. When you edit a VRRP instance in a CPE template, the instance is automatically modified on all devices that are using the template. You cannot edit a VRRP instance that is inherited from a template on a CPE device.

To edit a VRRP instance:

1. Edit a VRRP instance in one of the following ways:
 - If you want to edit a VRRP instance in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **VRRP** → **VRRP instances** tab.
 - If you want to edit a VRRP instance on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **VRRP** → **VRRP instances** tab and in the upper part of the settings area, select the **Override** check box.

A table of VRRP instances is displayed.

2. Click **Edit** next to the VRRP instance that you want to edit.
 3. This opens a window; in that window, in the **Name** field, enter the name of the VRRP instance. Maximum length: 16 characters.
 4. In the **VRID** field, enter the ID of the virtual router. You must specify the same ID when creating VRRP instances for all network interfaces that you want to combine into a virtual router. Range of values: 1 to 255.
 5. In the **Interface** drop-down list, select a previously [created network interface](#) that you want to add to the virtual router.
 6. In the **VIP** field, enter the virtual IP address that you want to assign to this network interface. You must assign the same virtual IP address to all network interfaces that you want to combine into a virtual router.
 7. In the **State** drop-down list, select the role of the network interface:
 - **Backup** is the backup network interface. Default value.
 - **Master** is the primary network interface.
 8. In the **Priority** field, enter the priority of the network interface. The greater the value, the higher the priority. When the primary network interface fails, it is replaced by the backup network interface with the highest priority. If, when selecting the new primary network interface, all backup network interfaces have the same priority, the new primary network interface is selected at random. Range of values: 1 to 1000. The default setting is **100**.
 9. In the **Advertise interval (sec.)** field, enter the time interval in seconds for sending control packets from a network interface to other network interfaces. Range of values: 1 to 60. The default setting is 5.
 10. If you do not want to change the role of the backup network interface that has become the primary router, even if the old primary network interface becomes operational again, select the **Nopreempt** check box. This check box is cleared by default.
 11. If you want to configure unicast sending of control packets by the network interface:
 - a. Select the **Unicast** check box. This check box is cleared by default.
 - b. In the **Main VRPP router IP** field, enter the IP address of the network interface from which you want to send control packets.
 - c. In the **Backup VRRP router IP** field, enter the IP address of the network interface to which you want to send control packets.
- By default, the network interface uses multicast to send control packets.
12. If you want to use a password for authentication of control packets on the network interface:
 - a. Select the **Authentication** check box. This check box is cleared by default.
 - b. Enter a password in the field that is displayed. Maximum length of the password: 16 characters. You must specify the same password for all network interfaces that you want to combine into a virtual router. To see the entered password, you can click the show icon .
 13. Click **Save**.

The VRRP instance is modified and updated in the table.

14. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Deleting a VRRP instance

You can delete a VRRP instance in a CPE template or on a device. When you delete a VRRP instance in a CPE template, the instance is automatically deleted on all devices that are using the template. You cannot delete a VRRP instance that is inherited from a template on a CPE device.

Deleted VRRP instances cannot be restored.

To delete a VRRP instance:

1. Delete a VRRP instance in one of the following ways:

- If you want to delete a VRRP instance in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **VRRP** → **VRRP instances** tab.
- If you want to delete a VRRP instance on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **VRRP** → **VRRP instances** tab and select the **Override** check box.

A table of VRRP instances is displayed.

2. Click **Delete** next to the VRRP instance that you want to delete.

3. In the confirmation window, click **Delete**.

The VRRP instance is deleted and is no longer displayed in the table.

4. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Managing VRRP instance groups

The table of VRRP instance groups is displayed in the CPE template and on the device:

- To display the table of VRRP instance groups in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template, and in the displayed settings area, select the **VRRP** → **VRRP instance groups** tab.
- To display the table of VRRP instance groups on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **VRRP** → **VRRP instance groups** tab.

Information about VRRP instance groups is displayed in the following columns of the table:

- **Name** is the name of the VRRP instance group.
- **VRRP instances** are [VRRP instances](#) added to the group.
- **Management** contains the actions that can be performed with the VRRP instance group.

Creating a VRRP instance group

You can create a VRRP instance group in a CPE template or on a device. When you create a VRRP instance group in a CPE template, the group is automatically created on all devices that are using the template.

To create a VRRP instance group:

1. Create a VRRP instance group in one of the following ways:

- If you want to create a VRRP instance group in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **VRRP** → **VRRP instance groups** tab.
- If you want to create a VRRP instance group on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **VRRP** → **VRRP instance groups** tab and select the **Override** check box.

A table of VRRP instance groups is displayed.

2. Click **+ VRRP instance group**.

3. This opens a window; in that window, in the **Name** field, enter the name of the VRRP instance group. Maximum length: 16 characters. The default setting is **1**.

4. In the **VRRP instances** drop-down list, select previously [created VRRP instances](#) that you want to add to the group.

5. Click **Create**.

The VRRP instance group is created and displayed in the table.

6. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Editing a VRRP instance group

You can edit a VRRP instance group in a CPE template or on a device. When you edit a VRRP instance group in a CPE template, the group is automatically modified on all devices that are using the template. You cannot edit a VRRP instance group that is inherited from a template on a CPE device.

To edit a group of VRRP instances:

1. Edit a VRRP instance group in one of the following ways:

- If you want to edit a VRRP instance group in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **VRRP** → **VRRP instance groups** tab.
- If you want to edit a VRRP instance group on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **VRRP** → **VRRP instance groups** tab and select the **Override** check box.

A table of VRRP instance groups is displayed.

2. Click **Edit** next to the VRRP instance group that you want to edit.
3. This opens a window; in that window, in the **Name** field, enter the name of the VRRP instance group. Maximum length: 16 characters. The default setting is 1.
4. In the **VRRP instances** drop-down list, select previously [created VRRP instances](#) that you want to add to the group.
5. Click **Save**.
The VRRP instance group is modified and updated in the table.
6. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Deleting a VRRP instance group

You can delete a VRRP instance group in a CPE template or on a device. When you delete a VRRP instance group in a CPE template, the group is automatically deleted on all devices that are using the template. You cannot delete a VRRP instance group that is inherited from a template on a CPE device.

Deleted VRRP instance groups cannot be restored.

To delete a VRRP instance group:

1. Delete a VRRP instance group in one of the following ways:
 - If you want to delete a VRRP instance group in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template and in the displayed settings area, select the **VRRP → VRRP instance groups** tab.
 - If you want to delete a VRRP instance group on a CPE device, go to the **SD-WAN → CPE** menu section, click the device, and in the displayed settings area, select the **VRRP → VRRP instance groups** tab and select the **Override** check box.

A table of VRRP instance groups is displayed.

2. Click **Delete** next to the VRRP instance group that you want to delete.
3. In the confirmation window, click **Delete**.
The VRRP instance group is deleted and is no longer displayed in the table.
4. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Transmission of multicast traffic using PIM and IGMP protocols

Kaspersky SD-WAN supports transmission of multicast traffic between CPE devices and external network devices using the PIM and IGMP protocols. You can specify the basic settings of the PIM protocol on CPE devices, for example, the rendezvous points to be used, and then create multicast interfaces for interaction with other devices. Previously [created network interfaces](#) are used as multicast interfaces.

If PIM connectivity is established between CPE devices and rendezvous points are defined for these devices, multicast interfaces can receive requests from clients over IGMP. These requests contain IP addresses of sources from which clients want to receive multicast traffic packets. When sources send multicast packets to a rendezvous point, clients receive these packets.

If necessary, you can use the PIM protocol to connect CPE devices to external routers. To do so, you must enable the PIM protocol on the multicast interface to which the external router is connected.

Basic PIM settings

You can specify basic PIM settings in a CPE template or on the device. When you specify PIM settings in a CPE template, such settings are automatically propagated to all devices that are using the template.

To modify the basic PIM settings:

1. Specify basic PIM settings in one of the following ways:
 - If you want to edit the basic PIM settings in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **Multicast** → **General settings** tab.
 - If you want to edit the basic PIM settings on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device and in the displayed settings area, select the **Multicast** → **General settings** tab.

Basic PIM settings are displayed.

2. In the **Multicast** drop-down list, select **Enabled**. By default, the **Disabled** option is selected.
3. Specify the rendezvous point for multicast traffic packet sources and clients that are connected to the CPE device:
 - a. Under **RP IP**, click **+ Add**.
 - b. In the displayed field, enter the IPv4 address of the rendezvous point.
 - c. If you want to specify a multicast group associated with the rendezvous point, under **RP group**, enter the IPv4 prefix of your multicast group. Each rendezvous point can be associated with a dedicated multicast group.

The rendezvous point is specified and displayed in the **RP IP** and **RP group** sections. You can specify multiple rendezvous points; to delete a rendezvous point, click the delete icon next to it.

4. In the **RP keepalive timer (sec.)** field, enter the lifetime in seconds of traffic streams between the source and the multicast group (S,G). The countdown is reset if the CPE device receives a register packet. Range of values: 31 to 60,000. The default setting is 185.
5. If you want to filter multicast traffic packets with the specified source IPv4 addresses on the CPE device, in the **PIM register accept list** drop-down list, select a previously [created prefix list](#).
6. If a CPE device is on the last hop and you want to prevent this device from switching over from the shared tree to the shortest path tree (SPT) when transmitting multicast traffic packets:
 - a. Select the **SPT switchover** check box. This check box is cleared by default.

- b. If you want to deny or allow switchover from the Rendezvous Point Tree (RPT) to the shortest path tree when transmitting traffic packets from multicast groups with specified source IPv4 prefixes, select a previously created prefix list in the **SPT prefix list** drop-down list. Whether switchover is denied or allowed is determined as follows:
- If the prefix list allows the IPv4 prefix, switchover does not occur.
 - If the prefix list denies the IPv4 prefix, switchover does occur.
7. If you want to perform ECMP balancing on a CPE device to distribute multicast traffic streams over multiple routes:
- a. Select the **ECMP** check box. This check box is cleared by default. For ECMP balancing, multiple routes must exist. If ECMP balancing is disabled, traffic is transmitted along one route.
- b. If you want to redistribute the entirety of the traffic between the remaining routes in case one of the multicast interfaces fails, select the **ECMP rebalance** check box. By default, the check box is cleared, and if one of the multicast interfaces fails, only the traffic that was transmitted through that multicast interface is redistributed.
8. In the **PIM join/prune interval (sec.)** field, enter the interval in seconds for multicast interfaces to send join/prune packets to PIM peers. Range of values: 60 to 600. The default setting is 60.
9. In the **PIM keepalive timer (sec.)** field, enter the lifetime in seconds of traffic streams between the source and the multicast group (S,G). The countdown is reset if the CPE device receives a join/prune packet. Range of values: 31 to 60,000. The default setting is 210.
10. If you want to have the CPE device relay traffic packets with specified source IPv4 prefixes from multicast groups upon request from the client (Source Specific Multicast; SSM), in the **SSM prefix list** drop-down list, select a previously created prefix list.
11. In the **RPF lookup mode** drop-down list, select a Reverse Path Forwarding (RPF) lookup mode on the CPE device:
- longer-prefix
 - lower-distance
 - mrrib-only
 - mrrib-then-urib (default)
 - urib-only
12. If you want to add a static IPv4 route to the multicast routing table of the CPE device:
- a. Under **Static multicast route**, click **+ Add**.
- b. In the **IP destination** field, enter the destination IPv4 address of the static route.
- c. In the **Type** drop-down list, select the source type of the static route:
- **Address** is an IPv4 address. If you select this value, in the **Nexthop** field, enter the source IPv4 address and prefix of the static route.
 - **Interface** is a previously [created network interface](#). If you select this value, from the **Nexthop** drop-down list, select the source network interface of the static route.

d. If necessary, in the **Distance** field, enter the metric of the static route. Range of values: 1 to 255.

The static route is added and displayed under **Static multicast route**. You can add multiple static routes; to delete a static route, click the delete icon next to it.

13. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Managing multicast interfaces

The table of multicast interfaces is displayed in the CPE template and on the device:

- To display the table of multicast interfaces in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template, and in the displayed settings area, select the **Multicast** → **Interfaces** tab.
- To display the table of multicast interfaces on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Multicast** → **Interfaces** tab.

Information about multicast interfaces is displayed in the following columns of the table:

- **Network interface** is the [network interface](#) used as a multicast interface.
- **PIM** specifies whether the exchange of messages with peers via the PIM protocol is enabled on the multicast interface:
 - **Enabled**
 - **Disabled**
- **IGMP** specifies whether the exchange of messages with peers via the IGMP protocol is enabled on the multicast interface:
 - **Enabled**
 - **Disabled**
- **DR priority** is the priority of the multicast interface. The highest-priority multicast interface becomes the designated router of the LAN segment. The greater the value, the higher the priority of the multicast interface.
- **Inherited** specifies whether the multicast interface is inherited from the CPE template:
 - **Yes**
 - **No**

This column is displayed only on the CPE device.

- **Management** contains the actions that can be performed with the multicast interface.

Creating a multicast interface

You can create a multicast interface in a CPE template or on an individual device. When you create a multicast interface in a CPE template, the interface is automatically created on all devices that are using the template.

To create a multicast interface:

1. Create a multicast interface in one of the following ways:

- If you want to create a multicast interface in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **Multicast** → **Interfaces** tab.
- If you want to create a multicast interface on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Multicast** → **Interfaces** tab and select the **Override** check box.

A table of multicast interfaces is displayed.

2. Click **+ Multicast interface**.

3. This opens a window, in that window, in the **Network interface** drop-down list, select a previously [created network interface](#) which you want to use as a multicast interface.

4. Configure the PIM protocol on the multicast interface:

- a. In the **PIM** drop-down list, select **Enabled**. By default, the **Disabled** option is selected.
- b. If you want to switch the multicast interface to passive mode, select the **Passive** check box. In passive mode, multicast interfaces do not exchange control packets. This check box is cleared by default.
- c. If you want to prohibit the exchange of bootstrap packets on the multicast interface, clear the **BSM** check box. This check box is selected by default.
- d. If you want to prohibit the exchange of unicast bootstrap packets on the multicast interface, clear the **Unicast BSM** check box. This check box is selected by default.
- e. In the **DR priority** field, enter the priority of the multicast interface. The highest-priority multicast interface becomes the designated router of the LAN segment. The greater the value, the higher the priority of the multicast interface. Range of values: 1 to 4,294,967,295. The default setting is **1**.
- f. In the **Hello (sec.)** field, enter the time interval in seconds that the multicast interface uses to send control packets to PIM peers. Range of values: 1 to 180. The default setting is **30**.
- g. In the **Hold (sec.)** field, enter the time interval in seconds that the multicast interface uses to receive control packets from PIM peers. If no control packets are received from a peer within the specified time, the multicast interface considers the peer unavailable. Range of values: 1 to 630. The default setting is **105**.
- h. If multiple IP addresses are assigned to a multicast interface and you want to use the specified IPv4 source address when sending PIM messages, enter the IPv4 address in the **Source IP** field.

5. Configure the IGMP protocol on the multicast interface:

- a. In the **IGMP** drop-down list, select **Enabled**. By default, the **Disabled** option is selected.
- b. In the **Version** drop-down list, select the version of the IGMP protocol on the multicast interface:
 - **2**
 - **3** (default)

- c. In the **Query interval (sec.)** field, enter the time interval in seconds for sending queries from the multicast interface to clients. Queries are used to determine if multicast traffic needs to be sent to clients. Range of values: 1 to 250. The default setting is 125.
- d. In the **Query response time (sec.)** field, enter the time in seconds that the multicast interface must wait to receive responses from clients. If no response to a query is received from the client within the specified time, the multicast interface does not send traffic packets. Range of values: 1 to 125. The default setting is 10.
- e. If you want to specify multicast groups:

1. Under **Join group**, click **+ Add**.
2. In the displayed field, enter the IPv4 address of the multicast group.
3. If you want to connect the multicast interface to the specified source of the multicast group, under **Source address**, enter the IPv4 address of the source.

The multicast group is specified and displayed in the **Join group** and **Source address** sections. You can specify multiple multicast groups; to delete a group, click the delete icon next to it.

You need to specify multicast groups in one of the following cases:

- The network segment has permanent clients to which you need to send traffic packets from a multicast group in a quick and stable way.
- The network segment does not contain clients or hosts in the segment cannot send report messages, but traffic packets from a multicast group must be sent to this segment.

6. Click **Save**.

The multicast interface is created and displayed in the table.

7. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Editing a multicast interface

You can edit multicast interface settings in a CPE template or on an individual device. When you edit a multicast interface in a CPE template, the interface is automatically modified on all devices that are using the template.

To edit a multicast interface:

1. Edit a multicast interface in one of the following ways:
 - If you want to edit a multicast interface in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **Multicast** → **Interfaces** tab.
 - If you want to edit a multicast interface on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Multicast** → **Interfaces** tab and select the **Override** check box.

A table of multicast interfaces is displayed.

2. Click **Edit** next to the multicast interface that you want to edit.

3. This opens a window, in that window, in the **Network interface** drop-down list, select a previously [created network interface](#) which you want to use as a multicast interface.
4. Configure the PIM protocol on the multicast interface:
 - a. In the **PIM** drop-down list, select **Enabled**. By default, the **Disabled** option is selected.
 - b. If you want to switch the multicast interface to passive mode, select the **Passive** check box. In passive mode, multicast interfaces do not exchange control packets. This check box is cleared by default.
 - c. If you want to prohibit the exchange of bootstrap packets on the multicast interface, clear the **BSM** check box. This check box is selected by default.
 - d. If you want to prohibit the exchange of unicast bootstrap packets on the multicast interface, clear the **Unicast BSM** check box. This check box is selected by default.
 - e. In the **DR priority** field, enter the priority of the multicast interface. The highest-priority multicast interface becomes the designated router of the LAN segment. The greater the value, the higher the priority of the multicast interface. Range of values: 1 to 4,294,967,295. The default setting is 1.
 - f. In the **Hello (sec.)** field, enter the time interval in seconds that the multicast interface uses to send control packets to PIM peers. Range of values: 1 to 180. The default setting is 30.
 - g. In the **Hold (sec.)** field, enter the time interval in seconds that the multicast interface uses to receive control packets from PIM peers. If no control packets are received from a peer within the specified time, the multicast interface considers the peer unavailable. Range of values: 1 to 630. The default setting is 105.
 - h. If multiple IP addresses are assigned to a multicast interface and you want to use the specified IPv4 source address when sending PIM messages, enter the IPv4 address in the **Source IP** field.
5. Configure the IGMP protocol on the multicast interface:
 - a. In the **IGMP** drop-down list, select **Enabled**. By default, the **Disabled** option is selected.
 - b. In the **Version** drop-down list, select the version of the IGMP protocol on the multicast interface:
 - 2
 - 3 (default)
 - c. In the **Query interval (sec.)** field, enter the time interval in seconds for sending queries from the multicast interface to clients. Queries are used to determine if multicast traffic needs to be sent to clients. Range of values: 1 to 250. The default setting is 125.
 - d. In the **Query response time (sec.)** field, enter the time in seconds that the multicast interface must wait to receive responses from clients. If no response to a query is received from the client within the specified time, the multicast interface does not send traffic packets. Range of values: 1 to 125. The default setting is 10.
 - e. If you want to specify multicast groups:
 1. Under **Join group**, click **+ Add**.
 2. In the displayed field, enter the IPv4 address of the multicast group.
 3. If you want to connect the multicast interface to the specified source of the multicast group, under **Source address**, enter the IPv4 address of the source.

The multicast group is specified and displayed in the **Join group** and **Source address** sections. You can specify multiple multicast groups; to delete a group, click the delete icon next to it.

You need to specify multicast groups in one of the following cases:

- The network segment has permanent clients to which you need to send traffic packets from a multicast group in a quick and stable way.
- The network segment does not contain clients or hosts in the segment cannot send report messages, but traffic packets from a multicast group must be sent to this segment.

6. Click **Save**.

The multicast interface is modified and updated in the table.

7. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Deleting a multicast interface

You can delete a multicast interface in a CPE template or on an individual device. When you delete a multicast interface in a CPE template, the interface is automatically deleted on all devices that are using the template.

Deleted multicast interfaces cannot be restored.

To delete a multicast interface:

1. Delete a multicast interface in one of the following ways:

- If you want to delete a multicast interface in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **Multicast** → **Interfaces** tab.
- If you want to delete a multicast interface on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Multicast** → **Interfaces** tab and select the **Override** check box.

A table of multicast interfaces is displayed.

2. Click **Delete** next to the multicast interface that you want to delete.

3. In the confirmation window, click **Delete**.

The multicast interface is deleted and is no longer displayed in the table.

4. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Managing virtual routing and forwarding (VRF) tables

Kaspersky SD-WAN supports the Virtual Routing and Forwarding (VRF) technology for creating up to 200 virtual routing and forwarding tables on CPE devices.

When creating a virtual routing and forwarding table, you must select [network interfaces](#) that you want to add to it. Network interfaces for connecting the CPE device to the controller and orchestrator are automatically added to the default virtual routing and forwarding table and you cannot add them to other tables. You cannot add the same network interface to multiple virtual routing and forwarding tables.


If two network interfaces are in different virtual routing and forwarding tables, the networks connected to them do not have access to each other. In this situation, network interfaces can have IP addresses from identical or overlapping subnets.

You can place [BGP routes](#) and static routes in virtual routing and forwarding tables. To place BGP routes into a virtual routing and forwarding table, specify that table when [editing basic BGP settings](#). To place a static route in a virtual routing and forwarding table, specify that table when [creating or editing the static route](#).

You can use virtual routing and forwarding tables in the following scenarios:


- [Network segmentation using virtual routing and forwarding tables](#) 

You can create virtual routing and forwarding tables to segment your network. In the figure below, Network 1 is built between the 'overlay1' network interface and user PCs, and Network 2 is built between the 'overlay2' network interface and ATMs. Both network interfaces are in the default virtual routing and forwarding table (Default VRF), so the networks have access to each other and are insecure.

 The 'overlay1' and 'overlay2' network interfaces are in the same virtual routing and forwarding table. The 'overlay1' network interface is connected to user PCs, and 'overlay2' is connected to ATMs. The networks have access to each other.

Network interfaces connected to different networks in the virtual default routing and forwarding table

To isolate Network 1 and Network 2, the overlay1 and overlay2 network interfaces must be added to separate virtual routing and forwarding tables, which creates two segments (see the figure below).


 The 'overlay1' and 'overlay2' network interfaces are in separate virtual routing and forwarding tables. The 'overlay1' network interface is connected to user PCs, and 'overlay2' is connected to ATMs.

Network interfaces connected to different networks are in separate virtual default routing and forwarding tables

- [Sending the 0.0.0.0/0 over BGP](#) 


You can create a separate virtual routing and forwarding table for sending the 0.0.0.0/0 route between devices over BGP. The figure below shows a CPE device with the gateway (GW) role and a standard device. All CPE devices in the network are added to the default virtual routing and forwarding table.

If a gateway sends the 0.0.0.0/0 BGP route from overlay network interface 10.10.10.254/24 to overlay network interface 10.10.10.1/24, such a route cannot be used. This is the case because the default virtual routing and forwarding table already has 0.0.0.0/0 routes with a lower administrative distance for connecting to the controller and orchestrator.

 The network interface of a CPE device with the gateway role is connected to the network interface of a standard device. In this case, all network interfaces of the standard device are added to the default virtual routing and forwarding table.

Sending the 0.0.0.0/0 route to a CPE device with the default virtual routing and forwarding table

To send route 0.0.0.0/0 over BGP through the overlay 10.10.10.254/24 network interface to overlay 10.10.10.1/24, you must create a separate table for the overlay 10.10.10.1/24 network interface and place BGP routes in it (see the figure below).

 The network interface of a CPE device with the gateway role is connected to the network interface of a standard device. At the same time, the BGP route exchange network interface of the standard CPE device is added to a separate virtual routing and forwarding table.

Sending the 0.0.0.0/0 route to a CPE device with a separate virtual routing and forwarding table for BGP routes

The table of virtual routing and forwarding tables is displayed in the CPE template and on the device:

- To display the table of virtual routing and forwarding tables in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template, and in the displayed settings area, select the **VRF** tab.
- To display the table of virtual routing and forwarding tables on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **VRF** tab.

Information about virtual routing and forwarding tables is displayed in the following columns of the table:

- **Name** is the name of the virtual routing and forwarding table.
- **Table** is the ID of the virtual routing and forwarding table.
- **Interfaces** are network interfaces added to the virtual routing and forwarding table.

Creating a virtual routing and forwarding table

You can create a virtual routing and forwarding table in a CPE template or on a device. When you create a virtual routing and forwarding table in a CPE template, the table is automatically created on all devices that are using the template.

To create a virtual routing and forwarding table:

1. Create a virtual routing and forwarding table in one of the following ways:
 - If you want to create a virtual routing and forwarding table in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **VRF** tab.

- If you want to create a virtual routing and forwarding table on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device and in the displayed settings area, select the **VRF** tab.

The table of virtual routing and forwarding tables is displayed.

2. Click **+ VRF**.

3. This opens a window; in that window, in the **Name** field, enter the name of the virtual routing and forwarding table.

4. In the **Table** field, enter the ID of the virtual routing and forwarding table. Range of values: 100 to 199.

5. In the **Interfaces** drop-down list, select previously [created network interfaces](#) that you want to add to the virtual routing and forwarding table. You cannot add the same network interface to multiple virtual routing and forwarding tables.

If you are adding a network interface with a name in the 'overlay.<number>' format (for example, 'overlay.100') to the virtual routing and forwarding table, you must select the **Enable automatically** and **Force IP, route, and gateway** check boxes when creating or [editing the network interface](#).

6. Click **Create**.

The virtual routing and forwarding table is created and displayed in the table.

7. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Modifying the virtual routing and forwarding table

You can edit a virtual routing and forwarding table in a CPE template or on a device. When you edit a virtual routing and forwarding table in a CPE template, the table is automatically modified on all devices that are using the template. You cannot edit a virtual routing and forwarding table that is inherited from a template on a CPE device.

To edit a virtual routing and forwarding table:

1. Edit a virtual routing and forwarding table in one of the following ways:

- If you want to edit a virtual routing and forwarding table in a CPE template, go to the **SD-WAN** → **CPE templates** menu section, click the template and in the displayed settings area, select the **VRF** tab.
- If you want to edit a virtual routing and forwarding table on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device and in the displayed settings area, select the **VRF** tab.

The table of virtual routing and forwarding tables is displayed.

2. Click **Edit** next to the virtual routing and forwarding table that you want to edit.

3. This opens a window; in that window, in the **Name** field, enter the name of the virtual routing and forwarding table.

4. In the **Table** field, enter the ID of the virtual routing and forwarding table. Range of values: 100 to 199.

5. In the **Interfaces** drop-down list, select previously [created network interfaces](#) that you want to add to the virtual routing and forwarding table. You cannot add the same network interface to multiple virtual routing and forwarding tables.

If you are adding a network interface with a name in the 'overlay.<number>' format (for example, 'overlay.100') to the virtual routing and forwarding table, you must select the **Enable automatically** and **Force IP, route, and gateway** check boxes when creating or [editing the network interface](#).

6. Click **Save**.

The virtual routing and forwarding table is modified and updated in the table.

7. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Deleting a virtual routing and forwarding table

You can delete a virtual routing and forwarding table in a CPE template or on a device. When you delete a virtual routing and forwarding table in a CPE template, the table is automatically deleted on all devices that are using the template. You cannot delete a virtual routing and forwarding table that is inherited from a template on a CPE device.

Deleted virtual routing and forwarding tables cannot be restored.

To delete a virtual routing and forwarding table:

1. Delete a virtual routing and forwarding table in one of the following ways:

- If you want to delete a virtual routing and forwarding table in a CPE template, go to the **SD-WAN → CPE templates** menu section, click the template and in the displayed settings area, select the **VRF** tab.
- If you want to delete a virtual routing and forwarding table on a CPE device, go to the **SD-WAN → CPE** menu section, click the device and in the displayed settings area, select the **VRF** tab.

The table of virtual routing and forwarding tables is displayed.

2. Click **Delete** next to the virtual routing and forwarding table that you want to delete.

3. In the confirmation window, click **Delete**.

The virtual routing and forwarding table is deleted and is no longer displayed in the table.

4. In the upper part of the settings area, click **Save** to save the settings of the CPE template or device.

Monitoring traffic packet information using the NetFlow protocol

Kaspersky SD-WAN supports NetFlow versions 1, 5, and 9 for monitoring information about traffic packets on a CPE device.

To avoid configuring each CPE device individually, you can specify basic NetFlow settings in a NetFlow template and then apply the template to devices when [adding](#) or [manually registering](#) them. If you edit a setting in a NetFlow template, that setting is automatically modified on all CPE devices that are using the template. When you edit a NetFlow setting on a CPE device, that setting becomes independent of the NetFlow template. When the same setting is edited in the NetFlow template, the change is not propagated to the CPE device.

When configuring basic NetFlow settings, you can specify up to four NetFlow collectors. If you want a CPE device to send information about traffic packets to NetFlow collectors, you must enable the NetFlow protocol on network interfaces. The NetFlow protocol can be enabled on a network interface when [creating](#) or [editing the network interface](#).

Managing NetFlow templates

To display the table of NetFlow templates, go to the **SD-WAN** → **NetFlow templates** section. One of the templates is the *default template*, which means it is pre-selected when [adding](#) and [manually registering a CPE device](#). By default, the **Default NetFlow template** is created on the administrator portal, which forms the basis for all other NetFlow templates you create. For [tenants](#), you must manually create and assign the default NetFlow template in the self-service portal.

Information about NetFlow templates is displayed in the following columns of the table:

- **ID** is the ID of the NetFlow template.
- **Name** is the name of the NetFlow template.
- **Usage** shows whether the NetFlow template is used by [CPE devices](#).
 - **Yes**
 - **No**
- **Updated** is the date and time when the CPE template settings were last modified.
- **User** is the name of the [user](#) which created the NetFlow template.
- **Owner** is the tenant to which the NetFlow template belongs.

The actions you can perform with the table are described in the [Managing solution component tables](#) instructions.

Creating a NetFlow template

To create a NetFlow template:

1. In the menu, go to the **SD-WAN** → **NetFlow templates** section.
A table of NetFlow templates is displayed.
2. In the upper part of the page, click **+ NetFlow template**.
3. This opens a window; in that window, enter the name of the NetFlow template.
4. Click **Create**.

The NetFlow template is created and displayed in the table.

Setting a default NetFlow template

You can set a NetFlow template as the default to have it preselected when [adding](#) or [manually registering a CPE device](#).

To set a default NetFlow template:

1. In the menu, go to the **SD-WAN** → **NetFlow templates** section.

A table of NetFlow templates is displayed.

2. Click the NetFlow template that you want to make the default template.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

3. In the upper part of the settings area, under **Actions**, click **Set as default template**.

The NetFlow template is set as the default template.

Exporting a NetFlow template

You can export a NetFlow template to subsequently [import it into another template](#).

To export a NetFlow template:

1. In the menu, go to the **SD-WAN** → **NetFlow templates** section.

A table of NetFlow templates is displayed.

2. Click the NetFlow template that you want to export.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

3. In the upper part of the settings area, under **Actions**, click **Export**.

An archive in the TAR.GZ format is saved on your local device. The archive does not contain information about CPE devices using the NetFlow template.

Importing a NetFlow template

You can import a previously [exported template](#) into a NetFlow template. NetFlow template settings are specified in accordance with the settings of the imported template. During import, you can select the settings that you want to leave unchanged.

A NetFlow template into which another template is imported remains applied to CPE devices, but the settings of those devices are not modified.

To import a NetFlow template:

1. In the menu, go to the **SD-WAN** → **NetFlow templates** section.

A table of NetFlow templates is displayed.

2. Click the NetFlow template into which you want to import another template.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

3. In the upper part of the settings area, under **Actions**, click **Import**.
4. This opens a window; in that window, clear the check boxes next to the NetFlow template settings that you want to leave unchanged after import.
5. In the **File** field, specify the path to the TAR.GZ archive.
6. Click **Import**.

NetFlow template settings are modified in accordance with the settings of the imported template.

Cloning a NetFlow template

You can clone a NetFlow template to create an identical template with a different name.

To clone a NetFlow template:

1. In the menu, go to the **SD-WAN** → **NetFlow templates** section.
A table of NetFlow templates is displayed.
2. Click the NetFlow template that you want to clone.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .
3. In the upper part of the settings area, under **Actions**, click **Clone**.
4. This opens a window; in that window, enter the name of the new NetFlow template.
5. Click **Clone**.

A copy of the NetFlow template with the new name is created and displayed in the table.

Viewing the usage of a NetFlow template

You can see which [CPE devices](#) are using the NetFlow template. If a NetFlow template is being used by at least one CPE device, such a template cannot be [deleted](#).

To view NetFlow template usage:

1. In the menu, go to the **SD-WAN** → **NetFlow templates** section.
A table of NetFlow templates is displayed.
2. Click the NetFlow template for which you want to view usage information.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .
3. In the upper part of the settings area, under **Actions**, click **Show usage**.

This opens a window with a table of CPE devices that are using the NetFlow template.

Deleting a NetFlow template

You cannot delete a NetFlow template if it is being used by at least one [CPE device](#). You need to [look up the usage of the NetFlow template](#) and make sure that it is not being used by any CPE device.

Deleted NetFlow templates cannot be restored.

To delete a NetFlow template:

1. In the menu, go to the **SD-WAN** → **NetFlow templates** section.

A table of NetFlow templates is displayed.

2. Click the NetFlow template that you want to delete.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

3. In the upper part of the settings area, under **Actions**, click **Delete**.

4. In the confirmation window, click **Delete**.

The NetFlow template is deleted and is no longer displayed in the table.

Basic NetFlow settings

You can specify basic NetFlow settings in a NetFlow template or on a CPE device. When you configure basic NetFlow settings in a NetFlow template, these settings are automatically propagated to all CPE devices that are using the template.

To modify the basic NetFlow settings:

1. Specify basic NetFlow settings in one of the following ways:

- If you want to edit basic NetFlow settings in a NetFlow template, go to the **SD-WAN** → **NetFlow templates** menu section and click the template.
- If you want to edit the basic NetFlow settings on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **NetFlow** tab and select the **Override** check box.

Basic NetFlow settings are displayed.

2. In the **NetFlow** drop-down list, select **Enabled**. By default, the **Disabled** option is selected.

3. Specify a NetFlow collector:

- a. Under **Collectors**, click **+ Add**.

- b. Under **Host**, enter the IPv4 address of the NetFlow collector.

- c. Under **Port**, enter the port number of the NetFlow collector. Range of values: 1 to 65,535.

The NetFlow collector is specified and displayed in the **Collectors** section. You can specify multiple NetFlow collectors; to delete a collector, click the delete icon next to it. For an individual CPE device, you can specify a maximum of four NetFlow collectors.

4. In the **Export version** drop-down list, select the version of the NetFlow protocol:

- 1
- 5
- 9 (default)

5. In the **Tracking level** drop-down list, select which traffic packet information you want the CPE device to track:

- **ETHER** to track the following information:
 - Source and destination IP addresses and ports
 - Source and destination MAC addresses
 - Outer VLAN tag
 - Protocol being used
- **FULL** to track the source and destination IP addresses and ports, as well as the protocol being used. Default value.
- **VLAN** to track the following information:
 - Source and destination IP addresses and ports
 - Outer VLAN tag
 - Protocol being used
- **PROTO** to track the source and destination IP addresses and the protocol being used.
- **IP** to track the source and destination IP addresses.

6. In the **Maximum flows** field, enter the maximum number of traffic flows that the CPE device can simultaneously track. Range of values: 1 to 65,535. The default setting is 8192.

The higher the value, the higher the CPU load on the CPE device.

7. In the **Sampling rate** field, specify how frequently you want the CPE device to track the traffic packet information. For example, if you enter 10, the CPE device tracks information about every tenth packet of traffic. Range of values: 1 to 8192. The default setting is 1024.

The lower the value, the more accurate the information and the higher the CPU load on the CPE device.

8. In the **Timeout maximum life (sec.)** field, enter the maximum time in seconds for which the CPE device can track traffic flow information. To disable this feature, enter 0. Range of values: 1 to 9999. The default setting is 60.

9. In the **Hop limit** field, enter the maximum number of hops to NetFlow collectors. Range of values: 1 to 255. The default setting is 64.
10. If you want the CPE device to track IPv6 traffic, in the **Track IPv6** drop-down list, select **Enabled**. By default, the **Disabled** option is selected.
11. In the upper part of the settings area, click **Save** to save the settings of the NetFlow template or CPE device.

If you want a CPE device to send information about traffic packets to NetFlow collectors, you must enable the NetFlow protocol on network interfaces. The NetFlow protocol can be enabled on a network interface when [creating](#) or [editing the network interface](#).

Changing the NetFlow template of a CPE Device

To change the NetFlow template of a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.
A table of CPE devices is displayed.
2. Click the CPE device for which you want to change the NetFlow template.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.
3. In the **NetFlow template** drop-down list, select a previously [created NetFlow template](#).
4. In the upper part of the settings area, click **Save** to save CPE device settings.

Diagnosing a CPE device

You can request diagnostic information and statistics, such as BGP, OSPF, and PIM protocol usage, from a CPE device. The diagnostic information returned in response to the request is displayed in the web interface of the orchestrator and, if necessary, can be downloaded as a TXT file.

Kaspersky SD-WAN also supports the following utilities for CPE device diagnostics:

- *Ping* is a utility for testing the connection between a CPE device and a specified IPv4 address. A report with the output of the utility is displayed in the orchestrator web interface.
- *Traceroute* is a utility for determining the route between a CPE device and a specified IPv4 address. A report with the output of the utility is displayed in the orchestrator web interface.
- *Tcpdump* is a utility for capturing traffic on a CPE device and writing this traffic to a report file. Capturing means a copy is made of the traffic, and the original traffic is relayed to its destination. The file with the captured traffic can be downloaded or deleted.
- *Iperf* is a utility for diagnosing network performance and writing the results to a report file. You can use the CPE device as an iperf server or as an iperf client. You can download or delete the network performance diagnostics file.
- *Sweep* is a utility for performing the following actions on a CPE device:

- Clearing the ARP cache
- Restarting the FRR (Free Range Routing) process
- Clearing the NAT session table

Running an utility is a task that the CPE device receives from the orchestrator; the task obeys the time period configured for [the CPE device for sending REST API requests to the orchestrator](#). If you want the utilities to run sooner, you can enable interactive mode on the CPE device.

In *interactive mode*, the CPE device uses a shorter interval for sending REST API requests to the orchestrator. Interactive mode ends automatically when the specified duration has passed. You can specify the following interactive mode settings when [configuring the connection of a CPE device to the orchestrator and controller](#):

- The period to wait until the CPE device sends another REST API request to the orchestrator in interactive mode
- The time after which the interactive mode is automatically disabled

Requesting diagnostic information

To request diagnostic information:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device on which you want to request diagnostic information.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. Select the **Diagnostic information** tab.

The diagnostic information request parameters are displayed.

4. Click **Request diagnostic information**.

5. In the **Name** drop-down list, select the type of diagnostic information you want to display:

- **disk usage** for information about the disk usage of the CPE device. Default value.
- **dump-flows** for information about OpenFlow flows.
- **dump-groups** for information about OpenFlow groups.
- **ip addresses** for information about IP addresses assigned to physical ports or virtual interfaces of the operating system of the CPE device.
- **vrf data** for information about [virtual routing and forwarding tables](#).
- **ip neighbors** for information about the IP neighbors of the CPE device, obtained from the ARP table or using the Neighbor Discovery Protocol.

- **ip routes** for information about IPv4 and IPv6 routes.
- **ip rules** for information about routing rules.
- **iptables** for information about iptables.
- **cpe log** for the [local log](#) of the CPE device.
- **ovs-ofctl show** for information about the virtual switch.
- **ovs-vsctl show** for information about the connection between the virtual switch and controllers.
- **ovs-vsctl list controller** for information about controllers specified for the virtual switch.
- **show ip ospf** for Information about the [OSPF routing](#) process.
- **show ip ospf interface** for information about [OSPF interfaces](#).
- **show ip ospf neighbor** - information about OSPF neighbors.
- **show ip ospf database** for the OSPF database.
- **bgp show ip route** for information about [BGP routes](#).
- **show ip bgp** for information about the BGP routing process.
- **show ip bgp summary** for brief information about the BGP routing process.
- **top process** for information about Linux processes.
- **uptime** for information about the CPE device uptime.
- **time sync** for information about time synchronization on the CPE device using an [NTP server](#).
- **netstat** for information about network connections that the CPE device has established.
- **sdwan intarfaces** for information about [SD-WAN interfaces](#).
- **modems** for information about [modems](#).
- **show bfd peers** for information about [BFD peers](#).
- **netflow dump-flows** for information about [NetFlow flows](#).
- **netflow statistics** for information about the use of the NetFlow protocol.
- **show bfd peers brief** for brief information about BFD peers.
- **show ip pim bsr** for information about the current bootstrap router (BSR).
- **show ip pim bsrp-info** for information about the group-to-rp mapping received from the bootstrap router.
- **show ip pim interface** for information about PIM interfaces. You can configure the PIM protocol when [creating](#) or [editing a mutlicast interface](#).
- **show ip pim interface traffic** for information about PIM traffic.

- **show ip pim join** for information about multicast groups to which the CPE device is connected.
- **show ip pim neighbor** for information about PIM neighbors.
- **show ip pim nexthop** for information about the next hops of multicast groups.
- **show ip pim rp-info** for information about rendezvous points. You can specify rendezvous points when [specifying basic PIM settings](#).
- **show ip pim secondary** for information about the backup PIM router.
- **show ip pim state** for information about the state of the PIM protocol.
- **show ip pim statistics** for Information about PIM protocol usage.
- **show ip pim upstream** for information about PIM sources.
- **show ip igmp groups** for information about IGMP groups.
- **show ip igmp interface** for information about IGMP interfaces. You can configure IGMP when [creating](#) or [editing a mutlicast interface](#).
- **show ip igmp interface detail** for detailed information about IGMP interfaces.
- **show ip igmp sources** for information about IGMP sources.
- **igmp statistics** for information about IGMP usage.
- **show ip multicast** for information about the multicast routing process.
- **show ip mroute** for information about multicast routes.
- **show ip mroute summary** for brief information about multicast routes.
- **vswitchd log** for the log of the ovs-vswitchd process.
- **firewall config** for information about the [firewall](#).
- **sw version** for the [firmware](#) version of the CPE device.
- **vrrp stats** for brief information about [VRRP](#) usage.
- **vrrp data** for information about VRRP usage.

6. If you want to filter the displayed diagnostic information:

a. In the **Find line by pattern** field, enter words that must be found in the lines of diagnostic information that you want to be displayed. Maximum length: 64 characters. If you want to display only lines that do not contain the words you entered, select the **Select non-matching lines** check box. This check box is cleared by default.

b. In the **Print N lines before and after** field, enter the number of blank lines you want to display before and after each line of diagnostic information.

7. If you want to download the file with diagnostic information, click **Download file with latest data**.

An TXT file is saved on your local device.

Enabling interactive mode

You can specify the following interactive mode settings when [configuring the connection of a CPE device to the orchestrator and controller](#):

- The period to wait until the CPE device sends another REST API request to the orchestrator in interactive mode
- The time after which the interactive mode is automatically disabled

To enable interactive mode:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device on which you want to enable interactive mode.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. In the upper part of the settings area, click **Enable interactive**.

Interactive mode is enabled on the CPE device.

Running the ping utility

To run the ping utility:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device on which you want to run the ping utility.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. Select the **Utilities** tab.

By default, the **Ping** tab is selected, which displays the ping utility settings.

4. In the **Destination IP address** field, enter the IPv4 address to which you want the CPE device to send ICMP requests.

5. If you want the CPE device to send ICMP requests from a specific previously [created network interface](#), in the **Source interface** drop-down list, select a network interface.

6. In the **Count** field, enter the number of ICMP requests that you want the CPE device to send. Range of values: 1 to 1,000,000. The default setting is 5.

7. In the **Timeout (sec.)** field, enter the time in seconds after which the CPE device must receive an ICMP response to consider the request a success. Range of values: 1 to 3600. The default setting is 2.
8. In the **Size** field, enter the size of the ICMP request in bytes. Range of values: 1 to 65,535. The default setting is 56.
9. In the **TTL** field, enter the maximum number of hops for ICMP requests. Range of values: 1 to 255. The default setting is 255.
10. In the **Interval** field, enter the interval in seconds for the CPE device to use when sending ICMP requests to the specified IPv4 address. Range of values: 1 to 300. The default setting is 1.
11. Click **Run**.

The ping utility is run on the CPE device, and a report containing the output of the ping utility is displayed in the lower part of the settings area.

Running the traceroute utility

To run the traceroute utility:

1. In the menu, go to the **SD-WAN** → **CPE** section.
A table of CPE devices is displayed.
2. Click the CPE device on which you want to run the traceroute utility.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.
3. Select the **Utilities** → **Traceroute** tab.
The traceroute utility settings are displayed.
4. In the **Destination IP address** field, enter the IPv4 address to which you want the CPE device to send a series of ICMP requests.
5. If you want the CPE device to send the series of ICMP requests from a specific previously [created network interface](#), in the **Source interface** drop-down list, select a network interface.
6. If you want the CPE device to use the DNS server to resolve IP addresses to domain names when creating the report with the utility output, select the **Resolve DNS names** check box. You can specify a DNS server when creating or [editing a network interface](#). IP addresses that cannot be resolved to domain names are also displayed in the report. This check box is cleared by default.
7. In the **Probes timeout (sec.)** field, enter the time in seconds after which the CPE device must receive a series of ICMP responses to consider the request a success. Range of values: 1 to 30. The default setting is 3.
8. In the **Max hops** field, enter the maximum number of hops for the series of ICMP requests. Range of values: 1 to 60. The default setting is 10.
9. Click **Run**.

The traceroute utility is run on the CPE device, and a report containing the output of the ping utility is displayed in the lower part of the settings area.

Running the tcpdump utility

If you have previously run the tcpdump utility, a [report file](#) was generated with the captured traffic. When you run the utility again, that report file is overwritten. You can [download the previous report file](#) if you want to keep it.

The tcpdump utility puts additional load on the CPU of the CPE device.

To run the tcpdump utility:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device on which you want to run the tcpdump utility.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. Select the **Utilities** → **Tcpdump** tab.

The tcpdump utility settings are displayed.

4. In the **Capture interface** drop-down list, select the previously [created network interface](#) on which you want to capture traffic.

5. In the **Direction** drop-down list, select the direction of the traffic you want to capture:

- **in** to capture incoming traffic.
- **out** to capture outgoing traffic.
- **in/out** to capture both incoming and outgoing traffic. Default value.

6. If you want the CPE device to use the DNS server to resolve IP addresses to domain names when creating the report file with the captured traffic, select the **Resolve DNS names** check box. You can specify a DNS server when creating or [editing a network interface](#). IP addresses that cannot be resolved to domain names are also reflected in the report file. This check box is cleared by default.

7. If you want to use a filter to capture traffic, in the **Capture expression (tcpdump filter format)** field, enter the syntax of the filter. Maximum length: 1024 characters. For example, you can use the following filters:

- `icmp` to capture only ICMP traffic packets.
- `host 1.2.3.4 and (port 80 or 443)` to capture only traffic packets with IPv4 address 1.2.3.4 and source or destination TCP port 80 or 443.
- `tcp[13] & 2 != 0` to capture only TCP SYN traffic packets.

Detailed information about traffic filters can be obtained from the [official tcpdump documentation](#) ².

8. In the **Maximum capture time (sec.)** field, enter the time in seconds after which you want traffic capture to stop. Range of values: 10 to 600. The default setting is 30.

9. In the **Max. captured packets** field, enter the number of traffic packets that you want collected before traffic capture stops. Range of values: 1 to 10,000. The default setting is **1000**.

Traffic capturing stops when the time specified in the **Maximum capture time (sec.)** field passes, or when the number of traffic packets specified in the **Max. captured packets** field is captured.

10. Click **Run**.

The tcpdump utility is run on the CPE device, and a report file with the captured traffic is generated.

Running the iperf utility

If you have already run the iperf utility, a [report file](#) was generated with network performance diagnostics results. When you run the utility again, that report file is overwritten. You can [download the previous report file](#) if you want to keep it.

To run the iperf utility:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device on which you want to run the iperf utility.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. Select the **Utilities** → **Iperf** tab.

The iperf utility settings are displayed.

4. Specify the mode in which you want to use the iperf utility on the CPE device by selecting one of the following options:

- **Server** to use the CPE device as an iperf server.
- **Client** to use the CPE device as an iperf client.

5. If you chose the **Server** option, configure the iperf server:

- a. In the **Port** field, enter the TCP or UDP port number of the iperf server. Range of values: 1001 to 65,535. The default setting is **7777**.

- b. In the **Report interval (sec.)** field, enter the interval in seconds for writing lines to the report file. Range of values: 0 to 60. The default setting is **3**.

- c. If you do not want to create a report file with network performance diagnostics results, select the **Do not report** check box. This check box is cleared by default.

- d. Under **Report format**, select the format of the network performance diagnostics results in the report file:

- **Kbit/sec** (default)

- **Mbit/sec**
- **Kbyte/sec**
- **Mbyte/sec**

e. In the **Run server for (sec.)** field, enter the duration in seconds for which you want the iperf server to run. Range of values: 60 to 3600. The default setting is 300.

6. If you chose the **Client** option, configure the iperf client:

a. In the **Server IP** field, enter the IPv4 address of the iperf server to which you want the client to connect.

b. In the **Port** field, enter the TCP or UDP port number of the iperf server to which you want the client to connect. Range of values: 1001 to 65,535. The default setting is 7777.

c. In the **Report interval (sec.)** field, enter the interval in seconds for writing lines to the performance diagnostics report file. Range of values: 0 to 60. The default setting is 3.

d. If you do not want to create a report file with network performance diagnostics results, select the **Do not report** check box. This check box is cleared by default.

e. Under **Report format**, select the format of the network performance diagnostics results in the report file:

- **Kbit/sec** (default)
- **Mbit/sec**
- **Kbyte/sec**
- **Mbyte/sec**

f. In the **Run client for (sec.)** field, enter the duration in seconds for which you want the iperf client to run. Range of values: 60 to 3600. The default setting is 60.

g. Specify the port type of the iperf server by selecting one of the following options:

- **TCP** (default).
- **UDP**

h. In the **Client bitrate** field, enter the bit rate of the iperf client in one of the following formats:

- `< bit rate in bits per second >`
For example, if you enter 10000, the bit rate is 10,000 bits per second.
- `< bit rate in kilobytes per second >k`
For example, if you enter 10k, the bit rate is 10 kbps.
- `< bit rate in kilobytes per second >K`
For example, if you enter 10K, the rate is 10 KB/s.
- `< bit rate in megabits per second >m`
For example, if you enter 10m, the bit rate is 10 Mbps.

- `<bit rate in megabytes per second>M`

For example, if you enter `10M`, the bit rate is 10 MB/s.

i. In the **Test direction** drop-down list, select the direction of traffic that you want to use for measuring network performance:

- **client-server** to use the traffic that the iperf client sends to the server. Default value.
- **server-client** to use the traffic that the iperf server sends to the client.
- **bidirectional** to use traffic that the iperf client sends to the server as well as the traffic that the iperf server sends to the client.

j. If necessary, in the **TCP windows size, bytes** field, enter the TCP window size in bytes. If you do not specify a value for this parameter, the TCP window size is automatically detected.

k. If necessary, in the **TCP MSS, bytes** field, enter the maximum TCP segment size in bytes.

7. Click **Run**.

The iperf utility is run on the CPE device, and a report file with the network diagnostics results is generated.

To manage the report file, click **Download results**.

Running the sweep utility

You can use the sweep utility to clear the ARP cache, restart the FRR (Free Range Routing) process, and clear the table of NAT sessions on the CPE device.

Restarting the FRR process and clearing the NAT session table may cause traffic transmission to stop for a few seconds.

To run the sweep utility:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device on which you want to run the sweep utility.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. Select the **Utilities** → **Sweep** tab.

The sweep utility settings are displayed.

4. If you want to clear the ARP cache:

a. Under **Clear ARP-cache on interface**, select the previously [created network interface](#) on which you want to clear the ARP cache. If you want to clear the ARP cache on all network interfaces, select **All**.

b. Click **Run**.

The ARP cache is cleared on the CPE device.

5. If you want to restart the FRR process, under **Restart FRR (routing) process**, click **Run**.

The FRR process is restarted on the CPE device.

6. If you want to clear the NAT session table, under **Clear NAT sessions table**, click **Run**. You can configure NAT on a CPE device using a [firewall](#).

The NAT session table is cleared on the CPE device.

Managing report files

Report files are generated from the output of the [tcpdump](#) and [iperf](#) utilities. To display the table of report files on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Utilities** → **Files** tab. Information about report files is displayed in the following columns of the table:

- **Type** is the type of the report file.
- **Created** is the date and time when the report file was created.

The actions you can perform with the table are described in the [Managing solution component tables](#) instructions.

Downloading a report file

To download a report file:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device from which you want to download the report file.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. Select the **Utilities** → **Files** tab.

A table of report files is displayed.

4. Click **Download file** next to the report file that you want to download.

An TXT file is saved on your local device.

Deleting a report file

Deleted report files cannot be restored.

To delete a report file:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device on which you want to delete a report file.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. Select the **Utilities** → **Files** tab.

A table of report files is displayed.

4. Click **Delete** next to the report file that you want to delete.

5. In the confirmation window, click **Delete**.

The report file is deleted and is no longer displayed in the table.

IP address and subnet ranges for CPE devices

You can create ranges of IP addresses and subnets to centrally assign IPv4 addresses to network interfaces when [creating](#) or [editing](#) such interfaces. You can also use IP address ranges to centrally assign IPv4 addresses to router IDs of CPE devices when [specifying basic BGP settings](#).

Managing IP address ranges

To display the table of IP address ranges, go to the **SD-WAN** → **IPAM** section. The **IP Pool** tab is selected by default. Information about IP address ranges is displayed in the following columns of the table:

- **Name** is the name of the IP address range.
- **CIDR** is the IPv4 prefix of the subnet in which the IP address range is located.
- **IP range** specifies the starting and ending values of the IP address range.
- **Usage** is the number of IP addresses in the range that have been assigned to [network interfaces](#) or router IDs of CPE devices.

The actions you can perform with the table are described in the [Managing solution component tables](#) instructions.

Creating an IP address range

To create an IP address range:

1. In the menu, go to the **SD-WAN** → **IPAM** section.
By default, the **IP Pool** tab is selected, displaying a table of IP address ranges.
2. In the upper part of the page, click **+ IP Pool**.
3. This opens a window; in that window, in the **Name** field, enter the name of the IP address range. Maximum length: 32 characters.
4. In the **CIDR** field, enter the IPv4 prefix of the subnet in which the IP address range is located.
5. Specify a range of IP addresses:
 - a. Under **IP range**, click **+ Add**.
 - b. In the fields that are displayed, enter the start and end values for the IP address range.

The range of IP addresses is specified and displayed in the **IP range** section. You can specify multiple ranges of IP addresses; to delete a range, click the delete icon next to it.

6. Click **Create**.

The IP address range is created and displayed in the table.

Editing an IP address range

To change an IP address range:

1. In the menu, go to the **SD-WAN** → **IPAM** section.

By default, the **IP Pool** tab is selected, displaying a table of IP address ranges.

2. Click the IP address range that you want to edit.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, displaying the settings of the IP address range.

3. This opens a window; in that window, in the **Name** field, enter the name of the IP address range. Maximum length: 32 characters.

4. In the **CIDR** field, enter the IPv4 prefix of the subnet in which the IP address range is located.

5. Specify a range of IP addresses:

- a. Under **IP range**, click **+ Add**.

- b. In the fields that are displayed, enter the start and end values for the IP address range.

The range of IP addresses is specified and displayed in the **IP range** section. You can specify multiple ranges of IP addresses; to delete a range, click the delete icon next to it.

6. In the upper part of the settings area, click **Save**.

The IP address range is modified and updated in the table.

Viewing the usage of an IP address range

You can view which [CPE templates](#) and [devices](#) are using an IP address range. If the IP address range is used by at least one CPE template or device, the range cannot be [deleted](#). You can also view information about IP addresses that have been assigned from the range.

To view the usage of an IP address range:

1. In the menu, go to the **SD-WAN** → **IPAM** section.

By default, the **IP Pool** tab is selected, displaying a table of IP address ranges.

2. Click the IP address range for which you want to view usage information.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, displaying the settings of the IP address range.

3. If necessary, do one of the following:

- If you want to see which CPE devices are using an IP address range, select the **Usage** → **CPE** tab.

A list of CPE devices that are using the IP address range is displayed.

- If you want to see which CPE templates are using an IP address range, select the **Usage** → **Template** tab. A list of CPE templates that are using the IP address range is displayed.
4. If you want to view information about IP addresses that have been assigned from the IP address range, select the **Leases** tab.
- A table of IP addresses assigned from the range is displayed. Information about IP addresses is displayed in the following columns of the table:
- **IP** is the IP address that has been assigned from the range.
 - **CPE** is the [CPE device](#) to which the IP address is assigned.
 - **Type** indicates whether the IP address is assigned to a [network interface](#) or router ID of the CPE device.
 - **Name** is the name of the network interface to which the IP address is assigned. If an IP address has been assigned to the router ID of the CPE device, no value is displayed in this column.
 - **Tenant** is the [tenant](#) to which the CPE device is assigned.

The actions you can perform with the lists and table are described in the [Managing solution component tables](#) instructions.

Deleting IP address ranges

You cannot delete an IP address range if it is being used by at least one CPE template or device. You need to [look up the usage of the IP address range](#) and make sure that it is not being used by any component.

Deleted IP address ranges cannot be restored.

To delete IP address ranges:

1. In the menu, go to the **SD-WAN** → **IPAM** section.
By default, the **IP Pool** tab is selected, displaying a table of IP address ranges.
2. To delete an individual IP address range:
 - a. Click the IP address range that you want to delete.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, displaying the settings of the IP address range.
 - b. In the upper part of the settings area, under **Actions**, click **Delete**.
3. To delete multiple IP address ranges:
 - a. Select check boxes next to IP address ranges that you want to delete.
 - b. In the upper part of the table, click **Actions** → **Delete**.
4. In the confirmation window, click **Delete**.

The IP address ranges are deleted and are no longer displayed in the table.

Managing subnet ranges

To display the table of subnet ranges, go to the **SD-WAN** → **IPAM** section and select the **Subnet Pool** tab. Information about subnet ranges is displayed in the following columns of the table:

- **Name** is the name of the subnet range.
- **CIDR** is the IPv4 prefix of the subnet range.
- **Usage** is the number of subnets that have been assigned to [network interfaces](#).

The actions you can perform with the table are described in the [Managing solution component tables](#) instructions.

Creating a subnet range

To create a subnet range:

1. In the menu, go to the **SD-WAN** → **IPAM** section.
By default, the **IP Pool** tab is selected, displaying a table of IP address ranges.
2. Select the **Subnet Pool** tab.
A table of subnet ranges is displayed.
3. In the upper part of the page, click **+ Subnet Pool**.
4. This opens a window; in that window, in the **Name** field, enter the name of the subnet range. Maximum length: 32 characters.
5. In the **Base CIDR** field, enter the IPv4 prefix of the subnet range.
6. In the **Sub-prefix** field, enter the length of the IPv4 prefix of subnets in the range. Range of values: 0 to 32.
7. Click **Create**.

The subnet range is created and displayed in the table.

Editing a subnet range

To edit a subnet range:

1. In the menu, go to the **SD-WAN** → **IPAM** section.
By default, the **IP Pool** tab is selected, displaying a table of IP address ranges.
2. Select the **Subnet Pool** tab.
A table of subnet ranges is displayed.
3. Click the subnet range that you want to edit.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, displaying the settings of the subnet range.

4. This opens a window; in that window, in the **Name** field, enter the name of the subnet range. Maximum length: 32 characters.
5. In the **Base CIDR** field, enter the IPv4 prefix of the subnet range.
6. In the **Sub-prefix** field, enter the length of the IPv4 prefix of subnets in the range. Range of values: 0 to 32.
7. In the upper part of the settings area, click **Save**.

The subnet range is modified and updated in the table.

Viewing the usage of a subnet range

You can view which [CPE templates](#) and [devices](#) are using a subnet range. If the subnet range is used by at least one CPE template or device, the range cannot be [deleted](#). You can also view information about subnets that have been assigned from the range.

To view the usage of a subnet range:

1. In the menu, go to the **SD-WAN** → **IPAM** section.

By default, the **IP Pool** tab is selected, displaying a table of IP address ranges.

2. Select the **Subnet Pool** tab.

A table of subnet ranges is displayed.

3. Click the CPE template for which you want to view usage information.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, displaying the settings of the subnet range.

4. If necessary, do one of the following:

- If you want to see which CPE devices are using a subnet range, select the **Usage** → **CPE** tab.
A list of CPE devices that are using the subnet range is displayed.
- If you want to see which CPE templates are using a subnet range, select the **Usage** → **Template** tab.
A list of CPE templates that are using the subnet range is displayed.

5. If you want to view information about subnets that have been assigned from the subnet range, select the **Leases** tab.

A table of subnets assigned from the range is displayed. Information about subnets is displayed in the following columns of the table:

- **CIDR** is the IPv4 prefix of the subnet that was assigned from the range.
- **CPE** is the [CPE device](#) to which an IPv4 address from the subnet is assigned.
- **Name** is the name of the [network interface](#) to which an IPv4 address from the subnet is assigned.

- **Tenant** is the [tenant](#) to which the CPE device is assigned.

The actions you can perform with the lists and table are described in the [Managing solution component tables](#) instructions.

Deleting subnet ranges

You cannot delete a subnet range if it is being used by at least one CPE template or device. You need to [look up the usage of the subnet range](#) and make sure that it is not being used by any component.

Deleted subnet ranges cannot be restored.

To delete subnet ranges:

1. In the menu, go to the **SD-WAN** → **IPAM** section.

By default, the **IP Pool** tab is selected, displaying a table of IP address ranges.

2. Select the **Subnet Pool** tab.

A table of subnet ranges is displayed.

3. To delete an individual subnet range:

- a. Click the subnet range that you want to delete.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, displaying the settings of the subnet range.

- b. In the upper part of the settings area, under **Actions**, click **Delete**.

4. To delete multiple subnet ranges:

- a. Select check boxes next to subnet ranges that you want to delete.

- b. In the upper part of the table, click **Actions** → **Delete**.

5. In the confirmation window, click **Delete**.

The subnet ranges are deleted and are no longer displayed in the table.

Managing the firewall

Kaspersky SD-WAN supports a firewall for filtering traffic packets on a CPE device. The firewall can accept, drop, or reject traffic packets. If a traffic packet is rejected, the sender receives an `icmp-reject` message. The firewall can apply each action to inbound and outbound traffic packets, as well as to traffic packets redirected between network interfaces and subnets.

To avoid configuring each device individually, you can specify firewall settings in a firewall template and then apply the template to devices when [adding](#) or [manually registering](#) them. If you edit a firewall setting in a template, that setting is automatically modified on all CPE devices that are using the template. When you edit a firewall setting on a CPE device, that setting becomes independent of the firewall template. When the same setting is edited in the firewall template, the change is not propagated to the CPE device.

To perform actions with traffic packets relayed through network interfaces and subnets, you must place these network interfaces and subnets in a *firewall zone* (hereinafter also referred to as 'zone'). You can create common zones that can be used by multiple CPE devices and zones on an individual device. When creating a zone, you specify actions that you want to be applied to traffic packets and add subnets to the zone. You can add network interfaces to a zone when [creating](#) or [editing](#) such network interfaces. To allow or deny traffic between two zones, you can create a *forwarding*.

You cannot edit a common zone because it can be used by a large number of CPE templates and devices, and editing such a zone would result in a mass update of all components that are using it, which would overload the orchestrator. If you want to edit the common zone, you must create a new common zone. To the created shared zone, you can add network interfaces and subnets that were added to the previous common zone.

To perform actions with traffic packets based on the specified criteria, you must create *firewall rules*. For example, you can create a firewall rule that rejects traffic packets with a specified source zone. If you want to specify the same IP addresses or subnets in multiple firewall rules, you can create an *IP set*.

When a traffic packet is forwarded to a CPE device, one of the firewall rules is applied to the traffic packet. If none of the firewall rules can be applied, the action specified in the settings of the zone to which this packet was sent is applied to the traffic packet. If the traffic packet was not forwarded to any of the zones, the default action is applied to it; you can specify the default action when configuring basic firewall settings.

The firewall supports the following network address translation (NAT) mechanisms:

- *DNAT rules* can replace the following elements of traffic packets with your specified values:
 - Destination IP addresses or prefixes
 - Destination zones
 - Destination ports (Port Address Translation, PAT)
- *SNAT rules* can replace source IP addresses or prefixes of traffic packets with your specified values.

DNAT rules and SNAT rules are applied to traffic packets based on the specified criteria. For example, you can create a DNAT rule that replaces the destination IP address of TCP traffic packets.

Managing firewall zones

Managing common zones of the firewall

To display the table of common firewall zones, go to the **SD-WAN** → **Firewall zones** menu section. Information about firewall zones is displayed in the following columns of the table:

- **Name** is the name of the firewall zone.
- **Usage** specifies whether the zone is used by [firewall templates](#), [CPE templates](#), and [devices](#):
 - **Yes**
 - **No**
- **Author** is the name of the [user](#) that created the firewall zone.
- **Created** is the date and time when the firewall zone was created.

The actions that you can perform with the table are described in the [Managing solution component tables](#) instructions.

Managing firewall zones on a CPE device

To display the table of firewall zones on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **Zones** tab. Information about firewall zones is displayed in the following columns of the table:

- **Name** is the name of the firewall zone.
- **Settings** contains the actions that the firewall must apply to traffic packets.
- **Interfaces/Networks** are [network interfaces](#) and subnets added to the firewall zone.

Creating a firewall zone

You can create a common firewall zone or a zone on the CPE device.

To create a firewall zone:

1. Create a firewall zone in one of the following ways:

- If you want to create a common firewall zone, go to the **SD-WAN** → **Firewall zones** section and in the upper part of the page, click **+ Firewall zone**.
- If you want to create a firewall zone on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **Zones** tab, select the **Override** check box, and click **+ Firewall zone**.

A table of firewall zones is displayed.

2. This opens a window; in that window, in the **Name** field, enter the name of the firewall zone. Maximum length: 255 characters.
3. In the **Input** drop-down list, select the action that you want the firewall to apply to inbound traffic packets:

- **ACCEPT** to accept traffic packets. Default value.
 - **DROP** to drop traffic packets.
 - **REJECT** to reject traffic packets with an `icmp-reject` message.
4. In the **Output** drop-down list, select the action that you want the firewall to apply to outbound traffic packets:
- **ACCEPT** to accept traffic packets. Default value.
 - **DROP** to drop traffic packets.
 - **REJECT** to reject traffic packets with an `icmp-reject` message.
5. In the **Forwarding** drop-down list, select the action that you want the firewall to apply to traffic packets relayed between network interfaces and subnets:
- **ACCEPT** to accept traffic packets. Default value.
 - **DROP** to drop traffic packets.
 - **REJECT** to reject traffic packets with an `icmp-reject` message.
6. If you want to replace the source IP address of outbound traffic packets from the zone with the IP address assigned to the egress [network interface](#):
- a. Select the **Masquerading** check box. This check box is cleared by default.
 - b. If you want to replace the source IP address only for traffic packets with the specified source subnet:
 1. Under **Masquerading source subnets**, click **+ Add**.
 2. In the field that is displayed, enter an IPv4 prefix.

The subnet is specified and displayed under **Masquerading source subnets**. You can specify multiple subnets; to delete a subnet, click the delete icon next to it.
 - c. If you want to replace the source IP address only for traffic packets with the specified destination subnet:
 1. Under **Masquerading destination subnets**, click **+ Add**.
 2. In the field that is displayed, enter an IPv4 prefix.

The subnet is specified and displayed under **Masquerading destination subnets**. You can specify multiple subnets; to delete a subnet, click the delete icon next to it.
7. Clear the **MSS clamp to PMTU** check box if you do not want the firewall to limit the Maximum Segment Size (MSS) of traffic packets relayed through the zone to the Path Maximum Transmission Unit (PMTU) value minus 40. The purpose of subtracting 40 is to exclude the size of the TCP header. This check box is selected by default.
8. If you want the firewall to keep a log of traffic packets dropped in the zone, select the **Drops logging** check box. If logs created on a CPE device are sent to a [Syslog server](#), you can view the logs on that server. If logs created on the CPE device are stored locally, you can view the logs by [requesting diagnostic information](#). This check box is cleared by default.

9. If network interfaces of CPE devices are connected to L3 switches or routers, and you want to relay traffic packets from subnets of these switches or routers through the firewall zone, add the subnet to the zone:

a. Under **Networks**, click **+ Add**.

b. In the field that is displayed, enter the IPv4 prefix of the subnet.

The subnet is added and displayed under **Networks**. You can add multiple subnets; to delete a subnet, click the delete icon next to it.

10. Click **Create**.

The firewall zone is created and displayed in the table.

11. If you have created a firewall zone on a CPE device, click **Save** in the upper part of the settings area to save the device settings.

You must add network interfaces to the created firewall zone. You can do this when [creating](#) or [editing a network interface](#). If you created a firewall zone on a CPE device, the network interfaces that you add to the zone must be created on the same device.

Editing the name of the firewall common zone

You can edit the name of a previously [created common firewall zone](#). The process of editing the name of a firewall zone on a CPE device is described in the [instructions on editing a firewall zone on the CPE device](#).

To edit the name of a common firewall zone:

1. In the menu, go to the **SD-WAN** → **Firewall zones** section.

A table of firewall zones is displayed.

2. Click the common firewall zone whose name you want to edit.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon.

3. In the upper part of the settings area, under **Actions**, click **Rename of Firewall zone**.

4. This opens a window; in that window, enter a new name for the common firewall zone.

5. Click **Rename**.

The name of the common firewall zone is modified and updated in the table.

Cloning a firewall common zone

You can clone a previously [created common firewall zone](#) to create an identical common firewall zone with a different name. Cloning firewall zones on a CPE device is not supported.

To clone a common firewall zone:

1. In the menu, go to the **SD-WAN** → **Firewall zones** section.

A table of firewall zones is displayed.

2. Click the common firewall zone which you want to clone.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

3. In the upper part of the settings area, under **Actions**, click **Clone**.

4. This opens a window; in that window, enter a name for the new common firewall zone.

5. Click **Clone**.

A copy of the common firewall zone with the new name is created and displayed in the table.

Viewing the usage of a firewall common zone

You can see which [firewall templates](#), [CPE templates](#), and [devices](#) are using a previously [created common zone](#). If at least one component uses the common firewall zone, such a zone cannot be [deleted](#).

To view the usage of a common firewall zone:

1. In the menu, go to the **SD-WAN** → **Firewall zones** section.

A table of firewall zones is displayed.

2. Click the common firewall zone whose usage you want to view.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

3. In the upper part of the settings area, under **Actions**, click **Show usage**.

This opens a window with a table of firewall templates, CPE templates, and devices that are using the common zone.

Editing a firewall zone on a CPE device

You can edit a previously [created firewall zone on a CPE device](#).

You cannot edit a common zone because it can be used by a large number of CPE templates and devices, and editing such a zone would result in a mass update of all components that are using it, which would overload the orchestrator. If you want to edit the common zone, you must create a new common zone. To the created shared zone, you can add network interfaces and subnets that were added to the previous common zone.

To edit a firewall zone on a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. Select the **Firewall settings** → **Zones** tab.

A table of firewall zones is displayed.

4. Select the **Override** check box.
5. Click the **Edit** button next to the zone that you want to edit.
6. This opens a window; in that window, in the **Name** field, enter the name of the firewall zone. Maximum length: 255 characters.
7. In the **Input** drop-down list, select the action that you want the firewall to apply to inbound traffic packets:
 - **ACCEPT** to accept traffic packets. Default value.
 - **DROP** to drop traffic packets.
 - **REJECT** to reject traffic packets with an `icmp-reject` message.
8. In the **Output** drop-down list, select the action that you want the firewall to apply to outbound traffic packets:
 - **ACCEPT** to accept traffic packets. Default value.
 - **DROP** to drop traffic packets.
 - **REJECT** to reject traffic packets with an `icmp-reject` message.
9. In the **Forwarding** drop-down list, select the action that you want the firewall to apply to traffic packets relayed between network interfaces and subnets:
 - **ACCEPT** to accept traffic packets. Default value.
 - **DROP** to drop traffic packets.
 - **REJECT** to reject traffic packets with an `icmp-reject` message.
10. If you want to replace the source IP address of outbound traffic packets from the zone with the IP address assigned to the egress [network interface](#):
 - a. Select the **Masquerading** check box. This check box is cleared by default.
 - b. If you want to replace the source IP address only for traffic packets with the specified source subnet:
 1. Under **Masquerading source subnets**, click **+ Add**.
 2. In the field that is displayed, enter an IPv4 prefix.

The subnet is specified and displayed under **Masquerading source subnets**. You can specify multiple subnets; to delete a subnet, click the delete icon next to it.
 - c. If you want to replace the source IP address only for traffic packets with the specified destination subnet:
 1. Under **Masquerading destination subnets**, click **+ Add**.
 2. In the field that is displayed, enter an IPv4 prefix.

The subnet is specified and displayed under **Masquerading destination subnets**. You can specify multiple subnets; to delete a subnet, click the delete icon next to it.

11. Clear the **MSS clamp to PMTU** check box if you do not want the firewall to limit the Maximum Segment Size (MSS) of traffic packets relayed through the zone to the Path Maximum Transmission Unit (PMTU) value minus 40. The purpose of subtracting 40 is to exclude the size of the TCP header. This check box is selected by default.
12. If you want the firewall to keep a log of traffic packets dropped in the zone, select the **Drops logging** check box. If logs created on a CPE device are sent to a [Syslog server](#), you can view the logs on that server. If logs created on the CPE device are stored locally, you can view the logs by [requesting diagnostic information](#). This check box is cleared by default.
13. If network interfaces of CPE devices are connected to L3 switches or routers, and you want to relay traffic packets from subnets of these switches or routers through the firewall zone, add the subnet to the zone:
 - a. Under **Networks**, click **+ Add**.
 - b. In the field that is displayed, enter the IPv4 prefix of the subnet.The subnet is added and displayed under **Networks**. You can add multiple subnets; to delete a subnet, click the delete icon next to it.
14. Click **Save**.

The firewall zone is modified and updated in the table.
15. In the upper part of the settings area, click **Save** to save CPE device settings.

Deleting a firewall zone

You can delete a common firewall zone or a zone on a CPE device.

Deleted firewall zones cannot be restored.

Deleting a firewall common zone

You cannot delete a common zone if it is being used by at least one [firewall template](#), [CPE template](#), or [device](#). You must [view the usage of the common firewall zone](#) and make sure that no component is using it.

To delete a common firewall zone:

1. In the menu, go to the **SD-WAN** → **Firewall zones** section.

A table of firewall zones is displayed.
2. Click the common firewall zone which you want to delete.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .
3. In the upper part of the settings area, under **Actions**, click **Delete**.
4. In the confirmation window, click **Delete**.

The common firewall zone is deleted and is no longer displayed in the table.

Deleting a firewall zone on a CPE device

To delete a firewall zone on a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. Select the **Firewall settings** → **Zones** tab.

A table of firewall zones is displayed.

4. Select the **Override** check box.

5. Click **Delete** next to the firewall zone that you want to delete.

6. In the confirmation window, click **Delete**.

The firewall zone is deleted and is no longer displayed in the table.

7. In the upper part of the settings area, click **Save** to save CPE device settings.

Managing firewall templates

The table of firewall templates is displayed under **SD-WAN** → **Firewall templates**. One of the templates is the *default template*, which means it is pre-selected when [adding](#) and [manually registering a CPE device](#). By default, the **Default firewall template** is created, which forms the basis for all other firewall templates you create. Information about firewall templates is displayed in the following columns of the table:

- **Name** is the name of the firewall template.
- **Usage** shows whether the firewall template is used by [CPE devices](#).
 - **Yes**
 - **No**
- **Owner** is the name of the [user](#) that created the firewall template.
- **Last update** is the date and time when the firewall template settings were last modified.

The actions that you can perform with the table are described in the [Managing solution component tables](#) instructions.

Firewall template settings are displayed on the following tabs:

- **Global settings** contains [basic settings of the firewall](#).
- **Rules** contains [firewall rules](#).

- **NAT** contains NAT settings. The following tabs are displayed on this tab:
 - **DNAT** contains [DNAT rules](#).
 - **SNAT** contains [SNAT rules](#).
- **Zones forwarding** contains [forwardings between zones](#).
- **IP sets** contains [IP sets](#).

Creating a firewall template

To create a firewall template:

1. Go to the **SD-WAN** → **Firewall templates** section.
A table of firewall templates is displayed.
2. In the upper part of the page, click **+ Firewall template**.
3. This opens a window; in that window, enter the name of the firewall template.
4. Click **Create**.

The firewall template is created and displayed in the table.

Setting the default firewall template

You can set a firewall template as the default to have it preselected when [adding](#) or [manually registering a CPE device](#).

To set a default firewall template:

1. Go to the **SD-WAN** → **Firewall templates** section.
A table of firewall templates is displayed.
2. Click the firewall template that you want to make the default template.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Global settings** tab is selected, which displays the main settings of the firewall template.
3. In the upper part of the settings area, under **Actions**, click **Set as default template**.

The firewall template is set as the default template.

Exporting a firewall template

You can export a firewall template to subsequently [import it into another template](#).

To export a firewall template:

1. Go to the **SD-WAN** → **Firewall templates** section.

A table of firewall templates is displayed.

2. Click the firewall template that you want to export.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Global settings** tab is selected, which displays the main settings of the firewall template.

3. In the upper part of the settings area, under **Actions**, click **Export**.

An archive in the TAR.GZ format is saved on your local device. The archive does not contain information about CPE devices using the firewall template.

Importing a firewall template

You can import a previously [exported template](#) into a firewall template. Firewall template settings are specified in accordance with the settings of the imported template. During import, you can select the tabs that you want to leave unchanged.

A firewall template into which another template is imported remains applied to CPE devices, but the settings of those devices are not modified.

To import a firewall template:

1. Go to the **SD-WAN** → **Firewall templates** section.

A table of firewall templates is displayed.

2. Click the firewall template into which you want to import another template.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Global settings** tab is selected, which displays the main settings of the firewall template.

3. In the upper part of the settings area, under **Actions**, click **Import**.

4. This opens a window; in that window, clear the check boxes next to the firewall template tabs that you want to leave unchanged after import.

5. In the **File** field, specify the path to the TAR.GZ archive.

6. Click **Import**.

Firewall template settings are modified in accordance with the settings of the imported template.

Cloning a firewall template

You can clone a firewall template to create an identical template with a different name.

To clone a firewall template:

1. Go to the **SD-WAN** → **Firewall templates** section.

A table of firewall templates is displayed.

2. Click the firewall template that you want to clone.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Global settings** tab is selected, which displays the main settings of the firewall template.

3. In the upper part of the settings area, under **Actions**, click **Clone**.
4. This opens a window; in that window, enter the name of the new firewall template.
5. Click **Clone**.

A copy of the firewall template with the new name is created and displayed in the table.

Viewing the usage of a firewall template

You can see which [CPE devices](#) are using the firewall template. If a firewall template is being used by at least one CPE device, such a template cannot be [deleted](#).

To view the usage of a firewall template:

1. Go to the **SD-WAN** → **Firewall templates** section.

A table of firewall templates is displayed.

2. Click the firewall template for which you want to view the usage.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Global settings** tab is selected, which displays the main settings of the firewall template.

3. In the upper part of the settings area, under **Actions**, click **Show associated CPEs**.

This opens a window with a table of CPE devices that are using the firewall template.

Deleting a firewall template

You cannot delete a firewall template if it is being used by at least one [CPE device](#). You need to [look up the usage of the firewall template](#) and make sure that it is not being used by any CPE device.

Deleted firewall templates cannot be restored.

To delete a firewall template:

1. Go to the **SD-WAN** → **Firewall templates** section.

A table of firewall templates is displayed.

2. Click the firewall template that you want to delete.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Global settings** tab is selected, which displays the main settings of the firewall template.

3. In the upper part of the settings area, under **Actions**, click **Delete**.
4. In the confirmation window, click **Delete**.

The firewall template is deleted and is no longer displayed in the table.

Basic firewall settings

You can configure basic firewall settings in a firewall template or on a CPE device. When you configure basic firewall settings in a firewall template, these settings are automatically propagated to all CPE devices that are using the template.

The firewall applies the actions specified in its basic settings to traffic packets. Traffic packets are affected by this if no [firewall rules](#) have been applied to them and they have not been forwarded to any of the [firewall zones](#).

To specify the basic firewall settings:

1. Specify basic firewall settings in one of the following ways:

- If you want to edit basic firewall settings in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section and click the template.
- If you want to edit basic firewall settings on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **Global settings** tab and select the **Override** check box.

Basic firewall settings are displayed.

2. If you want to disable SYN flood protection, clear the **Syn-flood protection** check box. This check box is selected by default. When SYN flood protection is enabled, a maximum of 25 traffic packets per second with the SYN, ACK, RST, and FIN flags can be sent to a CPE device.
3. If you want the firewall to drop traffic packets marked as invalid by the conntrack function, select the **Drop invalid packets** check box. This check box is cleared by default.
4. If you want to disable the DPI (Deep Packet Inspection) technology, clear the **Enable DPI** check box. This check box is selected by default. The DPI technology lets you [create firewall rules](#) that apply only to traffic packets of the specified application.

When the DPI technology is disabled, you cannot [configure DPI marking](#), and firewall rules that use this technology are automatically [disabled](#).

5. In the **Default INPUT action** drop-down list, select the action that you want the firewall to apply to inbound traffic packets:
 - **ACCEPT** to accept traffic packets. Default value.
 - **DROP** to drop traffic packets.
 - **REJECT** to reject traffic packets with an `icmp-reject` message.
6. In the **Default OUTPUT action** drop-down list, select the action that you want the firewall to apply to outbound traffic packets:
 - **ACCEPT** to accept traffic packets. Default value.

- **DROP** to drop traffic packets.
 - **REJECT** to reject traffic packets with an `icmp-reject` message.
7. In the **Default FORWARD action** drop-down list, select the action that you want the firewall to apply to traffic packets relayed between network interfaces and subnets:
- **ACCEPT** to accept traffic packets. Default value.
 - **DROP** to drop traffic packets.
 - **REJECT** to reject traffic packets with an `icmp-reject` message.
8. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Configuring DPI marking

Kaspersky SD-WAN supports [creating firewall rules](#) that are applied only to traffic packets of the specified application. You can specify the DPI marks that you want to govern which rules apply to which traffic packets.

You can configure DPI marking in a firewall template or on a CPE device. When you configure DPI marking in a firewall template, these settings are automatically propagated to all CPE devices that are using the template.

You cannot configure DPI marking if you disabled the DPI marking technology in [basic firewall settings](#).

To configure DPI marking for the firewall:

1. Configure DPI marking for the firewall is applied in one of the following ways:
 - If you want to configure DPI marking for the firewall in a firewall template, go to the **SD-WAN → Firewall templates** menu section, click the template, and in the displayed settings area, select the **DPI marking** tab.
 - If you want to configure DPI marking for the firewall on a CPE device, go to the **SD-WAN → CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings → DPI marking** tab and select the **Override** check box.

The DPI marking settings are displayed.

2. Select the check boxes next to the DPI marks which you want to govern which firewall rules apply to which traffic packets.
3. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Managing firewall rules

The table of firewall rules is displayed in the firewall template and on the CPE device:

- To display the table of firewall rules in a firewall template, go to the **SD-WAN → Firewall templates** menu section, click the template, and in the displayed settings area, select the **Rules** tab.

- To display the table of firewall rules on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **Rules** tab.

Information about firewall rules is displayed in the following columns of the table:

- **Name** is the name of the firewall rule.
- **Details** contains criteria according to which the firewall must apply the rule to traffic packets.
- **Action** is the action that the firewall rule must apply to traffic packets.

Creating a firewall rule

You can create a firewall rule in a firewall template or on a CPE device. When you create a firewall rule in a template, the rule is automatically created on all CPE devices that are using the template.

To create a firewall rule:

1. Create a firewall rule in one of the following ways:

- If you want to create a firewall rule in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **Rules** tab.
- If you want to create a firewall rule on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **Rules** tab and select the **Override** check box.

A table of firewall rules is displayed.

2. Click **+ Rule**.

3. This opens a window; in that window, in the **Name** field, enter the name of the firewall rule. Maximum length: 255 characters.

4. In the **Action** drop-down list, select the action that the firewall rule must apply to traffic packets:

- **ACCEPT** to accept traffic packets. Default value.
- **DROP** to drop traffic packets.
- **REJECT** to reject traffic packets with an `icmp-reject` message.
- **ADJ-MSS** to change the value in the MSS field in the TCP header of the traffic packets to the specified value. If you select this value, in the **MSS value** field, enter the MSS value. Range of values: 68 to 10,000.

5. Specify the criteria according to which the firewall must apply the rule to traffic packets:

- a. If you want to apply the firewall rule only to traffic packets with the specified source or destination IP addresses or subnets, in the **IP set** drop-down list, select a previously created [IP set](#). If you select a value from this drop-down list, the **Source IP** and **Destination IP** blocks become unavailable.
- b. If you want to apply the firewall rule only to traffic packets with the specified version of source or destination IP addresses or subnets, in the **IP version** drop-down list, select one of the following options:

- IPv4
- IPv6

If you do not select a value, the firewall rule is applied to traffic packets with any version of source or destination IP addresses or subnets.

- If you want to apply the firewall rule only to traffic packets with the specified source zone, in the **Source zone** drop-down list, select a previously [created zone](#).
- If you want to apply the firewall rule only to traffic packets with the specified destination zone, in the **Destination zone** drop-down list, select a previously created zone.
- If you want to apply the firewall rule only to traffic packets with the specified source IPv4 address or prefix:

- Under **Source IP**, click **+ Add**.
- In the field that is displayed, enter an IPv4 address or prefix.

The source IPv4 address or prefix is specified and displayed under **Source IP**. You can specify multiple IPv4 addresses or prefixes; to delete an IPv4 address or prefix, click the delete icon next to it.

- If you want to apply the firewall rule only to traffic packets with the specified destination IPv4 address or prefix:

- Under **Destination IP**, click **+ Add**.
- In the field that is displayed, enter an IPv4 address or prefix.

The destination IPv4 address or prefix is specified and displayed under **Destination IP**. You can specify multiple IPv4 addresses or prefixes; to delete an IPv4 address or prefix, click the delete icon next to it.

- If you want to apply the firewall rule only to traffic packets of the specified protocol, select a protocol in the **Protocol** drop-down list. When you select an option in this drop-down list, the **DPI protocol** drop-down list becomes unavailable.

With **TCP** or **UDP** selected, if you want to apply the firewall rule only to traffic packets with the specified source and/or destination ports:

- In the **Source port** field, enter a source port number or a range of source port numbers.
- In the **Destination port** field, enter a destination port number or a range of destination port numbers.

Range of values: 0 to 65,535. The format of the port number range is `< first value >-< last value >`. For example, you can enter `10` or `10-15`.

- If you want to apply the firewall rule only to traffic packets of the specified application, select an application in the **DPI protocol** drop-down list.

Traffic is attributed to applications using the DPI technology, which places additional load on the CPU of the CPE device.

You can [specify the DPI marks](#) that determine the traffic packets the rule is applied to. If you disabled the DPI technology when [specifying the basic settings of the firewall](#), the rule is automatically [disabled](#).

- Click **Create**.

The firewall rule is created and displayed in the table.

7. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

By default, the firewall rule is disabled. You must [enable the firewall rule](#) to have it applied to traffic packets.

Configuring the order of firewall rules

Firewall rules are applied to traffic packets in descending order, starting with the first rule at the top of the table. By default, firewall rules are displayed in the table in the order of [creation](#). The earlier a rule was created, the higher it is displayed in the table.

You can configure the order in which firewall rules are applied in a firewall template or on a CPE device. When you configure the order in which firewall rules are applied, that order is automatically propagated to all CPE devices that are using the template.

To configure the order in which firewall rules are applied:

1. Edit the order in which firewall rules are applied in one of the following ways:

- If you want to configure the order in which firewall rules are applied in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **Rules** tab.
- If you want to configure the order in which firewall rules are applied on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **Rules** tab and select the **Override** check box.

A table of firewall rules is displayed.

2. Configure the order in which firewall rules are applied by clicking the **Up** and **Down** buttons next to them.

3. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Editing a firewall rule

You can edit a firewall rule in a firewall template or on a CPE device. When you edit a firewall rule in a template, the rule is automatically modified on all CPE devices that are using the template.

To edit a firewall rule:

1. Edit a firewall rule in one of the following ways:

- If you want to edit a firewall rule in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **Rules** tab.
- If you want to edit a firewall rule on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **Rules** tab and select the **Override** check box.

A table of firewall rules is displayed.

2. Click **Edit** next to the firewall rule that you want to edit.
3. This opens a window; in that window, in the **Name** field, enter the name of the firewall rule. Maximum length: 255 characters.
4. In the **Action** drop-down list, select the action that the firewall rule must apply to traffic packets:
 - **ACCEPT** to accept traffic packets. Default value.
 - **DROP** to drop traffic packets.
 - **REJECT** to reject traffic packets with an `icmp-reject` message.
 - **ADJ-MSS** to change the value in the MSS field in the TCP header of the traffic packets to the specified value. If you select this value, in the **MSS value** field, enter the MSS value. Range of values: 68 to 10,000.
5. Specify the criteria according to which the firewall must apply the rule to traffic packets:
 - a. If you want to apply the firewall rule only to traffic packets with the specified source or destination IP addresses or subnets, in the **IP set** drop-down list, select a previously created [IP set](#). If you select a value from this drop-down list, the **Source IP** and **Destination IP** blocks become unavailable.
 - b. If you want to apply the firewall rule only to traffic packets with the specified version of source or destination IP addresses or subnets, in the **IP version** drop-down list, select one of the following options:
 - **IPv4**
 - **IPv6**If you do not select a value, the firewall rule is applied to traffic packets with any version of source or destination IP addresses or subnets.
 - c. If you want to apply the firewall rule only to traffic packets with the specified source zone, in the **Source zone** drop-down list, select a previously [created zone](#).
 - d. If you want to apply the firewall rule only to traffic packets with the specified destination zone, in the **Destination zone** drop-down list, select a previously created zone.
 - e. If you want to apply the firewall rule only to traffic packets with the specified source IPv4 address or prefix:
 1. Under **Source IP**, click **+ Add**.
 2. In the field that is displayed, enter an IPv4 address or prefix.The source IPv4 address or prefix is specified and displayed under **Source IP**. You can specify multiple IPv4 addresses or prefixes; to delete an IPv4 address or prefix, click the delete icon next to it.
 - f. If you want to apply the firewall rule only to traffic packets with the specified destination IPv4 address or prefix:
 1. Under **Destination IP**, click **+ Add**.
 2. In the field that is displayed, enter an IPv4 address or prefix.The destination IPv4 address or prefix is specified and displayed under **Destination IP**. You can specify multiple IPv4 addresses or prefixes; to delete an IPv4 address or prefix, click the delete icon next to it.

g. If you want to apply the firewall rule only to traffic packets of the specified protocol, select a protocol in the **Protocol** drop-down list. When you select an option in this drop-down list, the **DPI protocol** drop-down list becomes unavailable.

With **TCP** or **UDP** selected, if you want to apply the firewall rule only to traffic packets with the specified source and/or destination ports:

1. In the **Source port** field, enter a source port number or a range of source port numbers.
2. In the **Destination port** field, enter a destination port number or a range of destination port numbers.

Range of values: 0 to 65,535. The format of the port number range is `< first value >-< last value >`. For example, you can enter `10` or `10-15`.

h. If you want to apply the firewall rule only to traffic packets of the specified application, select an application in the **DPI protocol** drop-down list.

Traffic is attributed to applications using the DPI technology, which places additional load on the CPU of the CPE device.

You can [specify the DPI marks](#) that determine the traffic packets the rule is applied to. If you disabled the DPI technology when [specifying the basic settings of the firewall](#), the rule is automatically [disabled](#).

6. Click **Save**.

The firewall rule is modified and updated in the table.

7. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Enabling or disabling a firewall rule

By default, [firewall rules are created](#) in a disabled state. You must enable the firewall rule to have it applied to traffic packets.

You can enable or disable a firewall rule in a firewall template or on a CPE device. When you enable or disable a firewall rule in a template, the rule is automatically enabled or disabled on all CPE devices that are using the template.

To enable or disable a firewall rule:

1. Enable or disable a firewall rule in one of the following ways:
 - If you want to enable or disable a firewall rule in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **Rules** tab.
 - If you want to enable or disable a firewall rule on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **Rules** tab and select the **Override** check box.

A table of firewall rules is displayed.

2. Click **Enable** or **Disable** next to the firewall rule that you want to enable or disable.

The firewall rule is enabled or disabled.

3. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Deleting a firewall rule

You can delete a firewall rule in a firewall template or on a CPE device. When you delete a firewall rule in a template, the rule is automatically deleted on all CPE devices that are using the template.

Deleted firewall rules cannot be restored.

To delete a firewall rule:

1. Delete a firewall rule in one of the following ways:

- If you want to delete a firewall rule in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **Rules** tab.
- If you want to edit a firewall rule on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **Rules** tab and select the **Override** check box.

A table of firewall rules is displayed.

2. Click **Delete** next to the firewall rule that you want to delete.

3. In the confirmation window, click **Delete**.

The firewall rule is deleted and is no longer displayed in the table.

4. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Managing IP sets

The table of IP sets is displayed in the firewall template and on the CPE device:

- To display the table of IP sets in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template, and in the displayed settings area, select the **IP sets** tab.
- To display the table of IP sets on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **IP sets** tab.

Information about IP sets interfaces is displayed in the following columns of the table:

- **Name** is the name of the IP set.
- **Match** specifies whether the IP set is associated with the source or the destination of traffic packets, and whether the set contains IP addresses or subnets.
- **Entries** are IP addresses or subnets added to the set.

Creating an IP set

You can create an IP set in a firewall template or on a CPE device. When you create an IP set in a firewall template, the IP set is automatically created on all CPE devices that are using the template.

To create an IP set:

1. Create an IP set in one of the following ways:

- If you want to create an IP set in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **IP sets** tab.
- If you want to create an IP set on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **IP sets** tab and select the **Override** check box.

A table of IP sets is displayed.

2. Click **+ IP set**.

3. This opens a window; in that window, in the **Name** field, enter the name of the IP set. Maximum length: 255 characters.

4. In the **Direction** drop-down list, select whether the IP set is associated with the source or the destination of traffic packets:

- **Match source** if the set contains source IP addresses or subnets.
- **Match destination** if the set contains destination IP addresses or subnets.

5. In the **Type** drop-down list, select whether the set contains IP addresses or subnets.

- **Set of subnets** if the set contains subnets.
- **Set of IPs** if the set contains IP addresses.

6. If in the **Type** drop-down list, you selected **Set of subnets**, follow these steps to specify a subnet:

a. Under **Entries list**, click **+ Add**.

b. In the field that is displayed, enter an IPv4 prefix. You can specify ranges of IPv4 prefix components using square brackets, for example, 192.[165-168].2.0/24.

The subnet is specified and displayed under **Entries list**. You can specify multiple subnets; to delete a subnet, click the delete icon next to it.

7. If in the **Type** drop-down list, you selected **Set of IPs**, follow these steps to specify an IP address:

a. Under **Entries list**, click **+ Add**.

b. In the field that is displayed, enter an IPv4 address. You can specify ranges of IPv4 address components using square brackets, for example, 192.[165-168].2.0.

The IP address is specified and displayed in the **Entries list** section. You can specify multiple IP addresses; to delete an IP address, click the delete icon next to it.

8. Click **Create**.

The IP set is created and displayed in the table.

9. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Editing an IP set

You can edit an IP set in a firewall template or on a CPE device. When you edit an IP set in a firewall template, the set is automatically modified on all CPE devices that are using the template.

To edit an IP set:

1. Edit an IP set in one of the following ways:

- If you want to edit an IP set in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **IP sets** tab.
- If you want to edit an IP set on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **IP sets** tab and select the **Override** check box.

A table of IP sets is displayed.

2. Click **Edit** next to the IP set that you want to edit.

3. This opens a window; in that window, in the **Name** field, enter the name of the IP set. Maximum length: 255 characters.

4. In the **Direction** drop-down list, select whether the IP set is associated with the source or the destination of traffic packets:

- **Match source** if the set contains source IP addresses or subnets.
- **Match destination** if the set contains destination IP addresses or subnets.

5. In the **Type** drop-down list, select whether the set contains IP addresses or subnets.

- **Set of subnets** if the set contains subnets.
- **Set of IPs** if the set contains IP addresses.

6. If in the **Type** drop-down list, you selected **Set of subnets**, follow these steps to specify a subnet:

a. Under **Entries list**, click **+ Add**.

b. In the field that is displayed, enter an IPv4 prefix. You can specify ranges of IPv4 prefix components using square brackets, for example, 192.[165-168].2.0/24.

The subnet is specified and displayed under **Entries list**. You can specify multiple subnets; to delete a subnet, click the delete icon next to it.

7. If in the **Type** drop-down list, you selected **Set of IPs**, follow these steps to specify an IP address:

a. Under **Entries list**, click **+ Add**.

b. In the field that is displayed, enter an IPv4 address. You can specify ranges of IPv4 address components using square brackets, for example, 192.[165-168].2.0.

The IP address is specified and displayed in the **Entries list** section. You can specify multiple IP addresses; to delete an IP address, click the delete icon next to it.

8. Click **Save**.

The IP set is modified and updated in the table.

9. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Disabling or enabling an IP set

You can disable or enable an IP set in a firewall template or on a CPE device. When you disable or enable an IP set in a firewall template, the set is automatically disabled or enabled on all CPE devices that are using the template.

To disable or enable an IP set:

1. Disable or enable an IP set in one of the following ways:

- If you want to enable or disable an IP set in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **IP sets** tab.
- If you want to enable or disable an IP set on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **IP sets** tab and select the **Override** check box.

A table of IP sets is displayed.

2. Click **Disable** or **Enable** next to the IP set that you want to disable or enable.

The IP set is disabled or enabled.

3. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Deleting an IP set

You can delete an IP set in a firewall template or on a CPE device. When you delete an IP set in a firewall template, the IP set is automatically deleted on all CPE devices that are using the template.

Deleted IP sets cannot be restored.

To delete an IP set:

1. Delete an IP set in one of the following ways:

- If you want to delete an IP set in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **IP sets** tab.
- If you want to delete an IP set on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **IP sets** tab and select the **Override** check box.

A table of IP sets is displayed.

2. Click **Delete** next to the IP set that you want to delete.

3. In the confirmation window, click **Delete**.

The IP set is deleted and is no longer displayed in the table.

4. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Managing forwarding

The table of forwardings is displayed in the firewall template and on the CPE device:

- To display the table of forwardings in a CPE template, go to the **SD-WAN** → **Firewall templates** menu section, click the template, and in the displayed settings area, select the **Zones forwarding** tab.
- To display the table of forwardings on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **Zones forwarding** tab.

Information about forwardings is displayed in the following columns of the table:

- **From** for the outbound zone.
- **To** for the inbound zone.

Creating a forwarding

You can create a forwarding in a firewall template or on a CPE device. When you create a forwarding in a firewall template, the forwarding is automatically created on all CPE devices that are using the template.

To create a forwarding:

1. Create a forwarding in one of the following ways:

- If you want to create a forwarding in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **Zones forwarding** tab.
- If you want to create a forwarding on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **Zones forwarding** tab and select the **Override** check box.

A table of forwardings is displayed.

2. Click **+ Forwarding**.

3. In the window that opens, in the **From** drop-down list, select a previously [created outbound zone](#).
4. In the **To** drop-down list, select a previously created inbound zone.
5. Click **Create**.
The forwarding is created and displayed in the table.
6. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Deleting a forwarding

You can delete a forwarding in a firewall template or on a CPE device. When you delete a forwarding in a firewall template, the forwarding is automatically deleted on all CPE devices that are using the template.

Deleted forwardings cannot be restored.

To delete a forwarding:

1. Delete a forwarding in one of the following ways:
 - If you want to delete a forwarding in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **Zones forwarding** tab.
 - If you want to delete a forwarding on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **Zones forwarding** tab and select the **Override** check box.

A table of forwardings is displayed.

2. Click **Delete** next to the forwarding that you want to delete.
3. In the confirmation window, click **Delete**.
The forwarding is deleted and is no longer displayed in the table.
4. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Managing DNAT rules

The table of DNAT rules is displayed in the firewall template and on the CPE device:

- To display the table of DNAT rules in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the firewall template, and in the displayed settings area, select the **NAT** → **DNAT** tab.
- To display the table of DNAT rules on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **NAT** → **DNAT** tab.

Information about DNAT rules is displayed in the following columns of the table:

- **Name** is the name of the DNAT rule.

- **Incoming** contains the criteria according to which the firewall must apply the DNAT rule to traffic packets:
- **Redirect to** is the destination IP address and port of traffic packets after the DNAT rule is applied.

Creating a DNAT rule

You can create a DNAT rule in a firewall template or on a CPE device. When you create a DNAT rule in a firewall template, the rule is automatically created on all CPE devices that are using the template.

To create a DNAT rule:

1. Create a DNAT rule in one of the following ways:

- If you want to create a DNAT rule in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **NAT** → **DNAT** tab.
- If you want to create a DNAT rule on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device and in the displayed settings area, select the **Firewall settings** → **NAT** → **DNAT** tab and select the **Override** check box.

A table of DNAT rules is displayed.

2. Click **+ DNAT**.

3. This opens a window; in that window, in the **Name** field, enter the name of the DNAT rule. Maximum length: 255 characters.

4. Specify the criteria according to which the firewall must apply the DNAT rule to traffic packets:

a. In the **Protocol** drop-down list, select the protocol of traffic packets to which the firewall must apply the DNAT rule:

- **IP**
- **TCP**
- **UDP**
- **#** for custom or non-standard protocol. If you select this value, in the displayed **Protocol number** field, enter the protocol number in accordance with the [IANA standard](#).

b. In the **Destination IP** field, enter the destination IPv4 address or prefix of traffic packets to which the firewall must apply the DNAT rule.

c. If you want to apply the DNAT rule only to traffic packets with the specified source zone, in the **Source zone** drop-down list, select a previously [created zone](#).

d. If in the **Protocol** drop-down list, you selected **TCP** or **UDP**, and you want to apply the DNAT rule only to traffic packets with the specified destination port, enter the port number in the **Destination port** field. Range of values: 1 to 65,535.

e. If you want to apply the DNAT rule only to traffic packets with the specified source IPv4 address or prefix, in the **Source IP** field, enter an IPv4 address or prefix.

5. Specify how the DNAT rule must modify traffic packets:

- a. In the **Destination IP** field, enter a new IPv4 destination address or prefix.
- b. In the **Destination zone** drop-down list, select a new previously created destination zone.
- c. If in the **Protocol** drop-down list, you selected **TCP** or **UDP**, and you want to change the destination port number of traffic packets, enter a new port number in the **Destination port** field. Range of values: 1 to 65,535.

6. Click **Create**.

The DNAT rule is created and displayed in the table.

7. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Configuring the order of DNAT rules

DNAT rules are applied to traffic packets in descending order, starting with the first rule at the top of the table. By default, DNAT rules are displayed in the table in the order of [creation](#). The earlier a rule was created, the higher it is displayed in the table.

You can configure the order in which DNAT rules are applied in a firewall template or on a CPE device. When you configure the order in which DNAT rules are applied in a firewall template, that order is automatically propagated to all CPE devices that are using the template.

To configure the order in which DNAT rules are applied:

1. Edit the order in which the DNAT rules are applied in one of the following ways:

- If you want to configure the order in which DNAT rules are applied in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **NAT** → **DNAT** tab.
- If you want to configure the order in which DNAT rules are applied on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device and in the displayed settings area, select the **Firewall settings** → **NAT** → **DNAT** tab and select the **Override** check box.

A table of DNAT rules is displayed.

2. Configure the order in which DNAT rules are applied by clicking the **Up** and **Down** buttons next to it.

3. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Editing a DNAT rule

You can edit a DNAT rule in a firewall template or on a CPE device. When you edit a DNAT rule in a firewall template, the rule is automatically modified on all CPE devices that are using the template.

To edit a DNAT rule:

1. Edit a DNAT rule in one of the following ways:

- If you want to edit a DNAT rule in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **NAT** → **DNAT** tab.
- If you want to edit a DNAT rule on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device and in the displayed settings area, select the **Firewall settings** → **NAT** → **DNAT** tab and select the **Override** check box.

A table of DNAT rules is displayed.

2. Click **Edit** next to the DNAT rule that you want to edit.
3. This opens a window; in that window, in the **Name** field, enter the name of the DNAT rule. Maximum length: 255 characters.
4. Specify the criteria according to which the firewall must apply the DNAT rule to traffic packets:
 - a. In the **Protocol** drop-down list, select the protocol of traffic packets to which the firewall must apply the DNAT rule:
 - **IP**
 - **TCP**
 - **UDP**
 - **#** for custom or non-standard protocol. If you select this value, in the displayed **Protocol number** field, enter the protocol number in accordance with the [IANA standard](#).
 - b. In the **Destination IP** field, enter the destination IPv4 address or prefix of traffic packets to which the firewall must apply the DNAT rule.
 - c. If you want to apply the DNAT rule only to traffic packets with the specified source zone, in the **Source zone** drop-down list, select a previously [created zone](#).
 - d. If in the **Protocol** drop-down list, you selected **TCP** or **UDP**, and you want to apply the DNAT rule only to traffic packets with the specified destination port, enter the port number in the **Destination port** field. Range of values: 1 to 65,535.
 - e. If you want to apply the DNAT rule only to traffic packets with the specified source IPv4 address or prefix, in the **Source IP** field, enter an IPv4 address or prefix.
5. Specify how the DNAT rule must modify traffic packets:
 - a. In the **Destination IP** field, enter a new IPv4 destination address or prefix.
 - b. In the **Destination zone** drop-down list, select a new previously created destination zone.
 - c. If in the **Protocol** drop-down list, you selected **TCP** or **UDP**, and you want to change the destination port number of traffic packets, enter a new port number in the **Destination port** field. Range of values: 1 to 65,535.
6. Click **Save**.
The DNAT rule is modified and updated in the table.
7. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Disabling or enabling a DNAT rule

You can disable or enable a DNAT rule in a firewall template or on a CPE device. When you disable or enable a DNAT rule in a firewall template, the rule is automatically disabled or enabled on all CPE devices that are using the template.

To disable or enable a DNAT rule:

1. Disable or enable a DNAT rule in one of the following ways:

- If you want to disable or enable a DNAT rule in a firewall template, go to the **SD-WAN → Firewall templates** menu section, click the template and in the displayed settings area, select the **NAT → DNAT** tab.
- If you want to disable or enable a DNAT rule on a CPE device, go to the **SD-WAN menu section → CPE**, click on the device, in the displayed settings area select the **Firewall settings → NAT → DNAT** tab and select the **Override** check box.

A table of DNAT rules is displayed.

2. Click **Disable** or **Enable** next to the DNAT rule that you want to disable or enable.

The DNAT rule is disabled or enabled.

3. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Deleting a DNAT rule

You can delete a DNAT rule in a firewall template or on a CPE device. When you delete a DNAT rule in a firewall template, the rule is automatically deleted on all CPE devices that are using the template.

Deleted DNAT rules cannot be restored.

To delete a DNAT rule:

1. Delete a DNAT rule in one of the following ways:

- If you want to delete a DNAT rule in a firewall template, go to the **SD-WAN → Firewall templates** menu section, click the template and in the displayed settings area, select the **NAT → DNAT** tab.
- If you want to delete a DNAT rule on a CPE device, go to the **SD-WAN → CPE** menu section, click the device and in the displayed settings area select the **Firewall settings → NAT → DNAT** tab and select the **Override** check box.

A table of DNAT rules is displayed.

2. Click **Delete** next to the DNAT rule that you want to delete.

3. In the confirmation window, click **Delete**.

The DNAT rule is deleted and is no longer displayed in the table.

4. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Managing SNAT rules

The table of SNAT rules is displayed in the firewall template and on the CPE device:

- To display the table of SNAT rules in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template, and in the displayed settings area, select the **NAT** → **SNAT** tab.
- To display the table of SNAT rule groups on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Firewall settings** → **NAT** → **SNAT** tab and select the **Override** check box.

Information about SNAT rules is displayed in the following table columns:

- **Name** is the name of the SNAT rule.
- **Outgoing** are criteria according to which the firewall must apply the SNAT rule to traffic packets.
- **Action** is the action that the SNAT rule must apply to traffic packets.

Creating a SNAT rule

You can create a SNAT rule in a firewall template or on a CPE device. When you create a SNAT rule in a firewall template, the rule is automatically created on all CPE devices that are using the template.

To create a SNAT rule:

1. Create a SNAT rule in one of the following ways:

- If you want to create a SNAT rule in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **NAT** → **SNAT** tab.
- If you want to create a SNAT rule on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device and in the displayed settings area, select the **Firewall settings** → **NAT** → **SNAT** tab and select the **Override** check box.

A table of SNAT rules is displayed.

2. Click **+ SNAT**.

3. This opens a window; in that window, in the **Name** field, enter the name of the SNAT rule. Maximum length: 255 characters.

4. Specify the criteria according to which the firewall must apply the SNAT rule to traffic packets:

a. In the **Protocol** drop-down list, select the protocol of traffic packets to which the firewall must apply the SNAT rule:

- **TCP**

- **UDP**

- b. In the **Destination zone** drop-down list, select the previously [created](#) destination zone of traffic packets to which the firewall must apply the SNAT rule.
- c. If you want to apply the SNAT rule only to traffic packets with the specified source IPv4 address or prefix, in the **Source IP** field, enter an IPv4 address or prefix.
- d. If you want to apply the SNAT rule only to traffic packets with the specified destination IPv4 address or prefix, in the **Destination IP** field, enter an IPv4 address or prefix.

5. In the **Action** drop-down list, select **SNAT**.

6. In the **SNAT IP** field, enter a new source IP address or prefix that the SNAT rule must specify for traffic packets.

7. Click **Create**.

The SNAT rule is created and displayed in the table.

8. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Configuring the order of SNAT rules

SNAT rules are applied to traffic packets in descending order, starting with the first rule at the top of the table. By default, SNAT rules are displayed in the table in the order of [creation](#). The earlier a rule was created, the higher it is displayed in the table.

You can configure the order in which SNAT rules are applied in a firewall template or on a CPE device. When you configure the order in which SNAT rules are applied in a firewall template, that order is automatically propagated to all CPE devices that are using the template.

To configure the order in which SNAT rules are applied:

1. Edit the order in which the SNAT rules are applied in one of the following ways:
 - If you want to configure the order in which SNAT rules are applied in a firewall template, go to the **SD-WAN → Firewall templates** menu section, click the template and in the displayed settings area, select the **NAT → SNAT** tab.
 - If you want to configure the order in which SNAT rules are applied on a CPE device, go to the **SD-WAN → CPE** menu section, click on the device, in the displayed settings area, select the **Firewall settings → NAT → SNAT** tab and select the **Override** check box.

A table of SNAT rules is displayed.

2. Configure the order in which SNAT rules are applied by clicking the **Up** and **Down** buttons next to it.

3. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Editing a SNAT rule

You can edit a SNAT rule in a firewall template or on a CPE device. When you edit a SNAT rule in a firewall template, the rule is automatically modified on all CPE devices that are using the template.

To edit a SNAT rule:

1. Edit a SNAT rule in one of the following ways:

- If you want to edit a SNAT rule in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **NAT** → **SNAT** tab.
- If you want to edit a SNAT rule on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device and in the displayed settings area, select the **Firewall settings** → **NAT** → **SNAT** tab and select the **Override** check box.

A table of SNAT rules is displayed.

2. Click **Edit** next to the SNAT rule that you want to edit.

3. This opens a window; in that window, in the **Name** field, enter the name of the SNAT rule. Maximum length: 255 characters.

4. Specify the criteria according to which the firewall must apply the SNAT rule to traffic packets:

a. In the **Protocol** drop-down list, select the protocol of traffic packets to which the firewall must apply the SNAT rule:

- **TCP**
- **UDP**

b. In the **Destination zone** drop-down list, select the previously [created](#) destination zone of traffic packets to which the firewall must apply the SNAT rule.

c. If you want to apply the SNAT rule only to traffic packets with the specified source IPv4 address or prefix, in the **Source IP** field, enter an IPv4 address or prefix.

d. If you want to apply the SNAT rule only to traffic packets with the specified destination IPv4 address or prefix, in the **Destination IP** field, enter an IPv4 address or prefix.

5. In the **Action** drop-down list, select **SNAT**.

6. In the **SNAT IP** field, enter a new source IP address or prefix that the SNAT rule must specify for traffic packets.

7. Click **Save**.

The SNAT rule is modified and displayed in the table.

8. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Disabling or enabling a SNAT rule

You can disable or enable a SNAT rule in a firewall template or on a CPE device. When you disable or enable a SNAT rule in a firewall template, the rule is automatically disabled or enabled on all CPE devices that are using the template.

To disable or enable a SNAT rule:

1. Disable or enable a SNAT rule in one of the following ways:

- If you want to disable or enable a SNAT rule in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **NAT** → **SNAT** tab.
- If you want to disable or enable a SNAT rule on a CPE device, go to the **SD-WAN menu section** → **CPE**, click on the device, in the displayed settings area select the **Firewall settings** → **NAT** → **SNAT** tab and select the **Override** check box.

A table of SNAT rules is displayed.

2. Click **Disable** or **Enable** next to the SNAT rule that you want to disable or enable.

The SNAT rule is disabled or enabled.

3. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Deleting a SNAT rule

You can delete a SNAT rule in a firewall template or on a CPE device. When you delete a SNAT rule in a firewall template, the rule is automatically deleted on all CPE devices that are using the template.

Deleted SNAT rules cannot be restored.

To delete a SNAT rule:

1. Delete a SNAT rule in one of the following ways:

- If you want to delete a SNAT rule in a firewall template, go to the **SD-WAN** → **Firewall templates** menu section, click the template and in the displayed settings area, select the **NAT** → **SNAT** tab.
- If you want to delete a SNAT rule on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device and in the displayed settings area, select the **Firewall settings** → **NAT** → **SNAT** tab and select the **Override** check box.

A table of SNAT rules is displayed.

2. Click **Delete** next to the SNAT rule that you want to delete.

3. In the confirmation window, click **Delete**.

The SNAT rule is deleted and is no longer displayed in the table.

4. In the upper part of the settings area, click **Save** to save the settings of the firewall template or CPE device.

Editing a CPE device firewall template

Editing a CPE device firewall template may result in loss of communication between the CPE device and devices connected to it, as well as the loss of relayed traffic packets.

To edit a CPE device firewall template:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device whose firewall template you want to edit.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays general information about the CPE device. This tab also displays the table of **Out-of-band management** tasks being performed by the orchestrator.

3. In the **Firewall template** drop-down list, select a previously [created firewall template](#).

4. In the upper part of the settings area, click **Save** to save CPE device settings.

Managing network services and virtualization of network functions

Network services

Network services relay traffic over the network and apply network functions to it, such as WAN optimization, shaping, and traffic protection. Each network service has a topology that you build using a graphical design tool. You can add components to a topology and connect the components to each other.

You need to build a topology in a network service template and then [assign that template to a tenant](#). Components added to the template topology are automatically assigned to the tenant together with the network service template. A tenant can create and deploy network services using assigned templates, and edit network services that are already deployed.

If you need to apply network functions from different network services to traffic, you can connect such network services to a shared network service.

You can use network services to deploy [SD-WAN instances](#). [Log into the self-service portal of the tenant](#) for which you want to deploy an SD-WAN instance, [create a network service](#), add [control plane](#) components to the topology of that network service, and [deploy the network service](#). The network service for deploying SD-WAN instances is called the SD-WAN network service (SD-WAN service).

An example of a network service topology is shown in the figure below.



Network service topology

Network function virtualization

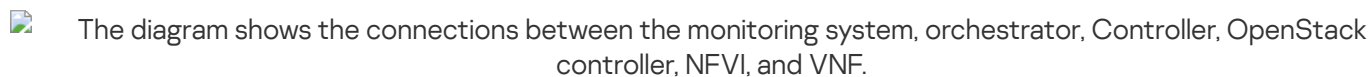
Network function virtualization (NFV) lets you use virtualized storage, compute resources, and networks to provide network functions and combine these functions into network services.

You can use [virtual network functions](#) (VNF) and [physical network functions](#) (PNF). The difference between virtual and physical network functions is that the physical network functions are deployed on dedicated hardware and do not use cloud resources.

Kaspersky SD-WAN complies with the architecture specified in the ETSI [NFV MANO specification](#) (NFV Management and Network Orchestration), which defines the following main functional components:

- [Orchestrator](#).
- [Virtual Network Function Managers \(VNFM\)](#).
- [Virtual Infrastructure Manager](#).
- The Zabbix monitoring system monitors the status of virtual and physical network functions and notifies the orchestrator when a network function needs to be restored or scaled.
- The NFV infrastructure consists of physical resources such as hardware storage, servers, and network devices.
- [SD-WAN Controller](#).

The figure below shows the relations between the solution components and the NFV infrastructure. Components of external solutions are marked in white, Kaspersky SD-WAN components are marked in green, and the red lines are connections between components.

 The diagram shows the connections between the monitoring system, orchestrator, Controller, OpenStack controller, NFVI, and VNF.

NFV infrastructure

Managing VNF and PNF packages







A *VNF* or *PNF* package is a ZIP archive in which you must place the following components to deploy a network function and manage its lifecycle:

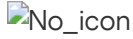
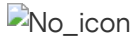
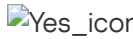


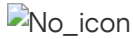
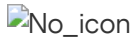
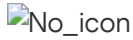
- The VNF/PNF descriptor is a file in the YAML format with parameters of the network function.
- The /image directory contains virtual machine images in the QCOW format for deploying the virtual network function. This directory is not included in the PNF package.
- The /scripts directory contains scripts for deploying and managing the network function.
- A PNG file to be used as the icon of the network function. This component is optional.
- A PDF file that contains technical documentation or specification of the virtual or physical network function. This component is optional.

You must upload the VNF or PNF package to the orchestrator web interface to add a virtual or physical network function to the topology when [managing a network service template](#) or [network service](#).

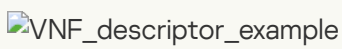
VNF descriptor

You can specify the following parameters and blocks in a VNF descriptor.

Value	Type	Mandatory	Description
name	Parameter		Name of the virtual network function.
description	Parameter		Brief description of the virtual network function.
provider	Parameter		Provider of the virtual network function.
version	Parameter		Version of the virtual network function.
description_file	Parameter		Name of the PDF file with the technical documentation or specification of the virtual network function. This file must be placed in the root directory of the VNF package. Users can view and download this file.
external_connections	Block		External connection points of the virtual network function. You can configure the specified external connection points of the

			virtual network function in the orchestrator web interface.
internal_connections	Block		Internal connection points of VDUs that are part of the virtual network function.
virtual_links	Block		Virtual links for connecting internal connection points. You must specify this block if you specified the internal_connections block.
images	Block		VDU disk images. You can deploy multiple VDUs using the same VDU disk image.
configurations	Block		Scripts for performing actions at various lifecycle stages of the virtual network function, for example, during deployment.
flavours	Block		Flavours of the virtual network function. You can select one of the specified flavours in the orchestrator web interface.
scaling	Block		Virtual network function scaling parameters.
user_configurations	Block		Additional tabs, fields, and drop-down lists that will be added to the settings area of the virtual network function .
backups	Block		Virtual network function backup tasks.

[VNF descriptor example](#)






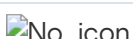


external_connections block

In the external_connections block, you can specify the names of external connection points using the following parameter:

- name

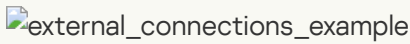
For each external connection point, you can specify the following parameters.

Value	Mandatory	Description
description		Brief description of the external connection point.
ip		IP address of the external connection point of the virtual network function.
mask		Subnet mask of the external connection point of the virtual network function.
gw		IP address of the gateway of the external connection point of the virtual network function.
dns		IP address of the DNS server of the external connection point of the virtual network function.
group		The group to which the external connection point of the virtual network function belongs. Mandatory parameter if multiple VDUs within the virtual network function use the same external connection point.

The following values can be specified for the `ip`, `mask`, `gw`, and `dns` settings:

- Enter a value manually — The IP address is assigned using DHCP via MAC-based reservation of an OpenStack port and cannot be changed.
- AUTO — The IP address is assigned automatically using an external DHCP server or scripts. Scripts can be specified in the `configurations_block`.
- MANUAL — You must specify the IP address manually.

[Example of an 'external_connections' block](#)

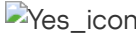
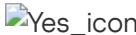


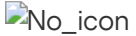




internal_connections block

In the `internal_connections` block, you can specify the names of internal connection points using the following parameter:

- `name`

For each internal connection point, you can specify the following parameters.

Value	Mandatory	Description
<code>description</code>		Brief description of the internal connection point.
<code>virtual_link_name</code>		The virtual link name of the internal connection point. Virtual links can be specified in the <code>virtual_links_block</code> .
<code>ip</code>		IP address of the internal connection point.
<code>mask</code>		Subnet mask of the internal connection point.
<code>gw</code>		IP address of the gateway of the internal connection point.
<code>dns</code>		IP address of the DNS server of the internal connection point.
<code>group</code>		The group to which the internal connection point belongs. Mandatory parameter if multiple VDUs within the virtual network function use the same internal connection point.

The following values can be specified for the `ip`, `mask`, `gw`, and `dns` settings:

- Enter a value manually — The IP address is assigned using DHCP via MAC-based reservation of an OpenStack port and cannot be changed.
- AUTO — The IP address is assigned automatically using an external DHCP server or scripts. Scripts can be specified in the `configurations_block`.

[Example of an 'internal_connections' block](#)



virtual_links block

In the `virtual_links` block, you can specify the names of virtual links using the following parameter:

- `name`

For each virtual link, you can specify the following parameters:

- `cidr`
IPv4 prefix of the virtual link.
- `ip_version`
Version of IP addresses in the subnet. Possible values: v4 and v6.

All parameters are mandatory.

[Example of a 'virtual_links' block](#)

A screenshot of a configuration block titled 'virtual_link_example' with a small icon to the left of the text.

images block

In the `images` block, you can specify the names of VDU disk images using the following parameter:

- `name`

For each VDU disk image, you can specify the following parameters:

- `container_format`
Container format of the VDU disk image.
- `disk_format`
Format of the VDU disk image.
- `type`
Type of the VIM, for example, OpenStack.
- `file_name`
File name of the VDU disk image. You must place the VDU disk image in the `/image` directory of the VNF package.

All parameters are mandatory.

[Example of an 'images' block](#)





A screenshot of a configuration block titled 'images_example' with a small icon to the left of the text.

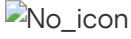
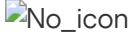
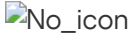
configurations block

In the configurations block, you can specify the names of scripts using the following parameter:


- name

For each script, you can specify the following parameters:

Value	Mandatory	Description
filename	 Yes	The file name of the script file, Ansible playbook, or user-data attribute for Cloud-init. You must place the script in the /scripts directory of the VNF package.
stage	 Yes	The stage of operation of the virtual network function at which the script must be run. Possible values: <ul style="list-style-type: none">• <code>initialization</code> to run the script on deployment of the virtual network function.• <code>termination</code> to run the script on deletion of the virtual network function.• <code>none</code> to run the script when the value in the field or drop-down list in the virtual network function settings area changes. You can specify the fields and drop-down lists in the user configurations block.
executor	 Yes	Interpreter. Possible values: <ul style="list-style-type: none">• <code>ansible</code>• <code>expect</code>• <code>/bin/sh</code>• <code>bin/bash</code>• <code>cloud-init</code> You can enter the path to a custom script executor, for example: <code>/user/bin/php</code>
authentication	 Yes	Method for authenticating the VNFM in the virtual network function for running scripts. Possible values: <ul style="list-style-type: none">• <code>key</code> means the VNFM is authenticated in the virtual network function using a key that is generated when the function is deployed. You need to use a script to get the key, so we recommend not to specify this value for the first script.• <code>password</code> means the VNFM is authenticated in the virtual network function using a user name and password. The user name and password can be specified in the flavours block inside the <code>vdus</code> block.

files_path		Path to files for running scripts using SSH. You need to create a directory inside the /scripts directory of the VNF package and place the files in that directory. The files are copied to the VDU.
config_drive		Whether or not you want to use config-drive. You can specify this parameter if you have specified cloud_init for the executor parameter. Possible values: true and false.
timeout		The time to wait for the script to finish, in seconds. If the script does not finish within the specified time, execution is terminated. You can specify this parameter if you have specified a path to a custom script executor for the executor parameter. The timeout starts at the moment the script is run.

[Example of a 'configurations' block [?]](#)

 configurations_example

flavours block

In the flavours block, you can specify the names of flavours by using the following parameter:

- name

For each flavour, you can specify the following parameters and blocks.

Value	Type	Description
description	Parameter	Brief description of the flavour.
position	Parameter	Sequential number of the flavour. The flavour with the lowest position has the lowest performance.
affinity	Block	Groups of VDUs that you want to be hosted on the same OpenStack host. We recommend hosting VDUs that require minimizing communication delays which each other on the same OpenStack host.
anti_affinity	Block	Groups of VDUs that you want to be hosted on distinct OpenStack hosts. We recommend deploying VDUs that may require vertical scaling or high availability on distinct OpenStack hosts.
management	Block	Parameters of VDU administration consoles.
vdus	Block	VDU settings.

All parameters and blocks are mandatory.

affinity and anti_affinity blocks

You can specify VDU groups using the following block:

groups

In this block, you can specify the names of VDU groups using the following parameter:

- name

For each VDU group, you can specify the VDU names using the following block:

vdu_name

[Example of 'affinity' and 'anti_affinity' blocks](#)

The image shows a screenshot of a configuration file or document. The text 'affinity_anti-affinity_example' is visible, indicating the content of the example block.

management block

In the management block, you can specify the following blocks:

- vnc

Parameters relevant to managing VDUs through the VNC console. You can specify VDU names using the following parameter:

- vdu_name

- ssh

Parameters relevant to managing VDUs through the SSH console. You can specify VDU names using the following parameter:

- vdu_name

For each VDU, you can specify the following parameters:

- def_user

Name of the user on whose behalf the SSH session is to be established.

- authentication

Method for authenticating the VNFM in the virtual network function for running scripts. Possible values:

- key means the VNFM is authenticated in the virtual network function using a key that is generated when the function is deployed. You need to get the key using a script. Scripts can be specified in the [configurations block](#).
- password means the VNFM is authenticated in the virtual network function using a user name and password. The user name and password can be specified in the vdu block.

All parameters are mandatory.

- web

Parameters relevant to managing VDUs through the web console. You can specify VDU names using the following parameter:

- vdu_name

For each VDU, you can specify the following parameters:

- protocol

Protocol for connecting to the web console. Possible values: http and https.

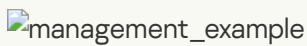
- port

Port for connecting to the web console. By default, port 80 is used. Range of values: 1 to 65,536.

- **path**
Path to the web console.
- **def_user**
User name for authenticating in the web console.
- **def_password**
Password for authenticating in the web console.

All parameters are optional.

[Example of a 'management' block ?](#)






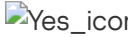
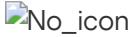
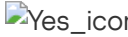





vdus block

In the `vdus` block, you can specify the names of VDUs using the following parameter:



- `name`


For each VDU, you can specify the following parameters and blocks:

Value	Type	Mandatory	Description
<code>password_rules</code>	Block	 No icon	<p>VDU password requirements. You can specify the following parameters:</p> <ul style="list-style-type: none">• length Minimum length of the password.• use_upper_case Whether users must use uppercase characters in their passwords. Possible values: <code>true</code> and <code>false</code>.• use_lower_case Whether users must use lowercase characters in the password. Possible values: <code>true</code> and <code>false</code>.• use_digits Whether users must use numeric characters in their passwords. Possible values: <code>true</code> and <code>false</code>.• specific_symbols Whether users must use special characters such as <code>\$</code> or <code>@</code> in the password.• specific_symbols_min_usage

			<p>Minimum number of special characters that must be present in the password.</p> <p>All parameters are optional.</p>
check_connection_mode	Parameter		Type of VDU availability test performed during deployment. Possible values: ssh and none. By default, an SSH test is performed.
zabbix_template	Parameter		Template for creating a host on Zabbix server corresponding to the virtual network function.
monitoring_type	Parameter		<p>Monitoring type of the virtual network function. Possible values:</p> <ul style="list-style-type: none"> • agent means monitoring using a Zabbix agent. • snmp means monitoring using the SNMP protocol.
ssh_port	Parameter		Port number for establishing an SSH session.
configurations	Block		Names of scripts to be run on the VDU. Scripts can be specified in the configurations block .
backups	Block		Names of backup tasks to be used on the VDU. Backup tasks can be specified under backups .
def_user	Parameter		User name for authenticating the VNFM in the virtual network function.
def_password	Parameter		Password for authenticating the VNFM in the virtual network function.
password_authentication	Parameter		Whether password authentication of the VNFM in the virtual network function is allowed. Possible values: yes and no.
disks	Block		<p>Names of the VDU virtual disks. You can specify the names using the following parameter:</p> <ul style="list-style-type: none"> - name <p>For each VDU disk, you can specify the following parameters:</p> <ul style="list-style-type: none"> • order Mounting order of the VDU virtual disk. Mandatory parameter. • type Type of the ephemeral OpenStack disk. Mandatory parameter. • image Name of the VDU virtual disk image. VDU virtual disk images can be specified in the images block. Optional parameter if you are creating a blank VDU disk. • storage_db

			Size of the VDU virtual disk in GB. Mandatory parameter.
cpu	Block		<p>VDU CPU parameters. You can specify the following parameters:</p> <ul style="list-style-type: none"> • smt Simultaneous multithreading requirements for VDU deployment. Possible values: <ul style="list-style-type: none"> • prefer to use simultaneous multithreading if it is enabled on the VDU host. • isolate to not use simultaneous multithreading. • require to use simultaneous multithreading. • cpu_pinning Whether you want to use CPU pinning. Possible values: <ul style="list-style-type: none"> • shared if you do not want to pin CPU cores to the VDU. • dedicated if you want to pin CPU cores to the VDU. • num_vpu Number of CPU cores pinned to the VDU. <p>All parameters are mandatory.</p>
memory	Block		<p>VDU RAM settings. You can specify the following parameters:</p> <ul style="list-style-type: none"> • total_memory_mb Amount of VDU RAM in MB. • page_size Size of memory pages when deploying the VDU. Possible values: <ul style="list-style-type: none"> • small for 4KB. • large for 2 MB or 1 GB. • any for any size. • 4KB • 2MB • 2048 • 1GB <p>All parameters are mandatory.</p>

network_interfaces	Block	 Yes_icon	<p>Network interface settings You can specify the names of network interface using the following parameter:</p> <ul style="list-style-type: none"> - name <p>For each network interface, you can specify the following parameters:</p> <ul style="list-style-type: none"> • type Type of the network interface. Mandatory parameter. Possible values: <ul style="list-style-type: none"> • data is a network interface for data transfer. • management is a management network interface that is mapped to a network port. • description Brief description of the network interface. Mandatory parameter. • connection_point_ref Names of external connection points of the management network interface. Mandatory parameter. You can specify external connection points in the external connections block. • port_security Whether you want to enable the Port security function. Optional parameter. Possible values: disabled and enabled. <p>If you need to specify the vNIC type of the network interface, you need to add the following block:</p> <pre>properties</pre> <p>In this block, you can specify the vNIC type using the following parameter:</p> <pre>vnic_type</pre> <p>Possible values:</p> <ul style="list-style-type: none"> • virtio • direct • macvtap • vhost
auto_healing	Block	 Yes_icon	<p>VDU auto-healing parameters. You can specify which external triggers must initiate VDU auto-healing using the following parameter:</p> <pre>triggers_set</pre>

			<p>Possible values:</p> <ul style="list-style-type: none"> • any to have any external trigger initiate VDU auto-healing. • all to initiate VDU auto-healing if all specified external triggers are triggered. • < trigger name > to initiate VDU auto-healing when the specified external trigger is triggered. <p>You can specify which external triggers must trigger to initiate VDU auto-healing using the following block:</p> <pre>triggers</pre> <p>In this block, you can specify the names of external triggers using the following parameter:</p> <ul style="list-style-type: none"> - name <p>Possible values:</p> <ul style="list-style-type: none"> • unreachable • scale_up • scale_down <p>You can specify the action that you want performed when an external trigger is triggered using the following block:</p> <pre>action_set</pre> <p>In this block, you can specify the action using the following parameter:</p> <ul style="list-style-type: none"> - type <p>Possible values:</p> <ul style="list-style-type: none"> • reprovision to reprovision the VDU. • reboot to restart the VDU. • script to run the specified script. When specifying this value, you must specify the name of the script using the following parameter: configuration_name_ref Scripts can be specified in the configurations block.
bootstrap_timeout	Parameter	 No_icon	SSH availability timeout during VDU deployment, in seconds. If the VDU is not available over SSH after the specified timeout expires, the deployment is rolled back.

[Example of a 'vdus' block](#)

scaling block

In the `scaling` block, you can specify the following blocks:

- `scale_in_status`
Whether horizontal scaling is allowed to a scaling option with a lower sequential number. Possible values are `permit` and `deny`.
- `scale_out_status`
Specifies whether horizontal scaling is allowed to a scaling option with a higher sequential number. Possible values are `permit` and `deny`.
- `scale_up_status`
Whether vertical scaling is allowed to a scaling option with a lower sequential number. Possible values are `permit` and `deny`.
- `scale_down_status`
Whether vertical scaling is allowed to a scaling option with a higher sequential number. Possible values are `permit` and `deny`.

All parameters are optional.

[Example of a 'scaling' block](#)

user_configurations block

You can specify the tabs that you want to be added to the [settings area of the virtual network function](#) using the following block:

tab

In this block, you can specify the names of tabs using the following parameter:

- `name`


For each tab, you can specify fields and drop-down lists using the following block:

variables

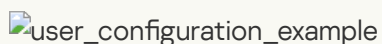
In this block, you can specify the names of fields and drop-down lists using the following parameter:

- `name`

For each field and drop-down list, you can specify the following parameters and blocks.

Value	Type	Mandatory	Description
description	Parameter		A brief description of the field or drop-down list.
input_type	Parameter		Whether you want to add a field or a drop-down list. Possible values: <ul style="list-style-type: none"> input to add a field. dropdown to add a drop-down list.
default_value	Parameter		Default value of the field. You can specify this parameter if you have specified input for the input_type parameter.
values	Block		The options that you want to be displayed in the drop-down list. You can specify this block if you have specified dropdown for the input_type parameter. You can specify the values using the following parameter: - value If you want to make one of the specified values the default, you must specify the following parameter after it: <code>is_default: true</code>
required	Parameter		Whether the field or drop-down list is required. Possible values: true and false.
type	Parameter		The type of the value that can be specified in the field or drop-down list, for example: <code>string</code>
example	Parameter		The tooltip to display when the value in a field or drop-down list changes.
update_configuration_name	Block		Names of the scripts to run when the value in a field or drop-down list changes. Scripts can be specified in the configurations block .

[Example of a 'user_configuration' block](#)



backups block

In the backups block, you can specify the names of backup tasks using the following parameter:

- name

For each backup task, you can specify the following parameters and blocks.

Value	Type	Description
description	Parameter	Brief description of the backup task.
backup	Block	<p>Backup parameters. You can specify the following parameters:</p> <ul style="list-style-type: none"> • path Path in the virtual network function directory where the files that you want to backup are located. • interval Backup interval. • store_config Number of backup copies to keep. • backup_type Type of backup. • authentication Method for authenticating the VNFM in the virtual network function for running scripts. Possible values: <ul style="list-style-type: none"> • key means the VNFM is authenticated in the virtual network function using a key that is generated when the function is deployed. You need to get the key using a script. Scripts can be specified in the configurations block. • password means the VNFM is authenticated in the virtual network function using a user name and password. The user name and password can be specified in the flavours block in the vdup block. • configuration_name_ref Name of the script that must be run before the backup begins. Scripts can be specified in the configurations block.
restore	Block	<p>Backup restoration parameters. You can specify the following parameters:</p> <ul style="list-style-type: none"> • path Path in the virtual network function directory where you want to place the restored files. • backup_type Type of backup. • authentication Method for authenticating the VNFM in the virtual network function for running scripts. Possible values: <ul style="list-style-type: none"> • key means the VNFM is authenticated in the virtual network function using a key that is generated when the function is deployed. You need to get the key using a script. Scripts can be specified in the configurations block. • password means the VNFM is authenticated in the virtual network function using a user name and password. The user name and password can be specified in the flavours block in the vdup block.

- | | |
|--|---|
| | <ul style="list-style-type: none">• <code>configuration_name_ref</code>
Name of the script that must be run after the restoration from backup begins. Scripts can be specified in the configurations block. |
|--|---|

All parameters and blocks are mandatory.

[Example of a 'backups' block](#)

 backups_example

Uploading a VNF or PNF package to the orchestrator web interface

To upload a VNF or PNF package to the orchestrator web interface:

1. In the menu, go to the **Catalog** section.
The network service management page is displayed.
2. In the upper part of the page, click **+ VNF** or **+ PNF**.
3. Select a VNF or PNF package.

The VNF or PNF is loaded into the orchestrator web interface and displayed in the **Catalog** pane.

Managing network service templates

A list of network service templates is displayed in the administrator portal in the **Infrastructure** section, in the **Catalog** pane on the **Templates** tab. Before managing network service templates, you must log in to the administrator portal.

Creating a network service template

To create a network service template:

1. In the menu, go to the **Catalog** section.
The network service management page is displayed.
2. In the upper part of the page, click **+ Template**.
The graphical design tool for building the topology is displayed.
3. Add components to the topology:
 - a. Drag components from the **Catalog** pane into the graphical design tool. This pane displays the following components:
 - Network service templates — when you add a network service template to a topology, the topology is constructed in accordance with the template.

- Shared network services — you must add a shared network service to the topology of network services that you want to connect to the shared network service. You can [specify a brief description of the shared network service in the topology](#).
- Virtual and physical network functions. The actions that you can perform on virtual and physical network functions in the topology are described in the [Managing virtual network functions in the topology](#) and [Managing physical network functions in the topology](#) sections.

b. Drag and drop connections from the **Links** tab into the graphical design tool. The following connections are displayed on this tab:

- **P2P** is the Point-to-Point transport service (P2P service). You can [configure a P2P service in the topology](#).
- **P2M** is the Point-to-Multipoint transport service (P2M service). You can [configure a P2M service in the topology](#).
- **M2M** is a Multipoint-to-Multipoint transport service (M2M service). You can [configure a M2M service in the topology](#).

The remaining links are relevant to network communication at the VIM level and are established between VNFs hosted by the OpenStack cloud platform:

- **OS shared** is the shared network through which the shared network service connects to network services. You can [configure a shared network in the topology](#).
- **OS vRouter** is the virtual L3 router. You can [configure a virtual router in the topology](#).
- **OS VLAN** is the VLAN for transmitting tagged L2 traffic of the 802.1Q standard You can [configure a VLAN in the topology](#).
- **OS VXLAN** is a VXLAN for tunneling. You can [configure a VXLAN in the topology](#).
- **OS flat** is the flat network for transmitting untagged L2 traffic You can [configure a flat network in the topology](#).

c. Select the **UNI** tab and drag CPE device [UNIs](#) to the graphical design tool. The tab displays two components, **UNI** and **WAN**. Both components designate abstract UNIs that the tenant must replace with real UNIs when [creating](#) or [editing a network service](#). The **WAN** component refers to UNIs that must be connected to the WAN.

You can [configure a UNI in the topology](#).

The components are added to the topology and displayed in the graphical design tool.

4. Connect the components added to the topology to each other:

- Click the link to which you want to connect a component.
- Click **Add leaf** to connect a component with the leaf role to the link. If you clicked a P2M service, you can click **Add root** to connect a component with the root role to the link.
- Click the component that you want to connect to the link. If you clicked a network function or shared network service, select the port to connect to in the displayed window.

The component is connected to the link, and a line is displayed between them in the topology. For example, the figure below shows the VLAN to which a virtual network function is connected.

Catalog_OS_VLAN_add_leaf

5. If you want to assign backup UNIs:

A backup UNI can be assigned only for UNIs which are connected to at least one link.

- a. Click the UNI for which you want to assign a backup UNI.
- b. Click **Reserve**.
- c. Click the UNI that you want to use as the backup.

The UNI is designated as the backup UNI, and a dotted line is displayed between the UNI, the backup UNI, and the connection to which the UNI is connected. For example, in the figure below, the WAN UNI is the backup interface for the UNI.

Catalog_backup_interface

6. To delete a component from the topology:

- a. Click the component that you want to remove from the topology.
- b. Click **Delete**.

The component is removed from the topology and is no longer displayed in the graphical design tool.

7. If you want to horizontally align the topology, click **Arrange**.

8. If you do not want to hide the descriptions of the added components in the topology, clear the **Description** check box. This check box is selected by default.

9. In the **Name** field, enter the name of the network service.

10. In the upper part of the graphical design tool, click **Save**.

The network service template is created and displayed in the **Catalog** pane, on the **Templates** tab.

Editing a network service template

When you edit a network service template, the changes are not applied to network services that have already been [created](#) and [deployed](#) using the template.

To edit a network service template:

1. In the menu, go to the **Catalog** section.
The network service management page is displayed.
2. In the **Catalog** pane, select the **Templates** tab.
A list of network service templates is displayed.
3. Click the network service template that you want to edit.

The graphical design tool for building the topology is displayed.

4. Add components to the topology:

a. Drag components from the **Catalog** pane into the graphical design tool. This pane displays the following components:

- Network service templates — when you add a network service template to a topology, the topology is constructed in accordance with the template.
- Shared network services — you must add a shared network service to the topology of network services that you want to connect to the shared network service. You can [specify a brief description of the shared network service in the topology](#).
- Virtual and physical network functions. The actions that you can perform on virtual and physical network functions in the topology are described in the [Managing virtual network functions in the topology](#) and [Managing physical network functions in the topology](#) sections.

b. Drag and drop connections from the **Links** tab into the graphical design tool. The following connections are displayed on this tab:

- **P2P** is the Point-to-Point transport service (P2P service). You can [configure a P2P service in the topology](#).
- **P2M** is the Point-to-Multipoint transport service (P2M service). You can [configure a P2M service in the topology](#).
- **M2M** is a Multipoint-to-Multipoint transport service (M2M service). You can [configure a M2M service in the topology](#).

The remaining links are relevant to network communication at the VIM level and are established between VNFs hosted by the OpenStack cloud platform:

- **OS shared** is the shared network through which the shared network service connects to network services. You can [configure a shared network in the topology](#).
- **OS vRouter** is the virtual L3 router. You can [configure a virtual router in the topology](#).
- **OS VLAN** is the VLAN for transmitting tagged L2 traffic of the 802.1Q standard. You can [configure a VLAN in the topology](#).
- **OS VXLAN** is a VXLAN for tunneling. You can [configure a VXLAN in the topology](#).
- **OS flat** is the flat network for transmitting untagged L2 traffic. You can [configure a flat network in the topology](#).

c. Select the **UNI** tab and drag CPE device **UNIs** to the graphical design tool. The tab displays two components, **UNI** and **WAN**. Both components designate abstract UNIs that the tenant must replace with real UNIs when [creating](#) or [editing a network service](#). The **WAN** component refers to UNIs that must be connected to the WAN.

You can [configure a UNI in the topology](#).

The components are added to the topology and displayed in the graphical design tool.

5. Connect the components added to the topology to each other:

- a. Click the link to which you want to connect a component.
- b. Click **Add leaf** to connect a component with the leaf role to the link. If you clicked a P2M service, you can click **Add root** to connect a component with the root role to the link.
- c. Click the component that you want to connect to the link. If you clicked a network function or shared network service, select the port to connect to in the displayed window.

The component is connected to the link, and a line is displayed between them in the topology. For example, the figure below shows the VLAN to which a virtual network function is connected.

Catalog_OS_VLAN_add_leaf

6. If you want to assign backup UNIs:

A backup UNI can be assigned only for UNIs which are connected to at least one link.

- a. Click the UNI for which you want to assign a backup UNI.
- b. Click **Reserve**.
- c. Click the UNI that you want to use as the backup.

The UNI is designated as the backup UNI, and a dotted line is displayed between the UNI, the backup UNI, and the connection to which the UNI is connected. For example, in the figure below, the WAN UNI is the backup interface for the UNI.

Catalog_backup_interface

7. To delete a component from the topology:

- a. Click the component that you want to remove from the topology.
- b. Click **Delete**.

The component is removed from the topology and is no longer displayed in the graphical design tool.

8. If you want to horizontally align the topology, click **Arrange**.

9. If you do not want to hide the descriptions of the added components in the topology, clear the **Description** check box. This check box is selected by default.

10. In the **Name** field, enter the name of the network service.

11. In the upper part of the graphical design tool, click **Save**.

The network service template is modified and updated in the **Templates** tab.

Deleting a network service template

Deleted network service templates cannot be restored.

To delete a network service template:

1. In the menu, go to the **Catalog** section.

The network service management page is displayed.

2. In the **Catalog** pane, select the **Templates** tab.

A list of network service templates is displayed.

3. Click the delete icon next to the network service template that you want to delete.

4. In the confirmation window, click **Delete**.

The network service template is deleted and is no longer displayed in the **Templates** tab.

Managing network services

The list of network services is displayed in the self-service portal in the **Infrastructure** section, on the **Network services** pane. Before managing network services, you must [log in to the tenant's self-service portal](#).

Creating a network service

To create a network service:

1. In the menu, go to the **Catalog** section.

The network service management page is displayed.

2. In the upper part of the **Network services** pane, click **+ Network service**.

The graphical design tool for building the topology is displayed.

3. Add components to the topology:

a. Drag components from the **Catalog** pane into the graphical design tool. This pane displays the following components:

- Network service templates — when you add a network service template to a topology, the topology is constructed in accordance with the template.
- Shared network services — you must add a shared network service to the topology of network services that you want to connect to the shared network service. You can [specify a brief description of the shared network service in the topology](#).
- Virtual and physical network functions. The actions that you can perform on virtual and physical network functions in the topology are described in the [Managing virtual network functions in the topology](#) and [Managing physical network functions in the topology](#) sections.

b. Drag and drop connections from the **Links** tab into the graphical design tool. The following connections are displayed on this tab:

- **P2P** is the Point-to-Point transport service (P2P service). You can [configure a P2P service in the topology](#).
- **P2M** is the Point-to-Multipoint transport service (P2M service). You can [configure a P2M service in the topology](#).

- **M2M** is a Multipoint-to-Multipoint transport service (M2M service). You can [configure a M2M service in the topology](#).

The remaining links are relevant to network communication at the VIM level and are established between VNFs hosted by the OpenStack cloud platform:

- **OS shared** is the shared network through which the shared network service connects to network services. You can [configure a shared network in the topology](#).
- **OS vRouter** is the virtual L3 router. You can [configure a virtual router in the topology](#).
- **OS VLAN** is the VLAN for transmitting tagged L2 traffic of the 802.1Q standard. You can [configure a VLAN in the topology](#).
- **OS VXLAN** is a VXLAN for tunneling. You can [configure a VXLAN in the topology](#).
- **OS flat** is the flat network for transmitting untagged L2 traffic. You can [configure a flat network in the topology](#).

c. Select the **UNI** tab and drag CPE device **UNIs** to the graphical design tool. If you are using a network service template, you must replace the abstract UNIs in the topology with real UNIs. Abstract UNIs can be designated by two components, **UNI** and **WAN**. The **WAN** component refers to UNIs that must be connected to the WAN.

You can [configure a UNI in the topology](#).

4. Connect the components added to the topology to each other:

- Click the link to which you want to connect a component.
- Click **Add leaf** to connect a component with the leaf role to the link. If you clicked a P2M service, you can click **Add root** to connect a component with the root role to the link.
- Click the component that you want to connect to the link. If you clicked a network function or shared network service, select the port to connect to in the displayed window.

The component is connected to the link, and a line is displayed between them in the topology. For example, the figure below shows the VLAN to which a virtual network function is connected.

Catalog_OS_VLAN_add_leaf

5. If you want to assign backup UNIs:

A backup UNI can be assigned only for UNIs which are connected to at least one link.

- Click the UNI for which you want to assign a backup UNI.
- Click **Reserve**.
- Click the UNI that you want to use as the backup.

The UNI is designated as the backup UNI, and a dotted line is displayed between the UNI, the backup UNI, and the connection to which the UNI is connected. For example, in the figure below, the WAN UNI is the backup interface for the UNI.

Catalog_backup_interface

6. To remove a component from the topology:
 - a. Click the component that you want to remove from the topology.
 - b. Click **Delete**.

The component is removed from the topology and is no longer displayed in the graphical design tool.

7. If you want to horizontally align the topology, click **Arrange**.
8. If you do not want to hide the descriptions of the added components in the topology, clear the **Description** check box. This check box is selected by default.
9. In the **Name** field, enter the name of the network service.
10. Finish creating the network service in one of the following ways:
 - To save the network service, click **Save**.
 - To save and deploy the network service, click **Deploy**.

The network service is created and displayed in **Network services** pane. If you clicked **Deploy**, the deployment of the network service begins, which may take several minutes. You can interrupt the deployment by clicking **Abort deploy**.

Editing a network service

To edit a network service:

1. In the menu, go to the **Catalog** section.

The network service management page is displayed.
2. In the **Network services** pane, select the network service that you want to edit.

The graphical design tool for building the topology is displayed.
3. In the upper part of the graphical design tool, click **Edit**.
4. Add components to the topology:
 - a. Drag components from the **Catalog** pane into the graphical design tool. This pane displays the following components:
 - Network service templates — when you add a network service template to a topology, the topology is constructed in accordance with the template.
 - Shared network services — you must add a shared network service to the topology of network services that you want to connect to the shared network service. You can [specify a brief description of the shared network service in the topology](#).
 - Virtual and physical network functions. The actions that you can perform on virtual and physical network functions in the topology are described in the [Managing virtual network functions in the topology](#) and [Managing physical network functions in the topology](#) sections.

b. Drag and drop connections from the **Links** tab into the graphical design tool. The following connections are displayed on this tab:

- **P2P** is the Point-to-Point transport service (P2P service). You can [configure a P2P service in the topology](#).
- **P2M** is the Point-to-Multipoint transport service (P2M service). You can [configure a P2M service in the topology](#).
- **M2M** is a Multipoint-to-Multipoint transport service (M2M service). You can [configure a M2M service in the topology](#).

The remaining links are relevant to network communication at the VIM level and are established between VNFs hosted by the OpenStack cloud platform:

- **OS shared** is the shared network through which the shared network service connects to network services. You can [configure a shared network in the topology](#).
- **OS vRouter** is the virtual L3 router. You can [configure a virtual router in the topology](#).
- **OS VLAN** is the VLAN for transmitting tagged L2 traffic of the 802.1Q standard You can [configure a VLAN in the topology](#).
- **OS VXLAN** is a VXLAN for tunneling. You can [configure a VXLAN in the topology](#).
- **OS flat** is the flat network for transmitting untagged L2 traffic You can [configure a flat network in the topology](#).

c. Select the **UNI** tab and drag CPE device [UNIs](#) to the graphical design tool. If you are using a network service template, you must replace the abstract UNIs in the topology with real UNIs. Abstract UNIs can be designated by two components, **UNI** and **WAN**. The **WAN** component refers to UNIs that must be connected to the WAN.

You can [configure a UNI in the topology](#).

5. Connect the components added to the topology to each other:

- a. Click the link to which you want to connect a component.
- b. Click **Add leaf** to connect a component with the leaf role to the link. If you clicked a P2M service, you can click **Add root** to connect a component with the root role to the link.
- c. Click the component that you want to connect to the link. If you clicked a network function or shared network service, select the port to connect to in the displayed window.

The component is connected to the link, and a line is displayed between them in the topology. For example, the figure below shows the VLAN to which a virtual network function is connected.

Catalog_OS_VLAN_add_leaf

6. If you want to assign backup UNIs:

A backup UNI can be assigned only for UNIs which are connected to at least one link.

- a. Click the UNI for which you want to assign a backup UNI.

b. Click **Reserve**.

c. Click the UNI that you want to use as the backup.

The UNI is designated as the backup UNI, and a dotted line is displayed between the UNI, the backup UNI, and the connection to which the UNI is connected. For example, in the figure below, the WAN UNI is the backup interface for the UNI.

Catalog_backup_interface

7. To remove a component from the topology:

a. Click the component that you want to remove from the topology.

b. Click **Delete**.

The component is removed from the topology and is no longer displayed in the graphical design tool.

8. If you want to horizontally align the topology, click **Arrange**.

9. If you do not want to hide the descriptions of the added components in the topology, clear the **Description** check box. This check box is selected by default.

10. In the **Name** field, enter the name of the network service.

11. Finish editing the network service in one of the following ways:

- If you are editing a network service that is not deployed, do one of the following:
 - To save the network service, click **Save**.
 - To save and deploy the network service, click **Deploy**.
- If you are editing a deployed network service, click **Deploy changes** to deploy your changes.

The network service is modified and updated in **Network services** pane. If you clicked **Deploy** or **Deploy changes**, deployment begins, which may take several minutes. You can interrupt the deployment by clicking **Abort deploy**.

Deploying a network service

If a virtual network function deployed on a uCPE device is added to the network service topology and there is connectivity between the orchestrator and the uCPE device, the network service is deployed when connectivity is restored.

To deploy a network service:

1. In the menu, go to the **Catalog** section.

The network service management page is displayed.

2. In the **Network services** pane, select the network service that you want to deploy.

The graphical design tool for building the topology is displayed.

3. In the upper part of the graphical design tool, click **Edit**.

4. Click **Deploy**.

This starts the deployment of the network service, which may take several minutes. You can interrupt the deployment by clicking **Abort deploy**.

Checking the consistency of a network service

The *consistency check* allows confirming that the components that are added to the network service topology actually exist.

To check the consistency of a network service:

1. In the menu, go to the **Catalog** section.

The network service management page is displayed.

2. In the **Network services** pane, click the settings icon → **Check consistency** next to the network service whose consistency you want to check.

3. In the confirmation window, click **Confirm**.

This begins the consistency check of the network service.

Redeploying a network service

Redeploying a network service may result in short-term interruptions or temporary inoperability. When planning redeployment activities, we recommend taking into account your organization's circumstances to minimize the disruptions.

To redeploy a network service:

1. In the menu, go to the **Catalog** section.

The network service management page is displayed.

2. In the **Network services** pane, click the settings icon → **Redeploy** next to the network service that you want to redeploy.

3. In the confirmation window, click **Confirm**.

This starts the redeployment of the network service, which may take several minutes. You can interrupt the deployment by clicking **Abort deploy**.

Disabling or enabling auto-healing for a network service

The Zabbix server [monitors](#) network service components and sends a REST API request to the orchestrator whenever a problem is detected. If the auto-healing functionality is enabled for the network service, the orchestrator initiates auto-healing for components with problems. By default, this functionality is enabled.


To disable or enable auto-healing for a network service:

1. In the menu, go to the **Catalog** section.

The network service management page is displayed.

2. In the **Network services** pane, click the settings icon → **Disable Auto-Healing** or **Enable Auto-Healing** next to the network service for which you want to disable or enable auto-healing.

Auto-healing is disabled or enabled for the network service.

Even if auto-healing is disabled for the network service, you can perform [auto-healing of virtual network functions added to the topology of the network service or VDUs that are part of the VNFs](#) .

You can auto-heal a virtual network function or a VDU that is part of it, even if you have [disabled auto-healing of the network service](#) to whose topology this function has been added.

To auto-heal a virtual network function or a VDU that is part of it:

1. On the self-service portal, go to the **Catalog** menu section.

The network service management page is displayed.

2. In the **Network services** pane, click the previously [deployed network service](#) to whose topology the virtual network function has been added.

The topology is displayed.

3. Click the virtual network function.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.

4. If you want to auto-heal the virtual network function, in the upper part of the settings area, click **Management** → **Healing VNF**.

5. If you want to auto-heal a VDU that is part of the virtual network function:

a. Select the **VDU management** tab.

A table of VDUs is displayed.

b. Click **Management** → **Healing VNF** next to the VDU that you want to auto-heal.

6. In the confirmation window, click **Apply**.

Auto-healing of the virtual network function or a VDU that is part of it begins.

Viewing the network service log

To view the log of a network service:

1. In the menu, go to the **Catalog** section.

The network service management page is displayed.

2. In the **Network services** pane, click the settings icon → **Open log** next to the network service whose log you want to view.

The page with the network service log is displayed.

Deleting a network service

Deleted network services cannot be restored.

To delete a network service:

1. In the menu, go to the **Catalog** section.
The network service management page is displayed.
2. In the **Network services** pane, click the settings icon → **Delete** next to the network service that you want to delete.
3. In the confirmation window, click **Delete**.

The network service is deleted and is no longer displayed in the **Network services** pane.

Specifying a brief description of a shared network service in the topology

To specify a brief description of a shared network service in a network service topology:

1. Navigate to the topology in one of the following ways:
 - Start [creating](#) or [editing a network service template](#).
 - Start [creating](#) or [editing a network service](#).
2. In the graphical design tool, click the shared network service for which you want to specify a brief description.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Settings** tab is selected, which displays a brief description of the shared network service.
3. In the **Description** field, enter a brief description of the shared network service.
4. In the upper part of the settings area, click **Save** to save shared network service settings.

Managing virtual network functions in the topology

To manage a virtual network function, click it in the topology when performing the following actions:

- When [creating](#) or [editing a network service template](#)
- When [creating](#) or [editing a network service](#)

Virtual network function settings are displayed on the following tabs:

- **Flavours** contains flavours of the virtual network function.

- **Connection points** contains external connection points of the virtual network function.
- **VNF settings** contains basic settings of the virtual network function.
- **Placement** contains placement settings of the virtual network function. You can place a virtual network function in a [data center](#) or on a uCPE device. This tab is displayed if you clicked the virtual network function when creating or editing a network service.

The following tabs are displayed if you clicked the virtual network function in the topology of a [deployed network service](#):

- **VDU management** is a table of VDUs that are part of the virtual network function. Information about VDUs is displayed in the following columns of the table:
 - **Name** is the name of the VDU.
 - **Instance name** is the ID of the VDU instance.
 - **Mgmt IP** is the IP address that the [management subnet](#) has assigned to the VDU.
 - **vCPU** is the number of virtual CPU cores assigned to the VDU.
 - **RAM** is the amount of RAM assigned to the VDU.
 - **Disk** is the amount of disk space assigned to the VDU.
- **Monitoring** contains [monitoring results of the virtual network function](#).
- **Problems** contains [problems that occurred during the operation of the virtual network function](#). In case of any problems, a red exclamation mark is displayed next to the tab.

Additional tabs may be displayed if you specified any in the [VNF descriptor](#) in the [user configurations block](#).

Selecting the flavour of a virtual network function

You can specify flavours in the [VNF descriptor](#) in the [flavours block](#).

To select a virtual network function flavour:

1. Navigate to the topology in one of the following ways:
 - Start [creating](#) or [editing a network service template](#).
 - Start [creating](#) or [editing a network service](#).
2. In the topology, click the virtual network function for which you want to select a deployment option.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.
3. Select a flavour for the virtual network function.
4. In the upper part of the settings area, click **Save** to save virtual network function settings.

Configuring external connection points of a virtual network function

You can specify external connection points of a virtual network function in the [VNF descriptor](#), in the [external connections block](#).

To configure external connection points of the virtual network function:

1. Navigate to the topology in one of the following ways:
 - Start [creating](#) or [editing a network service template](#).
 - Start [creating](#) or [editing a network service](#).
2. In the topology, click the virtual network function for which you want to configure external connection points.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.
3. Select the **Connection points** tab.
This displays the external connection points of the virtual network function.
4. In the **Type** drop-down list, select how you want to assign an IPv4 prefix to the external connection point:
 - **DHCP reservation** to use DHCP to assign an IPv4 prefix to the external mount point. If you select this option, do the following:
 - a. In the **IP** field, enter the IPv4 address that DHCP must assign to the external connection point.
 - b. In the **Mask** field, enter the subnet mask that DHCP must assign to the external connection point.
 - **AUTO** to automatically assign an IPv4 prefix to the external connection point. Default value.
5. In the **Description** field, enter a brief description of the external connection point.
6. If you want to designate the connection point as the trunk port, select the **Trunk** check box. This check box is cleared by default.
7. In the upper part of the settings area, click **Save** to save virtual network function settings.

Basic settings of a virtual network function

To edit basic settings of the virtual network function:

1. Navigate to the topology in one of the following ways:
 - Start [creating](#) or [editing a network service template](#).
 - Start [creating](#) or [editing a network service](#).
2. In the topology, click the virtual network function for which you want to configure basic settings.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.

3. Select the **VNF settings** tab.

Basic settings of the virtual network function are displayed.

4. In the **Name** field, enter the name of the virtual network function.

5. In the **Description** field, enter a brief description of the virtual network function.

6. In the **Order** field, enter the sequence number for deploying the virtual network function on the OpenStack cloud platform. When you [deploy a network service](#), the virtual network function with the lowest number is the first to be deployed. If none of the virtual network functions added to the network service topology have a sequence number specified, all virtual network functions are deployed simultaneously.

7. In the upper part of the settings area, click **Save** to save virtual network function settings.

Hosting the virtual network function in a data center and on a uCPE device

To place a virtual network function in a data center or on a uCPE device.

1. Navigate to the topology by starting to [create](#) or [edit a network service](#).

2. In the topology, click on the virtual network function that you want to place in a data center or on a uCPE device.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.

3. Select the **Placement** tab.

Placement settings of the virtual network function are displayed.

4. In the **Select placement type** list, select one of the following values:

- **Data center** to place the virtual network function in the specified data center. If you select this option, do the following:
 - a. In the **Data center** field, enter the name of a previously [created data center](#). As you type the name, you are prompted to select a data center from a drop-down list.
 - b. In the **VIM** field, enter the name of a previously deployed VIM for the VNF. As you type the name, you are prompted to select a VIM from a drop-down list.
- **uCPE** to place the VNF on the specified uCPE device. If you select this option, in the **uCPE** field, enter the name of the uCPE device. As you type the name, you are prompted to select a name from a drop-down list.

5. In the upper part of the settings area, click **Save** to save virtual network function settings.

Stopping or starting a virtual network function or a VDU that is part of it

You can stop a virtual network function or a VDU that is part of it to free up the computational resources of the OpenStack cloud platform. When you start a virtual network function or VDU, it begins consuming computational resources again. Processes running on a virtual network function or VDU are restarted.

To stop or start a virtual network function or a VDU that is part of it:

1. On the self-service portal, go to the **Catalog** menu section.
The network service management page is displayed.
2. In the **Network services** pane, click the previously [deployed network service](#) to whose topology the virtual network function has been added.
The topology is displayed.
3. Click the virtual network function.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.
4. If you want to stop or start the virtual network function, in the upper part of the settings area, click the **Management** → **Power** → **Stop VNF** or **Start VNF**.
5. If you want to stop or start a VDU that is part of the virtual network function:
 - a. Select the **VDU management** tab.
A table of VDUs is displayed.
 - b. Click **Management** → **Power** → **Stop VDU** or **Start VDU** next to the VDU that you want to stop or start.
6. In the confirmation window, click **Apply**.
The virtual network function or its VDU is stopped or started.

Pausing or unpausing a virtual network function or a VDU that is part of it

You can pause a virtual network function or a VDU that is part of it to pause processes running on it. However, the virtual network function or VDU continues to consume the computational resources of the OpenStack cloud platform. When you unpauses a virtual network function or VDU, processes running on it are resumed.

To pause or unpauses a virtual network function or a VDU that is part of it:

1. On the self-service portal, go to the **Catalog** menu section.
The network service management page is displayed.
2. In the **Network services** pane, click the previously [deployed network service](#) to whose topology the virtual network function has been added.
The topology is displayed.
3. Click the virtual network function.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.
4. If you want to pause or unpauses a virtual network function, in the upper part of the settings area, click **Management** → **Pause VNF** → **Power** or **Unpause VNF**.

5. If you want to pause or unpaue a VDU that is part of the virtual network function:

a. Select the **VDU management** tab.

A table of VDUs is displayed.

b. Click **Management** → **Power** → **Pause VDU** or **Unpause VDU**.

6. In the confirmation window, click **Apply**.

The virtual network function or its VDU is paused or unpaused.

Suspending or unsuspending a virtual network function or a VDU that is part of it

You can suspend a virtual network function or a VDU that is part of it to free up the computational resources of the OpenStack cloud platform. This saves the state of the virtual network function or VDU to the disk of the OpenStack virtual platform. When you unsuspend the virtual network function or VDU, it begins consuming computational resources again. Processes running on a virtual network function or VDU are resumed from the point at which its state was saved.

To suspend or unsuspend a virtual network function or a VDU that is part of it:

1. On the self-service portal, go to the **Catalog** menu section.

The network service management page is displayed.

2. In the **Network services** pane, click the previously [deployed network service](#) to whose topology the virtual network function has been added.

The topology is displayed.

3. Click the virtual network function.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.

4. If you want to suspend or resume a virtual network function, in the upper part of the settings area, click **Management** → **Suspend VNF** → **Power** or **Resume suspended VNF**.

5. If you want to suspend or unsuspend a VDU that is part of the virtual network function:

a. Select the **VDU management** tab.


A table of VDUs is displayed.

b. Click **Management** → **Power** → **Suspend VDU** or **Resume suspended VDU** next to the VDU that you want to suspend or reactivate.

6. In the confirmation window, click **Apply**.

The virtual network function or its VDU is suspended or unsuspending.

Soft rebooting a virtual network function or a VDU that is part of it

When a virtual network function is soft rebooted, all active VDUs in it are restarted. To soft reboot a virtual network function, at least one VDU in it must be in the [active state](#) .

You can suspend a virtual network function or a VDU that is part of it to free up the computational resources of the OpenStack cloud platform. This saves the state of the virtual network function or VDU to the disk of the OpenStack virtual platform. When you unsuspend the virtual network function or VDU, it begins consuming computational resources again. Processes running on a virtual network function or VDU are resumed from the point at which its state was saved.

To suspend or unsuspend a virtual network function or a VDU that is part of it:

1. On the self-service portal, go to the **Catalog** menu section.

The network service management page is displayed.

2. In the **Network services** pane, click the previously [deployed network service](#) to whose topology the virtual network function has been added.

The topology is displayed.

3. Click the virtual network function.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.

4. If you want to suspend or resume a virtual network function, in the upper part of the settings area, click **Management** → **Suspend VNF** → **Power** or **Resume suspended VNF**.

5. If you want to suspend or unsuspend a VDU that is part of the virtual network function:

- a. Select the **VDU management** tab.

A table of VDUs is displayed.

- b. Click **Management** → **Power** → **Suspend VDU** or **Resume suspended VDU** next to the VDU that you want to suspend or reactivate.

6. In the confirmation window, click **Apply**.

The virtual network function or its VDU is suspended or unsuspended.

To perform a soft reboot of a virtual network function or a VDU that is part of it:

1. On the self-service portal, go to the **Catalog** menu section.

The network service management page is displayed.

2. In the **Network services** pane, click the previously [deployed network service](#) to whose topology the virtual network function has been added.

The topology is displayed.

3. Click the virtual network function.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.

4. If you want to perform a soft reboot of the virtual network function, in the upper part of the settings area, click **Management** → **Power** → **Soft reboot VNF**.

5. If you want to soft reboot a VDU that is part of the virtual network function:

a. Select the **VDU management** tab.

A table of VDUs is displayed.

b. Click **Management** → **Power** → **Soft reboot VDU** next to the VDU that you want to soft reboot.

6. In the confirmation window, click **Apply**.

The virtual network function or its VDU is soft rebooted.

Hard rebooting of a virtual network function or a VDU that is part of it

A hard reboot simulates turning power on and off again. We recommend that performing a hard reboot only if [soft reboot](#) is not successful.

To perform a hard reboot of a virtual network function or a VDU that is part of it:

1. On the self-service portal, go to the **Catalog** menu section.

The network service management page is displayed.

2. In the **Network services** pane, click the previously [deployed network service](#) to whose topology the virtual network function has been added.

The topology is displayed.

3. Click the virtual network function.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.

4. If you want to perform a hard reboot of the virtual network function, in the upper part of the settings area, click **Management** → **Power** → **Hard reboot VNF**.

5. If you want to hard reboot a VDU that is part of the virtual network function:

a. Select the **VDU management** tab.

A table of VDUs is displayed.

b. Click **Management** → **Power** → **Hard reboot VDU** next to the VDU that you want to hard reboot.

6. In the confirmation window, click **Apply**.

A hard reboot of the VNF or its VDU is performed.

Redeploying a virtual network function or a VDU that is part of it

Redeployment of a virtual network function or a VDU that is part of it may result in short-term interruptions or temporary loss of function. When planning and coordinating redeployment activities, we recommend taking into account your organization's circumstances to minimize the disruptions.

To redeploy a virtual network function or a VDU that is part of it:

1. On the self-service portal, go to the **Catalog** menu section.
The network service management page is displayed.
2. In the **Network services** pane, click the previously [deployed network service](#) to whose topology the virtual network function has been added.
The topology is displayed.
3. Click the virtual network function.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.
4. If you want to redeploy the virtual network function, at the top of the configuration area, click **Management** → **Redeploy VNF**.
5. If you want to redeploy a VDU that is part of the virtual network function:
 - a. Select the **VDU management** tab.
A table of VDUs is displayed.
 - b. Click **Management** → **Healing VDU** next to the VDU that you want to redeploy.
6. In the confirmation window, click **Confirm**.

Redeployment of the virtual network function or its VDU begins, which may take several minutes. You can interrupt the deployment by clicking **Abort deploy**.

Auto-healing a virtual network function or a VDU that is part of it

You can auto-heal a virtual network function or a VDU that is part of it, even if you have [disabled auto-healing of the network service](#) to whose topology this function has been added.

To auto-heal a virtual network function or a VDU that is part of it:

1. In the self-service portal, go to the **Catalog** menu section.
The network service management page is displayed.
2. In the **Network services** pane, click the previously [deployed network service](#) to whose topology the virtual network function has been added.
The topology is displayed.
3. Click the virtual network function.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.
4. If you want to auto-heal the virtual network function, in the upper part of the settings area, click **Management** → **Healing VNF**.
5. If you want to auto-heal a VDU that is part of the virtual network function:
 - a. Select the **VDU management** tab.
A table of VDUs is displayed.

b. Click **Management** → **Healing VNF** next to the VDU that you want to auto-heal.

6. In the confirmation window, click **Apply**.

Auto-healing of the virtual network function or a VDU that is part of it begins.

Managing VDU snapshots

To display the table of VDU snapshots, click the virtual network function in the topology of the [deployed network service](#), select the **VDU management** tab, and click **Management** → **Snapshot** next to the VDU.

Information about VDU snapshots is displayed in the following columns of the table:

- **Name** is the name of the VDU snapshot.
- **Created at** is the date and time when the VDU snapshot was created.
- **Size** is the size of the VDU snapshot.
- **Description** is a brief description of the VDU snapshot.
- **Management** contains actions that can be performed on the VDU snapshot.

Creating a VDU snapshot

We do not recommend storing snapshots for a long time because their existence reduces the performance of the VDU.

To take a VDU snapshot:

1. In the self-service portal, go to the **Catalog** menu section.

The network service management page is displayed.

2. In the **Network services** pane, click the previously [deployed network service](#) to whose topology the virtual network function has been added.

The topology is displayed.

3. Click the virtual network function that includes the VDU.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.

4. Select the **VDU management** tab.

A table of VDUs is displayed.

5. Click **Power** → **Snapshot** next to the VDU for which you want to create a snapshot.

This opens a window with the table of VDU snapshots.

6. In the **Name** field, enter a name for the VDU snapshot.

7. In the **Description** field, enter a brief description of the VDU snapshot.

8. Click **Create**.

A snapshot of the VDU is created and displayed in the table.

Restoring VDU settings using a snapshot

To restoring VDU settings using a snapshot:

1. In the self-service portal, go to the **Catalog** menu section.

The network service management page is displayed.

2. In the **Network services** pane, click the previously [deployed network service](#) to whose topology the virtual network function has been added.

The topology is displayed.

3. Click the virtual network function that includes the VDU.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.

4. Select the **VDU management** tab.

A table of VDUs is displayed.

5. Click **Power** → **Snapshot** next to the VDU whose settings you want to restore using the snapshot.

This opens a window with the table of VDU snapshots.

6. Click **Management** → **Revert** next to the snapshot which you want to use to restore the VDU settings.

7. In the confirmation window, click **Revert**.

The VDU settings are restored in accordance with the snapshot.

Editing a VDU snapshot

To edit a VDU snapshot:

1. In the self-service portal, go to the **Catalog** menu section.

The network service management page is displayed.

2. In the **Network services** pane, click the previously [deployed network service](#) to whose topology the virtual network function has been added.

The topology is displayed.

3. Click the virtual network function that includes the VDU.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.

4. Select the **VDU management** tab.

A table of VDUs is displayed.

5. Click **Power** → **Snapshot** next to the VDU whose snapshot you want to edit.

This opens a window with the table of VDU snapshots.

6. Click **Management** → **Edit** next to the VDU snapshot that you want to edit.

7. In the **Name** field, enter a name for the VDU snapshot.

8. In the **Description** field, enter a brief description of the VDU snapshot.

9. Click **Save**.

The VDU snapshot is modified and updated in the table.

Deleting a VDU snapshot

Deleted VDU snapshots cannot be restored.

To delete a VDU snapshot:

1. In the self-service portal, go to the **Catalog** menu section.

The network service management page is displayed.

2. In the **Network services** pane, click the previously [deployed network service](#) to whose topology the virtual network function has been added.

The topology is displayed.

3. Click the virtual network function that includes the VDU.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.

4. Select the **VDU management** tab.

A table of VDUs is displayed.

5. Click **Power** → **Snapshot** next to the VDU whose snapshot you want to delete.

This opens a window with the table of VDU snapshots.

6. Click **Management** → **Delete** next to the VDU snapshot that you want to delete.

7. In the confirmation window, click **Delete**.

The VDU snapshot is deleted and is no longer displayed in the table.

Managing physical network functions in the topology

To manage a physical network function, click it in the topology when performing the following actions:

- When [creating](#) or [editing a network service template](#)
- When [creating](#) or [editing a network service](#)

Physical network function settings are displayed on the following tabs:

- **Flavours** contains flavours of the physical network function.
- **VNF settings** contains basic settings of the physical network function.

The following tabs are displayed if you clicked the physical network function in the topology of a [deployed network service](#):

- **Monitoring** contains [monitoring results of the physical network function](#).
- **Problems** contains [problems that occurred during the operation of the physical network function](#). In case of any problems, a red exclamation mark is displayed next to the tab.

Additional tabs may be displayed if you specified any in the PNF descriptor in the `user_configurations` block.

Selecting the flavour of a physical network function

You can specify flavours in the PNF descriptor in the `flavours` block.

To select a physical network function flavour:

1. Navigate to the topology in one of the following ways:
 - Start [creating](#) or [editing a network service template](#).
 - Start [creating](#) or [editing a network service](#).
2. In the topology, click the physical network function for which you want to select a deployment option.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.
3. Select a flavour for the physical network function.
4. In the upper part of the settings area, click **Save** to save physical network function settings.

Basic settings of a physical network function

To edit basic settings of the physical network function:

1. Navigate to the topology in one of the following ways:
 - Start [creating](#) or [editing a network service template](#).
 - Start [creating](#) or [editing a network service](#).
2. In the topology, click the physical network function for which you want to configure basic settings.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Flavours** tab is selected, which displays flavours.

3. Select the **PNF settings** tab.

Basic settings of the physical network function are displayed.

4. In the **Name** field, enter the name of the physical network function.

5. In the **Description** field, enter a brief description of the physical network function.

6. In the **Order** field, enter the sequence number for deploying the physical network function on the OpenStack cloud platform. When you [deploy a network service](#), the physical network function with the lowest number is the first to be deployed. If none of the physical network functions added to the topology have a sequence number specified, all physical network functions are deployed simultaneously.

7. In the upper part of the settings area, click **Save** to save physical network function settings.

Configuring a P2P service in the topology

To configure a P2P service in the topology:

1. Navigate to the topology in one of the following ways:

- Start [creating](#) or [editing a network service template](#).
- Start [creating](#) or [editing a network service](#).

2. In the topology, click the P2P service that you want to configure.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

3. In the **Name** field, enter the name of the transport service.

4. If necessary, in the **Description** field, enter a brief description of the transport service.

5. In the upper part of the settings area, click **Save** to save P2P service settings.

Configuring a P2M service in the topology

To configure a P2M service in the topology:

1. Navigate to the topology in one of the following ways:

- Start [creating](#) or [editing a network service template](#).
- Start [creating](#) or [editing a network service](#).

2. In the topology, click the P2M service that you want to configure.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

3. In the **Name** field, enter the name of the transport service.

4. If necessary, in the **Description** field, enter a brief description of the transport service.
5. In the **Connection points** field, enter the maximum number of transport service connection points. Range of values: 2 to 9999. If you do not specify a value for this setting, the number of connection points is unlimited.
6. In the **Mode** drop-down list, select whether you want to use the Default Forwarding Interface (DFI), to which unknown unicast traffic is sent, in the transport service:
 - **Classic** if you do not want to use DFI. Default value.
 - **DFI with FIB on root and leafs** if you want to use DFI on the service interface with the root role. The number of service interfaces with the leaf role is not limited. Backup service interfaces can be added for each service interface.
 - **DFI with FIB on leaf** if you want to use DFI on the service interface with the root role. The number of service interfaces with the leaf role is not limited. Service interfaces with the leaf role must be on the same CPE device. Backup service interfaces can be added for each service interface.

Backup service interfaces with the leaf role must be on the same CPE device, which must be different from the device hosting the primary service interfaces.
7. In the **MAC age (sec.)** field, enter the time period in seconds during which you want to keep entries in the MAC table on the controller. Range of values: 10 to 65,535. The default setting is **300**.
8. In the **MAC learn mode** drop-down list, select the action that you want to apply to a series of frames when the first frame is sent to the controller to learn the source MAC address:
 - **Learn and flood** means the controller remembers the MAC address of the source and checks for the presence of the destination MAC address in the MAC address table. If the destination MAC address is not in the table, the series of frames is sent to all service interfaces added to the transport service, except for the interface on which the series of frames originally arrived. Default value.
 - **Learn and drop** means the controller remembers the MAC address of the source and checks for the presence of the destination MAC address in the MAC address table. If the destination MAC address is not in the table, the series of frames is dropped.

If the destination MAC address is present in the MAC address table, the series of frames is sent to the destination service interface.
9. In the **MAC table size** field, enter the maximum number of entries in the MAC table on the controller. Range of values: 0 to 65,535. **0** means the number of entries is not limited. The default setting is **100**.
10. In the **MAC table overload** drop-down list, select the policy for processing new MAC addresses when the MAC table of the controller is full:
 - **Flood** means traffic with destination MAC addresses that have not been learned previously is transmitted as BUM traffic (Broadcast, unknown-unicast, and multicast). Default value.
 - **Drop** means that traffic with previously destination MAC addresses that have not been learned previously is dropped.
11. If you want to configure the assignment of IP address to virtual network functions using DHCP:
 - a. In the **OpenStack DHCP** drop-down list, select **Enabled**. The default setting is **Disable**.

- b. In the **CIDR** field, enter the IPv4 prefix of the OpenStack subnet that you want to assign IP addresses to virtual network functions.
- c. If you want the OpenStack subnet to assign a particular gateway to virtual network functions, enter the IPv4 address of the gateway in the **Gateway** field.
- d. Specify the range from which the OpenStack subnet must assign IP addresses to virtual network functions:

1. Under **Pools**, click **+ Pool**.
2. In the fields that are displayed, enter the start and end values for the IP address range.

The range of IP addresses is specified and displayed in the **Pools** section. You can specify multiple ranges of IP addresses; to delete a range, click **Delete** next to it.

- e. Specify the DNS server that the OpenStack subnet must assign to virtual network functions:

1. Under **DNS**, click **+ DNS**.
2. In the field that is displayed, enter the IPv4 address of the DNS server.

The DNS server is specified and displayed in the **DNS** section. You can specify multiple DNS servers; to delete a server, click **Delete** next to it.

12. In the upper part of the settings area, click **Save** to save P2M service settings.

Configuring a M2M service in the topology

To configure an M2M service in the topology:

1. Navigate to the topology in one of the following ways:
 - Start [creating](#) or [editing a network service template](#).
 - Start [creating](#) or [editing a network service](#).
2. In the topology, click the M2M service that you want to configure.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .
3. In the **Name** field, enter the name of the transport service.
4. If necessary, in the **Description** field, enter a brief description of the transport service.
5. In the **Connection points** field, enter the maximum number of transport service connection points. Range of values: 2 to 9999. If you do not specify a value for this setting, the number of connection points is unlimited.
6. In the **MAC age (sec.)** field, enter the time period in seconds during which you want to keep entries in the MAC table on the controller. Range of values: 10 to 65,535. The default setting is 300.
7. In the **MAC learn mode** drop-down list, select the action that you want to apply to a series of frames when the first frame is sent to the controller to learn the source MAC address:

- **Learn and flood** means the controller remembers the MAC address of the source and checks for the presence of the destination MAC address in the MAC address table. If the destination MAC address is not in the table, the series of frames is sent to all service interfaces added to the transport service, except for the interface on which the series of frames originally arrived. Default value.
- **Learn and drop** means the controller remembers the MAC address of the source and checks for the presence of the destination MAC address in the MAC address table. If the destination MAC address is not in the table, the series of frames is dropped.

If the destination MAC address is present in the MAC address table, the series of frames is sent to the destination service interface.

- In the **MAC table size** field, enter the maximum number of entries in the MAC table on the controller. Range of values: 0 to 65,535. 0 means the number of entries is not limited. The default setting is 100.
- In the **MAC table overload** drop-down list, select the policy for processing new MAC addresses when the MAC table of the controller is full:
 - **Flood** means traffic with destination MAC addresses that have not been learned previously is transmitted as BUM traffic (Broadcast, unknown-unicast, and multicast). Default value.
 - **Drop** means that traffic with previously destination MAC addresses that have not been learned previously is dropped.
- If you want to configure the assignment of IP address to virtual network functions using DHCP:
 - In the **OpenStack DHCP** drop-down list, select **Enabled**. The default setting is **Disable**.
 - In the **CIDR** field, enter the IPv4 prefix of the OpenStack subnet that you want to assign IP addresses to virtual network functions.
 - If you want the OpenStack subnet to assign a particular gateway to virtual network functions, enter the IPv4 address of the gateway in the **Gateway** field.
 - Specify the range from which the OpenStack subnet must assign IP addresses to virtual network functions:
 - Under **Pools**, click **+ Pool**.
 - In the fields that are displayed, enter the start and end values for the IP address range.

The range of IP addresses is specified and displayed in the **Pools** section. You can specify multiple ranges of IP addresses; to delete a range, click **Delete** next to it.
 - Specify the DNS server that the OpenStack subnet must assign to virtual network functions:
 - Under **DNS**, click **+ DNS**.
 - In the field that is displayed, enter the IPv4 address of the DNS server.

The DNS server is specified and displayed in the **DNS** section. You can specify multiple DNS servers; to delete a server, click **Delete** next to it.
- If you want to use an M2M service to create a shared network service, select the **Share network service** check box. This check box is cleared by default.

12. In the upper part of the settings area, click **Save** to save M2M service settings.

Configuring a shared network (OS 2 SHARED) in the topology

To configure a shared network in the topology:

1. Navigate to the topology in one of the following ways:

- Start [creating](#) or [editing a network service template](#).
- Start [creating](#) or [editing a network service](#).

2. In the topology, click the shared network that you want to configure.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

3. In the **Name** field, enter the name of the shared network.

4. If necessary, in the **Description** field, enter a brief description of the shared network.

5. In the upper part of the settings area, click **Save** to save shared network settings.

Configuring a virtual router (OS vRouter) in the topology

To configure a virtual router in the topology:

1. Navigate to the topology in one of the following ways:

- Start [creating](#) or [editing a network service template](#).
- Start [creating](#) or [editing a network service](#).

2. In the topology, click the virtual router that you want to configure.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

3. In the **Name** field, enter the name of the virtual router.

4. If necessary, in the **Description** field, enter a brief description of the virtual router.

5. If you want to set the 'up' value for the operating state of the virtual router, select the **Administrative state** check box. This check box is cleared by default.

6. In the upper part of the settings area, click **Save** to save virtual router settings.

Configuring a VLAN in the topology

To configure a VLAN in the topology:

1. Navigate to the topology in one of the following ways:

- Start [creating](#) or [editing a network service template](#).
- Start [creating](#) or [editing a network service](#).

2. In the topology, click the VLAN that you want to configure.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

3. In the **Name** field, enter the name of the VLAN.

4. If necessary, in the **Description** field, enter a brief description of the VLAN.

5. If you want to configure the assignment of IP address to virtual network functions using DHCP:

- a. In the **OpenStack DHCP** drop-down list, select **Enabled**. The default setting is **Disable**.
- b. In the **CIDR** field, enter the IPv4 prefix of the OpenStack subnet that you want to assign IP addresses to virtual network functions.
- c. If you want the OpenStack subnet to assign a particular gateway to virtual network functions, enter the IPv4 address of the gateway in the **Gateway** field.
- d. Specify the range from which the OpenStack subnet must assign IP addresses to virtual network functions:

1. Under **Pools**, click **+ Pool**.

2. In the fields that are displayed, enter the start and end values for the IP address range.

The range of IP addresses is specified and displayed in the **Pools** section. You can specify multiple ranges of IP addresses; to delete a range, click **Delete** next to it.

- e. Specify the DNS server that the OpenStack subnet must assign to virtual network functions:

1. Under **DNS**, click **+ DNS**.

2. In the field that is displayed, enter the IPv4 address of the DNS server.

The DNS server is specified and displayed in the **DNS** section. You can specify multiple DNS servers; to delete a server, click **Delete** next to it.

6. If you want to use the network to create a shared network service, select the **Share network** check box. This check box is cleared by default.

7. If you want to assign a VLAN tag to virtual network functions, in the **Segmentation ID** field, enter the VLAN tag.

8. In the upper part of the settings area, click **Save** to save VLAN settings.

Configuring a VXLAN in the topology

To configure a VXLAN in the topology:

1. Navigate to the topology in one of the following ways:

- Start [creating](#) or [editing a network service template](#).
- Start [creating](#) or [editing a network service](#).

2. In the topology, click the VXLAN that you want to configure.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

3. In the **Name** field, enter the name of the VXLAN.

4. If necessary, in the **Description** field, enter a brief description of the VXLAN.

5. If you want to configure the assignment of IP address to virtual network functions using DHCP:

- a. In the **OpenStack DHCP** drop-down list, select **Enabled**. The default setting is **Disable**.
- b. In the **CIDR** field, enter the IPv4 prefix of the OpenStack subnet that you want to assign IP addresses to virtual network functions.
- c. If you want the OpenStack subnet to assign a particular gateway to virtual network functions, enter the IPv4 address of the gateway in the **Gateway** field.
- d. Specify the range from which the OpenStack subnet must assign IP addresses to virtual network functions:

1. Under **Pools**, click **+ Pool**.

2. In the fields that are displayed, enter the start and end values for the IP address range.

The range of IP addresses is specified and displayed in the **Pools** section. You can specify multiple ranges of IP addresses; to delete a range, click **Delete** next to it.

- e. Specify the DNS server that the OpenStack subnet must assign to virtual network functions:

1. Under **DNS**, click **+ DNS**.

2. In the field that is displayed, enter the IPv4 address of the DNS server.

The DNS server is specified and displayed in the **DNS** section. You can specify multiple DNS servers; to delete a server, click **Delete** next to it.

6. If you want to use the network to create a shared network service, select the **Share network** check box. This check box is cleared by default.

7. If you want to assign a VXLAN tag to virtual network functions, in the **Segmentation ID** field, enter the VXLAN tag.

8. In the upper part of the settings area, click **Save** to save VXLAN settings.

Configuring a flat network in the topology

To configure a flat network in the topology:

1. Navigate to the topology in one of the following ways:

- Start [creating](#) or [editing a network service template](#).
- Start [creating](#) or [editing a network service](#).

2. In the topology, click the flat network that you want to configure.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

3. In the **Name** field, enter the name of the flat network.

4. If necessary, in the **Description** field, enter a brief description of the flat network.

5. If you want to configure the assignment of IP address to virtual network functions using DHCP:

- a. In the **OpenStack DHCP** drop-down list, select **Enabled**. The default setting is **Disable**.
- b. In the **CIDR** field, enter the IPv4 prefix of the OpenStack subnet that you want to assign IP addresses to virtual network functions.
- c. If you want the OpenStack subnet to assign a particular gateway to virtual network functions, enter the IPv4 address of the gateway in the **Gateway** field.
- d. Specify the range from which the OpenStack subnet must assign IP addresses to virtual network functions:

1. Under **Pools**, click **+ Pool**.

2. In the fields that are displayed, enter the start and end values for the IP address range.

The range of IP addresses is specified and displayed in the **Pools** section. You can specify multiple ranges of IP addresses; to delete a range, click **Delete** next to it.

- e. Specify the DNS server that the OpenStack subnet must assign to virtual network functions:

1. Under **DNS**, click **+ DNS**.

2. In the field that is displayed, enter the IPv4 address of the DNS server.

The DNS server is specified and displayed in the **DNS** section. You can specify multiple DNS servers; to delete a server, click **Delete** next to it.

6. If you want to use the network to create a shared network service, select the **Share network** check box. This check box is cleared by default.

7. In the upper part of the settings area, click **Save** to save flat network settings.

Configuring a UNI in the topology

To configure a UNI in the topology:

1. Navigate to the topology in one of the following ways:

- Start [creating](#) or [editing a network service template](#).
- Start [creating](#) or [editing a network service](#).

2. In the topology, click the UNI that you want to configure.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

3. In the **Name** field, enter the name of the UNI.

4. If necessary, in the **Description** field, enter a brief description of the UNI.

5. In the upper part of the settings area, click **Save** to save UNI settings.

Monitoring solution components

An external Zabbix monitoring system is used for monitoring of CPE devices, as well as virtual and physical network functions. You must deploy a Zabbix server on one of your locations, or connect an existing server, and deploy Zabbix proxy servers.

Zabbix proxy servers are used for receiving monitoring results at individual locations and sending these results to the Zabbix server. The Zabbix server processes the monitoring results, after which they are displayed in the web interface of the orchestrator.

The orchestrator uses an API to integrate with the Zabbix server. When you register a CPE device, [add a VNF or PNF to the network service topology](#), or [deploy a network service](#), a host is automatically created on the Zabbix server. This host corresponds to a CPE device, VNF, or PNF. You can specify the groups on the Zabbix server in which you want hosts to be placed.

Two monitoring methods are supported:

- Monitoring using Zabbix agents involves a component automatically sending monitoring data to a Zabbix proxy server.
- Monitoring via SNMP involves the Zabbix proxy server automatically connecting to a component via SNMP and receiving monitoring data.

For details about configuring the monitoring system, see the [official documentation of the Zabbix solution](#).

Specifying the Zabbix server

To specify the Zabbix server:

1. In the menu, go to the **Monitoring** section.

The settings for connecting to the Zabbix server are displayed.

2. In the **URL** field, enter the URL of the Zabbix API. The orchestrator sends HTTP requests to this URL to receive monitoring results and display them as charts.

The URL consists of the address of the Zabbix web interface and the `api_jsonrpc.php` file name, which is used for API calls. For example, if the Zabbix web interface is located at `http://192.168.2.1`, enter `http://192.168.2.1/api_jsonrpc.php`.

3. In the **Username** field, enter the user name for connecting the orchestrator to the Zabbix API. You must enter the user name of an account that has read and write permissions to groups on the Zabbix server, as well as permission to create groups.
4. In the **Password** field, enter the password for connecting to the Zabbix API.
5. In the **Grouping by Zabbix** drop-down list, select a method for grouping CPE device hosts, as well as virtual and physical network functions on the Zabbix server:
 - **By specified groups** to place hosts of CPE devices, virtual network functions, and physical network functions into the specified groups. If you select this option, do the following:
 - a. In the **VNF/PNF group** field, enter a group name for the virtual and physical network function hosts.
 - b. In the **CPE group** field, enter a group name for CPE device hosts.

- **By tenant** to place hosts of CPE devices, virtual network functions, and physical network functions into automatically created groups. Groups correspond to [tenants](#) to which the CPE devices, virtual network functions, and physical network functions are assigned.
6. In the **Triggers synchronization (sec.)** field, enter the interval in seconds for receiving notifications about [problems](#) from the Zabbix server on the orchestrator. Range of values: 5 to 600. The default setting is 600.
 7. Under the **Token** field, click **Generate** to generate a token that API requests from the Zabbix server to the orchestrator must contain. If an API request does not contain the token, the orchestrator does not accept such a request. Security is also protected by TLS certificates.
You can enter the token manually or view it by clicking the view icon .
 8. If you want to check the availability of the Zabbix server, click **Test connection**.
 9. Click **Apply**.

The Zabbix server is specified.

Specifying the Zabbix proxy server

To specify a Zabbix proxy server:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.
2. In the **Resources** pane, select the previously [created domain](#) and [data center](#) for which you want to specify a Zabbix proxy server.
3. Select the **System resources** tab.
The settings for connecting to the Zabbix proxy server and VNFM are displayed.
4. Under **Zabbix proxy**, in the **Name** field, enter the name of the Zabbix proxy server. The name must match the name specified in the Zabbix server settings.
5. In the **IP** field, enter the IP address of the Zabbix proxy server. The entered IP address must be accessible for the CPE devices and virtual and physical network functions that you want to monitor.
6. Click **Apply**.

The Zabbix proxy server is specified.

You can delete the Zabbix proxy server connection settings by clicking **Delete**.

Configuring CPE device monitoring

You can configure monitoring in a [CPE template](#). When you configure monitoring in a CPE template, the settings are propagated to all [devices](#) that are using the template.

To configure CPE device monitoring:

1. In the menu, go to the **SD-WAN** → **CPE templates** section.

A table of CPE templates is displayed.

2. Click the CPE template in which you want to configure monitoring.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. Select the **Monitoring** tab.

The CPE device monitoring settings are displayed.

4. In the **Monitoring type** drop-down list, select a monitoring method for the CPE device:

- **SNMP** means monitoring using the [SNMP protocol](#).
- **Agent** means monitoring using Zabbix agents.

5. In the **Zabbix template** field, enter the name of the Zabbix template.

6. In the upper part of the settings area, click **Save** to save CPE template settings.

Viewing monitoring results

You can view monitoring results for a SD-WAN instance, CPE device, a virtual network function, or a physical network function:

- To view the results of monitoring an SD-WAN instance, you need to go to the section **SD-WAN** → **SD-WAN instances** , click on the instance and in the displayed settings area, select the tab **Monitoring ...**
- To display monitoring results for a CPE device, go to the **SD-WAN** → **CPE** section, click the device, and in the displayed settings area, select the **Monitoring** tab.
- To view monitoring results for a virtual or physical network function, in the self-service portal, go to the **Catalog** menu section, and in the **Network services** pane, click a previously [deployed network service](#) to which the network function is added, click the virtual or physical network function, and in the displayed settings area, select the **Monitoring** tab.

In the drop-down list in the upper part of the settings area, you can select the parameter for which the monitoring results are displayed. To display monitoring results for a selected period, you can use the following time filters:

- **Real-time**
- **Day**
- **Week**
- **Month**

You can also specify the time period manually.

Viewing problems

The monitoring settings on the Zabbix server determine which problems warrant notifications and how these problems are classified according to their severity levels. The table of problems is displayed on the CPE device and on the virtual or physical network function:

- To display the table of problems on a CPE device, go to the **SD-WAN** → **CPE** menu section, click the device, and in the displayed settings area, select the **Problems** tab.
- To view the table of problems for a virtual or physical network function, in the self-service portal, go to the **Catalog** menu section, and in the **Network services** pane, click a previously [deployed network service](#) to which the network function is added, click the virtual or physical network function, and in the displayed settings area, select the **Problems** tab.

Information about problems is displayed in the following columns of the table:

- **Name** is the name of the problem.
- **Level** is the severity level of the problem:
 - **Average**
 - **Disaster**
 - **High**
 - **Information**
 - **Not classified**
- **Time** is the time when the problem occurred.
- **Duration** is the duration of the problem in seconds.

Viewing the status of the solution and its components

To view the status of solution components:

1. In the menu, go to the **Dashboard** section.

The following blocks of information are displayed:

- **Event errors** contains errors that occurred during events.
- **Task errors** contains errors that occurred when performing custom tasks.
- **Active sessions** contains active user sessions.
- **Resources** contains information about computing resource usage by solution components.
- **Service requests** contains [service requests](#).
- **Disconnected CPE** contains CPE devices to which access has been lost.
- **Errors on CPE** contains errors encountered by CPE devices.

- **Problems on CPE** contains [problems](#) encountered by CPE devices.
- **Problems on VNF/PNF** contains problems encountered by virtual and physical network functions.

If a solution component is operating correctly, the corresponding widget displays the *Everything is running smoothly* message. An update icon is displayed in the upper part of a block; when this icon is clicked, the displayed information is refreshed. You can drag widgets with the mouse to change the layout.

2. If you want to configure which blocks are displayed by default, click the settings icon in the upper part of the page → **Reset to default layout**.
3. If you want to set a different update interval for information in blocks:
 - a. In the upper part of the page, click the settings icon → **Set update interval**.
 - b. This opens a window; in that window, in the **Update dashboard every (sec.)** field, enter the interval in seconds for updating information in blocks. Range of values: 5 to 86,400. The default setting is 60.
 - c. Click **Ok**.

The update interval for information in the blocks is changed.

Viewing logs

You can view the logs of solution components for technical support purposes. Kaspersky SD-WAN does not send logs outside the perimeter of your organization's information infrastructure.

To view logs:

1. In the menu, go to the **Logs** section.
The log management page is displayed.
2. In the **Data centers** pane, select a previously [created data center](#) to which the solution components belong.
3. In the **Resources** pane, select the solution component whose log you want to view.

The log is displayed. By default, the **Tasks** tab is selected, which displays the table of custom tasks. Information about custom tasks is displayed in the following columns of the table:

- **Task action** is the action of the task.
- **Object** is the solution component associated with the task.
- **SR** is a link to the [service request](#) associated with the task.
- **Object ID** is the ID of the solution component associated with the task.
- **Object name** is the name of the solution component associated with the task.
- **Initiator** is the name of the [user](#) that ran the task.
- **Initiator IP** is the IP address of the user that ran the task.
- **Start time** is the date and time when the task began running.

- **End time** is the date and time when the task finished running.
4. If you want to view information about events that occurred during the operation of a solution component, select the **Events** tab.

A table of events is displayed. Information about events is displayed in the following columns of the table:

- **Event action** is the action of the event.
 - **Object** is the solution component associated with the event.
 - **SR** is a link to the service request associated with the event.
 - **Object name** is the name of the solution component associated with the event.
 - **Object ID** is the ID of the solution component associated with the event.
 - **Initiator** is the name of the user whose action caused the event.
 - **Time** is the date and time when the event was created.
5. If you want to view the service requests of a solution component, select the **Service requests** tab.

A table of service requests is displayed. Information about service requests is displayed in the following columns of the table:

- **Service request** is the name of the service request.
- **Status** is the status of the service request.
- **Initiator** is the name of the user whose action caused the service request.
- **Time** is the date and time when the service request was created.

The actions you can perform with the tables are described in the [Managing solution component tables](#) instructions.

Viewing and deleting service requests

Service requests are tasks that are performed while solution components are working and are automatically created as a result of user actions. For example, when a user applies a CPE template to a device, a corresponding service request is created.

Viewing service requests

You can view the service requests of a tenant, a CPE device, and an SD-WAN instance:

- To view service requests for a tenant, go to the **Tenants** section and under **Tenants**, select a tenant. The list of service requests is displayed under **Service requests**.
- To view service requests for an SD-WAN instance, you need to go to the section **SD-WAN→SD-WAN instances**, click on the instance and in the displayed settings area, select the tab **Service requests ...**. A table of service requests is displayed.

- To display service requests for a CPE device, go to the **SD-WAN** → **CPE** section, click the device, and in the displayed settings area, select the **Service requests** tab.

A table of service requests is displayed.

The list of service requests of a tenant displays the name and ID of the service request, as well as its creation date and time. Information about service requests of an SD-WAN instance and CPE device is displayed in the following table columns:

- **Name** is the name of the service request.
- **Created** is the date and time when the service request was created.
- **Task ID** is the ID of the service request.
- **Time** is the duration of the service request in seconds.
- **Status** is the status of the service request.
- **Actions** contains the actions can be performed with the service requests.

You can open a step-by-step log of a service request by doing one of the following:

- If you want to open the step-by-step log of a tenant's service request, click the name of the service request.
- If you want to open a step-by-step log of a service request for an SD-WAN instance or CPE device, click the ID of the service request.

A step-by-step log of the service request is displayed.

The log contains information about the steps at which the errors occurred, as well as a detailed description of the errors.

Deleting service requests

You can delete service requests of an SD-WAN instance or a CPE device. Deleting a service request stops the associated operation.

Deleted service requests cannot be restored.

To delete a service request, do one of the following:

- If you want to delete an individual service request, click **Delete** next to it.
- If you want to delete all service requests, in the upper part of the settings area, under **Actions**, click **Delete all service requests**.

The service requests are deleted and are no longer displayed in the table.

Sending CPE device notifications to users

Kaspersky SD-WAN supports sending notifications to [user](#) email addresses with the following information about CPE devices:

- Events from the [log](#):
 - Enabling and disabling a CPE device
 - Connecting or disconnecting a port
 - Connecting or disconnecting a link
- [Problems](#):
 - Encountered problems
 - Resolved problems

Information is accumulated for five seconds before the notification is sent. For example, if disconnecting a port causes five tunnels to be disconnected, this information must be accumulated and sent to the user in the same notification.

The platform administrator must specify the SMTP server to be used by all tenants for sending notifications. On the administrator portal, you can configure notifications about events and problems for all tenants. On the self-service portal, you can configure notifications about events and problems for an individual tenant.

Specifying the SMTP Server

To specify an SMTP server:

1. In the menu, go to the **Notification** section.
By default, the **SMTP** tab is selected, which displays the SMTP server connection settings.
2. Select the **Enable** check box to use the SMTP server. This check box is cleared by default.
3. In the **SMTP server** field, enter the IP address or domain name of the SMTP server.
4. In the **SMTP server port** field, enter the port number of the SMTP server. Range of values: 0 to 65,535. The default setting is 25.
5. In the **Sender email** field, enter the email address from which you want the SMTP server to send notifications to users.
6. If you want to configure encryption of the connection between Kaspersky SD-WAN and the SMTP server, in the **SSL/TLS** drop-down list, select one of the following values:
 - **None** to leave the connection unencrypted. Default value.
 - **STARTTLS** to determine the encryption method and then establish an encrypted connection.
 - **SMTPS** to establish an encrypted connection straight away.
7. If you want to enable Kaspersky SD-WAN authentication on the SMTP server:
 - a. Select the **Authentication** check box. This check box is cleared by default.

b. In the **Username** field, enter the user name that Kaspersky SD-WAN must use to authenticate on the SMTP server. Maximum length: 64 characters.

c. In the **Password** field, enter the password that Kaspersky SD-WAN must use to authenticate on the SMTP server. Maximum length: 64 characters. To see the entered password, you can click the show icon .

8. If you want to send a test message using the SMTP server:

a. Click **Test**.

b. This opens a window; in that window, enter the email address to which you want the SMTP server to send a test message.

c. Click **Send**.

A test message is sent to the specified email address with *Notification test* in the subject and body.

9. Click **Apply**.

The SMTP server is specified.

Configuring notifications

The platform administrator must [specify the SMTP server](#) to enable sending notifications to the user.

To configure notifications:

1. Navigate to the configuration of user notifications in one of the following ways:

- If you logged in to the administrator portal, go to the **Notification** menu section and select the **Alert** tab.
- If you logged in to the self-service portal, go to the **Notification** menu section.

Notification settings are displayed.

2. Select the **Enable** check box to send notifications to the user. This check box is cleared by default.

3. In the **Receiver email** field, enter the email address to which you want to send notifications.

4. In the **Subject** field, enter the subject text of the notification email messages. Maximum length: 64 characters.

5. Click **Apply**.

Notifications will be sent to the specified email address.

Selecting the Docker container log verbosity

Kaspersky SD-WAN automatically keeps logs of Docker containers, which are used to deploy and support solution components. You can select the level of detail of these logs for monitoring containers and quickly recovering from faults.

To select Docker container log verbosity:

1. In the lower part of the menu, click the settings icon → **Log settings**.

This opens a page displaying a table of Docker containers. Information about Docker containers is displayed in the following columns of the table:

- **Module name** is the name of the Docker container.
- **Logging level** is the Docker container log verbosity:

2. Select the Docker container verbosity level in one of the following ways:

- If you want to select the verbosity level of all Docker containers, click the corresponding button in the **General logging level** section.
- If you want to select the verbosity level for an individual Docker container, click the corresponding button next to it.

You can select the following verbosity levels for Docker containers:

- **TRACE** to have the log include the most complete information about the operation and condition of the module and its variables. You can use this level of detail for observing code execution, as well as for diagnostics and detailed analysis of errors that occur during development.
- **DEBUG** to have the log include the information necessary for debugging the module, such as the status of operations and values of variables. You can use this level of detail to diagnose errors and analyze module behavior.
- **INFO** to have the log include general information necessary for understanding the functioning of the module, for example, confirmations of operations. You can use this level of detail to track the progress of the execution of the module. This level of detail is selected by default for all containers.
- **WARN** to have the log include information about incidents that are not errors, but may compromise the operation of the container and require your intervention, such as problems with settings and deprecated functions. You can use this level of detail to prevent potential errors.
- **ERROR** to have the log include information about errors that occur during the execution of the code and require your intervention. An error message can contain information about the part of the container in which the error occurred, as well as detailed information about the error. You can use this level of detail to resolve occurring errors.

Monitoring CPE, VNF, and PNF devices using SNMP

You can use SNMP to monitor [CPE devices](#) as well as [virtual](#) and [physical network functions](#). You need to install an SNMP agent on the component that you want to monitor. The SNMP agent gathers monitoring data and sends it to the SNMP manager for processing. In Kaspersky SD-WAN, the Zabbix proxy server acts as the SNMP manager.

The SNMP manager and agents exchange requests and notifications. By default, SNMP agents receive requests from the manager on port 161. However, the SNMP manager can send requests through any available port. The response arrives on the same port from which the request was sent.

By default, the SNMP manager receives notifications from agents on port 162. However, agents can send notifications through any available port. Two types of notifications exist:

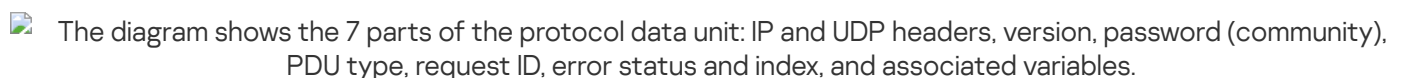
- *Traps* are notifications about events that the SNMP agent sends without a prior request from the manager. When a specified event occurs, such as a shutdown of a CPE device or one of its [network interfaces](#), the

SNMP agent generates a trap and sends it to the manager as a UPD message. Traps allow automatically informing the SNMP manager about events without waiting for a request.

- *Inform requests* are notifications similar to traps, which differ in that they require additional confirmation from the SNMP manager. When the SNMP agent sends an inform request to the manager, the agent waits to receive an acknowledgment. If the SNMP manager successfully receives and processes the inform request, it sends an acknowledgment message to the agent. The acknowledgment mechanism allows you to ensure the reliability of delivery of notifications.

When using the TLS or DTLS protocol, traps arrive on port 10162 of the SNMP manager, and information requests arrive on port 10161.

All basic protocol data units (PDUs) have the same structure (see figure below). The IP header and UDP header are used for encapsulation and are not actually part of the protocol data unit.

 The diagram shows the 7 parts of the protocol data unit: IP and UDP headers, version, password (community), PDU type, request ID, error status and index, and associated variables.

SNMP Protocol Data Unit diagram

To display the table of traps, go to the **Infrastructure** menu section, click **Management** → **Configuration menu** next to the controller to which the components that you want to monitor are connected, and in the displayed controller settings menu, go to the **SNMP** section. Information about traps is displayed in the following columns of the table:

- **#** is the serial number of the trap.
- **Manager IP** is the IP address or host name of the SNMP manager.
- **Manager port** is the port number of the SNMP manager.
- **Community** is the SNMP community string.
- **Allowed traps** are traps that SNMP agents must send to the manager.
- **Description** is a brief description of the trap.

Configuring the connection of the SNMP manager to agents

You must specify the settings for connecting the SNMP manager to agents installed on CPE devices, as well as on the virtual and physical network functions. The specified settings are used for all SNMP agents.

To configure the connection of the SNMP manager to agents:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. Click **Management** → **Configuration menu** next to the controller to which the components that you want to monitor are connected.

This opens the controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of controller nodes.

3. Go to the **SNMP** section.

A table of traps is displayed.

4. In the upper part of the page, under **Manager parameters**, click **Edit**.
5. This opens a window; in that window, in the **Address** field, enter the IP address or host name of the equipment on which the SNMP agent is installed, in the < transport protocol >: < IP address or host name > / < port number > format. For example, you can enter `udp:192.168.2.0/24`.
6. In the **Community** field, enter the SNMP community string. The community string is used as a password which the SNMP manager uses to connect to agents. The default setting is `public`, which provides read-only access. We recommend changing the default to a unique community string to ensure the security of communication between the SNMP manager and the agents.

You must specify the same community string when configuring the SNMP manager connection to agents and when [creating](#) or [editing](#) traps.

7. Click **Save**.

The connecting of the SNMP manager to agents is configured.

Creating a trap

You can create a trap that SNMP agents must send to the manager.

To create a trap:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.
2. Click **Management** → **Configuration menu** next to the controller to which the components that you want to monitor are connected.
This opens the controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of controller nodes.
3. Go to the **SNMP** section.
A table of traps is displayed.
4. Under **Trap parameters**, click **Edit**.
5. This opens a window; in that window, click **+ Add** to create a trap.
6. In the **Manager IP** field, enter the IP address or host name of the SNMP manager. Range of values: 1 to 255.
7. In the **Manager port** field, enter the port number of the SNMP manager. Range of values: 1 to 65,534. The default setting is 162.
8. In the **Community** field, enter the SNMP community string. The community string is used as a password which the SNMP manager uses to connect to agents. The default setting is `public`, which provides read-only access. We recommend changing the default to a unique community string to ensure the security of communication between the SNMP manager and the agents.

You must specify the same community string when [configuring the SNMP manager connection to agents](#) and when creating or [editing traps](#).

9. In the **Allowed traps** field, click **Edit** and clear the following check boxes to specify which traps SNMP agents must not send to the manager:
 - Clear the **Trap, when an interface is active** check box to prevent the SNMP agent from sending a trap to the manager when one of the ports of the component on which the agent is installed becomes active.
 - Clear the **Trap, when an interface is inactive** check box to prevent the SNMP agent from sending a trap to the manager when one of the ports of the component on which the agent is installed becomes inactive.
 - Clear the **Trap, when an equipment is active** check box to prevent the SNMP agent from sending a trap to the manager when the component on which the agent is installed becomes active.
 - Clear the **Trap, when an equipment is inactive** check box to prevent the SNMP agent from sending a trap to the manager when the component on which the agent is installed becomes inactive.

By default, the check boxes are selected.

10. Click **Back** to continue specifying trap settings.
11. In the **Description** field, enter a brief description of the trap.
12. Click **Save**.

The trap is created and displayed in the table.

Editing a trap

To edit a trap:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.
2. Click **Management** → **Configuration menu** next to the controller to which the components that you want to monitor are connected.

This opens the controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of controller nodes.
3. Go to the **SNMP** section.

A table of traps is displayed.
4. Under **Trap parameters**, click **Edit**.
5. This opens a window; in that window, in the **Manager IP** field, enter the IP address or host name of the SNMP manager. Range of values: 1 to 255.
6. In the **Manager port** field, enter the port number of the SNMP manager. Range of values: 1 to 65,534. The default setting is 162.

7. In the **Community** field, enter the SNMP community string. The community string is used as a password which the SNMP manager uses to connect to agents. The default setting is `public`, which provides read-only access. We recommend changing the default to a unique community string to ensure the security of communication between the SNMP manager and the agents.

You must specify the same community string when [configuring the SNMP manager connection to agents](#) and when [creating](#) or editing traps.

8. In the **Allowed traps** field, click **Edit** and clear the following check boxes to specify which traps SNMP agents must not send to the manager:

- Clear the **Trap, when an interface is active** check box to prevent the SNMP agent from sending a trap to the manager when one of the network interfaces of the CPE device or switch on which the agent is installed becomes active.
- Clear the **Trap, when an interface is inactive** check box to prevent the SNMP agent from sending a trap to the manager when one of the network interfaces of the CPE device or switch on which the agent is installed becomes inactive.
- Clear the **Trap, when an equipment is active** check box to prevent the SNMP agent from sending a trap to the manager when the CPE device or switch on which the agent is installed becomes active.
- Clear the **Trap, when an equipment is inactive** check box to prevent the SNMP agent from sending a trap to the manager when the CPE device or switch on which the agent is installed becomes inactive.

By default, the check boxes are selected.

9. Click **Back** to continue specifying trap settings.

10. In the **Description** field, enter a brief description of the trap.

11. Click **Save**.

The trap is modified and updated in the table.

Deleting a trap

Deleted traps cannot be restored.

To delete a trap:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. Click **Management** → **Configuration menu** next to the controller to which the components that you want to monitor are connected.

This opens the controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of controller nodes.

3. Go to the **SNMP** section.

A table of traps is displayed.

4. Under **Trap parameters**, click **Edit**.
5. This opens a window; in that window, click **Delete** next to the trap that you want to delete.
6. Click **Save**.

The trap is deleted and is no longer displayed in the table.

Link monitoring

To configure link monitoring:

1. Configure the link monitoring in one of the following ways:
 - In the menu, go to the **SD-WAN** → **CPE** section, click the device, and in the displayed settings area, select the **Tunnels** tab and click **Management** → **Set thresholds** next to the link. Only links established from the CPE device are displayed on that device.
 - In the menu, go to the **Infrastructure** section, click **Management** → **Configuration menu** next to the controller deployed for the instance, in the menu that is displayed, go to the **Tunnels** section and click **Management** → **Set thresholds** next to the link.
 - In the menu, go to the **Infrastructure** section, click **Management** → **Configuration menu** next to the controller deployed for the instance, in the menu that is displayed, go to the **Topology** section and in the displayed window, click **Set thresholds**.
2. Select the **Enable tunnel thresholds monitoring** check box enable link monitoring.
3. If you enabled link monitoring, configure the monitoring thresholds:
 - a. To set default monitoring thresholds, click **Set to default**.
 - b. If you want to use the link as the last resort option when routing traffic regardless of the link quality, select the **Unsolicited** check box. This check box is cleared by default.
 - c. In the **Interval for processing errors and utilization rate (sec.)** field, enter the interval in seconds for measuring the number of errors on the link and its level of utilization. Range of values: 1 to 300. The default setting is 60.
 - d. If you want to specify a threshold for the number of errors per second on the link, select the **Enable error monitoring** check box and in the **Critical error level (errors/sec.)** field, enter the threshold value. Range of values: 1 to 1,000,000. By default, the check box is cleared and the field is set to 1000.
 - e. If you want to specify a threshold for link utilization as a percentage of the bit rate of the service interface from which the link is established, select the **Enable utilization monitoring** check box and in the **Critical utilization level (%)** field, enter the threshold value. By default, the check box is cleared and the field is set to 95.
 - f. In the **Interval for processing latency, jitter, and packet loss (sec.)** field, enter the time interval, in seconds, for measuring latency, jitter, and packet loss on the link. Range of values: 1 to 600. The default setting is 30.
 - g. If you want to specify a threshold for latency in milliseconds for transmitting traffic over the link, select the **Enable latency monitoring** check box and in the **Critical latency level (ms.)** field, enter the threshold value.

Range of values: 5 to 1000. By default, the check box is cleared and the field is set to **100**.

h. If you want to specify a threshold for jitter time in milliseconds for transmitting traffic over the link, select the **Enable jitter monitoring** check box and in the **Critical jitter level (ms.)** field, enter the threshold value. Range of values: 5 to 1000. By default, the check box is cleared and the field is set to **100**.

i. If you want to specify a threshold for the percentage of lost traffic packages on the link, select the **Enable packet loss monitoring** check box and in the **Critical packet loss level (%)** field, enter the threshold value. Range of values: 1 to 100. By default, the check box is cleared and the field is set to **2**.

4. Save the link monitoring settings in one of the following ways:

- To save the link monitoring settings, click **Save**.
- If you want to save the link monitoring settings and specify the same settings on the corresponding opposite-direction link, click **Save for both tunnels**.

5. If you have configured link monitoring on a CPE device, click **Save** in the upper part of the settings area to save the device settings.

Tunnels, segments, and paths

Connections between [CPE devices](#) are established using tunnels. Tunnels are unidirectional, so when establishing a connection between two devices or between a device and the [control plane](#), both an inbound tunnel and an outbound tunnel must be created. Tunnels established between CPE devices are combined into a [topology](#).

The concept of a *tunnel* is closely related to the concept of a *link* because in the case of SD-WAN, links are formed inside tunnels. The tunnel interface directly connects to a port of the virtual switch on a CPE device on both sides, thereby forming a link. Thus, in Kaspersky SD-WAN, tunnels are a means of forming links.

The set of tunnels connecting two CPEs is a *segment*. Traffic can be distributed over multiple tunnels at the source CPE device at the beginning of the segment and relayed to the destination CPE device at the end of the segment.

The routes along which traffic can be transmitted within one segment are called *paths*. The following types of paths are supported:

- **Auto-SPF** (Shortest-Path Forwarding) is a path that is automatically calculated by the [SD-WAN Controller](#). Paths of this type cannot be created or deleted, and their settings cannot be edited.
- **Manual-TE** (Traffic Engineering) is a manually created path. To create this type of path, you need to specify the tunnels which the path traverses from the CPE device at the beginning of the segment to the device at the end of the segment.
- **Auto-TE** is a path automatically calculated by the SD-WAN Controller, taking into account the constraints that you specify when creating [transport services](#). As constraints you may use the values of monitoring indicators on the tunnels, for example, the indicator of the utilization level of a tunnel.

One segment can contain from 2 to 16 paths, and when transmitting traffic, the best path with the lowest value of the cost parameter is selected by default. If the best path is not available for traffic transmission for technical reasons, another path with the closest value of the cost parameter is selected.

Redundancy of links between CPE devices

All available links between CPE devices, such as Internet and LTE, are used simultaneously to prevent interruptions in communication.

Active/Active mode

In this mode, all [SD-WAN interfaces](#) of CPE devices with the WAN type are in the active state and relay user traffic.

The SD-WAN controller uses 2 to 16 paths to evenly distribute traffic among the tunnels and prevent congestion of the tunnels and performance problems for users. Three balancing types are supported:

- Per flow balancing, taking into account information at levels L2 to L4. Two modes are available:
 - Equal balancing — the streams are allocated evenly among paths.
 - Unequal balancing — the streams are allocated among paths proportionally to the costs of the tunnels.
- Per packet — packets are allocated in proportion to the cost of the tunnels during transmission.

- Broadcast — packets are sent to all tunnels simultaneously to prevent losses.

In Active/Active mode, the CPE device remains available as long as at least one link is operational.

Active/Standby mode

In this mode, you must select the primary and backup paths for the traffic without balancing. The rules for using the backup SD-WAN interface with the WAN type in case the path through the primary interface becomes unavailable are preloaded on the CPE device. If the primary path is disrupted, the packet switching rules are not rewritten, and the CPE device sends the packets through the backup interface.

You can configure redundancy at the transport service level. When creating a [transport service](#), you must specify backup service interfaces (backup SI). We recommend creating the primary and backup service interfaces on different CPE devices. Traffic is switched to the backup service interface if the primary SI is unavailable.


The solution supports creating backup service interfaces for all types of L2 transport services.

The figures below show typical examples of communication interruptions between CPE devices:


- Failure of one of the CPE devices.

The diagram shows two client locations connected by four CPE devices; one CPE device has failed.

- Failure of the WAN-type SD-WAN interface of one of the CPE devices.

The diagram shows two client locations connected by four CPE devices; a WAN interface of one device has failed.

- Loss of connectivity between two CPE devices.

The diagram shows two client locations connected by four CPE devices. However, there is no connectivity between two of the devices.

- Failure of the LAN-type SD-WAN interface of one of the CPE devices.

The diagram shows two client locations connected by four CPE devices; a LAN interface of one device has failed.

Configuring paths

You can configure paths in a CPE template, on an individual device, or in a segment. When you specify path settings in a CPE template or a segment, these settings are automatically propagated to all devices that are using the template or are included in the segment. Use the following instructions to configure paths:

- [Configuring paths in a CPE template](#) 

To configure paths in a CPE template:

1. In the menu, go to the **SD-WAN** → **CPE templates** subsection.

A table of CPE templates is displayed.

2. Click the CPE template.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. Select the **Multipathing** tab.

Path settings are displayed.

4. In the **Maximum number of paths** field, enter the maximum number of paths supported by the CPE device or segment. Range of values: 1 to 16. The default setting is 8.

5. In the **Maximum of Auto-SPF** field, enter the maximum number of Auto-SPF paths supported by the CPE device or segment. Paths of the Auto SPF type are automatically calculated by the SD-WAN Controller. Range of values: 1 to 8. The default setting is 2.

6. In the **Cost variance multiplier** field, enter the cost variance factor that determines how many times greater the cost of a route can be compared to the best route, to make the path eligible for being added to the segment. Range of values: 1.0 to 10.0.

The default setting is 10. You cannot enter a value in this field if the **Multi-weight balancing** check box is selected.

7. If you need to distribute traffic among paths approximately in proportion to the value of the Path.weight attribute, select the **Multi-weight balancing** check box. When the check box is cleared, traffic is evenly spread and the weight attribute for all paths is 1. This check box is selected by default.

8. In the upper part of the settings area, click **Save** to save CPE template settings.

- [Configuring paths on an individual CPE device](#) 

To configure paths on an individual CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays the current configuration of the CPE device. This tab also displays the table of **Out-of-band management** CPE device configurations.

3. Select the **Multipathing** tab.

Path settings are displayed.

4. In the **Maximum number of paths** field, enter the maximum number of paths supported by the CPE device or segment. Range of values: 1 to 16. The default setting is 8.

5. In the **Maximum of Auto-SPF** field, enter the maximum number of Auto-SPF paths supported by the CPE device or segment. Paths of the Auto SPF type are automatically calculated by the SD-WAN Controller. Range of values: 1 to 8. The default setting is 2.

6. In the **Cost variance multiplier** field, enter the cost variance factor that determines how many times greater the cost of a route can be compared to the best route, to make the path eligible for being added to the segment. Range of values: 1.0 to 10.0.

The default setting is 10. You cannot enter a value in this field if the **Multi-weight balancing** check box is selected.

7. If you need to distribute traffic among paths approximately in proportion to the value of the Path.weight attribute, select the **Multi-weight balancing** check box. When the check box is cleared, traffic is evenly spread and the weight attribute for all paths is 1. This check box is selected by default.

8. Click **Apply**.

- [Configuring paths in a segment](#) 

To configure paths in a segment:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Segments** section.

A table of segments is displayed.

4. Click **Management** next to the segment and in the drop-down list, select **Edit**.

This opens a window with path settings and a table of paths.

5. In the **Maximum number of paths** field, enter the maximum number of paths supported by the CPE device or segment. Range of values: 1 to 16. The default setting is 8.

6. In the **Maximum of Auto-SPF** field, enter the maximum number of Auto-SPF paths supported by the CPE device or segment. Paths of the Auto SPF type are automatically calculated by the SD-WAN Controller. Range of values: 1 to 8. The default setting is 2.

7. In the **Cost variance multiplier** field, enter the cost variance factor that determines how many times greater the cost of a route can be compared to the best route, to make the path eligible for being added to the segment. Range of values: 1.0 to 10.0.

The default setting is 10. You cannot enter a value in this field if the **Multi-weight balancing** check box is selected.

8. If you need to distribute traffic among paths approximately in proportion to the value of the Path.weight attribute, select the **Multi-weight balancing** check box. When the check box is cleared, traffic is evenly spread and the weight attribute for all paths is 1. This check box is selected by default.

9. Click **Save**.

Creating a Manual-TE path

To create a Manual-TE path, you must specify the tunnels which the path traverses from the CPE device at the start of the segment to the CPE device at the end of the segment. Two types of such paths are supported:

- *Fully defined paths* that identify each device and interface from the beginning to the end of the segment. In this case, you must specify each tunnel traversed by the path.
- *Hybrid paths* in which you can specify one or more intermediate devices and, if necessary, interfaces. In this case, traffic is automatically transmitted between network nodes that are not manually specified (the Auto-SPF path is used).

You can use [constraints](#) to add Manual-TE paths to [transport services](#).

Examples of possible Manual-TE paths:

In the above examples, the abbreviation Sw (switch) stands for CPE devices. The interface number is indicated after the device number, separated by a colon.

Fully defined path: Sw1:3 → Sw2:1, Sw2:2 → Sw4:1, Sw4:5 → SwN:2.

Hybrid path: Sw1 → Sw5, Sw5:3 → Sw4:3, Sw4 → SwN. In this case, the path from Sw1 to SwN is constructed as the Auto-SPF path between Sw1 and Sw5, the Sw5:3 → Sw4:3 tunnel, and the Auto-SPF path between Sw4 and SwN.

To create a Manual-TE path:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Segments** section.

A table of segments is displayed.

4. Click **Management** next to the segment and in the drop-down list, select **Edit**.

This opens a window with path settings and a table of paths.

5. Click **+ Manual-TE path**.

This opens a window with the Manual-TE path settings and a table of hops.

6. In the **Name** field, enter the name of the Manual-TE path.

7. In the **Maximum number of hops** field, enter the maximum number of hops in the path. Range of values: 1 to 8. The default setting is 4.

8. In the **From** drop-down list on the left, select the starting CPE device for the hop.

If no hops are created in the path, only the first device of the segment can be selected as the starting CPE device.

If at least one hop is created in the path, only the final device of the last hop can be selected as the starting CPE device.

9. If necessary, in the **Port** drop-down list on the left, select the network-to-network interface (NNI) of the starting CPE device for the hop. The default setting is **Automatically** and the interface is detected automatically.

10. In the **To** drop-down list on the right, select the CPE device at the end of the hop.

When the starting CPE device of a hop is set to **Automatically** in the **Port** drop-down list, you can select any device in the domain as the final device except those that are already being used in other hops. For the final hop, the **Automatically** value is automatically selected in the **Port** drop-down list. Thus, the hop uses an Auto-SPF path.

If an NNI is selected for the starting CPE device for a hop in the **Port** drop-down list, only the device to which a tunnel has been constructed from the NNI can be selected as the final device. For the final device of the hop, the NNI to which the path is constructed is automatically selected in the **Port** drop-down list. Thus, the hop uses the tunnel specified between the two devices.

11. If necessary, in the **Port** drop-down list on the right, select the network-to-network interface (NNI) of the CPE device at the end of the hop. The default setting is **Automatically** and the interface is detected automatically.
12. Click **Add** to add a hop to the Manual-TE path.
The hop is created and displayed in the table. The **Segments** column displays the cost of the hop, which is the sum of the cost of all tunnels added to it. You can add multiple hops if the maximum number of hops in the path is not reached.
13. Click **Create**.

A check is performed to see that the final device of the last hop matches the final device of the segment in which you are creating the Manual-TE path. If the check is successful, the Manual-TE path is created and added to the table, and the **Cost** column displays the cost of the path, which is the sum of the cost of all hops added to it.

Editing a Manual-TE path

To edit a Manual-TE path:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.
2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.
This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.
3. Go to the **Segments** section.
A table of segments is displayed.
4. Click **Management** next to the segment and in the drop-down list, select **Edit**.
This opens a window with path settings and a table of paths.
5. Click **Edit** next to the Manual-TE path.
This opens a window with the Manual-TE path settings and a table of hops.
6. Edit the settings as necessary. For a description of the settings, see the [instructions for creating a Manual-TE path](#).
7. Click **Save** to save the settings of the Manual-TE path.
8. Click **Save** to save the settings of the segment.

Deleting a hop from a Manual-TE path

Hops deleted from a Manual-TE path cannot be restored.

To delete a hop from the Manual-TE path:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Segments** section.

A table of segments is displayed.

4. Click **Management** next to the segment and in the drop-down list, select **Edit**.

This opens a window with path settings and a table of paths.

5. Click **Edit** next to the Manual-TE path.

This opens a window with the Manual-TE path settings and a table of hops.

6. Click **Delete** next to the hop.

The hop is deleted and is no longer displayed in the table.

7. Click **Save** to save the settings of the Manual-TE path.

8. Click **Save** to save the settings of the segment.

Deleting a Manual-TE path

Deleted Manual-TE paths cannot be restored.

To delete a Manual-TE path:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Segments** section.

A table of segments is displayed.

4. Click **Management** next to the segment and in the drop-down list, select **Edit**.

This opens a window with path settings and a table of paths.

5. Click **Delete** next to the Manual-TE path.

The Manual-TE path is deleted and is no longer displayed in the table.

6. Click **Save** to save the settings of the segment.

Specifying the cost of a link

You can specify the cost of an individual tunnel. The tunnels are displayed in a common table in the **Tunnels** section; in the graphical topology in the **Topology** section; and in the CPE device configuration on the **Tunnels** tab. Only tunnels built using the particular CPE device are displayed in the configuration of that device.

To indicate the cost of the tunnel, use the following instructions:

- [Specify the cost of the tunnel using the overall tunnel table](#) .

To specify the cost of a tunnel using the overall tunnel table:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.
2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.
This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.
3. Go to the **Tunnels** section.
A table of tunnels is displayed.
4. Click **Management** next to the tunnel and in the drop-down list, select **Set cost**.
5. This opens a window; in that window, select the **Override** check box to specify the cost of the tunnel.
6. In the **Tunnel cost** field, enter the cost of the tunnel.
7. To automatically assign the specified cost to the corresponding tunnel in the opposite direction, select the **Save for both tunnels** check box.
8. Click **Save**.

- [Specify the cost of a tunnel using the graphical topology](#) .

To specify the cost of a tunnel using the graphical topology:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Topology** section.

The SD-WAN topology is displayed.

4. Click the tunnel to open a window and in that window, click **Set cost**.

5. This opens a window; in that window, select the **Override** check box to specify the cost of the tunnel.

6. In the **Tunnel cost** field, enter the cost of the tunnel.

7. To automatically assign the specified cost to the corresponding tunnel in the opposite direction, select the **Save for both tunnels** check box.

8. Click **Save**.

- [Specifying the cost of a tunnel in the configuration of the CPE device](#) 

To specify the cost of a tunnel on an individual CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays the current configuration of the CPE device. This tab also displays the table of **Out-of-band management** CPE device configurations.

3. Select the **Tunnels** tab.

A table of tunnels is displayed.

4. Click **Management** next to the tunnel and in the drop-down list, select **Set cost**.

5. This opens a window; in that window, select the **Override** check box to specify the cost of the tunnel.

6. In the **Tunnel cost** field, enter the cost of the tunnel.

7. To automatically assign the specified cost to the corresponding tunnel in the opposite direction, select the **Save for both tunnels** check box.

8. Click **Save**.

9. In the upper part of the settings area, click **Save** to save CPE device settings.

Enabling Dampening

Dampening is a configurable mechanism that prevents the use of tunnels that change state too frequently. When determining instability, the following state changes are taken into account:

- UP/LIVE → DOWN/NOT-LIVE.
- DOWN/NOT-LIVE → UP/LIVE.
- UP/LIVE → UP/NOT-LIVE.
- UP/NOT-LIVE → UP/LIVE.

The LIVE and NOT-LIVE states are used to integrate the Dampening function with the Ethernet Connectivity Fault Management (CFM) protocol, which detects the loss of two-way Ethernet connectivity of the segment between peer switches without the service interface entering the DOWN state (Rx signal loss).

Dampening is applied to both ends of the Ethernet segment.

This functionality does the following within a deployed SD-WAN network:

- Detect frequent changes of the states of service interfaces.
- Move transport services suffering from instability of service interfaces to backup tunnels.
- Exclude segments tied to the service interfaces from route calculation for transport services.

When the Dampening functionality is enabled, each state change of the service interface through which the tunnel is constructed increases the Penalty value. If the Penalty factor reaches the threshold value within a certain period of time, access to the tunnel is restricted (its cost is increased 10,000 times for a certain period of time). The value of each of these parameters is specified when you enable the feature. By default, access to the tunnel is resumed if the state of the service interface does not change for 10 minutes.

You can enable Dampening on an individual tunnel. The tunnels are displayed in a common table in the **Tunnels** section; in the graphical topology in the **Topology** section; and in the CPE device configuration on the **Tunnels** tab. Only tunnels built using the particular CPE device are displayed in the configuration of that device.

To enable Dampening on a tunnel, use the following instructions:

- [Enabling Dampening on a tunnel using the overall table of tunnels](#) 

To enable Dampening on a tunnel using the overall table of tunnels:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.
2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.
This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.
3. Go to the **Tunnels** section.
A table of tunnels is displayed.
4. Click **Management** next to the tunnel and in the drop-down list, select **Dampening**.
5. This opens a window, in that window, select the **Enable** check box.
6. In the **Maximum suppress time (ms.)** field, enter the maximum length of time, in milliseconds, for which access to the tunnel can be restricted. When the specified time elapses, all Dampening counters on the tunnel are reset. The default setting is **600,000**.
7. In the **Penalty**, enter the number by which Penalty is incremented when the tunnel changes state. The default setting is **1**.
8. In the **Suppress threshold** field, enter the Penalty value at which access to the tunnel is restricted. The default setting is **4**.
9. In the **Update interval (ms.)** field, enter the time in milliseconds during which Penalty must attain the value specified in the **Suppress threshold** field for access to the tunnel to be restricted. The default setting is **120,000**.
10. To view Dampening statistics for a tunnel, click **Load statistics**.
11. Click **Save**.

- [Enabling Dampening on a tunnel using the graphical topology](#) 

To enable Dampening on a tunnel using the graphical topology:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.
2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.
This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.
3. Go to the **Topology** section.
The SD-WAN topology is displayed.
4. Click the tunnel to open a window and in that window, click **Dampening**.
5. This opens a window, in that window, select the **Enable** check box.
6. In the **Maximum suppress time (ms.)** field, enter the maximum length of time, in milliseconds, for which access to the tunnel can be restricted. When the specified time elapses, all Dampening counters on the tunnel are reset. The default setting is **600,000**.
7. In the **Penalty**, enter the number by which Penalty is incremented when the tunnel changes state. The default setting is **1**.
8. In the **Suppress threshold** field, enter the Penalty value at which access to the tunnel is restricted. The default setting is **4**.
9. In the **Update interval (ms.)** field, enter the time in milliseconds during which Penalty must attain the value specified in the **Suppress threshold** field for access to the tunnel to be restricted. The default setting is **120,000**.
10. To view Dampening statistics for a tunnel, click **Load statistics**.
11. Click **Save**.

- [Enabling Dampening on a tunnel in the configuration of an individual CPE device](#) 

To enable Dampening on a tunnel in the configuration of a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.
A table of CPE devices is displayed.
2. Click the CPE device.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays the current configuration of the CPE device. This tab also displays the table of **Out-of-band management** CPE device configurations.
3. Select the **Tunnels** tab.
A table of tunnels is displayed.
4. Click **Management** next to the tunnel and in the drop-down list, select **Dampening**.
5. This opens a window, in that window, select the **Enable** check box.
6. In the **Maximum suppress time (ms.)** field, enter the maximum length of time, in milliseconds, for which access to the tunnel can be restricted. When the specified time elapses, all Dampening counters on the tunnel are reset. The default setting is **600,000**.
7. In the **Penalty**, enter the number by which Penalty is incremented when the tunnel changes state. The default setting is **1**.
8. In the **Suppress threshold** field, enter the Penalty value at which access to the tunnel is restricted. The default setting is **4**.
9. In the **Update interval (ms.)** field, enter the time in milliseconds during which Penalty must attain the value specified in the **Suppress threshold** field for access to the tunnel to be restricted. The default setting is **120,000**.
10. To view Dampening statistics for a tunnel, click **Load statistics**.
11. Click **Save**.
12. In the upper part of the settings area, click **Save** to save CPE device settings.

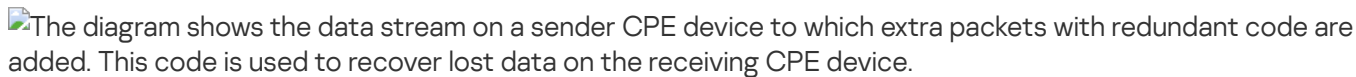
Enabling Forward Error Correction

The *Forward Error Correction (FEC)* functionality reduces the loss of traffic packets in links, especially for UDP applications, and the number of retransmissions, which lead to delays, and also recovers received data on the CPE device. Data recovery is provided by redundant encoding of the data stream on the device on the sending side.

We recommend using FEC on noisy links to reduce the packet loss and increase the speed of TCP connections.

The sender CPE encodes the stream of traffic packets egressing into the tunnel, adding redundant packets. The use of encoding on the sending and receiving sides may cause delays due to extra data processing. You can configure the degree of redundancy in the [settings of the SD-WAN Controller](#) or when you enable FEC.

The receiving CPE device buffers traffic packets received through the tunnel and decodes them, recovering lost packets, if possible. The general diagram of FEC is shown in the figure below.

The diagram shows the data stream on a sender CPE device to which extra packets with redundant code are added. This code is used to recover lost data on the receiving CPE device.

FEC diagram

You can enable FEC on an individual tunnel. The tunnels are displayed in a common table in the **Tunnels** section; in the graphical topology in the **Topology** section; and in the CPE device configuration on the **Tunnels** tab. Only tunnels built using the particular CPE device are displayed in the configuration of that device.

To enable FEC on a tunnel, use the following instructions:

- [Enabling FEC on a tunnel using the overall table of tunnels](#) .

To enable FEC on a tunnel using the overall table of tunnels:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.
2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.
This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.
3. Go to the **Tunnels** section.
A table of tunnels is displayed.
4. Click **Management** next to the tunnel and in the drop-down list, select **FEC/reordering**.
5. This opens a window; in that window, select the **Override** check box to configure FEC on the tunnel.
6. In the **Redundancy ratio (original/redundant packet)** drop-down list, select the degree of redundancy of transmitted traffic packets, which is the ratio between the original packets and extra packets containing redundant code. The default setting is **0:0 FEC off** and the functionality is not active.
7. In the **Timeout** field, enter the maximum time, in milliseconds, during which a traffic packet can stay in the queue for FEC to apply. Range of values: 1 to 1000.
8. Click **Save**.

- [Enabling FEC on a tunnel using the graphical topology](#) .

To enable FEC on a tunnel using the graphical topology:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Topology** section.

The SD-WAN topology is displayed.

4. Click the tunnel to open a window and in that window, click **FEC/reordering**.

5. This opens a window; in that window, select the **Override** check box to configure FEC on the tunnel.

6. In the **Redundancy ratio (original/redundant packet)** drop-down list, select the degree of redundancy of transmitted traffic packets, which is the ratio between the original packets and extra packets containing redundant code. The default setting is **0:0 FEC off** and the functionality is not active.

7. In the **Timeout** field, enter the maximum time, in milliseconds, during which a traffic packet can stay in the queue for FEC to apply. Range of values: 1 to 1000.

8. Click **Save**.

- [Enabling FEC on a tunnel in the configuration of an individual CPE device](#) 

To enable Dampening on a tunnel in the configuration of a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays the current configuration of the CPE device. This tab also displays the table of **Out-of-band management** CPE device configurations.

3. Select the **Tunnels** tab.

A table of tunnels is displayed.

4. Click **Management** next to the tunnel and in the drop-down list, select **FEC/reordering**.

5. This opens a window; in that window, select the **Override** check box to configure FEC on the tunnel.

6. In the **Redundancy ratio (original/redundant packet)** drop-down list, select the degree of redundancy of transmitted traffic packets, which is the ratio between the original packets and extra packets containing redundant code. The default setting is **0:0 FEC off** and the functionality is not active.

7. In the **Timeout** field, enter the maximum time, in milliseconds, during which a traffic packet can stay in the queue for FEC to apply. Range of values: 1 to 1000.

8. Click **Save**.

9. In the upper part of the settings area, click **Save** to save CPE device settings.

Determining the effective MTU in a link

Kaspersky SD-WAN can determine the supported MTU (maximum transmission unit) size on tunnels between two devices (a CPE device and an SD-WAN gateway or between two CPE devices).

Determining the maximum MTU size on tunnels is necessary to ensure the passage of user traffic through the SD-WAN network when the MTU on the underlay network is too low, and fragmented packets are blocked on the subsequent hop (see the figure below).

Diagram of IP packets passing through devices on the network, where fragmented packets are dropped

Example of a link with a reduced MTU size and fragmented packet getting dropped

The supported MTU size is calculated by sending variable-payload LLDP packets through all tunnels on the CPE device and the SD-WAN gateway. The minimum detectable MTU size is 1280 bytes, and the maximum size is 1500 bytes.

The supported MTU size is calculated:

- When the CPE device is turned on.
- With the frequency set in the [topology.link.pmtud.scheduler.interval.sec](#) property of the SD-WAN Controller. By default, the frequency is set to 86,400 seconds.

- Manually when you request it.

You can calculate the supported MTU size on an individual tunnel. The tunnels are displayed in a common table in the **Tunnels** section; in the graphical topology in the **Topology** section; and in the CPE device configuration on the **Tunnels** tab. Only tunnels built using the particular CPE device are displayed in the configuration of that device.

Supported MTU sizes are displayed in the **MTU** column of the tunnel table. If the value has not been calculated yet, the *Unknown* value is displayed.

To calculate the MTU on a tunnel, use the following instructions:

- [Calculating the MTU on a tunnel using the overall table of tunnels](#) 

To calculate the MTU on a tunnel using the overall table of tunnels:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Tunnels** section.

A table of tunnels is displayed.

4. Click **Management** next to the tunnel and in the drop-down list, select **Check MTU**.

The test result is displayed in the **MTU** column.


- [Calculating the MTU on a tunnel in the configuration of a CPE device](#) 

To calculate the MTU on a tunnel in the configuration of a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays the current configuration of the CPE device. This tab also displays the table of **Out-of-band management** CPE device configurations.

3. Select the **Tunnels** tab.

A table of tunnels is displayed.

4. Click **Management** next to the tunnel and in the drop-down list, select **Check MTU**.

The test result is displayed in the **MTU** column.

Kaspersky SD-WAN checks whether fragmentation of traffic packets is supported on CPE devices. A packet fragmentation test is started automatically. When each CPE device is enabled, it sends two ICMP requests to the IP addresses that you specified when [creating](#) or [editing](#) SD-WAN interfaces of the WAN type or in the configuration file of the controller.

The ICMP requests have a packet size of 1600 bytes. If at least one of these requests receives a response, a conclusion is made that the CPE device supports packet fragmentation. You can view the result of the fragmentation test result in the **Fragmentation** column of the [table of CPE devices](#) or the link table.

Traffic encryption

Traffic encryption is a mechanism of securing the exchange of traffic between [CPE devices](#) through tunnels. For example, you can encrypt traffic when sending data between devices over a tunnel built on top of an unsecured Internet connection.

The [SD-WAN Controller](#) automatically generates keys for encrypting and decrypting traffic and sends them to CPE devices. Traffic is encrypted on the source device with an encryption key before being sent to the tunnel. The destination device receives traffic from the tunnel and decrypts it with the decryption key.

The keys are regularly updated to deprive third parties of the opportunity to encrypt or decrypt the transmitted traffic if a key is intercepted. You can specify the length of time after which the keys are updated on CPE devices using the `Dtopology.Link.encryption.key.update.interval.minutes` [property](#) of the SD-WAN Controller.

Traffic encryption is supported only on CPE devices running Kaspersky SD-WAN software.

If traffic encryption is enabled on a CPE device, all outbound tunnels that involve this device send encrypted traffic (including new tunnels that will be established later).

If traffic encryption is disabled on a CPE device, it sends unencrypted traffic. Note that if you disable traffic encryption on a device that previously encrypted its outgoing traffic, the keys generated by the SD-WAN Controller for encrypting and decrypting traffic are deleted from all associated devices.

Traffic encryption can also be enabled or disabled on tunnels. For example, you can enable traffic encryption on a CPE device, but disable it on a tunnel established with the participation of this device. When enabling or disabling traffic encryption on a tunnel, you must configure both the outgoing and incoming tunnels in the same way.

Traffic encryption on a CPE device

If traffic encryption is enabled on a CPE device, encrypted traffic is transmitted through all tunnels established with its participation. The exception is cases when you enable traffic encryption on the device, but disable it on an individual tunnel.

You can enable or disable traffic encryption in a CPE template or an individual device. When you enable or disable traffic encryption in a CPE template, it is automatically enabled or disabled on all devices that are using that template. By default, traffic encryption is disabled.

To enable or disable traffic encryption in a CPE template:

1. In the menu, go to the **SD-WAN** → **CPE templates** subsection.
A table of CPE templates is displayed.

2. Click the CPE template.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. Select the **Tunnel encryption** tab.

The traffic encryption policy is displayed.

4. In the **Default encryption policy** drop-down list, select **Enabled** or **Disabled**.

5. In the upper part of the settings area, click **Save** to save CPE template settings.

To enable or disable traffic encryption on an individual CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays the current configuration of the CPE device. This tab also displays the table of **Out-of-band management** CPE device configurations.

3. Select the **Tunnel encryption** tab.

The traffic encryption policy is displayed.

4. Select the **Override** check box to ignore the applied CPE template and make the settings in the selected tab editable. This check box is cleared by default.

5. In the **Default encryption policy** drop-down list, select **Enabled** or **Disabled**.

6. In the upper part of the settings area, click **Save** to save CPE device settings.

Traffic encryption on a link

You can enable or disable traffic encryption on an individual tunnel. The tunnels are displayed in a common table in the **Tunnels** section; in the graphical topology in the **Topology** section; and in the CPE device configuration on the **Tunnels** tab. Only tunnels built using the particular CPE device are displayed in the configuration of that device.

When enabling or disabling traffic encryption on an individual tunnel, you must configure the opposite-direction tunnel in the same way. To enable or disable traffic encryption on a tunnel, use the following instructions:

- [Enabling or disabling traffic encryption on a tunnel using the overall table of tunnels](#) 

To enable or disable traffic encryption on a tunnel using the overall table of tunnels:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Tunnels** section.

A table of tunnels is displayed.

4. Click **Management** next to the tunnel and in the drop-down list, select **Set encryption**.

5. This opens a window; in that window, select or clear the **Override** check box to enable or disable encryption of the selected tunnel. This check box is cleared by default.

6. Select or clear the **Enable encryption** check box. This check box is cleared by default.

7. Click **Save**.

- [Enabling or disabling traffic encryption on a tunnel using the graphical topology](#) 

To enable or disable traffic encryption on a tunnel using the graphical topology:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Topology** section.

The SD-WAN topology is displayed.

4. Click the tunnel to open a window and in that window, click **Set encryption**.

5. This opens a window; in that window, select or clear the **Override** check box to enable or disable encryption of the selected tunnel. This check box is cleared by default.

6. Select or clear the **Enable encryption** check box. This check box is cleared by default.

7. Click **Save**.

- [Enabling or disabling traffic encryption on a tunnel in the configuration of a CPE device](#) 

To enable or disable traffic encryption on a tunnel in the configuration of a CPE device:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays the current configuration of the CPE device. This tab also displays the table of **Out-of-band management** CPE device configurations.

3. Select the **Tunnels** tab.

A table of tunnels is displayed.

4. Click **Management** next to the tunnel and in the drop-down list, select **Set encryption**.

5. This opens a window; in that window, select or clear the **Override** check box to enable or disable encryption of the selected tunnel. This check box is cleared by default.

6. Select or clear the **Enable encryption** check box. This check box is cleared by default.

7. In the upper part of the settings area, click **Save** to save CPE device settings.

Configuring topology

[Tunnels](#) form a *topology* that determines the connectivity of devices in the data plane and is responsible for optimizing the passage of traffic of transport services. In Kaspersky SD-WAN, devices can be arranged in one of the following topologies:

- *Hub-and-Spoke* is the default topology in which tunnels between CPE devices are established through the SD-WAN Gateway.
- *Full-Mesh* is a topology in which direct tunnels are created between all CPE devices.
- *Partial-Mesh* is a topology in which direct tunnels are established between some of the CPE devices.

A role is assigned to each CPE device: standard device or SD-WAN Gateway. Standard devices automatically establish tunnels with SD-WAN Gateways, which in turn establish tunnels with all devices on the network, including other gateways. By default, all devices are standard devices. The SD-WAN Gateway role is required to build a Hub-and-Spoke topology.

Standard devices can be assigned topology tags to make them transit devices. If two devices are assigned the same topology tag, a tunnel is automatically created between them. Other devices establish tunnels through transit devices. Topology tags and transit devices are used to build Full-Mesh and Partial-Mesh topologies.

In addition to topology tags, the solution also uses standard [tags](#) that allow you to classify CPE devices by various criteria, such as model, software version, or street address of the location, and perform group actions on the devices, such as firmware updates. Topology tags and standard tags are not related to each other in any way.

About the Hub-and-Spoke topology

The *Hub-and-Spoke topology* is a network architecture in which a hub site is connected to multiple spoke sites for the purposes of exchanging traffic. This topology is the most common for SD-WAN network design because it simplifies network management and provides a higher level of security by routing traffic through the hub site where traffic analysis and categorization is performed. The Hub-and-Spoke topology also enables more efficient use of bandwidth by optimizing and prioritizing traffic at the hub site.

This section describes examples of such topologies that you can build using Kaspersky SD-WAN. Note that when building a Hub-and-Spoke topology, you can use [QoS](#) to limit the bandwidth available to CPE devices or specific traffic classes.

Hub-and-Spoke without connection between remote offices

The figure below shows a topology in which remote locations are connected to the central office and cannot directly communicate with each other. SD-WAN networks built using this topology are easy to design and maintain, because all necessary network services and applications are located in the central data center.

CPE devices registering with the orchestrator are automatically included in the management transport service with the Leaf role and can be behind NAT (Network Address Translation) and PAT (Port Address Translation). In this topology, direct exchange of traffic between devices is not possible.

The diagram shows two locations connected to the central office.

Hub-and-Spoke topology without connection between remote offices

Hub-and-Spoke with connection between remote offices through the central office

The figure below shows a topology in which remote locations can communicate with each other through the central office. CPE devices registering with the orchestrator are automatically included in the transport service and can be behind NAT and PAT.

The diagram shows two locations connected to the central office and to each other.

Hub-and-Spoke topology with connection between remote offices through the central office


About Full-Mesh and Partial-Mesh topologies

Kaspersky SD-WAN supports Full-Mesh and Partial-Mesh topologies. To implement these topologies, the network administrator must grant permission to dynamically create direct tunnels between CPE devices.

Creating direct tunnels between CPE devices improves the performance of Kaspersky SD-WAN thanks to the following:

- Improved qualitative characteristics of the physical link between CPE devices, such as delay, loss, and jitter, compared to the CPE1 → gateway → CPE2 transit scenario of the [Hub-and-Spoke topology](#).
- Greater bandwidth of the direct physical link between CPE devices than in the CPE1 → gateway → CPE2 transit scenario.
- Conservation of the bandwidth of the physical link and of hardware resources of the gateway when using direct links.

An example of the Full-Mesh topology is shown in the figure below. In this topology, all CPE devices create direct tunnels among themselves, using all available physical links. This allows routing traffic between CPE1 and CPE2 directly. However, with a large number of CPEs and tunnels, this topology can be extremely taxing on the resources of the SD-WAN Controller.

Diagram: all devices are directly interconnected

Full-Mesh topology

An example of the Partial-Mesh topology is shown in the figure below. This topology is used when direct tunnels between some CPE devices may be undesirable, for example, for administrative reasons, or impossible for technical reasons. In this topology, the network administrator can group devices in such a way that devices in the same group communicate directly with each other, while communication with devices from other groups happens through a transit device.

Diagram: devices in a group are interlinked directly and linked to devices from other groups through a gateway

Partial-Mesh topology

A CPE device can belong to multiple groups at the same time, as shown in the figure below.

Diagram: CPE1 and CPE2 in group 1, CPE3 and CPE4 in group 2, CPE2 and CPE3 in group 3,

Partial-Mesh topology, CPE devices in multiple groups

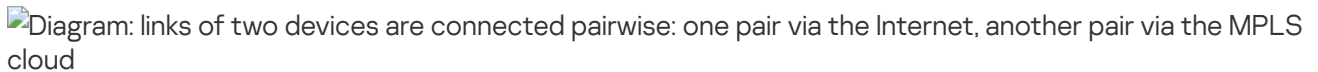
When creating direct tunnels between CPE devices, depending on the type of connectivity of the devices through physical links, the following variants of overlay connectivity are possible:

- All physical links have direct IP connectivity to each other (see the figure below). Thanks to the connectivity within the Internet, CPE devices can establish the maximum number of direct tunnels among themselves.

Diagram: all links of two devices are directly connected

Full physical connectivity between CPE devices

- Physical links have partial connectivity (see the figure below). In the example shown in the figure below, the Internet cloud and the MPLS cloud are not interconnected, so tunnels can only be established through WAN interfaces belonging to the same cloud. CPE1:WAN0 → CPE2:WAN1 and CPE1:WAN1 → CPE2:WAN0 tunnels cannot be created.

Diagram: links of two devices are connected pairwise: one pair via the Internet, another pair via the MPLS cloud

Partial physical connectivity between CPE devices

Other overlay network connectivity scenarios are also possible if IP connectivity between WAN interfaces of CPE devices within the same cloud is impossible for other reasons, for example, when using an MPLS topology that does not support direct communication between devices, or due to the presence of NAT/PAT or ACL on the Internet.

Creating a Hub-and-Spoke topology

A Hub-and-Spoke topology is built using roles that you assign to CPE devices. You can assign the role of a standard CPE device or an SD-WAN Gateway. Standard devices establish tunnels with each other through SD-WAN Gateways.

By default, all devices are assigned the standard device role. To build a Hub-and-Spoke topology, at least one device must be assigned the SD-WAN Gateway role.

You can assign a role in a CPE template or to an individual device. When you assign a role in a CPE template, the role is automatically assigned to all devices that are using that template. To build a Hub-and-Spoke topology, use the following instructions:

- [Assigning a role in a CPE template](#) .

To assign a role in a CPE template:

1. In the menu, go to the **SD-WAN** → **CPE templates** subsection.

A table of CPE templates is displayed.

2. Click the CPE template.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. Select the **Topology** tab.

The topology tag settings are displayed.

4. In the **Role** drop-down list, select the role:

- **CPE** for a standard CPE device.
- **Gateway** for an SD-WAN Gateway.

5. In the upper part of the settings area, click **Save** to save CPE template settings.

- [Assigning a role to an individual CPE device](#) 

To assign a role to an individual CPE device:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Topology tags** section.

The topology tag settings are displayed.

4. In the **Switch** drop-down list, select the CPE device.

5. In the **Role** drop-down list, select the role:

- **CPE** for a standard CPE device.
- **Gateway** for an SD-WAN Gateway.

6. In the upper part of the page, click **Save**.

You can also assign a role in the CPE device configuration.

To assign a role in the CPE device configuration:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays the current configuration of the CPE device. This tab also displays the table of **Out-of-band management** CPE device configurations.

3. Select the **Topology** tab.

The topology tag settings are displayed.

4. Select the **Override** check box to ignore the applied CPE template and make the settings in the selected tab editable. This check box is cleared by default.

5. In the **Role** drop-down list, select the role:

- **CPE** for a standard CPE device.
- **Gateway** for an SD-WAN Gateway.

6. In the upper part of the settings area, click **Save** to save CPE device settings.

Creating Full-Mesh and Partial-Mesh topologies

Full-Mesh and Partial-Mesh topologies are built using topology tags that you assign to CPE devices. You can only assign topology tags to standard devices. If two devices are assigned the same topology tag, a tunnel is automatically created between them.

In a Full-Mesh topology, all devices are assigned the same topology tag.

In a Partial-Mesh topology, devices are divided into groups based on the tags assigned to them, and communication between the devices happens through transit devices, which are devices to which tags from all groups are assigned.

You can assign a topology tag in a CPE template or to an individual device. When you assign a topology tag in a CPE template, the tag is automatically assigned to all devices that are using that template. To assign topology tags, use the following instructions:

- [Assigning a topology tag in a CPE template](#) 

To assign a topology tag in a CPE template:

1. In the menu, go to the **SD-WAN** → **CPE templates** subsection.

A table of CPE templates is displayed.

2. Click the CPE template.


The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. Select the **Topology** tab.

The topology tag settings are displayed.

4. Make sure that in the **Role** drop-down list, the **CPE** option is selected. The **Gateway** is not used to build Full-Mesh and Partial-Mesh topologies.

5. If you want to build a Partial-Mesh topology, to use a device as a transit device, select the **Transit CPE** check box. Transit devices are necessary to connect groups of devices together and make it possible for other devices to establish tunnels through these transit devices.

6. In the **Topology tags** field, enter a topology tag and click the add button . Devices with the same topology tags automatically establish direct tunnels with each other.

To build a Full-Mesh topology, assign the same topology tags to all devices.

To build a Partial-Mesh topology, assign topology tags to devices based on which group they belong to. Also assign all tags used in the topology to the transit device to make sure that all device groups are added to the topology.

The topology tag is assigned and displayed below the **Topology tags** field.

7. In the upper part of the settings area, click **Save** to save CPE template settings.

- [Assigning a topology tag to an individual CPE device](#) 

To assign a topology tag to an individual CPE device:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.


3. Go to the **Topology tags** section.

The topology tag settings are displayed.

4. In the **Switch** drop-down list, select the CPE device.

5. Make sure that in the **Role** drop-down list, the **CPE** option is selected. The **Gateway** is not used to build Full-Mesh and Partial-Mesh topologies.

6. If you want to build a Partial-Mesh topology, to use a device as a transit device, select the **Transit CPE** check box. Transit devices are necessary to connect groups of devices together and make it possible for other devices to establish tunnels through these transit devices.

7. In the **Topology tags** field, enter a topology tag and click the add button  plus button. Devices with the same topology tags automatically establish direct tunnels with each other.

To build a Full-Mesh topology, assign the same topology tags to all devices.

To build a Partial-Mesh topology, assign topology tags to devices based on which group they belong to. Also assign all tags used in the topology to the transit device to make sure that all device groups are added to the topology.

The topology tag is assigned and displayed below the **Topology tags** field.

8. In the upper part of the page, click **Save**.


You can also assign a topology tag in the CPE device configuration.

To assign a topology tag in the CPE device configuration:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device.


The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Configuration** tab is selected, which displays the current configuration of the CPE device. This tab also displays the table of **Out-of-band management** CPE device configurations.

3. Select the **Topology** tab.

The topology tag settings are displayed.

4. Select the **Override** check box to ignore the applied CPE template and make the settings in the selected tab editable. This check box is cleared by default.



5. In the **Switch** drop-down list, select the CPE device.

6. Make sure that in the **Role** drop-down list, the **CPE** option is selected. The **Gateway** is not used to build Full-Mesh and Partial-Mesh topologies.
7. If you want to build a Partial-Mesh topology, to use a device as a transit device, select the **Transit CPE** check box. Transit devices are necessary to connect groups of devices together and make it possible for other devices to establish tunnels through these transit devices.
8. In the **Topology tags** field, enter a topology tag and click the add button . Devices with the same topology tags automatically establish direct tunnels with each other.
To build a Full-Mesh topology, assign the same topology tags to all devices.
To build a Partial-Mesh topology, assign topology tags to devices based on which group they belong to. Also assign all tags used in the topology to the transit device to make sure that all device groups are added to the topology.
The topology tag is assigned and displayed below the **Topology tags** field.
9. In the upper part of the settings area, click **Save** to save CPE device settings.

If necessary, you can remove a topology tag in a CPE template or on an individual device. To remove topology tags, use the following instructions:

- [Removing a topology tag in a CPE template](#) 

To remove a topology tag in a CPE template:

1. In the menu, go to the **SD-WAN** → **CPE templates** subsection.
A table of CPE templates is displayed.
2. Click the CPE template.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.
3. Select the **Topology** tab.
The topology tag settings are displayed.
4. Click the delete button  next to the topology tag.
The topology tag is removed and is no longer displayed.
5. In the upper part of the settings area, click **Save** to save CPE template settings.

- [Removing a topology tag from an individual CPE device](#) 

To remove a topology tag from an individual CPE device:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Topology tags** section.

The topology tag settings are displayed.

4. In the **Switch** drop-down list, select the CPE device.

5. Click the delete button next to the topology tag.

The topology tag is removed and is no longer displayed.

6. In the upper part of the page, click **Save**.

You can also remove a topology tag in the CPE device configuration.

To remove a topology tag in the CPE device configuration:

1. In the menu, go to the **SD-WAN** → **CPE** section.

A table of CPE devices is displayed.

2. Click the CPE device.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon. By default, the **Configuration** tab is selected, which displays the current configuration of the CPE device. This tab also displays the table of **Out-of-band management** CPE device configurations.

3. Select the **Topology** tab.

The topology tag settings are displayed.

4. Select the **Override** check box to ignore the applied CPE template and make the settings in the selected tab editable. This check box is cleared by default.

5. Click the delete button next to the topology tag.

The topology tag is removed and is no longer displayed.

6. In the upper part of the settings area, click **Save** to save CPE device settings.

Quality of Service (QoS)

A *Quality of Service* (QoS) policy ensures data transfer in accordance with the requirements set for traffic classes. In Kaspersky SD-WAN, the following components contribute to the quality of service:

- *Traffic classes* are used to queue and prioritize traffic. For example, one of the classes can be used for real-time traffic that requires minimizing packet loss.
- *Traffic classifiers* determine whether or not to trust [DSCP values](#) (Differentiated Services Code Point) set in the traffic packet header fields; they also map DSCP values to traffic classifiers.
- *QoS rules* determine whether the bandwidth of traffic processed by traffic classifiers is limited.
- *Constraints* are used in [transport services](#) to comply with service level agreements (SLA). You can create two types of constraints:
 - *Manual TE* constraints are used to add Manual-TE paths to transport services. When configuring this type of constraints, you can enable the use of an Auto-SPF path if Manual-TE paths are not available.
 - *Threshold constraints* are used to build Auto-TE routes in transport services based on threshold values of monitoring indicators.

If a tunnel used in a transport service reaches the threshold values of the selected monitoring indicators, this tunnel is completely or partially excluded from the Auto-TE path calculation. Partially excluded tunnels can be taken into account when calculating the Auto-TE path if there are no alternative tunnels satisfying the constraint.

For example, you can create a constraint that completely excludes from the Auto-TE path calculation those tunnels that have reached the packet loss threshold. Thus, in a transport service that uses this constraint, traffic only travels through tunnels that have low packet loss.

- *Traffic classification rules* are used to identify traffic with particular values of the L2 – L4 header fields, as well as traffic of specified applications, in the overall stream of traffic. For each traffic classification rule, you must specify a sequence number and select a default action, which allows or prohibits further routing of the traffic. Classification rules are added to traffic filters.
- *Traffic filters* are used to ensure security by blocking excessive or dangerous traffic, to classify traffic, and to comply with SLA requirements for applications. Each filter consists of one or more traffic classification rules.

A maximum of 8 traffic queues can be used on the WAN and LAN interfaces. For each queue, you must specify the minimum and maximum bandwidth as a percentage of the total bandwidth set for the interface as a whole. The sum total of all minimum bandwidth values specified for queues may not exceed 100%.

The queues are strict priority and unreserved bandwidth is first offered to traffic from the higher-priority queue. Each queue is guaranteed certain minimum bandwidth in accordance with its specified minimum bandwidth value. An upper limit on the maximum bandwidth for higher-priority queues is necessary to allow traffic from lower-priority queues to still be transmitted.

You can configure queues when [creating](#) or [editing](#) WAN interfaces. Due to the fact that Kaspersky SD-WAN does not support creating LAN interfaces, queues can only be configured for LAN interfaces that already exist.

Service providers can use different QoS policies to mark queues in their networks and meet SLA requirements for the passage of client traffic. Therefore, when CPE devices are connected to links of different service providers, the CPE devices can flexibly relabel traffic of different queues for each WAN interface. To configure relabelling, you must change the value of the type of service (hereinafter also referred to as ToS) when configuring queues on the SD-WAN interface.

You can edit only the ToS values of the external (tunnel) headers of traffic packets going out of the WAN interfaces. ToS values of internal traffic packet headers cannot be edited.

Traffic classes

This section describes how to configure traffic classes.

Default traffic classes

Kaspersky SD-WAN has default traffic classes for processing and filtering different types of traffic (see the table below). You can create new traffic classes or modify existing ones. Default traffic classes are suitable for most deployment scenarios, and we do not recommend changing them.

Default traffic classes

Name	Internal tag	Queue	KOver	Exclude when computing path
Best effort	0	0	0	Yes
Business normal	1	1	1	No
Business critical	2	2	1	No
Video	3	3	1	No
Conference	4	4	1	No
Signaling	5	5	1	No
Real time	6	6	1	No
Network control	7	7	1	No

The default settings presented in the table are described in the instructions for [creating and editing traffic classes](#).

Creating or editing traffic classes

[Default traffic classes](#) are suitable for most Kaspersky SD-WAN deployment scenarios, and we do not recommend changing them.

You can create or modify 4 to 8 traffic classes in an SD-WAN instance template, or edit traffic classes in an already deployed SD-WAN instance. If you create traffic classes in an SD-WAN instance template and use that template to deploy an individual instance, the same traffic classes are automatically created in the deployed instance.

To create and edit traffic classes, use the following instructions:

- [Creating traffic classes in an SD-WAN instance template](#) ².

In one of the traffic classes you create, you must put *control traffic* that is used to manage the SD-WAN infrastructure and configure its components, including setting up and managing tunnels, exchanging routing information between devices, and monitoring the status and performance of the network. We recommend to assign control traffic to the highest priority to ensure efficient and reliable functioning of the network.

To create traffic classes in an SD-WAN instance template:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance templates** section.
A table of SD-WAN instance templates is displayed.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays the name of the SD-WAN instance template.
2. Select the **Traffic classes** tab.
A table of traffic classes is displayed.
3. Click **Edit**.
4. This opens a window; in that window, click **+ Traffic class** to add a traffic class.
5. In the **Name** column, enter a name for the traffic class.
6. In the **Queue** column, select the number of the queue into which you want to place traffic of the selected class. The higher the value, the higher the priority of the traffic class. You cannot specify the same priority for multiple traffic classes.
7. In the **KOver** column, select the overcommitment ratio of the traffic bandwidth, which sets the multiplier by which the bandwidth dedicated to the class can be increased if the total bandwidth is not fully utilized.
8. If you need to ignore the bandwidth available to the traffic class when calculating the route, select the **Exclude when computing path** check box. When this check box is selected, you cannot select the **KOver** ratio for the traffic class. By default, the check box is selected for the last traffic class in the table (**Best effort**).
9. In the **Default traffic class** drop-down list, select the class in which you want to place all traffic that is not included in other classes. By default, the last traffic class in the table is selected (**Best effort**).
10. In the **Control traffic class** drop-down list, select the class in which you want to place control traffic. By default, the first traffic class in the table is selected (**Network control**).
11. In the **Maximum reserved bandwidth (%)** drop-down list, select the percentage of the maximum traffic transfer rate that can be available for one of the created traffic classes. Range of values: 10 to 90. The default setting is **90**.
12. Click **Ok**.
13. In the upper part of the settings area, click **Save** to save the configuration of the SD-WAN instance template.

- [Editing traffic classes in an SD-WAN instance template](#) 

To edit a traffic class in an SD-WAN instance template:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance templates** section.

A table of SD-WAN instance templates is displayed.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays the name of the SD-WAN instance template.

2. Select the **Traffic classes** tab.

A table of traffic classes is displayed.

3. Click **Edit**.

4. This opens a window; in that window, edit the settings that you want to change. For a description of the settings, refer to the instructions for creating traffic classes in an SD-WAN instance template.

5. Click **Ok**.

6. In the upper part of the settings area, click **Save** to save the configuration of the SD-WAN instance template.

- [Editing traffic classes in an already deployed SD-WAN instance](#) 

To edit traffic classes in an already deployed SD-WAN instance:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **QoS** section.

The **Traffic classes** tab, which is selected by default, displays the table of traffic classes.

4. Click **Edit**.

5. This opens a window; in that window, in the **Name** column, enter a name for the traffic class.

6. In the **Queue** column, select the number of the queue into which you want to place traffic of the selected class. The higher the value, the higher the priority of the traffic class. You cannot specify the same priority for multiple traffic classes.

7. In the **KOver** column, select the overcommitment ratio of the traffic bandwidth, which sets the multiplier by which the bandwidth dedicated to the class can be increased if the total bandwidth is not fully utilized.

8. If you need to ignore the bandwidth available to the traffic class when calculating the route, select the **Exclude when computing path** check box. When this check box is selected, you cannot select the **KOver** ratio for the traffic class. By default, the check box is selected for the last traffic class in the table (**Best effort**).

9. In the **Maximum reserved bandwidth (%)** drop-down list, select the percentage of the maximum traffic transfer rate that can be available for one of the created traffic classes. Range of values: 10 to 90. The default setting is **90**.

10. Click **Ok**.

Traffic classifiers

This section describes how to configure traffic classes.

Creating a traffic classifier

You can create a traffic classifier in an SD-WAN instance template or in an instance that is already deployed. If you create a traffic classifier in an SD-WAN instance template and use that template to deploy an individual instance, the same traffic classifier is automatically created in the deployed instance.

To create a traffic classifier, use the following instructions:

- [Creating a traffic classifier in an SD-WAN instance template](#) 

To create a traffic classifier in an SD-WAN instance template:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance templates** section.

A table of SD-WAN instance templates is displayed.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays the name of the SD-WAN instance template.

2. Select the **Traffic classifiers** tab.

A table of traffic classes is displayed.

3. Click **+ Classifier**.

4. This opens a window; in that window, in the **Name** field, enter the name of the traffic classifier.

5. In the **Type** list, select one of the following values:

- **Trust** is a classifier that trusts the [DSCP values](#) set in the header fields of traffic packets. This is the default setting.
- **Untrust** is a classifier that does not trust the DSCP values set in the traffic packet header fields.

6. If you selected **Trust** in the **Type** list, map the classes to DSCP values in the traffic packet headers:

- a. In the **Traffic class** column, select the class into which you want to place the traffic.
- b. In the **External tag** column, click **Select** next to the package header that must contain the necessary DSCP value.
- c. Select the check boxes next to the displayed DSCP values that must be present in the packet header for the traffic to be placed in the selected class.
- d. Click **Ok**.

7. If in the **Type** list you selected **Untrust**, select the class in which you want to place all traffic in the **Traffic class** class drop-down list.

8. Click **Create**.

The traffic classifier is created and displayed in the table.

9. In the upper part of the settings area, click **Save** to save the configuration of the SD-WAN instance template.

- [Creating a traffic classifier in an already deployed SD-WAN instance](#) 

To create a traffic classifier in an already deployed SD-WAN instance:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **QoS** section.

The **Traffic classes** tab, which is selected by default, displays the table of traffic classes.

4. Select the **Traffic classifiers** tab.

A table of traffic classes is displayed.

5. Click **+ Classifier**.

6. This opens a window; in that window, in the **Name** field, enter the name of the traffic classifier.

7. In the **Type** list, select one of the following values:

- **Trust** is a classifier that trusts the [DSCP values](#) set in the header fields of traffic packets. This is the default setting.
- **Untrust** is a classifier that does not trust the DSCP values set in the traffic packet header fields.

8. If you selected **Trust** in the **Type** list, map the classes to DSCP values in the traffic packet headers:

- a. In the **Traffic class** column, select the class into which you want to place the traffic.
- b. In the **External tag** column, click **Select** next to the package header that must contain the necessary DSCP value.
- c. Select the check boxes next to the displayed DSCP values that must be present in the packet header for the traffic to be placed in the selected class.
- d. Click **Ok**.

9. If in the **Type** list you selected **Untrust**, select the class in which you want to place all traffic in the **Traffic class** class drop-down list.

10. Click **Create**.

The traffic classifier is created and displayed in the table.

Editing a traffic classifier

You can edit a traffic classifier in an SD-WAN instance template or in an instance that is already deployed. For a description of the settings, see the [instructions for creating a traffic classifier](#).

To edit a traffic classifier in an SD-WAN instance template:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance templates** section.

A table of SD-WAN instance templates is displayed.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays the name of the SD-WAN instance template.

2. Select the **Traffic classifiers** tab.

A table of traffic classes is displayed.

3. Click **Management** next to the traffic classifier and in the drop-down list, select **Edit**.

4. This opens a window; in that window, edit the settings that you want to change.

5. Click **Save**.

6. In the upper part of the settings area, click **Save** to save the configuration of the SD-WAN instance template.

To edit a traffic classifier in an already deployed SD-WAN instance:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **QoS** section.

The **Traffic classes** tab, which is selected by default, displays the table of traffic classes.

4. Select the **Traffic classifiers** tab.

A table of traffic classes is displayed.

5. Click **Management** next to the traffic classifier and in the drop-down list, select **Edit**.

6. This opens a window; in that window, edit the settings that you want to change.

7. Click **Save**.

Deleting a traffic classifier

You can delete a traffic classifier in an SD-WAN instance template or in an instance that is already deployed. Deleted traffic classifiers cannot be restored.

To delete a traffic classifier in an SD-WAN instance template:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance templates** section.

A table of SD-WAN instance templates is displayed.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays the name of the SD-WAN instance template.

2. Select the **Traffic classifiers** tab.

A table of traffic classes is displayed.

3. Click **Management** next to the traffic classifier and in the drop-down list, select **Delete**.

The traffic classifier is deleted and is no longer displayed in the table.

4. In the upper part of the settings area, click **Save** to save the configuration of the SD-WAN instance template.

To delete a traffic classifier in an already deployed SD-WAN instance:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **QoS** section.

The **Traffic classes** tab, which is selected by default, displays the table of traffic classes.

4. Select the **Traffic classifiers** tab.

A table of traffic classes is displayed.

5. Click **Management** next to the traffic classifier and in the drop-down list, select **Delete**.

6. In the confirmation window, click **Delete**.

The traffic classifier is deleted and is no longer displayed in the table.

QoS rules

This section describes how to configure QoS rules.

Creating a QoS rule

You can create a QoS rule in an SD-WAN instance template or in an instance that is already deployed. If you create a QoS rule in an SD-WAN instance template and use that template to deploy an individual instance, the same QoS rule is automatically created in the deployed instance.

Before creating a QoS rule, you must [create a traffic classifier](#).

To create a QoS rule, use the following instructions:

- [Creating a QoS rule in an SD-WAN instance template](#) ?

To create a QoS rule in an SD-WAN instance template:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance templates** section.

A table of SD-WAN instance templates is displayed.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays the name of the SD-WAN instance template.

2. Select the **QoS rules** tab.

A table of QoS rules is displayed.

3. Click **+ QoS rule**.

4. This opens a window; in that window, in the **Name** field, enter the name of the QoS rule.

5. In the **Classifier** drop-down list, select the previously created traffic classifier that you want to use in the QoS rule.

6. Configure traffic bandwidth limiting:

- If you do not want to limit the bandwidth of traffic processed by the previously selected classifier, select the **Unlimited** check box.
- If you want to limit the bandwidth of traffic processed by the previously selected classifier, clear the **Unlimited** check box.

This check box is selected by default.

QoS rules that do not limit traffic bandwidth provide users with the highest network performance, especially when dealing with applications and services with high bandwidth requirements. However, if your network is not resource-rich, bandwidth limiting may help avoid issues with congestion, performance, and traffic filtering for applications that have different priorities.

7. If you cleared the **Unlimited** check box, configure the traffic bandwidth limiting settings:

a. In the **MBR** field, enter the maximum bit rate. The default setting is **1**.

b. In the **Speed type** drop-down list, select the units of measurement for the maximum bit rate:

- **Kbit/sec** (selected by default)
- **Mbit/sec**
- **Gbit/sec**

c. If you have selected a classifier of the **Trust** type in the **Classifier** drop-down list, in the **Classifier** drop-down list, in the **Maximum reserved bandwidth (%)** column, specify the percentage of the total bit rate available to each class. The sum total of the values specified for each class must equal 100%.

8. Click **Create**.

The QoS rule is created and displayed in the table.

9. In the upper part of the settings area, click **Save** to save the configuration of the SD-WAN instance template.

- [Creating a QoS rule in an already deployed SD-WAN instance](#) 

To create a QoS rule in an already deployed SD-WAN instance:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of controller nodes.

3. Go to the **QoS** section.

The **Traffic classes** tab, which is selected by default, displays the table of traffic classes.

4. Select the **QoS rules** tab.

A table of QoS rules is displayed.

5. Click **+ QoS rule**.

6. This opens a window; in that window, in the **Name** field, enter the name of the QoS rule.

7. In the **Classifier** drop-down list, select the previously created traffic classifier that you want to use in the QoS rule.

8. Configure traffic bandwidth limiting:

- If you do not want to limit the bandwidth of traffic processed by the previously selected classifier, select the **Unlimited** check box.
- If you want to limit the bandwidth of traffic processed by the previously selected classifier, clear the **Unlimited** check box.

This check box is selected by default.

QoS rules that do not limit traffic bandwidth provide users with the highest network performance, especially when dealing with applications and services with high bandwidth requirements. However, if your network is not resource-rich, bandwidth limiting may help avoid issues with congestion, performance, and traffic filtering for applications that have different priorities.

9. If you cleared the **Unlimited** check box, configure the traffic bandwidth limiting settings:

a. In the **MBR** field, enter the maximum bit rate. The default setting is **1**.

b. In the **Speed type** drop-down list, select the units of measurement for the maximum bit rate:

- **Kbit/sec** (selected by default)
- **Mbit/sec**
- **Gbit/sec**

c. If you have selected a classifier of the **Trust** type in the **Classifier** drop-down list, in the **Classifier** drop-down list, in the **Maximum reserved bandwidth (%)** column, specify the percentage of the total bit rate available to each class. The sum total of the values specified for each class must equal 100%.

10. Click **Create**.

The QoS rule is created and displayed in the table.

Editing a QoS rule

You can edit a QoS rule in an SD-WAN instance template or in an instance that is already deployed. For a description of the settings, see the [instructions for creating a QoS rule](#).

To edit a QoS rule in an SD-WAN instance template:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance templates** section.

A table of SD-WAN instance templates is displayed.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays the name of the SD-WAN instance template.

2. Select the **QoS rules** tab.

A table of QoS rules is displayed.

3. Click **Management** next to the QoS rule and in the drop-down list, select **Edit**.

4. This opens a window; in that window, edit the settings that you want to change.

5. Click **Save**.

6. In the upper part of the settings area, click **Save** to save the configuration of the SD-WAN instance template.

To edit a QoS rule in an already deployed SD-WAN instance:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **QoS** section.

The **Traffic classes** tab, which is selected by default, displays the table of traffic classes.

4. Select the **QoS rules** tab.

A table of QoS rules is displayed.

5. Click **Management** next to the QoS rule and in the drop-down list, select **Edit**.

6. This opens a window; in that window, edit the settings that you want to change.

7. Click **Save**.

Deleting a QoS rule

You can delete a QoS rule in an SD-WAN instance template or in an instance that is already deployed. Deleted QoS rules cannot be restored.

To delete a QoS rule in an SD-WAN instance template:

1. In the menu, go to the **SD-WAN** → **SD-WAN instance templates** section.

A table of SD-WAN instance templates is displayed.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays the name of the SD-WAN instance template.

2. Select the **QoS rules** tab.

A table of QoS rules is displayed.

3. Click **Management** next to the QoS rule and in the drop-down list, select **Delete**.

The QoS rule is deleted and is no longer displayed in the table.

4. In the upper part of the settings area, click **Save** to save the configuration of the SD-WAN instance template.

To delete a QoS rule in an already deployed SD-WAN instance:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **QoS** section.

The **Traffic classes** tab, which is selected by default, displays the table of traffic classes.

4. Select the **QoS rules** tab.

A table of QoS rules is displayed.

5. Click **Management** next to the QoS rule and in the drop-down list, select **Delete**.

6. In the confirmation window, click **Delete**.

The QoS rule is deleted and is no longer displayed in the table.

Constraints

This section describes how to configure constraints.

Creating a Manual-TE constraint

Before creating a Manual-TE constraint, you must [create Manual-TE paths](#).

To create a Manual-TE constraint:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Constraints** section.

A table of Manual-TE constraints is displayed.

4. In the upper part of the page, click **+ Manual-TE constraint**.

5. This opens a window; in that window, in the **Name** field, enter the name of the Manual-TE constraint.

6. Select the **Use Manual-TE path** check box next to the Manual-TE paths that you want to add to the constraint. By default, the check boxes are cleared and no paths are added to the constraint.

7. To allow an Auto-SPF path to be used when no Manual-TE paths are available, select the **Ignore if no constrained path is found** check box next to the relevant Manual-TE paths. The check box can be selected only for paths that have the **Use Manual-TE path** check box selected. By default, the check boxes are cleared and Auto-SPF cannot be used as an alternative for all paths.

8. Click **Create**.

The Manual-TE constraint is created and displayed in the table.

Now you can specify the Manual-TE constraint in [transport service](#) settings to add Manual-TE paths contained in the constraint to the transport service.

Editing a Manual-TE constraint

To edit a Manual-TE constraint:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Constraints** section.

A table of Manual-TE constraints is displayed.

4. Click **Management** next to the Manual-TE constraint and in the drop-down list, select **Edit**.
5. This opens a window; in that window, edit the settings that you want to change. For a description of the settings, see the [instructions for creating a Manual-TE constraint](#).
6. Click **Save**.

Deleting a Manual-TE constraint

Deleted Manual-TE constraints cannot be restored.

To delete a Manual-TE constraint:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Constraints** section.

A table of Manual-TE constraints is displayed.

4. Click **Management** next to the Manual-TE constraint and in the drop-down list, select **Delete**.

5. In the confirmation window, click **Delete**.

The Manual-TE constraint is deleted and is no longer displayed in the table.

Creating a threshold constraint

Before creating a threshold constraint, you must [enable monitoring on tunnels](#).

To create a threshold constraint:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Constraints** section.

A table of Manual-TE constraints is displayed.

4. Select the **Thresholds** tab.

A table of threshold constraints is displayed.

5. In the upper part of the page, click **+ Threshold constraint**.
6. This opens a window; in that window, in the **Name** field, enter the name of the threshold constraint.
7. Select the **Do not use tunnels with threshold reached** check box next to monitoring indicators to have the threshold constraint exclude tunnels that have reached the threshold value of these indicators from the Auto-TE path calculation. By default, the **Do not use tunnels with threshold reached** check box is cleared and no monitoring indicators are used to exclude tunnels.
8. If necessary, select the **Ignore if no constrained path is found** check box next to the monitoring indicators to let the constraint include tunnels that have reached threshold values of these indicators in the Auto-TE path calculation when alternative tunnels do not exist. The check box can be selected only for tunnels that have the **Do not use tunnels with threshold reached** check box selected.

By default, the **Ignore if no constrained path is found** check box is cleared and the constraint excludes all tunnels that have reached the threshold values of the selected monitoring indicators from the Auto-TE path calculation.
9. Click **Create**.

The constraint is created and displayed in the table.

You can specify the constraint in [transport service](#) settings to use it for automatic calculation of the path.

Editing a threshold constraint

To edit a threshold constraint:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.
2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.
3. Go to the **Constraints** section.

A table of Manual-TE constraints is displayed.
4. Select the **Thresholds** tab.

A table of threshold constraints is displayed.
5. Click **Management** next to the threshold constraint and in the drop-down list, select **Edit**.
6. This opens a window; in that window, edit the settings that you want to change. For a description of the settings, see the [instructions for creating a threshold constraint](#).
7. Click **Save**.

Deleting a threshold constraint

Deleted threshold constraints cannot be restored.

To delete a threshold constraint:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Constraints** section.

A table of Manual-TE constraints is displayed.

4. Select the **Thresholds** tab.

A table of threshold constraints is displayed.

5. Click **Management** next to the threshold constraint and in the drop-down list, select **Delete**.

6. In the confirmation window, click **Delete**.

The threshold constraint is deleted and is no longer displayed in the table.

Traffic classification rules

This section describes how to configure traffic classification rules.

Creating a traffic classification rule

To create a traffic classification rule:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Traffic filters** section.

A table of traffic filters is displayed.

4. Select the **Rules** tab.

A table of traffic classification rules is displayed.

5. In the upper part of the page, click + **Qualification rule**.

6. This opens a window; in that window, in the **Name** field, enter the name of the traffic classification rule.

7. On the **L2 fields** tab, select the check boxes next to the L2 fields whose values the rule must use to identify traffic in the overall data stream. If the check box is selected, enter or select the required value. You can use the values of the following fields to identify traffic:

- **Outer VLAN ID** – range of values: 1 to 2094.
- **Outer VLAN PCP** – range of values: 0 to 7.
- **Source MAC**.
- **Source MAC mask**.
- **Destination MAC**.
- **Destination MAC mask**.
- **Ethertype** – possible values:
 - **0x0800** (selected by default)
 - **0x86dd**
 - **0x0806**

8. On the **L3 fields** tab, select the check boxes next to the L3 fields whose values the rule must use to identify traffic in the overall data stream. If the check box is selected, enter or select the required value. You can use the values of the following fields to identify traffic:

- **Protocol** – Possible values:
 - **IPv4**
 - **IPv6**
- **Source IP** – IPv4 address or IPv6 address depending on the selected protocol
- **Source IP prefix length** – Range of values for the IPv4 address: from 0 to 32; for IPv6 address: from 0 to 128
- **Destination IP** – IPv4 address or IPv6 address depending on the selected protocol
- **Destination IP prefix length** – Range of values for the IPv4 address: from 0 to 32; for IPv6 address: from 0 to 128
- **DSCP**
- **TOS**

9. On the **L4 fields** tab, select the check boxes next to the L4 fields whose values the rule must use to identify traffic in the overall data stream. If the check box is selected, enter or select the required value. You can use the values of the following fields to identify traffic:

- **IP protocol**
- **Source port list**
- **Destination port list**

- **ICMP type number**

10. On the **DPI** tab, select the application whose traffic the rule must identify in the overall data stream:

- a. Select the **Application** check box.
- b. In the drop-down list, select the application.

DPI (Deep Packet Inspection) classification is not supported for traffic generated by CPE devices.

11. Click **Create**.

The traffic classification rule is created and displayed in the table.

You can use a traffic classification rule when [creating a traffic filter](#).

Example of a created traffic classification rule:

You can create a traffic classification rule with the following parameters:

- On the **L2 fields** tab, in the **Outer VLAN ID** field, enter **1**.
- On the **L2 fields** tab, in the **Outer VLAN PCP** field, enter **3**.
- On the **L3 fields** tab, in the **Protocol** drop-down list, select **IPv4**.
- On the **L3 fields** tab, in the **Source IP** field, enter the **192.168.2.0/24** address.
In this case, the rule identifies traffic with the following properties in the overall data stream:
 - Outer VLAN tag – 1
 - Outer PCP tag – 3
 - Protocol – IPv4
 - Source IP address – 192.168.2.0/24Traffic that is missing at least one of these properties is not identified.

Editing a traffic classification rule

To edit a traffic classification rule:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Traffic filters** section.

A table of traffic filters is displayed.

4. Select the **Rules** tab.

A table of traffic classification rules is displayed.

5. Click **Management** next to the traffic classification rule and in the drop-down list, select **Edit**.

6. This opens a window; in that window, edit the settings that you want to change. For a description of the settings, see the [instructions for creating a traffic classification rule](#).

7. Click **Save**.

Deleting a traffic classification rule

Deleted traffic classification rules cannot be restored.

To delete a traffic classification rule:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Traffic filters** section.

A table of traffic filters is displayed.

4. Select the **Rules** tab.

A table of traffic classification rules is displayed.

5. Click **Management** next to the traffic classification rule and in the drop-down list, select **Delete**.

6. In the confirmation window, click **Delete**.

The traffic classification rule is deleted and is no longer displayed in the table.

Traffic filters

This section describes how to configure traffic filters.

Creating a traffic filter

Before creating a traffic filter, you must [create at least one traffic classification rule](#).

To create a traffic filter:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.
2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.
This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.
3. Go to the **Traffic filters** section.
A table of traffic filters is displayed.
4. In the upper part of the page, click **+ Traffic filter**.
5. This opens a window; in that window, in the **Name** field, enter the name of the traffic filter.
6. In the **Sequence** field, enter the sequential number of the traffic classification rule. The rule with the lowest number is processed first. Range of values: 1 to 998. You cannot specify the same sequence number for multiple rules. The default setting is 10.
7. In the **Qualification rule** drop-down list, select a previously created traffic classification rule that you want to add to the filter.
8. In the **Action** drop-down list, select the action that the traffic classification rule must apply to the traffic identified in the overall data stream:
 - **Permit** — Allow further routing of the traffic. This is the default setting.
 - **Deny** — Block further routing of the traffic.
9. Click **Add** to add a previously created traffic classification rule to the filter. You can add multiple rules.
10. In the **Default action (if sequence=999)** drop-down list, select the action that you want to apply to all other traffic:
 - **Permit** — Allow further routing of the traffic. This is the default setting.
 - **Deny** — Block further routing of the traffic.
11. Click **Create**.
The traffic filter is created and displayed in the table.

You can use a traffic filter when creating [transport services](#).

Editing a traffic filter

To edit a traffic filter:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Traffic filters** section.

A table of traffic filters is displayed.

4. Click **Management** next to the traffic filter and in the drop-down list, select **Edit**.

5. This opens a window; in that window, edit the settings that you want to change. For a description of the settings, see the [instructions for creating a traffic filter](#).

6. Click **Save**.

Deleting a traffic filter

Deleted traffic filters cannot be restored.

To delete a traffic filter:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **Traffic filters** section.

A table of traffic filters is displayed.

4. Click **Management** next to the traffic filter and in the drop-down list, select **Delete**.

5. In the confirmation window, click **Delete**.

The traffic filter is deleted and is no longer displayed in the table.

Transport services

Transport services, which are mechanisms used to transfer traffic between remote locations, play a critical role in ensuring reliable, efficient, and secure communication throughout the SD-WAN infrastructure. Transport services are constructed on top of segments and consist of [service interfaces](#).

Kaspersky SD-WAN supports creating the following transport services:

- Point-to-Point (P2P)
- Point-to-Multipoint (P2M)
- Multipoint-to-Multipoint (M2M)
- IP multicast
- L3 VPN

When creating transport services, you can add backup service interfaces. Backup and primary service interfaces can be created on the same CPE device. A backup service interface makes it possible to continue data transfer in the event of a failure of the primary service interface.

The settings of each individual transport service form a service topology that determines the type of connectivity between client devices connected to standard CPE devices and SD-WAN gateways.

Point-to-Point (P2P) transport service

Point-to-Point (E-line in the MEF classification, hereinafter also referred to as the P2P service) is a transport service within involves establishing a connection between two service interfaces of CPE devices on top of an Ethernet network for efficient and secure communication without the use of intermediate network devices. This is especially relevant when using applications that must transmit information in real time or exchange large files.

When creating a P2P service, you must specify the service interface that sends traffic (hereinafter referred to as the source interface) and the service interface that receives traffic (hereinafter referred to as the destination interface).

Creating a P2P service

Before creating a P2P service, you must complete the following steps:

- Activate CPE devices.
- Create a constraint ([Manual-TE](#) or [threshold](#)).
- [Create service interfaces](#).
- [Create a traffic filter](#).
- [Create a QoS rule](#).

To create a P2P transport service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **P2P services** section.

A table of P2P services is displayed.

4. In the upper part of the page, click **+ P2P service**.

5. This opens a window; in that window, in the **Name** field, enter the name of the transport service.

6. In the **Constraint** drop-down list, select a previously created constraint that you want to add to the transport service.

7. In the **Balancing mode** drop-down list, select the balancing mode for evenly distributing traffic among the tunnels to prevent congestion of individual tunnels and prevent performance issues for users:

- **Per-flow** — Balancing across flows (sessions). During transmission, flows are evenly distributed across the tunnels. This is the default setting.
- **Per-packet** — Per-packet balancing. During transmission, packets are distributed evenly across the tunnels.
- **Broadcast** — Packets are sent to all tunnels simultaneously to prevent losses.

8. If necessary, in the **Description** field, enter a brief description of the P2P service.

9. In the **Switch** and **Port** drop-down lists on the left, select the CPE device and the service interface created on it that you want to use as the source interface.

10. In the **Switch** and **Port** drop-down lists on the right, select the CPE device and the service interface created on it that you want to use as the destination interface.

11. To display service interfaces that were previously added to transport services in the **Port** drop-down lists, select the **Show used interfaces** check box. This check box is cleared by default.

12. To swap the values selected in the **Port** drop-down list for the source interface and the destination interface, select the **Switch interfaces** check box. This check box is cleared by default.

13. If necessary, add a backup source interface through which traffic must be transmitted if the primary interface goes out of service:

a. Select the **Use backup interface** check box. This check box is cleared by default.

b. In the **Backup switch** and **Backup port** drop-down lists, select the CPE device and the service interface created on it that you want to use as the backup service interface.

c. To display service interfaces that were previously added to transport services in the **Backup port** drop-down list, select the **Show used interfaces** check box. This check box is cleared by default.

If the primary service interface goes back online, the transport service continues to use the backup service interface.

14. In the **Inbound filter** drop-down lists on the left and right, select the previously created traffic filter for the source and destination interfaces.
15. In the **QoS** drop-down list, select the previously created QoS rule for the source interface.
16. If you need to monitor the status of both service interfaces and when one of them becomes disabled, automatically disable the other, select the **Propagate interface status** check box. This check box is cleared by default. This check box cannot be selected when the **Use backup interface** check box is selected.

When the service interface that was disabled first goes back online, the second service interface that was automatically disabled also resumes operation. This functionality works only if the Access encapsulation type is used on the service interfaces. The encapsulation type is selected when [creating the service interface](#).
17. Click **Create**.

The P2P service is created and displayed in the table.

Editing a P2P service

To edit a P2P service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.
2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.
3. Go to the **P2P services** section.

A table of P2P services is displayed.
4. Click **Management** next to the P2P service and in the drop-down list, select **Edit**.
5. This opens a window; in that window, edit the settings that you want to change. For a description of the settings, see the [instructions for creating a P2P service](#).
6. Click **Save**.

Deleting a P2P service

Deleted P2P services cannot be restored

To delete a P2P service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **P2P services** section.

A table of P2P services is displayed.

4. Click **Management** next to the P2P service and in the drop-down list, select **Delete**.

5. If you need to delete the service interfaces added to the P2P service, select the **Delete associated service interfaces** check box in the confirmation window.

6. Click **Delete**.

The P2P service is deleted and is no longer displayed in the table.

Viewing statistics of a P2P service

To view the statistics of a P2P service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **P2P services** section.

A table of P2P services is displayed.

4. Click **Management** next to the P2P service and in the drop-down list, select **Statistics**.

This opens a window with statistics of the P2P service.

Configuring the display of devices in a P2P service topology

To configure the display of devices in a P2P service topology

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.







3. Go to the **P2P services** section.

A table of P2P services is displayed.

4. Click **Management** next to the P2P service and in the drop-down list, select **Service topology**.

This opens a window with the P2P service topology.

5. If you need to change the relative position of CPE devices in the topology, use the following buttons in the upper part of the window:

- **Manual** to manually change the relative position of CPE devices.
- **Automatically** to select one of the values in the drop-down list to automatically generate the transport service topology:
 - **Physical simulation** – CPE devices are arranged in the diagram approximately in accordance with their actual location relative to each other. For example:
A topology of four CPE devices, constructed approximately in accordance with their real location.
 - **Random** – The arrangement of CPE devices is randomized. For example:
A topology of four CPE devices constructed randomly.
 - **Circle** – Devices are arranged in accordance with a ring topology. For example:
A ring topology of four CPE devices.
 - **Breadthfirst** – CPE devices are arranged horizontally. For example:
A topology of four CPE devices constructed horizontally.
 - **Concentric** – CPE devices are arranged concentrically. For example:
A concentric topology of four CPE devices.
 - **Grid** – CPE devices are arranged in accordance with a grid topology. For example:
A grid topology of four CPE devices.

6. If you want to display labels of CPE devices, select the following check boxes:

- **Name**
- **IP address**

These check boxes are cleared by default.

7. If necessary, display the tunnels used in a segment of two CPE devices:

- a. Select the **Segments** check box. This check box is cleared by default.
- b. Select devices from the drop-down lists below or in the diagram.

8. To open the window with control buttons and additional information about the CPE device or tunnel, click the icon of the device or tunnel.

Restarting a P2P service

You may need to restart a P2P service if a problem occurs during its operation (for example, with the network connection) or if changes made to the current configuration necessitate a restart.

To restart a P2P service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **P2P services** section.

A table of P2P services is displayed.

4. Click **Management** next to the P2P service and in the drop-down list, select **Reprovision**.

5. In the confirmation window, click **Reprovision**.

This opens a window with a success message about the restart of the P2P service. The SD-WAN Controller adds the P2P service to all CPE devices that were previously used in this service.

Point-to-Multipoint (P2M) transport service

Point-to-Multipoint (E-tree in the MEF classification, hereinafter also referred to as the P2M service) is a transport service involving a single service interface of a CPE device transmitting traffic in a centralized way to multiple interfaces on top of an Ethernet network based on a *tree* topology.

The hierarchical structure of the P2M service simplifies network management, ensures the reliability of data transfer without duplication, and improves the scalability of the network by accommodating new devices.

When creating a P2M service, you must assign one of the following roles to each service interface:

- **Root** is a service interface that can send traffic to interfaces with any role. At least one service interface must be assigned this role.
- **Leaf** is a service interface that can send traffic only to interfaces with the Root role.

Frames complying with the IEEE 802.1Q and 802.1AD standards can be transmitted.

Creating a P2M service

Before creating a P2M service, you must complete the following steps:

- Activate CPE devices.
- Create a constraint ([Manual-TE](#) or [threshold](#)).
- [Create service interfaces](#).

- Define the topology of the transport service and assign roles to service interfaces.
- [Create a traffic filter.](#)
- [Create a group of OpenFlow interfaces.](#)
- [Create a QoS rule.](#)

To create a P2M transport service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of controller nodes.

3. Go to the **P2M services** section.

A table of P2M services is displayed.

4. In the upper part of the page, click **+ P2M service**.

5. This opens a window; in that window, in the **Name** field, enter the name of the transport service.

6. In the **Constraint** drop-down list, select a previously created constraint that you want to add to the transport service.

7. In the **Balancing mode** drop-down list, select the balancing mode for evenly distributing traffic among the tunnels to prevent congestion of individual tunnels and prevent performance issues for users:

- **Per-flow** — Balancing across flows (sessions). During transmission, flows are evenly distributed across the tunnels. This is the default setting.
- **Per-packet** — Per-packet balancing. During transmission, packets are distributed evenly across the tunnels.
- **Broadcast** — Packets are sent to all tunnels simultaneously to prevent losses.

8. In the **MAC learn mode** drop-down list, select the action that you want to apply to a series of frames when the first frame is sent to the controller to learn the source MAC address:

- **Learn and flood** means the controller remembers the MAC address of the source and checks for the presence of the destination MAC address in the MAC address table. If the destination MAC address is not in the table, the series of frames is sent to all service interfaces added to the transport service, except for the interface on which the series of frames originally arrived. Default value.
- **Learn and drop** means the controller remembers the MAC address of the source and checks for the presence of the destination MAC address in the MAC address table. If the destination MAC address is not in the table, the series of frames is dropped.

If the destination MAC address is present in the MAC address table, the series of frames is sent to the destination service interface.

9. In the **MAC age (sec.)** field, enter the time period in seconds during which you want to keep entries in the MAC table on the controller. Range of values: 10 to 65,535. The default setting is 300.
10. In the **MAC table overload** drop-down list, select the policy for processing new MAC addresses when the MAC table of the controller is full:
 - **Flood** means traffic with destination MAC addresses that have not been learned previously is transmitted as BUM traffic (Broadcast, unknown-unicast, and multicast). Default value.
 - **Drop** means that traffic with previously destination MAC addresses that have not been learned previously is dropped.
11. In the **MAC table size** field, enter the maximum number of entries in the MAC table on the controller. Range of values: 0 to 65,535. 0 means the number of entries is not limited. The default setting is 100.
12. In the **Mode** drop-down list, select whether you want to use the Default Forwarding Interface (DFI), to which unknown unicast traffic is sent, in the transport service:
 - **Classic** if you do not want to use DFI. Default value.
 - **DFI with FIB on root and leafs** if you want to use DFI on the service interface with the root role. The number of service interfaces with the leaf role is not limited. Backup service interfaces can be added for each service interface.
 - **DFI with FIB on leaf** if you want to use DFI on the service interface with the root role. The number of service interfaces with the leaf role is not limited. Service interfaces with the leaf role must be on the same CPE device. Backup service interfaces can be added for each service interface.

Reserve service interfaces with the leaf role must be on the same CPE device, which must be different from the device hosting the primary service interfaces.
13. If necessary, in the **Description** field, enter a brief description of the transport service.
14. Click **Next** to proceed to the next group of settings.
15. In the **Switch** and **Port** drop-down lists on the right, select the CPE device and the service interface that you want to add to the transport service.
16. To display service interfaces that were previously added to transport services in the **Port** drop-down list, select the **Show used interfaces** check box. This check box is cleared by default.
17. In the **QoS** drop-down list, select the previously created QoS rule for the service interface.
18. In the **Inbound filter** drop-down list, select the previously created traffic filter for the service interface.
19. In the **Role** drop-down list, select the role of the service interface:
 - **Leaf**
 - **Root**
20. If necessary, add a backup service interface through which traffic must be transmitted if the primary interface goes out of service:
 - a. Select the **Use backup interface** check box. This check box is cleared by default.

- b. In the **Backup switch** and **Backup port** drop-down lists, select the CPE device and the service interface created on it that you want to use as the backup service interface.
- c. To display service interfaces that were previously added to transport services in the **Backup port** drop-down list, select the **Show used interfaces** check box. This check box is cleared by default.

If the primary service interface goes back online, the transport service continues to use the backup service interface.

21. To assign the DFI role to the service interface, select the **Default Forwarding Interface** check box. This check box cannot be selected if in the **Role** drop-down list for the service interface, you selected **Leaf**.
22. Click **+ Add** to add the service interface to the transport service.
The service interface is displayed in the lower part of the window. You can delete a service interface by clicking **Delete** next to it.
23. Click **Next** to proceed to the next group of settings.
24. In the **Group** drop-down list, select the previously created group of OpenFlow interfaces that you want to add. A service interface is automatically created on top of each OpenFlow interface in the group, and that service interface is added to the transport service.
25. In the **QoS** drop-down list, select the previously created QoS rule for service interfaces created on top of OpenFlow interfaces.
26. In the **VLAN ID** field, enter the outer VLAN tag value for service interfaces created on top of OpenFlow interfaces. You must take into account the following limitations regarding automatic creation of service interfaces on top of OpenFlow interfaces:
 - Only service interfaces with the VLAN encapsulation type can be created.
 - The VLAN tag value must be the same on all service interfaces.
27. In the **Role** drop-down list, select a role for service interfaces automatically created on top of OpenFlow interfaces:
 - **Leaf**
 - **Root**
28. Click **+ Add** to add the group of OpenFlow interfaces to the transport service.
The automatically created service interfaces are displayed in the lower part of the window. You can delete a service interface by clicking **Delete** next to it.
29. Click **Create**.
The P2M service is created and displayed in the table.

Editing a P2M service

To edit a P2M service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **P2M services** section.

A table of P2M services is displayed.

4. Click **Management** next to the P2M service and in the drop-down list, select **Edit**.

5. This opens a window; in that window, edit the settings that you want to change. For a description of the settings, see the [instructions for creating a P2M service](#).

6. Click **Save**.

Deleting a P2M service

Deleted P2M services cannot be restored.

To delete a P2M service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **P2M services** section.

A table of P2M services is displayed.

4. Click **Management** next to the P2M service and in the drop-down list, select **Delete**.

5. If you need to delete the service interfaces added to the P2M service, select the **Delete associated service interfaces** check box in the confirmation window.

6. Click **Delete**.

The P2M service is deleted and is no longer displayed in the table.

Viewing statistics of a P2M service

To view the statistics of a P2M service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **P2M services** section.

A table of P2M services is displayed.

4. Click **Management** next to the P2M service and in the drop-down list, select **Statistics**.

This opens a window with statistics of the P2M service.

Viewing the MAC table of a P2M service

To view the MAC table of a P2M service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **P2M services** section.

A table of P2M services is displayed.

4. Click **Management** next to the P2M service and in the drop-down list, select **MAC table**.

This opens a window with the MAC table of the P2M service.

5. To find a specific MAC address, enter it in the field and click **Find by MAC**.

6. To clear the MAC address table, click **Clear**.

Configuring the display of devices in a P2M service topology

To configure the display of devices in a P2M service topology

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.







3. Go to the **P2M services** section.

A table of P2M services is displayed.

4. Click **Management** next to the P2M service and in the drop-down list, select **Service topology**.

This opens a window with the P2M service topology.

5. If you need to change the relative position of CPE devices in the topology, use the following buttons in the upper part of the window:

- **Manual** to manually change the relative position of CPE devices.
- **Automatically** to select one of the values in the drop-down list to automatically generate the transport service topology:
 - **Physical simulation** – CPE devices are arranged in the diagram approximately in accordance with their actual location relative to each other. For example:
A topology of four CPE devices, constructed approximately in accordance with their real location.
 - **Random** – The arrangement of CPE devices is randomized. For example:
A topology of four CPE devices constructed randomly.
 - **Circle** – Devices are arranged in accordance with a ring topology. For example:
A ring topology of four CPE devices.
 - **Breadthfirst** – CPE devices are arranged horizontally. For example:
A topology of four CPE devices constructed horizontally.
 - **Concentric** – CPE devices are arranged concentrically. For example:
A concentric topology of four CPE devices.
 - **Grid** – CPE devices are arranged in accordance with a grid topology. For example:
A grid topology of four CPE devices.

6. If you want to display labels of CPE devices, select the following check boxes:

- **Name**
- **IP address**

These check boxes are cleared by default.

7. If necessary, display the tunnels used in a segment of two CPE devices:

- a. Select the **Segments** check box. This check box is cleared by default.
- b. Select devices from the drop-down lists below or in the diagram.

8. To open the window with control buttons and additional information about the CPE device or tunnel, click the icon of the device or tunnel.

Restarting a P2M service

You may need to restart a P2M service if a problem occurs during its operation (for example, with the network connection) or if changes made to the current configuration necessitate a restart.

To restart a P2M service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **P2M services** section.

A table of P2M services is displayed.

4. Click **Management** next to the P2M service and in the drop-down list, select **Reprovision**.

5. In the confirmation window, click **Confirm**.

This opens a window with a success message about the restart of the P2M service. The SD-WAN Controller adds the P2M service to all CPE devices that were previously used in this service.

Multipoint-to-Multipoint (M2M) transport service

Multipoint-to-Multipoint (E-LAN in the MEF classification, hereinafter also referred to as the M2M service) is a transport service that involves establishing a peer connection between interfaces of CPE devices on top of the local Ethernet network for communication and joint performance of tasks in a common networking environment without a centralized controller and a clearly defined hierarchy.

To populate the MAC table on the SD-WAN Controller, the M2M service uses the so-called MAC learning mechanism. At the same time, a separate bridge domain is also organized on each CPE device and the CPE device contains a separate table of MAC addresses.

Creating an M2M service

Before creating an M2M service, you must complete the following steps:

- Activate CPE devices.
- Create a constraint ([Manual-TE](#) or [threshold](#)).
- [Create service interfaces](#).
- [Create a traffic filter](#).
- [Create a group of OpenFlow interfaces](#).
- [Create a QoS rule](#).

To create an M2M transport service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of controller nodes.

3. Go to the **M2M services** section.

A table of M2M services is displayed.

4. In the upper part of the page, click **+ M2M service**.

5. This opens a window; in that window, in the **Name** field, enter the name of the transport service.

6. In the **Constraint** drop-down list, select a previously created constraint that you want to add to the transport service.

7. In the **Balancing mode** drop-down list, select the balancing mode for evenly distributing traffic among the tunnels to prevent congestion of individual tunnels and prevent performance issues for users:

- **Per-flow** — Balancing across flows (sessions). During transmission, flows are evenly distributed across the tunnels. This is the default setting.
- **Per-packet** — Per-packet balancing. During transmission, packets are distributed evenly across the tunnels.
- **Broadcast** — Packets are sent to all tunnels simultaneously to prevent losses.

8. In the **MAC learn mode** drop-down list, select the action that you want to apply to a series of frames when the first frame is sent to the controller to learn the source MAC address:

- **Learn and flood** means the controller remembers the MAC address of the source and checks for the presence of the destination MAC address in the MAC address table. If the destination MAC address is not in the table, the series of frames is sent to all service interfaces added to the transport service, except for the interface on which the series of frames originally arrived. Default value.
- **Learn and drop** means the controller remembers the MAC address of the source and checks for the presence of the destination MAC address in the MAC address table. If the destination MAC address is not in the table, the series of frames is dropped.

If the destination MAC address is present in the MAC address table, the series of frames is sent to the destination service interface.

9. In the **MAC age (sec.)** field, enter the time period in seconds during which you want to keep entries in the MAC table on the controller. Range of values: 10 to 65,535. The default setting is 300.

10. In the **MAC table overload** drop-down list, select the policy for processing new MAC addresses when the MAC table of the controller is full:

- **Flood** means traffic with destination MAC addresses that have not been learned previously is transmitted as BUM traffic (Broadcast, unknown-unicast, and multicast). Default value.
- **Drop** means that traffic with previously destination MAC addresses that have not been learned previously is dropped.

11. In the **MAC table size** field, enter the maximum number of entries in the MAC table on the controller. Range of values: 0 to 65,535. 0 means the number of entries is not limited. The default setting is 100.

12. If necessary, in the **Description** field, enter a brief description of the transport service.

13. Click **Next** to proceed to the next group of settings.
14. In the **Switch** and **Port** drop-down lists on the right, select the CPE device and the service interface that you want to add to the transport service.
15. To display service interfaces that were previously added to transport services in the **Port** drop-down list, select the **Show used interfaces** check box. This check box is cleared by default.
16. In the **QoS** drop-down list, select the previously created QoS rule for the service interface.
17. In the **Inbound filter** drop-down list, select the previously created traffic filter for the service interface.
18. If necessary, add a reserve service interface through which traffic must be transmitted if the primary interface goes out of service:
 - a. Select the **Use backup interface** check box. This check box is cleared by default.
 - b. In the **Backup switch** and **Backup port** drop-down lists, select the CPE device and the service interface created on it that you want to use as the backup service interface.
 - c. To display service interfaces that were previously added to transport services in the **Backup port** drop-down list, select the **Show used interfaces** check box. This check box is cleared by default.

If the primary service interface goes back online, the transport service continues to use the reserve service interface.

19. Click **+ Add** to add the service interface to the transport service.

The service interface is displayed in the lower part of the window. You can delete a service interface by clicking **Delete** next to it.
20. Click **Next** to proceed to the next group of settings.
21. In the **Group** drop-down list, select the previously created group of OpenFlow interfaces that you want to add. A service interface is automatically created on top of each OpenFlow interface in the group, and that service interface is added to the transport service.
22. In the **QoS** drop-down list, select the previously created QoS rule for service interfaces created on top of OpenFlow interfaces.
23. In the **VLAN ID** field, enter the outer VLAN tag value for service interfaces created on top of OpenFlow interfaces. You must take into account the following limitations regarding automatic creation of service interfaces on top of OpenFlow interfaces:
 - Only service interfaces with the VLAN encapsulation type can be created.
 - The VLAN tag value must be the same on all service interfaces.
24. Click **+ Add** to add the group of OpenFlow interfaces to the transport service.

The automatically created service interfaces are displayed in the lower part of the window. You can delete a service interface by clicking **Delete** next to it.
25. Click **Create**.

The M2M service is created and displayed in the table.

Editing an M2M service

To edit an M2M service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **M2M services** section.

A table of M2M services is displayed.

4. Click **Management** next to the M2M service and in the drop-down list, select **Edit**.

5. This opens a window; in that window, edit the settings that you want to change. For a description of the settings, see the [instructions for creating an M2M service](#).

6. Click **Save**.

Deleting an M2M service

Deleted M2M services cannot be restored.

To delete an M2M service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **M2M services** section.

A table of M2M services is displayed.

4. Click **Management** next to the M2M service and in the drop-down list, select **Delete**.

5. If you need to delete the service interfaces added to the M2M service, select the **Delete associated service interfaces** check box in the confirmation window.

6. Click **Delete**.

The M2M service is deleted and is no longer displayed in the table.

Viewing statistics of an M2M service

To view the statistics of an M2M service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **M2M services** section.

A table of M2M services is displayed.

4. Click **Management** next to the M2M service and in the drop-down list, select **Statistics**.

This opens a window with statistics of the M2M service.

Viewing the MAC table of an M2M service

To view the MAC table of an M2M service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **M2M services** section.

A table of M2M services is displayed.

4. Click **Management** next to the M2M service and in the drop-down list, select **MAC table**.

This opens a window with the MAC table of the M2M service.

5. To find a specific MAC address, enter it in the field and click **Find by MAC**.

6. To clear the MAC address table, click **Clear**.

Configuring the display of devices in an M2M service topology

To configure the display of devices in an M2M service topology:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.







3. Go to the **M2M services** section.

A table of M2M services is displayed.

4. Click **Management** next to the M2M service and in the drop-down list, select **Service topology**.

This opens a window with the M2M service topology.

5. If you need to change the relative position of CPE devices in the topology, use the following buttons in the upper part of the window:

- **Manual** to manually change the relative position of CPE devices.
- **Automatically** to select one of the values in the drop-down list to automatically generate the transport service topology:
 - **Physical simulation** – CPE devices are arranged in the diagram approximately in accordance with their actual location relative to each other. For example:
A topology of four CPE devices, constructed approximately in accordance with their real location.
 - **Random** – The arrangement of CPE devices is randomized. For example:
A topology of four CPE devices constructed randomly.
 - **Circle** – Devices are arranged in accordance with a ring topology. For example:
A ring topology of four CPE devices.
 - **Breadthfirst** – CPE devices are arranged horizontally. For example:
A topology of four CPE devices constructed horizontally.
 - **Concentric** – CPE devices are arranged concentrically. For example:
A concentric topology of four CPE devices.
 - **Grid** – CPE devices are arranged in accordance with a grid topology. For example:
A grid topology of four CPE devices.

6. If you want to display labels of CPE devices, select the following check boxes:

- **Name**
- **IP address**

These check boxes are cleared by default.

7. If necessary, display the tunnels used in a segment of two CPE devices:

- a. Select the **Segments** check box. This check box is cleared by default.
- b. Select devices from the drop-down lists below or in the diagram.

8. To open the window with control buttons and additional information about the CPE device or tunnel, click the icon of the device or tunnel.

Restarting an M2M service

You may need to restart an M2M service if a problem occurs during its operation (for example, with the network connection) or if changes made to the current configuration necessitate a restart.

To restart an M2M service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **M2M services** section.

A table of M2M services is displayed.

4. Click **Management** next to the M2M service and in the drop-down list, select **Reprovision**.

5. In the confirmation window, click **Confirm**.

This opens a window with a success message about the restart of the M2M service. The SD-WAN Controller adds the M2M service to all CPE devices that were previously used in this service.

IP multicast transport service

IP multicast (hereinafter also referred to as the IP multicast service) is a transport service that involves building a multicast traffic distribution tree within a domain for transmitting data to multiple destination interfaces from a single source interface via the IP protocol. This helps optimize bandwidth usage and reduce network congestion when the number of devices is large.

The root of the multicast traffic distribution tree is the service interface to which the traffic source is connected. The source service interface transmits traffic to the service interfaces to which subscribers are connected (subscriber interfaces). Subscriber interfaces can connect to multicast groups with a destination address in the IP address range 224.0.0.0/4 via the IGMPv2/v3 protocol.

Traffic is transmitted through the IP multicast transport service as Ethernet frames with an IP payload without additional encapsulation.

Creating an IP multicast service

Before creating an IP multicast service, you must complete the following steps:

- Activate CPE devices.

- [Create service interfaces](#) for the traffic source and subscriber.
- [Create a QoS rule](#).

To create an IP multicast transport service:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.
2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.
This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.
3. Go to the **IP multicast services** section.
A table of IP multicast services is displayed.
4. In the upper part of the page, click **+ IP multicast service**.
5. This opens a window; in that window, in the **Name** field, enter the name of the transport service.
6. In the **Source switch** and **Source port** drop-down lists, select the CPE device and the service interface created on it that you want to use as the source interface.
7. To display service interfaces that were previously added to transport services in the **Source port** drop-down list, select the **Show used interfaces** check box. This check box is cleared by default.
8. In the **Querier IP** field, enter the IP address of the source interface.
9. If necessary, add a backup source interface through which traffic must be transmitted if the primary interface goes out of service:
 - a. Select the **Use backup interface** check box. This check box is cleared by default.
 - b. In the **Backup switch** and **Backup port** drop-down lists, select the CPE device and the service interface created on it that you want to use as the backup service interface.
 - c. To display service interfaces that were previously added to transport services in the **Backup port** drop-down list, select the **Show used interfaces** check box. This check box is cleared by default.
 - d. To stop using the backup service interface if the primary service interface is restored, select the **Recovery auto-return** check box. This check box is cleared by default.
 - e. To build the multicast traffic distribution tree not only on the primary service interface, but also on the backup service interface, select the **Backup multicast tree** check box. As long as the primary service interface remains active, traffic packets on the backup service interface are dropped. This check box is selected by default.
10. Select the **IGMP proxy** check box to use an IGMP proxy server. This function keeps sending traffic to active multicast groups that have at least one service subscriber interface connected. This check box is cleared by default.
11. In the **QoS** drop-down list, select the previously created QoS rule for the source interface.
12. Click **Next** to proceed to the next group of settings.

13. In the **Consumer switch** and **Consumer port** drop-down lists on the right, select the CPE device and the service interface created on it that you want to use as the subscriber interface.
14. To display service interfaces that have been previously added to transport services in the **Consumer port** drop-down list, select the **Show used interfaces** check box. This check box is cleared by default.
15. Click **+ Add** to add the service interface to the transport service.
The service interface is displayed in the lower part of the window. You can delete a service interface by clicking **Delete** next to it. To continue configuring the IP multicast service, you must add at least one service interface.
16. Click **Next** to proceed to the next group of settings.
17. In the **IP address** field, enter the IP address of the multicast group. Range of values: 224.0.0.0 to 239.255.255.255.
18. In the **Mask** drop-down list, select an IP address mask. Range of values: 24 to 32.
19. In the **GBR** drop-down list, select the guaranteed bit rate (GBR) for the multicast group.
20. Click **+ Add** to add the multicast group to the transport service.
The multicast group is displayed in the lower part of the window. You can delete a multicast group by clicking **Delete** next to it. To continue configuring the IP multicast service, you must add at least one Multicast group.
21. Click **Create**.

The IP multicast service is created and displayed in the table.

Editing an IP multicast service

To edit an IP multicast service:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.
2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.
This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.
3. Go to the **IP multicast services** section.
A table of IP multicast services is displayed.
4. Click **Management** next to the IP multicast service and in the drop-down list, select one of the following values:
 - **Edit source interfaces**
 - **Edit consumer interfaces**
 - **Edit multicast groups**
5. This opens a window; in that window, edit the settings that you want to change. For a description of the settings, see the [instructions for creating an IP multicast service](#).

6. Click **Save**.

Deleting an IP multicast service

Deleted IP multicast services cannot be restored.

To delete an IP multicast service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **IP multicast services** section.

A table of IP multicast services is displayed.

4. Click **Management** next to the IP multicast service and in the drop-down list, select **Delete**.

5. If you need to delete the service interfaces added to the IP multicast service, select the **Delete associated service interfaces** check box in the confirmation window.

6. Click **Delete**.

The IP multicast service is deleted and is no longer displayed in the table.

Viewing statistics of an IP multicast service

To view the statistics of an IP multicast service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **IP multicast services** section.

A table of IP multicast services is displayed.

4. Click **Management** next to the IP multicast service and in the drop-down list, select **Statistics**.

This opens a window with statistics of the IP multicast service.

L3 VPN transport service

L3 VPN (hereinafter also referred to as the L3 VPN service) is a transport service that involves establishing a secure IP connection between remote networks and/or locations through a shared physical infrastructure to provide L3 routing.

An L3 VPN service logically isolates transmitted traffic by creating virtual private networks.

When creating an L3 VPN service, you must create L3 interfaces on top of service interfaces of CPE devices or M2M services for traffic transmission. You can also specify static routes to manually define and configure routing within the VPN network.

[Full-Mesh topology](#) is supported, which allows interoperability between any networks.

Creating an L3 VPN service

Before creating an L3 VPN service, you must complete the following steps:

- Activate CPE devices.
- Create a constraint ([Manual-TE](#) or [threshold](#)).
- Create [service interfaces](#) or [M2M transport services](#).
- [Create a QoS rule](#).
- [Create a traffic filter](#).

To create an L3 VPN transport service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of controller nodes.

3. Go to the **L3 VPN services** section.

A table of L3 VPN services is displayed.

4. In the upper part of the page, click **+ L3 VPN services**.

5. This opens a window; in that window, in the **Name** field, enter the name of the transport service.

6. In the **Constraint** drop-down list, select a previously created constraint that you want to add to the transport service.

7. In the **Balancing mode** drop-down list, select the balancing mode for evenly distributing traffic among the tunnels to prevent congestion of individual tunnels and prevent performance issues for users:

- **Per-flow** — Balancing across flows (sessions). During transmission, flows are evenly distributed across the tunnels. This is the default setting.

- **Per-packet** — Per-packet balancing. During transmission, packets are distributed evenly across the tunnels.
 - **Broadcast** — Packets are sent to all tunnels simultaneously to prevent losses.
8. Click **Next** to proceed to the next group of settings.
 9. In the **Mode** drop-down list, select the type of the L3 interface:
 - **M2M service** — Create an L3 interface on top of an [M2M service](#).
 - **Service interface** — Create an L3 interface on top of the service interface.
 10. If in the **Mode** drop-down list, you selected **M2M service**, in the **M2M service** drop-down list, select the M2M service on top of which you want to create an L3 interface.
 11. If in the **Mode** drop-down list, you selected **Service interface**, configure the service interface:
 - a. In the **Switch** and **Port** drop-down lists on the right, select the CPE device and the service interface created on it on top of which you want to create the L3 interface.
 - b. In the **QoS** drop-down list, select the previously created QoS rule for the service interface.
 - c. In the **Inbound filter** drop-down list, select the previously created traffic filter for the service interface.
 - d. To display service interfaces that were previously added to transport services in the **Port** drop-down list, select the **Show used interfaces** check box. This check box is cleared by default.
 12. In the **IP** field, enter the IP address of the L3 interface.
 13. In the **Prefix length** field, enter the length of the L3 interface prefix. Range of values: 0 to 32.
 14. In the **MAC address** field, enter the MAC address of the service interface. You can generate a MAC address by clicking **Generate**.
 15. In the **ARP age (sec.)** field, enter the time period in seconds during which entries are kept in the ARP table on the SD-WAN Controller. Range of values: 1 to 65,535. The default setting is **200**.
 16. Click **+ Add** to create the L3 interface.

The L3 interface is displayed in the lower part of the window. You can delete an L3 interface by clicking **Delete** next to it. To continue configuring the L3 VPN service, you must add at least one L3 interface.
 17. Click **Next** to proceed to the next group of settings.
 18. In the **IP** field, enter the IP address of the destination node or network.
 19. In the **Prefix length** field, enter the length of the destination node prefix. Range of values: 0 to 32.
 20. In the **SVI** drop-down list, select the L3 interface that you want to use for sending traffic packets to the destination node.
 21. In the **Gateway** field, enter the IP address of the gateway for routing traffic packets.
 22. In the **Metric** field, enter a metric for the static route. The default setting is **0**.
 23. Click **+ Add** to create the static route.

The static route is displayed in the lower part of the window. You can delete a static route by clicking **Delete** next to it.

24. Click **Next** to proceed to the next group of settings.

25. Click **Create**.

The L3 VPN service is created and displayed in the table.

Editing an L3 VPN service

To edit an L3 VPN service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **L3 VPN services** section.

A table of L3 VPN services is displayed.

4. Click **Management** next to the L3 VPN service and in the drop-down list, select **Edit**.

5. This opens a window; in that window, edit the settings that you want to change. For a description of the settings, see the [instructions for creating an L3 VPN service](#).

6. Click **Save**.

Restarting an L3 VPN service

You may need to restart an L3 VPN service if a problem occurs during its operation (for example, with the network connection) or if changes made to the current configuration necessitate a restart.

To restart an L3 VPN service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **L3 VPN services** section.

A table of L3 VPN services is displayed.

4. Click **Management** next to the L3 VPN service and in the drop-down list, select **Reprovision**.

5. In the confirmation window, click **Confirm**.

This opens a window with a success message about the restart of the L3 VPN service. The SD-WAN Controller adds the L3 VPN service to all CPE devices that were previously used in this service.

Deleting an L3 VPN service

Deleted L3 VPN services cannot be restored.

To delete an L3 VPN service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **L3 VPN services** section.

A table of L3 VPN services is displayed.

4. Click **Management** next to the L3 VPN service and in the drop-down list, select **Delete**.

5. If you need to delete the service interfaces added to the L3 VPN service, select the **Delete associated service interfaces** check box in the confirmation window.

6. Click **Delete**.

The L3 VPN service is deleted and is no longer displayed in the table.

Viewing the ARP table of an L3 VPN service

To view the ARP table of an L3 VPN service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **L3 VPN services** section.

A table of L3 VPN services is displayed.

4. Click **Management** next to the L3 VPN service and in the drop-down list, select **ARP table**.

The page with the ARP table of the L3 VPN service is displayed.

Creating a static record in the ARP table of an L3 VPN service

To create a static record in the ARP table of an L3 VPN service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **L3 VPN services** section.

A table of L3 VPN services is displayed.

4. Click **Management** next to the L3 VPN service and in the drop-down list, select **ARP table**.

The page with the ARP table of the L3 VPN service is displayed.

5. In the upper part of the page, click **+ Static ARP record**.

6. This opens a window; in that window, in the **Switch** and **Port** drop-down lists, select the CPE device and the service interface created on it for which you want to assign a mapping between the IP address and the MAC address.

7. In the **IP address** field, enter the IP address of the service interface.

8. In the **MAC** field, enter the MAC address of the service interface.

9. Click **Create**.

The static record is created and displayed in the ARP table of the L3 VPN service.

Editing a static record in the ARP table of an L3 VPN service

To edit a static record in the ARP table of an L3 VPN service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **L3 VPN services** section.

A table of L3 VPN services is displayed.

4. Click **Management** next to the L3 VPN service and in the drop-down list, select **ARP table**.

The page with the ARP table of the L3 VPN service is displayed.

5. Click **Management** next to the static record and in the drop-down list, select **Edit**.
6. This opens a window; in that window, edit the settings that you want to change. For a description of the settings, see the [instructions for creating a static record in the ARP table of an L3 VPN service](#).
7. Click **Save**.

Deleting a static record in the ARP table of an L3 VPN service

Deleted static records in the ARP table of an L3 VPN service cannot be restored.

To delete a static record in the ARP table of an L3 VPN service:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.
2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.
This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.
3. Go to the **L3 VPN services** section.
A table of L3 VPN services is displayed.
4. Click **Management** next to the L3 VPN service and in the drop-down list, select **ARP table**.
The page with the ARP table of the L3 VPN service is displayed.
5. Click **Management** next to the static record and in the drop-down list, select **Delete**.
6. In the confirmation window, click **Delete**.
The static record is deleted and is no longer displayed in the ARP table of the L3 VPN service.

Viewing the routing table of an L3 VPN service

To view the routing table of an L3 VPN service:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.
2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.
This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.
3. Go to the **L3 VPN services** section.
A table of L3 VPN services is displayed.
4. Click **Management** next to the L3 VPN service and in the drop-down list, select **Routing table**.

This opens a window with the routing table of the L3 VPN service.

Adding a transport service in a CPE template

You can add transport services in a CPE template and then apply the template to devices. In this case, service interfaces for connecting to the added transport services are automatically created on top of the OpenFlow interfaces that correspond to the LAN interfaces of CPE devices to which the template is applied. In this way, you avoid the need to create service interfaces manually and individually connect each CPE device to transport services.

Before adding a transport service to the CPE template configuration, you must complete the following steps:

- Create a transport service in the SD-WAN Controller configuration menu.
- [Create a QoS rule](#).

Note that all settings must match the previously created transport service. For example, you must use the same name and type.

To add a transport service in the CPE template:

1. In the menu, go to the **SD-WAN** → **CPE templates** subsection.

A table of CPE templates is displayed.

2. Click the CPE template.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. Select the **Transport services** tab.

A table of transport services is displayed.

4. Click **+ Transport service**.

5. This opens a window; in that window, in the **Name** field, enter the name of the transport service.

6. In the **QoS name** field, enter the name of the previously created QoS rule that is used in the transport service.

7. In the **Stage** drop-down list, select the state of the CPE device in which you want to add the service interface to the transport service.

- **Before activation** — The service interface is added to the transport service before activating the CPE device. This is the default setting.
- **After activation** — The service interface is added to the transport service after activating the CPE device.

8. In the **Type** drop-down list, select one of the following values:

- **P2M**
- **M2M**

- **L3 VPN**

9. In the **Encapsulation** drop-down list, select the type of encapsulation on the service interface:

- **Access** (selected by default).
- **VLAN**
- **Q-in-Q**

10. If in the **Encapsulation** drop-down list, you selected **VLAN**, in the **VLAN ID** field, enter the outer VLAN tag. Range of values: 1 to 4094.

11. If in the **Encapsulation** drop-down list, you selected **Q-in-Q**, follow these steps:

- a. In the **VLAN ID** field, enter the outer VLAN tag. Range of values: 1 to 4094.
- b. In the **Inner VLAN ID** field, enter the inner VLAN tag. Range of values: 1 to 4094.

12. If in the **Type** drop-down list, you selected **P2M**, in the **Role** drop-down list, select the role of the service interface:

- **Leaf** is a service interface that can send traffic only to interfaces with the Root role.
- **Root** is a service interface that can send traffic to interfaces with any role. At least one service interface must be assigned this role.

13. If in the **Type** drop-down list, you selected **L3VPN**, follow these steps:

- a. In the **IP address** field, enter the IP address.
- b. In the **Mask** field, enter the subnet mask. Range of values: 0 to 32.

14. Click **Create**.

The transport service is created and displayed in the table.

15. In the upper part of the settings area, click **Save** to save CPE template settings.

Editing a transport service in a CPE template

To edit a transport service in the configuration of a CPE template:

1. In the menu, go to the **SD-WAN** → **CPE templates** subsection.

A table of CPE templates is displayed.

2. Click the CPE template.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.

3. Select the **Transport services** tab.

A table of transport services is displayed.

4. Click **Edit** next to the transport service.
5. This opens a window; in that window, edit the settings that you want to change. For a description of the settings, see the [instructions for adding a transport service in the CPE template](#).
6. Click **Save**.

Deleting a transport service from a CPE template

Transport services that are deleted in the CPE template cannot be restored.

To delete a transport service in the configuration of a CPE template:

1. In the menu, go to the **SD-WAN** → **CPE templates** subsection.
A table of CPE templates is displayed.
2. Click the CPE template.
The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon . By default, the **Information** tab is selected, which displays general information about the CPE template.
3. Select the **Transport services** tab.
A table of transport services is displayed.
4. Click **Delete** next to the transport service.
The transport service is deleted and is no longer displayed in the table.
5. In the upper part of the settings area, click **Save** to save CPE template settings.

Scenario: Directing application traffic to a transport service

Kaspersky SD-WAN supports application-level traffic identification. This functionality can be used when defining [QoS policies](#) for the following purposes:

- Directing application traffic through a specific WAN interface of a CPE device, for example, in accordance with the SLA values of path metrics.
- Dropping the traffic of a certain application on the CPE device to prevent this traffic from entering the SD-WAN network.

This scenario provides step-by-step instructions for directing traffic of one or more applications to the transport service. Before following this scenario, you must create a [transport service](#) to which the application traffic is to be directed.

The scenario for directing application traffic to a transport service involves the following steps:

1 Creating a traffic classification rule

A traffic classification rule is used to identify the traffic of a specific application from the overall data stream. When [creating a traffic classification rule](#), you must select the L3 protocol on the **L3 fields** tab, and select the application whose traffic you want to direct to the transport service on the **DPI** tab.

If you want to direct traffic of multiple applications to a transport service, create a traffic classification rule for each of them.

2 Creating a traffic filter

A traffic filter determines whether the routing of an application's traffic is allowed. When [creating a traffic filter](#), you must add a traffic classification rule for an application or multiple classification rules.

3 Creating an ACL interface

An ACL interface applies a filter to traffic that passes through it. When [creating an ACL interface](#), you must select a traffic filter for the application.

4 Adding the ACL interface to the transport service

You must edit the settings of the [transport service](#) and add an ACL interface through which application traffic will arrive to the service.

Traffic mirroring

Kaspersky SD-WAN supports forwarding and mirroring traffic from collection points to the destination within an individual TAP service. Collection and destination points are service interfaces. Collection points can be both individual service interfaces and service interfaces used in transport services. Collection points are specified when creating a TAP service, but a destination must be created in advance.

Forwarding means sending traffic that arrives to collection points to the destination point, and mirroring means sending a copy of the traffic. Note that Kaspersky SD-WAN temporarily does not support forwarding and mirroring of outgoing traffic.

When creating a TAP service, you can also specify [traffic classification rules](#) that will be used at the destination to separate the data of interest from the overall stream.

Creating a traffic destination

A *destination* is a service interface that receives forwarded traffic from collection points that you specify when [creating the TAP service](#). Before creating a traffic destination, you must [create a service interface](#).

To create a traffic destination:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **TAP services** section.

By default, the **Mirroring destination** tab is selected, which displays the table of traffic destinations.

4. In the upper part of the page, click **+ Mirroring destination**.

5. This opens a window; in that window, in the **Switch** and **Port** drop-down lists, select the CPE device and the service interface created on that CPE device that you want to use as the traffic destination.

6. Click **Create**.

The traffic destination is created and displayed in the table.

Deleting a traffic destination

Deleted traffic destinations cannot be restored.

To delete a traffic destination:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **TAP services** section.

By default, the **Mirroring destination** tab is selected, which displays the table of traffic destinations.

4. Click **Delete** next to the traffic destination.

5. In the confirmation window, click **Delete**.

The traffic destination is deleted and is no longer displayed in the table.

Creating a TAP service

Before creating a TAP service, you must complete the following steps:

- [Create a traffic destination](#).
- [Create service interfaces](#) that will be used as traffic collection points.

Note that you can apply one or more [traffic classification rules](#) to the traffic destination.

To create a TAP service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.

2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.

3. Go to the **TAP services** section.

By default, the **Mirroring destination** tab is selected, which displays the table of traffic destinations.

4. Select the **TAP services** tab.

A table of TAP services is displayed.

5. In the upper part of the page, click **+ TAP service**.

6. To mirror traffic coming to collection points to the destination, select the **Mirror traffic** check box. When this check box is selected, a copy of the traffic is sent to the destination; when the check box is cleared, the traffic is relayed. This check box is cleared by default.

7. In the **Balancing mode** drop-down list, select the balancing mode for evenly distributing traffic among the tunnels to prevent congestion of individual tunnels and prevent performance issues for users:

- **Per-flow** — Balancing across flows (sessions). During transmission, flows are evenly distributed across the tunnels. This is the default setting.
- **Per-packet** — Per-packet balancing. During transmission, packets are distributed evenly across the tunnels.

- **Broadcast** — Packets are sent to all tunnels simultaneously to prevent losses.
8. In the **Mirroring destination** drop-down list, select the traffic destination.
 9. In the **Source point type** drop-down list, select one of the following values:
 - **Service interface** — Individual service interface.
 - **Transport service** — Service interface used in the transport service.
 10. If in the **Source point type** drop-down list, you selected **Transport service**, follow these steps:
 - a. In the **Type** drop-down list, select the type of the transport service:
 - **P2P**
 - **IP multicast**
 - **L3 VPN**
 - **P2M**
 - **M2M**
 - b. In the **Transport service** drop-down list, select the transport service.
 11. In the **Source points** drop-down list, select the service interfaces that you want to use as traffic collection points.
 12. Click **Next** and select the previously created traffic classification rules for the destination.
 13. Click **Create**.

The TAP service is created and displayed in the table.

Editing a TAP service

To edit a TAP service:

1. In the menu, go to the **Infrastructure** section.

This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.
2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.

This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.
3. Go to the **TAP services** section.

By default, the **Mirroring destination** tab is selected, which displays the table of traffic destinations.
4. Select the **TAP services** tab.

A table of TAP services is displayed.

5. Click **Management** next to the TAP service and in the drop-down list, select **Edit**.
6. This opens a window; in that window, edit the settings that you want to change. For a description of the settings, see the [instructions for creating a TAP service](#).
7. Click **Save**.

Viewing statistics of a TAP service

To view the statistics of a TAP service:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.
2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.
This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.
3. Go to the **TAP services** section.
By default, the **Mirroring destination** tab is selected, which displays the table of traffic destinations.
4. Select the **TAP services** tab.
A table of TAP services is displayed.
5. Click **Management** next to the TAP service and in the drop-down list, select **Statistics**.
This opens a window with statistics of the TAP service.

Deleting a TAP service

Deleted TAP services cannot be restored.

To delete a TAP service:

1. In the menu, go to the **Infrastructure** section.
This opens the resource management page. By default, the **Network resources** tab is selected, which displays the table of SD-WAN and SDN Controllers.
2. Click **Management** → **Configuration menu** next to the SD-WAN Controller.
This opens the Controller configuration menu. By default, you are taken to the **Controller nodes** section, which displays a table of Controller nodes.
3. Go to the **TAP services** section.
By default, the **Mirroring destination** tab is selected, which displays the table of traffic destinations.
4. Select the **TAP services** tab.
A table of TAP services is displayed.

5. Click **Management** next to the TAP service and in the drop-down list, select **Delete**.
6. To delete the service interfaces added to the TAP service, select the **Delete associated service interfaces** check box in the confirmation window.
7. Click **Delete**.

The TAP service is deleted and is no longer displayed in the table.

Task scheduler

Kaspersky SD-WAN supports using the scheduler to delay the running of tasks. You can use [tags](#) to group CPE devices to delay tasks on those devices.

The following types of delayed tasks are supported:

- [Running scripts on CPE devices](#). You must first add the scripts that you want to run to the CPE template.
- Updating firmware on CPE devices. You must first upload the firmware that you want to install to the orchestrator web interface.

When you schedule a delayed task, Kaspersky SD-WAN uses the time zone of the orchestrator host. For example, if you schedule a script to run on a CPE device at 2:00 p.m., the script runs at 2:00 p.m. in the time zone of the orchestrator, even if the time on the device is 6:00 p.m.

When configuring delayed running of tasks, consider the following:

- A 10-second inaccuracy is considered acceptable for the moment when the task is run.
- If a task does not run because the orchestrator is not available at the scheduled time, the task is displayed with the *Error* status.
- If multiple CPE device configuration tasks exist, they are performed in parallel. If the orchestrator cannot run all tasks in parallel, they are run in the order they were created.
- If you delete a CPE template that has associated tasks, the tasks are also deleted.
- If you delete a CPE device that has associated tasks, the tasks are also deleted.
- When you try to delete a script that is associated with tasks, you must additionally confirm this action.

You can manually run delayed tasks that have not yet been run.

Creating a delayed task

To create a delayed task:

1. In the menu, go to the **Scheduler** section.
The table of delayed tasks is displayed.
2. In the upper part of the page, click **Delayed task**.
3. This opens a window; in that window, in the **Type** drop-down list, select one of the following values:
 - **Script execution** — Delayed script run task.
 - **Delayed firmware update** — Delayed firmware update task.
4. Specify the settings of the delayed task. For a description of delayed task settings, see the following instructions:
 - [Delayed scripts](#).

- Updating firmware.

5. Click **Create**.

The delayed task is created and displayed in the table.

Executing a delayed task manually

To manually run a delayed task:

1. In the menu, go to the **Scheduler** section.

The table of delayed tasks is displayed.

2. If necessary, run an individual delayed task:

a. Click the delayed task.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

b. In the upper part of the settings area, under **Actions** click **Run now**.

3. If necessary, run multiple delayed tasks at the same time:

a. Select the check boxes next to delayed tasks.

b. In the upper part of the page, in the **Actions** drop-down box, select **Run now**.

4. In the confirmation window, click **Run now**.

One or multiple delayed tasks are run and their status in the table changes to *Executed*.

Deleting a delayed task

Deleted delayed tasks cannot be restored.

To delete a delayed task:

1. In the menu, go to the **Scheduler** section.

The table of delayed tasks is displayed.

2. If necessary, delete an individual delayed task:

a. Click the delayed task.

The settings area is displayed in the lower part of the page. You can expand the settings area to fill the entire page by clicking the expand icon .

b. In the upper part of the settings area, under **Actions** click **Delete**.

3. If necessary, delete multiple delayed tasks at the same time:

a. Select the check boxes next to delayed tasks.

b. In the upper part, in the **Actions** drop-down box, select **Delete**.

4. In the confirmation window, click **Delete**.

One or more delayed tasks are deleted and are no longer displayed in the table.

Glossary

Control plane

The control part of the network that controls the transmission of traffic packets through CPE devices. Performs functions such as network discovery, route calculation, traffic prioritisation, and security policy enforcement. The control plane allows centrally managing the network by providing a full-scale view of all performed operations. Consists of an orchestrator and an SD-WAN controller.

Customer Premise Equipment (CPE)

Telecommunication equipment, including virtual machines, located at the client premises. Used to connect the client location to the SD-WAN network, establish tunnels and transfer traffic between client locations. Traffic can be sent to a data center to provide network functions such as routing protocols, intrusion prevention, or anti-virus protection.

Data plane

The part of the network that processes and transmits traffic between different locations and devices. The data plane uses network protocols and algorithms to efficiently route and deliver traffic over the network. Consists of CPE devices.

DSCP values

6-bit values that define the priority of traffic packets and the type of service required. They are used in combination with traffic classes to provide appropriate priority and bandwidth to critical network traffic, such as traffic from audio and video streaming applications.

Orchestrator

Controls the solution infrastructure, functions as an NFV orchestrator (NFVO), and manages network services and distributed VNFMs. Can be managed via the web interface or REST API when using external northbound systems.

Physical Network Function (PNF)

Pre-deployed ready-to-use network functions that are uploaded to the orchestrator web interface. The orchestrator can then handle additional configuration of the PNF.

PNF package

A package, in TAR or ZIP format, that contains the data necessary for deploying and managing the PNF.

Port security

This function improves network security at the level of Ethernet ports of switches and prevents unauthorized access to the network by limiting the number of MAC addresses that can be associated with a single physical port. When enabled, only trusted devices with predefined MAC addresses can connect to the network.

SD-WAN Controller

Centrally manages the overlay network and network devices in accordance with the service chain topology via the OpenFlow protocol. Deployed as a virtual or physical network function.

SD-WAN Gateway

CPE device that has the SD-WAN gateway role. Gateways establish tunnels with all devices on the network, including other gateways, thus providing connectivity between all devices and the SD-WAN Controller. You can install multiple gateways for fault tolerance.

SD-WAN instance

A deployed Kaspersky SD-WAN solution for one of the tenants of your organization. It is an isolated entity and has its own network services, CPE devices, and quality of service parameters.

Software-Defined Networking (SDN)

Technology for building communication networks in which the control plane is separated from the data plane and is implemented in software using a centralized SDN controller.

Software-Defined Wide Area Network (SD-WAN)

Approach to building software-defined networks using a global computer network. SD-WAN networks allow connecting local area networks and users in geographically dispersed locations.

Tenant

A logical entity within which an individual SD-WAN instance is deployed. Solution components such as network service components, users, and CPE devices are assigned to a tenant, and subsequently, tenant administrators can manage the assigned components. For example, you can create a separate tenant for a customer of your organization.

Transport strategy

A transport service encapsulation mechanism that includes the algorithm for adding a stack of traffic packet header tags and the type of these tags. Kaspersky SD-WAN temporarily supports one transport strategy, **Generic VNI Swapping Transport**.

Universal CPE (uCPE)

CPEs with additional support for Virtual Network Function deployment. Note that the device must have sufficient hardware resources to avoid involving the data center or the cloud when providing the VNF.

Virtual Deployment Unit (VDU)

A virtual machine that acts as a VNF host and aggregates virtual computing resources, such as CPU and memory, required to run the VNF software, and also contains certain implementations of the network function, such as routing algorithms or load balancing logic.

Multiple VDUs can be combined into a single VNF to provide scalability and/or high availability. VDUs can be distributed across multiple physical servers; you can still manage them as a single VNF. VDUs interact with each other and other VNFs to perform their functions within a network service.

Virtual Infrastructure Manager (VIM)

Manages computational, networking, and storage resources within the NFV infrastructure. Serves to connect network functions with virtual links, subnets, and ports.

Can be deployed in the data center or on a uCPE device. Deploying the VIM in the data center implies centralized management of the VNF lifecycle, while a VIM deployed on a uCPE device allows delivering VNFs to remote locations and managing these VNFs locally. The deployed VIM must be added in the orchestrator web interface.

The OpenStack cloud platform is used as the VIM.

Virtual Network Function (VNF)

Network functions implemented as virtual machines on Commercial Off The Shelf (COTS) computer platforms.

Virtual Network Function Manager (VNFM)

Manages the lifecycle of virtual network functions using SSH, Ansible playbooks, scripts, and Cloud-init attributes.

VNF Package

A package, in TAR or ZIP format, that contains the data necessary for deploying and managing a VNF.

Contacting Technical Support

This section describes the ways to get technical support and the terms on which it is available.

How to obtain Technical Support

If you cannot find a solution to your problem in the documentation, we recommend that you contact Technical Support. Technical Support staff will answer your questions about deploying and using Kaspersky SD-WAN.

Kaspersky provides support for Kaspersky SD-WAN throughout its life cycle (see [application life cycle page](#)). Before contacting Technical Support, please read the [support rules](#).

You can contact Technical Support in one of the following ways:

- By sending a request to Kaspersky SD-WAN Technical Support at sdwan-support@kaspersky.com
- [By visiting the Technical Support website](#)
- By sending a request to Technical Support through the [Kaspersky CompanyAccount portal](#).

Technical Support via Kaspersky CompanyAccount

[Kaspersky CompanyAccount](#) is a portal for organizations that use Kaspersky applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction of users with Kaspersky staff via online requests. The Kaspersky CompanyAccount portal lets you monitor the progress of online requests as they are processed by Kaspersky staff, and keep a history of online requests.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single account lets you centrally manage online requests to Kaspersky issued by registered employees and also manage the permissions of these employees using Kaspersky CompanyAccount.

The Kaspersky CompanyAccount portal is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese
- Russian
- French
- Japanese

You can learn more about Kaspersky CompanyAccount on the [Technical Support website](#) [↗].

Information about third-party code

Information about third-party code is contained in the legal_notices.txt file in the application installation folder.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Active Directory is a trademark of the Microsoft group of companies.

Ansible, CentOS, Red Hat are trademarks or registered trademarks in the United States and other countries of Red Hat, Inc. or its subsidiaries.

Arm is a registered trademark of Arm Limited (or its subsidiaries) in the USA and/or other countries.

Atom, Celeron, Intel, and Xeon are trademarks of Intel Corporation registered in the United States of America and elsewhere.

Debian is a registered trademark of Software in the Public Interest, Inc.

Docker and the Docker logo are trademarks or registered trademarks of Docker, Inc. in the USA and/or other countries. Docker, Inc. and other parties may have rights to trademarks described with other terms used in this document.

Firefox is a trademark of the Mozilla Foundation in the USA and other countries.

Google Chrome is a trademark of Google LLC.

IBM is a trademark of International Business Machines Corporation registered in many jurisdictions around the world.

Kraftway is a registered trademark of AO Kraftway Corporation PLC.

Linux, LTS are registered trademarks of Linus Torvalds in the USA and other countries.

Microsoft Edge and Windows are trademarks of the Microsoft group of companies.

MIPS is a trademark or registered trademark of MIPS Technologies in the USA and other countries.

OpenStack is a registered trademark of the OpenStack Foundation in the USA and other countries.

OpenStreetMap is a trademark of the OpenStreetMap Foundation. This product is not affiliated with or endorsed by the OpenStreetMap Foundation.

Python is a trademark or registered trademark of the Python Software Foundation.

Safari is a trademark of Apple Inc.

SUSE is a trademark of SUSE LLC registered in the United States and elsewhere.

Ubuntu is a registered trademark of Canonical Ltd.

VMware is a trademark of VMware, Inc or a registered trademark of VMware, Inc. in the United States or other jurisdictions.

Zabbix is a registered trademark of Zabbix SIA.