

G&D RemoteAccess-GATE



EN Configuration and Operation

About this manual

This manual has been carefully compiled and examined to the state-of-the-art.

G&D neither explicitly nor implicitly takes guarantee or responsibility for the quality, efficiency and marketability of the product when used for a certain purpose that differs from the scope of service covered by this manual.

For damages which directly or indirectly result from the use of this manual as well as for incidental damages or consequential damages, G&D is liable only in cases of intent or gross negligence.

Caveat Emptor

G&D will not provide warranty for devices that:

- Are not used as intended.
- Are repaired or modified by unauthorized personnel.
- Show severe external damages that was not reported on the receipt of goods.
- Have been damaged by non G&D accessories.

G&D will not be liable for any consequential damages that could occur from using the products.

Proof of trademark

All product and company names mentioned in this manual, and other documents you have received alongside your G&D product, are trademarks or registered trademarks of the holder of rights.

© Guntermann & Drunck GmbH 2021. All rights reserved.

Version 1.00 – 20/01/2021

Firmware: 4.1.0

Guntermann & Drunck GmbH
Obere Leimbach 9
57074 Siegen

Germany

Phone +49 271 23872-0

Fax +49 271 23872-120

www.gdsys.de

sales@gdsys.de

Contents

Installation and Initial Configuration	1
Supported Browsers	1
Minimum Client and System Recommendations	1
Installation	2
Port Access and Configuration	3
Port Access	3
Port Configuration: KVM Port Settings - General, Video, Audio	4
Supported Preferred Video Resolutions	6
Port Configuration: Custom EDIDs	12
Port Configuration: Local Port Monitor EDID	13
Port Configuration: USB Connection Settings	13
KVM Clients	15
Virtual KVM Client (VKCS) Help	15
Java Requirements	16
Proxy Server Configuration	17
Connection Properties	18
Connection Info	20
Keyboard	20
Video	24
Mouse Options	25
Tool Options	30
View Options	37
Virtual Media	38
Digital Audio	41
External Device	46
Version Information - Virtual KVM Client	47
Active KVM Client (AKC) Help	48
Overview	48
AKC Supported Operating Systems	48
Prerequisites for Using AKC	48
Proxy Server Configuration	49
HTML KVM Client (HKC)	51
Connection Properties	52
Connection Info	55
Input Menu	56
Video Menu	68

View Menu.....	69
Tools Menu	69
Virtual Media Menu	71
Audio Menu	74
External Device Menu	76
Tips for Accessing RemoteAccess-GATE With Dual Monitor Setups.....	77

User Management 78

Gathering LDAP/Radius Information	79
Configuring Authentication.....	79
LDAP Authentication	81
Returning User Group Information from Active Directory Server.....	84
Radius Authentication	85
Returning User Group Information via RADIUS.....	86
Disabling External Authentication	86
Change Your Password.....	86
Connected Users.....	86
Users and Groups	87
Admin Group Special Privileges	93

Device Settings and Information 94

Device Information.....	94
Date and Time	96
Event Management	98
Send Email.....	100
SNMP Notifications	100
Syslog Messages	103
Keycode List	105
Network	106
Network Services	108
Discovery Port	108
HTTP/HTTPS Ports.....	109
SMTP Server Settings	110
SNMP Settings.....	111
SSH Settings	112
Serial Port	113
Terminal Block Control	114
Connecting the Terminal Block to a Motherboard	117

Virtual Media Shared Images	117
Security	118
Group Based Access Control.....	118
IP Access Control.....	119
KVM Security	120
Direct Port Access URL	122
Login Settings.....	123
Password Policy.....	124
TLS Certificate.....	125
Service Agreement.....	128
Maintenance	130
Backup and Restore.....	130
Event Log	132
Firmware History	133
Unit Reset.....	133
Update Firmware	134
Virtual Media	137
Overview	137
Virtual Media Performance Recommendations.....	138
Prerequisites for Using Virtual Media	138
RemoteAccess-GATE Virtual Media Prerequisites	138
Client PC VM Prerequisites	138
Target Server VM Prerequisites	138
Mounting Local Drives	139
Supported Tasks Via Virtual Media	139
Supported Virtual Media Types	139
Conditions when Read/Write is Not Available	140
Number of Supported Virtual Media Drives	140
Virtual Media in a Linux Environment.....	140
Active System Partitions.....	140
Mapped Drives.....	140
Drive Partitions.....	141
Root User Permission Requirement	141
Connect Drive Permissions (Linux).....	141
Virtual Media in a Mac Environment	141
Active System Partition.....	141
Drive Partitions.....	141
Connect Drive Permissions (Mac)	142

Virtual Media File Server Setup (File Server ISO Images Only).....	142
Diagnostics	143
Download Diagnostic	143
Network Diagnostics.....	143
CLI Commands	145
CLI: check.....	145
CLI: clear	145
CLI: config.....	146
CLI: config authentication.....	147
CLI: config device	150
CLI: config group	151
CLI: config network	152
CLI: config password.....	154
CLI: config security.....	155
CLI: config serial	157
CLI: config terminalblock	157
CLI: config time	158
CLI: config user	158
CLI: connect.....	160
CLI: diag.....	161
CLI: reset	162
CLI: show	163
CLI: exit.....	167
Specifications	168
TCP and UDP Ports Used.....	168
Index	169

Chapter 1 Installation and Initial Configuration

In This Chapter

Supported Browsers	1
Minimum Client and System Recommendations.....	1
Package Contents	2
Front View.....	2
Rear View.....	2
Connecting the Equipment	2
Initial Configuration	2
Option 1: Connect a PC to the LAN Port	2
Option 2: Connect an iOS device at the Local Port.....	2
Option 3: Serial configuration	2
Next Steps	2
KVM Client Options	2

Supported Browsers

- Chrome
- Edge
- Firefox
- Safari
- Internet Explorer

Minimum Client and System Recommendations

Minimum client requirements vary somewhat depending on what client you want to use, and what kind of video you plan to stream.

- ▶ **Network Speed Recommendation:**
 - A fast network like Gigabit Ethernet

► **Standalone Virtual KVM Client (VKCS) and Active KVM Client (AKC)**

- CPU:
 - For FullHD video: a modern and fast dual core CPU, such as Intel Core i3 4xxx or newer, or a quad core CPU. If you plan to run more than one KVM session, a quad core CPU is recommended.
 - For 4K video: a modern and fast quad core CPU, such as Intel Core i5 4xxx or newer. If you plan to run more than one 4K stream, a CPU with 6 or more cores is recommended, such as Intel Core i5/i7 8xxx.
- 8GB RAM
- Graphics Card: a modern OpenGL capable graphics card, such as GeForce or Radeon. At least 1GB.

► **HTML KVM Client (HKC):**

4K video not recommended on HKC.

- CPU: a modern and fast dual core CPU
- 8GB RAM
- OpenGL capable graphic card

Installation

The installation of the device is described in the separate Installation Guide.

Chapter 2 Port Access and Configuration

In This Chapter

Port Access	3
Port Configuration: KVM Port Settings - General, Video, Audio.....	4
Port Configuration: Custom EDIDs	12
Port Configuration: Local Port Monitor EDID.....	13
Port Configuration: USB Connection Settings	13

Port Access

Click Port Access to view the port preview and connect to the target.

► **Port Preview:**

- The preview image refreshes every 5 seconds.
- Your ability to see the preview depends on your privileges. If you do not have sufficient privileges, a message displays with details.



► **Connect to the target:**

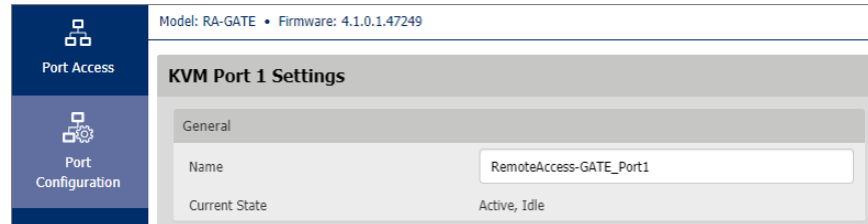
- Click the Connect button to open a connection to the target server.
- For help with using the KVM clients, see *KVM Clients* (on page 15).

Port Configuration: KVM Port Settings - General, Video, Audio

The Port Configuration page contains all port settings for the KVM port name and video resolution, as well as USB port and audio settings.

► **To access all port configuration:**

- Click Port Configuration.



► **KVM Port Settings:**

General Settings:

- To rename the KVM port: enter a new name and click Save.
- View the Current Port Status:
 - Active, Idle
 - Active, Busy: Connected, but PC Share is disabled. See *KVM Security* (on page 120).
 - Active, Connected: Connected, and PC Share is enabled.

Video Settings:

- Select **Enable VGA Mode** if the video input originates with a VGA or other analog source, through an HDMI adapter. In VGA mode, resolution is controlled on the video source device only.
- Select the **Preferred Video Resolution: Important!** The RemoteAccess-GATE uses an “EDID” data structure to tell the target server what video resolution is wanted. To change the video resolution on the target server, change the Preferred Video Resolution to the new resolution. This should change the resolution when you connect to the target; if not, you can then also change the resolution on the target server.
 - See *Supported Preferred Video Resolutions* (on page 6) for a list of all supported resolutions.
 - If you have a specific EDID to load, see *Port Configuration: Custom EDIDs* (on page 12).

- Set the **Video Interface** to HDMI or DVI (no audio).
- Set a longer **Cycle Time** if your target video is not responding properly to changes in preferred video resolution. Default is 200ms. A longer Cycle Time may allow your target to respond accurately to a new preferred video resolution.
- Select **Enable Video Throttle** to cap the client frame rate at half the frame rate of the incoming video. This can be useful to reduce network bandwidth and CPU load on the client.

Video Settings

❗ Enable VGA Mode when the video input originates with VGA or other analog source, through an HDMI adapter. In VGA mode, resolution is controlled on the video source device only.

Enable VGA Mode ☐

❗ Use these settings if necessary to help force digital video sources to desired screen resolution. Try a longer cycle time value if target does not respond properly.

Video Interface HDMI

Preferred Video Resolution 1920x1080 @ 60Hz

Cycle Time 200 ms

❗ Enable Video Throttle to cap the client frame rate at 1/2 that of the incoming video. This can be useful to reduce network bandwidth and/or CPU load on the client.

Enable Video Throttle ☐

Audio Settings

- If there is no audio, select Audio Compensation to enable it. You must reboot the RemoteAccess-GATE after disabling this function to allow a new audio connection to another target computer.

Audio Settings

❗ If there is no audio, please toggle Audio Compensation. Please reboot the device if you change this setting to connect it to another target computer.

Audio Compensation ☐

- Click Save to apply all settings.

Supported Preferred Video Resolutions

Each supported EDID is listed with the preferred video resolutions it can offer. The server will generally choose the largest resolution and refresh rate that it can support.

▶ 1024x768@60Hz

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz

▶ 1152x864@60Hz

- 640x480@60Hz, @72Hz, @75Hz, @85Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
- 1024x768@60Hz, @70Hz, @75Hz, @85Hz
- 1152x864@60Hz

▶ 1280x720@60Hz

- 640x480@60Hz, @72Hz, @75Hz, @85Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
- 1024x768@60Hz, @70Hz, @75Hz, @85Hz
- 1152x864@60Hz, @75Hz
- 1280x720@60Hz

▶ 1280x960@60Hz

- 640x480@60Hz, @72Hz, @75Hz, @85Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
- 1024x768@60Hz, @70Hz, @75Hz, @85Hz
- 1152x864@60Hz, @75Hz
- 1280x960@60Hz

▶ 1280x1024@60Hz

- 640x480@60Hz, @72Hz, @75Hz, @85Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
- 1024x768@60Hz, @70Hz, @75Hz, @85Hz
- 1152x864@60Hz, @75Hz

- 1280x1024@60Hz, @75Hz
- ▶ **1360x768@60Hz**
 - 640x480@60Hz, @72Hz, @75Hz
 - 720x400@70Hz
 - 800x600@56Hz, @60Hz, @72Hz, @75Hz
 - 1024x768@60Hz, @70Hz, @75Hz
 - 1152x864@60Hz, @75Hz
 - 1280x960@60Hz
 - 1280x1024@60Hz
 - 1360x768@60Hz
- ▶ **1440x900@60Hz**
 - 640x480@60Hz, @72Hz, @75Hz
 - 720x400@70Hz
 - 800x600@56Hz, @60Hz, @72Hz, @75Hz
 - 1024x768@60Hz, @70Hz, @75Hz
 - 1152x864@75Hz
 - 1280x960@60Hz
 - 1280x1024@60Hz
 - 1440x900@60Hz
- ▶ **1400x1050@60Hz**
 - 640x480@60Hz, @72Hz, @75Hz
 - 720x400@70Hz
 - 800x600@56Hz, @60Hz, @72Hz, @75Hz
 - 1024x768@60Hz, @70Hz, @75Hz
 - 1152x864@60Hz, @75Hz
 - 1280x960@60Hz
 - 1280x1024@60Hz, @75Hz
 - 1400x1050@60Hz
- ▶ **1600x900@60Hz**
 - 640x480@60Hz, @72Hz, @75Hz, @85Hz
 - 720x400@70Hz
 - 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
 - 1024x768@60Hz, @70Hz, @75Hz, @85Hz
 - 1152x864@60Hz, @75Hz, @85Hz
 - 1600x900@60Hz
- ▶ **1600x1200@60Hz**

- 640x480@60Hz, @72Hz, @75Hz, @85Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
- 1024x768@60Hz, @70Hz, @75Hz, @85Hz
- 1152x864@60Hz, @75Hz, @85Hz
- 1280x1024@75Hz
- 1600x1200@60Hz

► **1680x1050@60Hz**

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@60Hz, @75Hz
- 1280x960@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1680x1050@60Hz

► **1920x1080@60Hz (148.5MHz clock)**

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@60Hz
- 1280x960@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x1200@60Hz
- 1680x1050@60Hz
- 1920x1080@60Hz

► **1920x1200@60Hz (Reduced Blanking 154MHz clock)**

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@60Hz
- 1280x960@60Hz

- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x1200@60Hz
- 1680x1050@60Hz
- 1920x1080@60Hz
- 1920x1200@60Hz

▶ **1920x2160@60Hz**

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@60Hz
- 1280x960@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x1200@60Hz
- 1680x1050@60Hz
- 1920x1080@60Hz
- 1920x2160@60Hz

▶ **2560x1440@60Hz**

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 720x480@60Hz
- 720x576@50Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@50Hz, @60Hz
- 1280x800@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x900@60Hz
- 1680x720@60Hz
- 1680x1050@60Hz
- 1920x1080@24Hz, @30Hz, @60Hz
- 1920x1200@60Hz
- 2560x1080@30Hz

- 2560x1440@60Hz
- ▶ **2560x1600@60Hz**
 - 640x480@60Hz, @72Hz, @75Hz
 - 720x400@70Hz
 - 720x480@60Hz
 - 720x576@50Hz
 - 800x600@56Hz, @60Hz, @72Hz, @75Hz
 - 1024x768@60Hz, @70Hz, @75Hz
 - 1152x864@75Hz
 - 1280x720@50Hz, @60Hz
 - 1280x800@60Hz
 - 1280x1024@60Hz, @75Hz
 - 1440x900@60Hz
 - 1600x900@60Hz
 - 1680x720@60Hz
 - 1680x1050@60Hz
 - 1920x1080@24Hz, @30Hz, @60Hz
 - 1920x1200@60Hz
 - 2560x1080@30Hz
 - 2560x1600@60Hz
- ▶ **3840x1080@60Hz**
 - 640x480@60Hz, @72Hz, @75Hz
 - 720x400@70Hz
 - 720x480@60Hz
 - 720x576@50Hz
 - 800x600@56Hz, @60Hz, @72Hz, @75Hz
 - 1024x768@60Hz, @70Hz, @75Hz
 - 1152x864@75Hz
 - 1280x720@50Hz, @60Hz
 - 1280x800@60Hz
 - 1280x1024@60Hz, @75Hz
 - 1440x900@60Hz
 - 1600x900@60Hz
 - 1680x720@60Hz
 - 1680x1050@60Hz
 - 1920x1080@24Hz, @30Hz, @60Hz
 - 1920x1200@60Hz
 - 2560x1080@30Hz, @60Hz

- 2560x1440@60Hz
- 2560x1600@60Hz
- 3840x1080@60Hz

► **3840x1600@30Hz**

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 720x480@60Hz
- 720x576@50Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@60Hz
- 1280x800@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x900@60Hz
- 1680x1050@60Hz
- 1920x1080@60Hz
- 1920x1200@60Hz
- 2560x1080@60Hz
- 2560x1440@60Hz
- 3840x1600@30Hz

► **3840x2160@30Hz**

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 720x480@60Hz
- 720x576@50Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@50Hz, @60Hz
- 1280x800@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x900@60Hz
- 1680x720@60Hz
- 1680x1050@60Hz
- 1920x1080@24Hz, @30Hz, @60Hz

- 1920x1200@60Hz
- 2560x1080@60Hz
- 2560x1440@60Hz
- 2560x1600@60Hz
- 3440x1440@50Hz
- 3840x2160@24Hz, @25Hz, @30Hz
- 4096x2160@30Hz

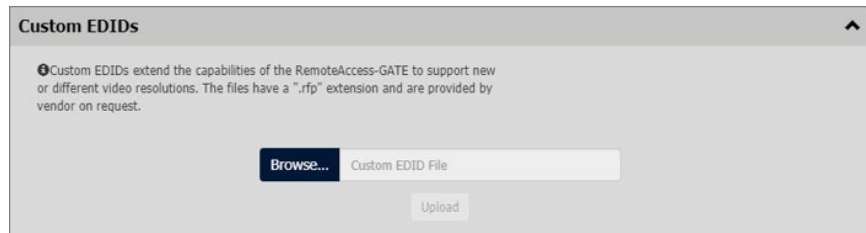
Port Configuration: Custom EDIDs

A custom EDID can be loaded to allow the RemoteAccess-GATE to support a new or different video resolution, or to specify a custom version of standard supported resolution. Only one custom EDID per resolution can be added. The files have a ".rfp" extension and are provided by the vendor on request.

You can upload up to 20 custom EDIDs with a maximum of 10 custom HDMI EDIDs and 10 custom DVI EDIDs. Custom EDIDs are not included in backups.

► To upload a custom EDID:

1. Click Port Configuration, then scroll down to Custom EDIDs.
2. Click Browse to find and select the .rfp EDID file.
3. Click Upload. Repeat these steps to add more files.
4. Once EDIDs are uploaded, they display in a list sorted by resolution.
 - Click Show Description to view the details.
 - Click the Delete icon to remove a file.



The screenshot shows a web interface titled "Custom EDIDs" with a small upward arrow icon in the top right corner. Below the title, there is a paragraph of text: "Custom EDIDs extend the capabilities of the RemoteAccess-GATE to support new or different video resolutions. The files have a ".rfp" extension and are provided by vendor on request." Below this text, there is a "Browse..." button next to a text input field labeled "Custom EDID File". Below the input field, there is an "Upload" button.

Port Configuration: Local Port Monitor EDID

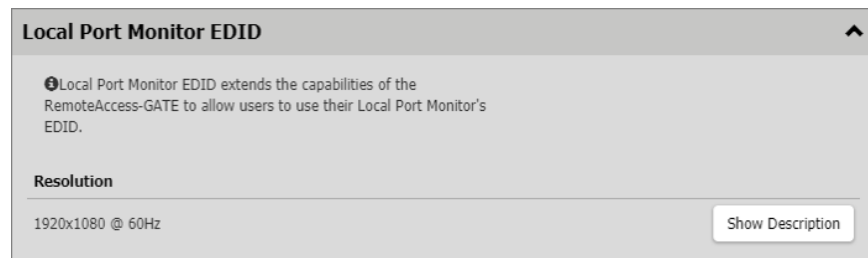
If a Local Port Monitor is attached to RemoteAccess-GATE, a Local Port Monitor EDID section appears on the Port Configuration page and the monitor's EDID is included in the Preferred Video Resolution. You can use the Local Port Monitor's EDID by selecting it as the Preferred Video Resolution.

If the Local Port Monitor is removed while it's EDID was in use as the preferred video resolution, the preferred video resolution will revert back to the default 1920x1080@60Hz standard EDID.

If a new monitor is attached, it will overwrite the old Local Port Monitor EDID.

► **To view Local Port Monitor EDID:**

1. Click Port Configuration, then scroll down to Local Port Monitor EDID.
2. The EDID of the currently attached local port monitor is listed.
 - Click Show Description to view the details.



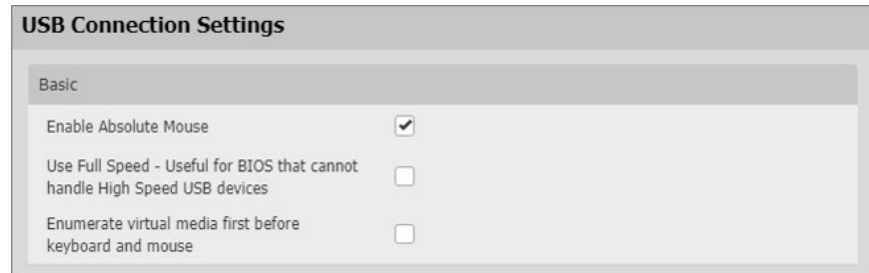
Port Configuration: USB Connection Settings

USB Connection Settings are disabled when the port is connected. All users must be disconnected from the KVM target to change the USB port settings.

► **To define USB connections for the target server:**

- Click Port Configuration, then scroll down to USB Connection Settings.
- Select the USB connection settings you will be using:
 - Enable Absolute Mouse - Disable if the target does not support absolute mouse mode
 - Use Full Speed - Useful for BIOS that cannot accommodate High Speed USB devices. Clear the checkbox to allow negotiation to the target's highest USB speed capability.

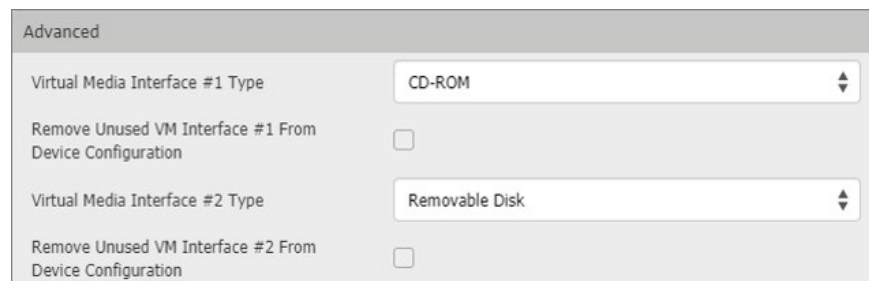
- Enumerate virtual media first before keyboard and mouse:
Useful to resolve issues when a target cannot detect USB mass storage at the BIOS.
- Click Save.



The screenshot shows the 'USB Connection Settings' window with the 'Basic' tab selected. It contains three settings: 'Enable Absolute Mouse' which is checked, 'Use Full Speed - Useful for BIOS that cannot handle High Speed USB devices' which is unchecked, and 'Enumerate virtual media first before keyboard and mouse' which is unchecked.

USB Connection Settings	
Basic	
Enable Absolute Mouse	<input checked="" type="checkbox"/>
Use Full Speed - Useful for BIOS that cannot handle High Speed USB devices	<input type="checkbox"/>
Enumerate virtual media first before keyboard and mouse	<input type="checkbox"/>

- Set Advanced Options as needed:
 - Virtual Media Interface Types: Both interfaces cannot be set to CDROM or Removable Disk.
 - Disabled
 - CDROM
 - Removable Disk
 - Auto - can function as either CDROM or Removable Drive but not both at the same time
 - Remove Unused VM Interface From Device Configuration: Select this option to remove the drive when VM is disconnected. Clear this option to allow empty drives.
- Click Save.



The screenshot shows the 'USB Connection Settings' window with the 'Advanced' tab selected. It contains four settings: 'Virtual Media Interface #1 Type' set to 'CD-ROM', 'Remove Unused VM Interface #1 From Device Configuration' which is unchecked, 'Virtual Media Interface #2 Type' set to 'Removable Disk', and 'Remove Unused VM Interface #2 From Device Configuration' which is unchecked.

Advanced	
Virtual Media Interface #1 Type	CD-ROM
Remove Unused VM Interface #1 From Device Configuration	<input type="checkbox"/>
Virtual Media Interface #2 Type	Removable Disk
Remove Unused VM Interface #2 From Device Configuration	<input type="checkbox"/>

Chapter 3 KVM Clients

RemoteAccess-GATE can be accessed with a variety of KVM clients that support your individual configuration.

- HKC is best for Linux and Mac users without Java.
- AKC is best for Windows Platforms, using Windows or Edge browsers.
- VKC is best for Linux and Mac users with Java.

KVM Client	Name	Platforms	Features
HTML KVM Client	HKC	<ul style="list-style-type: none">▪ Linux▪ Mac▪ Windows▪ HTML and Javascript	<ul style="list-style-type: none">▪ Java-Free▪ Supports most features▪ See HTML KVM Client (HKC) for supported features
Active KVM Client	AKC	<ul style="list-style-type: none">▪ Windows▪ Requires Microsoft .NET	<ul style="list-style-type: none">▪ Full-featured KVM Client▪ Java-Free
Virtual KVM Client	VKC	<ul style="list-style-type: none">▪ Linux▪ Mac▪ Windows	<ul style="list-style-type: none">▪ Full-featured KVM Client▪ Requires Java

In This Chapter

Virtual KVM Client (VKCS) Help.....	15
Active KVM Client (AKC) Help.....	48
HTML KVM Client (HKC)	51
Tips for Accessing Dominion KX IV-101 With Dual Monitor Setups.....	77

Virtual KVM Client (VKCS) Help

To launch VKCS, enter `https://< RemoteAccess-GATE IP address>/vkcs` in a browser.

Java Requirements

- A supported Java version is required.
- If Java is not installed, a prompt is displayed that the file cannot be opened, with an option to search for the program.

► VKCS Launching:

For all browsers, the VKCS standalone application needs to be downloaded everytime you use it.

- Chrome and Edge: The downloaded VKCS jnlp file must always be clicked at bottom left corner of browser window to launch.
- Internet Explorer: You must click Open at the bottom of the browser to launch.
- Safari: Save the jnlp file locally. Hold down the Ctrl key when selecting to open, then click Open in displayed prompt
- Firefox: The current default setting in Firefox on Windows saves the file and runs from the download. You can launch from the browser with this setting: Tools>Options>Applications, then select "Jnlp File" in the Content Type column, and change the Action from "Always ask" to "Use Java Web Launcher".

When launched from the Firefox browser, an executable warning message is displayed. There are two methods to suppress this:

- Launching via `jnlp://<IP address>/vkcs`

For details, go to: <https://superuser.com/questions/1441134/disable-firefoxs-open-executable-file-warning>

OR

- Add a new preference
"browser.download.skipConfirmLaunchExecutable" to
about:config.
- For details, go to <https://support.mozilla.org/en-US/questions/1260307>

Proxy Server Configuration

When the use of a Proxy Server is required, a SOCKS proxy must also be provided and configured on the remote client PC.

Note: If the installed proxy server is only capable of the HTTP proxy protocol, you cannot connect.

► **To configure the SOCKS proxy:**

1. On the remote client PC, select Control Panel > Internet Options.
 - a. On the Connections tab, click 'LAN settings'. The Local Area Network (LAN) Settings dialog opens.
 - b. Select 'Use a proxy server for your LAN'.
 - c. Click Advanced. The Proxy Settings dialog opens.
 - d. Configure the proxy servers for all protocols.

IMPORTANT: Do not select 'Use the same proxy server for all protocols'.

Note: The default port for a SOCKS proxy (1080) is different from HTTP proxy (3128).

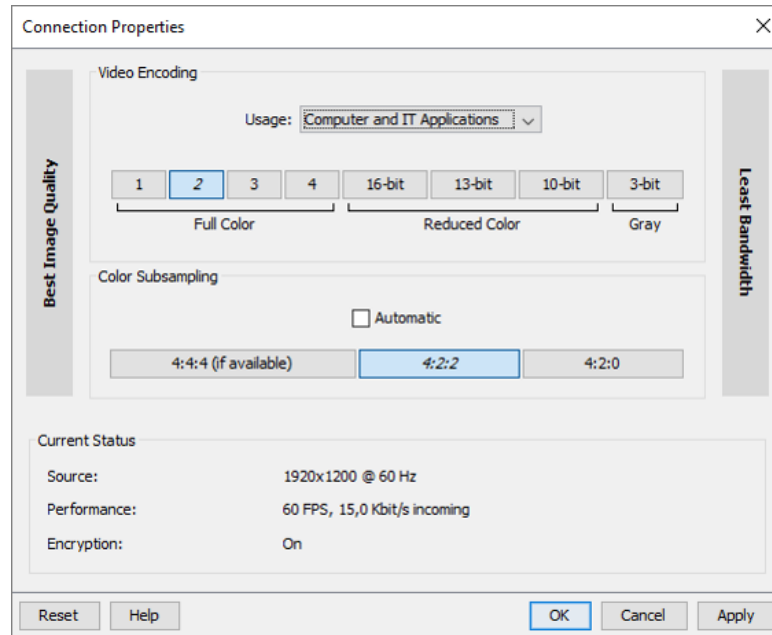
- e. Click OK at each dialog to apply the settings.
2. Next, configure the proxy settings for the Java™ applets:
 - a. Select Control Panel > Java.
 - b. On the General tab, click Network Settings. The Network Settings dialog opens.
 - c. Select "Use Proxy Server".
 - d. Click Advanced. The Advanced Network Settings dialog opens.
 - e. Configure the proxy servers for all protocols.

IMPORTANT: Do not select 'Use the same proxy server for all protocols'.

Note: The default port for a SOCKS proxy (1080) is different from HTTP proxy (3128).

Connection Properties

The Connection Properties dialog allows you to configure the video stream parameters to match your system capabilities with your performance needs.



► Video Encoding

This section selects the video encoding algorithm and quality setting.

- Usage: specify your general application area. This selection optimizes the available choices elsewhere in this dialog.
 - General Purpose Video: video content where smooth color reproduction is most important, such as movies, video games, and animations.
 - Computer and IT Applications: video content where text sharpness and clarity are important, such as computer graphical interfaces.

- **Encoder Mode:** Choose the encoder mode from the row of eight buttons. Options will vary depending on the Usage selection. In general, modes towards the left of the button bar offer higher image quality but consume higher bandwidth, and might cause frame rate to drop depending on network speed and/or client performance. Modes towards the right consume lower bandwidth at the cost of reduced image quality. In network- or client-constrained situations, modes towards the right may achieve better frame rates.

The default video mode is always "Full Color 2", which is a high-quality mode and works well for most uses in LAN environments. If needed, experiment with modes further towards the right to find the right balance of image quality and frame rate.

► Color Subsampling

Color subsampling reduces the color information in the encoded video stream.

- **Automatic:** Recommended. The optimal color subsampling mode will be enabled based on the selections in the video encoding section.
- **4:4:4:** Highest quality at significant bandwidth cost. Usually not necessary except for some situations in graphical user interfaces. Not supported for resolutions above 1920x1200, so for those resolutions color subsampling will automatically drop down to 4:2:2.
- **4:2:2:** Good blend of image quality and bandwidth.
- **4:2:0:** Maximum savings of network bandwidth and client load. Works fine for most general-purpose applications that don't emphasize high-resolution lines or text.

► Current Status

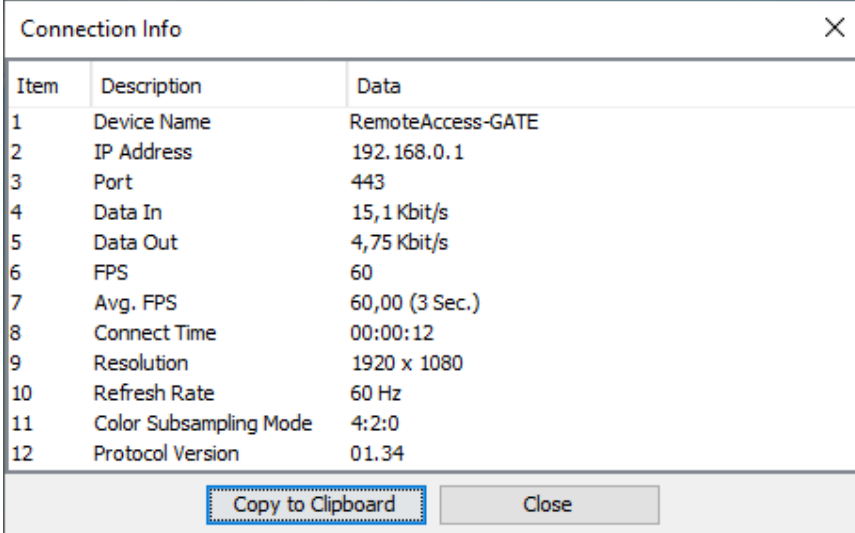
Current status includes real-time video performance statistics. As you change settings in the dialog, you can immediately see the effects on performance.

- **Source:** resolution and frame rate of the incoming video source.
- **Performance:** frames per second (FPS) being rendered in the client, and the data rate of the incoming video stream. These values are where you will see the effects of your video settings.
- **Encryption:** whether the video stream is encrypted or not. Encrypted streams usually have lower frame rates and lower bandwidth. Encryption is a global setting in security → KVM Security → "Apply Encryption Mode to KVM and Virtual Media".

Connection Info

Open the Connection Information dialog for real-time connection information on your current connection, and copy the information from the dialog as needed. To edit the connection properties, see **Connection Properties** (on page 18).

- To view the Connection Info, choose Connection > Info...



Item	Description	Data
1	Device Name	RemoteAccess-GATE
2	IP Address	192.168.0.1
3	Port	443
4	Data In	15,1 Kbit/s
5	Data Out	4,75 Kbit/s
6	FPS	60
7	Avg. FPS	60,00 (3 Sec.)
8	Connect Time	00:00:12
9	Resolution	1920 x 1080
10	Refresh Rate	60 Hz
11	Color Subsampling Mode	4:2:0
12	Protocol Version	01.34


Copy to Clipboard Close

Keyboard

Send Ctrl+Alt+Del Macro

Due to its frequent use, a Ctrl+Alt+Delete macro is preprogrammed.

Selecting Keyboard > Send Ctrl+Alt+Del, or clicking on the

Ctrl+Alt+Delete button  in the toolbar sends this key sequence to the server or to the KVM switch to which you are currently connected.

In contrast, if you were to physically press the Ctrl+Alt+Del keys, the command would first be intercepted by your own PC due to the structure of the Windows operating system, instead of sending the key sequence to the target server as intended.

Send LeftAlt+Tab (Switch Between Open Windows on a Target Server)

Select Keyboard > Send LeftAlt + Tab to switch between open windows on the target server.

Send Text to Target

► To use the Send Text to Target function for the macro:

1. Click the Keyboard > Send Text to Target. The Send Text to Target dialog appears.
2. Enter the text you want sent to the target.

Note: Non-English characters are not supported by the Send Text to Target function.

3. If the target uses a US/International keyboard layout, select the "Target system is set to the US/International keyboard layout" checkbox.
4. Click OK.

Keyboard Macros

Keyboard macros ensure that keystroke combinations intended for the target server are sent to and interpreted only by the target server. Otherwise, they might be interpreted by your client PC.

Macros are stored on the client PC and are PC-specific. If you use another PC, you cannot see your macros.

In addition, if another person uses your PC and logs in under a different name, that user will see your macros since they are computer-wide.

Build a New Macro

► To build a macro:

1. Click Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.
2. Click Add. The Add Keyboard Macro dialog appears.
3. Type a name for the macro in the Keyboard Macro Name field. This name appears in the Keyboard menu after it is created.
4. From the Hot-Key Combination field, select a keyboard combination from the drop-down list. This allows you to execute the macro with a predefined keystroke. **Optional**
5. In the Keys to Press drop-down list, select each key you would like to use to emulate the keystrokes that is used to perform the command. Select the keys in the order by which they are to be pressed. After each selection, select Add Key. As each key is selected, it appears in the Macro Sequence field and a Release Key command is automatically added after each selection.

For example, create a macro to close a window by selecting Left Ctrl + Esc. This appears in the Macro Sequence box as follows:

Press Left Alt

Press F4

Esc

Release F4

Esc

Release Left Alt

6. Review the Macro Sequence field to be sure the macro sequence is defined correctly.
 - a. To remove a step in the sequence, select it and click Remove.
 - b. To change the order of steps in the sequence, click the step and then click the up or down arrow buttons to reorder them as needed.
7. Click OK to save the macro. Click Clear to clear all field and start over. When you click OK, the Keyboard Macros dialog appears and lists the new keyboard macro.
8. Click Close to close the Keyboard Macros dialog. The macro now appears on the Keyboard menu in the application.
9. Select the new macro on the menu to run it or use the keystrokes you assigned to the macro.

Importing and Exporting Macros

Macros created in VKC cannot be used in AKC or vice versa. Macros created on HKC are only compatible with HKC, and cannot be used on AKC or VKC. Likewise, macros created on VKC or AKC cannot be used on HKC.

Import Macros

► To import macros:

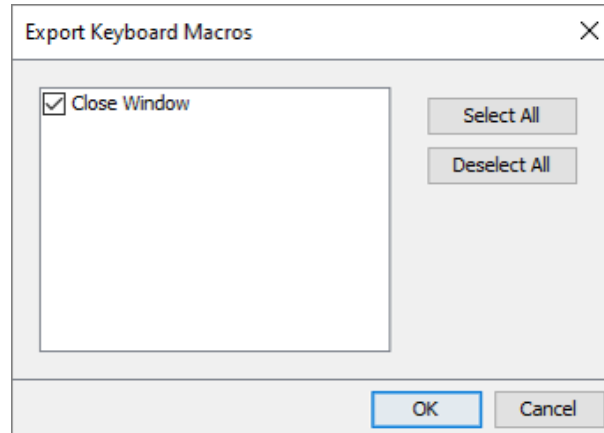
1. Choose Keyboard > Import Keyboard Macros to open the Import Macros dialog. Browse to the folder location of the macro file.
2. Click on the macro file and click Open to import the macro.
 - a. If too many macros are found in the file, an error message is displayed and the import terminates once OK is selected.
 - b. If the import fails, an error dialog appears and a message regarding why the import failed is displayed. Select OK to continue the import without importing the macros that cannot be imported.

3. Select the macros to be imported by checking their corresponding checkbox or using the Select All or Deselect All options.
4. Click OK to begin the import.
 - a. If a duplicate macro is found, the Import Macros dialog appears. Do one of the following:
 - Click Yes to replace the existing macro with the imported version.
 - Click Yes to All to replace the currently selected and any other duplicate macros that are found.
 - Click No to keep the original macro and proceed to the next macro
 - Click No to All keep the original macro and proceed to the next macro. Any other duplicates that are found are skipped as well.
 - Click Cancel to stop the import.
 - Alternatively, click Rename to rename the macro and import it. If Rename is selected, the Rename Macro dialog appears. Enter a new name for the macro in the field and click OK. The dialog closes and the process proceeds. If the name that is entered is a duplicate of a macro, an alert appears and you are required to enter another name for the macro.
 - b. If during the import process the number of allowed, imported macros is exceeded, a dialog appears. Click OK to attempt to continue importing macros or click Cancel to stop the import process.

The macros are then imported. If a macro is imported that contains a hot key that already exists, the hot key for the imported macro is discarded.

Export Macros

1. Choose Tools > Export Macros to open the Select Keyboard Macros to Export dialog.



2. Select the macros to be exported by checking their corresponding checkbox or using the Select All or Deselect All options.
3. Click OK. An "Export Keyboard Macros to" dialog is displayed. Locate and select the macro file. By default, the macro exists on your desktop.
4. Select the folder to save the macro file to, enter a name for the file and click Save. If the macro already exists, you receive an alert message.
5. Select Yes to overwrite the existing macro or No to close the alert without overwriting the macro.

Video

Refreshing the Screen

The Refresh Screen command forces a refresh of the video screen

- Choose Video > Refresh Screen, or click the Refresh Screen button




in the toolbar.

Screenshot from Target Command (Target Screenshot)

Take a screenshot of a target server using the Screenshot from Target server command. If needed, save this screenshot to a file location of your choosing as a bitmap, JPEG or PNG file.

► To take a screenshot of the target server:

1. Select Video > Screenshot from Target, or click the Target Screenshot button  on the toolbar.
2. In the Save dialog, choose the location to save the file, name the file, and select a file format from the 'Files of type' drop-down.
3. Click Save to save the screenshot.

Mouse Options

You can operate in either single mouse mode or dual mouse mode.

When in a dual mouse mode, and provided the option is properly configured, the mouse cursors align.

When controlling a target server, the Remote Console displays two mouse cursors - one belonging to your RemoteAccess-GATE client workstation, and the other belonging to the target server.

When there are two mouse cursors, the device offers several mouse modes:

- Absolute (Mouse Synchronization)
- Intelligent (Mouse Mode)
- Standard (Mouse Mode)

When the mouse pointer lies within the KVM Client target server window, mouse movements and clicks are directly transmitted to the connected target server.

While in motion, the client mouse pointer slightly leads the target mouse pointer due to mouse acceleration settings.

Single mouse mode allows you to view only the target server's pointer. You can use Single mouse mode when other modes don't work.

You can toggle between these two modes (single mouse and dual mouse).

Dual Mouse Modes

Absolute Mouse Synchronization

In this mode, absolute coordinates are used to keep the client and target cursors in synch, even when the target mouse is set to a different acceleration or speed.

This is the default mouse mode.

► To enter Absolute Mouse Synchronization:

- Choose Mouse > Absolute from the KVM client.

Intelligent Mouse Mode

In Intelligent Mouse mode, the device can detect the target mouse settings and synchronize the mouse cursors accordingly, allowing mouse acceleration on the target. Use intelligent mouse mode if absolute mouse mode is not supported on the target.

Enter Intelligent Mouse Mode

► To enter intelligent mouse mode:

- Choose Mouse > Intelligent.

Intelligent Mouse Synchronization Conditions

The Intelligent Mouse Synchronization command, available on the Mouse menu, automatically synchronizes mouse cursors during moments of inactivity. For this to work properly, however, the following conditions must be met:

- The active desktop should be disabled on the target.
- No windows should appear in the top left corner of the target page.
- There should not be an animated background in the top left corner of the target page.
- The target mouse cursor shape should be normal and not animated.
- The target mouse speeds should not be set to very slow or very high values.
- The target advanced mouse properties such as "Enhanced pointer precision" or "Snap mouse to default button in dialogs" should be disabled.
- The edges of the target video should be clearly visible (that is, a black border should be visible between the target desktop and the remote KVM console window when you scroll to an edge of the target video image).
- When using the intelligent mouse synchronization function, having a file icon or folder icon located in the upper left corner of your desktop may cause the function not to work properly. To be sure to avoid any problems with this function, do not have file icons or folder icons in the upper left corner of your desktop.

After autosensing the target video, manually initiate mouse synchronization by clicking the Synchronize Mouse button on the toolbar. This also applies when the resolution of the target changes if the mouse cursors start to desync from each other.

If intelligent mouse synchronization fails, this mode will revert to standard mouse synchronization behavior.

Please note that mouse configurations will vary on different target operating systems. Consult your OS guidelines for further details. Also note that intelligent mouse synchronization does not work with UNIX targets.

Standard Mouse Mode

Standard Mouse mode uses a standard mouse synchronization algorithm. The algorithm determines relative mouse positions on the client and target server.

In order for the client and target mouse cursors to stay in synch, mouse acceleration must be disabled. Additionally, specific mouse parameters must be set correctly.

► To enter Standard Mouse mode:

- Choose Mouse > Standard.

Mouse Synchronization Tips


If you have an issue with mouse synchronization:

1. Verify that the selected video resolution and refresh rate are among those supported by the device. The KVM Client Connection Info dialog displays the actual values that the device is seeing.
2. If that does not improve the mouse synchronization (for Linux, UNIX, and Solaris KVM target servers):
3. Open a terminal window.
4. Enter the following command: `xset mouse 1 1`
5. Close the terminal window.
6. Click the "KVM Client mouse synchronization" button.

Synchronize Your Mouse

In dual mouse mode, the Synchronize Mouse command forces realignment of the target server mouse cursor with the client mouse cursor.

► To synchronize the mouse cursors, do one of the following:

- Click the Synchronize Mouse button  in the KVM client toolbar, or select Mouse > Synchronize Mouse from the menu bar.

Note: This option is available only in Standard and Intelligent mouse modes.

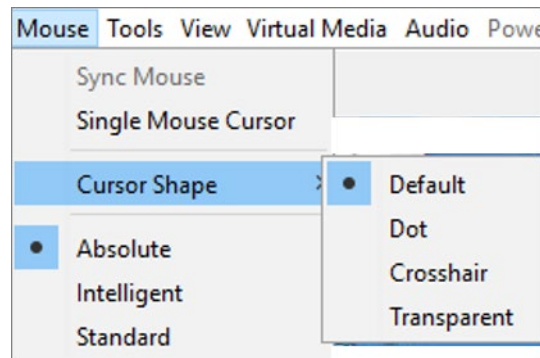
Cursor Shape

In dual mouse modes, you can select a custom cursor shape for your session. To make the cursor selection permanent, see ***Client Launch Settings*** (on page 34).

► To change the cursor shape:

- Choose Mouse > Cursor Shape, then select from the list.
 - Default arrow

- Dot
- Crosshair
- Transparent




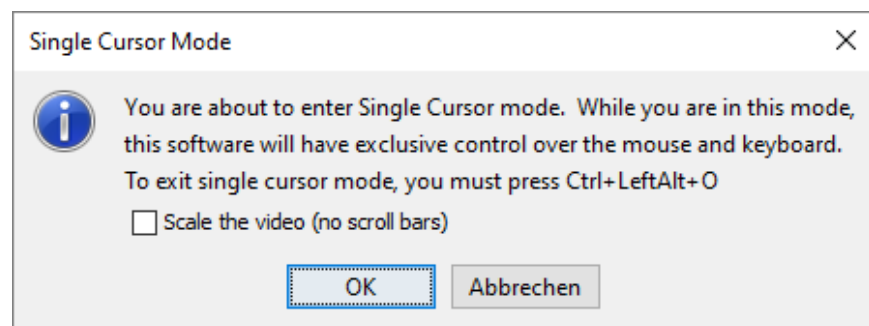
Single Mouse Mode

Single Mouse mode uses only the target server mouse cursor; the client mouse cursor no longer appears onscreen.

Note: Single mouse mode does not work on Windows or Linux targets when the client is running on a Virtual Machine.

► To enter single mouse mode, do one the following:

- Choose Mouse > Single Mouse Cursor.
- Click the Single/Double Mouse Cursor button  in the toolbar.



► To exit single mouse mode:

1. Press Ctrl+Alt+O on your keyboard to exit single mouse mode.

Tool Options

General Settings

► **To set the tools options:**

1. Click Tools > Options. The Options dialog appears.
2. OpenGL rendering of scaled KVM images is enabled by default. If there are performance issues, select the Disable Hardware Accelerated Rendering checkbox to disable. **Only available in AKC.**
3. Select the Enable Logging checkbox only if directed to by Technical Support.

This option creates a log file in your home directory.

4. Choose the Keyboard Type from the drop-down list (if necessary).

The options include:

- US/International
- French (France)
- German (Germany)
- Japanese
- United Kingdom
- Korean (Korea)
- French (Belgium)
- Norwegian (Norway)
- Portuguese (Portugal)
- Danish (Denmark)
- Swedish (Sweden)
- German (Switzerland)
- Hungarian (Hungary)
- Spanish (Spain)
- Italian (Italy)
- Slovenian
- Translation: French - US
- Translation: French - US International

In AKC, the keyboard type defaults to the local client, so this option does not apply.

5. Select Adjust Full Screen Window Size to Target Resolution Instead of Client Resolution if you prefer. Option not available for Linux clients. See ***Adjust Full Screen Window Size to Target Resolution*** (on page 33) for details and examples.

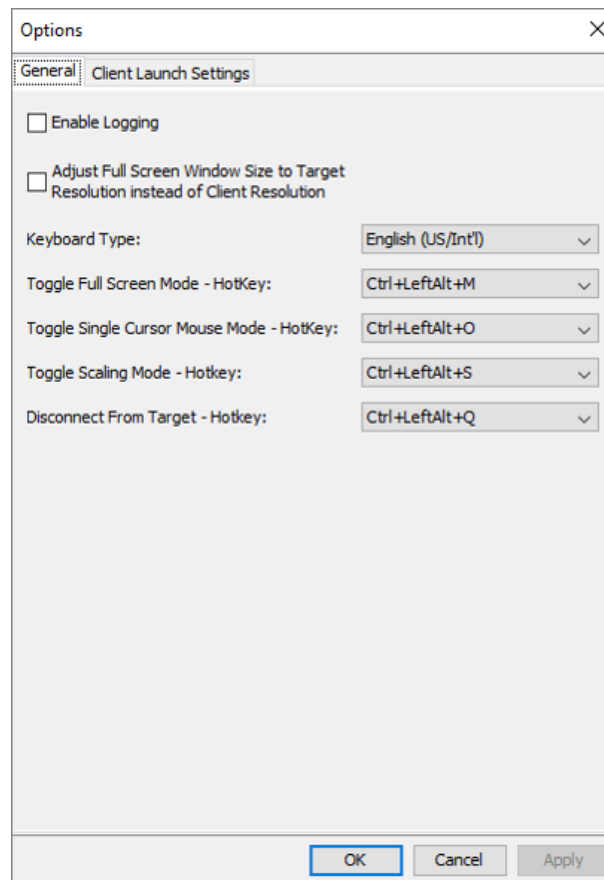
6. In Mac OS/VKCs launches only, Let Full Screen Window Cover the Main Menu Bar and the Dock is enabled by default. Use this setting to prevent the Java menubar from hiding the VKCs menubar when running VKCs in full-screen mode on Mac.
7. Configure hotkeys:
 - Toggle Full Screen Mode - Hotkey.
When you enter Full Screen mode, the display of the target server becomes full screen and acquires the same resolution as the target server.
This is the hot key used for toggling in and out of this mode.
 - Toggle Single Cursor Mode - Hotkey.
When you enter single cursor mode, only the target server mouse cursor is visible.
This is the hot key used to toggle in and out of single cursor mode, removing and bringing back the client mouse cursor.
 - Toggle Scaling Mode - Hotkey.
When you enter scaling mode, the target server scales to fit your display.
This is the hot key used to toggle in and out of scaling mode.
 - Disconnect from Target - Hotkey.
Enable this hotkey to allow users to quickly disconnect from the target.

For hotkey combinations, the application does not allow you to assign the same hotkey combination to more than one function.

For example, if Q is already applied to the Disconnect from Target function, it won't be available for the Toggle Full Screen Mode function.

Further, if a hotkey is added to the application due to an upgrade and the default value for the key is already in use, the next available value is applied to the function instead.

8. Click OK.



Keyboard Limitations

Turkish Keyboards

Turkish keyboards are only supported on Active KVM Client (AKC).

Slovenian Keyboards

The < key does not work on Slovenian keyboards due to a JRE limitation.

Language Configuration on Linux

Because the Sun JRE on Linux has problems generating the correct Key Events for foreign-language keyboards configured using System Preferences, configure foreign keyboards using the methods described in the following table.

Language	Configuration method
US Intl	Default
French	Keyboard Indicator

Language	Configuration method
German	System Settings (Control Center)
Japanese	System Settings (Control Center)
UK	System Settings (Control Center)
Korean	System Settings (Control Center)
Belgian	Keyboard Indicator
Norwegian	Keyboard Indicator
Danish	Keyboard Indicator
Swedish	Keyboard Indicator
Hungarian	System Settings (Control Center)
Spanish	System Settings (Control Center)
Italian	System Settings (Control Center)
Slovenian	System Settings (Control Center)
Portuguese	System Settings (Control Center)

Note: The Keyboard Indicator should be used on Linux systems using Gnome as a desktop environment.

Adjust Full Screen Window Size to Target Resolution

When Adjust Full Screen Window Size to Target Resolution Instead of Client Resolution is enabled, the client starts in full-screen in a window equal to the target's resolution, not the resolution of the client monitor. If you have a multi-monitor client, a full-screen window may cover more than one monitor. See **General Settings** (on page 30) for instructions on enabling the setting.

► Example:

The client has a multi-head environment with 8 monitors, 1920 x 1080 each with the following arrangement:

1	2	3	4
5	6	7	8

A KVM session is launched on monitor 6 with a the target resolution of 3840 x 1080. The client window opens on monitor 6 and 7 in native resolution and covers both monitors by 100%.

Client Launch Settings

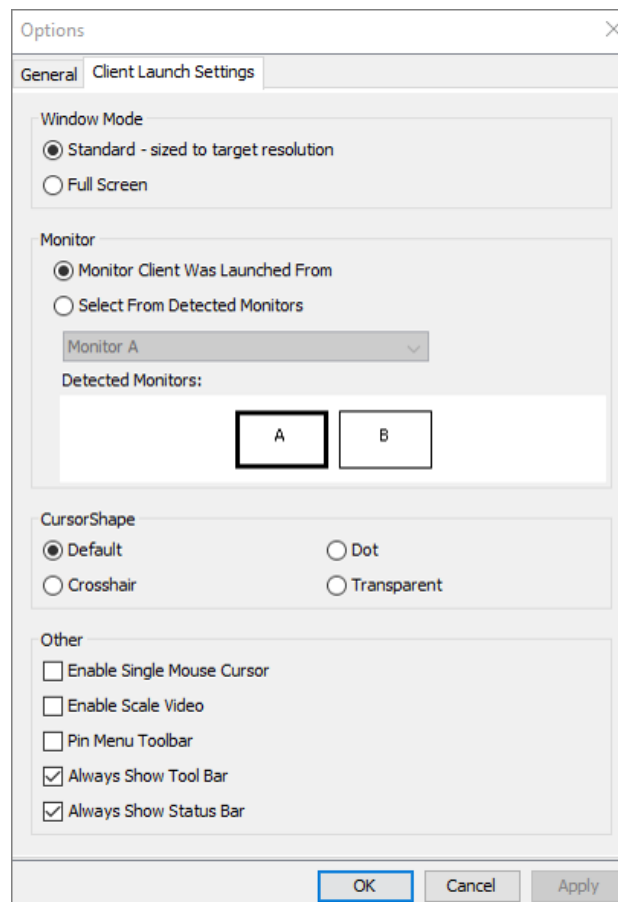
Configuring client launch settings allows you to define the screen settings for a KVM session.

► **To configure client launch settings:**

1. Click Tools > Options. The Options dialog appears.
2. Click on the Client Launch Settings tab.
 - To configure the **target window settings**:
 - Select 'Standard - sized to target Resolution' to open the window using the target's current resolution. If the target resolution is greater than the client resolution, the target window covers as much screen area as possible and scroll bars are added (if needed).
 - Select 'Full Screen' to open the target window in full screen mode.
 - To configure the **monitor on which the target viewer is launched**:
 - Select 'Monitor Client Was Launched From' if you want the target viewer to be launched using the same display as the application that is being used on the client (for example, a web browser or applet).
 - Use 'Select From Detected Monitors' to select from a list of monitors that are currently detected by the application. If a previously selected monitor is no longer detected, 'Currently Selected Monitor Not Detected' is displayed.
 - To configure **cursor shape**:
 - Select Default arrow, Dot, Crosshair, or Transparent to set the cursor shape for all sessions. Use the Mouse menu to change the cursor shape during a session.
 - To configure **additional launch settings**:

- Select 'Enable Single Cursor Mode' to enable single mouse mode as the default mouse mode when the server is accessed.
- Select 'Enable Scale Video' to automatically scale the display on the target server when it is accessed.
- Select 'Pin Menu Toolbar' if you want the toolbar to remain visible on the target when it is in Full Screen mode. By default, while the target is in Full Screen mode, the menu is only visible when you hover your mouse along the top of the screen.
- Always Show Tool Bar and Always Show Status Bar are per-user settings that are stored in the computer you are accessing the client from, so if you use a different computer, the setting may be different. Select to keep tool bar and status bar visible as default, deselect to keep tool bar and status bar hidden as default.

3. Click OK.



Collecting a Diagnostic Snapshot of the Target

Administrators are able to collect a "snapshot" of a target.

The "snapshot" function generate log files and image files from the target.

It then bundles these files in a zip file that can be sent to Technical Support to help diagnose technical problems you may be encountering.

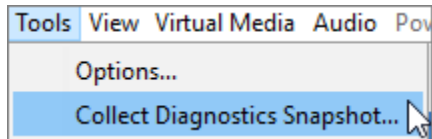
The following files are included in the zip file:

- screenshot_image.png
This is a screenshot of the target that captures a picture of the issue you are experiencing. This feature operates like the "Screenshot from Target" feature.
- raw_video_image.png:
A snapshot image created from raw video data. Please note that client's postprocessing is applied, just as if it were a "regular" screen update.
- raw_video_ycbcr420.bin:
Binary file of the raw snapshot.
- raw_video_ycbcr420.txt:
Text file containing data used to help diagnose issues.
- Log.txt file:
These are the client logs.

Note that the logs are included even if you have not enabled information to be captured in them. VKC uses internal memory to capture the information in this case.

Collect a Diagnostic Snapshot

- To capture a diagnostic snapshot:



Steps	
①	Access a target, and then click Tools > Collect a Diagnostic Snapshot. Several messages are displayed as the information is collected.
②	You are prompted to save the zip file containing the diagnostic files.
③	The zip file containing the diagnostic files is saved.

View Options

View Toolbar

You can use the Virtual KVM client with or without the toolbar display.

- To toggle the display of the toolbar (on and off):

- Choose View > View Toolbar.

View Status Bar

By default, the status bar is displayed at the bottom of the target window.

- To hide the status bar:

- Click View > Status Bar to deselect it.

- To restore the status bar:

- Click View > Status Bar to select it.

Scaling

Scaling your target window allows you to view the entire contents of the target server window.

This feature increases or reduces the size of the target video to fit the Virtual KVM Client window size, and maintains the aspect ratio so that you see the entire target server desktop without using the scroll bar.

► **To toggle scaling (on and off):**

- Choose View > Scaling.

Full Screen Mode

When you enter Full Screen mode, the target's full screen is displayed and acquires the same resolution as the target server.

The hot key used for exiting this mode is specified in the Options dialog, see *Tool Options* (on page 30).

While in Full Screen mode, moving your mouse to the top of the screen displays the Full Screen mode menu bar.

If you want the menu bar to remain visible while in Full Screen mode, enable the Pin Menu Toolbar option from the Tool Options dialog. See *Tool Options* (on page 30).

► **To enter full screen mode:**

- Choose View > Full Screen, or click the Full Screen button .

► **To exit full screen mode:**

- Press the hot key configured in the Tool's Options dialog. The default is Ctrl+Alt+M.

If you want to access the target in full screen mode at all times, you can make Full Screen mode the default.

► **To set Full Screen mode as the default mode:**

1. Click Tools > Options to open the Options dialog.
2. Select Enable Launch in Full Screen Mode and click OK.


Virtual Media

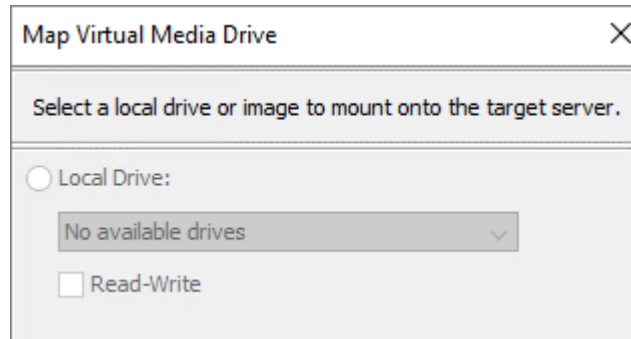
Access a Virtual Media Drive on a Client Computer

Important: Once you are connected to a virtual media drive, do not change mouse modes in the KVM client if you are performing file transfers, upgrades, installations or other similar actions. Doing so

may cause errors on the virtual media drive or cause the virtual media drive to fail.

► **To access a virtual media drive on the client computer:**

1. From the KVM client, choose Virtual Media > Connect Drive, or click the Connect Drive... button . The Map Virtual Media Drive dialog appears.



2. Choose the drive from the Local Drive drop-down list.
If you want Read and Write capabilities, select the Read-Write checkbox.
This option is disabled for nonremovable drives. See the ***Conditions when Read/Write is Not Available*** (on page 140) for more information.
When checked, you will be able to read or write to the connected USB disk.

WARNING: Enabling Read/Write access can be dangerous! Simultaneous access to the same drive from more than one entity can result in data corruption. If you do not require Write access, leave this option unselected.

3. Click OK. The media will be mounted on the target server virtually. You can access the media just like any other drive.

Access a Virtual Media Image File

Use the "Image File" option to access a disk image of a removable disk.

► **Image file guidelines:**

- Image files created using dd on Linux (dd if=/dev/sdb of=disk.img) or similar tools such as Win32DiskImager on Windows, or Mac Disk Utility are supported.
- Apple DMG files:
 - DMG image files of a FAT32 USB drive are recognized on all OSs.

- DMG images files of a folder on a Mac Drive are recognized only on Mac OS targets.
- Image should be created via Mac Disk Utility using the following settings: Encryption: None; Image format: read/write.
- Not supported: Encrypted or compressed dmg images, MacOS install images, DMG files downloaded from the Apple support site.

► **To access a virtual media image file:**


1. From the KVM client, choose Virtual Media > Connect Drive, or click the Connect Drive... button . The Map Virtual Media Drive dialog appears.
2. Select the Image File option, then click Browse to find and select the .img or .dmg file.
3. Click OK. The media will be mounted on the target server virtually.

Mounting CD-ROM/DVD-ROM/ISO Images

This option mounts CD-ROM, DVD-ROM, and ISO images.

Note: ISO9660 format is the standard supported. However, other CD-ROM extensions may also work.

► **To access a CD-ROM, DVD-ROM, or ISO image:**

1. From the KVM client, choose Virtual Media > Connect CD-ROM/ISO Image, or click the Connect CD ROM/ISO button  . The Map Virtual Media CD/ISO Image dialog appears.
2. For internal and external CD-ROM or DVD-ROM drives:
 - a. Choose the Local CD/DVD Drive option.
 - b. Choose the drive from the Local CD/DVD Drive drop-down list. All available internal and external CD and DVD drive names will be populated in the drop-down list.
 - c. Click OK.
3. For ISO images:
 - a. Choose the ISO Image option. Use this option when you want to access a disk image of a CD, DVD, or hard drive. ISO format is the only format supported.
 - b. Click Browse.
 - c. Navigate to the path containing the disk image you want to use and click Open. The path is populated in the Image Path field.
 - d. Click OK.
4. For remote ISO images on a file server:

- a. Choose the Remote Server ISO Image option.
- b. Choose Hostname and Image from the drop-down list. The file servers and image paths available are those that you configured using the Virtual Media Shared Images page. Only items you configured using the Virtual Media Shared Images page will be in the drop-down list.
- c. File Server Username - User name required for access to the file server. The name can include the domain name such as mydomain/username.
- d. File Server Password - Password required for access to the file server (field is masked as you type).
- e. Click OK.

The media will be mounted on the target server virtually. You can access the media just like any other drive.

Note: If you are working with files on a Linux® target, use the Linux Sync command after the files are copied using virtual media in order to view the copied files. Files may not appear until a sync is performed.

Note: If you are using the Windows 7® operating system®, Removable Disk is not displayed by default in the Window's My Computer folder when you mount a Local CD/DVD Drive or Local or Remote ISO Image. To view the Local CD/DVD Drive or Local or Remote ISO Image in this folder, select Tools > Folder Options > View and deselect "Hide empty drives in the Computer folder".

Disconnect from Virtual Media Drives

► To disconnect the virtual media drives:

- For local drives, choose Virtual Media > Disconnect Drive.
- For CD-ROM, DVD-ROM, and ISO images, choose Virtual Media > Disconnect CD-ROM/ISO Image.

Note: In addition to disconnecting the virtual media using the Disconnect command, simply closing the KVM connection closes the virtual media as well.

Digital Audio





The RemoteAccess-GATE supports audio playback over HDMI.

Supported Audio Device Formats

The following playback formats are supported:

- Stereo, 16bit, 44.1K
- Stereo, 16bit, 32K
- Stereo, 16bit, 48K

Digital Audio VKC and AKC Icons

Audio icons	Icon name	Description
  	Speaker	<p>These icons are located in status bar at the bottom of the client window.</p> <p>Green, blinking waves indicate an audio playback session is currently streaming.</p> <p>A black speaker icon is displayed when the session is muted.</p> <p>The icon is grayed out when no audio is connected.</p>
	Microphone	Playback is not supported. Microphone icon appears grayed out.

Audio Playback Recommendations and Requirements

► Audio level:

- Set the target audio level to a mid-range setting.
- For example, on a Windows® client, set the audio to 50 or lower.
- This setting must be configured through the playback device, not from the client audio device control.

Bandwidth Requirements

The table below details the audio playback bandwidth requirements to transport audio under each of the selected formats.

Audio format	Network bandwidth requirement
44.1 KHz, 16bit stereo	176 KB/s
32 KHz, 16bit stereo,	128KB/s
48 KHz, 16bit stereo	192KB/s

In practice, the bandwidth used when an audio device connects to a target is higher due to the keyboard and video data consumed when opening and using an audio application on the target.

A general recommendation is to have at least a 1.5MB connection before running audio/video.

However, high video-content, full-color connections using high-target screen resolutions consume much more bandwidth and impact the quality of the audio considerably.

To help mitigate quality degeneration, there are a number of recommended client settings that reduce the impact of video on audio quality at lower bandwidths:

- Connect audio playback at the lower quality formats. The impact of video consuming bandwidth is much less notable at 11k connections than at 44k
- Set the connection speed under Connection Properties to a value that best matches the client to server connection

Under Connection Properties, set the color depth to as low a value as possible. Reducing the color depth to 8 bit color considerably reduces the bandwidth consumed

Saving Audio Settings

Audio device settings are applied on a per RemoteAccess-GATE device basis.

Once the audio devices settings are configured and saved on the RemoteAccess-GATE, the same settings are applied to it.

For example, you can configure a Windows® audio device to use as stereo, 16 bit, 44.1K format.

When you connect to different targets and use that Windows audio device, the stereo, 16 bit, 44.1K format is applied to each target server.

For all devices, the device type, device format, and the buffer settings applied to the device are saved.

See ***Connecting and Disconnecting from a Digital Audio Device*** (on page 44) for information on connecting to and configuring an audio device, and ***Adjusting Buffer Size (Audio Settings)*** for information on audio device buffer settings.

If you are using the audio feature while running PC Share mode and VM Share mode so multiple users can access the same audio device on a target at once, the audio device settings of the user who initiates the session are applied to all users who join the session.

So, when a user joins an audio session, the target machine settings are used.

Connecting and Disconnecting from a Digital Audio Device


Audio device settings are applied on a per RemoteAccess-GATE device basis.

Once the audio devices settings are configured and saved on the RemoteAccess-GATE, the same settings are applied to it.

See ***Saving Audio Settings*** (on page 44) for more information.

Connect to a Digital Audio Device

► To connect to an audio device:

1. Connect the audio device to the remote client PC prior to launching the browser connection to the RemoteAccess-GATE.
2. Connect to the target from the Port Access page.
3. Once connected, click the Audio button  in the toolbar.

The Connect Audio Device dialog appears. A list of available audio devices connected to the remote client PC is displayed.

Note: If there are no available audio devices connected to the remote client PC, the Audio icon is grayed out. .

4. Check Connect Playback Device if you are connecting to a playback device.
5. Select the device that you wish to connect from the drop-down list.
6. Select the audio format for the playback device from the Format: drop-down.

Note: Select the format that you wish to use based on the available network bandwidth. Formats with lower sampling rates consume less bandwidth and may tolerate more network congestion.

7. Select the "Mount selected playback device automatically on connection to target" checkbox to automatically connect an audio playback device when you connect to an audio supporting target.
8. Click OK. If the audio connection is established, a confirmation message appears. Click OK.


If the connection was not established, an error message appears.

Once an audio connection is established, the Audio menu changes to Disconnect Audio. The settings for the audio device are saved and applied to subsequent connections to the audio device.

A Speaker icon is displayed in the status bar at the bottom of the client window. It is grayed out when no audio is being used.

Disconnect from an Audio Device

► To disconnect from the audio device:

- Click the Audio icon  in the toolbar and select OK when you are prompted to confirm the disconnect. A confirmation message appears. Click OK.

Adjusting Capture and Playback Buffer Size (Audio Settings)

Once an audio device is connected, the buffer size can be adjusted as needed.

This feature is useful for controlling the quality of the audio, which may be impacted by bandwidth limitations or network spikes.

Increasing the buffer size improves the audio quality but may impact the delivery speed.

The maximum available buffer size is 400 milliseconds since anything higher than that greatly impacts audio quality.

The buffer size can be adjusted whenever needed, including during an audio session.

Audio settings are configured in VKC or AKC.

Adjust Audio Settings

► To adjust audio settings:

1. Select Audio Settings from the Audio menu. The Audio Settings dialog opens.
2. Adjust the capture and/or playback buffer size as needed. Click OK.

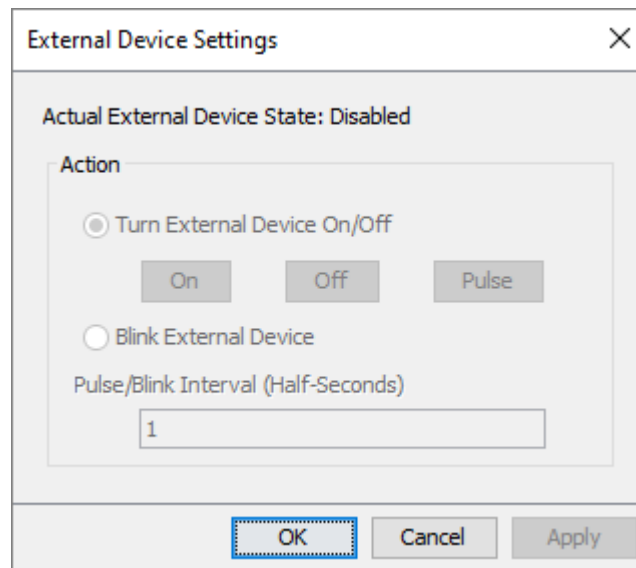
External Device

The External Device menu allows you to control the device connected at the terminal block of the RemoteAccess-GATE.

► External Device Settings:

1. Choose External Device > Settings to view the dialog.
2. The device state is listed.
3. Enabled devices can be controlled using the Actions options.
 - Turn External Device On/Off: Click On or Off to control terminal output relay.

- Blink External Device: Enter the half-second interval to control blinking of the external device.



The image shows a dialog box titled "External Device Settings" with a close button (X) in the top right corner. Inside the dialog, it states "Actual External Device State: Disabled". Below this, there is a section labeled "Action" containing two radio button options. The first option, "Turn External Device On/Off", is selected and has three buttons below it: "On", "Off", and "Pulse". The second option, "Blink External Device", is unselected. Below the radio buttons is a text input field labeled "Pulse/Blink Interval (Half-Seconds)" which contains the number "1". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply". The "OK" button is highlighted with a blue dashed border.

4. Click OK or Apply to save.

Version Information - Virtual KVM Client

For version information about the client, in case you require assistance from Technical Support.

- Choose Help > About.

Active KVM Client (AKC) Help

To launch AKC, enter `https://<IP address>/akc` in a browser.

Overview

The Active KVM Client (AKC) is based on Microsoft Windows .NET® technology.

This allows you to run the client in a Windows environments without Java.

AKC provides the same features as VKC with the exception of the following:

- Keyboard macros created in AKC cannot be used in any other client.
- Direct port access configuration
- AKC server certification validation configuration (see *Prerequisites for Using AKC* (on page 48))

For details on using the features, see Virtual KVM Client (VKC) Help.

AKC Supported Operating Systems

When launched from Internet Explorer®, the Active KVM Client (AKC) allows you to reach target servers via the RemoteAccess-GATE.

AKC is compatible with the following platforms:

- Windows 7® operating system (up to 64 bit)
- Windows 8® operating system (up to 64 bit)
- Windows 10 ® operating system (up to 64 bit)

Prerequisites for Using AKC

Allow Cookies

Ensure the cookies from the IP address of the device that is being accessed are not currently being blocked.

Include RemoteAccess-GATE IP Address in 'Trusted Sites Zone'

Windows® 7 users should ensure that the IP address of the device being accessed is included in their browser's Trusted Sites Zone.

Disable 'Protected Mode'

®Windows® 7 users should ensure that Protected Mode is not on when accessing this device.

Latest Edge Chromium 86.0.622.51

The new Edge Chromium browser has experimental ClickOnce support which must be enabled for AKC. The browser will not detect support for ClickOnce, so you will still need to download AKC manually.

- To enable ClickOnce in Edge: Type `edge://flags` in the browser, search for ClickOnce support, set to enabled and restart the browser.
- To download AKC manually: Go to the RemoteAccess-GATE URL, for example `https://[IP-Hostname]/akc` then select "Please click here" on the message showing that ClickOnce support has not been detected.

Proxy Server Configuration

When the use of a Proxy Server is required, a SOCKS proxy must also be provided and configured on the remote client PC.

Note: If the installed proxy server is only capable of the HTTP proxy protocol, you cannot connect.

► To configure the SOCKS proxy:

1. On the remote client PC, select Control Panel > Internet Options.
 - a. On the Connections tab, click 'LAN settings'. The Local Area Network (LAN) Settings dialog opens.
 - b. Select 'Use a proxy server for your LAN'.
 - c. Click Advanced. The Proxy Settings dialog opens.
 - d. Configure the proxy servers for all protocols.
IMPORTANT: Do not select 'Use the same proxy server for all protocols'.

Note: The default port for a SOCKS proxy [1080] is different from HTTP proxy [3128].

- e. Click OK at each dialog to apply the settings.
2. Next, configure the proxy settings for the Java™ applets:
 - a. Select Control Panel > Java.
 - b. On the General tab, click Network Settings. The Network Settings dialog opens.
 - c. Select "Use Proxy Server".
 - d. Click Advanced. The Advanced Network Settings dialog opens.
 - e. Configure the proxy servers for all protocols.

IMPORTANT: Do not select 'Use the same proxy server for all protocols'.

Note: The default port for a SOCKS proxy (1080) is different from HTTP proxy (3128).

HTML KVM Client (HKC)

The HTML KVM client (HKC) provides KVM over IP access that runs in the browser without the need for applets or browser plugins. HKC uses Javascript, NOT Java.

HKC runs on Linux and Mac clients, and on Windows clients in Internet Explorer 11 (not supported in IE 10 or lower), Edge, Firefox, Chrome and Safari browsers.

Many KVM features are supported. Future releases will provide more advanced KVM features.

► Supported Features:

- Connection Properties
- Input Settings
- Audio Playback
- Virtual Media
- Keyboard Macros
- Import and Export of Keyboard Macros
- Send Text to Target
- Keyboard and Mouse Settings
- Single Mouse Mode - not available on IE browser
- External Device

► Not supported:

- Video Settings
- Tools Menu for setting client launch settings, setting disconnect from target hotkey, or configuring toolbar display.
- Limited keyboard support: US-English, UK-English, French, and German are supported
- Hotkeys for keyboard macros
- Pre-populated keyboard macros for Sun targets
- Can only create Macros from keys that exist on the client PC (US-English, UK-English, French, or German), no special function keys
- Single Mouse mode - not available on IE
- Virtual Media write not supported
- Local file transfer supported by Chrome and Firefox browsers only
- USB drive connects
- Audio capture

► Known Issues:

- If HKC does not load, but rather displays a white screen, your browser memory may be full. Close all browser windows and try again.

Connection Properties

Connection properties manage streaming video performance over remote connections to target servers.

The properties are applied only to your connection - they do not impact the connection of other users accessing the same target servers.

If you make changes to connection properties, they are retained by the client.

► **To view connection properties:**

- Choose File > Connection Properties.

Connection Properties

Video Encoding

Usage: General Purpose Video

1 2 3 4 5 6 7 8

Full Color

Color Subsampling

☒ Automatic

4:4:4 (if available) 4:2:2 4:2:0

Source: 1920x1080 @ 60 Hz
Performance: 45.93 FPS, 155 Kbit/s incoming
Encryption: On

Reset Help OK Cancel Apply

► Video Encoding

This section selects the video encoding algorithm and quality setting.

- Usage: specify your general application area. This selection optimizes the available choices elsewhere in this dialog.
 - General Purpose Video: video content where smooth color reproduction is most important, such as movies, video games, and animations.
 - Computer and IT Applications: video content where text sharpness and clarity are important, such as computer graphical interfaces.

- **Encoder Mode:** Choose the encoder mode from the row of eight buttons. Options will vary depending on the Usage selection. In general, modes towards the left of the button bar offer higher image quality but consume higher bandwidth, and might cause frame rate to drop depending on network speed and/or client performance. Modes towards the right consume lower bandwidth at the cost of reduced image quality. In network- or client-constrained situations, modes towards the right may achieve better frame rates.

The default video mode is always "Full Color 2", which is a high-quality mode and works well for most uses in LAN environments. If needed, experiment with modes further towards the right to find the right balance of image quality and frame rate.

► Color Subsampling

Color subsampling reduces the color information in the encoded video stream.

- **Automatic:** Recommended. The optimal color subsampling mode will be enabled based on the selections in the video encoding section.
- **4:4:4:** Highest quality at significant bandwidth cost. Usually not necessary except for some situations in graphical user interfaces. Not supported for resolutions above 1920x1200, so for those resolutions color subsampling will automatically drop down to 4:2:2.
- **4:2:2:** Good blend of image quality and bandwidth.
- **4:2:0:** Maximum savings of network bandwidth and client load. Works fine for most general-purpose applications that don't emphasize high-resolution lines or text.

► Current Status

Current status includes real-time video performance statistics. As you change settings in the dialog, you can immediately see the effects on performance.

- **Source:** resolution and frame rate of the incoming video source.
- **Performance:** frames per second (FPS) being rendered in the client, and the data rate of the incoming video stream. These values are where you will see the effects of your video settings.
- **Encryption:** whether the video stream is encrypted or not. Encrypted streams usually have lower frame rates and lower bandwidth. Encryption is a global setting in security → KVM Security → "Apply Encryption Mode to KVM and Virtual Media".

Connection Info

Open the Connection Information dialog for real-time connection information on your current connection, and copy the information from the dialog as needed.

See Default Connection Properties for help configuring the connection properties.

- Name of the device
- IP address of the device
- Port - The KVM communication TCP/IP port used to access the device
- Data In/Second - Data rate received from the device
- Data Out/Second - Data rate sent to the device
- FPS - Video frames per second from the device.
- Average FPS - Average number of video frames per second.
- Connect Time - The duration of the current connection.
- Horizontal Resolution - The target server horizontal resolution.
- Vertical Resolution - The target server vertical resolution.
- Refresh Rate - Refresh rate of the target server.
- Protocol Version - communications protocol version.

► **To view connection info:**

- Choose File > Connection Info.

Connection Info	
Device Name:	RemoteAccess-GATE
IP Address:	192.168.0.1
Port:	443
Data In:	37.2 Kbit/s
Data Out:	3.30 Kbit/s
FPS:	40
Avg. FPS:	35.23
Connect Time:	00:02:44
Horizontal Resolution:	1920
Vertical Resolution:	1080
Refresh Rate:	60 Hz
Protocol Version:	1.34
<div>OK</div>	

Input Menu

Keyboard Layout

► **To set your keyboard type.**

- Choose Input > Keyboard Layout, then select your keyboard type.
 - de-de
 - de-ch
 - en-gb
 - en-us
 - fr

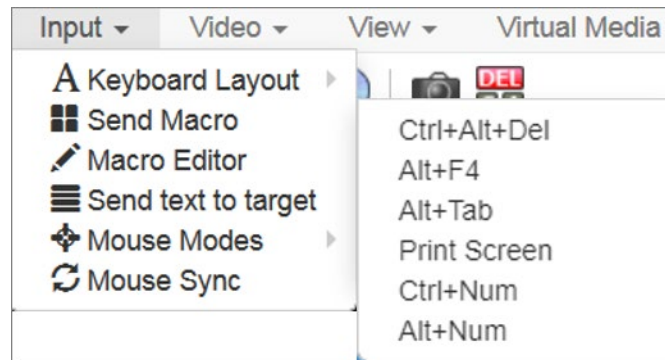
Send Macro

Due to frequent use, several keyboard macros are preprogrammed.

► **To send a preprogrammed macro:**

- Choose Input > Send Macro, then select the macro:
 - Ctrl+Alt+Del: Sends the key sequence to the target without affecting the client.
 - Alt+F4: Closes a window on a target server.
 - Alt+Tab: Switch between open windows on a target server.

- Print Screen: Take a screenshot of the target server.
- Ctrl+Num: Commonly used G&D hotkey to open the OSD (e.g. for matrix switches).
- Alt+Num: Commonly used G&D hotkey to open the OSD (various G&D devices).



Macro Editor

Keyboard macros ensure that keystroke combinations intended for the target server are sent to and interpreted only by the target server. Otherwise, they might be interpreted by your client PC.

Macros are stored on the client PC and are PC-specific. If you use another PC, you cannot see your macros.

In addition, if another person uses your PC and logs in under a different name, that user will see your macros since they are computer-wide.

Macros created with HKC are only available with the current browser and KVM device. If you use HKC in more than one browser, or more than one RemoteAccess-GATE, your macros will only be available on the browser and RemoteAccess-GATE where they were created. To reuse your macros in another RemoteAccess-GATE device, you can import and export the macro files. See *Import and Export Macros* (on page 62).

► **To access the Macro Editor:**

- Choose Inputs > Macro Editor.
- Select a macro from the Macros list to view the key combination.

Macro Editor

Name: Ctrl+Alt+Del

Macros	Keys
Ctrl+Alt+Del	press: CTRL LEFT
Alt+F4	press: ALT LEFT
Alt+Tab	press: DELETE
Print Screen	release: CTRL LEFT
Ctrl+Num	release: ALT LEFT
Alt+Num	release: DELETE

Buttons: Add Key, Add Delay, ↑, ↓, Delete

Buttons: Add New Macro, Delete Macro, Use in Toolbar

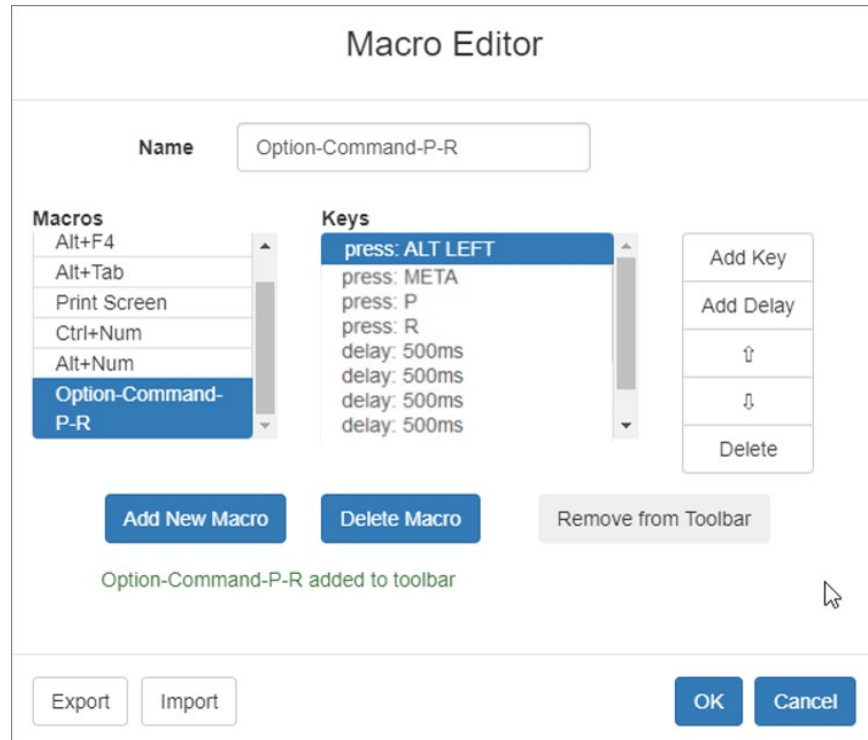
Buttons: Export, Import, OK, Cancel

Add New Macro**► To add a new macro:**

1. Choose Inputs > Macro Editor.
2. Click Add New Macro.

3. Enter a Name for the new macro. The name will appear in the Send Macro menu once the macro is saved.
4. Click Add Key, then press the key you want to add to the macro. The key press and key release appear in the Keys list.
 - To add more keys, click Add Key again, and press another key.
 - To remove a key, select it in the Keys list and click Delete Key
5. To put the keys in the correct sequence, click to select a key in the Keys list, then click the up and down arrows.
6. To add a 500 ms delay to a key sequence, click Add Delay. A delay in the middle of a press-and-release key sequence indicates holding down a key. Add multiple delays to indicate a longer press-and-hold of a key. Click the up and down arrows to move the delays into the correct sequence.

- Click OK to save. To use this macro from your toolbar, click Use in Toolbar. See **Add a Macro to the Toolbar** (on page 60) for more details.



This example shows a macro for a Mac startup sequence that requires a 2-second delay.

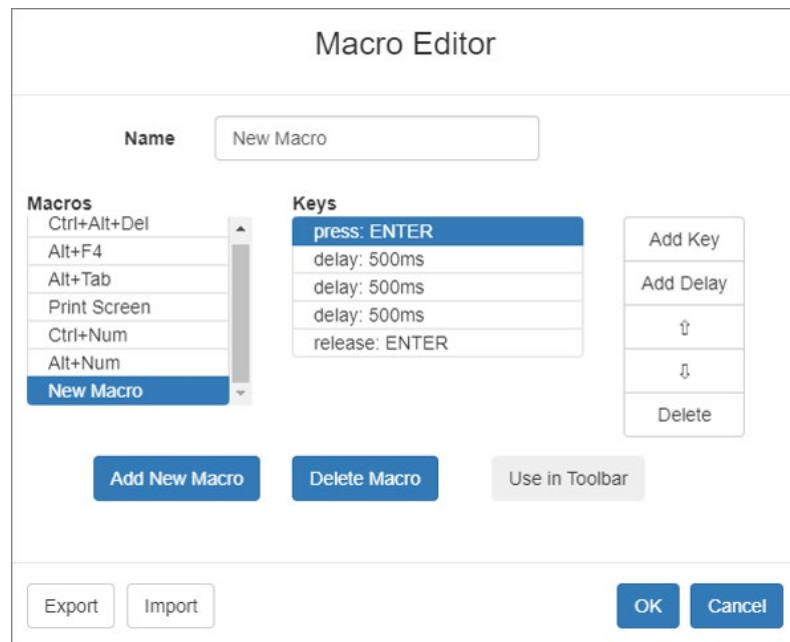
Add a Macro to the Toolbar

You can add a single macro to your HKC toolbar, so that you can use the macro by clicking an icon.

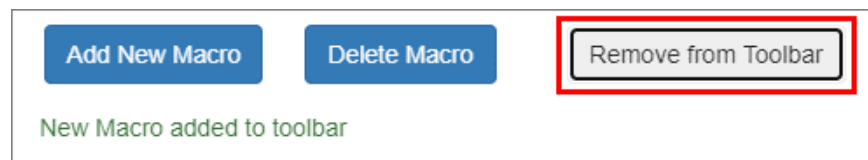
► To add a macro to the toolbar:

- Choose Inputs > Macro Editor.
- Select a macro from the Macros list.

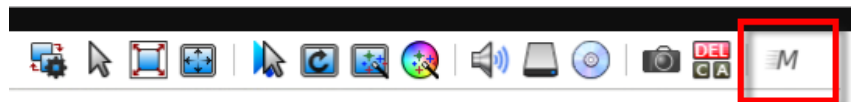
3. Click Use in Toolbar.



4. A message appears to confirm the macro is added to the toolbar.
 - To remove the macro from the toolbar, click Remove from Toolbar, or select a different macro and click Use in Toolbar.



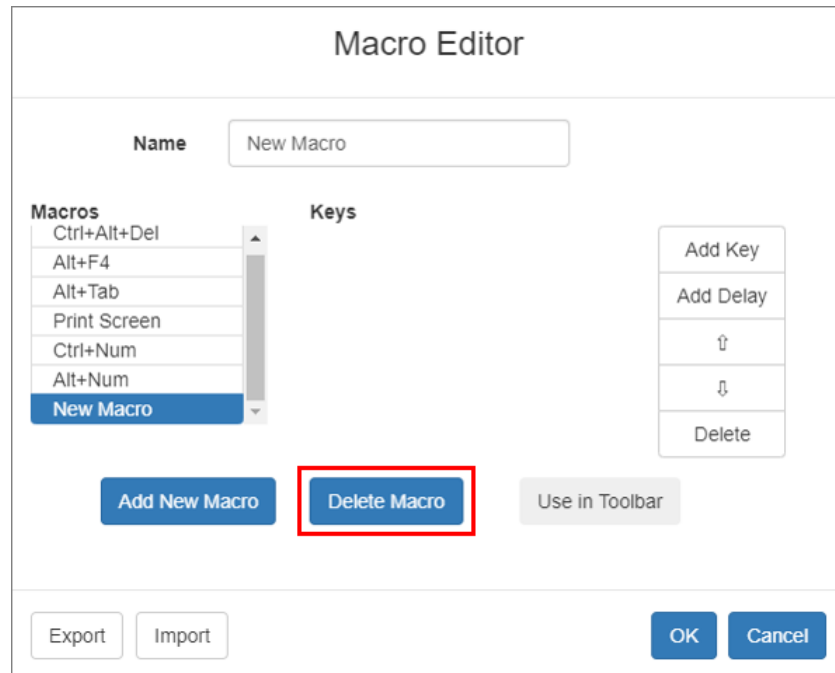
5. Click OK and exit the Macro Editor. The macro icon is added to the toolbar when one has been set.



Delete a Macro

► To delete a macro:

1. Choose Inputs > Macro Editor.
2. Select the macro, then click Delete Macro.
3. Click OK.



Import and Export Macros

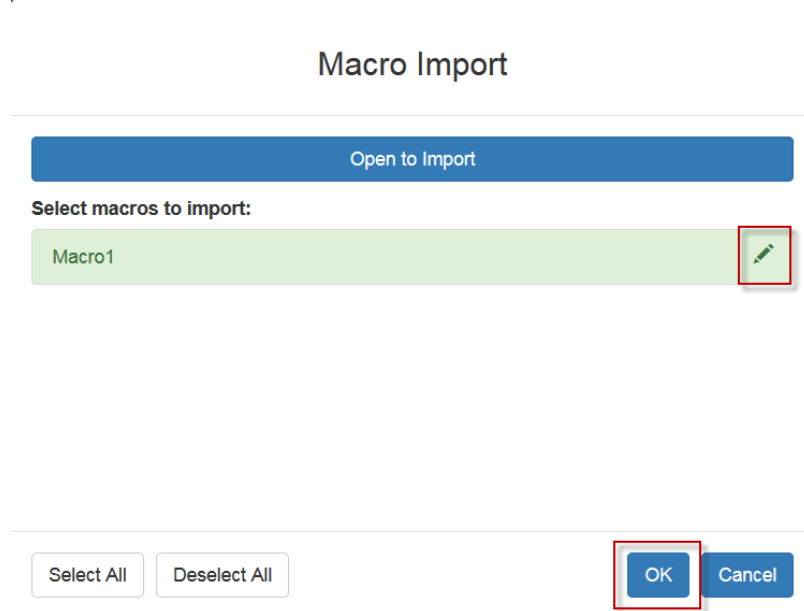
Macros created with HKC are only available with the current browser and KVM device. If you use HKC in more than one browser, or more than one RemoteAccess-GATE, your macros will only be available on the browser and RemoteAccess-GATE where they were created. To reuse your macros in another RemoteAccess-GATE device, you can import and export the macro files. Imported and exported macro files created on HKC are only compatible with HKC, and cannot be used on AKC or VKC. Likewise, macro files created on AKC or VKC cannot be imported for use on HKC.

Macros are exported to an xml file named "usermacros.xml". Files are saved in your browser's default download location. Default macros are not exported.

► To export and import macros:

1. Choose Input > Macro Editor. The list of macros created for your browser and RemoteAccess-GATE displays in the Macro Editor dialog.
2. To export the list, click the Export button, then save the file.
3. Log in to the RemoteAccess-GATE where you want to import the macros.
4. Choose Input > Macro Editor.

5. Click Import, then click Open to Import and select the usermacros.xml file, and click OK.
6. The macros found in the file display in the list. Select the macros you want to import, then click OK.
 - Macro names must be unique. If a macro with the same name already exists, an error message appears. Click the Edit icon to rename the macro, then click the checkmark to save the name.



Send Text to Target

Use the Send Text to Target function to send text directly to the target. If a text editor or command prompt is open and selected on the target, the text is pasted there.

► To send text to target:

1. Choose Input > Send Text to Target. The Send Text to Target dialog appears.
2. Enter the text you want sent to the target. Supported keyboard characters only.
3. Click OK.

Mouse Modes

You can operate in either single mouse mode or dual mouse mode.

When in a dual mouse mode, and provided the option is properly configured, the mouse cursors align.

When controlling a target server, the Remote Console displays two mouse cursors - one belonging to your RemoteAccess-GATE client workstation, and the other belonging to the target server.

When there are two mouse cursors, the device offers several mouse modes:

- Absolute (Mouse Synchronization)
- Intelligent (Mouse Mode)
- Standard (Mouse Mode)

When the mouse pointer lies within the KVM Client target server window, mouse movements and clicks are directly transmitted to the connected target server.

While in motion, the client mouse pointer slightly leads the target mouse pointer due to mouse acceleration settings.

Single mouse mode allows you to view only the target server's pointer. You can use Single mouse mode when other modes don't work.

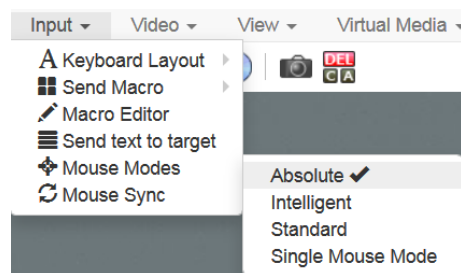
You can toggle between these two modes (single mouse and dual mouse).

Absolute

- In this mode, absolute coordinates are used to keep the client and target cursors in synch, even when the target mouse is set to a different acceleration or speed.

► To enter Absolute Mouse Synchronization Mode:

- Choose Input > Mouse Modes > Absolute.

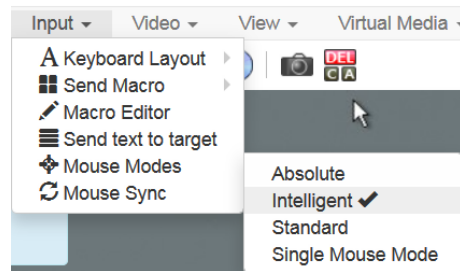


Intelligent

In Intelligent Mouse mode, the device can detect the target mouse settings and synchronize the mouse cursors accordingly, allowing mouse acceleration on the target.

► **To enter Intelligent mouse mode:**

- Choose Input > Mouse Mode > Intelligent. The mouse will synch. See ***Intelligent Mouse Synchronization Conditions*** (on page 27).

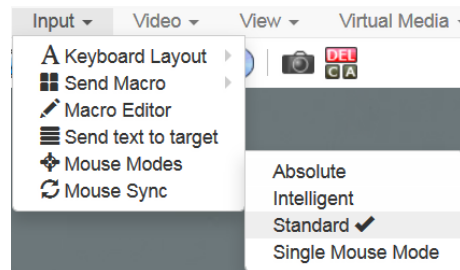
***Standard***

Standard Mouse mode uses a standard mouse synchronization algorithm. The algorithm determines relative mouse positions on the client and target server.

In order for the client and target mouse cursors to stay in synch, mouse acceleration must be disabled. Additionally, specific mouse parameters must be set correctly.

► **To enter Standard mouse mode:**

- Choose Input > Mouse Modes > Standard.



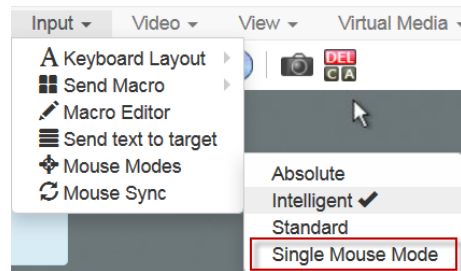
Single

Single Mouse mode uses only the target server mouse cursor; the client mouse cursor no longer appears onscreen.

Note: Single mouse mode does not work on Windows or Linux targets when the client is running on a Virtual Machine. Single mouse mode is not available on Internet Explorer.

► To enter Single mouse mode:

- Choose Inputs > Mouse Modes > Single.



- A message appears at the top of the client window: Press Esc to show your cursor.

► To exit Single mouse mode:

- Press Esc.
- Mouse mode changes back to dual mode.

Mouse Sync

In dual mouse mode, the Synchronize Mouse command forces realignment of the target server mouse cursor with the client mouse cursor.

Note: This option is available only in Standard and Intelligent mouse modes.

► To synchronize the mouse cursors:

- Choose Inputs > Mouse Sync.

Intelligent Mouse Synchronization Conditions

The Intelligent Mouse Synchronization command, available on the Mouse menu, automatically synchronizes mouse cursors during moments of inactivity. For this to work properly, however, the following conditions must be met:

- The active desktop should be disabled on the target.
- No windows should appear in the top left corner of the target page.
- There should not be an animated background in the top left corner of the target page.
- The target mouse cursor shape should be normal and not animated.
- The target mouse speeds should not be set to very slow or very high values.
- The target advanced mouse properties such as “Enhanced pointer precision” or “Snap mouse to default button in dialogs” should be disabled.
- The edges of the target video should be clearly visible (that is, a black border should be visible between the target desktop and the remote KVM console window when you scroll to an edge of the target video image).
- When using the intelligent mouse synchronization function, having a file icon or folder icon located in the upper left corner of your desktop may cause the function not to work properly. To be sure to avoid any problems with this function, do not have file icons or folder icons in the upper left corner of your desktop.

After autosensing the target video, manually initiate mouse synchronization by clicking the Synchronize Mouse button on the toolbar. This also applies when the resolution of the target changes if the mouse cursors start to desync from each other.

If intelligent mouse synchronization fails, this mode will revert to standard mouse synchronization behavior.

Please note that mouse configurations will vary on different target operating systems. Consult your OS guidelines for further details. Also note that intelligent mouse synchronization does not work with UNIX targets.

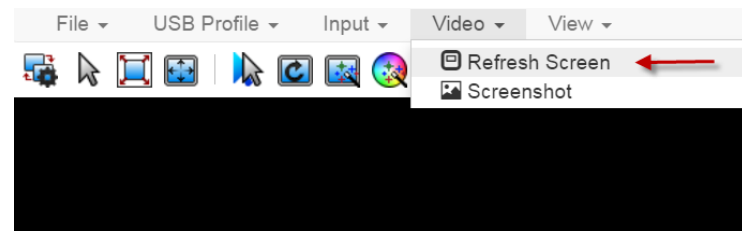
Video Menu

Refresh Screen

The Refresh Screen command forces a refresh of the video screen.

► To force a refresh of the video screen:

- Choose Video > Refresh Video.

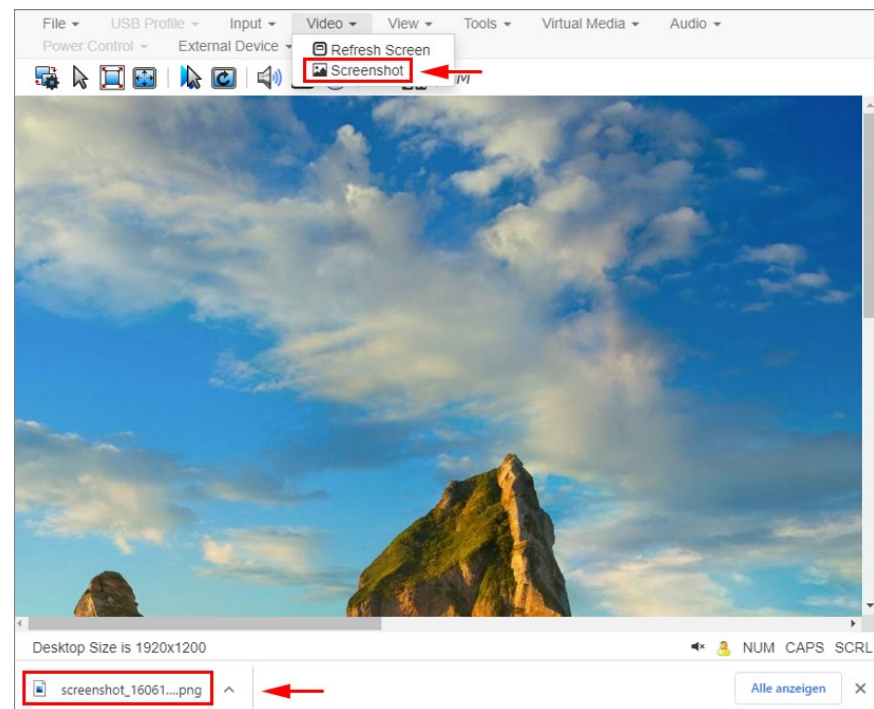


Screenshot

Take a screenshot of a target server using the Screenshot command.

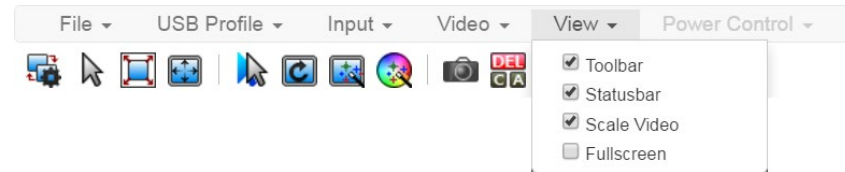
► To take a screenshot of the target server:

1. Choose Video > Screenshot.
2. The screenshot file appears as a download to view or save. Exact options depend on your client browser.



View Menu

The View Menu contains options to customize your HKC display.



► Toolbar and Statusbar:

The toolbar contains icons for some commands. The Statusbar displays screen resolution at the bottom of the client window.

► Scale Video:

Scale Video scales your video to view the entire contents of the target server window in your HKC window. The scaling maintains the aspect ratio so that you see the entire target server desktop without using the scroll bar.

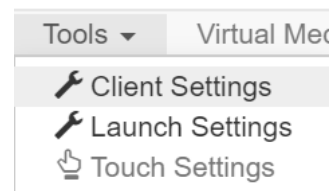
► Fullscreen:

Fullscreen sets the target window to the size of your full screen, removing your client from the view.

- Press Esc to exit fullscreen.

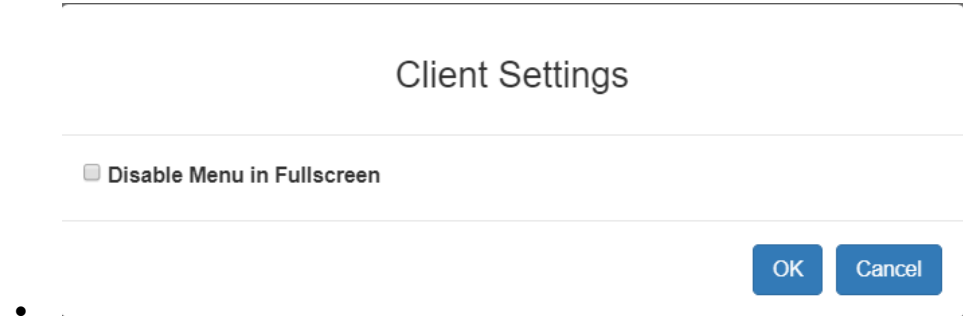
Tools Menu

The Tools menu contains options for HKC target connection settings.



► **Client Settings:**

- Choose Tools > Client Settings to access the Disable Menu in Fullscreen option.
- When selected, the menu bar will not be available in fullscreen mode. This setting is specific to the client, so it must be set for each client device and each browser used for access.



Client Settings

☐ **Disable Menu in Fullscreen**

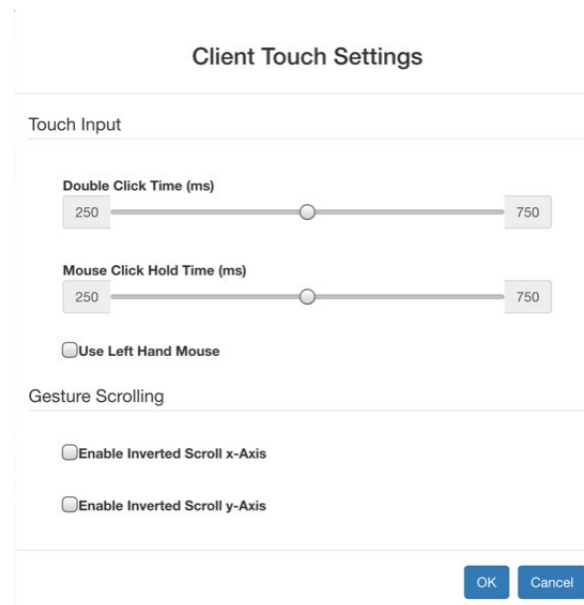
OK **Cancel**

► **Launch Settings:**

- Tap Tools > Launch Settings to access the Enable Scale Video option. When enabled, target video scales to the current KVM window size.

► **Touch Settings - enabled for iOS clients:**

- Tap Tools > Touch Settings to access the Client Touch Settings. Customize the Touch Input and Gesture Scrolling settings for your mobile device.



Client Touch Settings

Touch Input

Double Click Time (ms)
250 750

Mouse Click Hold Time (ms)
250 750

☐ **Use Left Hand Mouse**

Gesture Scrolling

☐ **Enable Inverted Scroll x-Axis**

☐ **Enable Inverted Scroll y-Axis**

OK **Cancel**

- Double Click Time: Time between two touch taps for the equivalent of a mouse double click.

- Mouse Click Hold Time: Time to hold after touch down for the equivalent of a mouse right click.
- Use Left Hand Mouse: Enable if the target OS's primary mouse button is set to Right.
- Enable Inverted Scroll x-Axis: If selected, two-finger movement to the right moves the screen to the left instead of the default right.
- Enable Inverted Scroll y-Axis: If selected, two-finger movement up moves the screen down instead of the default up.

Virtual Media Menu

Due to browser limitations, HKC supports a different set of virtual media functions than the other KVM Clients.

Due to browser resources, virtual media file transfer is slower on HKC than the other KVM clients.

Connect Files and Folders

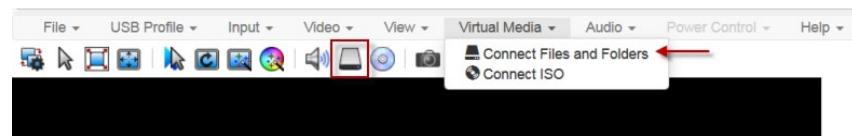
The Connect Files and Folders command provides an area to drag and drop files or folders that you want to connect to on virtual media.

Supported browsers: Chrome, Firefox, Safari

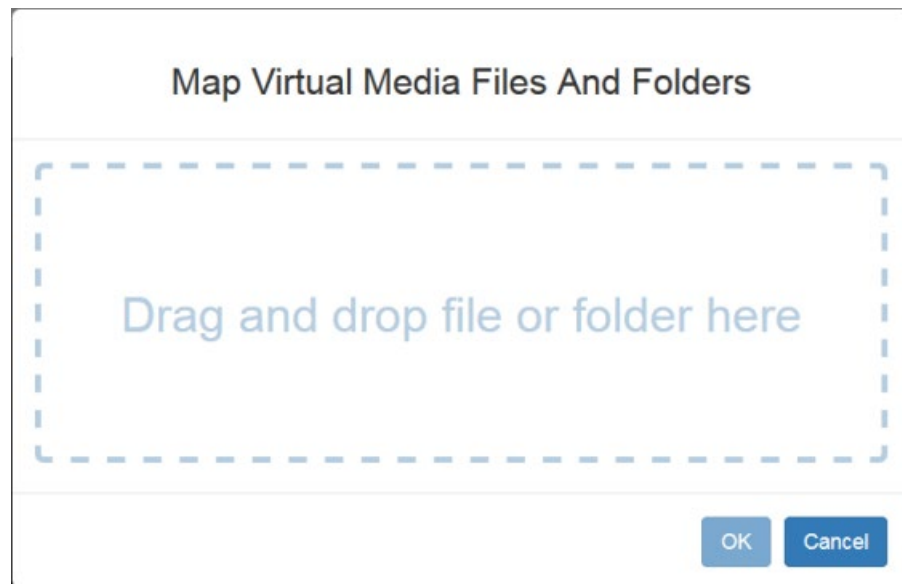
File size limit: 4GB per file

► To connect files and folders:

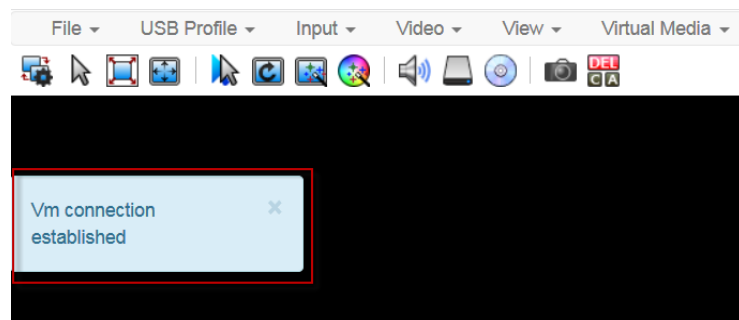
1. Choose Virtual Media > Connect Files and Folders. Or, click the matching icon in toolbar.



2. Drag files or folders onto the Map Virtual Media Files and Folders dialog. Click OK.

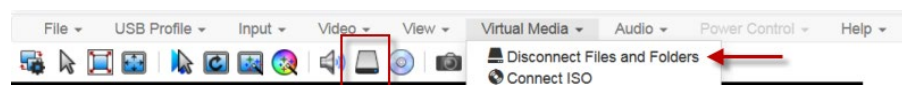


3. A message appears to show virtual media is connected. After a short time, a VM drive containing the selected files or folders will be mapped to the target server.



► **To disconnect files and folders:**

- Choose Virtual Media > Disconnect Files and Folders. Or, click the matching icon in the toolbar.



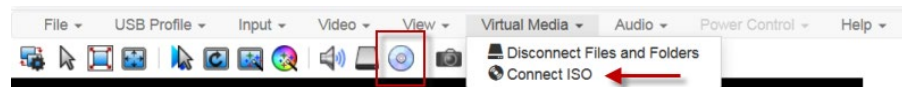
Connect ISO

The Connect ISO command maps a virtual media image file to the target. You can connect to ISO, DMG or IMG files from your client PC or to ISO files from a remote server.

Note: If connection to your SAMBA server is lost while transferring files from your image file to the target, keyboard and mouse control will be lost for several minutes, but will recover.

► To map virtual media image files:

1. Choose Virtual Media > Connect ISO. Or, click the matching icon in the toolbar.



2. Select the option for your file's location:

Map Virtual Media ISO Image

☒ **ISO Image**

Datei auswählen

Keine ausgewählt

☐ **Remote Server ISO Image**

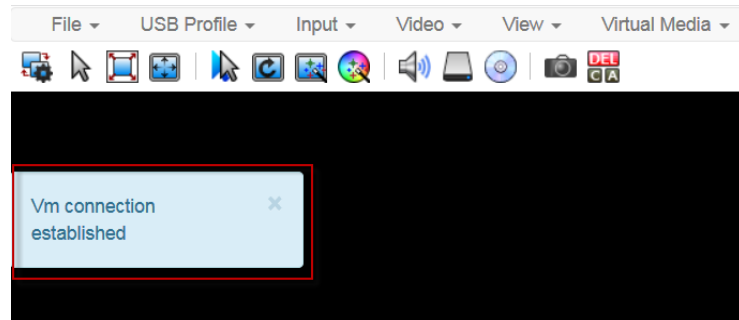
- Select ISO Image if the image file is directly accessible on your client. Click Browse, select the ISO, DMG or IMG file, and click OK. The filename appears next to the Browse button.

☒ **ISO Image**

Datei auswählen

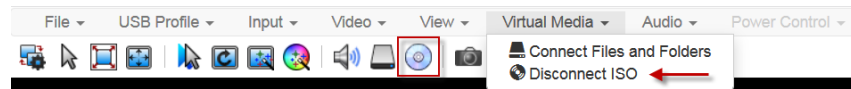
G&D.iso

- Select Remote Server ISO Image for ISO files on a remote server. Remote ISO files must be pre-configured by an administrator for the mapping to appear here. See Virtual Media File Server Setup (File Server ISO Images Only). Select the Hostname, then select the image file from the Image list. Enter the file server's username and password.
3. Click OK to map the selected file to the target. A message appears to show virtual media is connected.



► **To disconnect ISO:**

- Choose Virtual Media > Disconnect ISO. Or, click the matching icon in the toolbar.



Audio Menu

The Audio menu contains audio connection and settings.

Audio quality deteriorates if multiple target connections are open. To preserve quality, limit to four target connections open on HKC when an audio session is running.

Note: IE does not support audio. The menu will appear grayed out.

Connect Audio

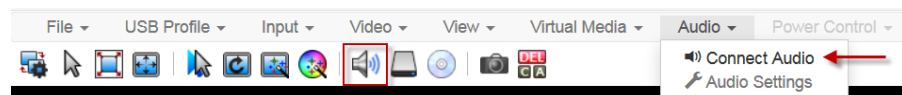
The Connect Audio command connects your playback device, selects audio format and gives an option to mount the selected playback device automatically when you connect to the target.

HKC connects the client PC's default audio playback device. To use a different device, it must be set as default in the client OS.

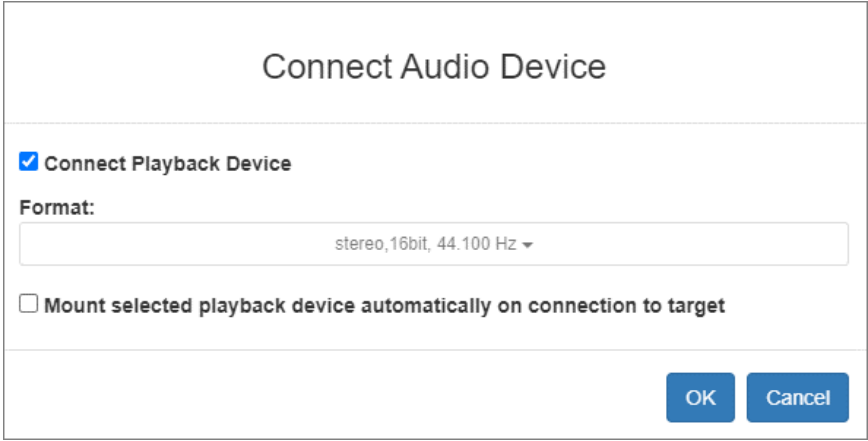
Note: For best quality, limit the number of audio sessions to a maximum of four KVM sessions.

► **To connect audio:**

1. Choose Audio > Connect Audio, or click the matching icon in the toolbar.



2. In the Connect Audio Device dialog, select the Connect Playback Device checkbox.



Connect Audio Device

☒ **Connect Playback Device**

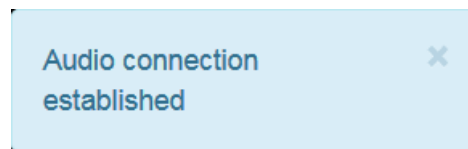
Format:

stereo, 16bit, 44.100 Hz ▼

☐ **Mount selected playback device automatically on connection to target**

OK
Cancel

3. Select the "Mount selected playback device automatically on connection to target" checkbox to enable the option. This setting will connect audio automatically the next time you connect to targets.
4. Click OK. A success message appears.



► **To disconnect audio:**

1. Choose Audio > Disconnect Audio, or click the matching icon in the toolbar.

Audio Settings

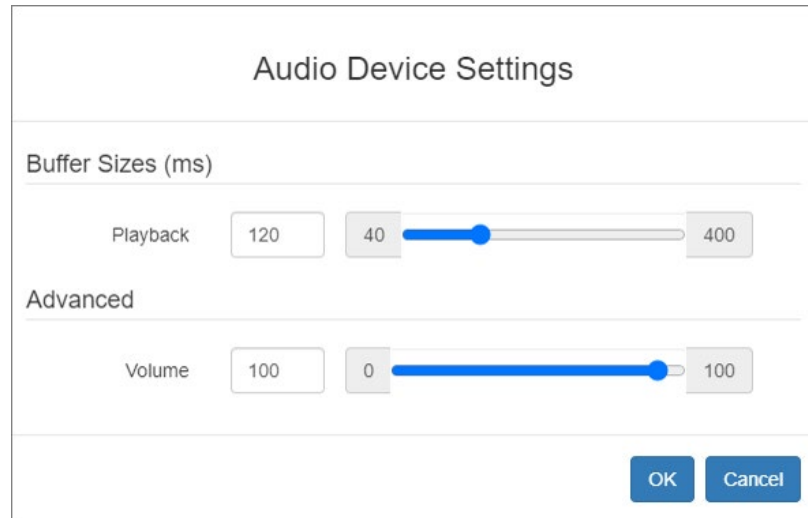
The Audio Settings option is enabled when audio is connected. Use the Audio Settings to set the buffer and volume.

Increasing the buffer size improves the audio quality but may impact the delivery speed.

The maximum available buffer size is 400 milliseconds since anything higher than that greatly impacts audio quality.

► **To configure audio settings:**

1. Choose Audio > Audio Settings while Audio is connected.
2. Set the Buffer and Volume using the arrows or sliders.



3. Click OK.

Auto Play in Safari

For HKC connections in the Safari browser that have auto mounted audio devices, make sure that the "Auto Play" setting is "Allow all Auto Play".

<https://support.apple.com/guide/safari/customize-settings-per-website-ibrw7f78f7fe/mac>

External Device Menu

The External Device menu allows you to control the device connected at the terminal block of the RemoteAccess-GATE.

► External Device Settings:

1. Choose External Device > Settings to view the dialog.
2. The device state is listed.
3. Enabled devices can be controlled using the Actions options.
 - Turn External Device On/Off: Click On or Off to control terminal output relay.

- **Blink External Device:** Enter the half-second interval to control blinking of the external device.

External Device Settings

External Device State: Disabled

Action

☒ Turn External Device On/Off

On

Off

☐ Blink External Device

☐ Pulse External Device

1

Pulse/Blink Interval (Half-Seconds)

OK

Cancel

Apply

4. Click OK or Apply to complete the action.

Tips for Accessing RemoteAccess-GATE With Dual Monitor Setups

When remotely accessing a RemoteAccess-GATE in a dual monitor setup, make sure the monitor out to RemoteAccess-GATE is set as the Primary Display. Align the two monitors horizontally with the monitor out to RemoteAccess-GATE in the left position. To ensure good mouse alignment in this scenario, use Intelligent Mouse Mode.

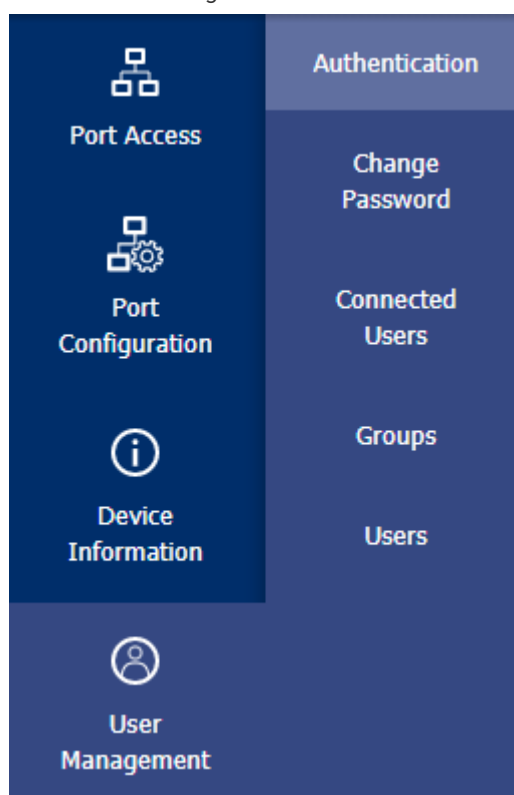
Note: For Windows 10 targets, you must disable all acceleration when using Intelligent Mouse Mode.

Chapter 4 User Management

RemoteAccess-GATE can be configured for local or remote authentication. To prepare for configuring external authentication, see ***Gathering LDAP/Radius Information*** (on page 79).

RemoteAccess-GATE is shipped with one built-in administrator account: **Admin**, which is ideal for initial login and system administration. You cannot delete 'Admin' or change its permissions, but you can change the username and password. For other security settings related to user management, see ***Security*** (on page 118).

Click User Management to view the submenu options.



In This Chapter

Gathering LDAP/Radius Information	79
Configuring Authentication.....	79
Disabling External Authentication	86
Change Your Password.....	86
Connected Users.....	86
Users and Groups	87

Gathering LDAP/Radius Information

You must have the following information about your AA server settings to configure external authentication. If you are not familiar with these settings, consult your AA server administrator for help.

► LDAP authentication:

- The IP address or hostname of the LDAP server
- The type of the LDAP server, usually one of the following options:
 - *OpenLDAP*
 - If using an OpenLDAP server, consult the LDAP administrator for the Bind Distinguished Name (DN) and password.
 - *Microsoft Active Directory® (AD)*
 - If using a Microsoft Active Directory server, consult your AD administrator for the name of the Active Directory Domain.
- The required type of LDAP Security (None, TLS, SmartTLS).
 - If Secure LDAP is in use, consult your LDAP administrator for the CA certificate file.
- The network port used by the LDAP server
- Bind Distinguished Name (DN) and password (if anonymous bind is NOT used)
- The Base DN of the server (used for searching for users)
- The login name attribute (or AuthorizationString)
- The user entry object class
- The user search subfilter (or BaseSearch)

► Radius authentication:

- The IP address or host name of the Radius server
- The type of Radius Authentication used by the Radius server (PAP or CHAP)
- Shared secret for a secure communication
- UDP authentication port and accounting port used by the Radius server

Configuring Authentication

Important: The device uses TLS instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

The RemoteAccess-GATE supports:

- Local user database on the RemoteAccess-GATE
- LDAP
- Radius

By default, the RemoteAccess-GATE is configured for local authentication. If you use this method, you only need to create user accounts. See [Creating Users](#).

If you prefer external authentication, you must provide the RemoteAccess-GATE with information about the external Authentication and Authorization (AA) server.

If you would like local authentication to be available as a backup method when external authentication is not available, create user accounts on the RemoteAccess-GATE in addition to providing the external AA server data. Note that local and external authentication cannot be used simultaneously. When configured for external authentication, all RemoteAccess-GATE users must have an account on the external AA server. Local-authentication-only users will have no access when external authentication is enabled, except for the admin, who can always access the RemoteAccess-GATE.

► **To select authentication type:**

1. Click User Management > Authentication.
2. Select Authentication Type:
 - Local
 - LDAP
 - Radius
3. Select the "Use Local authentication when Remote Authentication is not available" checkbox to allow local authentication as a backup method when external authentication is not available, such as when the server is down.
4. Click Save. The authentication type is enabled.

For help with adding your external servers, see ***LDAP Authentication*** (on page 81) and ***Radius Authentication*** (on page 85). For help with adding users, see ***Users and Groups*** (on page 87).


LDAP Authentication

Gather the information you need to add your LDAP servers to RemoteAccess-GATE. For help, see ***Gathering LDAP/Radius Information*** (on page 79).

► **To add LDAP servers:**

1. Click User Management > Authentication.
2. In the LDAP section, click New. Enter your LDAP details.

Field/setting	Description
IP Address / Hostname	<p>The IP address or hostname of your LDAP/LDAPS server.</p> <ul style="list-style-type: none"> Without encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if encryption is enabled.
Copy settings from existing LDAP server	<p>This checkbox appears only when there are existing AA server settings on the RemoteAccess-GATE. To duplicate any existing AA server's settings, refer to the duplicating procedure below.</p>
Type of LDAP Server	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> OpenLDAP Microsoft Active Directory. .

Field/setting	Description
Security	<p>Determine whether you would like to use TLS encryption, which allows the RemoteAccess-GATE to communicate securely with the LDAPS server.</p> <p>Three options are available:</p> <ul style="list-style-type: none"> ▪ StartTLS ▪ TLS ▪ None
Port (None/StartTLS)	<ul style="list-style-type: none"> ▪ The default Port is 389, or specify another port.
Port (TLS)	<p>Configurable only when "TLS" is selected in the Security field.</p> <p>The default port is 636, or specify another port.</p>
Enable verification of LDAP Server Certificate	<p>Select this checkbox if it is required to validate the LDAP server's certificate by the RemoteAccess-GATE prior to the connection.</p> <p>If the certificate validation fails, the connection is refused.</p>
CA Certificate	<p>Consult your AA server administrator to get the CA certificate file for the LDAPS server.</p> <p>Click  to select and install the certificate file.</p> <ul style="list-style-type: none"> ▪ Click Show to view the installed certificate's content. ▪ Click Remove to delete the installed certificate if it is inappropriate. <hr/> <p><i>Note: If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see TLS Certificate Chain.</i></p>
Allow expired and not yet valid certificates	<ul style="list-style-type: none"> ▪ Select this checkbox to make the authentication succeed regardless of the certificate's validity period. ▪ After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.

Field/setting	Description
Anonymous Bind	Use this checkbox to enable or disable anonymous bind. <ul style="list-style-type: none"> To use anonymous bind, select this checkbox. When a Bind DN and password are required to bind to the external LDAP/LDAPS server, deselect this checkbox.
Bind DN	Required after deselecting the Anonymous Bind checkbox. Distinguished Name (DN) of the user who is permitted to search the LDAP directory in the defined search base.
Bind Password, Confirm Bind Password	Required after deselecting the Anonymous Bind checkbox. Enter the Bind password.
Base DN for Search	Distinguished Name (DN) of the search base, which is the starting point of the LDAP search. <ul style="list-style-type: none"> Example: ou=dev,dc=example,dc=com
Login Name Attribute	The attribute of the LDAP user class which denotes the login name. <ul style="list-style-type: none"> Usually it is the uid.
User Entry Object Class	The object class for user entries. <ul style="list-style-type: none"> Usually it is inetOrgPerson.
User Search Subfilter	Search criteria for finding LDAP user objects within the directory tree.
Active Directory Domain	The name of the Active Directory Domain. <ul style="list-style-type: none"> Example: testradius.com

- Click Test Connection to check if RemoteAccess-GATE can connect with the server.
- Click Add Server. The new LDAP server is listed on the Authentication page. To add more servers, repeat the same steps. If you have multiple servers, use the arrow buttons to set their order, then click Save Order.

5. To start using these settings, make sure LDAP is selected and saved in the Authentication Type field. See *Configuring Authentication* (on page 79).

Returning User Group Information from Active Directory Server

The RemoteAccess-GATE supports user authentication to Active Directory® (AD) without requiring that users be defined locally on the RemoteAccess-GATE. This allows Active Directory user accounts and passwords to be maintained exclusively on the AD server. Authorization and AD user privileges are controlled and administered through the standard RemoteAccess-GATE policies and user group privileges that are applied locally to AD user groups.

IMPORTANT: If you are an existing user, and have already configured the Active Directory server by changing the AD schema, the RemoteAccess-GATE still supports this configuration and you do not need to perform the following operations. See *Updating the LDAP Schema* for information about updating the AD LDAP/LDAPS schema.

► **To enable your AD server on the RemoteAccess-GATE:**

1. Using the RemoteAccess-GATE, create special groups and assign proper permissions and privileges to these groups. For example, create groups such as KVM_Admin and KVM_Operator.
2. On your Active Directory server, create new groups with the same group names as in the previous step.
3. On your AD server, assign the RemoteAccess-GATE users to the groups created in step 2.
4. From the RemoteAccess-GATE, enable and configure your AD server properly. See *Implementing LDAP/LDAPS Remote Authentication*.

Important Notes

- Group Name is case sensitive.
- The RemoteAccess-GATE provides the following default groups that cannot be changed or deleted: Admin and <Unknown>. Verify that your Active Directory server does not use the same group names.
- If the group information returned from the Active Directory server does not match the RemoteAccess-GATE group configuration, the RemoteAccess-GATE automatically assigns the group of <Unknown> to users who authenticate successfully.
- If you use a dialback number, you must enter the following case-sensitive string: *msRADIUSCallbackNumber*.
- Based on recommendations from Microsoft, Global Groups with user accounts should be used, not Domain Local Groups.

Radius Authentication

Gather the information you need to add your Radius servers to RemoteAccess-GATE. For help, see *Gathering LDAP/Radius Information* (on page 79).

► To add Radius servers:

1. Click User Management > Authentication.
2. In the Radius section, click New. Enter your Radius details.

Field/setting	Description
IP Address / Hostname	The IP address or hostname of your Radius server.
Type of RADIUS Authentication	Select an authentication protocol. <ul style="list-style-type: none"> ▪ PAP (Password Authentication Protocol) ▪ CHAP (Challenge Handshake Authentication Protocol) CHAP is generally considered more secure because the user name and password are encrypted, while in PAP they are transmitted in the clear.
Authentication Port, Accounting Port	The defaults are standard ports -- 1812 and 1813. To use non-standard ports, type a new port number.
Timeout	This sets the maximum amount of time to establish contact with the Radius server before timing out. Type the timeout period in seconds.
Retries	Type the number of retries.
Shared Secret, Confirm Shared Secret	The shared secret is necessary to protect communication with the Radius server.

3. Click Test Connection to check if RemoteAccess-GATE can connect with the server.
4. Click Add Server. The new Radius server is listed on the Authentication page. To add more servers, repeat the same steps. If you have multiple servers, use the arrow buttons to set their order, then click Save Order.
5. To start using these settings, make sure Radius is selected and saved in the Authentication Type field. See *Configuring Authentication* (on page 79).

Returning User Group Information via RADIUS

When a RADIUS authentication attempt succeeds, the RemoteAccess-GATE determines the permissions for a given user based on the permissions of the user's group.

Your remote RADIUS server can provide these user group names by returning an attribute, implemented as a RADIUS FILTER-ID. The FILTER-ID should be formatted as follows: Raritan:G{*GROUP_NAME*} where *GROUP_NAME* is a string denoting the name of the group to which the user belongs.

Disabling External Authentication

► **To disable external authentication:**

1. Click User Management > Authentication.
2. In the Authentication Type, select Local.
3. Click Save.

Change Your Password

► **To change your password:**

1. Click User Management > Change Password.
2. Enter your old password, then enter your new password twice. Click Save.

Connected Users

You can check which users have logged in to the RemoteAccess-GATE and their status. If you have administrator privileges, you can terminate any user's connection to the RemoteAccess-GATE.

► **To view and manage connected users:**

1. Click User Management > Connected Users. A list of logged-in users displays.

Column	Description
User name	The login name of each connected user.
IP Address	The IP address of each user's host. For the login via a local connection (USB), <local> is displayed instead of an IP address.

Column	Description
Client Type	Web GUI: Refers to the web interface. CLI: Serial (local, such as USB connection) or SSH RDM: User Station
Idle Time	The length of time for which a user remains idle.

- a. To disconnect any user, click Disconnect.
- b. Click Disconnect on the confirmation message. The user is forced to log out.

Users and Groups

All users must have a user account, containing the login name and password. Multiple users can log in simultaneously using the same login name. The Admin user is created by default, and cannot be deleted, but you can change the username.

Privileges are assigned at the Group level, so you must also add groups, and assign your users to Groups. An admin group is created by default and has exclusive privileges. See *Admin Group Special Privileges* (on page 93).

When a user is assigned to multiple groups with different privilege levels, the highest-level of access specified is allowed to the user.

User group privilege changes take effect for the users in the group at the next login.

► To add groups:

1. Click User Management > Groups, then click the add group icon



Groups		🔍	👤	+
Group Name ▲	Description			
Admin	System defined administrator group including all privileges.			

2. Complete the New Group information:

Field/setting	Description
Group Name	<ul style="list-style-type: none"> ▪ 1 to 32 characters ▪ Case sensitive ▪ Spaces are permitted.

Field/setting	Description
Description	<ul style="list-style-type: none">Enter a description of the group's role.Up to 64 characters.

New Group

Settings

Group Name

Maintenance

Description

Maintenance privileges

3. Select the Privileges assigned to this group. All tasks noted here as exclusions are available exclusively to the admin group. See **Admin Group Special Privileges** (on page 93).
- Device Settings: All functions in the Device Settings menu except Enable and Configure SNMPv3

▪ Maintenance: All functions in the Maintenance menu except Backup/Restore and Reset to Factory Defaults

▪ PC Share: Simultaneous access to the same target by multiple users

▪ Security: All functions in the Security menu

▪ Terminal Block: All settings in Device Settings > Terminal Block, and access to the externally connected device using the KVM client

▪ User Management: All functions in the User Management menu except Disconnect Users

Privileges

☐ Device Access While Under CC-SG Management

☐ Device Settings


☒ Maintenance

☐ PC Share

☐ Security

☐ Terminal Block

☐ User Management

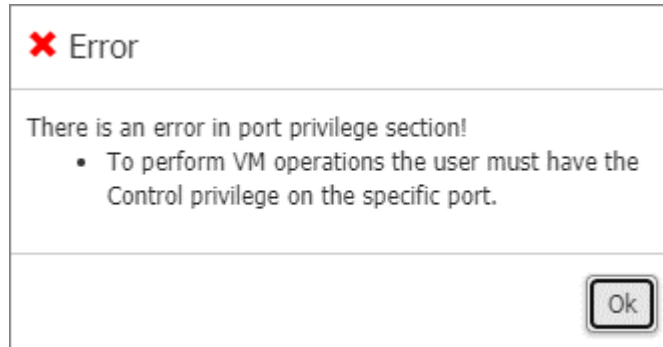


4. Select the Access and VM privileges for the KVM Port.

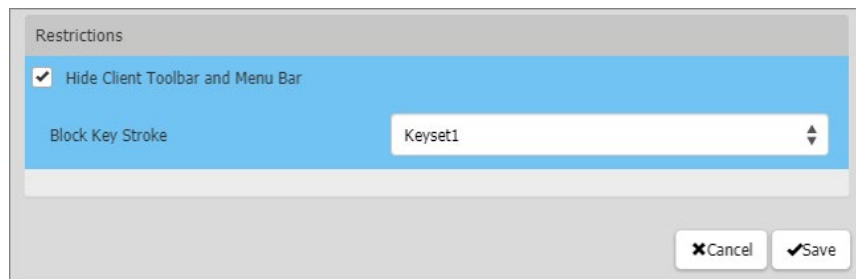
KVM Port	Access	VM Access
Port 1	<div>View</div>	<div>Deny</div>

- Access: Deny, View, Control
- VM Access: Deny, Read-only, Read-write

Some privileges require certain access permission. If you do not set the needed permissions, an error will display.



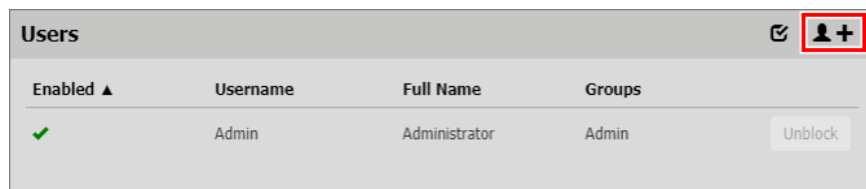
- The Restrictions section has options for restricting client views and blocking keys.
 - Select Hide Client Toolbar and Menu Bar to remove these components from view for this group. Scaling and hotkeys for Single Mouse and Full-Screen will be available.
 - In the Block Key Stroke field, select a keycode list to restrict the users in this group from using the keys in the list. See **Keycode List** (on page 105).



- Click Save. To assign these privileges and restrictions to users, select the group when you add or edit the user.

► **To add users:**

- Click User Management > Users, then click the add user icon



2. Complete the User information:

Field/setting	Description
Username	The name the user enters to log in to the RemoteAccess-GATE. <ul style="list-style-type: none"> 4 to 32 characters Case sensitive Spaces are NOT permitted.
Full Name	The user's first and last names. <ul style="list-style-type: none"> Up to 64 characters
Password, Confirm Password	<ul style="list-style-type: none"> 4 to 64 characters Case sensitive Spaces are permitted.
Telephone Number	The user's telephone number
eMail Address	The user's email address <ul style="list-style-type: none"> Up to 128 characters Case sensitive
Enable	When selected, the user can log in to the RemoteAccess-GATE.
Force password change on next login	When selected, a password change request automatically appears the next time the user logs in.

New User

User

Username

user

Full Name

User One

Password

Confirm password

Telephone Number

111-111-111

eMail Address

user@gdsys.de

Enable

☒

Force password change on next login:

☐

3. SSH: The SSH public key is required when public key authentication for SSH is enabled. See **SSH Settings** (on page 112).

4. Open the SSH public key with a text editor.
5. Copy and paste all content in the text editor into the SSH Public Key field.
6. **SNMPv3:** The SNMPv3 access permission is disabled by default. This section appears when the permission is enabled in the SNMP settings, or when a user is part of the admin group.

Field/setting	Description
Enable SNMPv3	Select this checkbox when intending to permit the SNMPv3 access by this user. Note: The SNMPv3 protocol must be enabled for SNMPv3 access. See Configuring SNMP Settings.
Security Level	Click the field to select a preferred security level from the list: <ul style="list-style-type: none"> ▪ None: No authentication and no privacy. This is the default. ▪ Authentication: Authentication and no privacy. ▪ Authentication & Privacy: Authentication and privacy.

- **Authentication Password:** This section is configurable only when 'Authentication' or 'Authentication & Privacy' is selected.

Field/setting	Description
Same as User Password	Select this checkbox if the authentication password is identical to the user's password. To specify a different authentication password, disable the checkbox.
Password, Confirm Password	Type the authentication password if the 'Same as User Password' checkbox is deselected. The password must consist of 8 to 32 ASCII printable characters.

- **Privacy Password:** This section is configurable only when 'Authentication & Privacy' is selected.

Field/setting	Description
Same as Authentication Password	Select this checkbox if the privacy password is identical to the authentication password.

Field/setting	Description
	To specify a different privacy password, disable the checkbox.
Password, Confirm Password	Type the privacy password if the 'Same as Authentication Password' checkbox is deselected. The password must consist of 8 to 32 ASCII printable characters.

- **Protocol:** This section is configurable only when 'Authentication' or 'Authentication & Privacy' is selected.

Field/setting	Description
Authentication	Click this field to select the desired authentication protocol. Two protocols are available: <ul style="list-style-type: none"> ▪ MD5 ▪ SHA-1 (default)
Privacy	Click this field to select the desired privacy protocol. Two protocols are available: <ul style="list-style-type: none"> ▪ DES (default) ▪ AES-128



The screenshot shows the 'SNMPv3' configuration window. It includes the following settings:

- Enable SNMPv3:** Checked.
- Security Level:** Set to 'Authentication & Privacy'.
- Authentication Password:**
 - Same as User Password:** Checked.
 - Password:** Empty text field.
 - Confirm Password:** Empty text field.
- Privacy Password:**
 - Same as Authentication Password:** Checked.
 - Password:** Empty text field.
 - Confirm Password:** Empty text field.
- Protocol:**
 - Authentication:** Set to 'SHA-1'.
 - Privacy:** Set to 'DES'.

1. Groups: Select the groups this user belongs to. Users have the privileges assigned to their groups.
2. Click Save.

► **To edit a user; change the admin username:**

1. Click User Management > Users, then click to select the user you want to edit.

Users				 
Enabled ▲	Username	Full Name	Groups	
✓	Admin	Administrator	Admin	<input type="button" value="Unblock"/>
✓	User1	User One	Admin	<input type="button" value="Unblock"/>

2. Change the user information as needed, then click Save.

Admin Group Special Privileges

The following special privileges are exclusively available to the admin group.

- Backup/Restore
- Disconnect Connected users
- Reset to Factory Defaults
- Diagnostics
- Enable SNMPv3 in the SNMP agent (SNMP gets and sets)
- Configure SNMPPv3 user parameters
 - Security Level
 - Authentication Protocol
 - Authentication Password
 - Privacy Password
 - Privacy Protocol

Chapter 5 Device Settings and Information

In This Chapter

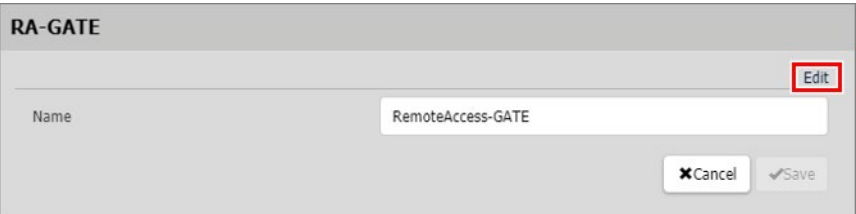
Device Information.....	94
Date and Time	96
Event Management	98
Keycode List	105
Network	106
Network Services.....	108
Serial Port	113
Terminal Block Control	114
Virtual Media Shared Images	117

Device Information

Click Device Information to view name, system, and network details about your RemoteAccess-GATE. In this page you can also rename your device, and view open source license information.

► **To edit your device name:**

- Click Device Information, then click Edit to enter a new name. Click Save.

A screenshot of a web interface titled "RA-GATE". It features a form with a label "Name" and a text input field containing "RemoteAccess-GATE". To the right of the input field is a red-bordered button labeled "Edit". At the bottom right of the form are two buttons: "Cancel" with a close icon and "Save" with a checkmark icon.

► **To view system details and status:**

- System Details: View the product name, model, firmware version, hardware ID, and serial number.
- System Status: View the internal temperatures status, and local monitor status.

System	
Detail	
Product	RemoteAccess-GATE
Model	RA-GATE
Firmware Version	4.1.0.1.47254
Hardware ID	3
Serial Number	2C90700240
Status	
Internal Temperature Current Value	38.6°C / 101.5°F
Internal Temperature Maximum Value	39.3°C / 102.8°F
Local Monitor	Not Detected

► **To view network details:**

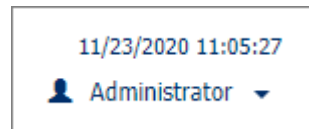
- View the network details as currently configured: IPv4 address, MAC address, Link state, DNS servers, DNS suffixes, DNS resolver preference, and IPv4/IPv6 routes.

Network	
Ethernet	
IPv4 address	192.168.0.1/24
MAC Address	00:0d:5d:1b:65:f3
Link State	1 GBit/s, full duplex, link OK, autonegotiation on
Common	
DNS Servers	none
DNS Suffixes	none
DNS Resolver Preference	IPv6 Address
IPv4 Routes	192.168.0.0/24 dev ETHERNET
IPv6 Routes	none

Date and Time

Set the internal clock on the RemoteAccess-GATE manually, or link to a Network Time Protocol (NTP) server.

The RemoteAccess-GATE system date and time appears in the upper right corner of the web interface.




► To set the date and time:

1. Click Device Settings > Date/Time.
2. Select your Time Zone.
3. If your area participates in daylight saving time, verify the Automatic Daylight Saving Time Adjustment checkbox is selected.
4. Select the Time Setup Method:
 - User Specified Time: Set the time manually.
 - Synchronize with NTP Server

User Specified Time


- Click the calendar icon to select the Date.
- Enter the time in Hours, Minutes and Seconds. Specify AM or PM. Click AM/PM to toggle the setting.
- Click Save.



The image shows a settings window titled "User Specified Time". It contains two main input sections. The first section is labeled "Date (YYYY-MM-DD)" and shows the date "2020-11-23" in a text field, with a small calendar icon to its right. The second section is labeled "Time (hh:mm:ss)" and features three spinners for hours, minutes, and seconds, with values "11", "06", and "28" respectively. To the right of these spinners is a button labeled "AM", which is highlighted with a red border. Above and below each spinner are small blue arrows for incrementing and decrementing the values. At the bottom right of the window is a "Save" button with a checkmark icon.

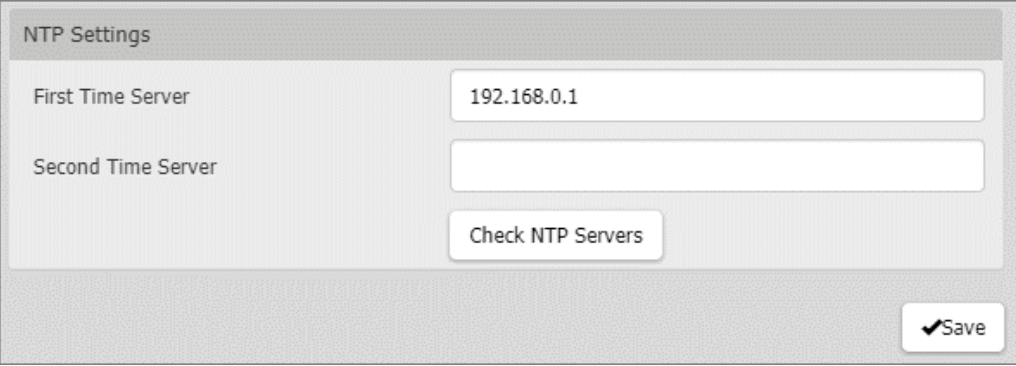
Synchronize with NTP server

- To use the DHCP-assigned NTP servers: **leave the First and Second time server fields blank**. DHCP-assigned NTP servers are available when either IPv4 or IPv6 DHCP is enabled. See **Network** (on page 106).



The screenshot shows the 'NTP Settings' form. It has a title bar 'NTP Settings'. Below it, there are two text input fields: 'First Time Server' and 'Second Time Server'. Both fields are empty. Below the fields is a button labeled 'Check NTP Servers'.

- To specify NTP servers manually, enter the primary NTP server in the First Time Server field. A secondary NTP server is optional. Click Check NTP Servers to verify. Click Save.



The screenshot shows the 'NTP Settings' form. It has a title bar 'NTP Settings'. Below it, there are two text input fields: 'First Time Server' and 'Second Time Server'. The 'First Time Server' field contains the text '192.168.0.1'. The 'Second Time Server' field is empty. Below the fields is a button labeled 'Check NTP Servers'. At the bottom right of the form is a button labeled 'Save' with a checkmark icon.

Event Management

All supported events are logged in the system log by default. You can also create additional actions for any event, including sending an email, sending an SNMP notification, and forwarding a syslog message.

► Configuring events and actions:

1. Click Device Settings > Event Management.

- The Event Management page shows events by Category. Click a category to view individual events. In this example, an action named "User events - email" has been added and assigned to all User Activity and User Administration events.

Event Management + New Action

Category	Event	User events - email	System Event Log Action
> All Events	***	<input type="checkbox"/>	<input checked="" type="checkbox"/>
> Device	***	<input type="checkbox"/>	<input checked="" type="checkbox"/>
> KVM Port	***	<input type="checkbox"/>	<input checked="" type="checkbox"/>
> Serial Port	***	<input type="checkbox"/>	<input checked="" type="checkbox"/>
▼ User Activity		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	User accepted the Restricted Service Agreement	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Authentication failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	User logon state	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Session timeout	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	User blocked	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
> User Administration	***	<input type="checkbox"/>	<input checked="" type="checkbox"/>

☒ Save

2. Select the event checkboxes to assign an action to an event. Click Save.

► **To add an action:**

1. Click New Action.

Event Management + New Action

2. Assign a name to this action.
3. Select the desired action and configure it.
 - Email Actions: See *Send Email* (on page 100)
 - SNMP Actions: See *SNMP Notifications* (on page 100)
 - Syslog Actions: See *Syslog Messages* (on page 103)
4. Click Create.

Send Email

Use this action to send an email according to your preconfigured SMTP settings, or create actions with one or more customized SMTP settings. See *Event Management* (on page 98) for help assigning this action to an event.

► To create the send email action:

The screenshot shows a 'New Action' dialog box with the following fields and options:

- Action Name:** Email Admins
- Action:** Send email (selected from a dropdown menu)
- Recipient Email Addresses:** info@gdsys.de
- SMTP Server:**
 - ☒ Use default settings
 - Server Name: not configured
 - Sender Email Address: not configured
 - Settings can be changed in SMTP Server settings.
 - ☐ Use custom settings

At the bottom right, there are 'Cancel' and 'Create' buttons.

1. Select Send Email from the Action list.
2. In the Recipient Email Addresses field, enter the email addresses of the recipients. Use a comma to separate multiple email addresses.
3. By default, the SMTP server settings will be used to complete this action. To view or change those settings, click the SMTP Server hyperlink.
 - To use a different SMTP server, click the "Use custom settings" radio button. The fields for customized SMTP settings appear. See *SMTP Server Settings* (on page 110).
4. Click Create.

SNMP Notifications

Use this action to send an SNMP notification to one or more SNMP servers.

See *Event Management* (on page 98) for help assigning this action to an event.

► To create the SNMP notification action:

1. Select Send SNMP Notification from the Action list.

2. Select the type of SNMP notification. Follow the procedure below based on your selection.

► **SNMP v2c notifications:**

New Action

Action Name

SNMP messages

Action

Send SNMP notification

Notification Type

SNMPv2c Trap

#	Host	Port	Community
1	192.168.0.1	162	users
2		162	
3		162	

✕ Cancel

✓ Create

1. In the Notification Type field, select SNMPv2c Trap.
2. In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent.
3. In the Port fields, enter the port number used to access the device(s).
4. In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the RemoteAccess-GATE and all SNMP management stations.
5. Click Create.

Tip: An SNMP v2c notification action permits a maximum of three SNMP destinations. If you need to assign more than 3 SNMP destinations to an event, you can create and assign multiple actions comprising all the destinations.

► **SNMP v3 notifications:**

Note: Duplicated SNMP Trap v3 secName (User ID) is not supported when multiple SNMP Trap destinations are configured.

New Action

Action Name

SNMP messages

Action

Send SNMP notification

Notification Type

SNMPv3 Trap

Engine ID

0x800035ae805df289f84ef2c5adc3ec115d5a1a63f7089d40dce11ede75736e40

Host

192.168.0.1

Port

162

User ID

user

Security Level

noAuthNoPriv

✕ Cancel

✓ Create

1. In the Notification Type field, select SNMPv3 Trap. The engine ID is prepopulated.
2. Enter the following as needed and then click OK to apply the settings:
 - a. Host: Enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent.
 - b. Port number
 - c. User ID for accessing the host -- make sure the User ID has SNMPv3 permission.
 - d. Select the host security level:

Security level	Description
"noAuthNoPriv"	Select this if no authorization or privacy protocols are needed.

Security level	Description
"authNoPriv"	<p>Select this if authorization is required but no privacy protocols are required.</p> <p>Select the authentication protocol - MD5 or SHA</p> <p>Enter the authentication passphrase and then confirm the authentication passphrase</p>
"authPriv"	<p>Select this if authentication and privacy protocols are required.</p> <p>Select the authentication protocol - MD5 or SHA</p> <p>Enter the authentication passphrase and confirm the authentication passphrase</p> <p>Select the Privacy Protocol - DES or AES</p> <p>Enter the privacy passphrase and then confirm the privacy passphrase</p>

3. Click Create.

Syslog Messages

Use this action to automatically forward event messages to the specified syslog server. Determine the syslog transmission mechanism you prefer when setting it up.

RemoteAccess-GATE may or may not detect syslog message transmission failure. Detected syslog failures and reasons are saved in the event log.

See *Event Management* (on page 98) for help assigning this action to an event.

► To create the syslog message action:

New Action

Action Name

Syslog Example

Action

Syslog message

Syslog Server

192.168.0.1

Transport Protocol

UDP

Legacy BSD Syslog Protocol

☒

UDP Port

514

Cancel

Create

1.

Select Syslog Message from the Action list.
2.

In the Syslog Server field, specify the IP address to which the syslog is forwarded.
3.

In the Transport Protocol field, select one of the syslog protocols: UDP, TCP, or TCP+TLS. The default is UDP.

Transport protocols	Next steps
UDP	<div><div><div>In the UDP Port field, type an appropriate port number. Default is 514.</div><div>Select the "Legacy BSD Syslog Protocol" checkbox if applicable.</div></div></div>
TCP	NO TLS certificate is required. Type an appropriate port number in the TCP Port field.
TCP+TLS	<div><div>A TLS certificate is required.</div><div><div>Type an appropriate port number in the "TCP Port" field. Default is 6514.</div><div><div>In the CA Certificate field, click <div>Browse...</div> to select a TLS certificate. After importing the certificate, click Show to view its contents, or click Remove to delete.</div><div>To allow event messages even if any TLS certificate in the selected certificate chain is outdated or not valid yet, select the "Allow expired and not yet valid certificates" checkbox.</div></div></div></div>

4.

Click Create.

Keycode List

Use the Keycode List feature to create lists of keys you want to block from being used. Assign the list to a user group to block the group from using those keys. Keycode lists are created by keyboard language type. You are provided with a list of keys that can be blocked for each keyboard type.

When users are assigned more than one blocked keycode list, a given key will be available if it is not included on every keycode list. For example, a user is in groups with both List1 and List2 assigned. If List1 restricts F1, but List2 does not restrict F1, the user would be able to use F1

► **To add a new keycode list:**

1. Click Device Settings > Keycode List.
2. Click New.
3. Enter a Keyset Name to identify this list of keys to be blocked.
The keyset name is used when you assign the list to a user group. See *Users and Groups* (on page 87).
4. Select the Keyboard Type by language.
5. Select each Key you want to block from the Keys list, then click Add Key.
The added keys appear in the Keys Selected list. Click the Remove button to delete a key from the list.
6. When complete, click Add Keyset.

► **To edit a keycode list:**

1. Click Device Settings > Keycode List.
2. Click a keycode list by name to select it. The selected list is highlighted blue.
3. Click Edit to make changes to the list, and click Modify Keyset to save.

► **To delete a keycode list:**

1. Click Device Settings > Keycode List.
2. Click a keycode list by name to select it. The selected list is highlighted blue.
3. Click Delete to remove the list.

► **To block a user group from a keyset:**

Select the keyset in the User Management > Group settings. See *Users and Groups* (on page 87).

Network

In the default setting of the device, the static IPv4 address 192.168.0.1 is assigned to the network interface.

If you have adjusted the network settings to obtain the IP address from a DHCP server, you can find your automatically assigned IP address in the Device Information page. See *Device Information* (on page 94).

► **IPv4 settings:**

Field/setting	Description
Enable IPv4	Enable or disable the IPv4 protocol.
IP auto configuration	Select the method to configure IPv4 settings. <ul style="list-style-type: none"> ▪ <i>DHCP</i>: Auto-configure IPv4 settings via DHCP servers. ▪ <i>Static</i>: Manually configure the IPv4 settings.

- **DHCP settings:** Optionally specify the preferred hostname, which must meet the following requirements:
 - Consists of alphanumeric characters and/or hyphens
 - Cannot begin or end with a hyphen
 - Cannot begin with a number
 - Cannot contain punctuation marks, spaces, and other symbols
 - Maximum 253 characters
- **Static settings:** Assign a static IPv4 address, which follows this syntax "IP address/prefix length".
Example: *192.168.0.1/24*

► **IPv6 settings:**

Field/setting	Description
Enable IPv6	Enable or disable the IPv6 protocol.
IP auto configuration	Select the method to configure IPv6 settings. <ul style="list-style-type: none"> ▪ <i>Automatic</i>: Auto-configure IPv6 settings via DHCPv6. ▪ <i>Static</i>: Manually configure the IPv6 settings.

- **Automatic settings:** Optionally specify the preferred hostname, which must meet the above requirements.
- **Static settings:** Assign a static IPv6 address, which follows this syntax "IP address/prefix length".

Example: `fd07:2fa:6cff:1111::0/128`

► Interface Settings:

Field	Description
Speed	<ul style="list-style-type: none"> ▪ Select a LAN speed. ▪ Auto: System determines the optimum LAN speed through auto-negotiation. ▪ 10 MBit/s: Speed is always 10 Mbps. ▪ 100 MBit/s: Speed is always 100 Mbps. ▪ 1 GBit/s: Speed is always 1 Gbps (1000 Mbps).
Duplex	<ul style="list-style-type: none"> ▪ Select a duplex mode. ▪ Auto: The RemoteAccess-GATE selects the optimum transmission mode through auto-negotiation. ▪ Full: Data is transmitted in both directions simultaneously. ▪ Half: Data is transmitted in one direction (to or from the RemoteAccess-GATE) at a time.
Current state	Show the LAN's current status, including the current speed and duplex mode.

Note: Auto-negotiation is disabled after setting both the speed and duplex settings of the RemoteAccess-GATE to NON-Auto values, which may result in a duplex mismatch.

► Common Network Settings:

Common Network Settings are OPTIONAL. If there are no specific local networking requirements, leave the default settings.

Field	Description
DNS resolver preference	<p>Determine which IP address is used when the DNS resolver returns both IPv4 and IPv6 addresses.</p> <ul style="list-style-type: none"> ▪ IPv4 Address: Use the IPv4 addresses. ▪ IPv6 Address: Use the IPv6 addresses.

Field	Description
DNS suffixes (optional)	Specify a DNS suffix name if needed.
First/Second DNS server	<p>Manually specify static DNS server(s).</p> <ul style="list-style-type: none"> ▪ If any static DNS server is specified in these fields, it will override the DHCP-assigned DNS server. ▪ If DHCP (or Automatic) is selected for IPv4/IPv6 settings, and there are NO static DNS servers specified, the RemoteAccess-GATE will use DHCP-assigned DNS servers.

Network Services

The RemoteAccess-GATE supports the following network communication services:

- Discovery
- HTTP/HTTPS
- SMTP Server
- SNMP
- SSH

Discovery Port

RemoteAccess-GATE uses the default Discovery Port 5000 for communication with other G&D products.

The device will transmit information about itself (make,model,firmware version,encryption) in clear text unless the encryption option is selected.

► To change the default discovery port:

1. Click Device Settings > Network Services > Discovery Port.
2. Enter the port number.
3. Select the Encrypted checkbox to encrypt the transmission of device information.
4. Click Save.

HTTP/HTTPS Ports

RemoteAccess-GATE uses the default HTTP/HTTPS ports 80/443. You can change the default if needed.

HTTP access will be redirected to HTTPS.

► To change the default HTTP/HTTPS ports:

1. Click Device Settings > Network Settings > HTTP/HTTPS Ports.
2. Select the HTTP Access checkbox if you need HTTP enabled.

Note: When HTTP is disabled, AKC is downloaded via HTTPS. Microsoft .NET will check if the device TLS certificate is valid. Device certificate must be added into the "Trusted Root Certification Authorities" zone, and the common name of the certificate should match the device IP address or hostname.

3. Enter the port numbers then click Save.

4. The connection to the device will refresh with new HTTP/HTTPS port numbers. You must login again.

SMTP Server Settings

To send event emails, you must configure the SMTP settings and enter an IP address for your SMTP server and a sender's email address. See ***Event Management*** (on page 98).


If any email messages fail to be sent successfully, the failure event and reason are available in the event log. See ***Event Log*** (on page 132).

► **To set SMTP server settings:**

1. Click Device Settings > Network Services > SMTP Server.
2. Enter the information needed.

Field	Description
IP address/host name	Type the name or IP address of the mail server.
Port	Type the port number. <ul style="list-style-type: none"> ▪ Default is 25
Sender email address	Type an email address for the sender.
Number of sending retries	Type the number of email retries. <ul style="list-style-type: none"> ▪ Default is 2 retries
Time between sending retries	Type the interval between email retries in minutes. <ul style="list-style-type: none"> ▪ Default is 2 minutes.
Server requires authentication	Select this checkbox if your SMTP server requires password authentication, then enter the username and password.
User name Password	<ul style="list-style-type: none"> ▪ 4 to 64 characters allowed. Case sensitive. ▪ No spaces allowed in user name. ▪ Spaces are allowed in password.
Enable SMTP over TLS (StartTLS)	Select this checkbox if your SMTP server supports TLS.

- **Settings for the CA Certificate:**

Field/setting	Description
	<ul style="list-style-type: none"> Click Browse to import a certificate file. Then you can: Click Show to view the certificate's content. Click Remove to delete the installed certificate.
Allow expired and not yet valid certificates	<ul style="list-style-type: none"> Select this checkbox to make the authentication succeed regardless of the certificate's validity period.

3. To test the settings:
 - a. Enter a Recipient Email Address. Separate multiple email addresses with a comma.
 - b. Click Send Test Email and verify emails are received.
4. Click Save.

Note: The RemoteAccess-GATE device's TLS-based protocols support AES 128 and 256-bit ciphers. The exact cipher to use is negotiated between the device and the client web browser. To force a specific cipher, check your client documentation for configuring AES settings.

SNMP Settings

You can enable or disable SNMP communication between an SNMP manager and the RemoteAccess-GATE.

► To configure SNMP communication:

1. Click Device Settings > Network Services > SNMP.
2. Enable or disable SNMP v1 / v2c and/or SNMP v3 by clicking the corresponding checkbox.
 - a. The SNMP v1/v2c read-only access is enabled by default. The default 'Read community string' is "public".
 - b. To enable read-write access, type the 'Write community string.' Usually the string is "private".
3. Enter the MIB-II system group information, if applicable.
 - a. sysContact - the contact person in charge of the system
 - b. sysName - the name assigned to the system
 - c. sysLocation - the location of the system
4. Click the download link to get the SNMP MIB to use with your SNMP manager.
5. Click Save.

The image shows a configuration window titled "SNMP". It is divided into three main sections:

- SNMP Agent:** Contains four settings:
 - "Enable SNMP v1 / v2c" with a checked checkbox.
 - "Read Community String" with a text field containing "public".
 - "Write Community String" with a text field containing "private".
 - "Enable SNMP v3" with an unchecked checkbox.
- MIB-II System Group:** Contains three text fields:
 - "sysContact" (empty)
 - "sysName" (empty)
 - "sysLocation" (empty)
- Download MIBs:** Contains a table with one row:

Download MIBs	
RADM-MIB	download

At the bottom right of the window are two buttons: "Cancel" (with a close icon) and "Save" (with a checkmark icon).

SSH Settings

Enable or disable SSH access to the CLI, change the TCP port, or set a password or public key for login over SSH.

► SSH settings:

1. Click Device Settings > Network Services > SSH.
2. To enable or disable SSH access, select or deselect the checkbox.
3. To change the default port 22, type a port number.
4. Select one of the authentication methods.
 - Password authentication only: Enables password-based login only.
 - Public key authentication only: Enables public key-based login only.
 - Password and public key authentication: Enables both password and public key-based login, which allows either login authentication method to be used. This is the default setting.

*If public key authentication is selected, you must enter a valid SSH public key for each user profile to log in over the SSH connection. See **Users and Groups** (on page 87)*

5. Click Save.

Serial Port

The Serial Port setting controls the baud rate of the RemoteAccess-GATE serial Service port. RemoteAccess-GATE 's serial port supports CLI serial console use only.

► **To configure the serial port:**

1. Click Device Settings > Serial Port.
2. Enter the Baud Rate and click Save.



The screenshot shows a web-based configuration interface for the Serial Port. It has a title bar labeled "Serial Port". Below the title bar, there is a label "Baud Rate" on the left. To its right is a text input field containing the value "115200". Further right is a small dropdown menu currently showing "bit/s". At the bottom right of the form is a button labeled "Save" with a checkmark icon.

Terminal Block Control

The Terminal Block Control feature allows you to configure an external device that is connected to the terminal block of the RemoteAccess-GATE.

The RemoteAccess-GATE has one input terminal and one output terminal.

► Input Terminal:

- Two pins
- Supports an external push button or switch input
- Binary switches only
- Use case: turning off remote access when maintenance is being performed on the target

► Output Terminal:

- Three pins
- Two relays. One Normally Open (NO), and Normally Closed (NC). Both relays share the same common, so it is preferred to use only one. When using both at the same time, the common must be wired correctly.
- Use cases: performing remote power control of a server via its power button, turning on a light when a remote user is connected, or turning on a door lock or camera.
- Supported output devices: LED, Buzzer, PC Power Button. Output devices must provide their own power.

► Permissions:

There are several types of permissions involved in configuring and using terminal block control.

- To configure the terminal block settings, you must have the Terminal Block privilege. See *Users and Groups* (on page 87). With this privilege, you can access the Device Settings > Terminal Block Control page, which allows you to enable or disable input and output, and set permissions to allow input control for remote and local users, and configure the action of the output control. See procedure below.
- In addition to setting the permissions in the Terminal Block page, you must give all remote and local users Port Access permissions. The KVM Client's External Device menu will be accessible to users with the correct combined permissions. See *Users and Groups* (on page 87).

- You must enable local port output. The setting Security > KVM Security > Disable Local Port Output will override all other permissions. See *KVM Security* (on page 120).

► **Terminal Block Control Settings: Input**

1. Click Device Settings > Terminal Block Control.

Input Configuration	
Enable External Input Switch	Enable or disable the input switch.
Current External Input Switch State	The current state is displayed: Open or Closed. When switch state is open, the device functions normally.
Give Remote Console User	Select the access permission for remote console users. <ul style="list-style-type: none"> ▪ Full Access: Default setting. ▪ Video Only ▪ No Access: No video, keyboard, and mouse activity allowed, VM session terminated, KVM session terminated, Connection to target disallowed.
Give Local Console User	Select the access permission for local console users. <ul style="list-style-type: none"> ▪ Full Access ▪ Video Only ▪ No Access

2. Click Save.

Terminal Block Control

Input

Enable External Input Switch ☒

Current External Input Switch State Open

Give Remote Console User

☒ Full Access
☐ Video Only
☐ No Access

Give Local Console User

☒ Full Access
☐ Video Only
☐ No Access

► **Terminal Block Control Output Settings and Actions:**

1. Click Device Settings > Terminal Block Control.
2. Scroll down for the Output settings and actions.

Output Configuration	
Enable External Device	Enable or disable the external device.
External Device State	The external device state is displayed: <ul style="list-style-type: none"> ▪ On ▪ Off ▪ Blinking ▪ Disabled
Action	Select the radio button for the output action you want to perform on the external device: <ul style="list-style-type: none"> ▪ Turn External Device On/Off: Click On or Off. ▪ Pulse External Device: Sends a pulse to the device, either off to on, or on to off. Initial state of pulse can be changed by clicking button "On" and "Off". ▪ Blink External Device: Make sure the blink interval is set as desired.
Blink/Pulse Interval	Set interval between blinks or pulses in half-seconds. Default is 1. <ul style="list-style-type: none"> ▪ Blink range: 1-10 ▪ Pulse range: 1 - 100

Output

Enable External Device ☒

External Device State Disabled

Action

☒ Turn External Device On/Off
☐ Blink External Device

On

Off

Pulse

Blink/Pulse Interval

1

half-seconds

Save

3. Click Save.

Connecting the Terminal Block to a Motherboard

RemoteAccess-GATE can control one external switch, either power SW or reset SW, by connecting the terminal block to the pins on a motherboard of the external device.

There are power SW and reset SW headers on most motherboards. They are normally connected to the push buttons on the front panel of the case.

- Connect the two pin header to NO(normally open) of the terminal block on the RemoteAccess-GATE.

Virtual Media Shared Images

Configure Virtual Media Shared Images when using virtual media to access file server ISO images. ISO9660 format is the standard supported. However, other CD-ROM extensions may also work.

Note: SMB/CIFS support is required on the file server.

► **To designate file server ISO images for virtual media access:**

1. Click Device Settings > Virtual Media Shared Images.
2. Click New to add a shared image.
3. Enter information about the file server ISO images that you want to access:
 - IP Address/Host Name: Host name or IP address of the file server. Up to 248 characters.
 - Share Name: Share name portion of the ISO image.
 - Image Path: Full path name of the location of the ISO image. For example, /path0/image0.iso, \path1\image1.iso, and so on.
 - Select the Enable Samba 1.0 checkbox to allow RemoteAccess-GATE to use an older Samba version. When unchecked, Samba 3.0 is used.
4. Click Test Connection to verify.
5. Click Add Shared Image.

Chapter 6 Security

In This Chapter

Group Based Access Control.....	118
IP Access Control.....	119
KVM Security	120
Login Settings	123
Password Policy.....	124
TLS Certificate.....	125
Service Agreement	128

Group Based Access Control

Group based access control rules are similar to IP access control rules, except that they are applied to members of a user group. This enables you to grant system permissions to groups, based on their IP addresses. The order of role-based access control rules is important, since the rules are executed in numerical order.

► **To create IPv4 or IPv6 group based access control rules:**

1. Choose Security > Group Based Access Control.
2. Select the Enable Group Based Access Control for IPv4 or scroll down to select the checkbox for IPv6.

#	Start IP	End IP	Group	Policy	
1	192.168.0.1	192.168.0.24	Admin	Deny	↑ ↓ 🗑️

3. Determine the default policy.
 - Accept: Accepts traffic when no matching rules are present.
 - Deny: Rejects any user's login attempt when no matching rules are present.

4. Create rules and put them in priority order.
 - Enter Start IP and End IP, Group the rule applies to, and Policy.
 - Click Append to add another rule. To add a rule above another, select a rule and click Insert Above.
 - To rearrange rules in order, click the arrow buttons on each rule.
 - To delete a rule, click the trashcan icon.
5. Click Save. Note that IPv4 and IPv6 rules are saved separately.

IP Access Control

IP access control rules (firewall rules) determine whether to accept or discard traffic to/from the RemoteAccess-GATE, based on the IP address of the host sending or receiving the traffic. When creating rules, keep these principles in mind:

- **Rule order is important.**
When traffic reaches or is sent from the RemoteAccess-GATE, the rules are executed in numerical order. Only the first rule that matches the IP address determines whether the traffic is accepted or discarded. Any subsequent rules matching the IP address are ignored.
- **Prefix length is required.**
When typing the IP address, you must specify it in the CIDR notation. That is, BOTH the address and the prefix length are included. For example, to specify a single address with the 24-bit prefix length, use this format:
x.x.x.x/24
/24 = the prefix length.

► To create IPv4 or IPv6 IP access control rules:

1. Choose Security > IP Access Control.
2. Select the Enable IP Access Control for IPv4 or scroll down to select the checkbox for IPv6.
3. Select the Default Policy:
 - Accept: Accepts traffic from all addresses.
 - Drop: Discards traffic from all addresses, without sending any failure notification to the source host.
 - Reject: Discards traffic from all addresses, and an ICMP message is sent to the source host for failure notification.
4. Go to the Inbound Rules section or the Outbound Rules section according to your needs.
 - Inbound rules control the data sent to the RemoteAccess-GATE.

- Outbound rules control the data sent from the RemoteAccess-GATE.
- 5. Create rules and put them in priority order.
 - Enter IP address and mask and select the Policy.
 - Click Append to add another rule. To add a rule above another, select a rule and click Insert Above.
 - To rearrange rules in order, click the arrow buttons on each rule. The selected rule displays in blue.
 - To delete a rule, click the trashcan icon.

IP Access Control

IPv4

Enable IPv4 access control ☒

Inbound Rules

Default policy: Accept

#	IP/Mask	Policy	
1	192.168.0.1/24	Drop	↑ ↓ 🗑️

Append Insert Above

Outbound Rules

Default policy: Accept

#	IP/Mask	Policy
no rules defined		

Append Insert Above

✓ Save

6. Click Save. Note that IPv4 and IPv6 rules are saved separately.

KVM Security

The KVM Security settings page includes options for encryption mode, virtual media, local ports, and other functions that affect the device locally.

► To configure KVM Security settings:

1. Click Security > KVM Security.

KVM Security

Apply Encryption Mode to KVM and Virtual Media ☒

PC Share ☐

PC Share Idle Timeout seconds

Virtual Media Share ☐

Disable Local Port Output ☐

Local Device Reset Mode

Enable Local Factory Reset

Enable Direct Port Access via URL ☐

2. Select options as needed.

Field/setting	Description
Apply Encryption Mode to KVM and Virtual Media	Select this checkbox to use encryption for virtual media as well as KVM.
PC Share	Select PC Share to allow concurrent remote KVM access, enabling up to eight remote users to simultaneously log into one RemoteAccess-GATE and concurrently view and control the same target server through the device.
PC Share Idle Timeout	Set an idle time limit for users in PC Share mode. If a user has not moved the mouse or entered keyboard input and the timeout period expires, the user relinquishes control, and another user can access keyboard and mouse control of the target.
Virtual Media Share	This option is available only when PC-Share mode is enabled. When selected, Virtual Media Share permits the sharing of virtual media and audio among multiple users, that is, several users can access the same virtual media or audio session. The default is disabled.
Disable Local Port Output	If you will be using the Terminal Block Control feature, make sure this checkbox is cleared. When Disable Local Port Output is selected, this setting will override all other permissions for terminal block control. See <i>Terminal Block Control</i> (on page 114).

Field/setting	Description
Local Device Reset Mode	<p>This option specifies which actions are taken when the hardware Reset button on the device is depressed. Choose one of the following options:</p> <ul style="list-style-type: none"> ▪ Enable Local Factory Reset (default): Returns the RemoteAccess-GATE device to the factory defaults. ▪ Enable Local Admin Password Reset: Resets the local administrator password only. The password is reset to "4658". ▪ Disable All Local Resets: No reset action is taken.
Enable Direct Port Access via URL	<p>When selected, users can access the target directly by entering login credentials for the RemoteAccess-GATE in a URL. See <i>Direct Port Access URL</i> (on page 122).</p>

Direct Port Access URL

When Direct Port Access is enabled, you can access a target directly with a special URL that you can bookmark. This allows you to bypass logging into the RemoteAccess-GATE to connect to the target.

- Username and password are optional. If username and password are not provided, a login dialog will be displayed and, after being authenticated, the user will be directly connected to the target.
- The port may be a port number or port name. If you are using a port name, the name must be unique or an error is reported. Port number is "1".
- If the port is omitted altogether, an error is reported.
- Any special characters in the username, password, or port name must be passed in encoded URL codes.

► Direct Port Access with VKCS:

If you are using VKCS and direct port access, use one of the following syntaxes for standard ports.

- | |
|---|
| <ul style="list-style-type: none"> ▪ <code>https://IPaddress/dpa.asp?username=username&password=password&port=1&client=vkcs</code> |
| |

- `https://IPAddress/dpa.asp?username=username&password=password&portname=port name&client=vkcs`

► **Direct Port Access with AKC:**

If you are using AKC and direct port access, use one of the following syntaxes for standard ports.

- | |
|--|
| ▪ <code>https://IPAddress/dpa.asp?username=username&password=password&port=1&client=akc</code> |
| |
| ▪ <code>https://IPAddress/dpa.asp?username=username&password=password&portname=port name&client=akc</code> |

► **Direct Port Access with HKC:**

If you are using HKC and direct port access, use one of the following syntaxes for standard ports.

- | |
|--|
| ▪ <code>https://IPAddress/dpa.asp?username=username&password=password&port=1&client=hkc</code> |
| |
| ▪ <code>https://IPAddress/dpa.asp?username=username&password=password&portname=port name&client=hkc</code> |

Login Settings

The Login Settings page contains options for user blocking and login limitations.

► **To configure login settings:**

1. Click Security > Login Settings.
2. To block users for failed logins, select the Block user on login failure checkbox, then configure the parameters.
 - Block timeout: Select the time period that users with failed logins will be blocked from logging in.
 - Maximum number of failed logins: Enter the number of failed login attempts that users can make before they are blocked.
3. To automatically logout users after an idle period, select a time in the Idle timeout period field. To allow idle users to remain logged in, select "infinite."

4. Select "Prevent concurrent login with same username" to prevent logins by more than one user with the same username. This setting does not apply to the default admin user.

Login Settings

User Blocking

Block user on login failure ☒

Block timeout 10 min

Maximum number of failed logins 3

Login Limitations

Idle timeout period 10 min

Prevent concurrent login with same username ☐

Save

5. Click Save.

Password Policy

The Password Policy page contains settings for password aging and strong passwords.

► To configure a password policy:

1. Click Security > Password Policy.
2. To enable Password Aging, which forces users to change their passwords at selected intervals:
 - Select the Enabled checkbox for Password Aging Interval.
 - Select a Password Aging Interval, from 7 days to 365 days.

Password Policy

Password Aging

Password aging interval ☐ Enabled

Password aging interval 60 d

3. To enable strong passwords and set their parameters:
 - Select the Enabled checkbox for Strong Passwords.

- Set a Minimum and Maximum Password Length. Minimum is 8. Maximum is 64.
- Select options to enforce at least one lower case, upper case, numeric, and/or special character.
- Specify the Password History Size, which controls how frequently passwords can be reused. Maximum is 12.

4. Click Save.

TLS Certificate

RemoteAccess-GATE uses TLS 1.3 for any encrypted network traffic between itself and a connected client. When establishing a connection, RemoteAccess-GATE has to identify itself to a client using a cryptographic certificate. The RemoteAccess-GATE contains a default certificate that you should replace with your own.

RemoteAccess-GATE can generate a Certificate Signing Request (CSR) or a self-signed certificate using SHA-2.

The CA verifies the identity of the originator of the CSR. The CA then returns a certificate containing its signature to the originator. The certificate, bearing the signature of the well-known CA, is used to vouch for the identity of the presenter of the certificate.

Important: Make sure your RemoteAccess-GATE date/time is set correctly.

*When a self-signed certificate is created, the RemoteAccess-GATE date and time are used to calculate the validity period. If the RemoteAccess-GATE date and time are not accurate, the certificate's valid date range may be incorrect, causing certificate validation to fail. See **Date and Time** (on page 96).*

Note: The CSR must be generated on the RemoteAccess-GATE.

Note: When upgrading firmware, the active certificate and CSR are not replaced.

► **To view and download the active certificate and key:**

1. Click Security > TLS Certificate. The active certificate details display.

Subject		Issuer	
Country	DE	Country	US
State or province	NRW	State or province	NJ
Locality	Siegen	Locality	Somerset
Organization	Guntermann & Drunck GmbH	Organization	Raritan Americas, Inc.
Organizational unit	F&E	Organizational unit	Engineering
Common name	G&D	Common name	Raritan CA
Email address	info@gdsys.de	Email address	not set

Miscellaneous	
Not valid before	Sep 16 00:00:50 2020 GMT
Not valid after	Sep 13 00:00:50 2034 GMT
Serial number	05
Key length	2048 bits

2. Click Download Key and Download Certificate to get the active certificate files.

► **To create and install a new SSL certificate:**

1. Click Security > TLS Certificate. Scroll down to the New TLS Certificate section.
2. Complete the Subject fields:
 - Country (ISO code) - The country where the organization is located. This is the two-letter ISO code, e.g. DE for Germany, or US for the U.S.
 - State/Province - The state or province where the organization is located.
 - Locality/City - The city where the organization is located.

- Organization - The name of the organization to which the RemoteAccess-GATE belongs.
 - Organizational unit - This field is used for specifying to which department within an organization the RemoteAccess-GATE belongs.
 - Common name - The network name of the RemoteAccess-GATE once it is installed on your network (usually the fully qualified domain name). The common name is identical to the name used to access the RemoteAccess-GATE with a web browser, but without the prefix "http://". In case the name given here and the actual network name differ, the browser displays a security warning when the RemoteAccess-GATE is accessed using HTTPS.
 - Email address - The email address of a contact person that is responsible for the RemoteAccess-GATE and its security.
3. Add up to 10 Subject Alternative Names (SAN) by clicking the Add Name button, then enter the hostname or IP in the field. SANs are the hostnames or IP addresses the certificate will be valid for.
 4. To generate, do one of the following:
 - To generate self-signed certificate, do the following:
 - a. In the Key Creation Parameters, select the Self-Sign checkbox . When you select this option, the RemoteAccess-GATE generates the certificate based on your entries, and acts as the signing certificate authority. The CSR does not need to be exported and used to generate a signed certificate.
 - b. Set the Validity in Days, which controls how many days until this certificate expires. Ensure the RemoteAccess-GATE date and time are correct. If the date and time are not correct, the certificate's valid date range may not be calculated correctly.
 - c. Click Create New TLS Key.
 - d. When the page refreshes, new buttons appear in the New TLS Certificate section, to allow you to install, download or delete the newly generated self-signed certificate and key.
 - e. **To start using the new certificate**, click Install Key and Certificate.
 - f. The page may refresh as the certificate loads.
 - To generate a CSR to send to the CA for certification:
 - a. In the Key Creation Parameters, enter a password in the Challenge and Confirm Challenge fields.
 - b. Click Create New TLS Key.

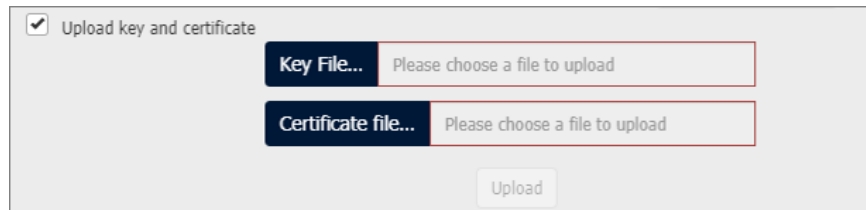
- c. When the page refreshes, new buttons appear in the New TLS Certificate section, to allow you to download the CSR, download the key, or delete the CSR.
- d. Click the Download the Certificate Signing Request button to download the CSR. Click the Download Key button to download the file containing the private key.
- e. Send the CSR to a CA for certification. You will get the new certificate from the CA.

Note: The CSR and the private key file are a matched set and should be treated accordingly. If the signed certificate is not matched with the private key used to generate the original CSR, the certificate will not be useful. This applies to uploading and downloading the CSR and private key files.

- Once you get the certificate from the CA, return to this page to upload it to the RemoteAccess-GATE. After uploading, click Install to start using the new certificate. The page may refresh as the certificate loads.

► **To upload a key and certificate:**

1. To activate the upload fields, click Security > TLS Certificate, then scroll down to the New TLS Certificate section.
2. Select the Upload Key and Certificate checkbox. The Browse and upload controls appear.



Service Agreement

The Service Agreement page allows you to enable an agreement that appears on the login page of the RemoteAccess-GATE. Users must select a checkbox on the agreement before logging in.

► **To configure the service agreement:**

1. Click Security > Service Agreement.


Restricted Service Agreement

Enforce restricted service agreement ☒

Unauthorized access prohibited; all access and activities not explicitly authorized by management are unauthorized. All activities are monitored and logged. There is no privacy on this system. Unauthorized access and activities or any criminal activity will be reported to appropriate authorities.

9703 characters remaining.

2. Select the Enforce Service Agreement checkbox.
3. Enter the agreement text in the field and click Save. The login page will present the service agreement. Users must select the checkbox before logging in.



Unauthorized access prohibited; all access and activities not explicitly authorized by management are unauthorized. All activities are monitored and logged. There is no privacy on this system. Unauthorized access and activities or any criminal activity will be reported to appropriate authorities.

☒ I understand and accept the Restricted Service Agreement

Login using HTML KVM Client

Other KVM clients offer better video and virtual media performance. [Learn more.](#)

Chapter 7 Maintenance

In This Chapter

Backup and Restore.....	130
Event Log	132
Firmware History	133
Unit Reset	133
Update Firmware	134

Backup and Restore

You must be a member of the admin group to download a backup file, and to restore a RemoteAccess-GATE with a backup file.

Backups can be encrypted by adding password protection. The password must be entered when the file is used to perform a restore.

► **To download the Device Settings backup file:**

1. Click Maintenance > Backup/Restore.
2. To password protect the backup file, enter a password in the Password Protection Used For Backup/Restore (Optional) field.
3. Click Download Device Settings to automatically download the backup_settings.rfp file.

Backup Restore

Password Protection Used For Backup/Restore (Optional)

Save Device Settings

Download Device Settings

Restore Device Settings


Browse...

☒ Protected ☐ Full

Upload & Restore Device Settings

► **To restore the RemoteAccess-GATE using a backup file:**

1. Click Maintenance > Backup/Restore.

2. Click  to select the backup file.
3. Select Protected or Full.
 - Protected: Restores all settings except for device specific settings: network information, names, preferred resolution.
 - Full: Restores everything.
4. If the file is password protected, enter the password in the Password Protection Used For Backup/Restore (Optional) field.
5. Click Upload & Restore Device Settings to upload the file.
6. Wait until the RemoteAccess-GATE resets and the Login page reappears, indicating that the restore is complete. Note: In a full restore, the IP address may have been changed. You must start a new browser session to login to the new IP address.

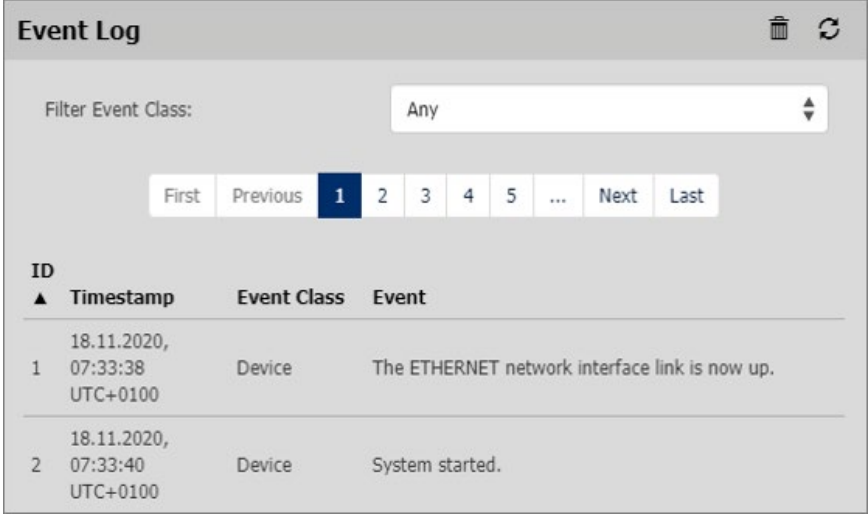
Event Log

The RemoteAccess-GATE captures certain system events and saves them in a local event log.

You can view over 2000 historical events that occurred on the RemoteAccess-GATE in the local event log. When the log size exceeds 256KB, each new entry overwrites the oldest one.

► Event Classes:

- Device
- KVM Port
- User Activity
- User Administration
- Serial Port



The screenshot shows the 'Event Log' window. At the top, there is a 'Filter Event Class:' dropdown menu set to 'Any'. Below it is a pagination bar with buttons: 'First', 'Previous', '1' (selected), '2', '3', '4', '5', '...', 'Next', and 'Last'. The main table has four columns: 'ID', 'Timestamp', 'Event Class', and 'Event'. The first two rows of data are visible.



ID	Timestamp	Event Class	Event
1	18.11.2020, 07:33:38 UTC+0100	Device	The ETHERNET network interface link is now up.
2	18.11.2020, 07:33:40 UTC+0100	Device	System started.

► To display the event log:

- Choose Maintenance > Event Log.

Each event entry consists of:

- ID number of the event
- Timestamp of the event: The timestamp in the event log is automatically converted to your computer's time zone. To avoid time confusion, apply the RemoteAccess-GATE time zone settings to your computer or mobile device.
- Event class
- A description of the event

- Refresh the event log by clicking the refresh icon  in the top-right corner.
- ▶ **To view by event category:**
 - Select an option in the Filter Event Class field.
- ▶ **To clear the local event log:**
 1. Click the trash icon  on the top-right corner.
 2. Click Clear Log on the confirmation message.

Firmware History

The firmware upgrade history is retained even after device reboot or firmware upgrade. The history is cleared in the event of a factory default reset.

- ▶ **To view the firmware update history:**
 - Choose Maintenance > Firmware History.

Each firmware update event consists of:

 - Update date and time
 - Previous firmware version
 - Update firmware version
 - Update result

Firmware Update History			
Timestamp ▼	Previous Version	Update Version	Status
23.11.2020, 07:24:34 UTC+0100	4.1.0.1.47249	4.1.0.1.47254	SUCCESSFUL

Unit Reset

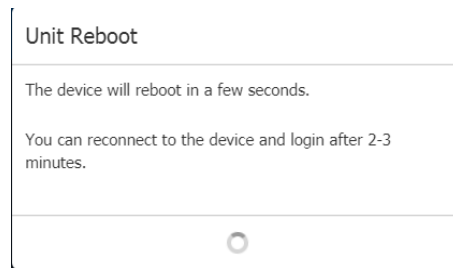
The Unit Reset section has options to remotely reboot or reset to factory defaults.

- Reboot Unit: Restarts the RemoteAccess-GATE.
- Reset to Factory Defaults: Removes all customized settings and returns the RemoteAccess-GATE to the factory default settings. Requires admin privilege.

Unit Reset	
Reboot Unit	Reset to Factory Defaults

► **To reboot the device:**

1. Choose Maintenance > Unit Reset.
2. Click Reboot Unit.
3. A confirmation message appears. Click Reboot to proceed.
A countdown timer appears.



4. When the restart is complete, the login page opens.

► **To reset to factory defaults:**

1. Click Maintenance > Unit Reset.
2. Click Reset to Factory Defaults. Click to confirm reset in the confirmation message.
3. A countdown timer appears. It takes about two minutes to complete.
4. When the reset is complete, proceed with initial configuration. See *Initial Configuration* (on page 2).

► **Other factory reset options:**

- Use the reset button on the RemoteAccess-GATE device. Press the reset button for 5 seconds. Device will reset and reboot.
- Perform the CLI command. See *CLI: reset* (on page 162)

Update Firmware

You must have the Maintenance privilege to update the RemoteAccess-GATE firmware.

► **To update the firmware:**

1. Click Maintenance > Update Firmware.
2. Click Browse to select an appropriate firmware file, then click Upload. A progress bar appears to indicate the upload process.

Update Firmware

Browse...

Upload

The firmware update is being prepared.

This may take up to a minute. On successful completion the firmware update will be started.

Please wait ...

3. Once complete, information of both installed and uploaded firmware versions as well as compatibility and signature-checking results are displayed.

Update Firmware

A new firmware has been uploaded to your device.

Version

Installed Version	4.1.0.1.47254
New Version	4.1.0.1.47254

Compatibility

✓ The uploaded firmware file is compatible with this device.

Signature

✓ The signature of the uploaded firmware file is valid.

View Certificate

✗ Discard Upload ✓ Update Firmware

- To cancel, click Discard Upload.
 - To proceed with the update, click Update Firmware.
4. When the update begins, another progress bar appears. Warning: Do NOT power off the RemoteAccess-GATE during the update. The LAN port LED on the device fast-blinks green during update.

The firmware update is in progress

This may take some minutes. Please do not power off the device while the update is in progress! After a successful update, the device will reboot automatically.

14%



Note: No users can successfully log in during the update. Logged in users are forced to suspend operations.

5. When the update is complete, the RemoteAccess-GATE reboots, and the Login page re-appears. The update and reboot process should take around 5 minutes. If your device displays a "Loading" screen after update and reboot for longer, you can safely restart your browser and login to the RemoteAccess-GATE again to check the update results.

*After Updating: The RemoteAccess-GATE MIB may have changed. If you are using an SNMP manager, you may need to re-download the MIB and make update. See **SNMP Settings** (on page 111).*

► The firmware update completed with warnings:

The message, "The firmware update completed with warnings" may appear before reboot if you completed your update while an iOS device was connected to the USB port on the RemoteAccess-GATE. This warning does not indicate any problems or that the update failed.

The firmware update completed with warnings

The device will now reboot. Please wait for five minutes, then follow this link to the [login page](#) to log in. If the device does not work correctly after the update, please contact Raritan support.

74%



Chapter 8 Virtual Media

In This Chapter

Overview	137
Virtual Media Performance Recommendations	138
Prerequisites for Using Virtual Media	138
Mounting Local Drives	139
Supported Tasks Via Virtual Media	139
Supported Virtual Media Types	139
Number of Supported Virtual Media Drives	140
Virtual Media in a Linux Environment	140
Virtual Media in a Mac Environment	141
Virtual Media File Server Setup (File Server ISO Images Only)	142

Overview

All RemoteAccess-GATE models support virtual media. Virtual media extends KVM capabilities by enabling target servers to remotely access media from a client PC and network file servers.

With this feature, media mounted on client PCs and network file servers are essentially "mounted virtually" by the target server. The target server can then read from and write to that media as if it were physically connected to the target server itself.

Each RemoteAccess-GATE comes equipped with virtual media to enable remote management tasks using the widest variety of CD, DVD, USB, audio devices, internal and remote drives, and images.

Virtual media sessions are secured using the strongest encryption offered by the browser, typically 256 bit AES. Older browsers may only support 128 bit AES.

HKC does not support all virtual media features. See HTML KVM Client (HKC) for details

Virtual Media Performance Recommendations

Additional studies of virtual media performance show that RemoteAccess-GATE virtual media performance can range up to 175 mbps.

► **For maximum performance:**

- Turn off encryption. Encryption has a large effect on performance.
- Utilize a high-speed laptop/PC with AKC or VKC KVM Clients.
- Writing to a virtual media drive connected to the KVM Client may be slower than reading from the drive.
- There may be performance variations across different USB drives.
- Network performance is also a factor.

Prerequisites for Using Virtual Media

RemoteAccess-GATE Virtual Media Prerequisites

- For users requiring access to virtual media, the RemoteAccess-GATE permissions must be set to allow access to the relevant port, as well as virtual media access (VM Access port permission) for the port. Port permissions are set at the group-level.
- If you want to use PC-Share, Security Settings must also be enabled in the Security Settings page. **Optional**
- A USB connection must exist between the device and the target server.
- You must choose the correct USB connection settings for the KVM target server you are connecting to.

Client PC VM Prerequisites

- Certain virtual media options require administrative privileges on the PC (for example, drive redirection of complete drives).

Note: If you are using Windows, disable User Account Control or select Run as Administrator when starting Internet Explorer. To do this, click the Start Menu, locate IE, right-click and select Run as Administrator.

Target Server VM Prerequisites

- KVM target servers must support USB connected drives.

Mounting Local Drives

This option mounts an entire drive, which means the entire disk drive is mounted virtually onto the target server.

Use this option for hard drives and external drives only. It does not include network drives, CD-ROM, or DVD-ROM drives.

Supported Tasks Via Virtual Media

Virtual media provides the ability to perform tasks remotely, such as:

- Transferring files
- Running diagnostics
- Installing or patching applications
- Complete installation of the operating system

Important: Once you are connected to a virtual media drive, do not change mouse modes in the KVM client if you are performing file transfers, upgrades, installations or other similar actions. Doing so may cause errors on the virtual media drive or cause the virtual media drive to fail.

Supported Virtual Media Types

The following virtual media types are supported for Windows®, Mac® and Linux™ clients when using AKC and VKC/VKCS.

- Internal and external hard drives
- Internal and USB-mounted CD and DVD drives
- USB mass storage devices
- PC hard drives
- ISO images (disk images)
- IMG files
- DMG files
- ISO9660 is the standard supported. However, other ISO standards can be used.

Note: Due to browser limitations, HKC supports a different set of virtual media types.

Conditions when Read/Write is Not Available

Virtual media Read/Write is not available in the following situations:

- For Linux® and Mac® clients
- When the drive is write-protected
- When the user does not have Read/Write permission:
 - Port Permission Access is set to None or View
 - Port Permission VM Access is set to Read-Only or Deny

Number of Supported Virtual Media Drives

With the virtual media feature, you can mount up to two drives (of different types) that are supported by the USB connection settings currently applied to the target. These drives are accessible for the duration of the KVM session.

For example, you can mount a specific CD-ROM, use it, and then disconnect it when you are done. The CD-ROM virtual media “channel” will remain open, however, so that you can virtually mount another CD-ROM. These virtual media “channels” remain open until the KVM session is closed as long as the USB settings support it.

To use virtual media, connect/attach the media to the client or network file server that you want to access from the target server.

This need not be the first step, but it must be done prior to attempting to access this media.

Virtual Media in a Linux Environment

Active System Partitions

You cannot mount active system partitions from a Linux client.

Linux Ext3/4 drive partitions need to be unmounted via `umount /dev/<device label>` prior to a making a virtual media connection.

Mapped Drives

Mapped drives from Linux clients are not locked when mounted onto connected targets.

Drive Partitions

The following drive partition limitations exist across operating systems:

- Windows® and Mac targets are not able to read Linux formatted partitions
- Windows and Linux cannot read Mac formatted partitions
- Only Windows Fat partitions are supported by Linux

Root User Permission Requirement

Your virtual media connection can be closed if you mount a CD ROM from a Linux client to a target and then unmount the CD ROM.

To avoid these issues, you must be a root user.

Connect Drive Permissions (Linux)

Linux users must have read-only permissions for the removable device they wish to connect to the target. For /dev/sdb1 run the following as root user:

```
root@administrator-desktop:~# chmod 664 /dev/sdb1
root@administrator-desktop:~# ls -l /dev/sdb1
brw-rw-r-- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
```

The drive is then available to connect to the target.

Virtual Media in a Mac Environment

Active System Partition

You cannot use virtual media to mount active system partitions for a Mac client.

Drive Partitions

The following drive partition limitations exist across operating systems:

- Windows® and Mac targets are not able to read Linux formatted partitions
- Windows cannot read Mac formatted partitions
- Windows FAT and NTFS are supported by Mac
- Mac users must unmount any devices that are already mounted in order to connect to a target server. Use `>diskutil umount /dev/disk1s1` to unmount the device and `diskutil mount /dev/disk1s1` to remount it.

Connect Drive Permissions (Mac)

For a device to be available to connect to a target from a Mac® client, you must have read-only permissions to the removable device, and also unmount the drive after doing so.

For /dev/sdb1, run the following commands as root user:

```
root@administrator-desktop:~# chmod 664 /dev/sdb1
root@administrator-desktop:~# ls -l /dev/sdb1
brw-rw-r-- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
root@administrator-desktop:~# diskutil unmount /dev/sdb1
```

Virtual Media File Server Setup (File Server ISO Images Only)

This feature is only required when using virtual media to access file server ISO images. ISO9660 format is the standard supported. However, other CD-ROM extensions may also work.

Note: SMB/CIFS support is required on the file server.

Use the Virtual Media Shared Images setup page to designate the files server(s) and image paths that you want to access using virtual media. File server ISO images specified here are available for selection in the Remote Server ISO Image Hostname and Image drop-down lists in the Map Virtual Media CD/ISO Image dialog. See **Mounting CD-ROM/DVD-ROM/ISO Images** (on page 40).

► **To designate file server ISO images for virtual media access:**

1. Choose Device Settings/Virtual Media Shared Images from the remote console. The Virtual Media Shared Images setup page opens.
2. Click New to open the Add Shared Image page.
3. Enter information about the file server ISO images that you want to access.
 - IP Address/Hostname
 - Share Name
 - Image Path
 - Select Enable SAMBA v1.0 as applicable.
4. Click Add Shared Image.

All media specified here are now available for selection in the Map Virtual Media CD/ISO Image dialog

Chapter 9 Diagnostics

In This Chapter

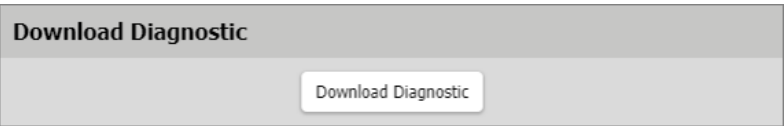
Download Diagnostic	143
Network Diagnostics.....	143

Download Diagnostic

You can download a diagnostic file from the RemoteAccess-GATE to a client machine. The file is compressed into a .zip file.

You must be a member of the admin group.

► **To download a diagnostic file:**



1. Click Diagnostics> Download Diagnostic.
2. Click Download Diagnostic, then save the file.

Network Diagnostics

RemoteAccess-GATE provides the following tools diagnosing potential networking issues.

- Ping
- Trace Route: Find out the route over the network between two hosts or systems.
- List TCP Connections: Display a list of TCP connections.

Choose Diagnostics > Network Diagnostics, and then perform any function below.

► **Ping:**

Enter the IP or hostname in the Network Host field, then set the of requests to send. Maximum is 20. This determines how many packets are sent for pinging the host. Click Run Ping to ping the host. The Ping results are then displayed.

► **Trace Route:**

1. Type values in the following fields.

Field/setting	Description
Hostname	The IP address or name of the host whose route you want to check.
Timeout(s)	A timeout value in seconds to end the trace route operation. Maximum 900 seconds.
Use ICMP packets	To use the Internet Control Message Protocol (ICMP) packets to perform the trace route command, select this checkbox.

2. Click Run. The Trace Route results are displayed.

► **List TCP Connections:**

1. Click the List TCP Connections title bar to show the list of active connections.

List TCP Connections						
Active Internet connections (w/o servers)						
#	Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
1	tcp	0	0	::ffff:192.168.0.1:443	::ffff:192.168.0.200:58611	TIME_WAIT
2	tcp	0	0	::ffff:192.168.0.1:443	::ffff:192.168.0.200:58188	ESTABLISHED

Chapter 10 CLI Commands

The RemoteAccess-GATE supports the following categories of commands in the CLI:

check	Check services
clear	Clear logs
config	Enter configuration view
connect	Connect to a target
diag	Enter diagnostics view
exit	Exit CLI session
reset	Reset device
show	Shows various device information

In This Chapter

CLI: check.....	145
CLI: clear	145
CLI: config.....	146
CLI: connect	160
CLI: diag.....	161
CLI: reset	162
CLI: show.....	163
CLI: exit.....	167

CLI: check

```
check
# check ntp
```

CLI: clear

```
clear
# clear eventlog
Do you really want to clear the event log? [y/n]
```

CLI: config

```
config
# config
config:#
```

► Available commands:

apply	Save changed settings and leave config mode
authentication	Configure authentication settings
cancel	Discard changed settings and leave config mode
check	Check services
device	Configure Device
group	Configure user groups
network	Configure network settings
password	Change password of currently logged in user
security	Configure security settings
serial	Configure serial port settings
terminalblock	Configure terminal block settings
time	Configure date/time settings
user	Configure users

CLI: config authentication

authentication

config # authentication

Available commands:

- ldap Configure LDAP server settings
- radius Configure Radius server settings
- type Configure authentication type (local/ldap/radius)

► LDAP:

add Add a new LDAP server

addClone Add a new LDAP server, cloning another server

delete Delete LDAP server

modify Modify an existing LDAP server

- config # authentication ldap add

authentication ldap add <host> <port> <security> <bindtype> <basedn>
 <loginnameattr> <userentryclass> [userSearchSubfilter
 <usersearchfilter>] [adDomain <addomain>] [verifyServerCertificate
 <certverify>] [allowExpiredCertificate <allowexpiredcert>] [bindDN
 <binddn>]

Add a new LDAP server

host IP address/host name

port Port number (0..4294967295)

type LDAP server type

(openldap/activeDirectory)

security Security type (none/startTls/tls)

bindtype Bind type

(anonymousBind/authenticatedBind)

basedn Base DN for search

loginnameattr Login name attribute

userentryclass User entry object class

userSearchSubfilter User search subfilter

adDomain Active directory domain

verifyServerCertificate Enable validation of LDAP server certificate
 (true/false)

allowExpiredCertificate Allow expired and not yet valid server
 certificates (true/false)

bindDN Bind DN

- config # authentication ldap addClone

```
authentication ldap addClone <index> <host>
```

Add a new LDAP server, cloning another server

index Source server index

host	IP address/host name
------	----------------------

- config # authentication ldap delete

authentication ldap delete <index>

Delete LDAP server

index	Server index
-------	--------------

- config # authentication ldap modify

authentication ldap modify <index> [host <host>] [port <port>]

```
[serverType ] [securityType <security>] [bindType <bindtype>]
```

```
[searchBaseDN <basedn>] [loginNameAttribute <loginnameattr>]
```

```
[userEntryObjectClass <userentryclass>] [userSearchSubfilter
```

<usersearchfilter>] [adDomain <addomain>] [verifyServerCertificate

```
<certverify> [certificate] [allowExpiredCertificate <allowexpiredcert>]
```

```
[bindDN <binddn>] [bindPassword] [sortPosition <position>]
```

Modify an existing LDAP server

index	Index
-------	-------

host	IP address/host name
------	----------------------

port	Port number (0..4294967295)
------	-----------------------------

serverType	LDAP server type
------------	------------------

```
(openldap/activeDirectory)
```

securityType	Security type (none/startTls/tls)
--------------	-----------------------------------

bindType	Bind type
----------	-----------

(anonymousBind/authenticatedBind)

searchBaseDN	Base DN for search
--------------	--------------------

loginNameAttribute	Login name attribute
--------------------	----------------------

userEntryObjectClass	User entry object class
----------------------	-------------------------

userSearchSubfilter	User search subfilter
---------------------	-----------------------

adDomain	Active directory domain
----------	-------------------------

verifyServerCertificate	Enable validation of LDAP server certificate (true/false)
-------------------------	---

certificate	Certificate CA chain
-------------	----------------------

allowExpiredCertificate	Allow expired and not yet valid server
certificates (true/false)	

bindDN	Bind DN
--------	---------

bindPassword	Bind password
sortPosition	New position in server list

► **RADIUS:**

- config # authentication radius

Available commands:

- add
Add a new Radius server

host	IP address/host name
type	Authentication type (pap/chap/msChapV2)
authport	Authentication port number (0..4294967295)
acctport	Accounting port number (0..4294967295)
timeout	Timeout (1..60)
retries	Number of retries (0..5)
- delete
Delete Radius server

index	Server index
-------	--------------
- modify
Modify a new Radius server
config:# authentication radius modify
authentication radius modify <index> [host <host>] [authType]
[authPort <authport>] [accountPort <acctport>] [timeout <timeout>]
[retries <retries>] [secret] [sortPosition <position>]

index	Index
host	IP address/host name
authType	Authentication type (pap/chap/msChapV2)
authPort	Authentication port number (0..4294967295)
accountPort	Accounting port number (0..4294967295)
timeout	Timeout (1..60)
retries	Number of retries (0..5)
secret	Shared secret
sortPosition	New position in server list

► **TYPE:**

- config # authentication type

authentication type [useLocalIfRemoteUnavailable <localfallback>]

Configure authentication type

type Authentication type (local/ldap/radius)

useLocalIfRemoteUnavailable Use local authentication if remote authentication is unavailable (true/false)

CLI: config device

device

config:# device name

device [name <name>]

Configure Device

name Device name

For example, to name device "newname", at config menu type "device name newname", then type "apply" to save.

CLI: config group

group

config:# group create

group create [name <name>] [privileges <privs>]

Create a new group

name Group name

privileges Group privileges (one or more (separated by '/') of
changeTerminalBlockSettings/deviceAccessUnderCcsG/deviceSettings/
maintenance/pcShare/portControl:1/portControl:all/portViewOnly:1/port
ViewOnly:all/portVmROnly:1/portVmROnly:all/portVmRW:1/portVmRW:al
l/securitySettings/userManagement)

config:# group delete [name <name>]

Delete group

name Group name (Admin)

config:# group modify [name <name>] [description <desc>]

[addPrivileges <addprivs>] [removePrivileges <removeprivs>]

Edit a group

name Group name (Admin)

description Group description

addPrivileges Add group privileges (one or more (separated by '/')
of
changeTerminalBlockSettings/deviceAccessUnderCcsG/deviceSettings/
maintenance/pcShare/portControl:1/portControl:all/portViewOnly:1/port
ViewOnly:all/portVmROnly:1/portVmROnly:all/portVmRW:1/portVmRW:al
l/securitySettings/userManagement)

removePrivileges Remove group privileges (one or more (separated
by '/') of
changeTerminalBlockSettings/deviceAccessUnderCcsG/deviceSettings/
maintenance/pcShare/portControl:1/portControl:all/portViewOnly:1/port
ViewOnly:all/portVmROnly:1/portVmROnly:all/portVmRW:1/portVmRW:al
l/securitySettings/userManagement)

CLI: config network

network

config:# network dns [firstServer <server1>] [secondServer <server2>]
[searchSuffixes <searchSuffixes>] [resolverPreference
<resolverPreference>]

Configure DNS settings

firstServer First DNS server

secondServer Second DNS server

searchSuffixes Search suffixes

resolverPreference DNS resolver preference (preferV4/preferV6)

config:# network ethernet [speed <speed>] [duplexMode
<duplexMode>]

Configure ethernet interface

speed Speed (1000Mbps/100Mbps/10Mbps/auto)

duplexMode Duplex mode (half/full/auto)

config:# network ipv4 gateway

network ipv4 gateway <gateway>

Configure default IPv4 gateway

gateway Default IPv4 gateway

config:# network ipv4 interface [enabled <enabled>] [configMethod
<configMethod>] [preferredHostName <prefHostname>] [address
<addrCidr>]

Configure interface IPv4 settings

enabled Enable/disable IPv4 protocol (true/false)

configMethod IPv4 Configuration method (dhcp/static)

preferredHostName Preferred host name

address IPv4 address/prefix-len

config:# network ipv6 gateway

network ipv6 gateway <gateway>

Configure default IPv6 gateway

gateway Default IPv6 gateway

```
config:# network ipv6 interface [enabled <enabled>] [configMethod
<configMethod>] [preferredHostName <prefHostname>] [address
<addrCidr>]
```

Configure interface IPv6 settings

enabled	Enable/disable IPv6 protocol (true/false)
configMethod	IPv6 Configuration method (automatic/static)
preferredHostName	Preferred host name
address	IPv6 address/prefix-len

```
config:# network services discovery
network services discovery [port <port>]
```

Configure Discovery Port

port	RDM discovery port (1..65535)
------	-------------------------------

```
config:# network services http [enabled <enabled>] [port <port>]
[enforceHttps <enforcehttps>]
```

Configure HTTP access

enabled	Enable/disable HTTP access (true/false)
port	HTTP access TCP port (1..65535)
enforceHttps	Enable HTTPS enforcement for web access (true/false)

```
config:# network services https [enabled <enabled>] [port <port>]
```

Configure HTTPS access

enabled	Enable/disable HTTPS access (true/false)
port	HTTPS access TCP port (1..65535)

```
config:# network services snmp [v1/v2c <v12enabled>] [v3 <v3enabled>]
[readCommunity <readcommunity>] [writeCommunity
<writecommunity>] [sysContact <syscontact>] [sysName <sysname>]
[sysLocation <syslocation>]
```

Configure SNMP settings

v1/v2c	Enable SNMP v1/v2c access (enable/disable)
v3	Enable SNMP v3 access (enable/disable)
readCommunity	SNMP read community string
writeCommunity	SNMP write community string

sysContact	MIB-II sysContact
sysName	MIB-II sysName
sysLocation	MIB-II sysLocation

config:# network services ssh [enabled <enabled>] [port <port>]
[authentication <authmode>]

Configure SSH access

enabled Enable/disable SSH access (true/false)

port SSH access TCP port (1..65535)

authentication Authentication type
(passwordOnly/publicKeyOnly/passwordOrPublicKey)

CLI: config password

config:# password

Then press Enter key. System will prompt for current password, new password, and confirm new password.

config:# apply

The password is changed if confirm password is correct.

CLI: config security

config:# security groupBasedAccessControl ipv4

security groupBasedAccessControl ipv4 [enabled <enable>]
[defaultPolicy <defpolicy>]

Configure group based access control settings for IPv4

enabled Enable group based access control (true/false)

defaultPolicy Default policy (allow/deny)

config:# security groupBasedAccessControl ipv6 [enabled <enable>]
[defaultPolicy <defpolicy>]

Configure group based access control settings for IPv6

enabled Enable group based access control (true/false)

defaultPolicy Default policy (allow/deny)

config:# security ipAccessControl ipv4

security ipAccessControl ipv4 [enabled <enable>] [defaultPolicyIn
<defpolicyin>] [defaultPolicyOut <defpolicyout>]

Configure IPv4 access control settings

enabled Enable IP access control (true/false)

defaultPolicyIn Default policy for inbound traffic
(accept/drop/reject)

defaultPolicyOut Default policy for outbound traffic
(accept/drop/reject)

config:# security ipAccessControl ipv6 [enabled <enable>]
[defaultPolicyIn <defpolicyin>] [defaultPolicyOut <defpolicyout>]

Configure IPv6 access control settings

enabled Enable IP access control (true/false)

defaultPolicyIn Default policy for inbound traffic
(accept/drop/reject)

defaultPolicyOut Default policy for outbound traffic
(accept/drop/reject)

config:# security loginLimits [singleLogin <singlelogin>] [passwordAging
<pwaging>] [passwordAgingInterval <pwaginginterval>] [idleTimeout
<idletimeout>]

Configure login limitations

singleLogin (enable/disable)	Prevent concurrent user login
passwordAging	Enable password aging (enable/disable)
passwordAgingInterval	Set password aging interval (in days) (7..365)
idleTimeout	Set user idle timeout (in minutes) (1..1440 or infinite)

```
config:# security restrictedServiceAgreement [enabled <enabled>]
[bannerContent]
```

Configure the Restricted Service Agreement banner

enabled (true/false)	Enable Restricted Service Agreement enforcement
bannerContent	The Restricted Service Agreement banner

```
config:# security strongPasswords [enabled <enable>]
[minimumLength <minlength>] [maxLength <maxlength>]
[enforceAtLeastOneLowerCaseCharacter <forcelower>]
[enforceAtLeastOneUpperCaseCharacter <forceupper>]
[enforceAtLeastOneNumericCharacter <forcenumeric>]
[enforceAtLeastOneSpecialCharacter <forcespecial>]
[passwordHistoryDepth <historydepth>]
```

Configure strong password requirements

enabled (true/false)	Enable strong passwords
minimumLength (8..32)	Minimum password length
maxLength (16..64)	Maximum password length
enforceAtLeastOneLowerCaseCharacter case character (enable/disable)	Enforce at least one lower case character
enforceAtLeastOneUpperCaseCharacter case character (enable/disable)	Enforce at least one upper case character
enforceAtLeastOneNumericCharacter numeric character (enable/disable)	Enforce at least one numeric character
enforceAtLeastOneSpecialCharacter character (enable/disable)	Enforce at least one special character
passwordHistoryDepth (1..12)	Password history depth

```
config:# security userBlocking [maximumNumberOfFailedLogins
<maxfails>] [blockTime <blocktime>]
```

Configure user blocking

maximumNumberOfFailedLogins Set maximum number of failed logins before blocking a user (3..10 or unlimited)

blockTime Set user block time (in minutes) (1..1440 or infinite)

CLI: config serial

```
config:# serial [consoleBaudRate <consolebps>] [modemBaudRate
<modembps>] [deviceDetectionType <detecttype>]
```

Configure serial port settings

consoleBaudRate Serial console baud rate (1200/2400/4800/9600/19200/38400/57600/115200)

modemBaudRate Modem baud rate (1200/2400/4800/9600/19200/38400/57600/115200)

deviceDetectionType Device detection mode (automatic/forceConsole/forceAnalogModem/forceGsmModem)

CLI: config terminalblock

```
config:# terminalblock [inputEnable <inputEnable>] [inputRemote
<inputRemote>] [inputLocal <inputLocal>] [outputEnable
<outputEnable>] [outputAction <outputAction>] [blinkInterval
<blinkInterval>]
```

Configure terminal block settings

inputEnable Enable/Disable input switch (enable/disable)

inputRemote Setup input remote console (fullAccess/videoOnly/noAccess)

inputLocal Setup input local console (fullAccess/videoOnly/noAccess)

outputEnable Enable/Disable output device (enable/disable)

outputAction Setup output action (deviceOff/deviceOn/blinkDevice)

blinkInterval Setup device blink interval(in half-seconds) (1..10)

CLI: config time

config:# time [method <method>] [zone] [autoDST <autodst>]

Configure date/time settings

method Time setup method (manual/ntp)

zone Select time zone

autoDST Automatic daylight saving time adjustment (enable/disable)

CLI: config user

config:# user create

user create [name <name>] [enabled <enabled>] [groups <groups>]

Create a new user

name User name

enabled User enabled state (true/false)

groups Groups (comma separated list of group names) (Admin)

- If user wants to create a new user "cccc" into groups "aaa" and "bbb bbb", you must use quotes around the group names, because spaces in the group names cannot be accepted. Example command:
 - user create name cccc enabled true groups "aaa/bbb bbb"

```
config:# user delete [name <name>]
```

Delete user

name User name (admin)

```
config:# user modify [name <name>] [password] [fullName <fullname>]
[telephoneNumber <telephone>] [eMailAddress <email>] [enabled
<enabled>] [forcePasswordChangeOnNextLogin <forcepwchange>]
[snmpV3Access <snmpv3>] [securityLevel <seclvl>]
[userPasswordAsAuthenticationPassphrase <pwauthpass>]
[authenticationPassPhrase]
[useAuthenticationPassPhraseAsPrivacyPassPhrase
<authpassasprivpass>] [privacyPassPhrase] [authenticationProtocol
<authproto>] [privacyProtocol <privproto>] [groups <groups>]
[sshPublicKey]
```

Create or edit user

name (admin)	User name
password password	Account
fullName	Full name
telephoneNumber number	Telephone
eMailAddress	E-mail address
enabled state (true/false)	User enabled
forcePasswordChangeOnNextLogin whether the user needs to change his password on next login (true/false)	Select
snmpV3Access SNMPv3 access (enable/disable)	Enable/disable
securityLevel level (noAuthNoPriv/authNoPriv/authPriv)	SNMPv3 security
userPasswordAsAuthenticationPassphrase as SNMPv3 authentication passphrase (true/false)	Use password
authenticationPassPhrase pass phrase	Authentication
useAuthenticationPassPhraseAsPrivacyPassPhrase authentication pass phrase as privacy pass phrase (true/false)	Use
privacyPassPhrase phrase	Privacy pass

authenticationProtocol protocol (MD5/SHA-1)	Authentication
privacyProtocol (DES/AES-128)	Privacy protocol
groups separated list of group names) (Admin)	Groups (Comma
sshPublicKey key	Set SSH public

CLI: connect

connect <port index> (1.1/1.2.../2.4)
See ***Supported CLI Commands*** (on page 15).

CLI: diag

diag

diag:# netstat

netstat <mode>

Netstat

mode Specify the netstat mode (ports/connections)

diag:# nslookup <host>

Name server query

host Host name or IP address to query DNS information for

diag:# ping <dest> [count <num_echos>] [size <packet_size>] [timeout
<timeout>]

Ping

dest Target host name or IP address

count Specify the number of echo requests to be sent (1..100) [5]

size Specify number of bytes in one request packet (1..65468) [56]

timeout Specify the maximum amount of time (in s) to wait for
responses (1..600)

diag:# traceroute <dest> [useICMP]

Trace route

dest Target host name or IP address

useICMP Use ICMP packets instead of UDP packets

CLI: reset

reset

reset

reset <command> [arguments...]

► **Available commands:**

factorydefaults Reset device to factory defaults

unit Reset and reboot device

reset factorydefaults

reset factorydefaults /y ...

Reset device to factory defaults

/y ... Assume 'yes' as answer to questions

reset unit /y ...

Reset and reboot device

/y ... Assume 'yes' as answer to questions

CLI: show

show

show <command> [arguments...]

► **Available commands:**

authentication	Shows info about authentication settings
connectedusers	Shows connected user information
device	Shows Device info.
eventlog	Shows event log
groups	Shows group information
history	Shows session command history
keyword	Shows configured serial port keywords
network	Shows all network information
security	Shows security settings
serial	Shows serial port parameters
terminalblock	Shows terminal block settings
time	Shows date/time information
user	Shows user information

```
# show authentication
```

```
Authentication type: Local
```

```
Configured LDAP servers:
```

```
# IP address  Server type
```

```
-----
```

```
No servers are currently configured.
```

```
Configured Radius servers:
```

```
# IP address  Authentication type  Ports (auth./acc.)
```

```
-----
```

```
No servers are currently configured.
```

```
#
```

```
# show connectedusers
```

```
-----
```

```
User Name      IP Address  Client Type  Idle Time
```

```
-----
```

```
Admin          192.168.0.200    Web GUI      0m
```

```
#
```

```
# show device
```

```
Device 'RemoteAccess-GATE'
```

```
Product:        RemoteAccess-GATE
```

```
Model:          RA-GATE
```

```
Firmware Version: 4.1.0.1.47281
```

```
Hardware ID:     3
```

```
Serial Number:   2C90700240
```

```
Internal Temperature Current Value: 36.3 C / 97.3 F
```

```
Internal Temperature Maximum Value: 38.8 C / 101.9 F
```

```
# show eventLog
```

```
Event Time      Event Class      Event Message
```

```

-----
-----
-----
2021-01-13 09:34:27 CET    User Activity  User 'Admin' from host
'192.168.0.200' logged in.
2021-01-13 09:42:31 CET    User Activity  User 'Admin' from host
'192.168.0.200' logged out.
2021-01-13 09:43:33 CET    User Activity  User 'Admin' from host
'192.168.0.200' logged in.

```

```
# show groups
```

```
Group 'Admin':
```

```
Description: System defined administrator group including all privileges.
```

```
Privileges:  adminPrivilege
```

```
# show keyword
```

```
Keyword: Example
```

```
Port: 1.1
```

```
# show network
```

```
DNS resolver
```

```
Server:          None
```

```
Search suffix:   None
```

```
Resolver preference: Prefer IPv6 addresses
```

```
Routing
```

```
IPv4
```

```
Default gateway:  None
```

```
Static routes:    None
```

```
IPv6
```

```
Default gateway:  None
```

```
Static routes:    None
```

Interface 'ETHERNET'

Link

Configured speed: Automatic

Configured duplex: Automatic

Link state: Autonegotiation On, 1 Gbit/s, Full Duplex, Link

OK

Authentication: No authentication

MAC address: 00:0d:5d:1b:65:f3

IPv4

Config method: Static

Address: 192.168.0.1/24

IPv6

Disabled

show security

IPv4 access control: Disabled

IPv6 access control: Disabled

Group based access control for IPv4: Disabled

Group based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login: No

Strong passwords: Disabled

Restricted Service Agreement: disabled

show serial

Configured console baud rate: 115200 bit/s

Configured modem baud rate: 115200 bit/s

Device detection type: Force console

Detected device: Console

show terminalblock

External input switch: Disabled

Current external switch state: Open

Give remote console user: Full Access

Give local console user: Full Access

External output device: Disabled

External device state: Disabled

Output action: Turn Device Off

Device blink interval: 1 (half-seconds)

show time

Device Time: 2021-01-13 09:41:23 CET

Time Zone: (UTC+01:00) Berlin

Setup Method: NTP synchronized

show user

User 'Admin':

Enabled: Yes

Groups: Admin

SNMP v3 Access: Disabled

CLI: exit

exit

exit

Appendix A Specifications

In This Chapter

TCP and UDP Ports Used	168
------------------------------	-----

TCP and UDP Ports Used

▶ Listening TCP Ports:

- * 80: http access (configurable)
- * 443: https access (configurable)
- * 22: SSH access (if enabled, configurable)
- * 68: DHCP access (if DHCP is enabled)

▶ Listening UDP Ports:

- * 162: SNMP access (if SNMP Agent is enabled)

▶ TCP Ports Outgoing:

- * 389: LDAP authentication (if LDAP is enabled, configurable)
- * 636: LDAPS/StartTLS (if LDAPS/StartTLS is enabled, configurable)
- * 25: SMTP (email) (if enabled)
- * 445: SMB (Windows File System) access (Remote ISO image access).

▶ UDP Ports Outgoing:

- * 514: Syslog (if enabled, configurable)
- * 1812: RADIUS authentication (if enabled, configurable)
- * 1813: RADIUS authentication (if enabled, configurable)

Index

A

- Absolute • 64
- Absolute Mouse Synchronization • 26
- Access a Virtual Media Drive on a Client Computer • 38
- Access a Virtual Media Image File • 39
- Active KVM Client (AKC) Help • 48
- Active System Partition • 141
- Active System Partitions • 140
- Add a Macro to the Toolbar • 60
- Add New Macro • 59
- Adjust Audio Settings • 46
- Adjust Full Screen Window Size to Target Resolution • 30, 33
- Adjusting Capture and Playback Buffer Size (Audio Settings) • 46
- Admin Group Special Privileges • 87, 88, 93
- AKC Supported Operating Systems • 48
- Allow Cookies • 48
- Audio Menu • 74
- Audio Playback Recommendations and Requirements • 42
- Audio Settings • 75
- Auto Play in Safari • 76

B

- Backup and Restore • 130
- Bandwidth Requirements • 42
- Build a New Macro • 21

C

- Change Your Password • 86
- CLI

- check • 145
- clear • 145
- config • 146
- config authentication • 147
- config device • 150
- config group • 151
- config network • 152
- config password • 154
- config security • 155
- config serial • 157
- config terminalblock • 157
- config time • 158
- config user • 158
- connect • 160
- diag • 161
- exit • 167
- reset • 134, 162
- show • 163
- CLI Commands • 145
- Client Launch Settings • 28, 34
- Client PC VM Prerequisites • 138
- Collect a Diagnostic Snapshot • 36
- Collecting a Diagnostic Snapshot of the Target • 36
- Conditions when Read/Write is Not Available • 39, 140
- Configuring Authentication • 79, 84, 85
- Connect Audio • 74
- Connect Drive Permissions (Linux) • 141
- Connect Drive Permissions (Mac) • 142
- Connect Files and Folders • 71
- Connect ISO • 73
- Connect to a Digital Audio Device • 44
- Connected Users • 86
- Connecting and Disconnecting from a Digital Audio Device • 44
- Connecting the Terminal Block to a Motherboard • 117
- Connection Info • 20, 55
- Connection Properties • 18, 20, 52
- Cursor Shape • 28

D

Date and Time • 96, 126
 Delete a Macro • 61
 Device Information • 94, 106
 Device Settings and Information • 94
 Diagnostics • 143
 Digital Audio • 41
 Digital Audio VKC and AKC Icons • 42
 Direct Port Access URL • 122
 Disable 'Protected Mode' • 48
 Disabling External Authentication • 86
 Disconnect from an Audio Device • 45
 Disconnect from Virtual Media Drives • 41
 Discovery Port • 108
 Dominion KX IV–101 Virtual Media
 Prerequisites • 138
 Download Diagnostic • 143
 Drive Partitions • 141
 Dual Mouse Modes • 26

E

Enter Intelligent Mouse Mode • 26
 Event Log • 110, 132
 Event Management • 98, 100, 103, 110
 Export Macros • 24
 External Device • 46
 External Device Menu • 76

F

Firmware History • 133
 Full Screen Mode • 38

G

Gathering LDAP/Radius Information • 78, 79, 81, 85
 General Settings • 30, 33
 Group Based Access Control • 118

H

HTML KVM Client (HKC) • 51
 HTTP/HTTPS Ports • 109

I

Import and Export Macros • 58, 62

Import Macros • 22
 Importing and Exporting Macros • 22
 Include Dominion KX IV–101 IP Address in
 'Trusted Sites Zone' • 48
 Initial Configuration • 134
 Input Menu • 56
 Installation and Initial Configuration • 1
 Intelligent • 65
 Intelligent Mouse Mode • 26
 Intelligent Mouse Synchronization Conditions
 • 27, 65, 67
 IP Access Control • 119

J

Java Requirements • 16

K

Keyboard • 20
 Keyboard Layout • 56
 Keyboard Limitations • 32
 Keyboard Macros • 21
 Keycode List • 89, 105
 KVM Clients • 3, 15
 KVM Security • 4, 115, 120

L

Latest Edge Chromium 86.0.622.51 • 49
 LDAP Authentication • 81
 Login Settings • 123

M

Macro Editor • 58
 Maintenance • 130
 Mapped Drives • 140
 Minimum Client and System
 Recommendations • 1, 2
 Mounting CD-ROM/DVD-ROM/ISO Images •
 40, 142
 Mounting Local Drives • 139
 Mouse Modes • 64
 Mouse Options • 25
 Mouse Sync • 66
 Mouse Synchronization Tips • 28

N

Network • 98, 106
 Network Diagnostics • 143
 Network Services • 108
 Number of Supported Virtual Media Drives • 140

O

Overview • 48, 137

P

Password Policy • 124
 Port Access • 3
 Port Access and Configuration • 3
 Port Configuration
 Custom EDIDs • 4, 12
 KVM Port Settings - General, Video, Audio • 4
 Local Port Monitor EDID • 13
 USB Connection Settings • 13
 Prerequisites for Using AKC • 48
 Prerequisites for Using Virtual Media • 138
 Proxy Server Configuration • 17, 49

R

Radius Authentication • 81, 85
 Refresh Screen • 68
 Refreshing the Screen • 24
 Returning User Group Information from Active Directory Server • 84
 Returning User Group Information via RADIUS • 86
 Root User Permission Requirement • 141

S

Saving Audio Settings • 44
 Scaling • 38
 Screenshot • 68
 Screenshot from Target Command (Target Screenshot) • 25
 Security • 78, 118
 Send Ctrl+Alt+Del Macro • 20
 Send Email • 99, 100

Send LeftAlt+Tab (Switch Between Open Windows on a Target Server) • 20
 Send Macro • 56
 Send Text to Target • 21, 63
 Serial Port • 113
 Service Agreement • 128
 Single • 66
 Single Mouse Mode • 29
 SMTP Server Settings • 100, 110
 SNMP Notifications • 99, 100
 SNMP Settings • 111, 136
 Specifications • 168
 SSH Settings • 90, 112
 Standard • 65
 Standard Mouse Mode • 28
 Supported Audio Device Formats • 42
 Supported Browsers • 1
 Supported CLI Commands • 160
 Supported Preferred Video Resolutions • 4, 6
 Supported Tasks Via Virtual Media • 139
 Supported Virtual Media Types • 139
 Synchronize Your Mouse • 28
 Syslog Messages • 99, 103

T

Target Server VM Prerequisites • 138
 TCP and UDP Ports Used • 168
 Terminal Block Control • 114, 121
 Tips for Accessing Dominion KX IV-101 With Dual Monitor Setups • 77
 TLS Certificate • 125
 Tool Options • 30, 38
 Tools Menu • 69

U

Unit Reset • 133
 Update Firmware • 134
 User Management • 78
 Users and Groups • 81, 87, 105, 106, 112, 114

V

Version Information - Virtual KVM Client • 47
 Video • 24
 Video Menu • 68
 View Menu • 69

[Index](#)

- View Options • 37
- View Status Bar • 37
- View Toolbar • 37
- Virtual KVM Client (VKCS) Help • 15
- Virtual Media • 38, 137
- Virtual Media File Server Setup (File Server
ISO Images Only) • 142
- Virtual Media in a Linux Environment • 140
- Virtual Media in a Mac Environment • 141
- Virtual Media Menu • 71
- Virtual Media Performance Recommendations
• 138
- Virtual Media Shared Images • 117



The manual is constantly updated and available on our website.

<https://gdsys.de/A9100376>

Guntermann & Drunck GmbH

Obere Leimbach 9
57074 Siegen

Germany

www.gdsys.de
sales@gdsys.de