SECURITY code

vGate R2

User guide

Work in a protected environment

© SECURITY CODE LLC, 2023. All rights reserved.

All rights to the operation manuals are reserved.

This document is part of the product package. It is covered by all terms of the license agreement. You may not copy this document in printed or electronic form, in whole or part, or deliver it to third parties on commercial purpose without a special written consent of Security Code LLC.

Security Code LLC reserves the right to change the information contained herein without special notice.

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
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
VM	Virtual machine
OS	Operating system

Introduction

This guide is designed for administrators of virtual infrastructures protected by vGate R2 (hereinafter — vGate). The document covers information required for work in a protected environment.

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
Preparing for vGate installation

User account for access to virtual infrastructure

For access to your virtual infrastructure, you must have the virtual infrastructure administrator account or the security administrator account with the virtual infrastructure administrator privileges (see the document [2]).

For security purposes, while creating the security administrator account, we recommend you specify the corresponding VMware vSphere or Skala-R administrator account that has read-only access to the virtual infrastructure element configuration.

Preparing network for vGate installation

Before starting the installation of vGate components, perform several preparatory actions:

- Connect the necessary additional equipment (security administrator workstation, vGate server, etc.).
- Configure your local network.
- Configure routing between subnets.

After this, make sure that virtual infrastructure control elements (vCenter (vCSA) servers, ESXi servers, Skala-R servers, etc.) are available from virtual infrastructure administrator workstations.

Local network configuration rules, hardware requirements, and the recommended procedure for configuring routing between subnets can be found in the document [2].

Examples of the VMware vSphere virtual infrastructure and vGate component location are shown in the following figures.

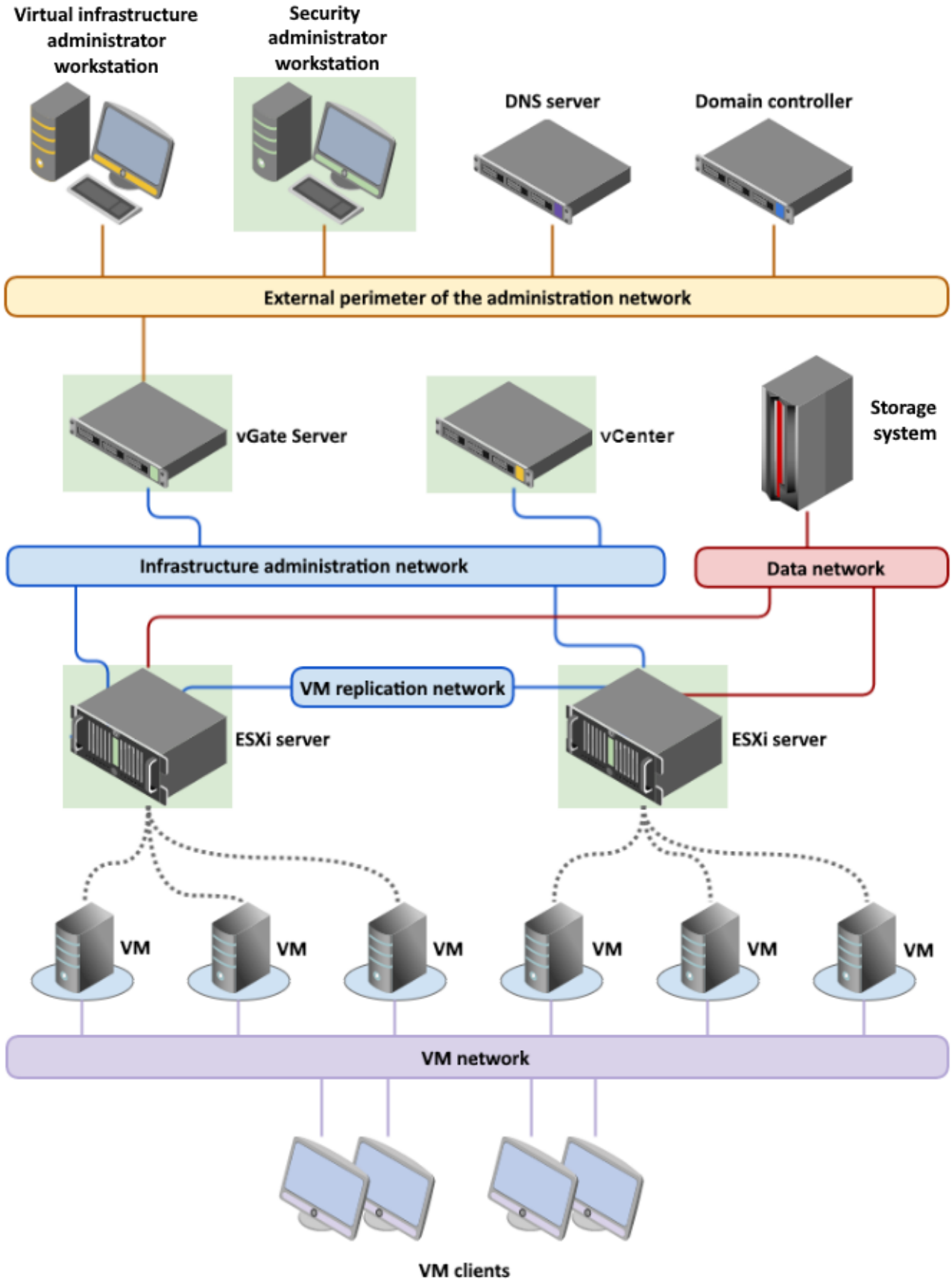


Figure 1. Network architecture and component location for VMware vSphere (traffic is routed by the vGate Server)

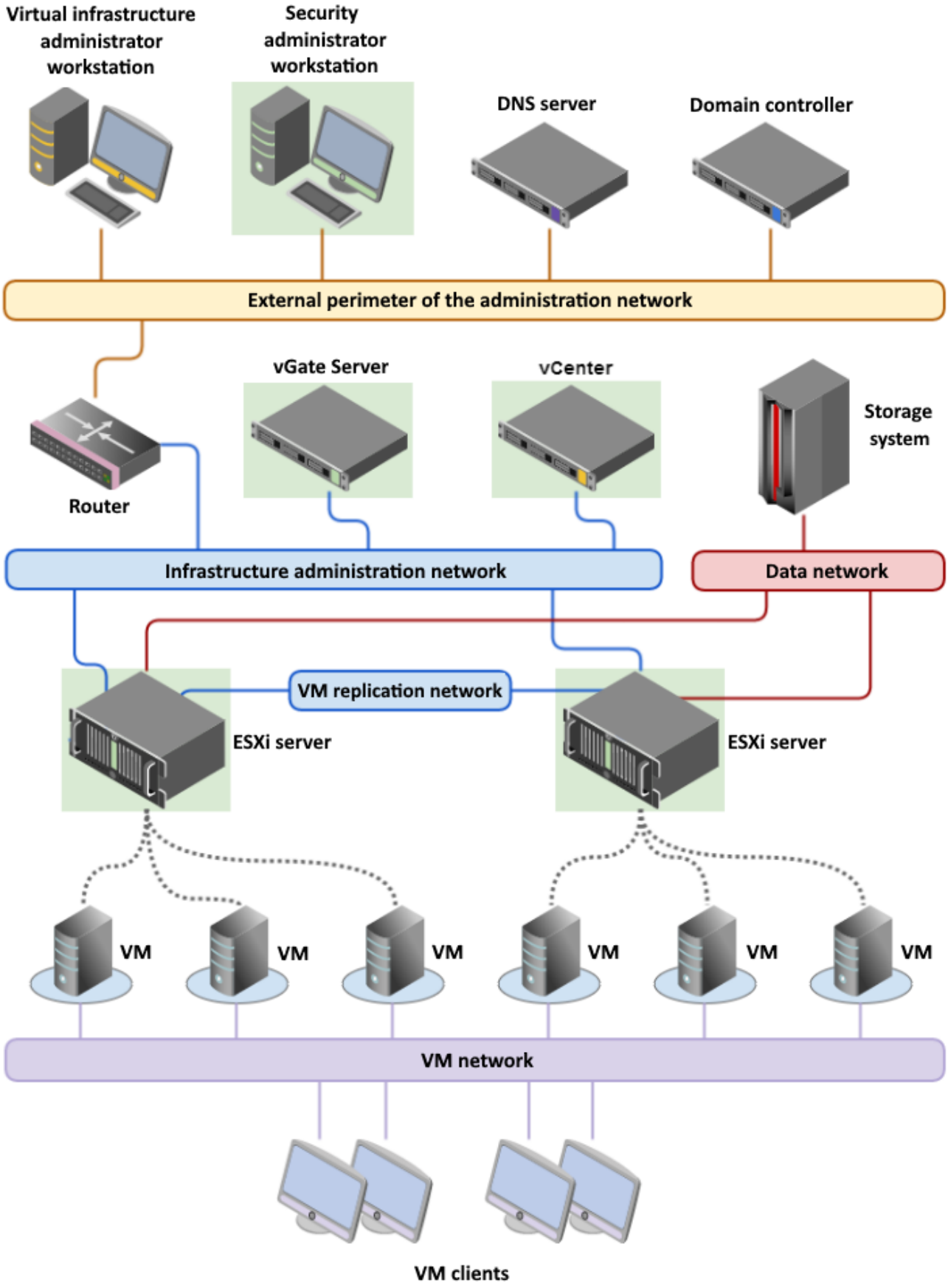


Figure 2. Network architecture and component location for VMware vSphere (traffic is routed using a router that already exists in the network)

Chapter 2
Work in Windows protected environment

Connection to a protected environment

Only authenticated users can manage virtual infrastructure. In vGate, the authentication procedure is mandatory for users (virtual infrastructure administrators), security administrators, and computers. Computer authentication is performed automatically.

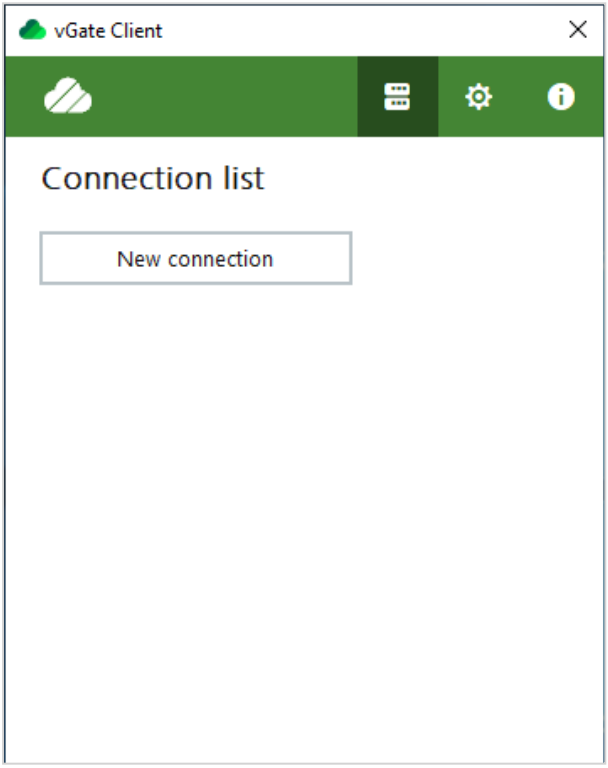
You can log on via the vGate Client (see p.**9**) or through the vGate web interface (see p.**19**).

Logging on via the vGate Client

To log on:

1. Log on to the system using the computer administrator credentials.
2. Run the "vGate Client" program as an administrator from the corresponding shortcut on the desktop, or click "Apps | Security Code | vGate Client" in the "Start" menu.

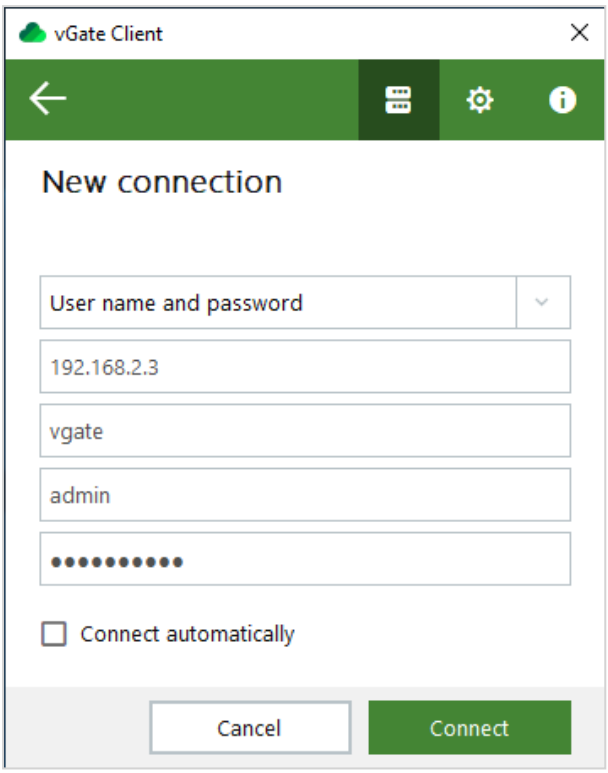
   The following dialog box appears.



3. To add a new connection to the vGate server, click the "New connection" button. If several vGate servers are in operation, configure a connection to the protected environment for each of them.

Note. Connection to several vGate servers is available only in vGate Enterprise and Enterprise Plus (details can be found in the document [1]).

The following dialog box appears.



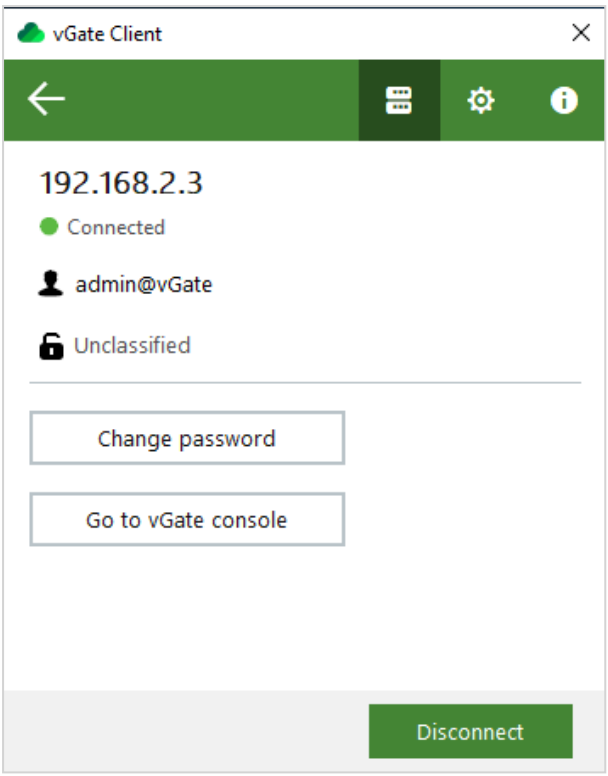
4. Enter user credentials, if necessary, modify the remaining parameters, and click the "Connect" button.

Parameter	Description
Authentication method	To connect to the protected environment using the vGate account, select the "User name and password" option (default). To use the credentials of the current Windows user, select the "Use the current Windows session" check box. This method is available if you use the AD integration mode in which the vGate server is a member of the Windows domain
IP address or server name	Network name or IP address of the vGate server
Domain	For an account from AD, select a domain from the list. If you log on using the vGate user credentials, specify the vGate account registry name specified while installing the vGate server (for example, "VGATE")
User name	Name of the security administrator or virtual infrastructure administrator. If the computer with the installed vGate Client is not a part of a domain from the list of trusted domains on the vGate server (see the "Trusted domains" section in the document [2]), you must specify the credentials of the security administrator with the "Account operator" privilege (see the "vGate accounts" section in the document [2]).
Password	Administrator password
Connect automatically	If you select this check box, the later connections of the user to the protected environment will be established automatically (without requesting a password)

Tip.

- To edit preferences for starting the vGate Client, click on the main menu (see p.12).
- To view information about the vGate Client version and copyrights, click on the main menu.

5. Connection to the vGate server appears in the list.



If you logged on to the vGate Client using the security administrator account, the vGate web console will be available by clicking the "Go to vGate console" button.

Note. If the report viewer tool is installed on the computer (see the "Reports" section in the document [2]), click the "Open reports" button to open a dialog box for configuring report parameters.

Logging on via a security token

To log on, you can use Rutoken or JaCarta token.

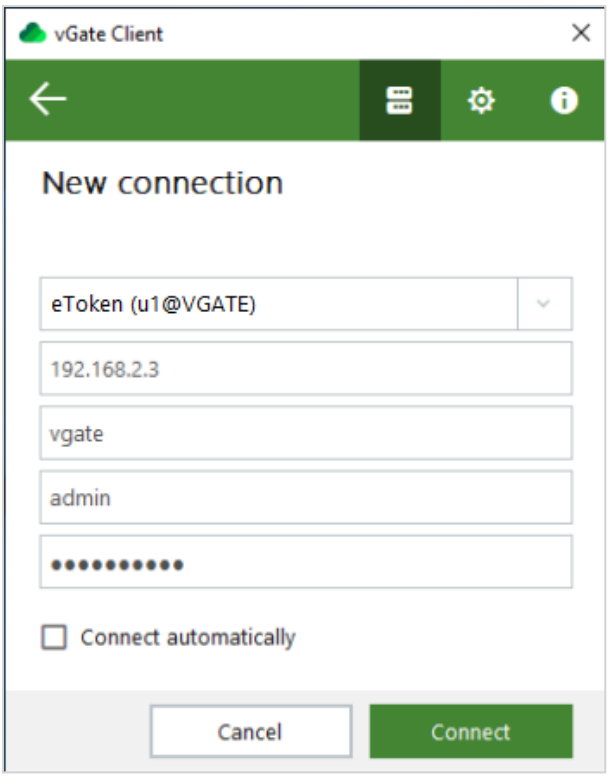
To obtain a security token, contact your security administrator. The security token configuration procedure is provided in the document [2].

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

To log on using a security token:

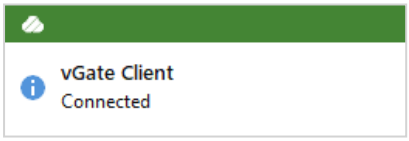
1. Connect the token to the computer where the vGate Client is installed.
2. Start the vGate Client (see p.**9**).

3. Select a vGate server and authentication method, enter a PIN code, then click the "Connect" button.



Checking connection status

Once you successfully logged on, a connection to the virtual infrastructure will be established. This is confirmed by an appearing message next to the vGate Client icon in the notification area.



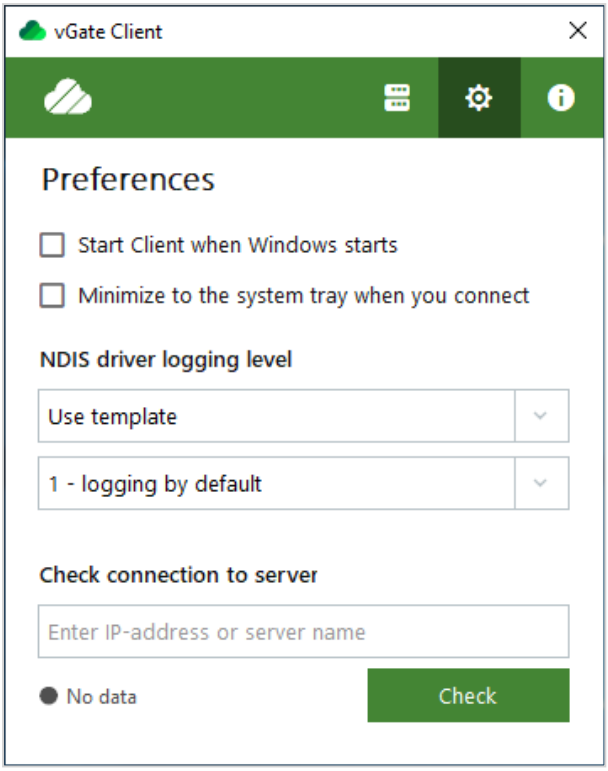
When establishing a new connection, the time of the previous logon to the vGate Client will be displayed in the message box.

Configuring preferences

To configure the vGate Client:

1. Open the vGate Client dialog box by double-clicking the corresponding icon on the taskbar.

2. Click on the main menu.
   The following dialog box appears.



3. Configure parameters by selecting the required check boxes.
4. If necessary, configure the NDIS driver logging level. It may be necessary for vGate troubleshooting. Specify the logging level manually or with the help of a template. The EnableLogging parameter will be set to a hex value in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vGateNdisDriver registry section.
5. To check the connection to the vGate server, enter the server IP address or FQDN in the "Check connection to server" field. By default, the field contains the server address specified for the first connection in the list of connections (see p.9).

Note. For correct operation of the checking connection mechanism, disable the Windows Firewall on the computer or take the following steps:

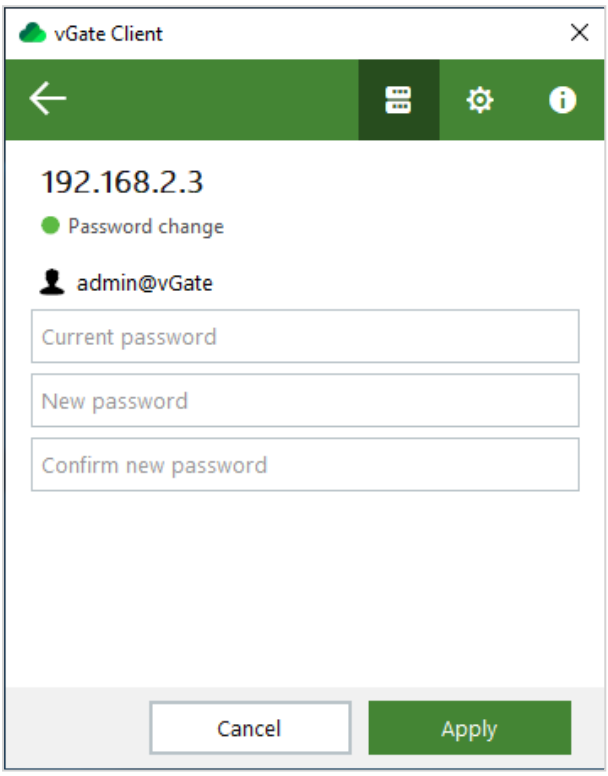
- in the Windows Firewall, create a rule with the "Program" type that allows incoming connections for the drvmgr.exe and client.exe services, or create rules that allow incoming connections through the ICMP and 144 protocols;
- on the vGate server, add a rule allowing incoming traffic through the ICMP protocol.

Changing password

Attention! The new password must meet the requirements specified by the security administrator. If the new password does not meet these requirements, a message prompting you to set another password will appear.

To change the user password:

1. Open the vGate Client dialog box by double-clicking the corresponding icon on the taskbar.
2. Select a connection and click the "Change password" button.
   The following dialog box appears.



3. Enter the current password, enter a new password twice, and click the "Apply" button.

Note. Password change in vGate is not available for Active Directory accounts. To do this, you can use the Active Directory administration tools.

Access to virtual infrastructure control elements

Rights to manage access control rules for the protected elements of a virtual infrastructure are granted to the security administrator. Therefore, if the virtual infrastructure administrator needs other rights or cannot access the required control elements, they have to contact the security administrator.

Note.

- If the virtual infrastructure administrator does not have rights to access the virtualization server, when attempting to log on to the vSphere Web Client, the "Connection is blocked" message from the vGate Client is displayed next to the notification area on the taskbar.
- If the virtual infrastructure management operation is blocked, the corresponding notification will be displayed in the vSphere Web Client informing that the operation has been blocked by vGate.

Specific features of work with confidentiality resources

A confidentiality level is assigned to each user, it allows executing operations with resources (ESXi servers, Skala-R servers, VM, storages, vSphere virtual networks) of a certain confidentiality level. The user can perform operations with resources with a confidentiality level equal to or lower than the user confidentiality level.

This rule controls rights to execute such operations as powering on, powering off a VM, changing VM settings (including network settings), accessing a VM datastore, moving a VM, etc.

Access level management

A session level that is equal to the user confidentiality level is assigned to each user session in the protected environment. The user can execute operations with resources with the confidentiality level equal or lower than the user level.

The privilege to control session level can be granted to users. In this case, while connecting to the protected environment, the session level is equal to the user confidentiality level, but the user can perform operations only with resources of 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.

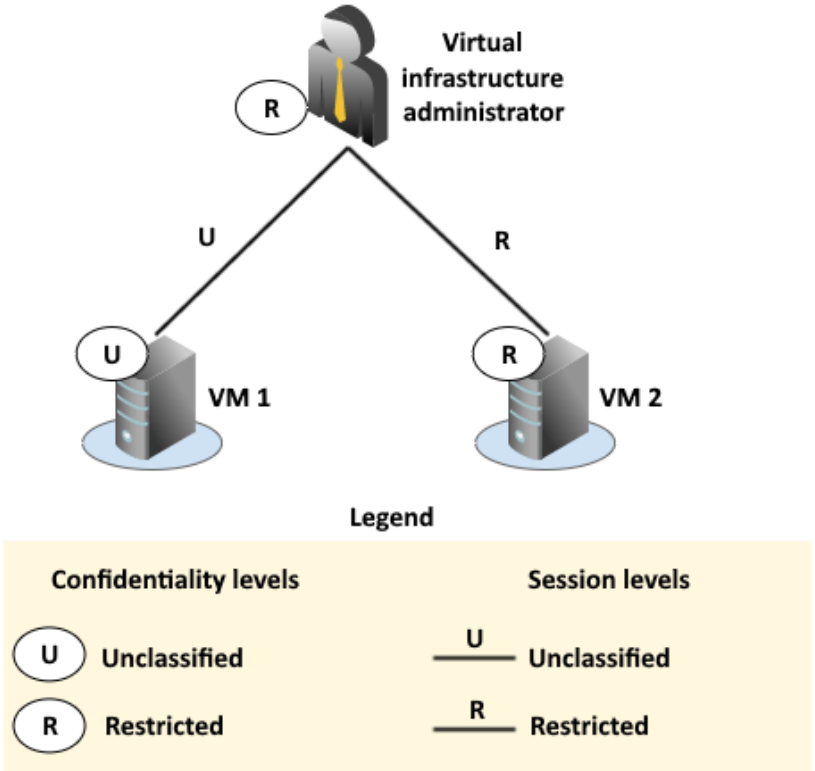
Note. The privilege to change the session level in the vGate Client is controlled by the security administrator. By default, this function is disabled. Details can be found in the "General settings" section of the document [2].

If users are granted the privilege to change the session level, the session level can take one of the following values (in ascending order):

- unclassified;
- restricted.

Therefore, by selecting the required session level, a user can execute operations with resources of different confidentiality levels (from "unclassified" to the maximum level available for the user).

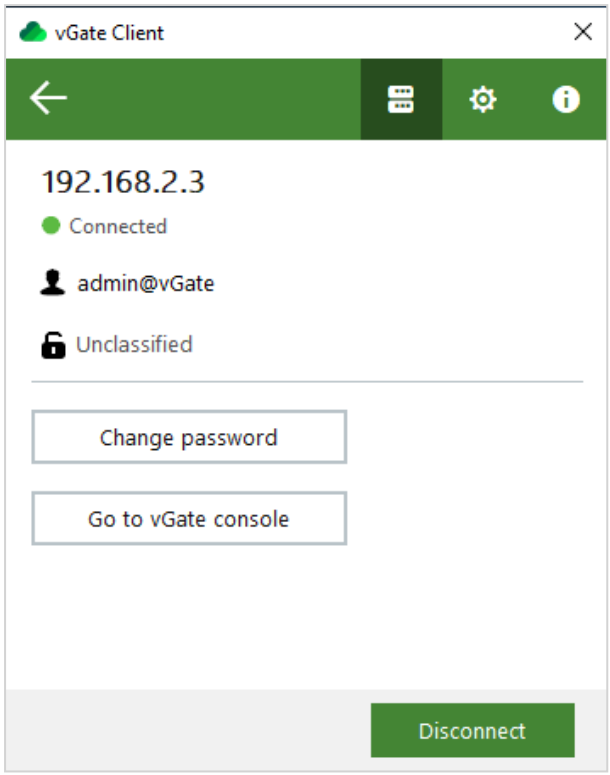
For example, the virtual infrastructure administrator can power on VM 1 or VM 2, if the session level equal to the confidentiality level of one of these virtual machines is selected.



Selecting session level

To select the session level:

1. Open the vGate Client dialog box by double-clicking the corresponding icon on the taskbar.



2. Click the current session level.

3. In the appeared submenu, select the required session level.

Putting new equipment into operation

In case of putting new virtual infrastructure equipment (ESXi servers, Skala-R Management servers, KVM servers, OpenNebula, Proxmox, VM storage units, physical network adapters, virtual networks) into operation, the security administrator must be informed about this. Also, the list of users to be granted access to these resources must be specified.

Secure VM deletion in VMware vSphere environment

Attention! To perform the secure VM deletion operation, the virtual infrastructure administrator must be granted access to the ESXi server or vCenter server (TCP ports 902 and 443), where the deleted VM is running, and have the "File operations in data storages" privilege.

For secure VM deletion without the possibility of restoring it, you must clean up VM disks prior to deleting this virtual machine.

If the "Clean up deleted virtual machine disks" policy (see the "Security policies" section in the document [2]) is assigned to the VM that you are removing, VM disk clearing is performed automatically.

Note. For correct operation of the policy, VM deletion must be performed on a computer with the installed vGate Client. In the rule of access to the virtualization server, to which the user is connecting, the "Traffic control" option must be enabled (see the "Configuring rules for access to vCenter and vSphere Web Client" section in the document [2]).

If the policy is not configured, you can use the vmdktool.exe utility. The utility can also be useful if not a VM but its disk was deleted.

Note. Before using the vmdktool utility, install the Microsoft Visual C++ 2015 Redistributable component with the KB2999226 update on the computer.

Prior to cleaning up the VM disk, make sure that there are no snapshots[1], after this, stop the VM.

Utility command line format

The command line of the secure VM deletion utility has the following input format:

To remove a VM from the ESXi server:

```
>vmdktool.exe –s [arg] –u [arg] -p [arg] -m [arg] -v [arg] –d [arg] –t [arg]
```

To remove a VM from the vCenter server:

```
>vmdktool.exe –s [arg] –u [arg] -p [arg] -m [arg] -v
vmPath=[arg] –d [arg] –t [arg]
```

A description of the utility command line parameters is given in the table.

Parameter	Description
-s [arg]	Network name or IP address of the ESXi/vCenter server
-u [arg]	Name of the ESXi/vCenter server administrator account
-p [arg]	Password of the ESXi/vCenter server administrator
-m [arg]	SSL certificate thumbprint
-v [arg]	Full path to the VM configuration file (*.vmx)
-d [arg]	Full path to the VM disk (*.vmdk)
-t [arg]	Number indicating a byte code to fill the VM disk with. Available values: from 0 to 255. Default value: 255

Note. The default ESXi server port number is 902, the default vCenter server port number is 443.

To view the utility help, use the following command:

```
>vmdktool.exe –?
```

An example of secure deletion

Suppose the following parameters are specified:

Parameter	Value
ESXi server name	esx5.esx.local
ESXi server administrator name	root
vCenter server name	vcenter60.vg.text
vCener server administrator name	admin@vsphere.local
Password of the ESXi/vCenter server administrator	P@ssw0rd
SSl certificate thumbprint	42:1A:39:6E:D3:4D:B6:A9: 5F:C4:1F:C4:B0:C3:4E:38: 42:6A:1C:71
Full path to the VM configuration file (*.vmx) for ESXi	"[storage1] vm4/vm4.vmx"
Full path to the VM configuration file (*.vmx) for vCenter	Datacenter/vm/vm4
Full path to the VM disk (*.vmdk)	[storage1] vm4/vm4.vmdk
Number indicating a byte code to fill the VM disk with	55

[1] Snapshot is a VM state snapshot (VM settings, disk state, memory state) in a certain period of time. Reverting to a snapshot restores the saved VM state.

To remove a VM from the ESXi server, enter the following command in the command line:

```
>vmdktool.exe -s esx5.esx.local -u root -p P@ssw0rd -m
42:1A:39:6E:D3:4D:B6:A9:5F:C4:1F:C4:B0:C3:4E:38:42:6A:1C:71
-v "[storage1] vm4/vm4.vmx" -d "[storage1] vm4/vm4.vmdk"
-t 55
```

To remove a VM from the vCenter server, enter the following command in the command line:

```
>vmdktool.exe -s vcenter60.vg.text -u admin@vsphere.local -p P@ssw0rd -m
42:1A:39:6E:D3:4D:B6:A9:5F:C4:1F:C4:B0:C3:4E:38:42:6A:1C:71
-v vmPath=Datacenter/vm/vm4 -d "[storage1] vm4/vm4.vmdk"
-t 55
```

Finishing work in a protected environment

To finish work in a protected environment:

1. Open the vGate Client dialog box by double-clicking the corresponding icon on the taskbar.
2. Select a connection and click the "Disconnect" button. Connection to the vGate server will be terminated.

Note. The "Exit" shortcut menu item closes the program. The vGate Client icon will be removed from the taskbar.

Chapter 3
Access to virtual infrastructure through the web interface

For user access to a virtual infrastructure without the vGate Client, the security administrator must create access rules for protected servers (see the document [2]).

Attention!

- A user cannot work in two different domains at the same time.
- When using the vGate Client and web interface for access to virtual infrastructure at the same time, the user session via the vGate Client has a higher priority.

Note. In case of access to a virtual infrastructure through the web interface, operations with files in datastores (download/upload) can be unavailable in the vSphere Web Client. In this case, use the ESXi Embedded Host Client.

To log on:

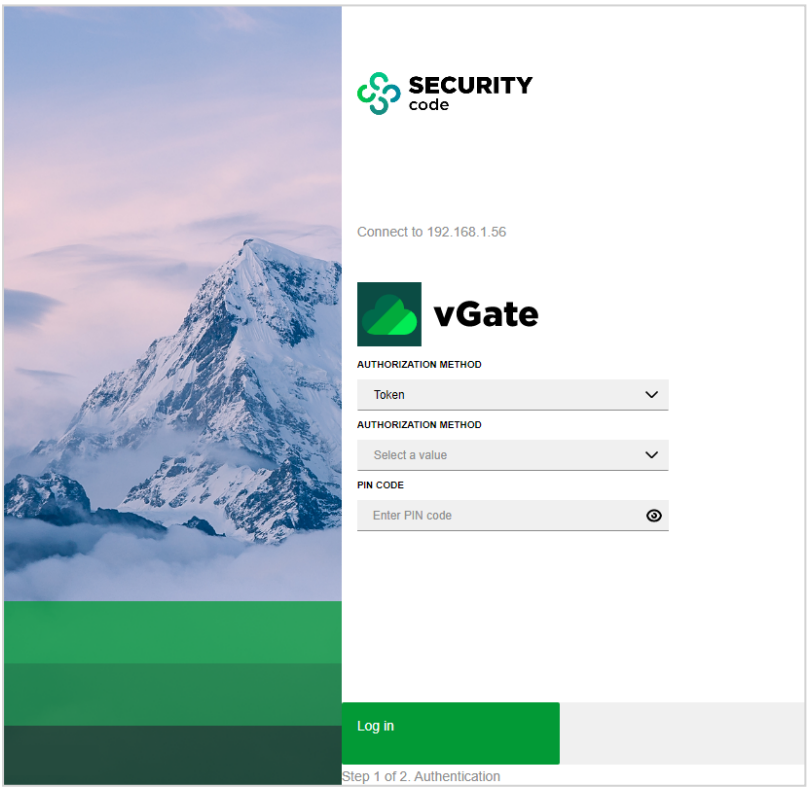
1. Open the web browser and type the following URL:

   https://<protected_server>

   where <protected_server> is the protected server IP address or FQDN.

   Note. For access to the vCenter (vCSA) server, we recommend using the server FQDN. When using the server IP address, logon will be successful only after the second attempt.

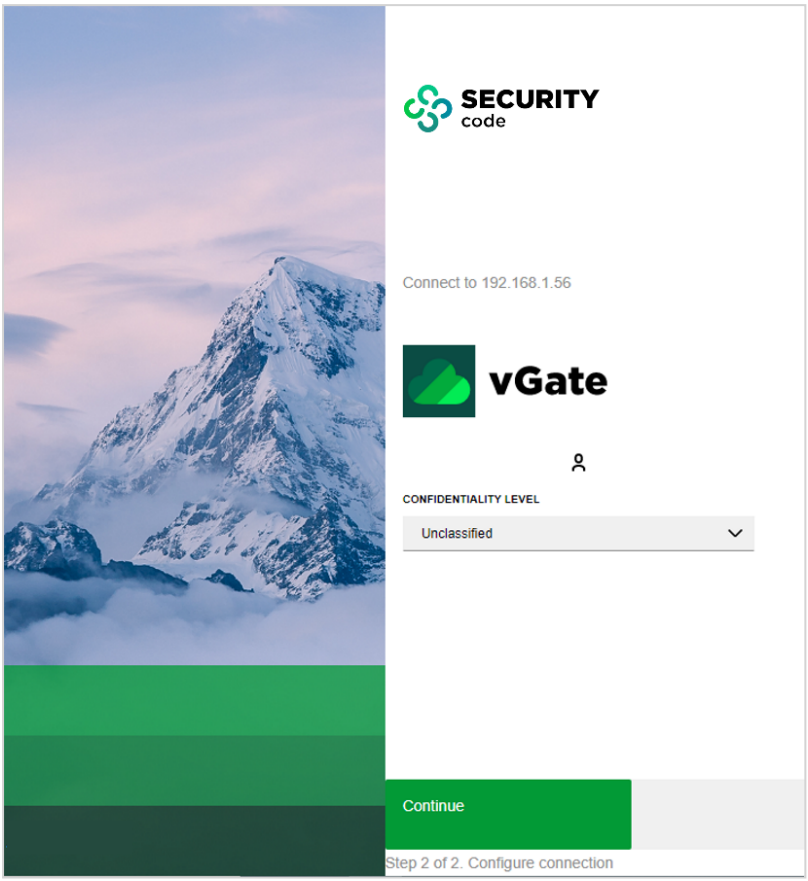
   The following dialog box appears.



2. Select an authorization method.

   If the "User name and password" option is selected, specify the user credentials. If the "Token" method is selected, select your security token in the drop-down list and type a PIN code. Click "Log in".

   The following dialog box appears.



Note. To change a user password, click the "Change password" button. In the appeared dialog box, type the current password and new password.

3. Select the session confidentiality level in the drop-down list (see p.**15**) and click the "Continue" button.

   The protected server page appears.

Note.

- In case of access to virtual infrastructure without the vGate Client, you can select the session confidentiality level and change the password only during the authentication.
- A user session expires after 15 minutes of the user inactivity. Forced logoff from the system is not supported.

Chapter 4
vGate Client operation in Linux OS

vGate Client operation is supported in Linux OS.

You can execute commands from the menu of the vGate authentication program (see below) or directly from the command line (see p.23).

Executing commands from the menu

Start the authentication program from the command line:

```
/opt/vgate/vgcconsole
```

In case of a successful connection to the authentication service, the menu with available commands appears.

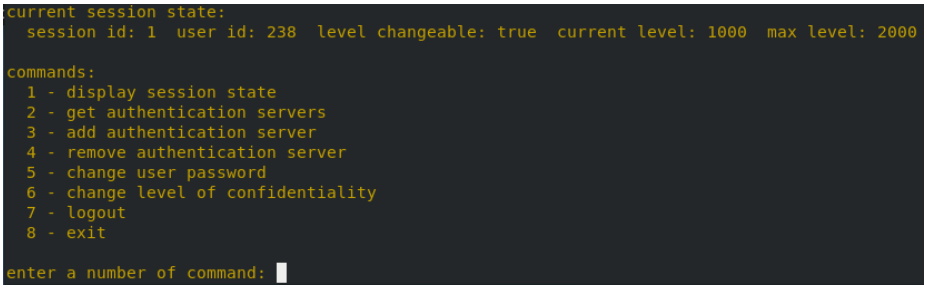
To execute the required command, enter the corresponding command number and click <Enter> button:

- 1 — request the vGate authentication program state;
- 2 — get the list of vGate servers;
- 3 — add a connection to the vGate server;
- 4 — delete a connection to the vGate server;
- 5 — user authentication;
- 6 — quit the authentication program.

Request the vGate authentication program state

If the user is successfully logged on, after executing the command, the following information will appear: the user identifier, current confidentiality level, the "level changeable" parameter, and maximum supported confidentiality level.

If the authentication fails, identifier will be equal to 0.



The following actions are available for authenticated users only:

- 5 — change the user password;
- 6 — change the user confidentiality level. The command is available only for vGate servers that support confidentiality level tracking ("level changeable: true");
- 7 — log off the system (without quitting the authentication program).

Get the list of vGate servers

Once the command is executed, the list of supported vGate servers appears. For each server, the following parameters are displayed: IP address, port, connection status, and vGate operation mode ("Soft mode"/"Normal mode"/"Disaster mode").

Add a connection to the vGate server

Once the command is executed, the following parameters of the added vGate server will be requested: IPv4 address of the server and IPv4 address of the client network gateway through which the client can connect to the server (necessary for "Simple Mode").

If the server is successfully added, the corresponding message will appear.

Note. You can ensure that the vGate server has been added to the list of supported servers by executing the "get authentication servers" command.

Remove a connection to the vGate server

Once the command is executed, IPv4 address of the vGate server, connection to which needed to be removed, will be requested.

If the vGate server is successfully removed from the list of supported servers, the corresponding message will appear.

Note. You can ensure that the vGate server has been removed from the list of supported servers by executing the "get authentication servers" command.

User authentication

Once the command is executed, you will be prompted to log on using the vGate server credentials or JaCarta-2 token (if it is available).

To log on using the vGate server credentials:

1. Type the "authenticate by credentials" command number and click <Enter>.

   A prompt to enter the authentication parameters appears.

```
|-> commands (authenticate):
      1 - authenticate by credentials
      2 - authenticate by hardware
      3 - step back

    enter a number of command: 1

    input parameters:
      input server address (IPv4): 192.168.1.10
      input server domain: VGATE
      input user name: xxx
      input user password:
```

2. Specify the parameters (vGate server IPv4 address, domain name, user name, and password) and click <Enter>.

Once the authentication is completed successfully, the corresponding message appears containing the following information: the user identifier, current confidentiality level, and maximum available confidentiality level.

Note. To return to the main menu, execute the "step back" command.

To log on using the JaCarta key:

1. Type the "authenticate by hardware" command number and click <Enter>.

   The list of available keys appears.

2. Type the required key number and click <Enter>.

   A prompt to enter the parameters for authentication (vGate server IPv4 address, domain name, PIN for access to the protected key container where the user name and password are stored) appears.

Once the authentication is completed successfully, the corresponding message appears containing the following information: the user identifier, current confidentiality level, and maximum available confidentiality level.

Note. Process of the authentication by a key may take a long time.

Quit the authentication program

Once the "exit" command is executed, the authentication program operation will be completed.

Executing commands from the command line

The vGate authentication program can be started together with the command executing one of the following actions.

To display detailed information about the program, enter the following command:

```
/opt/vgate/vgcconsole --help
```

The following commands to manage the authentication program are available.

- Request the vGate version:

  ```
  /opt/vgate/vgcconsole --version
  ```

- Request the vGate authentication program state:

  ```
  /opt/vgate/vgcconsole --display session state
  ```

  If the user is successfully logged on, a unique identifier will be assigned to the user. If the authentication fails, the identifier will be equal to 0.

  Also, the following information will be displayed: the current confidentiality level of the user, whether the level can be changed, and the maximum available confidentiality level.

- Get the list of supported vGate servers:

  ```
  /opt/vgate/vgcconsole --cmd=get_authentication_servers
  ```

- Add a vGate server to the list of supported servers:

  ```
  /opt/vgate/vgcconsole --cmd=add_authentication_server
  --server-address=IP_address
  ```

  where server-address is an IP address of the server to be added (for example, 192.168.1.11).

- Remove a vGate server from the list of supported servers:

  ```
  /opt/vgate/vgcconsole --cmd=remove_authentication_server
  --server-address=192.168.1.11
  ```

  where server-address is an IP address of the server to be removed (for example, 192.168.1.11).

- User authentication:

  ```
  /opt/vgate/vgcconsole --cmd=authenticate
  --server-address=192.168.1.11 --domain=VGATE
  --user-name=test --user-password=`123qwe
  ```

  where:

  - **server-address** is the vGate server IP address (for example, 192.168.1.11);
  - **domain** is the vGate account registry name specified during the vGate server installation (for example, VGATE);
  - **user-name** is the user name (for example, test);
  - **user-password** is the user password (for example, `123qwe).

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