



# G&D RemoteAccess-Workplace

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 2022. All rights reserved.

## Version 1.00 – 30/03/2022

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.com](http://www.gdsys.com)

[sales@gdsys.com](mailto:sales@gdsys.com)

# Contents

<b>Introduction</b>	<b>1</b>
Introduction to the Software .....	1
Login Screen .....	1
Main Menu, Port Navigator, Toolbar .....	2
Help on Hotkeys .....	3
<b>Getting Started</b>	<b>6</b>
Use the KVM Client .....	6
<b>Managing RemoteAccess-GATEs and Ports</b>	<b>10</b>
RemoteAccess-Workplace Configuration.....	10
Adding RemoteAccess-GATEs .....	12
Editing RemoteAccess-GATEs .....	13
Deleting RemoteAccess-GATEs .....	14
Importing RemoteAccess-GATEs.....	15
Bulk Import Examples .....	17
Configuring KVM Ports.....	17
Unavailable Hotkeys for Port Access .....	20
Port Data Retrieval Status .....	21
<b>Managing Targets and Access Methods</b>	<b>22</b>
Adding Targets and Access Methods .....	23
SSH, VNC, and RDP Access .....	24
WEB Access.....	25
ESXi Access .....	26
Multi KVM Access with RemoteAccess-GATEs .....	27
Editing and Deleting Targets and Access Methods .....	29
Configuring Access Settings .....	30
Known Limitations on Targets .....	33

<b>Navigation and Access</b>	<b>34</b>
Port Navigator .....	35
Identifying States of RemoteAccess-GATEs and Ports .....	39
Identifying External Media.....	40
Dual Video Port Status .....	40
Using Search .....	41
Using Filters .....	41
 <b>Port Scanner</b>	 <b>44</b>
Operating the Port Scanner .....	45
Scanner Options .....	47
Port Scanner Settings .....	48
Port Scanner Grid View .....	51
 <b>Using the KVM Client</b>	 <b>52</b>
Connection Properties.....	53
Default Connection Properties .....	55
Text Readability.....	56
Color Accuracy .....	56
Video Mode .....	56
Noise Filter.....	57
Keyboard Macros.....	57
Mouse Settings .....	58
Synchronize Mouse .....	59
Single Mouse Cursor .....	59
Dual Mouse Modes.....	60
Mouse Synchronization Tips .....	62
Video Settings .....	63
Advanced Video Settings .....	65
Advanced Color Settings.....	67
Peripheral Devices and USB Settings.....	68
Audio Device .....	70
Virtual Media .....	72
Disconnecting a Virtual Device .....	78
USB Profiles .....	79
External Device Control.....	81

View Settings .....	82
Fit window to Target .....	82
Retain Window Size .....	82
Scale Video .....	83
Show Window Decorations .....	83
Full-Screen Mode .....	83
Cursor Shape .....	84
Window Management .....	84
Dual Video Port Connections .....	86

## Setting User Preferences 87

---

Access Client Settings .....	88
Single Mouse Mode for Dual Monitor Targets .....	93
Managing Keyboard Macros .....	93
Executing Macros .....	95
Editing or Deleting Macros .....	96
Keyboard Macro Example .....	96
Audio Settings .....	97
Hotkeys and Gestures .....	98
Move Keys .....	100
Switch Keys .....	101
Window Layouts .....	101
Port Scanner Settings .....	103
Change Password .....	106

## Administration Features 107

---

Users .....	108
Editing or Deleting Users .....	110
User Groups .....	111
Privileges .....	113
Editing or Deleting User Groups .....	114
Autologin .....	115
LDAP .....	116
Adding LDAP Servers .....	117
Enabling or Disabling the LDAP Authentication .....	126
Searching for LDAP Users and Groups .....	127
Configuring the Maximum Search Results and Local Authentication Settings .....	129
Logging in with LDAP .....	130
LDAP Login Failure Message .....	130
Trusted Certificates .....	131
Removing an Installed Certificate .....	132
Certificate Failure Messages .....	133

## Contents

Server Certificate .....	134
Import Private Key and Certificate .....	135
Create Self Signed .....	136
Security Settings.....	138
Enable/Disable FIPS Mode and Certificate Settings .....	138
Strong Password Settings .....	139
User Blocking.....	142
Restricted Service Agreement.....	143
Display Settings .....	144
Customization.....	146
Customization Example .....	149
Remote Control .....	149
Remote Control via Web Browser .....	150
Remote Control via API.....	151
Keyboard/Mouse Sharing.....	154
Keyboard/Mouse Sharing in Single Cursor Mode .....	156
Configuring Keyboard/Mouse Sharing .....	156
Language Settings.....	159

## Maintenance Features 161

---

Event Log .....	162
Event Type and Description .....	163
Event Log Archives.....	163
Backup and Restore .....	167
Exporting and Importing Backup Files.....	168
Deleting Backup Files.....	168
Factory Reset.....	169
Software Update .....	170
Support .....	172
Support Login.....	172
Log Level for Diagnostic Log Files .....	173
Diagnostic Log File .....	174
About this Device .....	175

## System Settings 176

---

Date/Time .....	176
Time Zone.....	178
Keyboard.....	179
Keyboard Layouts.....	179
Mouse Keys .....	181
Monitor.....	182
Mouse .....	184

Network .....	185
Network Connections - Ethernet.....	185
Network Connections - Bond Connections .....	197
OpenVPN Connections .....	199
Default Shortcut Icons in the Main Toolbar .....	203
Keyboard Layout Icon.....	203
Volume Icon.....	203
Network Icon .....	203
Clock Icon.....	205
Location and Clock Time Format.....	207
<b>Additional Features</b>	<b>210</b>
Screen Unlocking .....	210
Factory Reset at Startup .....	210
Take a Screenshot.....	211
<b>Authentication of RemoteAccess-Workplaces and RemoteAccess-GATEs</b>	<b>212</b>
<b>Open Ports Recommendations</b>	<b>214</b>
<b>API</b>	<b>215</b>
Session Management .....	215
Session Creation and Login .....	215
Parameters .....	215
Response.....	215
Login Progress .....	216
Parameters .....	216
Response.....	216
Session Close / Logout.....	216
Parameters .....	216
Response.....	217
Example.....	217
Access Functionality.....	217
Get Devices and Targets .....	217
Get Devices and Ports.....	218
Get Targets and Access Points .....	219

## Contents

Handling of Access Client Sessions .....	220
Create Access Client Sessions .....	220
Close Access Client.....	220
Named Scenes (aka Window Layouts).....	221
Restore a Named Scene .....	221
Window Management.....	222
Maintenance .....	222
Identity Information.....	222
Firmware Operations .....	223
Firmware Update .....	223
Backup/Restore .....	224



# Introduction

This chapter introduces the RemoteAccess-Workplace.

## In This Chapter

Introduction to the Software ..... 1

---

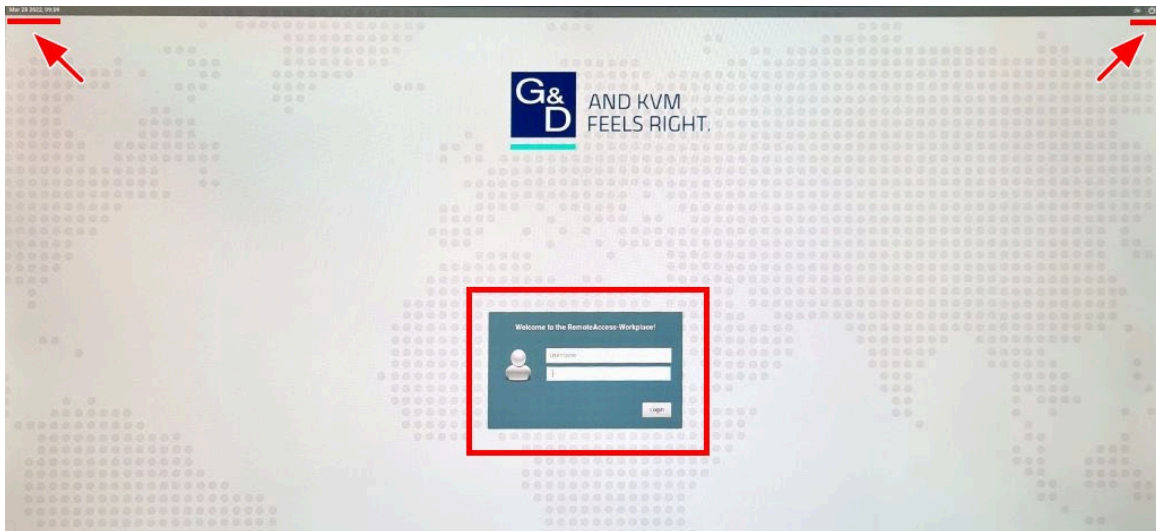
### Introduction to the Software



After powering on the RemoteAccess-Workplace, the Login Screen is shown.

After successfully logging in to the RemoteAccess-Workplace, the Main Screen displays.

---

#### Login Screen



- System date and time
-  Keyboard language (default DE German) and  Restart or Shut Down
- Login: The login icon indicates the authentication type being used: Local (grey icon) or LDAP (green icon).
- A local authentication checkbox is available whenever the username "admin" is entered, and when "Allow access for local users" is enabled in LDAP integration mode.

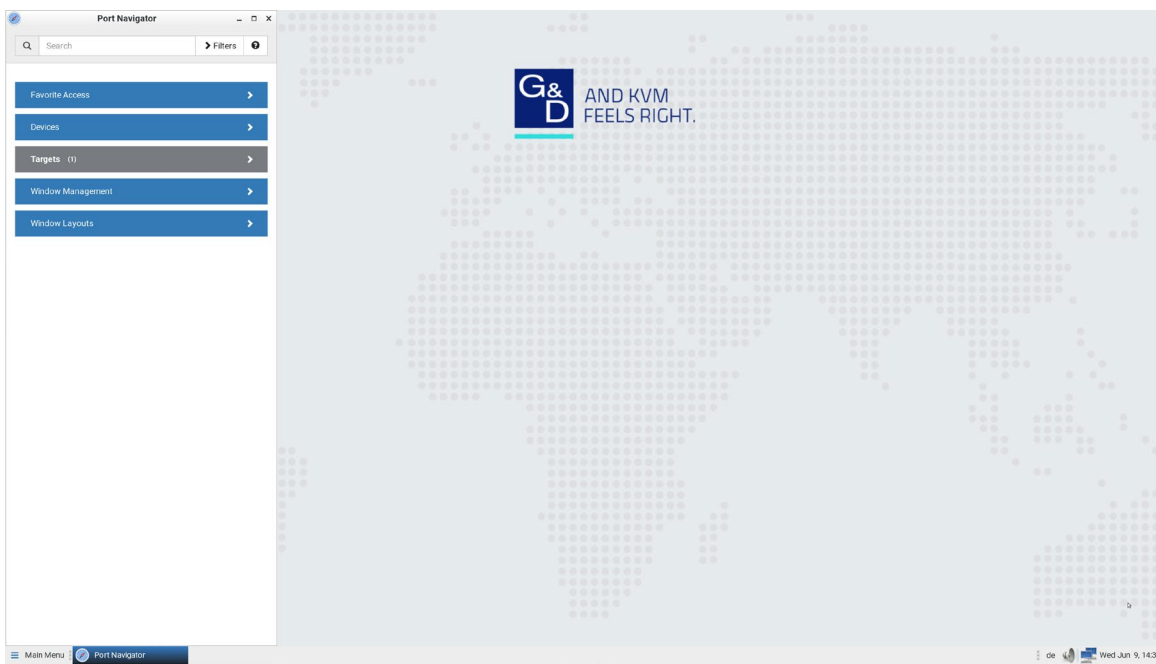
---

### Main Menu, Port Navigator, Toolbar

The screen displayed after login is the Main Screen. When logging in for the first time, a welcome message is displayed.

The Main Menu and toolbar is located at the bottom of this screen. This toolbar shows the Main Menu, shortcut icons and lists any open RemoteAccess-Workplace and KVM Client windows.

The Port Navigator opens by default, and can be closed then re-opened from the Main Menu.




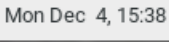


- **Main Menu:**  
This menu contains the primary RemoteAccess-Workplace commands and system settings.
- **Open window(s):**  
If any window is launched, its name is shown in the Toolbar. In the above diagram, only the Port Navigator window is launched.  
You can right-click any open window in the Toolbar to minimize, maximize, move, resize and so on.
- **Shortcut icons for viewing/configuring system settings:**  
Hover your mouse pointer over an icon to view information, or click or right-click it to configure settings.

---

*Note: The above diagram shows factory default icons. More icons may be available if you change any system settings. For example, **Monitor** (on page 182).*

---

Default icons	Description
	The Keyboard Layout icon indicates the current keyboard layout. The default is <i>de</i> (German). See <b>Keyboard Layout Icon</b> (on page 203).
	This icon controls the volume. See <b>Volume Icon</b> (on page 203).
	This icon shows or configures the network information. See <b>Network Icon</b> (on page 203).
	The Clock icon indicates the day of the week, date and current time. See <b>Clock Icon</b> (on page 205).

---

### Help on Hotkeys

You can also access this list of pre-programmed and user-configurable hot keys for the RemoteAccess-Workplace in the Main Menu.

- Choose Main Menu > Help > Help on Hotkeys.

### ► Hotkeys in the RemoteAccess-Workplace

RemoteAccess-Workplace has a number of pre-defined and user configurable hotkeys implemented to open tools, move or resize windows, open target windows or perform some operations.

Most of the desktop hotkeys can be configured by the user (Preferences > Hotkeys), including the possibility to disable them. The key combinations listed below are the factory defaults for these hotkeys. This guide does not mention operations whose hotkeys are disabled by default.

### ► RemoteAccess-Workplace Functions

- Ctrl + Alt + N  
Launch the RemoteAccess-Workplace Port Navigator
- Ctrl + Alt + C  
Launch the RemoteAccess-Workplace Configuration
- Ctrl + Alt + L  
Lock the RemoteAccess-Workplace Screen
- Ctrl + Alt + Del  
Shut down or restart the RemoteAccess-Workplace

## ► Window Management Functions

The following hotkeys are useful to close the currently active window or switch between windows.

- Alt + F4  
Close the active window.
- Alt + Tab  
Switch focus to the next window.
- Shift+Alt+Tab  
Switch focus to the previous window.

The next keys are used to move and resize the open windows and switch between windows. They are not configurable individually but can be enabled or disabled globally. Note that the keypad keys are functional independently of the status of Num Lock. Keypad 4, 6, 8, 2 act as Left, Right, Up and Down respectively.

- Shift+Win + [Left/Right/Up/Down]  
Switch focus to the window in the direction specified of the currently focused window.
- Ctrl+Alt+Shift+[Left/Right]  
Move the active window to the previous/next monitor.
- Ctrl+Alt+[Left/Right/Up/Down]  
Move the active window to the left/right/top/bottom edge of the current monitor.
- Ctrl+Alt+[Keypad-1/3/9/7]  
Move the active window to the corners of the current monitor.
- Ctrl+Shift+[Left/Right/Up/Down]  
Move the active window to the nearest edge in the direction specified.
- Ctrl+Windows + [Left/Right/Up/Down]  
Grows the active window until it touches the nearest edge in the direction specified.  
Edges are the outer edges of the other windows, monitor edges in multi monitor setups, or the desktop boundaries. If the window edge is at the screen edge already, it is shrunk instead.
- Alt+Windows + [Left/Right/Up/Down]  
Shrinks the active window until it touches the nearest edge in the direction specified. Edges are the outer edges of the other windows, monitor edges in multi monitor setups, or the desktop boundaries. If no edge is found, the window is halved in size.

### ► Access Client Functions

The following hotkeys are only available during a running target connection.

- Control Alt M  
Leave Single Cursor Mode (KVM Clients only). Only available if in single cursor mode. Single cursor mode not available if the hotkey is disabled.
- Ctrl + Alt+ F  
Enter or leave full screen mode on KVM and VNC Clients.
- Alt + Enter  
Enter or leave full screen mode on RDP clients.
- F11  
Leave full screen mode in SSH, Serial, or ESXi clients.

### ► Target Hotkeys

You can configure target hotkeys for quick access to KVM ports or other targets. For KVM ports, open the Configuration, select a RemoteAccess-GATE, select a port, and click Edit Preferences. For other targets, select Targets, choose an Access Point to this target, then click Edit Preferences. Select the hotkey you want to use for this port and click OK.

Options include:

- Ctrl+Shift +<F key>
- Ctrl+Shift +<letter>
- Ctrl+Alt+<number>
- Ctrl+Alt+<letter>
- Shift + Alt + <F key>
- Shift + Alt + <letter>
- Ctrl+Shift+Alt+<F key>
- Ctrl + Shift +Alt + <letter>

---

*Notes: A few hotkey combinations might be overridden by the RemoteAccess-Workplace system. Test all hotkey combinations to make sure they work properly.*

*Key combinations configured for RemoteAccess-Workplace Functions or Access Client Functions cannot be used as Target Hotkeys.*

---

# Getting Started

This chapter explains how to use the KVM Client.

---






## Use the KVM Client



The KVM Client window opens after accessing a port. The video of the target server that is connected to the port is displayed in the KVM Client. You can use the attached keyboard and mouse to control the target server.










The toolbar is split into two groups.

The left group comprises the following buttons that you can use to change settings and properties.


Button	Function
	<p><b>Connection Properties:</b></p> <p>Manages streaming video performance over <i>your</i> connection to the target server. The settings are stored persistently for the accessed port.</p> <p>Show information like FPS and video resolution.</p> <p>The factory default settings are ideal for most connections so it is not recommended to change the settings unless required.</p>
	<p><b>Keyboard:</b></p> <p>Shows a list of available hot key macros and sends the selected macro to the target server.</p>
	<p><b>Mouse:</b></p> <p>Switches between single mouse and various dual mouse modes, or synchronizes two mouse pointers onscreen.</p>
	<p><b>Video Settings:</b></p> <p>Adjusts video sensing and color calibration settings.</p>
	<p><b>Connect Audio, Mass Storage and SmartCard Devices:</b></p> <p>Connects or disconnects a virtual media drive or a smart card reader from the target server, if the target supports virtual media.</p> <p>For example, you can mount a CD-ROM or USB flash drive onto the target server.</p> <p>In addition, you can configure the audio connection to the target server.</p>

Button	Function
	<b>External Device Settings:</b> Access the settings for operating an external device.
	<b>View:</b> Shows several display options, such as Scale Video and Full-Screen Mode.

The right group comprises the following shortcut buttons for frequently-used functions. These functions are also available in the left group, but the shortcut buttons allow quick access with a click.

Button	Function
	<b>Synchronize Mouse:</b> Forces the target server's mouse pointer to align with the RemoteAccess-Workplace's in the dual mouse modes.
	<b>Auto-sense Video:</b> Forces the video re-sensing to adjust the video display.
	<b>Send Ctrl+Alt+Del:</b> Sends the hot key <i>Ctrl+Alt+Del</i> to the target server to ensure it is interpreted by that server.
	<b>Full-Screen Mode:</b> Displays the target server's video in full screen. Press <i>Ctrl+Alt+F</i> to quit the Full-Screen mode.
	<b>Fit window to Target:</b> Resizes the KVM Client window to the target server's desktop video.
	<b>Mute audio</b> Mute or unmute audio.
	<b>Mute microphone</b> Mute or unmute microphone.



Button	Function
	<b>Num Caps Scroll:</b> Displays the status of Num Lock, Caps Lock, and Scroll. Active functions are in bold text

For detailed information on the toolbar buttons, see *Using the KVM Client* (on page 52).

#### Automatic Reconnection

If your connection to the client fails, an automatic reconnection will be attempted in most cases. Reconnection is attempted at 30 second intervals until a successful connection is made.

A message appears when the connection drops with information about reconnection timing and options to cancel or quit.

Automatic reconnection is not attempted when the connection failure is due to:

- Configuration error detected. Certificate must be uploaded.
- User authentication failed.
- User authorization failed.
- User has been actively disconnected by an administrator.
- RemoteAccess-GATE version not supported by the client.

# Managing RemoteAccess-GATEs and Ports

RemoteAccess-GATEs and their KVM ports are managed in the RemoteAccess-Workplace Configuration window.

## In This Chapter

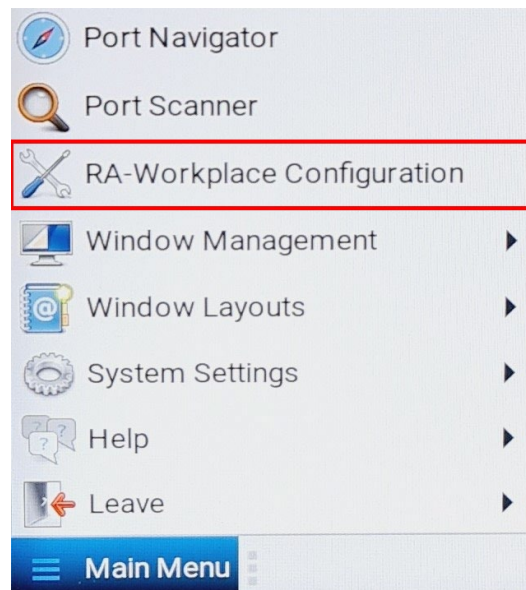
RemoteAccess-Workplace Configuration.....	10
Adding RemoteAccess-GATEs .....	12
Editing RemoteAccess-GATEs .....	13
Deleting RemoteAccess-GATEs.....	14
Importing RemoteAccess-GATEs.....	15
Configuring KVM Ports.....	17

---

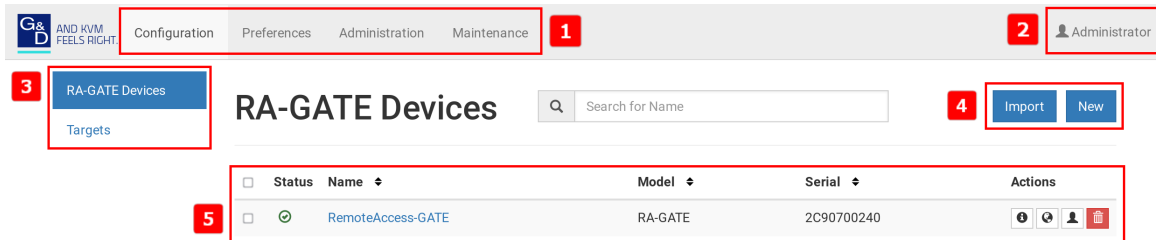
## RemoteAccess-Workplace Configuration

### ► To launch the RemoteAccess-Workplace Configuration window:

- Press *Ctrl+Alt+C*.
- OR choose Main Menu > RemoteAccess-Workplace Configuration.



The RemoteAccess-Workplace Configuration window opens.



#### 1. Configuration tabs:

- *Configuration*: Manage RemoteAccess-GATEs and Targets. See the other sections in this chapter.
- *Preferences*: Set personal preferences, such as audio settings. See **Setting User Preferences** (on page 87).
- *Administration*: Manage administration tasks. See **Administration Features** (on page 107).
- *Maintenance*: Manage maintenance tasks. See **Maintenance Features** (on page 161).

#### 2. Your user account:

Click to view your user account settings.

#### 3. RemoteAccess-GATEs and Targets options:

- *RemoteAccess-GATEs*: Add or Import RemoteAccess-GATEs and manage them.
- *Targets*: Add and manage Targets. See **Managing Targets and Access Methods** (on page 22).

#### 4. Import button and New button:

- By default, the RemoteAccess-GATE option is selected, and you can use the Import and New buttons to add or import RemoteAccess-GATEs. See **Adding RemoteAccess-GATEs** (on page 12) See **Importing RemoteAccess-GATEs** (on page 15).
- When the Targets option is selected, you can use the New button to add targets and access. Import is not available.

#### 5. A list of added RemoteAccess-GATEs:

- When the RemoteAccess-GATE option is selected, view the list of RemoteAccess-GATEs here, and click the desired RemoteAccess-GATE to show all of its KVM ports and details.
- When the Targets option is selected, view the list of Targets here, and click a Target to show its access methods and details.

---

## Adding RemoteAccess-GATEs

All RemoteAccess-GATEs added to this RemoteAccess-Workplace can be seen by all users who log in to this RemoteAccess-Workplace although they can only access those switches if they have provided proper user credentials. If users, RemoteAccess-GATEs, and the RemoteAccess-Workplace exist in the same LDAP environment, you can add your RemoteAccess-GATEs with single sign-on capability.

► **To add a RemoteAccess-GATE:**

1. Click New in the RemoteAccess-Workplace Configuration window. See *RemoteAccess-Workplace Configuration* (on page 10).
2. The following page opens, and the user must enter the required information. See *Step 3: Add RemoteAccess-GATEs*.

The screenshot shows a web-based configuration form for adding a RemoteAccess-GATE. The form is divided into four main sections: Network Address, Port Numbers, Authentication, and User Credentials. Each section contains input fields and informational text boxes.

- Network Address:** Contains a text input field for "\* IP Address / Hostname". A blue informational box states: "The given device will be added to the system-wide database of devices and hence its record can be seen and used by other users."
- Port Numbers:** Contains two text input fields. The first is labeled "Discovery Port" and has the value "5000". The second is labeled "HTTPS Port" and has the value "443".
- Authentication:** Contains a dropdown menu for "Method" with "Normal" selected. A blue informational box explains: "If **Authentication Method** is set to *Normal*, then each user must specify their credentials to gain access to this device. If the device and the RA-Workplace are using the same authentication service and **Authentication Method** is set accordingly then RA-Workplace will try to reuse the credentials provided at its login for accessing this device."
- User Credentials:** Contains two text input fields. The first is labeled "\* Name" and the second is labeled "\* Password". A blue informational box states: "These credentials are used to query for port information of the RA-GATE Device. The credentials are not shared with other users and hence must be provided by each user individually."

At the bottom of the form, there are two buttons: "Save" (in a blue box) and "Cancel" (in a white box with a grey border).

3. Click Save, and the new RemoteAccess-GATE's content is shown.

---

**Important:** If "Allow LDAP Single Sign-on" is enabled, LDAP users can omit entering credentials in favor of their LDAP credentials being used. Otherwise, user credentials for a RemoteAccess-GATE are saved on a per-user basis. Other users must enter and save their own user credentials for the RemoteAccess-GATE you added. See *Editing RemoteAccess-GATEs* (on page 13).

---

## Editing RemoteAccess-GATEs

Added RemoteAccess-GATEs are listed in the RemoteAccess-Workplace Configuration window.





Each RemoteAccess-GATE has three icons in the Actions column. You must have Device Administration privileges to delete, edit or add RemoteAccess-GATEs.

If you are not the one who added new RemoteAccess-GATEs to the RemoteAccess-Workplace, you must follow the procedure below to enter user credentials for newly-added RemoteAccess-GATEs.

---

*Note:* For the difference between a RemoteAccess-GATE's and the RemoteAccess-Workplace's user credentials, see **Authentication of RemoteAccess-Workplaces and RemoteAccess-GATEs** (on page 212).

---


Name ↕	Model ↕	Serial ↕	Actions
RemoteAccess-GATE	RA-GATE	2C90700240	   




► **To view the RemoteAccess-GATE's ports:**

- Click the desired RemoteAccess-GATE. The ports list opens. See *Configuring KVM Ports* (on page 17).


► **To change the RemoteAccess-GATE's IP address/host name or authentication method:**

1. Click the desired RemoteAccess-GATE's  button.
2. Click Edit to open the Edit RemoteAccess-GATE page.
3. Modify the IP address or host name, discovery and HTTPs ports, or change the authentication method. See **Adding RemoteAccess-GATEs** (on page 12).
4. Click Save.

► To open the RemoteAccess-GATE's administration page:

1. Click the desired RemoteAccess-GATE's  button.
2. The administration page launches. Login to access.




► To enter new user credentials for a RemoteAccess-GATE:

1. Click the  button of the desired RemoteAccess-GATE.
2. Enter new user credentials.
3. Click Save.


*Note: If you enter incorrect user credentials for a RemoteAccess-GATE, you may be blocked if User Blocking has been enabled on that RemoteAccess-GATE and too many incorrect attempts are made. When this occurs, contact the RemoteAccess-GATE's system administrator for help.*

## Deleting RemoteAccess-GATEs

The final button in the Actions column is used to delete this RemoteAccess-GATE.






Name ▾	Model ▾	Serial ▾	Actions
RemoteAccess-GATE	RA-GATE	2C90700240	   

► To delete a RemoteAccess-GATE:

1. Click the desired RemoteAccess-GATE's  button.
2. Click OK on the confirmation message.

► To delete multiple RemoteAccess-GATEs:

## RA-GATE Devices

<div>1</div> <input checked="" type="checkbox"/>	Status	Name ▾	Model ▾	Serial ▾	Actions
<input checked="" type="checkbox"/>		RemoteAccess-GATE	RA-GATE	2C90700240	   

2

---

## Importing RemoteAccess-GATEs

Bulk Import and Update allows you to add or update multiple RemoteAccess-GATEs at once using a CSV file found in the root folder of a connected USB storage device.

When you import, RemoteAccess-Workplace adds devices detected as new by their IP address/hostname. RemoteAccess-Workplace uses the credentials given in the CSV file. If credentials are blank in the file, none are added. When RemoteAccess-Workplace detects that a device identified in the CSV file already exists in the system, the import updates the credentials as given in the CSV. You can also optionally specify customized Discovery port and HTTPS port for each device.

### ► CSV file format:

The CSV file contains 5 columns: <ip address or hostname>, <username>, <password>, <discoveryport>, <HTTPSport>

---

*Note: Username and password are optional. If not imported, user must enter them later. Discovery port and HTTPS port are optional. If they are not specified, the default ports 5000 and 443 are used.*

---

See **Bulk Import Examples** (on page 17) for more details and limitations.

### ► To import RemoteAccess-GATEs:

1. Click Import in the RemoteAccess-Workplace Configuration window. See **RemoteAccess-Workplace Configuration** (on page 10). The Bulk Import/Update RemoteAccess-GATEs page opens.
2. The Storage list displays all CSV files found in the root folder of connected USB storage devices.

## Bulk Import / Update RA-GATE Devices

This dialog supports adding and updating many RA-GATE Devices at once via CSV-file.

On adding, devices are inserted into the system's database with their IP-address / hostname and optionally with credentials for the user who initiates the operation.

On updating, credentials of the initiating user can be updated or added for devices which are already part of the system.

The CSV-record format is as follows:

```
<hostname>,<username>,<password>,<discovery port>,<https port>
```

Example:

```
mydevice,admin,pass123,5000,443
```

Note: The credentials and port numbers are optional.

USB Storage	File Name	Size
DISK_IMG	import.csv	5 Bytes

Cancel

- Click the file you want to import. The Bulk Import page opens to display the file details:
  - File name and size
  - Errors, if any, with line number if appropriate
  - Total number of RemoteAccess-GATEs to be added
  - Number of RemoteAccess-GATEs to be added without credentials
  - Number of RemoteAccess-GATEs to be updated with new credentials
  - Number of RemoteAccess-GATEs to be updated by overwriting existing credentials

---

*Note: If errors are listed, the import button is disabled. Correct the file and try again.*

---



4. Click Start the Import/Update in the details dialog. Import progress shows in the dialog. When complete, a success message appears in the main page.

---

### Bulk Import Examples

#### ► Import / update listed RemoteAccess-GATEs:

```
192.168.2.104,Admin,4658
192.168.2.103,thomas,thomas,5000,443
192.168.5.52,user,password
```

#### ► Special characters and escaping

Line 1 is an example of using comma in a value.

Line 2 is an example for escaping ", the resulting password string is "password"

```
192.168.2.104,Admin,"46,58"
192.168.5.52,user,"""password"""
```

---

*Note: If you create the CSV file using Microsoft Excel or similar tools, you do not need to escape special characters. These tools handle the special characters automatically when creating the CSV file. Check the resulting CSV file if you are not sure.*

---

#### ► Commenting out

Use the hashtag character (#) in the first position of a line to comment out the line. Hostnames are not allowed to contain #.

```
192.168.2.104,Admin,4658
#192.168.2.103,thomas,thomas,5000,443
192.168.5.52,user,password
```





---

## Configuring KVM Ports


A RemoteAccess-GATE's ports are shown after a RemoteAccess-GATE is selected.



#### ► To configure a KVM port:

1. Click the desired RemoteAccess-GATE, and all of its KVM ports are listed on the screen. Note, to return to the devices view, click the Back to all RemoteAccess-GATEs link


-  The KVM port has been configured as a favorite port.
-  The port is included in Port Scanner.
-  The port is configured to automatically connect to audio when the connection launches.
-  The port is configured to automatically connect to microphone when the connection launches.
- The icon shown in the top-right corner of the Ports section indicates the KVM port information retrieval status. In this example, there is a green checkmark. See *Port Data Retrieval Status* (on page 21).

### Ports of RemoteAccess-GATE

New RA-GATE Device 

Name		No.	Type	Status	Availability	Hotkey	Action
RemoteAccess-GATE_Port1		1	VM	up	idle		

Back to all RA-GATE Devices

- Click  in the Action column of the port that you want to configure. A settings page opens.
- Configure the General Settings:

#### General Settings

☒ Hotkey

Ctrl+Alt

+

A

☒ Favorite

☐ Automatically connect Speaker

☐ Automatically connect Microphone

☐ Include in Port Scanner

You can assign a Hotkey for quickly accessing this KVM Port or Access Point.  
**Note:** Keypad keys are not recognized. Please use regular number keys only.

Checkbox	Function
Hotkey	<p>Assign a hotkey combination for quickly accessing this KVM port. Available options include:</p> <ul style="list-style-type: none"> <li>▪ <i>Ctrl + Shift + &lt;character&gt;</i></li> <li>▪ <i>Ctrl + Alt + &lt;character&gt;</i></li> <li>▪ <i>Shift + Alt + &lt;character&gt;</i></li> <li>▪ <i>Ctrl + Shift + Alt + &lt;character&gt;</i></li> </ul> <p>&lt;character&gt; is an alphanumeric character or function key.</p> <p>Some hotkey combinations cannot be used for port access and thus are not available. See <b><i>Unavailable Hotkeys for Port Access</i></b> (on page 20).</p>
Favorite	<p>If this checkbox is selected, this KVM port is shown in the Favorite Access panel. See <b><i>Port Navigator</i></b> (on page 35).</p>
Automatically connect Speaker	<p>Speaker will automatically be connected to this port at target launch.</p>
Automatically connect Microphone	<p>Microphone will automatically be connected to this port at target launch.</p>
Include in Port Scanner	<p>Add the port to the port scanner. See <b><i>Port Scanner</i></b> (on page 44).</p>

4. Configure the Target Window Settings if you want to override default settings.
  - To view your default target window settings, click the Access Client Settings button. See ***Access Client Settings*** (on page 88) for details on each.
  - If you want to override any of those settings for the port you are configuring, select the "Use port specific Access Client Settings" checkbox to enable the list.
  - Select the checkbox for each setting that should override the default setting.

Target Window Settings

☐ Use specific Target Window Settings

☒ Scale Video  
☒ Window Decorations  
☒ Show Tool Bar  
☒ Full-Screen Mode  
☐ Start in Single Mouse Cursor Mode  

Cursor Shape (in Double Cursor Mode)
 

Transparent

☒ Disable Banner Messages

By default, RemoteAccess-Workplace uses Target Window Settings which are valid for all ports and access points. However, here you can override these settings for this specific port or access point by checking **Use specific Target Window Settings**.

Adjust the default settings via the Access Client Settings dialog:

Access Client Settings

**Notes:**

- These setting don't apply to already active target sessions.
- To leave Full-Screen Mode, press the Full-Screen hotkey (**Ctrl+Alt+F** by default) in the Client.

5. Click Save.

## Unavailable Hotkeys for Port Access

The following hotkey combinations are not available for accessing KVM ports.

Unavailable hot keys	Notes
Ctrl + Shift + <number>	<number> = 0 to 9
Ctrl + Shift + Alt + <number>	
Shift + Alt + <number>	
Ctrl + Alt + <function_key>	<function_key> = F1 to F12
Ctrl + Alt + C Ctrl + Alt + F Ctrl + Alt + L Ctrl + Alt + M Ctrl + Alt + N	These hotkeys can be used if you first disable them as RemoteAccess-Workplace hotkeys. See Hotkeys for Controlling the RemoteAccess-Workplace.

Besides, you must NOT use the hotkeys specified in the Desktop Settings for port access. See Desktop Settings.





### Port Data Retrieval Status

An icon is displayed in the top-right corner of the Ports section in the RemoteAccess-Workplace Configuration window. This icon indicates the data retrieval status of the KVM ports on the selected RemoteAccess-GATE.

## Ports of RemoteAccess-GATE

New RA-GATE Device






Name		No.	Type	Status	Availability	Hotkey	Action
RemoteAccess-GATE_Port1	  	1	VM	up	idle		

Back to all RA-GATE Devices

Click this icon to view additional information.

The icon changes depending on the current retrieval status of KVM port information.

Icon	Port data retrieval state
	Port information on the selected RemoteAccess-GATE is accessible.
	Port information on the selected RemoteAccess-GATE is NOT accessible. Possible causes may include: <ul style="list-style-type: none"><li>▪ Incorrect user credentials are entered for the RemoteAccess-GATE.</li><li>▪ The presented certificate of the device cannot be verified, when certificate checking is enabled</li><li>▪ Network connectivity issues. For example, the selected RemoteAccess-GATE is not connected to the network.</li></ul>
	Port information on the selected RemoteAccess-GATE is NOT accessible because NO user credentials have been entered for this RemoteAccess-GATE. See <i><b>Editing RemoteAccess-GATEs</b></i> (on page 13).

The port data retrieval status will affect the device and port status shown in the Port Navigator window. See ***Identifying States of RemoteAccess-GATEs and Ports*** (on page 39).

# Managing Targets and Access Methods

Targets and Access methods are managed in the RemoteAccess-Workplace Configuration window. See ***RemoteAccess-Workplace Configuration*** (on page 10).

The Targets and Access methods feature offers different ways to view, manage, and connect to targets, using KVM port access, as well as RDP, SSH, and VNC. Additionally, you can add access to a Web application or ESXi virtual machine. You can configure these additional access methods for any KVM target. You can also configure access methods to reach a non-KVM target device or system that is directly connected to your network. These targets can be any device or system that can be remotely accessed by RemoteAccess-Workplace, such as a server, network switch, HVAC or other. Finally, the Dual KVM access method makes it possible to configure two RemoteAccess-GATE KVM ports into a virtual Dual Monitor KVM target in which the two independent ports are treated as if they were part of a dual monitor port group.

When a RemoteAccess-GATE is added, RemoteAccess-Workplace automatically detects ports and creates a Target with a KVM access method for each port. The Targets section of the RemoteAccess-Workplace Configuration and the Ports Navigator populates with this information. This gives you an alternative view of the KVM ports of your managed RemoteAccess-GATEs, which are still available to view and access under the Devices section of the Port Navigator. KVM access cannot be added manually-it is always based on access to RemoteAccess-GATEs you have added to RemoteAccess-Workplace.

You can add other targets and access methods manually to use RDP, SSH, VNC, ESXi, Web, and Dual KVM access.

## In This Chapter

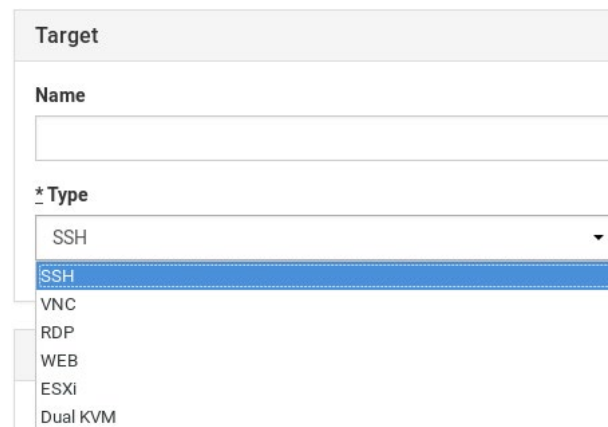
Adding Targets and Access Methods .....	23
Editing and Deleting Targets and Access Methods .....	29
Configuring Access Settings .....	30
Known Limitations on Targets .....	33

---

## Adding Targets and Access Methods

► **To add targets and access methods:**

1. In Main Menu, open the RemoteAccess-Workplace Configuration window, then click Targets.
2. The Targets list appears. Click New.
3. In the Add Access page, you will name the Target, and add the first access method.
  - Name: Enter a name for the target.
  - Type: Select the type of access method.
    - SSH
    - VNC
    - RDP
    - WEB
    - ESXi
    - Dual KVM



Target

Name

\* Type

SSH

VNC

RDP

WEB

ESXi

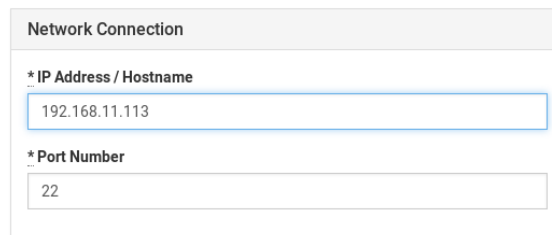
Dual KVM

4. Next steps vary based on Access Type.
  - **SSH, VNC, and RDP Access** (on page 23)
  - **WEB Access** (on page 25)
  - **ESXi Access** (on page 26)
  - **Multi KVM Access with RemoteAccess-GATES** (on page 27)

---

### SSH, VNC, and RDP Access

1. Add a target, then add the access method: *Adding Targets and Access Methods* (on page 23).
2. When Type is selected as: SSH, VNC, or RDP, the same information is required.
  - IP Address/Hostname: Enter the IP or hostname for the target.
  - Port Number: The default port number for the access type is populated automatically, but can be changed.



The 'Network Connection' form contains two input fields. The first field, labeled '\*IP Address / Hostname', contains the text '192.168.11.113'. The second field, labeled '\*Port Number', contains the text '22'.

- User Credentials: Enter the username and password as required for the access type. \*VNC requires password only.



The 'User Credentials' form contains two input fields. The first field, labeled 'Username', contains the text 'admin'. The second field, labeled 'Password', contains a series of dots representing a masked password.

3. Click Save. SSH/VNC/RDP access is added to the target and a list of all current access methods with options for editing displays.



---

## WEB Access

The WEB access method allows you to launch a web application in the RemoteAccess-Workplace's own web client. This can be used to launch the Remote Control feature to control another RemoteAccess-Workplace, or to access the web user interface of another KVM device.

See *Remote Control via Web Browser* (on page 150). The web client offers simple navigation only, and does not support Java, plugins, file upload/download, audio/video, webcams/microphones, opening new windows or tabs, or other advanced features. Single sign-on is not supported, so you must enter credentials each time you launch the WEB interface.

To launch WEB access, you must have the WEB Access privilege. To configure WEB access, you must have Device Administration or System Administration privilege.

1. Add a target, then add the access method: *Adding Targets and Access Methods* (on page 23).
2. Select WEB as the Access Type.
3. Enter the URL following this format: <schema>://<host>[:<port>]/<path>

For example: `https://www.example.com/test`

The screenshot shows a configuration dialog box for WEB Access. It has two main sections: 'Access' and 'Web Address'. In the 'Access' section, the '\* Type' dropdown menu is set to 'WEB'. The 'Web Address' section contains a light blue instructional box with the text: 'Enter a valid URL inclusive schema, host, optionally port and path: <schema>://<host>[:<port>]/<path>'. Below this, it states 'Valid schemas are https and http.' and provides an example: 'Example: https://www.example.com/test'. At the bottom of the 'Web Address' section is a text input field labeled '\* Url'. At the very bottom of the dialog are two buttons: 'Save' and 'Cancel'.

- Click Save. WEB access is added to the target and a list of all current access methods with options for editing displays.

WEB Access

URL

https://www.gdsys.de/support

Edit

Preferences

Delete

## ESXi Access

The ESXi access method allows you to access and control VMware ESXi virtual machines from the RemoteAccess-Workplace Navigator using the VMware “ESXi Embedded Host Client.” The ESXi server must support the ESXi Embedded Host Client and must be version 6.0 or higher. Upon launching, the Remote Console of the virtual machine is shown. Single sign-on is not supported, so you must enter credentials each time you launch the interface.

To launch ESXi Access, you must have the ESXi Access privilege. To configure ESXi access, you must have Device Administration or System Administration privilege.

- Add a target, then add the access method: *Adding Targets and Access Methods* (on page 23)
- Select ESXi as the Access Type.

Access

Type

ESXi

VMware Virtual Machine Address

Virtual Machine ID is the unique number identifying a particular VM of the ESXi-Server.

IP Address / Hostname of ESXi-Server

192.168.12.22

Virtual Machine ID

2

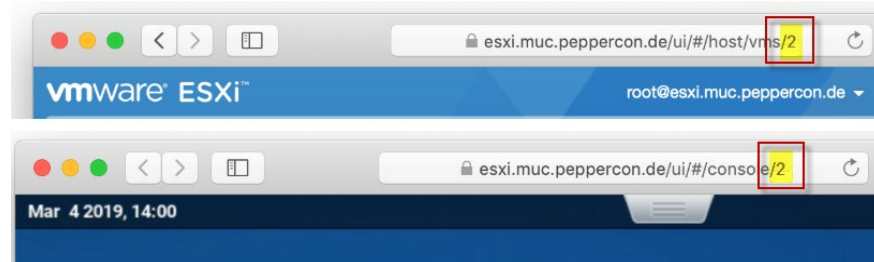
☒ Use Encryption

Save

Cancel

- Enter the IP Address or Hostname of the ESXi Server.

4. Enter the Virtual Machine ID. The ID can be found in the address bar of a browser where the URL to the virtual machine is displayed. The ID is the last component in the URL. See example images in host view and remote console view.



5. Select Use Encryption if you want to HTTPS as protocol for accessing the ESXi Remote Console.
6. Click Save. ESXi access is added to the target and a list of all access methods is displayed.

ESXi Access

IP Address / Hostname:

192.168.12.22

Virtual Machine ID:

2

Encrypted:

☒

Edit

Delete

### Multi KVM Access with RemoteAccess-GATEs

You can configure two or more KVM ports as a virtual multi-monitor KVM target. These independent ports are treated as a multi-monitor port group.

Important: Only RemoteAccess-GATE ports connected to the same target PC are supported. The screen configuration on the target PC must match the configuration selected in RemoteAccess-Workplace.

To configure the Multi KVM access method, select the KVM ports that you want to group virtually, and set one of the supported orientations. Once Multi KVM access is created, these multi-monitor access points will be marked as "M-KVM" in the Navigator. The KVM ports included will still also be listed as separate ports in the Navigator. It is possible to connect to the single ports independently, but not recommended as functionality of mouse/audio control is limited to the primary port. The Multi KVM targets cannot be added to the Port Scanner, but you can still add the single ports.

► **Supported Orientations:**

- Horizontal Dual
- Vertical Dual
- Horizontal Triple
- Vertical Triple
- Horizontal Quad
- Vertical Quad
- Quad 2x2
- Horizontal 5 Ports
- Vertical 5 Ports
- Horizontal 6 Ports
- Vertical 6 Ports
- 2x3 - 6 Ports
- 3x2 - 6 Ports

## Add Access to new Target

Target

Name

NewMultiKVM

Type

Multi KVM

Multi KVM Access Settings

You can configure two or more KVM Ports to a Virtual Multi Monitor KVM target here. These independent ports are treated as if they were part of a Multi Monitor Port Group.

Please select the Primary Port (located top left) and the Secondary port(s) (located right to the primary or below the primary) and the desired orientation (vertical, horizontal, etc.) here.

This is only supported for RA-GATE Devices.

Orientation

Horizontal (Dual)

Primary Port

RemoteAccess-GATE - 1 - RemoteAccess-GATE\_Port1

Secondary Port

RemoteAccess-GATE - 1 - RemoteAccess-GATE\_Port1

Save

Cancel

► **To configure Multi KVM Access:**

1. Add a target, then add the access method: ***Adding Targets and Access Methods*** (on page 23).
2. Select Multi KVM as the Access Type.
3. Select the orientation for the port group.
4. In the Primary Port and Secondary Port fields, you must select the KVM ports as follows:
  - Primary Port: The KVM port located in the top left of the orientation of ports.
  - Secondary Port: The KVM port located directly to the right of the primary, or directly below the primary.
  - Then, for configurations with more than 2 ports, select Ports 3, 4, 5, and 6. Fields open as needed for each orientation.

- Click Save. The new M-KVM target/access is added to the Targets list.





## Editing and Deleting Targets and Access Methods

Targets and Access methods are listed in the RemoteAccess-Workplace Configuration window.

You cannot delete KVM access, but all other access methods can be deleted. A Target must have at least one access method, or the target is deleted.

### ► To edit targets and access methods:

- In Main Menu, open the RemoteAccess-Workplace Configuration window, then click Targets.
- The Targets list appears. Use the Actions icons to edit as needed.

Name ↕	Model ↕	Serial ↕	Actions
RemoteAccess-GATE	RA-GATE	2C90700240	   



Edit settings for a port or access point. See ***Configuring KVM Ports*** (on page 17) for details on KVM port settings.  
See ***Configuring Access Settings*** (on page 30) for all other types.



Edit user credentials for any access method.



Delete an access method. You cannot delete KVM access. Deleting the last access method deletes the target.



Add an access method to the target.

## Configuring Access Settings

For each access type, you can configure General and Target Window Settings. Most settings are shared among all types of targets, but there are some unique settings in each category. Unique settings for each access type are outlined in the examples below.

By default, RemoteAccess-Workplace uses Target Window Settings that are valid for all ports and access points. You can override these settings for a specific port/access point by selecting the "Use Specific Target Window Settings". For details on all settings, and to set defaults, see ***Access Client Settings*** (on page 88)

### ► RDP Access Settings:

#### General Settings

☐ Hotkey
 

Ctrl+Alt

+

A

☐ Favorite

☐ Automatically connect Speaker

☐ Automatically connect Microphone

You can assign a Hotkey for quickly accessing this KVM Port or Access Point.  
**Note:** Keypad keys are not recognized. Please use regular number keys only.

#### Target Window Settings

☒ Use specific Target Window Settings
 

☒ Window Decorations
 ☐ Full-Screen Mode

By default, RemoteAccess-Workplace uses Target Window Settings which are valid for all ports and access points. However, here you can override these settings for this specific port or access point by checking **Use specific Target Window Settings**.

Adjust the default settings via the Access Client Settings dialog:

[Access Client Settings](#)

**Notes:**

- These setting don't apply to already active target sessions.
- The Full-Screen hotkey is always **Ctrl+Alt+Enter**.
- Multi-Monitor RDP targets are always launched in Full-Screen mode.

**Resizing Behavior**

Dynamic Resolution Change

**Transmission Quality**

Medium

**Preferred Resolution**

1024 x 768

**Display as Multi-Monitor Target**

Disabled

**Desktop Scaling**

100%

30

► VNC Access Settings:

General Settings

☐ Hotkey

Ctrl+Alt

+

A

☐ Favorite

☐ Automatically connect Speaker

☐ Automatically connect Microphone

☐ Include in Port Scanner

You can assign a Hotkey for quickly accessing this KVM Port or Access Point.

**Note:** Keypad keys are not recognized. Please use regular number keys only.

Target Window Settings

☐ Use specific Target Window Settings

☐ Scale Video

☒ Window Decorations

☐ Show Tool Bar

☐ Full-Screen Mode

☐ Start in Single Mouse Cursor Mode

Cursor Shape (in Double Cursor Mode)

Default

☐ Disable Banner Messages

By default, RemoteAccess-Workplace uses Target Window Settings which are valid for all ports and access points. However, here you can override these settings for this specific port or access point by checking **Use specific Target Window Settings**.

Adjust the default settings via the Access Client Settings dialog:

Access Client Settings

**Notes:**

- These setting don't apply to already active target sessions.
- To leave Full-Screen Mode, press the Full-Screen hotkey (Ctrl+Alt+F by default) in the Client.

► SSH Access Settings:

General Settings

☐ Hotkey

Ctrl+Alt

+

A

☐ Favorite

You can assign a Hotkey for quickly accessing this KVM Port or Access Point.

**Note:** Keypad keys are not recognized. Please use regular number keys only.

Target Window Settings

☐ Use specific Target Window Settings

☒ Window Decorations

☒ Show Menu Bar

☐ Full-Screen Mode

Console Size

80 x 24

By default, RemoteAccess-Workplace uses Target Window Settings which are valid for all ports and access points. However, here you can override these settings for this specific port or access point by checking **Use specific Target Window Settings**.

Adjust the default settings via the Access Client Settings dialog:

Access Client Settings

**Notes:**

- These setting don't apply to already active target sessions.
- The Full-Screen hotkey is always F11.

## ► WEB Access Settings:

### General Settings

☐ Hotkey 

Ctrl+Alt

 + 

A

☐ Favorite

You can assign a Hotkey for quickly accessing this KVM Port or Access Point.

**Note:** Keypad keys are not recognized. Please use regular number keys only.

### Target Window Settings

☐ Use specific Target Window Settings

☒ Window Decorations☒ Show Tool Bar☐ Full-Screen Mode

By default, RemoteAccess-Workplace uses Target Window Settings which are valid for all ports and access points. However, here you can override these settings for this specific port or access point by checking **Use specific Target Window Settings**.

Adjust the default settings via the Access Client Settings dialog:

Access Client Settings

**Notes:**

- These setting don't apply to already active target sessions.
- The Full-Screen hotkey is always *F11*.

## ► ESXi Access Settings:

### General Settings

☐ Hotkey 

Ctrl+Alt

 + 

A

☐ Favorite

You can assign a Hotkey for quickly accessing this KVM Port or Access Point.

**Note:** Keypad keys are not recognized. Please use regular number keys only.

### Target Window Settings

☐ Use specific Target Window Settings

☒ Window Decorations☐ Full-Screen Mode

By default, RemoteAccess-Workplace uses Target Window Settings which are valid for all ports and access points. However, here you can override these settings for this specific port or access point by checking **Use specific Target Window Settings**.

Adjust the default settings via the Access Client Settings dialog:

Access Client Settings

**Notes:**

- These setting don't apply to already active target sessions.
- The Full-Screen hotkey is always *F11*.



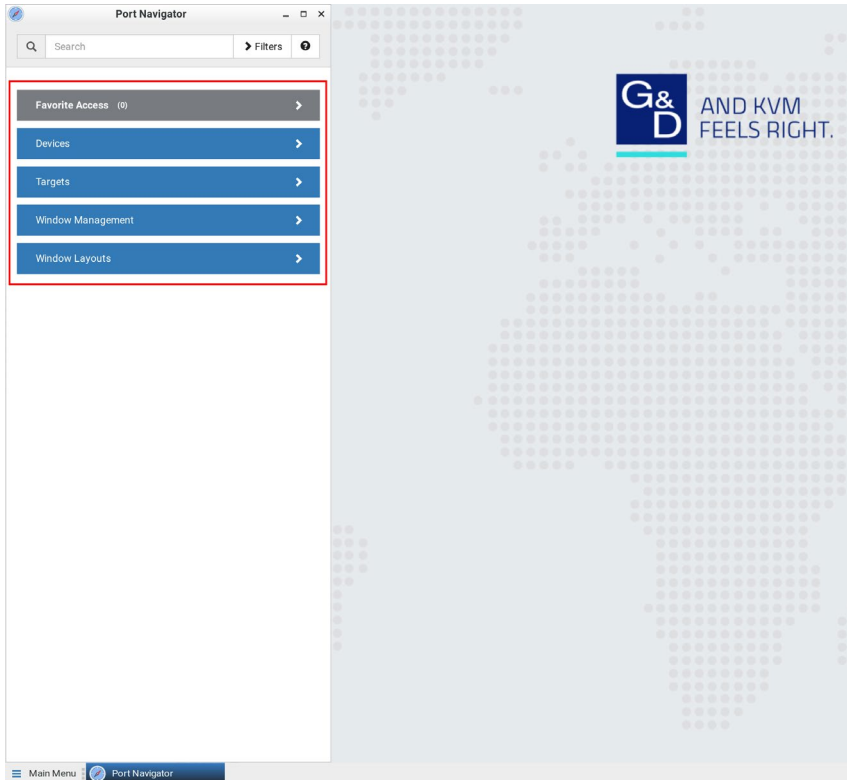
---

## Known Limitations on Targets

There are some known limitations on how Target access sessions function compared to typical KVM Client sessions.

- When opening a session, "Open in new / Open in current" is available for KVM and VNC. RDP and SSH only support "Open in new".
- VNC: Only RFB protocol versions 3.3 to 3.8 are supported. Proprietary extensions and versions are not supported, for example:
  - RealVNC protocol version 4.x and 5.x
  - TightVNC tight authentication
  - UltraVNC authentication
  - Connections over TLS, which is proprietary for some VNC servers
- If RDP connections to Windows targets fail, check these settings. Open the Edit Group Policy tool from Control Panel or use the Windows Search dialog (Windows Key + R, then type in gpedit.msc). Browse to: Local Computer Policy>Computer Configuration>Administrative Templates>Windows Components>Remote Desktop Services>Remote Desktop Session Host>Remote Session Environment. Disable "Use the hardware default graphics adapter for all Remote Desktop Services sessions."

# Navigation and Access



The Port Navigator contains three panels for accessing your ports and other targets:

- *Favorite Access*
- *Devices*
- *Targets*

And two panels for managing client windows:

- *Window Management*
- *Window Layouts*

The Navigator remembers the last-opened panel and returns to it when Navigator is opened again.

## ► To access a KVM port in the Devices panel:

1. Open the Devices panel. Once opened, the panel color turns gray.
2. Click a RemoteAccess-GATE.
3. Click a KVM or Serial port.

---

*Note: The RemoteAccess-Workplace CANNOT access a KVM port that is connected to a tiered RemoteAccess-GATE.*

---

## ► To access using the Targets panel:

1. Open the Targets panel.
2. Click a target to access it by the default access method. See **Port Navigator** (on page 35) for details on multiple access methods and so on.

## ► To use Window Management:

1. Open the Window Management panel.
2. Click an option for arranging your open client windows. See **Window Management** (on page 84) for more details.

► **To use Window Layouts:**

1. Open the Window Layouts panel.
2. Click a window layout to open it. You must setup and save layouts before you can select them here. See **Window Layouts** (on page 101) for more details and configuration.

**In This Chapter**

Port Navigator.....	35
Identifying States of RemoteAccess-GATEs and Ports.....	39
Identifying External Media.....	39
Dual Video Port Status.....	40
Using Search.....	41
Using Filters .....	41

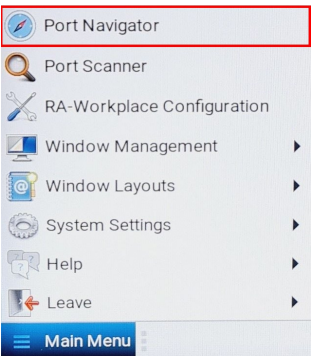
---

**Port Navigator**

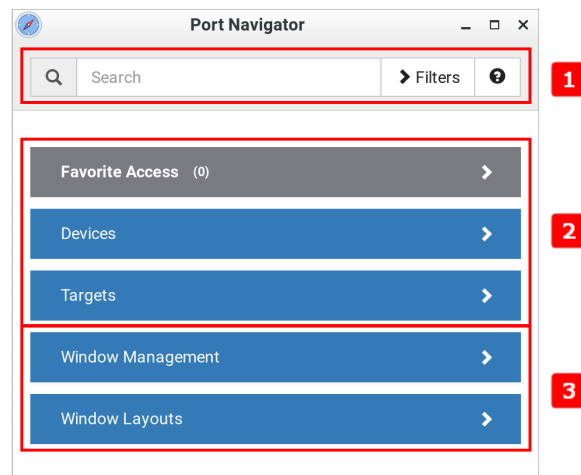
The Port Navigator window is displayed by default.

► **To launch Port Navigator:**

- Press *Ctrl+Alt+N*.
- OR choose Main Menu > Port Navigator.



The Port Navigator window opens.



## 1. Search, Filters, and Help:

### Search:

Searches for ports, switches, or targets and access points containing the search word(s). See *Using Search* (on page 41).

### Additional Filters:

Determines which items are displayed in this window based on connectivity and availability. See *Using Filters* (on page 41).

### Help ?:

Shows the colors and icons denoting RemoteAccess-GATE and port states. See *Identifying States of RemoteAccess-GATEs and Ports* (on page 39).

## 2. Favorite Access, Devices, and Targets:

### Favorite Access panel:

Shows a list of the favorite KVM ports you have configured. See *Configuring KVM Ports* (on page 17).

### Devices panel:

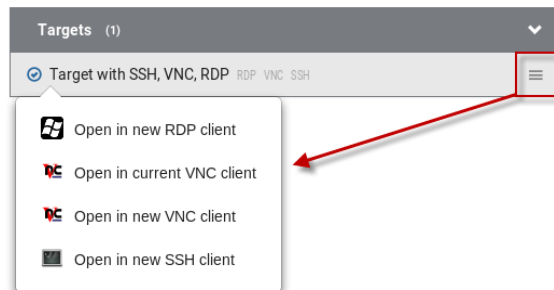
- Shows a list of all RemoteAccess-GATEs and ports
- Left-click on port opens the KVM or Serial client.
- Right-click on port opens the context menu.
- The default is to show switches whose status is Normal or Unknown. See *Using Filters* (on page 41).

**Targets panel:**

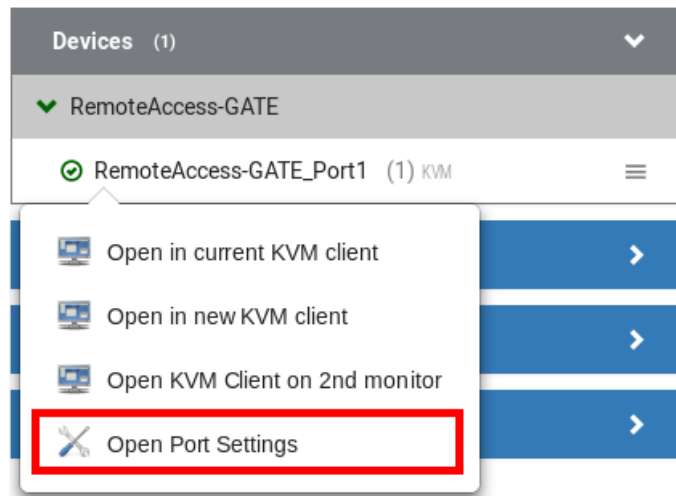
- Shows a list of all Targets. Targets with KVM access also show port status.
- Left-click on the Target opens the appropriate client. If there is more than one Access Point defined, the following hierarchy applies for which type of Access to use:
  - KVM
  - RDP
  - VNC
  - SSH
  - WEB
  - ESXi
- Next to the Target name, all configured access methods are listed. Click the access method directly to open the appropriate client. If there are multiple Access Points of the same type defined then the most recently added Access Point is opened.



- Right-click on the Target, or click the hamburger menu to list all access methods defined for the Target.



- If a secondary monitor is available for KVM or VNC targets, you can choose to open the target in the secondary monitor. Also on the right-click menu, choose Open Port Settings to jump to configuration.




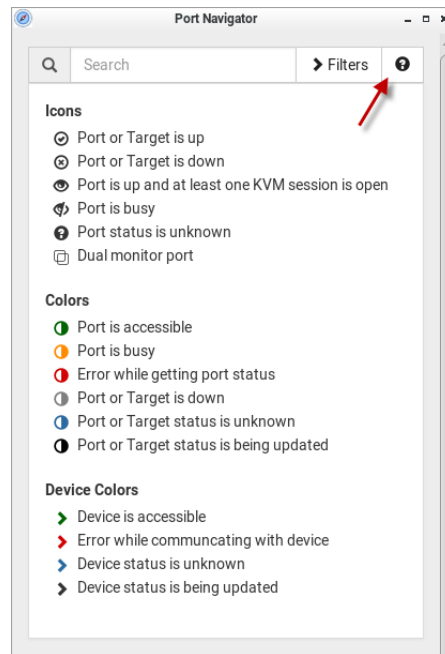
- The default is to show items whose status is Up. See *Using Filters* (on page 41).
  - For dual port video, the name of the dual port video group is displayed instead of the port names. Dual port video groups whose primary port is Up will show in the list.
3. **Window Management and Window Layouts:**
- Window Management: Manage open sessions with window management tools. See *Window Management* (on page 84).
  - Window Layouts: Access saved layouts. See *Window Layouts* (on page 101).

---

## Identifying States of RemoteAccess-GATEs and Ports

In the Port Navigator window, different icons and colors are applied to indicate current states of the added RemoteAccess-GATEs and ports.

Icon and color information is available by clicking the question mark icon .





---






## Identifying External Media

When external media are connected to a port via virtual media, the media icons display after the port name/number.

Devices (1) ▼

▼ RemoteAccess-GATE

✓ RemoteAccess-GATE\_Port1 (1)  

Icon	Port state
	Mass Storage
	ISO/CD device
	Microphone
	Speaker
	Smart Card Reader

---

## Dual Video Port Status

The primary port must have Status=Up to make a connection to both ports. The secondary port cannot be connected to directly, so its status is not reflected in the Navigator.

If the secondary port has Status=Down, there is still a dual monitor connection to both ports. There is either a "No Video" message or an error message such as "Cannot switch to port" on the secondary client. RemoteAccess-Workplace allows the user to connect to any target, independent of the status, using Filters. See *Using Filters* (on page 41).



---

## Using Search

The search box allows you to search for the KVM ports or switches that match the user's search words.



► **To search for KVM ports or switches:**

1. Open the panel where you want to perform the search function.
  - To search for a RemoteAccess-GATE, click the Devices panel.
    - To search KVM ports of a specific RemoteAccess-GATE in addition to RemoteAccess-GATEs, you can click the desired RemoteAccess-GATE to have its KVM ports displayed prior to using the Search function.

---

*Note: The RemoteAccess-Workplace will NOT search the KVM ports of those unselected RemoteAccess-GATEs in the Devices panel.*

---

- To search for a KVM port only, click the Targets panel.
  - To search for a "favorite" KVM port, click the Favorite Access panel.
2. Type the search word(s) in the Search box. Words are not case sensitive.
  3. The currently opened panel immediately shows the search result.

---

## Using Filters

By default, the Port Navigator window only shows devices that can be communicated with properly, and the ports and targets that are up. You can change the display criteria by using filters.



► **To change the filter:**

1. Click Filters, and the following checkboxes will appear.

**Device Connectivity**

☒ Normal

☐ Error

☒ Unknown

**Target and Port State and Availability**

☒ Up and Idle

☒ Up and Connected

☒ Up and Busy

☐ Down

**Target Access Type**

☒ KVM

☒ VNC

☒ RDP

☒ SSH

☒ WEB

☒ ESXi

2. Select or deselect any checkboxes to determine what is shown.

Checkbox	RemoteAccess-GATE's state
Normal	The RemoteAccess-GATE can communicate with the RemoteAccess-Workplace, and the device state is normal.
Error	The RemoteAccess-GATE cannot communicate with the RemoteAccess-Workplace.
Unknown	The RemoteAccess-GATE can communicate with the RemoteAccess-Workplace but cannot determine its device state.

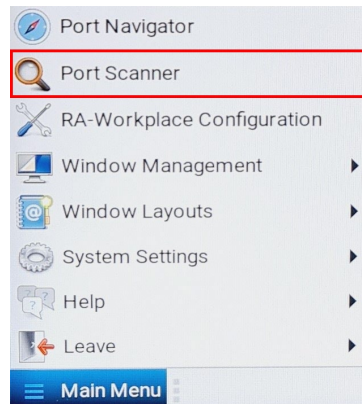
Checkbox	KVM ports or target state and availability
Up and Idle	The port is up, accessible and no KVM sessions are active.
Up and Connected	The port or target is up, and at least one KVM session is active.
Up and Busy	The port or target is up, but busy because an exclusive KVM session is active.
Down	The port is down.

3. For Target Access Type, select the access types you want to include.
4. When completed, click Filters again to hide the options.

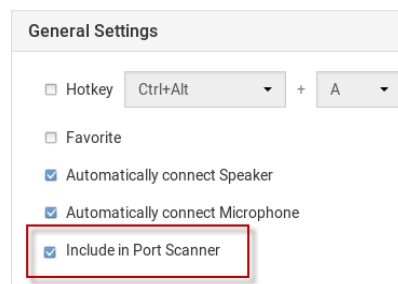
## Port Scanner

The Port Scanner displays an assortment of ports that you select, by scanning through each connection for a specified period of time. You can launch a KVM connection to any port shown in the scanner. The Port Scanner can also save target snapshots to an external USB device, when enabled. This is useful for forensic or surveillance purposes. See ***Port Scanner Settings*** (on page 48) for details on configuration and user privilege.

- Launch the Port Scanner from the Main Menu.



- Ports are included by selecting the setting "Include in Port Scanner" when configuring the port. Go to RemoteAccess-Workplace Configuration > Port Configuration settings. See ***Configuring KVM Ports*** (on page 17) for detailed instructions.



- The scanner allows you to pause and restart the scanning, open KVM sessions, show and hide thumbnails of each port, and set the scan options. See *Operating the Port Scanner* (on page 45).
- Audit log entries are created for each individual scanned port when you scan RemoteAccess-GATE ports.
- Window Management functions do not apply to the Port Scanner window.

In This Chapter

Operating the Port Scanner.....45

Scanner Options.....47

Port Scanner Settings.....48

Port Scanner Grid View.....51

Operating the Port Scanner

1. The main toolbar at the top of the Port Scanner has 4 buttons:



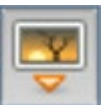
Resume the scanner.



Pause the scanner.



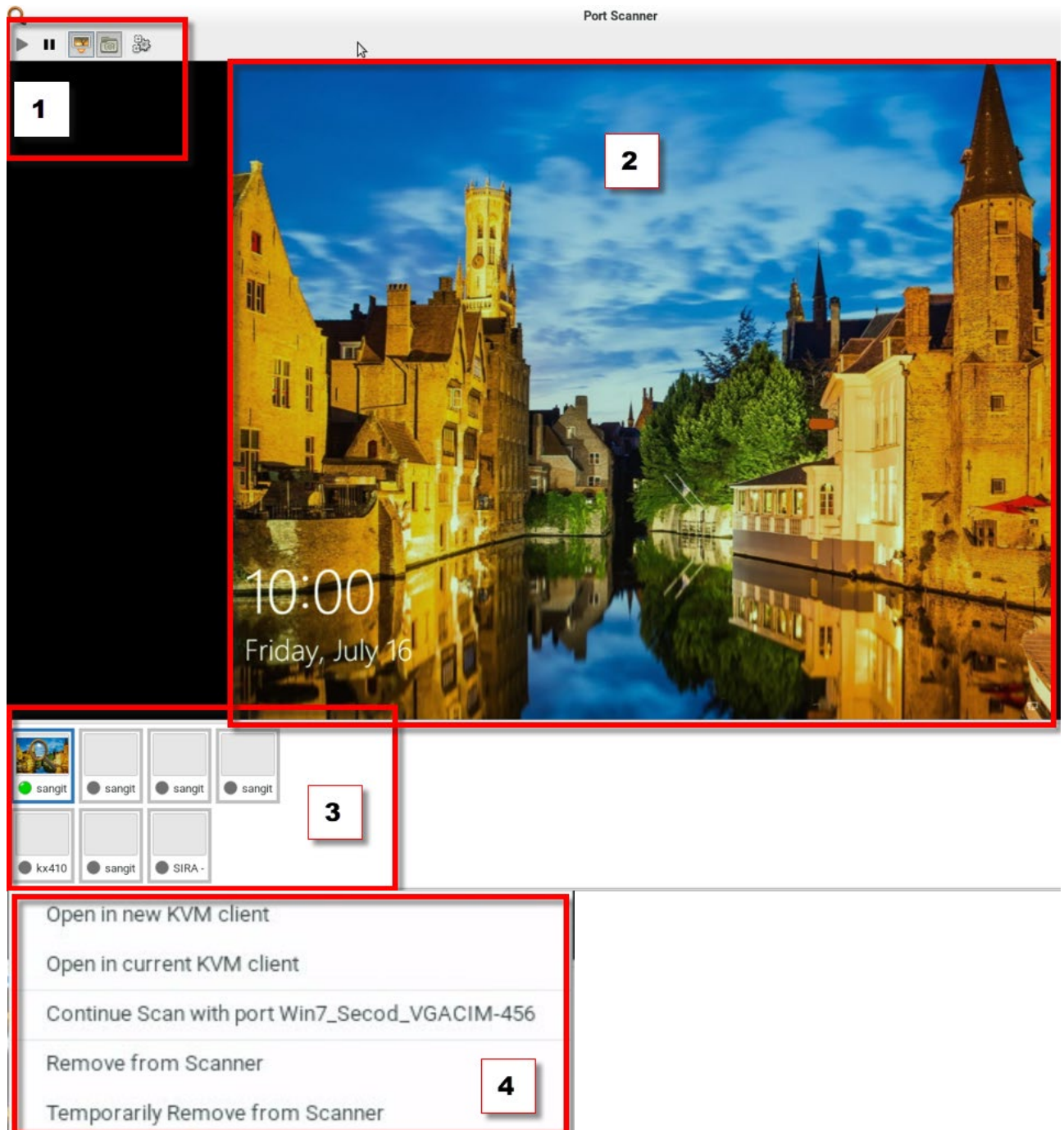
Show or hide the thumbnails.



Show or hide Live Preview image.



Configure the scanner options. See *Scanner Options* (on page 47).



2. The thumbnail preview shows all included ports. Choose vertical or horizontal placement in the scanner options.

3. The currently displayed port is highlighted in the thumbnails preview. Click the thumbnail once to view the port in the scanner. Double-click the thumbnail to open a KVM session to the port. Note that the default action of a double-click can be configured in Launch Settings. See ***Access Client Settings*** (on page 88)
4. Right-click a thumbnail to open a pop-up menu with more options:
  - Open in new KVM client: launch a KVM session to the port in a new window.
  - Open in current KVM client: launch a KVM session to the port in the current window.
  - Continue Scan with port "port name": Start scanning the selected port.
  - Remove from scanner: Turns off the "Include in Port Scanner" setting for the port.
  - Temporarily Remove from Scanner: The port is removed from this scanner session, but it is included the next time the scanner is started.

---

## Scanner Options

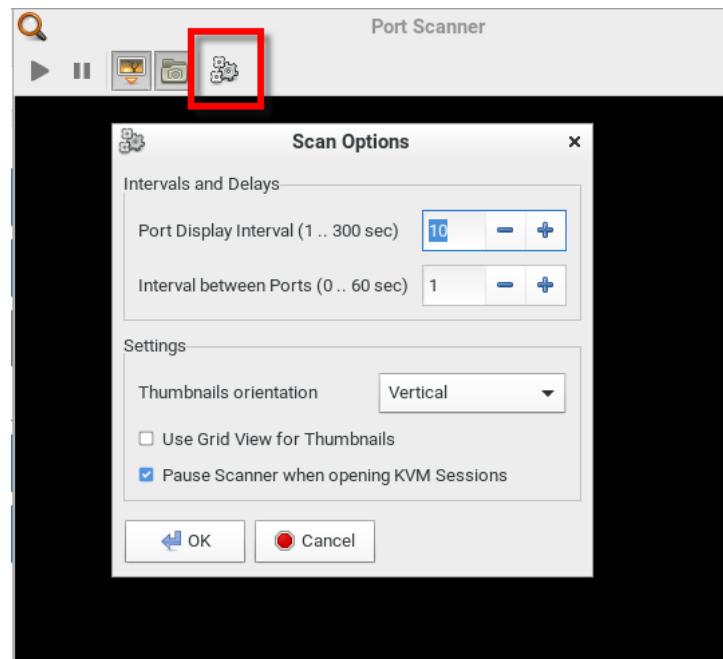
The port scanner can be configured to set intervals and delays, thumbnail orientation, and pause behavior.

See ***Port Scanner Settings*** (on page 48) to configure recording scanner snapshots.

### ► To set scanner options:

1. In the Main Menu, click Port Scanner to open the port scanning window.
2. Click the Scan Settings icon to open the options.
3. Configure intervals and delays:
  - a. Port Display Interval: Select the number of seconds to display each port before switching to next
  - b. Interval between Ports: Select the number of seconds to pause after Port Display Interval ends.
4. Configure settings:
  - a. Thumbnails orientation: Select Vertical or Horizontal to position thumbnails in relation to scan window.
  - b. Use Grid View for Thumbnails: Select this checkbox to enable grid view. See ***Port Scanner Grid View*** (on page 51).
  - c. Pause Scanner when opening KVM Sessions: Select this checkbox if the scanning should stop when you open a port into a full KVM session.

5. Click OK.



## Port Scanner Settings

You can configure the scanner intervals, delays, and orientation, and specify storage of snapshots from the scanner. Note that you can also configure intervals and orientation from the Port Scanner window. See **Scanner Options** (on page 47). However, snapshot settings only appear in the User Preferences > Port Scanner Settings page.

When enabled, snapshots are stored on an accessible USB device. The image saved is the thumbnail image from the scanner. Sub-directories are created on the USB drive per RemoteAccess-GATE, named after the device, port by number and name. Images are named by timestamp. Duplicate RemoteAccess-GATEs with the same name will all use the same directory.

You must have the "Scanner Snapshots" permission to capture snapshots from the scanner. See **User Groups** (on page 111).

### ► To configure port scanner settings:

1. If not displayed, launch the RemoteAccess-Workplace Configuration window. See **RemoteAccess-Workplace Configuration** (on page 10).



2. Click Preferences > Port Scanner Settings. The Port Scanner Settings page opens, showing the current preferences.
  - ☒ indicates the setting is enabled.
  - ☐ indicates the setting is disabled.

## Port Scanner Settings

Intervals and Delays
<b>Port Display Interval</b> 10 Seconds <b>Interval between Ports</b> 1 Second
Snapshot Recording
<b>Enable Snapshot Recording</b> <input type="checkbox"/> <b>Snapshot Recording Storage</b>
Settings
<b>Thumbnails Orientation</b> Vertical <b>Use Grid View for Thumbnails</b> <input checked="" type="checkbox"/> <b>Pause Scanner when opening KVM Sessions</b> <input checked="" type="checkbox"/>

Edit

3. Click Edit to make changes.
4. To set Intervals and Delays:
  - Port Display Interval (1..300 sec): Select the number of seconds to display each port before switching to next
  - Interval between Ports: Select the number of seconds to pause after Port Display Interval ends.

Intervals and Delays

Please choose the intervals for the Port Scanner here.

**Port Display Interval:** Select the number of seconds to display each port before switching to next.

**Interval between Ports:** Select the number of seconds to pause after Port Display Interval ends.

Port Display Interval (1 .. 300 sec)

10

– +

Interval between Ports (0 .. 60 sec)

1

– +

5. To set Snapshot Recording:
  - Enable Snapshot Recording: Click the checkbox to turn the feature on.
  - Make sure a USB drive is accessible.
  - Make sure you have the Record Scanner Snapshots privilege.

Snapshot Recording

The Port Scanner is able to save snapshot images of the target port to an external storage. Please select here if you want to enable this, and choose the external storage.

**Notes:**

- In order to save snapshots, insert a USB-Storage, such as a USB flash drive.
- You need to have the *Record Scanner Snapshots* privilege in order to save snapshots.

☐ Enable Snapshot Recording

No USB drive available

6. To configure remaining preferences:
  - **Thumbnails Orientation:** Select Vertical or Horizontal to position thumbnails in relation to scan window.
  - Select the **Use Grid View for Thumbnails checkbox** for an optional grid view that shows all thumbnails at once without scroll bars.
  - Select the **Pause Scanner when opening KVM Sessions** checkbox if the scanning should stop when you open a port into a full KVM session.

### Settings

Select additional settings:

**Thumbnails Orientation:** Select Vertical or Horizontal to position thumbnails in relation to scan window.

Select the **Use Grid View for Thumbnails** checkbox for an optional grid view that shows all thumbnails at once without scroll bars.

Select the **Pause Scanner when opening KVM Sessions** checkbox if the scanning should stop when you open a port into a full KVM session.

#### Thumbnails Orientation

Vertical

Use Grid View for Thumbnails ☒

Pause Scanner when opening KVM Sessions ☒

7. Click Save.

## Port Scanner Grid View

The RemoteAccess-Workplace port scanner offers a "grid" or "matrix" view option of ports from different devices. The grid view shows multiple thumbnails in a row/column view, all at the same time, and without scrolling. The number of ports is unlimited, varies as needed, and all ports are visible in the grid view.

The port scanner grid view can show ports from more than one RemoteAccess-GATE. Thumbnails can be arranged in a view, as a grid, without scroll bars. The thumbnails are automatically resized and arranged so that all ports in the port scanner are visible.

*Note: The thumbnail views in the grid view are periodically updated. Due to technical limitations in the processor and video resources, the grid view does not allow live-updates.*

### ► How the Grid View Works

The thumbnails section can optionally be a grid view, showing all the thumbnails at once without scrollbars.

The size and position of the thumbnails automatically adapt to the size of the thumbnails section, or the best fit.

The thumbnails section fills the entire space; if preferred, the live preview section can be hidden.

# Using the KVM Client

A KVM Client window opens after launching a port where a server is physically connected. When dual video ports are configured, connecting to the dual video port group opens two KVM client windows that are bound together. See *Dual Video Port Connections* (on page 86).

The server or PC connected to a KVM port is called the *target server*.

The RemoteAccess-Workplace's KVM Client settings are configured through the toolbar only. No menu bar is available.



## In This Chapter

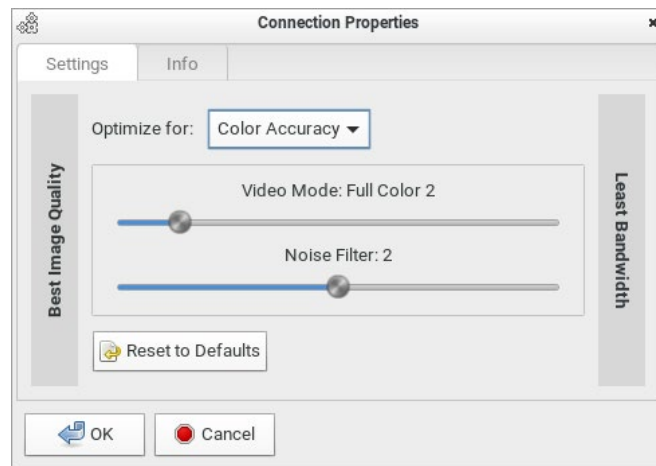
Connection Properties .....	53
Keyboard Macros.....	57
Mouse Settings .....	58
Video Settings .....	63
Peripheral Devices and USB Settings.....	68
Power Control.....	80
External Device Control .....	81
View Settings .....	82
Window Management .....	84
Dual Video Port Connections.....	86

## Connection Properties

Connection properties manage streaming video performance over connections to target servers. The properties are applied only to your connection, not the connection of other users accessing the same target server.

### ► To configure connection properties:

1. Click  to open the Connection Properties dialog.



2. The default connection settings are the optimal settings for video performance most of the time. Do NOT make changes unless required. See **Default Connection Properties** (on page 55).

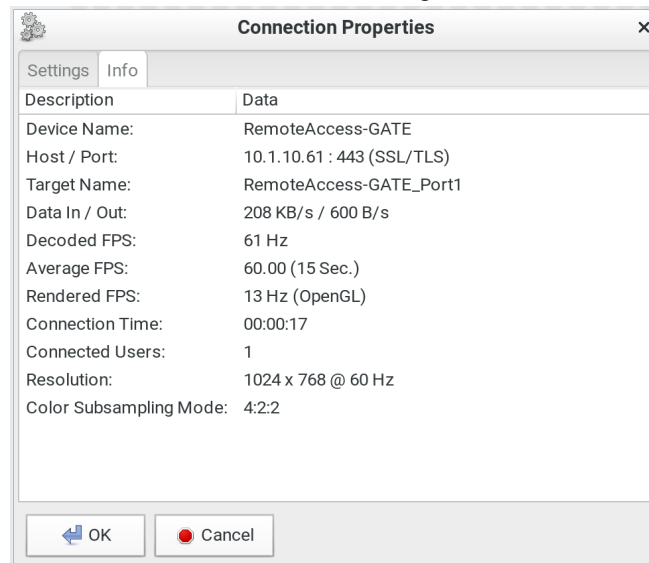
Setting	Description
Optimize for	Determine which aspect of video data is optimized for. There are two options: <ul style="list-style-type: none"> <li>▪ <b>Text Readability</b> (on page 56)</li> <li>▪ <b>Color Accuracy</b> (on page 56)</li> </ul>
Video Mode	This slider controls the video quality as well as the bandwidth. <ul style="list-style-type: none"> <li>▪ Left: higher quality with higher bandwidth consumed.</li> <li>▪ Right: lower quality with less bandwidth consumed. This is useful for low-bandwidth connections.</li> </ul> See <b>Video Mode</b> (on page 56).

Setting	Description
Noise Filter	This slider controls the noise filter threshold. <ul style="list-style-type: none"> <li>Left: higher threshold.</li> <li>Right: lower threshold.</li> </ul> See <b>Noise Filter</b> (on page 57).
Reset to Defaults	Reset connection properties to the factory defaults.

- Click OK to save any changes made. The settings are stored persistently for the accessed port.

► **To view connection information:**

- Click the Info tab in the same dialog.



Item	Description
Device Name	The RemoteAccess-GATE's name.
Host / Port	The RemoteAccess-GATE's IP address, and the TCP/IP port used to access the RemoteAccess-GATE.
Target Name	The accessed KVM port's name.

Item	Description
Data In / Out	Rate of data received and sent out to the RemoteAccess-GATE in bytes per second.
Decoded FPS	Number of frames per second that were received and decoded by the KVM Client.
Average FPS	Average number of frames per second
Rendered FPS	Number of frames per second that were displayed onscreen. Usually this number is similar to "Decoded FPS", but it may be lower on high graphics demand.
Connection Time	Duration of the current connection.
Connected Users	Number of connected users.
Resolution	Video resolution of the target server connected to this KVM port.

---

### Default Connection Properties

The RemoteAccess-Workplace comes configured to provide optimal performance for the majority of video streaming conditions.

Default connection settings are:

- Optimized for: Text Readability - video modes are designed to maximize text readability.  
This setting is ideal for general IT and computer applications, such as performing server administration.
- Video Mode - defaults to Full Color 2.  
Video frames transmit in high-quality, 24-bit color. This setting is suitable where a high-speed LAN is used.
- Noise Filter - defaults to 2.  
The noise filter setting does not often need to be changed.

---

### **Text Readability**

Text Readability is designed to provide video modes with lower color depth but text remains readable. Greyscale modes are even available when applying lower bandwidth settings.

This setting is ideal when working with computer GUIs, such as server administration.

When working in full color video modes, a slight contrast boost is provided, and text is sharper.

In lower quality video modes, bandwidth is decreased at the expense of accuracy.

---

### **Color Accuracy**

When Color Accuracy is selected, all video modes are rendered in full 24-bit color with more compression artifacts.

This setting applies to viewing video streams such as movies or other broadcast streams.

In lower quality video modes, sharpness of fine detail, such as text, is sacrificed.

---

### **Video Mode**

The Video Mode slider controls each video frame's encoding, affecting video quality, frame rate and bandwidth.

In general, moving the slider to the left results in higher quality at the cost of higher bandwidth and, in some cases, lower frame rate.

Moving the slider to the right enables stronger compression, reducing the bandwidth per frame, but video quality is reduced.

In situations where system bandwidth is a limiting factor, moving the video mode slider to the right can result in higher frame rates.

When Text Readability is selected as the Optimized setting, the four rightmost modes provide reduced color resolution or no color at all.

These modes are appropriate for administration work where text and GUI elements take priority, and bandwidth is at a premium.



---

## Noise Filter

Unless there is a specific need to do so, do not change the noise filter setting. The default setting is designed to work well in most situations.

The Noise Filter controls how much interframe noise is absorbed by the RemoteAccess-Workplace.


Moving the Noise Filter slider to the left lowers the filter threshold, resulting in higher dynamic video quality. However, more noise is likely to come through, resulting in higher bandwidth and lower frame rates.

Moving the slider to the right raises the threshold, allows less noise and less bandwidth is used. Video artifacts may be increased.

Moving the noise filter to the right may be useful when accessing a computer GUI over severely bandwidth-limited connections.

---

## Keyboard Macros

Click  to select one of the pre-programmed hotkey macros.



Send Ctrl+Alt+Del  
Send LeftAlt+Tab

---

*Note: If you have manually created any hotkey macros and have them enabled, these macros are displayed below "Send LeftAlt+Tab." See **Managing Keyboard Macros** (on page 93).*

---

### ► Send Ctrl+Alt+Del:

To send this key sequence to the target server you are accessing:

- Click  > Send Ctrl+Alt+Del.
- OR click   .

### ► Send LeftAlt+Tab:

This hotkey macro switches between open windows on the target server you are accessing.

Warning: If you physically press *Ctrl+Alt+Del* or *Left Alt+Tab* using the KEYBOARD, these key sequences are processed on the RemoteAccess-Workplace by default, instead of being transferred to the target server. To change the default behaviors so that they are processed on the target servers after being pressed on the keyboard, see Desktop Settings.


---

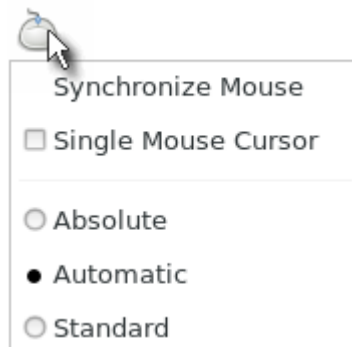
## Mouse Settings

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

Single mouse mode displays only one mouse pointer while dual mouse mode displays two.

In any mouse mode, when the mouse pointer lies within the KVM Client's target server window, mouse movements and clicks are directly transmitted to the target server.

Click  to select one mouse command or mode.



Single Mouse Cursor is for single mouse mode. Absolute, Automatic and Standard are the dual mouse modes.

---

**Important:** Make sure you have configured mouse settings on the target servers properly. For information on configuring mouse settings of target servers, refer to the RemoteAccess-GATE manual ([www.gdsys.com](http://www.gdsys.com)).



---

---

## Synchronize Mouse

In the dual mouse mode, the Synchronize Mouse command forces realignment of the target server's mouse cursor with the RemoteAccess-Workplace's. See **Dual Mouse Modes** (on page 60).

### ► To synchronize the mouse cursors:

- Click  > Synchronize Mouse.
- OR click .

---

*Note: This option is available in Automatic and Standard mouse modes only. However, mouse synchronization may not always be successful with this option. When this occurs, first check **Mouse Synchronization Tips** (on page 62). If the mouse synchronization issue still cannot be resolved, enter the Absolute or single mouse mode. See **Single Mouse Cursor** (on page 59) and **Absolute Mouse Mode** (on page 60).*


---

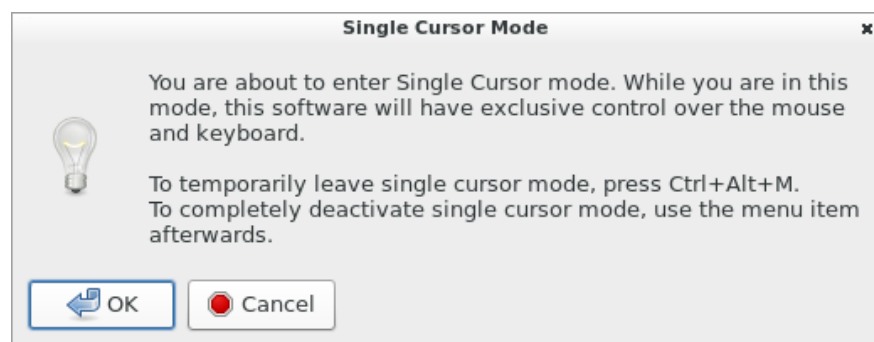
## Single Mouse Cursor

In single mouse mode, you only use the target server's mouse cursor, and the RemoteAccess-Workplace's mouse cursor no longer appears on the screen.

On fast LAN connections, you can use single mouse mode, and view only the target server's pointer.

### ► To enter the single mouse mode:

1. Click  > Single Mouse Cursor.
2. Click OK on the confirmation message.



► **To temporarily exit the single mouse mode and then return to this mode:**

1. Press Ctrl+Alt+M on your keyboard. A message appears, indicating that the single mouse mode is temporarily suspended.  
Now you can use the mouse to control the RemoteAccess-Workplace.
2. To return to the single mouse mode, click anywhere on the target server's image in the KVM Client.

---

### Dual Mouse Modes

In the dual mouse modes, two cursors appear onscreen. They are:

- The mouse cursor of the RemoteAccess-Workplace.
- The mouse cursor of the target server connected to the KVM port you are accessing.

Two mouse cursors align if properly configured.

While in motion, the RemoteAccess-Workplace's mouse pointer slightly leads the target server's mouse pointer.

### Absolute Mouse Mode

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

This mode is supported on target servers with USB ports and is the default mode for virtual media CIMs.

Use of virtual media CIMs on target servers is required for this mouse mode. See Virtual Media CIMs.

Most modern operating systems on the target servers shall support the Absolute mouse mode.

---

*Note: Some Linux, UNIX, Solaris or very "unusual" operating systems as well as some USB profiles may not support the Absolute mouse mode. In this case, use other mouse modes. For detailed information of each USB profile, see the section titled "Available USB Profiles" in the RemoteAccess-GATE manual ([www.gdsys.com](http://www.gdsys.com)).*

---

► **To enter the Absolute mouse mode:**

- Click  > Absolute.

### Automatic Mouse Mode

In this mode, the target server's mouse settings are detected and the mouse cursors synchronized accordingly, allowing mouse acceleration on the target server.

This mode is the default for non-VM target servers.

---

*Note: A non-VM target server is the target server using a CIM that does not support virtual media.*

---

#### ► To enter the Automatic mouse mode:

- Click  > Automatic.

#### ► Automatic mouse synchronization requirements:

The Synchronize Mouse command automatically synchronizes mouse cursors during moments of inactivity in the Automatic mouse mode. See ***Synchronize Mouse*** (on page 59).

For this to work properly, the following conditions must be met:

- No windows should appear in the top-left corner of the target server's page.
- There should not be an animated background in the top-left corner of the target server's page.
- The target server's mouse cursor shape should be normal and not animated.
- The target server's mouse speeds should not be set to very slow or very high values.
- Advanced mouse properties such as "Enhanced pointer precision" or "Snap mouse to default button in dialogs" should be disabled on the target servers.
- Choose "Best Possible Video Mode" in the Video Settings dialog of the KVM Client.
- The edges of the target server's video should be clearly visible (that is, a black border should be visible between the target server's desktop and the KVM Client window when you scroll to an edge of the target video image).

After autosensing the target server's video, manually perform the Synchronize Mouse command. This also applies when the resolution of the target server changes if the mouse cursors start to desync from each other.

If automatic mouse synchronization fails, this mode will revert to standard mouse synchronization behavior. See ***Standard Mouse Mode*** (on page 62).

Note that mouse configurations will vary on different target servers' operating systems. Consult your OS guidelines for further details.

---

*Note: Automatic mouse synchronization does not work with UNIX target servers.*

---

### Standard Mouse Mode

Standard mouse mode uses a standard mouse synchronization algorithm. The algorithm determines relative mouse positions on the RemoteAccess-Workplace and target server.

In order for the RemoteAccess-Workplace's and target server's mouse cursors to stay in synch, mouse acceleration must be disabled. Additionally, specific mouse parameters must be set correctly.



#### ► To enter the Standard mouse mode:

- Click  > 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 your RemoteAccess-Workplace.  
The KVM Client's Connection Properties dialog displays the actual values the RemoteAccess-Workplace is seeing.
2. Force a video auto-sense by clicking the KVM Client's Auto-sense Video button .
3. If that does not improve the mouse synchronization (for Linux, UNIX, and Solaris target servers):
  - a. Open a terminal window.
  - b. Enter this command: `xset mouse 1 1`
  - c. Close the terminal window.
4. Click the KVM Client's mouse synchronization button .

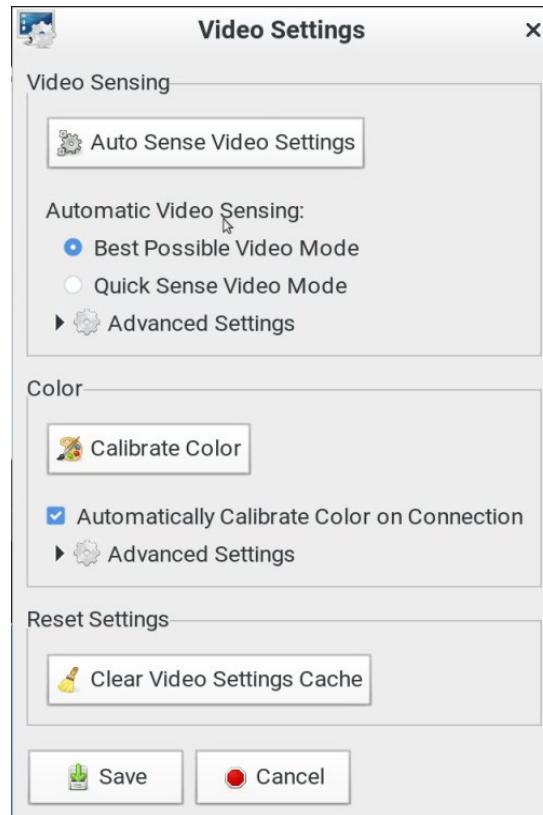
---

*Note: If the mouse synchronization issue still cannot be resolved, enter the Absolute or single mouse mode. See **Single Mouse Cursor** (on page 59) and **Absolute Mouse Mode** (on page 60).*


---

## Video Settings

Click  to open the Video Settings dialog.



### ▶ Video Sensing settings:

Setting	Description
Auto Sense Video Settings	<p>Automatically detects the target server's video settings (resolution, refresh rate) and redraws the video screen.</p> <p>Clicking  in the toolbar results in the same video re-sensing function.</p>

Setting	Description
Best Possible Video Mode	The RemoteAccess-Workplace will perform the full Auto Sense process when switching target servers or target resolutions. Selecting this option calibrates the video for the best image quality.
Quick Sense Video Mode	Uses a quick video Auto Sense to show the target server's video sooner.  This option is especially useful for entering a target server's BIOS configuration right after a reboot.
Advanced Settings	Adjusts the clock, phase, horizontal and vertical offset. See <b><i>Advanced Video Settings</i></b> (on page 65).

---

*Note: Some background screens, such as screens with very dark borders, may not center precisely. Use a different background or place a lighter colored icon in the upper-left corner of the screen.*

---

► **Color settings:**

Setting	Description
Calibrate Color	Optimizes the color levels (hue, brightness, saturation) of the transmitted video images. The color settings are on a target server-basis.  Note that this command applies to the current connection only.
Automatically Calibrate Color on Connection	Causes the RemoteAccess-Workplace to automatically update the color calibration once connected to a target server.
Advanced Settings	Adjusts brightness and contrast levels of red, green and blue colors. See <b><i>Advanced Color Settings</i></b> (on page 67).



### ► Reset Settings:

The Clear Video Settings Cache button resets the cache where video settings are stored, which is useful when old video settings no longer apply, such as when a target server is replaced.

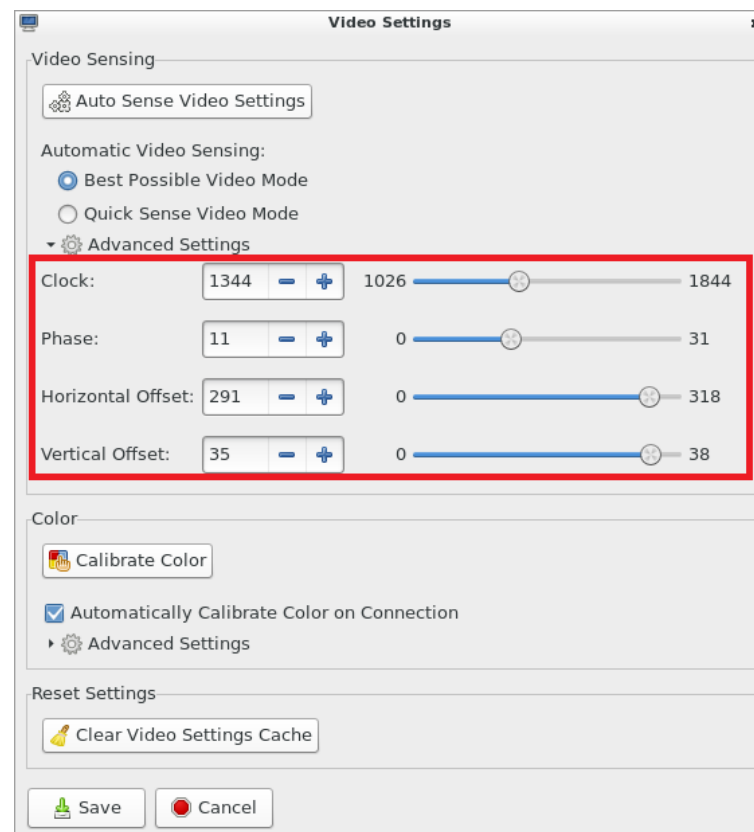
After calibrating the colors for a target server, color values are cached and reused whenever accessing that server. Changing resolutions resets the video to the cached values again.



Note that changes to the brightness and contrast levels are NOT cached.

When resetting the video settings cache, the RemoteAccess-Workplace automatically does a video auto-sense and color calibration. New values are cached and reused for accessing that target server next time.

## Advanced Video Settings

In the Video Settings dialog, click Advanced Settings in the Video Sensing section to show additional settings.

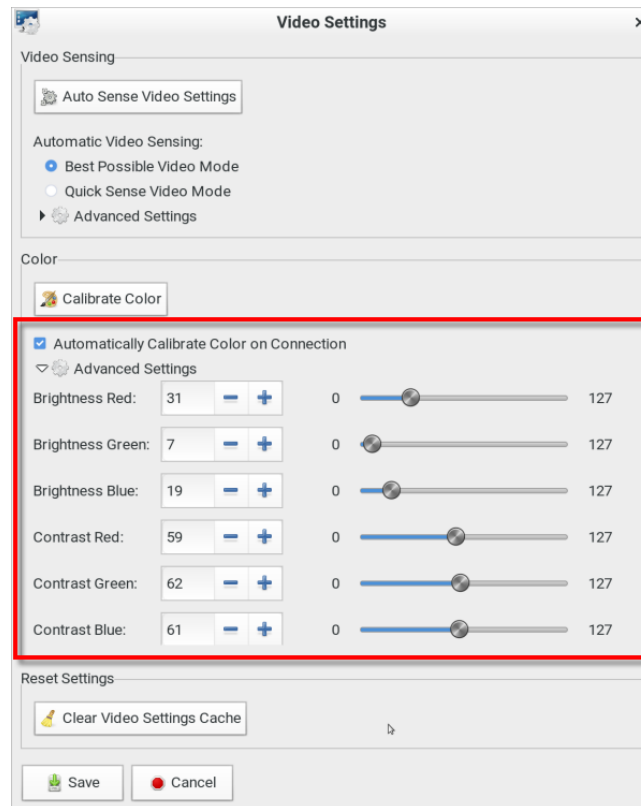




Click  or , drag sliders, or type a new numeric value in the text box to adjust corresponding settings.

Setting	Description
Clock	<p>Controls how quickly video pixels are displayed across the video screen. Changes made to clock settings cause the video image to stretch or shrink horizontally.</p> <p>Under most circumstances, this setting should not be changed because the auto detect is usually quite accurate.</p> <p>Odd number settings are recommended.</p>
Phase	<p>Phase values range from 0 to 31 and will wrap around. Stop at the phase value that produces the best video image for the active target server.</p>
Horizontal Offset	<p>Controls the horizontal positioning of the target server display on your monitor.</p>
Vertical Offset	<p>Controls the vertical positioning of the target server display on your monitor.</p>

## Advanced Color Settings

In the Video Settings dialog, click Advanced Settings in the Color section to show additional color settings.




Click  or , drag sliders, or type a new numeric value in the text box to adjust corresponding settings.

Setting	Description
Brightness Red	Controls the brightness of the target server's display for the red signal.
Brightness Green	Controls the brightness of the green signal.
Brightness Blue	Controls the brightness of the blue signal.
Contrast Red	Controls the red signal contrast.
Contrast Green	Controls the green signal contrast.

Setting	Description
Contrast Blue	Controls the blue signal contrast.

## Peripheral Devices and USB Settings

Click  to open the "Audio, Mass Storage and SmartCard Devices" dialog, where you can virtually connect up to two devices of different types to a target server.



**Important:** It is strongly recommended to mount virtual media or audio devices onto the target server prior to the smart card reader. If the sequence is reversed, you will be logged out of the target's operating system as the card reader will be temporarily disconnected while connecting the audio or virtual media device.

Section	Description
Connect New Device	<ul style="list-style-type: none"><li><i>Audio Device ...</i></li></ul> Click this button to virtually connect an audio device to the target server. See <b>Audio Device</b> (on page 70).

Section	Description
	<ul style="list-style-type: none"> <li>• <i>Mass Storage Device ...</i> Click this button to mount a USB drive onto the target server.</li> <li>• <i>CD-ROM Device / ISO File ...</i> This button mounts a DVD drive, CD-ROM drive, or an ISO image onto the target server. See <b><i>Virtual Media</i></b> (on page 72).</li> <li>• <i>SmartCard Reader...</i> This button connects a smart card reader to the target server. See <b><i>SmartCard Reader</i></b> (on page 77).</li> </ul>
Connected Devices	<p>This section lists all devices which have been "virtually" connected to the target server.</p> <p>See <b><i>Disconnecting a Virtual Device</i></b> (on page 77).</p>
USB Profiles	<p>Click it to select a USB configuration profile that best applies to the target server. See <b><i>USB Profiles</i></b> (on page 79).</p>

---

*Note: For detailed information of each USB profile, see the section titled "Available USB Profiles" in the RemoteAccess-GATE manual ([www.gdsys.com](http://www.gdsys.com)).*


---

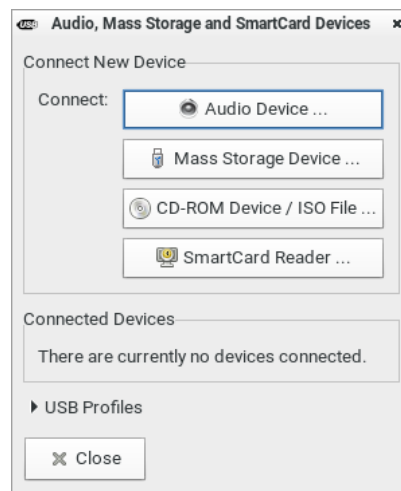
## Audio Device

Prior to connecting the audio devices to the target server, you may have to specify the audio devices you want to use. Per default, the front-panel analog speakers and microphone are used.

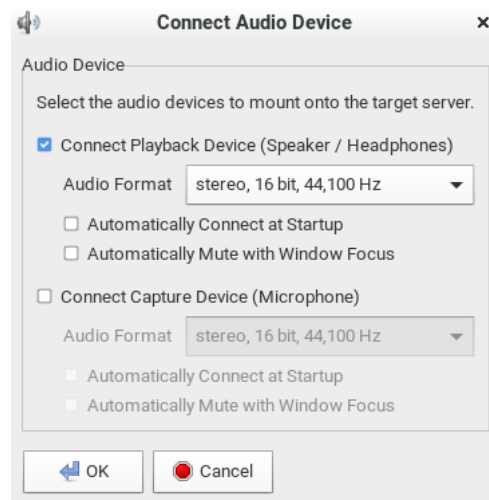
See *Audio Settings* (on page 97).

### ► To connect an audio device to the target server:

1. Click  to open the "Audio, Mass Storage and SmartCard Devices" dialog.



2. Click the "Audio Device ..." button. The Connect Audio Device dialog appears.



Checkbox	Description
Connect Playback Device (Speaker / Headphones)	<p>To manually connect an available audio playback device to the target server, select this checkbox.</p> <ul style="list-style-type: none"> <li>▪ Set the playback audio format in the Audio Format field.</li> <li>▪ Automatically Connect at Startup: The selected playback device will automatically be connected to the current target server whenever that target is accessed.</li> <li>▪ Automatically Mute with Window Focus: The selected device will automatically mute/unmute as window is active/inactive.</li> <li>▪ Mute/Unmute buttons are also available in the client toolbar for manual control.</li> </ul>
Connect Capture Device (Microphone)	<p>To manually connect an available audio recording device to the target server, select this checkbox.</p> <ul style="list-style-type: none"> <li>▪ Set the recorded audio format in the Audio Format field.</li> <li>▪ Automatically Connect at Startup: The selected microphone will automatically be connected to the current target server whenever that target is accessed.</li> <li>▪ Automatically Mute with Window Focus: The selected device will automatically mute/unmute as the window is active/inactive.</li> <li>▪ Mute/Unmute buttons are also available in the client toolbar for manual control.</li> </ul>

3. Click OK.

► **To disconnect the audio device from the target server:**

- See *Disconnecting a Virtual Device* (on page 77).

---

### **Virtual Media**

The RemoteAccess-Workplace supports virtual media (VM). Virtual media extends KVM capabilities by enabling target servers to remotely access media from the RemoteAccess-Workplace and network file servers.

With this feature, media mounted onto the RemoteAccess-Workplace 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.

Virtual media sessions are secured using 128 or 256 bit AES encryption.



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.

---

For the VM types supported by the RemoteAccess-Workplace, see *Supported Virtual Media Types* (on page 73).

#### Prerequisites for Using Virtual Media

##### ▶ RemoteAccess-GATE requirements:

- If you want to access virtual media, your "RemoteAccess-GATE" permissions must be set to allow access to the relevant KVM ports, as well as virtual media access (VM Access port permission) for those ports.

RemoteAccess-GATE permissions are determined according to the user credentials you entered for the RemoteAccess-GATEs. See *Editing RemoteAccess-GATEs* (on page 13).

- A USB connection through the virtual media CIM must exist between the RemoteAccess-GATE and the target server.

##### ▶ Target server requirements:

- You must choose the correct USB profile for the target server. See *Peripheral Devices and USB Settings* (on page 68).
- KVM target servers must support USB connected drives.

► **Supported Virtual Media Types:**

- External hard drives
- USB-mounted CD/DVD drives
- USB mass storage devices
- ISO images (disk images)


ISO9660 is the standard supported by G&D. However, other ISO standards can be used.

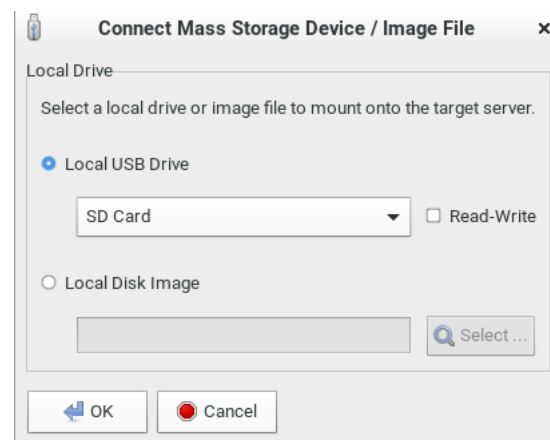
**Connecting Local USB Drives and Local Disk Images**

This option mounts an entire USB drive virtually onto the target server when you select the Local USB Drive option. Use this option for external drives only. It does not include CD-ROM, or DVD-ROM drives.

You can connect to a local disk image with the .img or .dmg extension. Apple DMG files must not be encrypted or compressed. The disk images should be in the root folder of an attached USB drive.

► **To mount a local USB drive:**

1. Click  to open the "Audio, Mass Storage and SmartCard Devices" dialog.
2. Click the "Mass Storage Device ..." button. The Connect Mass Storage Device/Image File dialog appears.



3. Choose the drive from the Local USB Drive drop-down list.

4. If you want Read and Write capabilities, select the Read-Write checkbox.
  - This option is not configurable in some scenarios. See ***Scenarios When Read/Write is Unavailable*** (on page 75).
  - When selected, you will be able to read or write to the connected USB drive.

---

*Note: Improper unmounting of the USB drive from the target server may result in data corruption. See **Disconnecting a Virtual Device** (on page 77). Therefore, if you do not require Write access, leave this option unselected.*

---

5. 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 server, 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.*

---

#### ► To connect to a Local Disk Image:

##### ***Scenarios When Read/Write is Unavailable***

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

- The drive is write-protected.
- The user credentials you entered for the RemoteAccess-GATE does not allow Read/Write permission on the KVM port you are accessing.

For information on how to enter user credentials for RemoteAccess-GATEs, see ***Editing RemoteAccess-GATEs*** (on page 13).

#### **Mounting CD-ROM/DVD-ROM/ISO Images**


ISO9660 format is the standard supported by G&D. However, other CD-ROM extensions may also work.

---

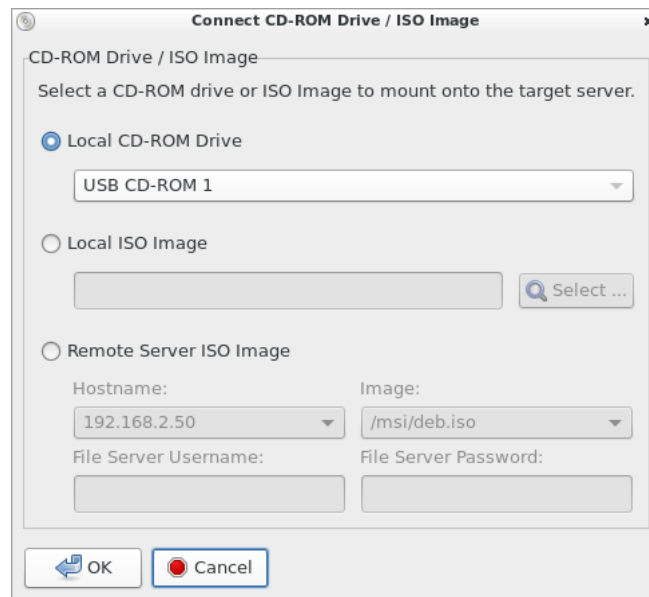
*Note: Audio CDs are not supported by virtual media so they do not work with the virtual media feature.*

---

#### ► To mount a CD-ROM , DVD-ROM or ISO image:

1. Click  to open the "Audio, Mass Storage and SmartCard Devices" dialog.

2. Click the "CD-ROM Device / ISO File ..." button. The Connect CD-ROM Drive / ISO Image dialog appears.



3. For USB CD-ROM/DVD-ROM drives:
  - a. Select the Local CD-ROM Drive option.
  - b. Choose the drive from the Local CD-ROM Drive drop-down list, which shows all available CD-ROM/DVD-ROM drive names.
4. For Local ISO Images: The ISO images must be on the root-folder of USB storage device.
  - a. Connect the USB-storage to the RemoteAccess-Workplace.
  - b. Select the Local ISO Image option. The Select button opens a dialog with a list of all ISO images found. Select the one you want to use and close the dialog with OK.
5. For remote ISO images on a file server:

Remote ISO images must be setup in RemoteAccess-Workplace to be available for selection by the KVM-Client. See Virtual Media File Server Setup.

  - a. Select the Remote Server ISO Image option.
  - b. Select Hostname and Image from the drop-down list.

The hostnames (file servers) and image paths available in the list are those that you configured using the RemoteAccess-GATE's File Server Setup page. See the RemoteAccess-GATE manual for further information.
  - 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).
6. Click OK.

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

► **To disconnect the CD-ROM , DVD-ROM or ISO image from the target server:**

- See *Disconnecting a Virtual Device* (on page 77).

### **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 profile currently applied to the target server. These drives are accessible for the duration of the KVM session.

For example, you can mount a specific CD-ROM, use it, and then physically 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 profile supports it.

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

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


---

## Disconnecting a Virtual Device

When the KVM Client is closed, the virtual media connection to the target server is closed. Devices are also disconnected when switching the KVM Client to a different port or RemoteAccess-GATE.

You can also use the Disconnect or Unmount button without closing the current KVM Client.

### ► To disconnect the virtual peripheral device(s):

1. It is highly recommended to first "safely remove" or "eject" the virtual media drive that you want to disconnect from the target server. If you have enabled the read/write mode, it may result in data loss when you do not perform this operation.
  - Refer to the user documentation of the target server's operating system for how to "safely remove" or "eject" a drive.
2. Click  to open the "Audio, Mass Storage and SmartCard Devices" dialog.

Existing virtual devices are listed in the Connected Devices section.



The devices that you can no longer mount onto the target server are disabled. Hover your mouse for a tooltip showing reasons.


3. Click the Disconnect button for the device you want to disconnect.
  - Click the Unmount button if you are disconnecting the smart card reader.
4. Click Yes on the confirmation message.

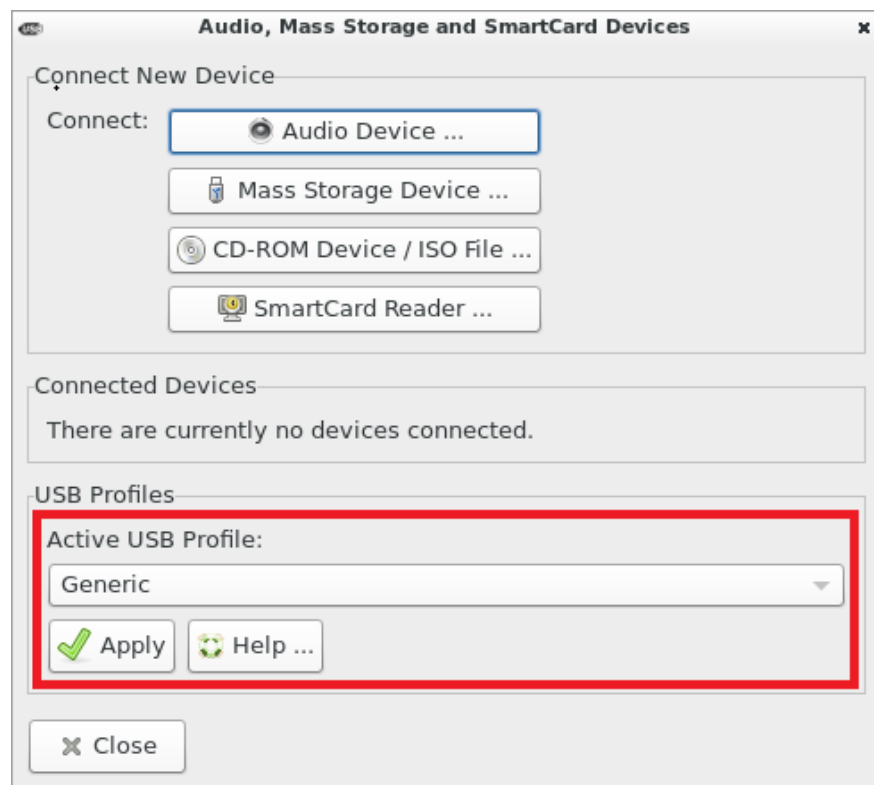
---

## USB Profiles

Usually the "Generic" USB profile works fine for most target servers. In case any of your target servers requires a special USB profile to have the remote audio devices, virtual media and card reader work properly, select a different USB profile for it.

► **To apply an appropriate USB profile to the target server:**

1. Click  to open the "Audio, Mass Storage and SmartCard Devices" dialog.
2. Click USB Profiles to expand it.



3. Select the desired USB profile from the Active USB Profile drop-down list, and click Apply.
  - If intended, click the Help button to view information similar to ***USB Profile Overview*** (on page 80).
  - For detailed information of each USB profile, see the section titled "Available USB Profiles" in the RemoteAccess-GATE's manual, which is accessible from the website ([www.gdsys.com](http://www.gdsys.com)).

### USB Profile Overview

Audio and mass storage devices are connected to the target server via USB ports of the CIM. Most of the time, this works without any problems. However, if you encounter any compatibility issues, you may have to change the USB configuration of the CIM.

G&D provides a standard selection of USB configuration profiles for a wide range of operating system and BIOS-level server implementations. These are intended to provide an optimal match between remote USB device and target server configurations.

The 'Generic' profile meets the needs of most commonly deployed target server configurations.

Additional profiles are made available to meet the specific needs of other commonly deployed server configurations (for example, Linux® and Mac OS X®).

There are also a number of profiles (designated by platform name and BIOS revision) to enhance virtual media function compatibility with the target server, for example, when operating at the BIOS level.

Administrators configure the KVM port with the USB profiles that best meet the needs of the user, and the target server configuration.

A user connecting to a target server chooses among these preselected profiles in the KVM Client, depending on the operational state of the target server.

For example, if the server is running Windows® operating system, it would be best to use the Generic profile.

To change settings in the BIOS menu or boot from a virtual media drive, depending on the target server model, a BIOS profile may be more appropriate.

If none of the standard USB profiles provided by G&D work with a provided target server, contact G&D Technical Support for assistance.

For detailed information of available USB profiles, refer to the user documentation of the RemoteAccess-GATE.

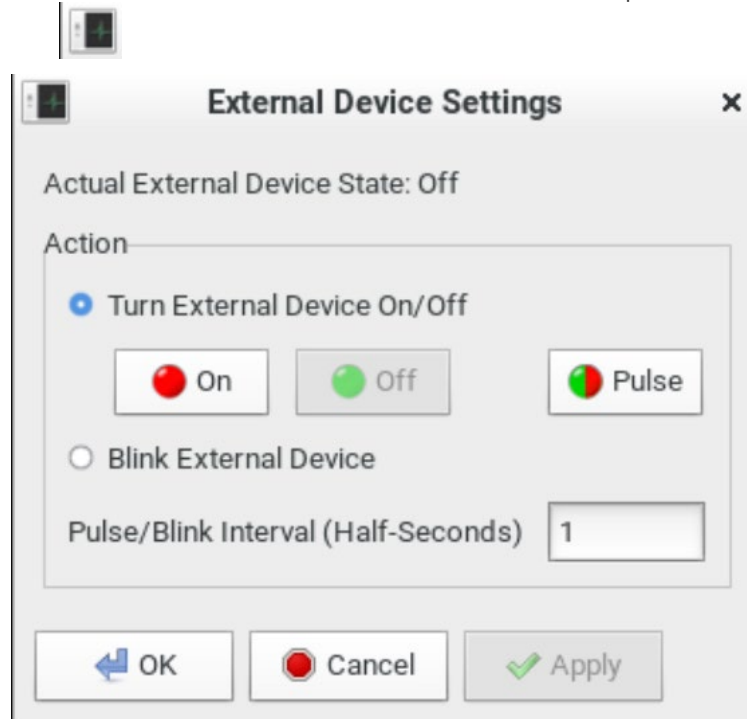


---

## External Device Control

RemoteAccessGATE targets may have connected external devices that can be controlled.


1. Click the External Device icon in the toolbar to open the settings:

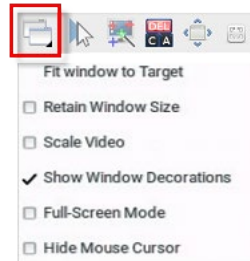


2. The device state is listed.
3. Enabled devices can be controlled using the Actions options.
  - Turn External Device On/Off: Click On or Off to control terminal output relay.
  - Pulse External Device: Sends a pulse to the device, either off to on, or on to off. Initial state of pulse can be changed by clicking button "On" and "Off".
  - Blink External Device: Enter the half-second interval to control blinking of the external device.
4. Click OK.

---

## View Settings

Click  to show available view options.





---

### Fit window to Target

The "Fit window to Target" command enlarges or shrinks the size of the KVM Client window to the target server's video resolution.

The KVM Client's scroll bars may or may not appear, depending on whether the target server's resolution is small enough for the KVM Client window to show the target server's entire desktop video.

#### ► To fit the KVM Client window to the target server:

- Click  > Fit window to Target.
- OR click .

---

### Retain Window Size

The Retain Window Size setting prevents changes made to the resolution of the target from affecting the KVM client's window size. The KVM client will display scroll bars or black borders when window size is retained.

---

### Scale Video

Selecting the Scale Video checkbox increases or reduces the size of the target server's video to fit the KVM Client window size.

This feature maintains the aspect ratio so that you see the entire target server's desktop without using the scroll bars.

---

*Tip: You can have this display option automatically enabled or disabled by setting your preferences on the KVM Client Settings page. See **Access Client Settings** (on page 88).*

---

#### ► To toggle video scaling:

- Click  > Scale Video.

---

### Show Window Decorations

You can use the KVM Client with or without the window decorations, including the window title and scroll bars.

---

*Tip: You can have this display option automatically enabled or disabled by setting your preferences on the KVM Client Settings page. See **Access Client Settings** (on page 88).*

---

#### ► To toggle the display of the window decorations:

- Click  > Show Window Decorations.



---

### Full-Screen Mode

When you enter full screen mode, the target server's video displays in the full screen and acquires the same resolution as the target server.

In full screen mode, the KVM Client's scroll bars are invisible, and its toolbar displays for several seconds only before disappearing from the screen.



#### ► To enter full screen mode:

1. Click  > Full-Screen Mode, or click .
2. A message indicating that the toolbar will be hidden and the key combination to trigger it temporarily displays on the screen and then disappears.

► **To display the toolbar in this mode:**

- Move your mouse to the top of the screen.


► **To exit full screen mode:**

- Press Ctrl+Alt+F on your keyboard.
- OR click  in the toolbar.
- OR click  > Full-Screen Mode.

---

### Cursor Shape

Select a Cursor Shape to customize the visible cursor, or use a transparent cursor to hide the RemoteAccess-Workplace's mouse cursor in the video area of the screen. The transparent mouse cursor is still visible in the toolbar area of the screen.

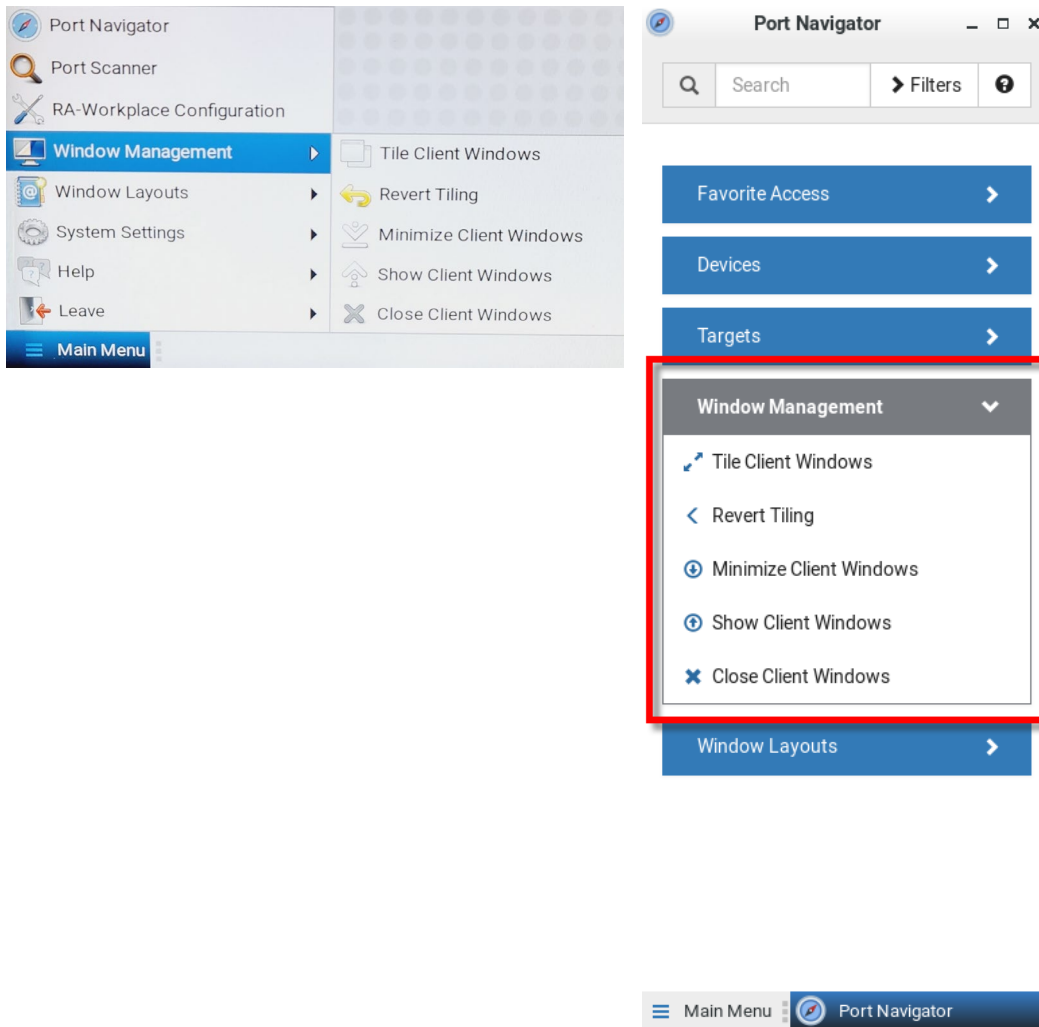
- Click  > Cursor Shape, then select from the list.
  - Default arrow
  - Dot
  - Crosshair
  - Transparent

---

## Window Management

Window Management helps you organize open sessions. All client types are included. Other RemoteAccess-Workplace windows, such as Port Navigator and the Port Scanner, are not included in window management. If two monitors are connected to the RemoteAccess-Workplace, the feature works separately on each monitor. Windows are not moved from one monitor to another. Windows crossing the edges of the monitor are restored so that the windows are fully within the monitor.

For information about saving and restoring window layouts, see ***Window Layouts*** (on page 101).



► **To use Window Management:**

1. Choose Main Menu > Window Management, then select an option.  
OR
2. Open the Port Navigator, then open the Window Management panel to select an option.

- Tile Client Windows: arranges all client windows in a tiled layout on desktop. Minimized windows will be unminimized.
- Revert Tiling: Undo last tiling operation and restore previous window sizes. Previously minimized windows will be minimized again.
- Minimize Client Windows: Minimizes all client windows from desktop to task bar.
- Show Client windows: Restores all client windows from task bar and to desktop
- Close Client Windows: Closes all client windows.

---

## Dual Video Port Connections

When connecting to a Dual Video port, two KVM client windows are opened. The two client windows are bound to each other.

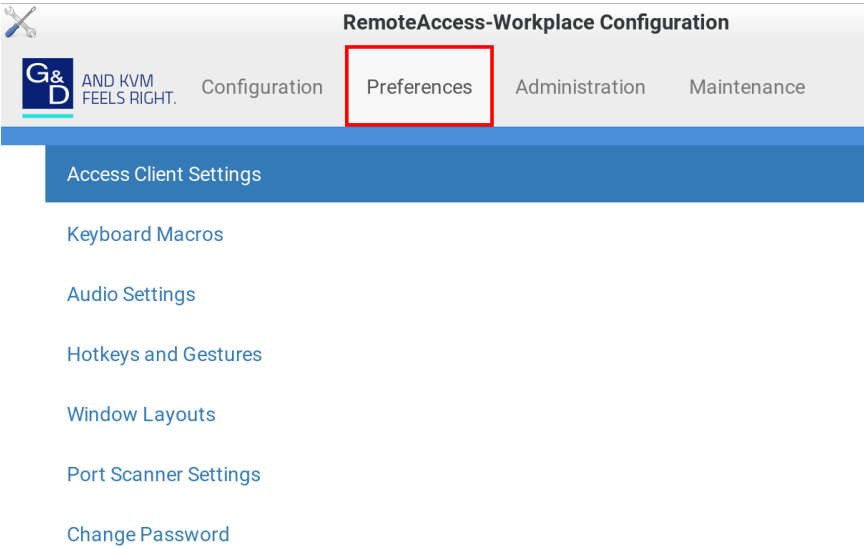
Window title: [<group\_name>] port\_name.

When one window is closed, the other one is closed automatically

Switching to and from Dual Video ports is not possible. When switching from a single port to a Dual Video port, the old connection is closed prior to connecting. When switching from a Dual Video port to another port, the connections are closed prior to connecting to the new port.

# Setting User Preferences

In the RemoteAccess-Workplace Configuration window, click Preferences to customize the following user settings.



## In This Chapter

Access Client Settings.....	88
Managing Keyboard Macros.....	93
Audio Settings.....	97
Hotkeys and Gestures .....	98
Window Layouts.....	101
Port Scanner Settings .....	103
Change Password.....	106

## Access Client Settings

You can configure settings for all access types, as well as general launch and connection settings. Users with the System Admin privilege can configure the default Access Client Settings for all new users.

- Video Target Window Settings
- Console Target Window Settings
- Web Target Window Settings
- Launch Settings
- Connection Settings

### ► To set your Access Client preferences:

1. If not displayed, launch the RemoteAccess-Workplace Configuration window. See **RemoteAccess-Workplace Configuration** (on page 10).
2. Click Preferences > Access Client Settings. The Access Client Settings page opens, showing the current preferences.
  - ☒ indicates the setting is enabled.
  - ☐ indicates the setting is disabled.

Video Target Window Settings	
Scale Video	<input type="checkbox"/> (KVM, VNC)
Positioning	Automatic (KVM, VNC)
Window Decorations	<input checked="" type="checkbox"/> (KVM, VNC, RDP, ESXi)
Show Tool Bar	<input checked="" type="checkbox"/> (KVM, VNC)
Full-Screen Mode	<input type="checkbox"/> (KVM, VNC, RDP, ESXi)
Single Mouse Cursor Mode	<input type="checkbox"/> (KVM)
Cursor Shape	Default (KVM, VNC)
Disable Banner Messages	<input type="checkbox"/> (KVM, VNC)
Resizing Behavior	Fixed Size (RDP)
Transmission Quality	Medium (RDP)
Preferred Resolution	1024 x 768 (RDP)
Display as Multi-Monitor Target	Disabled (RDP)
Desktop Scaling	100% (RDP)

3. Click Edit to make changes.
  - Video Target Window Settings: These selections determine the initial settings applied to the video targets with the Access Client.

---

*Note: You cannot connect to individual targets in a multi-monitor group.*

---



Scale Video	Enable or disable the Scale Video function. For details on Scale Video, see <b><i>Scale Video</i></b> (on page 83).
Positioning	<p>Determines where the Access Client shows up on the screen:</p> <ul style="list-style-type: none"> <li>▪ <b>Automatic:</b> The positioning of the Client is not restricted. For example, the first Client that appears may align with the top-left corner of the screen, but the second Client may align with the bottom-right corner of the screen.</li> <li>▪ <b>Left Upper Corner</b></li> <li>▪ <b>Right Upper Corner</b></li> </ul> <p>Note: For dual or multi-KVM targets, if more than two windows are involved, all windows will be launched in the Left Upper Corner.</p>
Window Decorations	Show or hide the window decorations. For details on window decorations, see <b><i>Show Window Decorations</i></b> (on page 83).
Show Tool Bar	Show or hide the client tool bar.
Start in Full-Screen Mode	<p>Enable or disable full-screen mode for KVM sessions.</p> <p>To exit full-screen mode, press Ctrl + Alt + F in the KVM Client.</p>
Start in Single Mouse Cursor Mode	<p>Enable or disable starting in single mouse mode.</p> <p>Note: When this setting is enable, you must click into the KVM window to locate the mouse when you begin the session.</p> <p>For details on this mouse mode, see <b><i>Single Mouse Cursor</i></b> (on page 59).</p> <p>For details on how this works with dual monitor targets, see <b><i>Single Mouse Mode for Dual Monitor Targets</i></b> (on page 93).</p>

Cursor Shape (in Double Cursor Mode)	Select customized cursor shape. <ul style="list-style-type: none"> <li>Default, Dot, Crosshair, Transparent</li> <li>Use the Transparent option to hide the mouse cursor.</li> </ul>
Disable Banner Messages	Select to remove banner messages from KVM and VNC sessions.
Resizing Behavior	Select resize preference for RDP sessions: <ul style="list-style-type: none"> <li>Fixed size, Dynamic Resolution Change, Scale</li> </ul>
Transmission Quality	Select preferred transmission quality for RDP sessions: <ul style="list-style-type: none"> <li>Best Quality (Slowest), Medium, Fastest (Lowest Quality)</li> </ul>
Preferred Resolution	Select preferred resolution for RDP sessions.
Display as Multi-Monitor Target	Select multi-monitor preferences for RDP sessions: <ul style="list-style-type: none"> <li>Disabled, Use 2 monitors, Use 3 monitors, Use all monitors.</li> </ul>
Desktop Scaling	<ul style="list-style-type: none"> <li>Select a desktop scaling percentage for RDP sessions.</li> </ul>

- Console Target Window Settings: These options apply to SSH and Serial access.

Console Target Window Settings	
<b>Window Decorations</b>	<input checked="" type="checkbox"/> (SSH, Ser)
<b>Show Menu Bar</b>	<input checked="" type="checkbox"/> (SSH)
<b>Full-Screen Mode</b>	<input type="checkbox"/> (SSH, Ser)
<b>Console Size</b>	80 x 24 (SSH, Ser)

Window Decorations	Show or hide the window decorations. For details on window decorations, see <b>Show Window Decorations</b> (on page 83).
Show Menu Bar	Show or hide the menu bar.

Start in Full-Screen Mode	<p>Enable or disable full-screen mode for console sessions.</p> <p>For SSH and Serial, the hot key for full screen is F11.</p> <p>To exit full-screen mode, press Ctrl + Alt + F in the KVM Client.</p>
Console Size	Select the preferred console size. Serial Client size may not be accurate.

▪ Web Target Window Settings:

Web Target Window Settings	
Window Decorations	<input checked="" type="checkbox"/> (WEB)
Show Tool Bar	<input checked="" type="checkbox"/> (WEB)
Full-Screen Mode	<input type="checkbox"/> (WEB)

Window Decorations	<p>Show or hide the window decorations.</p> <p>For details on window decorations, see <b><i>Show Window Decorations</i></b> (on page 83).</p>
Show Tool Bar	Show or hide the tool bar.
Start in Full-Screen Mode	<p>Enable or disable full-screen mode for web sessions.</p> <p>For web sessions, the full screen hot key is F11.</p> <p>To exit full-screen mode, press Ctrl + Alt + F in the KVM Client.</p>

- Launch Settings: These options configure the mouse button click behavior at the Port Navigator, the default action for the Port Hotkeys, and the launching of multiple KVM sessions to one target (when PC share is enabled). Options apply to KVM and VNC Access Clients only.

**Launch Settings**

<b>Left Mouse Button Click</b>	Switch existing Access Client
<b>Left Button Double Click</b>	Open a new Access Client
<b>Middle Button Click</b>	Open a new Access Client
<b>Port Hotkey Action</b>	Switch existing Access Client
<b>Multiple Sessions to one Target</b>	<input type="checkbox"/>

Switch existing Access Client	Switches the last active Access Client to the selected port or access point, if possible. Otherwise a new Access Client is opened.
Open a new Access Client	Always launches a new Access Client.
Open a new Access Client on secondary monitor	Always launches a new Access Client on the secondary monitor, if available.
Multiple Sessions to One Target: Enabled	Launches multiple KVM sessions to one new KVM target if: (1) Open a New Access Client is selected where RemoteAccess-Workplace creates a second window for this target, and (2) PC Share is enabled.

- Connection Settings: Selecting the "Warn if a Virtual Media Connection is about to be disconnected" checkbox will cause a warning message to display if this event occurs.

**Connection Settings**

If a KVM Client is switched to another port while a Virtual Media Connection is established, then the Virtual Media Connection is terminated. With this option you can choose whether you want to see a warning in this case.

☐ Warn if a Virtual Media Connection is about to be disconnected

1. Click Save. Note additional options when settings have been configured:
  - To save these settings as the default for all new users, click Set as Default. System Admin privilege required.

- To delete all target/port-specific access client settings for the current user, click Reset all Target Specific.

Edit

Set as Default

Reset all Target Specific

---

### Single Mouse Mode for Dual Monitor Targets

When Start in Single Mouse Cursor Mode is enabled for a dual monitor target:

- The top-left display KVM client is brought to front (instead of the primary) because this one controls the mouse.

---

## Managing Keyboard Macros

Keyboard macros can be created to use instead of physical keystroke combinations, so that the actions intended for the target server are sent to and interpreted only by the target server. Otherwise, they might be interpreted by the RemoteAccess-Workplace itself.

Keyboard macros are stored on the RemoteAccess-Workplace, and only the user who created them can see and use these macros.

### ► To create a keyboard/hotkey macro:

1. If not displayed, launch the RemoteAccess-Workplace Configuration window. See *RemoteAccess-Workplace Configuration* (on page 10).
2. Click Preferences > Keyboard Macros > New Keyboard Macro. The New Keyboard Macro page opens.

## New Keyboard Macro

☒ Enabled

\* Name

\* Sequence

Key Sets:

Keys:

Left Ctrl  
Right Ctrl  
Left Alt  
Right Alt  
Left Shift  
Right Shift  
Scroll Lock  
Caps Lock  
Num Lock  
Left Windows Key

▶  
▲  
▼  
◀

Save Cancel

- Enter information for the new keyboard macro. The fields marked with the symbol \* are mandatory.

Field/option	Description
Enabled	Select this checkbox so that the new macro can appear in the KVM Client of this RemoteAccess-Workplace. See <b><i>Executing Macros</i></b> (on page 95).
Name	Type a name for the new macro.
Key Sets	Select the key set containing the desired keys. See Available Key Sets. All keys that the selected key set contains are listed in the Keys box.
Keys	Select each desired key from the list and click ▶ to add it to the right box. Double-click also adds. <ul style="list-style-type: none"> <li>Select the keys in the order by which they are to be pressed.</li> <li>A Release key command is automatically added for each key added to the right box. See <b><i>Keyboard Macro Example</i></b> (on page 96).</li> </ul>


- If needed, make changes to the keys shown in the right box.

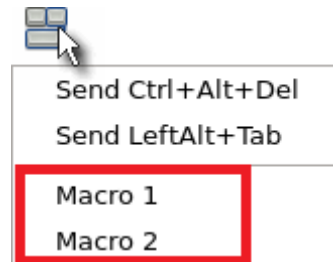
- To resort the key commands, select a key command and click ▲ or ▼ to move it up or down.
  - To remove a key command, select it and click ◀.
5. Click Save, and the new macro's content is shown.
  6. Click one of these buttons according to your needs.
    - Back: Return to the Keyboard Macro page.
    - Edit: Modify this macro.
    - Delete: Remove this macro.

---

### Executing Macros

Manually-created keyboard macros, if they are enabled, appear following the pre-programmed keyboard macros in the keyboard pull-down list of the KVM Client. See *Using the KVM Client* (on page 52).

Click  to show the keyboard macro list, and select the desired macro to send it to the target server.














## Editing or Deleting Macros

To view all manually-created keyboard macros in the RemoteAccess-Workplace Configuration window, click Preferences > Keyboard Macros.


### Keyboard Macros

[New Keyboard Macro](#)


Enabled	Name ^	Actions
	macro 3	 Edit  Delete
	macro 2	 Edit  Delete
	macro 1	 Edit  Delete

- Click the Name column header to sort the list.
- An enabled macro shows  in the Enabled column.
- A disabled macro shows .

#### ► To edit a keyboard macro:

1. Click the desired macro's  Edit button.
2. Make necessary changes to the information shown. See *Managing Keyboard Macros* (on page 93).

#### ► To delete a keyboard macro:

1. Click the desired macro's  Delete button.
2. Click OK on the confirmation message.

## Keyboard Macro Example

For example, you can create a keyboard macro to close a window by selecting Left Alt+F4.

The macro's content looks like the following.

```
Press Left Alt
Press F4
Release F4
Release Left Alt
```



## Audio Settings

The default audio playback/capture devices used by the RemoteAccess-Workplace are the front-panel analog speakers and microphone.

You can change this by setting other audio devices you prefer as the audio playback and/or capture devices. Note that the audio configuration changes made by any user apply on a RemoteAccess-Workplace basis so the changes impact all users of this RemoteAccess-Workplace.

► **To determine the audio appliances used by the RemoteAccess-Workplace:**

1. If not displayed, launch the RemoteAccess-Workplace Configuration window. See *RemoteAccess-Workplace Configuration* (on page 10).
2. Click Preferences > Audio Settings. The Audio Settings page opens, indicating the current audio playback and capture devices being used.


## Audio Settings

Speaker and Microphone Defaults

**Speaker:** Speaker / Headphones (Built-in Audio)


**Microphone:** Microphone (Built-in Audio)


Edit

3. Click Edit, if intending to make changes.
4. In the Speaker section, select the audio playback device you prefer.
  - The audio playback devices which are not available are marked with .
5. In the Microphone section, select the audio capture device you prefer.
6. Click Save.
7. (Optional) To test whether the currently selected speaker works, click the Test Speaker buttons.

Test Speaker

Play Audio:

Left Speaker 

Right Speaker 

---

## Hotkeys and Gestures

You can enable, disable and customize hotkeys and gestures to control the RemoteAccess-Workplace, manage windows, or control KVM Client functions. These hotkeys and gestures are executed on the RemoteAccess-Workplace rather than being transmitted to any target servers you are operating. Many functions are programmed and enabled by default.

For a complete list of pre-programmed hotkeys of the RemoteAccess-Workplace, go to Main Menu > Help > Help on Hotkeys, and see ***Help on Hotkeys*** (on page 3).

There are several categories of hotkeys and gestures:

- **RemoteAccess-Workplace Functions Hotkeys:** Configure hotkeys that are always processed locally by the RemoteAccess-Workplace desktop. They are not sent to a target server if you use them from within a KVM session. If you want to use any of these key combinations, such as Alt+Tab or Ctrl+Alt+Delete, in KVM sessions, you should make sure that key combination is not assigned in this category, or disable that function it is assigned to.
- **Window Management Hotkeys and Gestures:** Configure hotkeys to close windows, switch between windows, or move them around on your desktop.
  - When Switch Keys is enabled, you can use Shift + Windows + Arrow to switch between open windows.
  - Move Keys are key combinations that move the foreground window around on the desktop. You can disable this function. See ***Move Keys*** (on page 100).
  - When Dragging with Alt Key is enabled, you can drag windows around on the RemoteAccess-Workplace desktop using the mouse. Disable this feature if you want Alt Drag to apply to the target server.

- **KVM Client Hotkeys:** Configure hotkeys for functions within the KVM Client. Note that if you disable the hotkey for single mouse mode, this function is disabled.
- **KVM Port Hotkeys:** Hotkeys that have been configured for ports appear here.
- **Target Access Hotkeys:** Configure hotkeys for functions within the SSH, VNC and RDP clients. Hotkeys that have been configured in those clients appear here.
- **Window Layout Hotkeys:** Configure hotkeys to manage your window layouts. See *Window Layouts* (on page 101).

► **To configure hotkeys and gestures:**

1. Launch the RemoteAccess-Workplace Configuration window.
2. Click Preferences > Hotkeys and Gestures. The Hotkeys and Gestures page opens, showing the current settings for all categories.
3. Scroll down and click Edit to make changes:
  - To enable, select a key combination for the function from its drop-down list.
  - To disable, select Disabled from its drop-down list.
4. Click Save.

RA-Workplace Functions Hotkeys

Port Navigator

Ctrl+Alt+N

RemoteAccess-Workplace Configuration

Ctrl+Alt+C

Port Scanner

Shift+Alt+P

Tile KVM Windows

Disabled

Revert Tiling

Disabled

Minimize KVM Windows

Disabled

Show KVM Windows

Disabled

Save

Cancel

The hotkeys configured here are always processed locally by the RemoteAccess-Workplace desktop. They are not sent to target servers if you use them from within a KVM session.

If you want to use such hotkeys as Alt+Tab or Ctrl+Alt+Delete in a KVM session, you should reconfigure these desktop hotkeys to different key combinations or disable them.

### Move Keys

Move Keys are key combinations that move the foreground window around on the desktop. You can enable or disable these hotkeys using the "Move Keys" setting. See *Hotkeys and Gestures* (on page 98).

Hotkey	Function
Ctrl + Alt + Shift + ⬅	When there are two monitors connected, move the window to the other monitor.
Ctrl + Alt + Shift + ➡	
Ctrl + Alt + ⬆	Move the window to the screen edge in the specified direction on the monitor.
Ctrl + Alt + ⬇	
Ctrl + Alt + ⬅	
Ctrl + Alt + ➡	
Ctrl + Alt + 1 (on the keypad)	Move the window to the screen corner in the specified direction on the monitor.
Ctrl + Alt + 3 (on the keypad)	
Ctrl + Alt + 7 (on the keypad)	
Ctrl + Alt + 9 (on the keypad)	
Ctrl + Shift + ⬆	Move the window, in the specified direction, to the nearest edge, which is one of the following: <ul style="list-style-type: none"> <li>▪ Borders of another window</li> <li>▪ Monitor edges in the dual-monitor configuration</li> <li>▪ Desktop boundaries</li> </ul>
Ctrl + Shift + ⬇	
Ctrl + Shift + ⬅	
Ctrl + Shift + ➡	
Ctrl + Windows + ⬆	Enlarge the window in the specified direction until its border touches the nearest edge, which is one of the following: <ul style="list-style-type: none"> <li>▪ Borders of another window</li> <li>▪ Monitor edges in the dual-monitor configuration</li> <li>▪ Desktop boundaries</li> </ul> <p><i>Note: If the window border already aligns with the screen edge, the window size shrinks instead.</i></p>
Ctrl + Windows + ⬇	
Ctrl + Windows + ⬅	
Ctrl + Windows + ➡	

Hotkey	Function
Alt + Windows + ↑	Shrink the window in the specified direction until its border touches the nearest edge, which is one of the following: <ul style="list-style-type: none"> <li>▪ Borders of another window</li> <li>▪ Monitor edges in the dual-monitor configuration</li> <li>▪ Desktop boundaries</li> </ul> <hr/> <i>Note: If no nearest edges are found in the specified direction, the window size is halved instead.</i>
Alt + Windows + ↓	
Alt + Windows + ←	
Alt + Windows + →	

### Switch Keys

Switch keys allow you to switch between open windows using Shift + Windows + Arrow keys.

To enable or disable switch keys, see *Hotkeys and Gestures* (on page 98).

## Window Layouts

The window layouts feature allows you to save layouts of running access client windows so that the specific layout can be restored upon selection. The window layout data that is saved includes the visual attributes of each access client session, such as size, position, and displaying monitor, as well as the connection information for each.

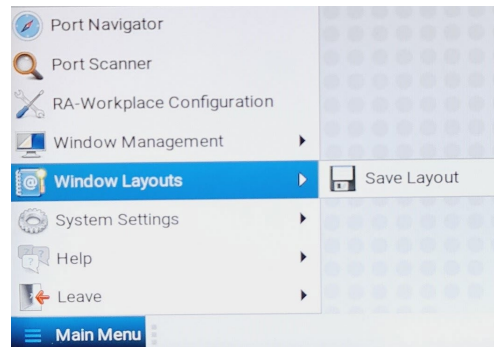
Layouts are saved on a per user basis. The layouts saved by one user are not available to other users. There is a maximum of 16 named layouts per user.

You can access Window Layouts in the Port Navigator or the Main Menu.

### ► To save a layout:

1. Arrange your client windows as desired. They can be freely sized and positioned across all monitors.

2. In Main Menu: Click Window Layouts > Save Layout. If previously saved layouts exist, the menu also includes an option to save as new, or overwrite a named layouts, such as Save Layout (current layout name). New layouts are automatically assigned names.



3. A desktop notification pops up to confirm the layout is saved and to display the name.

### ► To restore a layout:

- In Main Menu: Click Window Layouts, then click the named layout you want to restore.

When the layout is selected, all currently open clients are closed, and the selected layout is restored.

Upon restoring a layout, some targets may not be available. The clients for those targets are restored anyway with their visual attributes and an error message that their target cannot be connected.

### ► To manage layouts:

The tools for window layout management allow you to set a layout to be restored upon login, rename or delete layouts, and assign hotkeys to layouts.

- In RemoteAccess-Workplace Configuration: Click Preferences > Window Layouts.
1. Login Layout: The layout that is restored on a user's login.
    - None: default, no layout is restored upon login.
    - As saved on last logout: Upon the next logout, the state of all clients is saved as a layout, and this layout is restored on the next login. This type of saved layout does not overwrite a named layout that is selected at the time of logout.
    - List of named layouts: Select a named layout from your list of saved layouts.
  2. Saved Layouts: Lists all named layouts and provides options.
    - Each layout has options to Restore, Edit or Delete.

- Click Restore to open the layout now. This option works the same as the Main Menu: Window Layouts selection.
- Click Edit to change the name or hotkey. Names must be 4-32 characters. Hotkeys will be verified for availability.
- Click Delete on a layout, or select multiple layouts and click Delete Selected to remove layouts. Click to confirm deletion.

---

## Port Scanner Settings

You can configure the scanner intervals, delays, and orientation, and specify storage of snapshots from the scanner. Note that you can also configure intervals and orientation from the Port Scanner window. See ***Scanner Options*** (on page 47). However, snapshot settings only appear in the User Preferences > Port Scanner Settings page.

When enabled, snapshots are stored on an accessible USB device. The image saved is the thumbnail image from the scanner. Sub-directories are created on the USB drive per RemoteAccess-GATE, named after the device, port by number and name. Images are named by timestamp. Duplicate RemoteAccess-GATEs with the same name will all use the same directory.

You must have the "Scanner Snapshots" permission to capture snapshots from the scanner. See ***User Groups*** (on page 111).

### ► To configure port scanner settings:

1. If not displayed, launch the RemoteAccess-Workplace Configuration window. See ***RemoteAccess-Workplace Configuration*** (on page 10).
2. Click Preferences > Port Scanner Settings. The Port Scanner Settings page opens, showing the current preferences.
  - ☒ indicates the setting is enabled.
  - ☐ indicates the setting is disabled.

## Port Scanner Settings

Intervals and Delays
<b>Port Display Interval</b> 10 Seconds
<b>Interval between Ports</b> 1 Second

Snapshot Recording
<b>Enable Snapshot Recording</b> <input type="checkbox"/>
<b>Snapshot Recording Storage</b>

Settings
<b>Thumbnails Orientation</b> Vertical
<b>Use Grid View for Thumbnails</b> <input checked="" type="checkbox"/>
<b>Pause Scanner when opening KVM Sessions</b> <input checked="" type="checkbox"/>

Edit

- Click Edit to make changes.
- To set Intervals and Delays:
  - Port Display Interval (1..300 sec): Select the number of seconds to display each port before switching to next
  - Interval between Ports: Select the number of seconds to pause after Port Display Interval ends.



Intervals and Delays

Please choose the intervals for the Port Scanner here.

**Port Display Interval:** Select the number of seconds to display each port before switching to next.

**Interval between Ports:** Select the number of seconds to pause after Port Display Interval ends.

Port Display Interval (1 .. 300 sec)

10

Interval between Ports (0 .. 60 sec)

1

5. To set Snapshot Recording:
  - Enable Snapshot Recording: Click the checkbox to turn the feature on.
  - Make sure a USB drive is accessible.
  - Make sure you have the Record Scanner Snapshots privilege.

Snapshot Recording

The Port Scanner is able to save snapshot images of the target port to an external storage. Please select here if you want to enable this, and choose the external storage.

**Notes:**

- In order to save snapshots, insert a USB-Storage, such as a USB flash drive.
- You need to have the *Record Scanner Snapshots* privilege in order to save snapshots.

☐ Enable Snapshot Recording

No USB drive available

6. To configure remaining preferences:
  - **Thumbnails Orientation:** Select Vertical or Horizontal to position thumbnails in relation to scan window.
  - Select the **Use Grid View for Thumbnails checkbox** for an optional grid view that shows all thumbnails at once without scroll bars.
  - Select the **Pause Scanner when opening KVM Sessions** checkbox if the scanning should stop when you open a port into a full KVM session.

### Settings

Select additional settings:

**Thumbnails Orientation:** Select Vertical or Horizontal to position thumbnails in relation to scan window.

Select the **Use Grid View for Thumbnails** checkbox for an optional grid view that shows all thumbnails at once without scroll bars.

Select the **Pause Scanner when opening KVM Sessions** checkbox if the scanning should stop when you open a port into a full KVM session.

#### Thumbnails Orientation

Vertical

Use Grid View for Thumbnails ☒

Pause Scanner when opening KVM Sessions ☒

7. Click Save.

---

## Change Password

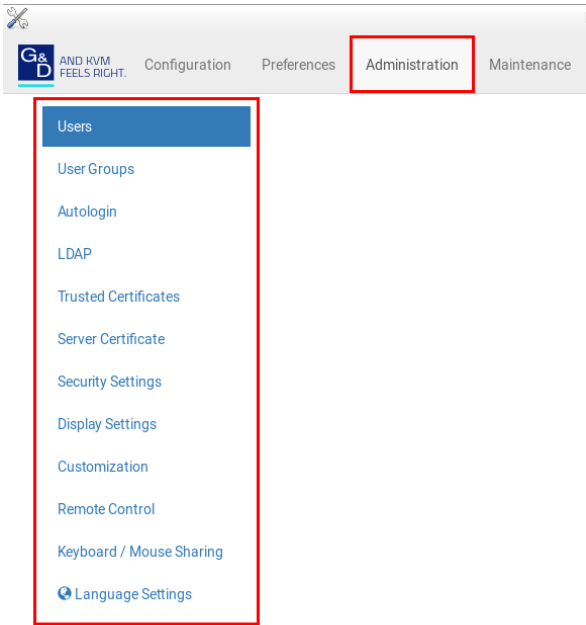
You can change your own password.

### ► To change your password:

1. If not displayed, launch the RemoteAccess-Workplace Configuration window. See ***RemoteAccess-Workplace Configuration*** (on page 10).
2. Click Preferences > Change Password. The Change Password page opens, and you can enter new password.
3. Click Save.

# Administration Features

In the RemoteAccess-Workplace Configuration window, click Administration to perform the following RemoteAccess-Workplace administration tasks.



## In This Chapter

Users .....	108
User Groups.....	111
Autologin.....	115
LDAP .....	116
Trusted Certificates.....	131
Server Certificate .....	134
Security Settings .....	138
Display Settings.....	144
Customization.....	146
Remote Control .....	149
Keyboard/Mouse Sharing.....	154
Language Settings.....	159

---

## Users

The RemoteAccess-Workplace provides a built-in administrator account, which is ideal for initial login and system administration.

### User

The screenshot shows the configuration page for a user named 'admin'. The fields are as follows:

<b>Login:</b>	admin
<b>Type:</b>	Local
<b>Name:</b>	Administrator
<b>Email:</b>	
<b>Privileges:</b>	System Administration Take Screenshots Device Administration SSH Access RDP Access VNC Access Device Access
<b>User Groups:</b>	

At the bottom of the form, there are two buttons: 'Back to all Users' and 'Edit'.

You can add user profiles with configurable privileges for other users to operate and administer the RemoteAccess-Workplace.

Note that the RemoteAccess-Workplace's user profiles determine the permissions users are granted to have on the RemoteAccess-Workplace instead of the RemoteAccess-GATEs. See ***Authentication of RemoteAccess-Workplaces and RemoteAccess-GATEs*** (on page 212).

#### ► To create a user profile:

1. If not displayed, launch the RemoteAccess-Workplace Configuration window. See ***RemoteAccess-Workplace Configuration*** (on page 10).
2. In the RemoteAccess-Workplace Configuration menu, click Administration > Users > New User. The New User page opens.

## New User

**\* Login**

  
☐ Authenticate via LDAP  

**Email**

**Name**

**\* Password**

**\* Password confirmation**

**\* Selected User Groups**

◀◀

◀

▶

▶▶

**Available User Groups**

System Administrators  
Devices Administrators  
Devices Users

3. Enter information for the new user. The fields marked with \* are mandatory.

Field	Description
Login	User name for logging in to the RemoteAccess-Workplace. <ul style="list-style-type: none"> <li>2 to 255 characters</li> <li>Restricted character: colon (:)</li> </ul>
Authenticate via LDAP	Select this checkbox if this user will be authenticated via LDAP. See <b>LDAP</b> (on page 116). If deselected, this user is authenticated via the local database of the RemoteAccess-Workplace and you must store user passwords on the RemoteAccess-Workplace.
Email	The email address to reach the user.
Name	Real name or nickname of the user.

Field	Description
Password, Password confirmation	Password for logging in to the RemoteAccess-Workplace. A minimum of five characters are required.
Selected User Groups	Assigning user groups determines the permissions granted to this user. See <b>User Groups</b> (on page 111). <ul style="list-style-type: none"> <li>Use the arrow buttons to move the user groups as needed. The user will be a member of the groups in the Selected User Groups list.</li> </ul>

- Click Save, and the new user profile's content is shown.

## Editing or Deleting Users

To view existing user profiles in the RemoteAccess-Workplace Configuration window, click Administration > Users.

Select an option in the Type field to show the desired user types. Note that this field is configurable only for users with the "System Administration" permission.

- Local:** Shows local users only, who are authenticated via the RemoteAccess-Workplace's local database. This is the default when the LDAP authentication is disabled.
- LDAP:** Shows the users who are authenticated via LDAP. This is the default when the LDAP authentication is enabled.
- All:** Shows all users, including Local, and LDAP. You must be the admin user to view all users.

## Users


Delete Selected
New User

<input type="checkbox"/>	Login	Name	Type	User Groups	Actions
<input type="checkbox"/>	admin	Administrator	Local		<a href="#">Edit</a>
<input type="checkbox"/>	user 1	User 1	Local	System Administrators Devices Administrators Devices Users	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	user2	User 2	Local	Devices Administrators	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	user3	User 3	LDAP Authenticated	Devices Users	<a href="#">Edit</a> <a href="#">Delete</a>


Click each user's login name to view details.

Note that you cannot delete the built-in *Admin* user, but you can modify its data other than the privileges (user groups).

► **To modify a user profile:**

1. Click the desired user's  **Edit** button. The Edit User page opens.
2. Make necessary changes to the information shown. See ***Users*** (on page 108).
  - You cannot change the login name.
  - To change the user's password, type the new password in the "Password" and "Password confirmation" fields. A minimum of five characters are required.
3. Click Save.

► **To delete a user profile:**

1. Click the desired user's  **Delete** button, or select the checkboxes for users you want to delete and click Delete Selected.
2. Click OK on the confirmation message.

---

## User Groups

A user group determines the privileges its members can have.

There are several factory default user groups.

User groups	Default privileges
System Administrators	System Administration. See <b><i>Privileges</i></b> (on page 113).
Devices Administrators	Device Administration. Device Access.
Devices Users	Device Access. Change Preferences.
Restricted Users	Device Access

The Restricted Users group lacks the Change Preferences privilege, so this group can be used for access-only users.

You can create a new user group if the default user groups do not satisfy your needs.

► **To create a new user group:**

1. If not displayed, launch the RemoteAccess-Workplace Configuration window. See *RemoteAccess-Workplace Configuration* (on page 10).
2. Click Administration > User Groups > New User Group. The New User Group page opens.

## New User Group

**\*Name**

**\*Privileges**

- ☐ Device Access
- ☐ ESXi Access
- ☐ WEB Access
- ☐ VNC Access
- ☐ RDP Access
- ☐ SSH Access
- ☐ Change Preferences
- ☐ Device Administration
- ☐ Record Scanner Snapshots
- ☐ Take Screenshots
- ☐ System Administration

**Device Access** includes the permission to:

- Login
- Open KVM and serial sessions

**VNC Access, RDP Access, SSH Access, WEB Access and ESXi Access** include:

- Open VNC, RDP, SSH, Web and ESXi sessions

**Change Preferences** includes:

- Alter personal settings

**Device Administration** includes:

- Change Preferences permission
- Device Access permission
- VNC Access, RDP Access, SSH Access, WEB Access and ESXi Access permissions
- Addition and removal of RA-GATE Devices
- Add, edit and remove VNC, RDP, SSH, Web and ESXi Access

**Take Screenshots** includes:

- Take a screenshot and export it to a USB drive

**Record Scanner Snapshots** includes:

- Record snapshots from the Port Scanner

**System Administration** permits everything

3. Enter information for the new user group.

Field	Description
Name	Type a name for the new user group.
Privileges	Assign one or multiple privileges to the new user group. See <i>Privileges</i> (on page 113).

4. Click Save, and the new user group's data is shown.



---

**Privileges**

Privilege	Operations permitted
Device Access	<ul style="list-style-type: none"> <li>Log in to the RemoteAccess-Workplace.</li> <li>Open KVM and serial sessions.</li> </ul>
ESXi Access WEB Access	<ul style="list-style-type: none"> <li>Open ESXi or WEB sessions.</li> </ul>
VNC Access RDP Access SSH Access	<ul style="list-style-type: none"> <li>Open VNC, RDP, and SSH sessions.</li> <li>This permission alone does not grant login privileges. User must also be a member of a group with System Administration, Device Administration or Device Access privileges.</li> </ul>
Change Preferences	<ul style="list-style-type: none"> <li>Alter personal settings</li> <li>Users who don't have this privilege cannot launch RemoteAccess-Workplace Configuration, window layouts, or system settings</li> </ul>
Device Administration	<ul style="list-style-type: none"> <li>Log in to the RemoteAccess-Workplace.</li> <li>Change Preferences permission.</li> <li>Device Access permission.</li> <li>ESXi Access, WEB Access, VNC Access, RDP Access and SSH Access permissions.</li> <li>RemoteAccess-GATE addition and removal.</li> <li>Add, edit and remove ESXi, WEB, VNC, RDP and SSH access.</li> </ul>
Take Screenshots	<ul style="list-style-type: none"> <li>Take a screenshot and export it to a USB drive using the hotkey.</li> <li>This permission alone does not grant login privileges. User must also be a member of a group with System Administration, Device Administration or Device Access privileges.</li> </ul>

Privilege	Operations permitted
Record Scanner Snapshots	<ul style="list-style-type: none"> <li>Record snapshots from the Port Scanner.</li> </ul>
System Administration	All operations on the RemoteAccess-Workplace are permitted.









## Editing or Deleting User Groups

To view all user groups in the RemoteAccess-Workplace Configuration window, click Administration > User Groups.

## User Groups

Delete Selected

New User Group

<input type="checkbox"/>	Name ↕	Privileges ↕	Users	Actions
<input type="checkbox"/>	Devices Administrators	Device Administration Device Access	Miles	 Edit  Delete
<input type="checkbox"/>	Devices Users	Change Preferences Device Access	Lulu Mila Orly	 Edit  Delete
<input type="checkbox"/>	Restricted Users	Device Access	Goldie	 Edit  Delete
<input type="checkbox"/>	System Administrators	System Administration	Omar	 Edit  Delete


The Users column lists the names of all users who belong to this user group. If the real name is not available in the user profile, the user's login name is shown. See **Users** (on page 108).

Each user group shows a maximum of five users in this view.


Click each user group's name to view its details.

You can delete any user group even if it contains users.

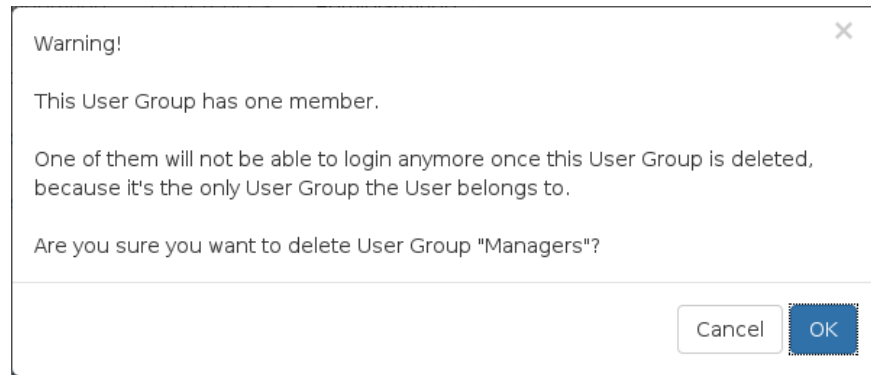
### ► To modify a user group:

1. Click the desired user group's  Edit button.
2. Make necessary changes to the information shown. See **User Groups** (on page 111).
3. Click Save.

### ► To delete a user group:

1. Click the desired user group's  Delete button.
2. A confirmation message appears.

- If any user will not be able to log in after losing this user group, the confirmation message shows a warning similar to the following diagram. This is because the selected user group is the only user group that one or some of the group members have.



3. Click OK to confirm the deletion or Cancel to abort it.

---

## Autologin

Enable the Autologin feature to allow a selected user to be automatically logged into the RemoteAccess-Workplace when it boots up. To change users, log out, then re-login as the new user.

---

*Note: To configure Autologin for keyboard/mouse sharing setups, see **Configuring Keyboard/Mouse Sharing** (on page 156).*

---

### ► To configure Autologin:

1. If not displayed, launch the RemoteAccess-Workplace Configuration window. See **RemoteAccess-Workplace Configuration** (on page 10).
2. Click Administration > Autologin. The Autologin Settings page opens.
3. Click Edit to change the settings.
4. Select the Enabled checkbox to enable Autologin, then select the user name in the list.

---

*Note: Password is always required when configuring Autologin. When upgrading from a previous software version, Autologin is automatically disabled. When upgrading, you will have to reconfigure Autologin because the password is required.*

---

---

## LDAP

The external LDAP authentication has the following two modes:

- Authentication and authorization via LDAP
- Only authentication via LDAP

---

*Note: For single sign-on capability in RemoteAccess-Workplace, your RemoteAccess-GATEs, the RemoteAccess-Workplace and your users must exist in the same LDAP environment, and the value of "login name attribute" should be the same as UID.*

---

► **Authentication and authorization via LDAP:**

- a. On the LDAP server(s), create both USERS AND USER GROUPS for the RemoteAccess-Workplace.
- b. On the RemoteAccess-Workplace, create user groups whose group names are the same as those on the LDAP server(s). See **User Groups** (on page 111).
  - You can also import desired user groups from the LDAP server into the RemoteAccess-Workplace after performing an LDAP search for user group objects. See **Searching for LDAP Users and Groups** (on page 127).
  - User names for this LDAP authentication mode are NOT needed on the RemoteAccess-Workplace.

LDAP alias, which allows one user to have multiple logins, such as multiple common names, does NOT work in the LDAP authentication and authorization mode.

► **Only authentication via LDAP:**

- a. On the LDAP server(s), create users for the RemoteAccess-Workplace.
  - User groups are NOT needed on the LDAP server(s).
- b. On the RemoteAccess-Workplace, create both USERS AND USER GROUPS. The user names must be the same as those on the LDAP server(s), but the user passwords are not stored on the RemoteAccess-Workplace. See **Users** (on page 108) and **User Groups** (on page 111).
  - You can also import desired user names from the LDAP server into the RemoteAccess-Workplace after performing an LDAP search for user objects. See **Searching for LDAP Users and Groups** (on page 127).

LDAP alias works fine in the LDAP authentication only mode.

► **RemoteAccess-Workplace configuration required for either LDAP authentication mode:**

- Add the LDAP server(s). See ***Adding LDAP Servers*** (on page 117).
- Enable the LDAP authentication. See ***Enabling or Disabling the LDAP Authentication*** (on page 126) or ***Configuring the Maximum Search Results and Local Authentication Settings*** (on page 129).

---

*TIP: When "admin" is entered as the username and LDAP is enabled, an additional checkbox "Authenticate Locally" appears on the login page. You can select Authenticate Locally to authenticate using RemoteAccess-Workplace's local database instead of the LDAP server(s) regardless of the LDAP authentication mode.*

---

## Adding LDAP Servers


To apply external LDAP authentication, at least one LDAP server must be added to the RemoteAccess-Workplace. If you are not familiar with the LDAP settings, consult your LDAP administrator for help.

If there are multiple LDAP servers added, the order of the LDAP servers determines the authentication priority. The RemoteAccess-Workplace first connects to the first LDAP server for user authentication, then the second if the first LDAP server fails, and so on until it successfully authenticates the user. If all LDAP servers fail the authentication, the user's access is denied.

► **To add LDAP servers:**

1. If not displayed, launch the RemoteAccess-Workplace Configuration window. See ***RemoteAccess-Workplace Configuration*** (on page 10).

Add New Server

2. Click Administration > LDAP > . The New LDAP Server page opens, with 5 groups of settings displayed.

3. The General section determines general LDAP settings.

General

Type

Active Directory Server

Order

1

☒ Active

Setting	Description
Type	The type of the new LDAP server: <ul style="list-style-type: none"><li>Active Directory Server: Microsoft Active Directory</li><li>LDAP server: OpenLDAP</li></ul>
Order	The order of this LDAP server, which determines the authentication priority when there are multiple LDAP servers. If adding more than one LDAP server, you can change the priority by selecting the sequential number of any existing LDAP server. That existing LDAP server and all servers that follow it will move down one position in the order.
Active	Leave this checkbox enabled unless you want to disable this LDAP server temporarily.

4. Enter the LDAP server's data in the Connection section.

**Connection**

**Domain**

☐ Use Host

**Hostname/IP-Address**

☐ Use TLS/SSL

**Port**

*Default: 389*

☒ Check Server Certificate

[Manage certificates](#)

Setting	Description
Domain	<p><b>Configurable when "Type" is set to "Active Directory Server."</b></p> <p>The Active Directory server's domain name. Usually the RemoteAccess-Workplace can determine the Active Directory server's host name via its domain name and DNS. If you select the following Use Host checkbox, this behavior is replaced.</p>
Use Host	<p><b>Configurable when "Type" is set to "Active Directory Server."</b></p> <p>Enable this checkbox when intending to manually specify the host name or IP address of the Active Directory server.</p>
Hostname/ IP-Address	The LDAP server's host name or IP address.
Use TLS/SSL	Select this checkbox if the security connection is required for the LDAP server.
Port	<p>TCP port for the LDAP authentication, whose default is either of the following:</p> <ul style="list-style-type: none"> <li>▪ 389 (standard)</li> <li>▪ 636 (TLS/SSL)</li> </ul>
Check Server Certificates	<p><b>Configurable when the Use TLS/SSL checkbox is selected.</b></p> <p>Select this checkbox if it is required to validate the LDAP server's certificate by the list of accepted certificates on the RemoteAccess-Workplace prior to the connection. If the certificate validation fails, the connection is refused.</p>
Manage certificates	Click this link for installing a CA certificate as needed. See <i><b>Trusted Certificates</b></i> (on page 131).

---

*Note: The LDAPS connections, which have the encrypted LDAP enabled, are NOT using the FIPS accredited cryptographic code.*

---



5. Enter the bind credentials in the Bind section.

Bind

**Base DN**

**Login Name Attribute**

sAMAccountName

*Default: sAMAccountName*

**Search Filter**

(objectClass=user)

*Default: (objectClass=user)*

**Search Scope**

Subtree

▼

**Search Credentials**

no search

▼

**Admin DN**

**Admin Password**

....

☒ Bind After Search

Setting	Description
<b>Base DN</b>	<p>Distinguished Name (DN) of the search base, which is the starting point of the LDAP search.</p> <ul style="list-style-type: none"> <li>Example: ou=dev,dc=example,dc=com</li> </ul>
<b>Login Name Attribute</b>	<p>The attribute of the LDAP user class which denotes the login name.</p> <p>Note that only relative distinguished names (RDNs) can be specified in this field.</p> <ul style="list-style-type: none"> <li>Example: cn</li> </ul>
<b>Search Filter</b>	<p>Search criteria for finding LDAP user objects within the directory tree.</p>
<b>Search Scope</b>	<p>The depth to search for LDAP user objects, which starts at the directory level denoted by the "Base DN."</p> <ul style="list-style-type: none"> <li>One: Searches one level below the base DN, with the base excluded.</li> <li>Subtree: Searches all levels below the base DN, including the base.</li> </ul>
<b>Search Credentials</b>	<p>If the authentication of a user requires the LDAP search, specify the search credentials for it:</p> <ul style="list-style-type: none"> <li>no search: No LDAP search is performed.</li> <li>anonymous: Enables the LDAP search without dedicated search credentials.</li> <li>use admin credentials: Enables the LDAP search by entering the dedicated search credentials - a DN and password.</li> </ul>
<b>Admin DN, Admin Password</b>	<p><b>Configurable when "Search Credentials" is set to "use admin credentials."</b></p> <p>Distinguished Name and password of the administrator user who is permitted to perform the LDAP search.</p>

Setting	Description
<b>Bind After Search</b>	<p>Configurable when "Search Credentials" is NOT set to "no search."</p> <p>Select this checkbox if the LDAP bind operation shall be performed with a DN derived from a search operation for the user who's trying to log in.</p> <p>Usually this checkbox is:</p> <ul style="list-style-type: none"> <li>▪ Deselected for the "Active Directory Server."</li> <li>▪ Selected for the "LDAP server."</li> </ul>

6. To use LDAP groups for the authorization, configure the Groups section.

Groups

☒ Use Groups For Authorization

☐ Use Group Search DN

**Group Search DN**

**Group ID Attribute**


*Default: sAMAccountName*

**Group Member Attribute**


*Default: member*

**Group Search Filter**


*Default: (objectClass=group)*

**Group Search Scope**

Setting	Description
<b>Use Groups For Authorization</b>	<p>Select this checkbox if authorization via LDAP is intended. See <b>LDAP</b> (on page 116).</p> <p>When disabled, authorization is managed by the RemoteAccess-Workplace, and this LDAP server only manages authentication.</p>
<b>Use Group Search DN</b>	<p>Select this checkbox when intending to search a dedicated base DN instead of the "Base DN" for user groups.</p> <p>When disabled, "Base DN" is used for group searches.</p>
<b>Group Search DN</b>	<p><b>Configurable when "Use Group Search DN" is enabled.</b></p> <p>The dedicated base DN for group searches.</p>
<b>Group ID Attribute</b>	<p>The attribute of the LDAP group class which denotes the ID of the group which is used to match local group names.</p>
<b>Group Member Attribute</b>	<p>The attribute of the LDAP group class which denotes the users who belong to a group.</p> <p>Its value must be either one below:</p> <ul style="list-style-type: none"> <li>▪ A user's DN</li> <li>▪ Value of the "Login Name Attribute"</li> </ul> <hr/> <p><i>Note: If the value is not either one, the group member detection may not work as expected.</i></p>
<b>Group Search Filter</b>	<p>Search criteria for finding LDAP group objects within the directory tree.</p>

Setting	Description
<b>Group Search Scope</b>	<p>The depth to search for LDAP group objects, which starts at the directory level denoted by the "Base DN" or a group search base DN.</p> <ul style="list-style-type: none"> <li>One: Searches one level below the base DN, with the base excluded.</li> <li>Subtree: Searches all levels below the base DN, including the base.</li> </ul>

- To test whether the connection to the new LDAP server can be successfully established, type the LDAP user name and password in the Test Connection section and click Test.

Test Connection

Login

Password

Test

- Click Save.
- Repeat the same steps to add more LDAP servers as needed.

### Editing or Deleting LDAP Servers


To show a list of existing LDAP servers, click Administration > LDAP.

In the Active column:


- ☒ indicates that LDAP server is enabled.
- ☐ indicates that LDAP server is disabled.

LDAP Servers					Search	Add New Server	Settings	LDAP is disabled
Order	Active	Host	Port	Type				
1	<input checked="" type="checkbox"/>	10.1.10.61	389	Active Directory Server	<input checked="" type="checkbox"/> Edit	<input type="checkbox"/> Delete		

► **To modify an LDAP server setting:**




1. Click the desired LDAP server's  button. The Edit LDAP Server page opens.
2. Make necessary changes to the information shown. For information on each field, see **Adding LDAP Servers** (on page 117).
3. Click Save.


► **To delete an LDAP server:**


1. Click the desired server's  button.
2. Click OK on the confirmation message.

### Enabling or Disabling the LDAP Authentication



Click Administration > LDAP to open the LDAP Servers page. The right-most button indicates the current LDAP authentication setting.

LDAP Servers					<a href="#">Search</a> <a href="#">Add New Server</a> <a href="#">Settings</a> <a href="#">LDAP is disabled</a>	
Order	Active	Host	Port	Type		
1		10.1.10.61	389	Active Directory Server		

When that page shows , the LDAP authentication is currently disabled, which is the default. While disabled, all users are authenticated via the local database of the RemoteAccess-Workplace so their user credentials must be available on the RemoteAccess-Workplace. Therefore, only local users can log in. See **Users** (on page 108).

When that page shows , the LDAP authentication is currently enabled. While enabled, all users are authenticated via the LDAP servers so only LDAP users can log in. The only local user that can log in is the *admin* user.

► **To enable/disable the LDAP authentication:**

- To enable it, click .
- To disable it, click .

---

*Tip 1: You can also enable or disable the LDAP authentication on the Edit LDAP Settings page. See **Configuring the Maximum Search Results and Local Authentication Settings** (on page 129).*

---


*Tip 2: To enable or disable a specific LDAP server only, select or deselect the desired LDAP server's Active checkbox. See **Editing or Deleting LDAP Servers** (on page 125).*

---

### Searching for LDAP Users and Groups

When the LDAP authentication is being enabled, you can manually search for LDAP users or user groups as needed.

► **To search for LDAP user or group objects:**

1. Click Administration > LDAP > . The "Search for LDAP Users" page opens.
  - If the Search button is disabled, enable the LDAP authentication first. See ***Enabling or Disabling the LDAP Authentication*** (on page 126).

## Search for LDAP Users

### Authenticate

#### Server

#### \* Search Credentials

#### Bind DN

#### Password




### Search

#### Type

#### Base DN

#### Search Filter

#### Search Scope

2. In the Server field, select the desired LDAP server from the list of *active* LDAP servers.

3. The following settings on this page are pre-populated with the values of the selected LDAP server, but you can adjust them to match your search needs. If you are not familiar with the LDAP settings, consult your LDAP administrator for help.

Setting	Description
<b>Search Credentials</b>	One or two options are available, depending on the selected LDAP server's configuration. <ul style="list-style-type: none"> <li>stored admin credentials: Use the admin credentials stored in the LDAP server's configuration.</li> <li>specify below: Use the search credentials specified in the following two fields.</li> </ul>
<b>Bind DN, Password</b>	With "specify below" selected, you must specify the search credentials in the two fields.
<b>Type</b>	The type of user data to search - Users or Groups.
<b>Base DN</b>	Distinguished Name (DN) of the search base, which is the starting point of the LDAP search.
<b>Search Filter</b>	Search criteria for finding LDAP user objects within the directory tree.
<b>Search Scope</b>	The depth to search for LDAP user or group objects, which starts at the directory level denoted by the "Base DN." <ul style="list-style-type: none"> <li>Base: Searches the base DN only.</li> <li>One: Searches one level below the base DN, with the base excluded.</li> <li>Subtree: Searches all levels below the base DN, including the base.</li> </ul>

4. Click Search.
5. From the search result, you can select desired LDAP users or groups and add them to the RemoteAccess-Workplace by clicking the buttons below.
- Add as local user:*



This button is displayed for those users who are not added to the RemoteAccess-Workplace yet. Click this button to add the LDAP user as a local user who can also be authenticated via LDAP in the "LDAP authentication only" mode. Its authorization is managed by the RemoteAccess-Workplace so ensure this user is a member of at least one user group in the local database. See ***Editing or Deleting Users*** (on page 110).

- *Add this group:*

This button is displayed for those groups that are not available on the RemoteAccess-Workplace yet. Click this button to add the LDAP group as a user group with the "Device Access" privilege assigned. To modify the privileges, see ***Editing or Deleting User Groups*** (on page 114).

- *Add selected:*

To select multiple LDAP users or groups at a time, select their checkboxes and then click this button.

---

### Configuring the Maximum Search Results and Local Authentication Settings

In the LDAP settings, you can set parameters for maximum search results and allow access for local users.

By default, these options are disabled.

- **Max Search Results:** The default limitation is 1000. If the found result entries are more than the upper limit you set, those result entries exceeding the maximum are not displayed but a message shows up to remind you to specify a more accurate search filter.
- **Allow access to local users:** When this setting is enabled, an option is added to the login screen to allow users to select local authentication instead of LDAP authentication.

► **To configure the maximum LDAP search results:**

1. Click Administration > LDAP, then click the Settings button.
2. The Edit LDAP Settings page opens.

## Edit LDAP Settings



☒ Enabled

☐ Allow access for local users

Max Search Results

1000

Save Cancel

3. LDAP authentication must be enabled to set the upper limit for the LDAP search results. To enable, select the Enabled checkbox.
4. Select the desired value in the Max Search Results field: *10*, *100*, *1000* or *10000*.
5. Select "Allow access for local users" to enable the login screen checkbox for local authentication.
6. Click Save.

---

### Logging in with LDAP

When LDAP is enabled, RemoteAccess-Workplace presents a different login page. The login icon indicates the authentication type being used: Local, or LDAP.

When local users are allowed, an extra checkbox is also available for users to "Authenticate locally". See ***Configuring the Maximum Search Results and Local Authentication Settings*** (on page 129) for help with this setting.

---

### LDAP Login Failure Message

Certificate hostname verification added in release 1.3 may cause an error upon upgrade if LDAP servers were added using IP address instead of hostname.

LDAP user login attempt may fail with the event log message:

- Login of 'name' failed with hostname "IP Address" does not match the certificate at LDAPs://<IP address>

► **To resolve:**

- Update the LDAP server configuration. You may add the hostname, or disable TLS/SSL:

1. Open the RemoteAccess-Workplace Configuration page. Choose Administration > LDAP.
  - Click the LDAP server's Edit button. Enter the hostname in the Hostname/IP-Address field, instead of the IP address.
  - OR, if you prefer, disable Use TLS/SSL for LDAP server.
2. Click Save.

---

## Trusted Certificates


You must install trusted certificates on the RemoteAccess-Workplace in these scenarios:

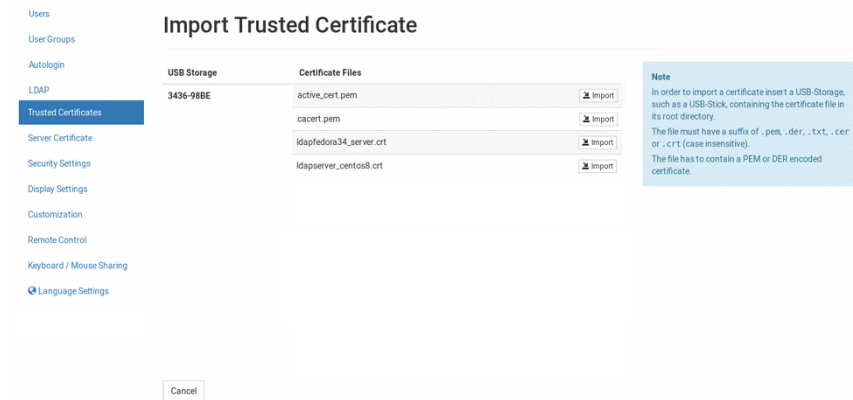
- A valid CA certificate is required to establish the LDAP connection. Then you must:
  - a. Consult your LDAP server administrator to get the CA certificate file.
  - b. Install this CA certificate onto the RemoteAccess-Workplace.
- When FIPS mode is enabled, all encrypted connections to RemoteAccess-GATEs are processed using the FIPS accredited cryptographic code and the authenticity of those RemoteAccess-GATEs is checked via their certificate chain. When Check RemoteAccess-GATE Certificate is enabled, authenticity of RemoteAccess-GATEs is checked via their certificate chain. You must install the trusted device- or root-certificate of each RemoteAccess-GATE on the RemoteAccess-Workplace, or the connection to the RemoteAccess-GATEs fails.

For more details about creating certificates that are accepted, see Certificate Requirements.

► **To install the CA certificate(s) on the RemoteAccess-Workplace:**

1. Plug a USB drive containing the appropriate certificate file into the RemoteAccess-Workplace.

- Click Administration > Trusted Certificates, then click the Import Certificate button  **Import Certificate**. The Import Trusted Certificate page opens with a list of detected certificates.



- Click Import to install the desired certificate onto the RemoteAccess-Workplace. Certificate files must be one of the following types: PEM, DER, TXT, CER, or CRT.
- The content of the installed certificate is displayed.
  - To show a list of installed certificates, click Back to all Certificates.
  - To remove this certificate, click Remove and then OK.
- If multiple certificates are needed, repeat the same steps to install more.

## Removing an Installed Certificate

If any installed certificate is outdated, invalid or no longer required, you can remove it.

### ► To remove a certificate from the RemoteAccess-Workplace:

- Click Administration > Certificates. A list of installed certificates is displayed.
- Click the red trash icon for the certificate you want to remove. Or, click the certificate that you want to remove to check the contents first, then click Remove.
- Click OK on the confirmation message.

---

### **Certificate Failure Messages**

In the FIPS mode and when Check RemoteAccess-GATE Certificates is enabled, if the KVM connection failure is resulted from the absence of a valid RemoteAccess-GATE certificate on the RemoteAccess-Workplace, an error message appears.

## Server Certificate

Services that occur over network, such as remote control, are secured with TLS. This requires the installation of a TLS certificate on the RemoteAccess-Workplace.

By default, the RemoteAccess-Workplace has a demo certificate. You must have System Administrator privileges to view, download or change the certificate. A new certificate can be installed by:

- Uploading a new certificate and private key. See **Import Private Key and Certificate** (on page 135).
- Create a private key and a self-signed certificate in the RemoteAccess-Workplace interface. See **Create Self Signed** (on page 136).

*Note: It is strongly recommended to update the preinstalled demo server certificate if you want to use the Remote Control feature. See **Remote Control via Web Browser** (on page 150).*

*If the demo server certificate is not updated, a warning message is displayed: "You're still using the preinstalled server certificate. Please change it!"*

► **To view the current server certificate:**

- Click Administration > Server Certificate. The summary information of the installed certification displays. Click Details for more.
- When a USB drive is connected, you can export the file.

## Server Certificate

 Import

 Create Self Signed

**Note**

Here you see a short summary of the installed Server Certificate which is used for HTTPS connections of Remote Control.

The Certificate can be exported if an USB flash drive is connected.

A new Certificate can be imported from a connected USB flash drive or it is possible to create a new self signed Certificate.

**Active TLS Certificate**

**Common Name** G&D  
**Serial Number** 00:00:00:00:00:00:05  
**Expires On** 2034-09-13 00:00:50 UTC

[Details](#)

Export to

G\_D\_STICK

## Import Private Key and Certificate

If you would like to use your own private key and certificate, you can import it from an attached USB drive.

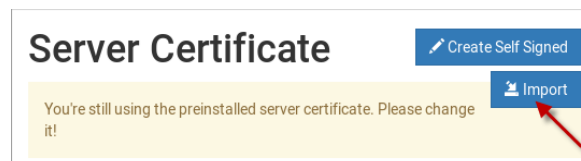
Passphrase protected keys are not supported. The private key and certificate must be combined in one file. The following file types are supported:

- PEM format (.txt, .pem)
- PKCS12 (.p12, .pfx)

If the uploaded certificate is invalid, does not match the rules, or cannot be parsed otherwise, an error message displays.

### ► To import private key and certificate:

1. Plug a USB drive containing the appropriate certificate file in the root directory into the RemoteAccess-Workplace
2. Click Administration > Server Certificate.
3. Click the Import button.




4. The certificate filenames found on the USB flash drive appear in a list. Click Import for the correct file.

## Import Private Key and Certificate

### Note

In order to import a certificate insert a USB-Storage, such as a USB-Stick, containing the certificate file in its root directory.  
The file must have a suffix of .pem, .txt, .p12 or .pfx (case insensitive).  
The file has to contain the pair of key and certificate in one file. Passphrase protected keys are not supported.

USB Storage	Certificate Files
DISK_IMG	certificate_key.txt 

5. The file is imported and validated. The certificate details are displayed.
6. Click Install New Certificate to use the imported certificate. Installing the certificate requires a reboot.

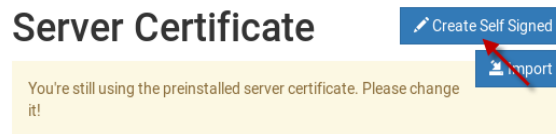
---

### Create Self Signed

If you would like to use a self signed certificate, you can create the Private Key and the Certificate using RemoteAccess-Workplace. After creating the certificate, you will install it.

► **To create a self signed certificate:**

1. Click Administration > Server Certificate.
2. Click the Create Self Signed button.



3. Enter certificate details and key parameters.
  - Country Code: Must be uppercase, 2-letter country code.
  - State or Province
  - Locality
  - Organization: Optional.
  - Organizational Unit: Optional.
  - Common Name: Must be a hostname.
  - Email address: Optional.
  - Key Length: 2048 or 4096.
  - Validity in days: 1 to 36525.



- Click Create.

## Create Self Signed Certificate

Subject	Key Creation Parameters
<b>Country Code</b> <input type="text"/>	<b>Key Length</b> <input type="text" value="2048"/>
<b>* State or Province</b> <input type="text"/>	<b>Validity in days</b> <input type="text"/>
<b>* Locality</b> <input type="text"/>	
<b>Organization</b> <input type="text"/>	
<b>Organizational Unit</b> <input type="text"/>	
<b>Common Name</b> <input type="text"/>	
<b>Email Address</b> <input type="text"/>	
<input type="button" value="Create"/>	<input type="button" value="Cancel"/>

- The certificate and key details display. If you approve, click Install to use this certificate. Installing the certificate requires a reboot.

---

## Security Settings

---

### Enable/Disable FIPS Mode and Certificate Settings

The RemoteAccess-Workplace optionally uses a FIPS 140-2 encryption module that supports the Security Requirements for Cryptographic Modules of the Federal Information Processing Standards (FIPS), which is defined in the *FIPS PUB 140-2* (<http://www.nist.gov/cmvp/>), *Annex A: Approved Security Functions*. These standards are used to protect the Federal government's sensitive information with the cryptographic-based security systems in the U.S. and Canada.

The Check RemoteAccess-GATE Certificates option allows RemoteAccess-Workplace to enforce SSL certificate checks in communication for both port information and KVM sessions.



When FIPS mode is enabled, all encrypted connections to RemoteAccess-GATEs are processed using the FIPS accredited cryptographic code and the authenticity of those RemoteAccess-GATEs is checked via their certificate chain. When Check RemoteAccess-GATE Certificate is enabled, authenticity of RemoteAccess-GATEs is checked via their certificate chain. You must install the trusted device- or root-certificate of each RemoteAccess-GATE on the RemoteAccess-Workplace, or the connection to the RemoteAccess-GATEs fails. See **Trusted Certificates** (on page 131).

---

*Note: The LDAPS connections, which have the encrypted LDAP enabled, are NOT using the FIPS accredited cryptographic code.*

---

► **To enable or disable the FIPS mode and configure certificate settings:**

1. Click Administration > Security Settings. The Security Settings page opens.
  -  indicates the setting is enabled.
  -  indicates the setting is disabled.

## Security Settings

FIPS 140-2 Mode	
FIPS 140-2 Mode <input type="checkbox"/>	<p>The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government computer security standard used to accredit cryptographic modules. If the FIPS 140-2 Mode option is enabled then all encrypted connections to RA-GATE Devices are processed using FIPS accredited cryptographic code and authenticity of those devices is checked via their certificate chain. It is required to install trusted device- or root-certificates using the Trusted Certificates dialog.</p> <p>Note, however, that LDAPS connections, if encrypted LDAP is enabled, are currently <b>not using FIPS</b> accredited cryptographic code.</p>

Certificate Settings	
Check RA-GATE Device Certificates <input type="checkbox"/>	<p>Checking of RA-GATE Device Certificates ensures authenticity of those devices. Make sure to install appropriate certificates before enabling this option.</p> <p><a href="#">Manage Certificates</a></p> <p>Note that after enabling <b>Check RA-GATE Device</b> established connections will not be re-established. These connections are unencrypted until new login.</p>

*Note: These options require certificates to be installed. Click **Manage Certificates** to check certificates or install more. See **Trusted Certificates** (on page 131).*

- Click Edit, and then select or deselect the checkboxes for FIPS or Certificate Settings.

*Note: If certificates have not been installed yet, you will see a message. Click **Manage Certificates** to go to the import page. Certificate hostname verification is enforced.*

- Click Save.
- Click OK on the confirmation message.
- The RemoteAccess-Workplace now reboots if FIPS mode was changed. Wait until the Login Screen appears.

### Strong Password Settings

Password aging and strong passwords can be enabled to offer additional security. Password Aging forces users to change passwords regularly. Strong Passwords can be enabled to specify length and characters required, and limit reuse of old passwords.

#### ► To configure password settings:

- Click Administration > Security Settings. The Security Settings page opens.
  - ☒ indicates the setting is enabled.
  - ☐ indicates the setting is disabled.

**Password Settings**

In order to improve the system's security, you can set a password expiration interval, or you can enable strong passwords.

**Notes:**

- If Password Aging is enabled and a user has last changed his password with an old firmware release prior to Strong Passwords support, the user will be forced to change his password on the next login, regardless of the Password Aging Interval.
- The Strong Password setting only applies to newly set passwords. In case users have "weak" passwords and strong passwords are enabled later, they will not be forced to change their password.

**Password Aging**  
☐  
**Password Aging Interval**  
60 Days  
**Strong Passwords**  
☒  
**Minimum Password Length**  
8  
**Enforce Lower Case Character**  
☒  
**Enforce Upper Case Character**  
☒  
**Enforce Numeric Character**  
☒  
**Enforce Special Character**  
☐  
**Password History Size**  
5

Edit

2. Click Edit, then scroll down to the password options.

## 3. Specify options for Password Aging:

- Select the Password Aging checkbox to enable the feature.
- Password Aging Interval: All users are required to change their password at the selected interval.

☒ Password Aging**Password Aging Interval**

60 Days	▼
7 Days	
14 Days	
30 Days	
60 Days	
90 Days	
180 Days	
365 Days	

## 4. Strong Passwords:

- Select the Strong Passwords checkbox to enable the feature. This requires users to create passwords that meet the additional criteria specified.
- Minimum Password Length: The minimum number of characters required in a password.
- Enforce characters: Users must include at least one of the specified characters, Lower Case, Upper Case, Numeric, Special.
- Select a Password History Size: The number specifies how many previous passwords are kept in the history and cannot be reused. For example, if Password History Size is set to 5, users cannot reuse any of their previous five passwords.

☒ Strong Passwords**Minimum Password Length**

8	-	+
---	---	---

☒ Enforce at least one Lower Case Character☒ Enforce at least one Upper Case Character☒ Enforce at least one Numeric Character☐ Enforce at least one Special Character**Password History Size**

5	-	+
---	---	---

## 5. Scroll down to click Save.

---

## User Blocking

The User Blocking options specify the criteria by which users are blocked from accessing the system after the specified number of unsuccessful login attempts.

The admin user is excluded from User Blocking.

If a blocked user tries to log in, "Authentication Failed" is displayed at the login screen. The user is not notified that they are blocked. An event log message is generated when a user is blocked.

### ► Unblocking:

Users are automatically unblocked after the specified amount of time, or a System Administrator user can unblock the user early in the Users configuration. The blocking status is shown on the Users list.

### ► To configure user blocking:

1. Click Administration > Security Settings. The Security Settings page opens.
  - ☒ indicates the setting is enabled.
  - ☐ indicates the setting is disabled.

**User Blocking**

With these settings, users can be blocked from accessing the system after a specified number of unsuccessful login attempts.

**Enabled**  
☒

**Block Timeout**  
10 Minutes

**Count of Failed Logins**  
3

2. Click Edit, then scroll down to the user blocking options.
3. To enable user blocking, select the Block Users on Login Failures checkbox.
4. Block Timeout: The time period that the users with failed logins will be blocked from logging in.

- Count of Failed Logins: The maximum number of failed logins before blocking a user.

User Blocking

With these settings, users can be blocked from accessing the system after a specified number of unsuccessful login attempts.

☒ Block Users on Login Failures

**Block Timeout**

10 Minutes

**Count of Failed Logins**

3

- Scroll down to click Save.

## Restricted Service Agreement

After the Restricted Service Agreement feature is enabled, the agreement's content is displayed on the login screen. Users must select a checkbox to agree to the statement to login.

### ► To configure the RSA:

- Click Administration > Security Settings. The Security Settings page opens.
  - ☒ indicates the setting is enabled.
  - ☐ indicates the setting is disabled.

Restricted Service Agreement

**Enforced**

☐

**Text**

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.

- Click Edit then scroll down to the Restricted Service Agreement options.
- To enable the feature, select the Enforce Restricted Service Agreement checkbox.

4. A default agreement is provided. You can edit or replace the default text as needed.

**Restricted Service Agreement**  
☒ Enforce Restricted Service Agreement  
**Restricted Service Agreement Text**  

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.

5. Click Save.

---

## Display Settings

The RemoteAccess-Workplace display can be configured to lock the screen or turn off the monitor in certain conditions.

Display settings include screen locking and scaling. The settings are applied to all users.

You must have "System Administrators" privileges to configure display settings.

---

*Note: Port Scanning sessions and KVM sessions do not prevent monitor turn-off and/or screen locking when those options are configured.*

---

► **To edit the display settings:**

1. Click Administration > Display Settings.
2. Click Edit.
3. To turn off the monitor after an idle timeout period, select the time period:
  - Select Never to keep monitor on.
  - Select 1, 2, 3, 5, 10, 15, 30 or 60 Minutes to enable the monitor turn off after the specified idle time period.
4. To lock the screen when idle, check the Lock Screen when idle checkbox. Lock Screen can only be enabled with Turn off Monitor after idle timeout. The screen is locked during the idle time period.



5. In the Scaling Settings, select the Desktop Scaling that works best for your monitor: 100% or 200%. If you are using a 4k HD monitor, 200% scaling may be preferable.
6. Click Save.

## Edit Display Settings

Screen Locking Settings

Turn off Monitor after idle timeout

Never

☐ Lock Screen when idle

Scaling Settings

Desktop Scaling

100%

Save

Cancel

---

## Customization

To customize your RemoteAccess-Workplace GUI appearance, you can replace the default G&D desktop background, application logo, and login screen with your own images and messaging. System Administration privilege is required.

Customizations are applied for all users. Changes are logged to the event log with image name and user who performed the change. Customization's are included in backups and restore, while a factory reset restores the original default images. You can also restore the defaults at anytime.

Image files must be saved to the root directory of a USB stick for upload.

---

*Note: If the desktop does not show the new background image, it is likely the image file is broken. Replace with a different image file.*

---

► **Image requirements:**

- Desktop background image: JPG, PNG, or SVG images up to 128 MB. Solid background color that is not transparent
- Application logo: Appears in the Configuration application in the top-left corner. JPG, PNG, or SVG images up to 512KB. Application logo images are automatically scaled to 110 x 48 pixels, or 220 x 96 pixels when 200% desktop scaling is used.
- Logo on the login screen: JPG, PNG, or SVG images up to 512 KB. Logo images are automatically scaled to 80 x 80 pixels, or 160 x 160 pixels when 200% desktop scaling is used.

► **To customize the RemoteAccess-Workplace:**

1. Save the desired image files to a USB flash drive, and connect the USB flash drive to the RemoteAccess-Workplace.
2. Click Administration > Customization and click Edit for the section you want to change.
  - Desktop Background: background image only
  - Application: logo image only
  - Login screen: logo image, plus Header and Message text options

## Customization

**Desktop Background**  
  
**Current Background:**  
[Default]  

Edit

**Application**  
  
**Logo:**  
[Default]  

Edit

**Login Screen**  
  
**Logo:**  
[Default]  
**Heading:**  
[Default]  
**Message:**  
[Default]  

Edit

3. If a custom image is currently in use, the file name is listed, while non-customized sections will show "Default". Image files found on the USB device are listed as options. Click the Apply button for the image file you want to use.

Or, to restore the default image, click Install Default. This option is disabled when a custom file is not in use.

Once the image is set, click Back to return to the options.

**Current Background:**



[Default]

[Install Default](#)**Note**

In order to update the desktop background, insert a USB-Storage, such as a USB flash drive, containing the image file in its root directory.

The image file must have a suffix of .jpg, .png or .svg (case insensitive) and only files with a maximum size of 128 MB are allowed.

The background image will apply to all users and the default background can be restored via 'Install Default' button.

USB Storage	Background Image	Size	
DC82-5D08	image1.jpg	440 KB	 Apply
	image2.jpg	607 KB	 Apply

- In this example, the current desktop background is the default G&D branding, and there are 2 image files found on the connected USB device. Both listed images meet the requirements for a background image as JPG files under 128MB.
4. For Login Screen customization, you can also enter a custom Heading and Message, then click Save.

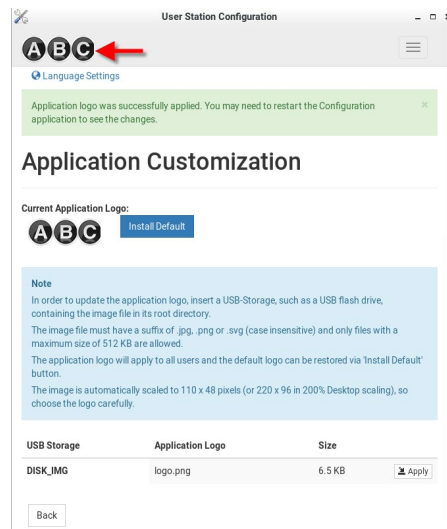
**Heading****Message**[Save](#)[Cancel](#)

5. Desktop background image changes take effect immediately. Log out to see the login screen changes on your next login attempt.

## Customization Example

### ▶ Customized "ABC" logo on RemoteAccess-Workplace Configuration:

In this example, the customized "application logo" was just saved.



## Remote Control

One common use case for remote control is to connect the controlled RemoteAccess-Workplace to a wall monitor and remotely control the display of various target servers on monitor via web browser.

Using a web browser, connect to the Remote Control interface of the RemoteAccess-Workplace using the IP address or hostname as the URL. Login as usual. Upon successful login, the RemoteAccess-Workplace presents the Port Navigator just as it appears in the local console. Selecting and opening ports works the same as in the local console, but the KVM clients open in full screen mode at the RemoteAccess-Workplace that is being remotely controlled. If "Unrestricted Navigator" is enabled, you can also use window management and window layout features, launch multiple sessions, and use non-full-screen view.

Remote Control can also be accomplished via the RESTful API (HTTPS & JSON) to control RemoteAccess-Workplace programmatically from customer applications. There are two main use cases: to launch sessions or window layouts and/or to perform administrative tasks.

---

## Remote Control via Web Browser

The remote control via web browser configuration allows the RemoteAccess-Workplace to be controlled via web browser accessed by a smart phone or PC that can reach the RemoteAccess-Workplace on the network.

By default, Remote Control via web browser offers full-screen sessions only, without access to Window Layouts or Window Management. Enable the Unrestricted Navigator setting to add those features to remote control sessions.

### ► Supported browsers:

- Chrome 60+
- Firefox 52+
- Safari 11+
- Edge 42+

### ► To configure remote control:

You must have the System Administration privilege.

1. Click Administration > Remote Control.
2. Click the Edit button to enable the options.
3. Select Enable Remote Control via HTTPS to enable the feature.
4. Allow HTTP:
  - If "Allow HTTP" is checked, Remote Control is available via both HTTP and HTTPS. There is no redirect.
  - If "Allow HTTP" is not checked, HTTP is redirected to HTTPS.
5. Unrestricted Navigator: Enable Unrestricted Navigator to allow additional features:
  - The Unrestricted Navigator can launch sessions in non-full-screen mode, and show multiple sessions at the same time.
  - Windows Layout and Window Management functions can be used from Remote Control.
6. Click Save.

### Remote Control via Web Browser

This option enables Remote Control of the User Station via HTTPS.

HTTP access is possible but not recommended.

By default, Remote Control is limited to one access client session in full-screen. If **Unrestricted Navigator** is enabled, then the remote Navigator allows to launch sessions in non-full-screen mode, and show multiple sessions at the same time. Also, in unrestricted mode, Window Layouts and Window Management functions can be used from Remote Control.

- ☒ Enable Remote Control via HTTPS
- ☐ Allow HTTP
- ☐ Unrestricted Navigator

### Remote Control via API

The RemoteAccess-Workplace supports a remote RESTful API via HTTPS, allowing programmed remote control to:

- Launch Access Client sessions or Windows Layouts.
- Perform certain administrative tasks.
- See **API** (on page 215) for API documentation.

#### ► API Overview

- The API can be enabled independently from the regular remote control setting.
- The API uses HTTPS (HTTP is not an option), listening on port 8443.
- If remote control is enabled, the API is available only on port 8443.
- Regular remote control cannot be used on port 8443.
- The API is not available on regular remote control ports 80 and 443.
- The API uses JSON documents for both POST request data (method parameters) and responses.
- One checkbox on the Remote Control page enables/disables the API access, which is disabled by default.
- The API Description document (in OpenAPI format) can be exported to a USB drive.
- The TLS certificate can be configured using the Server Certification setting of the Configuration tool.

#### ► To configure Remote Control via API:

1. Click Administration > Remote Control.
2. Click the Edit button to enable the options.
3. Select the Enable Remote Control via HTTPS checkbox.

4. Select the Remote Control via API checkbox.
  - Export the API file to a connected USB drive. Choose a file format and click "Export the API file".
5. Click Save.

## Edit Remote Control Settings

Remote Control via Web Browser

☒ Enable Remote Control via HTTPS

☐ Allow HTTP

☐ Unrestricted Navigator

This option enables Remote Control of the RA-Workplace via HTTPS.

HTTP access is possible but not recommended.

By default, Remote Control is limited to one access client session in full-screen. If **Unrestricted Navigator** is enabled, then the remote Navigator allows to launch sessions in non-full-screen mode, and show multiple sessions at the same time. Also, in unrestricted mode, Window Layouts and Window Management functions can be used from Remote Control.

Remote Control via API

☒ Remote Control API

Export API description file to

VERBATIM\_HD

Remote Control is also available via an REST API (over HTTPS) on port 8433. You can export an OpenAPI specification file here.

For further documentation and examples, please contact G&D support.

Save

Cancel

### Using the API

1. Create a login session to authenticate on further calls. There are API calls to create the login session.



2. The remote API session is bound to a local user session. If an API user logs in, the following will happen:
  - If the API user is already logged in on the local console, the API will take over the session.
  - If no user is logged in on the local console, the API user will be automatically logged in.
  - If another user is logged in on the local console, then the user is logged off and the API user is logged in.
3. Once the session is created, the API uses HTTP cookies for authentication. When the session is created, the client receives cookies. These cookies must be sent back on further API requests.
4. When finished, the API user can log off the session. Logging off also terminates the session on the local console.

See **API** (on page 215) for details.

---

## Keyboard/Mouse Sharing

Keyboard and Mouse Sharing allows you to control several RemoteAccess-Workplaces by one keyboard and mouse that is connected to one of the RemoteAccess-Workplaces. This can be useful in a control room setting with multiple monitors connected to multiple RemoteAccess-Workplaces.

---

*Note: The Keyboard/Mouse Sharing feature does not support Caps Lock.*

---

- RemoteAccess-Workplace 6 Monitor Vertical Configuration Example:



To configure, designate the RemoteAccess-Workplace with the keyboard and mouse connected as "Controller". The RemoteAccess-Workplaces you intend to share the keyboard and mouse with are designated as "client". For the initial configuration, connect a keyboard and mouse to each client RemoteAccess-Workplace. You can remove these when the configuration is complete. Login to each client

RemoteAccess-Workplace to enter the controller's IP address/hostname and assign the client a unique screen name. In the controller setup, add the unique client names to the Arrangement of Screens, a grid representing the physical screen location. Screens can be added in any formation up to a 5 by 3 grid, as long as each screen has a neighbor on at least one edge. See *Configuring Keyboard/Mouse Sharing* (on page 156) for detailed instructions.

Once configured, the Mouse will move either horizontally or vertically from screen to screen. Each RemoteAccess-Workplace can have its own extended desktop with multiple monitors, so the Mouse will move from the ends of each extended desktop. Each RemoteAccess-Workplace is still independent. You cannot drag KVM Windows from one RemoteAccess-Workplace to another.

#### ► Example Arrangement of Screens:

The Arrangement of Screens is used to define how the mouse and keyboard moves between the screens of the Controller and Client RemoteAccess-Workplaces. The mouse can move either horizontally or vertically as shown.

Settings					
Screen Name		RAW4			
Arrangement of Screens		Client5	Client1	RAW4	Client2
					Client3
					Client4

- Moving the Mouse to the right edge of Client5 will move to the left edge of Client1
- Moving the Mouse to the left edge of Client2 will move to the right edge of RAW4
- Moving the Mouse to the bottom edge of Client3 will move to the top edge of Client4

---

### Keyboard/Mouse Sharing in Single Cursor Mode

To use the Single Mouse Cursor Mode of the KVM client while Keyboard/Mouse Sharing is active, follow this procedure:

1. Move the mouse pointer to the display of the RemoteAccess-Workplace that should be used with Single Mouse Cursor Mode in the KVM client.
2. Press the Scroll Lock key to lock the mouse pointer to this RemoteAccess-Workplace.
3. Single Mouse Cursor Mode will now work in the KVM client.
4. After leaving Single Mouse Cursor Mode in the KVM client, press the Scroll Lock key again to unlock the mouse pointer.

---

### Configuring Keyboard/Mouse Sharing

If you need to configure your monitors first, see *Monitor* (on page 182).

Controller is the RemoteAccess-Workplace where the keyboard and mouse are physically connected. Clients are RemoteAccess-Workplaces that will share the Controller's keyboard and mouse.

► **To configure client screens:**

1. Login to a client RemoteAccess-Workplace.
2. Click Administration > Keyboard/Mouse Sharing.

General	
Enabled	<input type="checkbox"/>
Mode	Client (Use another RA-Workplace's mouse and keyboard)
Share Window Layouts	<input type="checkbox"/>
Automatically log in/out Users	<input type="checkbox"/>

3. Click Edit, then select Enabled.

4. Select Client in the Mode field.

☒ Enabled

**\*Mode**

Client ▼

5. Select the Share Window Layouts option to allow saved layouts to be shared among all clients in the keyboard/mouse sharing configuration.
  - Window Layouts must be created on all RemoteAccess-Workplaces manually.
  - When you restore a layout on one RemoteAccess-Workplace, all others restore the Window Layout with the same name.
6. Select the Automatically Log in/out Users option to automatically login/logout to all RemoteAccess-Workplaces connected by keyboard/mouse sharing while using the configuration.
7. In the Client Settings, enter a Screen Name to identify this client. All screens in the sharing formation must have unique names.
  - Up to 64 characters.
  - Alphanumeric characters allowed.
  - Hyphen and underscore allowed.
8. Enter the IP address/Hostname of the Controller RemoteAccess-Workplace, which is where the keyboard and mouse are connected.

**\*Screen Name**

RAW4

**\*IP Address / Hostname of Controller RA-Workplace**

192.168.50.51

9. Click Save. Repeat this task for all client screens.

► **To configure the Controller:**

1. Login to the Controller RemoteAccess-Workplace.
2. Click Administration > Keyboard/Mouse Sharing.
3. Click Edit, then select Enabled.
4. Select Controller in the Mode field.
5. Select the Share Window Layouts option to allow saved layouts to be shared among all clients in the keyboard/mouse sharing configuration.
6. Select the Automatically Log in/out Users option to automatically login/logout to all RemoteAccess-Workplaces connected by keyboard/mouse sharing while using the configuration.
7. In the Controller Settings, enter a Screen Name to identify this Controller screen. All screens in the sharing formation must have unique names.

- Up to 64 characters.
  - Alphanumeric characters allowed.
  - Hyphen and underscore allowed.
8. In the Arrangement of Screens fields, enter the names of this controller screen and all client screens in the position representing their location in the sharing formation.
- Make sure the names entered here match the names in the "Screen Name" field in each client RemoteAccess-Workplace's configuration exactly.
  - No duplicate names allowed.
  - Each screen must have at least one neighbor screen, either beside, above or below.
9. Click Save.

Controller Settings

\* Screen Name

screenB2

The Screen Name is the name which identifies this RA-Workplace. It must be unique among all RA-Workplaces sharing one set of keyboard and mouse.

Please specify the Screen Names of all RA-Workplaces sharing keyboard and mouse and their arrangement in the grid below. This RA-Workplace's Screen Name must be part of the screen arrangement.

\* Arrangement of Screens

screenA1	screenA2	screenA3		
screenB1	screenB2	screenB3		

Clear

Save

Cancel

---

## Language Settings

The Language Settings feature allows you to change the RemoteAccess-Workplace GUI and system language.

- English
- French: Français
- German: Deutsch
- Chinese (Simplified): 中文(简体)
- Japanese: 日本語

After setting a new language, you must reboot to fully update the language in every area. Note that some text is not available in all languages. Language setting is part of backup and restore, but upon factory reset the language setting is English.

Chinese and Japanese input methods are not supported.

### ► To change the language setting:

1. Click Administration > Language Settings. The current language selection is listed.

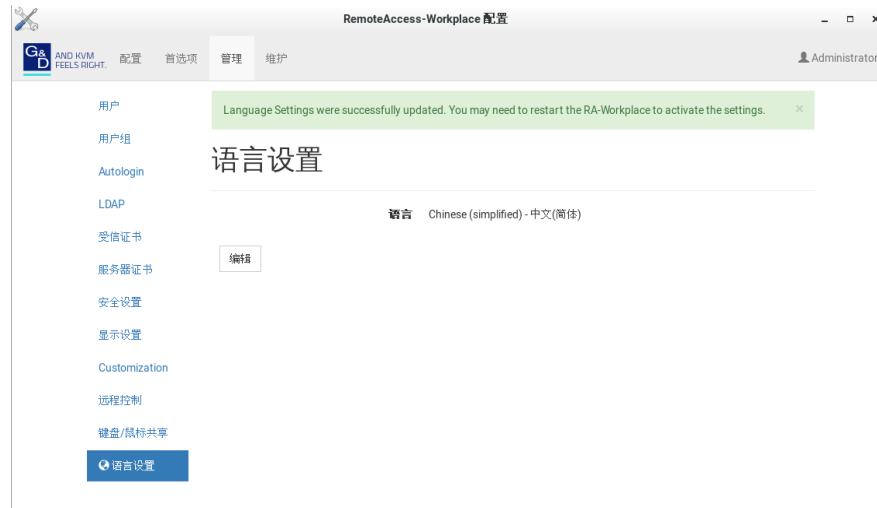
A blue rectangular button with a white globe icon on the left and the text "Language Settings" in white.

2. Click Edit, then select the language from the list.

### Language

English
English
German - Deutsch
French - Français
Chinese (simplified) - 中文(简体)
Japanese - 日本語

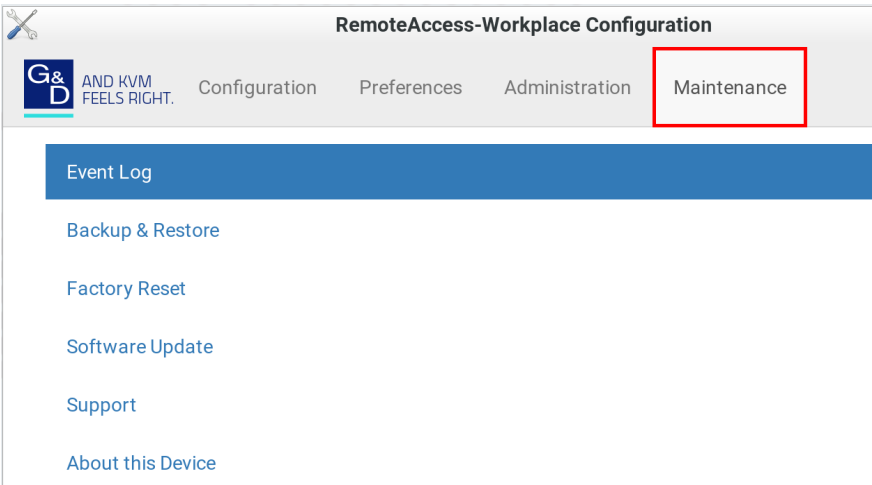
3. Click Save. You will see an immediate change in the GUI, but you must reboot the RemoteAccess-Workplace to ensure a full language update.





# Maintenance Features

In the RemoteAccess-Workplace Configuration window, click Maintenance to perform the following RemoteAccess-Workplace maintenance tasks.



## In This Chapter

Event Log .....	162
Backup and Restore .....	167
Factory Reset.....	169
Software Update .....	170
Support .....	172
About this Device .....	175

## Event Log

The Event Log is an application level log of activity taking place in the RemoteAccess-Workplace. It records who did a certain task and when it was done. For example, login and logout, open connection to a KVM-port, updating the software and so on. The Event Log also records system incidents that cannot be shown otherwise, such as LDAP authentication and authorization processing and decisions.

The Event Log is different from the Diagnostic Log File that can be downloaded from the RemoteAccess-Workplace, which contains the raw system logs that cannot be conveniently read or filtered.

### Event Log

[Archives](#)

**From**

**To**

**Event Type**

**Level**

**Items per page**

[Search](#)

Date (EST -0500)	Level	Type	Description
2017-03-03 15:04:10	Info	Auth Event	Local user admin logged in
2017-03-03 15:02:07	Info	Auth Event	Local user admin logged out

#### ► To search and view the Event Log:

1. If not displayed, launch the RemoteAccess-Workplace Configuration window. See *RemoteAccess-Workplace Configuration* (on page 10).
2. Click Maintenance> Event Log. The Event Log page opens.
3. Search functions appear at the top of the screen. The most recent seven days of entries in the event log appear at the bottom of the screen.
  - Search by date: Select a date range in the From and To fields.
  - Search by Event Type: See *Event Type and Description* (on page 163). When Authentication is selected, you can select a user from the User field.
  - Search by Event Severity: Info, Warning, or Critical.
  - Items per Page: Select how many records to display per page of search results.

- Click Search. The filtered list of events appears at the bottom of the search controls.

---

### Event Type and Description

The Event Log includes the following events types.

- Authentication Events: Description includes user name and local or LDAP category
- LDAP Events: Errors and information for LDAP authentication and authorization
- KVM Access Events: Access of KVM ports. Description includes device, port and user name
- RDP, SSH, VNC, Web, and ESXi Access Events: Access sessions opened and/or closed.
- System Events: Changes of the system such as adding users or RemoteAccess-GATEs. User is logged in description when applicable.

---

### Event Log Archives

Event Log records can be archived to clear the database. Event Log archives are always created and stored inside the RemoteAccess-Workplace. The file created is a compressed CSV file containing one line per record and all attributes of the record. Each record has a timestamp in UTC.

All stored archives are listed with the following details:

- date of creation
- filename: raw-event-log-archive-`<year>-<month>-<day>-<time>`.gz
  - example: raw-event-log-archive-2016-11-18-140000.gz
- size

```
2016-11-15 16:08:57 UTC,System Event,Info,System started
2016-11-15 16:09:06 UTC,Auth Event,Info,Local user admin logged in
2016-11-15 16:09:59 UTC,System Event,Info,User admin was updated by User admin.
2016-11-15 16:15:40 UTC,System Event,Info,A firmware update to version 1.2.0.5.178 was started by user admin
```

You can create a manual archive at anytime. See *Create an Archive* (on page 164).

The RemoteAccess-Workplace also automatically creates an archive if the total amount of event log records reaches a certain threshold. See *Automatic Archives* (on page 165).

### Create an Archive

1. If not displayed, launch the RemoteAccess-Workplace Configuration window. See ***RemoteAccess-Workplace Configuration*** (on page 10).
2. Click Maintenance> Event Log. The Event Log page opens.
3. Click Archives. The Event Log Archives page opens.
4. Choose how records will be included in the archive: Age or Date
  - In the Age field: select a file age to include:
    - 1 week
    - 1 month
    - 2 months
    - 6 months
    - 1 year (default)
    - 2 years
    - 5 years
    - 10 years
  - Or, select "older than selected Date" to enable the Date field, and choose a specific Date in the calendar. To choose a specific time, use the clock icon on the calendar, as shown.
  - All events logged older than the selected Age, or older than the selected Date will be archived.
5. Click Archive.
6. Click OK in the confirmation dialog.

## Event Log Archives

Oldest Record: 2021-05-18 00:38:47

Any record older than the selected date will be archived.

### Age

older than selected Date

### Date

2021-06-01 00:00:00 +02:00



Archive

### Automatic Archives

RemoteAccess-Workplace will automatically create archives in cases where the database has become full of too many records.

Automatic archives are implemented with two thresholds, Warning and Critical. The thresholds are checked once per day. If thresholds are met, an error message appears in the event log. The archive is created automatically when the Critical threshold is met.

#### ► Warning threshold:

A warning message displays in the Event Log page when 2 million records has been reached:

**There are more than 2 Million entries in event log. Please archive event log entries or auto-archiving will be started once event log grows above 3 Million entries.**


#### ► Critical threshold:


The critical threshold is 3 million records. An automatic archive is created, including all log entries above the warning threshold of 2 million records. Automatic archiving doesn't trigger immediately upon reaching 3 million entries, but will run once per day.



The automatic archive creation is logged in the Event Log with username <system>

### Exporting Archive Files

To export an archive file, you must connect a USB flash drive to the RemoteAccess-Workplace first. When the RemoteAccess-Workplace

detects the connected USB drive, the export button  appears.

1. Click the Export icon  of the file you want to export to USB.

Filename	Status	Size	Date (EST -0500)		
log-archive-20170221122350-6a0ed89e75ed.zip	Done	304 Bytes	2017-03-04 12:25:05		


[Back](#)

2. The file is exported to the USB drive.

### Deleting Archive Files

You can delete an archive file. If you want to save the file off the RemoteAccess-Workplace before deleting it, see *Exporting Archive Files* (on page 165).

1. If not displayed, launch the RemoteAccess-Workplace Configuration window. See *RemoteAccess-Workplace Configuration* (on page 10).
2. Click Maintenance> Event Log. The Event Log page opens.
3. Click Archives. The Event Log Archives page opens.
4. All archive files are listed at the bottom of the page. Click the Delete icon next to the file you want to delete.

Filename	Status	Size	Date (EST -0500)	
log-archive-20170221122350-6a0ed89e75ed.zip	Done	304 Bytes	2017-03-04 12:25:05	

Back

5. A confirmation message appears. Deleting cannot be undone. Click OK to delete the archive file.

### Archive File Storage

The amount of storage to keep Event Log archives inside RemoteAccess-Workplace is limited. If no more storage is available, you will see an error message upon attempting to create a new archive.

The error message prompts you to delete old archive files.

You can export files to external storage before deleting, if needed. See *Exporting Archive Files* (on page 165).

You must delete archive files before you can create the new archive. See *Deleting Archive Files* (on page 166).

If the storage is full when an automatic archive must be created, the oldest archives are automatically deleted until there is enough space to write the new archive.

Deletion of each archive is logged into the Event Log

---

## Backup and Restore

The RemoteAccess-Workplace allows you to back up the latest settings and data with one click. By default, the backup files are stored in the RemoteAccess-Workplace.

In case you have to restore to the previous settings and data, select the backup file you need and perform the restore command.

Note that the following system settings are NOT stored in the backup file so they CANNOT be restored.

- Network, see **Network Connections - Ethernet** (on page 185)
- Date/Time, see **Date/Time** (on page 176)
- Event Log Archives
- Backup Files

---


*Tip: You can export or import backup files from a USB flash drive. See **Exporting and Importing Backup Files** (on page 168).*

---

### ► To back up the current settings and data:

1. If not displayed, launch the RemoteAccess-Workplace Configuration window. See **RemoteAccess-Workplace Configuration** (on page 10).
2. Click Maintenance > Backup & Restore. The Backup & Restore page opens.
3. Click Create Backup.
4. Once completed, the Backup Archives page lists the backup file, with the filename, software version and file size shown on the screen.

### ► To restore to the previous settings and data:



1. If there are any existing backup files, the Backup Archives page lists all of them.
2. Determine the desired file and click the restore icon  button.  
Or, click the filename link to view details, and click the Restore button in the details page.
3. Click OK on the confirmation message.
4. A text screen appears to show restore progress. When restore is completed, RemoteAccess-Workplace restarts and opens the login page.

---

## Exporting and Importing Backup Files

To export or import a backup file, you must connect a USB flash drive to the RemoteAccess-Workplace first.

### ► To export backup files:

1. Connect a USB drive formatted with any of the following file system.
  - VFAT (FAT16, FAT32)
  - NTFS
  - EXT2, EXT3, EXT4
  - Btrfs
  - XFS
2. Click Maintenance > Backup & Restore. The Backup & Restore page opens. When the RemoteAccess-Workplace detects the connected USB drive, the export button  appears in the Actions column.
3. Click the  button of the desired backup file.

The selected file is exported to the connected USB drive and therefore listed in the "Import Archive from USB Drive" section.

### ► To import backup files:

Make sure the connected USB drive contains backup files in its *root* directory.

1. Click Maintenance > Backup & Restore. The Backup & Restore page opens.
2. Click Import Backup. The Import Backup from USB Storage page opens. All backup files detected on the USB drive are listed.
3. Click the import button of the desired backup file.

The selected file is imported from the connected USB drive, and shown in the Backup & Restore page.

---

## Deleting Backup Files

To check the creation date of a backup file before removing it:

The creation date and time stamp is included as the last set of numbers in the filename, after software version and sometimes serial number. The date is expressed in 8 digits.

### ► Examples:

Backup filename with version number and date/time stamp:

RAW\_backup\_4.1.0.5.284\_20191014090046.dat




The software version is 4.1.0.5.284. The date is 20191014, October 14, 2019.

Backup filename with version number, serial number, and date/time stamp:

```
RAW_backup_4.1.0.5.284_22U9674800_20191014090046.dat
```

► **To remove a backup file:**

1. To show existing backup files, click Administration > Backup & Restore.
2. Click the  button of the desired file.
3. Click OK on the confirmation message.

---

## Factory Reset

The factory reset feature resets all of your RemoteAccess-Workplace's settings to the factory defaults except for Network Settings and Date/Time Settings. All other customized data is removed simultaneously, including:

- All RemoteAccess-GATEs added to the RemoteAccess-Workplace
- User credentials entered for each RemoteAccess-GATE
- All Targets and access
- User profiles
- "admin" user profile is recreated with factory default settings
- User groups other than the built-in user groups
- Built-in user groups reset to factory default settings
- All user preferences settings
- System settings
- Trusted certificates
- Server certificates
- Desktop background
- Backup files
- Log files

---

*Note: To perform factory reset at startup instead of using the RemoteAccess-Workplace Configuration window, see **Factory Reset at Startup** (on page 210).*

---

► **To perform the factory reset:**

1. If not displayed, launch the RemoteAccess-Workplace Configuration window. See **RemoteAccess-Workplace Configuration** (on page 10).

2. Click Maintenance > Factory Reset. The factory reset page opens.  
Read this page before proceeding to the next step.

## Reset to Factory Defaults

### Attention

This function will erase all data from your RA-Workplace's storage, including:

- RemoteAccess-GATE Devices
- Credentials to access RA-GATE Devices
- Targets and their Access Points
- Users and Groups
- User Preferences
- System Settings
- Trusted Certificates
- Server Certificate
- Desktop Background
- Backup Files
- Log Files

You will be logged out and the system will reboot while the reset is executed. Afterwards you can login as user **Admin**.

 Perform Factory Reset

3. Click Perform Factory Reset. A confirmation message appears.
4. Click OK to confirm the operation or Cancel to abort it.

---

## Software Update

The software update feature only permits software UPGRADE, not downgrade.

---

*Note: To perform software downgrade, contact G&D Technical Support for help.*

---

To perform the software update, you must meet the following requirements:

- You have a USB flash drive with one of the following formats, or a USB CD-ROM/DVD-ROM drive for inserting a CD/DVD disc containing the software file.
  - VFAT (FAT16, FAT32)
  - NTFS
  - EXT2, EXT3, EXT4
  - Btrfs
  - XFS


- The version of the software which you will install is equal to or higher than the software version currently running on your RemoteAccess-Workplace. See **About this Device** (on page 175).

---

**Important: It is strongly recommended to back up all data and settings and export to a USB drive prior to the software update. See *Backup and Restore* (on page 167).**

---

► **To perform the software UPGRADE:**

1. Get the newest RemoteAccess-Workplace software file from G&D's Technical Support (www.gdsys.com).
2. Copy the file named "RAW\_<version>\_update.bin" to the **root directory** of your USB flash drive or CD/DVD disc.
3. On the RemoteAccess-Workplace, log in as a user who has the System Administration privilege.
4. Connect the USB flash drive or a USB CD-ROM/DVD-ROM drive to the RemoteAccess-Workplace.
5. Launch the RemoteAccess-Workplace Configuration window. See **RemoteAccess-Workplace Configuration** (on page 10).
6. Click Maintenance > Software Update. The Software Updates page opens, with a list of software files found in the root directory of the USB flash drive or CD/DVD disc.
7. Click the desired file, and it will be analyzed. Verify the minimum required version and validity check results.
8. Click Start the Update  to perform the software upgrade.

---

*Warning: Do NOT power off the RemoteAccess-Workplace during the software upgrade.*

---

9. Click OK on the confirmation message.
10. When the upgrade completes, the RemoteAccess-Workplace reboots, and then the login screen is shown.

---

*Note: If the software upgrade fails, and the RemoteAccess-Workplace is unable to operate, contact G&D Technical Support.*

---

## Support

The Support page provides two features that help G&D Technical Support to troubleshoot your RemoteAccess-Workplace issues.

- **Support Login:** This feature allows the Technical Support to remotely access your RemoteAccess-Workplace.
- **Log Level:** This feature allows you to set the log level of the Diagnostic Log file. Note, this file is different from the Event Log.
- **Diagnostic Log File:** This feature downloads a diagnostic log file from your RemoteAccess-Workplace, which is helpful for troubleshooting.

### Support Login

The Support Login feature allows remote access from G&D Technical Support.

By default, this feature is disabled for security.

You *MUST NOT* enable this feature unless you are instructed by G&D Technical Support to do so.

#### ► To permit remote access from G&D Technical Support:

1. If not displayed, launch the RemoteAccess-Workplace Configuration window. See ***RemoteAccess-Workplace Configuration*** (on page 10).
2. Click Maintenance > Support. The Support page opens.

In the Support Login section:

- ☒ indicates the setting is enabled.
- ☐ indicates the setting is disabled.

#### Support Login

The Support Login may be used to examine the system in case of problems. Under normal circumstances it must be disabled!

#### Support Login



3. Click Edit.
4. Select the Support Login checkbox.
5. Click Save.

6. Provide your RemoteAccess-Workplace's IP address to G&D Technical Support.
  - To retrieve the IP address(es), right-click the network icon in the Main Toolbar to select Connection Information. See ***Network Icon*** (on page 203).

---

**Important: Disable this feature immediately after G&D Technical Support finishes the troubleshooting task.**

---

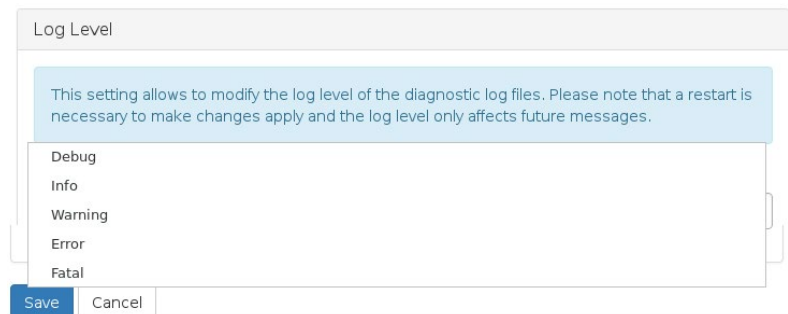
### Log Level for Diagnostic Log Files

1. If not displayed, launch the RemoteAccess-Workplace Configuration window. See ***RemoteAccess-Workplace Configuration*** (on page 10).
2. Click Maintenance > Support. The Support page opens.
3. Click Edit.
4. In the Log Level section, select which logs to include in the diagnostic log file.

---

*Note: Selecting Debug may affect system performance.*

---



5. Click Save. Click OK in the confirmation message to set the level and restart the RemoteAccess-Workplace.

---

### Diagnostic Log File

When the RemoteAccess-Workplace does not work properly, you can export the RemoteAccess-Workplace's diagnostic log file to a connected USB flash drive, and send the file to the G&D Technical Support for troubleshooting.

You must have the System Administration permission to perform this operation.

Note: The Diagnostic Log File is different from the Event Log. See Event Log.

► **To download the diagnostic log from the RemoteAccess-Workplace:**

1. Make sure your RemoteAccess-Workplace has a USB drive connected.
2. In the RemoteAccess-Workplace Configuration window, click Maintenance > Support.
3. Select the USB drive from the drop-down list, and click "Export to" to export the diagnostic log.

**Diagnostic Log File**

This allows the export of diagnostic log files to a connected USB Storage for sending to G&D Support. Please do not remove the USB Storage during export!

Export to

VERBATIM\_HD ▼

4. Wait until the RemoteAccess-Workplace finishes the export, displaying the "Successfully finished" message as well as the filename of the diagnostic log.
5. Send the file to G&D Technical Support.

---

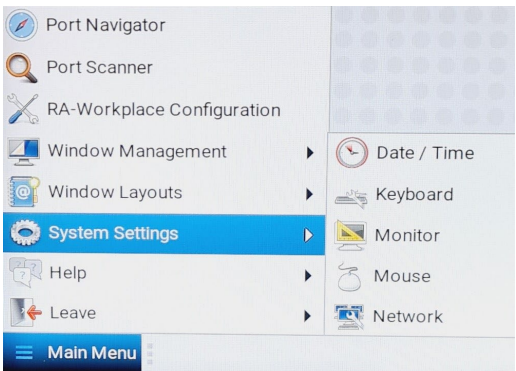
## About this Device

The "About this Device" page shows the firmware version information and the product serial number. You can access this page from the Main Menu or the RemoteAccess-Workplace Configuration window.

- In the RemoteAccess-Workplace Configuration window, click Maintenance > About this Device.
- In the Main Menu, choose Help > About this Device.

# System Settings

System Settings are found in the Main Menu.



## In This Chapter

Date/Time .....	176
Keyboard.....	179
Monitor .....	182
Mouse .....	184
Network .....	185
Default Shortcut Icons in the Main Toolbar .....	203

---

### Date/Time

1. Choose Main Menu > System Settings > Date/Time. The date/time dialog appears.



- See **Time Zone** (on page 178) for details on how time zone is used by manual and NTP date/time configurations.

**Configure Date and Time**

**Preferences**

Synchronize date and time over the network ☒

Time zone: Europe/Berlin Edit

**Time**

10 52 21

**Date**

< June > < 2021 >

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

Cancel OK Apply

► **To manually set date and time:**

- Click Edit and set the correct Time Zone if needed, then use the Time and Date sections to configure the current date and time. Note that the Time section uses a 24-Hour clock. Click Apply or OK when complete.

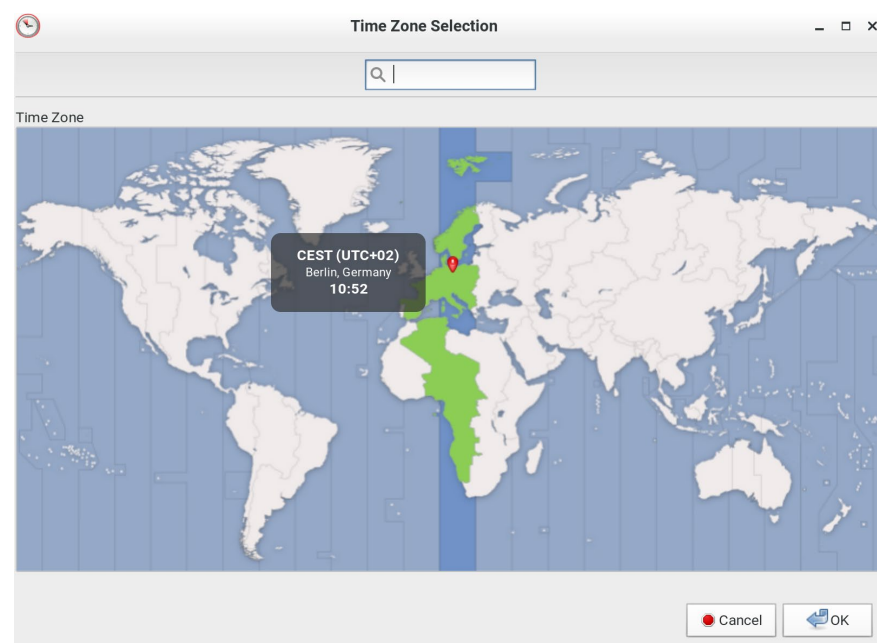
► **To use NTP:**

- Turn on "Synchronize date and time over network".
- Click Edit and set the correct Time Zone if needed.

## Time Zone

The time zone setting is important for both manual and NTP-synchronized time. If it is correct, do NOT change it unless required.

- For the time synchronized with an NTP server, time zone changes affect the time displayed onscreen, daylight savings time, and internal UTC-based clock of the RemoteAccess-Workplace.
- For the manual date and time, time zone changes do NOT affect the time displayed onscreen, but they affect the internal UTC-based clock.

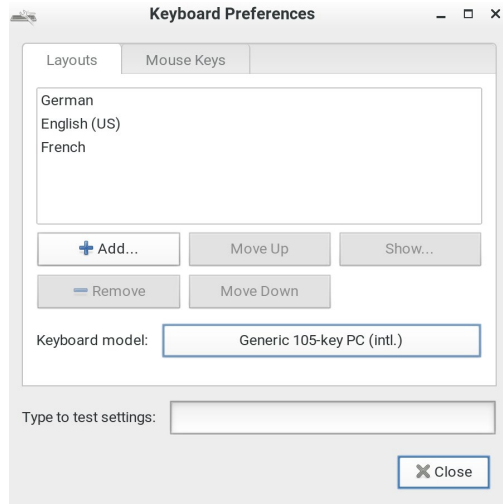


- Click Edit in the Date/Time settings to access the time zone map.
- Use the search box to find your city or zone. Select it to highlight it on the map, then click OK.

---

## Keyboard

1. Choose Main Menu > System Settings > Keyboard. The Keyboard Preferences dialog appears.



2. Click any tab to configure different keyboard settings.
  - Configure the keyboard layout in the tab labeled **Keyboard Layouts** (on page 179).
  - To use the keypad to move the mouse pointer, configure **Mouse Keys** (on page 181).
3. In the "Type to test settings" field, type anything to verify the current keyboard settings.

---

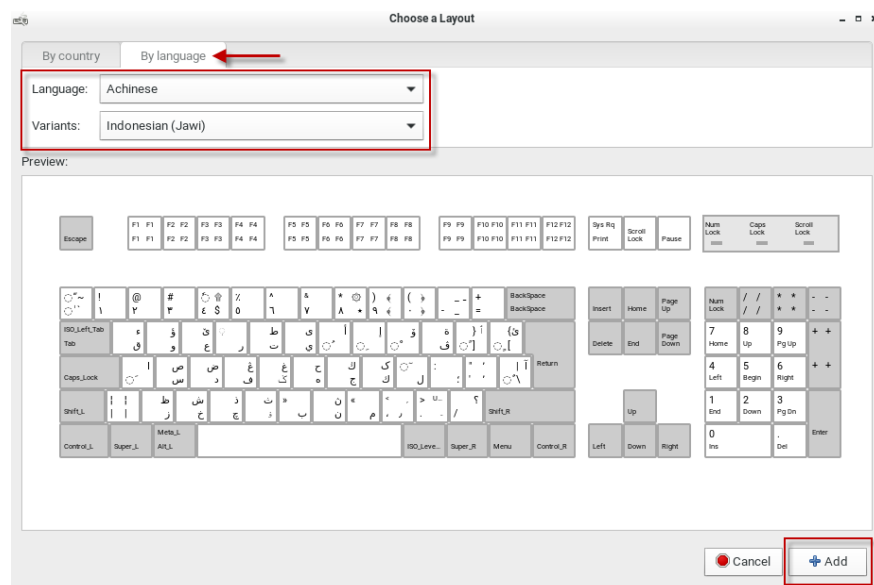
### Keyboard Layouts

In the Layouts tab, available keyboard layouts are all shown. The same keyboard layout list is also available when working with the keyboard icon in the Main Toolbar. Any changes made to the dialog's keyboard layout list also change the keyboard layout list available in the Main Toolbar. See **Main Menu, Port Navigator, Toolbar** (on page 2).

A maximum of four layouts are supported. If you have four layouts, you must remove one before you can add a new layout.

► **To manage available keyboard layouts:**

- To resort the keyboard layout list, select one layout and click Move Up or Move Down.
- To delete a layout from the list, select it and click Remove.
- To view keyboard layout looks like, select it and click Show.
- To add a layout to the list, click Add. If four layouts are already listed, you must remove one before you can add another. After clicking Add, select a layout by Country or Language to preview the keyboard layout. Click Add to add the layout to your list.



► **To determine the keyboard model:**

- Click the button in the "Keyboard model" field. Then select the vendor and model of your keyboard.

► **Reset to Defaults:**

- Click this button to reset all keyboard settings to the defaults.

## Mouse Keys

When you want to use the numeric keypad to control the mouse pointer/cursor, select the checkbox labeled "Pointer can be controlled using the keyboard."

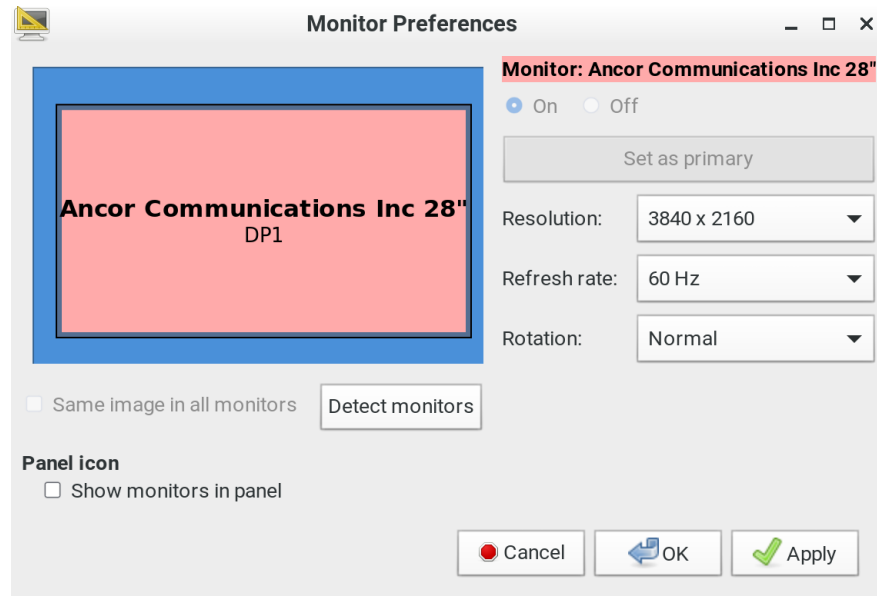
When enabled, each keypad key functions as the following table.

Key	Function
0	Depress the selected button
.	Release the selected button
1	Move toward the bottom-left corner
2	Move down
3	Move toward the bottom-right corner
4	Move left
5	Click the selected button
6	Move right
7	Move toward the top-left corner
8	Move up
9	Move toward the top-right corner
Num Lock	The other alternative to activate or deactivate the Mouse Keys function is to press: <i>Left Alt+Left Shift+Num Lock</i>
/	Select primary button
*	Select modifier button
-	Select alternate button
+	Double click the selected button
Enter	Enter

- Acceleration: Use the slider bar to adjust the pointer acceleration rate. Left side is faster and right side is slower.
- Speed: Use the slider bar to adjust the pointer speed. Left side is slower and right side is faster.
- Delay: Use the slider bar to adjust the delay prior to pointer movement. Left side is shorter and right side is faster.

## Monitor

1. Choose Main Menu > System Settings > Monitor. The Monitor Preferences dialog appears.



2. Perform or configure any of the following function:

Setting/button	Function
On/Off	Turn on or off this monitor, if there are two monitors connected to the RemoteAccess-Workplace. This setting is disabled when only one monitor is connected.
Set as primary	Click this button to specify this monitor as the primary monitor, when there are two monitors connected. This button is disabled when: <ul style="list-style-type: none"> <li>▪ Only one monitor is connected.</li> <li>▪ OR this monitor has been set as the primary one.</li> </ul>
Resolution	Determine the video resolution applied to this monitor.
Refresh rate	Determine the refresh rate applied to this monitor.

Setting/button	Function
Rotation	Determine how the image on the screen should be rotated, if intended.
Same image in all monitors	If two monitors are connected, determine whether both monitors show the same image. This setting is disabled when only one monitor is connected.
Detect monitors	Click this button if any connected monitor is not detected. Usually it is not necessary to use this function when there is only one monitor connected.
Show monitors in panel	Determine whether the monitor shortcut icon is added to the Main Toolbar. See <b>Main Menu, Port Navigator, Toolbar</b> (on page 2).

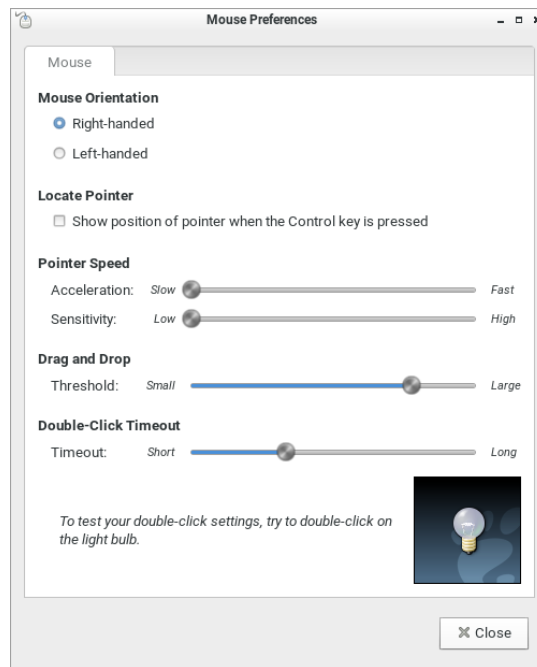
3. If any settings are changed, click OK to close the dialog, Apply to keep the dialog open, or Cancel to cancel.
  - If clicking OK or Apply, a confirmation message appears. Click Restore Previous Configuration to restore to the original settings, or click Keep This Configuration to apply the new settings.

---

## Mouse

The mouse preferences dialog affects how your mouse works in RemoteAccess-Workplace screens only. These settings do not affect your mouse in the KVM Client. For those settings, see ***Mouse Settings*** (on page 58)

1. Choose Main Menu > System Settings > Mouse. The Mouse Preferences dialog appears.



2. The following mouse settings can be adjusted:
  - Mouse Orientation: Right-handed or Left-handed
  - Locate Pointer: Select this option to show the position of the pointer when the Control key is pressed.
  - Pointer Speed: Adjust Acceleration and Sensitivity.
  - Drag and Drop: Adjust the threshold for drag and drop operations.
  - Double-Click Timeout: Adjust from short to long. Double-click the lightbulb graphic to test the setting.
3. Click Close to exit the dialog.



## Network

### Network Connections - Ethernet

You can connect the two LAN ports of the RemoteAccess-Workplace to the same or diverse subnets.

If you have connected both LAN ports to the network(s) when turning on or restarting the RemoteAccess-Workplace, the RemoteAccess-Workplace *randomly* selects one of the network connections as the default one. However, if you change the network settings of either or both connections, the "final" one that is changed will automatically become the default connection.

*Note: You can identify the default connection in the Connection Information dialog. See **Network Icon** (on page 203).*

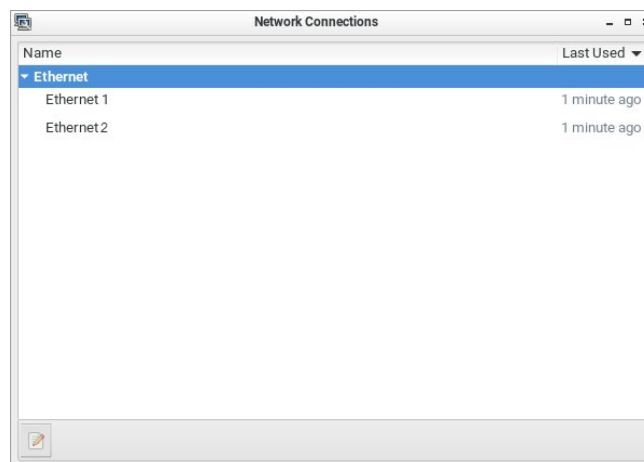
By default, both IPv4 and IPv6 addressing are enabled for both LAN ports, and the following are the default network settings:

- IPv4: *Automatic (DHCP)*
- IPv6: *Automatic*

You can also set additional ethernet options, such as MTU and Wake on LAN: See **Ethernet Settings** (on page 195). You can also configure bond devices: See **Network Connections - Bond Connections** (on page 197).

#### ► To change network settings:

1. Choose Main Menu > System Settings > Network. The Network Connections dialog appears, with two factory default connections listed for two LAN ports.
  - *Ethernet 1* is for LAN port 1, and *Ethernet 2* is for the other.



2. Select the desired connection, and click Edit. A dialog appears.

3. Enter a new name in the Connection name field if desired.

4. Click the IPv4 Settings or IPv6 Settings tab to configure network settings properly.

- **IPv4 Settings:**

Setting	Description
Method	<p>Select one of the following as the connection method and configure associated settings:</p> <ul style="list-style-type: none"> <li>▪ Automatic (DHCP)</li> <li>▪ Automatic (DHCP) addresses only</li> <li>▪ Manual</li> <li>▪ Disabled</li> </ul> <p>See <i>IPv4 Settings</i> (on page 187).</p>

- **IPv6 Settings:**

Setting	Description
Method	Select one of the following as the connection method: <ul style="list-style-type: none"><li>▪ Ignore</li><li>▪ Automatic</li><li>▪ Automatic, addresses only</li><li>▪ Automatic, DHCP only</li><li>▪ Manual</li></ul> See <i>IPv6 Settings</i> (on page 191).

5. Click OK. The new network settings apply now.

*Note: You can retrieve current IP addresses from the Connection Information dialog. See **Network Icon** (on page 203).*

IPv4 Settings

The screenshot shows the 'Editing Ethernet 1' window with the 'IPv4 Settings' tab selected. The 'Connection name' is 'Ethernet 1'. The 'Method' dropdown is set to 'Automatic (DHCP)'. Below this, there's a section for 'Additional static addresses' with columns for 'Address', 'Netmask', and 'Gateway', and buttons for '+ Add' and 'Delete'. Further down are input fields for 'Additional DNS servers', 'Additional search domains', 'DHCP client ID', and 'DHCP hostname'. A checkbox labeled 'Require IPv4 addressing for this connection to complete' is at the bottom left. A 'Routes...' button is at the bottom right. At the very bottom are 'Cancel' and 'OK' buttons.

- **Automatic (DHCP):**  
The DHCP server in the network automatically assigns an IPv4 address to the RemoteAccess-Workplace as well as DNS server(s) and domain(s).  
The following settings are configurable for this method.

Setting	Description
Additional DNS servers	<p><b>Optional.</b></p> <p>You may specify IP addresses of one or multiple additional DNS servers for resolving host names.</p> <p>Use commas to separate multiple servers.</p>
Additional search domains	<p><b>Optional.</b></p> <p>You may specify IP addresses of one or multiple additional domains for resolving host names.</p> <p>Use commas to separate multiple domains.</p>
DHCP client ID	<p><b>Optional.</b></p> <p>You can specify a DHCP client ID for identifying this RemoteAccess-Workplace in the network.</p>
DHCP client hostname	<p>Optional.</p> <p>You can specify a preferred hostname to send to the DHCP server to use for DNS name resolution</p>
Require IPv4 addressing for this connection to complete	<p>When deselected, either IPv4 or IPv6 addressing can be used to establish the connection.</p> <p>When selected, only IPv4 addressing is used for making the connection.</p>

Setting	Description
Routes	<p><b>Optional.</b></p> <p>Configure the IPv4 routing for this RemoteAccess-Workplace.</p> <ul style="list-style-type: none"> <li>Click Add to add one or multiple routing addresses for the RemoteAccess-Workplace to reach in the network.</li> <li>To remove any existing routes, select it and click Delete.</li> <li><i>Ignore automatically obtained routes:</i> Select this checkbox only when you want to use manually-specified routes.</li> <li><i>Use this connection only for resources on its network:</i> If selected, this connection will be used only when retrieving resources from the network. It will never be used as the default network connection.</li> </ul>

*Note: You can retrieve current IP addresses from the Connection Information dialog. See **Network Icon** (on page 203).*

► **Automatic (DHCP) addresses only:**

The DHCP server in the network automatically assigns an IPv4 address to the RemoteAccess-Workplace, but no DNS servers or domain servers are specified.

The following settings are configurable for this method.

Setting	Description
DNS servers	<p>Specify IP addresses of one or multiple DNS servers.</p> <p>Use commas to separate multiple servers.</p>
Search domains	<p>Specify IP addresses of one or multiple domains for resolving host names.</p> <p>Use commas to separate multiple domains.</p>
DHCP client ID	See the above table for information of these



Setting	Description
Require IPv4 addressing for this connection to complete	fields/options.
Routes	

► **Manual:**

Select this method when intending to manually assign a static IP address to the RemoteAccess-Workplace.

In the Addresses section, click Add and then type the RemoteAccess-Workplace's IPv4 address, netmask and gateway in this section. At least one IPv4 address, netmask and gateway must be specified.

**Addresses**

Address	Netmask	Gateway	 Add
192.168.60.80	24	192.168.60.1	
			 Delete

The following settings are configurable for this method. See the above table for associated information.

- DNS servers
- Search domains
- Require IPv4 addressing for this connection to complete
- Routes

► **Disabled:**

The IPv4 networking settings are all disabled.

## IPv6 Settings

Editing Ethernet 1

Ethernet IPv4 Settings IPv6 Settings

Method: Automatic

**Additional static addresses**

Address	Prefix	Gateway

+ Add  
Delete

Additional DNS servers:

Additional search domains:

IPv6 privacy extensions: Disabled

IPv6 address generation mode: Stable privacy

☐ Require IPv6 addressing for this connection to complete

Routes...

Cancel OK

## ► Automatic:

IPv6 auto-configuration automatically assigns an IPv6 address to the RemoteAccess-Workplace, and retrieves the information of DNS server(s) and domain(s) from the DHCP server.

The following settings are configurable for this method.

Setting	Description
Additional DNS servers	<b>Optional.</b> You may specify IP addresses of one or multiple additional DNS servers for resolving host names. Use commas to separate multiple servers.
Additional search domains	<b>Optional.</b> You may specify IP addresses of one or multiple additional domains for resolving host names. Use commas to separate multiple domains.

Setting	Description
IPv6 privacy extensions	<p>Determine whether and how privacy extensions apply to the IPv6 addressing.</p> <ul style="list-style-type: none"> <li>▪ Disabled: Disables privacy extensions.</li> <li>▪ Enabled (prefer public address): Enables privacy extensions and a public address is preferred.</li> <li>▪ Enabled (prefer temporary address): Enables privacy extensions and a temporary address is preferred.</li> </ul>
IPv6 address generation mode	<p>Determine how the address is generated:</p> <ul style="list-style-type: none"> <li>▪ Stable privacy</li> <li>▪ EUI 64</li> </ul>
Require IPv6 addressing for this connection to complete	<p>When deselected, either IPv4 or IPv6 addressing can be used to establish the connection.</p> <p>When selected, only IPv6 addressing is used for making the connection.</p>
Routes	<p><b>Optional.</b></p> <p>Configure the IPv6 routing for this RemoteAccess-Workplace.</p> <ul style="list-style-type: none"> <li>▪ Click Add to add one or multiple routing addresses for the RemoteAccess-Workplace to reach in the network.</li> <li>▪ To remove any existing routes, select it and click Delete.</li> <li>▪ <i>Ignore automatically obtained routes:</i> Select this checkbox only when you want to use manually-specified routes.</li> <li>▪ <i>Use this connection only for resources on its network:</i> If selected, this connection will be used only when retrieving resources from the network. It will never be used as the default network connection.</li> </ul>



---

*Note: You can retrieve current IP addresses from the Connection Information dialog. See **Network Icon** (on page 203).*

---

► **Automatic, addresses only:**

IPv6 autoconfiguration automatically assigns an IPv6 address to the RemoteAccess-Workplace, but no DNS servers or domain servers are specified.

The following settings are configurable for this method.

Setting	Description
DNS servers	Specify IP addresses of one or multiple DNS servers. Use commas to separate multiple servers.
Search domains	Specify IP addresses of one or multiple domains for resolving host names. Use commas to separate multiple domains.
IPv6 privacy extensions	See the above table for information of these fields/options.
Require IPv6 addressing for this connection to complete	
Routes	

► **Automatic, DHCP only:**

The DHCPv6 server in the network automatically assigns an IPv6 address to the RemoteAccess-Workplace, and specify DNS server(s) and domain(s).


The following settings are configurable for this method. See the above table for associated information.

- IPv6 address generation mode
- Require IPv6 addressing for this connection to complete
- Routes



► **Manual:**

Select this method when intending to manually assign a static IP address to the RemoteAccess-Workplace.

In the Addresses section, click Add and then type the RemoteAccess-Workplace's IPv6 address, prefix and gateway in this section. At least one IPv6 address, prefix and gateway must be specified.

**Addresses** 

Address	Prefix	Gateway
2605:0:2:1::5	64	2605:0:2:3::1

The following settings are configurable for this method. See the above table for associated information.

- DNS servers
- Search domains
- IPv6 address generation mode
- Require IPv6 addressing for this connection to complete
- Routes

► **Ignore:**

The IPv6 networking settings are all disabled.

## Ethernet Settings

Editing Ethernet 1

Connection name: Ethernet 1

Ethernet IPv4 Settings IPv6 Settings Miscellaneous

Device: [dropdown]

MTU: automatic [minus] [plus] bytes

Wake on LAN: ☒ Default ☐ Phy ☐ Unicast ☐ Multicast  
☐ Ignore ☐ Broadcast ☐ Arp ☐ Magic

Wake on LAN password: [text field]

Link negotiation: Ignore [dropdown]

Speed: 100 Mb/s [dropdown]

Duplex: Full [dropdown]

Cancel OK

### ▶ MTU:

- Select Automatic, or click plus/minus to specify the maximum number of bytes per packet.

MTU: [5] [minus] [plus] bytes

► **Wake on LAN:**

- Default: Leave as default, or deselect to enable other options.
- Phy
- Unicast
- Multicast
- Ignore
- Broadcast Arp
- Magic: Requires Wake on LAN password.

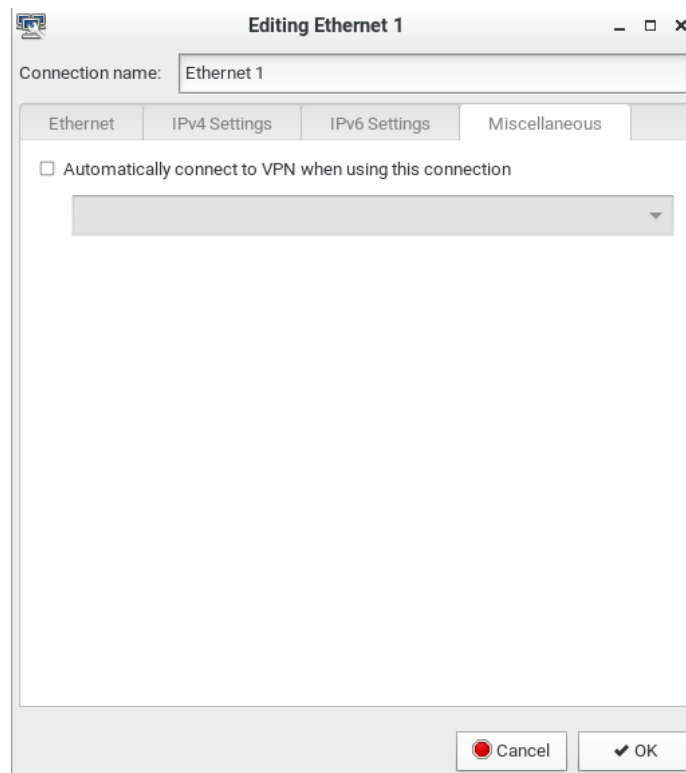
► **Link Negotiation:**

- Ignore
- Automatic
- Manual: Set Speed and Duplex.

### Miscellaneous Settings

The Miscellaneous settings tab is used when you have a VPN configuration.

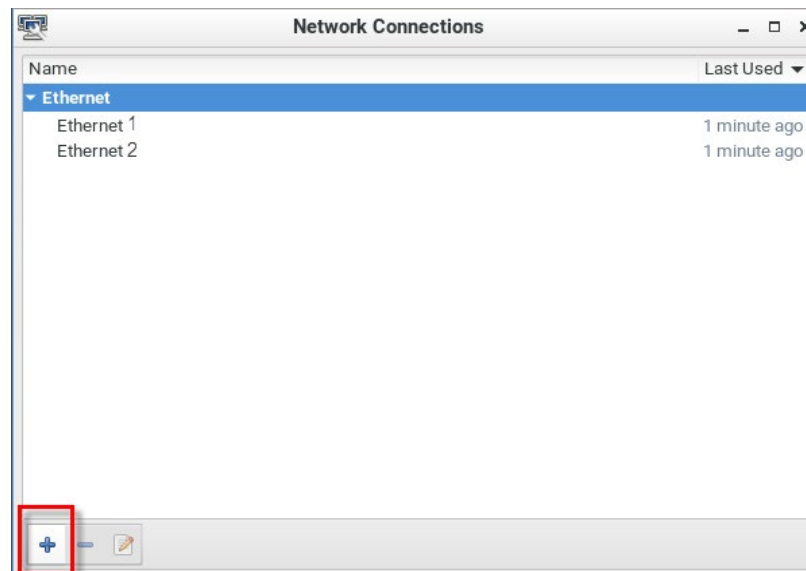
- Select the "Automatically connect to VPN when using this connection" to make sure your configured VPN is used automatically whenever the selected network is active.



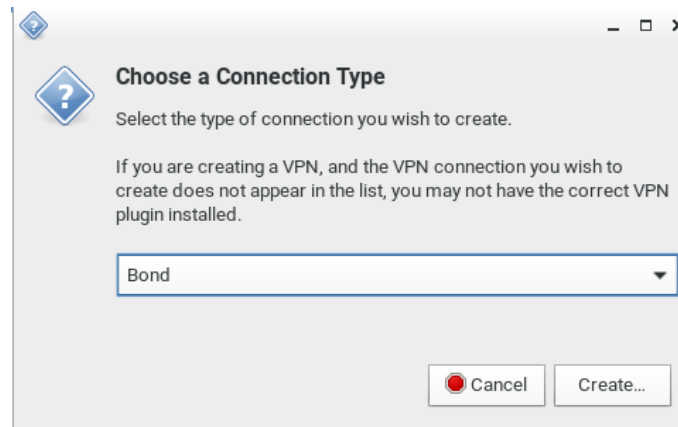
## Network Connections - Bond Connections

To create NIC redundancy, you can configure network bonding devices to replace the standard Ethernet configuration. This setup doubles the maximum network speed if both ports are used and provides redundancy. The RemoteAccess-Workplace network will continue to work if either one of the ports fails.

1. Choose Main Menu > System Settings > Network. The Network Connections dialog opens.
2. Click the Add Icon (plus sign).



3. In the Choose a Connection Type dialog, select Bond, then click Create.



4. The Bond Connection dialog opens.

**Editing Bond connection 1**

Connection name:

Bond | IPv4 Settings | IPv6 Settings | Miscellaneous

Interface name:

Bonded connections:

Mode:

Link Monitoring:

Monitoring frequency:    ms

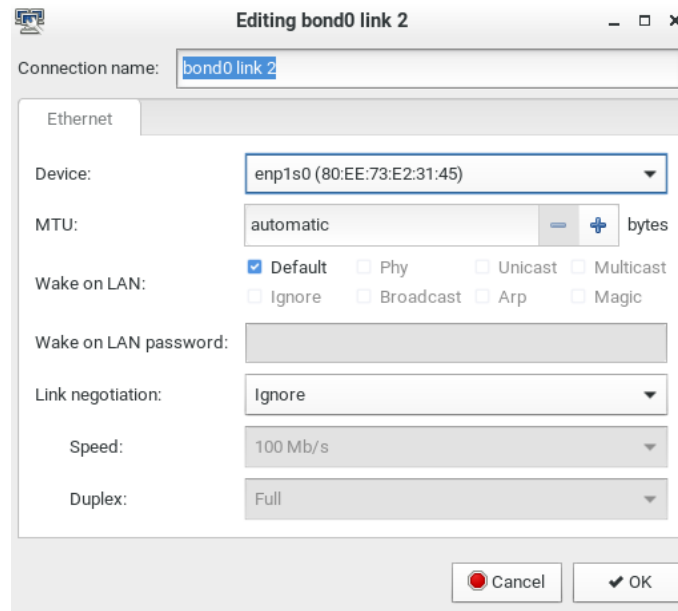
Link up delay:    ms

Link down delay:    ms

MTU:    bytes

5. In the Bond tab, click Add.
6. Select the connection type you want to use for the bond connection, then click Create to create the first bond link for the first network interface.
7. In the bond link dialog, select the MAC address of the interface in the Device field. Click OK.

8. Click Add again to add the second bond link, which is automatically set as the same connection type.



9. Click OK to save.
10. Return to the Main Menu > System Settings > Network page. Remove the old "Ethernet" entries, and keep the newly created "Bond Connection" entries.

---

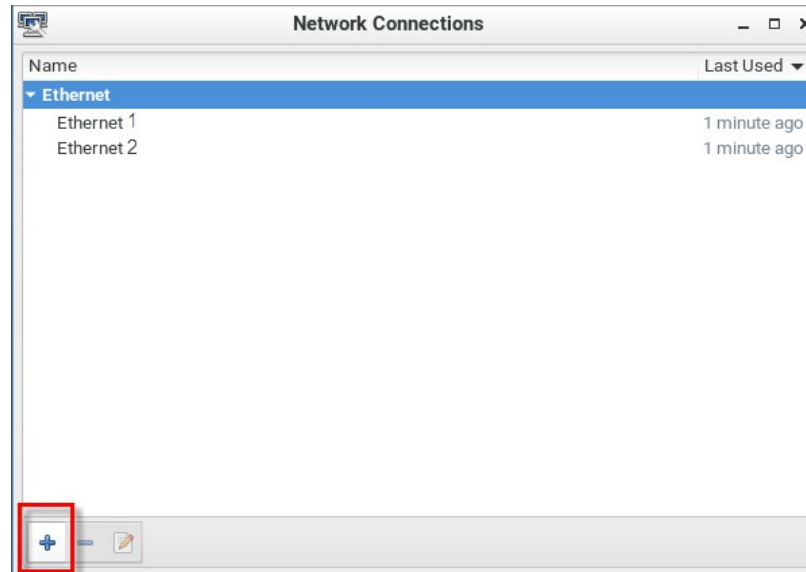
## OpenVPN Connections

An OpenVPN configuration can be uploaded to the RemoteAccess-Workplace to use a VPN client for all connections. You must provide a valid config file including certificates server details as filetype .OVPN. Consult the OpenVPN documentation for details on creating the file. Once uploaded, if your configuration setup includes "connect automatically", the VPN will be connected when RemoteAccess-Workplace reboots.

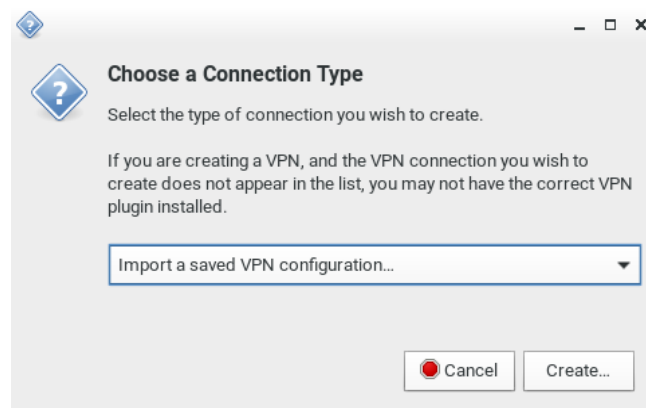
### ► To add OpenVPN connection:

1. Choose Main Menu > System Settings > Network. The Network Connections dialog opens.

2. Click the Add Icon (plus sign).

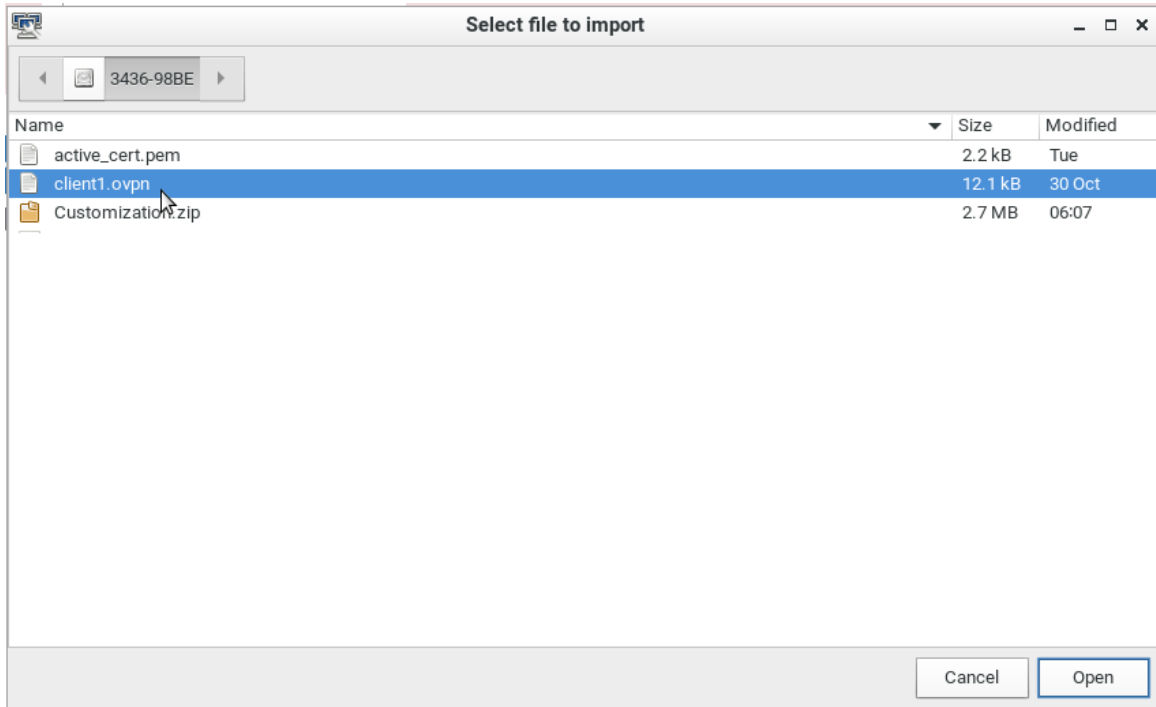


- In the Choose a Connection Type dialog, select "Import a saved VPN configuration..." then click Create.

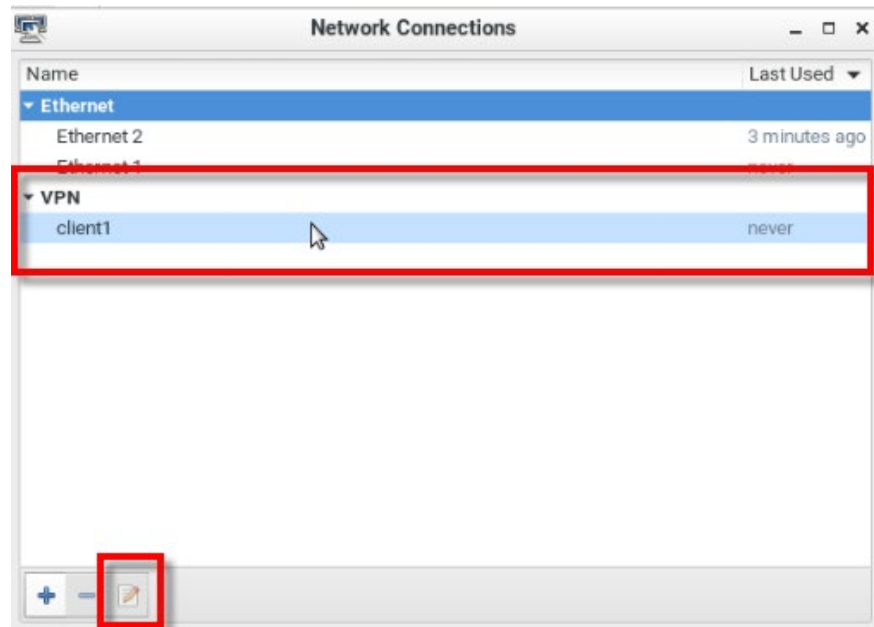




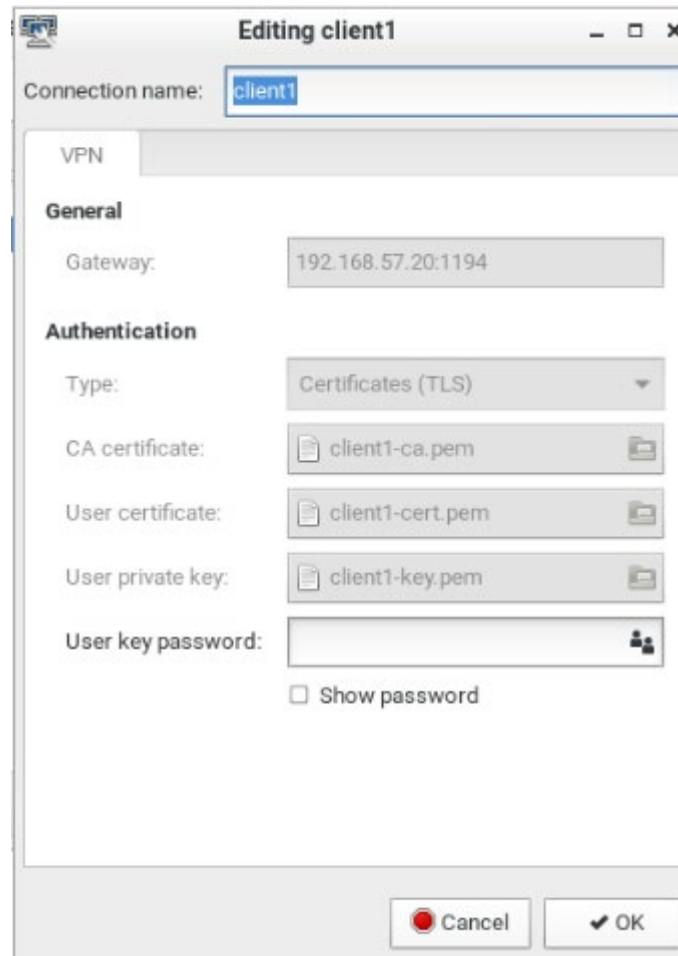
1. An upload dialog appears. Select the .ovpn config file, then click Open.



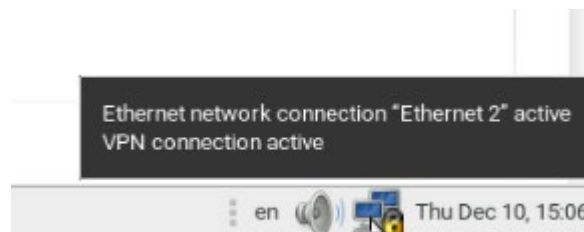
2. The VPN client is added. Select it and click the Edit icon.



3. Edit the VPN Connection name and/or enter password.



4. Click OK. When the VPN is connected, status bar will show that it is active. The "Lock" icon displays in the status bar when a user logs in with active VPN.



5. To automatically connect to VPN, edit the network connection, go to the Miscellaneous tab, and select "Automatically connect to VPN when using this connection". See *Miscellaneous Settings* (on page 196)

---

## Default Shortcut Icons in the Main Toolbar

Shortcut icons in the Main Toolbar provides quick access to some system settings. For information on the Main Toolbar, see **Main Menu, Port Navigator, Toolbar** (on page 2).

This section introduces the following factory default icons.



---

### Keyboard Layout Icon



#### ▶ Clicking the icon:

The keyboard layout switches among available languages. By default, the following languages are available.

- *en* - English (US)
- *fr* - French
- *de* - German

#### ▶ Right-clicking the icon:

A shortcut menu with these commands displays.

- *Layouts*: Changes the keyboard layout.
- *Keyboard Preferences*: Triggers the Keyboard Preferences dialog. See **Keyboard** (on page 179).
- *Show Current Layout*: Shows a keyboard image to indicate the current layout.

---

### Volume Icon



#### ▶ Clicking the icon:

A slider bar displays for you to adjust the volume.

#### ▶ Right-clicking the icon:

A shortcut menu with this command displays.

- *Mute*: Mutes the sound.

---

### Network Icon



► **Clicking the icon:**

A list of available Ethernet networks and connections displays.

- Only one network connection is shown if only one LAN port is connected to the network.
- Two network connections are listed if both LAN ports are connected to the network.
- By default, *Ethernet 1* is for LAN port 1, and *Ethernet 2* is for the other.
- You must have the System permission to make changes to network settings.

An "active" network connection is highlighted in bold, with a Disconnect command following it. To disable any active connection, select Disconnect.

- The formatting of that connection's name turns from bold to normal, indicating that it becomes inactive.

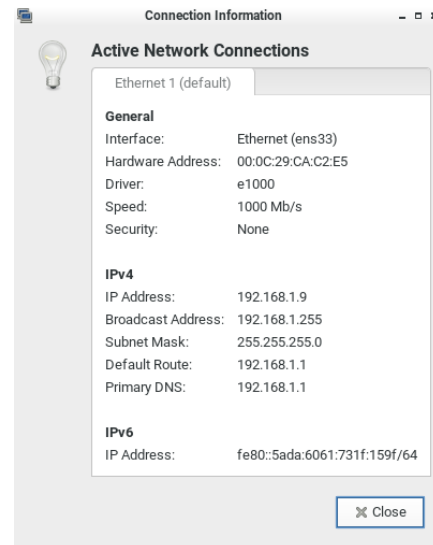
To activate any disabled network connection shown in the list, click it.

- The formatting of that connection's name turns from normal to bold, indicating that it becomes active.

► **Right-clicking the icon:**

A shortcut menu with these commands displays.

- *Enable Networking*: Enables or disables the networking capability. The default is to enable it.
- *Connection Information*: This command shows the networking information of the RemoteAccess-Workplace, including IPv4 and IPv6 addresses.



- When only one network connection is active, this dialog shows one tab.
- When both network connections are active, this dialog shows two tabs.
- The default connection has the word "default" shown on its tab.
- *Edit Connections*: This triggers the Network Connections dialog. See ***Network Connections - Ethernet*** (on page 185).

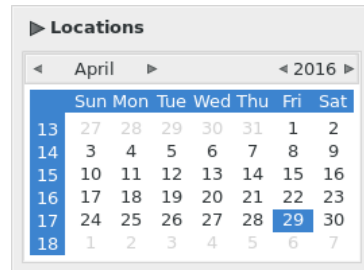
---

## Clock Icon

Mon Dec 4, 15:38

### ► Clicking the icon:

A calendar with Locations section displays.



Click Locations to:

- Determine the location and time zone of the RemoteAccess-Workplace.
- Change the time format of the clock shown in the Main Toolbar.

For details, see ***Location and Clock Time Format*** (on page 207).

To close the calendar, click the clock icon in the Main Toolbar again.

### ► Right-clicking the icon:

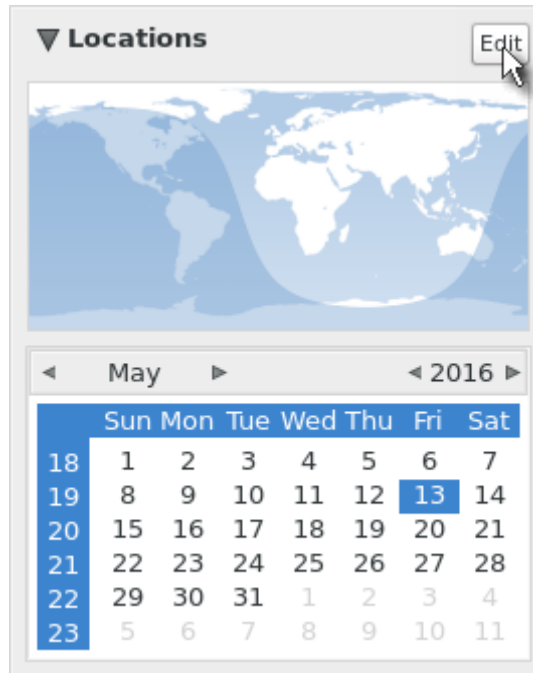
A shortcut menu with this command displays. You must have the System permission to change Date/Time settings.

- ***Adjust Date & Time***: This triggers the date/time dialog. You must have Systems permissions to change the date and time. See ***Date/Time*** (on page 176).

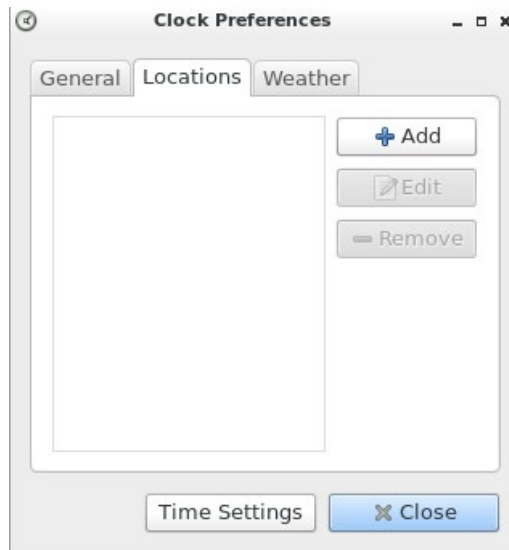
---

## Location and Clock Time Format

After expanding the Locations section, click Edit.



The Clock Preferences dialog appears. Click the desired tab or button to configure settings.



► **Time Settings:**

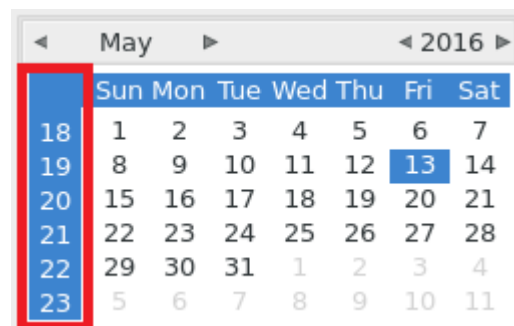
- See ***Date/Time*** (on page 176).

► **Locations:**

- Click Add to specify your city or country.
  - You can simply type the city or country name in the Location Name field and then select the correct one from the list that appears.
  - If your city's or country's name is not available in the list, you can manually specify the Timezone, Latitude and Longitude.
- To modify or delete any existing location in the Locations tab, select it and click Edit or Remove.

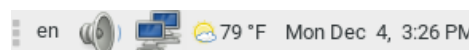
► **General:**

- *Clock Format:* Select the desired clock format to be shown in the Main Toolbar - 12 or 24 hour format.
- *Panel Display:* Select the information that is shown or available via the Main Toolbar - date, seconds, week numbers, weather and temperature.
  - Date and seconds, if selected, are shown in the clock on the Main Toolbar.
  - Week numbers, if selected, are shown in the calendar. A week number is the week's sequential number in a year.



- Weather and temperature, if selected, are shown in the following two positions:

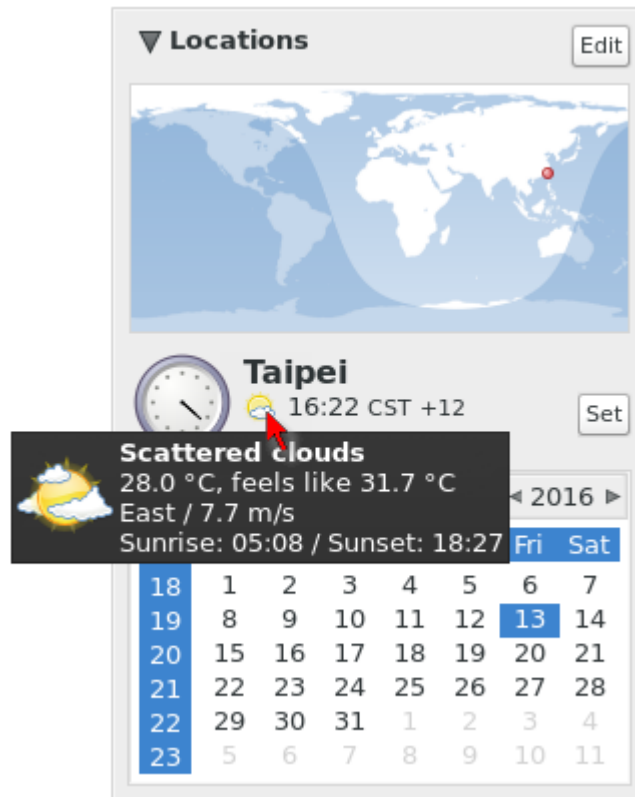
- **The Main Toolbar**





- **The Locations section:** When you hover your mouse pointer over the weather icon below the location name, more information is displayed, including the weather, temperature, wind speed and the time for sunrise/sunset.

*Tip: If the system's time zone setting is different from the selected location's and you have the System Administration privilege, a "Set" button appears to the right of the location name when hovering the mouse pointer around it. You can click the button to set the location's time zone as the system's time zone.*



► **Weather:**

- Determine the temperature unit: C (degree Celsius), F (degree Fahrenheit) or K (degree Kelvin).
- Determine the wind speed unit: m/s, km/h, mph, knots, or Beaufort scale.

# Additional Features

## In This Chapter

Screen Unlocking .....	210
Factory Reset at Startup .....	210
Take a Screenshot.....	211

---

### Screen Unlocking

When the RemoteAccess-Workplace screen is locked, no data is displayed onscreen.

---

*Note: See Desktop Settings for details on screen locking.*

---

When you attempt to unlock the screen, a password prompt appears. Only the user who locked the screen can unlock the RemoteAccess-Workplace. Other users must log out and then log in to the RemoteAccess-Workplace if intending to operate it.

► **To unlock the RemoteAccess-Workplace:**

1. Press any key on the keyboard.
2. A password prompt displays.
3. Enter the password of the user who triggered the screen-locking mode.
4. Click Unlock.

► **To log out of the RemoteAccess-Workplace:**

1. At the password prompt, click Log Out. NO password is needed.
2. The Login Screen displays, and any user can log in.

---

### Factory Reset at Startup

In addition to the factory reset feature in the RemoteAccess-Workplace Configuration window, you can reset the RemoteAccess-Workplace to factory defaults by performing the factory reset during the device boot.

Only the admin user can perform the factory reset at startup. Note that the factory reset removes all customized data. See **Factory Reset** (on page 169).

► **To perform factory reset when the device boots up:**

1. Restart or boot up the RemoteAccess-Workplace.
2. When a blinking text cursor displays on the top-left corner of the screen after the initial BIOS image, press Esc within a second.
3. A menu with the two options below is shown.
  - Boot RemoteAccess-Workplace
  - Reset RemoteAccess-Workplace to Factory Defaults
4. Select Reset RemoteAccess-Workplace to Factory Defaults.
  - To abandon the factory reset, select the other option.
5. When the system prompts you to enter user credentials, type the admin credentials: "Admin" user and the current admin password.
  - The default admin password is "4658"
6. If the admin credentials are correct, the RemoteAccess-Workplace performs the factory reset and then reboots. If the credentials are incorrect, the RemoteAccess-Workplace returns back to the menu.

---

## Take a Screenshot

To take a screenshot, you must be in a user group with the Take Screenshot privilege and a privilege such as Device Access that allows you to login. See **Privileges** (on page 113).

A hotkey must be configured for the function.

Your screenshot is saved to a connected USB storage device. If more than one USB storage is detected, the first device by alphabetical device name is chosen.

---

*Note: Active RDP sessions may affect the screenshot commands. When an RDP session is open, make sure to click in the RemoteAccess-Workplace desktop before taking a screenshot.*

---

► **To enable the hotkey for taking a screenshot:**

1. Open RemoteAccess-Workplace Configuration, then choose Preferences > Hotkeys.
2. Scroll down to "Screenshot of Desktop" and "Screenshot of Active Window". If the functions are enabled, use the hotkey displayed. If the functions are disabled, click Edit, then select a hotkey for the function.

See **Hotkeys and Gestures** (on page 98).

## Appendix A Authentication of RemoteAccess-Workplaces and RemoteAccess-GATEs

User credentials you use to log in to the RemoteAccess-Workplace can be different or identical to the user credentials you enter for accessing the port information of any RemoteAccess-GATE.

### ► RemoteAccess-Workplace's user credentials:

User credentials for logging in to the RemoteAccess-Workplace determine the tasks/permissions you are allowed to perform on the RemoteAccess-Workplace, but not the tasks/permissions you can perform on RemoteAccess-GATEs and KVM ports.

For example, user credentials of the RemoteAccess-Workplace determine whether you can add or remove the data of RemoteAccess-GATEs, or whether you can back up and restore the RemoteAccess-Workplace settings.

For detailed information on what you can do on a RemoteAccess-Workplace, see *Privileges* (on page 113).

### ► RemoteAccess-GATE's user credentials:

User credentials entered for RemoteAccess-GATEs determine the tasks/permissions you are allowed to perform while accessing computer devices connected to KVM ports (that is, target servers).

For example, user credentials for the RemoteAccess-GATE determine whether you can access all KVM ports on this RemoteAccess-GATE, or whether you can perform the virtual media or power control function on a KVM port/target server.

This is why users of the RemoteAccess-Workplace CANNOT share user credentials of RemoteAccess-GATEs, and each user must enter and save his or her own user credentials for RemoteAccess-GATEs respectively. See *Editing RemoteAccess-GATEs* (on page 13). However, if LDAP is enabled, and you can add your RemoteAccess-GATEs with a special setting that makes single sign-on possible. See *Adding RemoteAccess-GATEs* (on page 12), and also check the LDAP help for more details. See *LDAP* (on page 116).

For detailed information on what you can do with a KVM port/target server, see the user documentation for RemoteAccess-GATEs, which is accessible from G&D's website ([www.gdsys.com](http://www.gdsys.com)).

► **Examples:**

The following table illustrates different combinations of user credentials for RemoteAccess-Workplaces and RemoteAccess-GATEs.

User account for the RemoteAccess-Workplace	Tasks you can do on the RemoteAccess-Workplace	User account for the RemoteAccess-GATE	Tasks you can do on a KVM port/target server
Admin	<p>You can do anything, including:</p> <ul style="list-style-type: none"> <li>▪ System administration, such as backup or software update.</li> <li>▪ Device administration, such as adding RemoteAccess-GATEs.</li> <li>▪ Device access, such as access to the data of all RemoteAccess-GATEs and KVM ports.</li> </ul>	user-A	<p>Limited privileges are granted:</p> <ul style="list-style-type: none"> <li>▪ Port access permitted.</li> <li>▪ No virtual media access permitted.</li> <li>▪ No power control permitted.</li> </ul>
user-1	<p>Limited privileges are granted:</p> <ul style="list-style-type: none"> <li>▪ Device access permitted.</li> <li>▪ No device administration permitted.</li> <li>▪ No system administration permitted</li> </ul>	Admin	<p>You can do anything, including:</p> <ul style="list-style-type: none"> <li>▪ Port access.</li> <li>▪ Virtual media access.</li> <li>▪ Power control permitted.</li> </ul>
Admin	You can do anything. See above.	Admin	You can do anything. See above.

## Appendix B Open Ports Recommendations

### ► Listening Ports:

By default, the RemoteAccess-Workplace does not have any listening ports opened unless the following settings are enabled:

- 443 (HTTPS) if Remote Control is enabled
- 22 (SSH) if Support Login is enabled
- 24800 if Keyboard/Mouse sharing is enabled

### ► Outgoing TCP Ports:

- 5000 and 443 for the communication to the RemoteAccess-GATE
- 5900 for VNC targets (configurable; some VNC clients may use other ports)
- 3389 for RDP targets (configurable)
- 22 for SSH targets (configurable)
- 80 and 443 for web targets
- 24800 for Keyboard/Mouse sharing
- LDAP uses port 389 or 636 (if TLS is used).

# Appendix C API

## In This Chapter

Session Management .....	215
Login Progress .....	216
Session Close / Logout.....	216
Access Functionality.....	217
Handling of Access Client Sessions .....	220
Maintenance .....	222

---

## Session Management

---

### Session Creation and Login

In order to use the API, users need to authenticate and create a session. The first step is always a POST to /session/login with the user credentials.

---

### Parameters

- username: The login name of the user. Required.
- password: The user's password. Required.
- user\_type: The type of the user. Optional. May be one of
  - "local" (users existing in the RemoteAccess-Workplace only)
  - "ldap" (LDAP authenticated users).
  - If not specified, local user is assumed.

---

### Response

- result: The result of the authentication process. One of:
  - success: The authentication was successful and the user is logged in. The session can be used immediately for further operations.
  - failed: The authentication failed. Either the given credentials are incorrect, or the user type is incorrect.

- `in_progress`: The authentication was successful, but the user is not logged in immediately. Instead, the login process is started and takes some time. There is another response value `"auth_id"` which can be used to wait for the login process to finish. Use a POST to the URL `/session/progress` to query the login process's status.

---

*NOTE: You cannot use this session for further requests until the login process is finished \*and\* you requested this finished state via `/session/progress`.*

---

- `auth_id`: The ID of the login process. Only used if `"result"` is `"in_progress"` and needs to be used for `/session/progress` to query the login process's progress.

---

## Login Progress

If the login process is started asynchronously and the `/session/login` call returned `"in_progress"` and `result`, it is required to wait until the login process is finished before making any further API calls. It is required to request the status of the login process until it is signalled to be finished. Use the `/session/progress` call to get the status.

---

### Parameters

- `auth_id`: The authentication ID returned by a call to `/session/login`.

---

### Response

- `progress`: The current status/progress of the login process. One of:
  - `unknown`: The `auth_id` is invalid, or the login process was not able to start correctly.
  - `initializing`: The login process is about to start.
  - `started`: The login process has started, but is not finished yet.
  - `done`: The login process is finished. From now on, you may use this session for further API requests.

---

## Session Close / Logout

When the remote API session is not needed anymore, it should be closed. When the session is closed, the user is logged out of the RemoteAccess-Workplace. Use a request to `/session/logout` to achieve this.

---

### Parameters

- `none`



---

**Response**

- **result:** A boolean value. True is the logout was successful, false otherwise (e.g. the user was already logged out of other reasons).
- **error:** Optional. An error if the result is false.

---

**Example**

- First, start the login process:

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d
'{"username":"Admin", "password":"4658", "user_type": "local"}'
https://192.168.3.175:8443/api/v1/session/login
{"result":"in_progress","auth_id":"4dc950f2-2f8b-424b-ba31-d6fb33f943b7"}
```

- Wait for the login process to end:

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d
'{"auth_id":"4dc950f2-2f8b-424b-ba31-d6fb33f943b7"}'
https://192.168.3.175:8443/api/v1/session/progress
{"progress":"started"}
```

- Now wait some seconds

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d
'{"auth_id":"4dc950f2-2f8b-424b-ba31-d6fb33f943b7"}'
https://192.168.3.175:8443/api/v1/session/progress
{"progress":"done"}
```

- Now, use the session for further request.
- Close the session and logout:

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json"
https://192.168.3.175:8443/api/v1/session/logout
{"result":true}
```

- The user is logged out, the session is closed.

---

**Access Functionality**

---

**Get Devices and Targets**

The RemoteAccess-Workplace supports two views on target systems:

- **Access Device centric view:** There are access devices, each device has one or more ports to connect to the target systems.
- **Targets view:** There are targets, each of them has one or more ways (access points) to access it.

For both views, there are ways to enumerate the access methods.

---

### Get Devices and Ports

In order to get all access devices with their ports, send a GET request to the `/access/items` URL. The result is an array of items (access devices) with all ports of the device. Some of the ports may not be accessible (either due to missing permissions, or if a port is unsupported). Also, a device may have multi-monitor port groups. In that case, the single ports are not accessible, but the port groups are.

Each of the items has the following members:

- `id`: The ID of the item.
- `name`: The name of the item.
- `ports`: An array of ports (see below)
- `port_groups`: An array of multi-monitor port groups (see below)

Each of the ports in the `ports` array has the following properties:

- `id`: The ID of the port
- `name`: The name of the port
- `port_type`: The type (KVM, Serial or unsupported port type)
- `status`: The port status of the port associated with this access point (KVM access points only)
- `availability`: The availability status of the port associated with this access point (KVM access points only)
- `access_id`: The ID of the access point, belonging to this port. Use the ID to create an access session to this access point of this port. If this port is not accessible, the this property is missing.

Each of the port groups in the `port_groups` array has the following properties:

- `id`: The ID of the port group
- `name`: The name of the port group
- `port_ids`: an array of port IDs forming this port group
- `access_id`: The ID of the access point, belonging to this port group. Use the ID to create an access session to this access point of this port group. If this port group is not accessible, this property is missing.

---

### Get Targets and Access Points

In order to get all targets and their access points, send a GET request to the `/access/targets` URL. You will retrieve an array of targets. Each target has an ID, a name and an array of Access Points. Each of the Access Points have an access ID (required to launch a target connection to this access point) and a type (KVM, Serial, SSH, VNC, etc.). The KVM and Serial targets which represent a port of a access device also have a status (up or down?) and an availability setting.

The call returns an array of targets. Each target has the following members:

- `id`: The ID of the target.
- `name`: The name of the target.
- `access`: An array of access points to this target (see below).

Each of the access points has the following members:

- `access_id`: The ID of this access point. Use the ID to create an access session to this access point of this target.
- `access_type`: The type of this access point (KVM, Serial, RDP, VNC, etc.). The "multi\_kvm" type refers to a pre-configured multi monitor target on the access device, "virt\_multi\_kvm" is a virtual multi monitor target configured on the RemoteAccess-Workplace.
- `status`: The port status of the port associated with this access point (KVM access points only)
- `availability`: The availability status of the port associated with this access point (KVM access points only)

---

## Handling of Access Client Sessions

---

### Create Access Client Sessions

Access Clients (KVM, VNC, RDP, SSH, etc.) can be opened and closed via API.

To open an Access Client session, POST to the `/access/open_client` URL. This call has the following parameters:

- `access_id` (required): The Access Point ID. In order to get the ID, see above (Get Devices and Targets).
- `options` (optional): An array of key/value pairs to configure the session. See the API description for a list of available options.

#### ► Examples

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d
'{"access_id": 2}' https://192.168.3.175:8443/api/v1/access/open_client
{"result":true}
```

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d
'{"access_id": 2, "options": [ {"key": "current", "value": "true" } ]}'
https://192.168.3.175:8443/api/v1/access/open_client
{"result":true}
```

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d
'{"access_id": 2, "options": [ {"key": "fullscreen", "value": "false" },
{ "key": "x", "value": "1200" }, { "key": "y", "value": "800" }, { "key":
"width", "value": "300" }, { "key": "height", "value": "200" }, { "key":
"scale", "value": "true" } ]}'
https://192.168.3.175:8443/api/v1/access/open_client
{"result":true}
```

---

### Close Access Client

In order to close an Access Client session, POST to the `/access/close_client` URL. This call has one parameter: the Access Point ID. In order to get the ID, see above (Get Devices and Targets).

#### ► Example

```
curl -c cookies.txt -b cookies.txt --H "Content-Type: application/json" -d
'{"access_id": 2}' https://192.168.3.175:8443/api/v1/access/close_client
{"result":true}
```

---

## Named Scenes (aka Window Layouts)

Named Scenes (or Window Layouts) are collections of Access Client windows which can be saved and restored with all their positions and sizes. With the API, users can currently get a list of available scenes, and they can restore (or open) a scene. It is not possible to create new scenes or overwrite existing scenes currently.

### ► Get a list of scenes

To get a list of scenes, use a GET request to the `/access/scenes` URL. The API will return an array of scenes. Each scene has an ID (member `"id"`) and a `"name"`. One of the scenes may be the active one (the `"is_active"` member is true for this scene).

### ► Example

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json"
https://192.168.3.175:8443/api/v1/access/scenes
{"named_scenes":[{"id":22,"name":"Window Layout
1","is_active":false},{"id":23,"name":"Window Layout
2","is_active":true}]}
```

---

## Restore a Named Scene

To restore a Named Scene, POST to the `/access/open_scene` URL. This request has 2 parameters:

- `scene_id` (required): The ID of the scene. To get the ID of a scene, see above (Get a list of scenes).

### ► Example

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d
'{"scene_id": 23}' https://192.168.3.175:8443/api/v1/access/open_scene
{"result":true}
```

---

## Window Management

The RemoteAccess-Workplace API allows some special Window Management functions to arrange or close Access Client windows. To perform such an operation, POST to the /access/window\_management URL. This call has one parameter: the operation to perform. This may be one of the following:

- tile: Arrange the windows in tiles.
- untile: Un-do the latest "tile" operation.
- minimize: Minimize all windows
- unminimize: Restore the windows
- close: Close all client windows

### ► Example

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d
'{"operation": "close"}'
https://192.168.3.175:8443/api/v1/access/window_management
{"result":true}
```

---

## Maintenance

The RemoteAccess-Workplace supports some basic maintenance functions via the API. It currently has functions for identity, firmware information and update and settings backup/restore.

---

*Note: The firmware update and backup/restore functionality requires System Administration privileges.*

---

## Identity Information

In order to get some basic identity information, use a GET request to the /maintenance/identity URL. You will get the product code, the vendor, the device's serial number and the MAC addresses.

### ► Example

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json"
https://192.168.3.175:8443/api/v1/maintenance/identity
```

---

## Firmware Operations

### ► Software Versions

To retrieve some informations about the firmware versions, send a GET request to the `/maintenance/firmware` URL. The resulting object contains the versions of the installed firmware, the underlying operating system and the Linux kernel version.

### ► Example

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json"
https://192.168.3.175:8443/api/v1/maintenance/firmware
{"firmware_version":"4.4.0.5.85.20210323123034","base_os_version":"CentOS Linux release 7.9.2009 (Core)","kernel_version":"Linux 3.10.0-1160.6.1.el7.x86_64"}
```

---

## Firmware Update

To perform a software upgrade, use a POST request to the `/firmware/upgrade` URL. This request has one parameter: the URI of the firmware file. The RemoteAccess-Workplace will download this firmware upgrade file and apply it, if it is a valid update image. This call returns a boolean result, whether the update was initiated successfully or not. In case of an error, an error string is also returned.

---

*Note: Importing the firmware upgrade is done synchronously. Especially the download, but also the unpacking, will take some seconds to complete. Also, this API call just initiates the upgrade. Once the import is complete and the upgrade file is valid, this API function returns and the actual upgrade is done in background. API users have no control over the actual upgrade process. When the upgrade process is done, the RemoteAccess-Workplace will automatically reboot.*

---

### ► Example

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d
'{"uri":"https://192.168.2.101/RAW_4.4.0.5.226_update.bin"}'
https://192.168.3.175:8443/api/v1/maintenance/firmware/upgrade
{"result":false,"error":"The provided software version is too old! It must
be equal or newer than the current version."}

curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d
'{"uri":"https://192.168.2.101/RAW_4.4.0.5.230_update.bin"}'
https://192.168.3.175:8443/api/v1/maintenance/firmware/upgrade
{"result":true}
```

---

## Backup/Restore

With the RemoteAccess-Workplace Remote API, you can access system backup files. You can list all backups available in the system, you can download or upload them, you can restore or delete backups.

### ► Get all backups in the system

In order to get a list of all backup files currently available in the system, use a GET request to the `/maintenance/backups` URL.

The response is an array "backups" with all backups in the system. Each entry has the following members:

- `id`: The ID of the backup.
- `filename`: The name of the file internally representing this backup.
- `status`: The current status of the update. Since updates are created asynchronously, the creation of a backup may not be finished yet when you retrieve it. The following values are possible:
  - `initialized`: The backup has just been started. It is not created yet.
  - `working`: The backup process has started, but is not finished yet.
  - `complete`: The backup is finished and can be used.

### ► Get one backup in the system (metadata only)

If you are interested in one backup only (e.g. if you are waiting for the backup process to finish), you don't have to query the whole list of backups. When you know the ID of a backup, you can GET this backup's metadata only by sending a GET request to the `/maintenance/backups/<id_of_the_backup>` URL.

The response is similar to the list above, but only one backup is returned.

### ► Get the content of one backup file

To get the binary file data of a backup file, use a GET request to the `/maintenance/backups/<id_of_the_backup>/content` URL. This call returns the data in form of a Base64 encoded string (or an error in case something went wrong).

### ► Delete a backup in the system

To delete a backup in the system, use a GET request to the `/maintenance/backups/<id_of_the_backup>/destroy` URL. The call returns the result of the operation and an error string in case there was an error.

### ► Create a new backup



If you want to create a new backup of the system at the state it is currently in, then use a GET request to the `/maintenance/backups/new` URL. This returns the result (success or fail), the ID of the new backup (if successful) or an error string if something went wrong.

You can use the ID returned by this call for later use of the backup, e.g. you can download it later. Please note that the backup is created in the background and cannot be used immediately. Please request the details of this backup until the state property changes to "complete".

#### ► Import a backup file

There is also the possibility to upload or import backups into the system. Use a POST request to the `/api/v1/maintenance/backups/import` URL.

You can either upload the file directly (using a Base64 encoded string) (use the "content" parameter), or an URL can be specified (use the "uri" parameter), where the RemoteAccess-Workplace downloads the backup file from. This returns the result (success or fail), the ID of the new backup (if successful) or an error string if something went wrong.

Please note that you cannot have the same backup file more than once in the system. Uploading a backup which already exists will fail.

#### ► Restore a backup

To restore a backup, use a GET request to the `/maintenance/backups/<id_of_the_backup>/restore` URL. This returns the result (success or fail) and an error message in case of failure.

Please note that this call only initiates the restore process. The main work of restoring a backup is done in background, with shut down web services. It is not possible to see the progress or status of the restore process. When this call returns "success", this means the restore was successfully started. But it does not mean, the backup was successfully restored.

#### ► Example

- First, get a list of all backups in the system.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json"
https://192.168.3.175:8443/api/v1/maintenance/backups
```

```
{
  "backups": [
    { "id":11,"filename":"RAW_backup_4.4.0.5.85.20210324092030_12345_20
210325104406.dat","status":"complete" },
```

```
{ "id":10,"filename":"RAW_backup_4.4.0.5.85.20210324092030_12345_20
210325104402.dat","status":"complete" }
]
}
```

- Delete the existing backups.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json"
https://192.168.3.175:8443/api/v1/maintenance/backups/10/destroy
{"result":true}
```

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json"
https://192.168.3.175:8443/api/v1/maintenance/backups/11/destroy
{"result":true}
```

- Get the list again, which is now empty.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json"
https://192.168.3.175:8443/api/v1/maintenance/backups
{"backups":[]}
```

- Create a new backup

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json"
https://192.168.3.175:8443/api/v1/maintenance/backups/new
{"result":true,"backup_id":12}
```

- Now query the state of this backup

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json"
https://192.168.3.175:8443/api/v1/maintenance/backups/12
{"backup":{"id":12,"filename":"RAW_backup_4.4.0.5.85.20210324092030
_12345_20210325104912.dat","status":"working"}}
```

- The backup is not finished yet (status is "working"), wait some time and try again.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json"
https://192.168.3.175:8443/api/v1/maintenance/backups/12
{"backup":{"id":12,"filename":"RAW_backup_4.4.0.5.85.20210324092030
_12345_20210325104912.dat","status":"complete"}}
```

- The backup is now complete. Download it to a file.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json"
https://192.168.3.175:8443/api/v1/maintenance/backups/12/content >
backup.txt
{"content":{"[...]..."}}
```

- Delete the backup.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json"
https://192.168.3.175:8443/api/v1/maintenance/backups/12/destroy
{"result":true}
```

- Upload the backup again.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d
"@backup.txt"
https://192.168.3.175:8443/api/v1/maintenance/backups/import
{"result":true,"backup_id":13}
```

- Wait until the status of this backup is "complete".

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json"
https://192.168.3.175:8443/api/v1/maintenance/backups/13
{"backup":{"id":12,"filename":"RAW_backup_4.4.0.5.85.20210324092030
_20210325104912.dat","status":"complete"}}
```

- Or: Import the backup using an URL.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d
'{"uri":"http://192.168.2.101/backup.bin"}'
https://192.168.3.175:8443/api/v1/maintenance/backups/import
{"result":true,"backup_id":13}
```

- Now restore this backup.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json"
https://192.168.3.175:8443/api/v1/maintenance/backups/13/restore
{"result":true}
```

- The backup is restored in background. The RemoteAccess-Workplace reboots when finished.



## G&D. AND KVM FEELS RIGHT.

### Hauptsitz | Headquarter

Guntermann & Drunck GmbH Systementwicklung

Obere Leimbach 9 | D-57074 Siegen | Phone +49 271 23872-0  
sales@gdsys.com | www.gdsys.com

### US-Büro | US-Office

G&D North America Inc.

4001 W. Alemada Avenue | Suite 100, Burbank, CA 91505 | Phone +1-818-748-3383  
sales.us@gdsys.com | www.gdsys.com