SECURITY code

vGate R2

Administrator guide

Quick start

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 **4**

Introduction **5**

vGate components **6**

Putting vGate into operation **8**

Troubleshooting **9**

Common issues 9

Questions and answers 9

Documentation **10**

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
PSC	Platform Services Controller is a component that supports the operation of VMware virtual infrastructure services
VM	Virtual machine
OS	Operating system

Introduction

This guide is designed for administrators of vGate R2 (hereinafter — vGate). The document covers information required for the initial setup 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/.

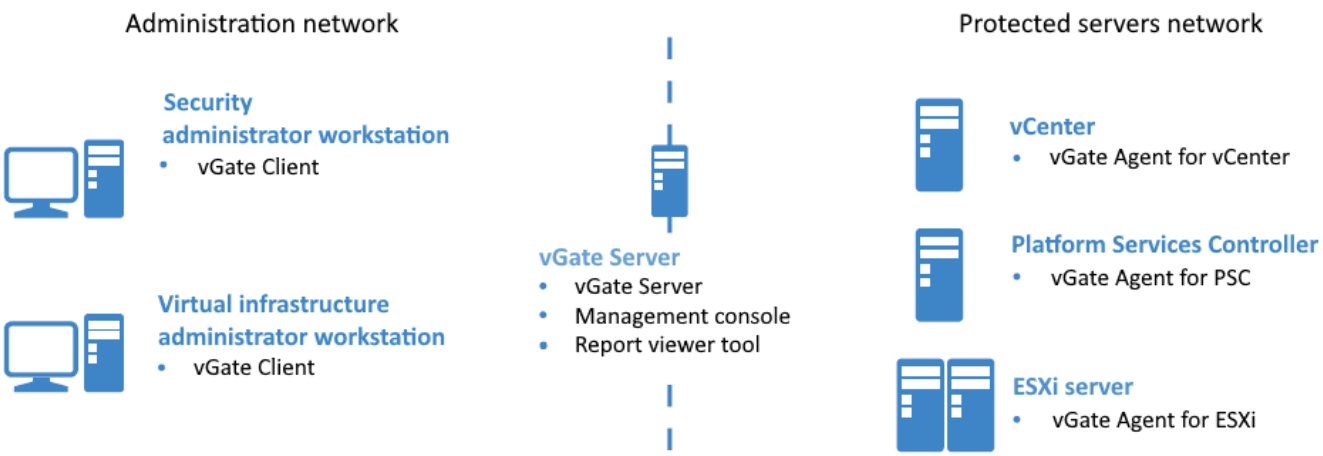
You can contact the company representatives regarding the organization of the training process by email: education@securitycode.ru.

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.

vGate components

While deploying, vGate components are located according to the figure below:



The main functions of the vGate components are presented in the table below.

Component	Functions
vGate Server	• User and computer authentication. • Control of access to the virtual infrastructure management tools. • Audit of security events. • Data storing (account information, event log, and vGate configuration). • Data replication (if a redundant server is used in the system). • Synchronization of vGate server settings. • Automatic deployment of vGate agents on ESXi servers
Redundant vGate Server	• Storing the settings and the list of users. • Data replication. • Main server replacement in case of failure
vGate Client	• User identification and authentication. • Computer identification and authentication. • Integrity control of the vGate client components. • Selecting session level while working with confidential resources (with enabled session level control). • Audit of security events
vGate Agent for ESXi	• VM integrity control and trusted boot loading. • Integrity control of vGate modules and settings. • Integrity control of ESXi server configuration files. • Integrity control of container images. • Audit of security events. • Protection from unauthorized access to the administration network. • Device mounting control. • Providing the trusted software environment
vGate Agent for vCenter (vCSA)	• Protection from unauthorized access to the administration network. • Incoming traffic filtering
vGate Agent for PSC	Protection from unauthorized access to the administration network
vGate Agent for KVM	• Protection of KVM, Skala-R, Proxmox and OpenNebula virtualization servers. • VM integrity control and trusted boot loading. • Protection from unauthorized access to the administration network. • Audit of security events

Component	Functions
Web console	• Centralized management of vGate. • Management of user and computer accounts. • Assigning privileges for access to protected objects. • Installing and configuring vGate agents on protected servers. • Import and export of vGate configuration. • Configuring the hot standby function. • Configuring mandatory access control. • Configuring protected objects' security policies. • Calculating VM configuration checksums. • Configuring and viewing the event log. • Configuring firewall rules. • Monitoring of security events. • Synchronization of vGate servers. • Configuring JaCarta and Rutoken
Monitoring server	Collecting and correlating virtual infrastructure events
Analysis server	Analysis of VM network traffic within the "Deep packet inspection" function
Report viewer tool	Preparing reports on the status of the virtual infrastructure security parameters, occurred events, and changes in configuration

Putting vGate into operation

The brief plan for the vGate software deployment and configuration is given below. The details of the vGate configuration are provided in the document [2].

To deploy and configure vGate:

1. Read the product usage restrictions (see the Release Notes).
2. Read the system requirements (see the "Hardware and software requirements" section in the document [2]).
3. Configure the administration network by separating it from the protected computer network and virtual machine network (see the "Local network configuration rules" section in the document [2]).
4. Choose a traffic routing method (see the "Configuration of routing between subnets" section in the document [2]):
   - using the vGate server;
   - using a third-party router.
5. If necessary, prepare the redundant vGate server.
6. Install the vGate server and report viewer tool (see the "vGate server installation and setup" section in the document [2]).
7. If you intend to use the replication mechanism, install the vGate software on the redundant vGate server (see the "vGate server installation and setup in the replication mode" section in the document [2]).
8. Install the "vGate Client" component on the virtual infrastructure administrator workstation (see the "vGate Client installation on Windows OS" section or the "vGate Client installation on Linux OS" section in the document [2]).
9. Log on to the vGate web console using the security administrator credentials (see the "Web console" section in the document [2]).
10. In the web console, register the license for using vGate (see the "License" section in the document [2]).
11. Configure the server connection settings depending on the configuration of the virtual infrastructure. If the vCenter (ESXi) server, Cloud Director server, Embedded Harbor Registry, KVM virtualization servers, Proxmox server, OpenNebula platform or Skala-R Management server are deployed, specify the parameters for connecting to them (see the "Connection to servers" section in the document [2]).
12. Add the vCenter server and all ESXi servers, Cloud Director server, Embedded Harbor registry (if available), Skala-R Management server and all Skala-R servers, KVM-server, Proxmox and OpenNebula servers to the list of protected servers (see the "Protected servers" section in the document [2]).
13. Install vGate Agents on all protected vCenter (vCSA), ESXi, KVM, Skala-R, Proxmox, OpenNebula servers (see the "vGate agent installation" in the document [2]).
14. Create user accounts (see the "User account management" section in the document [2]).
15. Add rules for access to protected servers (see the "Control of access to protected servers" section in the document [2]).
16. Configure security labels and assign them to user accounts and virtual infrastructure objects (see the "Configuring mandatory access control to confidential resources" section in the document [2]).
17. Assign security policy sets to protected objects or object groups (see the "Security policies" section in the document [2]).
18. Configure firewall rules for protected VMware vSphere servers (see the "Firewall" section in the document [2]).

Troubleshooting

Common issues

The list of issues that may occur while working with the vGate software and their solutions are given in the Troubleshooting.html file (it is located on the setup disk in the \Documentation folder)
vGate performance features and possible issues are given in the ReleaseNotes.html file (it is located on the setup disk in the \Documentation folder)

Questions and answers

This section contains the list of frequently asked questions and answers to them.

Question	Answer
Does vGate 4.7 support work with several vCenter servers?	Yes. To do this, you need to link vCenter servers using the VMware vCenter linked mode
How to reinstall vGate service accounts in Active Directory?	**1.** Remove vGate service accounts from AD. **2.** Run the vGate server setup program. **3.** In the appeared dialog box, click the "Change" button and follow the wizard instructions. All current vGate settings will be saved. **4.** Once the installation is completed, new vGate service accounts will be created in AD. **5.** Disable automatic change of passwords for vGate service accounts
Why does the vGate client installation on a computer from the protected server network end with an error?	The vGate client installation within the protected perimeter is not supported (see the "Local network configuration" section in the document [2])

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