SECURITY
code

vGate R2

Administrator guide

Installation, configuration and operation

Mailing address:	**P.O. Box 66, Moscow, Russian Federation, 115127 Security Code LLC**
Phone:	**+7 495 982-30-20**
Email:	**info@securitycode.ru**
Web:	**https://www.securitycode.net/**

Table of contents

List of terms and abbreviations

AD	Active Directory is the MS Windows directory service
DNS	Domain Name System
IOPS	Input/output operations per second is the number of operations that are carried out by the SAN in one second
iSCSI	Internet Small Computer System Interface is a protocol for management of data storage and transmission systems based on TCP/IP
vCenter	The tool for centralized management of ESXi servers and virtual machines
vCSA	vCenter Server Appliance is a virtual module with the installed vCenter server and services that are connected with it
PSC	Platform Services Controller is a component that supports the operation of VMware virtual infrastructure services
VM	Virtual machine
OS	Operating system
RAM	Random access memory
SAN	Storage area network
CPU	Central processing unit

Introduction

This guide is designed for administrators of vGate R2 (hereinafter — vGate). The document covers information required for installation, configuration, and operation of vGate.

vGate is designed to protect virtual infrastructures deployed using the VMware vSphere, KVM, OpenNebula, Proxmox and Skala-R virtualization systems.

Website. You can go to Security Code LLC website (https://www.securitycode.net/) or contact the company representatives by email: support@securitycode.ru.

Training courses. You can learn more about the hardware and software products of the Security Code LLC in the authorized training centers. The list of training centers and learning terms are available at https://www.securitycode.net/company/training/.

You can contact the company representatives regarding the organization of the training process by email: education@securitycode.ru.

The latest version of the operation manuals for the product "vGate R2" is available on the company's website at https://www.securitycode.net/products/vgate/.

You can request the latest version of Release Notes by email: vgateinfo@securitycode.ru.

Chapter 1
vGate installation

Hardware and software requirements

System requirements

Computers with installed vGate components must meet the following system requirements.

Component	Operating system
vGate Server	• Windows Server 2012 R2 6.3.9600 x64; • Windows Server 2016 1607 x64 + Update KB4103720; • Windows Server 2019 1809, 2109 x64; • Windows Server 2022 (21H2). Minimum bandwidth for a replication network — 10 Mbps. The vGate Server component requires 10 GB on the hard drive. Additionally: • JaCarta drivers (if using JaCarta security token). • Rutoken S, Lite and digital signature drivers (if using Rutoken security token).
Redundant vGate Server	• Windows Server 2012 R2 6.3.9600 x64; • Windows Server 2016 1607 x64 + Update KB4103720; • Windows Server 2019 1809, 2109 x64; • Windows Server 2022 (21H2). The vGate Server component requires 10 GB on the hard drive. Minimum bandwidth for a replication network — 10 Mbps
vGate Client	• Microsoft Windows 10 1809, 2109 x64; • Windows 11; • Windows Server 2012 R2 6.3.9600 x64; • Windows Server 2016 1607 x64 + Update KB4103720; • Windows Server 2019 1809, 2109 x64; • Windows Server 2022 (21H2); • Linux Alt 8 SP with kernel version 5.10.150.std.def. The vGate Client component requires 200 MB on the hard drive. Additionally: • JaCarta drivers (if using JaCarta security token). • Rutoken S, Lite and digital signature drivers (if using Rutoken security token). vGate does not support simultaneous operation of JaCarta and Rutoken tokens while logging on via the vGate Client
Web console	• Yandex Browser 23.1.2.987 (64-bit); • Microsoft Edge 91.0.864.48 (64-bit); • Google Chrome 91.0.4472.101 (64-bit) and 91.0.4472.106 (32-bit); • Firefox 89.0 (64-bit); • Safari 12.1.2
vGate management console and report viewer tool	• Microsoft Windows 10 1809, 2109 x64; • Windows 11 (21H2); • Windows Server 2012 R2 6.3.9600 x64; • Windows Server 2016 1607 x64 + Update KB4103720; • Windows Server 2019 1809, 2109 x64; • Windows Server 2022 (21H2)
vGate Agent for ESXi	• VMware vSphere 6.5 (VMware ESXi Server 6.5); • VMware vSphere 6.7 (VMware ESXi Server 6.7); • VMware vSphere 7.0 (VMware ESXi Server 7.0). If you intend to use the firewall component, the server must have at least 6 GB of RAM. Operation of the vGate software on custom images of vSphere (from providers of HP and IBM servers and so on) is not guaranteed. The firewall component is not supported for VMware ESXi 7.0 Update 3i

vGate Agent for vCenter (vCSA)	• Windows Server 2012 R2 6.3.9600 x64; • Windows Server 2016 1607 x64 + Update KB4103720; • Windows Server 2019 1809 x64; • Photon OS; • VMware vSphere 6.5 (VMware vCenter Server 6.5); • VMware vSphere 6.7 (VMware vCenter Server 6.7); • VMware vCenter Server Appliance 6.5; • VMware vCenter Server Appliance 6.7; • VMware vCenter Server Appliance 7.0. vGate Agent for vCenter requires 200 MB on the hard drive. Operation of the vGate software on the vSphere custom images (from providers of HP and IBM servers and so on) is not guaranteed
vGate Agent for PSC	• Platform Services Controller 6.7; • Platform Services Controller Appliance 6.7
vGate Agent for KVM	• Ubuntu 18.04.6 LTS; • Ubuntu 20.04.3 LTS; • Astra Linux Common Edition "Орел" 2.12.22; • Alt Virtualization Server 10; • Alt Server 8 SP; • R-virtualization platform 7. Additionally, the Glibc package must be installed on a KVM server
	The vGate software integration with the following KVM virtualization management tools is supported: • Proxmox 7.2; • OpenNebula 5.10.5, Proxmox 7.0 (included in Alt Virtualization Server 10); • Skala-R Management 1.80 and 1.93
Monitoring server	• VMware vSphere 6.5; • VMware vSphere 6.7; • VMware vSphere 7.0. Virtual machine requirements: • CPU cores - 2; • RAM - 4 GB; • free space - 20 GB
Analysis server	Virtual machine requirements: • CPU cores - 2 for each network interface for traffic analysis; • RAM - 4 GB; • free space - 20 GB

Hardware requirements for the vGate software are the same as requirements for operating systems.

Attention! The system has the following limitations:

- Installation of the vGate Server and vGate Agent for vCenter on the domain controller is not supported.
- IPv6 is not supported. Therefore, when installing the vGate Server, the IPv6 protocol must be disabled in the network adapter properties.

Attention! To install vGate on the computers with OS Windows, disable the Self-Defense component in Kaspersky Endpoint Security.

The table below shows the recommended system requirements for vGate 4.7 depending on the virtual infrastructure size.

Number of vGate Agents	CPU threads	RAM (GB)	Disk (IOPS)
up to 10	4	5	100
up to 50	6	8	300
100-300	10	16	550
300-500	12	24	1050
500-700	16	28	1550
700-900	18	32	3000

Hardware requirements

Configuration requirements for the computer on which vGate components are installed are the same as the requirements for the OS running on that computer.

Virtualization servers must be equipped with the required number of independent Ethernet interfaces in order to implement a local network configuration.

There must be at least one Ethernet interface on the vGate server computer when deploying vGate using a router (see p.**16**), and at least two Ethernet interfaces when using the vGate Server for traffic routing (see p.**20**).

Attention! vGate operation when using Fibre Channel is not guaranteed.

Attention! The computers on which vGate components will be installed must have the required number of physical Ethernet interfaces. vGate operation with virtual networks adapters on physical computers is not supported.

Attention! Installation of the vGate Server on VM is allowed, but we do not recommend locating it on the server protected by the vGate.

Installation plan

We recommend the following procedure of vGate deployment:

№	Installation step	Specific features	Description
1	**Local network configuration**		See p.**12**
2	**vGate Server installation and setup**	If you do not intend to replicate the vGate Server, the vGate Server is installed and initial setup is performed. The chief security officer account is created during the software installation process	See p.**15**
	vGate Server installation and setup in the replication mode	If you intend to replicate the vGate Server (this function is available in vGate Enterprise and Enterprise Plus only). Main server: • The vGate Server installation and initial setup is performed. The chief security officer account is created during the software installation process. • The "Replication configuration" component is installed. Redundant server: • The redundant vGate Server installation and initial setup is performed	See p.**25**
3	**vGate Agent installation**	In the web console, vGate Agents are installed: • on the vCenter server (vCSA) if it is available in the configuration; • on ESXi servers; • on KVM servers; • on Skala-R servers; • on Proxmox and OpenNebula servers (included in Alt Virtualization Server 10). If necessary, the vGate Agent can be installed using the vGate setup program directly on the computer with the installed VMware vCenter. The agentless operation control is available for the vCSA server version 7.0 Update 1 (see p.**86**). The agentless operation control is enabled by default for the Skala-R Management server	See p.**85** and p.**164**
4	**Monitoring server installation and setup**	If necessary, deploy the vGate monitoring components as follows: • the monitoring server is deployed and configured; • the connection to the vCenter is configured; • in the vGate web console, the connection to the monitoring server is configured	See p.**45**
5	**Analysis server installation and setup**	If necessary, the vGate components that provide deep packet inspection functions are installed	See p.**46**
6	**Software installation on the security administrator workstation**	The vGate Client is installed. This step must be skipped if the security administrator workstation is located on the vGate Server	See p.**44**

№	Installation step	Specific features	Description
7	**Software installation on the virtual infrastructure administrator workstation**	If necessary, the vGate Client is installed	See p.44
8	**Software installation on other computers of the external administration network perimeter**	The vGate Client is installed on computers that are located in the external perimeter of the administration network if incoming connections to the internal perimeter will be established from them	See p.44

Local network configuration

Local network configuration rules

In order to ensure security, the network must be configured before installing vGate components, based on the following rules:

- The virtual infrastructure administration network (secure network perimeter where ESXi, vCenter, Skala-R, Skala-R Management, KVM, Proxmox, OpenNebula servers and other virtual infrastructure elements are located) must be separated from the virtual machine network and other virtual infrastructure networks.
- If vMotion and Fault Tolerance functions are used in the virtual infrastructure, we recommend organizing an individual network for virtual machine replication by separating it from administration networks and virtual machine networks.
- If virtual machine data is stored outside the virtualization servers in a separate storage system, we recommend creating a data transmission network based on Ethernet technology (iSCSI) or Fiber channel. If necessary, the data transmission network and the virtual machine replication network can be combined.

To work in the network configured in this way, virtualization servers must have the required number of sufficient Ethernet interfaces.

Attention! We do not recommend using the DHCP protocol for Ethernet interfaces connected to the secure network perimeter and the administration network perimeter.

Attention! When using the Active Directory integration mode, during which the vGate Server is included in the Windows domain, follow the recommendations below:

- do not locate the domain controller within the secure perimeter of the virtual infrastructure administration network;
- the vGate Server does not support automatic change of passwords for vGate service accounts in the Windows domain. Therefore, it is necessary to create an individual organization unit (OU), where accounts of vGate Servers will be located, and disable automatic change of passwords for it. For this purpose, assign a group policy to this OU and assign the "Enabled" value to the parameter "Domain member: Disable machine account password changes" or the "999 days" value to the parameter "Domain member: maximum machine account password age" in branch "Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options". This OU is selected during a certain step of the vGate server installation.

Note. Once the vGate Server, vGate Client or vGate Agent for vCenter are installed, the "Security Code vGate NDIS 6.0 network filter driver" network service appears in the list of components (in the network adapter properties).

Before configuring a local network, we recommend you read the documentation for VMware and Skala-R products.

Examples of the VMware virtual infrastructure and vGate component location are presented in figures 1 and 2.

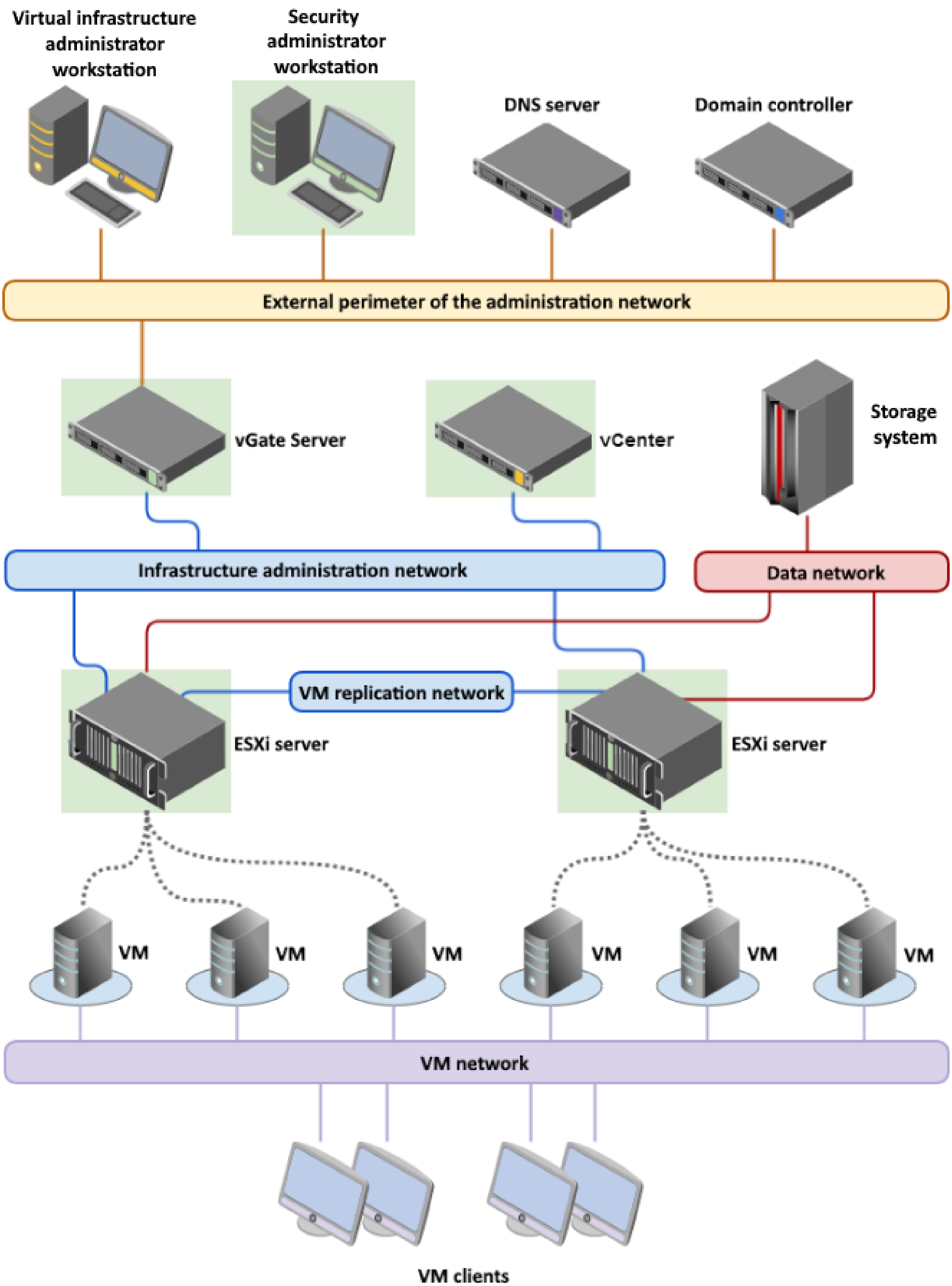


Figure 1. Network architecture and component location (traffic is routed by the vGate Server)

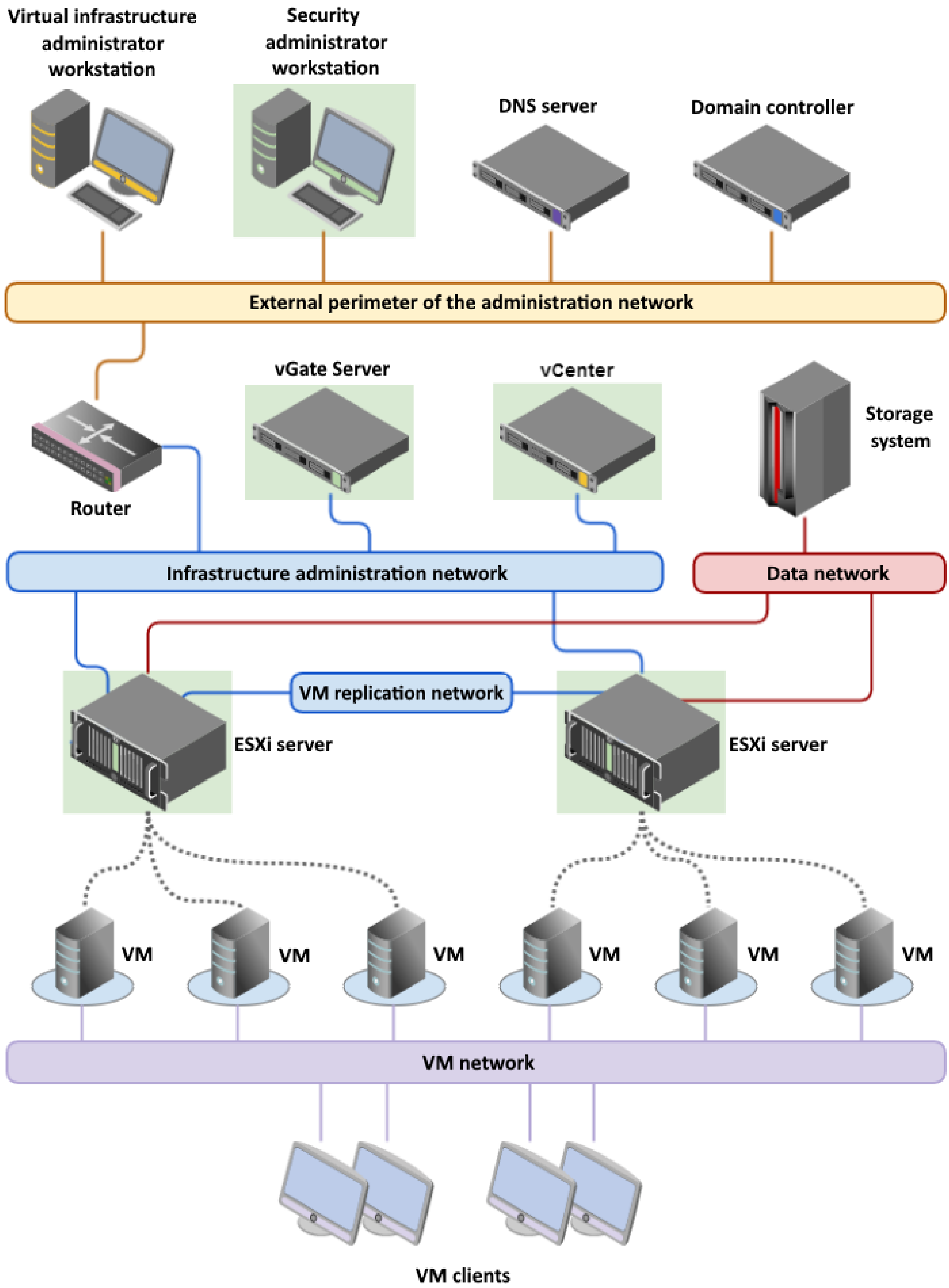


Figure 2. Network architecture and component location (traffic is routed using a router that already exists in the network)

Configuration of routing between subnets

Attention! After configuring a local network, you must configure routing between subnets, as well as make sure that access from virtual infrastructure administrator workstations to virtual infrastructure control elements is available. Only after this, you can start installing and configuring vGate components.

The main routing configuration options are listed in the table below.

Option	Specific features of configuration
Using a third-party router	On the virtual infrastructure administrator workstations, select the router that already exists in the external administration network perimeter as a default gateway. You must also prohibit direct network connections between the virtual infrastructure administrator workstations and protected servers
Using vGate Server as a gateway	On all virtual infrastructure administrator workstations, select the IP address of the external network adapter of the vGate Server as a default gateway. On all computers in the secure perimeter of the infrastructure administration network (ESXi, vCenter, Skala-R, KVM, OpenNebula, Proxmox servers), select the IP address of the secure perimeter adapter of the vGate Server as a default gateway
Retrieving a route from the vGate Server	On all computers in the secure perimeter of the administration network (ESXi, vCenter, Skala-R, KVM, OpenNebula, Proxmox servers), select the IP address of the secure perimeter adapter of the vGate Server as a default gateway. In the web console, retrieving the route to the secure network from the vGate Server must be configured (see configuring network and access control on p.**60**) In this case, the route to the secure network is added from the vGate Server on virtual infrastructure administrator workstations when the vGate authentication service is started. After this, the route is saved in the local routing table of the computer

If you intend to use a configuration with a redundant vGate Server, the DNS server must be located in the external network. Besides this, a CNAME record specifying the main server must be configured in DNS. In this case, when installing vGate clients, the main server CNAME record must be specified.

vGate Server installation and setup

Installation and operation of the vGate server differ, depending on the method of traffic routing management between the external and protected perimeter of the administration network:

- Using the existing router in the network (see p.**16**).

  In this mode, the vGate Server is located in the secure perimeter of the administration network, in the same subnet, where protected servers are located (see Figure 2 on p.**14**). This mode does not require reconfiguration of the existing network and provides the availability of a certified firewall (router) in the external administration network to filter network traffic to protected servers. On the router, access from virtual infrastructure administrator and security administrator workstations to the protected subnet or individual servers should be closed, and access to the vGate Server should be allowed. For details on configuring a router, see p.**191**.
- Using the vGate Server (see p.**20**).

  In this mode, protected servers should be located in a separate subnet. On all computers in the secure perimeter of the administration network (ESXi, vCenter, Skala-R, KVM, OpenNebula, Proxmox servers), specify the IP address of the secure perimeter adapter of the vGate Server as a default gateway. On all virtual infrastructure administrator workstations, specify the IP address of the network adapter of the vGate server in the external administration network as a default gateway.

  This mode does not require additional router configuration.

Attention!

- If you intend to use Active Directory, the computer designated to be the vGate Server, should be added to the domain.
- If the vGate Server computer was added to the domain after the vGate software installation, this domain should be added to the list of trusted domains in the vGate web console (see p.**67**).

Attention! If you intend to use the report viewer function on the computer designated to be the vGate Server , Microsoft Report Viewer 2010 SP1 Redistributable Package should be installed in advance. To do this, run the ReportViewer.exe file from the folder \Redistributables\Microsoft Report Viewer Redistributable 2010 of the setup disk, and follow the setup wizard instructions.

Installation using a third-party router

Prepare your computer before installation:

On the computer designated to be the vGate Server, configure one LAN connection.

Adapter	Subnet	LAN settings
Adapter 1	Infrastructure administration network	IP address used by ESXi, vCenter, Skala-R and KVM servers for configuration and audit. The examples use the IP address: **192.168.1.2**

To install the vGate Server:

1. Log on using the computer administrator credentials.
2. Insert the setup disk into the drive.

   Note. If the setup program does not start automatically, run the autorun.exe file from the \autorun folder.

   The starting dialog box of the setup program appears.
3. In the starting dialog box, click the "vGate Server" link.

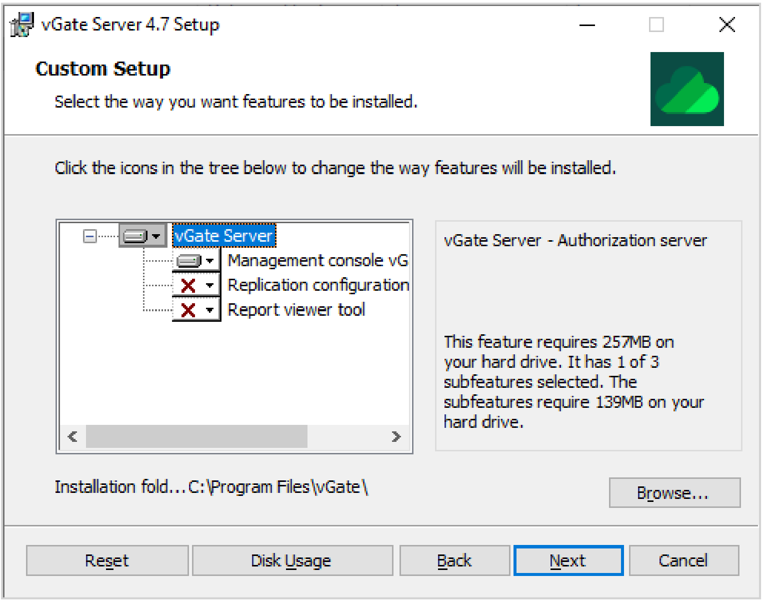
   Tip. To install this product, you can also run the \vGate\vGateServer.msi file from the setup disk.

   The program will complete certain preparations, after which the welcome dialog box appears.
4. Click "Next".

   The license agreement dialog box appears.
5. Read the entire license agreement, select the "I accept the terms in the License Agreement" check box and click "Next".

   Tip. In order to obtain a paper copy of the license agreement, click "Print".

   A dialog box to select components to be installed appears.



6. Select components to be installed.

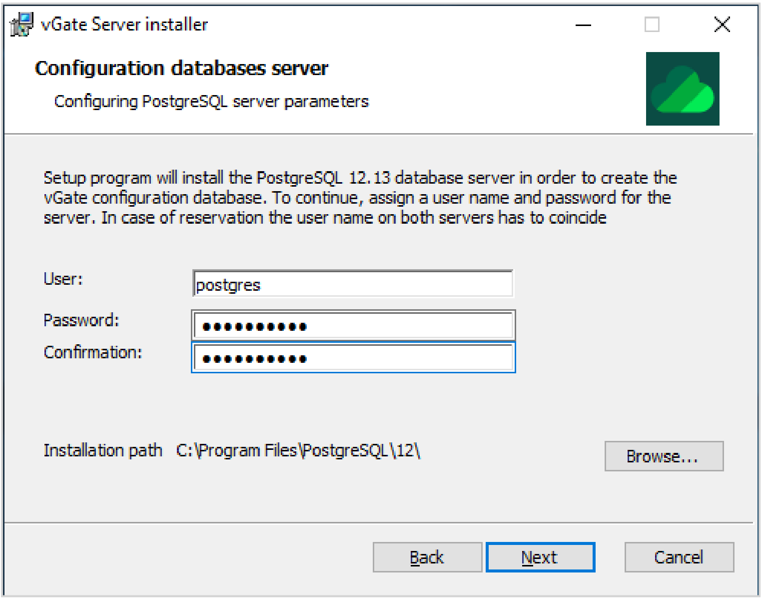
   Note.
   - In order to use the report viewer function, select the "Report viewer tool" component for installation. To do this, open the drop-down menu to the left of the component name and select "Will be installed on local hard drive".
   - The "Replication configuration" component is not installed by default. If you intend to replicate the vGate Server (see p.25), select this component for installation. To prohibit the component installation, in the drop-down menu to the left of the component name select "Entire feature will be unavailable".

A dialog box has the following buttons:

Button	Action
Browse	Opens the dialog box for modifying the path to the setup directory
Disk usage	Opens the dialog box with information about free space on disks of the computer
Reset	Returns installation components to their default state

7. Click "Next".

The following dialog box appears.

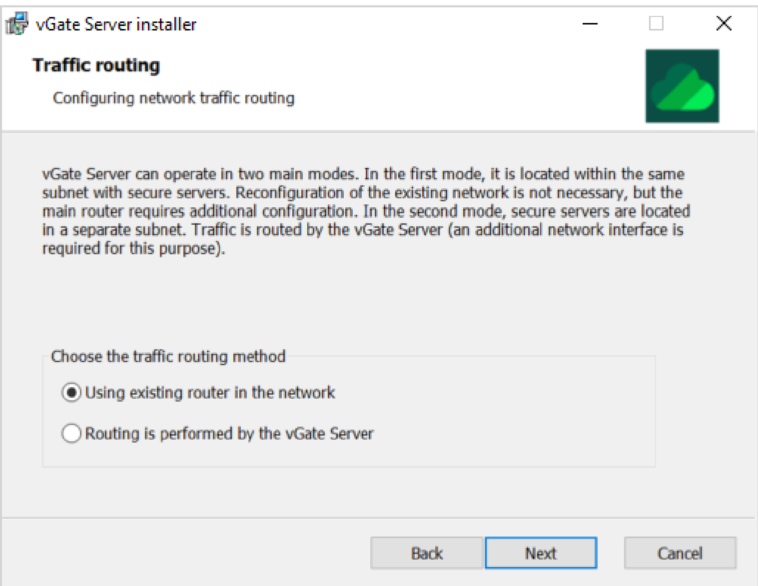


8. Enter the name and password of the PostgreSQL database server user. If necessary, modify the path to the folder for database installation, and click "Next". When you install vGate in replication mode, PostgreSQL user names on the main and redundant servers must match.

Note.

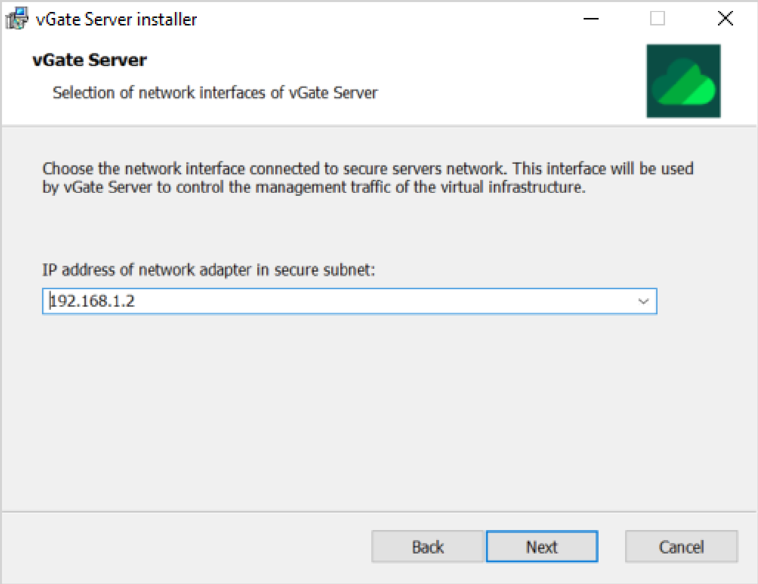
- PostgreSQL 12.13 server will be installed automatically while installing vGate. vGate configuration database will be created on it. If the PostgreSQL server is already installed on the computer, you must remove it before the vGate software installation.
- By default, vGate 4.0 and later uses PostgreSQL database port 5432. This port can only be changed if PostgreSQL is installed separately (before the vGate software installation). PostgreSQL database ports for the main and redundant server must match.

The following dialog box appears.



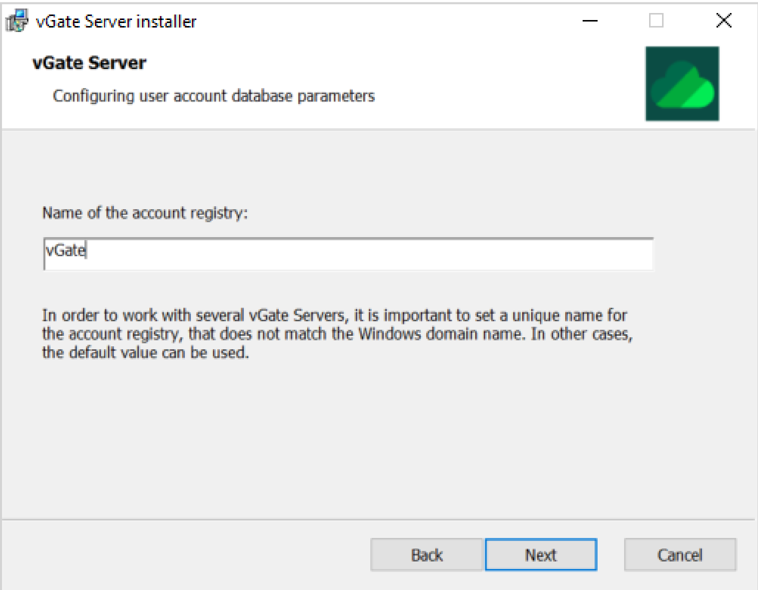
9. Select the "Using existing router in the network" traffic routing method and click "Next".

The following dialog box appears.



10. Enter the IP address of the adapter 1 of the vGate Server, through which routes will pass to/from the secure perimeter of the administration network, and click "Next".

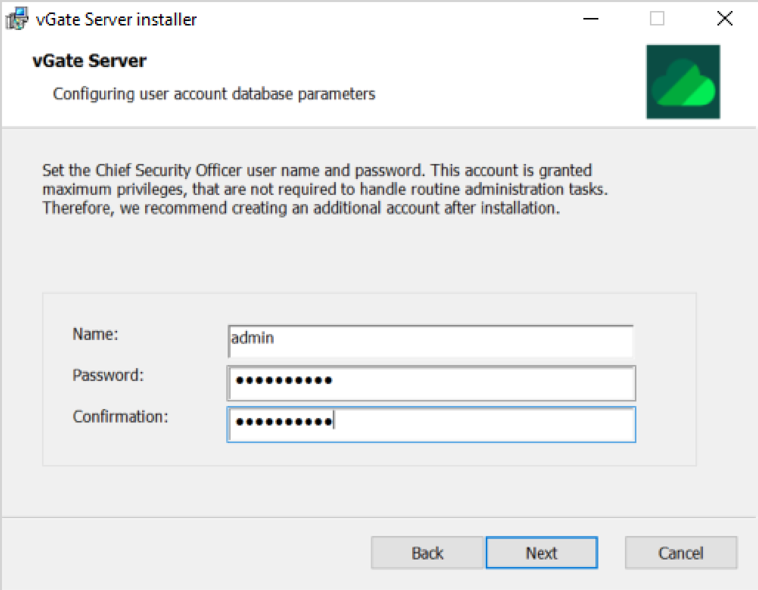
The following dialog box appears.



Note. If you intend to use several vGate Servers in the network, specify a unique name for the vGate account registry during installation of each vGate Server.

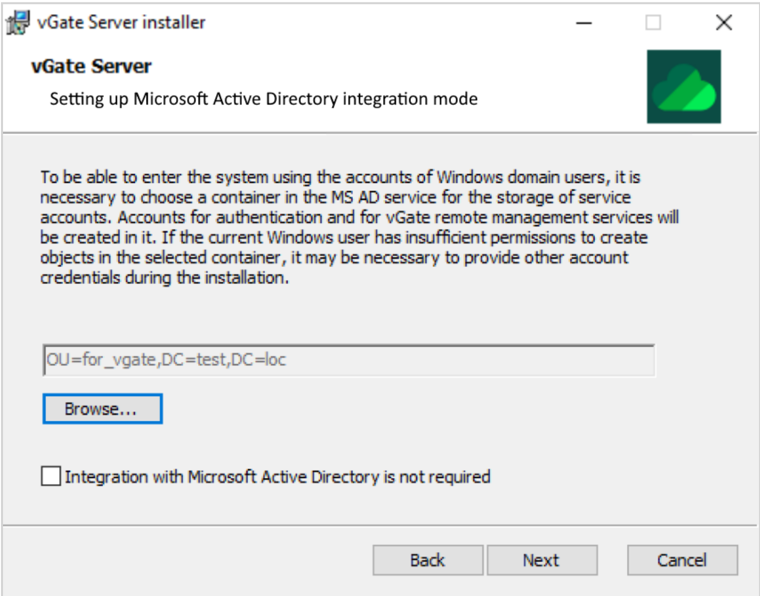
11. Enter the name of the vGate account registry and click "Next".

The following dialog box appears.



12. Enter the chief security officer credentials and click "Next".

If the computer's account is in the Windows domain, the following dialog box will appear.



Note. If the local administrator's account is used, error message "Could not connect to the directory service" will appear. The field for selecting the container for vGate accounts will be empty, and the "Browse" button will be unavailable.

13. Specify the organizational unit (OU) created during configuration of the local network (see p. **12**) to store vGate service accounts, and click "Next".

Tip. Select the "Integration with Microsoft Active Directory is not required" check box if you do not expect authentication in vGate with a reference to Windows domain user credentials.

Note. If the administrator account does not have Account Operator privileges, the installation program will prompt you to enter the credentials of the account with such privileges. Otherwise, the installation will be stopped.

A dialog box appears saying that everything is ready for the installation.

14. Click the "Install" button.

The process of file copying to the hard disk and configuring the installed components will be started. The progress will be displayed in the installation program dialog box in the form of a progress bar.

After successful installation and configuration of components, a dialog box informing you about successful completion of the installation will appear.

15. Click "Finish".

Note. In some cases, a requirement to restart the computer will appear. To restart, click the "Yes" button in the message box.

Installation for working without a standalone router

Prepare your computer before installation:

On the computer designated to be the vGate Server, configure two LAN connections.

Adapter	Subnet	LAN settings
Adapter 1	Infrastructure administration network	IP address from the address range of the secure network perimeter used by ESXi, vCenter, Skala-R and KVM servers for configuration and audit. The examples use the IP address: **192.168.1.2**
Adapter 2	Network of the external administration perimeter	IP address from the address range of the external network used for connections to virtual infrastructure administrator and security administrator workstations. The examples use the IP address: **192.168.2.3**

To install the vGate Server:

1. Log on using the computer administrator credentials.
2. Insert the setup disk into the drive.

   Note. If the setup program does not start automatically, run the autorun.exe file from the \autorun folder.

   The starting dialog box of the setup program appears.
3. In the starting dialog box, click the "vGate Server" link.

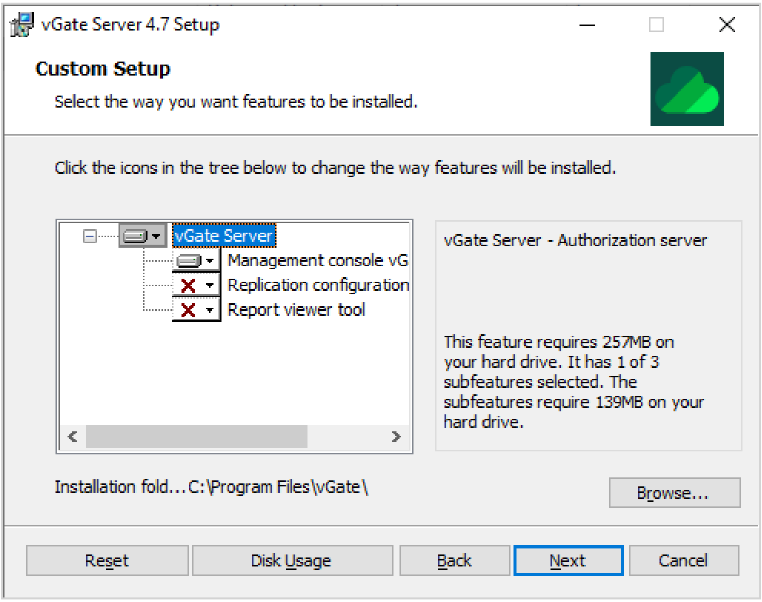
   Tip. To install this product, you can also run the \vGate\vGateServer.msi file from the setup disk.

   The program will complete certain preparations, after which the welcome dialog box appears.
4. Click "Next".

   The license agreement dialog box appears.
5. Read the entire license agreement, select the "I accept the terms in the License Agreement" check box and click "Next".

   Tip. In order to obtain a paper copy of the license agreement, click "Print".

   A dialog box to select components to be installed appears.



6. Select components to be installed.

Note.

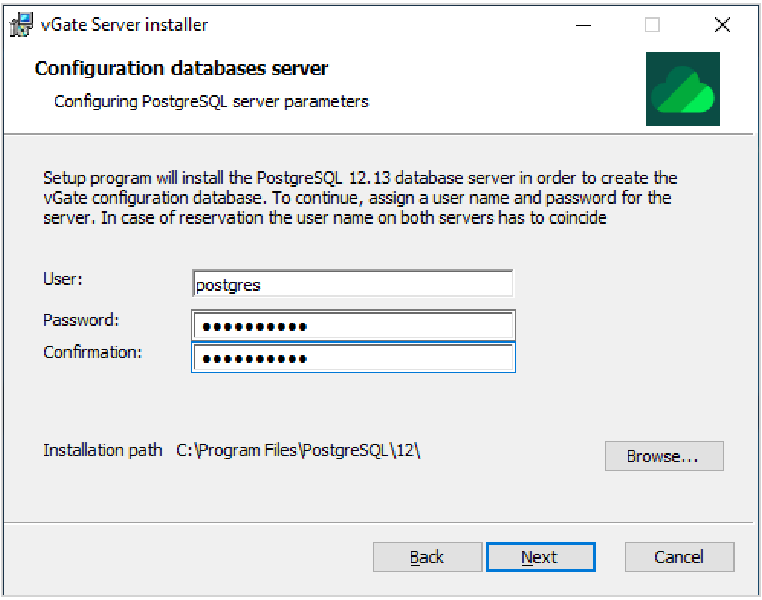
- In order to use the report viewer function, select the "Report viewer tool" component for installation. To do this, open the drop-down menu to the left of the component name and select "Will be installed on local hard drive".
- The "Replication configuration" component is not installed by default. If you intend to replicate the vGate Server (see p.25), select this component for installation. To prohibit the component installation, in the drop-down menu to the left of the component name select "Entire feature will be unavailable".

A dialog box has the following buttons:

Button	Action
Browse	Opens the dialog box for modifying the path to the setup directory
Disk usage	Opens the dialog box with information about free space on disks of the computer
Reset	Returns installation components to their default state

7. Click "Next".

The following dialog box appears.

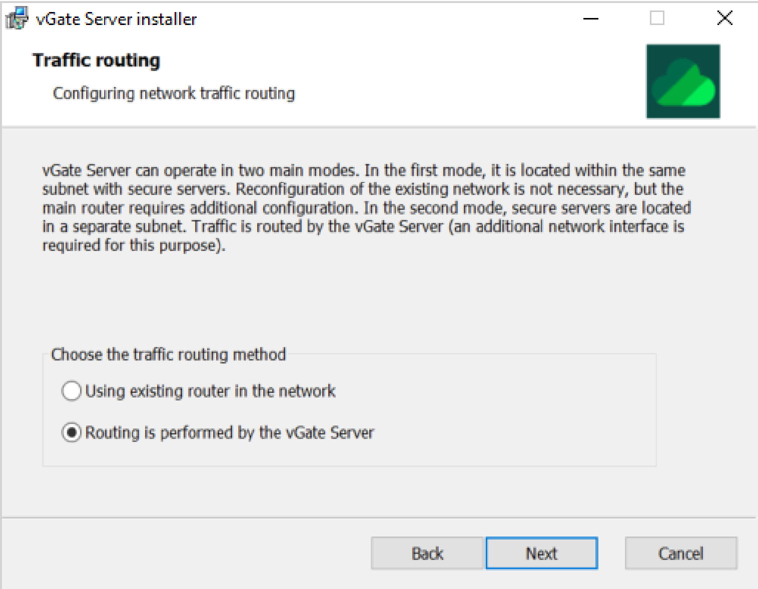


8. Enter the name and password of the PostgreSQL database server user. If necessary, modify the path to the folder for database installation, and click "Next". When you install vGate in replication mode, PostgreSQL user names on the main and redundant servers must match.

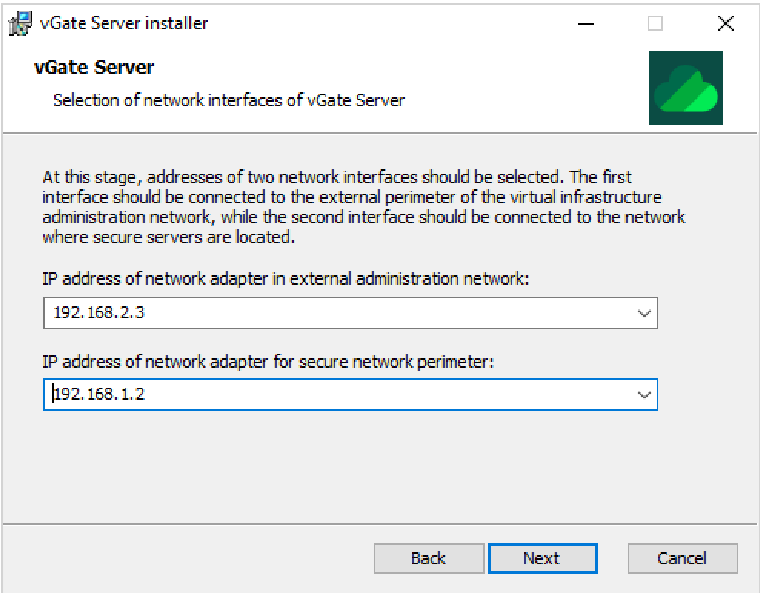
Note.

- PostgreSQL 12.13 server will be installed automatically while installing vGate. vGate configuration database will be created on it. If the PostgreSQL server is already installed on the computer, you must remove it before the vGate software installation.
- By default, vGate 4.0 and later uses PostgreSQL database port 5432. This port can only be changed if PostgreSQL is installed separately (before the vGate software installation). PostgreSQL database ports for the main and redundant server must match.

The following dialog box appears.



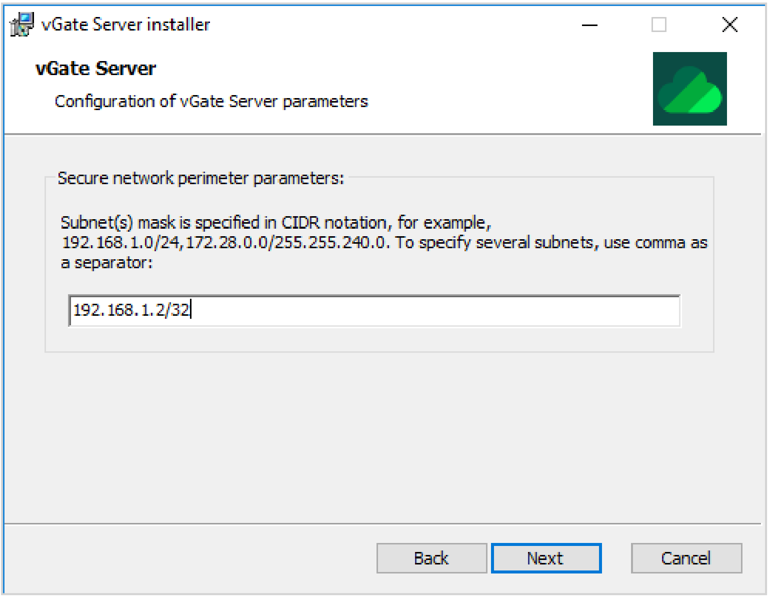
9. Select the "Routing is performed by the vGate Server" traffic routing method and click "Next".
   The following dialog box appears.



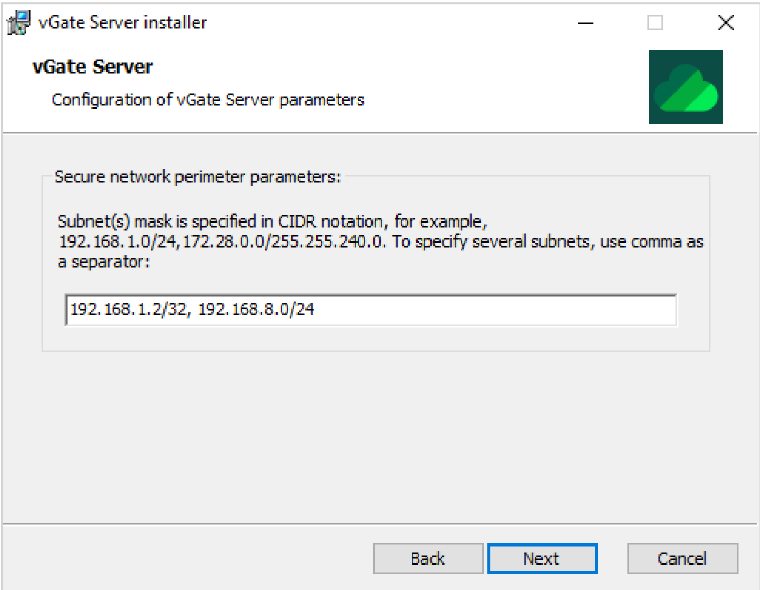
10. Enter network parameters of the vGate Server and click "Next".

Parameter	**Description**
IP address of network adapter in external administration network	IP address of the server in the external perimeter of infrastructure administration network (subnets, where the security administrator and virtual infrastructure administrator workstations are located)
IP address of network adapter for secure network perimeter	IP address of the server in the secure perimeter of infrastructure administration network (subnets, where virtual infrastructure protected servers are located)

The following dialog box appears.



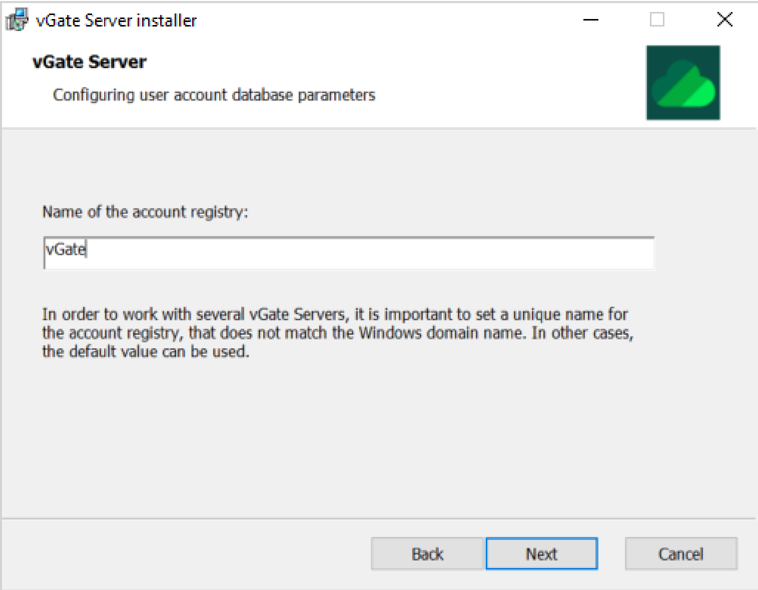
11. If the secure perimeter of the administration network is made up of several subnets, enter their IP addresses using the comma as a separator.



Therefore, data transfer into the secure perimeter is only allowed when the destination IP address corresponds to one of the specified subnets.

12. Validate IP addresses of subnets where protected ESXi, KVM, Skala-R, OpenNebula and Proxmox servers are located, and click "Next".

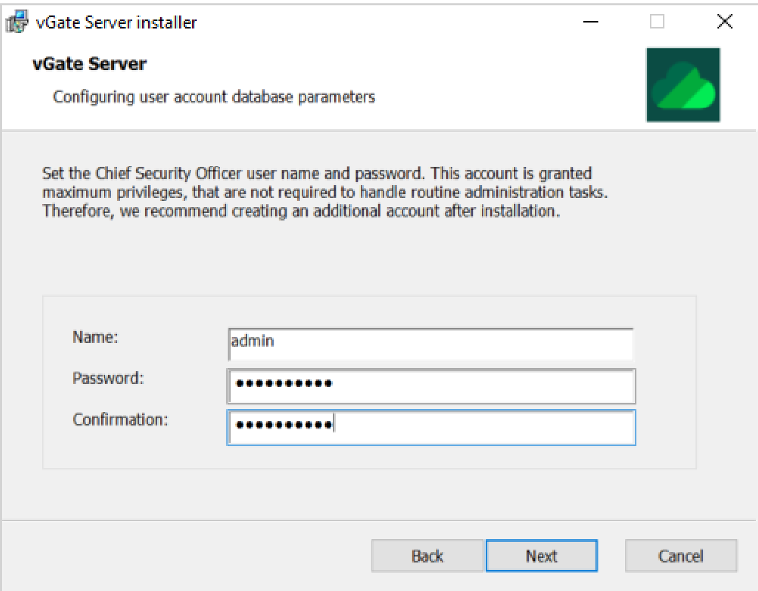
The following dialog box appears.



Note. If you intend to use several vGate Servers in the network, specify a unique name for the vGate account registry during installation of each vGate Server.

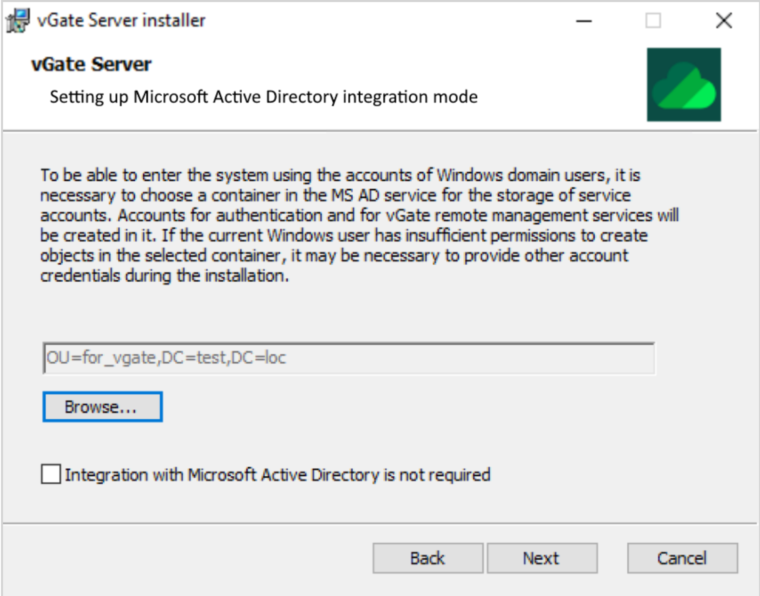
13. Enter the name of the vGate account registry and click "Next".

The following dialog box appears.



14. Enter the chief security officer credentials and click "Next".

If the computer's account is in the Windows domain, the following dialog box will appear.



Note. If the local administrator's account is used, error message "Could not connect to the directory service" will appear. The field for selecting the container for vGate accounts will be empty, and the "Browse" button will be unavailable.

15. Specify the organizational unit (OU) created during configuration of the local network (see p.**12**) to store vGate service accounts, and click "Next".

Tip. Select the "Integration with Microsoft Active Directory is not required" check box if you do not expect authentication in vGate with a reference to Windows domain user credentials.

Note. If the administrator account does not have Account Operator privileges, the installation program will prompt you to enter the credentials of the account with such privileges. Otherwise, the installation will be stopped.

A dialog box appears saying that everything is ready for the installation.

16. Click the "Install" button.

The process of file copying to the hard disk and configuring the installed components will be started. The progress will be displayed in the installation program dialog box in the form of a progress bar.

After successful installation and configuration of components, a dialog box informing you about successful completion of the installation will appear.

17. Click "Finish".

Note. In some cases, a requirement to restart the computer will appear. To restart, click the "Yes" button in the message box.

vGate Server installation and setup in the replication mode

The vGate Server replication mechanism is available in vGate Enterprise and Enterprise Plus only (see the "Functionality" section in the document [1]).

vGate provides the vGate Server replication mechanism. For this purpose, you must install two vGate Servers — the main and the redundant servers — and configure data replication between them. In case of the main server failure, control is switched to the redundant vGate Server manually or automatically (if the hot standby function is set up, see p.**62**).

Attention! Before installing the redundant vGate Server, the vGate demo license or the vGate Enterprise/Enterprise Plus license must be registered in the vGate R2 web console.

Installation and later operation of the vGate Server with replication is possible in two modes, depending on the method of traffic routing between the external and secure perimeters of the administration network:

- Using the existing router in the network (see p.**26**).

  In this mode, the vGate Server is located in the secure perimeter of the administration network, in the same subnet, where protected servers are located (see Figure 2 on p.**14**). This mode does not require reconfiguration of the existing network and provides the availability of a certified firewall (router) in the external administration network to filter network traffic to protected servers. On the router, access from virtual infrastructure administrator and security administrator workstations to the protected subnet or individual servers should be closed, and access to the vGate Server should be allowed. For details on configuring a router, see p.**191**.

- Using the vGate Server (see p.**34**).

  In this mode, protected servers should be located in a separate subnet. On all computers in the secure perimeter of the administration network (ESXi, vCenter, Skala-R, KVM, OpenNebula, Proxmox servers), specify the IP address of the secure perimeter adapter of the vGate Server as a default gateway. On all virtual infrastructure administrator workstations, specify the IP address of the network adapter of the vGate server in the external administration network as a default gateway.

  This mode does not require additional router configuration.

Attention!

- If you intend to use Active Directory, the computers designated to be the main vGate Server and the redundant vGate Server, should be added to the same domain.
- If the vGate Server computer was added to the domain after the vGate software installation, this domain should be added to the list of trusted domains in the vGate web console (see p.67).

Attention! If you intend to use the report viewer function on the computers designated to be the main vGate Server and the redundant vGate Server, Microsoft Report Viewer 2010 SP1 Redistributable Package should be installed in advance. To do this, run the ReportViewer.exe file from the folder \Redistributables\Microsoft Report Viewer Redistributable 2010 of the setup disk, and follow the setup wizard instructions.

Installation using a third-party router

Prepare your computer before installation:

On the computer designated to be the main vGate Server, configure two LAN connections.

Adapter	Subnet	LAN settings
Adapter 1	Infrastructure administration network	• The main IP address used by ESXi, vCenter, Skala-R and KVM servers for configuration and audit. The examples use the IP address: **192.168.1.2**. • An additional IP address used in case of the main server failure. The examples use the IP address: **192.168.1.12**.
Adapter 2	Replication network	IP address from the address range of replication network to be used for data replication between the main and redundant vGate Servers. The examples use the IP address: **192.168.3.2**

Note. IP address for replication should not belong to the infrastructure administration network.

On the computer designated to be the redundant vGate Server, configure two LAN connections.

Adapter	Subnet	LAN settings
Adapter 1	Infrastructure administration network	IP address, used by ESXi, vCenter, Skala-R and KVM servers for configuration and audit. The examples use the IP address: **192.168.1.22**
Adapter 2	Replication network	IP address from the address range of the replication network, used for connection to the main vGate Server. The examples use the IP address: **192.168.3.22**

Note. IP address for replication should not belong to the infrastructure administration network.

To install the main vGate Server:

1. Log on using the computer administrator credentials.
2. Insert the setup disk into the drive.

   Note. If the setup program does not start automatically, run the autorun.exe file from the \autorun folder.

   The starting dialog box of the setup program appears.
3. In the starting dialog box, click the "vGate Server" link.

Tip. To install this product, you can also run the \vGate\vGateServer.msi file from the setup disk.

The program will complete certain preparations, after which the welcome dialog box appears.

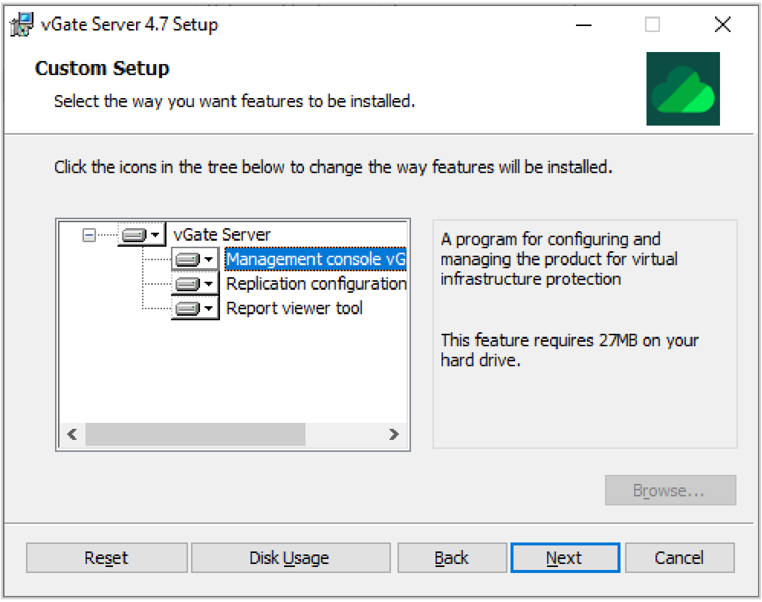
4. Click "Next".

   The license agreement dialog box appears.

5. Read the entire license agreement, select the "I accept the terms in the License Agreement" check box and click "Next".

Tip. In order to obtain a paper copy of the license agreement, click "Print".

A dialog box to select components to be installed appears.



6. Select components to be installed.

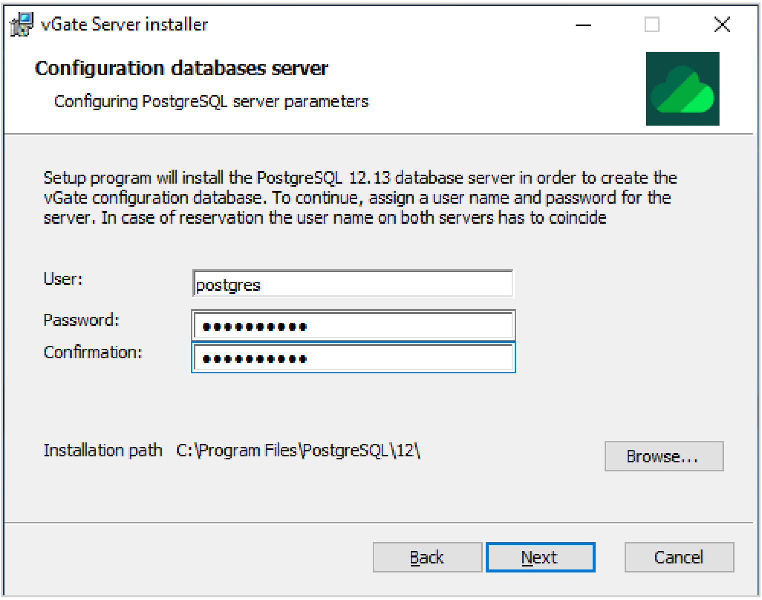
Note.
- In order to use the report viewer function, select the "Report viewer tool" component for installation. To do this, open the drop-down menu to the left of the component name and select "Will be installed on local hard drive".
- Select the "Replication configuration" component for installation.

A dialog box has the following buttons:

Button	Action
Browse	Opens the dialog box for modifying the path to the setup directory
Disk usage	Opens the dialog box with information about free space on disks of the computer
Reset	Returns installation components to their default state

7. Click "Next".

   The following dialog box appears.

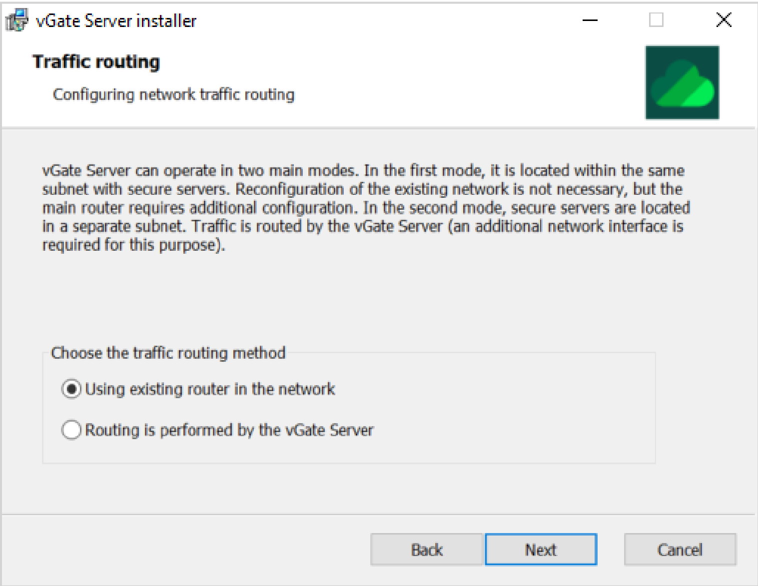


8. Enter the name and password of the PostgreSQL database server user. If necessary, modify the path to the folder for database installation, and click "Next". When you install vGate in replication mode, PostgreSQL user names on the main and redundant servers must match.

Note.

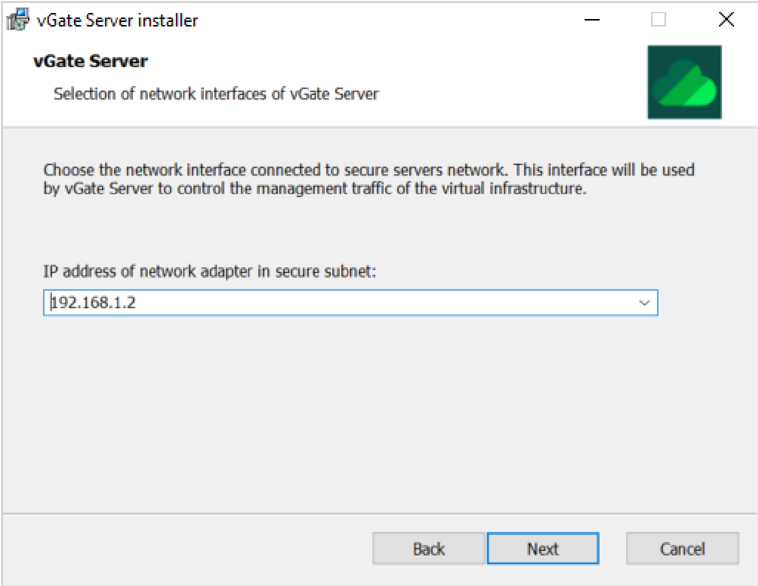
- PostgreSQL 12.13 server will be installed automatically while installing vGate. vGate configuration database will be created on it. If the PostgreSQL server is already installed on the computer, you must remove it before the vGate software installation.
- By default, vGate 4.0 and later uses PostgreSQL database port 5432. This port can only be changed if PostgreSQL is installed separately (before the vGate software installation). PostgreSQL database ports for the main and redundant server must match.

The following dialog box appears.



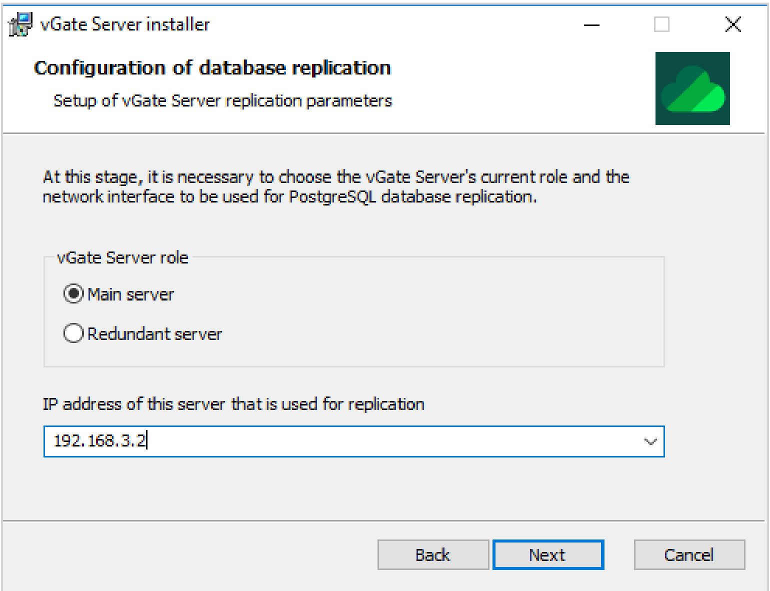
9. Select the "Using existing router in the network" traffic routing method and click "Next".

The following dialog box appears.



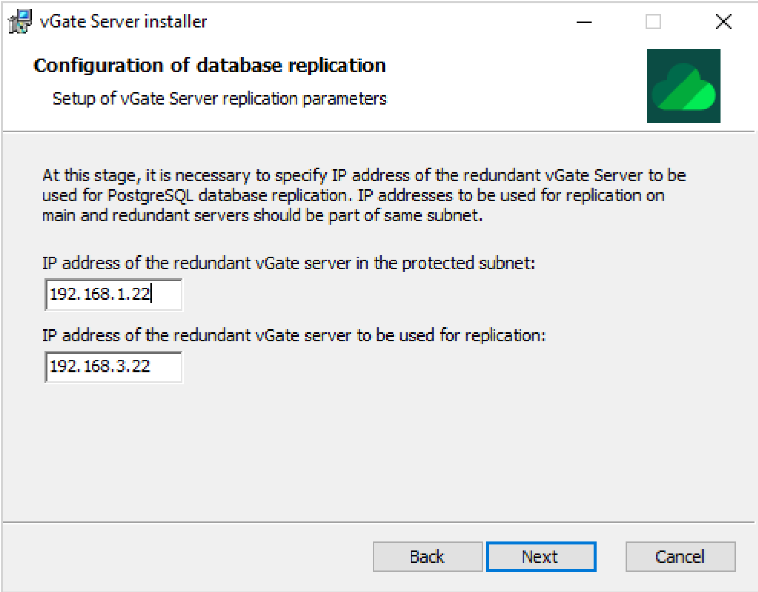
10. Enter the IP address of the adapter 1 of the vGate Server, through which routes will pass to/from the secure perimeter of the administration network, and click "Next".

As you select the "Replication configuration" component for installation, a dialog box for setting up the replication parameters will appear.



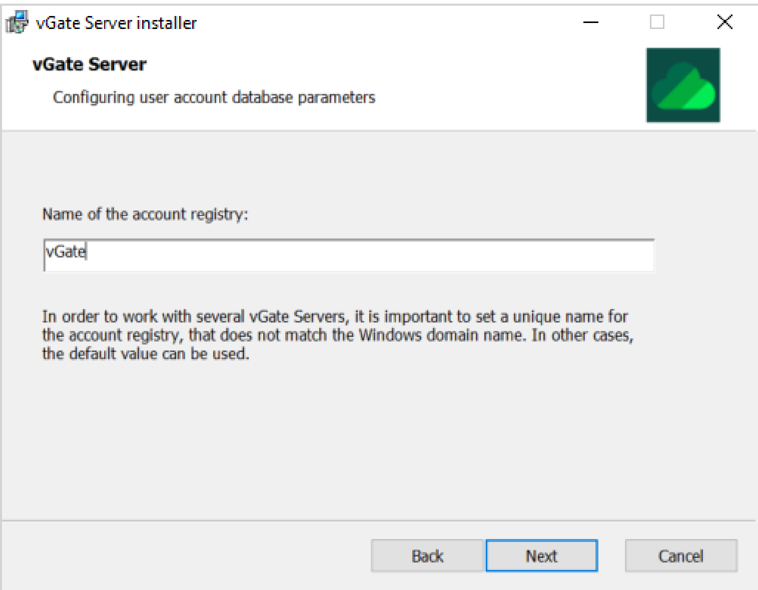
11. Set the vGate Server role to "Main server", enter the server IP address to be used for data replication between the main and redundant vGate Servers in the replication network. After this, click "Next".

    A dialog box for setting up the redundant server parameters appears.



12. Specify the IP address of the redundant vGate Server in the protected subnet, as well as the IP address of the redundant vGate Server to be used for replication. After this, click "Next".

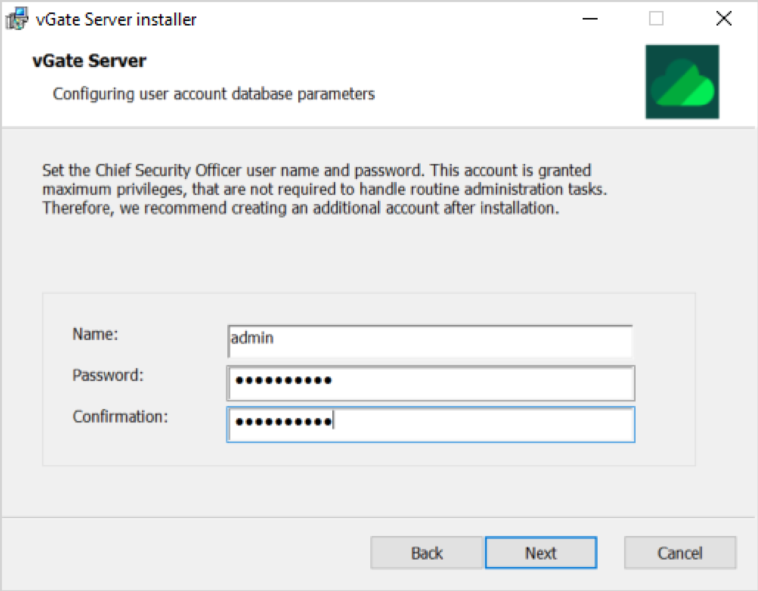
    The following dialog box appears.



Note. If you intend to use several vGate Servers in the network, specify a unique name for the vGate account registry during installation of each vGate Server.

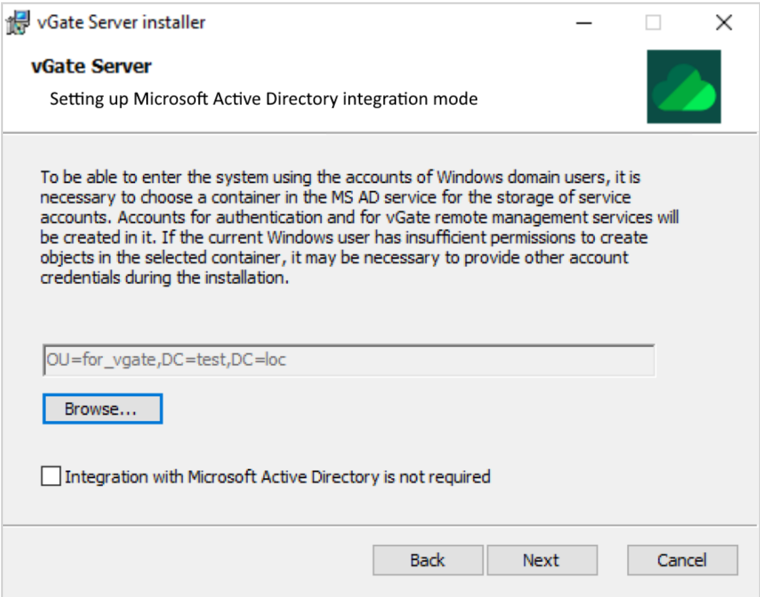
13. Enter the name of the vGate account registry and click "Next".

The following dialog box appears.



14. Enter the chief security officer credentials and click "Next".

If the computer's account is in the Windows domain, the following dialog box will appear.



Note. If the local administrator's account is used, error message "Could not connect to the directory service" will appear. The field for selecting the container for vGate accounts will be empty, and the "Browse" button will be unavailable.

15. Specify the organizational unit (OU) created during configuration of the local network (see p.**12**) to store vGate service accounts, and click "Next".

Tip. Select the "Integration with Microsoft Active Directory is not required" check box if you do not expect authentication in vGate with a reference to Windows domain user credentials.

Note. If the administrator account does not have Account Operator privileges, the installation program will prompt you to enter the credentials of the account with such privileges. Otherwise, the installation will be stopped.

A dialog box appears saying that everything is ready for the installation.

16. Click the "Install" button.

The process of file copying to the hard disk and configuring the installed components will be started. The progress will be displayed in the installation program dialog box in the form of a progress bar.

After successful installation and configuration of components, a dialog box informing you about successful completion of the installation will appear.

17. Click "Finish".

Note. In some cases, a requirement to restart the computer will appear. To restart, click the "Yes" button in the message box.

To install the redundant vGate Server

1. Log on using the computer administrator credentials.
2. Insert the setup disk into the drive.

Note. If the setup program does not start automatically, run the autorun.exe file from the \autorun folder.

The starting dialog box of the setup program appears.

3. In the starting dialog box, click the "vGate Server" link.

Tip. To install this product, you can also run the \vGate\vGateServer.msi file from the setup disk.

The setup program will complete certain preparations, after which the welcome dialog box will appear.

4. Click "Next".

The license agreement dialog box appears.

5. Read the entire license agreement, select the "I accept the terms in the License Agreement" check box and click "Next".

Tip. In order to obtain a paper copy of the license agreement, click "Print".

A dialog box to select components to be installed will appear.

6. Open the drop-down menu to the left of the "Replication configuration" component and select "Will be installed on local hard drive". Click "Next".

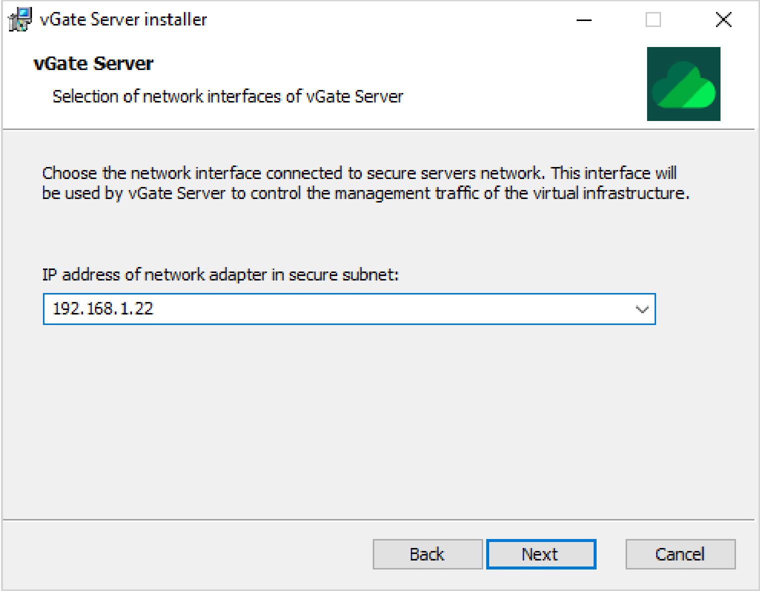
The dialog box for PostgreSQL database installation appears.

7. Enter the name and password of the PostgreSQL database server user. If necessary, modify the path to the folder for database installation, and click "Next".

The dialog box to select the traffic routing method appears.

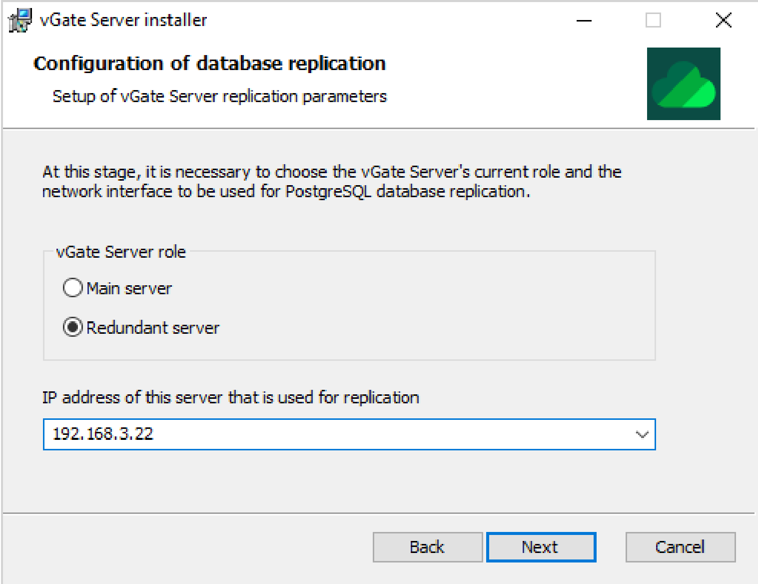
8. Select the traffic routing method "Using existing router in the network" and click "Next".

A dialog box for setting up the network parameters appears.



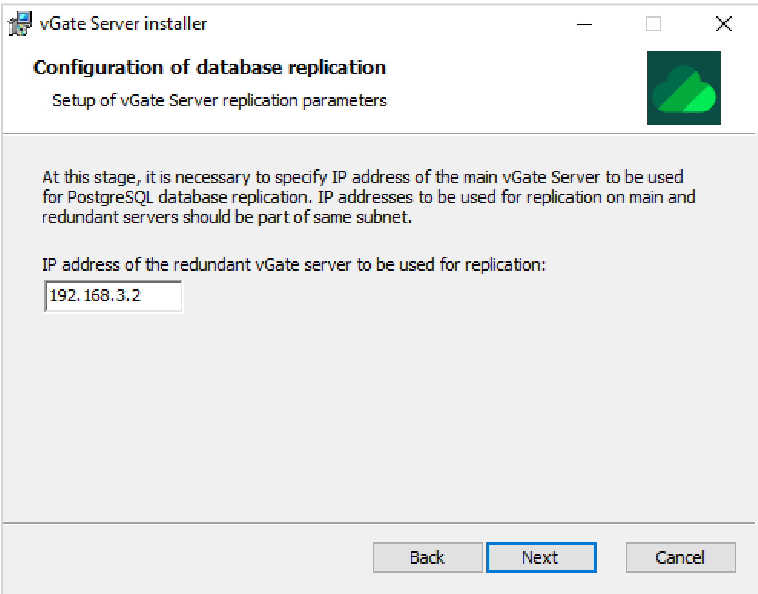
9. Enter IP address of the network adapter of the redundant vGate Server and click "Next".

   A dialog box for setting up the replication parameters appears on the screen.



10. Set the vGate Server role to "Redundant server", enter IP address of the server to be used for data replication between the main and redundant vGate Servers in the replication network. After this, click "Next".

    A dialog box for setting up the main server parameters appears.



11. Enter the IP address of the main vGate Server in the replication network to be used for replication and click "Next".

    A dialog box appears saying that everything is ready for the installation.

12. Click "Install".

    The process of file copying to the hard disk and configuring the installed components will be started. The progress will be displayed in the installation program dialog in the form of a progress bar.

    After successful installation and configuration of components, a dialog box informing you about successful completion of the installation will appear.

13. Click "Finish".

Note. In some cases, a requirement to restart the computer will appear. To restart, click the "Yes" button in the message box.

Details on configuring the replication between the main and redundant servers can be found on p.51.

Installation for working without a standalone router

Installation of the vGate Server with replication in routing mode via the vGate Server.

Prepare your computer before installation:

On the computer designated to be the main vGate Server, configure three LAN connections.

Adapter	Subnet	LAN settings
Adapter 1	Infrastructure administration network	• The main IP address from the address range of the secure network perimeter used by ESXi, vCenter, Skala-R and KVM servers for configuration and audit. The examples use the IP address: **192.168.1.2**. • An additional IP address used in case of the main server failure. The examples use the IP address: **192.168.1.12**.
Adapter 2	Network of the external administration perimeter	IP address from the address range of the external network used for connections to virtual infrastructure administrator and security administrator workstations. The examples use the IP address: **192.168.2.3**
Adapter 3	Replication network	IP address from the address range of the replication network to be used for replication between the main and redundant vGate Server. The examples use the IP address: **192.168.3.2**

Note. IP address for replication should not belong to the infrastructure administration network.

On the computer designated to be the redundant vGate Server, configure three LAN connections.

Adapter	Subnet	LAN settings
Adapter 1	Infrastructure administration network	IP address from the address range of the secure perimeter, used by ESXi, vCenter, Skala-R and KVM servers for configuration and audit. The examples use the IP address: **192.168.1.22**
Adapter 2	Network of the external administration perimeter	IP address from the address range of the external network, used for connections to virtual infrastructure administrator and security administrator workstations. The examples use the IP address: **192.168.2.4**
Adapter 3	Replication network	IP address from the address range of the replication network, used for connection to the main vGate Server. The examples use the IP address: **192.168.3.22**

Note. IP address for replication should not belong to the infrastructure administration network.

To install the main vGate Server:

1. Log on using the computer administrator credentials.
2. Insert the setup disk into the drive.

   Note. If the setup program does not start automatically, run the autorun.exe file from the \autorun folder.

   The starting dialog box of the setup program appears.
3. In the starting dialog box, click the "vGate Server" link.

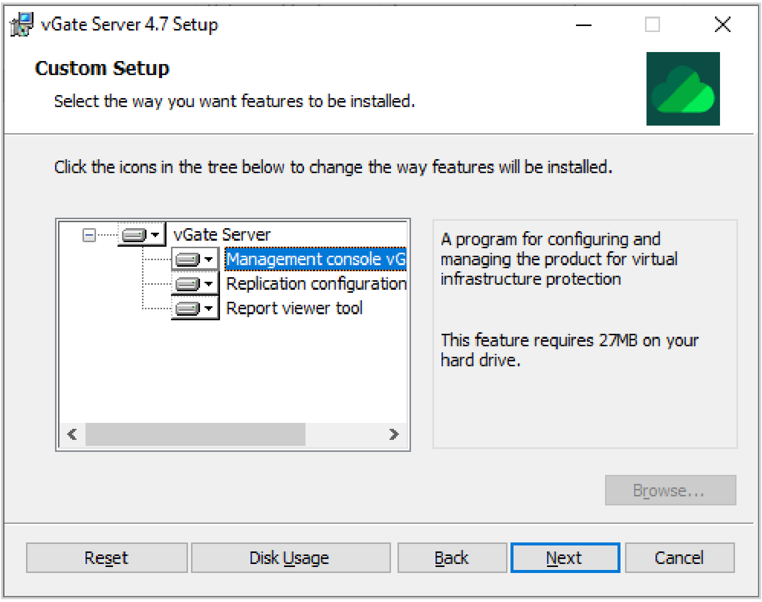
   Tip. To install this product, you can also run the \vGate\vGateServer.msi file from the setup disk.

   The program will complete certain preparations, after which the welcome dialog box appears.
4. Click "Next".

   The license agreement dialog box appears.
5. Read the entire license agreement, select the "I accept the terms in the License Agreement" check box and click "Next".

   Tip. In order to obtain a paper copy of the license agreement, click "Print".

A dialog box to select components to be installed appears.



6. Select components to be installed.

Note.

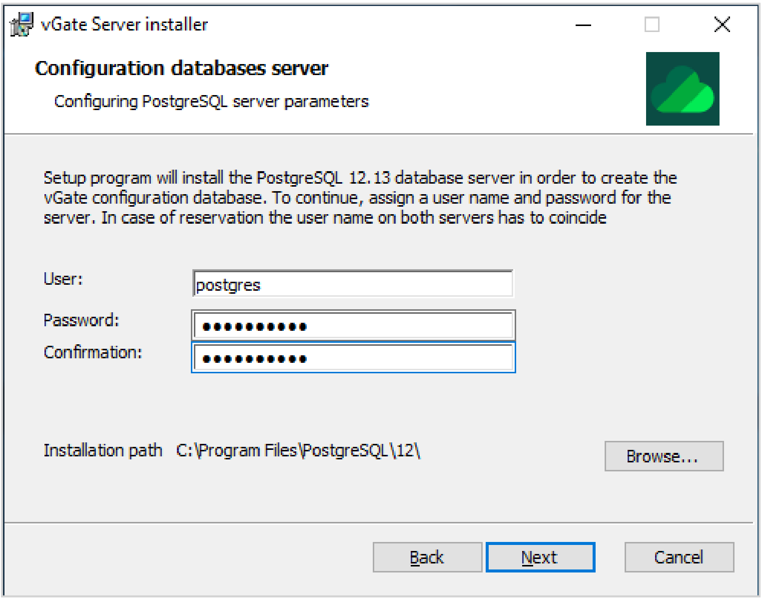
- In order to use the report viewer function, select the "Report viewer tool" component for installation. To do this, open the drop-down menu to the left of the component name and select "Will be installed on local hard drive".
- Select the "Replication configuration" component for installation.

A dialog box has the following buttons:

Button	Action
Browse	Opens the dialog box for modifying the path to the setup directory
Disk usage	Opens the dialog box with information about free space on disks of the computer
Reset	Returns installation components to their default state

7. Click "Next".

The following dialog box appears.

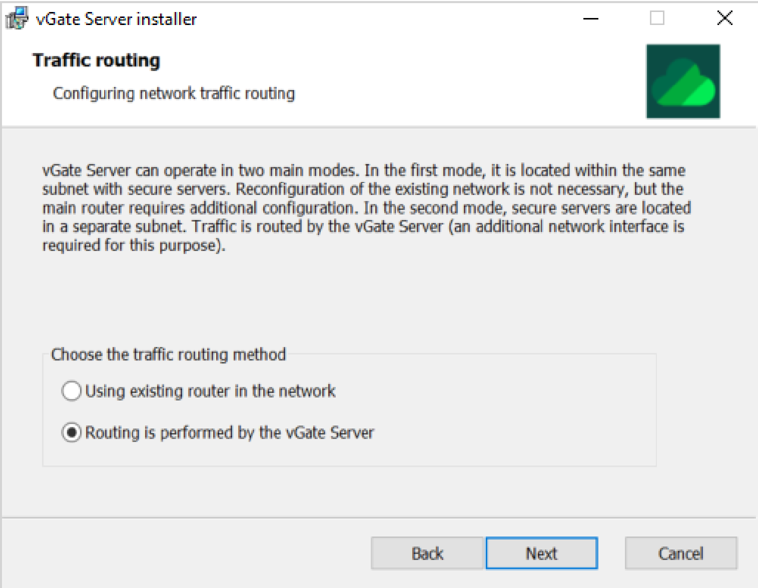


8. Enter the name and password of the PostgreSQL database server user. If necessary, modify the path to the folder for database installation, and click "Next". When you install vGate in replication mode, PostgreSQL user names on the main and redundant servers must match.

Note.

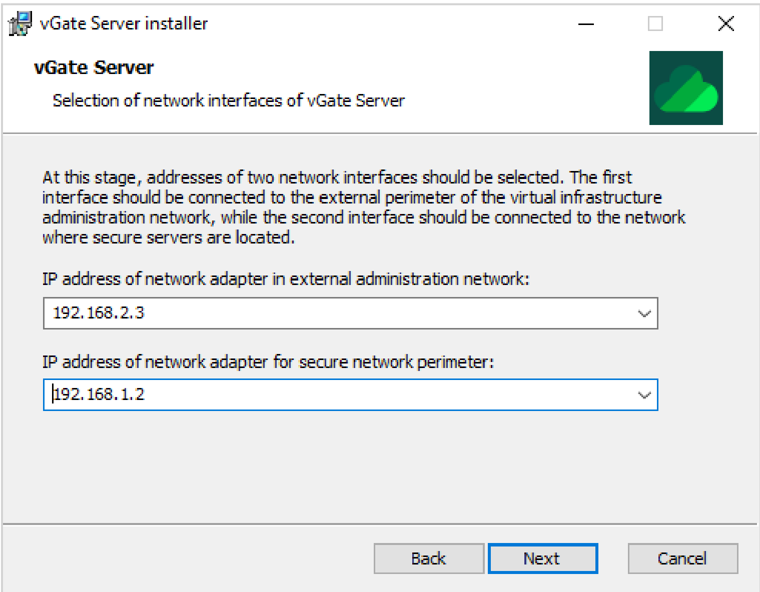
- PostgreSQL 12.13 server will be installed automatically while installing vGate. vGate configuration database will be created on it. If the PostgreSQL server is already installed on the computer, you must remove it before the vGate software installation.
- By default, vGate 4.0 and later uses PostgreSQL database port 5432. This port can only be changed if PostgreSQL is installed separately (before the vGate software installation). PostgreSQL database ports for the main and redundant server must match.

The following dialog box appears.



9. Select the "Routing is performed by the vGate Server" traffic routing method and click "Next".

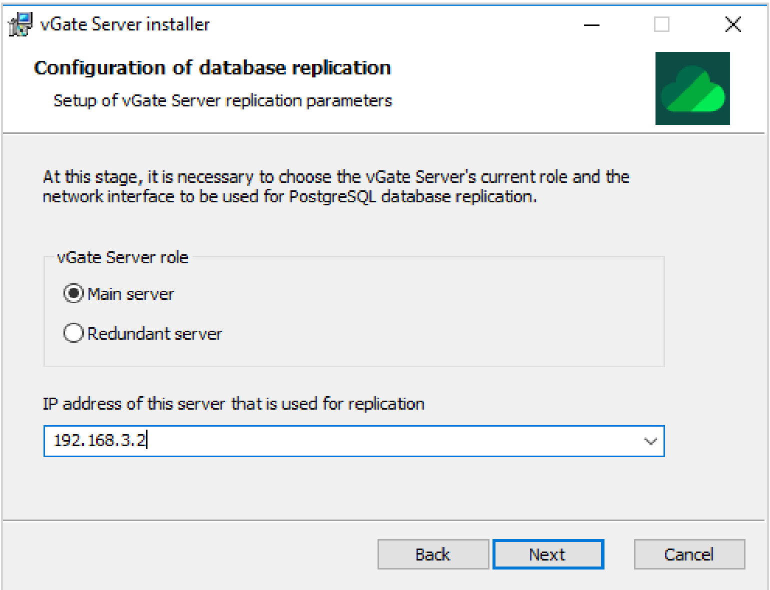
The following dialog box appears.



10. Enter network parameters of the vGate Server and click "Next".

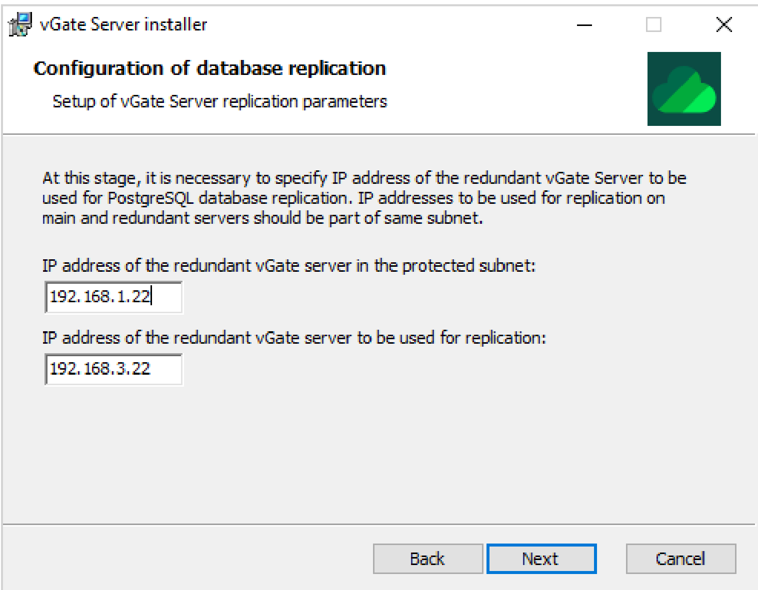
Parameter	Description
IP address of network adapter in external administration network	IP address of the server in the external perimeter of infrastructure administration network (subnets, where the security administrator and virtual infrastructure administrator workstations are located)
IP address of network adapter for secure network perimeter	IP address of the server in the secure perimeter of infrastructure administration network (subnets, where virtual infrastructure protected servers are located)

As you select the "Replication configuration" component for installation, a dialog box for setting up the replication parameters will appear.



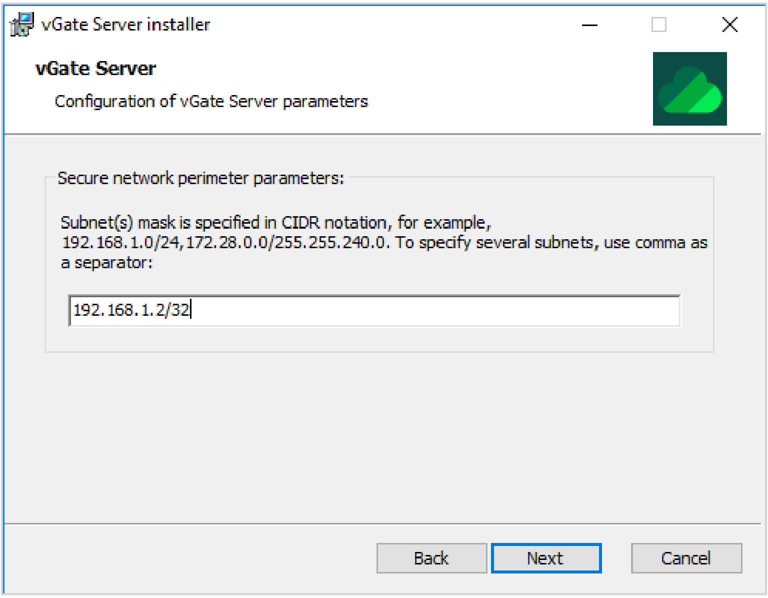
11. Set the vGate Server role to "Main server", enter the server IP address to be used for data replication between the main and redundant vGate Servers in the replication network. After this, click "Next".

A dialog box for setting up the redundant server parameters appears.

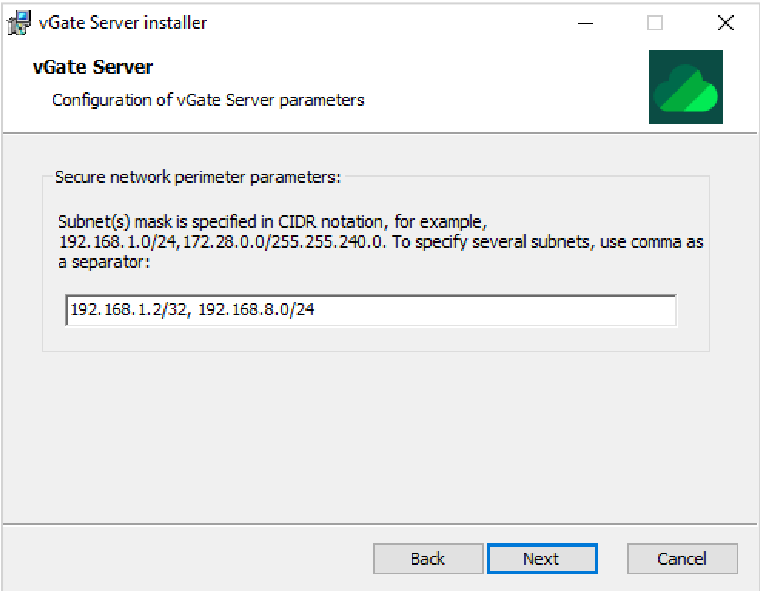


12. Specify the IP address of the redundant vGate Server in the protected subnet, as well as the IP address of the redundant vGate Server to be used for replication. After this, click "Next".

    The following dialog box appears.



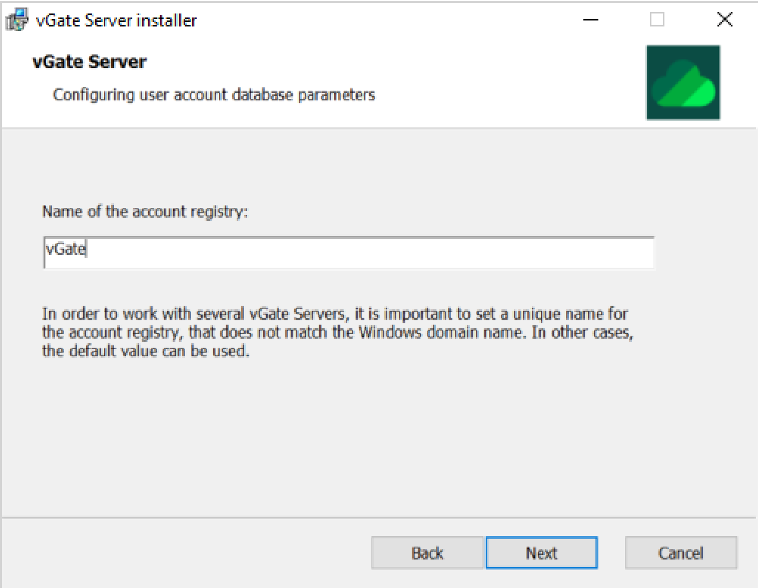
13. If the secure perimeter of the administration network is made up of several subnets, enter their IP addresses using the comma as a separator.



    Therefore, data transfer into the secure perimeter is only allowed when the destination IP address corresponds to one of the specified subnets.

14. Validate IP addresses of subnets where protected ESXi, KVM, Skala-R, OpenNebula and Proxmox servers are located, and click "Next".

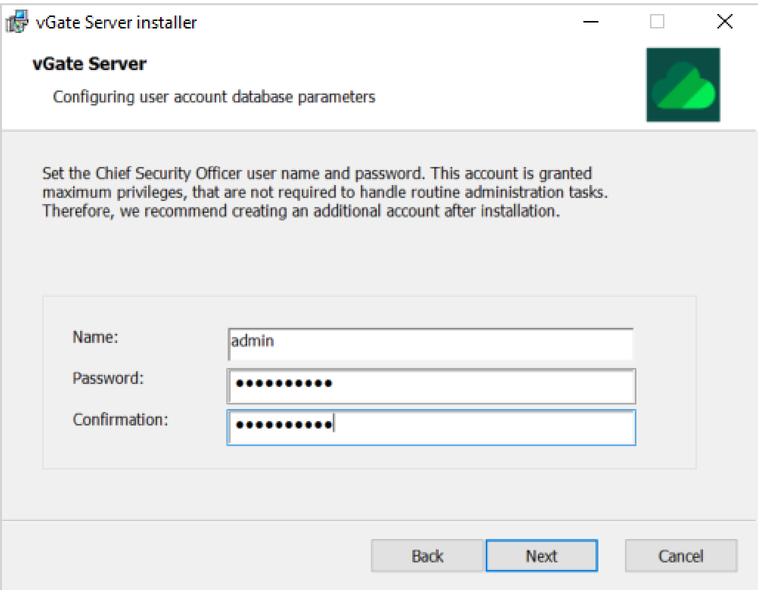
The following dialog box appears.



Note. If you intend to use several vGate Servers in the network, specify a unique name for the vGate account registry during installation of each vGate Server.

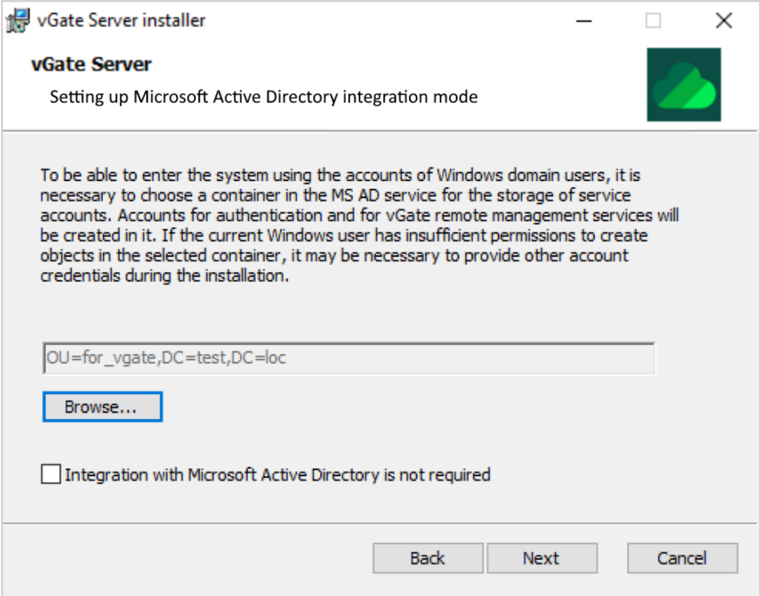
15. Enter the name of the vGate account registry and click "Next".

The following dialog box appears.



16. Enter the chief security officer credentials and click "Next".

If the computer's account is in the Windows domain, the following dialog box will appear.



Note. If the local administrator's account is used, error message "Could not connect to the directory service" will appear. The field for selecting the container for vGate accounts will be empty, and the "Browse" button will be unavailable.

17. Specify the organizational unit (OU) created during configuration of the local network (see p. **12**) to store vGate service accounts, and click "Next".

Tip. Select the "Integration with Microsoft Active Directory is not required" check box if you do not expect authentication in vGate with a reference to Windows domain user credentials.

Note. If the administrator account does not have Account Operator privileges, the installation program will prompt you to enter the credentials of the account with such privileges. Otherwise, the installation will be stopped.

A dialog box appears saying that everything is ready for the installation.

18. Click the "Install" button.

The process of file copying to the hard disk and configuring the installed components will be started. The progress will be displayed in the installation program dialog box in the form of a progress bar.

After successful installation and configuration of components, a dialog box informing you about successful completion of the installation will appear.

19. Click "Finish".

Note. In some cases, a requirement to restart the computer will appear. To restart, click the "Yes" button in the message box.

To install the redundant vGate Server:

1. Log on using the computer administrator credentials.
2. Insert the setup disk into the drive.

   Note. If the setup program does not start automatically, run the autorun.exe file from the \autorun folder.

   The starting dialog box of the setup program appears.
3. In the starting dialog box, click the "vGate Server" link.

   Tip. To install this product, you can also run the \vGate\vGateServer.msi file from the setup disk.

   The setup program will complete certain preparations, after which the welcome dialog box will appear.
4. Click "Next".

   The license agreement dialog box appears.

5. Read the entire license agreement, select the "I accept the terms in the License Agreement" check box and click "Next".

Tip. In order to obtain a paper copy of the license agreement, click "Print".

A dialog box to select components to be installed will appear.

6. Open the drop-down menu to the left of the "Replication configuration" component and select "Will be installed on local hard drive". Click "Next".

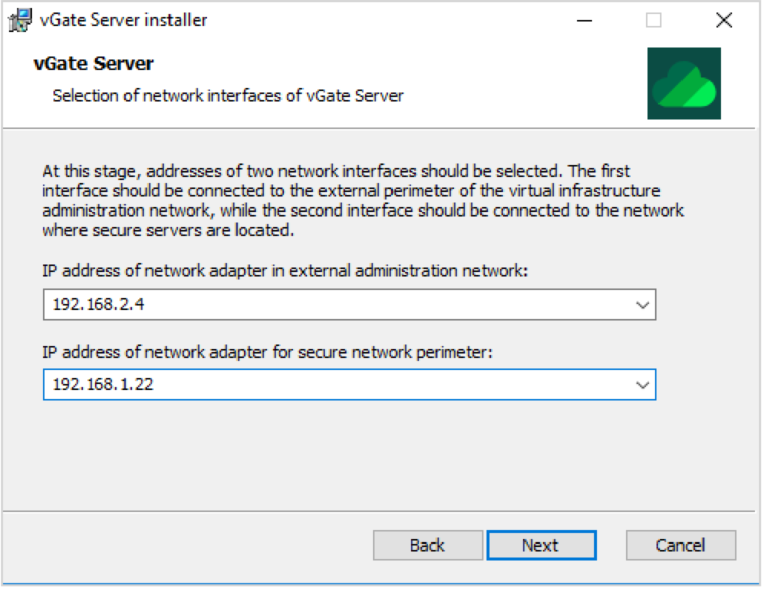
The dialog box for PostgreSQL database installation appears.

7. Enter the name and password of the PostgreSQL database server user. If necessary, modify the path to the folder for database installation, and click "Next".

The dialog box to select the traffic routing method appears.

8. Select the traffic routing method "Routing is performed by the vGate Server" and click "Next".

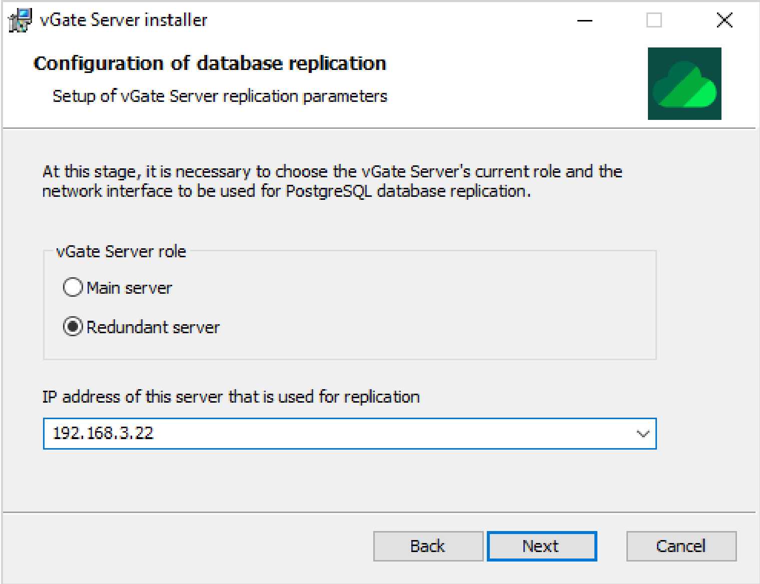
A dialog box for setting up the network parameters appears.



9. Enter the network parameters of the redundant vGate Server and click "Next".

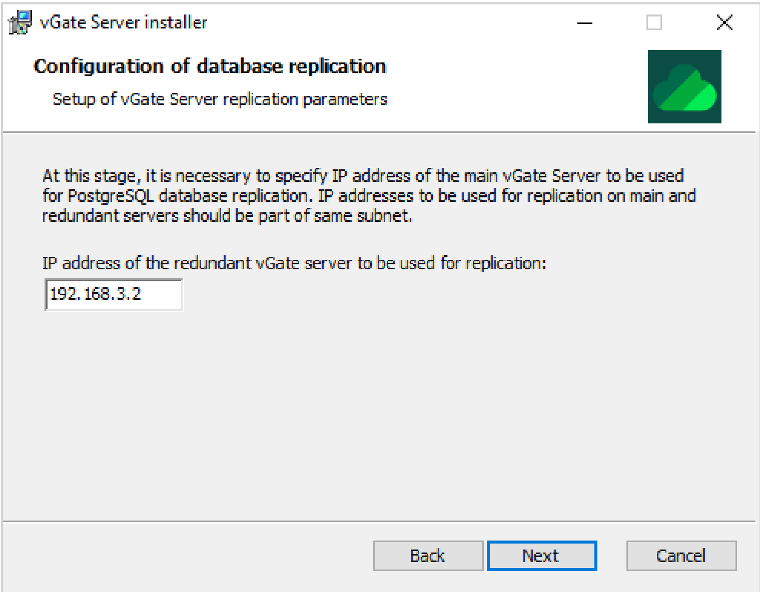
Parameter	Description
IP address of network adapter in external administration network	IP address of redundant server in external perimeter of infrastructure administration network
IP address of network adapter for secure perimeter	IP address of redundant server in infrastructure administration network

A dialog box for setting up the replication parameters appears on the screen.



10. Set the vGate Server role to "Redundant server", enter IP address of the server to be used for data replication between the main and redundant vGate Servers in the replication network. After this, click "Next".

    A dialog box for setting up the main server parameters appears.



11. Enter the IP address of the main vGate Server in the replication network to be used for replication and click "Next".

    A dialog box appears saying that everything is ready for the installation.
12. Click "Install".

    The process of file copying to the hard disk and configuring the installed components will be started. The progress will be displayed in the installation program dialog in the form of a progress bar.

    After successful installation and configuration of components, a dialog box informing you about successful completion of the installation will appear.
13. Click "Finish".

Note. In some cases, a requirement to restart the computer will appear. To restart, click the "Yes" button in the message box.

Details on configuring the replication between the main and redundant servers can be found on p.**51**.

vGate Server installation on VM

Attention! Installation of the vGate Server on VM is allowed, but we do not recommend locating it on the server protected by the vGate.

In case you do not have a free physical server, the vGate Servers (both the main and redundant ones) can be deployed on a VM.

Prior to installing the main or the redundant vGate Server on virtual machine, prepare an ESXi server that meets the following requirements:

- at least two physical network adapters are available;
- sufficient RAM and disk space for running one virtual machine controlled by Windows 10 or Windows Server 2012 R2/2016/2019/2022.

After this, on the ESXi server, create a virtual machine with one of the following OS:

- Windows Server 2012 R2 6.3.9600 x64;
- Windows Server 2016 1607 x64 + Update 4103720;
- Windows Server 2019 1809, 2109 x64;
- Windows Server 2022.

The procedure of installing the main or the redundant vGate Server on VM is exactly the same as the installation on a standalone computer (see p.**15** and p.**25**).

Note. If the vGate Server is installed on a virtual machine, the "Trusted boot loading of virtual machines" security policy is supported for this VM (see p.**95**).

Preparation of the virtualization server for vGate installation with replication

Using a router:

1. Create a virtual switch (vSwitch1) on the ESXi server and bind it to the physical network adapter (vmnic0) connected to the physical network that is used as a network of protected servers.
2. Create a group of VM ports (VMNetwork1) on the virtual switch (vSwitch1).
3. Create a virtual switch (vSwitch2) on the ESXi server and bind it to the physical network adapter (vmnic1) connected to the physical network that is used as a replication network.
4. Create a group of VM ports (VMNetwork2) on the virtual switch (vSwitch2).
5. Create two virtual machines (VM1 and VM2) on the ESXi server and add two previously created port groups (VMNetwork1 and VMNetwork2) to each of them.
6. Install guest OS from the list of operating systems supported by the vGate Server on both virtual machines.
7. In the guest operating systems of these virtual machines, configure network adapters and install the vGate Server with replication (see p.**25**).

In case of traffic routing using the vGate Server:

1. Create a virtual switch (vSwitch1) on the ESXi server and bind it to the physical network adapter (vmnic0) connected to the physical network that is used as infrastructure administration network.
2. Create a group of VM ports (VMNetwork1) on the virtual switch (vSwitch1).
3. Create a virtual switch (vSwitch2) on the ESXi server and bind it to the physical network adapter (vmnic1) connected to the physical network that is used as a replication network.
4. Create a group of VM ports (VMNetwork2) on the virtual switch (vSwitch2).
5. Create a virtual switch (vSwitch3) on the ESXi server and bind it to the physical network adapter (vmnic2) connected to the physical network that is used as an external perimeter administration network (where security administrator and virtual infrastructure administrator workstations are located).
6. Create a group of VM ports (VMNetwork3) on the virtual switch (vSwitch3).
7. Create two virtual machines (VM1 and VM2) and add three previously created port groups (VMNetwork1, VMNetwork2 and VMNetwork3) to each of them.
8. Install guest OS from the list of operating systems supported by the vGate Server on both virtual machines.
9. In the guest operating systems of these virtual machines, configure network adapters and install the vGate Server with replication (see p.**25**).

vGate Client installation on Windows OS

To install the vGate Client:

1. Log on using the computer administrator credentials.
2. Insert the setup disk into the drive. If the setup program does not start automatically, run the autorun.exe file from the \autorun folder.

   A dialog box listing the setup disk software appears.
3. Click the "vGate Client" link.

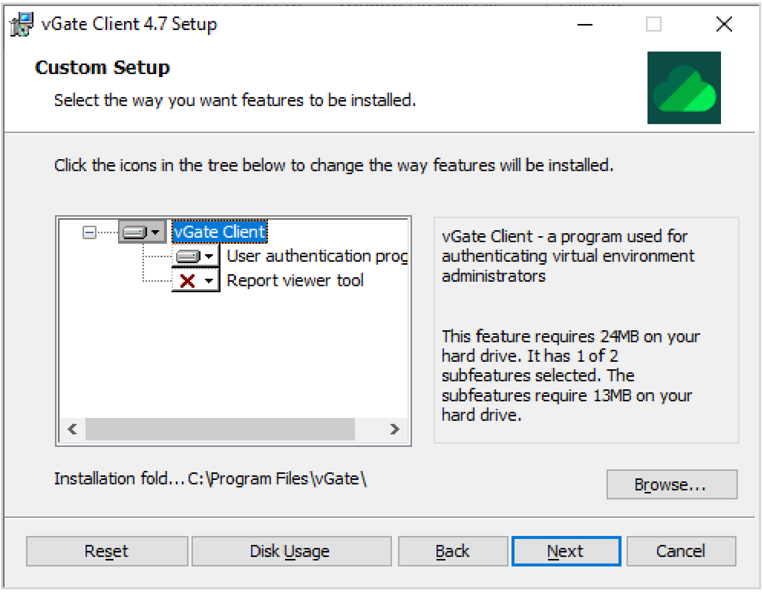
   Tip. To install this product, you can also run the \vGate\vGateClient.msi file from the setup disk.

   The setup program will complete certain preparations, after which the welcome dialog box will appear.
4. Click "Next".

   The license agreement dialog box appears.
5. Read the entire license agreement, select the "I accept the terms in the License Agreement" check box and click "Next".

   Tip. In order to obtain a paper copy of the license agreement, click "Print".

   A dialog box to select components to be installed appears.

6. Select components to be installed and click "Next".

   Note. It is possible to control several vGate Servers from one virtual infrastructure administrator or security administrator workstation (see the "User authentication" section in the document [4]).

   A dialog box appears saying that everything is ready for the installation.
7. Click "Install".

   The process of file copying to the hard disk and configuring the installed components will be started. The progress will be displayed in the installation program dialog box in the form of a progress bar.

   After successful installation and configuration of components, a dialog box informing you about successful completion of the installation will appear.
8. Click "Finish".

   Note. Once the vGate Client is installed, we recommend restarting the computer.

vGate Client installation on Linux OS

vGate Client installation on Linux OS is performed with the help of the RPM Package Manager.

Attention! vGate Client installation should be started on behalf of the computer administrator. Also, you must allow SELinux to run the RPM package scripts using SELinux rules or enable SELinux in permissive mode, or disable it for the period of packet installation.

To install the vGate Client, run the command:

```
rpm -iv /tmp/vgclient_5.10.150.std.def.alt0.c9f.2-4.7.XXXXX.0-0.x86_64.rpm
```

where 4.7.XXXXX.0 is the vGate software version.

While installing the RPM package, compliance of kernel and distribution versions with the versions for which the package is built will be ensured.

If the RPM package installation ended with an error, you must remove the vGate Client from the system (see p.**50**).

Note. A configuration file is installed with minimum parameters. For example, it does not contain connections to vGate Servers, which should be added by the user with the help of the authentication program (see the "vGate Client operation in Linux OS" section in the document [4]).

Monitoring server installation and setup

To use the security monitoring function (see p.**135**), you need to deploy the monitoring server.

To deploy the monitoring server:

1. In VMware vCenter, import the virtual machine from the Monitoring.ovf template that is located on the vGate setup disk in the \monitoring folder.
2. Start the VM and enter the following credentials:

   Monitoring login: administrator

   Password: qwe
3. Run the command:

   ```
   sudo vgate-config
   ```

   The list of available commands appears:

   ```
   administrator@monitoring:~$ sudo vgate-config
   [sudo] password for administrator:
   Usage: vgate-config [OPTIONS] COMMAND [ARGS]...

   Options:
     --help  Show this message and exit.

   Commands:
     users         List users.
     users delete  Delete user.
     users create  Create new user.
     network       Configure network interface.
     vcenter       Configure vCenter connection.
   ```
4. To configure network interface, run the command:

   ```
   sudo vgate-config network
   ```
5. Specify the IP address of the monitoring server, subnet mask, network gateway and DNS server.

   ```
   administrator@monitoring:~$ sudo vgate-config network
   Configuring network interface: eth0
   IP Address: 192.168.2.150
   Netmask: 255.255.255.0
   Default gateway: 192.168.2.10
   DNS Nameservers []: 192.168.2.2

   Network interface has been configured successfully.
   ```

Tip. You can skip this step by pressing Enter.

6. If the virtual infrastructure contains the vCenter server, configure the monitoring server connection to it.

   To do this, run the command:

   ```
   sudo vgate-config vcenter create
   ```

   ```
   administrator@monitoring:~$ sudo vgate-config vcenter create
   vCenter host: 192.168.1.70
   Username: administrator@virt.loc
   Password:

   vCenter has been configured successfully.
   ```

   The monitoring server can be connected to several vCenter servers.

   Note.
   - You can see the list of connected servers by running the "sudo vgate-config vcenter" command.
   - We do not recommend adding more than three vCenter servers.

   Attention! For VMware vCenter Server for Windows, you must create a rule in the vGate web console that allows access from the IP address of the monitoring server to the vCenter server. For correct storing of the audit messages you must specify the virtual infrastructure administrator credentials via TCP port 443 (see p.**111**). Also, make sure that port 443 is not blocked by the vCenter Firewall.

7. Create the user account for connection to the monitoring server.

   To do this, run the command and specify the user name and password:

   ```
   sudo vgate-config users create
   ```

After configuring the parameters, connect to the monitoring server in the vGate web console (see p.**70**) using the account created in step 7.

Analysis server installation and setup

The analysis server provides the deep packet inspection function (see p.**149**).

To deploy the analysis server:

1. In VMware vCenter, import the virtual machine from the OVF template that is located on the vGate setup disk in the \dpi_template\dpi.ova folder.
2. Start the VM and enter the following credentials:

   Login: dpi

   Password: `123qwe
3. To configure the IP address of the network adapter for connection to the vGate Server, modify the ifcfg-ens33 file by running the command:

   ```
   sudo nano /etc/sysconfig/network-scripts/ifcfg-ens33
   ```
4. To configure the IP address of the network adapter for VM traffic analysis, modify the ifcfg-ens36 and ifcfg-ens37 files.

   Note. The network adapter for traffic analysis must be connected to the same virtual switch port group, to which controlled virtual machines are connected. The Promiscuous mode must be enabled for this port group.

Chapter 2
Update to vGate 4.7 from vGate 4.5 and 4.6

Update plan

We recommend the following procedure for updating the vGate components:

№	Installation step	Specific features	Description
1	**Configuration backup**		See p.**47**
2	**Export of the vGate configuration**	Export of vGate 4.5 and 4.6 configuration is performed in the vGate web console	See p.**61**
3	**Uninstallation of vGate 4.5 and 4.6**	On the "Protected servers" page of the web console, vGate Agents are removed from all protected servers	See p.**85**
		The vGate Service Pack software (if available) is uninstalled on computers with the installed vGate Server	
		The vGate Server, vGate Client, PostrgreSQL 12.11 and monitoring server (if available) software is removed	See p.**49**
4	**Installation of vGate 4.7**	The vGate Server, vGate Client and vGate Agents are installed. If using the security monitoring function and DPI function, you must also install and configure the monitoring server and the analysis server	See p.**11**
5	**Import of the vGate configuration**	In the web console, vGate configuration from the step 2 is imported	See p.**61**

Note. If hot standby was used in the management console, once the update is completed, configure this function in the vGate web console (see p.**62**).

Attention! The vGate for Skala-R 4.6 configuration cannot be imported to vGate 4.7.

Configuration backup

Before updating to the new version of vGate, you need to perform the vGate configuration database backup with the help of db-util.exe utility. The utility is located in the folder where the vGate Server component has been installed.

To create a backup copy of the vGate configuration:

1. On the main vGate Server, create a folder where configuration copy will be stored.
2. Open the command prompt and run the following command:

   ```
   db-util.exe -b c:\Backup
   ```

   where:

   - db-util.exe — path to the utility exe file;
   - c:\Backup — path to the folder created for storing backup configuration.
3. Make sure that this folder includes the configuration copy.

Restoring the vGate Server

If the vGate Server update failed, to restore the vGate Server to the previously installed version perform the following steps.

To restore the vGate Server:

1. Uninstall the main vGate Server (see p.**50**).
2. Remove PostgreSQL from the main vGate Server. Once PostgreSQL is uninstalled, remove the residual vGate setup folders and PostgreSQL software.
3. Install the vGate Server with the version that was previously installed.
4. Perform the vGate configuration recovery from the backup copy using the db_util.exe utility (see below).

Restoring a configuration backup

The db_util.exe utitlity is used to restore the vGate configuration from the backup copy.

To restore a configuration backup:

1. Stop all vGate services (otherwise backup will not be proceeded).

   Note. Additionally, disable the hot standby function (see p.62), if this function is used.

2. Open the command prompt and run the following command:

   ```
   db-util.exe -r c:\Backup
   ```

   where:

   - db-util.exe — path to the utility exe file;
   - c:\Backup — path to the folder created for storing backup configuration.

   Tip. If necessary, you can use the following parameters:
   - -f [--force] – configuration backup command -r [--restore] will not request the confirmation of operation;
   - -v [--verbose] – replication and backup operations will be detailed.

   Example: db-util.exe -v -r c:\Backup -f.

3. Remove the following files from the vGate\Kerberos setup folder:

   - krb5kt;
   - .k5.VGATE, where VGATE — name of the vGate account registry.

4. Start vGate services that were stopped. If necessary, enable the hot standby function (see p.62).

   Note. If integration with Active Directory was used while configuring vGate, once the backup is finished, add the domain where the vGate Server is located to the list of trusted domains.

   Note. Once the backup is finished, replication may be disabled due to WAL journal overfilling. Run the db-util.exe --recreate-replica command to restart the replication (see p.187).

Chapter 3
Reinstalling and uninstalling vGate

Setup programs for the vGate Server, vGate Client and vGate Agent for vCenter allow you to modify the setup parameters and the list of installed components, as well as to remove installed software from the computer.

Before performing these steps, close the management console and vGate Client.

To start the setup program:

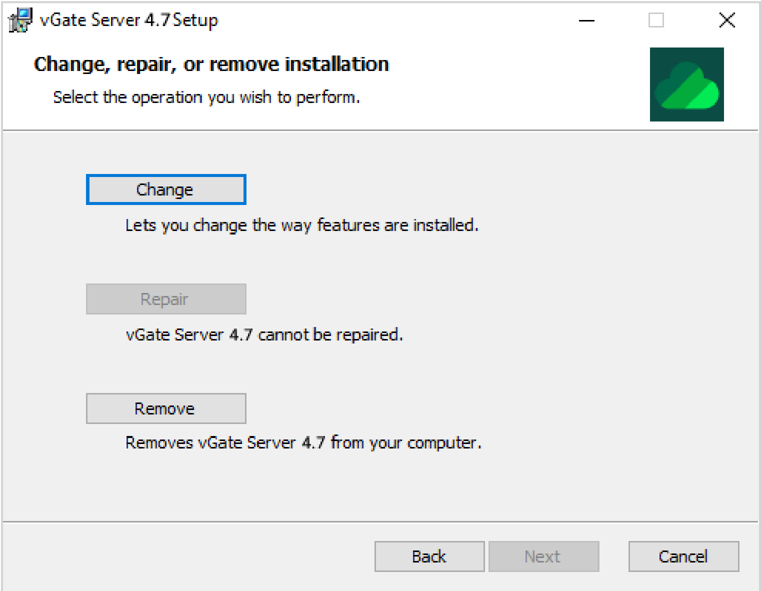
1. Run the corresponding setup program.

   Tip. You can do this using two methods:
   - Run the vGateServer.msi, vGateClient.msi, vGateVpxAgent.msi files from the \vGate\ folder on the setup disk.
   - In Control Panel, open the "Programs and features" component. In the list of installed programs, select the "vGate Server 4.7", "vGate Authentication Client 4.7" or "vGate Agent for VMware vCenter 4.7" and click the "Change" button.

   The program will complete certain preparations, after which the welcome dialog box will appear.

2. Click "Next".

   The "Change, repair or remove installation" dialog box appears.



Modification of installer parameters

In this operation mode, the installation program allows you to modify the list of installed components:

- add or remove the "Replication configuration" component on the vGate Server;
- install or remove the "Control of network connections" component on the computer, where the vGate Agent for vCenter is installed;
- install or remove the "Report viewer tool" component on the computer, where the vGate Server is installed.

To modify installation parameters:

1. Click "Change".
2. Modify the parameters following the installer instructions.

Replication components reinstallation

To reinstall replication components:

1. Uninstall the redundant vGate Server. To do this, use the "vGate Server" component installer (see p.**50**) or the "Apps and features" tool of the Windows OS. Once the installation procedure is finished, restart the computer.
2. Uninstall the "Replication configuration" component on the main vGate Server. To do this, use the "vGate Server" component installer (see p.**50**) or the "Apps and features" tool of the Windows OS. Once the installation procedure is finished, restart the computer.
3. Install the "Replication configuration" components on the main vGate Server, and then on the redundant vGate Server (see p.**25**).

Removing

Attention!

- Before removing of the vGate Server, you need to remove vGate Agents from all ESXi, Skala-R and KVM servers in the web console (see p.85), as well as the vGate Client and the vGate Service Pack software (if available).
- To remove the vGate Agent from the ESXi server 7.0, power off virtual machines running on this server.

To remove the software:

1. Click "Remove" in the "Change, repair or remove installation" dialog box.

   A dialog box appears saying that everything is ready for the removing.
2. Click "Remove".

   The process of installed components removing will be started. After successful removing, a dialog box informing you about successful completion of the operation will appear.
3. Click "Finish".

vGate Agents 2.4 and later deployed on ESXi servers can be deleted manually.

To remove vGate Agents from ESXi servers manually:

1. On the ESXi server, open the service console and execute the command for displaying the vGate Agent version:

   ```
   esxcli software vib list | grep sc-vgate-agent
   ```
2. Execute the command for removing agents:

   ```
   esxcli software vib remove -n sc-vgate-agent
   ```

   or

   ```
   esxcli software vib remove --vibname=sc-vgate-agent
   ```

Removing vGate Client on Linux

On Linux OS, the vGate Client removal is performed using the RPM Packet Manager.

Attention! The vGateClient removal should be started on behalf of the computer administrator. Also, you must allow SELinux to run the RPM package scripts using SELinux rules or enable SELinux in permissive mode, or disable it for the period of packet removal.

To remove the vGate Client, run the command:

```
rpm -ev vgclient_5.10.std.def.alt0.M80C.1-4.7.10893.0-0.x86_64.rpm
```

While removing the software, binary files and configuration files are removed. Log files and the vGate authentication service (aupa.exe) configuration file will not be removed.

To view details on the installed software, execute the command:

```
rpm -qa vgclient*
```

Chapter 4
Replication

The replication mechanism is used to ensure fault tolerance of the main server. It requires putting into operation an additional (redundant) vGate Server.

The vGate Server replication mechanism is available in vGate Enterprise and Enterprise Plus only (see the "Functionality" section in the document [1]).

Putting the redundant vGate Server into operation

Plan

We recommend the following procedure for putting the redundant vGate Server into operation:

№	Step	Specific features	Description
1.	**Primary setup**		See below
2.	**Installation of the redundant vGate Server and management console**	It is performed on the redundant server	See p.32 or p.40 (depending on the selected traffic routing method)
3.	**Configuration of vCenter traffic filtering**	It is performed in the web console or with the help of the drvmgr utility	See p.52

Attention! Before installing the redundant vGate Server, the vGate demo license or the vGate Enterprise/Enterprise Plus license should be registered in the vGate R2 web console.

Primary setup

Attention! If you intend to use configuration with the redundant vGate Server, a local network should include a DNS server. We recommend locating it in the external network.

Before putting the redundant vGate Server into operation:

1. Configure network connections of the main and redundant servers as described on p.26 (using a third-party router) or on p.34 (without using a standalone router).
2. Install the "Replication configuration" component on the main server. Install the redundant vGate Server software on the redundant server. The installation procedure is described on p.32 (using a router) or on p.40 (without using a standalone router).
3. In the DNS settings, configure the CNAME record indicating the main server FQDN.
4. When installing vGate Clients on user workstations and computers, specify the full domain name (FQDN) of the CNAME record as the vGate Server. The vGate Client installation procedure is described on p.44.

As an example, in this chapter, we will use servers with the following settings.

Main server

Adapter	Subnet	Local network settings
Adapter 1	Infrastructure administration network	• IP address that is used by ESXi, vCenter and Skala-R servers for configuration and audit: **192.168.1.2** • Additional IP address that is used in case of the main server failure and its replacement by the redundant server: **192.168.1.12**
Adapter 2	Network of the external administration perimeter	• IP address from the address range of the external network, used for connection to virtual infrastructure administrator and security administrator workstations: **192.168.2.3**
Adapter 3	Replication network	• IP adress from the address range of the replication network to be used for replication between the main and redundant vGate Servers: **192.168.3.2**

Redundant server

Adapter	Subnet	Local network settings
Adapter 1	Infrastructure administration network	• IP address that is used by ESXi, vCenter and Skala-R servers for configuration and audit: **192.168.1.22**
Adapter 2	Network of the external administration perimeter	• IP address that is used for connection with virtual infrastructure administrator and security administrator workstations: **192.168.2.4**
Adapter 3	Replication network	• IP address from the address range of the replication network, used for connection to the main vGate Server: **192.168.3.22**

In the example, traffic routing between the external perimeter of the administration network and protected servers network is performed by the vGate Server. If a router is used, fault tolerance is ensured in the same way.

Configuring rules for vCenter traffic filtering

If while installing the vGate Agent for vCenter, the "Control of network connections" component was selected, access to vCenter will be allowed only from the main IP address of the vGate Server protected perimeter. For correct operation of the replication mechanism for the vGate Server, where two IP addresses of the protected perimeter are used, add access rules for the additional IP address of the main vGate Server, as well as for IP address of the protected perimeter of the redundant vGate Server.

These access rules can be configured in the web console or using the drvmgr utility. Details on configuring rules for access to vCenter and on the drvmgr utility format can be found on p.**111** and p.**189**.

Automatic switching to the redundant vGate Server

Replication in vGate includes the option of automatic switching to the redundant vGate Server in case of the main server failure (see p.**62**).

In order to implement this functionality, the vGate Server replication service (fmsvc.exe) runs on the main and redundant servers. This service performs monitoring of the second node of the vGate servers cluster.

The redundant vGate Server attempts to connect to the main vGate Server regularly after the specified interval. Two scenarios resulting in automatic switching from the main server to the redundant server are described below.

No connection between the main and redundant servers

If there is no connection between the main and redundant servers, the following conditions are checked:

1. Connection between the redundant vGate Server and at least one protected server is available (with the installed vGate Agent).
2. After the specified number of unsuccessful attempts to connect to the services (see p.**62**), the situation does not change.

If these conditions are met, control is automatically passed to the redundant vGate Server. The following operations are performed on the former main server:

1. The main IP address (192.168.1.2) is removed from the network adapter settings.
2. The vGate authentication service (aupa.exe) and the vGate proxy service (vcp.exe) is stopped.
3. An anonymous rule is enabled for access to this server over the RDP protocol.

Automatic replication recovery

If connection between servers was restored after changing server roles, automatic replication recovery is available. This option is enabled by default.

Installing the redundant server software on a new server

After role changing you can instal the redundant vGate Server software on a new server.

Note. On the new redundant server, use the IP address of the former redundant server in the replication network. If you need to specify a different IP address, reinstall the replication component on the new main server, specifying the new IP address of the redundant server.

Note. You can get access to the former main vGate Server locally or via the RDP protocol (this function must be enabled in the OS settings).

To install the redundant server software:

1. Remove the vGate software, PostgreSQL database server and their installation folders.
2. Install the vGate software with the "Replication configuration" component (see p.25).

Connection between the main and redundant servers is available

If a connection between the main and redundant servers is available, the following conditions are checked:

1. At least one of the aupa.exe, inchd.exe, julius.exe, krb5kdcd, rhuid.exe, vcp.exe, viena.exe, nssm.exe services is not running on the main server.
2. After the specified number of unsuccessful attempts to connect to the services (see p.62), the situation does not change.

If these conditions are met, role changing is performed. If this operation ends with an error, switching to the redundant vGate server is forced. The operations described above are performed on the former main server.

Monitoring replication

Failover Monitor has the monitoring replication mechanism which manages the messages about changing the replication status.

Message about the replication crash/recovery is saved to the event log of the server, which sent the request, to the vGate log and to the Failover Monitor log file.

The main reasons of the replication failure:

- lag between the redundant and main vGate Servers under heavy load on the database;
- failure of one of the vGate Servers;
- communication failure between the main and redundant servers in the replication network.

Main server replacement in case of failure

If the function of automatic switching to the redundant vGate Server is not configured in the vGate management console, then, in case of the main vGate Server failure, you have to manually switch server roles until the main server is recovered or replaced.

Note. IP addresses of the main and redundant vGate Servers specified in the table (see p.51) are used as examples in the procedures in this section.

Passing control to the redundant vGate Server

1. Power off the main server.
2. Start the vGate web console on behalf of the computer administrator (see p.56).
3. Go to the "Settings" section of the web console, open the "Authorization server" tab and click the "Change server roles" button. In the appeared confirmation dialog box, click "Yes". Server roles will be changed.

   The main server IP address (192.168.1.2) will be assigned to the redundant server, and the redundant server IP address (192.168.1.22) will become an additional one.
4. In the DNS settings, modify the CNAME record settings by configuring the link to the redundant server FQDN.
5. If the traffic routing is performed by vGate Servers, modify the settings of the route to the protected perimeter for all computers in the external network, on which the vGate Client is not installed, taking into account the new external IP address of the vGate Server (192.168.2.4).

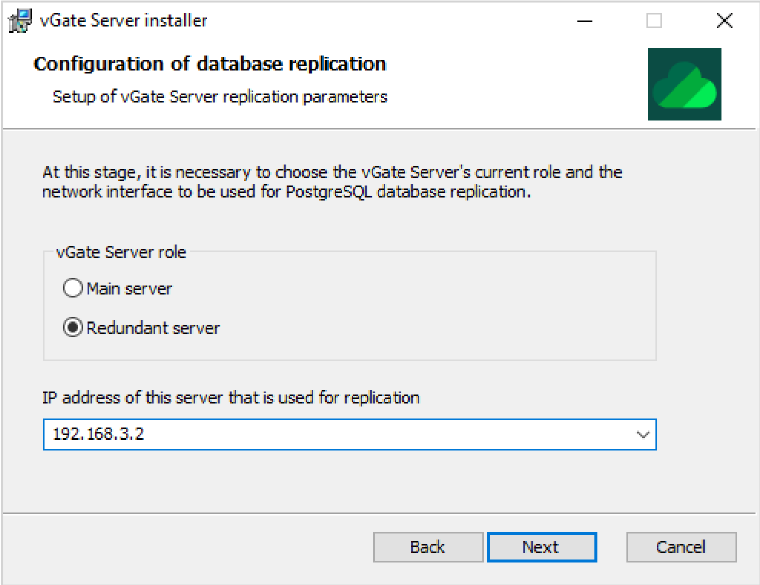
   Note. If the vGate Client is installed on an external computer, the route will be automatically changed, when the following conditions are met:
   - in the vGate configuration, the "Add a route to the secure network on the client" option is enabled;
   - the external computer and vGate Server are located in the same subnet.

Putting a new server into operation

To put a new server into operation:

1. On the new server, configure local network connections according to the redundant server scheme (see p.26 or p.34 depending on the selected method of traffic routing). Specify 192.168.1.12 as IP address in the infrastructure administration network and 192.168.2.3 as IP address of the external perimeter.

2. Install the redundant vGate Server software (see p.**32** or p.**40** depending on the selected traffic routing method). During the step **6** of the installation, specify 192.168.3.22 and 192.168.3.2 as IP addresses of the main and redundant servers in the replication network respectively.



Note. If, instead of putting a new main server into operation, the former main server is recovered after failure, remove the main IP address of the server from the adapter 1 settings (192.168.1.2). Server 1 should have only one IP address of the infrastructure administration network (192.168.1.12). After this, remove the vGate software and PostgreSQL database server software from that server, and install the redundant vGate server.

Changing roles of vGate Servers

In case of the main vGate Server maintenance, you can change the server role for a while.

To change the vGate Servers roles:

1. On the main server, open the "vGate Server" group of parameters in the "Configuration" section and click the "Assign as redundant' link button. In the appearing dialog box, click the "Change role" button.
2. Open the management console on the redundant server (new main server).
3. In DNS settings, modify the CNAME record settings by configuring the link to the new main server.
4. If the traffic routing is performed by vGate Servers, modify the settings of the route to the protected perimeter for all external computers, where the vGate Client is not installed, taking into account the new IP address of the vGate Server in the external perimeter of the administration network (192.168.2.3).

Note. Once the maintenance is finished, perform the reverse procedure of changing roles of vGate servers.

Note. If the vGate Client is installed on an external computer, the route will be automatically changed, when the following conditions are met:
- in the vGate configuration, the "Add route to secure network on client" option is enabled;
- the external computer and vGate Server are located in the same subnet.

vGate Server reinstallation

Redundant vGate Server reinstallation

In case of routine or emergency replacement of the redundant vGate Server, this server should be reinstalled.

Note. On the new redundant server, use the IP address of the former redundant server in the replication network. If you need to specify a different IP address, reinstall the replication component on the new main server, specifying the new IP address of the redundant server.

To reinstall the redundant server:

1. If necessary, remove the vGate software and PostgreSQL database server software from the computer designated to be the redundant vGate Server

Note. Once the PostgreSQL software is removed, delete the installation folder of this software.

2. On the main vGate Server, reinstall the "Replication configuration" component and configure the replication between the main and redundant vGate Servers.
3. On the computer designated to be the redundant vGate Server, install the vGate R2 software (see p.**25**).

Main vGate Server reinstallation

To reinstall the main vGate Server, we recommend performing the same steps as when replacing the main server in case of a failure (see p.**53**).

Chapter 5
Configuring vGate

Web console

You can configure the vGate software with the help of the web console.

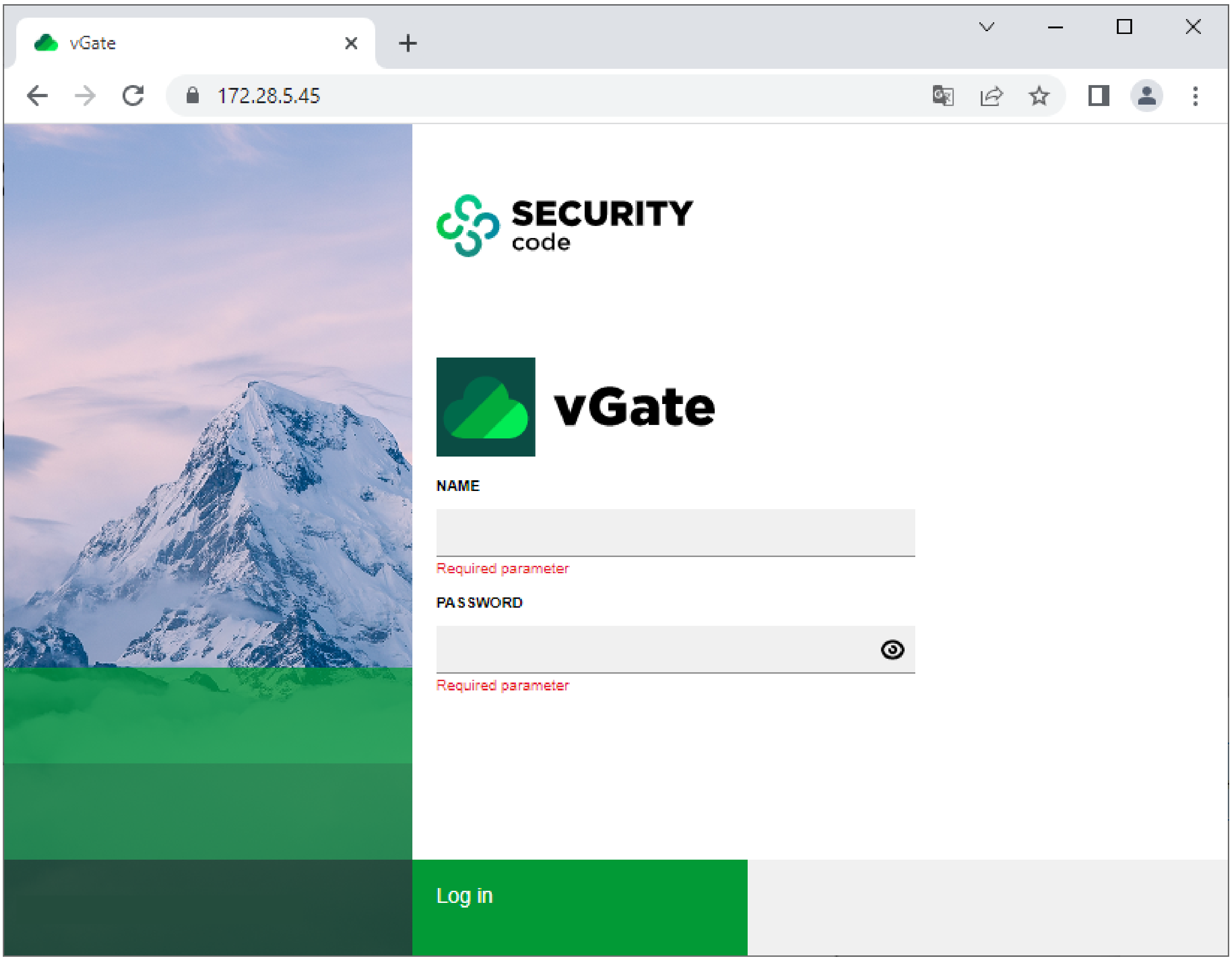
Access to the web console is possible from the administration network using the security administrator credentials (see p.**87**).

To open the web console, in the "Start" menu, click ''Apps | Security Code | vGate management console" or open a web browser and type the following URL:

https://<server-IP>

Where <server-IP> is the vGate server IP address or network name.

The web application welcome page appears.



Specify the security administrator login and password, then click the "Log in" button. The vGate web console appears. If password expired, a dialog box for changing password will appear (see p.**59**).

Attention! When connecting to the web application from the external perimeter of the administration network, in the vGate web console add a rule allowing user access to the vGate server over the TCP protocol and port 443 (see p.107). To change the default port, open the file vGate\Web\dist\lib\site-packages\app\config\app.conf and add the following section:

```
httpd: {
port: <new port number>
}
```

After this, restart the vGate web console service (vgate.webapp).

The main menu of the web console consists of the following sections:

- Firewall (see p.**143**);
- Monitoring (see p.**135**);
- Protected servers (see p.**79**);
- Access rules (see p.**108**);
- Security configuration of servers (see p.**123**);
- Virtual machines (see p.**153**);
- vCenter traffic filtering (see p.**111**);
- vSphere virtual networks (see p.**114**);
- Object groups (see p.**91**);
- vSphere network adapters;
- Storage;
- Security policies (see p.**95**);
- Reports (see p.**161**);
- Event log (see p.**155**);
- User accounts (see p.**87**);
- Policy compliance (see p.**105**);
- Organizations (see p.**134**);
- Container images (see p.**151**);
- Settings (see p.**59**);
- About vGate.

The vGate web console top panel contains:

- vGate mode configuration (see p.**78**);
- Notifications about events;
- vGate theme toggle;
- Links to the vGate documentation;
- Administrator account configuration.

Configuration plan

Configuration plan

1. Register the existing license for using vGate (see p.**73**).
2. If the VMware vSphere virtual infrastructure does not contain the vCenter server and a shared user account is used to connect to protected ESXi servers, specify the parameters of connection to one of the ESXi servers (see p.**64**). After this, add this ESXi server to the list of protected servers (see p.**79**) and install the vGate agent on it (see p.**85**). Repeat these actions for all protected ESXi servers.

   Note. The list of ESXi servers found during the search will contain only the server whose connection parameters are specified in the settings at the moment.

3. If the VMware vSphere virtual infrastructure contains the vCenter server, specify the parameters of connection to it (see p.**64**). Add the vCenter server, all ESXi servers related to it, and Platform Services Controller server (in VMware vSphere 6.7) to the list of protected servers (see p.**79**). After this, all virtual machines related to this vCenter appear in the list of protected virtual machines.
4. If the Skala-R Management server is used in the virtual infrastructure, specify the parameters of connection to it (see p.**64**). After this, add all Skala-R virtualization servers to the list of protected servers (see p.**79**). If a standalone Skala-R server is used, configure a connection to it as to the KVM server (see below).
5. If the virtual infrastructure contains the KVM virtualization server, Proxmox server, OpenNebula platform, Cloud Director server, or embedded Harbor Registry, specify the parameters of connection to them (see p.**64**), and then add them to the list of protected servers (see p.**79**). Install vGate agents on all added servers (see p.**85**).
6. If, apart from virtualization servers, the virtual infrastructure contains other servers and devices requiring management in the virtual infrastructure administration network (for example, a storage system, etc.), they must be also added to the list of protected servers using the "Standalone server" button.
7. Install vGate agents on all added vCenter, ESXi, KVM, Proxmox, OpenNebula, and Skala-R servers (see p.**85**). The vGate agent is not installed on the Skala-R Management server and OpenNebula platform.
8. Create accounts for vGate users. If the vGate server is in the domain, add AD accounts of users, computers, and groups which should be granted access to protected objects (see p.**87**).
9. For each user, configure the required rules for access to the virtual infrastructure management components (see p.**107**).

   Attention! Once users are granted access to protected servers, vGate must be switched from test operation mode to normal operation mode (see p.78).

10. Configure other functions if necessary.

Note. If several vCenter servers linked using the VMware vCenter Linked Mode are in operation in a company, once one of the servers is added to the list of protected objects, all servers related to it will appear in the list of available virtualization servers. If servers are not linked, to protect the perimeter of each vCenter server, a separate vGate server must be deployed and appropriately configured.

Settings

To modify the vGate settings, in the main menu of the web console go to the "Settings" section and open the required tab:

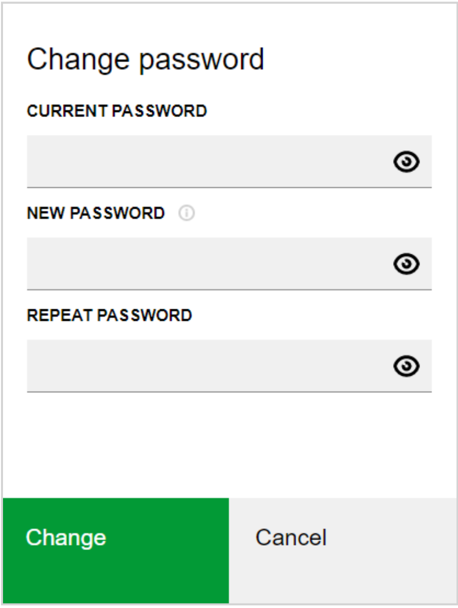
- General (see p.60);
- Authorization server (see p.62);
- Synchronization (see p.63);
- Connection to servers (see p.64);
- Protected subnets (see p.67);
- Trusted domains (see p.67);
- Event log (see p.69);
- Monitoring (see p.70);
- Reports (see p.71);
- Notifications (see p.72);
- License (see p.73);
- Password policies (see p.73);
- Mandatory access control (see p.74);
- Logging (see p.77).

In the web console, you can change the administrator password and select the vGate operation mode.

To change the administrator password:

1. In the upper right corner of the web console, click the security administrator name. In the opened menu, select "Change password".

The following dialog box appears on the screen.



2. Specify the current password, then type the new password twice and click the "Change" button.

The password must be at least 7 characters long. The password must contain at least 4 character classes (a-z, A-Z, numbers, special characters) and at least 2 new characters. Password reuse is not permitted.

To change the operation mode:

At the top of the web console, click the current mode and select the desired vGate mode from the drop-down list (see p.78).

General settings

To modify general settings:

1. Go to the "Settings" section and open the "General" tab.
2. Specify the parameters and click the "Save" button.

Parameter	Description
Session settings	
Session timeout, minutes	Time in minutes, after which an inactive administrator session in the vGate web console will be ended
License	
Warn before license expires, in days	Number of days before the license expiration, when the respective warning will be displayed. By default, the warning appears thirty days before the expiration date
Network and access control settings	
Add a route to the secure network on the client	Select this check box to add a route to the secure network. In order to allow the virtual infrastructure administrator to access the control elements of the virtual infrastructure located within the secure perimeter, routing rules must be configured in a certain way. One option of the routing configuration requires adding a route to the secure subnet for virtual infrastructure administrator workstations from the vGate Server when the vGate authentication service is started. After this, the route is saved in the local routing table of the PC. Details on routing configuration options can be found on p.**12**
Access control by confidentiality levels	Select this check box to enable access control by confidentiality levels. Confidentiality levels and categories are used for mandatory access control (see p.**115**)
Access control by confidentiality categories	Select this check box to enable access control by confidentiality categories. Confidentiality levels and categories are used for mandatory access control (see p.**115**)
Session level control	Select this check box to enable the session level control. By default, the user session in the secure environment is assigned the same confidentiality level as the confidentiality level assigned to the user. The user can perform operations with resources with the same or a lower confidentiality level. Examples can be found in the document [1]). If necessary, the privilege to control (choose) the session level in the vGate client can be granted to all vGate users. In this case, while connecting to the secure environment, the session level is equal to the user confidentiality level, but the user can perform operations only with resources with the same confidentiality level. To access resources with a different confidentiality level, the user can change the session level while working, but the session level cannot be higher than the user confidentiality level. The list of main operations with confidential resources and conditions for their execution, when using the session level control, can be found on p.**177**
Block concurrent sessions of virtual infrastructure administrators	Select this check box to limit the number of parallel virtual infrastructure sessions on different workstations. Once this parameter is enabled, all concurrent virtual infrastructure administrator sessions are ended
Automatic adding of virtual machines to the groups and segments	
Enable automatic adding of virtual machines	To disable automatic adding of virtual machines for all groups, turn off this toggle (see p.**91**). By default, automatic adding is enabled
Add new virtual machines every, minutes	Specify the interval. By default, automatic adding of virtual machines to the groups is performed every 10 minutes
Trusted domains	
Allow all AD users to connect to vGate	To allow all AD users who do not have user accounts in vGate to log in, turn on this toggle (see p.**67**)
Audit of access rule events	
Register events of permitting unsigned traffic	Select this check box to enable registration of events of permitting unsigned traffic by access rules

Parameter	Description
Register events of blocking unsigned traffic	Select this check box to enable registration of events of blocking unsigned traffic by access rules
Deep packet inspection	
Priority in case of rule conflict	Specify the type of firewall rules (blocking or allowing), which will have the priority in case of rule conflict. Rules are processed based on their priority. Details on firewall rules can be found on p.**146**
Audit database backup	
Enable event database backup	To enable saving all audit events to the specified folder on the vGate server when parameter values (see below) are exceeded, turn on this toggle
Event retention period	Audit event retention period after the expiration of which event database backup is performed
Maximum database size, MB	Database size at which event database backup is performed
Event unload path	Path to the directory for saving audit database

3. To export or import the vGate configuration (details on p.**61**), click the "Export configuration" or "Import configuration" button respectively.

Export and import of vGate configuration

Attention! vGate configuration can be exported or imported in the web console if the following conditions are met:
- web console is started using the main security administrator credentials;
- in the parameters of connection to the virtualization server (see p.64), vSphere administrator credentials (ESXi server administrator if using the configuration without vCenter), KVM or Skala-R Management administrator credentials are specified.

In the web console, you can export or import the vGate configuration. The configuration is exported to the XML file and can be used to restore the current vGate server settings.

The configuration file contains information about the following objects:

- general information about the system (vGate version, operation mode);
- configured security policy sets;
- configured confidentiality levels and categories;
- firewall settings;
- created groups and objects that are added to them;
- protected servers, access rules, firewall rules;
- virtual infrastructure objects and security labels assigned to them;
- user accounts, their parameters and security labels assigned to them;
- general vGate settings (matrix of allowed combinations of confidentiality levels and categories, network, access control and licensing settings, mandatory access control, protected subnets, report settings);
- audit settings;
- correlation rules configured for monitoring.

Note. In vGate, control of VMware operations which are related to network and performed bypassing vGate is not supported, therefore, these operations will not be imported when importing the vGate configuration of earlier versions (4.4 and earlier).

To export a configuration:

1. In the main menu, go to the "Settings" section and open the "General" tab.

2. Click the "Export configuration" button.

A panel for exporting the vGate configuration appears.

3. If necessary, turn on the "Protect file with a password" toggle and enter the password twice.

4. Click the "Export" button.

If the "Protect file with a password" parameter is disabled, the vGate configuration will be exported to the XML file. If the parameter is enabled, the configuration will be exported to the *.vgcb file.

To import a configuration:

1. In the main menu, go to the "Settings" section and open the "General" tab.

2. Click the "Import configuration" button.

   A panel for importing a configuration appears.

   Note. If the firewall component (see p.143) is enabled on a server and disabled in the configuration file, after importing this configuration, the firewall component remains enabled on the server.

3. Select the vGate configuration file. If necessary, turn on the "Overwrite data" toggle to replace all information on existing objects by the information on objects with the same name or identifier from the configuration file that is being imported.

   If you import a file that is protected with a password (in *.vgcb format), enter a password.

   Attention!
   - If the "Overwrite data" option is enabled, the "Account is disabled" and "User must change password at next logon" properties will be assigned to the new user accounts not from Active Directory when importing. If the "Overwrite data" option is disabled, these properties will be assigned to all imported accounts not from Active Directory.
   - If the "Overwrite data" option is disabled, imported settings will not be restored on servers from the list of protected servers in the vGate web console.

4. Click the "Send" button.

   vGate configuration is imported in the background. To update the settings correctly, the program operation must be suspended, otherwise some changes may be lost.

   Details on the configuration import result can be found in the event log (see p.69).

vGate Server replication

Replication in vGate includes the option to automatically switch to a redundant vGate server in case of the main server failure. To access the hot standby function, a redundant server must be put into operation (see p.51).

The vGate server replication function is available only in vGate Enterprise and Enterprise Plus (see the "Functionality" section in the document [1]).

Attention!
- For operation of the replication function, the DHCP Client service must be enabled on vGate servers.
- If the "Control of network connections" vGate component is installed on protected vCenter servers, for correct operation of automatic switching to redundant vGate server, add access rules allowing connections from the redundant server IP address to the vCenter server via the TCP protocol and any port (see p.111) .

To configure the hot standby function:

1. In the "Settings" section of the web console, go to the "Authorization server" tab.

   The hot standby parameters appear.

2. Configure the parameters.

Parameter	Description
Switch vGate to a redundant server automatically	Turn on this toggle to enable the option of automatic switching to a redundant vGate server in case of the main server failure
Maximum timeout between connection checks, seconds	Specify the time interval for checking connection between vGate servers. Minimum value is 120 seconds
Number of unsuccessfull connection attempts	Specify the number of unsuccessfull attempts to establish connection between vGate servers after which control is automatically passed to the redundant server

3. Click "Save". Hot standby configuration will be saved.

   Function of automatic switching will operate only if the list of protected servers on the main vGate server contains virtualization servers.

If you need to change the main server role to the redundant, and change the redundant server role to the main (for example, in case of the main server failure), you can change server roles in the vGate web console.

To change roles of vGate servers:

1. In the "Authorization server" tab of the "Settings" section, click the "Change server roles" button. A dialog box for approving changes appears.
2. Click "Yes". Server roles will be changed.

Synchronization of vGate server settings

vGate supports simultaneous operation of several vGate servers. The vGate administrator can synchronize vGate server settings in the web console on the security administrator workstation.

This function is supported in vGate Enterprise and Enterprise Plus only (see the "Functionality" section in the document [1]).

When the settings synchronization wizard is started, the license parameters are checked on vGate servers to which the vGate Client is connected. For correct operation of the wizard, the following conditions must be met:

- activation key for the vGate Enterprise, Enterprise Plus or vGate demo version on all vGate servers;
- total number of physical sockets on virtualization servers must not exceed the value defined in the license. This condition will be checked only if the license identifiers match on vGate servers.

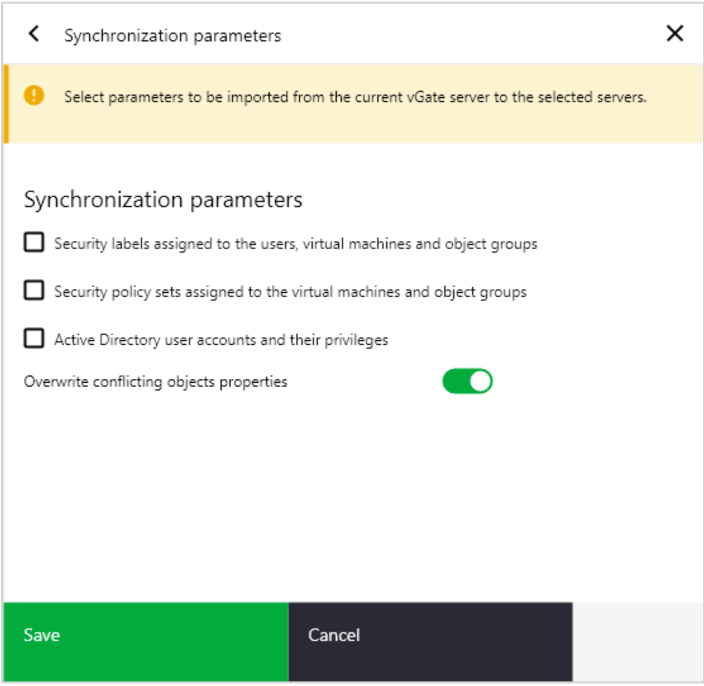
To synchronize server settings:

1. Go to the "General" tab in the "Settings" section.

   The list of vGate servers contains only those servers to which the vGate Client is connected.
2. To add a vGate server, click the "Create" button. A panel for adding a server appears on the right.
3. Specify the vGate server IP address, FQDN or NetBIOS name, as well as the vGate server user name, then click the "Apply" button. The server will appear in the list of vGate servers.

   Attention! We recommend connecting to vGate servers on which the data synchronization will be performed using the main security administrator account. Otherwise, data may be lost while transferring accounts with the "Account operator" privilege. In this case, all Active Directory accounts will be imported, but the settings of their access rights will be lost.
4. Connect to the added vGate server. To do this, select the server in the list and click the "Connect to server" button. A panel for connecting to the server appears on the right.
5. Enter the password of the user specified in step 3, then click "Apply". Once a connection to the vGate server is established, the server status will change to "Connected".
6. Select servers whose settings will be synchronized with the current vGate server settings, then click "Synchronize".

   A panel for configuring the synchronization parameters appears.



7. Specify the settings to be imported to the selected vGate servers, and click "Save".

Parameter	Description
Security labels assigned to the users, virtual machines and object groups	Select this check box to synchronize: • confidentiality categories; • confidentiality levels; • associations of confidentiality categories with object groups, virtual machines and Active Directory users; • associations of confidentiality levels with object groups, virtual machines and Active Directory users
Security policy sets assigned to the virtual machines and object groups	Select this check box to synchronize security policy sets and their associations with the virtual machines and object groups. The following security policies are synchronized in the disabled mode, since they have settings that are specific for each vGate server (for example, IP address): • "Trusted boot loading of virtual machines"; • "Integrity control of virtual machine templates"; • "Configure NTP time synchronization"; • "Configure a centralized location to collect ESXi host core dumps"; • "Control access to VMs through VMsafe CPU/memory APIs"; • "Restrict access to VMSafe Network API"; • "Configure remote logging for ESXi hosts"; • "Ensure proper SNMP configuration"; • "Configure the ESXi host firewall to restrict access to services running on the host"; • "Configure persistent logging for all ESXi host". After synchronization, configure these policies manually
Active Directory user accounts and their privileges	Select this check box to synchronize Active Directory user accounts and their privileges
Overwrite conflicting objects properties	Select this check box to overwrite properties of identical objects while synchronizing. Identical objects are the objects having the same identifiers (for virtual machines, Active Directory users and confidentiality levels) or names (for confidentiality categories and security policy sets)

Attention! If vGate servers that are being synchronized control different virtual infrastructures and the target virtualization server is not added to the list of protected servers, migrating virtual machines can be blocked by vGate. To migrate virtual machines to the server that is not added to the list of protected by vGate, temporarily disable access control by confidentiality levels and categories (see p.60).

8. Settings of vGate servers will be synchronized. Once the synchronization process is completed, a panel containig the operation results appears.
9. To view detailed report about the synchronization process, click the "Download the synchronization log" link button.

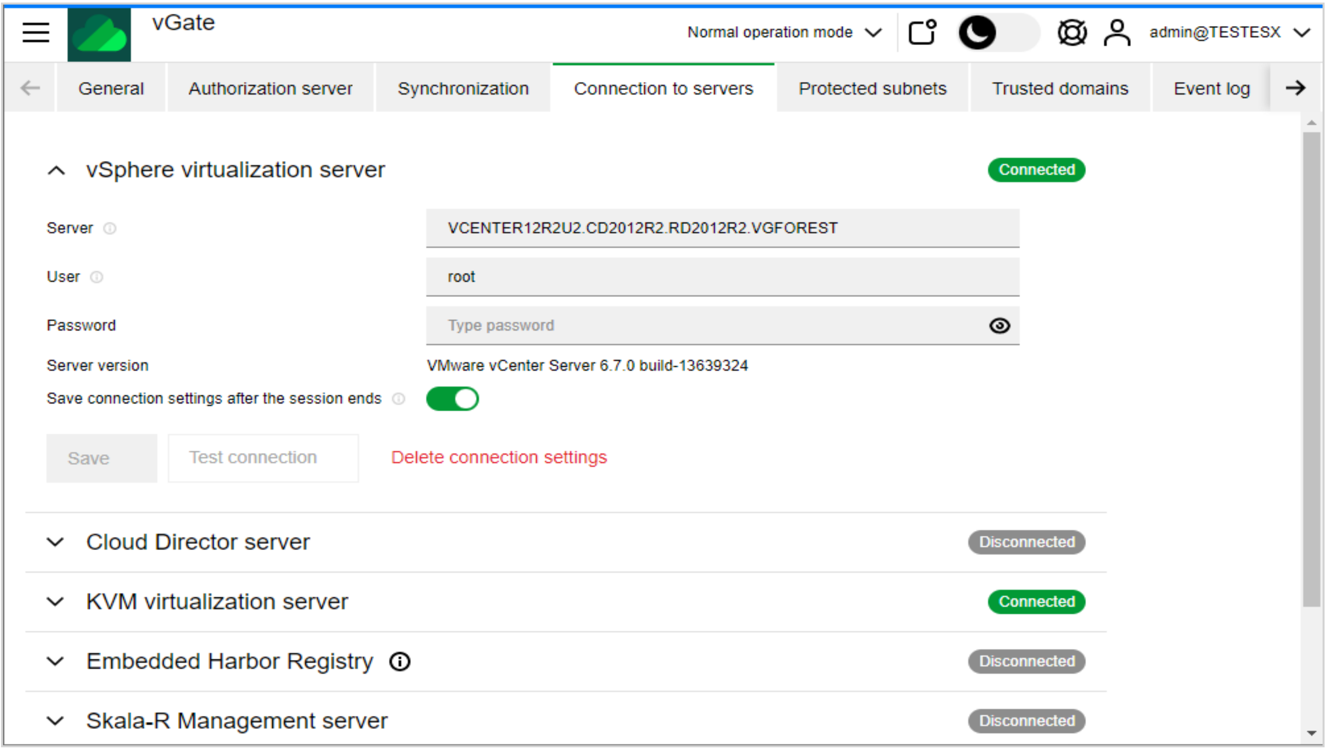
Connection to servers

Depending on the virtual infrastructure configuration, different connection options should be used:

- If the vCenter server is used, specify the parameters of connection to it.
- If there is no vCenter server, while several ESXi servers are used, specify the parameters of connection to one of them. In this case, only connected ESXi server appears in the "Add ESXi servers" list, when registering protected servers. To configure vGate, you need to consistently configure connection to each protected ESXi server and add each server to the list of protected servers (see p.58). In the following, consistent connection to ESXi servers will be required only to recalculate checksums of VM and VM templates that are located on this ESXi server and to enable VM traffic control in the "Firewall" section. This is not required when managing user access privileges.
- If the Skala-R Management server is used, specify the parameters of connection to it. Credentials are requsted only when saving the parameters of connection to the Skala-R Management server or when adding the first Skala-R server to the list of protected servers.
- If KVM servers/standalone Skala-R servers are used in the virtual infrastructure, specify the parameters of connection to one of them.
- If the Proxmox server or OpenNebula platform is used to manage KVM servers, specify the parameters of connection to them.

- If the Cloud Director server is used, specify the parameters of connection to it. In the following, when adding protected Cloud Director servers, credentials will not be requested.
- If the embedded Harbor Registry is used, specify the parameters of connection to it. In the following, when adding the embedded Harbor Registry to the list of protected servers, credentials will not be requested.

To configure connection to servers, in the main menu of the web console, open the "Settings" section and go to the "Connection to servers" tab.



vSphere virtualization server

To configure connection parameters:

1. Open the "vSphere virtualization server" group of parameters, specify the network name or IP address of the ESXi server or vCenter server, as well as the ESXi (vCenter) server administrator name and password.

   Attention! When configuring the connection parameters to the vCenter server, use the vSphere administrator credentials.

2. The "Save connection settings after the session ends" check box is selected by default. Saved parameters of connection to the ESXi server or vCenter will be used later when starting the web console by the current user on this computer. If the check box is not selected, connection parameters is used in the current web console session only, and some operations in the virtual infrastructure are not controlled by vGate.
3. Click the "Test connection" button to test the specified credentials.
4. Click the "Save" button to save the connection parameters.

   Note. To delete the virtualization server connection settings, click the "Delete connection settings" button.

Cloud Director server

The vGate software supports control of the Cloud Director operations. To use this function, configure a connection to the Cloud Director server.

Control of the Cloud Director operations is available only in vGate Enterprise and Enterprise Plus (see the "Functionality" section in the document [1]).

To configure connection parameters:

1. Open the "Cloud Director server" group of parameters, specify the network name or IP address of the Cloud Director server, as well as the server administrator name and password.
2. Click the "Test connection" button to test the specified credentials.
3. Click the "Save" button to save the connection parameters.

Note.
- If a vCenter server is added to the list of protected servers, the Cloud Director server must be connected to it.
- Redundant Cloud Director servers can be registered in vGate by repeating the steps 1-3. In this case, connection to the main Cloud Director server should be configured last.
- If the Cloud Director server connection parameters to which are saved in the vGate configuration is out of service, you need to configure connection to the one of available redundant servers.

Note. To delete the virtualization server connection settings, click the "Delete connection settings" button.

KVM virtualization server

Access to all KVM/standalone Skala-R servers are granted using the root user account. Credentials are requested only when saving the parameters of connection to one of the virtualization servers or when adding the first server to the list of protected servers (see p.79) .

On KVM/Skala-R servers, access through SSH (port 22) must be enabled and allowed.

To configure connection parameters:

1. Open the "KVM virtualization server" group of parameters, specify the KVM/standalone Skala-R server network name or IP address.
2. Specify the name and password of the root user on the server. An account shared for all protected KVM/Skala-R servers is needed for communcation with servers.
3. Click the "Test connection" button to test the specified credentials.
4. Click the "Save" button to save the connection parameters.

Note. To delete the virtualization server connection settings, click the "Delete connection settings" button.

Embedded Harbor Registry

The vGate software supports integrity control of container images stored in the embedded Harbor Registry (see p.151). To get started, configure connection to the embedded Harbor Registry.

Integrity control of embedded Harbor Registry container images is available only in vGate Enterprise Plus (see the "Functionality" section in the document [1]).

To configure connection parameters:

1. Open the "Embedded Harbor Registry" group of parameters, specify the embedded Harbor Registry IP address, as well as the name and password of the user who has access to all projects in the embedded Harbor Registry.

Note. If the vCenter administrator credentials are saved in the "Virtualization server" section, they can be used to connect to the embedded Harbor Registry. To do this, turn on the "Use connection settings to the vCenter server" toggle.

2. Click the "Test connection" to test the specified credentials.
3. Click the "Save" button to save the connection parameters.

Note. To delete the virtualization server connection settings, click the "Delete connection settings" button.

Skala-R Management server

The process of configuring a connection to the Skala-R Management server is given below. If a standalone Skala-R server is used in the infrastructure, connection to it is configured in the "KVM virtualization server" section (see above).

To configure connection parameters:

1. Open the "Skala-R Management server" group of parameters, specify the Skala-R Management server network name or IP address. If Skala-R Management is deployed on several servers (HA-cluster), specify virtual IP address configured during the installation.
2. Specify the Skala-R Management administrator name and password.
3. Click the "Test connection" button to test the specified credentials.
4. Click the "Save" button to save the connection parameters.

Note. To delete the virtualization server connection settings, click the "Delete connection settings" button.

OpenNebula platform/Proxmox server

The process of configuring a connection to the KVM management servers based on OpenNebula and Proxmox. The root user account is needed for communication with servers.

On OpenNebula and Proxmox servers, access through SSH (port 22) must be enabled and allowed.

Note.
- A connection to the OpenNebula server is established through HTTPS (port 443), and to the Proxmox server throgh HTTPS (port 8006). If the servers are configured for connection by other ports and protocols, connection to them will be failed.
- For connection to the OpenNebula management server, a configured proxy server that will route a traffic from HTTP (OpenNebula is used by default) to HTTPS is required.

To configure connection parameters:

1. Open the "OpenNebula platform"/"Proxmox server" group of parameters, specify the server network name or IP address, as well as the root user credentials.
2. Click the "Test connection" button to test the specified credentials.
3. Click the "Save" button to save the connection parameters.

   Note. To delete the virtualization server connection settings, click the "Delete connection settings" button.

Protected subnets

If the network traffic is routed by the vGate server, all new subnets appearing in the network configuration must be added to the list of protected subnets.

To add a protected subnet:

1. In the main menu, go to the "Settings" section and open the "Protected subnets" tab.

   The list of protected subnets appears.

   Note. To modify the list of protected subnets, use the "Edit" and "Delete" buttons.
2. Click the "Add" button. The panel for adding a subnet appears.
3. Specify the subnet IP address and mask, then click the "Save" button.

Trusted domains

By default, you can add accounts to the list of vGate users from the domain where the vGate server is located. Beside this, you can configure adding accounts from other domains of the same forest. To do this, add such domains to the list of trusted domains in the web console.

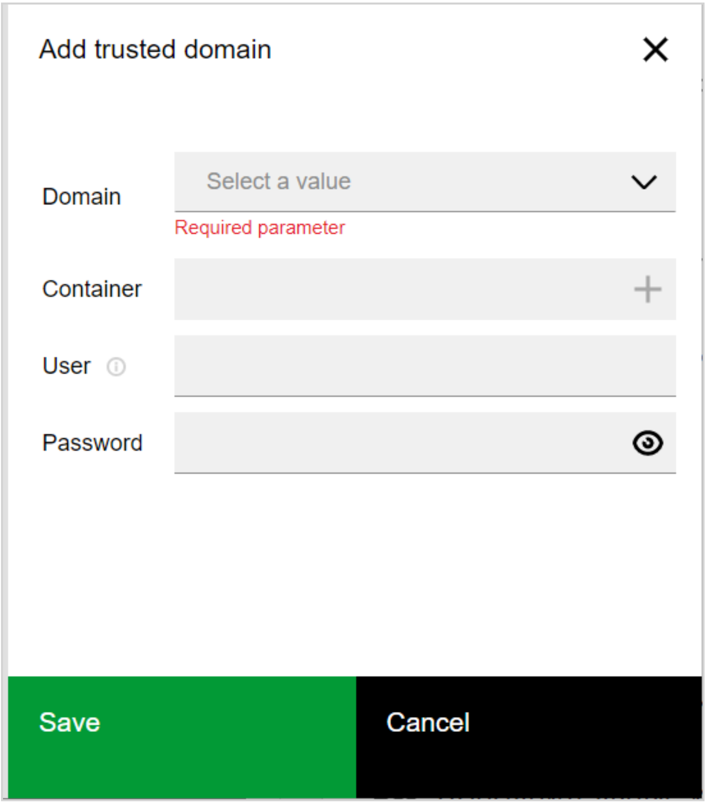
To add a domain:

1. In the main menu, go to the "Settings" section and open the "Trusted domains" tab.

   The list of trusted domains appears.

   Note. To remove a domain from the list of trusted domains, select it in the list and click the "Delete" button.

2. Click the "Add" button. The panel for adding a trusted domain appears.



3. Specify parameters of the trusted domain and click the "Save" button.

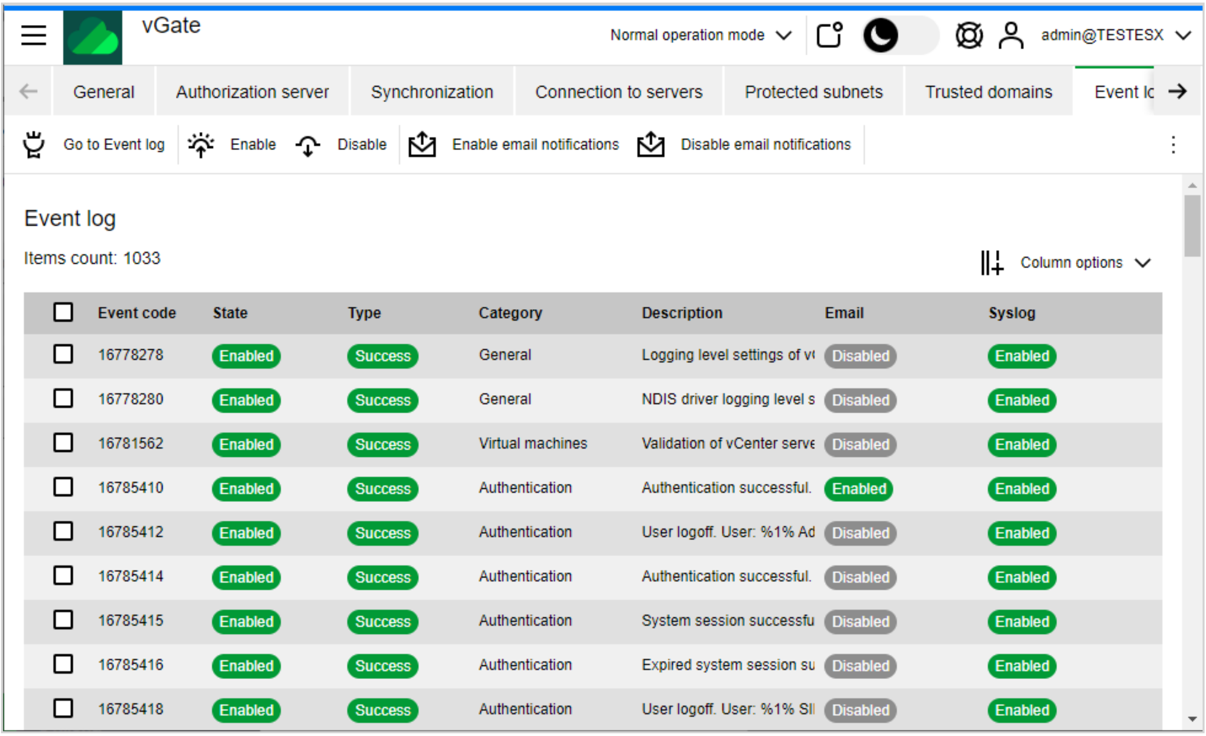
Parameter	Description
Domain	Active Directory domain name
Container	OU name in the Active Directory domain that is designated to store vGate service accounts
User	Name of the user who has administrative privileges in the domain
Password	Password of the user who has administrative privileges in the domain

Event log

vGate allows you to modify settings of receiving audit events.

To configure audit parameters:

1. In the main menu, go to the "Settings" section and open the "Event log" tab.
The list of vGate security events appears.



Note. To configure the table columns, click "Column options" and select the required options.

2. To manage audit settings, use the following buttons.

Button	Description
Go to Event log	Go to the "Event log" section in the vGate web console (see p.**156**)
Enable/ Disable	Enable/Disable the registration of the selected event
Enable email notifications/ Disable email notifications	Enable/Disable sending notifications about this audit event by emali. Configuration of sending email notifications is performed in the "Settings" section of the vGate web console (see p.**72**)
Enable syslog notifications/ Disable syslog notifications	Enable/Disable sending the selected audit event to the Syslog server. Configuration of Syslog parameters is performed in the "Settings" section of the vGate web console (see p.**72**)
Filtering	Filter audit events. It is performed in the same way as filtering in the "Event log" section of the vGate web console (see p.**157**)

Note. If no events are selected on the "Event log" page, then, when clicking "Enable", "Disable", "Enable email notifications", "Disable email notifications", "Enable syslog notifications", "Disable syslog notifications" buttons, actions will be applied to all events.

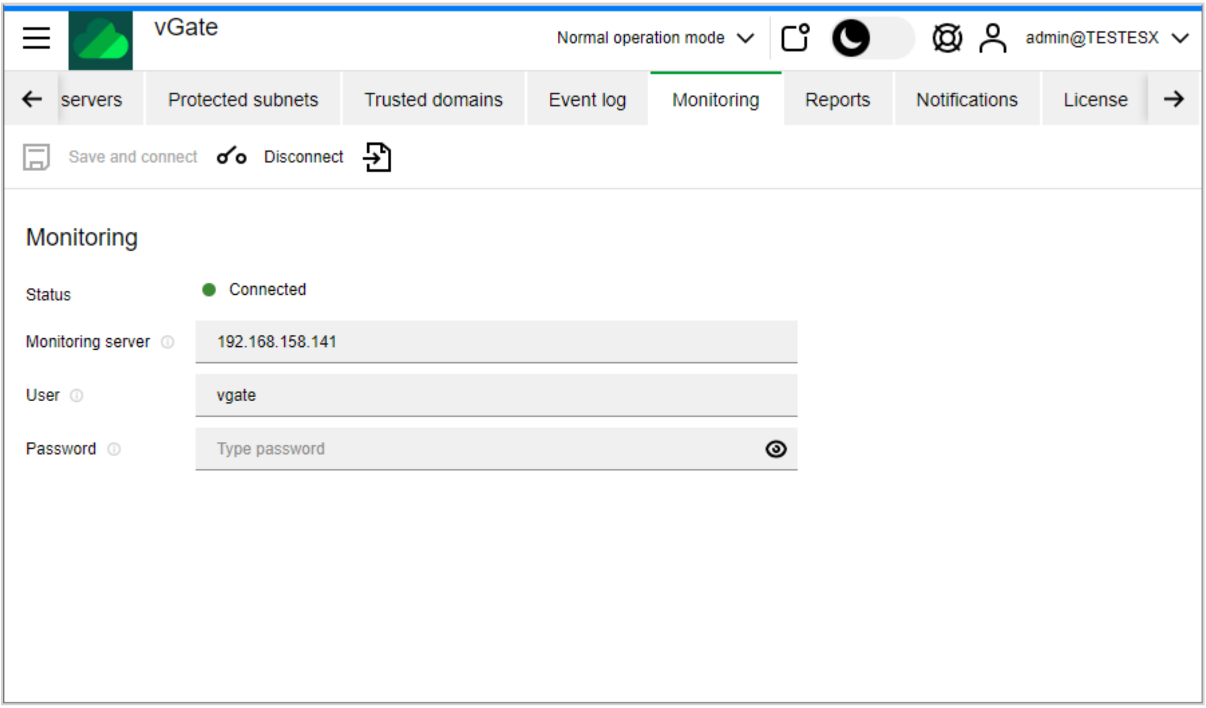
Monitoring

To use the security monitoring function, configure a connection to the monitoring server that is deployed in the network (see p.**45**).

To connect to the monitoring server:

1. In the main menu, go to the "Settings" section and open the "Monitoring" tab.

   The following window appears.



2. Specify parameters of connection to the monitoring server and click "Save and connect".

Parameter	Description
Monitoring server	Specify the monitoring server network name or IP address
User	Name of the user created during the monitoring server installation (see p.**45**)
Password	User password specified during the monitoring server installation (see p.**45**)

   The connection to the monitoring server will be established.

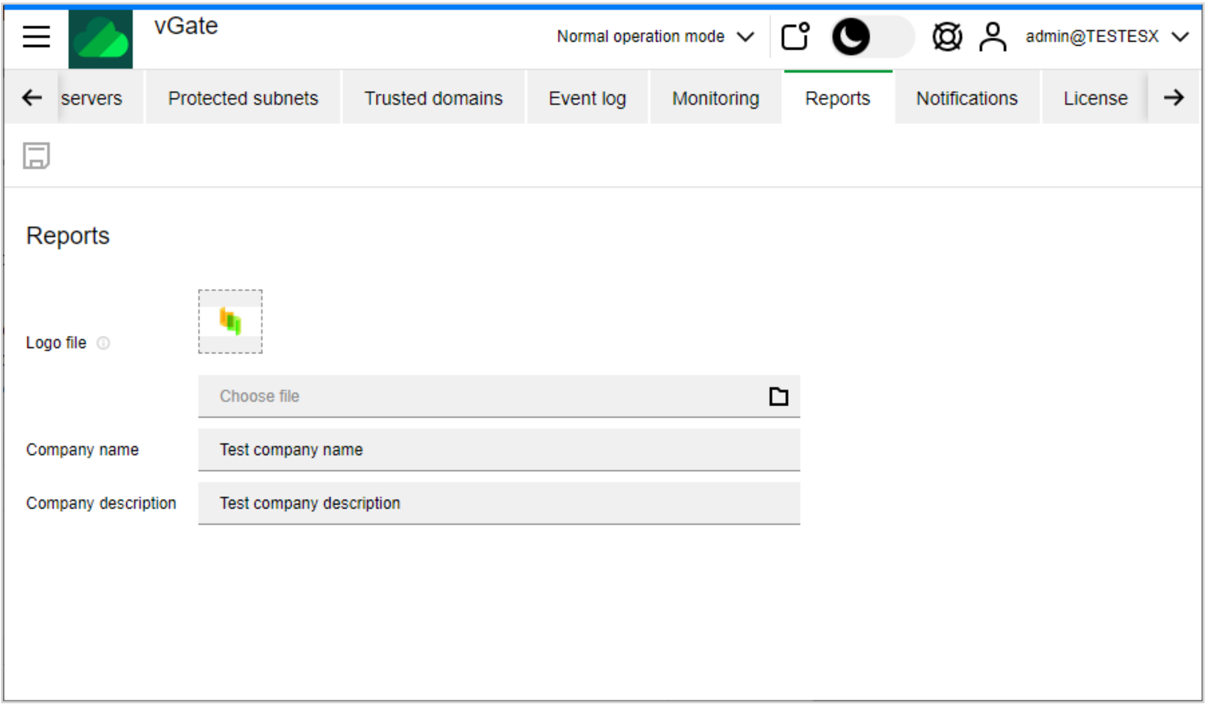
Also, vGate supports import of correlation rule templates that are used for the infrastructure monitoring. To import, click the "Import templates" button and select the needed file. New templates appear in the list (see p.**137**).

Reports

Configuration of displaying vGate reports (see p.161).

To configure parameters for creating reports:

1. In the "Settings" section, open the "Reports" tab.



2. Specify the settings for creating reports.

Parameter	Description
Logo file	Path to the company logo file. Files can be uploaded in the following formats: *.bmp, *.bzlib, *.cairo, *.flif, *.freetype, *.gslib, *.heic, *.img, *.jp2, *.jpeg, *.lcms, *.lqr, *.lzma, *.openexr, *.pangocairo, *.png, *.ps, *.raw, *.rsvg, *.tiff, *.webp, *.xml, *.zlib. The logo is placed on the report cover page
Company name	Name of the company whose virtual infrastructure is protected by vGate. This name will appear on the title page of the reports
Company description	Description of the company whose virtual infrastructure is protected by vGate. This description will appear on the title page of the reports

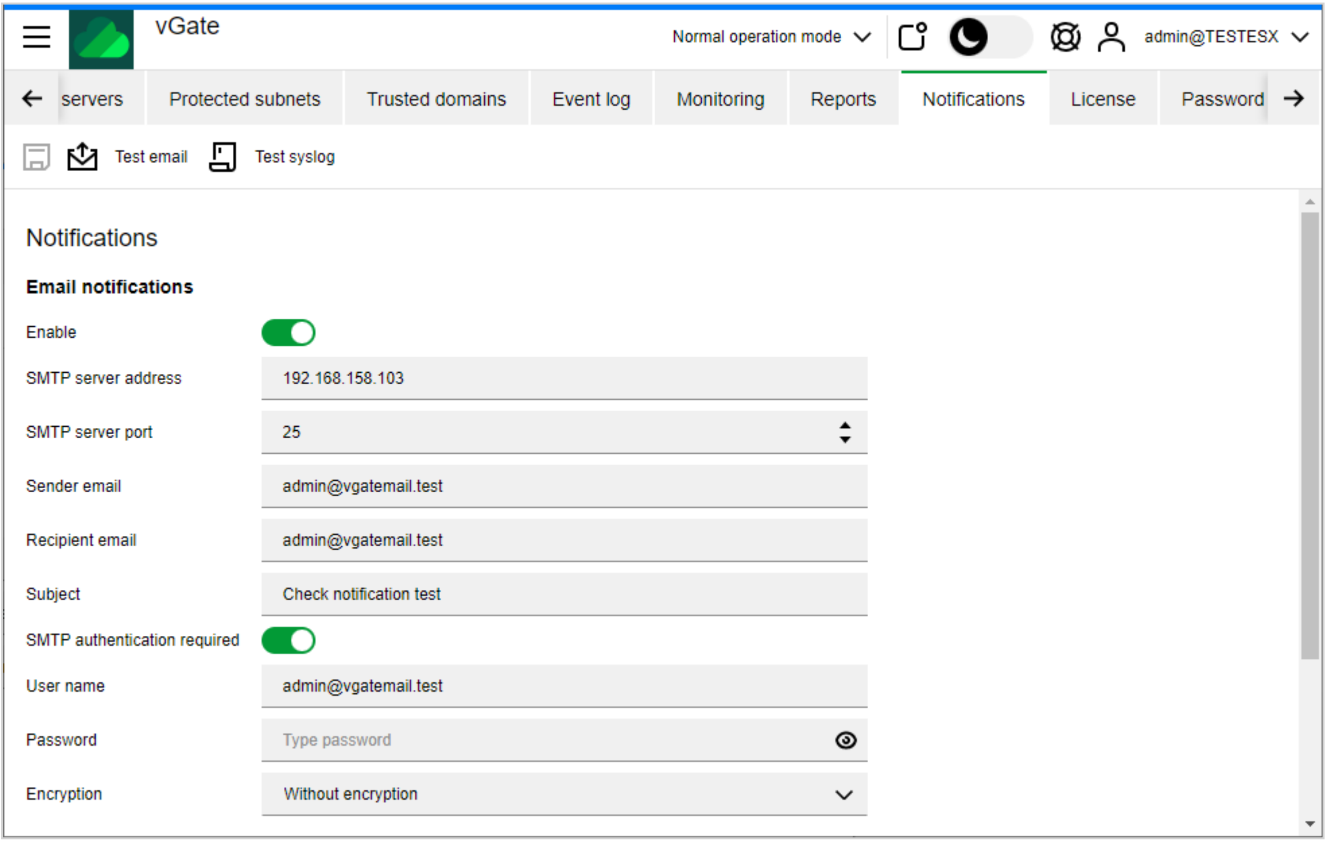
3. Click "Save" to save the settings.

Notifications

vGate allows you to configure sending notifications about audit events via SMTP and Syslog protocols.

To view or edit parameters of notifications, in the main menu go to the "Settings" section and open the "Notifications" tab.

The following window appears.



To configure notification sending over SMTP protocol:

1. In the email notifications area, turn on the "Enable" toggle.
2. Specify the SMTP server address and check the notification sending parameters.

Parameter	Description
SMTP server address	SMTP server IP address or network name
SMTP server port	SMTP server port (default value is 25)
Sender email	Sender address
Recipient email	Recipient address. The ";" character is used as a separator between addresses when specifying several recipients
Subject	The default subject is "Notification from vGate server"

3. If authentication is required for access to the specified SMTP server, turn on the "SMTP authentication required" toggle and specify the user authentication credentials.

Parameter	Description
User name	User name
Password	User password for access to the SMTP server
Encryption	Encryption type used for authentication

Tip. To check notification sending, click the "Test email" button.

4. Click "Save".

To configure notification sending over Syslog protocol:

1. In the syslog notifications area, turn on the "Enable" toggle.
2. Specify parameters for sending notifications and click "Save".

Parameter	Description
Syslog server address	Syslog server IP address or name
Syslog server port	Syslog server port

Tip. To check notification sending, click the "Test syslog" button.

License

To use the vGate software in the demonstration mode, an activation key is required (see the "Rules of license usage" section in the document [1]). The vGate demonstration mode supports all functions available in the Enterprise Plus edition (see the "Functionality" section in the document [1]) without any restrictions. To use full vGate functionality after expiration of the demonstration mode, you need to acquire the license and register the obtained activation key. Details on the license usage can be found in the document [1].

To upload license:

1. In the main menu, go to the "Settings" section and open the "License" tab.

   The information on the current vGate license appears.
2. To upload the new license, click the "Upload license" button, select a file and click "Open".

Password policies

Password policies allow you to ensure that passwords meet complexity requirements.

Note. Password policies do not apply to the Windows domain user accounts.

All passwords configured for virtual infrastructure administrators and security administrators must comply with the policies. When changing user password in the web console or vGate client, new password compliance with the configured password policies is reviewed.

Note. To prevent the usage of easily-guessed passwords, each password is checked against the list of frequently used passwords. A password can be used only if there are no such password in the list. Details on the list of frequently used passwords can be found on p.177.

By default, some parameters of password policies are configured in the system (details below). If necessary, the security administrator can modify these parameters.

To configure password policies:

1. In the main menu, go to the "Settings" section and open the "Password policies" tab.

   A window for configuring password policies appears.

2. Modify parameter values and click "Save".

Maximum password age (days)
Defines the period of time during which the current password is valid. Once the specified time period expires, the current password becomes invalid and must be changed. This parameter can be set to any value between 1 and 365 days
Enforce password history (passwords)
Defines the number of old passwords for each user data on which is stored in the system. When changing a user password, a new password is checked against the list of old passwords of this user. If the new password matches one of the old passwords, this password cannot be used. This parameter can be set to any value between 1 and 15
Minimum password length (characters)
Defines the minimum number of characters in the password. The user cannot set the password whose length is less than this value. This parameter can be set to any value between 1 and 100
Minimum number of character types
Defines the number of character types (uppercase and lowercase letters, digits, etc.) in password. This parameter can be set to any value between 1 and 4. The "1" value means that the password can include any characters, for example, only lowercase letters
Differ from the previous password (characters)
Defines the number of characters by which the new password should differ from the old password during the change. This parameter can be set to any value between 1 and 100
Lock inactive user accounts after (days)
Defines the period of time after the expiration of which inactive accounts are disabled. The security administrator can enable a locked user account (if necessary). This parameter can be set to any value between 1 and 1095 days
Maximum number of failed logon attempts
Defines the number of failed password entry attempts after which the account will be locked. The security administrator can enable the locked user account (if necessary). This parameter can be set to any value between 1 and 255

Note. Once password policies are modified, new policies come into effect on user workstations after a little delay, because the data on user workstations is updated approximately once a minute.

Mandatory access control

Confidentiality categories

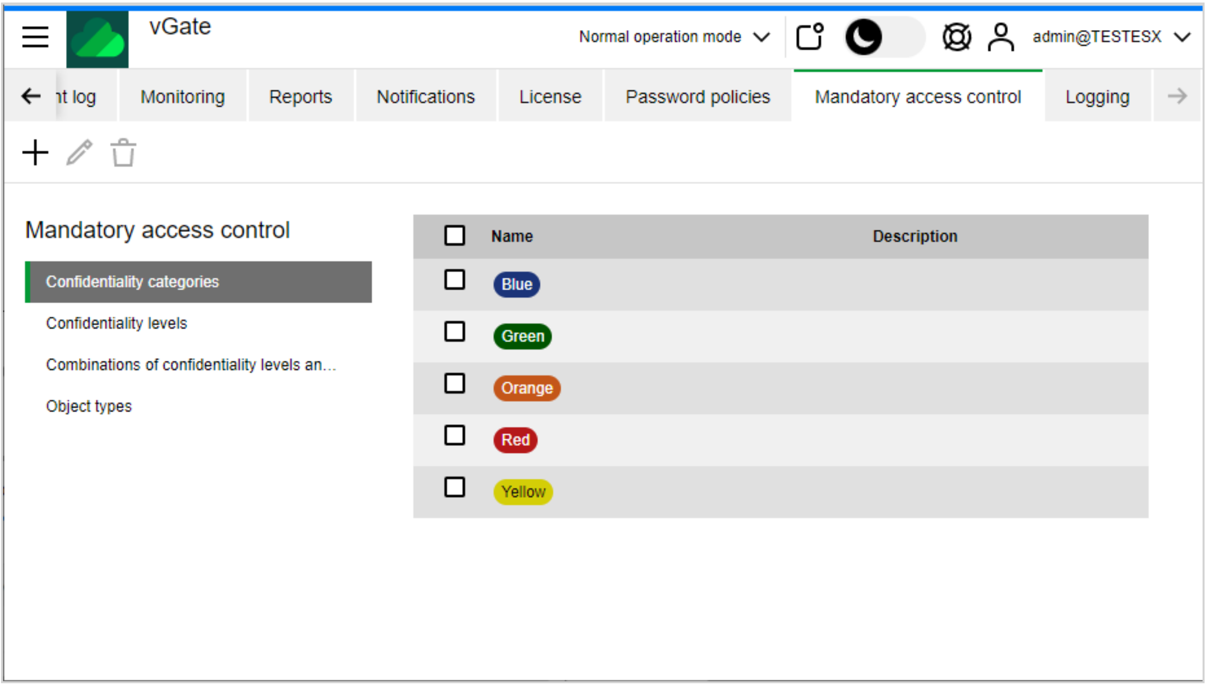
By default, the list of available confidentiality categories is configured in vGate. It includes 5 categories indicated by different colors. The list of categories can be adjusted to user objectives.

To add a confidentiality category:

1. In the main menu, go to the "Settings" section and open the "Mandatory access control" tab.

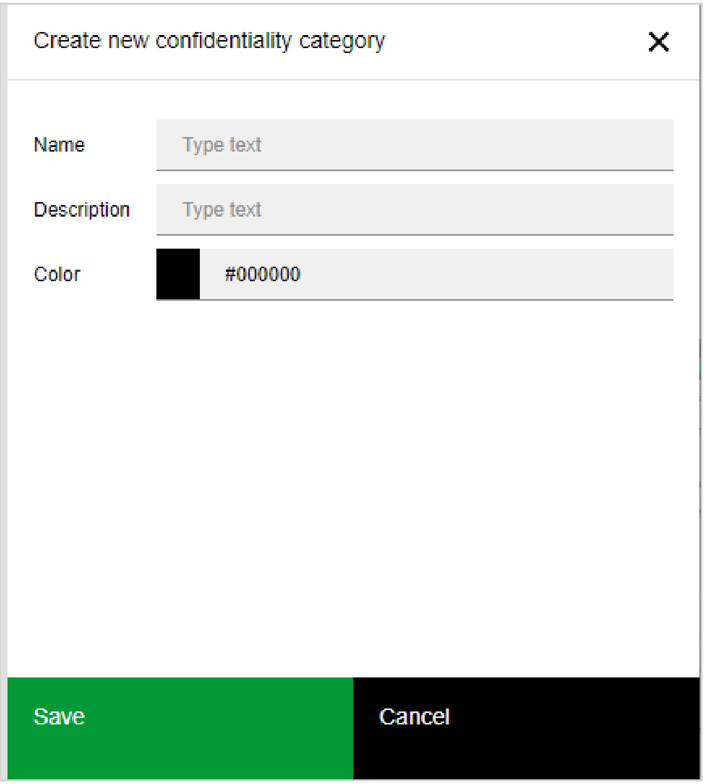
2. Open the "Confidentiality categories" tab.

The table with available confidentiality categories appears.



Note. To modify the list of confidentiality categories, use the "Edit" and "Delete" buttons.

3. Click the "Add" button. A panel for creating a new confidentiality category appears.

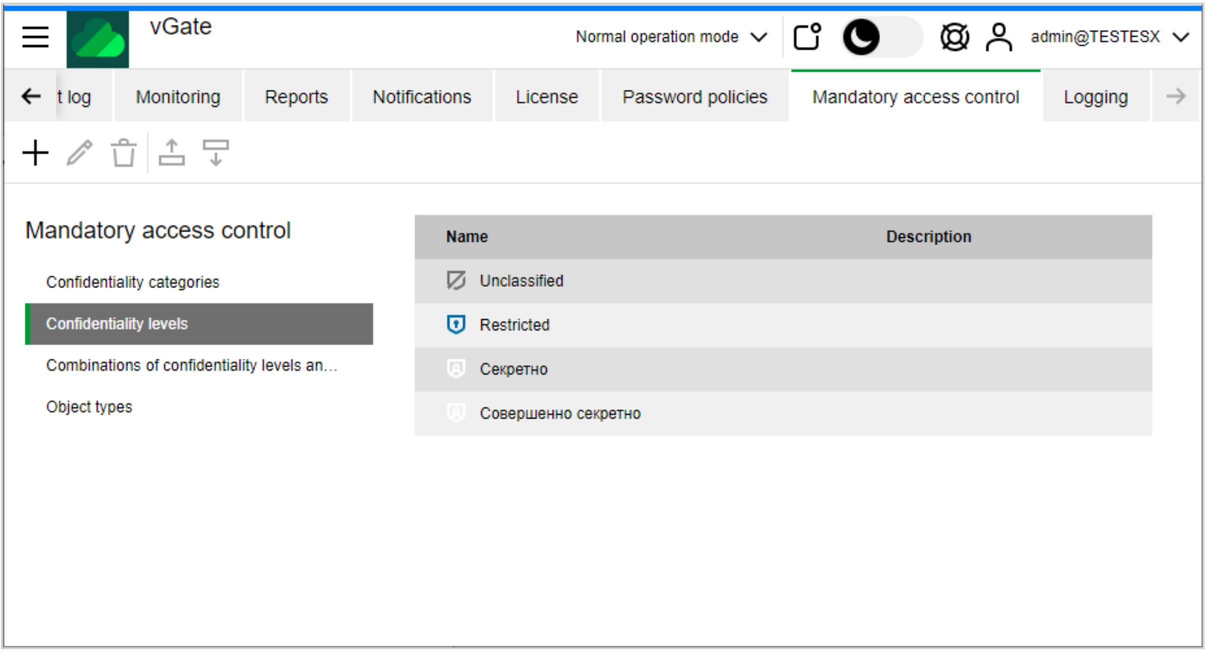


4. Specify the category name and description, and select a color.
   Click "Save". The category appears in the table.

Confidentiality levels

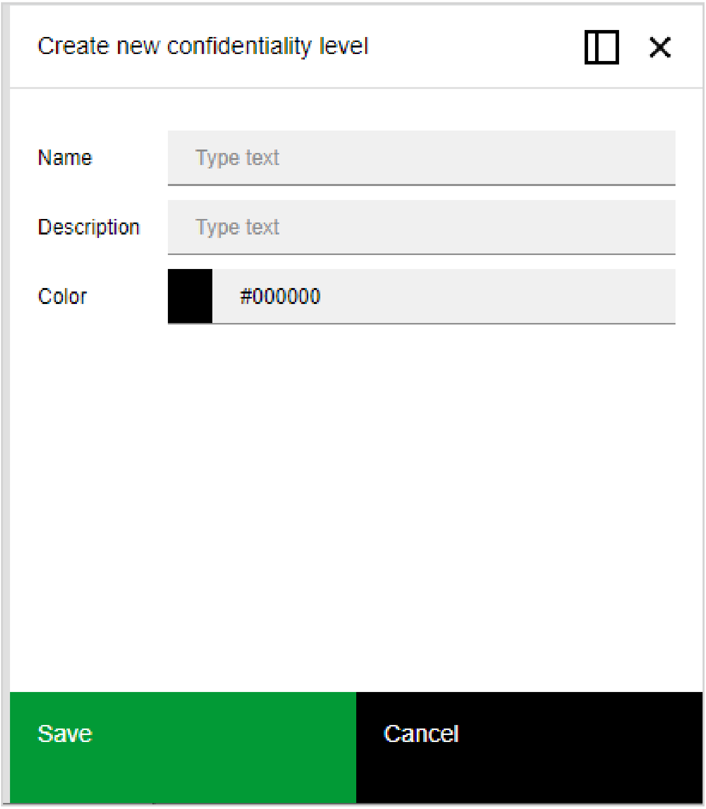
To add a confidentiality level:

1. Open the "Confidentiality levels" tab.
   The table with available confidentiality levels appears.



Note.
- To modify the list of confidentiality levels, use the "Edit" and "Delete" buttons.
- To modify the hierarchy of confidentiality levels, use the "Move up" and "Move down" buttons.

2. Click the "Add" button. A panel for creating a new confidentiality level appears.



3. Specify the level name and description, and select a color.
   Click "Save". The level appears in the table.

Combinations of confidentiality levels and categories

When assigning compound labels (labels that includes both confidentiality levels and categories) to the objects, it is automatically checked if it is possible to assign a label with the confidentiality level and category combination specified by the security administrator. To do this, the matrix of acceptable combinations of confidentiality levels and categories is used. When attempting to assign a label with an invalid combination, a warning appears informing that this label cannot be assigned.

By default, any combinations of confidentiality levels and categories are allowed in the matrix.

To configure the matrix of combinations of confidentiality levels and categories:

1. Open the "Combinations of confidentiality levels and categories" tab.

   The matrix with combinations of confidentiality levels and categories appears.
2. Specify necessary combinations and click "Save".

Object types

vGate allows you to define a list of objects to which the mandatory access control mechanism is applied. By default, control of security labels is enabled for all object types: users, ESXi, vCenter, KVM, Skala-R virtualization servers, virtual machines, virtual networks, distributed virtual switches, network adapters, storages, Cloud Director organizations. If necessary, the mandatory access control mechanism can be disabled for the selected objects.

To configure the mandatory access control mechanism:

1. In the main menu, go to the "Settings" section and open the "Mandatory access control" tab.
2. Open the "Object types" tab.

   The list of object types appears.
3. Select object types to which the mandatory access control mechanism will be applied (compliance of security labels will be checked), then click "Save".

Logging

Logging the system events of the vGate components on the vGate server can be configured via the vGate web interface.

To configure logging levels in the web console:

1. In the main menu, go to the "Settings" section and open the "Logging" tab.

   The list of services and their logging levels appears.
2. For each vGate service select a logging level and click "Save".

Type	Description
INFO	This message type contains information on events that appear while operating and do not lead to application errors
VERBOSE	This message type shows the detailed information on component operation
DEBUG	These messages contain information that can be useful while debugging
WARNING	This message type contains information on events that can lead to application errors
ERROR	These messages are used in case of the current operation failure

   Changes in logging levels come into effect after some time (1 minute) or after restart of the services.

   Note. vGate object logging can also be configured in the HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate\Logging registry branch by changing the LoggingLevel value for each service. The value of the LoggingLevel key in the Logging root folder provides logging settings for services that do not have an individual branch in the registry ("Other services" in the vGate web console).

3. Configuration of NDIS driver logging level may be requested for vGate troubleshooting. Specify the logging level with the help of template or manually using the information from the technical support.

   The EnableLogging parameters will be set to a hex value in the registry section

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vGateNdisDriver.

Configuring vGate operation modes

Apart from the normal operation mode, vGate supports additional modes for a lower degree of control of the virtual infrastructure administering for service purposes.

Mode	Description
Normal operation mode	In this mode, all vGate functionality for the virtual infrastructure protection is available. The mode must be enabled to ensure full-scale protection
Test operation mode	This mode allows putting vGate into operation or configuring it without limiting the operation of the current network infrastructure. It ensures access to virtual infrastructure servers regardless of access control rules configured in vGate. The mode is enabled be default only after the primary installation of vGate (see below)
Emergency operation mode	This mode is designed to suspend protection in case of failure of IT infrastructure elements. It allows bypassing vGate restrictions of access to the virtual environment administration during the infrastructure recovery period (see p.**79**). Unlike the normal or test operation modes, security events are not registered in the emergency operation mode

Test operation mode

By default, vGate operates in the test operation mode after the primary setup and installation. This mode ensures access to the virtual infrastructure servers from virtual infrastructure administrator and security administrator workstations without configuration of access control rules and allows putting vGate into operation or configuring it without limiting the operation of the existing network infrastructure.

vGate operation features in the test operation mode:

- Connections to all servers located within the secure perimeter of the administration network from any computers using all protocols and ports are allowed for authenticated vGate users.
- Connections to all servers in the secure perimeter using the ICMP protocol (ping command) is allowed for users which are not authenticated in vGate.

Tip. To view the list of access rules that ensure vGate operation in the test operation mode, you can use the drvmgr.exe (p.**189**) utility.

- If access rules are configured in the vGate management console (see p.**108**), access of vGate users to protected servers is granted according to these rules.
- Ability to perform operations with virtual infrastructure objects is controlled according to the configured security labels (the mandatory access control mechanism operates as in the normal operation mode).
- Events related to connections to servers in the secure perimeter are registered in the vGate event log.
- Trusted boot loading of virtual machines is supported (the "Trusted boot loading of virtual machines" policy operates as in the normal operation mode).
- Firewall rule that allows all virtual machine traffic is enabled. The rule has the minimum priority.

Once the list of protected servers is modified and access control rules for protected servers are configured, vGate must be switched to the normal operation mode.

Normal operation mode

To ensure full-scale protection of the virtual infrastructure, once access control rules for protected servers are configured, switch vGate to the normal operation mode .

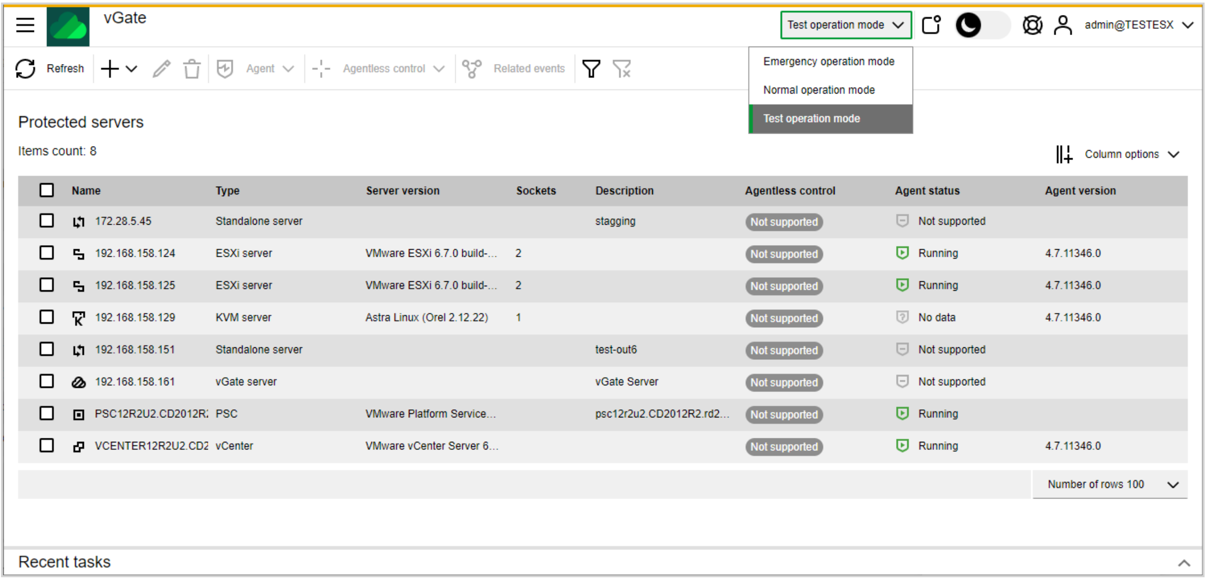
Control of user access to virtual infrastructure servers in the normal operation mode is performed according to the rules configured by the administrator in the vGate web console (details on configuring access to protected servers can be found on p.**107**).

If necessary (for example, to reduce control of access to servers in the secure perimeter in case of the virtual infrastructure reorganization), vGate can be switched to the test operation mode.

Attention! If the infrastructure includes the vCenter server with the installed vGate agent, parameters of connection to the virtualization server must be saved to switch the operation mode (see p.**64**).

To switch vGate to the normal operation mode:

1. At the top of the web console, click the "Test operation mode" button and select the "Normal operation mode" option in the drop-down list.



A warning about switching vGate to the normal operation mode appears.

2. Click "OK" in the warning dialog box.

   The vGate normal operation mode will be enabled.

Emergency operation mode

Emergency mode is designed to suspend protection in case of failure of IT infrastructure elements. This mode allows administrator to bypass restrictions of access to the virtual environment administration during the infrastructure recovery period.

Attention! To ensure full-scale protection of the virtual infrastructure, switch vGate to the normal operation mode after the infrastructure recovery.

The following functions are suspended in the emergency operation mode:

- vGate agents operation;
- operation of security policies;
- operation of access rules for protected servers and rules for filtering network connections to vCenter;
- control of security labels;
- VM traffic control;
- audit of security events for vGate agents on protected servers.

When switching to the emergency operation mode and from it, credentials for access to protected ESXi servers (if they are not controlled by the vCenter (vCSA) server) and to the PSC server (VMware vSphere 6.7) will be requested.

Attention! If the infrastructure includes the vCenter server with the installed vGate agent, parameters of connection to the virtualization server must be saved to switch the operation mode (see p.64).

While recovering the infrastructure operation, changes in the configuration of protected servers may occur. Before switching vGate to the normal operation mode, make sure that vGate configuration complies with the configuration plan (see p.58).

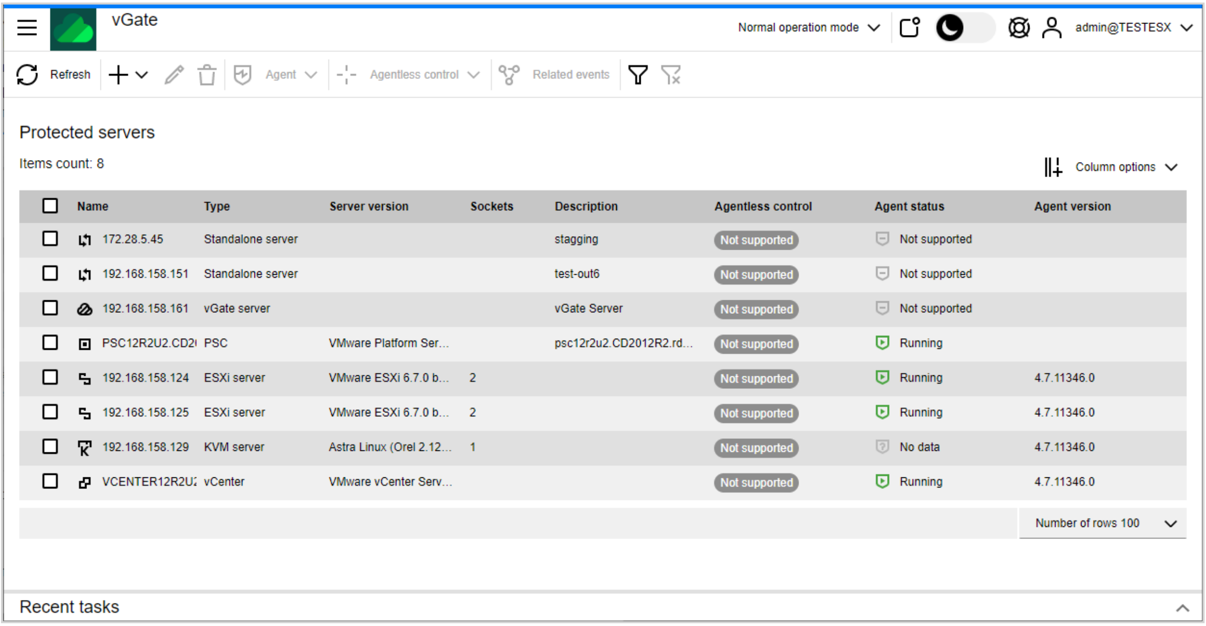
Protected servers

The list of protected servers can include ESXi servers, vCenter, PSC, Cloud Director servers, embedded Harbor Registry, KVM servers, OpenNebula servers, Proxmox servers, Skala-R servers, and other virtual infrastructure elements that are located in the secure perimeter of the administration network and have an IP address (for example, DNS).

To add an ESXi, vCenter or PSC server:

1. In the main menu, go to the "Protected servers" section.

   The list of protected servers appears.

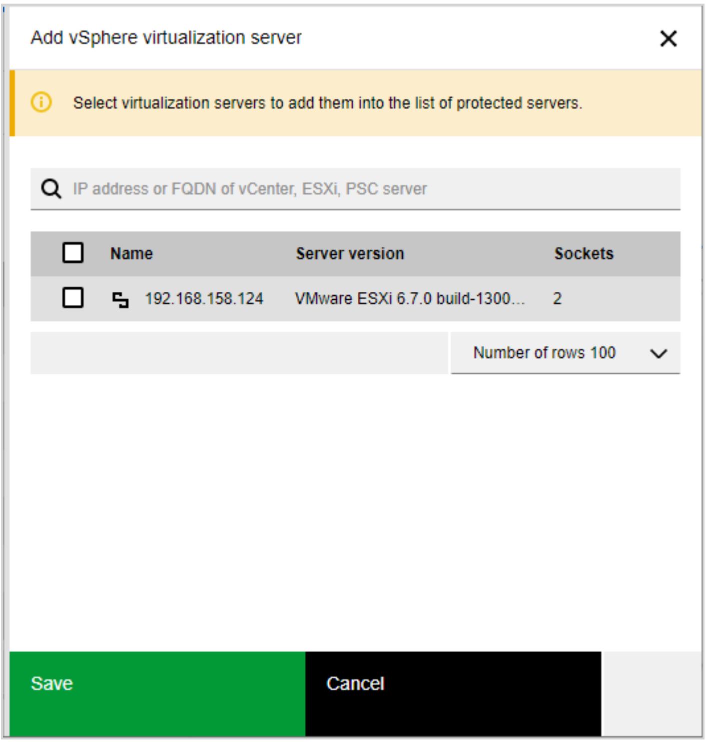


   At the bottom of the page, the information about the recent operations with protected servers is presented.

   Note.
   - To configure the table columns, click "Column options" and select the required options.
   - To modify the list of protected servers, use the "Edit" and "Delete" buttons.
   - To use filters, click "Filtering", set the required criteria in the appeared panel and click "Apply". To reset the search results, click the "Reset filters" button.
   - To view security events related to a certain server, select the required server and click "Related events".

2. To add a virtualization server to the list of protected by vGate, click "Add" and select "vSphere virtualization server" in the drop-down list.

   A panel for adding virtualization servers with the list of servers appears on the right.



Note. Depending on the specified connection parameters (see p.**64**), the list will either contain one virtualization server or a vCenter server and all virtualization servers controlled by it.

3. Select the required servers in the list and click the "Save" button.

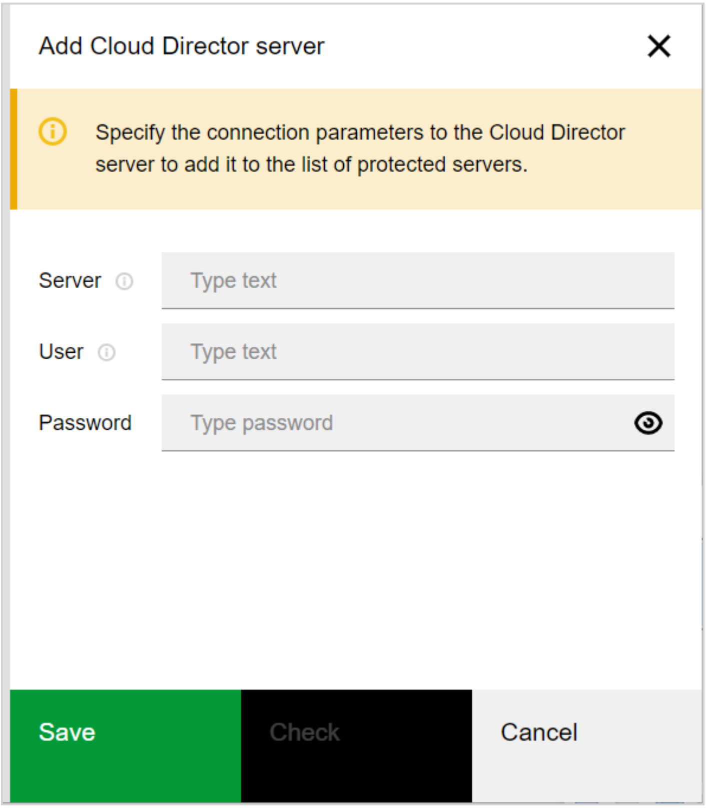
Tip. To select several elements in the list, use <Shift> and <Ctrl> keys.

To add a Cloud Director server:

1. Go to the "Protected servers" section, click "Add" and select "Cloud Director server" in the drop-down list.

   If parameters of connection to the Cloud Director server are saved in the "Connection to servers" section (see p.**64**), a confirmation to add the server to the list of protected servers will appear. Click "Yes", after this the server will appear in the list.

   If parameters of connection to the Cloud Director server are not saved in the settings, a panel for adding a Cloud Director server will appear.



2. Specify the server IP address or network name, as well as the administrator credentials for connection to it.
3. Click the "Check" button to test connection to the server using the specified credentials.
4. Click "Save".

   The Cloud Director server will be added to the list of protected servers.

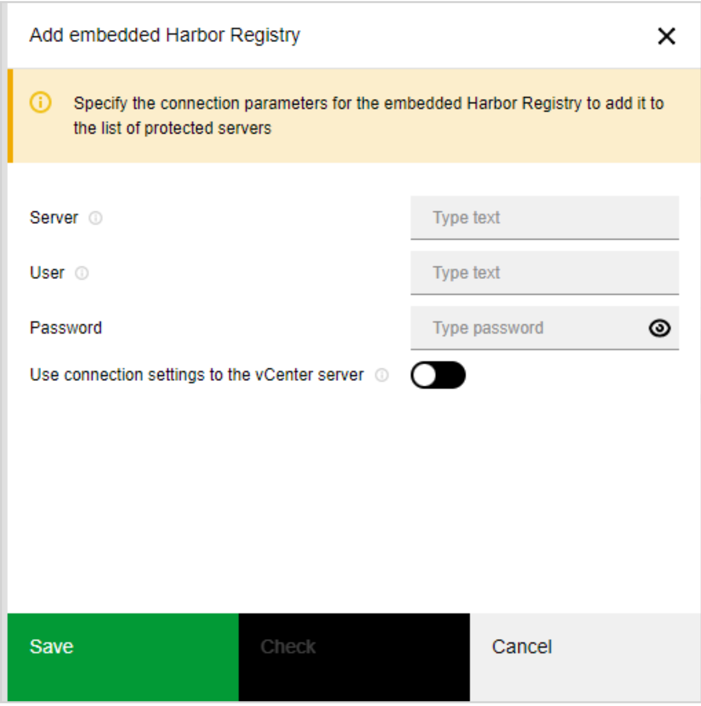
Note.
- If a vCenter server is added to the list of protected servers, a Cloud Director server must be connected to it.
- To register redundant Cloud Director servers in vGate, repeat steps 2-4. In this case, connection to the main Cloud Director server should be configured last.
- If the Cloud Director server, connection parameters to which are saved in the vGate configuration settings, is out of service, you need to configure connection to one of available redundant servers.

To add an embedded Harbor Registry:

1. Go to the "Protected servers" section, click "Add" and select "Embedded Harbor Registry" in the drop-down list.

   If parameters of connection to the embedded Harbor Registry are saved in the "Connection to servers" section (see p.64), a confirmation to add the embedded Harbor Registry to the list of protected servers will appear. Click "Yes", after this the embedded Harbor Registry will appear in the list.

   If parameters of connection to the embedded Harbor Registry are not saved in the settings, a panel for adding the embedded Harbor Registry will appear.

2. Specify the embedded Harbor Registry IP address, as well as the administrator credentials for connection to it.

   Note. To use for the vCenter server administrator credentials for connection, turn on the "Use connection settings to the vCenter server" toggle.

3. Click the "Check" button to test connection to the server using the specified credentials.
4. Click the "Save" button.

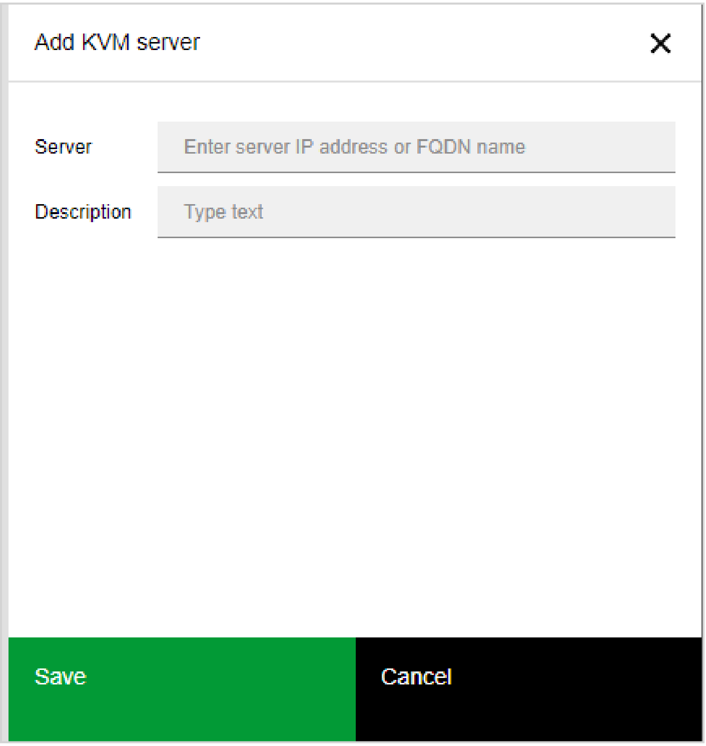
   The embedded Harbor Registry will be added to the list of protected servers.

To add a KVM virtualization server/standalone Skala-R server:

1. Go to the "Protected servers" section, click "Add" and select "KVM virtualization server" in the drop-down list.

   If parameters of connection to the KVM server/standalone Skala-R server are saved in the "Connection to servers" section (see p.**64**), a panel for adding a protected server will appear. Specify the server IP address. If necessary, add a description, and click the "Save" button. The server appears in the list of protected servers.

   If parameters of connection to the server are not saved in the settings, a panel for connecting to the server will appear.



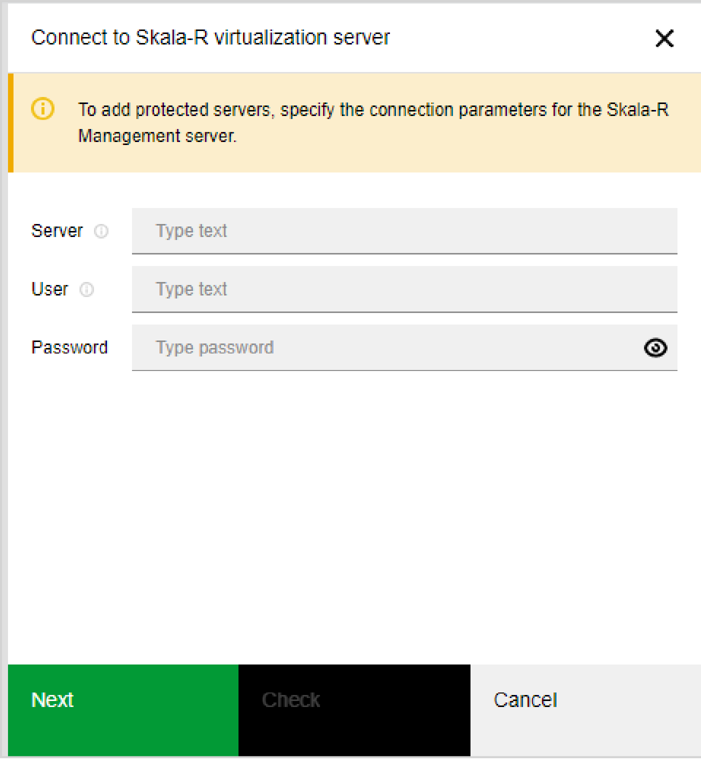
2. Specify the KVM server/standalone Skala-R server IP address or network name, as well as credentials for connection to it. To manage servers, the root user account shared for all protected KVM servers/standalone Skala-R servers is required. Credentials are requested only when adding the first server.
3. Click the "Check" button to test connection to the server using the specified credentials.
4. Click "Save".

   The virtualization server will be added to the list of protected servers.

To add a Skala-R server that is controlled by Skala-R Management:

1. Go to the "Protected servers" section, click "Add" and select "Skala-R server virtualization server" in the drop-down list.

   If parameters of connection to the Skala-R Management server are not saved in the "Connection to servers" section (see p.**64**), a panel for connecting to the server appears.



2. Specify the Skala-R Management server/HA-cluster IP address or network name, as well as the administrator credentials for connection to it (see p.**64**).
3. Click the "Check" button to test connection to the server using the specified credentials.
4. Click "Save". A connection to the virtualization server will be established.
5. If parameters of connection to the Skala-R Management server are saved in the settings, a panel for adding servers to the list of protected servers appears.
6. Select Skala-R virtualization servers to add them to the list of protected servers and click the "Save" button.

To add an OpenNebula/Proxmox server:

1. Go to the "Protected servers" section, click "Add" and select "OpenNebula server" or "Proxmox server" in the drop-down list.

   If parameters of connection to a server are not saved in the "Connection to servers" section (see p.**64**), a panel for connecting to the server appears.
2. Specify the OpenNebula/Proxmox server IP address or network name, as well as the administrator credentials for connection to it (see p.**64**).
3. Click the "Check" button to test connection to the server using the specified credentials.
4. Click "Save". A connection to the virtualization server will be established.
5. If parameters of connection to the OpenNebula platfrom/Proxmox server are saved in the settings, a panel for adding servers to the list of protected servers appears.
6. Select virtualization servers to add them to the list of protected servers and click the "Save" button.
7. While adding OpenNebula servers, a panel for connecting to the selected server appears. Specify the root user name and password, then click "Save". If different parameters are used for connection to OpenNebula servers, configure a separate connection for each of them.

   Attention! For correct displaying of OpenNebula virtual machines, add the OpenNebula management server to the list of protected servers in the web console.

To register another object of the virtual infrastructure:

1. Go to the "Protected servers" section, click "Add" and select "Standalone server" in the drop-down list.

   A panel for adding a standalone server appears on the right.
2. Specify the server IP address or network name, enter a comment (if necessary) and click "Save".

   New records will appear in the list of protected servers.

vGate agent installation

vGate agent installation on servers is performed in the web console. Before installing agents, you must specify parameters of connection to virtualization servers (see p.**64**) and add them to the list of protected servers (see p.**79**).

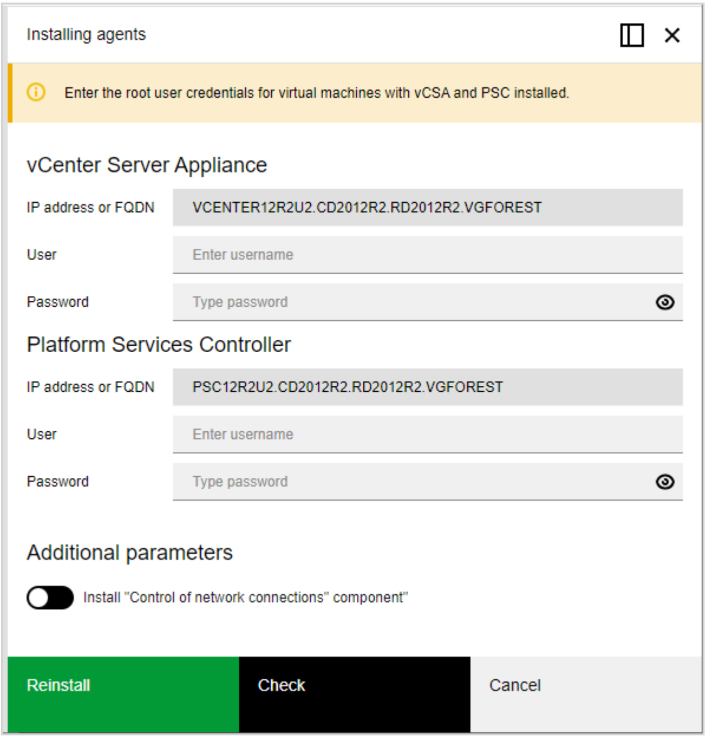
Attention! If the virtual infrastructure configuration includes vCenter, and ESXi servers are managed using vCenter Client or vSphere Web Client, the vGate agent must be installed on the vCenter server before the deployment of vGate agents on ESXi servers.

Note. If necessary, vGate agent for vCenter server (VMware vSphere 6.5 or 6.7) that is deployed on Windows OS can be installed manually using the vGate setup program directly on a computer with the installed VMware vCenter (see p.164).

To install vGate agent on a protected server:

1. In the "Protected servers" section, select a protected server and click the "Agent" button.
2. Select "Install" in the drop-down list.

   A panel for installing vGate agents appears.



3. Depending on the virtual infrastructure architecture, credentials for connection to different servers (vCenter, ESXi, PSC, ESXi PSC or ESXi passive, KVM, Skala-R, OpenNebula, Proxmox) will be requested. Specify IP addresses (FQDN), administrator names and passwords for servers. The root user account is required for communication with KVM, Skala-R, Proxmox and OpenNebula servers.

   Note.
   - vGate agent will be installed only on those servers for which the specified root user account is used.
   - If parameters of connection to vCenter, KVM, Skala-R Management and Proxmox servers are saved in the "Connection to servers" section (see p.64), credentials will not be requested.
   - To install the vGate agent on KVM, Skala-R, Proxmox, OpenNebula servers, access through SSH (port 22) must be enabled and allowed.

4. Turn on the "Install "Control of network connections" component" toggle to restrict incoming network connections on the vCenter server after the vGate agent installation. Details on configuring the vCenter traffic filtering can be found on p.**111**.
5. Click the "Check" button to test connection to the server using the specified credentials. To start installation, click "Install".

   After the vGate agent installation, the "Agent status" field of the server changes to "Running".

To reinstall, suspend or remove the vGate agent on a server, select the server in the list of protected servers, click "Agent" and then select "Reinstall", "Pause" (supported for ESXi servers only) or "Remove" respectively. When removing the vGate agent from the vCenter (vCSA) server, in vSphere 6.7 the vGate agent will be automatically removed from PSC.

Attention! After the vGate agent installation/removal, vCSA web services (vsphere-ui and vsphere-client) will be automatically rebooted. While performing this operation, vCSA management in vSphere Web Client is not available.

Note.
- vGate Standard allows you to protect one vCenter server only. If several vCenter servers are operated in a company, and these servers are interconnected using the VMware vCenter Linked Mode, the vGate agent must be installed on each of them. This function is available in vGate Enterprise and Enterprise Plus only (see the "Functionality" section in the document [1]).
- If the Secret Net Studio software is operated on the computer, where the vGate agent for vCenter will be installed, you must disable the Secret Net firewall before installation.

Attention! On the vCenter server, port 38085 is used for vGate by default. If necessary, you can change the port. To do this:
- close the vGate management console;
- change the VcpOnVCenterPort port value in the registry section HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate;
- restart the vGate management service (rhuid.exe).

Attention! If a firewall (red hat firewall or ufw) is enabled on a KVM server while installing the vGate agent, rules that allow incoming connections by the following ports will be created in the firewall settings:
- 3806 — agent TCP service (sc_agentd);
- 3812 — integrity control TCP service(inchd);
- 50001 — virtualization control TCP service (libvirtd);
- 50002 — TCP service for wiping (sc_worker).

If another firewall is installed on the server, you must manually create rules that allow incoming connections for ports listed above.

Agentless control

Control of operations without the vGate agent installation is available for vCSA servers.

Note. By default, agentless control is enabled for Skala-R Management servers.

Agentless control is supported for VMware vCenter Server Appliance 7.0 update 1 and later.

Note. Agentless control of operations for several servers is supported only if they are interconnected using VMware vCenter Linked Mode.

To enable agentless control on a vCSA server:

1. Go to the "Protected servers" section and select the vCSA server in the list of protected objects.
2. Click the "Agentless control" button and select "Enable" in the drop-down list.

Automatic deployment of vGate agents on ESXi servers using VMware Auto Deploy

This function is available only in vGate Enterprise and Enterprise Plus.

VMware vSphere includes the "Auto Deploy" feature designed for automatic deployment of ESXi servers. The VibModifcator.exe utility is a part of the vGate software, it allows you to create a vGate agents installation archive and add it to an ESXi image used by VMware Auto Deploy.

The utility is located in the vGate installation folder on the vGate server, and it is available in the command prompt. To view detailed information about the utility, open the command prompt and type the following command:

```
VibModificator.exe –h
```

To create a file archive from a template:

1. Open the command prompt on behalf of the administrator and run the following command:

   ```
   C:\Program Files\vGate\VibModificator.exe -z -p <path>
   ```

   where:
   - z — command for creating ZIP archive from the sc-vgate-autodeploy-xxxxx-esxi-template.vib template;
   - p **<path>** — path to the folder where the archive will be saved. If the folder does not exist, it will be created. By default, the archive will be saved to the vGate installation folder (C:\Program Files\vGate).

   The sc-vgate-autodeploy-xxxxx-esxi-offline-bundle.zip file will be created in the specified folder as a result of this command.

Note. Results of the VibModificator.exe utility and the "VibModificator.exe -z -p **<path>**" command are the same.

2. To add the archive to the ESXi image, copy it on the vCenter server.

To create a VIB file from a template:

1. Open the command prompt on behalf of the administrator and run the following command:

```
C:\Program Files\vGate\VibModificator.exe -s -p <path>
```

where:

- s — command for creating file set from the sc-vgate-autodeploy-xxxxx-esxi-template.vib template;
- p **<path>** — path to the folder, where the set will be saved. If the folder does not exist, it will be created. By default, the set will be saved to the vGate installation folder (C:\Program Files\vGate).

The folder containing the sc- vgate-autodeploy-xxxxx-esxi.vib file and XML file set will be created in the specified directory.

2. If necessary, check the VIB file by running the following command:

```
C:\Program Files\vGate\VibModificator.exe -c -n sc-vgate-autodeploy-xxxxx-esxi.vib
```

where:

- c — command for searching registry values in the VIB file;
- n **sc-vgate-autodeploy-xxxxx-esxi.vib** — the VIB archive template name. By default, VIB archive searching is performed in the current folder.

The list of found parameters or an empty string (if no parameters have been found) will appear. Registry keys are used for the VIB file and for checking. For example:

- AutodeployPort registry keys: deploy port is 9989, firewall port is 9989;
- RhuidHttpPort registry keys: haron port is 80, haron address is 192.168.5.30.

3. Add the received XML files and VIB file to the ZIP archive, then copy it to the vCenter server to add it to the ESXi image.

To automatically deploy the vGate agent on ESXi server:

1. Add the created archive that includes the vgate-autodeploy-xxxxx-esxi.vib file to an ESXi server image that is used by VMware Auto Deploy.
2. Power on the ESXi server. In the vGate web console, add the server to the list of protected objects.

   In a few minutes the vGate agent will be automatically installed on the ESXi server. To speed up the process, you can install the vGate agent manually (see p.**85**). In the future, vGate agent will be installed automatically when you restart the ESXi server.
3. Create the required rules for user access to the ESXi server (see p.**107**).

User account management

vGate accounts

Initially, user account management is performed by the chief security administrator, whose account is created during the vGate server installation. In the future, you can grant the privilege to manage the list of users to the security administrator account.

The security administrator can register two types of users: virtual infrastructure administrator and security administrator (see the "Administrative function differentiation" section in the document [1]).

If the vGate management is performed by several security administrators, additional accounts must be configured for each of them.

Attention! The chief security administrator has a number of privileges in comparison with accounts configured in the web console. Only this account can add access rules for the external adapter of the main or redundant vGate server, modify the chief security administrator account, as well as create accounts with the "Account operator" privilege (see p.**90**).

For user (virtual infrastructure administrator) authentication in vGate, you can use existing Windows domain user accounts. To do this, import AD user accounts, computers and groups from the domain where the vGate server is located or from a trusted domain (see p.**67**). All domain users are automatically added to the "Authenticated" group, and the respective rules of access to protected servers are applied to them (see p.**107**).

For mandatory access control, domain accounts must be registered in the vGate web console.

Attention!
- vGate supports operation only with one nesting level of the Active Directory groups.
- Operation with nested groups is performed only if the Active Directory domain controller transfers information about user membership in nested groups.

Initially, the list of users can include computer accounts. They are automatically created while installing the vGate client on computers in the external perimeter of the administration network, which are not joined to the vGate server domain or to the trusted domains. Computer accounts are automatically assigned the password which is stored in the system in a protected format and is used for authentication. Such accounts are used for computers authentication, as well as for organizing access of these computers' services to protected ESXi servers and other administration network nodes.

Computer account names have the following format:

<computer name>$@<account registry name>

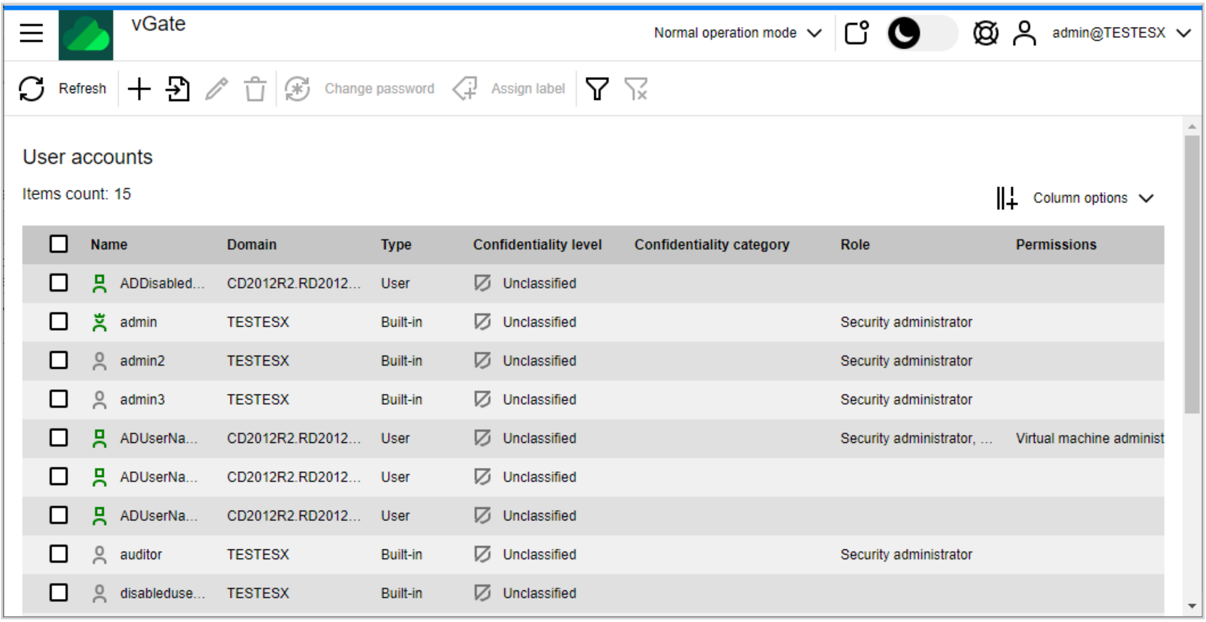
For example: arm$@VGATE.

Attention! We do not recommend removing computer accounts, since the vGate client reinstallation will be required for their recovery.

To create an account:

1. In the main menu, go to the "User accounts" section.

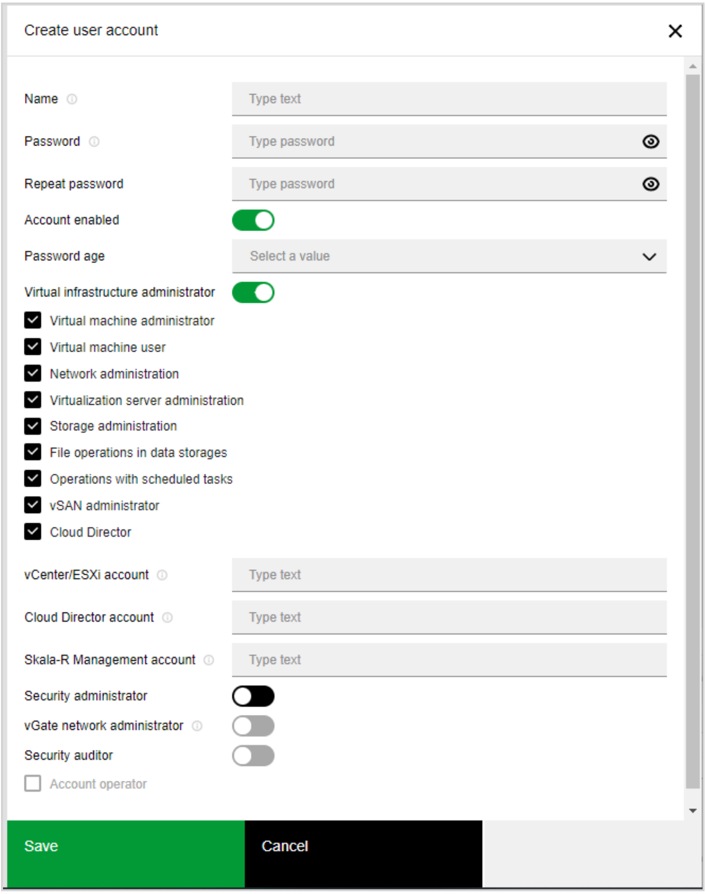
   The following window appears.



Note.
- To configure the table columns, click "Column options" and select the required options.
- To refresh the list of accounts, click the "Refresh" button.
- To use filters, click "Filtering" , set the required criteria in the appeared panel and click "Apply". To reset the search results, click the "Reset filters" button.

2. Click the "Create" button.

A panel for creating an account appears on the right.



3. Specify the user name, type the password twice. If necessary, configure the account parameters.

Parameter	Description
Account enabled	Accounts are enabled by default. Turn off this toggle to temporarily disable the created account. If an account is disabled, you cannot log on using this account. The user who is already authorized can continue working after account disabling until the next authorization attempt. You cannot disable the chief security administrator account that was created during the vGate server installation
Password age	Select the password age in the list. Password parameters coniguration is not available for the Active Directory accounts
Virtual infrastructure administrator	Turn on this toggle to create a virtual infrastructure administrator account and select privileges that will be granted to the virtual infrastructure administrator in the list. Details on privileges of different types of users can be found on p.**167**
vCenter/ESXi account	Specify the vSphere administrator account name to control user access to the VMware vSphere environment (see p.**90**)
Cloud Director account	To control Cloud Director operations, specify the Cloud Director user account name (see p.**90**)
Skala-R Management account	To control the user access to the Skala-R environment, specify the name of the Skala-R Management server administrator. By default, this field is empty. It means that this user can log on to the Skala-R environment using any account
Security administrator	To create a security administrator account, turn on this toggle and select privileges that will be granted to the security administrator in the list

Parameter	Description
vGate network administrator	Turn on this toggle to allow this user to view and modify the vGate firewall parameters (see p.**143**). This privilege can be granted to the security administrator only
Security auditor	Turn on this toggle to grant read-only permissions in the vGate management program to the user
Account operator	Select this check box to allow the user to modify the list of users. When this parameter is selected, the security administrator access privileges are automatically granted to the user

Note. For correct operation of the "File operations in data storages" privilege, the corresponding access rule must be configured for this user.

4. Click "Save".

   The account appears in the list.

Note.
- To modify account parameters, select a user in the list and click "Edit".
- To change a user password or remove an account, use the "Change password" and "Delete" buttons. When removing an account, you will be asked if access rules for this user should be removed. Password changing is not available for Active Directory accounts.
- Procedure of password changing in the vGate client is given in the document [4].
- To assign a security label to an account, select the required account and click "Assign label". A panel for assigning security labels appears (see p.120).

To import an account from Active Directory:

1. On the "User accounts" page click the "Import" button. A panel for adding an account appears.
2. Select an account (user, computer or group) in the list to add it from Active Directory and configure the parameters for operation in vGate (see above).
3. Click "Save". The account appears in the list.

vCenter/ESXi account

By default, the "vCenter/ESXi account" field in the panel for creating the vGate user account is empty. This means that this user can log in to the VMware vSphere environment using any account.

To control user access to the vSphere environment, specify one or several VMware accounts in this field. Each account must be specified in all supported formats: "domain\user", "user@domain", "full.domain.name\user" and "user@full.domain.name". Use the ";" character as a separator between records in different formats.

For example:

vsphere\admin;admin@vsphere;vsphere.local\admin;admin@vsphere.local

After this, the vGate user will be able to log in to the vSphere environment using the specified accounts only.

The parameter is useful for limiting the security administrator privileges when operating in the virtual infrastructure. For full-scale differentiation of administrative functions, the security administrator privileges must be limited to only viewing the parameters. Therefore, the "vCenter/ESXi account" field allows matching the security administrator account to an account with limited privileges in the VMware environment.

Cloud Director account

When performing Cloud Director operations control (see p.**134**), all requests to the Cloud Director server go through the vGate server. Thus, all users (including provider and tenant) that will work with the Cloud Director server must be registered.

For the Cloud Director user who needs access to the provider or tenant portals, create the vGate account with the "Access to the virtual infrastructure allowed" and "Cloud Director administrator" privileges by specifying the Cloud Director user credentials in the "Cloud Director account" field.

Note. By default, the "Cloud Director account" field is empty. This means that this user can log into the Cloud Director environment using any account.

Configuring password policies

Password policies allow you to ensure that user passwords meet the complexity requirements. To configure password policies, go to the "Settings" section (see p.**73**).

Usage of security tokens

You can use Rutoken and JaCarta security tokens to log on via the web console.

Note. vGate does not support simultaneous operation of JaCarta and Rutoken security tokens when logging on via the vGate Client.

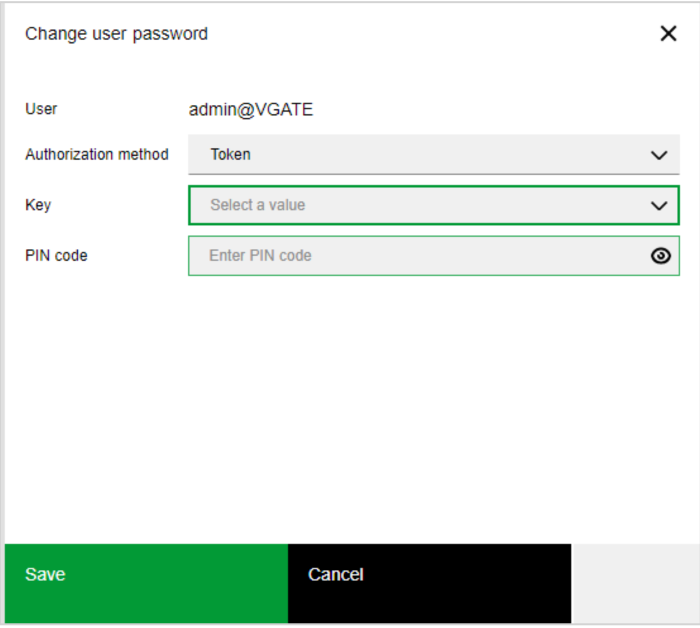
To configure a security token (Rutoken/JaCarta):

1. Initialize your security token in the Rutoken or JaCarta software according to the documentation for these products.

   Note.
   For correct operation of a security token, install the Rutoken/JaCarta device driver (JaCarta Unified Client) on the computer designated to be the vGate server, and on the virtual infrastructure administrator/security administrator workstation. You can install the vGate software and the Rutoken/JaCarta drivers in any order. JaCarta Unified Client is located in the Redistributables\JaCarta folder, Rutoken driver is located in the Redistributables\Rutoken folder on the vGate setup disk. For JaCarta token to operate in the vGate web console, install the JC- WebClient software (https://www.aladdin-rd.ru/support/downloads/jc-webclient).

2. Connect the token to the computer, where the vGate web console is opened.
3. In the web console, go to the "User accounts" section and select a user to which you want to assign the token. Then click "Change password".

   The following panel appears.



4. Select "Token" as an authorization method. The security token settings appear.
5. Select the required Rutoken/JaCarta key and specify a PIN code for it.
6. Click the "Save" button.

   The password will be saved to the token.

Note.
- Details on logon via a security token can be found in the document [4].
- vGate does not support security token assignment to the objects from Active Directory. If you need to configure a security token for such users, use the network version of Secret Net. In this case, the security token assigned to the Secret Net domain account is used for logon to the Windows OS. When logging on to vGate, select the "Use the current Windows session" check box.

Grouping objects

In the vGate web console, you can combine virtual infrastructure objects into groups. The following objects can be added to groups: protected servers, virtual machines, virtual machine templates, network adapters, storage units, virtual switches, virtual networks, Cloud Director organizations.

Security labels and security policies can be assigned to object groups. The new settings will be automatically applied for all objects in a group.

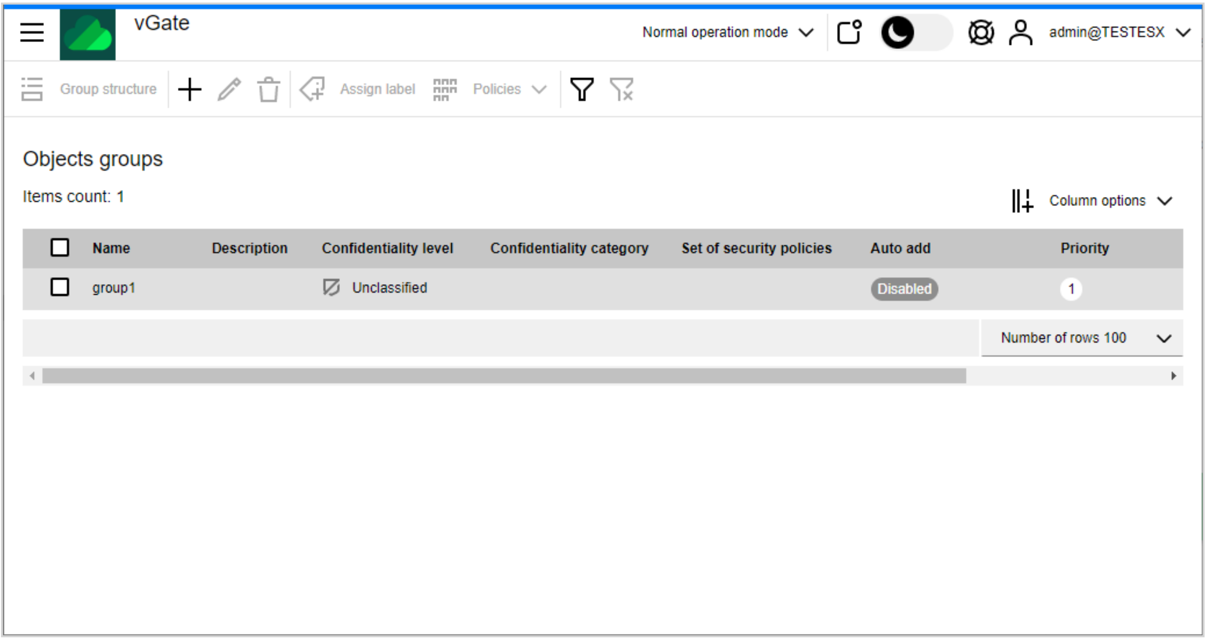
Attention! We do not recommend using %, /, \ characters in the names of VMware virtual machines. It may cause problems while adding these virtual machines to groups.

Attention! When assigning the "Integrity control of virtual machine templates" policy with the "Integrity control of virtual disks" parameter enabled to the group that contains virtual machine templates, operation of calculating disk image checksums may take a long time.

To create a group of objects:

1. In the web console, go to the "Objects groups" section.

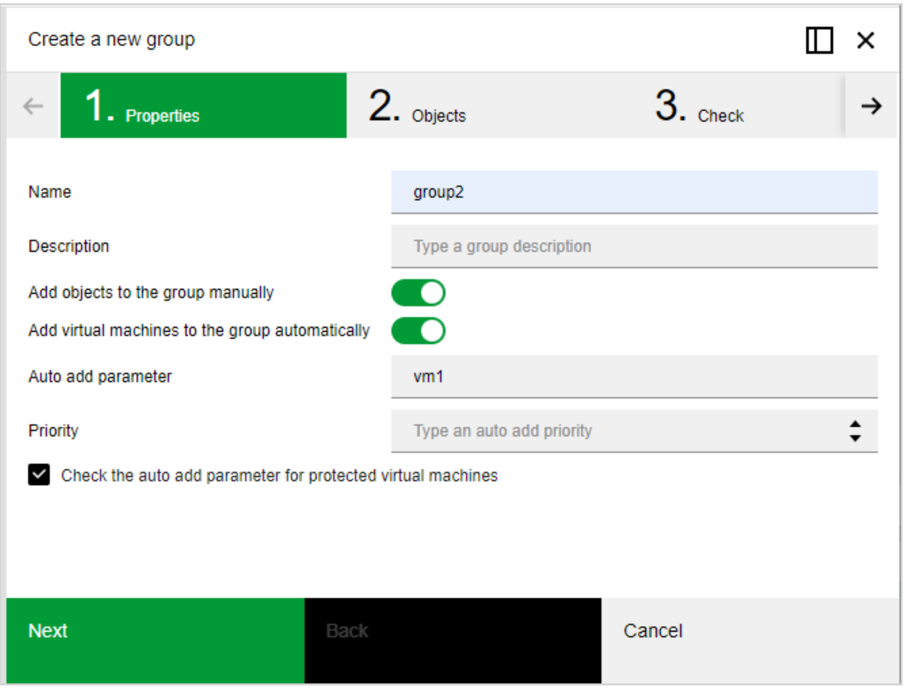
   The list of groups appears.



2. To create a group, click the "Add" button.

   Attention! To create a group, parameters of connection to the virtualization server must be saved in the web console (see p.64).

   A panel for creating a new group appears.



3. Configure parameters of the new group and click "Next".

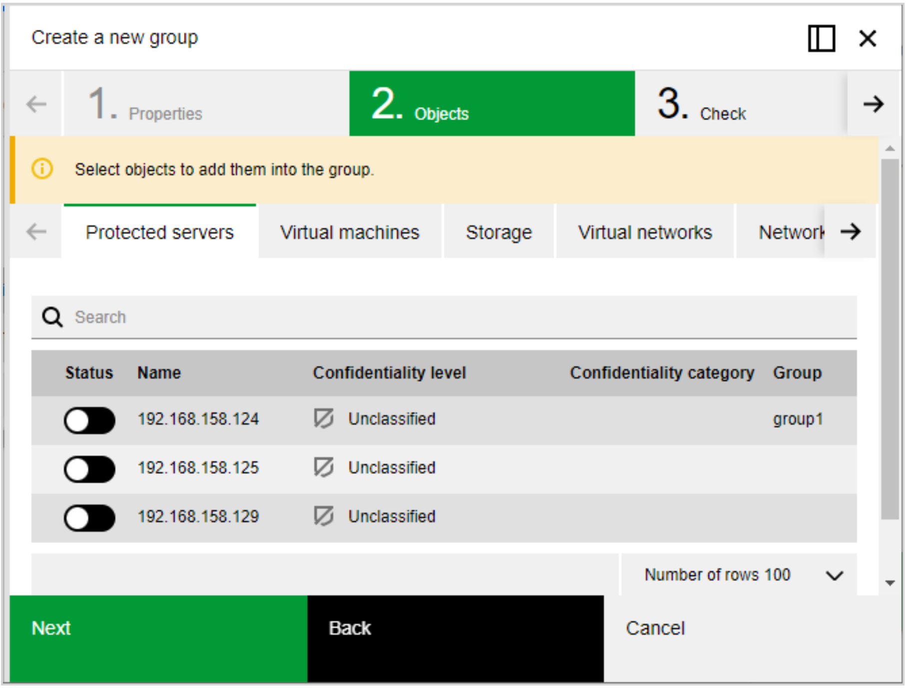
Parameter	Description
Name	Group name
Description	Group description. This parameter is not mandatory
Add objects to the group manually	Turn on this toggle to select objects for adding to the group in the next step
Add virtual machines to the group automatically	To enable the automatic addition of virtual machines to the group according to the specified parameter, turn on this toggle. Specify the auto add parameter and priority
Auto add parameter	Type the text you want to search for in the virtual machine names. The search will find any names that include the specified text. The search is not registry sensitive. Special characters that define search rules are not supported
Priority	Specify the priority, according to which the group to which an object will be added is determined, if its name corresponds to several auto add parameters. When changing the priority of one of the groups, the priorities of the other groups are automatically recalculated to avoid the duplication of priorities and gaps between the priority values
Check the auto add parameter for protected virtual machines	Select this check box to check operation of the auto add rule configured above for existing virtual machines in the next step. The selected virtual machines will be immediately added to the group. Virtual machines which are not selected during the scan cannot be added to the group automatically in the future

By default, automatic adding of virtual machines to the groups is performed every 10 minutes. If necessary, you can change the settings of automatic adding in the web console. To do this, go to the "Settings" section, open the "General" tab, in the "Automatic adding of virtual machines to the groups and segments" area change the "Add new virtual machines every, minutes" parameter value.

Note

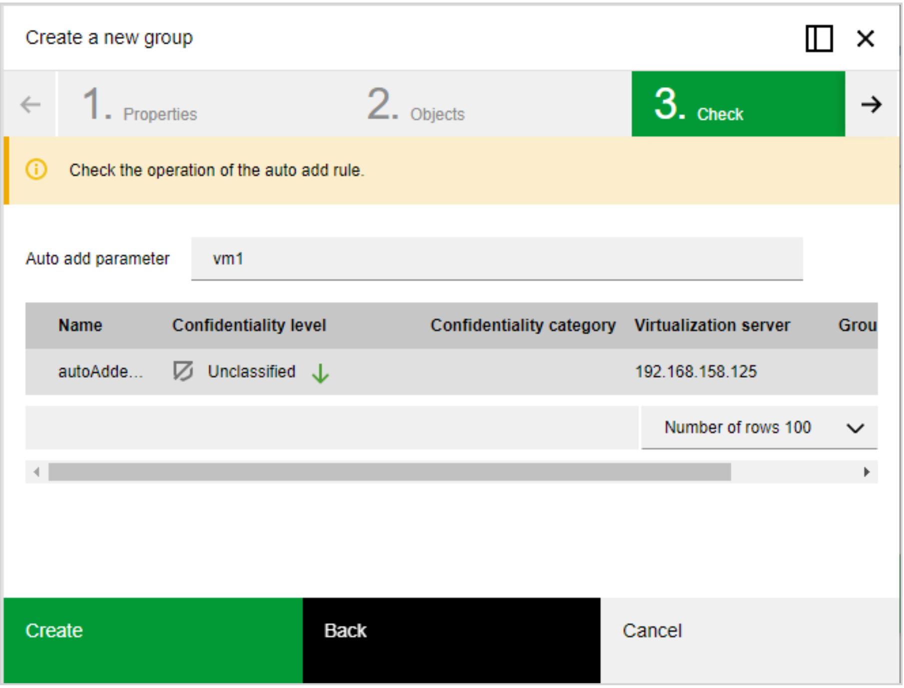
- Adding an object (including automatic adding) to the group is possible only if the object does not belong to another group. If you add an object to the new group manually, this object will be removed from its previous group.
- New virtual machines are automatically added to the groups according to the auto add parameter.
- When adding an object to the group with configured security labels and policies, these settings are applied to the object. All previous security labels and policies are canceled for this object.
- Automatic addition to a group is possible only for virtual machines with which no previous operations were performed using the vGate software (adding to group, assigning security labels or policies).

If the "Add objects to the group manually" toggle is turned on, a panel for selecting objects appears.



4. Select protected objects in the list to add them to the group, and click "Next".

If the "Check the auto add parameter for protected virtual machines" check box is selected, a panel for checking the auto add rule operation appears.



5. Check the automatic adding rule on a given parameter. Click the "Create" button.

   The group will be created.

   Attention! Adding objects to a group may take a long time.

Note. To disable the auto add function for all groups, set the parameter AddVmToGroupTimeout=0 in the HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate registry section.

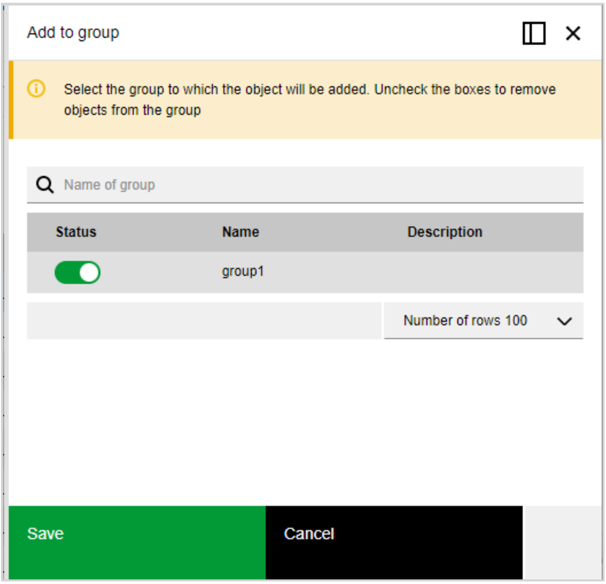
To add an object to the group:

1. In the web console, go to the "Security configuration of servers", "Virtual machines", "Storage", "vSphere virtual networks", "vSphere network adapters" or "Organization" section.

   The list of objects appears.

2. Select an object and click "Add to group".

   A panel for selecting a group appears.



3. Select the required group and click "Save". The virtual infrastructure object will be added to the group.

To remove an object from the group:

1. Go to the "Objects groups" section, select the required group and click the "Group structure" button.

   A panel containig the list of objects appears on the right.
2. Select the required object and click the "Delete" button. The object will be removed from the group.

   Note. Once the object is removed from the group, all security labels and policies assigned to it will be removed. The "Unclassified" confidentiality level will be assigned to the object.

Security policies

Security policies contain settings for protected objects, which allow ensuring compliance with the requirements of some security standards.

Assigning security policies and using the mandatory access control mechanism allow you to ensure the required security level.

Security policies can be assigned to the following objects:

- ESXi server;
- vGate server;
- virtual machine;
- virtual machine template;
- network adapter;
- distributed virtual switch;
- container image of an embedded Harbor Registry.

Note. Security policies are assigned to a distributed virtual switch (distributed vSwitch) with the help of clacl.exe utility (see p.186).

Procedure for assigning policies

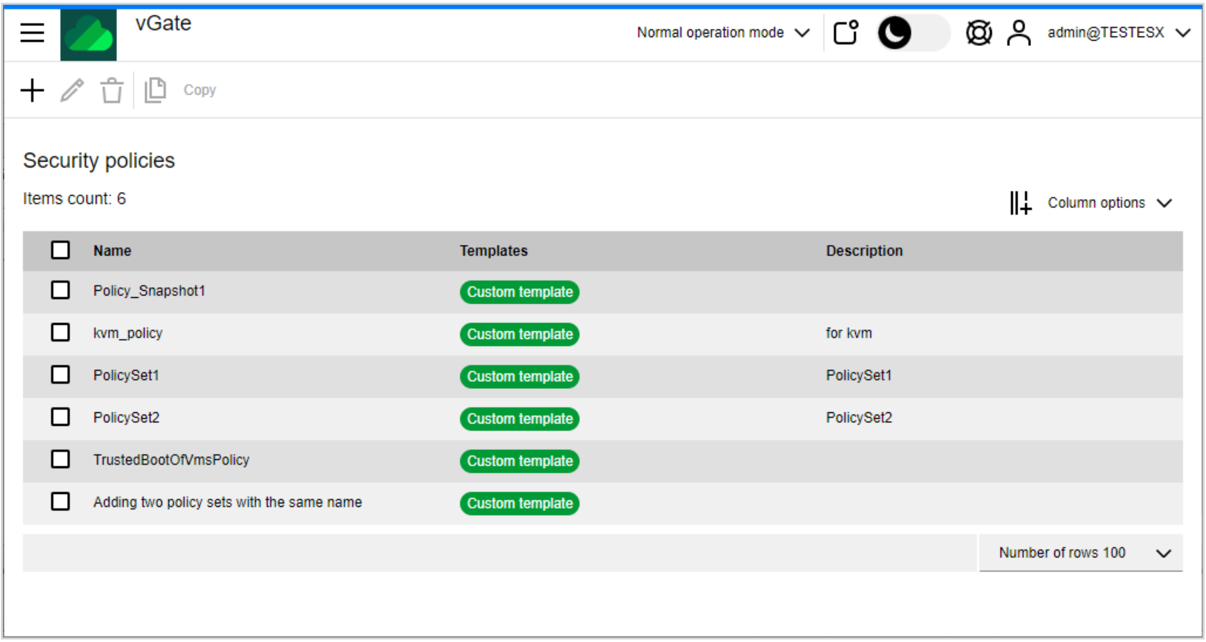
- A policy set is created (see p.95) from a template (see p.98);
- The created policy set is assigned to an object or object group (see p.97).

Creating policy sets

To create a policy set:

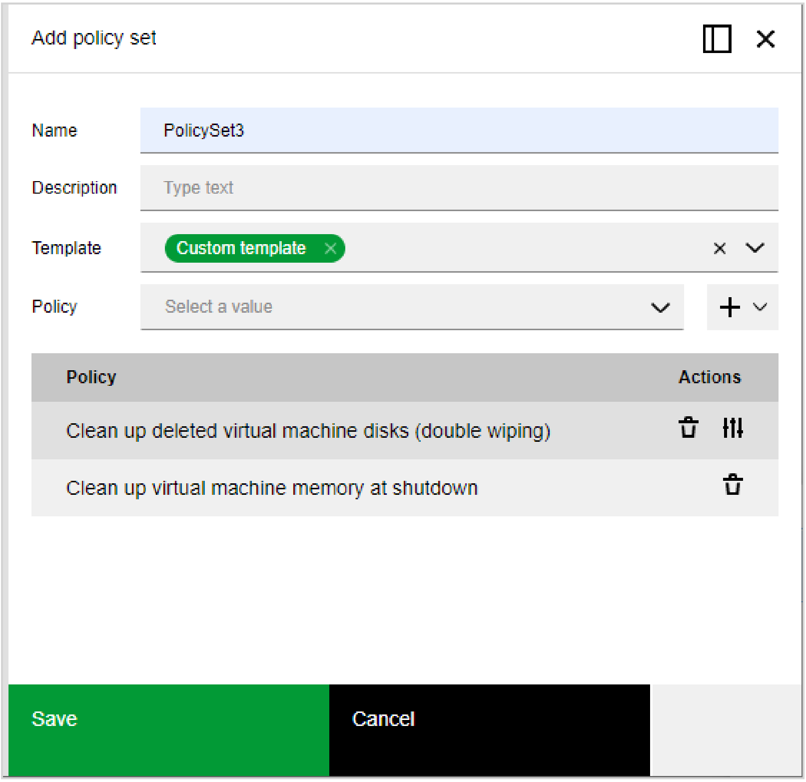
1. In the main menu, go to the "Security policies" section.

   The following window appears.



   Note. To configure the table columns, click "Column options" and select the required options.

2. Click the "Create" button.
   A panel for adding a policy set appears.



3. Specify the policy set name, enter a description (if necessary).
4. To create a new custom policy set, select the required policy from the "Policy" drop-down list and click "Add". The policy appears in the list below. Repeat this action for all policies to be added to the set.

   Note.
   - To add all existing policies to the set, click the "Add all" button.
   - To remove a policy from the set, select the desired policy in the list and click the "Bucket" icon to the right of it.

5. To create a policy set based on an existing template, select the template (see p.**98**). If several standards are selected, a new (combined) set will include all policies from the selected templates. Policies from the template appears in the list below.
6. Edit configurable policies. To do this, select the required policy in the list and click the "Configure" icon to the right of it. In the appeared panel, specify the policy parameters and click "Save".

   Note. Policies that are not configured can be found at the top of the list, and others are sorted in alphabetical order.

7. Once all changes are completed, click the "Save" button.

Note.
- To modify a security policy set, select it in the list and click the "Edit" button.
- Use the "Delete" button to remove a policy set.
- To copy a security policy set, select it in the list and click the "Copy" button.

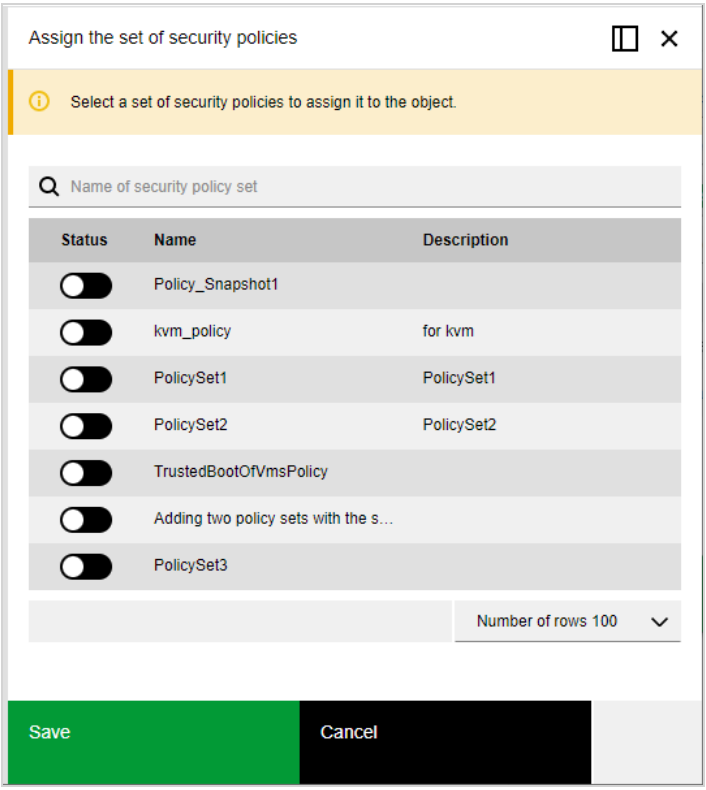
Assigning a policy set to an object or group

To assign a policy set:

1. Go to the "Security configuration of servers", "Virtual machines", "Objects groups", "Container images" or "vSphere network adapters" section and select objects to which you want to assign policies from the list.

   Note. Virtual machine templates are displayed in the "Virtual machine" section.

   Click the "Policies" button and then "Assign". A panel for assigning security policies appears.



   Note. To unassign a policy set, click "Policies" and then "Unassign".

2. Select the required policy sets and click "Save".

   The name of the policy set assigned to the object will be displayed in the "Set of security policies" column.

Note.
- When assigning policies to the ESXi server, checks included in this policy will be performed after a certain period of time. This period is specified on the vGate server in the HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate registry section with the help of the VagentdCheckTimeout parameter (in seconds). By default, the interval value is set to 10 minutes.
- If the settings in the registry have been changed, before installing/reinstalling the vGate agent on the ESXi server, wait a minute or restart the vGate management service (rhuid.exe).

Note.
- You can review policy changes in the "Policy compliance" section.
- You can get information about the status of all policies assigned to protected objects, as well as about errors using the "Compliance with security standards" type of reports (see p.161). Details on an error can be found in the corresponding message of the event log (see p.156).

Policy set templates

Security policies are combined into standard security policy sets (templates).

Security policy set	Description
vGate	A set of policies designed for vGate that allows configuring more secure operation mode of ESXi servers, virtual machines and virtual network switches
vGate for KVM	A set of policies for ensuring protection of KVM servers and virtual machines
vGate for Skala-R	A set of policies for ensuring protection of Skala-R servers and virtual machines
PCI DSS v.3.2	The recommended policy set for ensuring the virtual environment's compliance with the PCI DSS requirements. Requirements and Security Assessment Procedures v3.2
VMware 6.5 SCG	A set of policies for ensuring the virtual environment's compliance with the VMware vSphere 6.5 Security Configuration Guide requirements
VMware 6.7 SCG	A set of policies for ensuring the virtual environment's compliance with the VMware vSphere 6.7 Security Configuration Guide requirements
VMware 7 SCG	A set of policies for ensuring the virtual environment's compliance with the VMware vSphere 7 Security Configuration Guide requirements
CIS for ESXi 6.5	A set of policies for ensuring the virtual environment's compliance with the CIS Security Configuration Benchmark for VMware vSphere (ESXi 6.5) recommendations
CIS for ESXi 6.7	A set of policies for ensuring the virtual environment's compliance with the CIS VMware ESXi 6.7 Benchmark version 1.0.1 recommendations
CIS for ESXi 7.0	A set of policies for ensuring the virtual environment's compliance with the CIS VMware ESXi 7.0 Benchmark recommendations

ESXi server security policies

The following security policies can be assigned to ESXi servers:

Policy	Description
ESXi application whitelist	The policy ensures the trusted ESXi server environment. The list of applications that are allowed to be executed by default is stored on the ESXi server. If necessary, the security administrator can add applications to this list or remove them using the management console
Block USB media at ESXi servers	The policy prevents plugging USB devices in the ESXi server. After enabling this policy, the affected ESXi server must be restarted
Establish and maintain file system integrity	The policy restricts access to service configuration files
Explicitly disable copy/paste operations	The policy disables clipboard operations for each virtual machine. After enabling this policy, virtual machines must be restarted
Ensure that vSphere management traffic is on a restricted network	The policy ensures using different networks for Service Console (or Management vmkernel interface for ESXi server) and virtual machines
Enable bidirectional CHAP, also known as Mutual CHAP, authentication for iSCSI traffic	The policy enables CHAP for authentication when connecting iSCSI devices
Limit VM logging	The policy sets the following logging parameters for each virtual machine: log.rotateSize=100000, log.keepOld=10
Disable virtual disk shrinking	The policy disables virtual disk shrinking for each virtual machine. After enabling this policy, virtual machines must be restarted
Limit sharing of console connections	This policy protects open administrator remote console from other connections. Connection of remote console to only one virtual machine will be allowed. Other requests will be rejected until the first session is closed. After enabling this policy, virtual machines must be restarted

Policy	Description
Do not send host information to guests	The policy disables sending information about ESXi server boot loading to guests, since an adversary could potentially use this information to perform further attacks on the host. After enabling this policy, virtual machines must be restarted
Limit informational messages from the VM to the VMX file	The policy sets the maximum size of the VMX file. Uncontrolled size of the VMX file can lead to denial of service if the datastore is filled. The file is limited to a size of 1MB, this capacity should be sufficient for most cases. After enabling this policy, virtual machines must be restarted
Avoid using independent nonpersistent disks	The policy checks and informs about the usage of independent-nonpersistent disks of virtual machines. After enabling this policy, virtual machines must be restarted
Disable Managed Object Browser (MOB)	The policy restricts the usage of Managed Object Browser
Control access to VMs through VMsafe CPU/memory APIs	If the virtual machine is not protected by products for monitoring of unauthorized usage of the VMsafe CPU/memory APIs, you must control it. The policy checks that this API is disabled and not configured for all virtual machines on the server. If you need to use this API, turn on the "Allow VMsafe API" toggle and specify the IP address and port for accessing the VMsafe CPU/Memory API. In this case, the policy will check and/or apply the specified parameters vmsafe.enable, vmsafe.agentAddress, and vmsafe.agentPort
Control access to VMs through the dvfilter network APIs	If the VM does not need to be protected using dvfilter Network API, make sure that VMX file does not contain records of the type "ethernet0.filter1.name = dv-filter1", where "ethernet0" — VM network adapter, "filter1" – number of the filter, "dv-filter1" — name of the core module that protects this VM. If the VM must be protected, make sure that the name of the core module is correctly specified. After enabling this policy, virtual machines must be restarted
Configure persistent logging for all ESXi host	The policy allows you to specify the path to the log file in the datastore. It ensures that the log cannot be lost while restarting the server
Restrict access to VMsafe Network API	The policy prohibits access to VMsafe Network API
Ensure proper SNMP configuration	The policy allows you to check SNMP agent settings and specify them if necessary. Use ";" as separator to specify multiple societies and receivers of SNMP data
Enable lockdown mode to restrict remote access	Enabling lockdown mode disables direct access to an ESXi host requiring the host be managed remotely from vCenter server. This is done to ensure the roles and access controls implemented in vCenter are always enforced and users cannot bypass them by logging in to a host directly. By forcing all interaction to occur through vCenter Server, the risk of someone inadvertently attaining elevated privileges or performing tasks that are not properly audited is greatly reduced. Lockdown mode does not apply to users who log in using authorized keys. In this case, root users are not prevented from accessing a host via the SSH protocol even when the host is in Lockdown Mode. Note that users listed in the DCUI. Access list for each host are allowed to override Lockdown Mode and login to the DCUI. By default, this list contains only the root user
Disable DCUI to prevent local administrative control	The policy restricts the usage of Direct Console User Interface
Verify no unauthorized kernel modules are loaded on the host	The policy checks loaded kernel modules and informs about the usage of modules that do not have a valid digital signature. The list of unsigned modules that are allowed to be loaded can be adjusted
Disable IPv6	The policy allows you to disable the IPv6 Protocol if it is not used. Once the policy has been applied, the server should be restarted
Prevent unauthorized removal, connection and modification of devices	The policy prohibits monitoring ESXi server devices from within the guest operating system
Configure NTP time synchronization	The policy allows you to configure time synchronization
Configure remote logging for ESXi hosts	The policy allows you to configure logging ESXi server events on the remote syslog server
Clean up virtual machine memory at shutdown	The policy ensures cleaning up the virtual machine memory when the work is over. After enabling this policy, virtual machine must be restarted
Clean up virtual machine memory at shutdown (double wipe)	The policy ensures cleaning up the virtual machine memory when the work is over. To comply with the most strong security requirements this operation is performed twice. After enabling this policy, virtual machine must be restarted

Policy	Description
Ensure that "Forged Transmits", "MAC Address Changes", "Promiscuous Mode" on virtual switches is set to reject	The policy sets the following parameters to reject: "Forged Transmits", "MAC Address Changes", "Promiscuous Mode"
Ensure that port groups are not configured to VLAN 4095 except for Virtual Guest Tagging (VGT)	When a port group is set to VLAN 4095, this activates VGT mode. In this mode, the vSwitch passes all network frames to the guest VM without modifying the VLAN tags, leaving it to the guest to deal with them. VLAN 4095 should be used only if the guest has been specifically configured to manage VLAN tags itself. The policy is assigned to the ESXi server and prohibits setting VLAN value to 4095
Ensure that port groups are not configured to the value of the native VLAN	ESXi servers do not use the native VLAN concept. Frames with VLAN specified in the port group will have a certain tag. Frames with VLAN not specified in the port group are not tagged, and they will be considered belonging to the native VLAN of the physical switch. For example, frames on VLAN 1 from a Cisco physical switch will be untagged, because this is considered the native VLAN. However, frames from ESXi specified as VLAN 1 will be tagged with a "1". Therefore, traffic from ESXi that is destined for the native VLAN will not be correctly routed (because it is tagged with a "1" instead of being untagged), and traffic from the physical switch coming from the native VLAN will not be visible (because it is not tagged). The policy is assigned to the ESXi server and prohibit to use the native VLAN identifier that is specified in the policy settings
Disable tools auto install	The VMware Tools auto install can initiate an automatic reboot of the computer, The policy prohibit automatic installation of VMware Tools and prevent automatic reboot of the computer.
Disable VM Monitor Control	When virtual machines are running on the ESXi server, they are "aware" that they are running in a virtual environment and this information is available for VMware Tools inside the guest OS. This can give attackers information about the platform that they are running on that they may not get from a normal physical server. The policy completely disables all handlers for virtual machines, the guest OS is not aware that it is running in a virtual environment at all
Disable certain unexposed features	Some VMX parameters don't apply on vSphere because VMware virtual machines work on both vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which the guest can affect the host
Disable ESXi Shell unless needed for diagnostics or troubleshooting	ESXi Shell is an interactive command line environment available from the DCUI or remotely via SSH. Access to this mode requires the root password of the server. The ESXi Shell can be turned on and off for individual hosts. Activities performed from the ESXi Shell bypass vCenter RBAC and audit controls. The ESXi shell should only be turned on when needed to troubleshoot/resolve problems that cannot be fixed through the vSphere Web Client, vCLI/PowerCLI or VMware Host Client
Disable SSH	The ESXi shell, when enabled, can be accessed directly from the host console through the DCUI or remotely using SSH. Remote access to the host should be limited to the vSphere Client, remote command-line tools (vCLI/PowerCLI), and through the published APIs. Remote access to the host using SSH should be disabled under normal circumstances
Enable BPDU filter on the ESXi host to prevent being locked out of physical switch ports with Portfast and BPDU Guard enabled	BPDU Guard and Portfast are commonly enabled on the physical switch to which the ESXi host is directly connected to reduce the STP convergence delay. If a BPDU packet is sent from a virtual machine on the ESXi host to the physical switch configured in this way, a cascading lockout of all the uplink interfaces from the ESXi host can occur. To prevent this type of lockout, BPDU Filter can be enabled on the ESXi host to drop any BPDU packets being sent to the physical switch. Note that certain SSL VPNs which use Windows bridging capability can legitimately generate BPDU packets. The administrator should verify that there are no legitimate BPDU packets generated by virtual machines on the ESXi host prior to enabling BPDU Filter. If BPDU Filter is enabled in this situation, enabling Reject Forged Transmits on the virtual switch port group adds protection against Spanning Tree loops
Set a timeout to limit how long the ESXi Shell and SSH services are allowed to run	When the ESXi Shell or SSH services are enabled on a host they will run indefinitely. To avoid having these services left running, set the ESXiShellTimeOut. The ESXiShellTimeOut defines a period of time after which the ESXi Shell and SSH services will automatically be terminated
Set a timeout to automatically terminate idle ESXi Shell and SSH sessions	If a user forgets to log out of their SSH session, the idle connection will remains open indefinitely, increasing the potential for someone to gain privileged access to the host. The ESXiShellInteractiveTimeOut allows you to automatically terminate idle shell sessions

Policy	Description
Set DCUI.Access to allow trusted users to override lockdown mode	Lockdown mode disables direct host access requiring that the administrator manages hosts only from vCenter Server. However, if a host becomes isolated from vCenter Server, the administrator is locked out and can no longer manage the host. If you are using normal lockdown mode, you can avoid becoming locked out of an ESXi host that is running in lockdown mode by setting DCUI. Access to a list of highly trusted users who can override lockdown mode and access the DCUI
Configure a centralized location to collect ESXi host core dumps	When a host crashes, an analysis of the resultant core dump is essential to the ability to identify the cause of the crash and, in turn, find a solution to the problem. If centralizaed dump collecting is configured, memory files are successfully saved and they can be accessed at any time in case of server problems
Remove keys from SSH authorized_keys file	ESXi hosts come with SSH which can be enabled to allow remote access without requiring user authentication. To enable password free access, copy the remote users public key into the "/etc/ssh/keys-root/authorized_keys" file on the ESXi host. The presence of the remote user's public key in the "authorized_keys" file identifies the user as trusted, meaning the user is granted access to the host without providing a password. The restricting access mode does not apply to the root user if this user connects to server using the file that contains authorized keys. In this case, the root user can access ESXi server via SSH even when the server is in the restricting access mode
Verify Image Profile and VIB Acceptance Levels	The policy verifies the ESXi Image Profile to allow only signed VIBs. An unsigned VIB represents untested code installed on an ESXi host. The ESXi Image profile supports four acceptance levels: (1) VMwareCertified - VIBs created, tested and signed by VMware; (2) VMwareAccepted - VIBs created by a VMware partner but tested and signed by VMware; (3) PartnerSupported - VIBs created, tested and signed by a certified VMware partner and (4) CommunitySupported - VIBs that have not been tested by VMware or a VMware partner. Community Supported VIBs are not supported and do not have a digital signature. To protect the security and integrity of your ESXi hosts do not allow unsigned (CommunitySupported) VIBs to be installed on your hosts
Disable VIX messages from the VM	The VIX API is a library for writing scripts and programs to manipulate virtual machines. If you do not make use of custom VIX programming in your environment, then you should consider disabling certain features to reduce the potential for vulnerabilities. The ability to send messages from the VM to the host is one of these features. Note that disabling this feature does NOT adversely affect the functioning of VIX operations that originate outside the guest, so certain VMware and 3rd party solutions that rely upon this capability should continue to work. This interface is outdated. Enabling this option ensures that any legacy interface is disabled for auditing purposes
Disconnect unauthorized devices	The policy ensures that no device is connected to a virtual machine if it is not required. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation. For less commonly used devices that are not required, either the parameter should not be present or its value must be FALSE. Note that the parameters listed are not sufficient to ensure that a device is usable; other required parameters specify how each device is instantiated
Deny access to the virtual machine console via VNC	The VM console allows connecting to VM the same way as connecting to a physical server. The VM console is available via the VNC protocol. To use the VNC protocol, you need to enable firewall rules on each ESXi server where the virtual machine is running
Establish a password policy for password complexity	ESXi uses the pam_passwdqc.so plug-in to set password strength and complexity. It is important to use passwords that are not easily guessed and that are difficult for password generators to determine. Note that there are no limitations for the root user password
Configure the ESXi host firewall to restrict access to services running on the host	Unrestricted access to services running on an ESXi host can expose a host to outside attacks and unauthorized access. Reduce the risk by configuring the ESXi firewall to only allow access from authorized networks. Rules format: "Ruleset Name: 1.1.1.1, 2.2.2.2/24, 3.3.3.3"
Disable all but VGA mode on virtual machines	The policy sets the virtual machine advanced setting of "svga.vgaonly" to TRUE
DCUI timeout value	DCUI is used for directly logging into ESXi host and carrying out host management tasks. The idle connections to DCUI must be terminated to avoid any unintended usage of the DCUI originating from a left-over login session. The UserVars.DcuiTimeOut parameter automatically terminates sessions after the timeout

Policy	Description
Set the time after which a locked account is automatically unlocked	Multiple account login failures for the same account could possibly be a threat vector trying to brute force the system or cause denial of service. Such attempts to brute force the system should be limited by locking out the account (for 900 seconds by default) after reaching a threshold. The policy allows you to increase this value
Set the count of maximum failed login attempts before the account is locked out	Multiple account login failures for the same account could possibly be a threat vector trying to brute force the system or cause denial of service. Such attempts to brute force the system should be limited by locking out the account after reaching a threshold. The default value of login attempts is 10. The policy sets this parameter to 3
Ensure default setting for intra-VM TPS is correct	The policy enables additional security parameters Mem.ShareForceSalting when using the Transparent Page Sharing (TPS) technology. By default, TPS allows virtual machines to share identical memory pages. This policy enables additional check of the sched.mem.pshare.salt parameter in the vmx file to avoid unauthorized access to memory pages. By default, the sched.mem.pshare.salt parameter contains unique vc.uuid values for each VM. Therefore, virtual machines will not share identical memory pages
Check for enablement of salted VM''s that are sharing memory pages	If the Mem.ShareForceSalting parameter is enabled in Transperent Page Sharing, the additional parameter sched.mem.pshare.salt is checked in vmx file. The policy specifies the sched.mem.pshare.salt parameter value, it allows virtual machines to use identical memory pages
Integrity control of the ESXi server configuration files	The policy is intended for tracking unauthorized changes in ESXi server configuration files by monitoring the integrity of these files. The policy is applied to the selected configuration files (sets of files)
Enforce password history	Due to password complexity requirements, users sometimes try to reuse old passwords. This policy allows to set for each user the number of old passwords that will be stored by the system, and prohibit their reuse. The value is from 0 to 100. If the value is 0, passwords are not saved
Use only VIB packages	The policy allows installing ESXi software only using VIB packages. When a system is compromised, the rule makes it harder for attackers to use readymade toolkits and increases the chances of detecting an intrusion
Configure ESXi server logging level	The policy sets the logging level for the ESXi server
Disable 3D graphics in virtual machines	This policy prohibits the use 3D acceleration in virtual machines. This policy applies to all virtual machines of the ESXi server
Disable legacy SSL and TLS protocols	This policy disables the following legacy protocols: SSL v3, TLS v1, TLS v1.1. By default, the ESXi server version 7.0 uses TLS v1.2
Deny access to the guest OS when disabling the remote console	The policy blocks a user's session in the guest operating system of the virtual machine if there are no active remote console sessions. Thus, an attacker will not be able to use open sessions to access the guest OS. This policy applies to all virtual machines of the ESXi server

vSphere VM security policies

The following security policies can be assigned to virtual machines.

Policy	Description
Trusted boot loading of virtual machines	Turns on integrity control and trusted loading mechanisms for virtual machines. Blocks starting VM if its integrity is compromised
List of prohibited devices	Prevents certain devices from being mounted to virtual machines. Controls modifying of already added devices
Disable cloning of virtual machines	Blocks the ability to clone virtual machines
Prohibition of operations with virtual machine snapshots	The policy blocks creating and deleting VM snapshots, as well as reverting to VM snapshots
Deny use of the VM console	The policy blocks access to the VM console

Policy	Description
Clean up deleted virtual machine disks	Wipes the content of virtual disks when the virtual machine is deleted. This operation is performed by writing zero values. This policy is not supported for VM disks that have snapshots. Before deleting a VM, all its snapshots must be deleted
Clean up deleted virtual machine disks (double wiping)	Wipes the content of virtual disks when the virtual machine is deleted. To comply with the most strong security requirements this operation is performed twice. This policy is not supported for VM disks having snapshots. Before deleting a VM, all its snapshots must be deleted

VMware vSphere VM template security policies

The following security policy can be assigned to a virtual machine template.

Policy	Description
Integrity control of virtual machine templates	The policy is intended to prevent unauthorized operations on virtual machine templates by controlling the integrity of virtual machine template configurations and disks

Network adapter security policies

The following security policy can be assigned to a physical network adapter pNIC.

Policy	Description
Prevent mixing various types of network traffic	The policy blocks connection of network port group with the VMKernel type to the virtual switch

Distributed virtual switch security policies

Note. Security policies are assigned to a distributed vSwitch with the help of the clacl.exe utility (see p.186).

The following security policies can be assigned to a distributed vSwitch.

Policy	Description
Ensure that the "MAC Address Changes" policy is set to reject	If the virtual machine operating system changes the MAC address, it can send frames with an impersonated source MAC address at any time. This allows it to stage malicious attacks on the devices in a network by impersonating a network adapter authorized by the receiving network. This will prevent VMs from changing their effective MAC address. It will affect applications that require this functionality. An example of an application like this is Microsoft Clustering, which requires systems to effectively share a MAC address. This will also affect how a layer 2 bridge will operate. This will also affect applications that require a specific MAC address for licensing. An exception should be made for the port group to which these applications are connected
Ensure that the "Forged Transmits" policy is set to reject	If the virtual machine operating system changes the MAC address, it can send frames with an impersonated source MAC address at any time. This allows it to stage malicious attacks on the devices in a network by impersonating a network adapter authorized by the receiving network. By default, the forged transmissions are allowed. This means that dvPortgroup does not compare source and effective MAC addresses. To protect against MAC impersonation, forged transmits must be prohibited on all virtual switches
Ensure that the "Promiscuous Mode" policy is set to reject	When promiscuous mode is enabled for a dvPortgroup, all virtual machines connected to the dvPortgroup have the potential of reading all packets across that network, meaning only the virtual machines connected to that dvPortgroup. Promiscuous mode is disabled by default on the ESXI Server, and this is the recommended setting. However, there might be a legitimate reason to enable it for debugging, monitoring or troubleshooting reasons. Security devices might require the ability to see all packets on a virtual switch. An exception should be made for the dvPortgroups that these applications are connected to, in order to allow for full-time visibility to the traffic on that dvPortgroup. Comparing to the standard virtual switches (vSwitches), dvSwitches allows the promiscuous mode only on the level of port group (dvPortgroup level)

Container image security policies

The following security policy can be assigned to a container image that is stored in the embedded Harbor Registry.

Policy	Description
Integrity control of container images	This policy prohibits an unauthorized running of container images, the integrity of which has been compromised. Integrity control of images is performed by monitoring the invariability of their checksums

KVM VM security policies

The following security policies can be assigned to virtual machines on KVM servers.

Policy	Description
Trusted boot loading of KVM	Turns on integrity control and trusted loading mechanisms for virtual machines on the KVM server. Blocks starting VM if its integrity is compromised
Clean up deleted KVM disks	Wipes the content of virtual disks when the virtual machine on the KVM server is deleted. The operation is performed by writing zero values. The policy is not supported for disks of VM which have snapshots. Before deleting a VM, all its snapshots must be deleted

OpenNebula VM security policies

The following security policies can be assigned to KVM virtual machines on OpenNebula servers:

Policy	Description
Trusted boot loading of OpenNebula	Turns on integrity control and trusted loading mechanisms for virtual machines on the OpenNebula server. Blocks starting VM if its integrity is compromised
Clean up deleted OpenNebula disks	Wipes the content of virtual disks when the virtual machine is deleted. This operation is performed by writing zero values. The policy is not supported for virtual machines which use disks in the Persistent mode. The policy is not supported for disks of VM which have snapshots. Before deleting a VM, all its snapshots must be deleted. For correct operation of the policy, VM must be deleted on a computer with the installed vGate Client. In the rule of access to the virtualization server, to which a user connects, the "Traffic control" parameter must be enabled (see p.**107**)

Proxmox VM security policies

The following security policies can be assigned to KVM virtual machines on Proxmox servers:

Policy	Description
Trusted boot loading of Proxmox	Turns on integrity control and trusted loading mechanisms for virtual machines on the Proxmox server. Blocks starting VM if its integrity is compromised
Clean up deleted Proxmox disks	Wipes the content of virtual disks when the virtual machine is deleted. This operation is performed by writing zero values. The policy is not supported for disks of VM which have snapshots. Before deleting a VM, all its snapshots must be deleted

Skala-R VM security policies

The following security policies can be assigned to virtual machines on Skala-R servers.

Policy	Description
Trusted boot loading of Skala-R	Turns on integrity control and trusted loading mechanisms for virtual machines on the Skala-R server. Blocks starting VM if its integrity is compromised
Clean up deleted Skala-R disks	Wipes the content of virtual disks when the virtual machine is deleted. This operation is performed by writing zero values

vGate server security policies

The following security policies can be assigned to the vGate server.

Policy	Description
Block concurrent sessions of virtual infrastructure administrators	The policy limits the number of concurrent sessions of virtual infrastructure administrator from different workstations. Once this policy is assigned, all concurrent virtual infrastructure administrator sessions are terminated
Password complexity requirements	The policy ensures that the password meets the specified requirements. By default, the policy set the following parameter values: • Maximum password age (days) — 90; • Enforce password history (passwords) — 5; • Minimum password length (characters) — 16; • Minimum number of character types — 4; • Differ from the previous password (characters) — 3; • Lock inactive user accounts after (days) — 45; • Maximum number of &failed logon attempts — 2. Details on the parameters can be found on p.**73**
Session timeout in the web console	The policy allows you to set the time after which an inactive administrator session in the vGate web console will end. The default value is 15 minutes
Audit database backup	The policy allows you to enable and configure backup of the vGate event database to the selected directory on the vGate server when the values of the specified parameters are exceeded. By default, the policy set the following parameter values: • Event retention period (months) — 6; • Maximum database size (MB) — 3072

Policy compliance

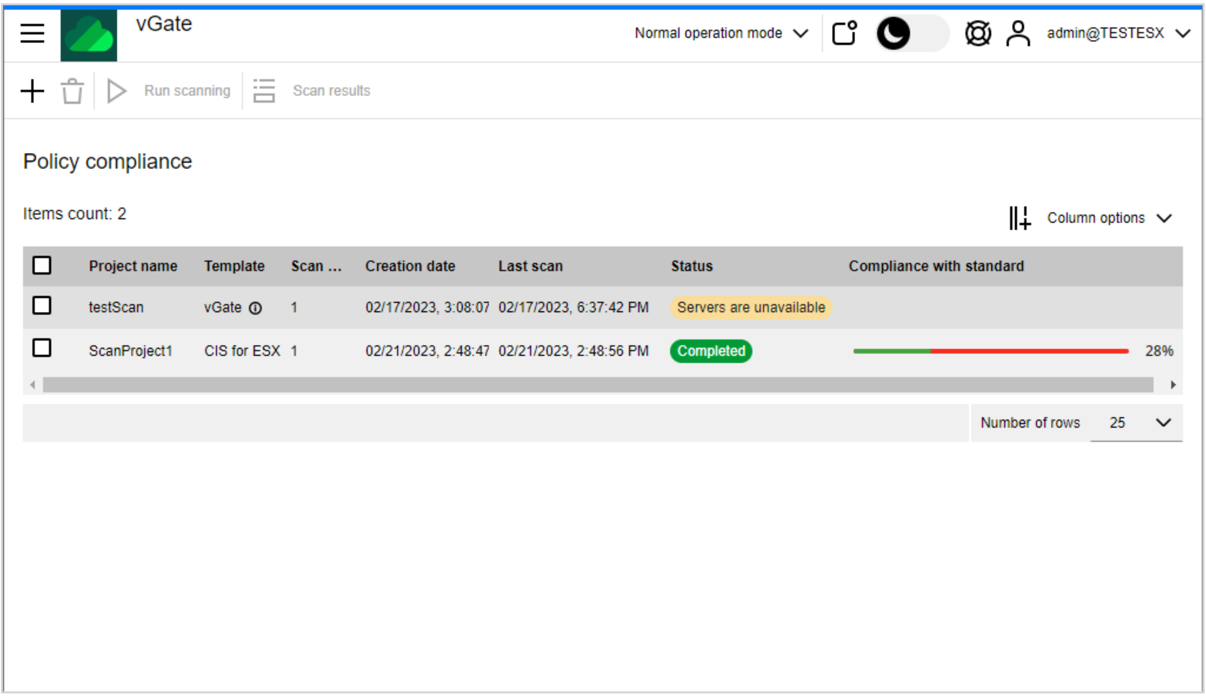
This function is available in vGate Enterprise Plus only (see the "Functionality" section in the document [1]).

vGate allows you to review protected ESXi servers for compliance with security policies. To review servers, create a scan project.

To create a scan project:

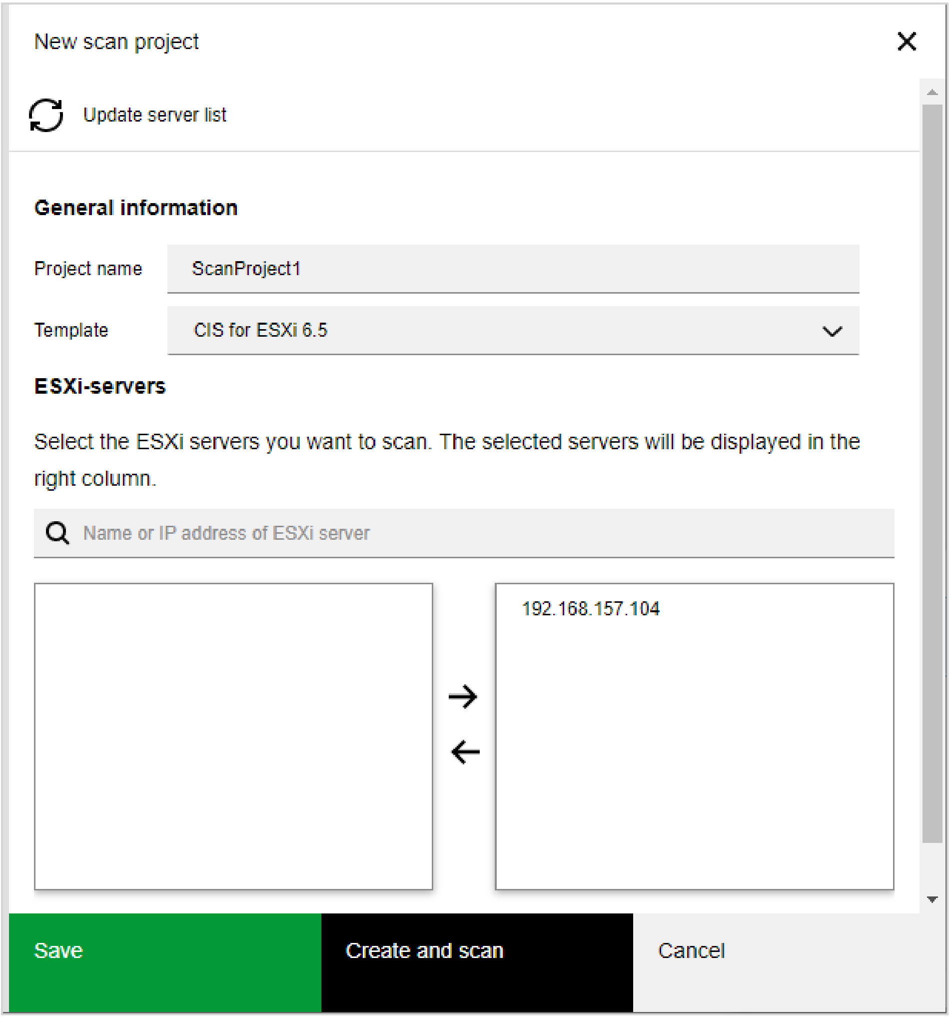
1. In the main menu, go to the "Policy compliance" section.

   The following window appears.



Note. To configure the table columns, click "Column options" and select the required options.

2. Click the "Create" button.
   A panel for creating a scan project appears.



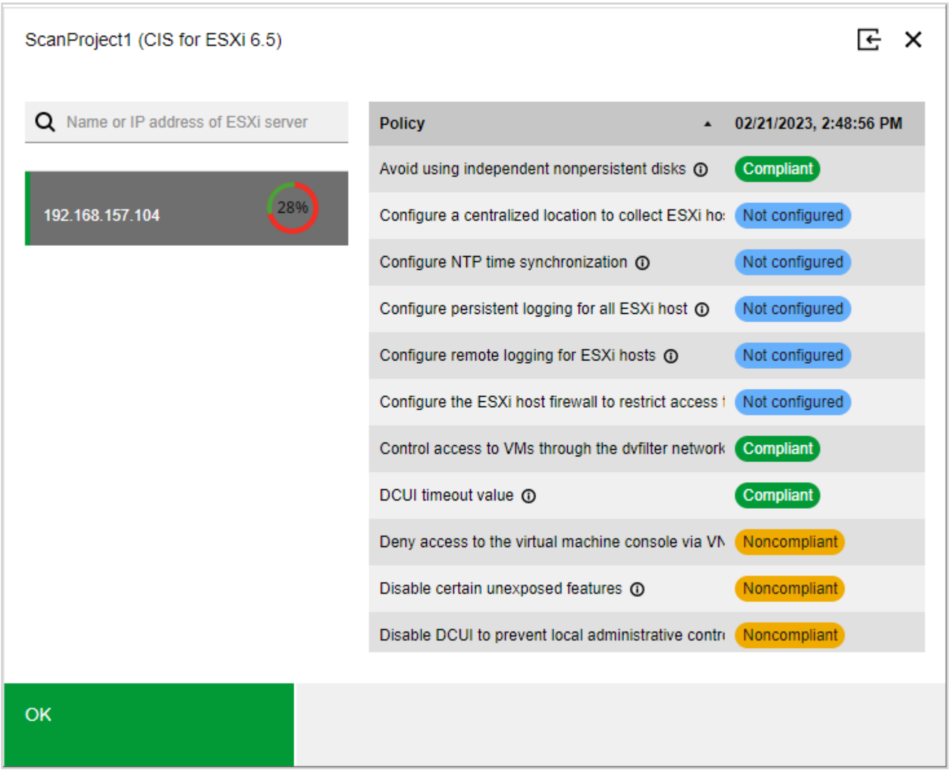
3. Specify the project name and select a template (security policy set) compliance with which will be reviewed.
4. Select ESXi servers to be reviewed for compliance with the specified template, then click → .
5. Click the "Save" button to save the project or click the "Create and scan" to save the project and run scanning.

Note.
- To perform scanning of the saved project, click the "Run scanning" button on the "Policy compliance" page.
- To delete a scan project, select it in the list and click the "Delete" button.

To view the scan results:

1. On the "Policy compliance" page, select the desired scan project in the list.
2. Click the "Scan results" button.

3. A panel containing the report on ESXi servers compliance with security policies appears on the right.



Control of access to protected servers

Before performing this procedure, create the required user and computer accounts whose access to protected objects of the administration network has to be regulated. For this, do the following:

- register vGate users (see p.**87**);
- if necessary, install vGate clients on computers with services that require incoming connections to the secure perimeter to establish authorized access of computer services to protected ESXi servers and other nodes of the secure network.

Attention! Once users are granted access to protected servers, vGate must be switched from test operation mode to normal operation mode (see p.78).

Configuring rules for access to vCenter and vSphere Web Client

To grant the virtual infrastructure administrator access to protected servers after deployment of vGate agents, you must configure access control rules in the vGate web console (see p.**108**).

If you use vSphere Web Client for administering the virtual infrastructure, access control rules based on the following templates should be added to vCenter servers and vSphere Web Client:

- **User access to vCenter**

  The template contains a set of access control rules for granting the virtual infrastructure administrator access to vCenter. The template contains access ports for vCenter that are configured by default (TCP-ports 80, 443, 6501, 6502, 8084, 9084, 9087, 8000, 8001, 6500, 8098, 8099, 8109, 514, 1514). This set of rules should be configured for the vCenter server. The virtual infrastructure administrator account should be specified as the user for which the rules are applied.

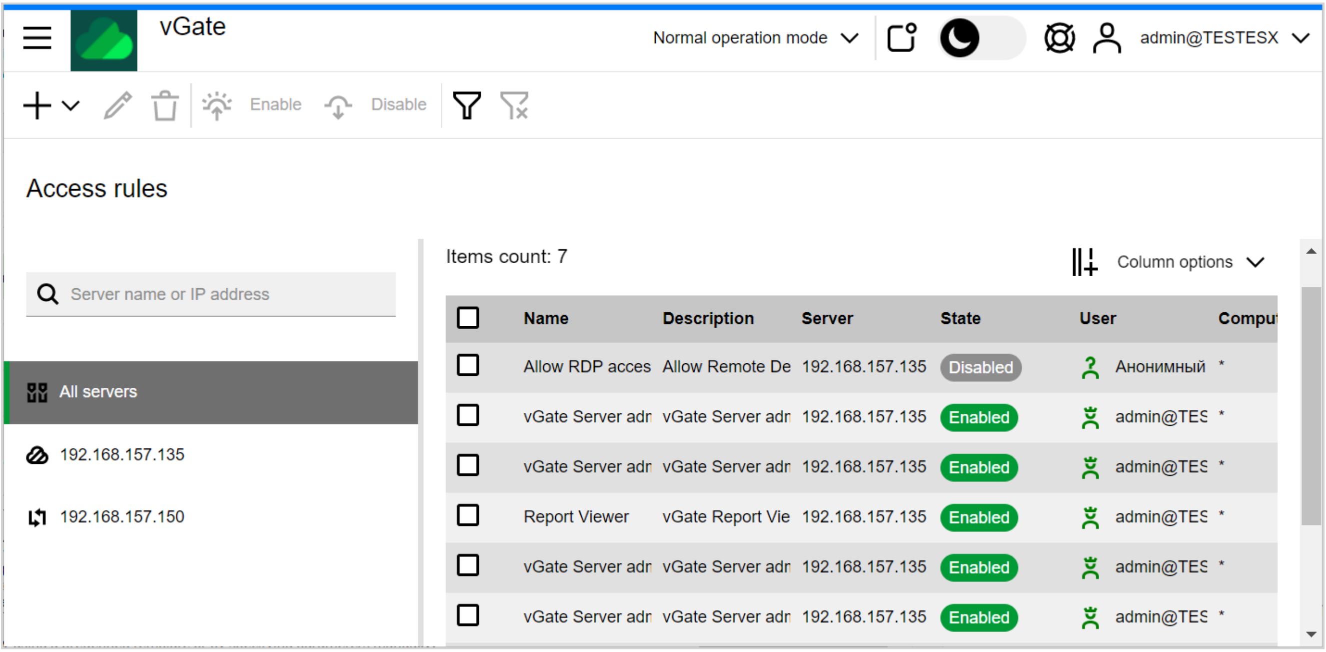
- **User connection using vSphere Web Client v6.x/v7.x**

  The template contains access control rules for granting user access to vCenter using Web Client for vSphere 6.5 and later. For access via the vSphere Web Client protocol, TCP port 443 is specified in the template.

Access rules

To configure access to protected servers, go to the "Access rules" section of the main menu.

The following window appears.



Note.

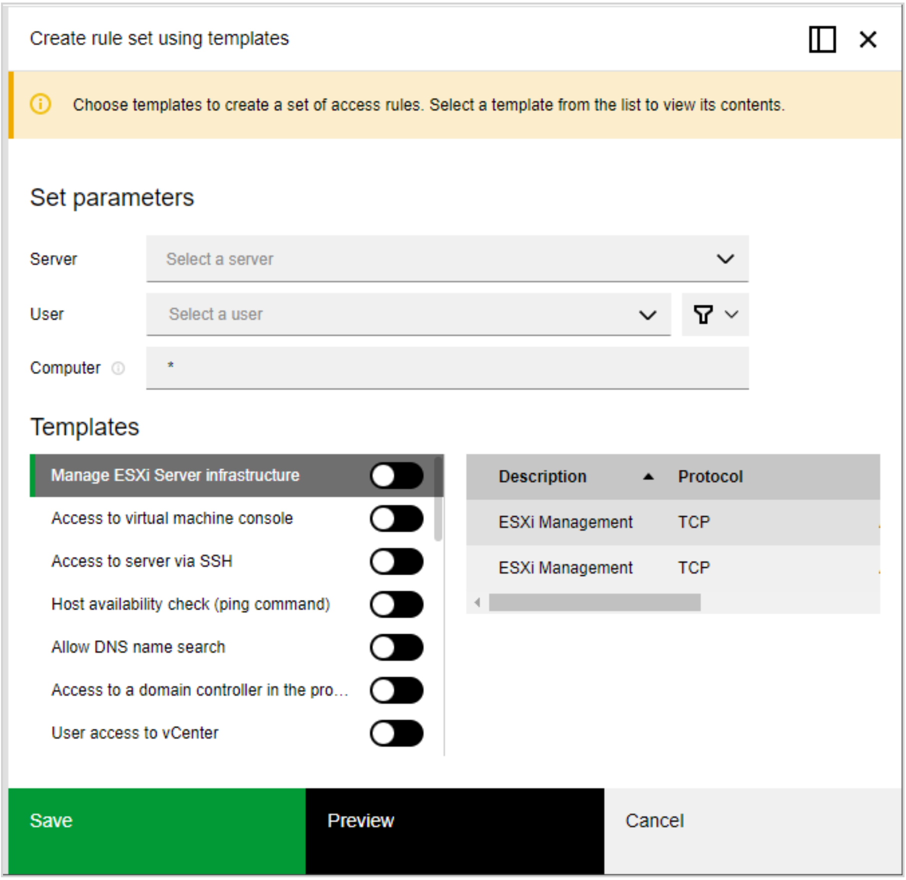
- To configure the table columns, click "Column options" and select the required options.
- To modify the list of access rules, use the "Edit" or "Delete" buttons.
- To manage a rule, use the "Enable" and "Disable" buttons.
- To use filters, click "Filtering", set the required criteria in the appeared panel and click "Apply". To reset the search results, click the "Reset filters" button.

Select the required server in the list on the left. The list of active rules will be displayed in the table. You can create a new rule by using a predefined template or by specifying parameters manually.

To create a set of template-based rules:

1. Click the "Create a rule" button, then select "Use template".

   A panel for creating a rule set using templates configured for control of access to the virtual infrastructure objects appears.



2. Specify the main parameters of the rule set.

Parameter	Description
Server	Protected server to which this rule set will be applied
User	Account of the user or computer to which this rule set will be applied. Only accounts registered in vGate appear in the list. The "Authenticated" value means that rules are active for all user and computer accounts that are registered in vGate or located in the domain which is added to the list of trusted domains on the vGate server. The "Anonymous" value means that no authentication is required for access under such a rule (available only if traffic routing is performed by the vGate server). Rules for anonymous users do not apply to authenticated users
Computer	Computer from which the user has the configured access (not used for a computer account). Valid values: NetBIOS name, DNS name, IP address, "*" (shows that the rule applies to any computer).

3. Select templates for creating the rule set. To do this, turn on the toggle next to a template name.

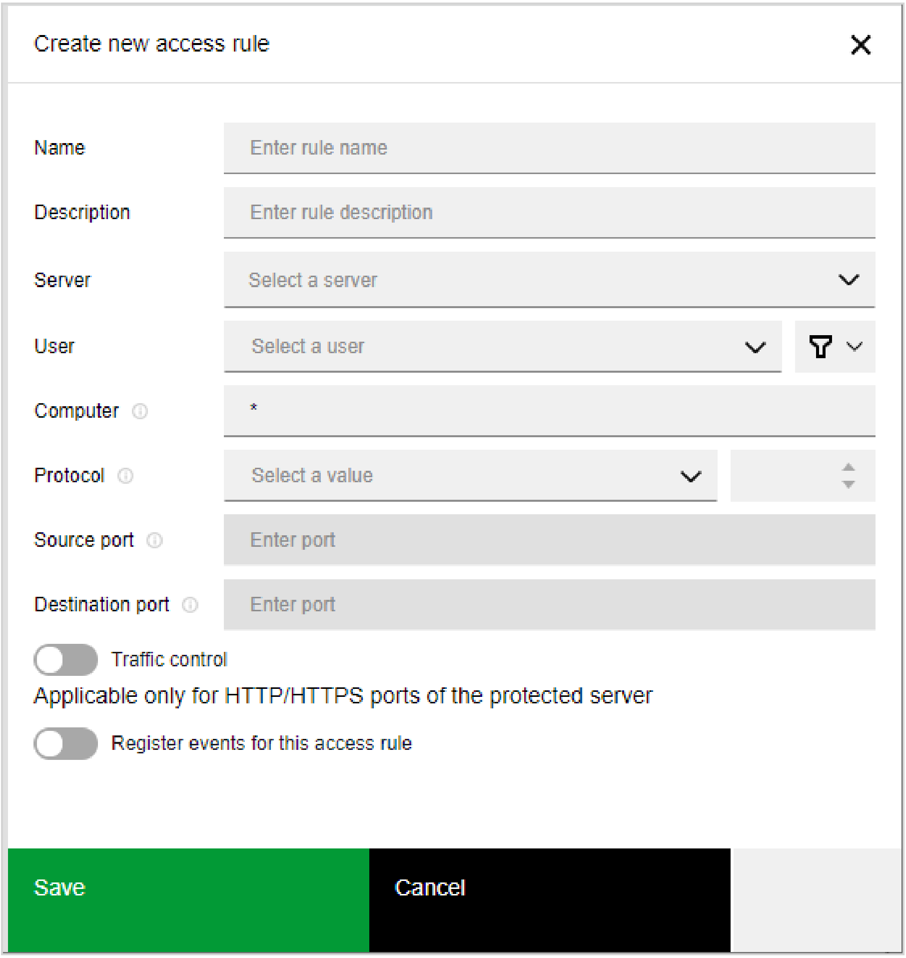
Note. Select a template to view the list of access rules which are included to it. For detailed information about the rules, seep.175.

4. Click "Save".

   Access rules will be added to the list.

To create a new rule:

1. Click the "Create a rule" button and then click "New rule". A panel for creating a new rule appears.



2. Specify the required parameters

Parameter	Description
Name	Rule name
Description	Rule description
Server	Protected server to which this rule will be applied
User	User or computer account to which this rule will be applied
Computer	Computer from which the user has the configured access (not used for a computer account). Valid values: NetBIOS name, DNS name, IP address, "*" (shows that the rule applies to any computer).
Protocol	Type or number of the connection protocol
Source port	Source port. The port number must be between 1 and 65535. To connect by any port, specify the "*" (asterisk) value
Destination port	Destination port. The port number must be between 1 and 65535. To connect by any port, specify the "*" (asterisk) value

Note. If the traffic is routed by a separate switch, anonymous rules can be created using the clacl.exe utility (see p.185).

3. If necessary, turn on the following toggles.

Parameter	Description
Traffic control	HTTPS traffic filtering for the protected vCenter server. vGate proxy service (vcp.exe) will perform the detailed traffic analysis for the vCenter server while traffic is routed through the vGate server
Register events for this access rule	This parameter enables event registration for this access rule

4. Click "Save". The rule will be added to the list.

vCenter traffic filtering

vGate agent, which is installed on the vCenter server, filters the incoming traffic.

By default, once the vGate agent has been installed, all outgoing and only the following incoming connections are always allowed:

- access from the vGate server over TCP and ICMP protocols through all ports;
- access from any computer over the UDP protocol through all ports.

These basic rules for network connection filtering are marked gray in the list, they cannot be removed by the administrator. Besides this, rules for the following connections may be included in the list:

- access from any IP address to the VMware vSphere Update Manager SOAP port (by default, 8084), if the service is installed on vCenter;
- access from any IP address to port 3389 over the RDP protocol, if the remote desktop option is enabled on vCenter;
- access from any computer over the ICMP protocol (ping command).

Attention! If you need to grant access to vCenter from any other direction, add traffic filtering rules in the vGate web console.

The vCenter traffic filtering mechanism is available in the vGate web console.

Note. To create vCenter firewall rules, you can also use the drvmgr.exe utility (see p.189).

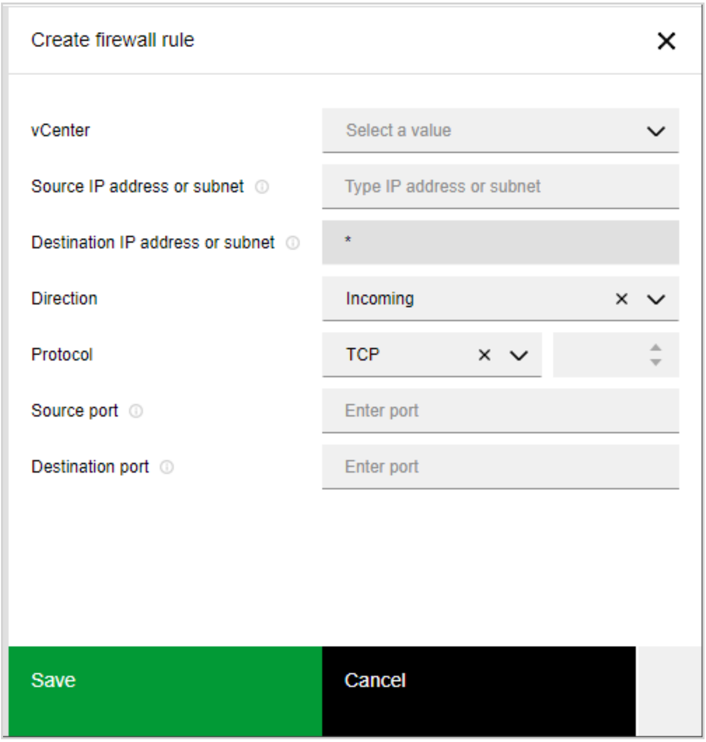
To create a firewall rule:

1. In the main menu, go to the "vCenter traffic filtering" section.
   The list of vCenter servers and their rules appears.
2. Select the vCenter server for which you want to create a firewall rule. The list of active rules for this server appears in the table on the right.

   Note.
   - To configure the table columns, click "Column options" and select the required options.
   - To use filters, click "Filtering", set the required criteria in the appeared panel and click "Apply". To reset the search results, click the "Reset filters" button.
   - To modify the list of firewall rules, use the "Edit" and "Delete" buttons.

3. Click the "Add" button.

A panel for creating a firewall rule appears.



4. Specify the rule parameters.

Parameter	Description
vCenter	Select the required vCenter server in the list
Source IP address or subnet	IP address of the server to be granted access to vCenter or a subnet address if you need to allow incoming connections from all servers in this subnet. The field is active if the incoming traffic direction is selected
Destination IP address or subnet	IP address of the server to which vCenter will be allowed to connect or a subnet address if you need to allow outgoing connections for all servers in this subnet. The field is active if the outgoing traffic direction is selected
Direction	Direction of the network traffic for which the rule is applied (incoming or outgoing)
Protocol	Connection protocol type: TCP, UDP, ICMP or IP-level (IP protocol number on the network level)
Source port	Source port on the server from which connection to vCenter is established. The port number must be between 1 and 65535. To connect by any port, specify the "*" (asterisk) value
Destination port	Target port on the vCenter server. The port number must be between 1 and 65535. To connect by any port, specify the "*" (asterisk) value

5. Click the "Save" button.

The rule will appear in the list.

Rules of access to redundant vGate server

Access rules for the redundant vGate server are configured using the drvmgr.exe utility. To execute the rule creation command, run the utility on the redundant vGate server, open the command prompt and go to the vGate installation folder. Details about the utility can be found on p.**189**.

Example of the rule configuration

```
drvmgr a any any 192.168.1.0:any,255.255.255.0 192.168.1.100:3389 0x206
```

The created rule allows an anonymous user to connect from any server and port in the 192.168.1.0 subnet to the vGate server with the 192.168.1.100 address through port 3389.

Configuring access to virtual infrastructure without vGate client

The virtual infrastructure administrator has access to protected servers via the vGate web interface (without the vGate client). To do this, configure access control rules.

Note. vGate does not support access to the vCenter (vCSA) server with an external PSC without the vGate Client. If there is such a server, we do not recommend configuring access control rules for access via the web interface.

To grant access via the web interface:

1. Configure an access control rule for providing anonymous user access to the protected server (see p.**107**) over the TCP protocol. Set the source port value to "*" (any port) and the destination port value to 443, turn on the "Traffic control" toggle.
2. For the vGate server, configure an access control rule for providing an anonymous user access over the TCP protocol to the port 3900. Set the source port value to "*" (any port).

   Note. The port 3900 value can be changed in the HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate registry section with the help of the WebClientAuthPort parameter. By default, there is no record in registry.
3. If a third-party router is used in the network (see **1**), make sure that the traffic is routed from the virtual infrastructure administrator workstation to the protected server through the vGate server.

   To check this configuration, you can trace the route to the protected server. While checking, packets must be routed through the vGate server.

   Example

```
Tracing route to protected.server [172.24.12.20]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  router [172.24.11.10]
  2     1 ms    <1 ms    <1 ms  vGate.server [172.24.12.10]
  3     1 ms    <1 ms    <1 ms  protected.server [172.24.12.20]

Trace complete.
```

   where:

   - 172.24.11.10 — IP address of the router;
   - 172.24.12.10 — IP address of the vGate server;
   - 172.24.12.20 — IP address of the protected server.
4. Once these rules are applied, the virtual infrastructure administrator is granted access to the protected server.

You can also use the following templates to create access rules.

- **User access to the protected server with authentication via the web interface**

  Contains a rule for providing anonymous user access to ESXi, vCenter, Cloud Director, and other protected servers with authentication via the web interface. This rule allows access over the TCP protocol (HTTPS port 443).
- **Access to the vGate server for user authentication via the web interface**

  Contains rule for providing access to the vGate server for authenticating an anonymous user via the web interface. This rules allows access over the vGate protocol (TCP port 3900).

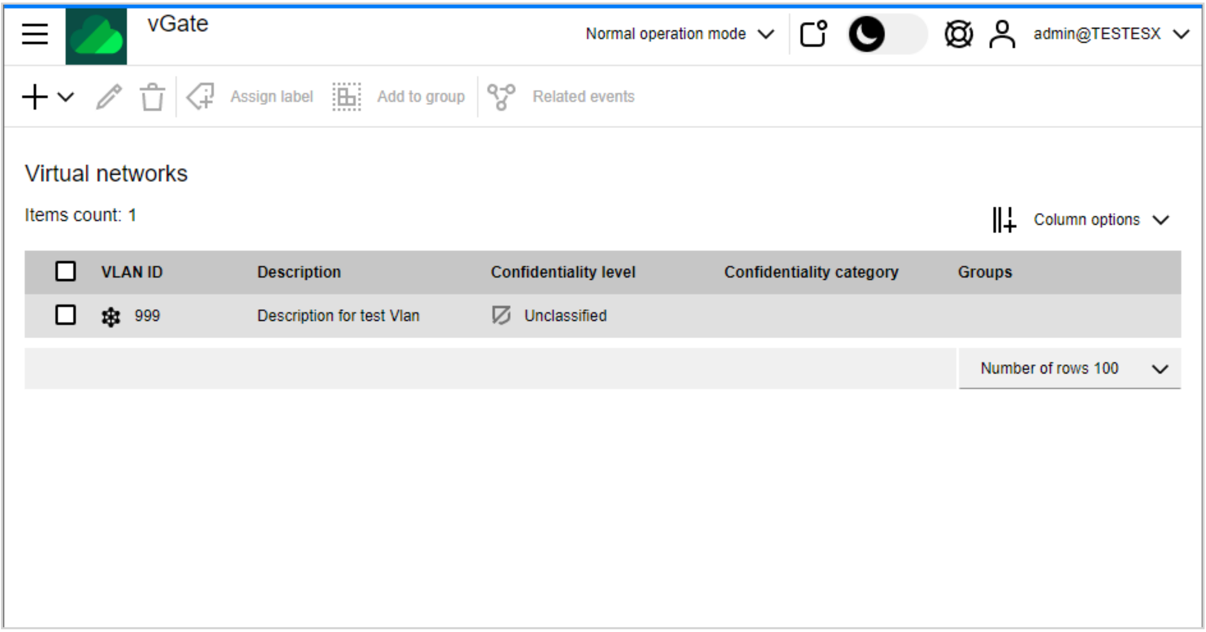
vSphere virtual networks

In the web console, you can manage virtual networks and assign security labels to them (see p.120).

To add a virtual network:

1. In the main menu, go to the "vSphere virtual networks" section.

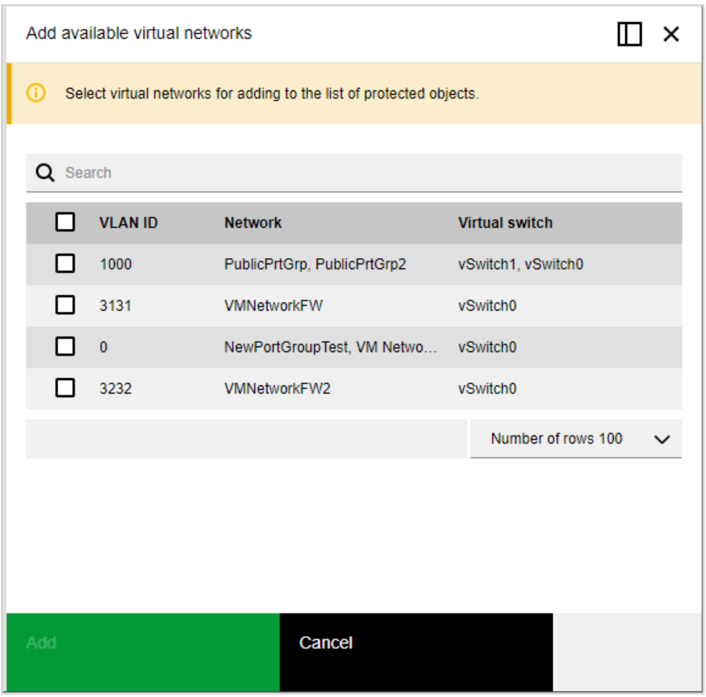
The following window appears.



Note.

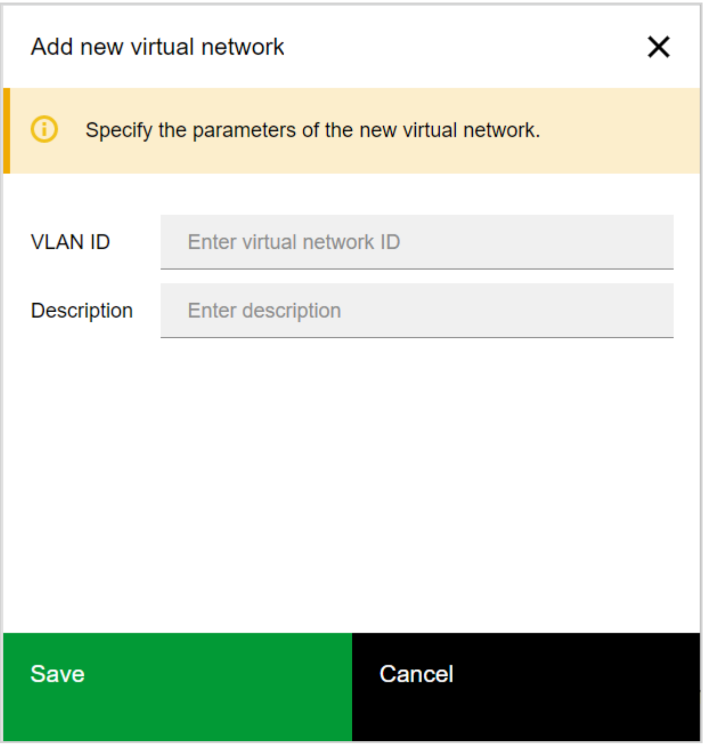
- To configure the table columns, click "Column options" and select the required options.
- To view security events related to a certain virtual network, select it and click "Related events".
- To modify the list of virtual networks, use the "Edit" and "Delete" buttons.

2. Click the "Add" button and choose a virtual network addition method. If the "Available virtual network" option is selected, the following panel appears.



3. To add a network, select it in the list and click the "Add" button. The virtual network appears in the table.

4. If the "New virtual network" option is selected at the step 2, the following panel appears.



To add a new network, specify the network ID and description, then click the "Save" button.

The virtual network appears in the table.

Configuring mandatory control of access to confidential resources

Mandatory access control is configured as follows:

- acceptable security labels are selected and configured (see below);
- access control by the selected type of security labels is enabled (see p.**60**);
- security labels are assigned to user accounts and virtual infrastructure objects (see p.**120**).

Note. Details on configuring the list of object types for which security label matching will be checked can be found on p.77.

Attention! Be careful when assigning labels. If a user or resource has no assigned confidentiality level, the "Unclassified" level is automatically assigned to this object.

Selecting and configuring acceptable security labels

When configuring the mandatory access control mechanism, you should use labels of the same type. Details on label types can be found in the "Mandatory control of access to confidential resources" section in the document [1].

Selection of acceptable security labels depends on the contents of information that is processed in the virtual infrastructure:

- If the virtual infrastructure processes the information classified as a state secret or personal data, hierarchical labels should be used;
- If the virtual infrastructure does **not** process the information classified as a state secret or personal data, non-hierarchical labels should be used.

To ensure more granular control of access to virtual infrastructure objects, you can use compound labels. For example, compound labels can be used to differentiate access to personal data or data that is classified as a state secret that is processed in different company departments.

Attention! Since this method requires a deep understanding of the function's operation logic and taking into account all relations between virtual infrastructure objects, it should be used for specific purposes only.

If non-hierarchical labels are used, enable access control by confidentiality categories (see p.**60**). Besides this, you can adjust the list of acceptable categories for your tasks (details on configuring the list of categories can be found on p.**74**).

Example. You can use titles of different company departments as categories (for example, "Accounting", "Development department", "Sales department", "Management"). This allows restricting personnel access to resources of other departments.

In case of using compound labels, you should configure the matrix of acceptable combinations of confidentiality levels and categories (see p.**77**).

General procedure and rules for assigning security labels in the VMware vSphere environment

Rules and procedure for security label assignment depend on the type of labels in use, as well as on the virtual infrastructure condition:

- new virtual infrastructure: ESXi servers are put into operation, physical network adapters are connected, datastores are configured, but virtual machines are not yet created;
- virtual infrastructure is in use: virtual machines are running on ESXi servers.

Examples of assigning security labels to virtual infrastructure objects are presented on p.**118**.

Rules and procedure for configuring confidentiality levels

When assigning hierarchical labels (confidentiality levels) to virtual infrastructure objects, the following procedure and rules should be followed.

1. Assign a confidentiality level to each virtual infrastructure administrator account in accordance with the level of user access to confidential resources.
2. Assign a confidentiality level to each protected ESXi server in accordance with the confidentiality level of the information that will be processed on it. If you intend to process information of different confidentiality levels on the ESXi server:
   - turn on the "Allowed to run VM with a lower confidentiality level" toggle;
   - assign the confidentiality level to the ESXi server that matches the maximum confidentiality level of the information that is processed on it.
3. Assign a confidentiality level to each physical network adapter of the ESXi server. Confidentiality level of each physical network adapter of the ESXi server must not be higher that the confidentiality level of that server. If traffic from virtual networks having different confidentiality levels is intended to pass through a single physical network adapter, turn on the "Traffic is allowed for VLAN with a lower level" toggle.

   Note. The function operation scenario of mixing traffic from virtual networks having different confidentiality levels on the physical adapter is considered to be less secure.
4. If you intend to use virtual networks (VLAN), add them to the list of virtual networks in the web console (see p.**114**) and assign a confidentiality level to each of them. The VLAN confidentiality level should be:
   - not higher than the confidentiality level of the physical network adapter to which this VLAN is connected (if the "Traffic is allowed for VLAN with a lower level" option is enabled);
   - equal to the confidentiality level of the physical network adapter to which it is connected (if the "Traffic is allowed for VLAN with a lower level" option is disabled).

   If the confidentiality level of the physical network adapter is other than "Unclassified" and VLAN is not intended to be used:
   - add VLAN with ID=0 to the list of virtual networks (in the web console);
   - assign a confidentiality level to the added VLAN that is equal to the confidentiality level of the physical network adapter.
5. Assign a confidentiality level to each VM datastore in accordance with the confidentiality level of the information that will be stored on it. If you intend to store data with different confidentiality levels in the datastore:
   - turn on the "Allowed to store VM with the lower level" toggle;
   - assign the confidentiality level to the datastore that matches the maximum confidentiality level of the information that is stored on it.

   If you are assigning confidentiality levels to objects of the new virtual infrastructure, the procedure is completed. New virtual machines will receive confidentiality labels automatically when being created. At the same time, virtual machine is assigned the confidentiality level of the datastore where VM files are located. If you are assigning confidentiality levels to objects of an existing virtual infrastructure, go to step **6**.

6. Assign confidentiality levels to all existing virtual machines. The VM confidentiality level should be as follows:
   - not higher than the confidentiality level of the ESXi server where it is running (if the "Allowed to run VM with a lower confidentiality level" option is enabled), or equal to the ESXi server level (if the option is disabled);
   - not higher than the confidentiality level of the datastore where VM files are stored (if the "Allowed to store VM with the lower level" option is enabled), or equal to the datastore confidentiality level (if the option is disabled);

   If you plan to move the VM to another ESXi server, the VM confidentiality level should be no higher than the ESXi server confidentiality level. If the VM is connected to several networks, turn on the "Can connect to networks with a lower level".

   Tip. When performing operations with virtual machines, you can choose from two VM display options: as a list or as a tree that corresponds to the hierarchy of vSphere virtual infrastructure. Use link buttons "List" and "Hierarchy" to switch between the modes.

Note. When creating a new VM with several network adapters, correspondence between confidentiality levels of the VM, network adapters, VLAN and datastores is reviewed. Therefore, when creating a VM with several network adapters, at first, we recommend creating a VM without network adapters, and then creating network adapters with the required confidentiality levels.

In the process of the further virtual infrastructure operation, the security administrator should in a timely manner assign confidentiality levels to new objects that are introduced into the virtual infrastructure (ESXi servers, VM datastores, physical network adapters, virtual networks), as well as to new user accounts.

Note. When performing migration (on the vGate server) of the running virtual machine to the ESXi server with a lower confidentiality level, the process hangs in vSphere.

Rules for assigning confidentiality categories

When assigning non-hierarchical labels (confidentiality categories) to virtual infrastructure objects, the following procedure and rules should be followed.

1. Assign a confidentiality category to each virtual infrastructure administrator account in accordance with the level of user access to certain categories of resources. Each user can be granted access to one or several categories of resources.
2. Assign one or several confidentiality categories to each of the protected ESXi servers in accordance with the confidentiality category of the information that will be processed on them. If data of different categories will be processed on ESXi server, set the list of these categories.
3. Assign a confidentiality category to each physical network adapter of the ESXi server. Note that the list of categories for each physical network adapter must have at least one shared category with the ESXi server list of categories.
4. If you intend to use virtual networks (VLAN), add them to the list of virtual networks in the web console and assign confidentiality categories to each of them in accordance with the confidentiality category of the information that is transferred in it. Note that the list of categories for each virtual network must have at least one shared category with the list of categories of the physical network adapter.
5. Assign confidentiality categories to each of VM datastores that should be equal to the confidentiality categories of the information that is stored on them. Note that the list of the datastore confidentiality categories must include at least one shared category with the list of categories of each of ESXi servers.

   If you are assigning confidentiality categories to new virtual infrastructure objects, the procedure is completed. New virtual machines will receive confidentiality labels automatically when being created. Note that VM is assigned a category from the list of categories of the datastore that is equal to the category from the list of categories of the user who is creating VM. If there are several of them, the list of categories is assigned to VM. If you are assigning confidentiality categories to objects of an existing virtual infrastructure, go to step **6**.
6. Assign confidentiality categories to all existing virtual machines. The list of VM confidentiality categories must include at least one shared category with:
   - the list of categories of the ESXi server on which it is running;
   - the list of categories of the datastore where VM files are stored.

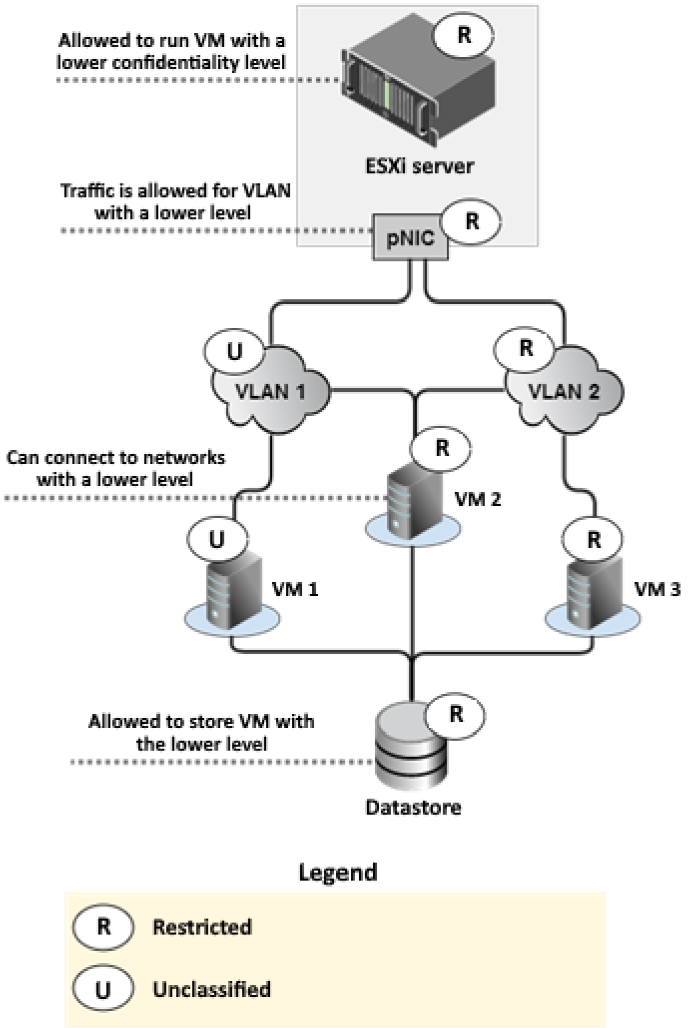
Note. When creating a new VM with several network adapters, correspondence between confidentiality categories of VM, network adapters, VLAN and datastores is reviewed. Therefore, at first, we recommend creating a VM without network adapters, and then creating network adapters with the required confidentiality categories.

In the process of further operation of the virtual infrastructure, the security administrator should in a timely manner assign confidentiality categories to new objects that are introduced into the virtual infrastructure (ESXi servers, VM datastores, physical network adapters, virtual networks), as well as to new user accounts.

Examples of assigning security labels to virtual infrastructure objects

Example 1. Using confidentiality levels

An example of assigning confidentiality levels to virtual infrastructure objects is presented in the figure below.



In Example 1, the ESXi server is used for the processing of both unclassified and restricted data. Therefore, the ESXi server is assigned the "Restricted" confidentiality level and the "Allowed to run VM with a lower confidentiality level" option is enabled.

The ESXi server has a physical network adapter - pNIC with the "Restricted" confidentiality level that is connected to both VLAN 1 and VLAN 2. VLAN 1 has the "Unclassified" confidentiality level, VLAN 2 has the "Restricted" confidentiality level. Therefore, the additional "Traffic is allowed for VLAN with a lower level" option is enabled.

Three virtual machines are running on the ESXi server:

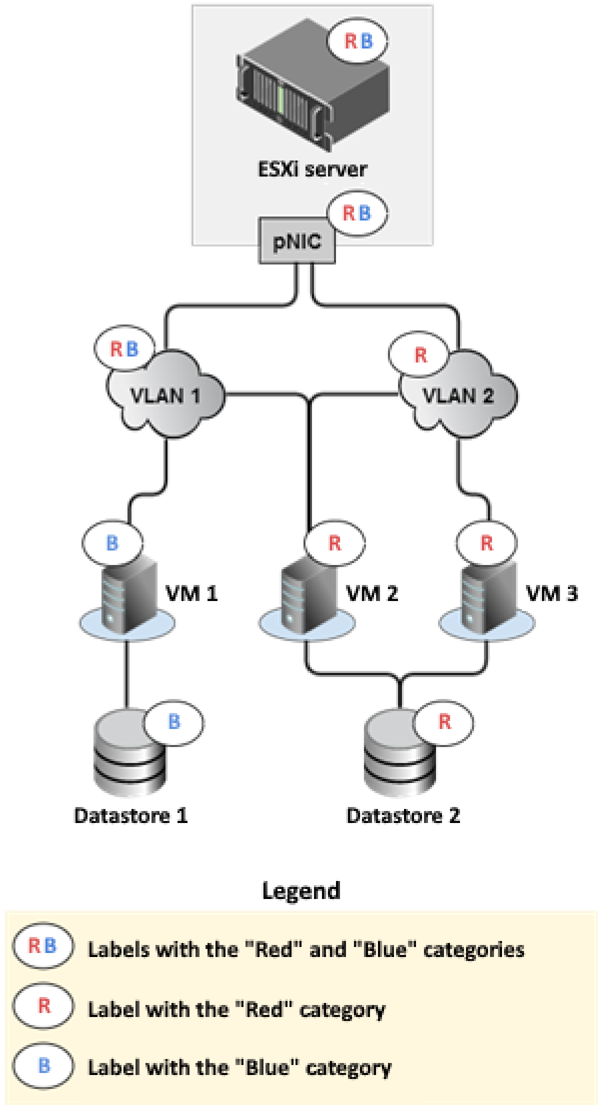
- unclassified information is stored on VM 1;
- VM 2 is a third-party firewall that isolates access between networks of different confidentiality levels.
- restricted information is stored on VM 3.

VM 1 and VM 3 are assigned confidentiality levels in accordance with the level of information that is stored on them ("Unclassified" and "Restricted" respectively). VM 2 is assigned the confidentiality level that corresponds to the maximum confidentiality level of the information that is stored on it, i.e. "Restricted". Besides this, the additional "Can connect to networks with a lower level" option is enabled for VM 2.

VM files are stored in the datastore with the "Restricted" confidentiality level. Since the datastore contains VM files with different confidentiality levels, the additional "Allowed to store VM with the lower level" option is enabled for the datastore.

Example 2. Using confidentiality categories

An example of assigning confidentiality categories to virtual infrastructure objects is presented in the figure below.



In Example 2, the ESXi server is used to process the data with the "Blue" and "Red" categories.

The ESXi server has a physical network adapter - pNIC that is connected to both VLAN 1 and VLAN 2. Data of the "Blue" and "Red" categories is processed in VLAN 1, while only the "Red" category of data is processed in VLAN 2. Therefore, the list of "Blue" and "Red" categories is assigned to pNIC and VLAN 1, while the "Red" confidentiality category is assigned to VLAN 2.

Three virtual machines are running on the ESXi server:

- data of the "Blue" category is contained on VM 1;
- VM 2 is a third-party firewall that isolates access between the networks of different confidentiality categories and contains information of the "Red" category.
- data of the "Red" category is stored on VM 3.

Two datastores are used to store files of different confidentiality categories: Datastore 1 with the "Blue" confidentiality category and Datastore 2 with the "Red" confidentiality category.

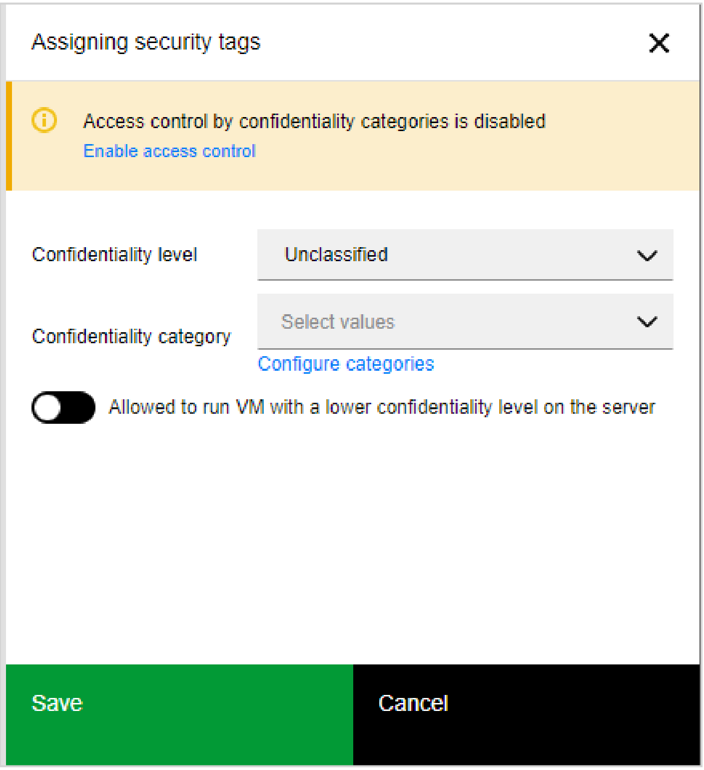
Assigning security labels

Attention! Before assigning security labels to virtual networks, they must be added to the list in the web console (see p.114).

To assign security labels:

1. In the web console, select an object to which you want to assign a security label and click the "Assign label" button.

   A panel for assigning security labels appears.



2. Select the desired confidentiality level and confidentiality category. To enable access control by confidentiality categories and levels, click the "Enable access control" link button.

   Note. To modify the list of confidentiality categories or the list of confidentiality levels, as well as their combinations and object types, click the "Configure categories" link button (see p.74).

3. If necessary, configure additional parameters that are given below. Click the "Save" button.

Parameter	Description
Allowed to run VM with a lower confidentiality level	Additional parameter for virtualization servers
Allowed to store VM with the lower level	Additional parameter for storage units
Can connect to networks with a lower level	Additional parameter for VM
Traffic is allowed for VLAN with a lower level	Additional parameter for physical network adapter
Access to objects with a lower level is allowed	Additional parameter for objects groups

Attention! Additional parameters are taken into account only if confidentiality levels are used the mandatory access control configuration.

Configuring mandatory access control exceptions

vGate allows configuring exceptions from mandatory access control for certain object types of the virtual infrastructure. Objects for which access control based on security labels is not required must be added to the list of exceptions using the clacl.exe utility.

Creating a list of exceptions

Open the command prompt and run the following command:

```
clacl.exe smarkers set-trumps –t <object types> -k admin -s pAsswor1d
```

where:

- **<object type>** — type of the virtual infrastructure object, for which the exception is being configured:
  - **A** — network adapter;
  - **B** — Skala-R storage;
  - **C** — vCenter;
  - **D** — DVSwitch;
  - **E** — ESXi server;
  - **F** — OpenNebula virtual machine;
  - **G** — object group;
  - **K** — KVM server;
  - **L** — Skala-R virtual machine;
  - **N** — virtual network;
  - **O** — Cloud Director organization;
  - **S** — storage;
  - **U** — user;
  - **V** — virtual machine;
  - **X** — Proxmox virtual machine.
- **admin** — security administrator name;
- **pAsswor1d** — security administrator password.

Example

```
clacl.exe smarkers set-trumps –t ADN -k admin@VGATE -s 1
```

Viewing the current list of exceptions

Open the command prompt and run the following command:

```
clacl.exe smarkers get-trumps -k admin -s pAsswor1d
```

where:

- **admin** — security administrator name;
- **pAsswor1d** — security administrator password.

Example

```
clacl.exe smarkers get-trumps -k admin@VGATE -s 1
Network Adapter, VLAN, DVSwitch
Done.
```

Clearing the list of exceptions

Open the command prompt and run the following command:

```
clacl.exe smarkers set-trumps -t "" -k admin -s pAsswor1d
```

where:

- **admin** — security administrator name;
- **pAsswor1d** — security administrator password.

Example

```
clacl.exe smarkers set-trumps -t "" -k admin@VGATE -s 1
```

Access to VM console

Access to a VM console can be granted or prohibited on an individual basis for each user registered in the vGate web console.

Access is regulated as follows:

- by the "Virtual machine user" account property (see p.87);
- by the "Deny use of the VM console" security policy (see p.95);
- by the mandatory access control mechanism.

The "Virtual machine user" property is assigned to a user by default. It allows using console on all virtual machines. This access permission can be removed by the security administrator when creating or editing the user account in the account properties dialog box (p.87).

The security administrator can prohibit using the console on specific virtual machines for all users. The "Deny use of the VM console" (see p.102) security policy from the "vGate" template is designed for this purpose. If this policy is assigned to a VM, user access to the VM console will not be allowed even if the "Virtual machine user" property is assigned to this user.

If a user attempts to access the VM console using VMware Remote Console, the user session level compliance with the VM confidentiality level is reviewed, the user privileges is also checked. The VM confidentiality level should not be higher than the user session level. Otherwise, access to the VM console will be prohibited.

When accessing a VM console via the web console (browser), only user privileges are controlled.

Examples of configuring access to VM console

1. The user has the "Virtual machine user" access right, and the "Deny use of the VM console" policy is not assigned to the VM.

   If the user attempts to access the VM console, the console will be opened.

2. The user has the "Virtual machine user" access right, and the "Deny use of the VM console" policy is assigned to the VM.

   If the user attempts to access the VM console, the console will not be opened. Message informing that vGate blocked the operation due to violation of security policies.

3. The user does not have the "Virtual machine user" access right, and the "Deny use of the VM console" policy is assigned to the VM.

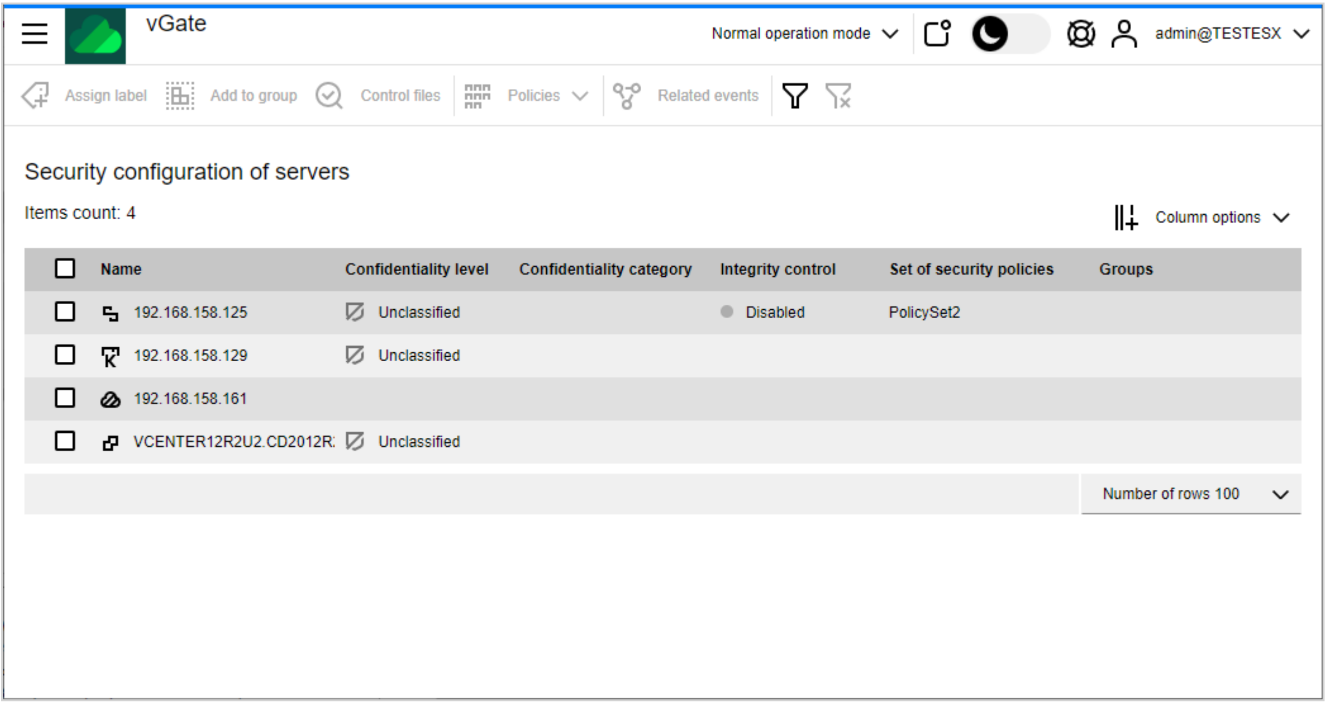
   If the user attempts to access the VM console, the console will not be opened. Message informing that vGate blocked the operation due to insufficient privileges.

4. The user does not have the "Virtual machine user" access right, and the "Deny use of the VM console" policy is not assigned to the VM.

   If the user attempts to access the VM console, the console will not be opened. Message informing that vGate blocked the operation due to insufficient privileges.

Security configuration of servers

The following functions are available on this page: management of security policies, mandatory access control, integrity control of protected servers.



Note.

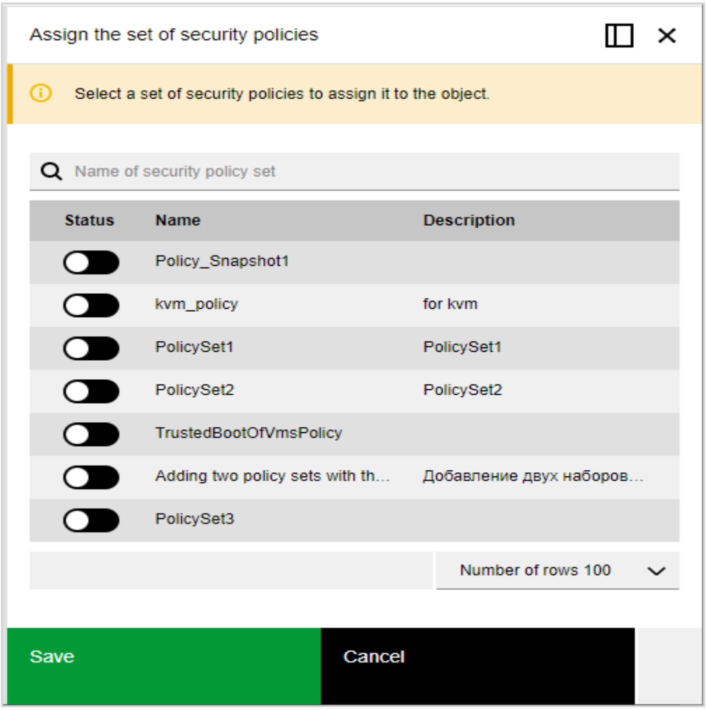
- To configure the table columns, click "Column options" and select the required options.
- To use filters, click "Filtering", set the required criteria in the appeared panel and click "Apply". To reset the search results, click the "Reset filters" button.
- To view security events related to a certain server, select the server and click "Related events".

To assign security labels, on the "Security configuration of servers" page select the required server and click the "Assign label" button (see p.**120**).

To assign security policies:

1. Select the required server and click the "Policies" button. Select "Assign" from the drop-down list.

   A panel for assigning security policies appears.



2. Turn on toggles for security policy sets that you want to assign to the object, then click "Save".

> **Note.** To create a new security policy set, go to the "Security policies" section (seep.95).

3. To apply the assigned policies, select the required server and click the "Policies" button, then select "Apply" from the drop-down list.

To confirm integrity:

1. Select a virtualization server whose configuration changes needed to be approved, then click the "Control files" button.

> **Note.** Integrity control is performed for protected ESXi servers and vCSA servers to which the "Integrity control of ESXi server configuration files" and "Integrity control of vCSA configuration files" policies are assigned.

2. A panel for approving the configuration changes appears. It contains the information about files that have been changed. Click the "Accept" button to confirm integrity.

Integrity control

Integrity control is performed only for objects to which one of the following policies is assigned (see p.95):

- Trusted boot loading of virtual machines;
- Trusted boot loading of KVM;
- Trusted boot loading of Proxmox;
- Trusted boot loading of OpenNebula;
- Trusted boot loading of Skala-R;
- Integrity control of virtual machine templates;
- Integrity control of ESXi server configuration files;
- Integrity control of container images.

Objects and methods of control

In vGate, the integrity control function is used to protect the following objects on the vGate server, protected virtualization servers and the virtual infrastructure administrator and security administrator workstations.

Component	Object of control	Parameters and methods of control
vGate Server	vGate run units	The following parameters are reviewed periodically: • integrity of the template file with checksums; • integrity of the full name of each file specified in the template; • integrity of the data in each file specified in the template. Events of integrity violation on the vGate server are registered in the vGate database. The check interval is set in seconds in the Windows registry, HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate\InchInterval key for 64-bit Windows. By default, the interval value is set to 600 seconds. In case of the vGate server integrity violation, vGate authentication service (aupa.exe) and vGate proxy service (vcp.exe) are stopped
vGate Client	vGate run units	Parameters of control are the same as parameters on the vGate server. Events of integrity violation are registered in the Windows Application Event Log on the workstation. In case of the vGate client integrity violation, vGate authentication service (aupa.exe) on the workstation is stopped
vCenter server	vGate run units	Parameters of control are the same as parameters on the vGate server, except for stopping the vGate authentication service (aupa.exe) in case of integrity violation
vCSA	Configuration files	vCSA configuration files are controlled. Control of the following files is supported: • VMware files; • /bin, /lib, /usr/lib directory files. Checksums are reviewed every 10 minutes, on a user request or when the following operations are performed with vCSA: • Power On; • Shut Down; • Suspend; • Reset

Component	Object of control	Parameters and methods of control
ESXi server	VM files	Controlled: • *.vmx is the main VM configuration file; • *.nvram is the BIOS configuration file (bin file) • *.vmsd is the configuration file of VM snapshots. The list of controlled files and VMX file parameters are configured in the "Trusted boot loading of virtual machines" policy (see p.**127**). Integrity is checked when starting a VM, and after a predefined time interval by the vGate agent (vagentd) service on the ESXi server. File checksums are stored centrally in the database for each virtual machine. Interval is specified on the ESXi server in the /etc/config/vgate/vgate.cfg configuration file, vagentd section, interval parameter (in seconds). By default, the interval value is set to 600 seconds
	VM template files	Controlled: • *.vmtx is the VM template file; • *.nvram is the BIOS configuration file (bin file) • *.vmdk is the template virtual disk image file; • *flat.vmdk it the VM data file. The list of controlled files and file parameters are configured in the "Integrity control of virtual machine templates" policy (see p.**127**). Integrity is checked after a predefined time interval by the vGate agent (vagentd) service on the ESXi server. File checksums are stored centrally in the database for each virtual machine template. The time interval is specified on the vGate server in the HKEY_LOCAL_ MACHINE\SOFTWARE\Security Code\vGate registry section with the help of the VagentdCheckTimeout parameter (in seconds). By default, the interval value is set to 1800 seconds. If the settings in the registry were changed, before installing/reinstalling the vGate agent on the ESXi server, wait a minute or restart the vGate management service (rhuid.exe).
	Configuration files	ESXi server configuration files are controlled. Control of the following files is supported: • boot sectors; • boot loader configuration files; • initial boot image • network configuration files; • OS control files; • /bin, /lib, /usr/lib directory files; • SSH files; • time configuration files; • certificates; • user record files. Checksums are reviewed every 10 minutes, on a user request or when the following operations are performed with the ESXi server: Power On, Shut Down, Reboot, Enter Standby Mode
Embedded Harbor Registry	Container image	Container image files that are stored in the embedded Harbor Registry are controlled
KVM server	VM files	The main VM configuration file is controlled
Proxmox server	VM files	The main VM configuration file is controlled
OpenNebula server	VM files	The main VM configuration file is controlled
Skala-R server	VM files	The main VM configuration file is controlled. The list of parameters is configured in the "Trusted boot loading of Skala-R" policy

Configuring ESXi VM integrity control

Attention! We do not recommend enabling integrity control on the vGate server for more than 500 virtual machines at the same time.

Integrity control is applied only to those virtual machines to which the "Trusted boot loading of virtual machines" policy is assigned.

Configuring objects of control

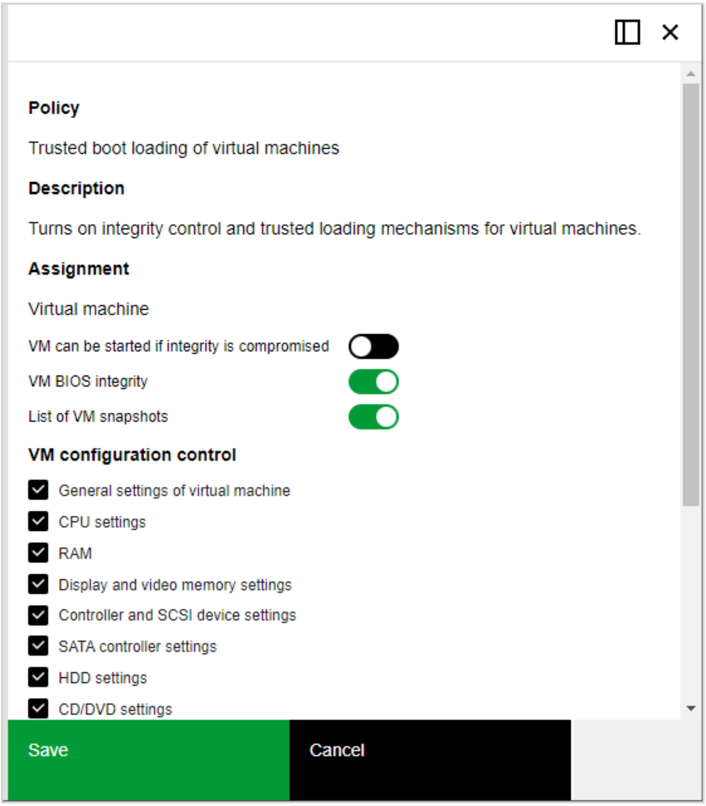
vGate allows you to perform detailed VM integrity control configuration:

- allow or prohibit starting a VM if the configuration integrity is compromised;
- select VM configuration files (VMX, NVRAM, VMSD files) for which the compliance of checksums will be reviewed;
- select VM configuration parameters (VMX file parameters) which value changes will be controlled by the "Trusted boot loading of virtual machines" policy.

Configuration is performed while modifying the "Integrity control of virtual machine templates" policy parameters.

To configure policy parameters:

1. In the main menu, go to the "Security policies" section and open a policy set that includes the "Trusted boot loading of virtual machines" policy (see p.**95**).
2. Configure the parameters of the "Trusted boot loading of virtual machines" policy.



Parameter	Description
VM can be started if integrity is compromised	This option is enabled by default. To prohibit starting VM when checksums of controlled VM configuration files do not match, turn off the toggle.
VM BIOS integrity	This option is enabled by default. To disable integrity control of BIOS configuration files (NVRAM files), turn off the toggle.
List of VM snapshots	This option is enabled by default. To disable integrity control of configuration files of VM snapshots (VMSD files), turn off the toggle
VM configuration control	The list of VM configuration parameters (VMX file attributes) controlled by the policy (detailed information on compliance of controlled parameters with a certain VMX file attributes can be found below). To disable control of changes for the specified VM property, clear the corresponding check box

Attention! Once you modified parameters of the "Trusted boot loading of virtual machines" policy, assign this policy to VM again. When converting virtual machine to template, to enable integrity control of this template, assign the "Integrity control of virtual machine templates" policy to it (see p.130).

3. Once you completed all changes, click the "Save" button.

Attention! Operations of removing and converting VM to template are blocked for all virtual machines to which the "Trusted boot loading of virtual machines" policy is assigned.

Calculating checksums

VM integrity is controlled by the vGate agents installed on ESXi servers (see p.85).

For each VM to which the "Trusted boot loading of virtual machines" policy is assigned, the reference checksum is calculated and used for integrity control. When migrating a VM from another server, its checksum must be recalculated by approving virtual machine changes in the "Virtual machine" section of the web console. Otherwise, the integrity violation will be registered.

Control of changes and VM status

On the ESXi server, the VM reference checksum is compared to the current checksum every 10 minutes (as well as when starting a VM or checking policies manually). If VM checksums do not match, integrity violation is registered, the VM status is changed (value in the "Integrity control" column), and starting this VM can be prohibited.

Note. In case of mismatch of checksums, starting of virtual machines will not be blocked if the "VM can be started if integrity is compromised" option is enabled in the "Trusted boot loading of virtual machines" policy (this option is enabled by default).

The administrator can accept (confirm) changes or reject them depending on the VM status (see p.154). When accepting changes, the reference VM checksum is replaced by the current (i.e. checksum is recalculated). Besides this, when accepting changes, the current VM configuration file is saved in the database. When rejecting changes, the current configuration file is replaced by the reference file (that was saved in the database during the last confirmation).

Attention! When rejecting changes in VM configuration, parameters that are not controlled by the "Trusted boot loading of virtual machines" policy will also be affected.

VM statuses, their description and available administrator actions with VM are presented in the table below.

Status	Description and available operations
Disabled	Integrity control for VM is not enabled
Counting error	An error occurred while calculating checksums. Depending on the error, you will have to wait until the status changes or accept the changes again. If confirmation is not available, the "Accept" button will not be available.
Integrity violated	VM integrity is compromised. The detailed information about the event can be found in the event log (see p.156). Rejecting changes is not available, you can only accept changes
In process of confirmation	The process of confirming changes and calculating new reference checksums has been started
Integrity agreed	Changes have been accepted
VMX file modified	VMX file has been changed. You can accept or reject changes

Controlled VMX file attributes

The "Trusted boot loading of virtual machines" policy can be configured to control VMX file parameters (if one or several options are selected in the "VM configuration control" list, see p.127). In this case, while reviewing VM parameters changes, not only checksums of configuration files are compared, but also values of individual VMX file attributes. Value changes are reviewed for the set of predefined attributes and attributes that match a regular expression.

Parameters of the "Trusted boot loading of virtual machines" policy and VMX file attributes corresponding to them are presented in the table below.

Policy parameter	VMX file attributes
General settings of virtual machine	• bios.bootdelay, bios.bootretry.delay, bios.bootretry.enabled, bios.forcesetuponce, chipset.onlinestandby, disable_acceleration, displayname, firmware, guestos, logging, monitor.virtual_exec, monitor.virtual_mmu, powertype.poweroff, powertype.poweron, powertype.reset, powertype.suspend, sched.swap.hostlocal, tools.synctime, tools.upgrade.policy, toolscripts.afterpoweron, toolscripts.afterresume, toolscripts.beforepoweroff, toolscripts.beforesuspend, uuid.bios, vmx.buildtype, wwn.enabled, wwn.node, wwn.port, wwn.type, bios440.filename, config.version, extendedconfigfile, nvram, sched.swap.derivedname, vc.uuid, virtualhw.version • attributes that match a regular expression hpet\d+\.present
CPU settings	• numvcpus, cpuid.corespersocket, vcpu.hotadd, sched.cpu.affinity, sched.cpu.htsharing, sched.cpu.shares, sched.cpu.max, sched.cpu.min, sched.cpu.units • attributes that match a regular expression cpuid\.(?:0|1|80000001)\.e[a-d]x(?:\.amd)
RAM	memsize, mem.hotadd, sched.mem.max, sched.mem.min, sched.mem.minsize, sched.mem.shares
Display and video memory settings	mks.enable3d, svga.autodetect, svga.maxheight, svga.maxwidth, svga.numdisplays, svga.present, svga.vramsize
Controller and SCSI device settings	Attributes that match a regular expression scsi(\d+)\.(?:present|sharedbus|virtualdev)
SATA controller settings	Attributes that match a regular expression sata(\d+)\.(?:present|pcislotnumber)
HDD settings	Attributes that match a regular expression (?:scsi|sata|ide)(\d+:\d+)\..+
CD/DVD settings	Attributes that match a regular expression (?:ide|sata)(\d+:\d+)\..+
Floppy disk drive	Attributes that match a regular expression floppy(\d+)\..+
PCI device settings	Attributes that match a regular expression pcipassthru(\d+)\..+
Network adapter settings	Attributes that match a regular expression ethernet(\d+)\..+
Serial port setting	Attributes that match a regular expression serial(\d+)\..+
Parallel port settings	Attributes that match a regular expression parallel(\d+)\..+
Controller and USB device settings	• ehci.present, usb.present, usb_xhci.present • attributes that match a regular expression usb\.autoconnect\.device\d+
VMCI protocol control	vmci.filter.enable, vmci0.id, vmci0.present, vmci0.unrestricted
Parameters controlled by vGate security policies	isolation.bios.bbs.disable, isolation.device.connectable.disable, isolation.device.edit.disable, isolation.ghi.host.shellaction.disable, isolation.monitor.control.disable, isolation.tools.autoinstall.disable, isolation.tools.diskshrink.disable, isolation.tools.diskwiper.disable, isolation.tools.disptoporequest.disable, isolation.tools.dnd.disable, isolation.tools.getcreds.disable, isolation.tools.ghi.autologon.disable, isolation.tools.ghi.launchmenu.change, isolation.tools.ghi.protocolhandler.info.disable, isolation.tools.ghi.trayicon.disable, isolation.tools.guestdndversionset.disable, isolation.tools.memschedfakesamplestats.disable, isolation.tools.paste.disable, isolation.tools.setguioptions.enable, isolation.tools.trashfolderstate.disable, isolation.tools.unity.disable, isolation.tools.unity.push.update.disable, isolation.tools.unity.taskbar.disable, isolation.tools.unity.windowcontents.disable, isolation.tools.unityactive.disable, isolation.tools.unityinterlockoperation.disable, isolation.tools.vixmessage.disable, isolation.tools.vmxdndversionget.disable, log.keepold, log.rotatesize, remotedisplay.maxconnections, remotedisplay.vnc.enabled, tools.guestlib.enablehostinfo, tools.setinfo.sizelimit, vmsafe.agentaddress, vmsafe.agentport, vmsafe.enable

Configuring integrity control of KVM/Skala-R/Proxmox/OpenNebula virtual machines

Integrity control is applied only to those virtual machines to which the respective policy is assigned. The policy is configured in the same way as in the configuration of the "Trusted boot loading of virtual machines" policy (see p.127).

Configuring integrity control of ESXi VM template

Integrity control is applied only to those VM templates to which the "Integrity control of virtual machine templates" policy is assigned.

Configuring objects of control

vGate allows you to perform detailed VM template integrity control configuration:

- allow or prohibit operations with a VM template if the configuration integrity is compromised;

  Attention! Operations of removing and converting VM to template are blocked for all virtual machines to which the "Integrity control of virtual machine templates" policy is assigned.

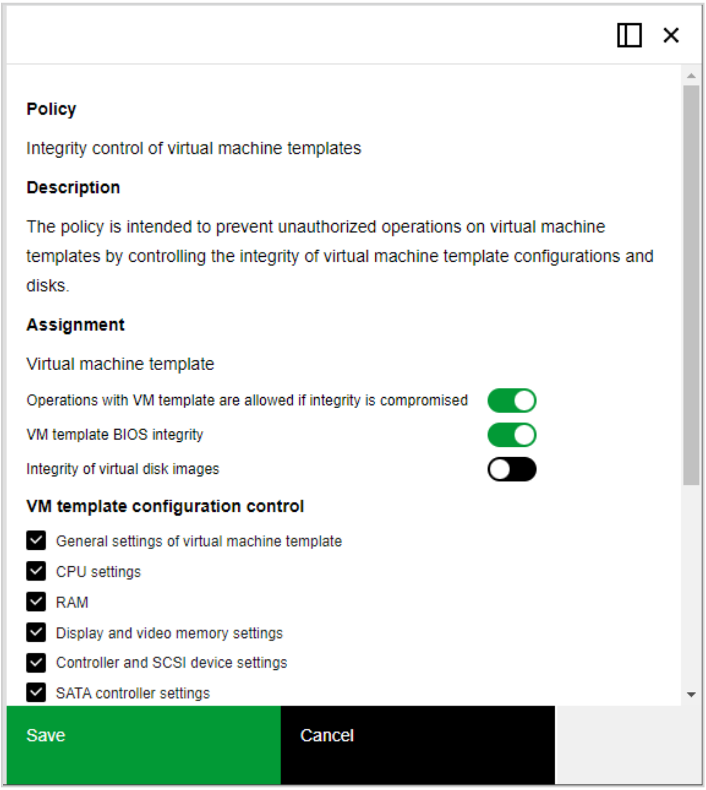
- select VM template configuration files (NVRAM, VMDK files) for which checksums will be checked;
- select VM template configuration parameters (VMTX file parameters), which value changes will be controlled by the policy.

Configuration is performed while modifying the "Integrity control of virtual machine templates" policy parameters.

To configure policy parameters:

1. Select the "Integrity control of virtual machine templates" policy in the list and click the "Edit" button.

   A panel for editing the policy parameters appears.



2. Configure the policy parameters.

Parameter	Description
Operations with VM template are allowed if integrity is compromised	This option is enabled by default. To prohibit operations with the template if checksums of template files and their reference values do not match, turn off this toggle
VM template BIOS integrity	This option is enabled by default. To disable integrity control of BIOS configuration files (NVRAM files) of the VM template, turn off the toggle.
Integrity of virtual disk images	To enable integrity control of virtual disk images (VMDK files), turn on this toggle. Calculating checksums of disk images may take a long time
VM template configuration control	The list of VM template configuration parameters (VMTX file attributes) controlled by the policy is the same as the list of VM configuration parameters (see p.**127**). To disable control of changes for a certain VM template property, clear the corresponding check box

vGate supports integrity control of virtual disk images up to 10 VM templates with the total capacity of disks equal to 500 GB.

Example.

- If virtual infrastructure includes 4 VM templates, the total capacity of disks of templates with enabled integrity control can be 400 GB (if each image takes 100 GB).
- If virtual infrastructure includes 10 VM templates, the total capacity of disks of templates with enabled integrity control can be 500 GB (if each image takes 50 GB).

Attention! If the "Integrity of virtual disk images" option is enabled, checksums are recalculated for VM templates to which the "Integrity control of virtual machine templates" policy is assigned.

3. Once you completed all changes, click the "Save" button.

Attention! Once you modified parameters of the "Integrity control of virtual machine templates" policy, assign this policy to the VM template again. When converting template to the virtual machine, to enable integrity control of this VM, assign the "Integrity control of virtual machine" policy to it (see p.127).

Calculating checksums and control of template changes

For each template to which the "Integrity control of virtual machine templates" policy is assigned, the reference checksum is calculated and used for integrity control.

The VM template reference checksum is compared to the current checksum every 30 minutes or when checking policies manually.

If VM template checksums do not match, integrity violation is registered, VM template status is changed (value in the "Integrity control" column) and operations with this template can be prohibited if the "Operations with VM template are allowed if integrity is compromised" option is enabled in the "Integrity control of virtual machines" policy.

Depending on the VM template status, the administrator can accept or reject changes (see p.**154**).

Note. When calculating checksums of virtual disk images, the "Requires confirmation" VM template status can appear. This status does not require any actions.

Configuring integrity control of ESXi server configuration files

Integrity control is applied only to those ESXi servers to which the "Integrity control of ESXi server configuration files" policy is assigned.

Configuring objects of control

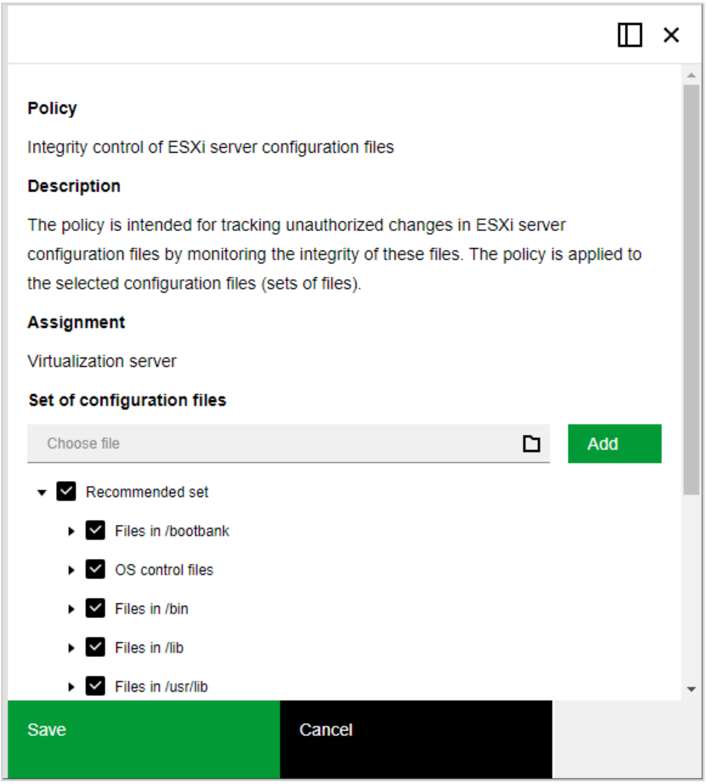
You can use the recommended set of files or create a custom set of ESXi server configuration files for which compliance of checksums will be reviewed.

Configuration is performed while modifying the "Integrity control of ESXi server configuration files" policy parameters.

To configure policy parameters:

1. Select the "Integrity control of ESXi server configuration files" policy in the list and click the "Edit" button.

A panel for configuring the policy parameters appears.



2. By default, the policy contains the recommended set of configuration files. To add a new set of files for integrity control, select a file and click the "Add" button.

   UTF-8 text file must include paths to the protected server configuration files located in different rows.
3. Select files for which you want to enable integrity control, then click the "Save" button.

Calculating checksums and control of changes

Integrity of configuration files is controlled by vGate agents installed on ESXi servers. For each configuration file, the reference checksum is calculated and used for integrity control.

Checksum and path to the configuration file are stored in the database and checked every 10 minutes or at the user's request. If checksums do not match, integrity violation is registered, ESXi server status changes (value in the "Integrity control" column).

Depending on the protected server status, the administrator can accept changes or reject them in the "Security configuration of servers" section (see p.124).

Configuring integrity control of container images

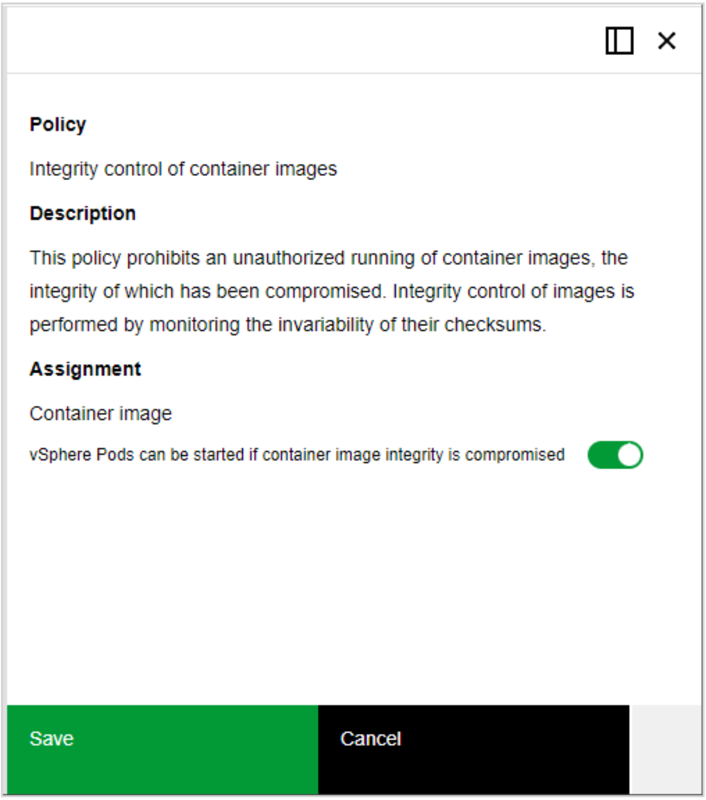
Integrity control is applied only to those container images to which the "Integrity control of container images" policy is assigned. The policy prohibits an unauthorized running of container images, the integrity of which has been compromised. Integrity control of images is performed by monitoring the invariability of their checksums.

Configuring the "Integrity control of container images" policy

To configure policy parameters:

1. In the main menu, go to the "Security policies" section and open the set of policies that includes the "Integrity control of container images" policy (see p.95). This policy is included in the "vGate" policy template.

2. If necessary, turn on the "vSphere Pods can be started if container image integrity is compromised" toggle.



3. Once you completed all changes, click the "Save" button.

Calculating checksums

Integrity of container images is controlled by vGate agents installed on an ESXi server.

For integrity control of container images, reference checksums from the Harbor Registry are used. Details on approving and rejecting changes of container images can be found in the "Container images" section (see p.**151**).

Control of changes and image container status

By default, image container reference checksum is compared to the current checksum every 10 minutes. You can change this value on the vGate server in the HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate registry section with the help of the HarborImagesInchTimeout parameter (in seconds).

If checksums do not match, integrity violation is registered, image container status is changed in the "Integrity control" column.

Note. In case of mismatch of checksums, starting a vSphere Pod will not be blocked if the "vSphere Pod can be started if integrity is compromised" option is enabled in the "Integrity control of container images" policy (this option is enabled by default).

The administrator can approve (confirm) changes or reject them depending on the container image status (see p.**151**). Approving changes is available if the container image has the "Integrity violated" status. When approving changes, the reference container image checksum is replaced by the current checksum (i.e. checksum is recalculated).

Integrity control statuses, their description and available administrator actions with container image are presented in the table below.

Status	Description and available operations
Disabled	Integrity control for the container image is not configured
Counting error	An error occurred while calculating checksums. Depending on the error, you will have to wait until the status changes or approve the changes again. If approval is not available, the "Approve" button will not be available. If an error occurs while recalculating checksums, its causes may be detected when analyzing the vGateAdmin.log file located in the product installation directory on the vGate server
Integrity violated	Image container integrity is compromised. The detailed information about the event can be found in the event log (see p.**156**). Rejecting changes is not available, you can only approve changes
Integrity agreed	Changes have been approved

Cloud Director operations control

vGate supports VMware Cloud Director operations control.

This function is available only in vGate Enterprise and Enterprise Plus.

Note. Cloud Director operations control is supported only in versions 10.0 (10.0.0.1, 10.0.0.2, 10.0.0.3), 10.1 (10.1.1, 10.1.2, 10.1.3), 10.2 (10.2.1, 10.2.2), 10.3.

To get started with Cloud Director in vGate:

1. Configure a connection to the Cloud Director server (see p.**64**).
2. Add the Cloud Director server to the list of protected servers (see p.**79**).
3. Configure rules for access to the Cloud Director server (see p.**107**). To do this, use the "Access to Cloud Director" rule template for authenticated users and "User access to the protected server with authentication via the web interface" for anonymous users (when accessing Cloud Director without the vGate client).

   Note. When using anonymous user access, assign the "Access to the vGate server for user authentication via the web interface" rule to the vGate server.

Management of Cloud Director organizations

In the web console, you can manage organizations of the Cloud Director server, whose connection parameters are specified in the "Settings" section (see p.**79**).

To manage organizations:

1. In the web console, go to the "Organizations" section.

   The list of Cloud Director organizations appears.

   Note. For the convenience of working with objects of organizations in vSphere Web Client, we recommend naming all virtual machines and containers (vApp) within each organization according to a certain template.

2. The following actions are available:
   - view an organization properties;
   - assign labels;

   Note. For mandatory access control using vGate, labels should be assigned not only to organizations but also to virtual machines created within them.

   - add an organization to a group and remove an organization from it;
   - view related events;
   - refresh the list of organizations.

Restrictions when working with Cloud Director

When working with Cloud Director in vGate, the following restrictions must be considered.

- To correctly move organizations between datastores, we recommend moving not more than one organization at a time.
- By default, working with Cloud Director over vcd-cli is blocked. To unlock access to Cloud Director using the utility, set the VcpVcdCliEnabled key value in the HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate registry branch to 1. Once you finished work with the vcd-cli utility, we recommend you set the registry key to the initial value (0).
- vGate does not support control of operations related to NSX-T resources.

Security monitoring

This function is available in vGate Enterprise Plus only (see the "Functionality" section in the document [1]).

vGate security monitoring allows collecting and analyzing the data on events that occur on the following objects of the virtual infrastructure: vGate server, protected servers and administration network computers with the installed vGate Client.

Connecting to the monitoring server

For the monitoring function to operate, connect to the vGate monitoring server that is deployed in the network (see p.45). The connection setup is given on p.70.

Dashboard

Dashboard is a configurable set of diagram widgets. Diagrams display the data on events and incidents occurring in the virtual infrastructure in a graphical form.

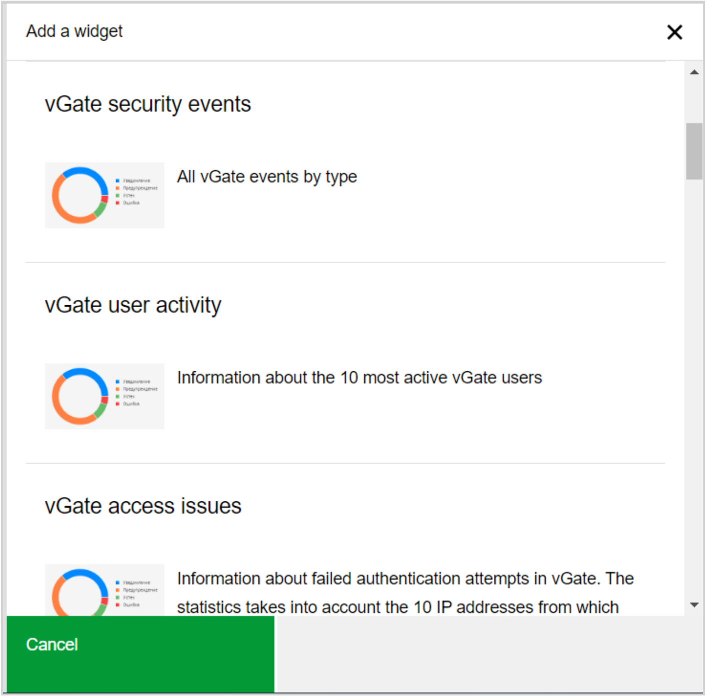
Note. The order of widgets can be changed using drag-and-drop.

To configure the dashboard:

1. In the main menu, go to the "Monitoring" section and open the "Dashboard" tab.

   An empty dashboard appears.
2. Click the "Add widget" button.

   A panel for adding a widget appears.



3. Select a widget that you want to add to the dashboard.

Widget	Description
Logs heatmap	Information about the number of logs for each day. Each color represents the number of logs for the given day
vGate security events	All vGate events by type
vGate user activity	Information about top 10 vGate users based on their activity
vGate access issues	Information about failed authentication attempts in vGate. The statistics takes into account 10 IP addresses from which the maximum number of failed access attempts were made
Problems in vGate	Information about errors and issues that occured during vGate operation
Violations of network connection filtering rules	Information about unauthorized access attempts that violate firewall rules. The statistics includes 10 IP addresses from which the maximum number of unsuccessful access attempts were made
Violations of VMware access rules	Information about unauthorized access attempts with violation of VMware mandatory access control rules. The statistics takes into account 10 users who made failed attempts more often than other users
Incidents	Number of vGate incidents, distributed by their priority
Virtual machine integrity violations	Number of events related to the integrity violations of the VM files
Bypassing vGate	Number of virtual infrastructure operations bypassing vGate, distributed by their priority
Creating VMware virtual machines	Information about VMware virtual machine creation events, The statistics takes into account 10 datastores on which the most virtual machines were created
Compliance with the sets of security policies	Information on compliance of protected servers with the sets of security policies
VMware virtual machine migrations	Information about VMware virtual machine migration events. The statictics takes into account 10 virtual machines that migrated most often
ESXi servers with enabled traffic filtering component	Information about the number of ESXi servers on which the virtual machine traffic filtering component is enabled
Virtual machines for which traffic is controlled	Information about the number of virtual machines for which network traffic is controlled
Active firewall rules	Information about the number of virtual machine firewall rules enabled
Statistics of firewall rules triggering	Information about events of virtial machine traffic filtering rules triggering. 10 rules for which the most packages were checked are displayed
Compliance of ESXi servers with security policies	Information about VMware ESXi servers compliance with security standards
Allowed traffic between segments	Select the widget type: • Top 10 segments by allowed traffic — information about the virtual infrastructure segments for which the most amount of network traffic was transferred. The statistics takes into account 10 segments with the most amount of traffic. • Allowed traffic for the selected segment — information about the allowed network traffic for the selected virtual infrastructure segment. Select one segment for which the statistics will be displayed. • Allowed traffic between selected segments — information about the allowed network traffic between the selected virtual infrastructure segments. Select from 2 to 10 segments

Widget	Description
Blocked traffic between segments	Select the widget type: • Top 10 segments by blocked traffic — information about the virtual infrastructure segments for which the most amount of network traffic was blocked. The statistics takes into account 10 segments with the most amount of traffic. • Blocked traffic for the selected segment — information about the blocked network traffic for the selected virtual infrastructure segment. Select one segment for which the statistics will be displayed. • Blocked traffic between selected segments — information about the blocked network traffic between the selected virtual infrastructure segments. Select from 2 to 10 segments
Objects and user accounts by confidentiality categories	Information about the number of protected objects and user accounts for each confidentiality category
Objects and user accounts by confidentiality levels	Information about the number of protected objects and user accounts for each confidentiality level

The selected diagram appears.

4. Repeat actions described above to add all necessary widgets.

Note.
- To remove a widget from the dashboard, click the "Bucket" icon in the upper right corner of the widget.
- Some widgets are configurable. To configure a widget, click the "Settings" icon in the upper right corner of the widget.

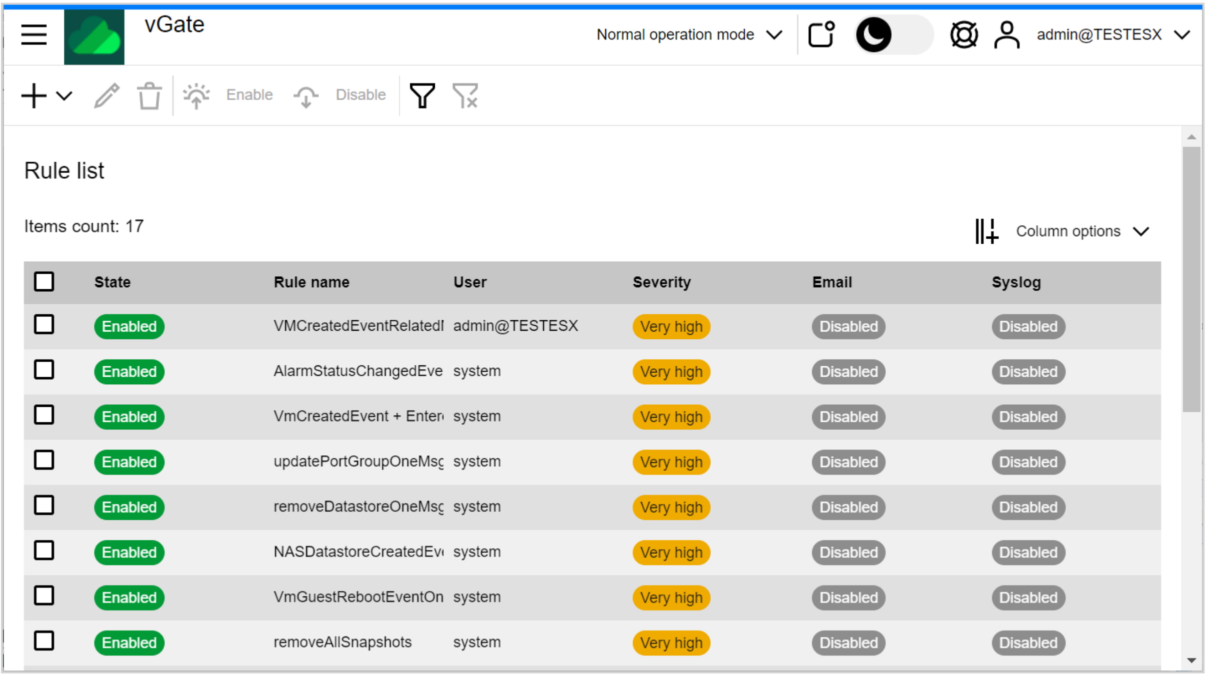
Creating correlation rules

Correlation rules allow you to monitor certain events occurring under specified conditions in the virtual infrastructure. If rules are triggered, alerts are created.

To create a rule:

1. In the main menu, go to the "Monitoring" section and open the "Rule list" tab.

The following window appears.



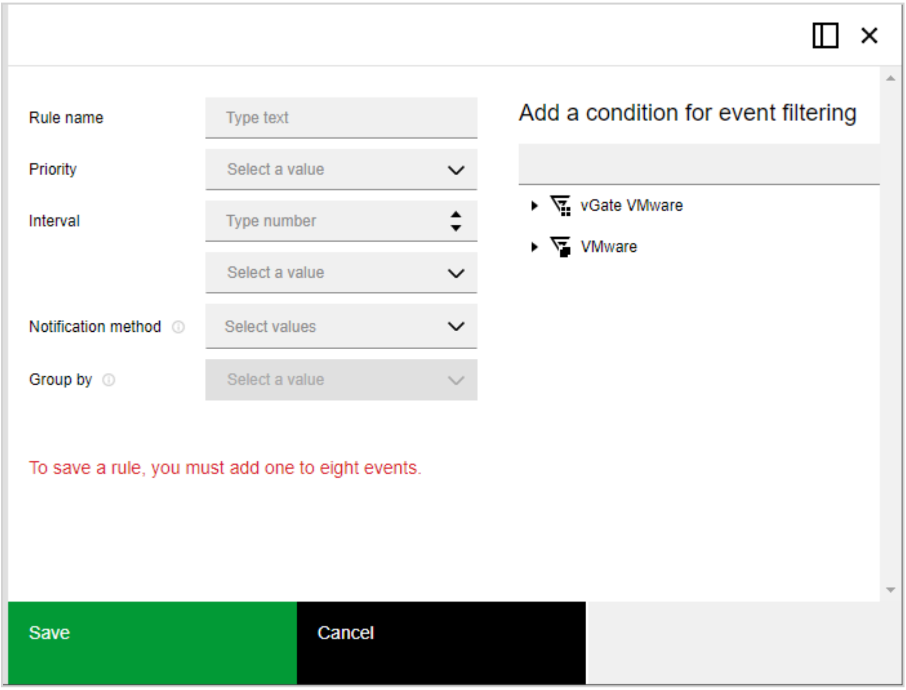
2. Click the "Add" button, select the required action in the drop-down list:

- Add a rule (see p.**138**);
- Add a template-based rule (see p.**140**);
- Add a rule bypassing vGate (see p.**141**).

Tip.
- To manage a rule, use the "Enable" and "Disable" buttons. To delete a rule, click the "Delete" button. To modify a rule, click the "Edit" button.
- To use filters, click "Filtering", set the required criteria in the appeared panel and click "Apply". To reset the search results, click the "Reset filters" button.
- To configure the table columns, click "Column options" and select the required options.

3. A panel for adding a correlation rule appears.

Adding a new rule

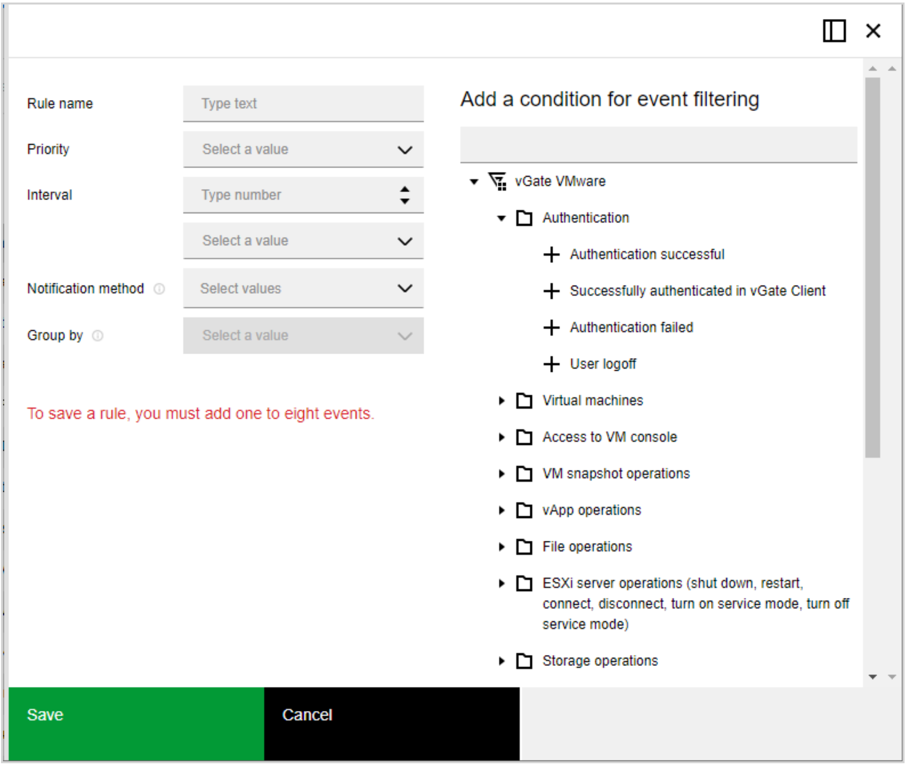


To add a rule:

1. Specify the following parameters

Parameter	Description
Rule name	Specify the rule name
Priority	Specify the rule severity
Interval	Specify the interval of checking events in seconds, minutes or hours
Notification method	Select how to notify when the rule is triggered
Group by	Select the parameter by which occurred events will be grouped

2. Select events that will be tracked by this rule. To do this, select an event in the list on the right of the panel an click +. An area for adding filters becomes available.



Note.
- To remove the event condition, click ✕.
- Use the search bar to quickly search for virtual machines.

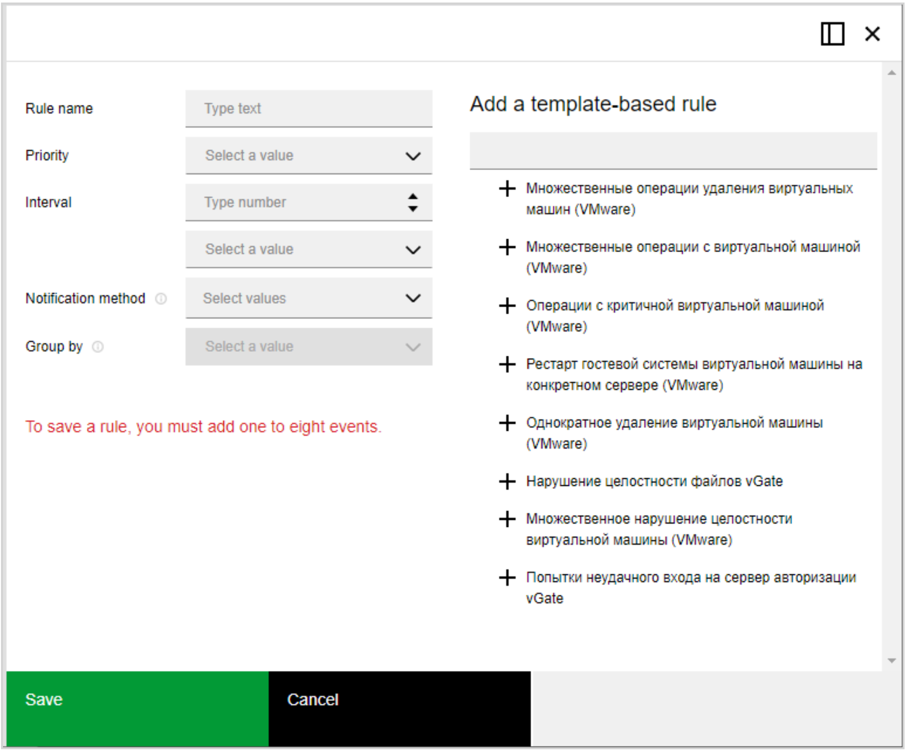
3. Specify the number of events required to trigger the rule, specify filter parameters and click the "Add filter" button.

Parameter	Description
Object	Select one of event parameters
Expression	Select an expression from the drop-down list to create the condition: • Contains; • Equal; • Non equal
Value	Specify the value that the selected event parameter should take to trigger the rule

Tip. To add additional conditions for event filtering, repeat steps 2–5.

4. The added filters appear in the table on the left of the panel. To remove a filter, select it and click the "Delete" button. To remove all filters, click the "Clear" button.
5. At the bottom of the panel, click the "Save" button. The rule will be added to the list.

Adding a template-based rule

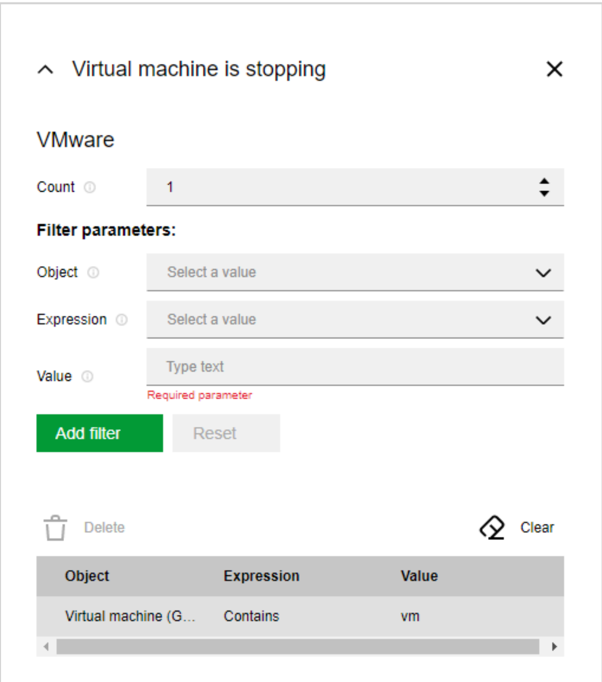


To add a template-based rule:

1. On the right of the panel, select a template from the list of templates and click +. The rule parameters will appear on the left of the panel.

   Note. Use the search bar to quickly search for virtual machines.

   On the left of the panel, an area for adding filters becomes available.



   Note. To remove the event condition, click ✕.

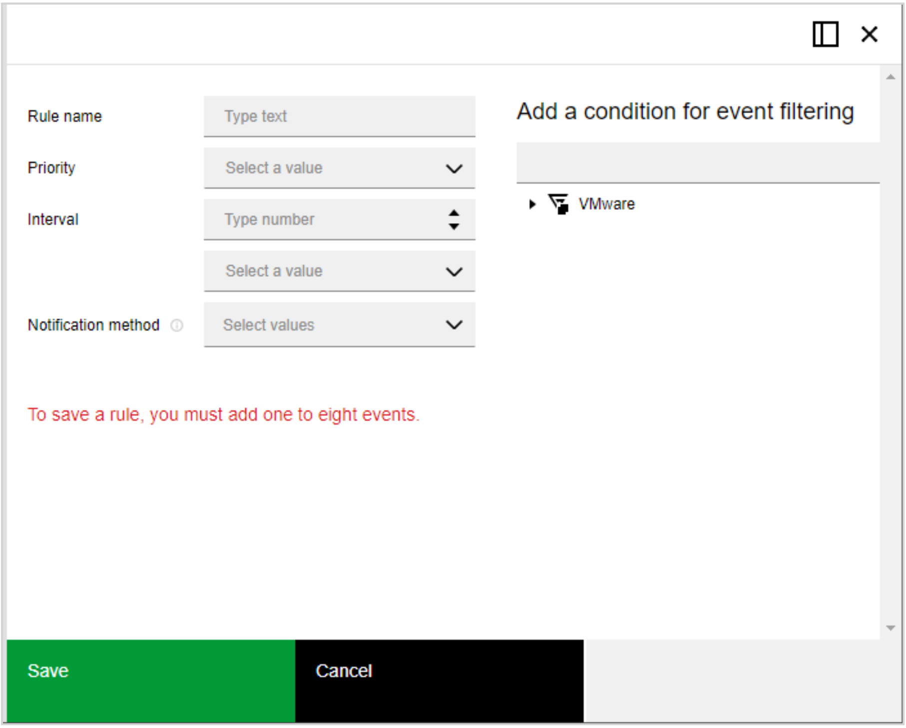
2. Specify the number of events required to trigger the rule and add filters (see steps 4-5 on the p.**138**).

   Note. To remove a filter or all filters, use the "Remove" and "Clear" buttons above the table.

3. Click the "Save" button. The rule will be added to the list.

> **Note.** When creating template-based rules, adding event filtering condition is not available. To add additional events to a template-based rule, select the rule in the list of rules and click the "Edit" button.

Adding a rule bypassing vGate



To add a rule:

1. Specify the rule name, priority and interval, then select event types to track in the virtual infrastructure. The rule triggers if the selected events are registered on objects of the virtual infrastructure and vGate does not receive the respective audit events in a set amount of time.

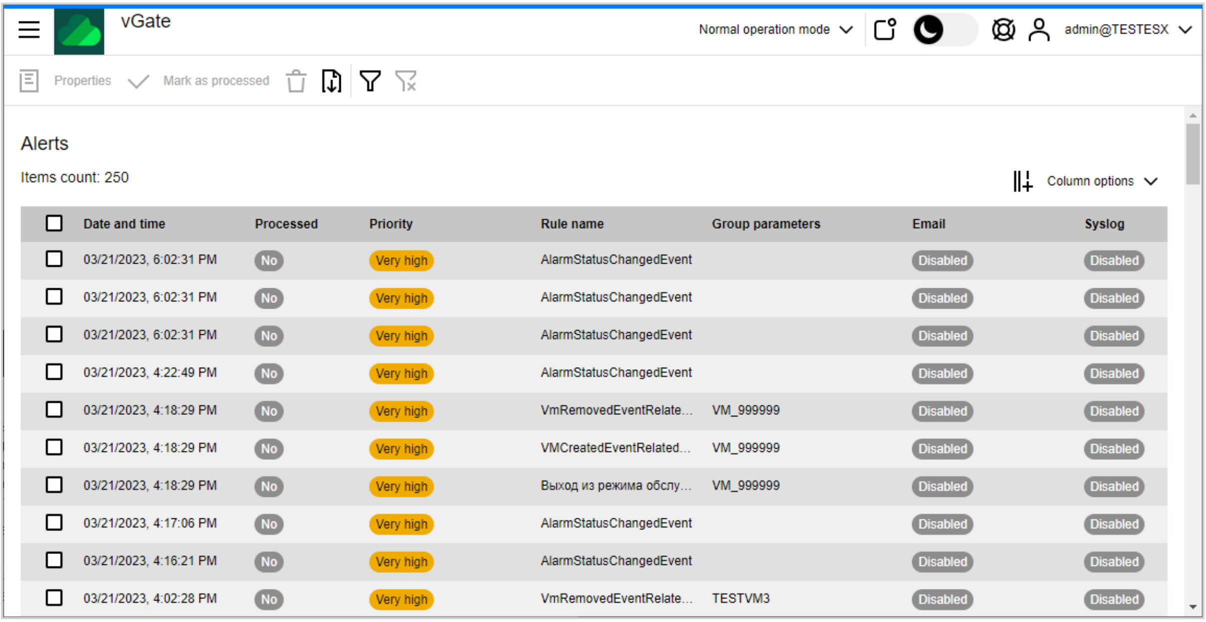
> **Note.**
> - Considering that information about events on the vCenter server is requested every 60 seconds, we recommend you to set interval to at least 90 seconds when creating a rule.
> - Use the search bar to quickly search for virtual machines.

2. Click the "Save" button, the rule will be added to the list.

Alerts

Alerts are events that are created when correlation rules trigger.

To view the list of alerts, go to the "Monitoring" section of the main menu and open the "Alerts" tab.



Note. Information about alerts is also displayed as diagrams on the Dashboard (see p.135).

To view detailed information about an event, select it in the list and click the "Properties" button.

To mark an alert as viewed, click the "Mark as processed" button.

To delete the selected alert, click the "Mark as processed" button and then click "Delete". To export the text file containing the list of events, click the "Download selected alerts"/"Download all alerts".

Note.

- To filter alerts, click the "Filtering" button, set the required criteria in the appeared panel and click the "Apply" button. To reset the search results, click the "Reset filters" button.
- To configure the table columns, click "Column options" and select the required options.

Firewall

The vGate software includes the "Firewall" component that allows filtering network traffic in the network of VMware vSphere virtual machines including located on different vGate servers.

This function is available in vGate Enterprise Plus only (see the "Functionality" section in the document [1]).

To work with the "Firewall" component, a user must have the "vGate network administrator" privilege (see **1**).

Firewalling is provided by the virtual machine traffic filtering component. By default, this component is installed with the vGate agent for ESXi server (see p.**85**).

Attention! If firewall rules (see p.146) were created with the specified MAC/IP addresses of the source or destination, they will stop operating if these parameters changes. vGate monitors changes of these parameters for firewall rules assigned to virtual machines and segments, but for correct operation of the "Firewall" component, we recommend you prohibit MAC address changes. To do this, in vSwitch settings select the "Reject" value for the "Forged Transmits" and "MAC Address Change" parameters, or assign the "Ensure that "Forged Transmits", "MAC Address Changes", "Promiscuous Mode" on virtual switches is set to reject" policy to the ESXi server. Also assign the "Ensure that the "MAC Address Changes" policy is set to reject" and "Ensure that the "Forged Transmits" policy is set to reject" policies to the distributed virtual switch to monitor changes of virtual switch security policies.

To configure the firewall:

1. Install vGate agents on ESXi servers (see p.**85**).
2. Enable firewall on protected ESXi servers (see p.**143**).
3. Select in the list virtual machines whose traffic you want to control (see p.**144**).

   Attention! To view the relevant list of virtual machines, parameters of connection to the virtualization server must be saved in the vGate web console (see p.64).
4. If necessary, group virtual machines into virtual infrastructure segments (see p.**145**).
5. Create firewall rules (see p.**146**).
6. To view information about active sessions, open the "Active sessions" tab (see p.**148**).

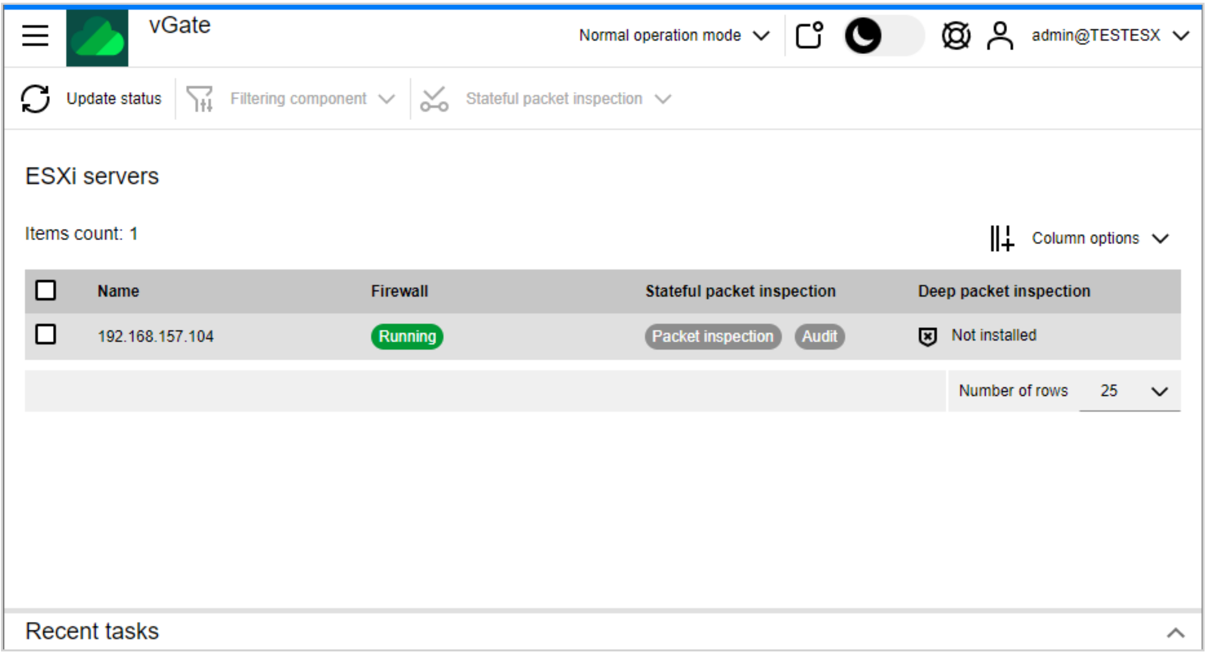
Enabling firewall on ESXi servers

By default, vGate firewall component on protected ESXi servers is disabled.

To enable firewall:

1. In the main menu, go to the "Firewall" section and open the "ESXi servers" tab.

   The following window appears.



Note. At the bottom of the page, information about the recent operations with virtual machines is presented.

2. Select the required virtualization servers in the list, click the "Filtering component" button and select "Enable" in the drop-down list.

   The firewall component will be enabled on the selected virtualization servers.

   Note.
   - To disable the firewall component, select ESXi servers, click the "Filtering component" button and select "Disable" in the drop-down list. Click the "Update status" button to update information about firewall components on these servers.
   - To configure the table columns, click "Column options" and select the required options.

3. To enable the stateful packet inspection function, select ESXi servers, click the "Stateful packet inspection" button and select "Enable" from the drop-down list.

   Note.
   - To enable logging of the audit events that occur when the stateful packet inspection function is enabled, select the "Register stateful packet inspection events" check box.
   - To disable the stateful packet inspection function, select ESXi servers, click the "Stateful packet inspection" and select "Disable".

Enabling traffic control for virtual machines

Attention! Do not enable traffic control for the virtual machine where the vGate server is located. This can lead to the system failure.

To enable VM traffic control:

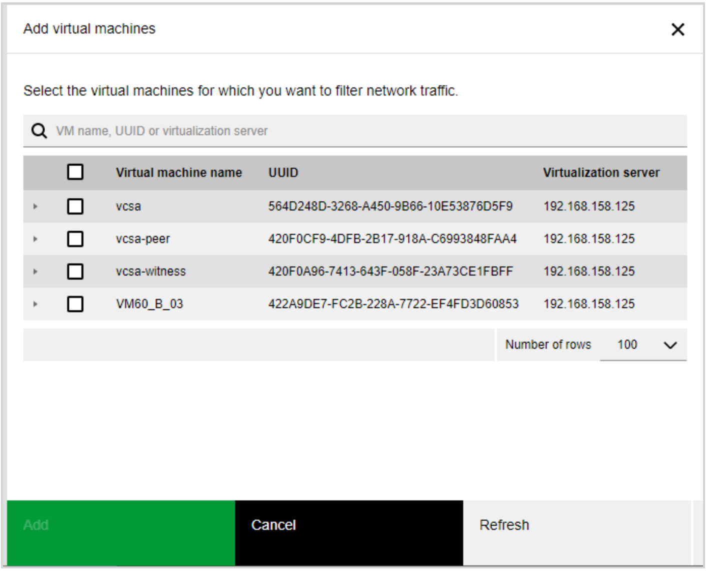
1. In the main menu, go to the "Firewall" section and open the "Virtual machines" tab.

   The list displays virtual machines for which traffic is monitored. To view the relevant list of virtual machines, parameters of connection to the virtualization server must be saved in the web console (see p.**64**).

   Note.
   - To configure the table columns, click "Column options" and select the required options.
   - To use filters, click "Filtering", set the required criteria in the appeared panel and click "Apply". To reset the search results, click the "Reset filters" button.
   - At the bottom of the page, information about the recent operations with virtual machines is presented.

2. To add a virtual machine to the list of protected virtual machines, click the "Add" button.

   A panel for adding virtual machines appears.



3. The list displays all virtual machines located on ESXi servers with the enabled firewall component. Select the required virtual machines and click the "Add" button.

   Note. If VMware Tools is installed on the virtual machine, the table will contain an additional information about the VM (virtual network and IP address).

   The virtual machine will be added to the list of virtual machines controlled by the firewall component.

4. To enable the firewall component on running virtual machines, restart this virtual machines with the help of Suspend/Resume or Power off/Power on commands.

To disable traffic control for a virtual machine, select it in the list and click the "Delete" button. Action applies only to virtual machines that are selected on the current page of the list.

Note. To disable the firewall component on virtual machines after removing them from the list of protected objects, power off the virtual machines (Suspend, Power Off, Shut down) and then restart them (Power On).

Segments

To create firewall rules (see p.**146**) for several virtual machines at the same time, you can group virtual machines into virtual infrastructure segments.

Attention!

- A virtual machine cannot be a part of more than one segment of the virtual infrastructure.
- A virtual infrastructure segment cannot be empty. If no virtual machines remain in the segment as a result of editing, this segment will be automatically deleted.

To create a virtual infrastructure segment:

1. In the main menu, go to the "Firewall" section and open the "Segments" tab.

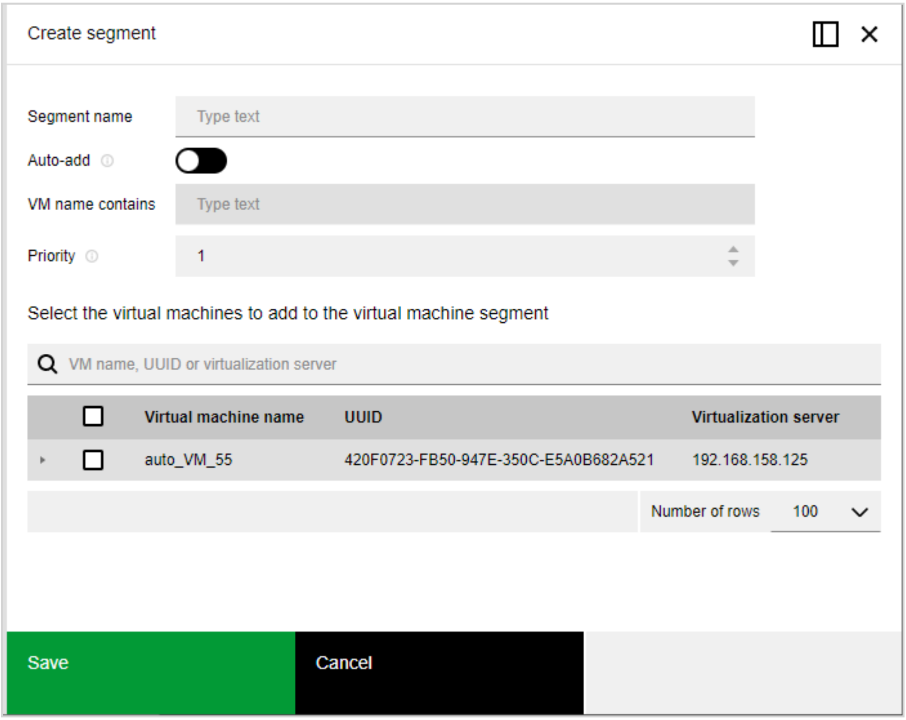
The list of segments appears.

Note.

- To use filters, click "Filtering", set the required criteria in the appeared panel and click "Apply". To reset the search results, click the "Reset filters" button.
- To modify the list of segments, use the "Edit" and "Delete" butons.
- At the bottom of the page, information about the recent operations with virtual machines is presented.

2. Click the "Create" button.

A panel for selecting virtual machines to be added to the segment appears on the right. The list displays all virtual machines with enabled traffic control (see p.**144**).



3. Specify the parameters of the new segment, select check boxes for virtual machines to be added to the segment, then click the "Save" button.

Parameter	Description
Segment name	Specify a unique segment name. The segment name may contain only Latin letters, digits, spaces, hyphens and underscores
Auto-add	Turn on the toggle to configure automatic adding of new virtual machines to the virtual infrastructure segment according to the "VM name contains" parameter
VM name contains	Type the text that you want to search for in the virtual machine names
Priority	Specify the priority according to which the virtual machine will be added to the segment if the virtual machine name corresponds to several segments. When changing the priority of one of the segments, the priorities of the remaining segments are automatically recalculated to avoid duplication of priorities and gaps between priority values

Note.
- To view detailed information about VM adapters, click ▶ next to the VM name.
- Use the search bar to quickly search for virtual machines. All columns in the table are searched.

The virtual machines will be added to the created virtual infrastructure segment.

Note. To allow network traffic between virtual machines from the same virtual infrastructure segment, create an allowing firewall rule (see p.146) and specify this segment as the source and destination.

Management of firewall rules

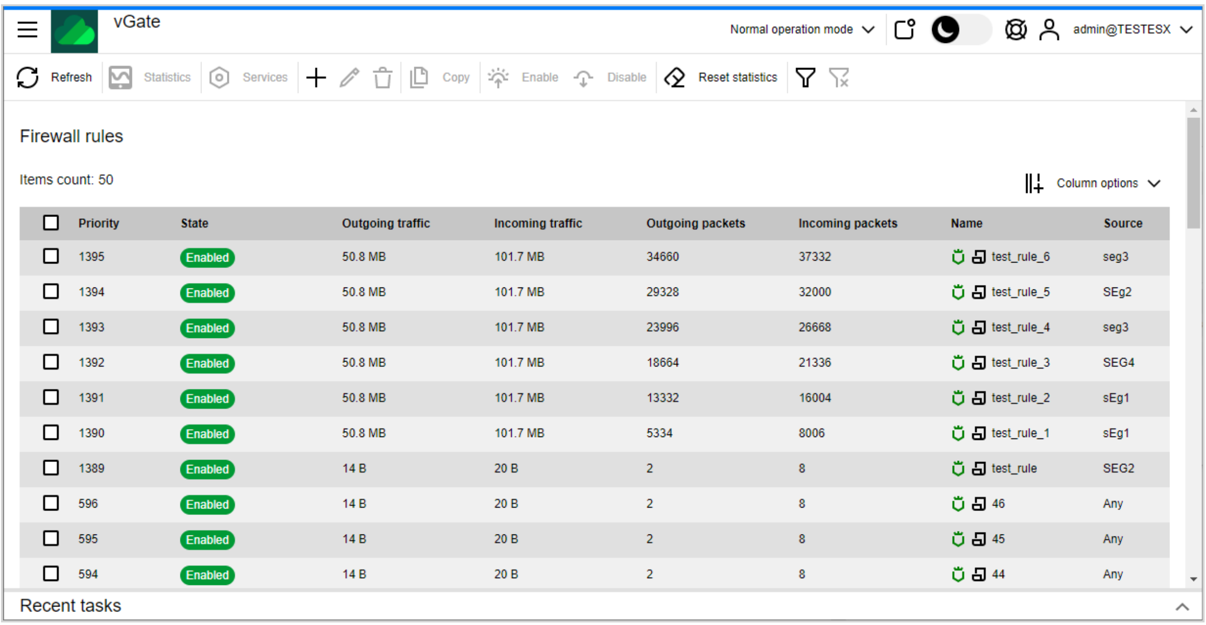
Firewall rules are used to configure network traffic filtering. By default, the list contains rules that allow all incoming and outgoing traffic in normal, test and emergency operation modes. Rules for test and emergency modes cannot be edited.

Firewall rules can be created for a certain virtual machine (see below) or for several virtual machines (see p.145).

To create a firewall rule:

1. In the main menu, go to the "Firewall" section, then open the "Firewall rules" tab.

   The list of firewall rules appears.



The number of sent packets and the amount of network traffic may be overestimated.

Note.
- To configure the table columns, click "Column options" and select the required options.
- To use filters, click "Filtering", set the required criteria in the appeared panel and click "Apply". To reset the search results, click the "Reset filters" button.
- At the bottom of the page, information about the recent operations with virtual machines is presented.

2. To create a new rule, click the "Create" button.

   A panel for creating a firewall rule appears.

3. Specify the following parameters and click the "Save" button.

Parameter	Description
Priority	Firewall rules are processed according to the specified priorities. The priority must be a unique value between 100 and 2100. The emergency operation mode rule has the highest priority, the test operation mode rule has the lowest priority
State	Select the rule status (enabled or disabled)
Name	Unique rule name
Source type	Types of objects (sources of network packets) for which this rule will be used: • IP address; • subnet; • IP address range; • MAC address; • virtual machine; • virtual infrastructure segment; • any
Source	Specify the source with the type that was selected above
Destination type	Types of objects (destinations for network packets) for which this rule will be active: • IP address; • subnet; • IP address range; • MAC address; • virtual machine; • virtual infrastructure segment; • any
Destination	Specify the destination with the type that was selected above
Direction	Direction of the packet passing while checking the firewall rule
Service	Select a service for which this rule will be active. The list contains services created earlier on the "Services" page (see p.**149**). The "Protocol", "Source type", "Destination type" rule parameters will be filled out automatically
Protocol	Select a protocol type the rule applies to
Source port	The source port this rule applies to, or "*" (asterisk) if the rule must apply to all ports. The port value must be between 1 and 65535.
Destination port	The destination port this rule applies to, or "*" (asterisk) if the rule must apply to all ports.
Packet type	Select a packet type
Action	Select an action that will be executed by this rule
Traffic logging	Allows you to enable firewall rule logging. Logs are stored on ESXi servers, from which they are sent to the vGate server. If traffic logging is enabled, network traffic will be displayed in the "Active sessions" section of the "vNetwork" component (see p.**148**)
Active sessions	Displaying the information about network traffic for this firewall rule on the "Active sessions" page
Event logging	Logging events of triggering this firewall rule in the vGate log

The firewall rule will be added to the list.

Note.
- To enable or disable a firewall rule, select it in the list and click the "Enable" or "Disable" button respectively. To modify the rule settings, click the "Edit" button.
- To remove a rule, select it in the list and click the "Delete" button. Action applies only to rules that are selected on the current page of the list.
- To copy a firewall rule, select it in the list and click the "Copy" button. Adding new firewall rule panel appears with the specified parameters of the copied rule.
- To reset statistics on packets that were transferred by a rule, select the required rule and click the "Reset statistics" button.
- To view services, select the required firewall rule and click the "Services" button.

Attention! If a virtual machine or a virtual infrastructure segment that was specified as a source or destination in the firewall rules is deleted, these rules will be disabled and the corresponding parameters will be set to the "Any" value.

Active sessions

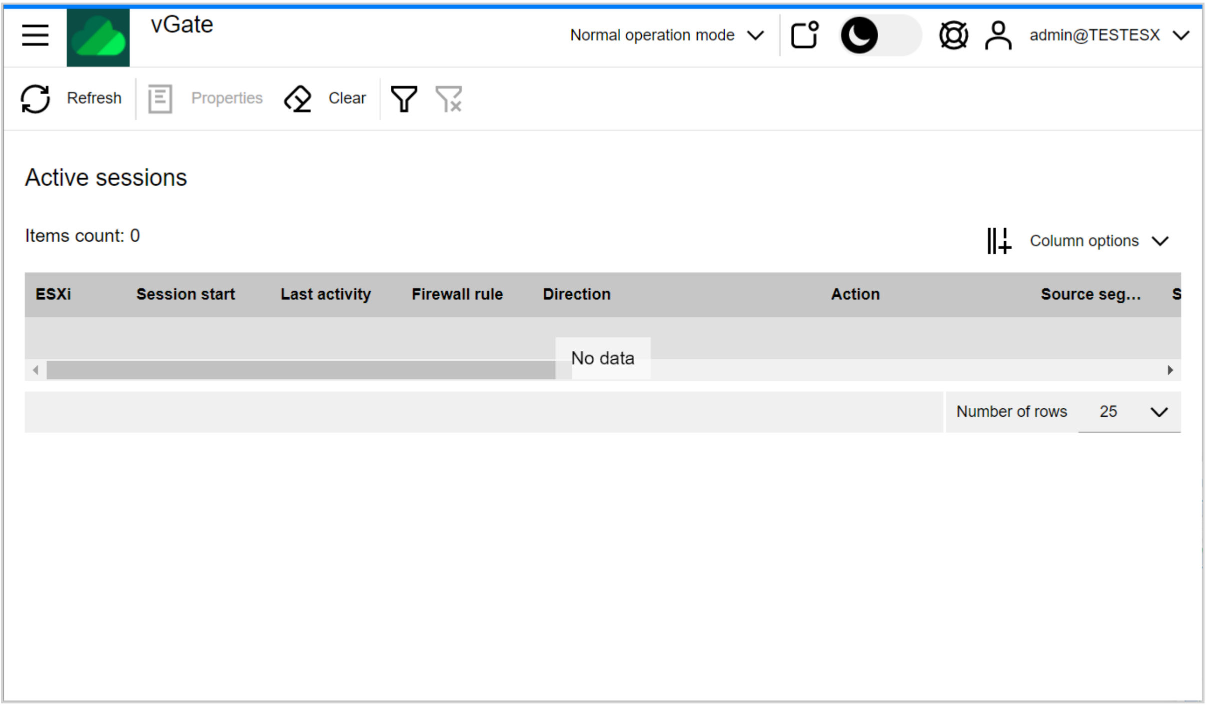
The "Active sessions" section contains information about the network traffic that was transferred or blocked according to the firewall rules.

Note. If logging is enabled for a firewall rule, network traffic by this rule is included in the statistics of active sessions (see p.146).

To view active sessions:

1. In the main menu, go to the "Firewall" section and open the "Active sessions" tab.

   The list of sessions appears.



Note.
- To configure the table columns, click "Column options" and select the required options.
- To use filters, click "Filtering", set the required criteria in the appeared panel and click "Apply". To reset the search results, click the "Reset filters" button.

2. Select the required session in the list and click the "Properties" button.

   A panel containing the session details appears. To save the session properties to the clipboard, click the "Copy" button.

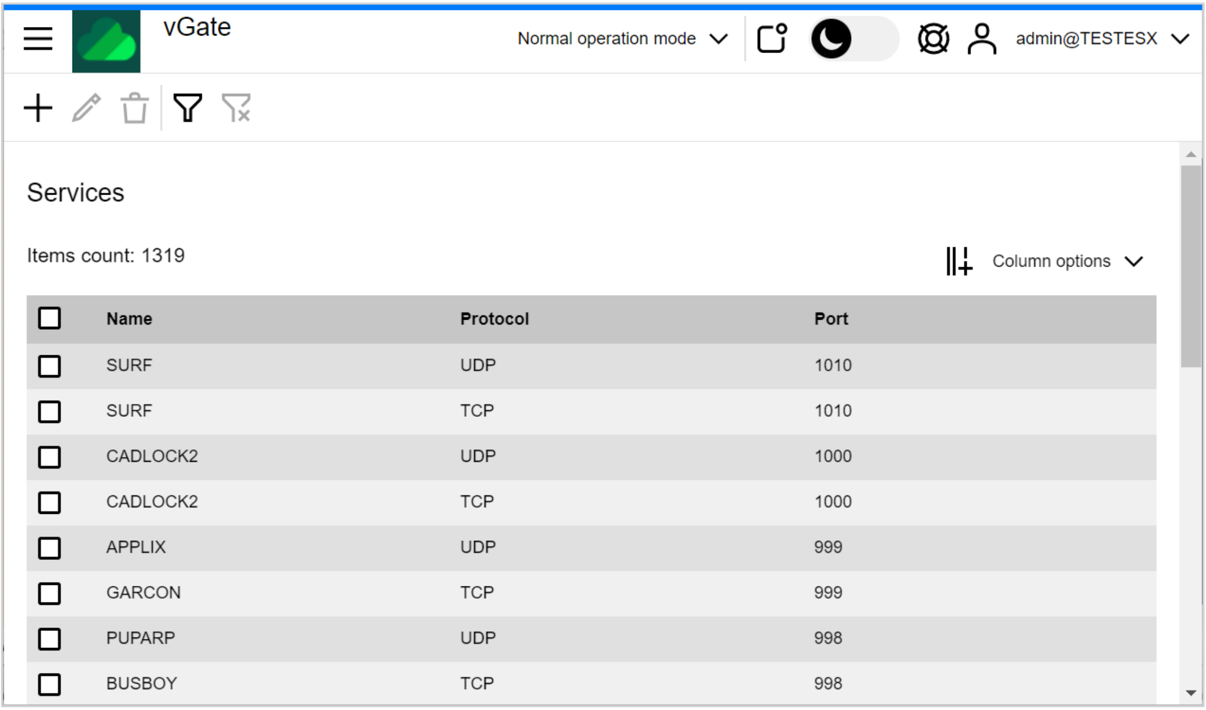
Note. When transferring or blocking network traffic between two virtual machines, two sessions will be displayed in the "Active session" section if both virtual machines are controlled by the "Firewall" component. If only one VM is controlled by the "Firewall" component, one session will be displayed.

Services

vGate allows configuring services to be controlled by the firewall rules of the "Firewall" component (see p.**146**).

To configure services to be controlled:

1. In the main menu, go to the "Firewall" section and open the "Services" tab.
   The following window appears.



2. To add a network service to the list of services controlled by vGate, click the "Add" button.
   The panel for adding a service appears on the right.
3. Specify the service name, select a protocol (TCP or UDP), specify the port number and click the "Save" button.
   The service will be added to the list.

Note.
- To remove a service, select it in the list and click the "Delete" button. The action applies only to services that are selected on the current page.
- To modify a service, select it in the list and click the "Edit" button. The panel for editing the service with the specified parameters appears.
- To use filters, click "Filtering", set the required criteria in the appeared panel and click "Apply". To reset the search results, click the "Reset filters" button.

Deep packet inspection rules (beta version)

vGate supports deep packet inspection.

Before enabling the deep packet inspection function, deploy and configure the vGate analysis server in the network (see p.**46**).

Note. For correct operation of deep packet inspection, create allowing firewall rules (see p.146) for objects whose network traffic need to be examined. Otherwise, the network traffic will be immediately blocked.

To enable/disable deep packet inspection:

1. Enable the firewall component on ESXi servers (see p.**143**).
2. Enable deep packet inspection on ESXi servers using the clacl.exe utility (see p.**186**). To do this, open the command prompt and run the following command:
   clacl.exe firewall-dpi deploy -h **<ESXi server IP address>** -v **<vCenter>** -u **<vCenter user>** -w **<vCenter user password>** -t **<analysis server IP address>** -g **<analysis server user>** -x **<analysis server user password>** -i **<vGate server>** -k **<security administrator>** -s **<security administrator password>**

Once the command is successfully executed, the "Running" status appears in the "Deep packet inspection" column of the corresponding ESXi server on the "ESXi servers" tab.

3. To disable deep packet inspection, run the following command:

   clacl.exe firewall-dpi undeploy –h **<ESXi server IP address>** –v **<vCenter>** –u **<vCenter user>** –w **<vCenter user password>** –t **<analysis server IP address>** –g **<analysis server user>** –x **<analysis server user password>** –i **<vGate server>** –k **<security administrator>** –s **<security administrator password>**

Deep packet inspection rules are used for deep packet inspection of protected servers.

To create a deep packet inspection rule:

1. In the main menu, go to the "Firewall" section and open the "Deep packet inspection rules" tab.

   The list of rules appears.

   Note.
   - To configure the table columns, click "Column options" and select the required options.
   - To use filters, click "Filtering", set the required criteria in the appeared panel and click "Apply". To reset the search results, click the "Reset filters" button.
   - To modify the list of rules, use the "Edit" and "Delete" buttons.

2. To create a new rule, click the "Create" button.

   A panel for creating a deep packet inspection rule appears.

3. Specify the following parameters and click the "Save" button.

Parameter	Description
State	Select the rule status (Enabled/Disabled)
Object type	Types of objects (sources of network packets) this rule applies to: • virtual machine; • virtual infrastructure segment;
Object	Specify the source with the type that was selected above
Application protocol	Application protocol this rule applies to
Action	Select an action that will be executed by this rule

   The rule will be added to the list.

Container images

vGate supports integrity control of container images stored in the vSphere embedded Harbor Registry (see p.**132**).

This function is available only in vGate Enterprise Plus.

To get started with an embedded Harbor Registry in vGate:

1. Configure connection to the embedded Harbor Registry (see p.**64**).
2. Add the Harbor Registry to the list of protected servers (see p.**79**).
3. Configure rules for access to the Harbor Registry (see p.**107**). To do this, use the "User access to VMware Harbor" template.

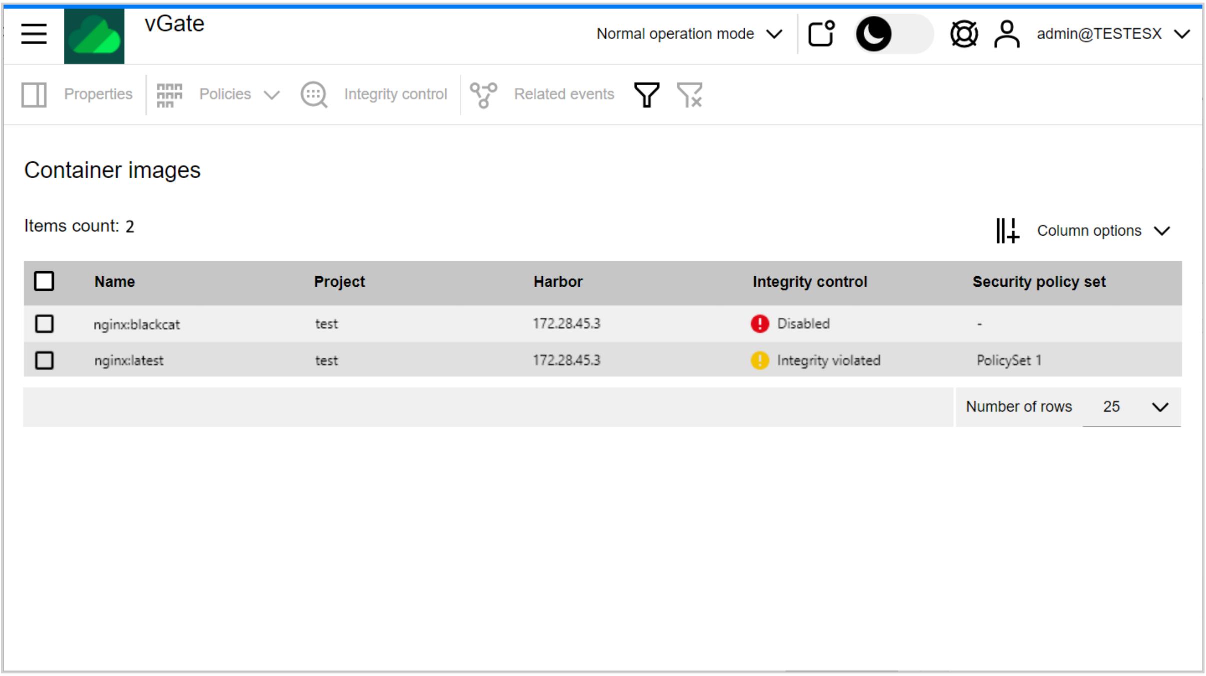
Integrity control is applied only to those container images, to which the "Integrity control of container images" policy is assigned. The policy is designed to prohibit unauthorized start of containers from images, integrity of which is compromised. Integrity control of images is performed by monitoring the invariability of their checksums.

Approving and rejecting changes

To approve or reject changes:

1. In the main menu, go to the "Container images" section:

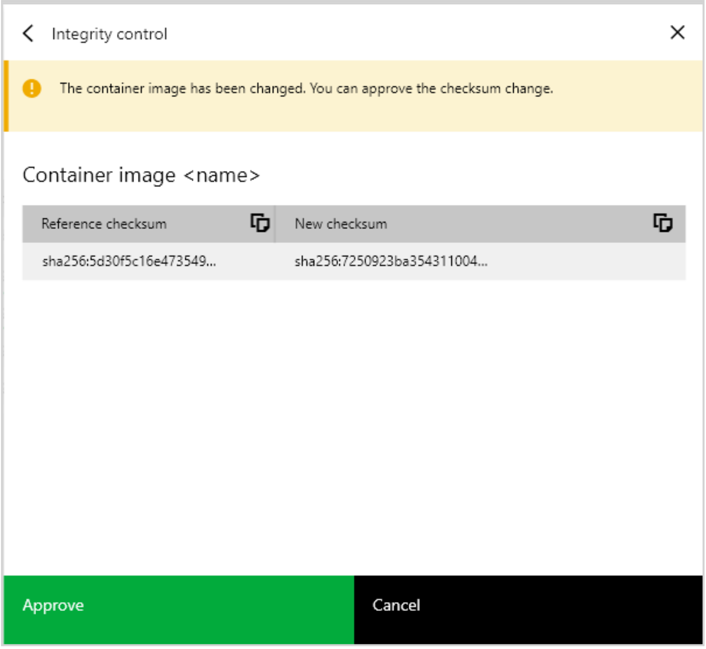
   The following window appears.



Note.

- To configure the table columns, click "Column options" and select the required options.
- To use filters, click "Filtering", set the required criteria in the appeared panel and click "Apply". To cancel the filtering, click "Reset filters".
- To view security events related to a certain server, select it and click "Related events".
- To view detailed information about a container image, select it in the list and click the "Properties" button.
- To assign a security policy set, select the required container image, click the "Policies" button and select "Assign" in the drop-down list. To unassign a policy set, select "Unassign" in the drop-down list.

2. Select the required container image in the list and click the "Integrity control" button.
   Integrity control panel appears.



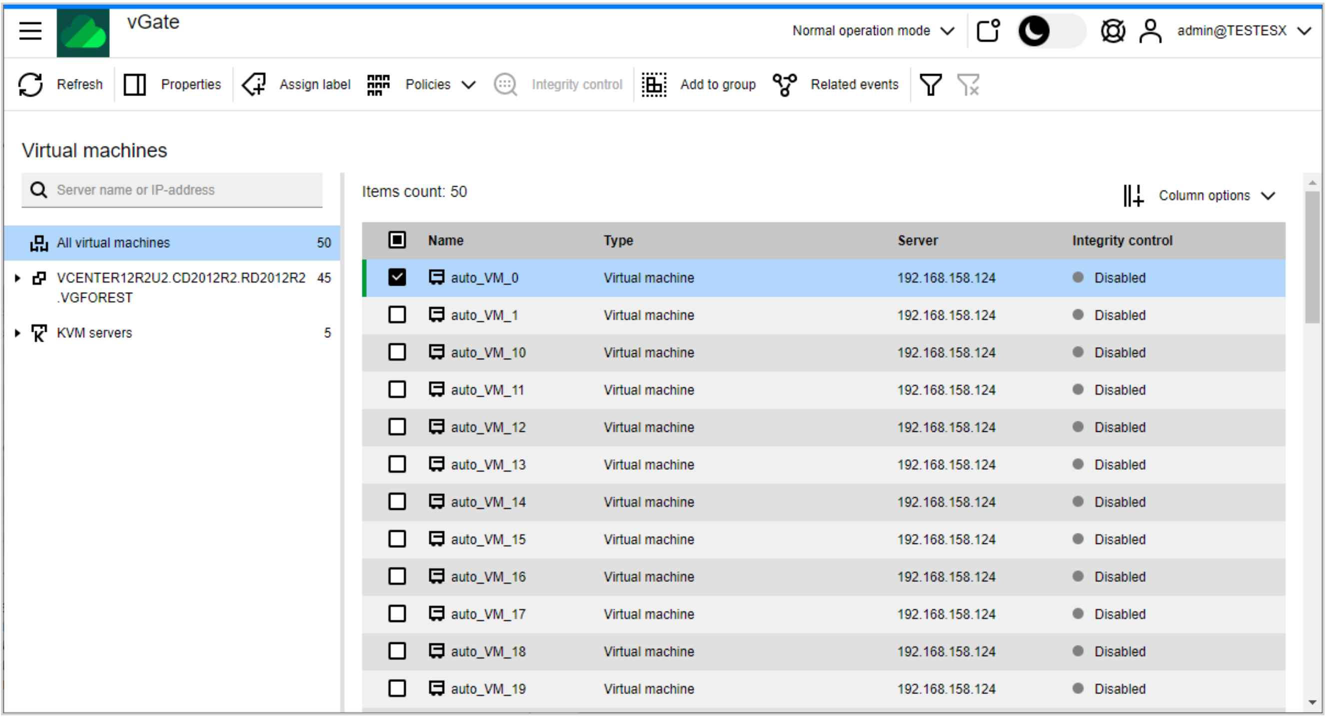
Note. To copy the checksum value, click the "Copy" button.

3. To approve the changes, click the "Approve" button.

Virtual machines

To work with virtual machines and virtual machine templates, go to the "Virtual machines" section of the main menu.

The following window appears.



Note.

- To configure the table columns, click "Column options" and select the required options.
- To refresh the list of virtual machines, click the "Refresh" button.
- To use filters, click "Filtering", set the required criteria in the appeared panel and click "Apply". To cancel the filtering, click "Reset filters".
- To view security events related to a certain virtual machine, select it and click the "Related events" button.

To view detailed information about a virtual machine, select it in the list and click the "Properties" button.

To assign or unassign a security policy, select the required virtual machine in the list and click the "Policies" button. Details on assigning security policies to objects can be found on p.**97**.

To add a virtual machine to the group, select it in the list and click the "Add to group" button. Details on how to group objects can be found on p.**91**.

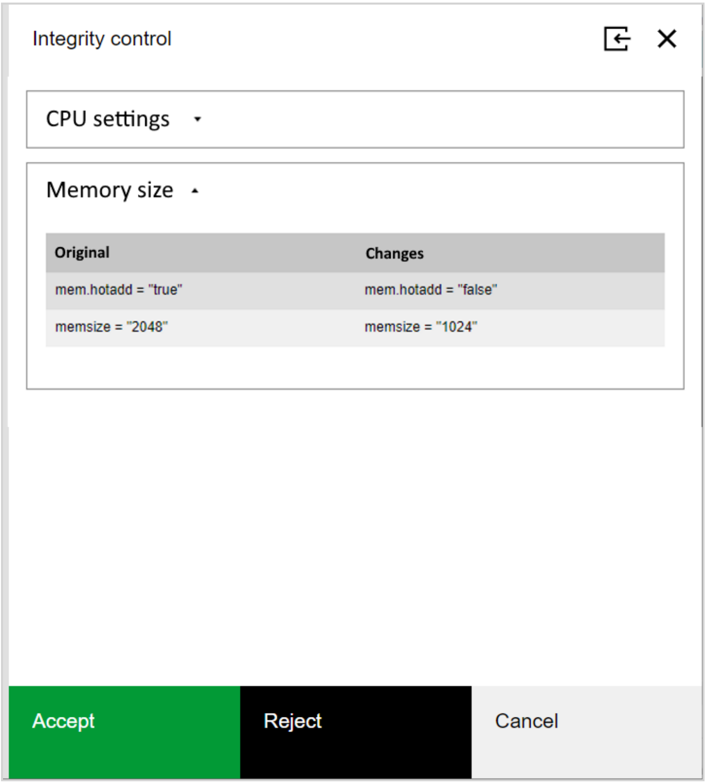
Approving and rejecting changes

vGate supports integrity control of virtual machines (see p.127). Integrity control is applied only to those virtual machines, to which the "Trusted boot loading of virtual machines" policy is assigned.

To approve or reject changes:

1. Select the required virtual machine and click the "Integrity control" button.

   Integrity control panel appears.



2. To approve changes, click "Accept". To reject changes, click "Reject".

   The system will recalculate checksums of all VM files (components). Once the operation is completed, a message informing about it will appear.

Chapter 6
Audit of security events

Security events are registered on all ESXi servers with installed vGate agents. Then, the log data is sent to the vGate server for centralized storage.

On computers with installed vGate agents in the external administration network perimeter, logs are stored locally in the Windows Application Event Log. To view them (locally or remotely), use the Windows Event Viewer.

Event properties

Table 1. Description of event properties

Property	Description
Components	
vGate proxy service	Events related to the operation of the vGate proxy service installed on the vGate server
vGate Agent for ESXi	Events related to the operation of the vGate Agent for ESXi
vGate Agent for vCenter	Events related to the operation of the vGate Agent for vCenter
vGate Agent for KVM	Events related to the operation of the vGate Agent for KVM
Authentication service	Authentication events
Integrity control service	Events related to the integrity control service operation on all computers
Remote management service[1]	Events related to the operation of the remote management service
Service for collecting events on vCenter	Events related to the operation of the service for collecting events on vCenter
Categories	
Authentication	Authentication events (attempts of access to the virtual infrastructure control elements are registered)
Virtual machines	Events related to permission or prohibition to start virtual machines
KVM virtual machines	Events related to permission or prohibition to start KVM virtual machines
General	Events related to the system in general. For example, events related to the exceeded number of licenses
Policies	Events related to security policies
Deployment	Events related to the installation of vGate agents on protected servers
Firewall	Events related to the network traffic filtering
Service	Events related to starting or stopping the services (system services)
Access rules	Events related to access control rules
Integrity	Events related to compromised integrity control
Types	
Warning	Warning about a failed operation that can be a threat to system security
Success	Message informing about successful operations related to system security
Information	Message informing about successful operations that are not directly related to system security
Error	Message informing about failed operations that are not directly related to system security
Other	

[1] Remote management service is a special service operating on the vGate server and controlling all vGate subsystems, including protected servers. The management console and the clacl.exe utility also operate using this service.

Property	Description
Date	Date and time of event
Source	Computer where the event has been registered
Event code	Unique number code of event
Description	Detailed description of event

Specific features of registration of events related to integrity control

vGate Server
Integrity violation events on the vGate server are registered in the vGate database. The check interval is set in the Windows registry, HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate\InchInterval key (in seconds). By default, the interval value is set to 600 seconds.
Virtual infrastructure administrator workstation
Integrity violation events on the virtual infrastructure administrator workstation are registered in the local Windows Application Event Log. The check interval is set in the Windows registry, HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate\InchInterval key (in seconds). By default, the interval value is set to 600 seconds.
Security administrator workstation
Integrity violation events on the security administrator workstation are registered in the local Windows Application Event Log. The check interval is set in the Windows registry, HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate\InchInterval key (in seconds). By default, the interval value is set to 600 seconds.
ESXi server
Integrity violation events on ESXi servers are registered in the vGate database. The check interval is set in the /etc/config/vgate/vgate.cfg configuration file, vagentd: section, interval parameter (in seconds). By default, the interval value is set to 600 seconds.
vCenter server
Integrity violation events on vCenter servers are registered in the vGate database. The check interval is set in the Windows registry, HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate\InchInterval key (in seconds). By default, the interval value is set to 600 seconds.

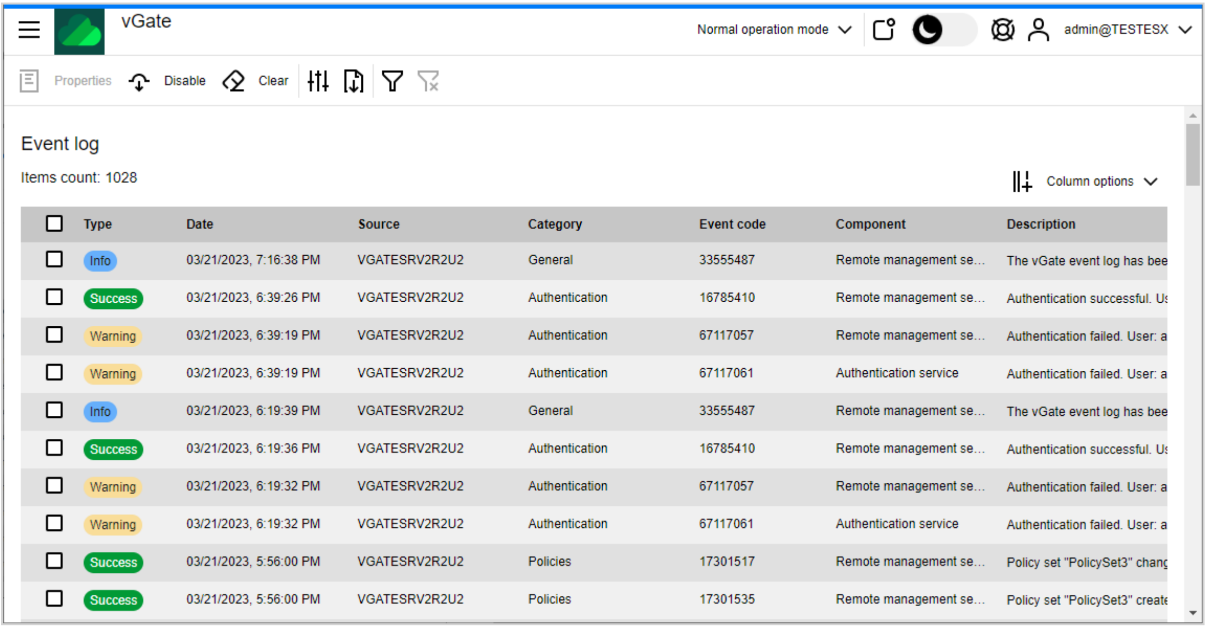
Viewing event log

In the vGate web console, you can view the security event log. It displays information on operations with virtual infrastructure segments, firewall rules and changes of vGate agent statuses. Use the drvmgr.exe utility to view detailed information about blocked network packets on ESXi servers.

To view the security event log:

1. In the main menu, go to the "Event log" section.

   A table containing the list of events appears.



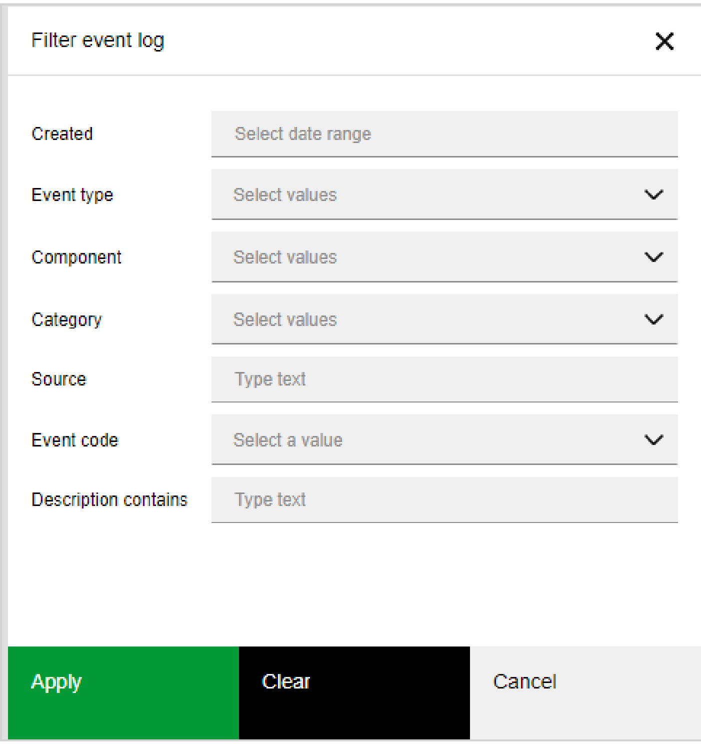
Type	Date	Source	Category	Event code	Component	Description
Info	03/21/2023, 7:16:38 PM	VGATESRV2R2U2	General	33555487	Remote management se...	The vGate event log has bee
Success	03/21/2023, 6:39:26 PM	VGATESRV2R2U2	Authentication	16785410	Remote management se...	Authentication successful. Us
Warning	03/21/2023, 6:39:19 PM	VGATESRV2R2U2	Authentication	67117057	Remote management se...	Authentication failed. User: a
Warning	03/21/2023, 6:39:19 PM	VGATESRV2R2U2	Authentication	67117061	Authentication service	Authentication failed. User: a
Info	03/21/2023, 6:19:39 PM	VGATESRV2R2U2	General	33555487	Remote management se...	The vGate event log has bee
Success	03/21/2023, 6:19:36 PM	VGATESRV2R2U2	Authentication	16785410	Remote management se...	Authentication successful. Us
Warning	03/21/2023, 6:19:32 PM	VGATESRV2R2U2	Authentication	67117057	Remote management se...	Authentication failed. User: a
Warning	03/21/2023, 6:19:32 PM	VGATESRV2R2U2	Authentication	67117061	Authentication service	Authentication failed. User: a
Success	03/21/2023, 5:56:00 PM	VGATESRV2R2U2	Policies	17301517	Remote management se...	Policy set "PolicySet3" chang
Success	03/21/2023, 5:56:00 PM	VGATESRV2R2U2	Policies	17301535	Remote management se...	Policy set "PolicySet3" create

Note.

- To enable registration of an event, select it in the table and click the "Enable" button.
- To configure the table columns, click "Column options" and select the required options.
- To configure parameters of event registration, click the "Settings" button (see p.69).

2. To filter security events, click the "Filtering" button.

   A panel for filtering the security event log appears.



3. Specify the record selection conditions.

Parameter	Description
Created	Specify the time period to search for log records (during which events have occured)
Event type	Select the required types of events
Component	Select the required vGate components
Category	Select the required categories of events
Source	Specify the source of events
Event code	Unique number code of event
Description contains	Type text to search for in event descriptions

Note. To return to the default set of record filtering parameters, click the "Clear" button.

Details on event properties can be found on p.**155**.

4. Click the "Apply" button.

   The corresponding list of events will appear in the table.

   Note. To reset the search results, click the "Reset filters" button.

5. To view detailed information about an event, select the required event and click the "Properties" button.

   The event properties panel appears.

   Tip. The "Copy" button allows you to copy the contents of all event fields to the clipboard, from where the contents can be pasted into any text editor.

6. When you finish viewing the event details, click the "Close" button.

Viewing related events for a selected object

By default, the list of events contains the records related to all objects of the virtual infrastructure. If necessary, the security administrator can quickly access the list of events related to a certain object (protected server, virtual machine, storage unit, virtual network, network adapter, user account).

To view related security events:

1. In the main menu, go to the section corresponding to the required object: "Protected servers", "Virtual machines", "Storage", "vSphere virtual networks", "vSphere network adapters", "User accounts", "Organizations" or "Container images".
2. Select the required object and click the "Related events" button. A table containing the list of security events related to the selected object appears.
3. Click the "Filtering" button. A panel for filtering the security event log appears. The "Description contains" field contains the indication of the selected object property, based on which the object-related events have been selected.

Object	Property
Protected server	Server IP address
Virtual machine	Virtual machine identifier (UUID)
Datastore	Datastore identifier
vSphere virtual network	Virtual network identifier (VLAN ID)
vSphere network adapter	Network adapter MAC address
Account	User account name
Organization	Organization name
Container image	Container image name

Saving event log

To save the security event log:

1. In the main menu, go to the "Event log" section.
   A table containing the list of events appears.
2. Click the "Download all events" button.
3. A confirmation to continue appears, click "Yes".
   Events will be saved to the .csv file. Downloading a file with a large number of events may take a long time.

Clearing event log

Tip. Before clearing the log, you can save it to a file (see above).

To clear the security event log:

1. In the main menu, go to the "Event log" section.
   A table containing the list of events appears.
2. Click the "Clear" button.
   A panel for selecting the time period appears.
3. Specify the date and time, then click "Apply".
   Records about events, registered before the specified date, will be removed from the log.

Configuring the list of registered events

By default, all possible security events are registered in the vGate log. If such a detailed monitoring is not necessary, the security administrator can disable the events that do not need to be logged (for example, configure logging of errors only).

To disable registration of an event, select it in the list and click the "Disable" button. Event log configuration is available in the "Settings" section (see p.69).

Note. Events corresponding to failed authentication attempts of an Active Directory user are not registered in the vGate server log. To register such events, configure the "Audit account logon events" policy on the domain controller. Events can be viewed in the audit on the domain controller.

vGate integration with SIEM system

vGate can send security events to SIEM systems (Security information and event management). The Syslog protocol is used to send messages.

A message contains variables (event code, category, application identifier, server name etc.), but does not include the event description. To retrieve the event description in SIEM, use the management information database (MIB). The MIB file is located on the vGate setup disk. The database is imported using the SIEM system.

Example:

Authentication error in one of the vGate services will be described in the MIB file as follows:

```
rhuidAuthFailed TRAP-TYPE
ENTERPRISE vgateTraps
VARIABLES
{
vgateMessageSeverity,
vvgateMessageCategory,
vgateApplicationID,
vgateHostName,
vgateMessageDatetime,
vgateVar1,
vgateVar2,
vgateVar3
}
DESCRIPTION
"Authentication failed. User: vgateVar1 Address: vgateVar2 Reason: vgateVar3"

--#TYPE "Authentication failed. (67117057)"
--#SEVERITY MINOR
--#CATEGORY "Authentication events"

::= 67117057
```

where:

- **vgateMessageSeverity** — code, supported values are described in the MIB file;
- **vgateMessageCategory** — message category, supported values are described in the MIB file;
- **vgateApplicationID** — application identifier, supported values are described in the MIB file;
- **vgateHostName** — name of the server from which the message was sent;
- **vgateMessageDatetime** — time when the message was sent;
- **vgateVar1, vgateVar2, vgateVar3** — variables, the values of which are not known in advance. For example, user or virtual machine name.

The message code (67117057) and all variables from the "VARIABLES" list will be sent to the SIEM system in their initial sequence.

Chapter 7
Reports

In the web console, you can prepare reports on vGate security events.

This function is available in vGate Enterprise Plus only (see the "Functionality" section in the document [1]).

Types of reports

vGate allows preparing the following types of reports:

Title	Description
vMonitor incidents	The report displays statistics on last 10 vMonitor incidents
User Activity in vGate	The report displays statistics on the most active users. The percentage ratio of authentication events and selected user accounts during the specified period is displayed
Most used protocols and ports when attempting to get unauthorized access to protected objects in vGate	The report displays statistics on the most frequently used types of access to protected objects (protocols and ports)
Top Security Events in vGate	The report displays statistics on the most frequent security events
Dashboard	The report displays graphs with monitoring events that have occurred
Firewall events	The report displays statistics on the last events in the "vNetwork" section
KVM virtual machine power on statistics	The report provides information on KVM virtual machine power on statistics during the specified period
VMware vSphere virtual machine power on statistics	The report provides information on VMware vSphere virtual machine power on statistics during the specified period
Access Control Settings	The report provides information about effective permissions for the protected infrastructure objects in vGate
Access Rules Summary in vGate	The report provides information about the access control rules for protected servers
Assigned Security Policy in vGate	The report displays which security policies are assigned to virtual infrastructure objects
Monitoring rules	The report provides information about enabled correlation rules
Firewall	The report provides information about firewall settings
Off Hours Access	The report provides information about off-hour logon attempts
Security Policy Management in vGate for vSphere	The report displays the history of changes of security policies during the specified period
Security Label History	The report displays the history of changes of security labels in the vGate mandatory access control settings during the specified period
Access Rules Management	The report displays the history of changes of vGate network access rules during the specified period
Usage of vCenter/ESXi Accounts	The report displays the usage history of vCenter/ESXi accounts associated with vGate accounts
Modification of Policy-Controlled Settings	The report provides information about unauthorized attempts to change the environment settings enforced by security policies
Security Policy Assignment in vGate for vSphere	The report provides information on events of assignment and dismissal of security policies during the specified period
Failed Logons: vGate	The report provides information about failed logon attempts to the vGate during the specified period
Failed Logons: vSphere	The report provides information about failed logon attempts to the vSphere using the VMware user account during the specified period

Title	Description
Trusted Boot Loading Issues in vGate for vSphere	The report shows which virtual machines could not be started due to compromising of their configuration itegrity
Failed Password Change Attempts in vGate	The report provides information on failed attempts to change a password for vGate account during the specified period
vGate Account Management	The report provides information on creation, modification and deletion of vGate accounts
Virtual infrastructure management	The report provides information about a user activity during the specified period
Security standards and regulations compliance	This report group provides information on servers compliance with security standards. Before creating a report, assign the required security policy set to the ESXi server

Pre-configuration

Plan

To generate reports using the web console, the following pre-configuration is required:

№	Step	Specific features	Description
1.	**Installation of the report viewer component**	Install Microsoft Report Viewer 2010 SP1 Redistributable Package and the "Report viewer" component on the computer designated to be the vGate server	See p.**15**
2.	**Parameters configuration**	Report creation parameters are configured in the "Settings" section of the web console	See p.**71**
3.	**Access rights configuration**	The following access rule for the vGate server is created in the "Access rules" section of the web console: TCP protocol, 443 destination port	See p.**108**

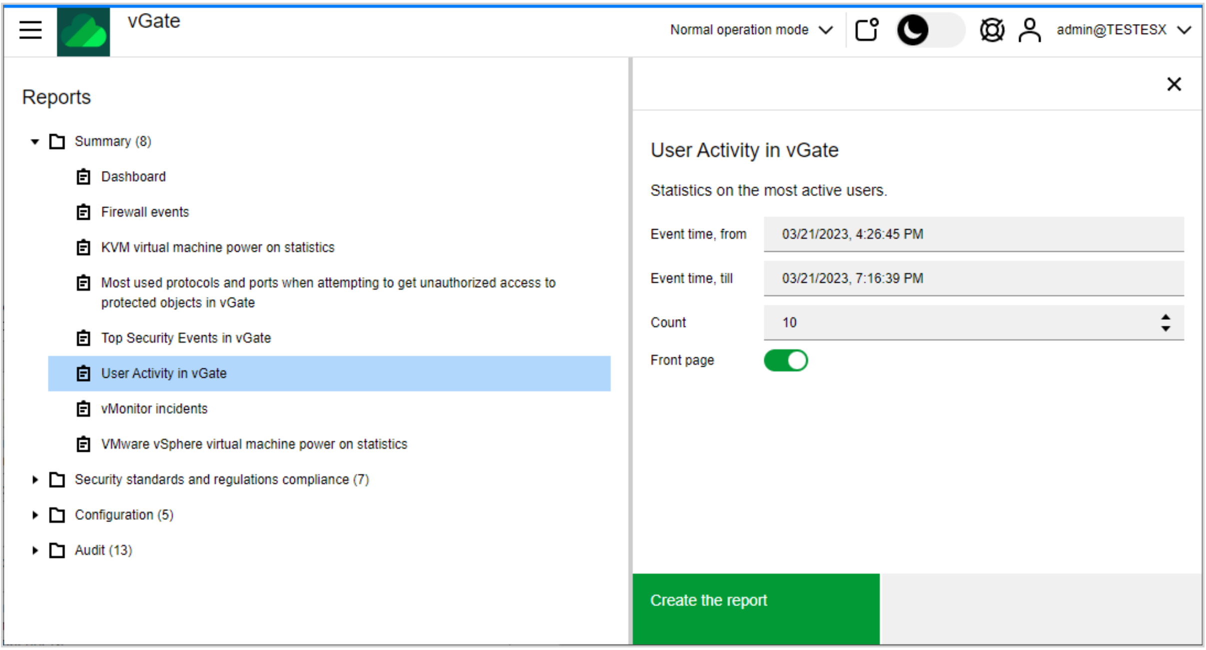
Creating reports

To create a report:

1. In the main menu, go to the "Reports" section.

The list of report categories appears.

2. Select the required report in one of the categories. A panel for configuring the report parameters appears.



3. If necessary, modify the report parameters, then click the "Create the report" button. The report will be created according to the specified settings (see p.**71**).

Parameter	Description
Event time, from	Specify the start date and time of the period during which events have been logged
Event time, till	Specify the end date and time of the period during which events have been logged
Severity	Select the required severity level from the drop-down list. This parameter is specified for the "vMonitor incidents" and "Monitoring rules" reports
Count	Specify the number of items in the statistics
Front page	To create a report with the front page, turn on this toggle
Last, days	Specify the number of days to generate a report. This parameter is specified for the "VMware vSphere virtual machine power on statistics" report
Expand	Select the security standards, information about compliance with which will be provided in the report. This parameter is specified for the "Security standards and regulations compliance" group of reports
Object	Select objects to be included in the report
Include policy descriptions	To add policy descriptions to the report, turn on this toggle
Policy sets	Select policy sets to be included in the report
Group by	Select the method of data grouping in the report
Object type	Select types of objects to be included in the report
Initiator	Select user accounts to be included in the report
ESXi servers	Select ESXi servers to be included in the report
Business hours, from	Specify the start date and time of the period that will be considered a working day. This parameter is specified for the "Off Hours Access" report
Business hours, till	Specify the end date and time of the period that will be considered a working day. This parameter is specified for the "Off Hours Access" report
Number of events	Specify the number of events in the report. For the "Virtual infrastructure management" and "Usage of vCenter/ESXi Accounts" reports, specify the number of events for each selected user. For the "Access Rules Management" report, specify the number of events for each object/user
Actions	Select operations with respect to the data to be included in the report
vCenter/ESXi accounts	Select vCenter/ESXi accounts to be included in the report. This parameter is specified for the "Usage of vCenter/ESXi Accounts" report
Interval, minutes	Specify the event logging interval. This parameter is specified for the "Modification of Policy-Controlled Settings" report
Failed attempts, from	Specify the minimum number of failed logon attempts at which an event will be added to the report. This parameter is specified for the "Failed Logons: vGate" and "Failed Logons: vSphere" reports

Appendix

Manual vGate Agent installation on vCenter

The vGate Agent installation on the vCenter server (VMware vSphere 6.5 or 6.7) deployed on Windows OS is performed during the vGate setup in the web console (see p.85). If necessary, the component can be installed using the vGate setup program directly on the computer with the installed VMware vCenter.

Note.

- vGate Standard allows you to protect one vCenter server only. If several vCenter servers are operated in a company, and these servers are interconnected using the VMware vCenter Linked Mode, the vGate agent must be installed on each of them. This function is available in vGate Enterprise and Enterprise Plus only (see the "Functionality" section in the document [1]).
- If the Secret Net Studio software is operated on the computer, where the vGate agent for vCenter will be installed, you must disable the Secret Net firewall before installation.

To install the vGate Agent on the vCenter server:

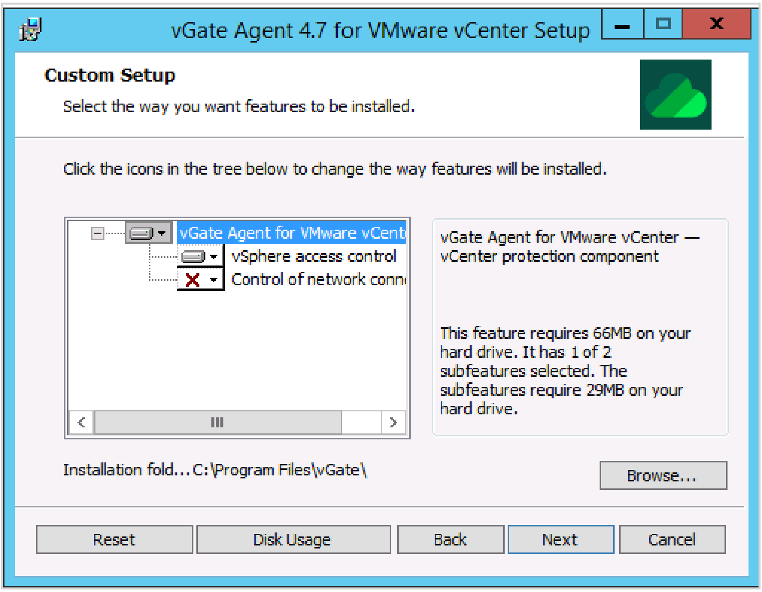
1. Log in using the computer administrator permissions.
2. Insert the setup disk into the CD-ROM drive.
3. Run the vGateVpxAgent.msi file from the setup disk.

   The setup program will complete certain preparations, after which the welcome dialog box will appear.
4. Click "Next".

   The license agreement dialog box appears on the screen.
5. Read the entire license agreement, select the "I accept the terms in the License Agreement" check box and click "Next".

   Tip. In order to obtain a paper copy of the license agreement, click "Print".

   A dialog box to select components to be installed appears.

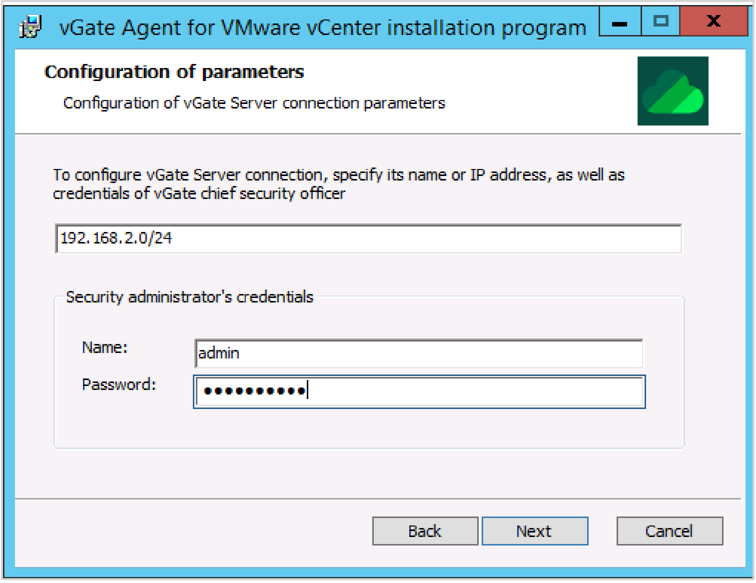


Note. The "Control of network connections" is not installed by default. If the component is selected for installation, incoming network connections will be restricted after the vGate Agent installation on the vCenter server. Details on configuring the vCenter traffic filtering can be found on p.111.

Tip. To select the component for installation, open the drop-down menu to the left of the component name and select "Will be installed on local hard drive". To prohibit the component installation, in the drop-down menu to the left of the component name select "Entire feature will be unavailable".

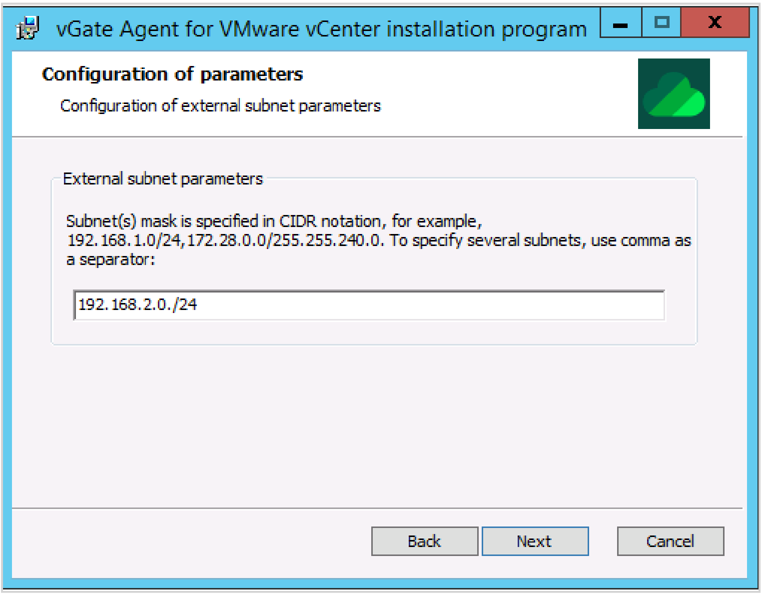
6. If necessary, modify the path to the setup directory, and click "Next".

The following dialog box appears.



7. Enter the name or IP address of the vGate Server, as well as the security administrator credentials, then click "Next".

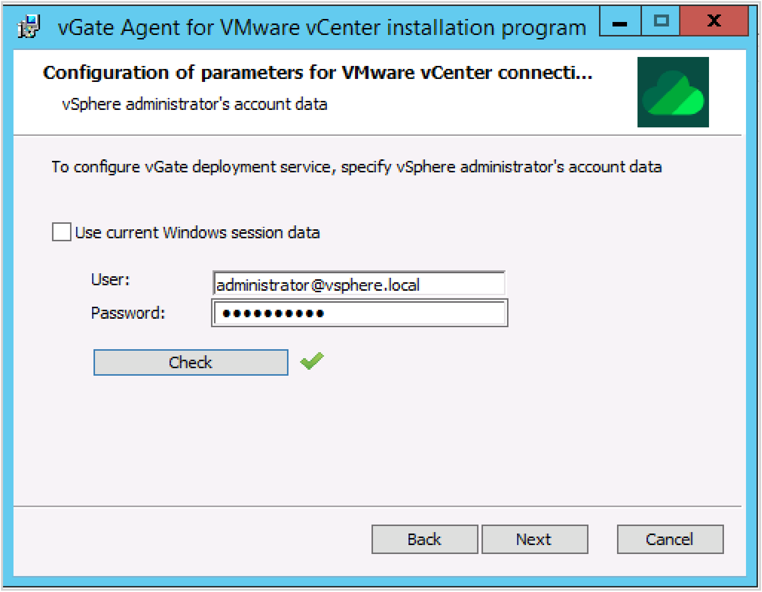
If the "Control of network connections" component was selected during the step **5**, the following dialog box will appear on the screen.



8. Specify parameters of the external virtual infrastructure administration subnet (subnets), where secure administrator and virtual infrastructure administrator workstations are located, and click the "Next" button.

Note. Connection to vCenter will be allowed only if the administrator workstation IP address corresponds to one of the specified subnets.

The following dialog box appears.



9. Specify the vSphere administrator credentials to configure the vGate deployment service, and click the "Check" button to verify the specified credentials.

Note. A message informing about the check results appears. In the message box, click "OK".

If the "Use current Windows session data" check box is selected, the system account will be used.

Click "Next". A dialog box appears saying that everything is ready for the installation.

10. Click "Install".

The process of file copying to the hard disk and configuring the installed components will be started. The progress will be displayed in the installation program dialog in the form of a progress bar.

After successful installation and configuration of components, a dialog box informing about successful completion of the installation will appear.

11. Click "Finish".

Note. In some cases, a requirement to restart the computer may appear. To restart, click "Yes".

User privileges in the VMware vSphere environment

Different operations in the VMware vSphere virtual infrastructure are available for different vGate user types.

Role	Available operations
Virtual machine administrator	**Virtual machines** • Power on, power off, restart a VM. • Suspend a VM. • Access a VM console. • Access a VM console by VMRC. • Change VM settings. • Restart a guest OS. • Shut down a guest OS. • Clone a VM. • Clone a VM to a template. • Convert a VM to a template. • Convert a template to a VM. • Clone a template to a template. • Migrate a VM. • Create a VM. • Create a VM from a template. • Delete a VM. • Delete a template from Disk. • Remove a VM from Inventory • Export a VM (you must have the "File operations in data storages" privilege). • Delete a folder (for VM). • Import a VM. • Import an OVF VM. • Export a VM to OVF (you must have the "File operations in data storages" privilege). • Operations with VM snapshots (take snapshot, rename snapshot, delete snapshot, delete all snapshots). • Revert to latest VM snapshot. • Revert to a VM snapshot. • Consolidate VM disks. • Register a VM from a datastore. • Register a VM from a datastore to a vApp. • Operations with scheduled tasks: power on a VM, shut down a guest OS, restart a guest OS, power off a VM, suspend a VM, restart a VM, migrate a VM, clone a VM, change VM settings, take a VM snapshot, create a new VM (security label inheritance is not supported), change a scheduled task, run a scheduled task, remove a scheduled task. To perform these operations, you must have the "Operations with scheduled tasks" privilege. • Move a VM to a different vApp or resource pool. **vApp (virtual machine group)** • Power on, power off, suspend a vApp. • Clone a vApp. • Create a vApp. • Delete a vApp from Disk. • Delete a folder (for vApp). • Remove a vApp from Inventory. • Export and import a vApp

Role	Available operations
Virtual machine user	**Virtual machines** • Power on a VM. • Power off a VM. • Shut down a guest OS. • Access a VM console. • Restart a guest OS. • Restart a VM. • Suspend a VM. • Take snapshots of a VM console. • Delete a folder (for VM). • Operations with scheduled tasks: power on a VM, shut down a guest OS, restart a guest OS, power off a VM, suspend a VM, restart a VM, change VM settings, change a scheduled task, run a scheduled task, remove a scheduled task. To perform these operations, you must have the "Operations with scheduled tasks" privilege. **vApp (virtual machine group)** • Power on a vApp. • Power off a vApp. • Suspend a vApp
Network administration	• Create port groups. • Edit port groups. • Delete a folder (for VM). • Edit virtual switch settings
Virtualization server administration	• Add a host to a cluster. • Place a host in Maintenance mode. • Place a host in Lockdown mode. • Disconnect a host from vCenter. • Connect/reconnect a host to vCenter. • Shut down a host. • Reboot a host. • Place a host in standby mode. • View ESXi log files. • Upload files to an AutoDeploy datastore. • Remove a host that is a part of a cluster from the vCenter inventory. • Remove a cluster from the vCenter inventory. • Delete a folder (for host). • Delete a folder (for VM). • Add a standalone host to a vCenter. • Add a host to a vCenter cluster. • Stop/start/restart a host service. • Edit host service policies. • Enable/edit/disable firewall rules. • Change advanced settings of a host. • Edit the time configuration settings of a host. • Edit date and time. • Edit VM startup. • Manage a host acceptance level. • Install packet updates. • Edit dump encryption settings. • Add a host to a cluster/remove a host from a cluster. • Create/edit/delete a host profile. • Attach/apply/detach a host profile. • Attach/apply/detach a host profile (in a cluster).

Role	Available operations
	• Enable/edit/disable firewall rules. • Edit host customizations. • Edit host customizations (in a cluster). • Reset host customizations. • Add vFlash resource capacity. • Operations with scheduled tasks: add a host to a cluster, edit a resource pool, change a scheduled task, run a scheduled task, remove a scheduled task. To perform these operations, you must have the "Operations with scheduled tasks" privilege
Storage administration	• View datastore information. • Delete a datastore (you must have the "Virtualization server administrator" privilege). • Browse files in a datastore. • Delete a file from a datastore. • Move files between datastores. • Copy files between datastores. • Format VM disks. • Modify a datastore capacity. • Modify VM disk capacity. • Create a datastore (you must have the "Virtualization server administrator" privilege). • Rename a datastore. • Mount a datastore (you must have the "Virtualization server administrator" privilege). • Unmount a datastore (you must have the "Virtualization server administrator" privilege). • Mount/rename/remove an NFS datastore (you must have the "Virtualization server administrator" privilege). • Expand a datastore. • Clear a partition table. • Delete a folder (for VM)
File operations in data storages	• Upload files or folders to datastores. • Download files from datastores. • Import an OVF VM. • Export a VM to OVF (you must have the "Virtual machine administrator" privilege)
vSAN administrator	• Enable/disable a vSAN cluster. • Enable/disable deduplication and compression. • Enable/disable encryption. • Edit encryption settings. • Generate new encryption keys. • Edit the "Allow reduced redundancy" option. • Enable/disable the vSAN iSCSI Target Service. • Edit vSAN Advanced Options. • Claim unused disks. • Create a disk group. • Add disks to a group. • Remove a disk from a group/remove a disk group. • Mount a disk group. • Unmount a disk group. • Recreate a disk group. • Manage a fault domain. • Move a host to a domain. • Move host out of a domain. • Remove a fault domain. • Configure a stretched cluster. • Disable a stretched cluster.

Role	Available operations
	• Change the vSAN witness host. • Add a new iSCSI Target. • Edit an iSCSI Target. • Remove an iSCSI Target. • Add Allowed Initiators to the vSAN iSCSI Target. • Remove Allowed Initiators from the vSAN iSCSI Target. • Add, change and remove a vSAN iSCSI LUN. • Connect and disconnect a vSAN iSCSI LUN. • Create and delete a vSAN iSCSI Initiator Group. • Add a vSAN iSCSI Initiator to the Initiator Group. • Remove a vSAN iSCSI Initiator from the Initiator Group. • Add a new accessible target for a client/group. • Delete an accessible target for a client/group
Cloud Director administrator	• Log in to the Cloud Director interface. • Create and delete an organization. • Activate and deactivate an organization. • Migrate a tenant storage. • Open an organization on the tenant portal. • Edit an organization name. • Edit an organization name/description. • Configure catalogs, email and policies for an organization. • Configure SAML. • Regenerate a SAML certificate. • Configure LDAP. • Create and delete a virtual data center. • Activate or deactivate an organization virtual data center. • Open an organization virtual data center on the tenant portal. • Edit a virtual data center name/description. • Edit the resource allocation settings of a virtual data center. • Modify the storage settings of a virtual data center. • Activate/deactivate a VM storage policy for a virtual data center. • Assign the default VM storage policy to a virtual data center. • Edit the limit of a VM storage policy on a virtual data center. • Edit the network settings of a virtual data center. • Activate or deactivate a VM placement policy for a virtual data center. • Assign the default VM placement policy to a virtual data center. • Activate/deactivate a VM sizing policy for a virtual data center. • Assign the default VM sizing policy to a virtual data center. • Activate/deactivate the distributed firewall feature. • Add, edit, delete a distributed firewall rule with the General category. • Add, edit, delete a distributed firewall rule with the Ethernet category. • Add, edit and delete an IP set. • Add, edit and delete a MAC set. • Add, edit and delete a security group. • Add, edit and delete a security tag. • Create, edit and delete an edge gateway. • Edit the general settings of an edge gateway. • Edit an edge gateway network and subnet. • Edit the default gateway of an edge gateway. • Edit the rate limits of an edge gateway. • Edit the IP settings of an edge gateway.

Role	Available operations
	• Edit the suballocated IP pools on an edge gateway. • Redeploy an edge gateway. • Activate/deactivate distributed routing on an edge gateway. • Edit firewall rules of an edge gateway. • Configure DHCP for an edge gateway. • Configure NAT for an edge gateway. • Configure routing on an edge gateway. • Edit the load balancer settings on an edge gateway. • Configure IPsec VPN for an edge gateway. • Configure L2 VPN for an edge gateway. • Configure SSL VPN-Plus for an edge gateway. • Configure a set of SSL certificates for an edge gateway. • Edit the syslog server settings for an edge gateway. • Configure the SSH settings for an edge gateway. • Work on the tenant portal

Access to virtual machine files

To access the virtual machine files located in the storage area network (SAN), configure the vGate software respectively.

To configure access to files:

1. Edit the user account, that will be used to perform operations with files, select the "File operation in data storages" and "Virtual machine administrator" check boxes (see p.**87**).
2. For the required ESXi server, create the "Manage ESXi server infrastructure" rule, applied to the user from the step **1**.

Note. If there are several ESXi servers, create the rule for each of them.

TCP and UDP ports used in vSphere

ESXi server

Port	Protocol	Source	Destination	Purpose
9	UDP	vCenter Server	ESXi Host	Used by Wake-on-LAN
22	TCP	SSH Client	ESXi Host	Required for SSH access
53	UDP	ESXi Host	DNS Server	DNS client
68	UDP	DHCP Server	ESXi Host	DHCP client for IPv4
80	TCP	Web Browser	ESXi Host	Welcome page with download links for different interfaces
161	UDP	SNMP Server	ESXi Host	Allows ESXi servers to connect to an SNMP server
427	TCP/UDP	CIM Server	ESXi Host	The CIM client uses the Service Location Protocol, version 2 (SLPv2) to find CIM servers
443	TCP	vSphere Web Client	ESXi Host	Client connections
546	TCP/UDP	DHCP Server	ESXi Host	DHCP client for IPv4
547	TCP/UDP	ESXi Host	DHCP Server	DHCP client for IPv4
902	TCP/UDP	VMware vCenter Agent	ESXi Host	vGate Agent for vCenter
2233	TCP	ESXi Host	vSAN Transport	vSAN reliable datagram transport. Uses TCP and is used for vSAN storage IO. If disabled, vSAN does not work
3260	TCP	ESXi Host	Software iSCSI Client	Software for iSCSI

Port	Protocol	Source	Destination	Purpose
5671	TCP	ESXi Host	RabbitMQ proxy	A proxy running on the ESXi host that allows applications running inside virtual machines to communicate to the AMQP brokers running in the vCenter network domain. The virtual machine does not have to be on the network, that is, no NIC is required. The proxy connects to the brokers in the vCenter network domain. Therefore, the outgoing connection IP addresses should at least include the current brokers in use or future brokers. Brokers can be added if customer would like to scale up
5988, 8889	TCP	CIM Server 8889-OpenWSMAN Daemon	ESXi Host	5988 is a server for CIM (Common Information Model). 8889 is a WS-Management (Web Services Management)
5989	TCP	CIM Secure Server	ESXi Host	Secure server for CIM
6999	UDP	NSX Distributed Logical Router Service	ESXi Host	NSX Virtual Distributed Router service (NSX Distributed Logical Router in earlier versions of the product). The firewall port associated with this service is opened when NSX VIBs are installed and the VDR module is created. If no VDR instances are associated with the host, the port does not have to be open
8000	TCP	ESXi Host	ESXi Host	It is required for a virtual machine migration with vMotion. ESXi servers listen on port 8000 for TCP connections from remote ESXi servers for vMotion traffic
8080	TCP	vsanvp	ESXi Host	VSAN VASA Vendor Provider. Used by the Storage Management Service (SMS) that is a part of vCenter to access information about vSAN profiles, capabilities and compliance. If this parameter is disabled, Virtual SAN Storage Profile Based Management (SPBM) is not available
8100, 8200, 8300	TCP/UDP	Fault Tolerance	ESXi Host	Traffic between servers for vSphere Fault Tolerance (FT)
8301, 8302	UDP	DVSSync	ESXi Host	DVSSync ports are used to synchronize states of distributed virtual ports between servers that have VMware FT record/replay enabled. Only hosts that run primary or backup virtual machines must have these ports open. On hosts that are not using VMware FT these ports do not have to be open
12345, 23451	UDP	ESXi Host	vSAN Clustering Service	Cluster Monitoring, Membership, and Directory Service used by vSAN
44046, 31031	TCP	ESXi Host	HBR	Used for ongoing replication traffic by vSphere Replication and VMware Site Recovery Manager
80, 9000	TCP	ESXi Host	vCenter Server	vSphere Update Manager

vCenter

Port	Protocol	Purpose
22	TCP	System port for SSHD
53	TCP/UDP	DNS service port
80	TCP	vCenter server requires port 80 for direct HTTP connections. Port 80 redirects requests to the HTTPS port 443
88	TCP	Active Directory server. This port must be opened for server to join Active Directory
123	UDP	NTP client port
135	UDP	vCenter Server Appliance port for the Active Directory authentication
161	UDP	SNMP server port
389	TCP/UDP	This is the LDAP port number for the Directory Services for the vCenter server group. The port should be opened on the local and all remote instances of the vCenter servers
443	TCP	The default port used by the vCenter Server system to listen for connections from the vSphere client. The port is used to get information about third-party client connections to servers
514	TCP/UDP	vSphere Syslog Collector port for the vCenter server on Windows and vSphere Syslog Service port for vCenter Server Appliance
636	TCP	vCenter Single Sign-On LDAPS port. For backward compatibility with vSphere 6.0 only
902	TCP/UDP	The default port used by the vCenter Server to send data to managed hosts. Managed hosts also regularly send data via the UDP port 902 to the vCenter server. This port must not be blocked by firewalls between the server and hosts or between hosts
1514	TCP	vSphere Syslog Collector TLS port for the vCenter server on Windows and vSphere Syslog Service TLS port for vCenter Server Appliance
2012	TCP	RPC control interface port for vCenter Single Sign-On
2014	TCP	RPC port for all VMCA (VMware Certificate Authority) APIs
2015	TCP	DNS management port
2020	TCP/UDP	Authentication management port
5480	TCP	Appliance Management Interface port
6500	TCP/UDP	ESXi Dump Collector port
6501	TCP	Auto Deploy service port
6502	TCP	Auto Deploy control port
7080, 12721	TCP	Secure Token Service internal ports
7081	TCP	VMware Platform Services Controller Web Client internal port
7475, 7476	TCP	VMware vSphere Authentication Proxy port
8109	TCP	VMware Syslog Collector service port. The service is used for centralized collection of log files
8200, 8201, 8300, 8301	TCP	vCenter Appliance Management internal ports
8084	TCP	vSphere Update Manager SOAP port for vSphere v6.x, vSphere Lifecycle Manager SOAP port for vSphere v7.x
9084	TCP	vSphere Update Manager Web Server port for vSphere v6.x, vSphere Lifecycle Manager Web Server Port for vSphere v7.x. HTTP port used by ESXi servers to access path files from the vSphere Update Manager server
9087	TCP	vSphere Update Manager Web SSL port for vSphere v6.x, vSphere Lifecycle Manager Web SSL port for vSphere v7.x. HTTPS port that is used by the vSphere Update Manager client plug-in to upload host update files to the vSphere Update Manager server
9443	TCP	vSphere Client HTTPS port

Port	Protocol	Purpose
15007, 15008	TCP	vService Manager (VSM) port. This service registers vCenter server extensions. Open this port only if it is required by the extensions that you plan to use
15080	TCP	Analytics service internal port
31031, 44046 (by default)	TCP	vSphere Replication port
5355	UDP	The systemd-resolve process uses this port for allowing domain names, IPv4 and IPv6 addresses, DNS resource records and services

vCenter ports for internal communication

Port	Protocol	Purpose
5443	TCP	Internal port for the vCenter server GUI
5444, 5432	TCP	Internal port for monitoring vPostgreSQL
5090	TCP	Internal port for the vCenter server GUI
7080	TCP	Secure Token Service internal port
7081	UDP	Platform Services Controller internal port
8000	UDP	ESXi Dump Collector internal port
8006	UDP	Monitoring of the Virtual SAN performance
8085	TCP/UDP	Internal ports that are used by the vCenter VPXD SDK service
8095	TCP	Port for VMware vCenter services
8098, 8099	TCP/UDP	Port that is used by VMware Image Builder Manager
8190, 8191, 22000, 22100, 21100	TCP	VMware vSphere Profile-Driven Storage service port
8200, 8201, 5480	TCP/UDP	Appliance Management internal ports
8300, 8301	TCP	Appliance Management reserved ports
8900	TCP	Internal port for monitoring API
9090	TCP	vSphere Web Client internal port
10080	TCP	Inventory service internal port
10201	TCP/UDP	Message Bus Configuration Service internal port
11080	TCP	vCenter Server Appliance internal ports for HTTP and screen saver
12721	TCP/UDP	Secure Token service internal port
12080	TCP	Licensing service internal port
12346, 12347, 4298	TCP	Internal port for VMware Cloud Management SDKs (vAPI)
13080, 6070	TCP	Port that is used by the Performance Charts service
14080	TCP	Port that is used by the Syslog service
15005, 15006	TCP	ESX Agent Manager internal port
16666, 16667	TCP	Content Library ports

List of access rule templates

Protocol	Source port	Destination port
Manage ESXi Server infrastructure		
TCP	Any	443
TCP	Any	902
Access to virtual machine console		
TCP	Any	902
Access to ESXi via SSH		
TCP	Any	22
Access to a domain controller in the protected administration network		
TCP	Any	53
TCP	Any	88
TCP	Any	135
TCP	Any	139
TCP	Any	445
TCP	Any	464
TCP	Any	3268
TCP	Any	3269
UDP	Any	53
UDP	Any	88
UDP	Any	135
UDP	Any	138
UDP	Any	389
UDP	Any	445
UDP	Any	464
Host availability check (ping command)		
ICMP	Any	Any
Allow DNS name search		
UDP	Any	53
User access to vCenter		
TCP	Any	80
TCP	Any	443
TCP	Any	514
TCP	Any	1514
TCP	Any	6500
TCP	Any	6501
TCP	Any	6502
TCP	Any	8000
TCP	Any	8001
TCP	Any	8084
TCP	Any	9084
TCP	Any	9087

Protocol	Source port	Destination port
TCP	Any	8098
TCP	Any	8099
TCP	Any	8109
View Connection Server access to vCenter		
TCP	Any	443
TCP	Any	8443
TCP	Any	18443
Allow access to View Connection Server		
TCP	Any	443
TCP	Any	80
vGate Report Viewer access to vGate Server		
TCP	Any	5432
vGate Server administration		
TCP	Any	3802
TCP	Any	3803
TCP	Any	3806
vGate Server administration via web console		
TCP	Any	443
Allow SNMP monitoring of protected servers		
UDP	Any	161
Allow the reception of SNMP traps		
UDP	Any	162
Allow Remote Desktop connections		
TCP	Any	3389
Allow vGate authentication service connections		
TCP	Any	3801
UDP	Any	3801
TCP	Any	3800
UDP	Any	3800
UDP	Any	88
UDP	Any	3808
User access to VMware vSphere virtual infrastructure components		
TCP	Any	443
Allow access to vRealize Operations Manager		
TCP	Any	443
User access to the Embedded Harbor Registry		
TCP	Any	443
Access to the vGate server for user authentication via the web interface		
TCP	Any	3900
Access Web Client Remote Console Plug-in for vCenter		
TCP	Any	443
User access to the protected server with authentication via the web interface		
TCP	Any	443

Protocol	Source port	Destination port
User access to the Skala-R Management server		
TCP	Any	443
User access to the Proxmox virtualization server web inteface		
TCP	Any	8006
User access to the protected Proxmox virtualization server with authentication via the web inteface		
TCP	Any	8006

Integrity control. List of vGate modules to be checked

The list of vGate modules to be checked is presented in the esign.json configuration file, which can be found in the vGate setup directory.

List of frequently used passwords

The list of frequently used passwords contains the list of WellKnown passwords. When creating a user account or changing a password, the system makes sure the new password is not included in the list.

The list of frequently used passwords is stored in the pwdict.txt file in the following directory on the vGate server: \<vGate setup directory>\Kerberos\.

If necessary, the list of passwords can be modified.

To modify the list of passwords:

1. Open the pwdict.txt file in any text editor.
2. Edit the list of passwords. When adding a new password to the list, put each password on a new line.
3. Save the file with the same name.
4. Restart the "vGate Kerberos KDC Service" service.

Note. While using the replication mechanism, the list of frequently used passwords is not automatically copied to the redundant server. The file with the list of passwords must be copied manually in advance.

List of basic operations with confidential resources and their execution conditions

To grant the virtual infrastructure administrator access to virtual infrastructure objects for executing basic operations, certain conditions must be met. As a rule, permissions to perform operations are regulated by the mandatory access control mechanism on the basis of security labels assigned to virtual infrastructure objects and user accounts (details can be found in the "Configuring mandatory control of access to confidential resources" section of the document [1]).

Some operations are regulated by security policies (details can be found in the "Security policies" section of the document [1]) or by special user privileges. Some operations with virtual infrastructure objects are not regulated, i. e. they are always available.

In the table below, operations, which are regulated by the mandatory access control mechanism, and their execution conditions when using the session level control mechanism are presented (see p.60). If one of the conditions is not met, the operation will not be executed.

Attention! If the session level control mechanism is disabled, the user session level must be higher or equal to the object confidentiality level, in order to execute the operations below.

Conditions of operation execution	
Confidentiality level	**Confidentiality categories**
VM PowerOn	
1. The user session level must be equal to the VM confidentiality level. **2.** If the "Allowed to run VM with a lower confidentiality level" option is enabled, the ESXi server confidentiality level must be not lower than the VM confidentiality level. Otherwise, the ESXi server confidentiality level must be equal to the VM confidentiality level	**1.** The list of user categories must include at least one VM category. **2.** The list of ESXi server categories must include at least one VM category
VM PowerOff/Reset/Suspend	
The user session level must be equal to the VM confidentiality level	The list of user categories must include at least one VM category
Restart Guest/Shutdown Guest	
The user session level must be equal to the VM confidentiality level	The list of user categories must include at least one VM category
VM Migrate (VMMotion)	
1. The user session level must be equal to the confidentiality level of the target ESXi server. **2.** If the "Allowed to run VM with a lower confidentiality level" option is enabled for the target ESXi server, the confidentiality level of this server must be not lower than the VM confidentiality level. Otherwise, the target ESXi server confidentiality level must be equal to the VM confidentiality level	**1.** The list of user categories must include at least one of the target ESXi server categories. **2.** The list of target ESXi server categories must include at least one VM category
VM Delete from Disk	
The user session level must be equal to the VM confidentiality level	The list of user categories must include at least one VM category
VM Create	
The confidentiality level of the storage, which is selected for storing the VM disks, is automatically assigned to the VM. **1.** The user session level must be equal to the ESXi server confidentiality level. **2.** If the "Edit the virtual machine settings before completion" option is selected during the last step of VM creation, the VM confidentiality level must be equal to the confidentiality level of the virtual network to which the VM is connected (if there is a virtual network)	The category from the storage list of categories, which matches the category from the user list of categories, is automatically assigned to the VM. If there are several of them, the list of categories is assigned to the VM. **1.** The list of user categories must include at least one ESXi server category. **2.** If the "Edit the virtual machine settings before completion" option is selected during the last step of VM creation, the list of VM confidentiality categories must include at least one of the categories of each virtual network to which the VM is connected (if there is a virtual network)

Conditions of operation execution	
Confidentiality level	**Confidentiality categories**
Relocate VM (Change Datastore)	
1. The user session level must be equal to the confidentiality level of the target ESXi server to which the VM is relocated. 2. If the "Allowed to run VM with a lower confidentiality level" option is enabled for the target ESXi server, the confidentiality level of this server must be not lower than the VM confidentiality level. Otherwise, the target ESXi server confidentiality level must be equal to the VM confidentiality level. 3. If the "Allowed to store VM with the lower level" option is enabled for the target storage, the confidentiality level of this storage must be not lower than the VM confidentiality level. Otherwise, the target storage confidentiality level must be equal to the VM confidentiality level	1. The list of user categories must include at least one of the target ESXi server categories. 2. The target ESXi server list of categories must include at least one VM category. 3. The target storage list of categories must include at least one VM category
Clone VM	
1. The user session level must be equal to the VM confidentiality level. 2. The target ESXi server confidentiality level must be equal to the VM confidentiality level. 3. The target storage confidentiality level must be equal to the VM confidentiality level. 4. The VM confidentiality level is inherited	1. The list of user categories must include at least one VM category. 2. The list of target ESXi server categories must include at least one VM category. 3. The target storage list of categories must include at least one VM category. 4. The VM confidentiality category is inherited
VM Edit settings	
The user session level must be equal to the VM confidentiality level	The list of user categories must include at least one VM category
VM Edit Network **VM Properties->Edit Settings->Hardware->Add->Ethernet Adapter** **VM Properties->Edit Settings->Hardware->[selecting adapter]->Remove** **VM Properties->Edit Settings->Hardware->[selecting adapter]->Network Label**	
1. The user session level must be equal to the VM confidentiality level. 2. If the "Can connect to networks with a lower level" option is enabled for VM, the VM confidentiality level must be not lower than the confidentiality level of each virtual network to which the VM is connected, or physical adapter (if virtual networks are not used). If the "Can connect to networks with a lower level" option is disabled, the VM confidentiality level must be equal to the confidentiality level of the virtual network to which the VM is connected, or physical adapter (if virtual networks are not used)	1. The list of user categories must include at least one VM category. 2. The list of VM categories must include at least one of the categories of each virtual network to which the VM is connected (if they are available), or physical adapter (if virtual networks are not used)

Conditions of operation execution	
Confidentiality level	**Confidentiality categories**
Update Network Config Host Properties->Configuration->Networking->Add Networking Host Properties->Configuration->Networking->[selecting vSwitch]->Properties->Ports->Add	
If the "Traffic is allowed for VLAN with a lower level" option is disabled, the virtual network confidentiality level must be equal to the physical network adapter confidentiality level. If this option is enabled, the confidentiality level of each virtual network must be not higher than the physical network adapter confidentiality level	The virtual network list of categories must include at least one of the physical network adapter categories
Add Port Group	
If the "Traffic is allowed for VLAN with a lower level" option is disabled, the virtual network confidentiality level must be equal to the confidentiality level of the physical network adapter	The virtual network list of categories must include at least one of the physical network adapter categories
Update Port Group Host Properties->Configuration->Networking->[selecting vSwitch]->Properties->Ports-> [selecting port group]->Edit	
When attempting to edit the virtual network, confidentiality level of the source virtual network and new virtual network must be the same	The new virtual network list of categories must include at least one of the source virtual network categories
Update Virtual Switch Host Properties->Configuration->Networking->[selecting vSwitch]->Properties->Network Adapter-> Add Host Properties->Configuration->Networking->[selecting vSwitch]->Properties->Network Adapter-> Remove	
If the "Traffic is allowed for VLAN with a lower level" option is disabled, the virtual network confidentiality level must be equal to the confidentiality level of the new physical network adapter	The virtual network list of categories must include at least one of the physical network adapter categories
VM Add Virtual Disk	
If the "Allowed to store VM with the lower level" option is enabled, the storage confidentiality level must be not lower than the VM confidentiality level. Otherwise, the target storage confidentiality level must be equal to the VM confidentiality level	The list of VM categories must include at least one storage category
ESXi Browse data storage	
The user confidentiality level[2] must be not lower than the storage confidentiality level	The list of user categories must include at least one storage category
Delete file in Browse data store dialog	
The session confidentiality level must be equal to the storage confidentiality level	The list of user categories must include at least one storage category

[2]Note that the user session level and its confidentiality level are not the same thing. The user confidentiality level is assigned by the security administrator in the management console. The session level is assigned by the virtual infrastructure administrator prior to operating in the secure mode.

Conditions of operation execution	
Confidentiality level	**Confidentiality categories**
Copy/Move file in Browse data store dialog	
1. The user session level must be equal to the source storage confidentiality level. **2.** If the "Allowed to store VM with the lower level" option is enabled for the target storage, the confidentiality level of this storage must be not lower than the confidentiality level of the source storage. Otherwise, confidentiality levels of the source and target storages must be the same	**1.** The list of user categories must include at least one storage category. **2.** The source storage list of categories must include at least one of the target storage categories
Copy/Move file in Browse data store file from VMware Remote Command Line Interface (RCLI)	
1. The user session level must be equal to the storage confidentiality level. **2.** If the "Allowed to store VM with the lower level" option is enabled for the target storage, the confidentiality level of this storage must be not lower than the confidentiality level of the source storage. Otherwise, confidentiality levels of the source and target storage must be the same	**1.** The list of user categories must include at least one storage category. **2.** The source storage list of categories must include at least one of the target storage categories

Parameters of configurable security policies

When creating a policy set, you may need to configure some of the security policies in it. Policies that must be configured can be found at the beginning of the list and have the "Policy parameters must be configured" status. Their parameters must be specified before saving the policy set.

Note. You cannot save the policy set until additional parameters (for example, password, IP address etc.) are specified for all policies with the "Policy parameters must be configured" status.

Most of the security policies with configurable parameters are not required to be configured when creating a set. Such policies should be configured depending on the requirements for checks they perform.

Configurable security policies and description of their parameters are presented in the table below.

Parameters of policies that must be configured

Parameter	Description
Configure the ESXi host firewall to restrict access to services running on the host	
Rules for network packet filtering	To add a rule, select a service in the drop-down list, specify the IP address or subnet range, from which access to ports of this service is allowed, then click the "Add" button. The rules are specified in the following format: "Ruleset Name: 1.1.1.1, 2.2.2.2/24, 3.3.3.3". For example: DNS Client: 192.168.3.0/24, 172.28.0.0/16
Configure persistent logging for all ESXi host	
Path to folder	Path to the log file on the ESXi server. For example: [datastore name]/logfiles/hostname.log
Configure remote logging for ESXi hosts	
IP address of the syslog server	IP address of the remote syslog server
Syslog server port	Syslog server port. By default, the parameter is set to 514

Parameters of other configurable policies

Parameter	Description
Verify no unauthorized kernel modules are loaded on the host	
Kernel modules without signatures that can be loaded	The list of unsigned kernel modules that can be loaded. To add a module to the list, specify its name and click the "Add" button
Ensure that port groups are not configured to the value of the native VLAN	
Value of native VLAN identifier	The native VLAN identifier value (by default, 1) which is not allowed to be used for port groups of the ESXi server virtual switch
Trusted boot loading of virtual machines	
VM can be started if integrity is compromised	This option is enabled by default. To prohibit VM starting when checksums of controlled VM configuration files do not match, turn off the toggle.
VM BIOS integrity	To enable integrity control of BIOS configuration files (NVRAM files), turn on this toggle
List of VM snapshots	To enable integrity control of VM snapshot configuration files (VMSD files), turn on this toggle
VM configuration control	The list of controlled VM configuration parameters (VMX file parameters). To define the list of parameters, whose values will be controlled by the policy, select the required items in the list. Details on the correspondence of parameters in this list and certain VMX file parameters can be found on p.**127**
Integrity control of virtual machine templates	
Operations with VM template are allowed if integrity is compromised	This option is enabled by default. To prohibit operations with the template when checksums of template files and their reference values do not match, turn off this toggle
VM template BIOS integrity	This option is enabled by default. To disable integrity control of BIOS configuration files (NVRAM files) of the VM template, turn off the toggle.
Integrity of virtual disk images	To enable integrity control of virtual disk images of the VM template (VMDK files), turn on this toggle. Calculating checksums of disk images may take a long time
Set a timeout to automatically terminate idle ESXi Shell and SSH sessions	
Set ESXi Shell and SSH session idle timeout in seconds	Period of time after which unused Shell and SSH sessions are closed. By default, it is set to 300 seconds
Set a timeout to limit how long the ESXi Shell and SSH services are allowed to run	
Limiting of Shell and SSH services operation in seconds	Period of time after which Shell and SSH sessions are closed automatically. By default, it is set to 600 seconds
Control access to VMs through VMsafe CPU/memory APIs	
Allow VMsafe API	To allow access to virtual machines via the VMSafe program interface, turn on this toggle
IP address of VMsafe virtual machine	IP address of the virtual machine that is used to protect other virtual machines with the help of the VMSafe technology
TCP port of VM safe virtual machine	The VMSafe virtual machine TCP port (by default, 65535)

Parameter	Description
Disable certain unexposed features	
Disable HGFS	To prohibit using the HGFS server (Host Guest File System), turn on this toggle. HGFS server shutdown will result in stopping APIs that use the server to send/receive file to/from the guest system (some VIX commands or VMware Tools auto-upgrader)
Clean up deleted virtual machine disks	
Reset operation timeout (in minutes)	Period of time for execution of the reset operation, after which it will be considered failed and requiring restart. By default, the parameter value is set to 60 minutes
Clean up deleted virtual machine disks (double wiping)	
Reset operation timeout (in minutes)	Period of time for execution of the reset operation, after which it will be considered failed and requiring restart. By default, the parameter value is set to 60 minutes
Enable bidirectional CHAP, also known as Mutual CHAP, authentication for iSCSI traffic	
Check bidirectional CHAP authentication	To enable checking of bidirectional CHAP authentication, turn on this toggle
Control access to VMs through the dvfilter network APIs	
List of filters in format: "ethernetX.filterN.name = filter name"	The list of access filters in the following format "ethernet0.filter1.name = dv-filter1", where "ethernet0" — VM network adapter, "filter1" – filter number, "dv-filter1" — module name of the kernel that implements VM protection. To add a rule to the list, specify it in this field and click "Add"
Configure a centralized location to collect ESXi host core dumps	
Memory dump storage server (IP address:port)	IP address and port of the server for memory dump storage (the ":" symbol is used as a separator)
Active interface of memory dump network storage	Name of the ESXi server network adapter (for example, vmk0)
Limit VM logging	
Number of files	Number of log files for simultaneous storage on the ESXi server (by default, 10)
File size (bytes)	Log file size in bytes. By default, the parameter value is set to 1 000 000 bytes
Limit informational messages from the VM to the VMX file	
Maximum VMX file size (bytes)	Maximum VMX file size in bytes. By default, the parameter value is set to 1 048 576 bytes
Disconnect unauthorized devices	
IDE	To check connection to the ESXi server of devices through the IDE interface, turn on this toggle
Floppy	To check connection to the ESXi server of floppy disks, turn on this toggle
Parallel	To check connection to the ESXi server of devices through the parallel port, turn on this toggle
Serial	To check connection to the ESXi server of devices through the serial port, turn on this toggle
USB	To check connection to the ESXi server of devices through the USB port, turn on this toggle

Parameter	Description
Ensure proper SNMP configuration (only for ESXi)	
SNMP agent is on	Turn on this toggle, when using an audit event notification list through the SNMP protocol
SNMP agent port	SNMP agent port. By default, the parameter value is set to 161
SNMP communities. Use ";" as a separator	SNMP community name. When specifying several communities, use the ";" symbol as a separator
Address for receiving SNMP data (in the server@port/community format)	Address of the server for the receipt of SNMP messages in the server@port/community format. When specifying several servers, use the ";" symbol as a separator
Verify Image Profile and VIB Acceptance Levels	
Acceptance level	Acceptance level to which VIB packets, allowed to be installed on the ESXi server, must correspond. Available values: PartnerSupported, VMwareAccepted or VMwareCertified
Configure NTP time synchronization	
NTP server pool	The list of NTP servers that are used for time synchronization. To add a new server to the NTP server pool, specify its address and click the "Add" button. For the ESXi server 7.0, you can add only IP address of the NTP server. To remove a server from the list, click the "Delete" button
Establish a password policy for password complexity	
PAM module arguments	Parameters of the pam_passwdqc.so module that are used by the password complexity policy. By default, retry=5 min=disabled,disabled,disabled,disabled,14
List of prohibited devices	
List of prohibited devices	List of virtual devices that are prohibited to connect to a virtual machine To add a new device type, specify its name or select the required value in the drop-drown list, then click "Add".
ESXi application whitelist	
List of programs that can be started on ESXi host	List of programs that can be started on the ESXi server. To add a program to the list, click the "Add" button
Force shutdown of unauthorized programs	To prevent starting of unauthorized programs, turn on this toggle. Otherwise, when starting a program from the list, the audit event will be registered without prohibiting the program start
Set DCUI.Access to allow trusted users to override lockdown mode	
Trusted users	Specify the name of the user who will be allowed to directly access the ESXi server and click the "Add" button. By default, the ESXi server administrator (the root user) is included in the list

The clacl.exe utility

vGate includes the clacl.exe utility for configuring vGate. Most of the utility commands are equal to the features of the management console.

The utility is available from the command prompt on the vGate server and on the security administrator workstation. To view detailed information about the utility, open the command prompt and execute the following command:

```
clacl.exe –H
```

Export and import of the vGate configuration

Using the clacl.exe utility, you can export or import the vGate configuration.

To export a configuration:

- Open the command prompt and run the following command:

  clacl.exe common export-objects -x **<path to file>** -k **<administrator>** -s **<password>**

  where:

  - x **<path to file>** — path to the XML file, where the vGate configuration is saved;
  - **<administrator>** — name of the security administrator;
  - **<password>** — password of the security administrator.

To import a configuration:

- Open the command prompt and run the following command:

  clacl.exe common import-objects -x **<path to file>**-e **<true/false>** -k **<administrator>** -s **<password>**

  where:

  - x **<path to file>** — path to the XML file from which the vGate configuration will be imported;
  - e **<true/false>** — if this parameter is set to **true**, the configuration will be updated, even if there are conflicts with the current vGate configuration.

Note. During the utility operation, a message may appear prompting for additional parameters, for example, vCenter server address and vSphere administrator credentials.

Selective vGate Agent installation on vCenter

Using the clacl.exe utility, you can selectively install the vGate Agent on the vCenter server.

For the initial installation without the "vSphere access control" component:

- Open the command prompt and run the following command:

  clacl.exe deploy install-vpx --features drv -h **<vCenter>** -u **<Windows user>**
  -w **<Windows password>** --vc-user **<administrator>** --vc-password **<password>**
  -i **<vGate server>** -k **<security administrator>** -s **<security administrator password>**

  where:

  - drv — name of the "Control of network connections" component;
  - **<vCenter>** — name or IP address of the vCenter server;
  - **<Windows user>** —Windows user name for access to the vCenter computer;
  - **<Windows password>** — Windows user password for access to the vCenter computer;
  - **<administrator>** — vGate administrator name;
  - **<password>** — vGate administrator password;
  - **<vGate server>** — name or IP address of the vGate server;
  - **<security administrator>** — security administrator name;
  - **<security administrator password>** — vGate security administrator password.

To reinstall without the "vSphere access control":

- Open the command prompt and run the following command:

  clacl.exe deploy modify-vpx -d vcp -h **<vCenter>** -u **<Windows user>** -w **<Windows password>** --vc-user **<administrator>** --vc-password **<password>** -i **<vGate server>** -k **<security administrator>** -s **<security administrator password>**

  where vcp — name of the "vSphere access control" component.

To install without the "Control of network connections" component:

- Open the command prompt and run the following command:

  clacl.exe deploy modify-vpx -d drv -h **<vCenter>** -u **<Windows user>** -w **<Windows password>** --vc-user **<administrator>** --vc-password **<password>** -i **<vGate server>** -k **<security administrator>** -s **<security administrator password>**.

To install all components:

- Open the command prompt and run the following command:

  clacl.exe deploy install-vpx --features vcp,drv -h **<vCenter>** -u **<Windows user>**
  -w **<Windows password>** --vc-user **<administrator>** --vc-password **<password>**
  -i **<vGate server>** -k **<security administrator>** -s **<security administrator password>**.

Enabling the "Deep packet inspection" function

Using the clacl.exe utility, you can enable the "Deep packet inspection" function on ESXi servers (see p.**143**).

Attention! For working with the "Firewall" component, the "vGate network administrator" privilege must be granted to the security administrator (see 1).

To enable deep packet inspection:

- Open the command prompt and run the following command:

  clacl.exe firewall-dpi deploy -h **<ESXi server IP address>** -v **<vCenter>** -u **<vCenter user>**
  -w **<vCenter user password>** -t **<analysis server IP address>**
  -g **<analysis server user>** -x **<analysis server user password>**
  -i **<vGate server>** -k **<security administrator>** -s **<security administrator password>**

Once the command is successfully executed, in the "Firewall/ESXi servers" section of the web console, the corresponding ESXi server status appears in the "Deep packet inspection" column.

To disable deep packet inspection:

- Open the command prompt and run the following command:

  clacl.exe firewall-dpi undeploy -h **<ESXi server IP address>** -v **<vCenter>** -u **<vCenter user>**
  -w **<vCenter user password>** -t **<analysis server IP address>**
  -g **<analysis server user>** -x **<analysis server user password>**
  -i **<vGate server>** -k **<security administrator>** -s **<security administrator password>**

Assigning security policies to distributed virtual switch

Using the clacl.exe utility, you can assign security policies to a distributed virtual switch.

To assign policies:

- Open the command prompt and run the following command:

  clacl.exe policies assign -o **<vSwitch>** -t D -m **<policy set>**
  -v **<vCenter server>** -u **<Windows user>** -w **<Windows password>**
  -i **<vGate server>** -k **<security administrator>** -s **<security administrator password>**

  where:

  - **<vSwitch>**— identifier of the distributed virtual switch;
  - **<policy set>**— policy set name;
  - **<vCenter>** — name or IP address of the vCenter server;
  - **<Windows user>** — Windows user name for access to the vCenter computer;
  - **<Windows password>** — Windows user password for access to the vCenter computer;

- **<vGate server>** — name or IP address of the vGate server;
- **<security administrator>** — security administrator name;
- **<security administrator password>** — vGate security administrator password.

Example:

policies assign -o newDVSwitchForTestsWAE -t D -m RejectPoliciesForDVPortgroup
-v vcenter.CD2012R2.rd2012r2.vgforest -u root -w 2552 -i 192.168.158.160 -k admin@TESTESX
-s Password`123

Changing port that is used for access to ESXi servers in secure perimeter

Using the clacl.exe utility, you can change the port number that is used for access to ESXi servers in the secure perimeter.

By default, port 902 is used in access rule templates (see p.**175**).

Attention!

- For correct operation of the template-based access rules, we recommend not changing the port.
- If the port has been changed, you must check the configuration of access rules. If necessary, edit rules in the "Access rules" section of the web console (see p.**108**).

To change the port:

- Open the command prompt and run the following command:

  clacl.exe options set -n vmware_console_target_port -v <port>

  where **<port>**— new port number.

The db-util.exe utility

vGate includes the db-util.exe utility for managing the configuration database and vGate server replication settings

The utility is located in the vGate server installation directory.

To view detailed information about the utility, open the command prompt and execute the following command:

```
db-util.exe -h
```

Checking connection to the PostgreSQL server

Using the db-util.exe utility, you can check credentials that are used for connection to the PostgreSQL server.

- Open the command prompt and run the following command:

  db-util.exe --test-connect **<server>** -D **<database>**-U **<user** -P **<password>**

  where:

  - **<server>** — name or IP address of the server where the database is located;
  - **<database>** — name of the database;
  - **<user>** — name of the user to access the database;
  - **<password>** — password of the user to access the database.

  A message with the results of test connection to the database appears.

Moving deleted audit events

When clearing the event log in the vGate web console, audit events are marked as deleted, but they are not deleted physically from the database. Using the db-util.exe utility, you can unload the deleted audit messages to the selected catalog, thus removing them from the database.

To remove the deleted events from the database:

- Open the command prompt and run one of the following commands:

  db-util.exe --hard-compact **<path>**

  db-util.exe --soft-compact **<path>**

where:

- hard-compact command — performs the compressing of a database. It can disrupt the replication, if it is enabled;
- soft-compact command — performs the compressing of a database. It does not clear memory on the disk after deleting records from the database. This command does not affect the replication;
- **<path>** — path to the created directory for storing the deleted events.

The gzip archieve will be created in the specified directory with the following name

vgate-audit-[DATETIME].gz, где DATETIME — command execution date and time.

Note. If the redundant vGate Server is installed and db-util.exe --hard-compact command is executed, to recovery the replication, run the db-util.exe --recreate-replica command on the redundant vGate Server.

To upload deleted events back to the database:

- Open the command prompt and run the following command:

  db-util.exe --load **<path>**

Configuring replication parameters

Using the db-util utility, you can delete settings of data replication between the main and redundant vGate Servers.

To delete replication settings:

- Open the command prompt on the main vGate Server and run the following command:

  db-util.exe --delete-cluster

To recover the replication:

- Open the command prompt on the redundant vGate Server and run the following command:

  db-util.exe --recreate-replica **<IP>**: **<port>**

  where:

  - **<IP>** — the main vGate Server IP address;
  - **<port>** — PostgreSQL port of the main vGate Server, by default, 5432.

To view information about a lag between the redundant and main vGate Servers:

- Open the command prompt on the redundant vGate Server and run the following command:

  db-util.exe --replication-delay

  As a result of this command, information about a lag between the redundant and main vGate Servers appears on the screen. It can be bytes of PostgreSQL WAL-logs or -1 if an error occured (replication is not enabled, WAL is full, no connection between the main and redundant vGate Servers).

Changing the vGate Server role

Using the db-util.exe utility, you can change roles of the vGate servers: make the main server the redundant server or make the redundant server the main server (for example, in case of the main server failure).

To change server roles:

- Open the command prompt on the main vGate Server and run the following command:

  db-util.exe --switch-roles-fm --log **<path>**

  where **<path>** — path to the log file of the role change operation.

  Note. The --log **<path>** parameter is not required. By default, the operation log file will be saved to the product setup directory (vGate\Logs).

Passing control to the redundant vGate Server

In case of the main vGate Server failure, you can temporarily make the redundant server the main one.

Attention! We do not recommend passing control to the redundant vGate Server if the automatic failover is enabled.

To pass control to the redundant server:

- Open the command prompt on the redundant vGate Server and run the following command:

  db-util.exe --failover --log **<path>**

  Note. The --log **<path>** parameter is not required. By default, the operation log file will be saved to the product setup directory (vGate\Logs).

The drvmgr.exe utility

You can create firewall rules for the vCenter server using the drvmgr.exe utility. The utility is executed on the vCenter server or on the vGate server.

Attention!
- This utility cannot be used on vCSA servers.
- To run the utility on the vGate server, open the command prompt on behalf of the administrator and go to the vGate setup folder.
- If the Windows Server 2012 R2 OS is installed on the vCenter computer and User Account Control (UAC) is enabled, run the drvmgr.exe utility on behalf of the administrator to configure firewall rules.

Description of some drvmgr.exe utility commands is given below.

> drvmgr
Displays help
> drvmgr i 0x031
Displays current firewall rules
>drvmgr A user protocol IP_from[:source_port[,mask]] [destination_port] [Flags]
Add a firewall rule
>drvmgr R user protocol IP_from[:source_port[,mask]] [destination_port] [Flags]
Remove a firewall rule

Description of the utility command parameters is given in the table below.

Parameter	Description
user	User name
protocol	Protocol type (TCP, UDP, ICMP)
IP_from[:source_ port[,mask]]	Source parameters in the following format: "IP address: port number, mask". Port number and mask are not mandatory
[destination_port]	The server port to which access is granted. This parameter is not mandatory
[Flags]	Flag can take the following values: • 1 — packets pass without any restrictions; • 4 — access control rules are saved in the registry (when adding a rule) or removed from the registry (when removing a rule); • 8 — if the packet is allowed from the TCP port 902, file exchange in browse datastore is allowed
You can use "any" as a parameter value. It means that the parameter can take any value	

To view details on flags, use the help:

```
known flags: 0x001 - disable proxy redirection
             0x002 - rule not deleted while clearing rule table
             0x004 - rule saved to (or removed from) registry
             0x008 - enable TCP-902 data transfers
             0x100 - disable traffic within already opened TCP sessions
             0x200 - traffic is unsigned
             0x400 - deny traffic from protected networks
            0x1000 - force redirection to VCP port
            0x2000 - force redirection to original port
           0x10000 - source port in range from portMin to portMax
           0x20000 - destination port in range from portMin to portMax
```

Example of configuring a vCenter firewall rule

To add a rule allowing incoming connections from the 172.28.36.0 network to any vCenter port via any protocol, execute the following command:

```
>drvmgr A any any 172.28.36.0:any,255.255.255.0 any 4
```

To remove this rule, use the following command:

```
>drvmgr R any any 172.28.36.0:any,255.255.255.0 any 4
```

The cfgTransfer.exe utility

vGate includes the CfgTransfer.exe utility for exporting the vGate configuration (for version 4.0 and higher).

The utility is located in the \vGate directory on the vGate setup disk.

To view detailed information about the utility, open the command prompt and execute the following command:

```
cfgtransfer.exe -h
```

The CfgTransfer.exe is supposed to be used with the installed vGate server.

If the vGate software was removed before exporting a configuration, the following parameters must be specified in the HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate registry section:

- HaronIntIface (string) — the vGate server IP address in the infrastructure administration network;
- BdPort (string) — database port. It is specified if a port other than the default port (5432) was used;
- RhuidPort (DWORD) — any value;
- NetworkMode (string) — the vGate operation mode ("router" — if vGate is installed for working without a standalone router, "simple" — if a standalone router is used);
- AddVmToGroupTimeout (DWORD) — timeout of automatic adding virtual machines to groups.

To export a configuration:

Open the command prompt and run the following command:

```
cfgtransfer.exe -f <path to file> -d <PostgreSQL user name> -p <PostgreSQL user password>
```

where f **<path to file>** — path to the XML file to which the vGate configuration will be saved.

Note. PostgreSQL user name and password are specified during the vGate server installation. By default, user name is set to "postgres".

The command may contain the pg_only (-o) key. In this case, data will be exported only from the database, without polling protected servers.

If the configuration includes a vCenter server, the command may contain the following keys:

- vc (-v) — vCenter name or IP address;
- user (-u) — user name for access to the vCenter server;
- pwd (-w) — user password for access to the vCenter server.

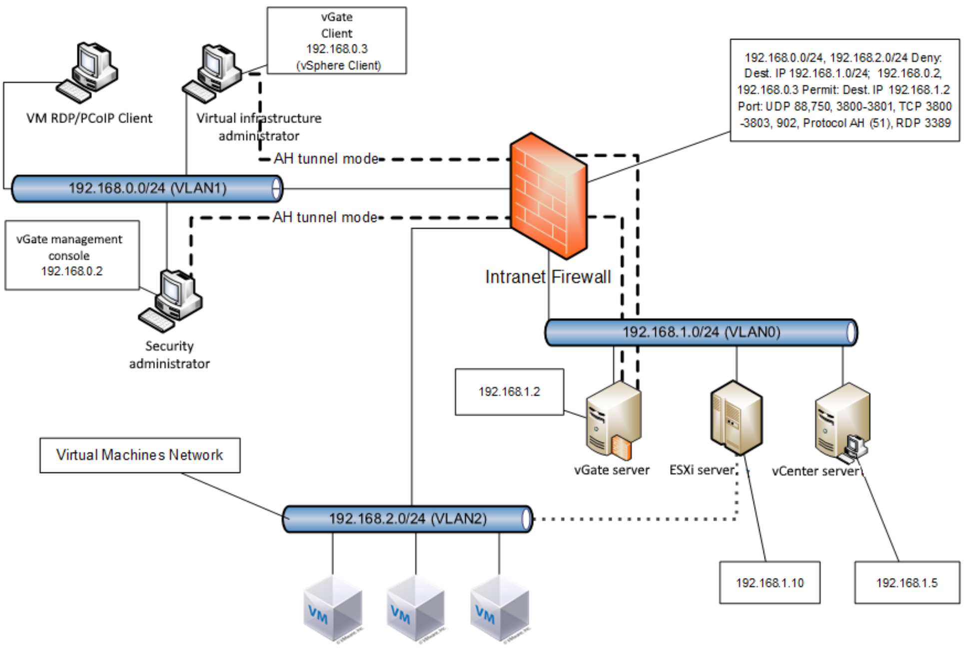
Configuring router

If the traffic routing between the network of protected servers and external perimeter of the administration network is performed by a standalone router, in the router settings, create rules allowing connections between the vGate Server and workstations of the security administrator and virtual infrastructure administrator through the following ports:

- port TCP 3801;
- port UDP 3801;
- port TCP 3800;
- port UDP 3800;
- port TCP 3802;
- port TCP 3803;
- port TCP 3806;
- port TCP 3808 (if using the vGate server replication);
- port TCP 3814;
- port TCP 902;
- port UDP 88;
- port UDP 750;
- port TCP 3389 (when connecting to the vGate server via RDP);
- protocol AH (№ 51).

Network layout

The diagram displays the layout of virtual infrastructure elements and vGate software components installed using a third-party router.



Where:

- 192.168.0.0/24 — infrastructure administration network;
- 192.168.1.0/24, 192168.2.0/24 — protected networks.

When installing the vGate software using a router (Intranet Firewall), that is located in the network, you must create rules for access from the infrastructure administration network to the protected network, and traffic between these networks must be prohibited. You need to allow access to the protected network for the security administator and virtual infrastructure administrator computer accounts. The ports listed above must be opened for them on the vGate server.

Example of configuring Cisco PIX router

To create rules allowing connections between the vGate Server and workstations of the security administrator and virtual infrastructure administrator, execute the following commands in the command prompt:

```
access-list 102 permit tcp 192.168.1.0 255.255.255.0 host 192.168.2.10 range 3800
3801 3802 3803
access-list 102 permit udp 192.168.1.0 255.255.255.0 host 192.168.2.10 range 3800
3801
access-list 102 permit ah 192.168.1.0 255.255.255.0 host 192.168.2.10
access-list 103 permit ah host 192.168.2.10 192.168.1.0 255.255.255.0
access-group 102 in interface outside
access-group 103 in interface inside
```

where:

- 192.168.1.0/24 — administration network where workstations of the security administrator and virtual infrastructure administrator are located;
- 192.168.2.0/24 — network of protected servers of the virtual infrastructure;
- 192.168.2.10 — IP address of the vGate Server network adapter in the secure network.

Configuring View Connection Server

vGate must be configured to ensure correct operation of the View Connection Server that is a part of the VMware View software. The setup procedure differs depending on the traffic routing method: using the vGate server or using a router that already exists in the network.

Attention! Before configuring, make sure that all VMware View components are operating properly in the existing network infrastructure.

Configuration in case of traffic routing through the vGate server

Plan

If the "Routing is performed by the vGate Server" option was selected during the vGate Server deployment, to ensure correct operation of the View Connection Server, you must do the following:

№	Step	Specific features	Description
1.	**View Connection Server location**	View Connection Server is located in the external perimeter of the administration network	See below
2.	**vGate Client installation**	To access the secure perimeter on the View Connection Server, the vGate Client must be installed	See p.**44**
3.	**Account configuration**	You must configure the View Connection Server computer account in vGate	See p.**87**
4.	**Access control rules configuration**	For the View Connection Server computer account, that was created during the previous step, you must configure a certain set of access control rules for the vCenter server	See p.**192**
5.	**vCenter access configuration**	This step is necessary only if the vGate Agent is already installed on the vCenter Server and ports other than default are used by the View Connection Server for access to it. In this case, configure rules for View Connection Server access to the vCenter server through the required ports	See p.**111**

View Connection Server location

Computer where the View Connection Server is installed must have at least two Ethernet interfaces. One of them will be connected to the external perimeter of virtual infrastructure administration network, while the other will be connected to the VM network where user workstations are located.

Access control rules configuration

To grant View Connection Server access to vCenter, configure a certain set of access control rules to vCenter for the account of the View Connection Server computer. The set of access control rules for View Connection Server access to the vCenter server is included in the "Allow access to View Connection Server" template.

In this template, default ports for View Connection Server access to vCenter are specified (8443, 443 and 18443). If ports other than default are used, numbers of these ports must be specified in the access control rules.

Attention! When adding a set of access control rules, based on the "Allow access to View Connection Server" template, make sure that no access rule for port 443 for all users is assigned to the vCenter server. If such a rule exists, remove it and create similar rules for certain users instead of it.

If support of View Client with Local Mode is intended, configure another access control rule for the View Connection Server computer account. This rule must allow access to the ESXi server, where VM with the View Transfer Server is running, through the TCP port 902.

Details on configuring access control rules can be found on p.**108**.

Attention!

- For support of View Client with Local Mode, in properties of the View Connection Server computer account, select the "File operations in data storages" check box.
- To ensure security, we recommend not granting access to other objects (or through other ports) of the secure perimeter for the View Connection Server computer account.

Configuration when using a third-party router

If the "Using existing router in the network" traffic routing method was selected during the vGate Server deployment, no reconfiguration of the existing network is required. For correct operation of the View Connection Server, the following steps must be completed.

To configure the View Connection Server operation:

1. Locate the View Connection Server within the secure perimeter of the administration network.

   Tip. The secure perimeter of the administration network may consist of different subnets that are routed by the existing equipment. The View Connection Server and the vGate Server can be located in the same subnet or in different subnets.

2. Add the View Connection Server to the list of protected servers as a standalone server (see p.**79**).
3. Configure control rules for the virtual infrastructure administrator access to the View Connection Server from the external perimeter of the administration network.

   To manage the View Connection Server from the external perimeter of the administration network, configure a set of access control rules for the View Connection Server, based on the "Allow access to View Connection Server" template. In this template, default ports for access to the View Connection Server are specified (80 and 443). If ports other than default are used, numbers of these ports must be specified in the access control rules.

   Details on configuring access control rules can be found on p.**108**.

4. Configure the existing network equipment to prohibit access to the View Connection Server from the virtual infrastructure administrator workstations. Make sure that the vGate Server is available from the virtual infrastructure workstations (see p.**191**). In this case, View Connection Server administrators will be able to manage VMware View only after they are authenticated in vGate via the vGate Client.

vGate and Secret Net Studio integration

vGate can work in tandem with Secret Net Studio 8.9.

vGate and Secret Net Studio components can be installed (uninstalled) in any order.

Attention! Installation of the vGate Server and Secret Net Studio Security Server on the same computer is not supported.

Attention! If the Secret Net Studio software with enabled data wipe mechanism is installed on the vGate Server, we recommend not using the db-util utility.

If the Application Control Execution (AEC) mechanism operates in hard mode in Secret Net Studio, to install the vGate components, disable the AEC mechanism or deactivate AEC hard mode.

Also, you can install vGate using the account to which the AEC mechanism is not applied.

Note. Since AEC is not applied to users included in the local group of administrators, you can install the vGate software using such an account. We recommend logging on to the computer in the unclassified session.

Once the vGate installation is completed, make sure that AEC do not prohibit executing modules and downloading libraries necessary for the vGate operation. Procedure for configuring the AEC mechanism is given in the Secret Net Studio documentation (see "Administrator guide. Setup and operation").

Note. If you plan to work in Secret Net Studio with different confidentiality levels, with the enabled flow control mode, a configuration of the redirection function for vGate and vSphere Client files in the mandatory access control mechanism may be required (the configuration procedure is given the Secret Net Studio documentation, see "Administrator guide. Setup and operation").

If the integrity check mechanism or AEC mechanism is enabled and configured for vGate, while reinstalling vGate, reference values of controlled parameters in the Secret Net Studio tasks must be recalculated.

vGate and Veritas Backup Exec 21.0 integration

To configure simultaneous operation of vGate and Veritas Backup Exec 21.0, follow the recommendations specified in the Veritas Backup Exec 21.0 documentation (see the "Using Backup Exec with firewalls" and "Backup Exec ports" sections).

Attention!

- While recovering virtual machines from backup copies, audit notifications about security policy violations may appear in the vGate web console. To disable displaying such notifications, you can suspend the vGate agent operation on the ESXi server in the vGate web console.
- When the recovery operation is completed, virtual machine integrity control check may be required.

vGate and Kaspersky Anti-Virus software integration

Configuring Kaspersky Endpoint Security 11

For access to vCenter while using vGate and Kaspersky Endpoint Security 11 at the same time, you may need to disable control of ports 80 and 443 in the Kaspersky Endpoint Security settings.

Attention! For correct installation of the vGate software on computers with the Windows OS, during the installation, disable self-protection in Kaspersky Endpoint Security.

Configuring vGate for working with Kaspersky Security for Virtualization

For simultaneous operation of vGate and Kaspersky Security for Virtualization 5.0, vGate configuration must be performed.

If the "Control of network connections" component is installed on the vCenter server, for the "Kaspersky Security for Virtualization 5.0" components, located inside the secure perimeter, you must create rules for the following connections to vCenter:

- incoming connections from the VMware vShield server to TCP ports 443 and 7444;
- incoming connections from the VM, on which the File Antivirus component is installed, to TCP port 443;
- incoming connections from the VM, on which the Kaspersky Security Center component is installed, to TCP ports 139, 443 and 445.

Details on configuring rules can be found on p.**111**.

When connecting to the protected servers from the external perimeter of the administration network via the Kaspersky Security Center administrative console, create the following access control rules in the "Protected servers" section of the vGate management console:

- for the VMware vShield server: TCP protocol, destination port 443;
- for the Kaspersky Security Center server: TCP protocol, destination ports 8060, 13000 and 14000;
- for the ESXi server: TCP protocol, destination port 443;
- for the vCenter server: TCP protocol, destination port 443.

As a user to which these rules will be applied, specify the virtual infrastructure administrator account that uses the Kaspersky Security Center administrative console.

Details on configuring access control rules can be found on p.**107**.

Attention! We do not recommend assigning the "Trusted boot loading of virtual machines" security policy to virtual machines that are used by the Kaspersky Security for Virtualization 5.0 software:

- VMware vShield virtual machine;
- safe virtual machine with the "File Antivirus" component;
- safe virtual machine with the "Network threat detection" component.

vGate Client and Continent integration

The vGate software can work in tandem with the Continent software.

For correct operation of the vGate Client, data exchange between the Continent Client and the vGate Server over the AH protocol (IP protocol 51) must be allowed.

To ensure data exchange in the Continent 3.9.1 software:

1. In the Continent Access Server management program, create firewall rules that ensure AH packets passing from the Continent Client to the vGate Server.

   In the firewall rules, specify the following values:

Parameter	Value
Source	Continent Client IP address
Destination	vGate Server IP address
Service	AH protocol (IP protocol 51)
Action	Accept

2. Add the created firewall rules to the list of rules of the Continent user account.

To ensure data exchange in Continent 4.0.3 and 4.1:

1. In the Configuration Manager, go to "Access Server | Firewall" and create a firewall rule with the parameters listed above.
2. Click "Services", then right-click the list of the services and click "Add".
3. Click the "Create" button in the appeared window.

   The "Service" dialog box appears.
4. In the "Protocol" field, specify "51". Enter the service name and click the "OK" button.
5. Select "Skip" in the "Action" shortcut menu.
6. Save changes to the Security Management Server configuration. To apply the changes in the Security Gateway configuration, apply policy on the required Continent components.

If AH packets do not pass after installing a policy with the Firewall rule, you need to break existing connections on the required Security Gateways.

Note.
- To break existing connections in Continent 4.0.3, select the "Force rematch connections" option in the Security Gateway settings. If in the future this option is not necessary, set its initial value.
- To break existing connections in Continent 4.1, go to the "Structure" section of the Configuration Manager. In the list of security gateways, select the required component and click the "Reset sessions" button on the toolbar.

vGate Client and firewalls integration

When using the vGate Client together with third-party firewalls, for correct operation of vGate, create rules in the firewall settings that allow outgoing connections through the following ports:

- port TCP 3801;
- port UDP 3801;
- port TCP 3800;
- port UDP 3800;
- port TCP 5432;
- port UDP 750;
- port UDP 88;
- port TCP 3802;
- port TCP 3803;

Also, it may be necessary to create an allowing rule for protocol 51, and add all subnets of the secure perimeter as well as all IP addresses of the main and redundant vGate Servers to the list of trusted networks.

Windows Firewall settings

When installing the vGate software on the computer designated to be the vGate Server, permissions for incoming connections through the following ports will be created in the Windows Firewall settings.

Port	Protocol	Purpose
0	TCP	vGate deployment service
80	TCP	vGate Agent for ESXi service
88	UDP	vGate Kerberos IV KDC Service
443	TCP	vGate proxy service
750	UDP	vGate Kerberos V5 KDC Service
3800	TCP	vGate authentication service
3800	UDP	vGate authentication service
3801	UDP	Configuration of the vGate authentication service
3801	TCP	vGate user management service
3802	TCP	vGate remote management service
3803	TCP	Status of asynchronous operations of the vGate remote management service
3805	UDP	vGate audit service
3806	TCP	gRPC port for vGate
3808	TCP	vGate Server replication port
3809	TCP	vGate audit service (gRPC port)
3814	TCP	gRPC port for vGate
3815	TCP	vGate backend gRPC port
3900	TCP	Port for authenticating an anonymous user via the vGate web console
5432	TCP	Port for PostrgeSQL replication
20443	TCP	vGate service for vSphere virtual infrastructure control
30443	TCP	vGate service for vSphere virtual infrastructure control (vCSA)
40443	TCP	Port for redirecting Stunnel from PSC for vGate

When using the vGate Server together with third-party firewalls, you must also open the above-mentioned ports.

Note. We recommend disabling third-party firewalls on the computer designated to be the vGate Server/redundant vGate Server.

Documentation

1.	vGate R2. Administrator guide. Principles of operation
2.	vGate R2. Administrator guide. Installation, configuration and operation
3.	vGate R2. Administrator guide. Quick start
4.	vGate R2. User guide. Work in a protected environment