IBM Global Console Manager Firmware Update Guide

IBM Global 2x2x16 Console Manager (GCM16), 1754-D1X (1754-HC1)
IBM Global 4x2x32 Console Manager (GCM32), 1754-D2X (1754-HC2)

This page has been intentionally left blank

Second Edition (August, 2019)

Contents

Chapter 1 Introduction 1
Attention! 1
Prequisites 1
Chapter 2 Firmware update via remote OWBI 2
Default log on credentials 2
Checking current KVM firmware 2
Auto-updating attached Cable Options 2
Enabling CO auto-updating 3
Firmware update via Filesystem 5
Firmware update via TFTP 8
KVM firmware update via ftp 11
Firmware update via http 14
Chapter 3 Firmware update via local OWBI 17
Checking current KVM firmware 17
Auto-updating attached Cable Options 18
Enabling CO auto-updating 18
Firmware update with USB memory key 21
Prerequisites 21
Update procedure 21
Other methods to update the KVM firmware 23
Chapter 4 Added Functions 24
Blocking and unblocking TCP port 3871 24
Introduction 24
Disabling TCP port 3871 25
Appendix A. Disclaimer 28
Appendix B. Notices 29
Important 29
Customer responsibilities for code installation 30
Customer responsibilities 30
Trademarks 31
Printing this document 32
Fonts used in this document 33

Chapter 1 Introduction

This document provides information on the various methods on how to upgrade the firmware of the following IBM Keyboard, Video, and mouse switches (KVM):

- IBM Global 2x2x16 Console Manager (GCM16), 1754-D1X (1754-HC1)
- IBM Global 4x2x32 Console Manager (GCM32), 1754-D2X (1754-HC2)

There are two general interfaces that can be used for upgrading the firmware of an IBM Local Console Manager:

1. The remote On-board Web Interface (OWBI)
2. The local On-board Web Interface (OWBI)

Both methods require that an IP address, either IPv4 or IPv6, is assigned to the KVM switch to be upgraded.

The remote and local OWBI are very similar and have only minor differences.

Attention!

Before upgrading the firmware of the KVM switch all KVM sessions should be closed as else these will be disconnected. The KVM switch will automatically reboot after the code update has been applied.

Prequisites

In order to be able to update the firmware of an IBM GCM16 or GCM32 unit a valid IPv4 and / or IPv6 address needs to be assigned to the KVM switch.

Further either an ftp or a tftp or a http server must be available in the LAN where the firmware file for the KVM switch is located on.

Chapter 2 Firmware update via remote OWBI

Before following the instructions of this chapter review Chapter 1 .

This KVM switch has an On-board Web Interface which can be accessed via https.

In order to update the firmware the remote user must be logged on with unit administrative privileges.

Default log on credentials

The default Username for the administrator is *Admin* (case sensitive!) and no password.

Checking current KVM firmware

Checking the current KVM firmware can be done by clicking in the main menu under “Appliance” on “Versions”.

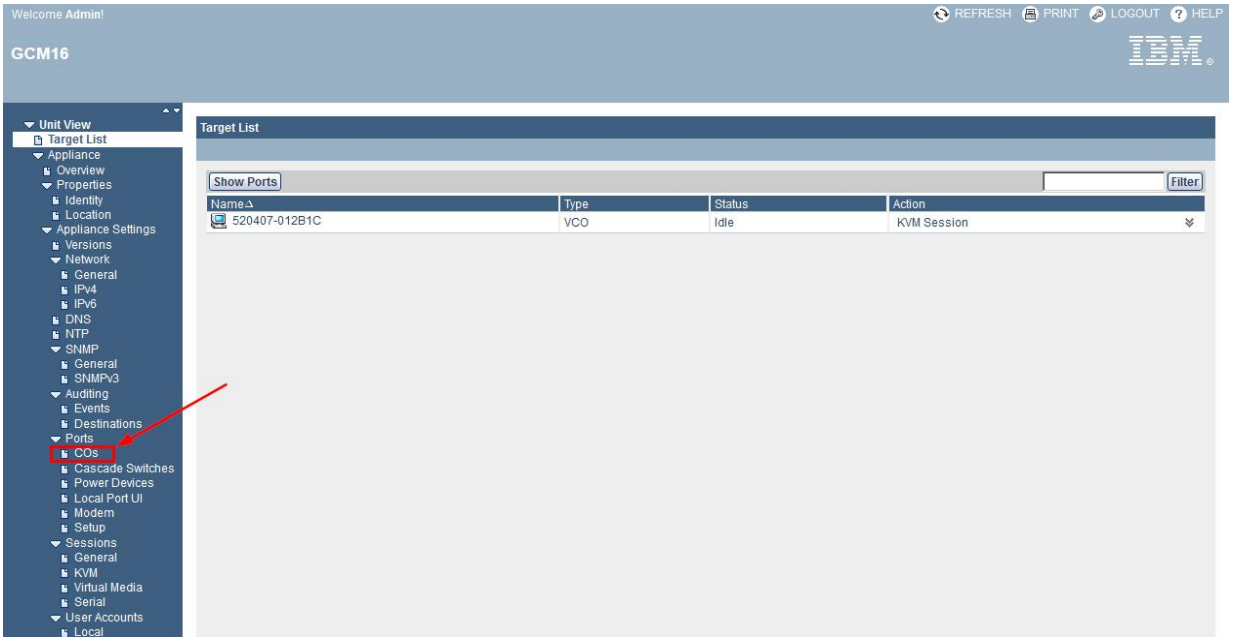
Auto-updating attached Cable Options

It is strongly recommended to ensure that any Cable Option (CO) gets updated when applying the firmware to the KVM switch. The auto-upgrade function guarantees that the CO firmware is compatible with the switch firmware. As COs come online, their firmware is automatically upgraded to that available on the switch.

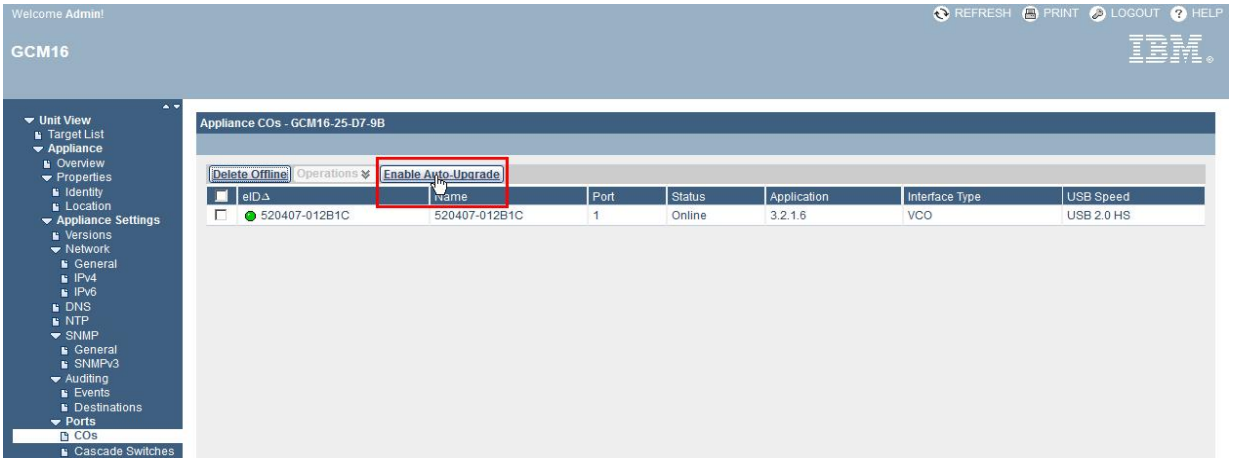
Enabling CO auto-updating

Notes: Before following the instructions of this chapter review Chapter 1 Introduction and the section Default log on credentials in Chapter 2.

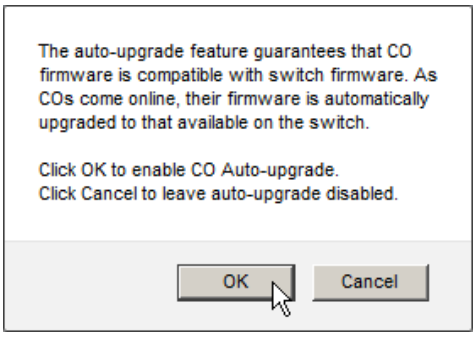
1. On the main menu click on “COs” under “Target List”



2. Click on “Enable Auto-Upgrade”



and confirm the selection by clicking on “OK” in the pop up window



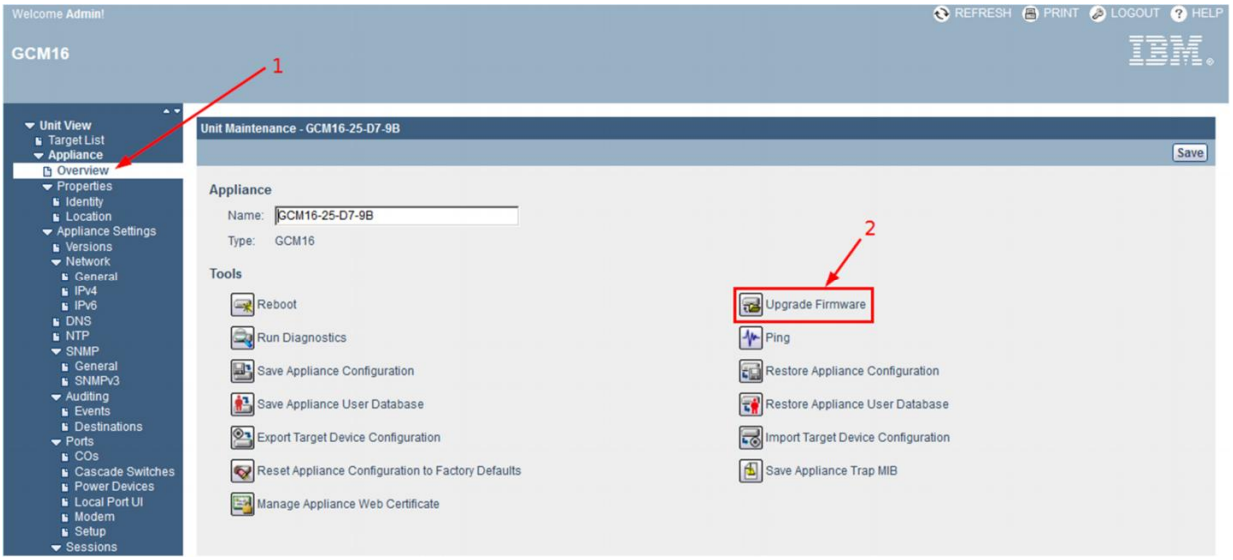
3. CO Auto-upgrade is now enabled

Firmware update via Filesystem

Notes:

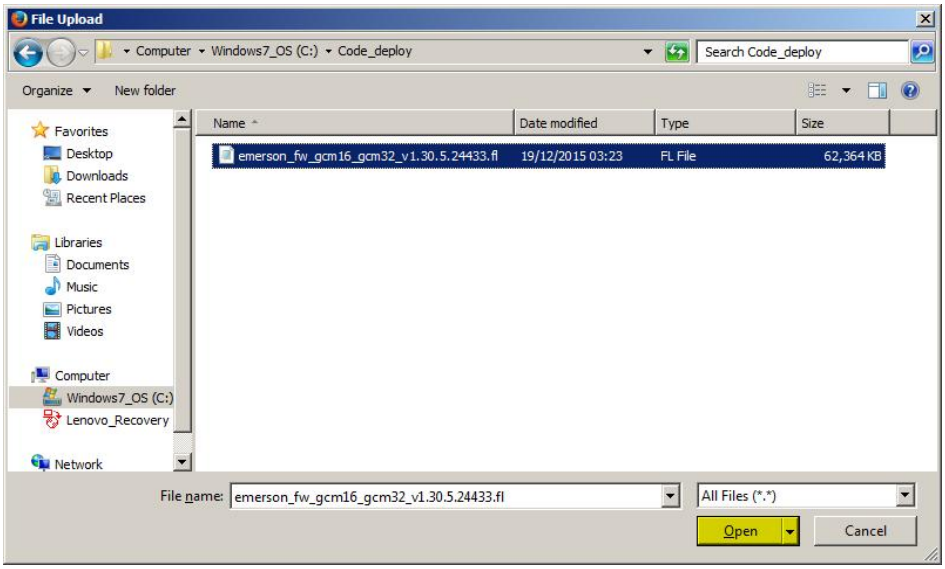
- Before following the instructions of this chapter review Chapter 1 Introduction and the section Default log on credentials in Chapter 2
- The firmware file name in this chapter are used for illustration purposes only. The actual firmware file name may be different

1. On the main menu on the left side click on “Overview” and then on the icon “Upgrade Firmware”

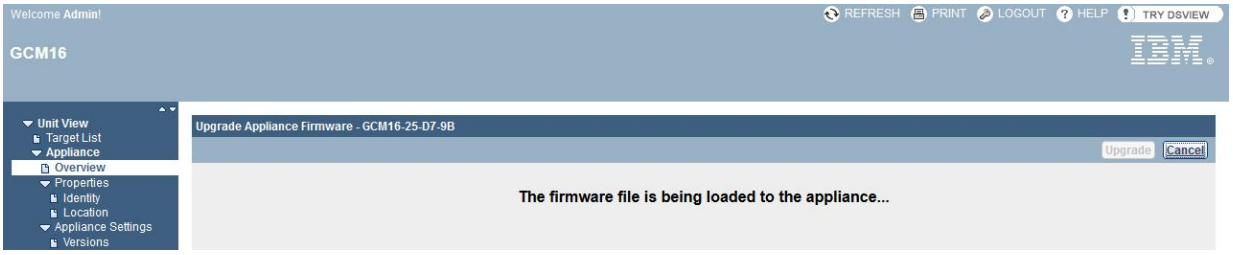


2. Click on the radio button left of “Filesystem”, click the “Browse” 1 button to navigate to the KVM firmware file on your local computer, and then click on “Upgrade” 2 button in order to initiate the firmware update

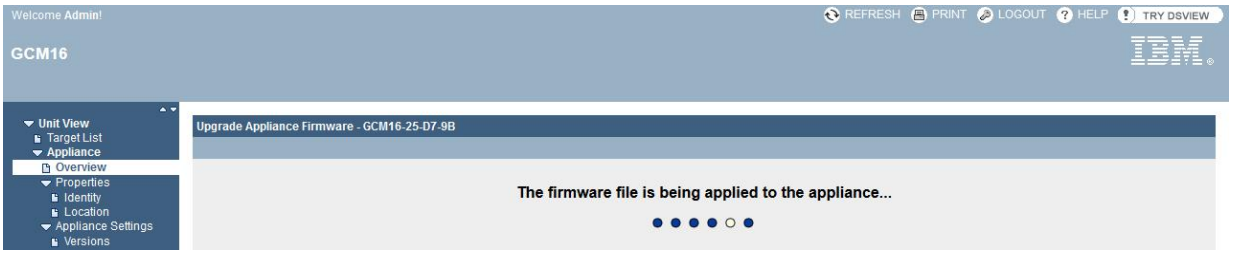
3. Browse to the directory containing the firmware file, click on it, click the “Open” button and then click on the “Upgrade” button to start the firmware update



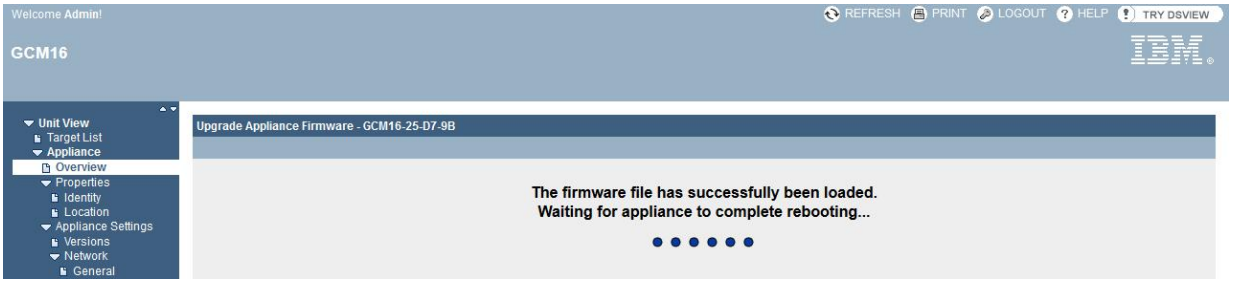
4. The firmware file will be transferred to the KVM switch



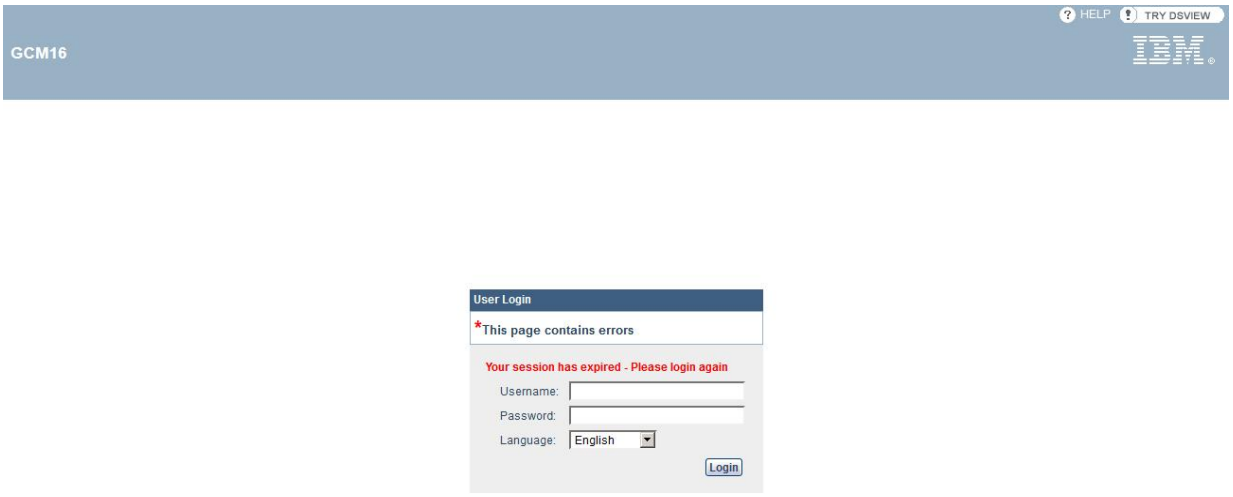
5. The firmware will be applied, that is flashed, to the KVM switch



6. Once the update has completed the KVM switch will reboot



7. After the firmware update is complete, the web browser should automatically reload to display the logon screen. If the browser does not auto-refresh then manually reload the page after a couple of minutes in order to display the logon screen

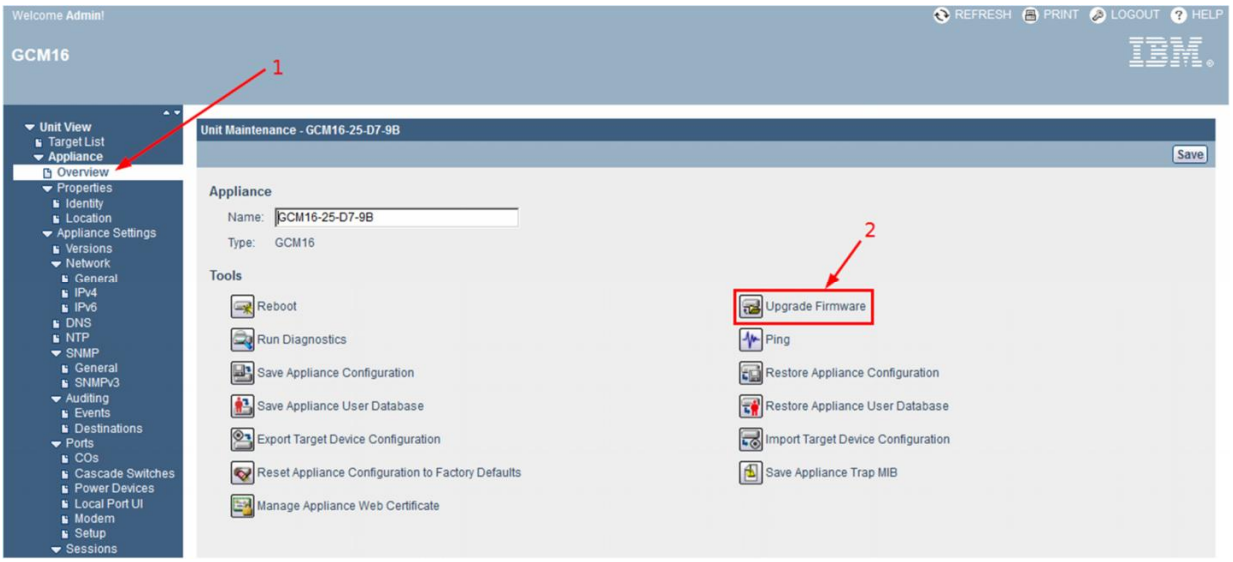


Firmware update via TFTP

Notes:

- Before following the instructions of this chapter review Chapter 1 Introduction and the section Default log on credentials in Chapter 2
- tftp is a simple and unsecure file transfer protocol
- The firmware file name in this chapter are used for illustration purposes only. The actual firmware file name may be different

1. On the main menu on the left side click on “Overview” and then on the icon “Upgrade Firmware”

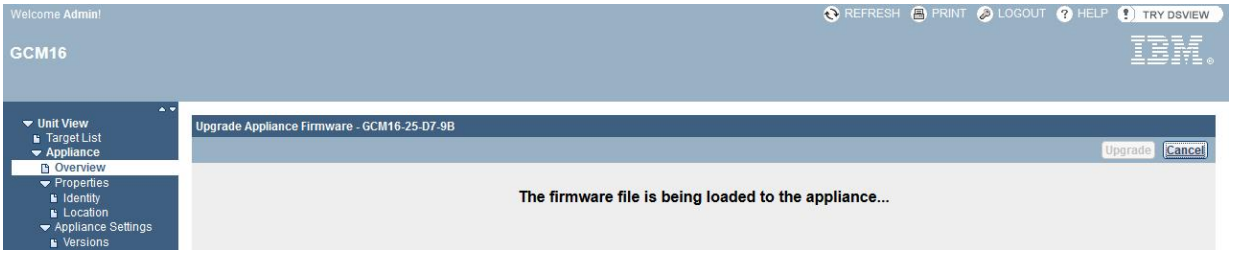


2. Click on the radio button left of “TFTP” 1, enter the IP address of the tftp server, and then click on the “Upgrade” 2 in order to initiate the firmware update

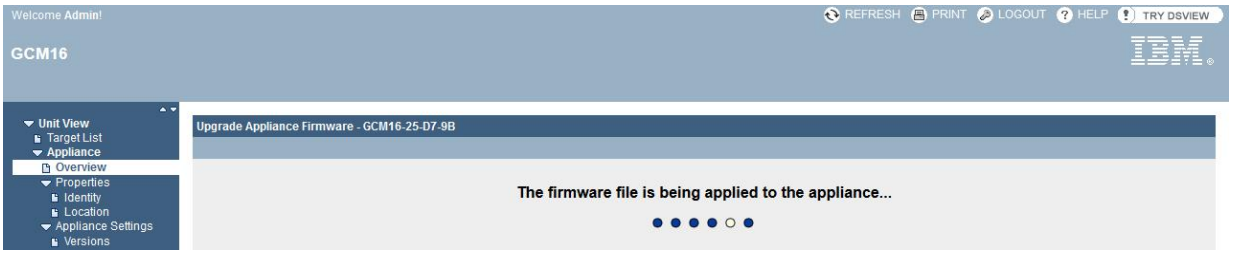
Note: If the firmware file resides in a subdirectory of the tftp server, for example in the directory */fw_files* then precede the firmware file with the fully qualified path and firmware file name, e.g.

/fw_files/emerson_fw_gcm16_gcm32_1.30.5.24433.fl

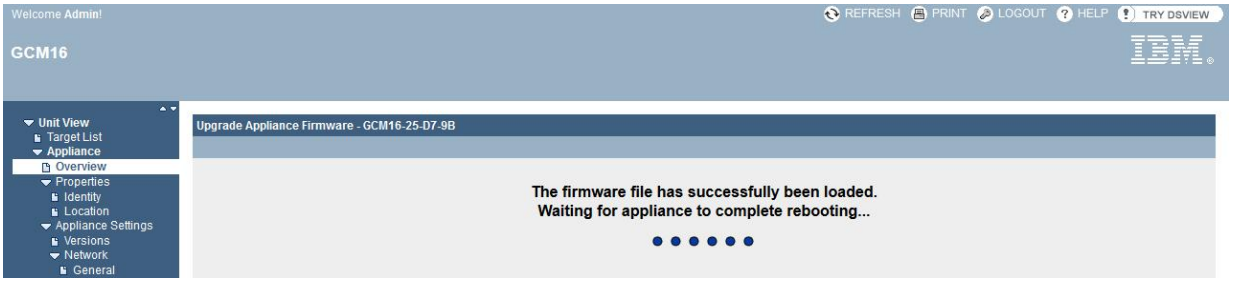
3. The firmware file will be transferred to the KVM switch



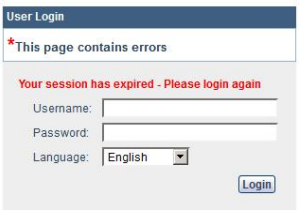
4. The firmware will be applied, that is flashed, to the KVM switch



5. Once the update has completed the KVM switch will reboot



6. After the firmware update is complete, the web browser should automatically reload to display the logon screen. If the browser does not auto-refresh then manually reload the page after a couple of minutes in order to display the logon screen

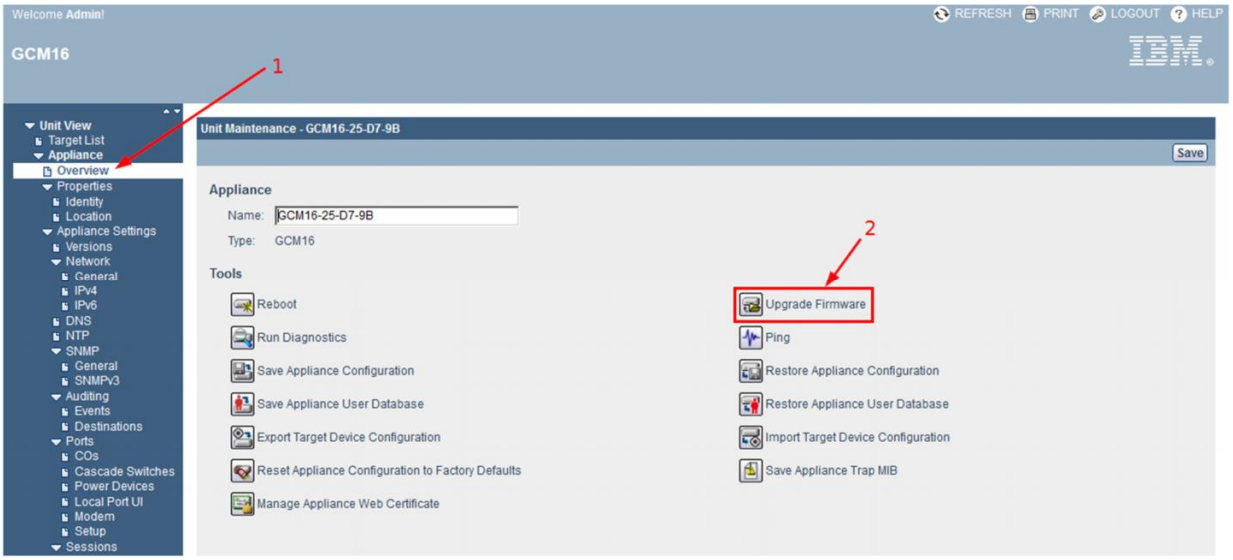


KVM firmware update via ftp

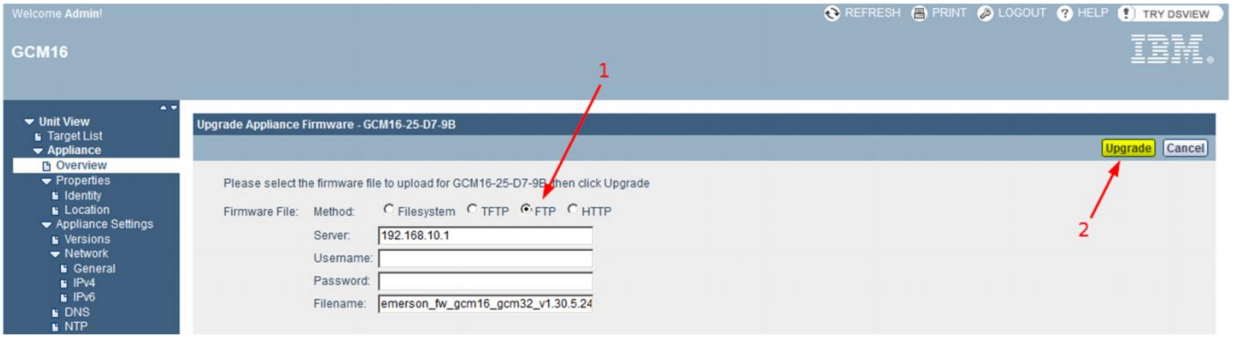
Notes:

- Before following the instructions of this chapter review Chapter 1 Introduction and the section Default log on credentials in Chapter 2
- The KVM switch does not support the ftps or sftp protocols for firmware updates
- The firmware file name in this chapter are used for illustration purposes only. The actual firmware file name may be different

1. On the main menu on the left side click on “Overview” and then on the icon “Upgrade Firmware”



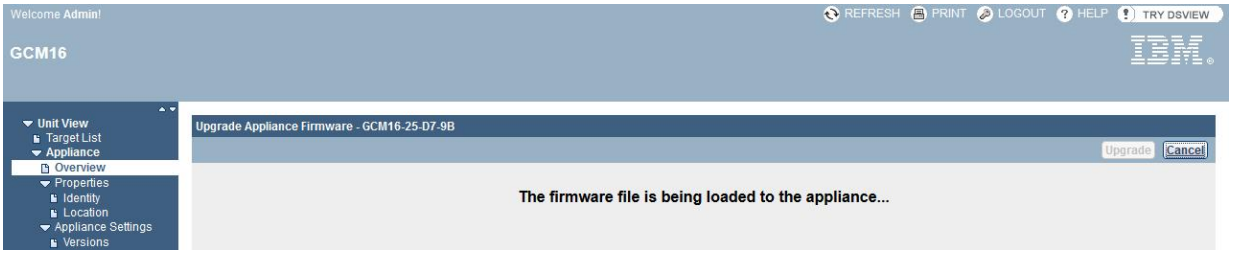
2. Click on the radio button left of “FTP” **1**, enter the IP address of the ftp server, and if required also the log on credentials for the ftp server. Click on the “Upgrade” **2** button in order to initiate the firmware update



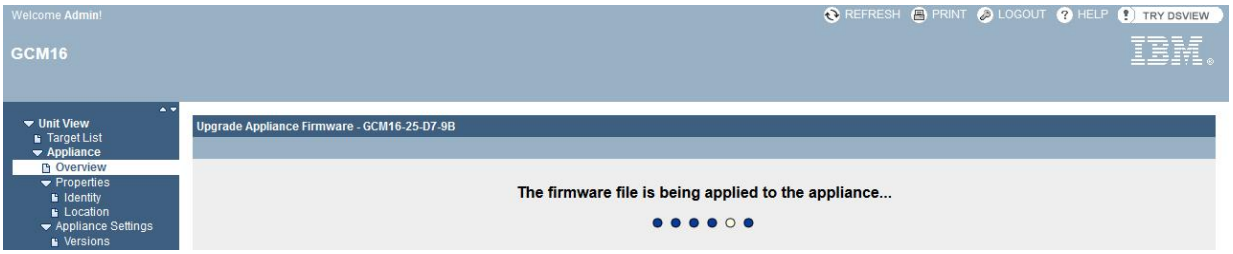
Note: If the firmware file resides in a subdirectory of the ftp server, for example in the directory */fw_files* then precede the firmware file with the fully qualified path and firmware file name, e.g.

/fw_files/emerson_fw_lcm8_16_1.2.46.0.fl

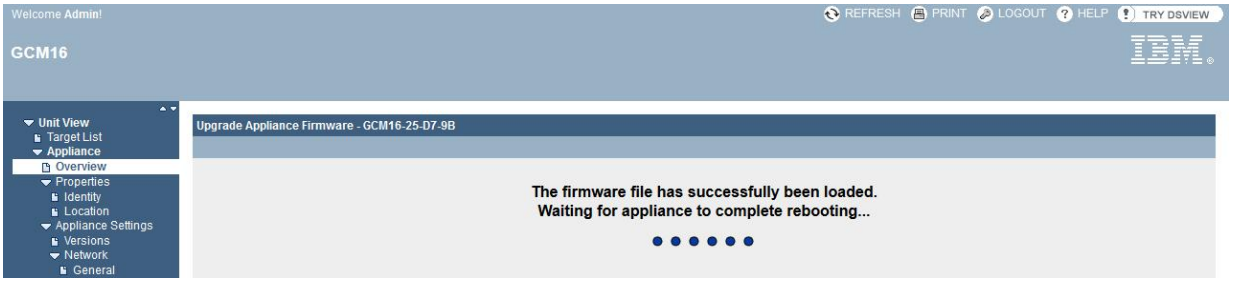
3. The firmware file will be transferred to the KVM switch



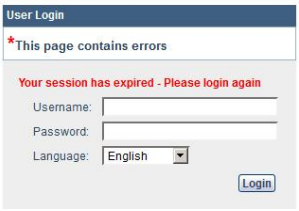
4. The firmware will be applied, that is flashed, to the KVM switch



5. Once the update has completed the KVM switch will reboot



6. After the firmware update is complete, the web browser should automatically reload to display the logon screen. If the browser does not auto-refresh then manually reload the page after a couple of minutes in order to display the logon screen

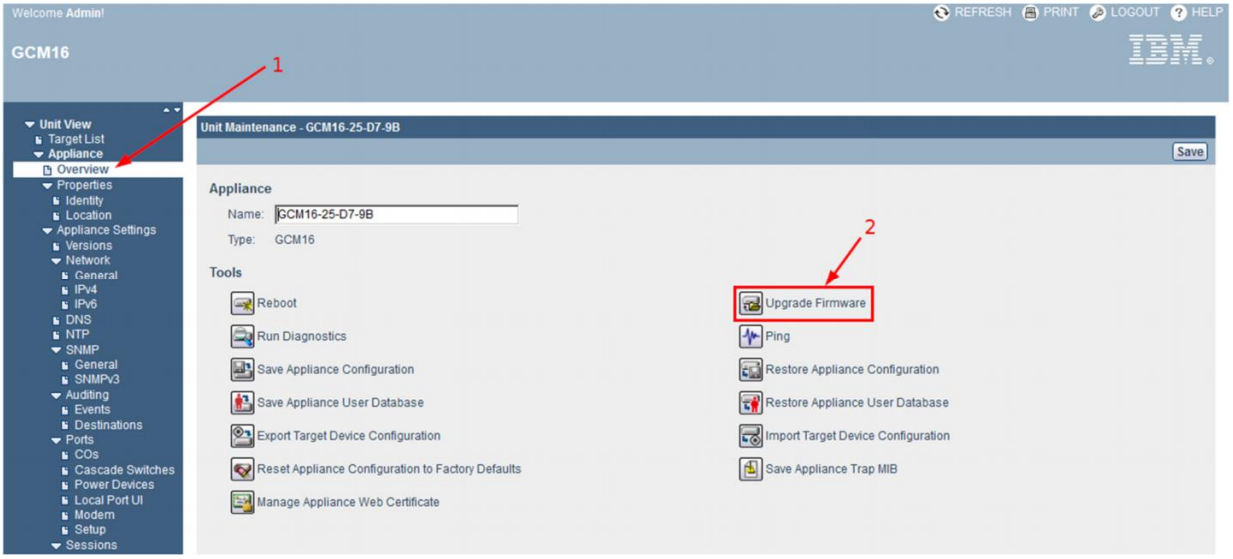


Firmware update via http

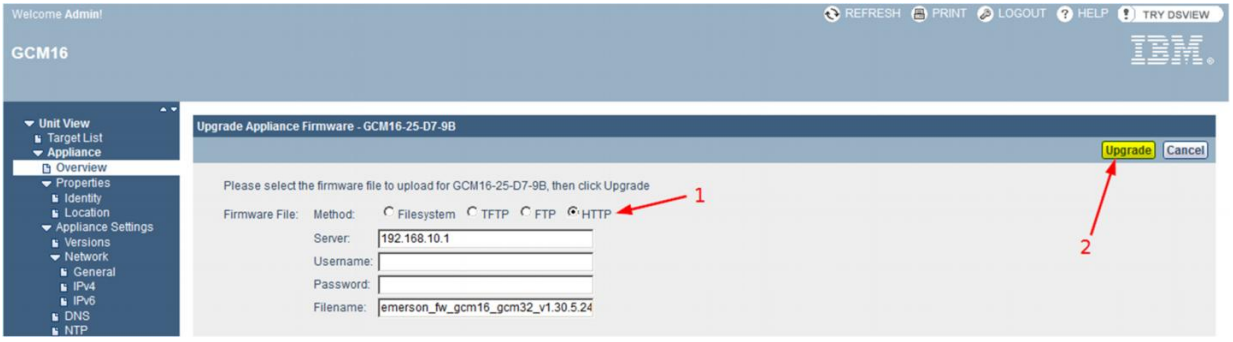
Notes:

- Before following the instructions of this chapter review Chapter 1 Introduction and the section Default log on credentials in Chapter 2
- The KVM switch does not support the https protocol for firmware updates
- The firmware file name in this chapter are used for illustration purposes only. The actual firmware file name may be different

1. On the main menu on the left side click on “Overview” and then on the icon “Upgrade Firmware”



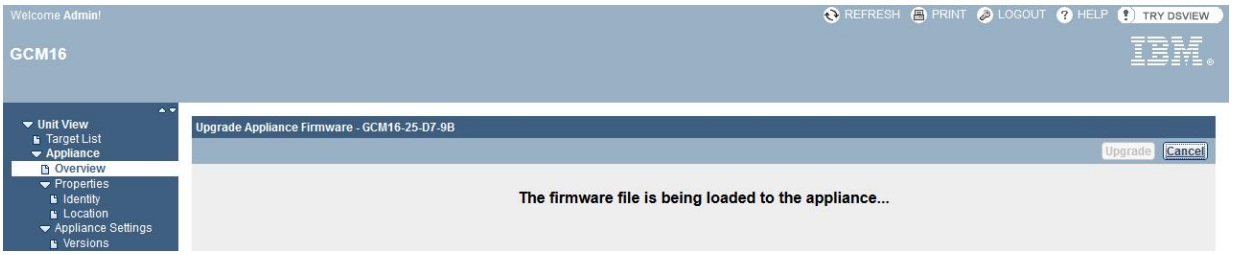
2. Click on the radio button left of “HTTP” **1**, enter the IP address of the http server, and if required also the log on credentials for the http server. Click on the “Upgrade” **2** button in order to initiate the firmware update



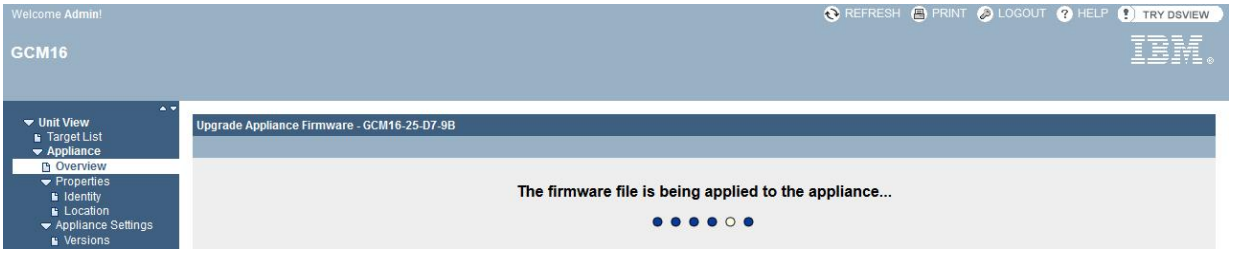
Note: If the firmware file resides in a subdirectory of the http server, for example in the directory */fw_files* then precede the firmware file with the fully qualified path and firmware file name, e.g.

/fw_files/emerson_fw_lcm8_16_1.2.46.0.fl

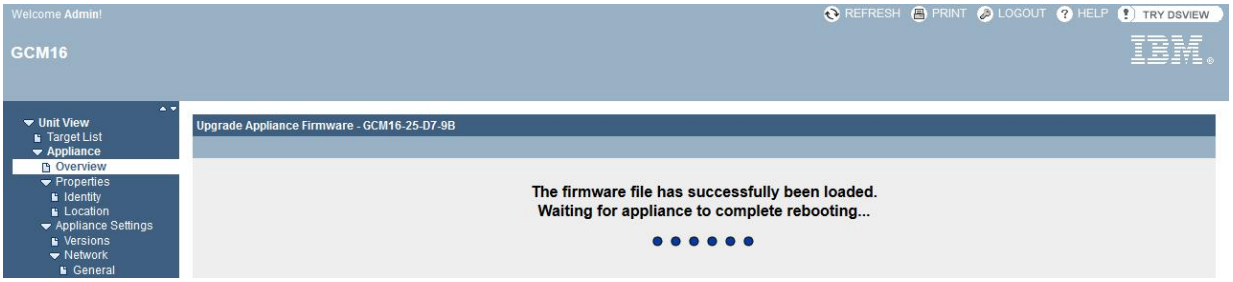
3. The firmware file will be transferred to the KVM switch



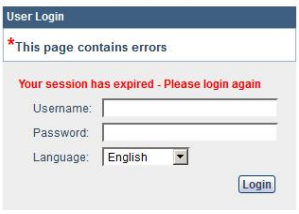
4. The firmware will be applied, that is flashed, to the KVM switch



5. Once the update has completed the KVM switch will reboot



6. After the firmware update is complete, the web browser should automatically reload to display the logon screen. If the browser does not auto-refresh then manually reload the page after a couple of minutes in order to display the logon screen



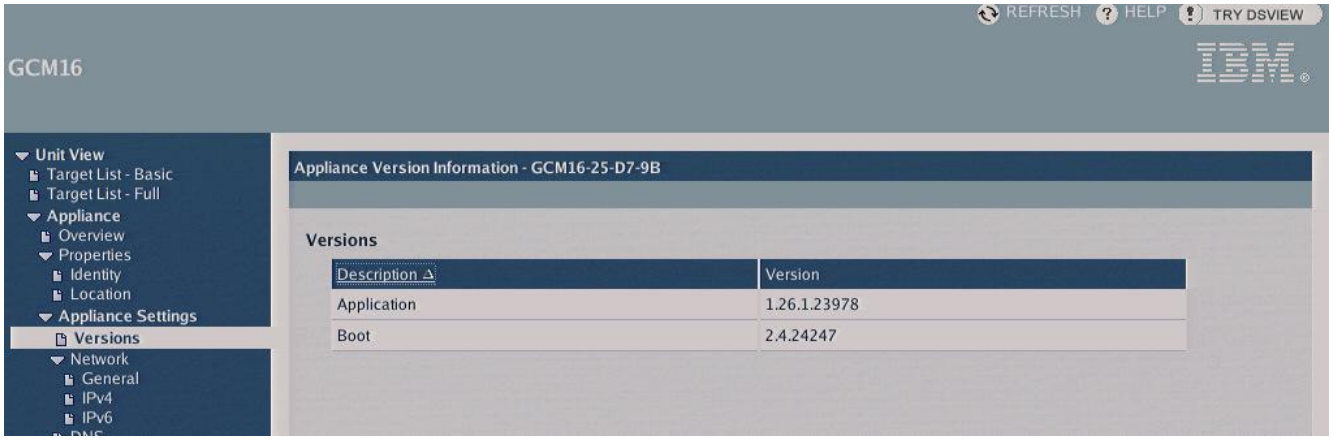
Chapter 3 Firmware update via local OWBI

Before following the instructions of this chapter review Chapter 1 Introduction.

The local On-board Web Interface (OWBI) is displayed e.g. after powering up the KVM switch. Its structure is similar to the remote On-board Web Interface (OWBI).

Checking current KVM firmware

Checking the current KVM firmware can be done by clicking in the main menu under “Appliance” on “Versions”.

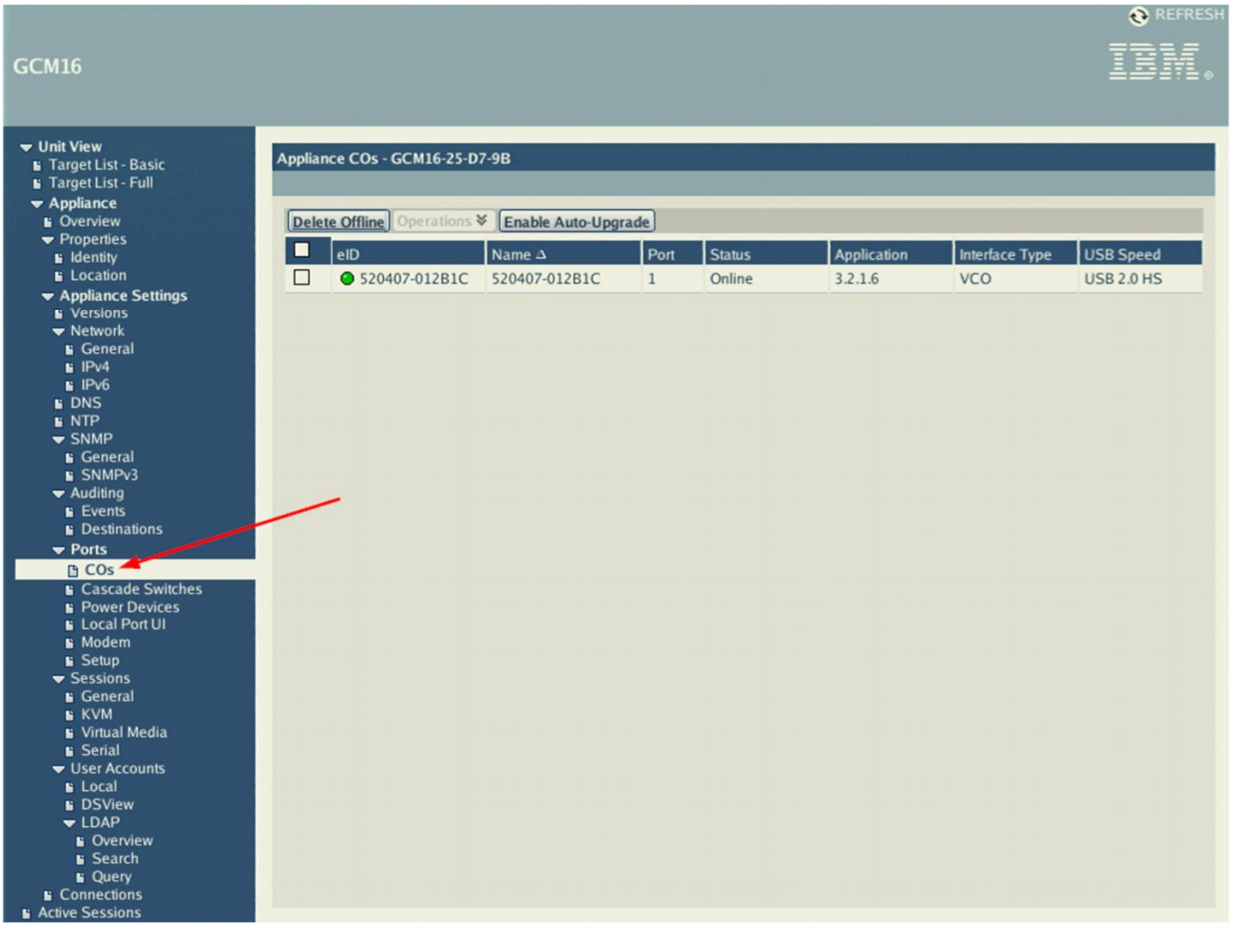


Auto-updating attached Cable Options

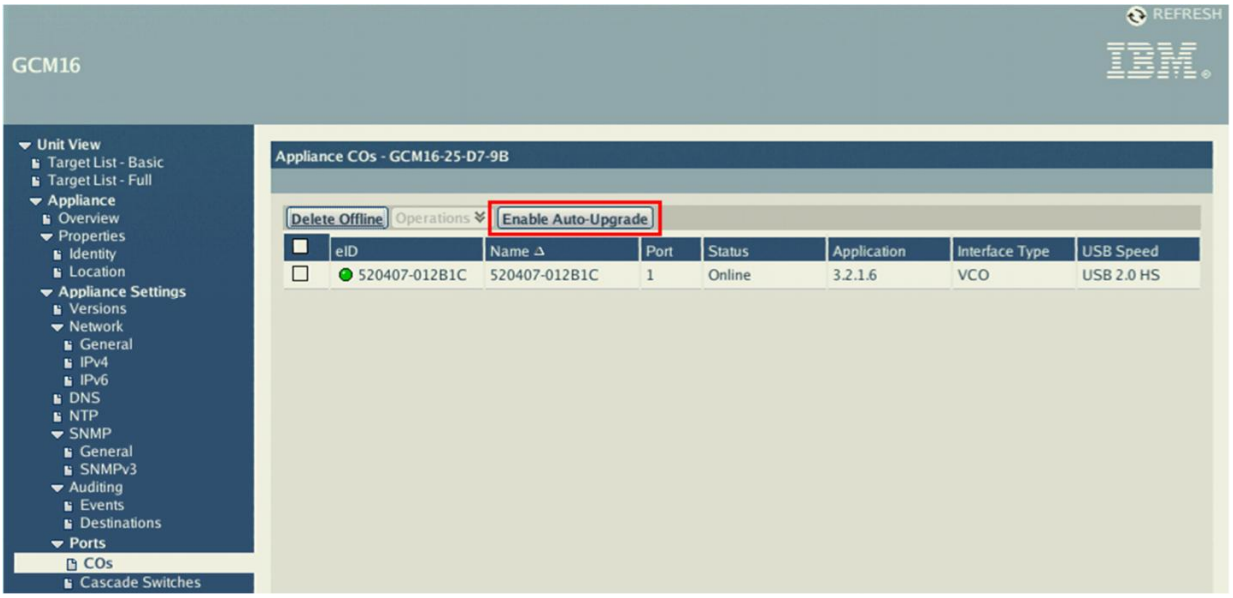
It is strongly recommended to ensure that any Cable Option (CO) gets updated when applying the firmware to the KVM switch. The auto-upgrade function guarantees that the CO firmware is compatible with the switch firmware. As COs come online, their firmware is automatically upgraded to that available on the switch.

Enabling CO auto-updating

1. On the main menu click on “COs” under “Target List”



2. Click on “Enable Auto-Upgrade”



and confirm the selection by clicking on “Yes” in the pop up window

3. CO Auto-upgrade is now enabled

Firmware update with USB memory key

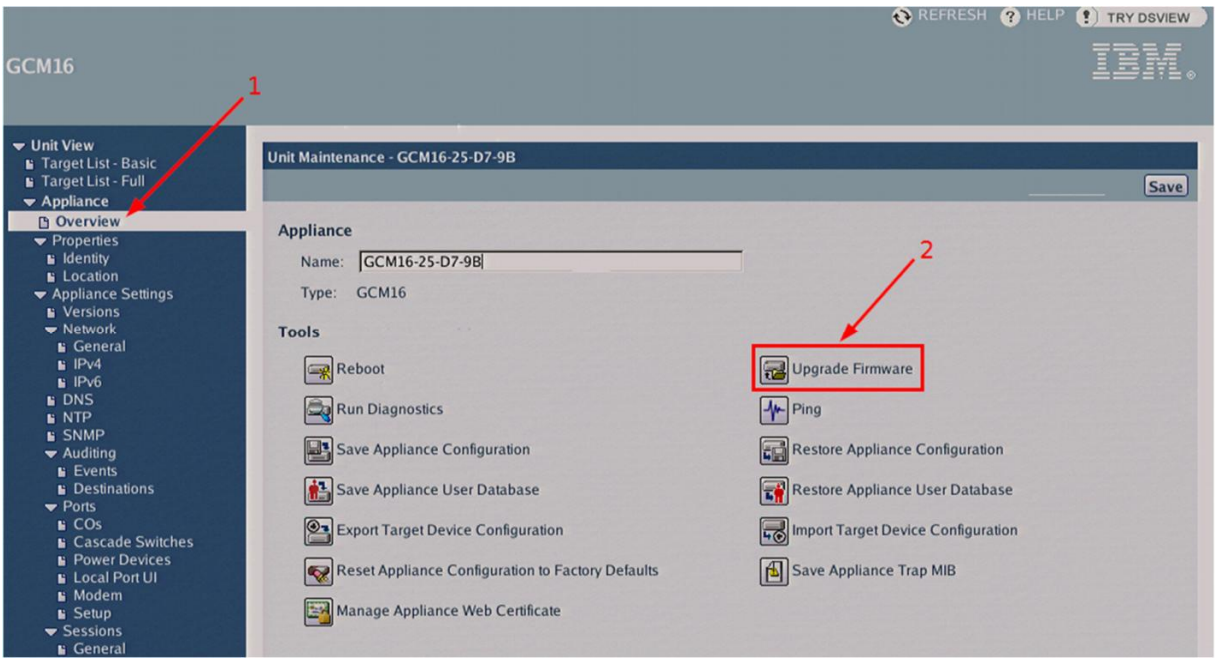
Prerequisites

The USB memory key / USB pen drive / USB flash drive must have a standard USB-A plug in order to update the KVM firmware.

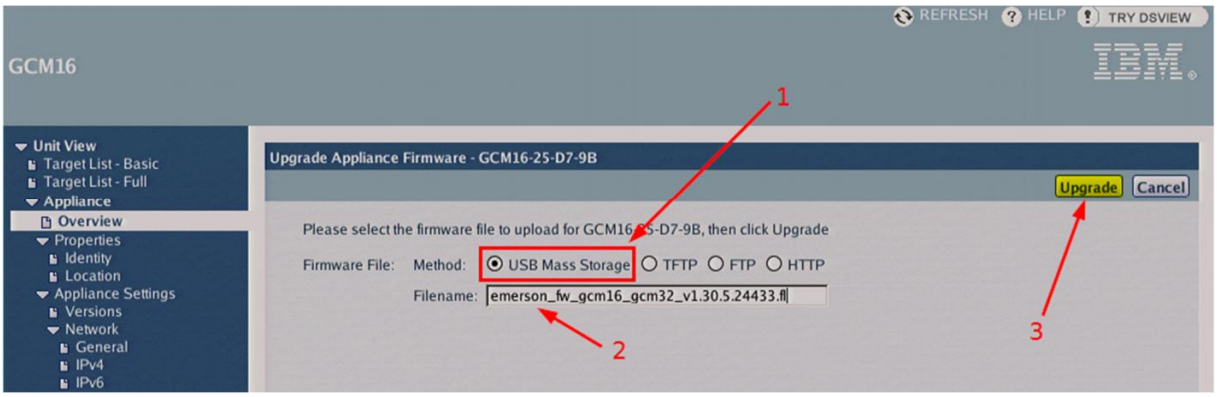
The USB memory key must be FAT32 formatted as else the KVM will not recognise any files on the USB memory key.

Update procedure

1. On the main menu on the left side click on “Overview” **1**, in the “Unit Maintenance” window click on the icon “Upgrade Firmware” **2**



2. In the window “Upgrade Appliance Firmware” click the radio button left to “USB Mass Storage” **1**, then enter in the “Filename” field the name of the firmware file **2** and then click on the “Upgrade” button **3**

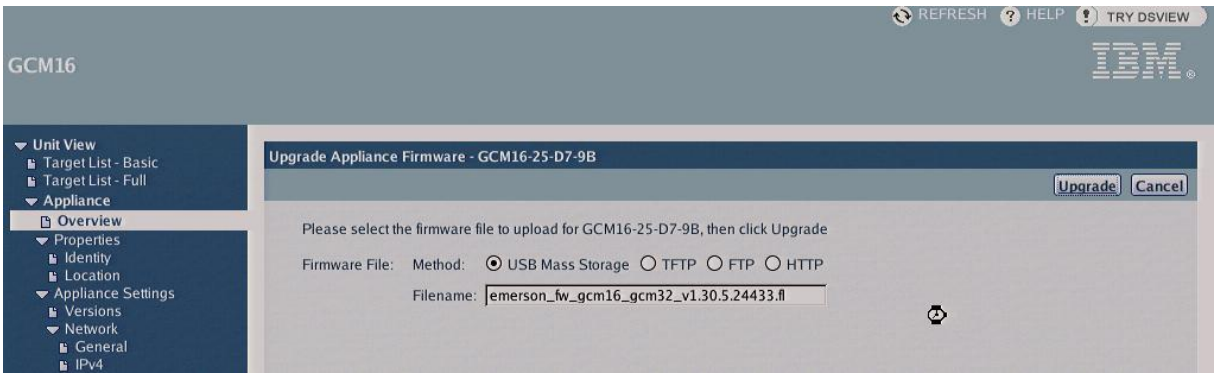


Note: If the firmware file resides in a subdirectory of the USB memory key, for example in the directory */fw_files* then precede the firmware file with the fully qualified path and firmware file name, e.g.

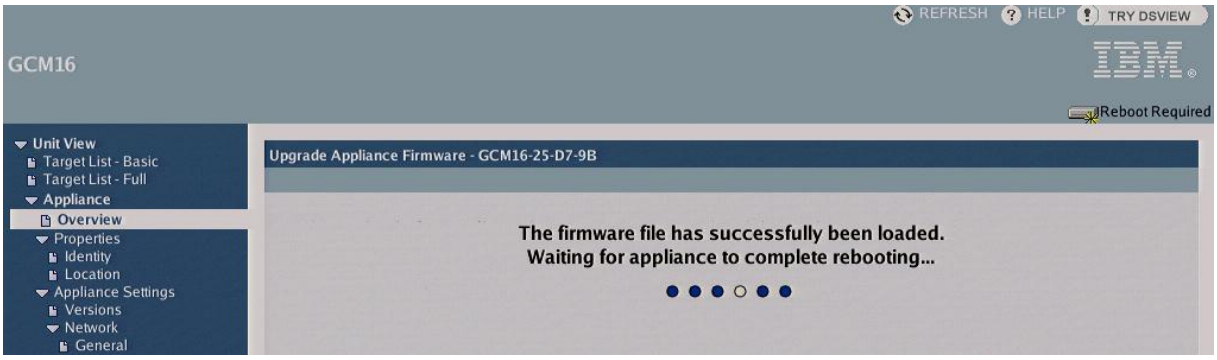
/fw_files/emerson_fw_lcm8_16_1.2.46.0.fl

In the above image the firmware file resides in the root directory of the USB memory key.

3. During the firmware upgrade of the KVM switch a watch symbol is displayed



4. At the end of the firmware update the KVM switch will reboot



Other methods to update the KVM firmware

Other methods to update the KVM firmware are described in the relevant sections of Chapter 2 Firmware update via remote OWBI. The procedure and the menu of the remote OWBI is similar to the local OWBI. The following additional methods are available:

Firmware update via TFTP.....8
KVM firmware update via ftp 11
Firmware update via http 14

Please also review Chapter 1 Introduction for additional information prior to updating the KVM firmware.

Chapter 4 Added Functions

This chapter discusses added features in the firmware which are not to be found in the relevant KVM User's Guide.

Blocking and unblocking TCP port 3871

Introduction

The firmware releases for the IBM Global Console Managers contain security fixes for any IP related security problems which are recorded in CVEs. The TCP port 3871 is used by the Avocent DS View Port to communicate with the IBM Global Console Managers. This requires that TCP port 3871 is open on the KVM switch. The Avocent DS View application secures any communication between the software and the KVM switch. Per default TCP port 3871 is open on the KVM switch.

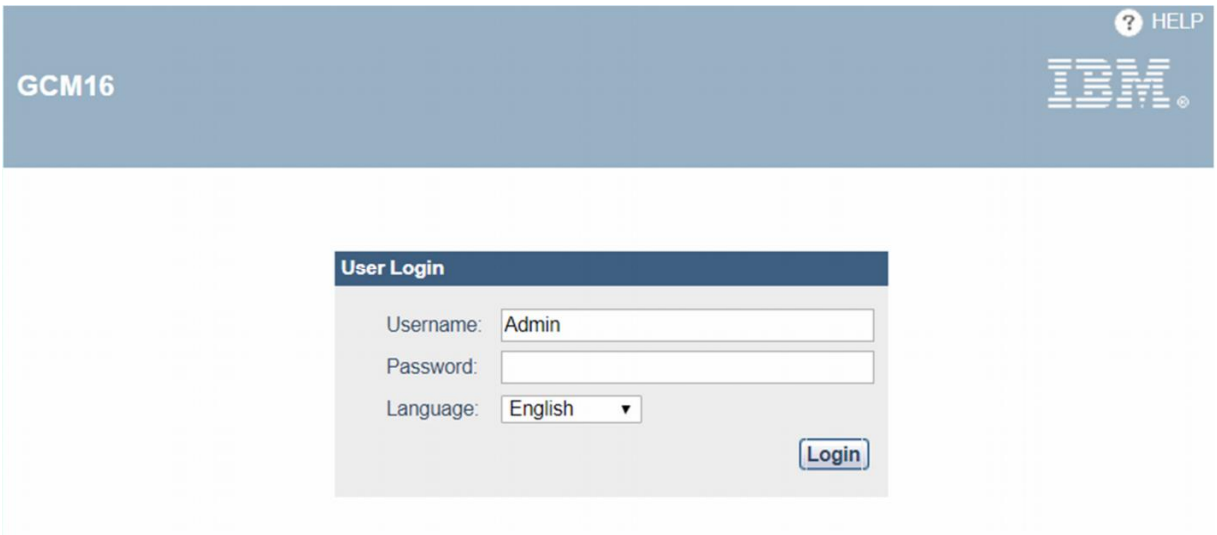
Users may find that when the Avocent DS View application is not in use that the KVM switch appears to be vulnerable to CVEs which are resolved according to the KVM switch firmware change log file. In order to eliminate these vulnerabilities it is possible to disable TCP port 3871. This requires that the KVM switch is at least at Application firmware v2.4.0.25463.

Disabling TCP port 3871

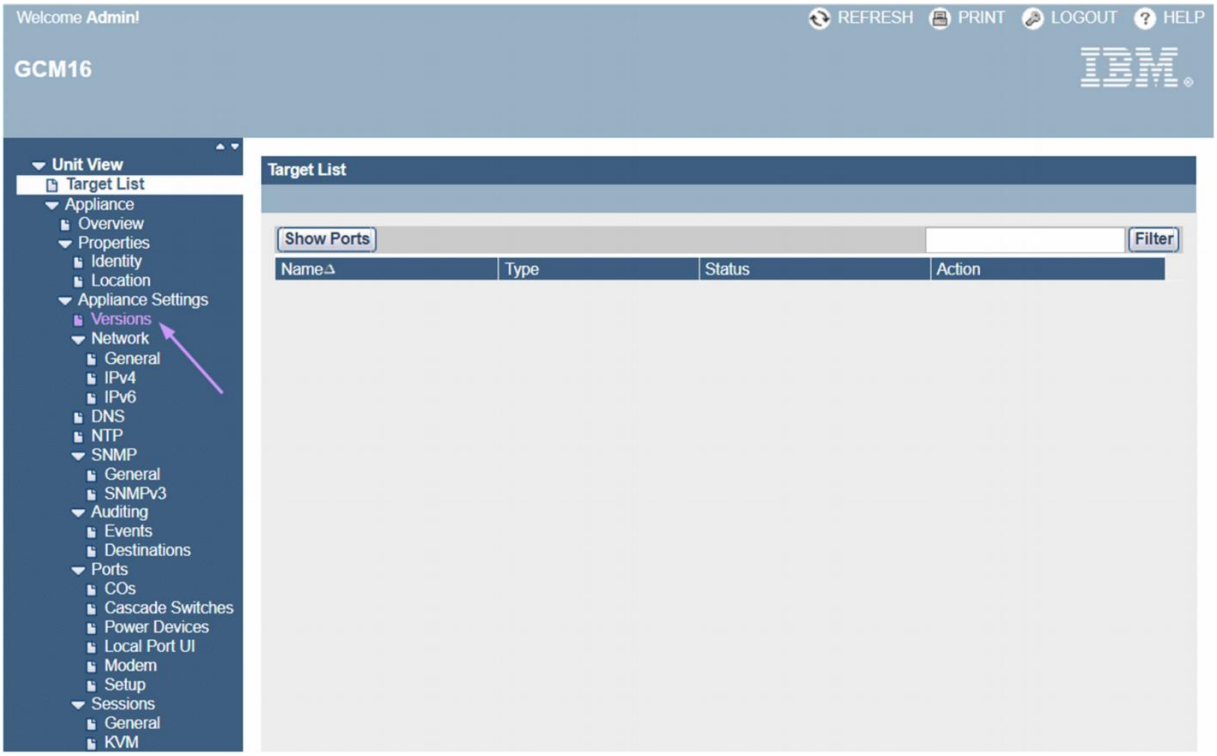
Notes:

- The procedure is identical for both via local On-board Web Interface (OWBI) and remote OWBI
- In order to complete this task the users must be logged on to the unit as Administrator
- Before following the instructions of this chapter review Chapter 1 Introduction and the section Default log on credentials in Chapter 2

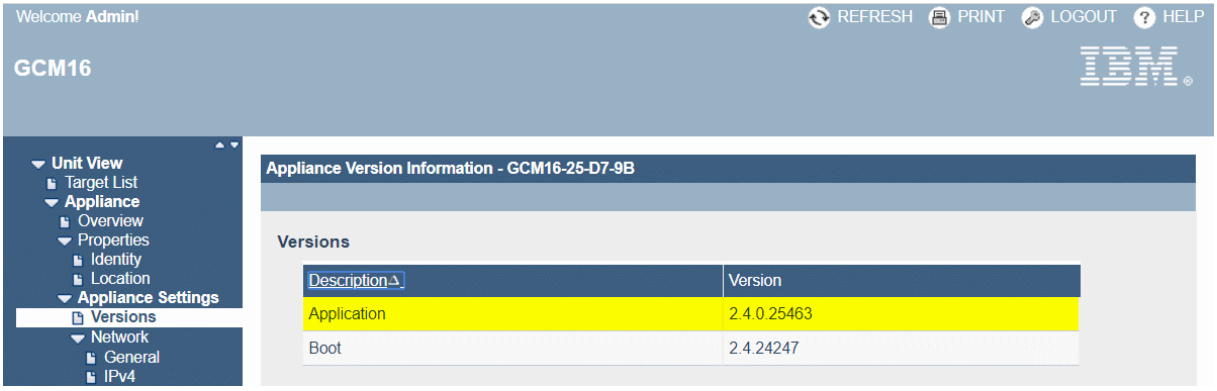
1. Log on the KVM switch with administrative privileges



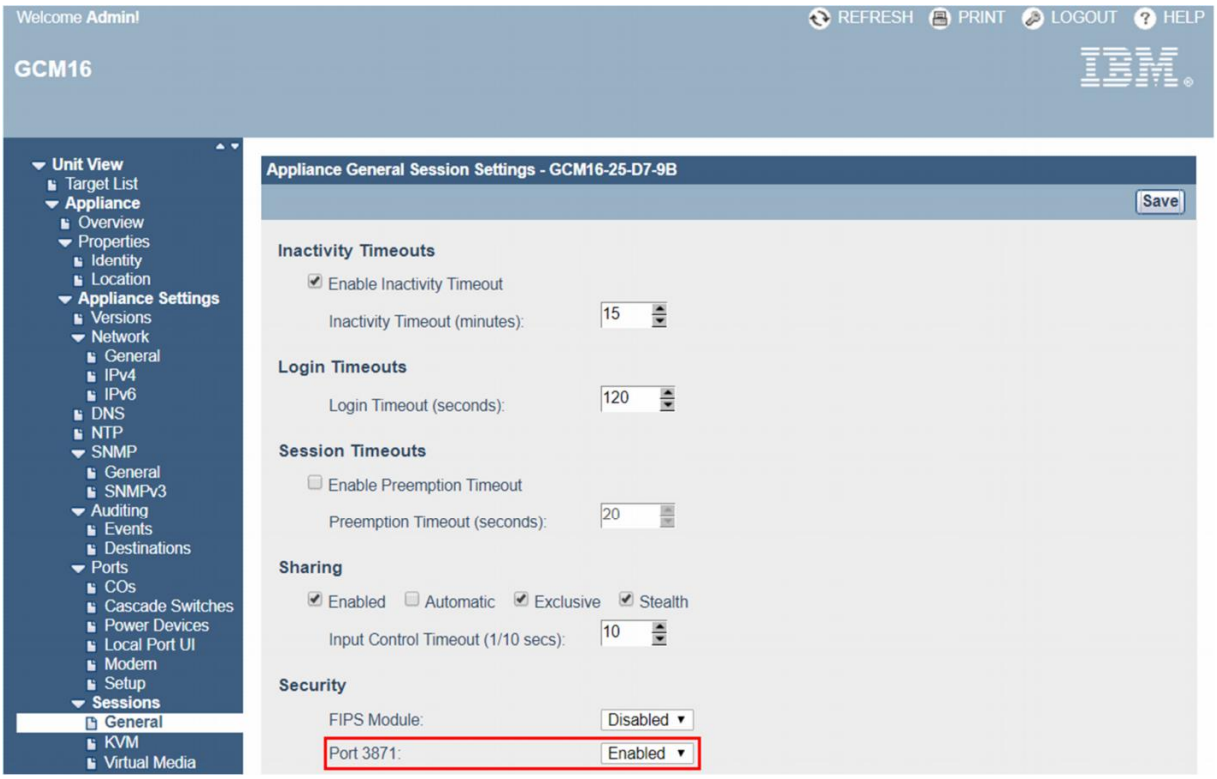
2. Once logged into the KVM switch, click on "Versions"



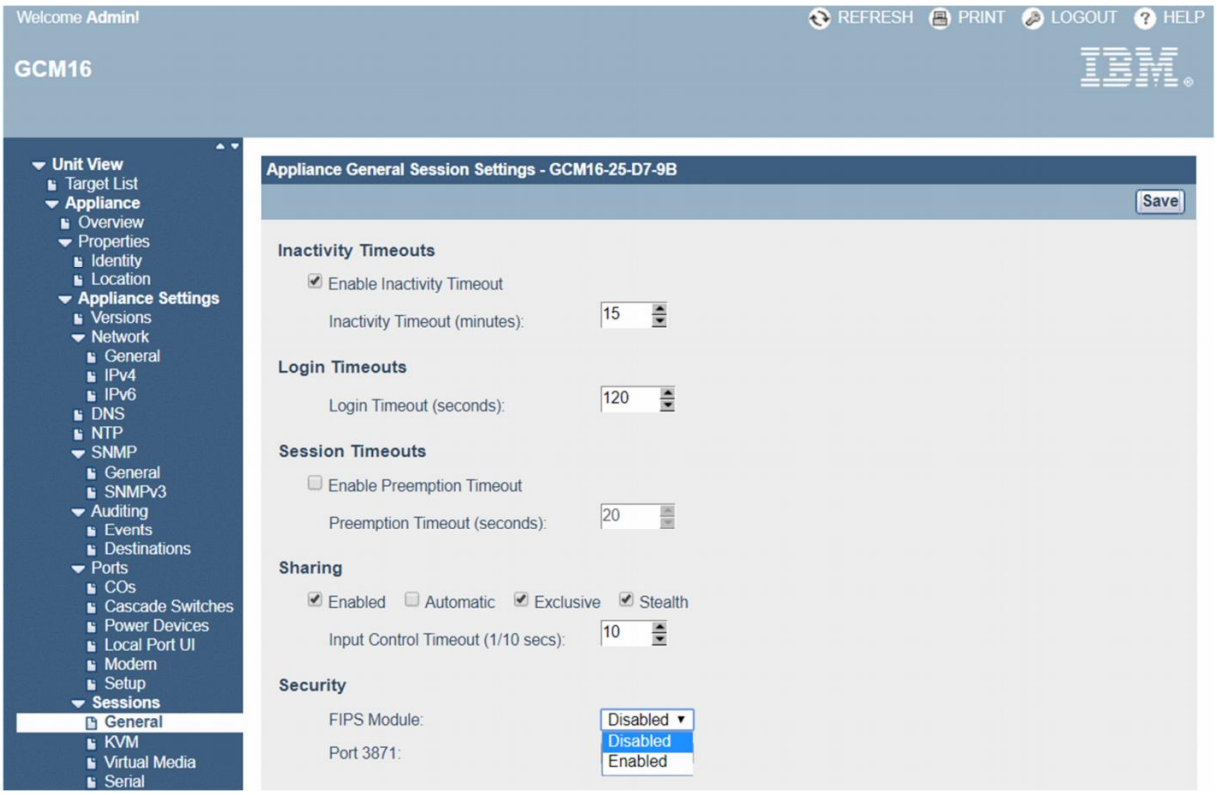
3. Confirm that the KVM switch is at least on Application firmware v2.4.0.25463



4. Click on "General". Under "Security"select the arrow down in the box right to "TCP Port 3871"



5. Change the settings as desired



Appendix A. Disclaimer

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.

Lenovo cannot accept any liability for any kind for damages caused by following the instructions provided in this document.

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.

Appendix B. Notices

Important

The information in this document should be used as a guide only, since hardware and software levels and releases may vary, and numerous hardware and software combinations are possible. Lenovo makes no representation or guarantee regarding the functionality of specific hardware or software products.

This does not imply that the network operating system will work under all combinations of hardware and software.

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.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

Customer responsibilities for code installation

The customer is responsible for installation of code.

"Code" can refer to firmware, uEFI, IMM, BIOS, device drivers, utility programs and diagnostics.

Customer responsibilities

You are responsible for downloading or obtaining from Lenovo or IBM, and installing designated Machine Code (microcode, uEFI, IMM, basic input/output system code (called "BIOS"), utility programs, device drivers, and diagnostics delivered with a Lenovo or IBM machine) and other software updates in a timely manner from a Lenovo or IBM Internet Web site or from other electronic media, and following the instructions that Lenovo or IBM provides. You may request Lenovo or IBM to install Machine Code changes; however, you may be charged for that service.

Lenovo and / or IBM may release changes to the Machine Code. The Machine Code changes are available for download by selecting your product from either a Lenovo support web site or from IBM FixCentral.

You may also obtain updated code by contacting your Lenovo or IBM representative.

If the machine does not function as warranted and your problem can be resolved through your application of downloadable Machine Code, you are responsible for downloading and installing these designated Machine Code changes as Lenovo or IBM specifies. If you would prefer, you may request Lenovo or IBM to install the downloadable Machine Code changes; however, you may be charged for that service.

For further information see also these support documents:

- Before you call Lenovo Service
- Lenovo Warranty Policies

Lenovo Data Center (DCG) Server support phone numbers are listed at

https://datacentersupport.lenovo.com/supportphonelist

Trademarks

Lenovo, the Lenovo logo, and "For Those Who Do" are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. These and other Lenovo trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by Lenovo at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. 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:

BladeCenter®	Lenovo®	System x®
Flex System™	Lenovo(logo)®	ThinkSystem

The following terms are trademarks of other companies:

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

Printing this document

This document has been created in the paper format DIN A4. The paper size is normed by the Deutsche Institut für Normung e. V. in norm DIN 476 and in International Standard ISO 216.

The below illustration shows the difference of a DIN A4 sheet versus a US Letter sheet and the associated sizes in millimetres and inches.

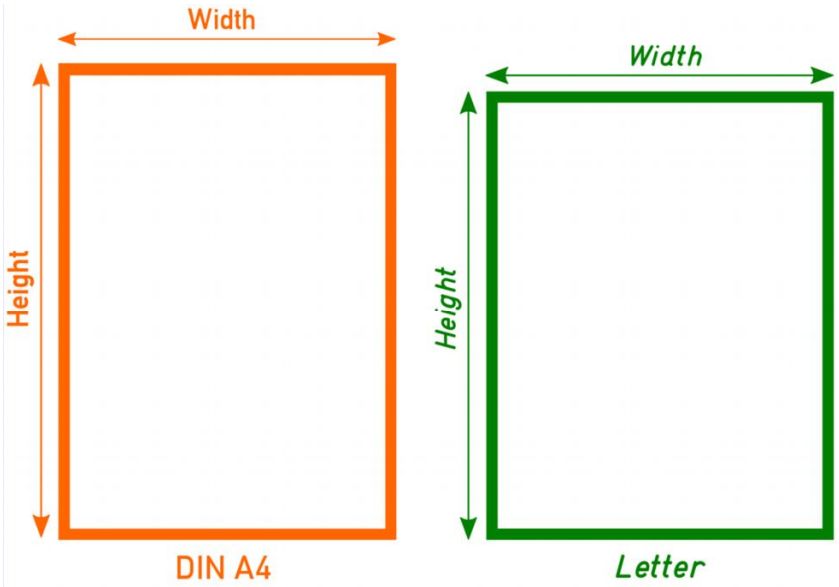


Illustration: Din A4 paper versus Letter paper

Paper Format	Width	Height	Width	Height
DIN A4	210 mm	297 mm	8.268 in	11.693 in
US Letter	215.9 mm	279.4 mm	8.5 in	11 in

Values with decimals are approximate values

When printing this document it may be necessary to scale the output to fit the printer margins.

Fonts used in this document

This document has been written using various Open Source or free fonts.

The fonts for this document were chosen in order to allow anybody to read this document as easy as possible. The following people have helped:

Sharon Duncan Dyslexia Scotland http://www.dyslexiascotland.org.uk/	Helped with chosing the right standard fonts and providing additional helpful information on the subject matter.
Joanne Marttila Pierson, Ph.D., CCC-SLP Project Manager, DyslexiaHelp http://www.dyslexiahelp.umich.edu/	Helped with providing information which mono-spaced font can be used in documents

The author of this document is very grateful for the help received.