GCM16 and GCM32 Global Console Managers
Product Guide

The Global 2X2X16 Console Manager (GCM16) and Global 4X2X32 Console Manager (GCM32) are the next generation digital keyboard-video-mouse (KVM) console managers that provide KVM-over-IP and serial console management technology in a single appliance. Either console lets you access and manage all servers remotely, even to the system BIOS, using your existing IP infrastructure.

The GCM16 has 16 target ports and supports up to 2 local users and 2 remote users, and the GCM32 has 32 target ports and supports up to 2 local users and 4 remote users. Figure 1 shows these two models.

Figure 1. The Global Console Managers: GCM16 (top) and GCM32 (bottom)

Did you know?

The GCM16 and GCM32 Global Console Managers provide enhanced remote management, access, and security capabilities with out-of-band access to servers, network equipment, and other devices with serial configuration or console ports all from a single appliance. This unified approach improves staff efficiency by reducing the time required to remotely diagnose, reconfigure, repair, or restore servers as well as network devices and other hardware with serial configuration or management consoles, or both.

The serial capabilities of these appliances enable connecting and managing nearly any device with a serial port directly from the console manager, including switches, routers, and PDUs. SSH and Telnet connections are supported.

Part number information

Ordering information is shown in Table 1. Note that when ordering with feature codes, use machine type-model 1754HC1 for the GCM16 and 1754HC2 for the GCM32.

Table 1. Ordering part numbers and feature codes

Description	Part number	GCM16 feature code	GCM32 feature code
Global Console Manager GCM16	1754D1X	1754HC1 fc 6694	Not applicable
Global Console Manager GCM32	1754D2X	Not applicable	1754HC2 fc 6695
Virtual Media Conversion Option Gen2 (VCO2)	46M5383	1754HC1 fc 5341	1754HC2 fc 5341
Serial Conversion Option (SCO)	46M5382	1754HC1 fc 5340	1754HC2 fc 5340

The GCM16 Global Console Manager includes the following items:

- 16-port console switch
- Mounting hardware for EIA space for rack sidewall compartment
- One 1U filler panel
- Two C13/C14 rack power cables
- RJ45-DB9F DCE adapter for use with Setup port
- RJ45-DB9M DTE adapter for use with Modem port
- 16 terminators for daisy-chaining configurations
- Installation publications and warranty

The GCM32 Global Console Manager includes the following items:

- 32-port console switch
- Mounting hardware for EIA space for rack sidewall compartment
- One 1U filler panel
- Two C13/C14 rack power cables
- RJ45-DB9F DCE adapter for use with Setup port
- RJ45-DB9M DTE adapter for use with Modem port
- 32 terminators for daisy-chaining configurations
- Installation publications and warranty

Each of the Conversion Option parts listed in Table 1 ships with:

- One Conversion Option
- Installation publications and warranty

The GCM digital console switches enable you to share one workspace (keyboard, mouse, and display) across many target systems. The target systems are connected to the console switch via CAT-5 cables and the appropriate conversion option at the target end. Conversion options are available with either USB or PS/2 connectors. Connections to serial devices are also supported with serial conversion options.

With server densities continually increasing, cable bulk remains a major concern for network administrators. The GCM16 and GCM32 switches significantly reduce KVM cable volume in the rack by utilizing the innovative conversion option cables and single, industry-standard CAT-5 UTP cabling. This allows a higher server density while providing greater airflow and cooling capacity. In addition, multiple target systems can be daisy-chained together using CAT-5 cables, and then all connected to the console switch using one cable, thereby eliminating a lot of cable clutter.

Feature comparison

The GCM16 and GCM32 replace the GCM2 Global Console Manager. Table 2 compares the console switches.

Table 2. Comparison of features

Feature	GCM16	GCM32
Model	1754D1X	1754D2X
Number of local concurrent users	2	2
Number of remote concurrent users	2	4
Local user connections - KVM	VGA + 2x USB	VGA + 2x USB
Local user connections - total USB	4 (including 2 for K & M)	4 (including 2 for K & M)
Maximum number of target systems - Direct (ARI ports)	16	32
Maximum number of target systems - Daisy-chained	256	512
Maximum number of target systems - Tiered configuration	1024 (2 levels)	1024 (2 levels)
Maximum video resolution	1600 x 1200 standard 1680 x 1050 widescreen	1600 x 1200 standard 1680 x 1050 widescreen
User interface	Web GUI (local and remote)	Web GUI (local and remote)
Manage remotely with Virtual Console Software (VCS)	Yes	Yes
Manage remotely with Avocent DSView	Yes*	Yes*
Keep Alive feature in Conversion Options	Yes	Yes
IPV6 support	Yes	Yes
User Authentication via user database in console switch	Yes	Yes
User Authentication via remote LDAP server	Yes	Yes
AES encryption	Yes	Yes
Manage serial devices	Yes	Yes
Manage intelligent power devices	Yes	Yes
Smart Card or Common Access Card support	Yes	Yes
Support for Virtual Media Conversion Option Gen2, VCO2 (46M5383)	Yes	Yes
Support for Serial Conversion Option, (SCO) 46M5382	Yes	Yes
Virtual media	Yes	Yes
Tiering	Yes	Yes
Gigabit Ethernet (10/100/1000 Mbps)	Yes (2)†	Yes (2)†
Serial port	Yes	Yes
Modem port for out-of-band access	Yes	Yes
Firmware upgrades to the console switch	Yes	Yes
Firmware upgrades to the COs	Yes	Yes
Input power	100-240V, 50/60 Hz 18 W power	100-240V, 50/60 Hz 24 W power
Redundant power supplies	Yes	Yes

* Avocent DSView management software available directly from Vertiv
† Ethernet ports are redundant for increased availability

Connections

Figure 2 shows the connections on the GCM32 Global Console Manager. The GCM16 Global Console Manager has identical connections except it only has 16 ARI ports, whereas the GCM32 has 32 ARI ports.

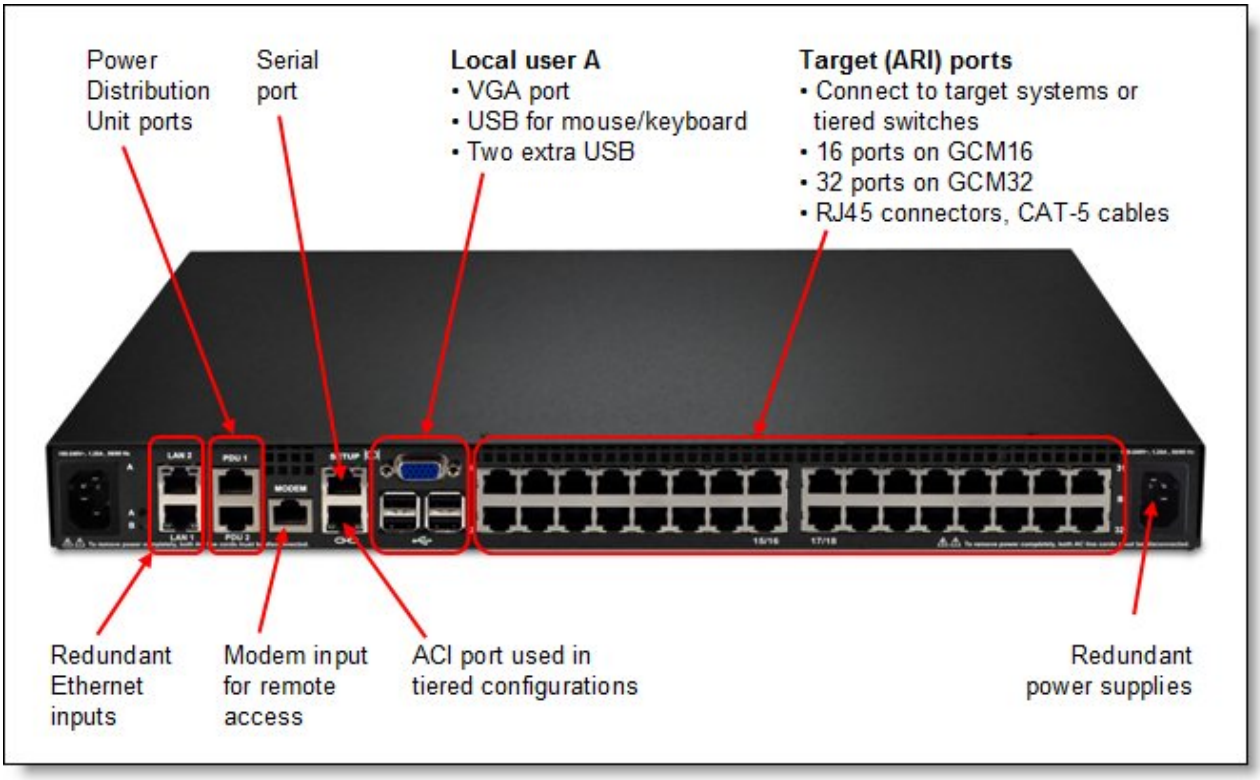

Figure 2. Connections on the GCM32 Global Console Manager

Note: Figure 2 shows the rear of the unit. There are no connectors on the front of the unit.

Features

Details about the features of the GCM16 and GCM32 are as follows:

Number of local concurrent users:

The GCM16 and GCM32 console switches enable one or two local user to access any attached servers. If the target device is currently in use, the user attempting to gain access will be given an opportunity to force a connection to the device if their preemption level is equal to or higher than the current user's level. If the user attempting to gain access has a lower preemption level, the active user will be asked if they wish to give up control to the new user (a timeout is also configurable).

The GCM16 and GCM32 both support two independent local users as shown in Figure 3. One local user attaches to the VGA and USB ports on the console switch as shown in Figure 2. The second local user attaches to a tiered (slave) console switch (see "Tiered consoles" below for more information). These two ports are independent of one another (that is, not pre-emptive or shared). This configuration allows you to place a console in every rack, for local connectivity to those servers complete with local KVM access, plus tier up to a master console that has local KVM access to all the servers attached to all attached console switches.

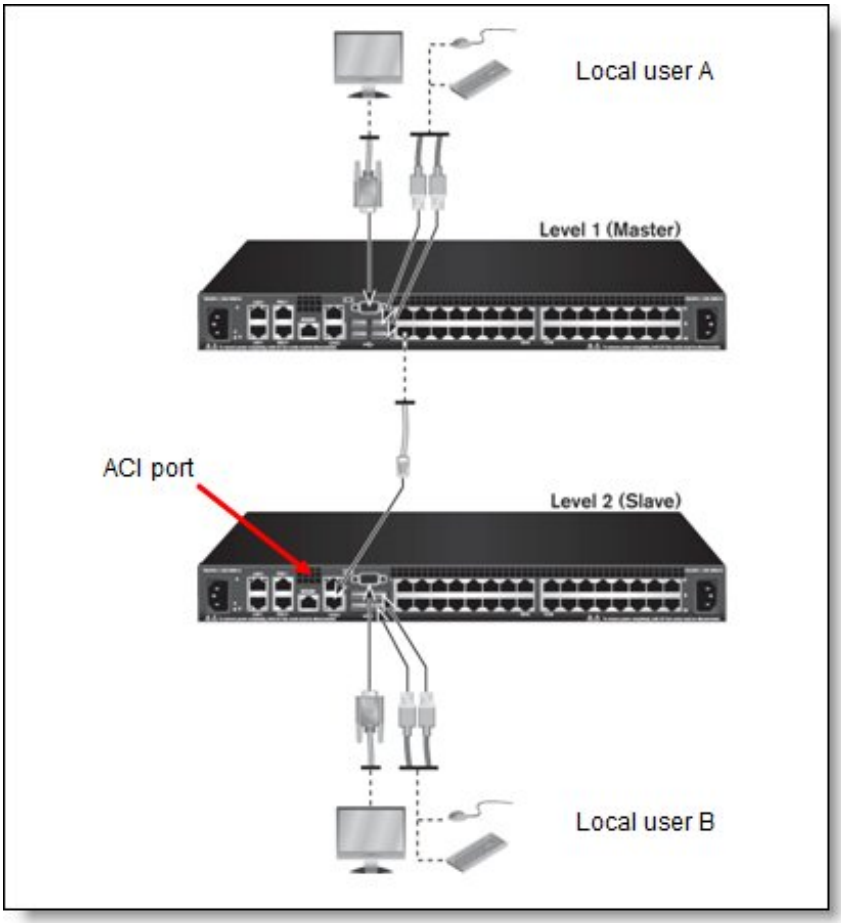

Figure 3. Two local users in a tiered configuration

Local user connections:

Local displays are connected to the console switch using VGA analog connections. Keyboard and mouse must be USB attached and two USB ports are provided for this purpose. Two additional USB ports are provided for the attachment of devices such as optical drives or memory keys. These devices can be made available on remote target systems provided Virtual Media Conversion Options are used to connect to those target systems. Note, however, that the Virtual Media Conversion Option does not support chaining of target systems.

Target systems:

The GCM16 has 16 target system ports (known as analog rack interface or ARI ports) and the GCM32 has 32 target system ports. These can be directly attached to systems with the appropriate USB or PS/2 conversion option connector on the end. These connections use standard CAT-5 cables. You can increase the number of connected target systems by two methods: chaining or a tiered arrangement of switches (more about these below). Both methods mean that each of the 16 or 32 ports will have multiple systems connected to it. You can mix connection methods.

Remote access via Ethernet or Modem:

Remote access to console switch and to the target systems is via a Web browser. The switch provides agentless remote control and access. No special software or drivers are required on the attached servers or client. Access is normally via a standard Ethernet network, requiring that the console switch be connected to the network via one or both Ethernet ports. Connecting both ports provides redundancy. Additionally, if a modem is connected to the modem port on the console switch and the modem is connected to a telephone (PSTN) system, then you can dial the console switch via your modem and establish an out-of-band connection to the console switch using the Point-to-Point Protocol (PPP) for remote control. V.34, V.90, or V.92 connections are supported.

Conversion Options:

These are cable-connector combinations that are connected between the CAT-5 cables from the console switches to the target systems. The figure below shows the conversion option cables that can be used with the console switches. The part numbers are listed in the Part number information section.

The Virtual Media Conversion Options (VCO and VCO2) supports the virtual media capability of the console switches; however, they do not support chaining.

Note: The KVM and USB conversion options are withdrawn from marketing.

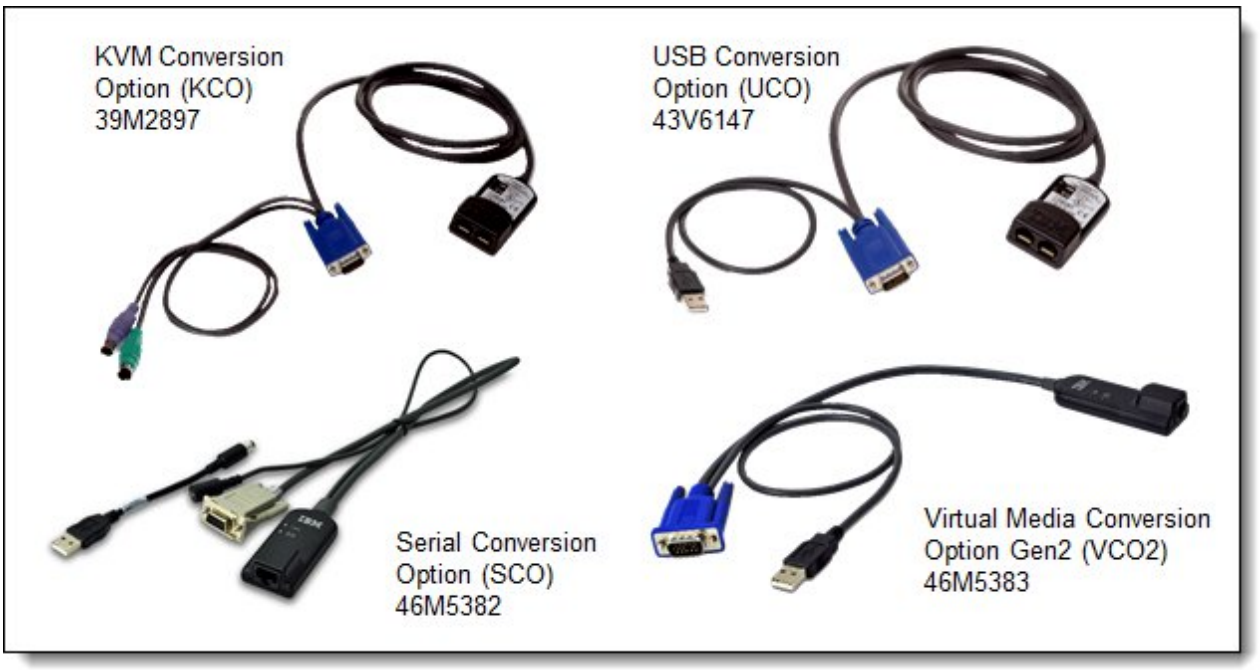

Figure 4. Available conversion options

The built-in memory of each connection option helps simplify configuration by assigning and retaining unique server identification codes for each attached server. This integrated intelligence enhances security and helps prevent unauthorized access to a server through cable manipulation. The connection option is powered directly from the server, providing Keep Alive functionality even if the server is not powered on.

Supported video resolutions are listed in the following table.

Table 3. Supported video resolutions

VCO2 Standard (4x3)	VCO Widescreen (withdrawn)	KCO & UCO (withdrawn)
640 x 480 @ 60 Hz 800 x 600 @ 75 Hz 960 x 700 @ 75 Hz 1024 x 768 @ 75 Hz 1280 x 1024 @ 75 Hz 1600 x 1200 @ 60 Hz	800 x 500 @ 60 Hz 1024 x 640 @ 60 Hz 1280 x 800 @ 60 Hz 1440 x 900 @ 60 Hz 1680 x 1050 @ 60 Hz 1920 x 1080 @ 60 Hz	640 x 480 @ 60 Hz 800 x 600 @ 75Hz 1024 x 768 @ 75 Hz 1280 x 1024 @ 75 Hz

Local and remote user interfaces:

The OSCAR interface of older console switches has been replaced by a Web browser interface, which is accessible both locally and remotely. You can use the local management interface by connecting directly to the local port to manage the GCM16 and GCM32 switches. You can also use the remote browser interface to manage your switch. The browser interface is launched directly from the switch, and any devices connected to the GCM16 and GCM32 switches are automatically detected. The local and remote user interfaces share a similar look and feel.

Virtual Media:

The GCM16 and GCM32 support virtual media when the target systems are connected using the Virtual Media Conversion Option Gen2 (VCO2), part number 46M5383. You can use virtual media support to connect USB 2.0 media devices to the console switch using one of the four USB ports and make those devices available to any connected system. With this feature, you can install software; install, upgrade, or recover the operating system; update the BIOS code; or boot the target system from a USB drive.

Control of how the USB device is connected to the target system is managed through the user interface. The browser interface presents the following configuration options:

- Virtual Media Locked: The locking option specifies whether a virtual media session is locked to the KVM session on the target device. When locking is enabled (default) and the KVM session is closed, the virtual media session will also be closed. When locking is disabled and the KVM session is closed, the virtual media session will remain active.
- Allow Reserved Sessions: Ensures that a virtual media connection can only be accessed with your username and that no other user can create a KVM connection to that target device. When the associated KVM session is disconnected, the virtual media session may be disconnected according to the Locked setting.
- Write Access: With this option, you can specify whether the target system can write to the USB device (assuming it is writable).
- Encryption: You can configure encryption levels for virtual media sessions. The choices are: None (default), 128-bit SSL (ARCFOUR), DES, 3DES, and AES.

Note that USB ports are assigned to a single virtual media session and cannot be independently mapped. This means you cannot map one USB device to one target system and another USB device to another target system.

Use of LDAP and smart cards to authenticate access:

The GCM16 and GCM32 support Lightweight Directory Access Protocol (LDAP) for integration with existing authentication/security models. This ensures that you maintain only one set of user credentials and can maintain strict password rules.

The GCM16 and GCM32 switches also allow you to use smart cards to ensure access is authorized. Smart cards are pocket-sized cards that store and process information. Smart cards such as the Common Access Card (CAC) can be used to store identification and authentication to enable access to computers, networks, and secure rooms or buildings. Smart card readers are connected directly to the switch via one of the USB ports, or they can be connected to any remote workstation that is running the remote browser interface or DSView management software and is connected to the switch using an Ethernet connection.

Note: For smart card use, the target device must be connected to the console switch using the Virtual Media Conversion Option Gen2 (VCO2), part number 46M5383.

Use of encryption:

The GCM16 and GCM32 support encryption for KVM signals and for remote media. Available encryption levels are 128-bit SSL, DES, 3DES, or AES. These are configurable via the browser interface.

True serial capabilities:

The GCM16 and GCM32 switches support Serial Conversion Option (SCO) cables that provide serial capabilities through Telnet. The capability provides a proper serial connection, not serial-to-VGA conversion. You can launch an SSH session or a serial client from the on-board Web interface to connect the targets that are connected to the GCM16 and GCM32 switches with an SCO cable. The SCO includes a separate USB-to-barrel power cord adapter - see Figure 2. Connect the USB end of the adapter to an available USB port on the target system to supply power to the SCO.

Managing Intelligent Power Distribution Units:

The dedicated Power Distribution Unit (PDU) ports on the GCM16 and GCM32 switches support the direct attachment of certain Avocent-branded Intelligent PDUs and can provide the ability to view and manage these units directly through the switch. Lenovo Intelligent PDUs are not supported.

Tiered consoles

You can tier multiple rack console switches to enable access to additional servers. In a tiered system, an ARI port on the main rack console switch connects to the ACI port of a tiered rack console switch (see Figure 3 for locations of these ports). Consider a tiered configuration if you want to manage servers connected to multiple switches from one central location. For example, you could have a primary GCM16 console switch with 16 switches tiered underneath it that all have servers chained on their ports.

The GCM16 and GCM32 support two levels of tiering. The use of virtual media and smart card authentication are both supported only when primary and secondary switches are GCM16 or GCM32 console switches.

Figure 6 shows an example of tiered consoles.

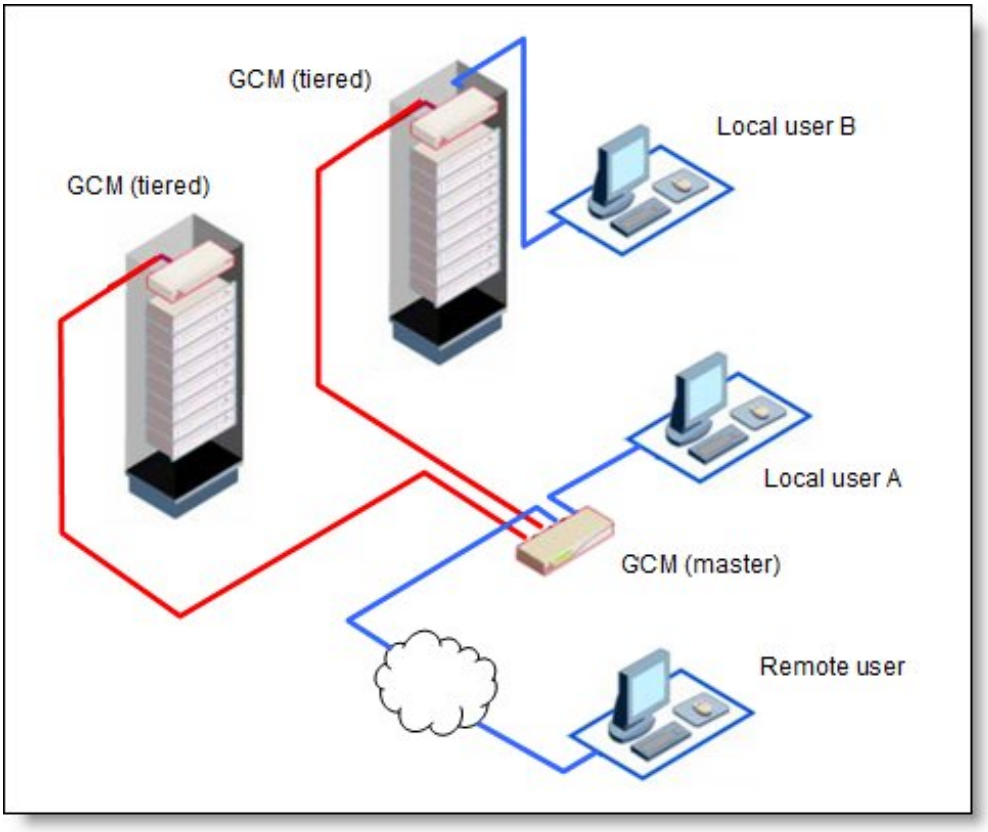

Figure 5. Tiered consoles

If there are local users attached to other tiered consoles, each can control target systems connected to that specific console. The local user at the primary console (Local user A in Figure 6) can preempt other local users if necessary.

The GCM16 and GCM32 support up to 1024 target systems in a tiered configuration.

Physical specifications

The GCM16 has the following specifications:

Height: 4.37 cm (1.72 inches) - 1 rack unit (1R)
Width: 43.18 cm (17 inches)
Depth: 32.4 cm (9.2 inches)
Weight: 3.2 kg (7.0 lb)

The GCM32 has the following specifications:

Height: 4.37 cm (1.72 inches) - 1 rack unit (1R)
Width: 43.18 cm (17 inches)
Depth: 32.4 cm (9.2 inches)
Weight: 3.5 kg (7.6 lb)

Operating environment

The adapter is supported in this environment:

- Temperature:
  - Operating: 0° to 50°C (32° to 132°F)
  - Non-operating: -20° to 70°C (-4° to 158°F)
- Relative humidity:
  - Operating: 20% to 80% (relative, non-condensing)
  - Non-operating: 5% to 95% (relative, 38.7 °C maximum wet bulb temperature)

Warranty

The GCM16 and GCM32 have a three-year limited warranty.

Avocent DSView management software

Avocent DSView management software, available directly from Avocent, provides data centers with a secure, centralized management solution for all IT assets. This software allows administrators to access, diagnose, and modify any managed device from any point on the globe, regardless of the health or status of the OS or the network connection to those devices. This software effortlessly extends the GCM16 and GCM32 KVM and serial management capabilities to include support for blades, embedded service processors, virtual servers, and other 3rd party devices in heterogeneous data center or remote office environments, making them more manageable, accessible, extensible, and secure.

This comprehensive control and manageability solution delivers secure, automated, real-time tracking and control of all your physical and virtual servers and embedded technologies, providing increased agility and security with a tangible return on investment.

Avocent DSView software features:

- Single, secure, browser-based interface to manage your entire datacenter or remote office
- Manages both physical and virtual assets
- Hub and spoke architecture for redundancy and real-time synchronization
- 60 day free software support

The DSView software is available directly from Vertiv:
https://www.vertivco.com/en-us/products-catalog/monitoring-control-and-management/software/avocent-dsview-management-software/

Related publications and links

For more information refer to these documents and Web links:

- Lenovo Press Product Guides for console switches and console kits:
  https://lenovopress.com/servers/options/kvm
- Global Console Manager GCM16 and GCM32 Installation and User's Guide
  https://support.lenovo.com/docs/UM103260
- Virtual Console Software Installation and User's Guide
  https://support.lenovo.com/docs/UM103259
- Avocent DSView from Vertiv
  https://www.vertivco.com/en-us/products-catalog/monitoring-control-and-management/software/avocent-dsview-management-software/

Related product families

Product families related to this document are the following:

- KVM Switches & Consoles

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION ”AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This document, TIPS0772, was created or updated on June 2, 2020.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/TIPS0772
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/TIPS0772.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®

Other company, product, or service names may be trademarks or service marks of others.