Draco vario Secure Remote Access Gateway CON Module

Series R488

Document R488_en
Edition: 2022-03-24

Introduction

This manual contains important safety instructions as well as instructions for setting up the product and operating it. Please read the general safety instructions (see chapter 1.3, page 11) and additional notice in the respective chapters. Read carefully through the User Manual before you switch on the product.

Product Identification

The model and serial number of your products are indicated on the bottom of our products. Always refer to this information when you need to contact your dealer or the support of IHSE GmbH (see chapter 18, page 185).

Trademarks and Trade Names

All trademark and trade names mentioned in this document are acknowledged to be the property of their respective owners.

Validity of this Manual

This manual applies to all products of the series named on the cover page. Differences between the various models are clearly described.

The manufacturer reserves the right to change specifications, functions or circuitry of the series described here without notice. Information in this manual can be changed, expanded, or deleted without notice. You can find the current version of the manual in the download area of our website.

Copyright

Available Documentation

Name	Format	Description	Provision
User Manual	PDF	Provides an overview of the product together with technical data and safety instructions. Contains all instructions required to operate the product to a basic level.	Download from website
Quick Setup	Print	Provides a quick installation guide and safety instructions.	Contained in the scope of delivery

Contact

IHSE GmbH

Benzstraße 1

88094 Oberteuringen

Germany

phone: +49 7546-9248-0

fax: +49 7546-9248-48

e-mail: info@ihse.com

website: https://www.ihse.com

Table of Contents

1 Important Information

1.1 Symbols for Warnings and Helpful Information

The meaning of the symbols used for warnings and helpful information in this manual is described below:

NOTICE
NOTICE identifies information, if not observed, endangers the functionality of your device or the security of your data.

This symbol indicates information about special features on the device or when using device and function variants.

This symbol indicates instructions for procedures recommended by the manufacturer for an effective utilization of the device potential.

1.2 Spellings

Uniform spellings are used in this manual for better readability or easier assignment.

The following spellings are used for products:

Product	Description
SIRA CON	Draco vario Secure Remote Access Gateway CON Module IP Encoder for remote access via TCP/IP and with built-in HDMI CON Cat X/ fiber connection to CPU Unit or matrix and with local feed-through for connecting a HDMI monitor, keyboard, and mouse.
SIRA Stand-alone	Draco vario Secure Remote Access Gateway Stand-alone Module HDMI IP Encoder for remote access via TCP/IP and with HDMI and USB input for direct connection to video/USB sources, with local feed-through port for connecting HDMI monitor, keyboard, and mouse.
SIRA Module	For descriptions managing both the SIRA CON and the SIRA Stand-alone.
SIRA Client	Client software accessible via browser and IP address to connect to a target.
Client Hot Key	Hot Key to manage functions within the Client software.
Target	Source with CPU Unit directly or via matrix connected to a SIRA CON, or a local source directly connected to the SIRA Stand-alone.
Source	Computer, graphics card (USB, video, audio, data).
Sink	Console (monitor, keyboard, mouse, video, audio, data).
CPU Unit	Encoder to connect to the source.
CON Unit	Decoder to connect at the peripherals.

The following spellings are used for keyboard commands:

Keyboard command	Description
key	Key on the keyboard
key + key	Press keys simultaneously
key, key	Press keys successively
2x key	Press key quickly, twice in a row (like a mouse double-click)

The following spellings are used for software descriptions:

Spelling	Description
Bold print	Description of terms that are used in the management software, e.g., menus and buttons
Bold print > Bold print	Management software: selection of a menu item in the menu bar or the toolbar, e.g., **Extras > Options**

Mouse button	Description
Left mouse button	Primary mouse button* (default in most operating systems)
Right mouse button	Secondary mouse button*
* Unless you have customized your mouse settings in the used operating system.	
Descriptions containing "click", "mouse click" or "double-click" each means a click with the primary (left) mouse button. If the right mouse button has to be used, this is explicitly declared in the description.	

1.3 EU Declaration of Conformity

Please find the EU Declaration of Conformity for the device under:
www.ihse.com/eu-declaration-of-conformity

A copy of the original, product-specific EU Declaration of Conformity can be provided upon request. For contact details, see page 2 of this manual.

2 Safety instructions

To ensure reliable and safe long-term operation of your device, please note the following guidelines:

- ➡ Read this user manual carefully.
- ➡ Only use the device according to this user manual. Failure to follow the instructions described can damage the device or endanger the security of your data.
- ➡ Take any required ESD precautions.

⚠ WARNING

Risk of electric shock due to freely accessible power connections when the chassis is open

Risk of bruising, abrasion or shearing of fingertips due to rotating fan when the chassis is open

If the chassis is opened while power is supplied to the device, electric shock may occur if the internal wiring is touched. If a running fan is touched while the case is open, bruises, abrasions or shearing of fingertips may occur.

There are no necessary maintenance procedures that require opening the chassis.

- ➡ Do NOT remove the cover of the chassis.
- ➡ Do NOT install the device in environments where children are likely to be present.

⚠ CAUTION

Risk of burns due to tremendously heated chassis surface after a long period of operation

When the chassis is fully equipped, the surface of the chassis can become very warm after a long period of operation. If the chassis surface is touched after a long period of operation, this can cause skin burns.

- ➡ Protective gloves must be worn to transport a fully equipped chassis after a long period of operation.
- ➡ Ensure that there is sufficient distance from the operator, e.g., for mounting under a table.
- ➡ Do NOT install the device in environments where children are likely to be present.

Installation Location

While operating the device and the power supply units can get warm. Damage to the device can occur in a damp environment.

- ➡ Use the device only in dry, indoor environments.
- ➡ Use the device only in a room with adequate ventilation.
- ➡ For rack-mount installations, at least 0.5 RU (rack unit) is required above the device for ventilation.
- ➡ Do not place the power supply units directly on top of the device.
- ➡ Existing ventilation openings on the device must always be free.
- ➡ If installing the device under the table, place the device at a sufficient distance from the operator.
- ➡ Place all power sockets including the sockets for the supplied external power supply units easily accessible and directly next to each other.

Connection

- ➡ Check the device and the power supply units for visible damage before connecting it.
- ➡ Only connect the device if the device and the ports are not damaged.
- ➡ Only use power supply units originally supplied with the product or manufacturer-approved replacements.
- ➡ Only use power supply units without any visible damage at the chassis or the cable.
- ➡ Connect all power supply units to grounded outlets.
- ➡ Ensure that the ground connection is maintained from the outlet socket through to the power supply unit's AC power input.
- ➡ Only connect the device to KVM devices using the interconnecting cable - not to other devices, particularly not to telecommunications or network devices.

Disconnect the Device from the Circuit

NOTICE
The cable plugs on the device side can contain a lock. In the event of a necessary quick and complete disconnection from external electric circuits: ➡ Remove all corresponding cable plugs from the socket, ➡ Or set the power switch of the power outlets (if available) to the “Off” position.

3 Consignes de Sécurité

Pour garantir un fonctionnement fiable et sûr de votre périphérique à long terme, veuillez respecter les directives suivantes :

- Lisez attentivement ce manuel d'utilisation.
- N'utilisez le périphérique que conformément à ce manuel d'utilisation. Le non-respect des instructions décrites peut endommager le périphérique ou mettre en danger la sécurité de vos données
- Prenez toutes les précautions nécessaires contre les décharges électrostatiques.

⚠ AVERTISSEMENT

Risque de choc électrique dues de l'accès libre aux connexions électriques lorsque le châssis est ouvert
Risque de contusion, d'abrasion ou de cisaillement des bouts des doigts dues de la rotation du ventilateur lorsque le châssis est ouvert

Si le châssis est ouvert alors que le périphérique est sous tension, un choc électrique peut se produire si le câblage interne est touché.

Si vous touchez un ventilateur en marche alors que le châssis est ouvert, vous risquez de vous blesser, de vous abraser ou de vous cisailler le bout des doigts.

Aucune procédure d'entretien nécessaire ne requiert l'ouverture du châssis.

- Ne retirez PAS le couvercle du châssis.
- N'installez PAS le périphérique dans des environnements où des enfants sont susceptibles d'être présents.

⚠ ATTENTION

Risque de brûlures dues à la surface du châssis très chaude après une longue période d'utilisation

Lorsque le châssis est entièrement équipé, la surface du châssis peut devenir très chaude après une longue période de fonctionnement.

Si la surface du châssis est touchée après une longue période d'utilisation, cela peut provoquer des brûlures de la peau.

- Des gants de protection doivent être portés pour transporter un châssis entièrement équipé après une longue période d'opération.
- Veillez à ce que la distance avec l'opérateur soit suffisante, par exemple pour un montage sous une table.
- N'installez PAS le périphérique dans des environnements où des enfants sont susceptibles d'être présents.

Emplacement de l'installation

Pendant le fonctionnement, le périphérique et les unités d'alimentation peuvent chauffer. Le périphérique peut être endommagé dans un environnement humide.

- N'utilisez le périphérique que dans un environnement sec et intérieur.
- N'utilisez le périphérique dans un lieu correctement ventilée.
- Pour les installations en rack, au moins 0,5 RU (unité de rack) est nécessaire au-dessus du périphérique pour la ventilation.
- Ne placez jamais les unités d'alimentation sur le dessus du périphérique.
- Les ouvertures de ventilation existantes sur le périphérique doivent toujours être libres.
- Si vous installez le périphérique sous la table, placez le périphérique à une distance suffisante de l'opérateur.

- ➡ Placez toutes les prises de courant, y compris les prises de courant pour les unités d'alimentation externes fournis, de manière facilement accessible et directement les unes à côté des autres.

Connexion

- ➡ Avant de connecter le périphérique et les unités d'alimentation, vérifiez qu'ils ne présentent pas de dommages visibles.
- ➡ Seulement connectez le périphérique et les unités d'alimentation que si le périphérique et les ports ne sont pas endommagés.
- ➡ Utilisez uniquement les unités d'alimentation fournis à l'origine avec le produit ou des pièces de rechange approuvées par le fabricant.
- ➡ N'utilisez que des unités d'alimentation sans dommages visibles au niveau du châssis ou du câble.
- ➡ Connectez tous les unités d'alimentation à des prises de terre.
- ➡ Raccordez tous les unités d'alimentation à des prises de courant mises à la terre.
- ➡ Veillez à ce que la connexion à la terre soit maintenue depuis la prise de courant jusqu'à l'entrée d'alimentation CA du les unités d'alimentation.
- ➡ Ne connectez le périphérique qu'à des périphériques KVM à l'aide du câble d'interconnexion - pas à d'autres périphériques, en particulier pas à des périphériques de télécommunications ou de réseau.

Déconnecter le périphérique du circuit

AVIS
Les fiches de câble du côté du périphérique peuvent contenir un verrou. En cas de nécessité d'une déconnexion rapide et complète des circuits électriques externes : ➡ Retirez toutes les fiches de câble correspondantes de la prise. ➡ Ou mettez l'interrupteur des prises de courant (si elles existent) sur la position « Off ».

4 Description

4.1 Intended Use

The SIRA CON and the SIRA Stand-alone are developed and intended to be used in a Draco vario chassis to access to a target from remote locations via TCP/IP with encrypted signal transmission. The SIRA CON can access to matrix connected targets.

For information about Draco vario chassis, please refer to the 474-BODY user manual.

SIRA CONs with Cat X Interface:
SIRA CONs with Cat X connections are unsuitable for connection between buildings. Use a fiber optic-based extender module instead.

SIRA CONs with Fiber Interface:
SIRA CONs with fiber connections can also be used with applications in environments which are subject to electromagnetic interference.

NOTICE

Interferences when the immunity limit values are exceeded

If the limit values listed in EN55024 are exceeded, reliable and fault-free functioning of the devices cannot be guaranteed.

NOTICE

Radio interference in a domestic environment

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

- ➡ Follow the safety and installation instructions given in this manual.
- ➡ Use connection cables according to the specifications for the length and type given in this manual.

4.2 System Compatibility

4.2.1 Chassis Compatibility

Both the SIRA CON and the SIRA Stand-alone are developed to be used with Draco vario chassis. Please refer to the chassis user manual.

The following table lists compatibility (X) and non-compatibility (-) of SIRA modules with Draco vario chassis.

Mounting Chassis

Type	R488-BIPC	R488-BIPCR	R488-BIPS	R488-BIPSR	R488-BIPHHL
474-BODY2	-	-	-	-	X
474-BODY2R	-	-	-	-	X
474-BODY2N	-	-	-	-	X
474-BODY2DC-12 474-BODY2DC-24 474-BODY2DC-48	-	-	-	-	X
474-BODY4	-	-	-	-	X
474-BODY4R	-	-	-	-	X
474-BODY6R-R1	-	-	-	-	X
474-BODY6DC-12 474-BODY6DC-24 474-BODY6DC-48	-	-	-	-	X

Slide-in Chassis

Type	R488-BIPC	R488-BIPCR	R488-BIPS	R488-BIPSR	R488-BIPHHL
474-BODY2BPF 474-BODY2BPF-S 474-BODY2BPF-SNMP	X	X	X	X	X
474-BODY6BP 474-BODY6BP-S 474-BODY6BP-SNMP	X	X	X	X	X
474-BODY6BPF 474-BODY6BPF-S	X	X	X	X	X
474-BODY21/4U	X	X	X	X	X
474-BODY21/4UR	X	X	X	X	X

4.2.2 Video Compatibility

Extender modules are operated with a different firmware and technology and are not completely compatible with each other. The following table lists video compatibility (X) and non-video compatibility (-) (see footnotes).

		R474	R477	R481	R482		R483		R486	R488	R490	R492	R493		R495
		SH	SH	SH	SH	DH	SH	DH	DH	SH	SH	SH	SH	DH	SH
L474	SH	X	X	X	X	X	X	X	X	X	X	-	-	X	-
L477	SH	X	X	X	X	X	X	X	X	X	X	-	-	X	-
L481	SH	X	X	X	X	X	X	X	X	X	X	-	-	X	-
L482	SH	X	X	X	X	X	X	X	X	X	X	-	-	X	-
	DH	X	X	X	X	X	X	X	X	X	X	-	-	X	-
L483	SH	X	X	X	X	X	X	X	X	X	X	-	-	X	-
	DH	X	X	X	X	X	X	X	X	X	X	-	-	X	-
L484	SH	X	X	X	X	X	X	X	X	X	X	-	-	X	-
L486	DH	X	X	X	X	X	X	X	X	X	X	-	-	X	-
L488	SH	X	X	X	X	X	X	X	X	X	X			X	
L490	SH	-	-	-	-	-	-	-	-	-	X	X	X	X	X
L491	SH	-	-	-	-	-	-	-	-	-	X	X	X	X	X
L492	SH	-	-	-	-	-	-	-	-	-	X	X	X	X	X
L493	SH	-	-	-	-	-	-	-	-	-	X	X	X	X	X
	DH	-	-	-	-	-	-	-	-	-	X	X	X	X	X
L494	SH										X	X	X	X	X
L495*	SH	-	-	-	-	-	-	-	-	-	X	X	X	X	X

1) Compatibility is based on video/USB-HID signal only, not on the embedded signals like audio or USB 2.0.
2) Compatible up to the maximum specified resolution of the console.
No image is displayed when a Single Link CON Unit (e.g., R482-B2HC with 1080p monitor) is switched to a Dual Link CPU Unit (e.g., L482-BDHC with a 4k30 video signal) unless the configuration is set up accordingly.
3) Compatible up to the maximum transmission speed and interface compatibility (see chapter 17.2.1, page 177).
4) If using CPU Unit and CON Unit with different video signals (e.g., a DP 1.1 CON Unit with a HDMI CPU Unit), transmitting the EDID to the CPU Unit will result in an error.

4.2.3 Interconnection Compatibility

Extender modules are available in the following connection versions. The type of interconnection of extenders can be recognized by the article number:

- Interconnection via Cat X cable ("C")
- Interconnection (1.25 Gbit/s = "1G") via single-mode fiber cable ("S")
- High speed interconnection (3.125 Gbit/s = 3G) via single-mode fiber cable ("X")

Fiber devices can be used with Multi-mode and Single-mode cables (see chapter 17.3.2, page 181).

Point-to-point Interconnection between Extender Modules

	Cat X 1G	Fiber 1G	Fiber 3G
Cat X 1G	Compatible	Not compatible	Not compatible
Fiber 1G	Not compatible	Compatible	Not compatible
Fiber 3G	Not compatible	Not compatible	Compatible

Interconnection of Extender Modules via Matrix or Cross-Repeater 485-BX/485-BXX

	Cat X 1G	Fiber 1G	Fiber 3G
Cat X 1G	Compatible	Compatible	Not compatible
Fiber 1G	Compatible	Compatible	Not compatible
Fiber 3G	Not compatible	Not compatible	Compatible

Interconnection of Extender Modules via Draco tera Matrix with Bridge Card

	Cat X 1G CON Unit	Fiber 1G CON Unit	Fiber 3G CON Unit
Cat X 1G CPU Unit	Compatible	Compatible	Compatible
Fiber 1G CPU Unit	Compatible	Compatible	Compatible
Fiber 3G CPU Unit	Not compatible	Not compatible	Compatible

A special card (bridge card) is available to be used with the matrix Draco tera enterprise and Draco tera flex to connect up to 8 CPU Units with 1G transmission speed (Cat X or fiber version). The transmission speed will be increased within the bridge card from 1G to 3G. The signals are transmitted to the backplane of the matrix and can be output to up to 8 CON Units, connected to the matrix.

This function is only available in one direction.

1G CPU Unit - Draco tera enterprise and Draco tera flex with bridge card - 3G CON Unit

4.3 Installation Examples

SIRA CON

The next two sections illustrate typical installations of KVM extender modules together with a SIRA CON.

The CPU Unit is connected directly to the source using the supplied cables. The CON Unit is connected to the console. The CPU Unit and the CON Unit communicate with each other through the interconnect cables.

SIRA Stand-alone

The third section shows a SIRA Stand-alone installation with direct connection to the source and available access via TCP/IP.

4.3.1 Point-to-Point Installation SIRA CON

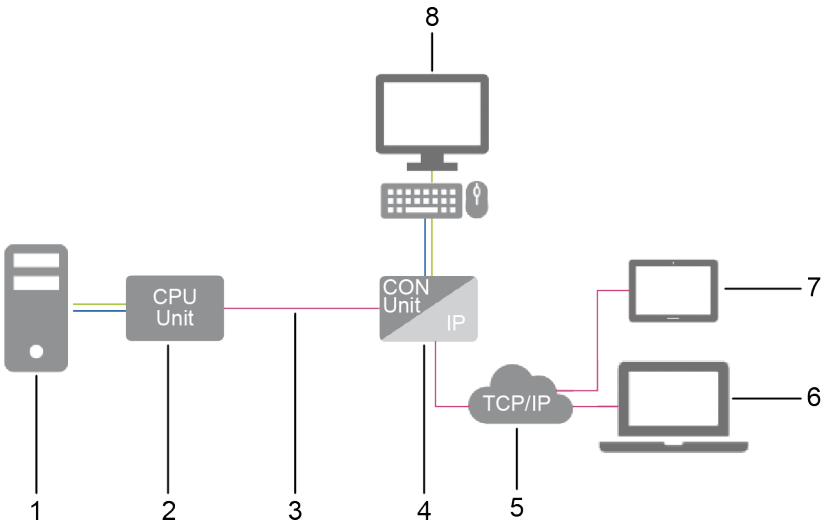


Fig. 1 Point-to-Point installation example (SIRA CON with console and remote access)

1 Source
2 CPU Unit
3 Interconnect cable
4 SIRA CON
5 TCP/IP network
6 Notebook
7 Tablet
8 Console (monitor, keyboard, mouse)

4.3.2 Matrix Installation SIRA CON

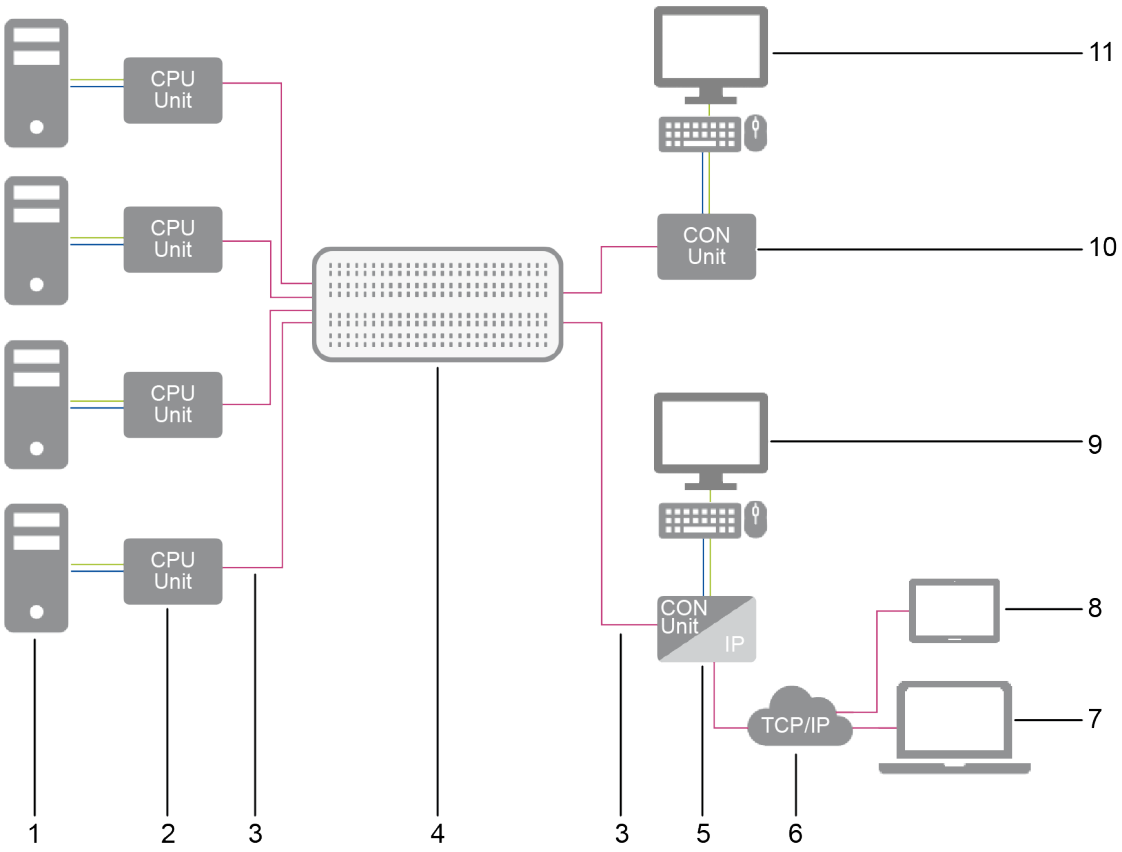


Fig. 2 Matrix installation example (Single-Head console and SIRA CON with console and remote access)

1 Sources
2 CPU Units
3 Interconnect cables
4 Matrix
5 SIRA CON
6 TCP/IP network
7 Notebook
8 Tablet
9 Console (monitor, keyboard, mouse)
10 CON Unit
11 Console (monitor, keyboard, mouse)

4.3.3 Local Installation SIRA Stand-alone

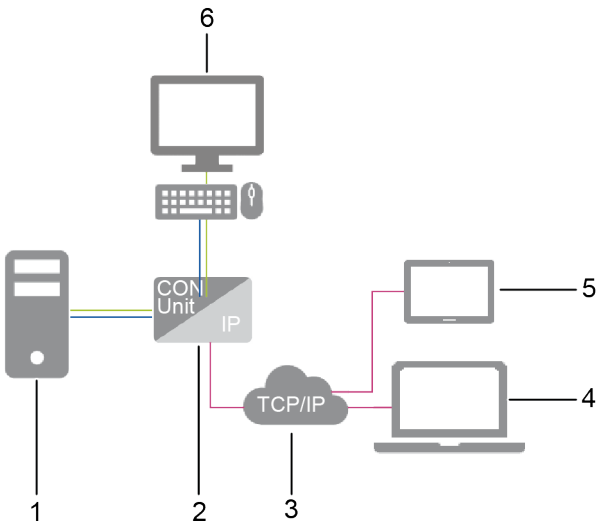


Fig. 3 Local installation example (SIRA Stand-alone with console, local source, and remote access)

1 Source
2 SIRA Stand-alone
3 TCP/IP network
4 Notebook
5 Tablet
6 Console (monitor, keyboard, mouse)

4.4 Product Types

4.4.1 Draco vario SIRA CON

Product type	Interconnection		HDMI output resolution/frame rate	USB Type A	RJ45
R488-BIPC	1x	RJ45 Cat X 1G	1x up to 3840 x 2160 @ 30 Hz	2x USB-HID/USB*	1x 1G LAN
R488-BIPCR	2x				
R488-BIPS	1x	LC Duplex Single-mode fiber 1G	1x up to 3840 x 2160 @ 30 Hz	2x USB-HID/USB*	1x 1G LAN
R488-BIPSR	2x				

* Preparation for future WEB UI configuration via USB and application for mobile devices.

4.4.2 Draco vario SIRA Stand-alone

Product type	HDMI input	USB Type B	HDMI output resolution/frame rate	USB Type A	RJ45
R488-BIPHHL	1x	1x USB-HID/ transparent USB	1x up to 3840 x 2160 @ 30 Hz	2x USB-HID/USB*	1x 1G LAN

* Preparation for future WEB UI configuration via USB and application for mobile devices.

4.5 Accessories for SIRA Module HDMI

Part. No.	Description	Interface
VC-HD2HDSL-018-MM	HDMI cable 1.8m male/male with 1x SupraLock	Video
247-U1	USB cable Type A-B, 1.8 m	USB/USB-HID
247-U2	USB cable Type A-B, 3.0 m	USB/USB-HID
436-USB20	USB extension cable Type A-A, 3.0 m	USB/USB-HID

4.6 Scope of Delivery

Depending on the order, the scope of delivery contains the following items and may vary depending on country of delivery and customer specification:

Product type	Scope of delivery
Draco vario Secure IP Gateway CON Module	• 1x SIRA module in Draco vario chassis • Quick Setup
Draco vario Secure IP Gateway Module HDMI	• 1x SIRA Stand-alone in Draco vario chassis • 1x HDMI cable 1.8m male/male with 1x SupraLock • 1x USB cable 1.8 m (type A-B) • Quick Setup

If anything is missing, please contact your distributor.

4.7 Device Views

4.7.1 SIRA CON R488-BIPC

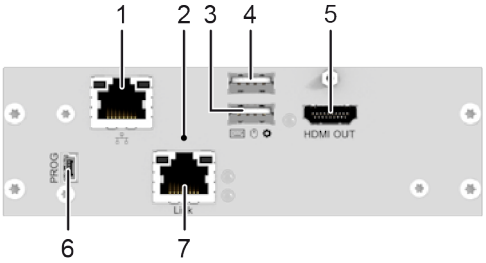


Fig. 4 Interface side R488-BIPC

1 RJ45, network interface
2 Reset button
3 USB Type A, USB-HID device 1
4 USB Type A, USB-HID device 2
5 HDMI output
6 Mini-USB, service interface
7 Cat X, interconnection

4.7.2 SIRA CON R488-BIPCR

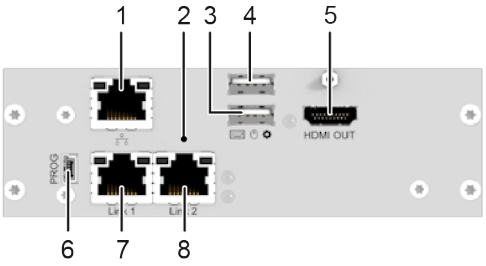


Fig. 5 Interface side R488-BIPCR

1 RJ45, network interface
2 Reset button
3 USB Type A, USB-HID device 1
4 USB Type A, USB-HID device 2
5 HDMI output
6 Mini-USB, service interface
7 Cat X, primary interconnection 1
8 Cat X, secondary interconnection 2

4.7.3 SIRA CON R488-BIPS

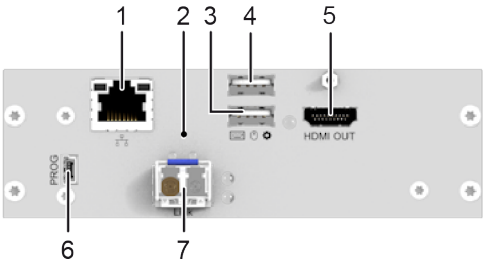


Fig. 6 Interface side R488-BIPS

1 RJ45, network interface
2 Reset button
3 USB Type A, USB-HID device 1
4 USB Type A, USB-HID device 2
5 HDMI output
6 Mini-USB, service interface
7 Fiber, interconnection

4.7.4 SIRA CON R488-BIPSR

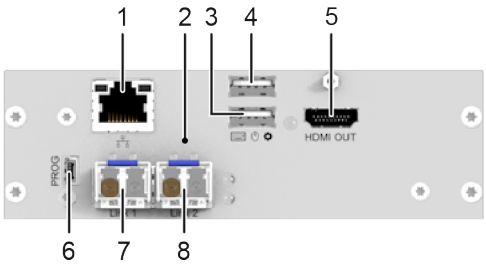


Fig. 7 Interface side R488-BIPSR

1 RJ45, network interface
2 Reset button
3 USB Type A, USB-HID device 1
4 USB Type A, USB-HID device 2
5 HDMI output
6 Mini-USB, service interface
7 Fiber, primary interconnection 1
8 Fiber, secondary interconnection 2

4.7.5 SIRA Stand-alone R488-BIPHHL

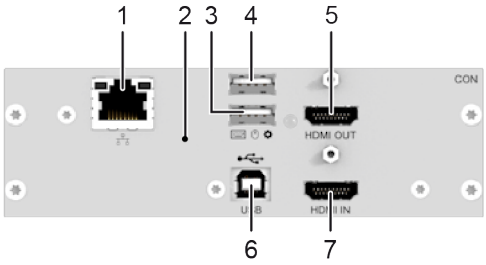


Fig. 8 Interface side R488-BIPHHL

1 RJ45, network interface
2 Reset button
3 USB Type A, USB-HID device 1
4 USB Type A, USB-HID device 2
5 HDMI output
6 USB Type B, USB-HID
7 HDMI input

4.8 Status Indication of SIRA CON and SIRA Stand-alone

4.8.1 LEDs on Board

All modules have one multicolor LED for status indication on the PCB that is visible on the lower hole of the chassis front side at the modules of following chassis:

474-BODY2, 474-BODY2R, 474-BODY2N, 474-BODY4, 474-BODY4R and 474-BODY6R-R1.

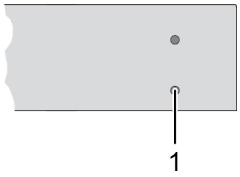


Fig. 9 Chassis front view with LEDs of modules

1 PCB LED of the module

LED Status	Description
Dark red	Video processor in failure status (e.g., incorrect firmware uploaded.
Red	No video signal available, no USB-HID connection available.
Green	Video signal available, no USB-HID connection available.
Violet	No video signal available, USB-HID connection available.
Light blue	Video signal available, USB-HID connection available.

4.8.2 LEDs for Power Supply Voltage

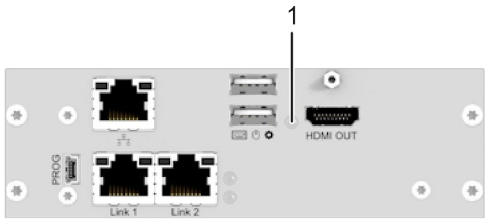


Fig. 10 Interface side - Power supply voltage LED (Example R488-BIPCR)

1 Power Status LED

The following table show the respective LED states/colors of the power supply voltage LED for the respective situation.

LED 1	Description
Off	No power supply voltage available.
Green	Power supply voltage available.
Slowly flashing green	Power supply voltage available, session active

4.8.3 LEDs for Network Connection

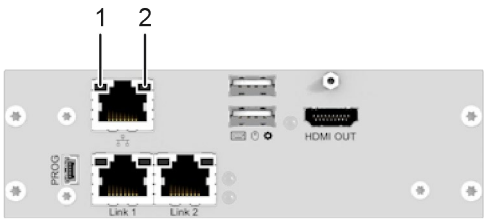


Fig. 11 Interface side - Network LED (Example R488-BIPCR)

1 Status LED 1
2 Status LED 2

For an easier identification, the LED representation and column designation in the table was selected analogously to the LED position on the ports.

The following tables show the respective LED states/colors of the network connection LED and activity LED for the respective situation.

LED 1	LED 2	Description
Off	Off	No network connection available.
Off	Green	Network connection available, no data traffic available.
Off	Slowly flashing green	Network connection available, data traffic active.

4.8.4 LEDs for Interconnection Cat X

The LED status of the interconnection is described using the redundant SIRA CON as an example.

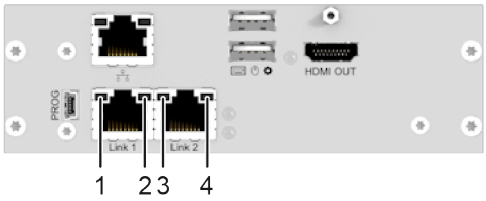


Fig. 12 Interface side - Interconnection LEDs (Example R488-BIPCR)

1 Failure LED link 1
2 Status LED link 1
3 Failure LED link 2
4 Status LED link 2

The following table shows the respective interconnection LED states/colors (left LED 1, 3 and right LED 2, 4) for the respective situation.

Pos. 1/3	Pos. 2/4	Description
Off	Green	Interconnection available.
Off	Flashing green	No interconnection available.
Flashing green	Green	Interconnection failure (flashes for approx. 20 s following each occurring connection failure).

4.8.5 LEDs for Interconnection Fiber

The LED status of the interconnection is described using the redundant SIRA CON as an example.

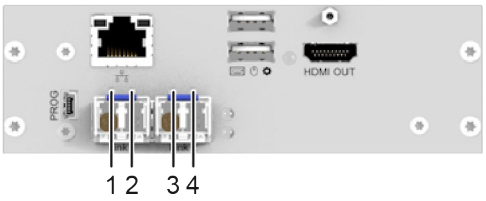


Fig. 13 Interface side - Interconnection LEDs (Example R488-BIPSR)

1 Failure LED link 1
2 Status LED link 1
3 Failure LED link 2
4 Status LED link 2

The following table shows the respective interconnection LED states/colors (left LED 1, 3 and right LED 2, 4) for the respective situation.

Pos. 1/3	Pos. 2/4	Description
Off	Green	Interconnection available.
Off	Flashing red	No interconnection available.
Flashing red	Green	Interconnection failure (flashes for approx. 20 s following each occurring connection failure).

4.8.6 LEDs for USB-HID and Video Connection

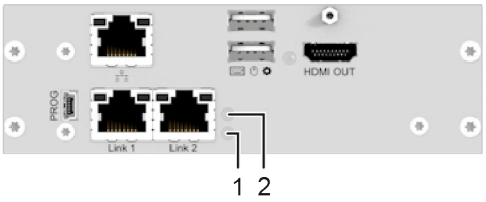


Fig. 14 Interface side - Interconnection LEDs (Example R488-BIPSR)

1 Status LED USB-HID and video status of video channel 1
2 Status LED USB-HID and video status of video channel 2

When SIRA Modules are directly connected, the LEDs behave differently depending on whether there is a link connection between the CON Unit and the target, whether a video signal is present, at which resolution a video signal is transmitted, or whether a USB connection exists.

The following tables show the respective LED states/colors (upper LED (2) and the lower LED (1)) of the modules for the respective situation.

The USB connection is missing, when the command mode is started, or when the CON Unit currently has no USB-HID control with shared operation of a redundant CPU Unit.

Pos.	LED CON Unit	Description
2	 Flashing red/violet	Without link connection.
1	 Flashing red/violet	
2	 Violet	With link connection, without video signal.
1	 Violet	
2	 Flashing red/violet	With link connection, with video signal, without USB connection, resolution up to 1920 x 1080 @ 60 Hz.
1	 Flashing green/light blue	
2	 Flashing green/light blue	With link connection, with video signal, without USB connection, resolution between 1920 x 1080 @ 60 Hz and 3840 x 2160 @ 30 Hz.
1	 Flashing green/light blue	
2	 Violet	With link connection, video signal and USB connection, resolution up to 1920 x 1080 @ 60 Hz.
1	 Light blue	
2	 Light blue	With link connection, video signal and USB connection, resolution between 1920 x 1080 @ 60 Hz and 3840 x 2160 @ 30 Hz.
1	 Light blue	

5 Access Option

You have following options to configure and/or operate the extender module and add-on module:

Access option	Description
Command mode	The SIRA CON BIPx include a command mode that enables access to several functions of connected KVM devices, e.g., Draco U-Switch or Draco tera matrix switch when using additional keyboard commands. In addition, individual extender module functions for USB-HID Ghosting and the EDID, as well as switching via command mode and additional keyboard commands can be executed.
HTML KVM Client (HKC)	HKC is best for Linux and MacOS users without Java and runs on any browser, including mobile. Quickest and easiest to log into, but video performance and virtual media functionality are limited. 4K video is not recommended.
Active KVM Client (AKC)	Recommended high-performance client for Microsoft Windows Platforms without the need of Java, using Microsoft Edge, Internet Explorer 11, or any other browser with ClickOnce plug-in. AKC is based on Microsoft Windows .NET technology. AKC will load and launch automatically when the link is clicked (see chapter 7.2, page 65).
Virtual KVM Client Stand-alone (VKCS)	Recommended high-performance client for Linux and MacOS users with Java 1.8. After clicking the link (see chapter 7.1.1, page 36), VKCS will download. If the browser does not download VKCS automatically, click the downloaded `.jnlp` file (or ctrl-click on Mac) to launch.

5.1 Command Mode

To start the command mode, use a keyboard sequence (Hot Key) both at the keyboard plugged in a SIRA CON and via remote session via TCP/IP. The command mode can also be called up using a keyboard with USB-HID interface connected to an add-on module.

To exit the command mode, press Esc.

NOTICE

While in command mode,

- ➡ the **Caps Lock** and **Scroll Lock** LEDs on the keyboard are flashing,
- ➡ the USB-HID devices are not operable, mouse and keyboard functions are deactivated,
- ➡ only selected keyboard commands are available.

If there is no keyboard command entered within 10 seconds after activating the command mode, it will be deactivated automatically.

The following keyboard commands are used to enter, and to exit the command mode, and to change the Hot Key.

Function	Keyboard command
Start the command mode	2x Left Shift (Hot Key, factory setting)
Exit the command mode	Esc and also Left Shift + Esc, if necessary
Change the Hot Key	current Hot Key, c, new Hot Key Code, Enter

NOTICE
In a combined KVM matrix/U-switch configuration, select different Hot Keys for the connected extender modules, e.g., 2x Left Shift for access to the matrix and e.g., 2x Right Shift for access to the U-Switch.

Hot Keys currently can only be changed at the console and only for that console.

Hot Key Code

The Hot Key to start the command mode can be changed. The following table lists the Hot Key codes for the available Hot Keys.

Hot Key Code	Hot Key
0	Freely selectable, except Esc, Del and Enter
2	2x Scroll
3	2x Left Shift (default)
4	2x Left Ctrl
5	2x Left Alt
6	2x Right Shift
7	2x Right Ctrl
8	2x Right Alt

Change the current Hot Key via Hot Key Code (exemplary)

To change the current Hot Key to, e.g., 2x Left Alt, enter Hot Key, c, 5, Enter.

Set a freely selectable Hot Key (exemplary)

To set a freely selectable Hot Key (e.g., 2x Space), enter Hot Key, c, 0, Space, Enter.

Keyboard commands are fixed to the position of the keys on the keyboard. Keyboard mapping tables may vary for country-specific layouts.

➥ Note the key position of a freely defined Hot Key when changing the keyboard layout, e.g., from QWERTZ to AZERTY. E.g., if defining 2x a as Hot Key on a German or US keyboard layout, the French keyboard layout (AZERTY) requires then 2x q as Hot Key to be pressed instead.

Reset the Hot Key

To set a Hot Key back to default settings, press Right Shift + Del within 5 s after switching on the CON Unit or plugging in a keyboard.

The Hot Key is set back to Left Shift.

6 Installation and Initial Configuration

6.1 Connecting the Hardware

6.1.1 Connecting SIRA CON

1. Switch off all devices.
2. Connect the monitor(s), keyboard, and mouse to the SIRA CON.
3. Connect the SIRA CON to the network using the LAN port.
4. Connect the chassis of the SIRA CON to the power supply unit(s)/power socket(s).
5. Connect the SIRA CON to the matrix.

Establishing a matrix connection and changing the Hot Key of the SIRA CON is described in the respective Draco tera matrix manual.

6.1.2 Connecting SIRA Stand-alone

1. Connect the target with an HDMI cable to the HDMI input port of the SIRA Stand-alone using the provided HDMI cable. If the target video has no HDMI output, use a cable- or video-adapter.
2. Connect the target to the USB Type B of the SIRA Stand-alone port using the provided USB cable.
3. Connect the monitor(s), keyboard, and mouse to the SIRA Stand-alone.
4. Connect the SIRA Stand-alone to the network using the LAN port.
5. Connect the chassis of the SIRA Stand-alone to the power supply unit(s)/power socket(s).

6.2 System Requirements

6.2.1 Minimum Client and System Recommendations

Minimum client requirements vary somewhat depending on the client and the desired video stream.

Computer/Software/Network		Requirements/Recommendations	
Network	Speed	Fast network like Gigabit Ethernet or WiFi 802.11ac	
Virtual KVM Client Stand-alone (VKCS) and Active KVM Client (AKC)	CPU	FullHD video	A modern and fast dual core CPU, such as Intel Core i3 4xxx or newer, or a quad core CPU. If you plan to run more than one KVM session, a quad core CPU is recommended.
		4K video	A modern and fast quad core CPU, such as Intel Core i5 4xxx or newer. If you plan to run more than one 4K stream, a CPU with 6 or more cores is recommended, such as Intel Core i5/i7 8xxx.
	RAM	8 GB recommended.	
	Graphics Card	Modern OpenGL capable graphics card, such as GeForce or Radeon. At least 1GB.	
HTML KVM Client (HKC)*	CPU	A modern and fast dual core CPU.	
	RAM	8 GB recommended.	
	Graphics card	OpenGL.	

* 4K video not recommended on HKC

6.2.2 Client Options

The modules can be accessed via TCP/IP with a variety of KVM clients that support individual configuration.

KVM Client	Name	Platforms	Supported browsers	Features
HTML KVM Client	HKC	• Linux • MacOS • Microsoft Windows • HTML and Javascript	• Microsoft Internet Explorer 11 (minimum) • Microsoft Edge • Firefox • Google Chrome • Apple Safari	• Java-free • Supports most features • See HTML KVM Client (HKC) for supported features
Active KVM Client	AKC	• Microsoft Windows 7, 8, 10 (up to 64 bit) • Requires Microsoft .NET	• Microsoft Edge • Microsoft Internet Explorer 11 • Other browsers with ClickOnce plug-in	• Java-free • Full-featured KVM Client
Virtual KVM Client Stand-alone	VKCS	• Linux • MacOS • Microsoft Windows	• Firefox • Google Chrome	• Requires Java • Full-featured KVM Client

See the Release Notes for supported versions of platforms, operating systems, Java and browsers.

6.3 Initial Configuration

6.3.1 Connecting to the SIRA Modules via TCP/IP

1. Ensure the SIRA module and the computer are connected to the LAN via network cable.
2. Open a browser.
3. Enter the IP address of the SIRA module (default 192.168.100.88/24).
   A login dialog appears.
4. Enter the username and the password (default: admin/admin).
   The HTML KVM Client (HKC) is loaded by default.

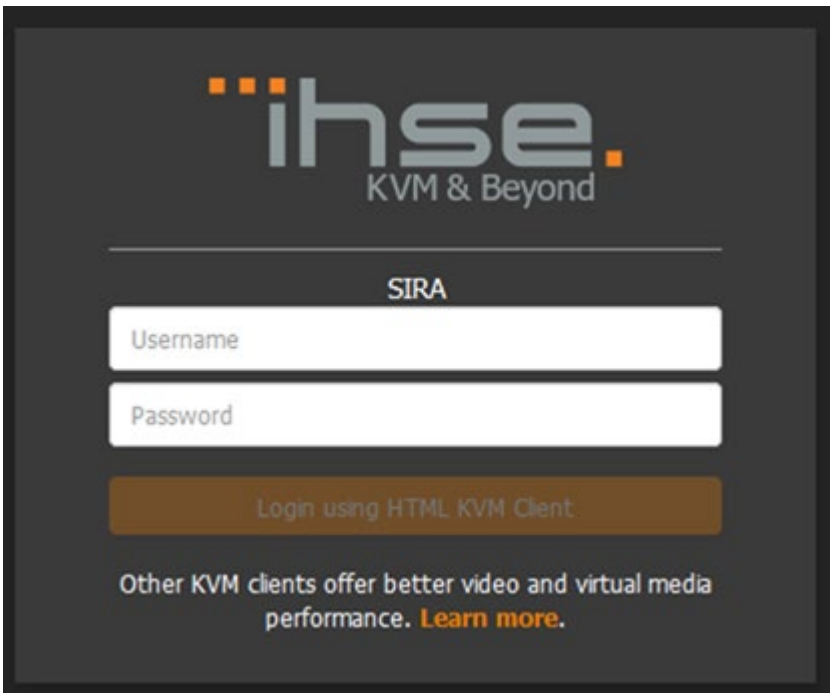
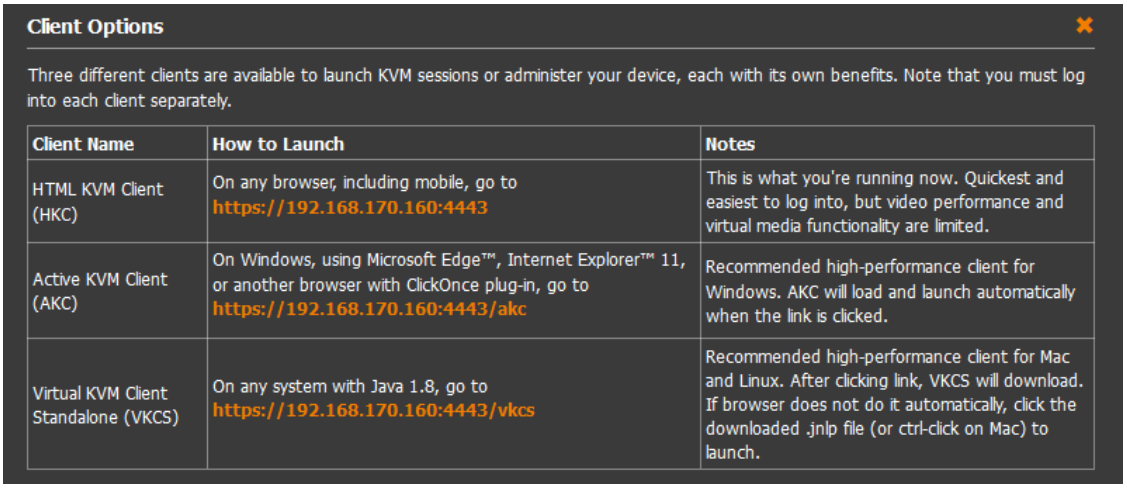


Fig. 15 SIRA Client - HKC login dialog

➡ Click the **Learn more** link in the login dialog to view other KVM client options.

The **Learn more** link launches a client options dialog.



Client Options

Three different clients are available to launch KVM sessions or administer your device, each with its own benefits. Note that you must log into each client separately.

Client Name	How to Launch	Notes
HTML KVM Client (HKC)	On any browser, including mobile, go to https://192.168.170.160:4443	This is what you're running now. Quickest and easiest to log into, but video performance and virtual media functionality are limited.
Active KVM Client (AKC)	On Windows, using Microsoft Edge™, Internet Explorer™ 11, or another browser with ClickOnce plug-in, go to https://192.168.170.160:4443/akc	Recommended high-performance client for Windows. AKC will load and launch automatically when the link is clicked.
Virtual KVM Client Standalone (VKCS)	On any system with Java 1.8, go to https://192.168.170.160:4443/vkcs	Recommended high-performance client for Mac and Linux. After clicking link, VKCS will download. If browser does not do it automatically, click the downloaded .jnlp file (or ctrl-click on Mac) to launch.

Fig. 16

➡ Click the provided links to launch a different client.
https://IP address launches HKC
https://IP address/akc launches AKC
https://IP address/vkcs launches VKCS

When a different client is selected, the SIRA Module automatically checks the system to make sure it meets the requirements of the client. If the system is ready, the selected client loads. If the system needs to meet additional requirements, another message displays with details.

For AKC and VKCS, the browser may display a "This site is not secure" warning message until having installed valid certificates.

➡ Click to accept the warnings and go to the site.

➡ See chapter 12.6, page 155 for help installing certificates that prevent these warnings.

➡ For more details and instructions for using all clients, see chapter 7, page 36.

6.3.2 Next Steps

- Configure network settings, see chapter 10.4.1, page 117)
- Configure time settings, see chapter 10.1, page 104
- Install certificates see chapter 12.6.2, page 156
- Configure users, see chapter 11, page 129
- Configure port settings, see chapter 8, page 94

7 KVM Clients

7.1 Virtual KVM Client Stand-alone (VKCS) Help

7.1.1 VKCS Download and Launch

Requirements

➡ Check the browsers available for this application (see chapter 6.2.2, page 33).

➡ Check the release notes for latest supported Java version.

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

➡ To launch VKCS, enter https://IP address/vkcs in a browser.

The downloaded application is available only for the specified IP address of a SIRA Module. We recommend renaming the downloaded application including the IP address and saving it for further use, e.g., on the desktop. Otherwise, the application must be downloaded every time of use.

Downloading via Google Chrome and Microsoft Edge

➡ Click the downloaded VKCS `.jnlp` file at bottom left corner of the browser window to save and to launch.

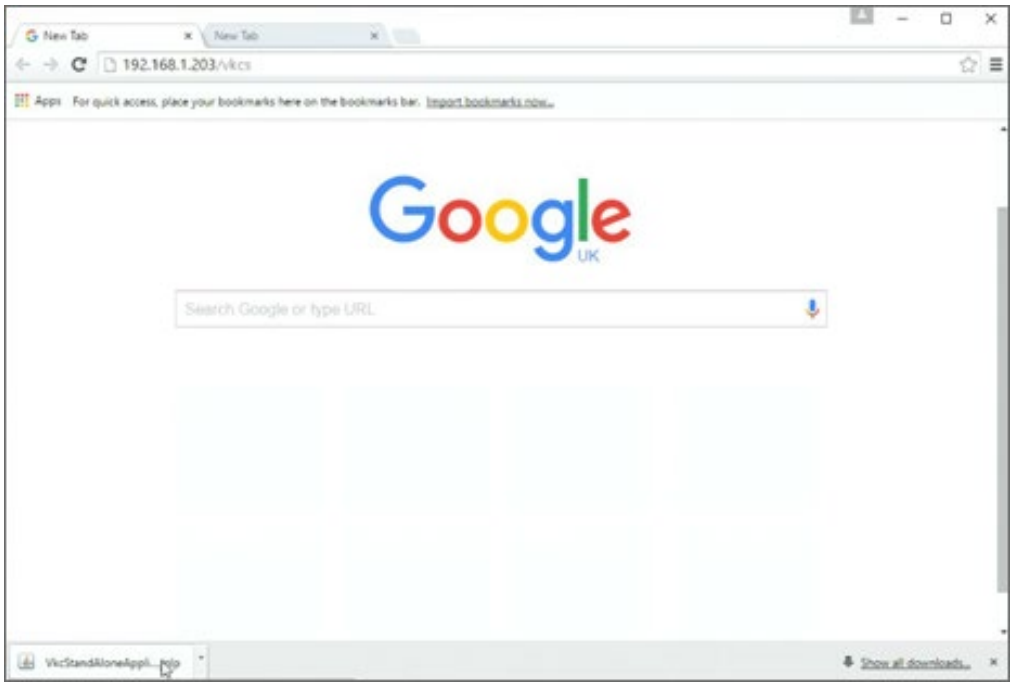


*Fig. 17 VKCS **Downloaded .jnlp file in Google Chrome and Microsoft Edge***

Downloading via Microsoft Internet Explorer

➡ Click **Open** at the bottom of the browser to launch or **View downloads** to save the downloaded VKCS `.jnlp` file.

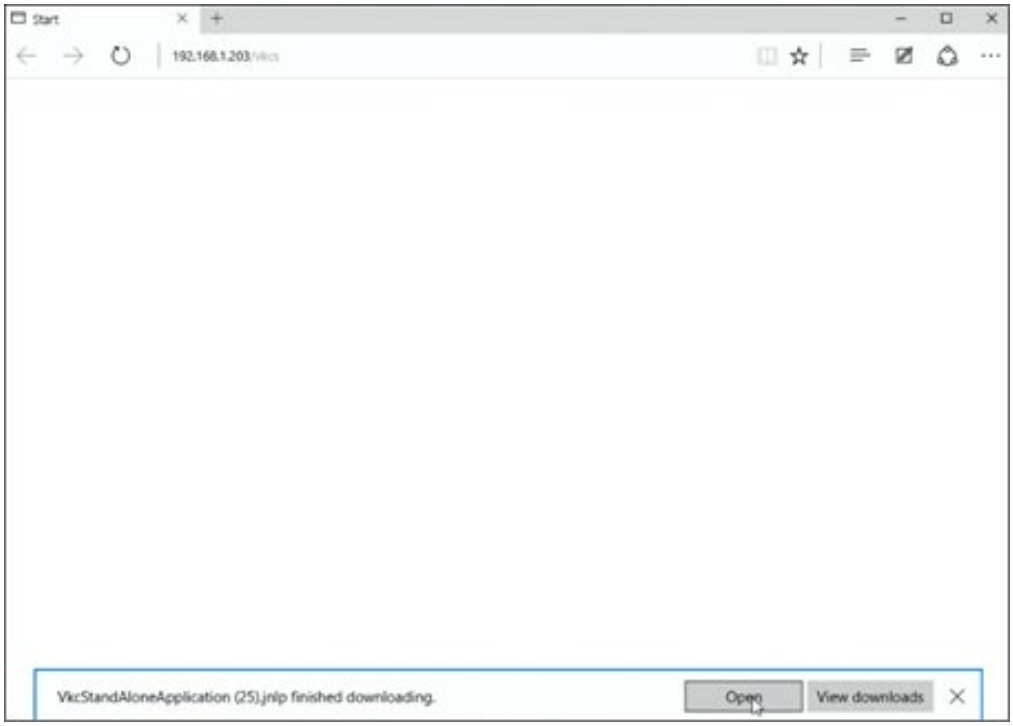


*Fig. 18 VKCS **Downloaded .jnlp file in Microsoft Internet Explorer***

Downloading via Safari

1. Save the `.jnlp` file locally.
2. Hold down CTRL when selecting to open, then click **Open** in appeared dialog.

Downloading via Firefox

The current default setting in Firefox on Windows saves the file and runs from the download. You can launch from the browser with this setting:

1. Open the Firefox Settings.
2. In the **General** tab scroll to **Files and Applications**.
3. Under **Applications** select `Jnlp File` in the **Content Type** column.
4. Change the **Action** from **Always ask** to **Use Java Web Launcher**.

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

- Launching via jnlp://IP address/vkcs

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

OR

- Add a new preference "browser.download.skipConfirmLaunchExecutable" to about:config.

  For details, go to https://support.mozilla.org/en-US/questions/1260307

7.1.2 Accessing the Target

When launching the VKCS, the **Port Access** of the configuration menu is opened with a preview image if a target is connected to the SIRA Module.

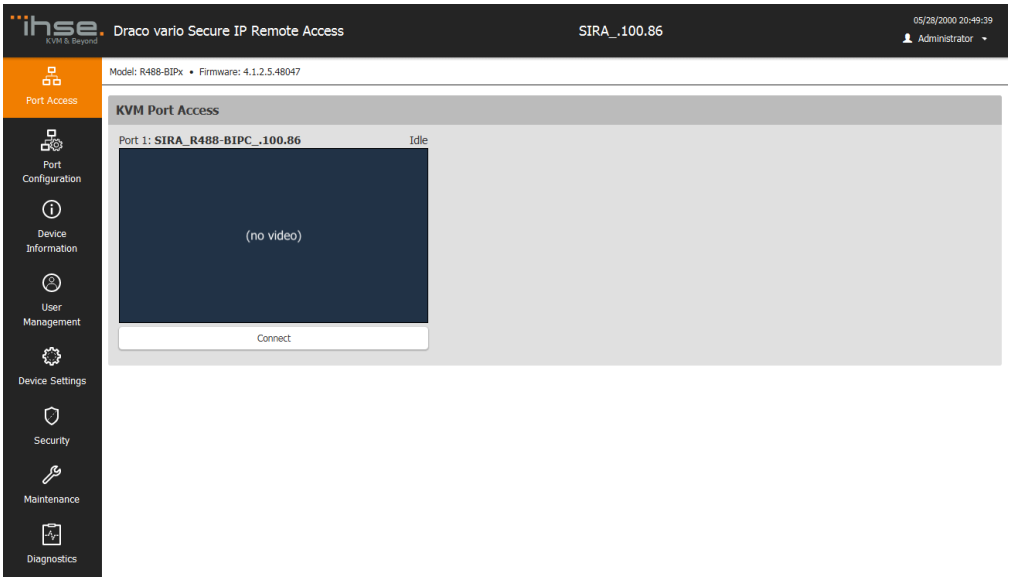


*Fig. 19 VKCS **SIRA Configuration menu - Port Access***

➡ Click **Connect** in the working area to start a browser session allowing KVM access to the target.

The configuration menu of the VKCS is opened.

Clicking any of the options of the left task bar will prompt you to other configuration menus. For details to the configuration menu, see from chapter 89, page 94.

7.1.3 VKCS Modes of Operation

7.1.3.1 VKCS View

When the SIRA CON is connected to a matrix and is not switched to a CPU Unit, or the SIRA Stand-alone is not connected to a target, the screen is black.

In the client, there is a menu bar with drop-down menus and a toolbar for quick access to functions. All functions are described in chapter 7.1.

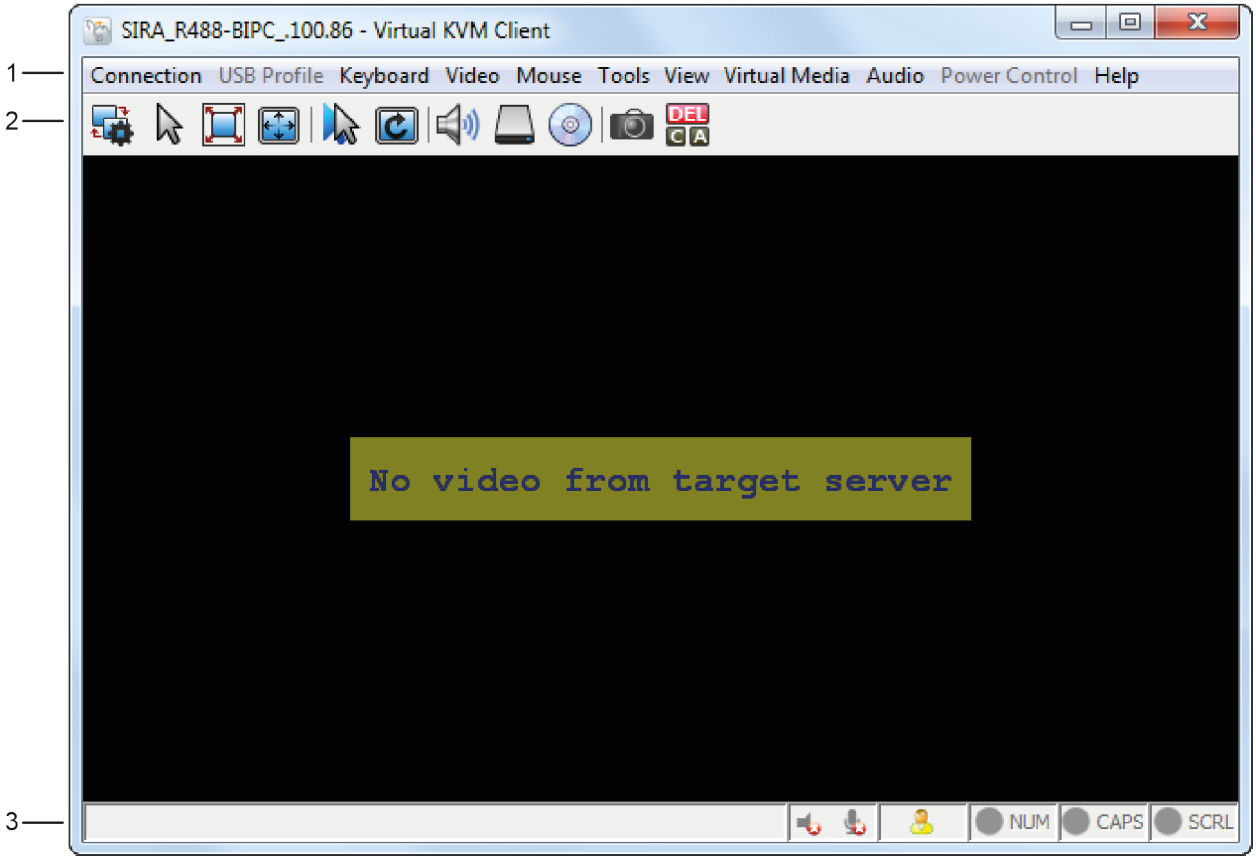


*Fig. 20 VKCS **View***

1 Menu bar
2 Toolbar
3 Status bar

7.1.3.2 VKCS Toolbar

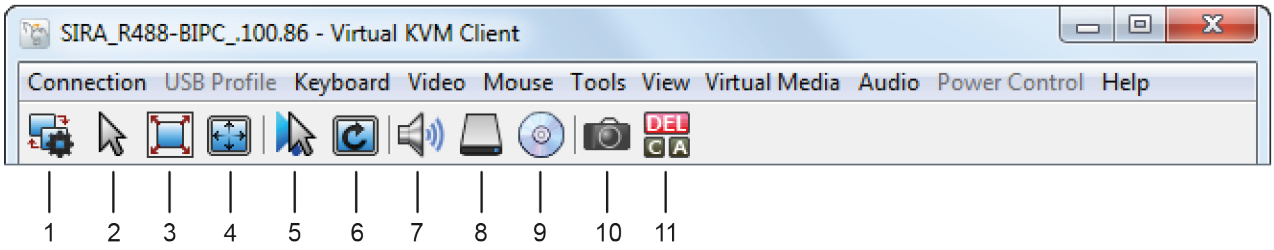


*Fig. 21 VKCS **Toolbar***

1 Connection Properties
2 Single Mouse cursor
3 Full Screen
4 Resize video to fit screen
5 Synchronize Mouse
6 Refresh Video
7 Connect Audio
8 Connect Drive
9 Connect CD-ROM/ISO
10 Target Screenshot
11 Send Ctrl+Alt+Del macro

7.1.3.3 View Options

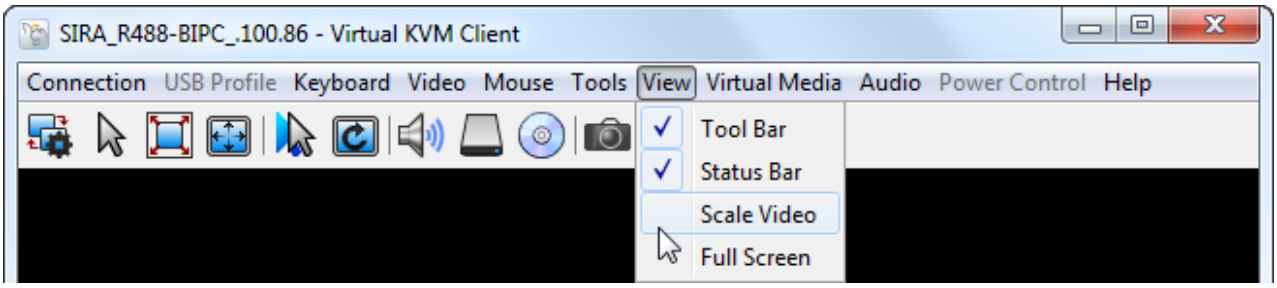


*Fig. 22 VKCS **Toolbar***

7.1.3.3.1 View Toolbar

By default, the toolbar is displayed at the top of the target window.

➡ Click **View > View Toolbar** to hide or to display the toolbar.

7.1.3.3.2 View Status Bar

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

➡ Click **View > Status Bar** to hide or to display the status bar.

7.1.3.3.3 Scale Video Mode

This feature increases or reduces the size of the target video to fit the Virtual KVM Client window size and maintains the aspect ratio so that the entire contents of the target is visible without using the scroll bar.

➡ Click **View > Scale Video** to toggle scaling (on and off).

7.1.3.3.4 Full Screen Mode

Selecting the Full Screen mode, the target's full screen is displayed and acquires the same resolution as the target.

The Client Hot Key used for exiting this mode is specified in the Tool's Options dialog, see chapter 7.1.9.1, page 52).

Entering Full Screen Mode

1. Click **View > Full Screen** or click in the toolbar.

Exiting Full Screen Mode

➡ Press the Client Hot Key configured in the Tool's **Options** dialog. The default is `Ctrl+Alt+M`.

Full Screen Mode as the Default Mode

To access the target in full screen mode at all times, make **Full Screen** mode the default.

1. Click **Tools > Options** to open the **Options** dialog.
2. Tick the **Enable Launch in Full Screen Mode** checkbox.
3. Click **OK**.

7.1.3.4 Full Screen Mode Menu Bar

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

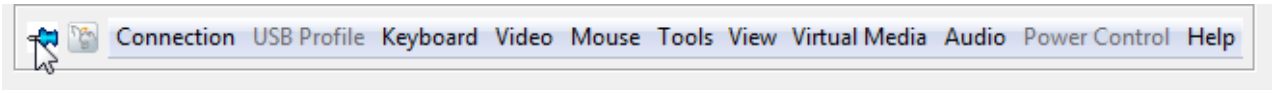


*Fig. 23 VKCS **Full Screen Mode Menu Bar***

To remain the menu bar visible while in **Full Screen** mode, tick the **Pin Menu Toolbar** checkbox from the **Options** dialog (see chapter 7.1.9.2, page 55).

7.1.4 Connection Properties

Connection properties manage streaming video performance over remote connections to targets. Additionally, it shows the current signal details such as framerate and used transmission bandwidth.

The properties are applied only to the own connection. They do not impact the connection of other users accessing the same targets. Changes of connection properties are retained by the client.

➡ Click **Connection > Properties…** in the menu bar or click in the toolbar.

The **Connection Properties** menu appears.

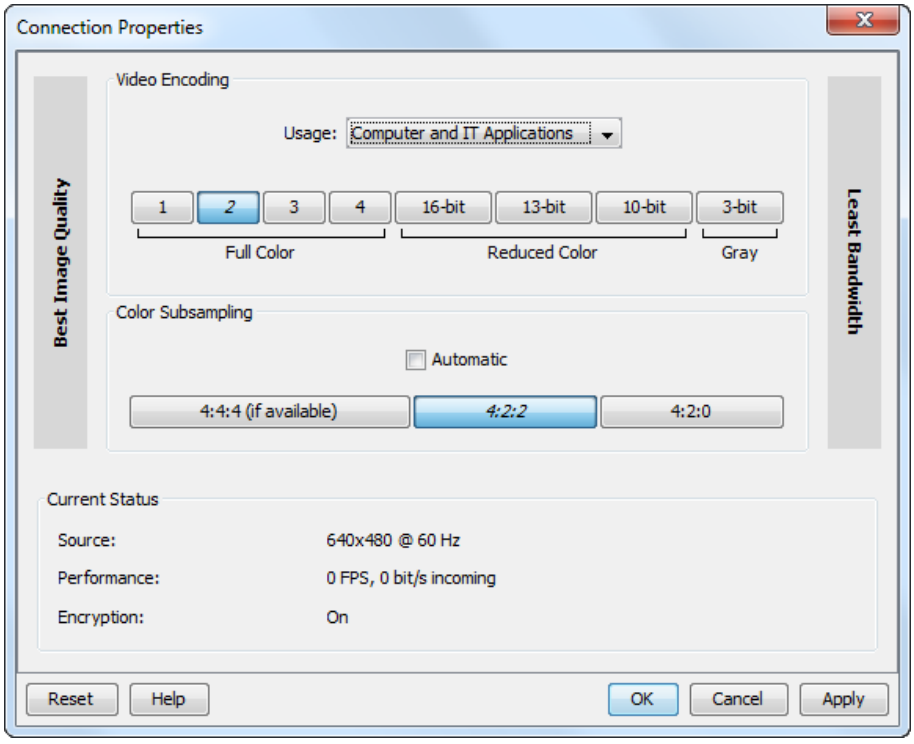


*Fig. 24 VKCS **Connection Properties***

Video Encoding

This section selects the video encoding algorithm and quality setting.

- **Usage**: specify your general application area. This selection optimizes the available choices elsewhere in this dialog.
  - **General Purpose Video**: video content where smooth color reproduction is most important, such as movies, video games, and animations.
  - **Computer and IT Applications**: video content where text sharpness and clarity are important, such as computer graphical interfaces.
- **Encoder Mode**: Choose the encoder mode from the row of eight buttons. Options will vary depending on the **Usage** selection. In general, modes towards the left of the button bar offer higher image quality but consume higher bandwidth and might cause frame rate to drop depending on network speed and/or client performance. Modes towards the right consume lower bandwidth at the cost of reduced image quality. In network- or client-constrained situations, modes towards the right may achieve better frame rates.
  The default video mode is always **Full Color 2**, which is a high-quality mode and works well for most uses in LAN environments. If needed, experiment with modes further towards the right to find the right balance of image quality and frame rate.

Color Subsampling

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

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

Current Status

Current status includes real-time video performance statistics. When changing settings in the dialog, the effects on performance can immediately be seen.

- **Source**: resolution and frame rate of the incoming video source.
- **Performance**: frames per second (FPS) being rendered in the client, and the data rate of the incoming video stream. These values are where you will see the effects of your video settings.
- **Encryption**: whether the video stream is encrypted or not. Encrypted streams usually have lower frame rates and lower bandwidth. Encryption is a global setting in the configuration menu of the SIRA Module. To activate **Apply Encryption Mode to KVM and Virtual Media**, see chapter 12.3, page 152.

7.1.5 Connection Info

1. Click **Connection > Info…** in the menu bar.

   The **Connection Info** dialog appears with real-time connection information on the current connection.
2. Click **Copy to Clipboard** if information from the dialog is needed.
3. To edit the connection properties, see chapter 7.1.4, page 41).

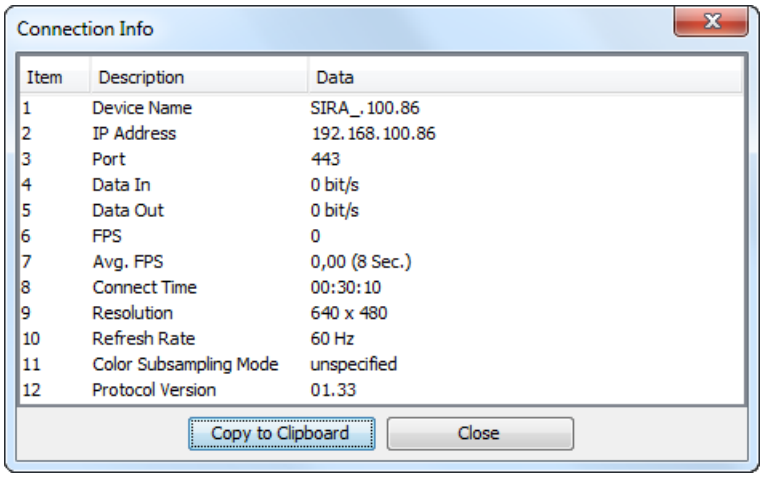


*Fig. 25 VKCS **Connection Info***

7.1.6 Keyboard

Keyboard macros ensure that keystroke combinations intended for the target are sent to and interpreted only by the target. Otherwise, they might be interpreted by the client computer due to the structure of the operating system.

Macros are stored on the client computer and are computer-specific. If using another computer with the same SIRA Module, the created macros are not available.

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

Macros created in one client can only be used in the client they have been created. They are not usable in another client. E.g., VKCS macros are not usable in HKC or AKC.

7.1.6.1 Preprogrammed Macros

Due to its frequent use, some macros are preprogrammed and there is the possibility to program further macros for the target.

Send CTRL+ALT+DEL

➡ Click **Keyboard > Send CTRL+ALT+DEL** in the menu bar or click DEL C A in the toolbar to send this key sequence to the target or to the matrix to which the SIRA Module is currently connected.

Send LeftAlt+Tab

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

Send Text to Target

To use the **Send Text to Target** function for the macro, proceed as follows:

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

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

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

7.1.6.2 Add a Keyboard Macro

To build a macro, proceed as follows:

1. Click **Keyboard > Keyboard Macros**.
   The **Keyboard Macros** dialog appears.
2. Click **Add**.
   The **Add Keyboard Macro** dialog appears.

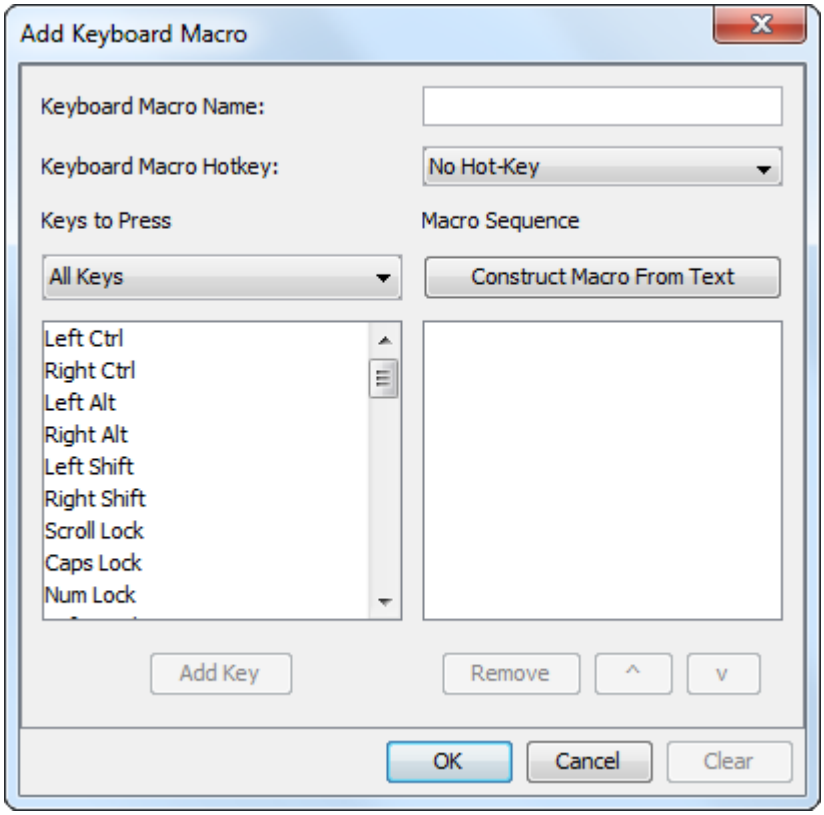


*Fig. 26 VKCS **Keyboard - Keyboard Macros - Add Keyboard Macro***

3. Type a name for the macro in the **Keyboard Macro Name** field.
   This name appears in the **Keyboard Macro** drop-down menu after it is created.
4. Select a keystroke to define the new macro:
   4.1. Option 1: Select a keyboard combination from the **Keyboard Macro Hotkey** drop-down list.
   This allows to execute the macro with a predefined keystroke.

4.2. Option 2: In the list below **Keys to Press**, select each key that is intended to be used to emulate the keystrokes that is used to perform the command. Select the keys in the order by which they are to be pressed. After each selection, select **Add Key**.

As each key is selected, it appears in the field fellow **Macro Sequence** and a **Release Key** command is automatically added after each selection.

For example, create a macro to close a window by selecting Left Alt + F4. This appears in the **Macro Sequence** field as follows:

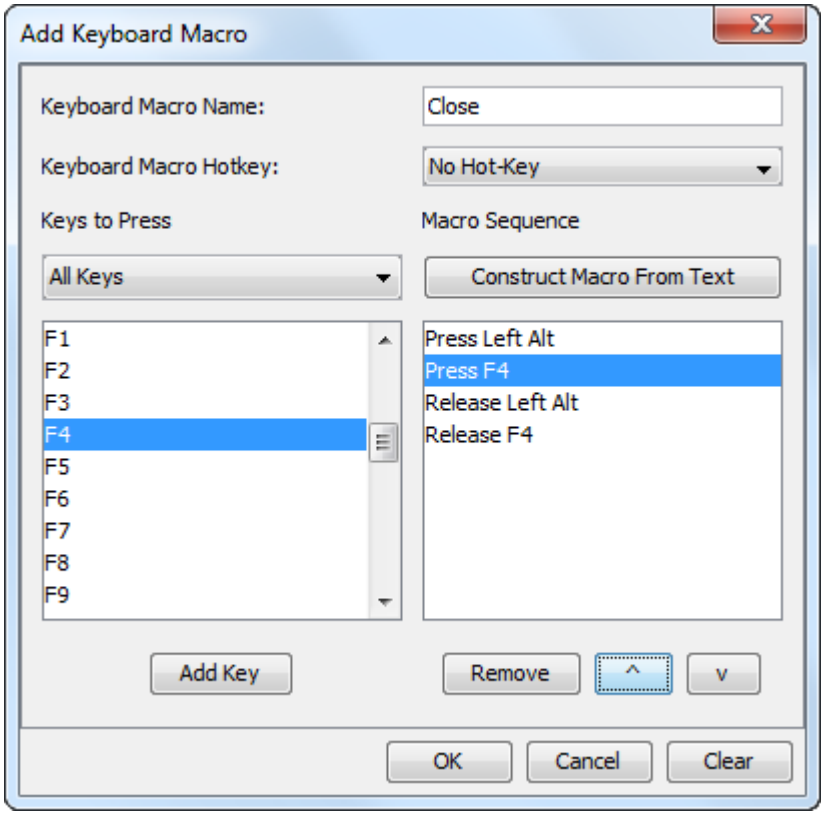


*Fig. 27 VKCS **Keyboard - Keyboard Macros - Add Keyboard Macro - Added Keyboard Macro***

5. Review the **Macro Sequence** field to be sure the macro sequence is defined correctly.
   5.1. To remove a step in the sequence, click the step and click **Remove**.
   5.2. To put the steps in the correct sequence, click the step in the **Macro Sequence** box and click **^** or **v**.
6. Click **OK** to save the macro or click **Clear** to clear all field and start over.

   Clicking **OK**, the **Keyboard Macros** dialog appears and lists the new keyboard macro.

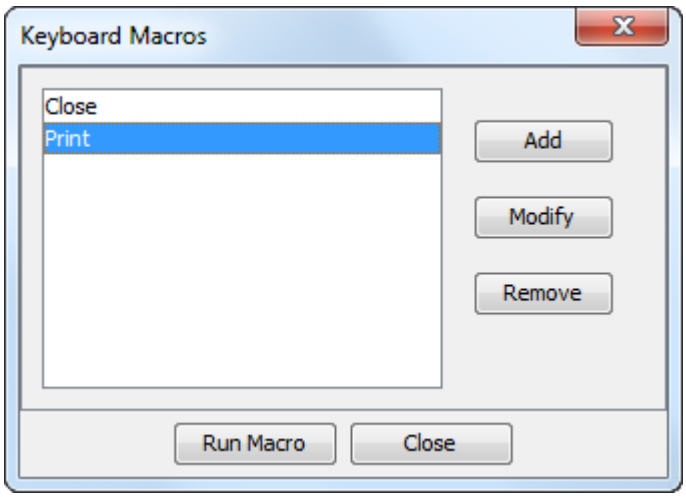


*Fig. 28 VKCS **Keyboard - Keyboard Macros - Keyboard macro list***

7. Click **Close** to close the **Keyboard Macros** dialog.
   The macro now appears in the **Keyboard** menu below **Keyboard Macros**.
8. Select the new macro on the menu to run it or use the keystrokes that are assigned to the macro.

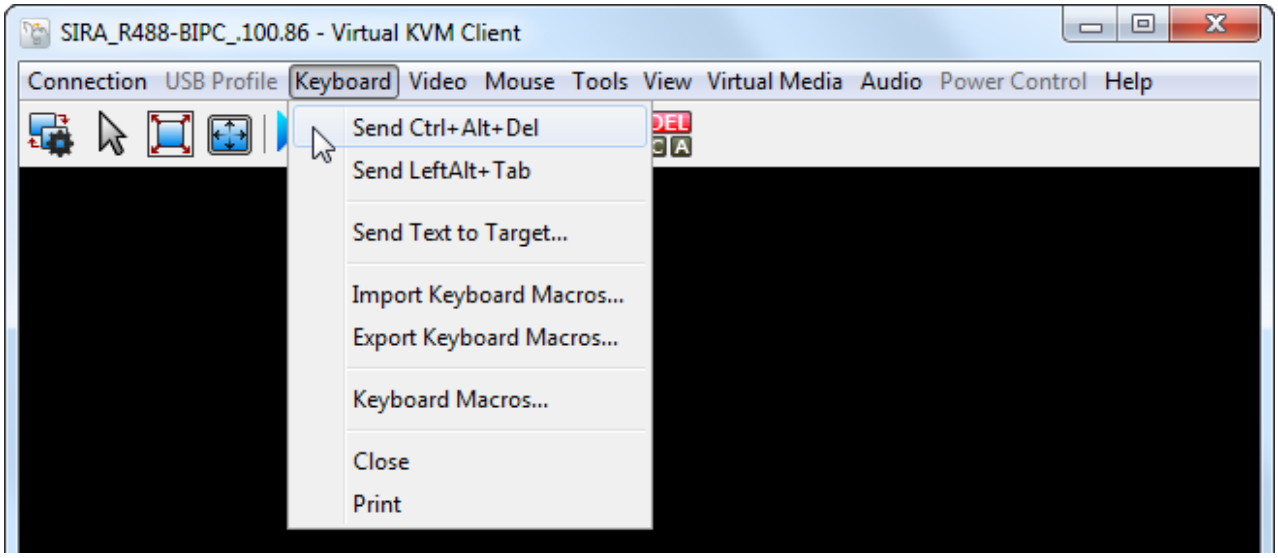


*Fig. 29 VKCS **Keyboard drop-down menu - New macros***

7.1.6.3 Export Macros

To export macros, proceed as follows:

1. Click **Keyboard > Export Keyboard Macros**.
   The **Export Keyboard Macros** dialog appears.
2. Tick the macro checkboxes to be exported or click **Select All**. To remove all selected macros click **Deselect All**.
3. Click **OK**.

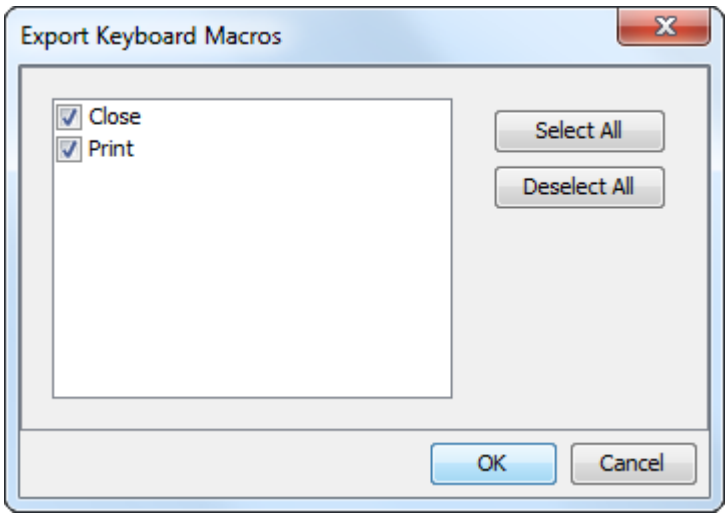


*Fig. 30 VKCS **Export Keyboard Macros***

The **Export Keyboard Macros to** dialog appears.

4. In the **Export Keyboard Macros to** dialog, go to the location to save the export file (`.xml`) and name the export file.
5. Click **Save**.

   If the macro already exists, an alert message appears.
6. Select **Yes** to overwrite the existing macro or **No** to close the alert without overwriting the macro.

7.1.6.4 Import Macros

To import macros, proceed as follows:

1. Click **Keyboard > Import Keyboard Macros.**

   The **Import Keyboard Macros from** dialog appears.
2. Go location of the macro file and click the macro file (`.xml`).
3. Click **Open** to import the macro.

   If the import fails, an error dialog appears and a message regarding why the import failed is displayed. Select **OK** to continue the import without importing the macros that cannot be imported.
4. Select the macros to be imported by ticking their corresponding checkbox or click **Select All**. To remove all selected macros click **Deselect All**.
5. Click **OK** to begin the import.

   5.1. If a duplicate macro is found, the **Import Macros** dialog appears. Do one of the following:
   - Click **Yes** to replace the existing macro with the imported version.
   - Click **Yes to All** to replace the currently selected and any other duplicate macros that are found.
   - Click **No** to keep the original macro and proceed to the next macro.
   - Click **No to All** keep the original macro and proceed to the next macro.
     Any other duplicates that are found are skipped as well.
   - Click **Cancel** to stop the import.
   - Alternatively, click **Rename** to rename the macro and import it.
     If **Rename** is selected, the **Rename Macro** dialog appears. Enter a new name for the macro in the field and click **OK**.
     The dialog closes and the process proceeds.
     If the name that is entered is a duplicate of a macro, an alert appears. Enter another name for the macro.

5.2. If during the import process the number of allowed, imported macros is exceeded, a dialog appears.
Click **OK** to attempt to continue importing macros or click **Cancel** to stop the import process.

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

7.1.7 Video

7.1.7.1 Refresh the Screen

➡ Click **Video > Refresh Screen** or click  in the toolbar to force a refresh of the video screen.

7.1.7.2 Screenshot from Target

1. Click **Video > Screenshot from Target…** or click  in the toolbar.
2. In the **Save** dialog, choose the location to save the file, name the file, and select a file format from the **Files of type** drop-down list.
3. Click **Save** to save the screenshot as a bitmap, JPEG or PNG file.

7.1.8 Mouse Options

Operation can be performed in both single mouse mode or dual mouse mode.

When in a dual mouse mode, and provided the option is properly configured, the mouse cursors align. When controlling a target, the remote console displays two mouse cursors - one belonging to the SIRA Module client workstation, and the other belonging to the target.

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

- Absolute (Mouse Synchronization, default)
- Intelligent (Mouse Mode)
- Standard (Mouse Mode) (see chapter 16.2, page 175 to avoid mouse disfunction)

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

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

Single mouse mode allows to view only the target's pointer. Use the single mouse mode when other modes don't work.

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

Recommendations

Mouse setting	Used product
Absolute	Preferred setting for use cases with **R488-BIPHHL** and being directly connected to a source computer.
Single Mouse Cursor	To be configured for **R488-BIPC**, **R488-BIPCR**, **R488-BIPS** and **R488-BIPSR** and when using **R488-BIPHHL** connected to any KVM system.

7.1.8.1 Dual Mouse Modes

7.1.8.1.1 Absolute Mouse Synchronization

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

➡ Choose **Mouse > Absolute**.

7.1.8.1.2 Intelligent Mouse Mode

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

➡ Click **Mouse > Intelligent**.

Intelligent Mouse Synchronization Conditions

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

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

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

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

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

7.1.8.1.3 Standard Mouse Mode

Standard Mouse mode uses a standard mouse synchronization algorithm. The algorithm determines relative mouse positions on the client and target. For the client and target mouse cursors to stay in synch, mouse acceleration must be disabled. Additionally, specific mouse parameters must be set correctly.

➡ Click **Mouse > Standard** to enter Standard mouse mode.

See source computer settings from chapter 16.2, page 175 to avoid mouse disfunction.

7.1.8.1.4 Synchronize Mouse

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

To synchronize the mouse cursors, proceed as follows:

➡ Click **Mouse > Synchronize Mouse** or click in the toolbar.

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

7.1.8.1.5 Mouse Synchronization Tips

If there is an issue with mouse synchronization:

1. Verify that the selected video resolution and refresh rate are among those supported by the device. The client **Connection Info** dialog displays the actual values that the device is seeing.
2. If that does not improve the mouse synchronization (for Linux KVM targets):
   2.1. Open a terminal window.
   2.2. Enter the following command: `xset mouse 1 1`.
   2.3. Close the terminal window.
   2.4. Click **Mouse > Synchronize Mouse** or click in the toolbar.

7.1.8.1.6 Cursor Shape

In dual mouse modes, a custom cursor shape can be defined for the session. To make the cursor selection permanent, see chapter 7.1.9.2, page 55).

To change the cursor shape, proceed as follows:

➡ Click **Mouse > Cursor Shape**, then select from the list.

- Default arrow
- Dot
- Crosshair
- Transparent

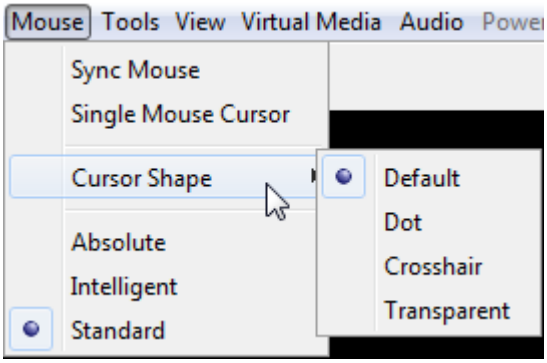


*Fig. 31 VKCS **Mouse - Cursor Shape***

7.1.8.2 Single Mouse Mode

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

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

Activate Single-Mouse Cursor

➡ Click **Mouse > Single-Mouse Cursor** or click in the toolbar.

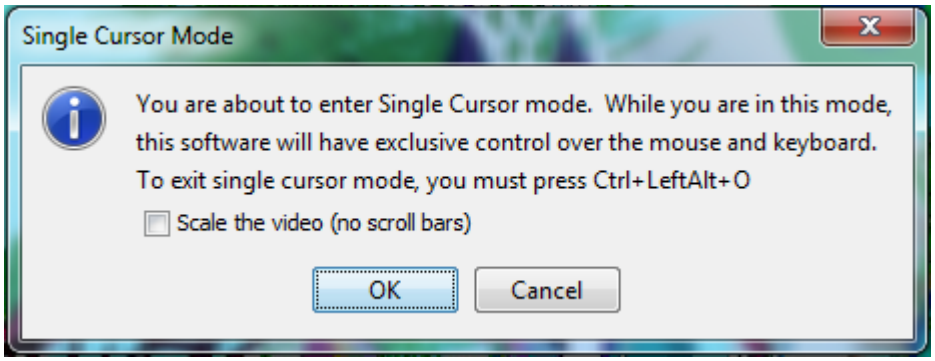


*Fig. 32 VKCS **Mouse - Single Mouse Cursor - Message***

Exit Single-Mouse Cursor

➡ Press Ctrl+Alt+O to exit single mouse mode.

7.1.9 Tool Options

7.1.9.1 General Settings

OpenGL rendering of scaled KVM images is enabled by default.

Only available in AKC: If there are performance issues, tick the **Disable Hardware Accelerated Rendering** checkbox to disable the hardware accelerated rendering.

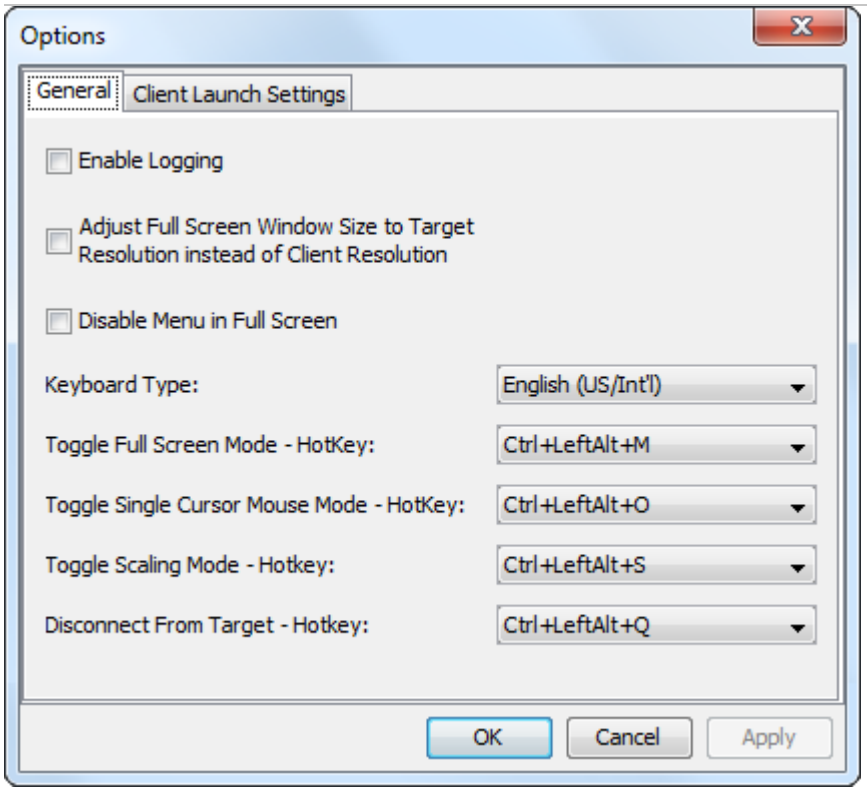


*Fig. 33 VKCS **Tools - Options - General***

These functions can be configured:

Function	Description and options
Enable Logging	Creates a log file in the home directory
Adjust Full Screen Window Size to Target Resolution instead of Client Resolution	Client starts in full screen in a window equal to the target's resolution, not the resolution of the client monitor. If using a multi-monitor client, a full-screen window may cover more than one monitor (see chapter 7.1.9.1.2, page 54). **Note:** Option not available for Linux clients.

Function	Description and options		
Keyboard Type	Keyboard limitations, see chapter 7.1.9.1.1, page 54. **Note:** In AKC, the keyboard type defaults to the local client, so this option does not apply. • US/International • French (France) • German (Germany) • Japanese • United Kingdom • Korean (Korea) • French (Belgium) • Norwegian (Norway) • Portuguese (Portugal) • Danish (Denmark) • Swedish (Sweden) • German (Switzerland) • Hungarian (Hungary) • Spanish (Spain) • Italian (Italy) • Slovenian • Translation: French - US • Translation: French - US International		
Client Hotkey	Ctrl+LeftAlt+M	Toggle Full Screen Mode	Used for toggling in and out of this mode (see chapter 7.1.3.3.4, page 40).
	Ctrl+LeftAlt+O	Toggle Single Mouse Cursor Mode	Used to toggle in and out of single cursor mode, removing and bringing back the client mouse cursor (see chapter 7.1.8.2, page 51).
	Ctrl+LeftAlt+S	Toggle Scale Video Mode	Used for toggling in and out of this mode (see chapter 7.1.3.3.3, page 40).
	Ctrl+LeftAlt+Q	Disconnect from Target	Used to quickly disconnect from the target while closing the client.

To set the tools options, proceed as follows:

1. Click **Tools > Options**.

   The **Options** dialog appears.
2. Tick the **Enable Logging** checkbox only if directed to by Technical Support.
3. Tick the **Adjust Full Screen Window Size to Target Resolution instead of Client Resolution** checkbox if preferred.
4. In Mac OS/VKCS launches only, **Let Full Screen Window Cover the Main Menu Bar** and the Dock is enabled by default. Use this setting to prevent the Java menu bar from hiding the VKCS menu bar when running VKCS in full-screen mode on Mac.
5. Choose the **Keyboard Type** from the drop-down list if necessary.
6. Select the desired Client Hot Key.

   For Client Hot Key combinations, the application does not allow to assign the same Client Hot Key combination to more than one function.

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

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

7. Click **OK**.

7.1.9.1.1 Keyboard Limitations

Turkish Keyboards

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

Slovenian Keyboards

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

Language Configuration on Linux

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

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

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

7.1.9.1.2 Adjust Full Screen Window Size to Target Resolution

When **Adjust Full Screen Window Size to Target Resolution instead of Client Resolution** is enabled, the client starts in full screen in a window equal to the target's resolution, not the resolution of the client monitor. If using a multi-monitor client, a full-screen window may cover more than one monitor. See chapter 7.1.9.1, page 52 for instructions on enabling the setting.

Example:

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

1	2	3	4
5	6	7	8

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

7.1.9.2 Client Launch Settings

The screen settings for a KVM session can be configuring in this menu.

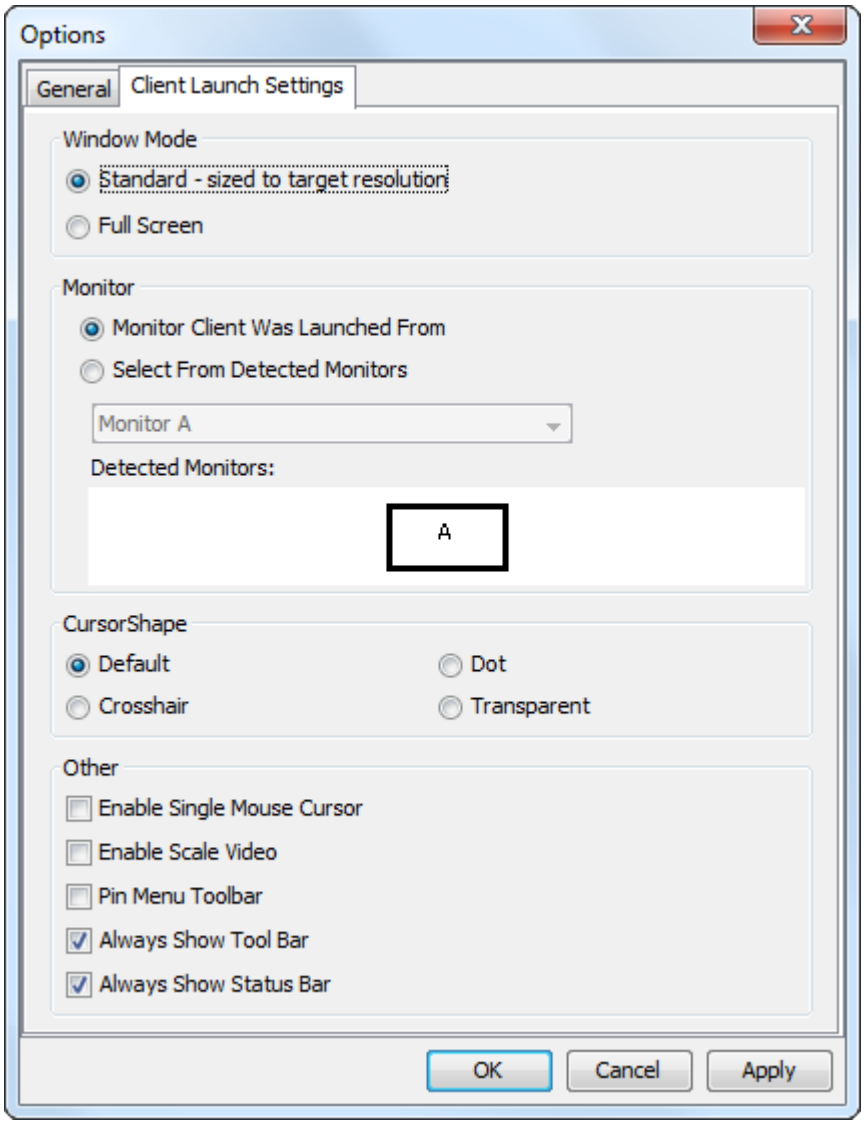


*Fig. 34 VKCS **Tools - Options - Client Launch Settings***

To configure client launch settings, proceed as follows:

1. Click **Tools > Options**.

   The **Options** dialog appears.
2. Click on the **Client Launch Settings** tab.
3. To configure the target window settings:
   - 3.1. Select **Standard - sized to target resolution** to open the window using the target's current resolution. If the target resolution is greater than the client resolution, the target window covers as much screen area as possible and scroll bars are added (if needed).
   - 3.2. Select **Full Screen** to open the target window in full screen mode.
4. To configure the monitor display:
   - 4.1. Select **Monitor Client Was Launched From** if the target viewer is to be launched using the same display as the application that is being used on the client (for example, a web browser or applet).
   - 4.2. Use **Select From Detected Monitors** to select from a list of monitors that are currently detected by the application. If a previously selected monitor is no longer detected, a message **Currently Selected Monitor Not Detected** is displayed.

5. To configure cursor shape:
   5.1. Select **Default**, **Dot**, **Crosshair**, or **Transparent** to set the cursor shape for all sessions. Use the **Mouse** menu to change the cursor shape during a session.
6. To configure additional launch settings:
   6.1. Tick the **Enable Single Cursor Mode** checkbox to enable single mouse mode as the default mouse mode when the server is accessed.
   6.2. Tick the **Enable Scale Video** checkbox to automatically scale the display on the target when it is accessed.
   6.3. Tick the **Pin Menu Toolbar** checkbox if the toolbar should remain visible on the target when it is in Full Screen mode. By default, while the target is in Full Screen mode, the menu is only visible when hovering the mouse along the top of the screen.
   6.4. **Always Show Tool Bar** and **Always Show Status Bar** are per-user settings that are stored in the computer the client is accessed from. If using another computer, the setting may be different. Select to keep tool bar and status bar visible as default, deselect to keep tool bar and status bar hidden as default.
7. Click **OK**.

7.1.9.3 Collecting a Diagnostic Snapshot of the Target

Administrators are able to collect a snapshot of a target.

The **Snapshot of a Target** function generate log files and image files from the target. These files are bundled in a zip file that can be sent to Technical Support to help diagnose technical problems if encountering.

The following files are included in the zip file:

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

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

To collect a Diagnostic Snapshot, proceed as follows:

1. Connect to a target.
2. Click **Tools > Collect a Diagnostic Snapshot**.
   Several messages are displayed as the information is collected.
3. In the **Save** dialog, choose the location to save the file, name the file.
4. Click **Save**.
   The zip file containing the diagnostic files is saved.

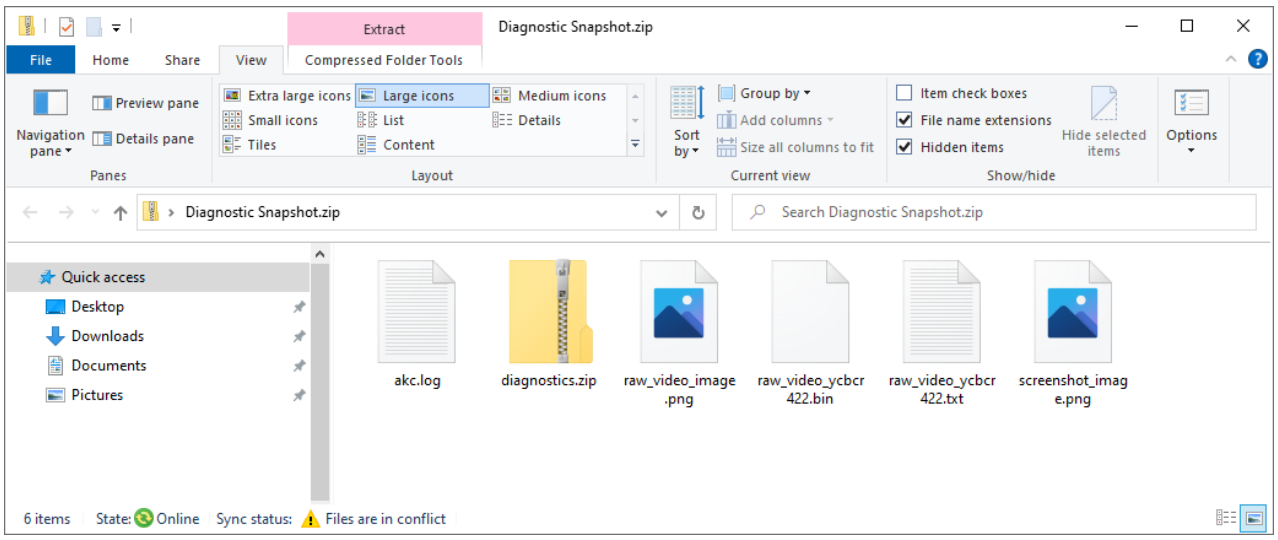


*Fig. 35 VKCS **Tools - Options - Client Launch Settings***

7.1.10 Virtual Media

7.1.10.1 Access a Virtual Media Drive on a Client Computer

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

To access a virtual media drive on the client computer, proceed as follows:

1. Click **Virtual Media > Connect Drive** or click in the toolbar.

   The Map Virtual Media Drive dialog appears.

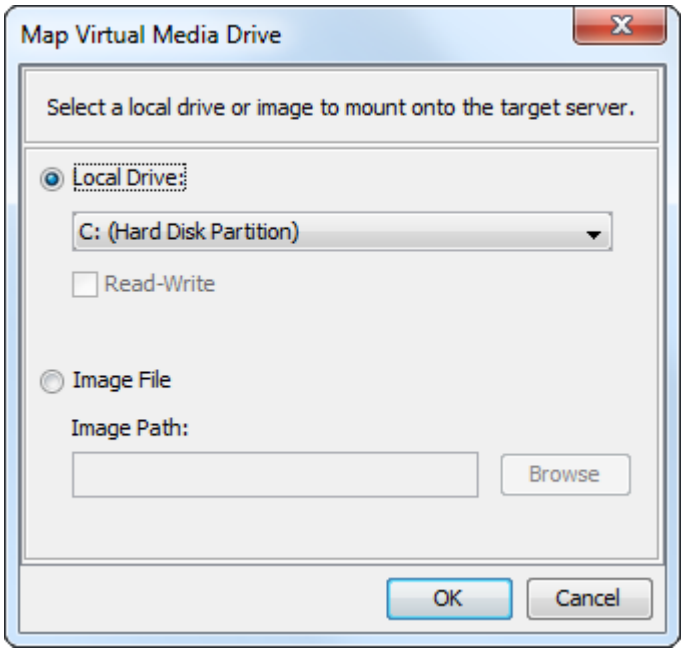


*Fig. 36 VKCS **Virtual Media - Map Virtual Media Drive***

2. Select the drive from the **Local Drive** drop-down list.
3. Tick the **Read-Write** checkbox if Read and Write capabilities are necessary.

   When checked, the connected USB disk is permitted to read or write.

   This option is disabled for nonremovable drives (see chapter 14.7, page 170) for more information.

NOTICE
Possible data corruption Enabling Read/Write access can be critical. Simultaneous access to the same drive from more than one entity can result in data corruption. ➡ Leave this option unselected if Write access is not required.

4. Click **OK**.

   The media will be mounted on the target virtually. The media is accessible just like any other drive.

7.1.10.2 Access a Virtual Media Image File

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

Image File Guidelines

- Image files created using dd on Linux (dd if=/dev/sdb of=disk.img) or similar tools such as Win32DiskImager on Windows, or Mac Disk Utility are supported.
- Apple DMG files:
  - DMG image files of a FAT32 USB drive are recognized on all OSs.
  - DMG images files of a folder on a Mac Drive are recognized only on Mac OS targets.
  - Image should be created via Mac Disk Utility using the following settings: Encryption: None; Image format: read/write.
  - Not supported: Encrypted or compressed dmg images, MacOS install images, DMG files downloaded from the Apple support site.

To access a virtual media image file, proceed as follows:

1. Click **Virtual Media > Connect Drive** or click  in the toolbar.
   The **Map Virtual Media Drive** dialog appears.

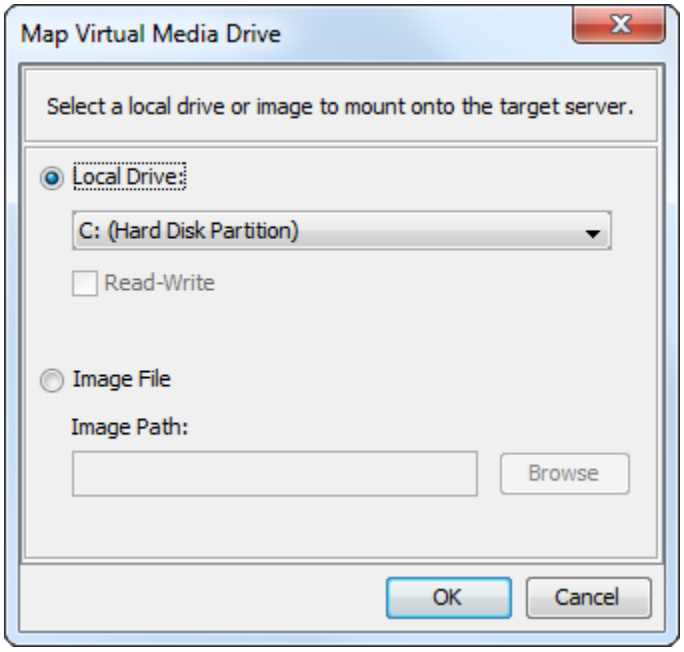


*Fig. 37 VKCS **Virtual Media - Map Virtual Media Drive***

2. Select the **Image File** option.
3. Click **Browse** to find and select the `.img` or `.dmg` file.
4. Click **OK**.
   The media will be mounted on the target virtually.

7.1.10.3 Mounting CD-ROM/DVD-ROM/ISO Images

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

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

To access a CD-ROM, DVD-ROM, or ISO image, proceed as follows:

1. Click **Virtual Media > Connect CD-ROM/ISO Image** or click in the toolbar.
   The Map Virtual Media CD/ISO Image dialog appears.

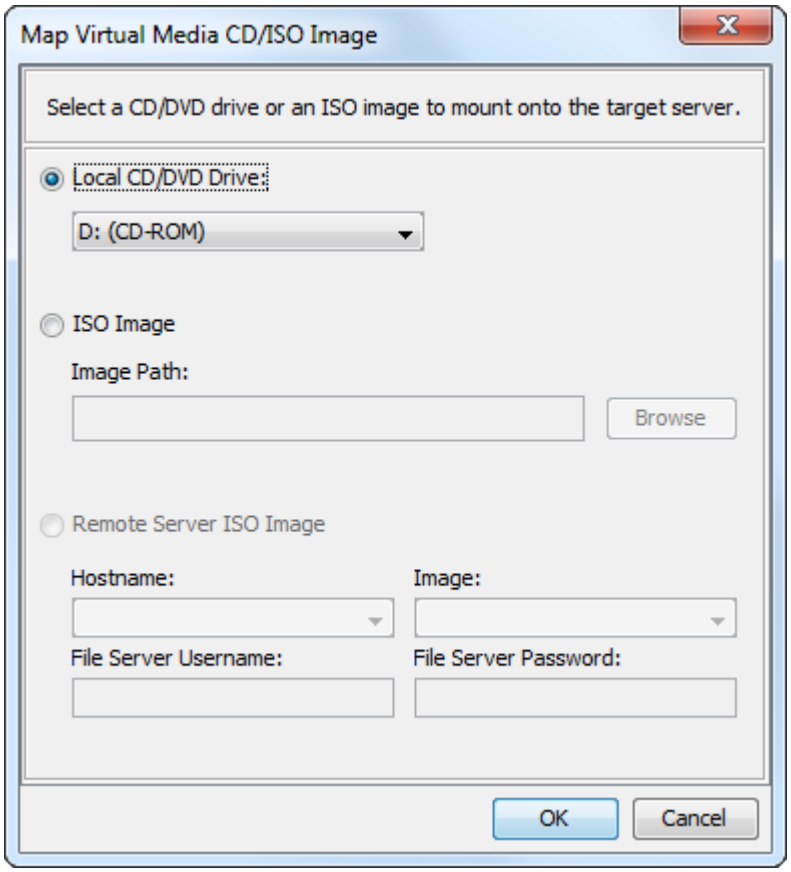


*Fig. 38 VKCS **Virtual Media - Map Virtual Media CD/ISO Image***

2. For internal and external CD-ROM or DVD-ROM drives:
   2.1. Select the **Local CD/DVD Drive** option.
   2.2. Select the drive from the **Local CD/DVD Drive** drop-down list.
   All available internal and external CD and DVD drive names will be populated in the drop-down list.
   2.3. Click **OK**.
3. For ISO images:
   3.1. Select the **ISO Image** option.
   Use this option when to access a disk image of a CD, DVD, or hard drive. ISO format is the only format supported.
   3.2. Click **Browse**.
   3.3. Navigate to the path containing the disk image to be use.
   3.4. Click **Open**.
   The path is populated in the **Image Path** field.

3.5. Click **OK**.

4. For remote ISO images on a file server:

4.1. Select the **Remote Server ISO Image** option.

4.2. Select **Hostname** and **Image** from the drop-down list.

The file servers and image paths available are those that have been configured using the **Virtual Media Shared Images** menu (see chapter 10.6, page 125). Only configured items using the **Virtual Media Shared Images** menu will be in the drop-down list.

4.3. **File Server Username** - User name required for access to the file server. The name can include the domain name such as mydomain/username.

4.4. **File Server Password** - Password required for access to the file server (field is masked as you type).

4.5. Click **OK**.

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

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

If you are using the Windows 7 operating system, **Removable Disk** is not displayed by default in the Window's **My Computer** folder when mounting a Local CD/DVD Drive or Local or Remote ISO Image.

➡ To view the Local CD/DVD Drive or Local or Remote ISO Image in this folder, select in the Windows Explorer **View > Options > Change folder and search options > View** and deselect **Hide empty drives**.

7.1.10.4 Disconnect from Virtual Media Drives

To disconnect the virtual media drives, proceed as follows:

- For local drives, click **Virtual Media > Disconnect Drive** in the menu bar.
- For CD-ROM, DVD-ROM, and ISO images, click **Virtual Media > Disconnect CD-ROM/ISO Image**.
- Simply closing the KVM connection closes the virtual media as well.

7.1.11 Digital Audio

The SIRA Module supports audio playback over HDMI.

7.1.11.1 Supported Audio Device Formats

The following playback formats are supported:

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

7.1.11.2 Digital Audio Icons

These icons are located in the status bar at the bottom of the client window:

Icon name	Audio icon	Description
Speaker		Green, blinking waves indicate an audio playback session is currently streaming.
		A black speaker icon is displayed when the session is muted.
		The icon is grayed out when no audio is connected
Microphone		Playback is not supported. Microphone icon appears grayed out.

7.1.11.3 Audio Playback Recommendations and Requirements

Audio level

➔ Set the target audio level to a mid-range setting. For example, on a Windows client, set the audio to 50 % or lower.

This setting must be configured through the playback device, not from the client audio device control.

7.1.11.4 Bandwidth Requirements

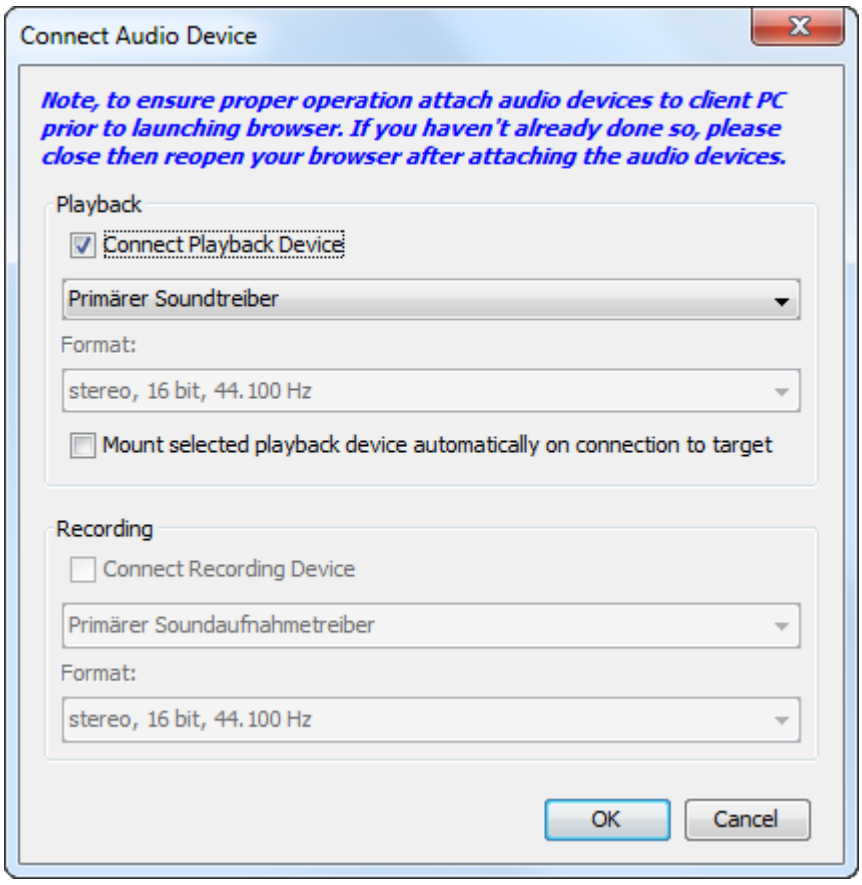


*Fig. 39 VKCS **Connect Audio Device***

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

Audio format	Network bandwidth requirement
Stereo, 16 bit, 44.1 kHz	176 kB/s
Stereo, 16 bit, 32 kHz	128 kB/s
Stereo, 16 bit, 48 kHz	192 kB/s

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

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

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

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

- Connect audio playback at the lower quality formats. The impact of video consuming bandwidth is much less notable at 11 kHz connections than at 44 kHz.
- Set the connection speed under **Connection Properties** (see chapter 7.1.3.3, page 40) to a value that best matches the client to server connection.
- Set the color depth under **Connection Properties** to as low a value as possible. Reducing the color depth to 8 bit color considerably reduces the bandwidth consumed.

7.1.11.5 Saving Audio Settings

Audio device settings are set individually for each SIRA Module device. Once the audio devices settings are configured and saved on the SIRA Module, the same settings are applied to it.

For example, a Windows audio device is configured to be used as stereo, 16 bit, 44.1 kHz format. When you connect to different targets and use that Windows audio device, the stereo, 16 bit, 44.1 kHz format is applied to each target.

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

See chapter 7.1.11.8, page 64 for information audio settings.

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

7.1.11.6 Connect to a Digital Audio Device

To connect to an audio device, proceed as follows:

1. Connect the audio device to the remote client computer prior to launching the browser connection to the SIRA Module.
2. Connect to the target from the **Port Access** page of the SIRA Module configuration menu.
3. Once connected, click **Audio > Connect Audio** or click  in the toolbar.

   The **Connect Audio Device** dialog appears. A list of available audio devices connected to the remote client PC is displayed.
   If there are no available audio devices connected to the remote client computer, the **Audio** icon is grayed out.
4. Tick the **Connect Playback Device** checkbox to connect to a playback device.
5. Select the device to be connected from the drop-down list.

6. Select the audio format for the playback device from the **Format** drop-down list.

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

7. Tick the **Mount selected playback device automatically on connection to target** checkbox to automatically connect an audio playback device when connecting to an audio supporting target.
8. Click **OK**.

   If the audio connection is established, a confirmation message appears.
9. Click **OK**.

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

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

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

7.1.11.7 Disconnect from an Audio Device

To disconnect from an audio device, proceed as follows:

1. Click the Audio icon in the toolbar.
2. Select **OK** when you are prompted to confirm the disconnect.

   A confirmation message appears.
3. Click **OK**.

7.1.11.8 Adjusting Audio Settings

Once an audio device is connected, the buffer size can be adjusted as needed. This feature is useful for controlling the quality of the audio, which may be impacted by bandwidth limitations or network spikes.

Increasing the buffer size improves the audio quality but may impact the delivery speed. The maximum available buffer size is 400 milliseconds since anything higher than that greatly impacts audio quality.

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

Audio settings are configured in VKCS or AKC.

To adjust audio settings, proceed as follows:

1. Select **Audio Settings** from the Audio menu.

   The **Audio Settings** dialog opens.
2. Adjust the **Capture Buffer Size** and/or **Playback Buffer Size** as needed.
3. Click **OK**.

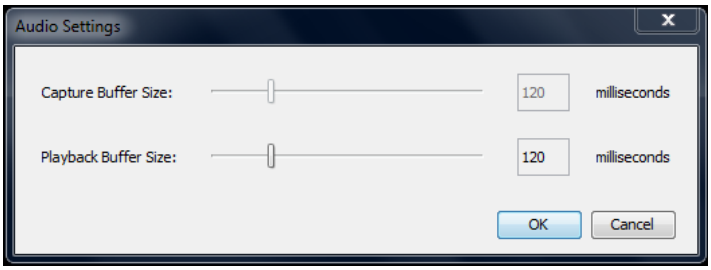


*Fig. 40 VKCS **Audio - Audio Settings***

7.1.12 Client Hotkeys

Important **Quick-Hotkeys** improving usability outside the dock are:

Client Hotkey	Description
Ctrl+LeftAlt+M	Toggles between FullScreen mode and Window mode.
Ctrl+LeftAlt+O	Toggles between single mouse mode and normal mouse mode.
Ctrl+LeftAlt+S	Toggles image scaling.
Ctrl+LeftAlt+Q	Disconnects from target and closes the client session.

7.1.13 Version Information

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

➡ Choose Help > About IHSE SIRA Client.

7.2 Active KVM Client (AKC) Help

The Client does not require an installation routine. No admin rights are required.

➡ For accessing the SIRA Module via Internet only TCP/IP Ports 80 and 443 are required.

AKC will load and launch automatically when the link is clicked.

➡ To launch AKC, enter https://IP address/akc in a browser.

7.2.1 Features

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

- Keyboard macros created in AKC cannot be used in any other client.
- Direct port access configuration
- AKC server certification validation configuration (see chapter 7.2.3, page 66)

For details on configuring and using the features, see Virtual KVM Client Stand-alone (VKCS) Help (see chapter 7.1, page 36).

7.2.2 Prerequisites for Using AKC

Prerequisites	Description
Cookies	Ensure the cookies from the IP address of the device that is being accessed are not currently being blocked.
Trusted Sites Zone	As Windows 7 user ensure that the IP address of the device being accessed is included in the browser's Trusted Sites Zone.
Protected Mode	As Windows 7 user ensure that Protected Mode is not on when accessing this device.
ClickOnce for Edge Chromium browser	The new Edge Chromium browser 86.0.622.51 has experimental ClickOnce support which must be enabled for AKC. ➡ To enable ClockOnce, enter edge://flags in the browser, search for ClickOnce support, set to enabled and restart the browser.

7.2.3 Proxy Server Configuration

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

If the installed proxy server is only capable of the HTTP proxy protocol, connection is not possible.

To configure the SOCKS proxy, proceed as follows:

1. On the remote client PC, select **Control Panel > Internet Options**.
   1.2. Click **LAN Settings** on the **Connections** tab.
   The **Local Area Network (LAN) Settings** dialog opens.
   1.3. Select **Use a proxy server for your LAN**.
   1.4. Click **Advanced**.
   The **Proxy Settings** dialog opens.
   1.5. Configure the proxy servers for all protocols.

NOTICE
➡ Do not select **Use the same proxy server for all protocols**.

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

   1.6. Click **OK** at each dialog to apply the settings.
2. Next, configure the proxy settings for the Java applets:
   2.1. Select **Control Panel > Java**.
   2.2. Click **Network Settings** on the **General** tab.
   The **Network Settings** dialog opens.
   2.3. Select **Use Proxy Server**.
   2.4. Click **Advanced**.
   The **Advanced Network Settings** dialog opens.
   2.5. Configure the proxy servers for all protocols.

NOTICE
➡ Do not select **Use the same proxy server for all protocols**.

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

7.2.4 Download and Launch

If the browser will not detect support for ClickOnce, so it is required to download AKC manually.

To download AKC manually, proceed as follows:

1. Go to the SIRA Module URL, for example https://192.168.100.88/24/akc (default IP address).
   The message **Your connection isn't private** may appear.
2. Click **Advanced**.
3. Click **Continue to IP-address (unsafe)**.
4. Select **Click here** on the message showing that ClickOnce support has not been detected.
   The message **Open this file?** appears.
5. Click **Open**.

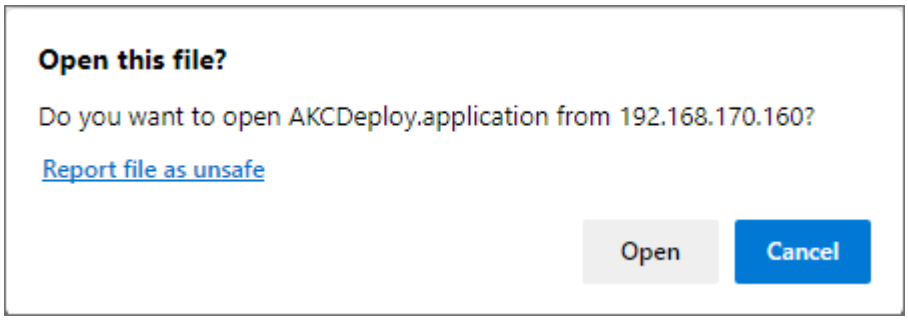


Fig. 41 AKC - Download - Message

6. If **Security Alerts** appear, click **Yes**.
   A login dialog appears.
7. Enter the username and the password (default: admin/admin).
   The Active KVM Client (AKC) is loaded.

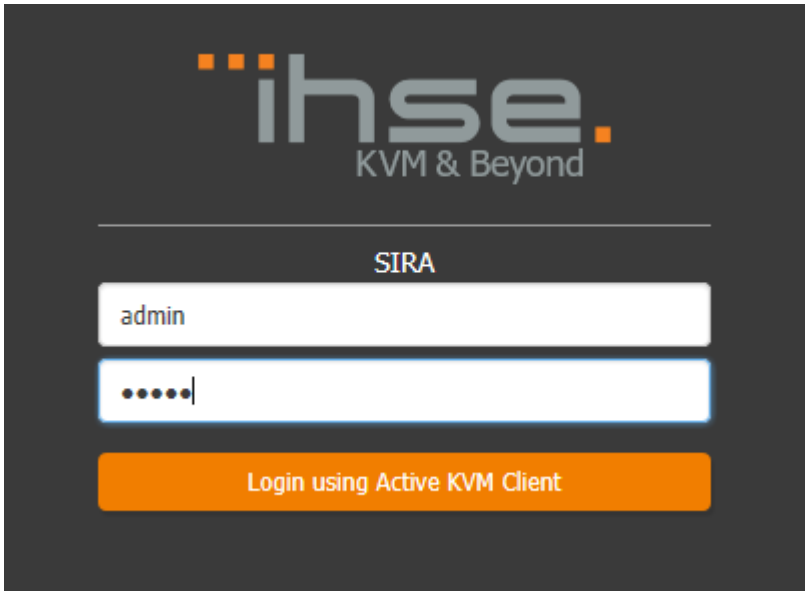


Fig. 42 AKC login dialog

7.2.5 Download and Launch

If receiving a `.zip` file from the manufacturer's technical support, a desktop shortcut can be used for easy access with Windows operating systems via AKC.

To install a desktop shortcut, proceed as follows:

1. Please unzip the `SIRA – Client.ZIP` file to the desktop (or any other directory).
2. Open the directory `SIRA – Client` and create a link to `kxgui.exe`.
3. Move this link straight onto the desktop and rename it to `SIRA`.
4. Now open the properties window of that link 

with a right mouse click.

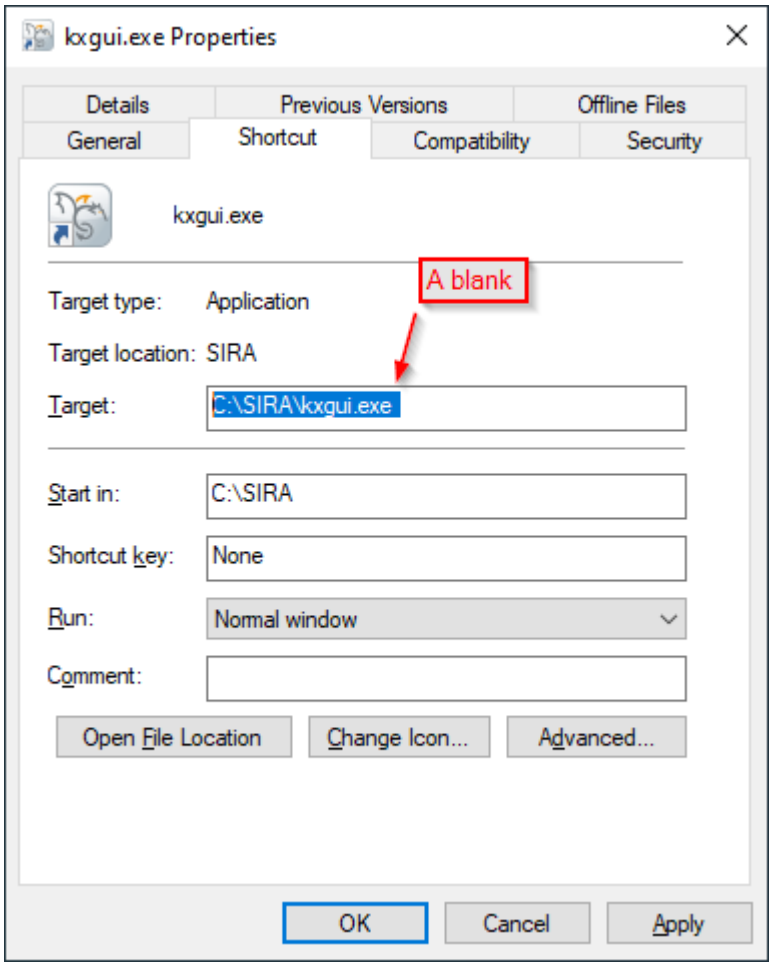


Fig. 43 AKC Properties Window - Shortcut

5. Copy the following string into the **Target** line at the end after `…\kxgui.exe` inclusive the blank after `…\kxgui.exe` .
6. For use with your personal SIRA Gateway simply replace the IP address and port number and the credentials as required. Access to a factory default unit would look as follows:

   "\\Directory of unzipped SIRA Resource Files\kxgui.exe" /host 192.168.100.88 /port 443 /ssl false /username admin /password admin /portid 1 /portname "Port 1"
7. Close the properties window and start the session via double click.

7.3 HTML KVM Client (HKC)

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

Supported features	Not supported features
• Connection properties • Input settings • Audio playback • Virtual media (except writing) • Keyboard support for US-English, UK-English, French, and German • Keyboard macros • Import and export of keyboard macros • Send text to target • Keyboard and mouse settings • Single mouse mode within all browsers (except Internet Explorer) • Local file transfer supported by Chrome and Firefox browsers only	• Video settings • Tools menu for setting client launch settings, setting disconnect from target hotkey, or configuring toolbar display. • Limited keyboard support (see left column) • Hotkeys for keyboard macros • Pre-populated keyboard macros for Sun targets • Can only create macros from keys that exist on the client PC (US-English, UK-English, French, or German), no special function keys • Single mouse mode not available on IE • Virtual media write not supported • USB drive connects • Audio capture

If HKC does not load, but rather displays a white screen, the browser memory may be full.

➡ Close all browser windows and try again.

7.3.1 Connection Properties

Connection properties manage streaming video performance over remote connections to targets. Additionally, it shows the current signal details such as framerate and used transmission bandwidth.

The properties are applied only to the own connection. They do not impact the connection of other users accessing the same targets. Changes of connection properties are retained by the client.

➡ Click **File > Connection Properties…** to open the **Connection Properties** menu.

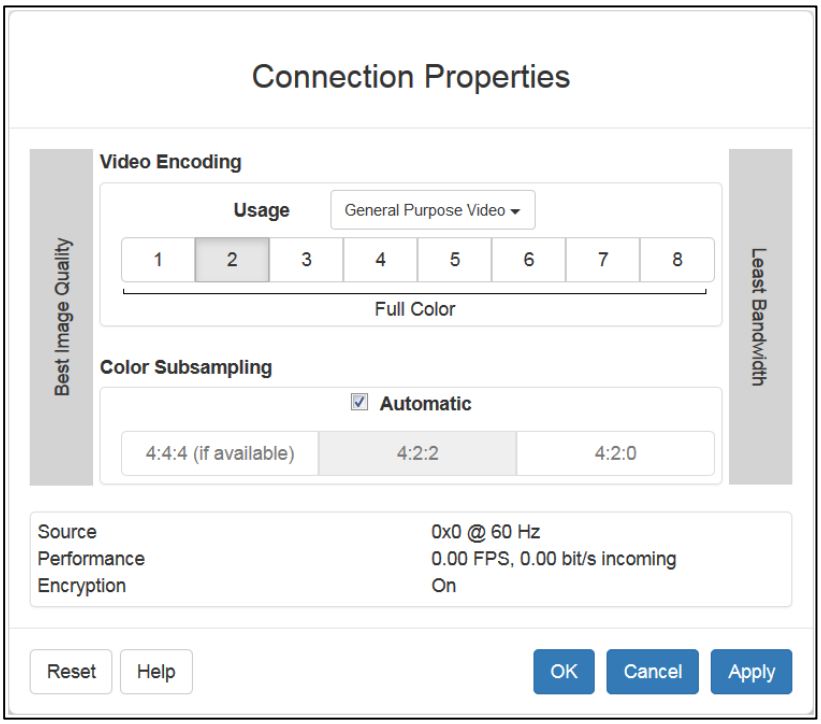


*Fig. 44 HKC **Connection Properties***

Video Encoding

This section selects the video encoding algorithm and quality setting.

- **Usage**: specify your general application area. This selection optimizes the available choices elsewhere in this dialog.
  - General Purpose Video: video content where smooth color reproduction is most important, such as movies, video games, and animations.
  - Computer and IT Applications: video content where text sharpness and clarity are important, such as computer graphical interfaces.
- **Encoder Mode**: Choose the encoder mode from the row of eight buttons. Options will vary depending on the **Usage** selection. In general, modes towards the left of the button bar offer higher image quality but consume higher bandwidth and might cause frame rate to drop depending on network speed and/or client performance. Modes towards the right consume lower bandwidth at the cost of reduced image quality. In network- or client-constrained situations, modes towards the right may achieve better frame rates.
  The default video mode is always **Full Color 2**, which is a high-quality mode and works well for most uses in LAN environments. If needed, experiment with modes further towards the right to find the right balance of image quality and frame rate.

Color Subsampling

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

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

Current Status

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

- **Source**: resolution and frame rate of the incoming video source.
- **Performance**: frames per second (FPS) being rendered in the client, and the data rate of the incoming video stream. These values are where you will see the effects of your video settings.
- **Encryption**: whether the video stream is encrypted or not. Encrypted streams usually have lower frame rates and lower bandwidth. Encryption is a global setting in security. Tick the **Apply Encryption Mode to KVM and Virtual Media** checkbox under **Security > KVM Security** (see chapter 12.3, page 152).

7.3.2 Connection Info

1. Click **File > Connection Info**.

   The **Connection Info** dialog appears with real-time connection information on the current connection.
2. Copy the information from the dialog to the clipboard as needed.
3. To edit the connection properties, see chapter 7.3.1, page 70).

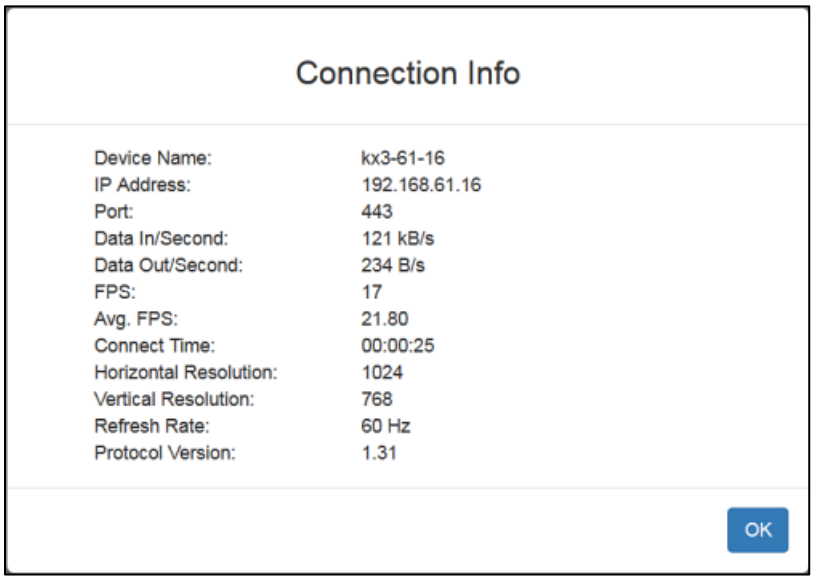


*Fig. 45 HKC **Connection Info***

See Default Connection Properties for help configuring the connection properties.

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

7.3.3 Input Menu

7.3.3.1 Keyboard Layout

To send a keyboard type, proceed as follows:

➡ Click **Input > Keyboard Layout**, then select your keyboard type.

- de-de
- de-ch
- en-gb
- en-us
- fr

7.3.3.2 Send Macro

Due to frequent use, several keyboard macros are preprogrammed.

To send a preprogrammed macro, proceed as follows:

➡ Click **Input > Send Macro**, then select the macro:

- **Ctrl+Alt+Del**: Sends the key sequence to the target without affecting the client.
- **Alt+F4**: Closes a window on a target.
- **Alt+Tab**: Switch between open windows on a target.
- **Print Screen**: Take a screenshot of the target.

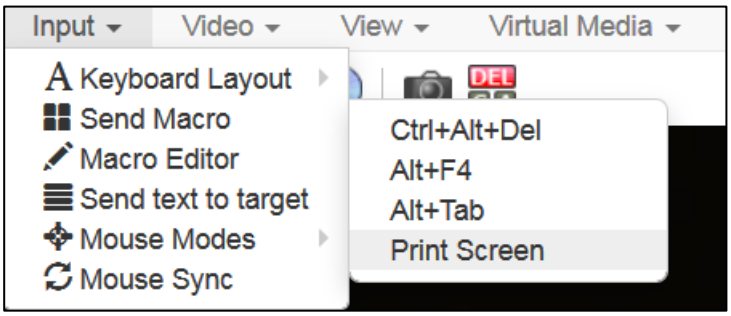


*Fig. 46 HKC **Input - Send Macro - Macro selection***

7.3.3.3 Macro Editor

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

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

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

Macros created with HKC are only available with the current browser and KVM device. If you use HKC in more than one browser, or more than one SIRA Module, your macros will only be available on the browser and SIRA Module where they were created. To reuse your macros in another SIRA Module device, you can import and export the macro files. See ***Import and Export Macros*** (on page 76).

To view the key combination of an existing macro, proceed as follows:

1. Click **Input > Macro Editor**.

   The **Macro Editor** dialog appears
2. Select a macro from the **Macros** list to view the key combination.

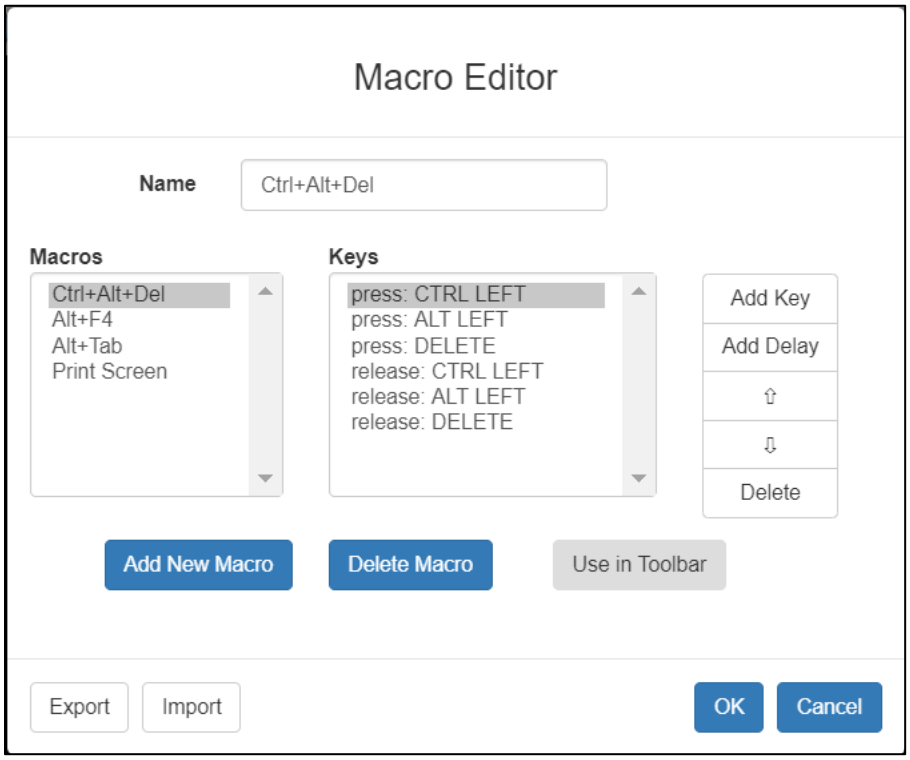


*Fig. 47 HKC **Macro Editor - View key combination of existing macro***

7.3.3.3.1 Add New Macro

To add a new macro, proceed as follows:

1. Click **Input > Macro Editor**.

   The **Macro Editor** dialog appears

2. Click **Add New Macro**.

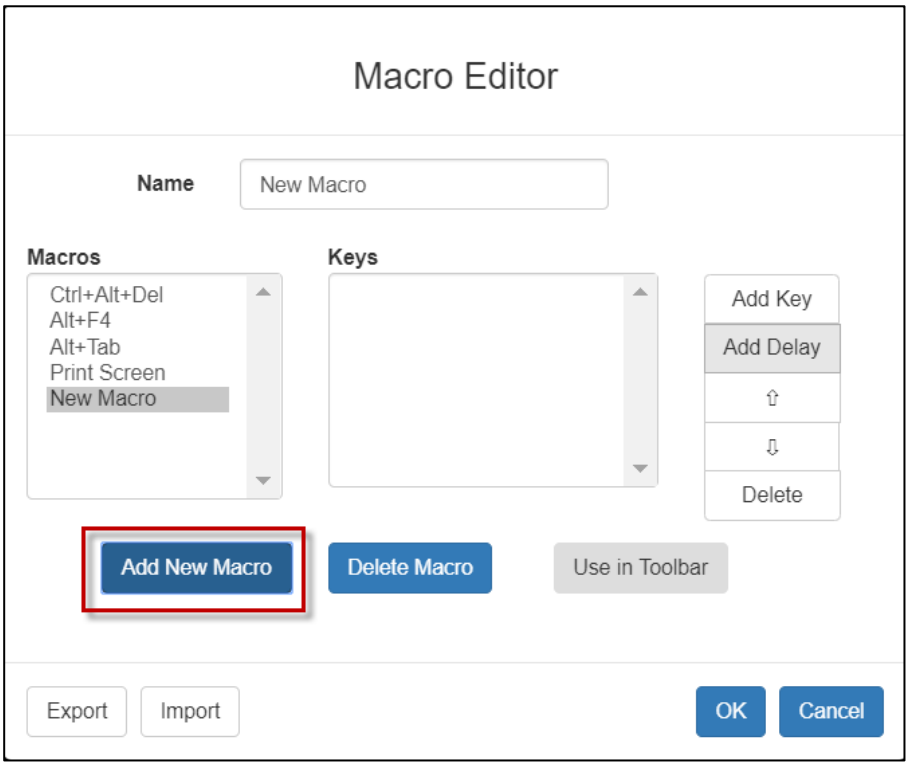


*Fig. 48 HKC **Input - Macro Editor - Add New Macro***

3. Enter a name under **Name** for the new macro.

   The name will appear in the **Send Macro** menu once the macro is saved.

4. Click **Add Key**, then press the key to be added to the macro.

   The key press and key release appear in the **Keys** list.

   4.1. To add more keys, click **Add Key** again, and press another key.

   4.2. To remove a key, select it in the **Keys** list and click **Delete Key**.

5. To put the keys in the correct sequence, click to select a key in the **Keys** list and click ⇧ or ⇩.

6. To add a 500 ms delay to a key sequence, click **Add Delay**. A delay in the middle of a press-and-release key sequence indicates holding down a key. Add multiple delays to indicate a longer press-and-hold of a key. Click ⇧ or ⇩ to move the delays into the correct sequence.

7. Click **OK** to save.

8. To use this macro from your toolbar, click **Use in Toolbar** (see chapter 7.3.3.3.2, page 75).

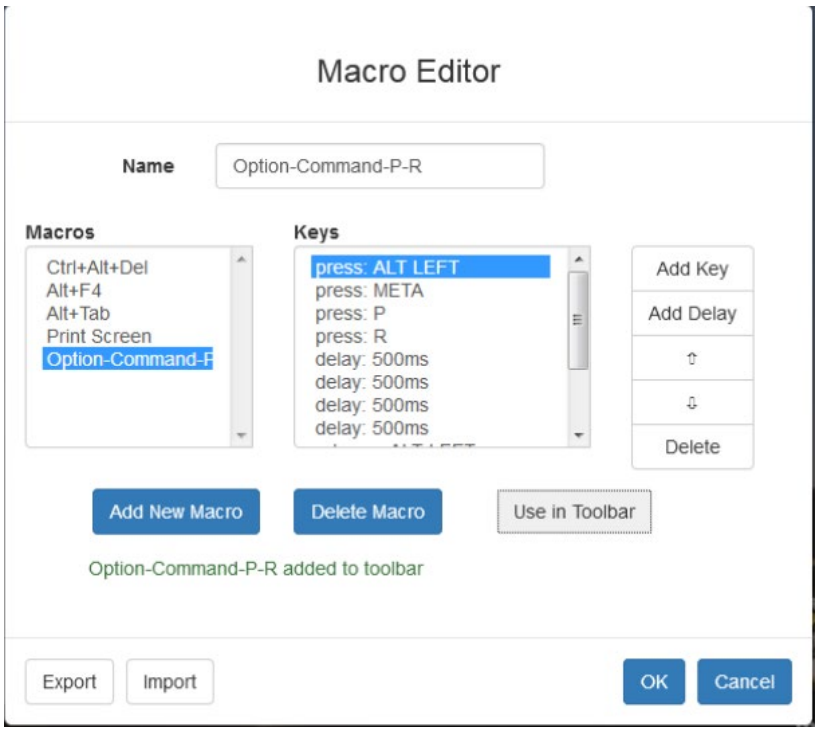


*Fig. 49 HKC **Input - Macro Editor - New macro added***

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

7.3.3.3.2 Add a Macro to the Toolbar

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

To add a macro to the toolbar, proceed as follows:

1. Click **Inputs > Macro Editor**.
2. Select a macro from the **Macros** list.
3. Click **Use in Toolbar**.

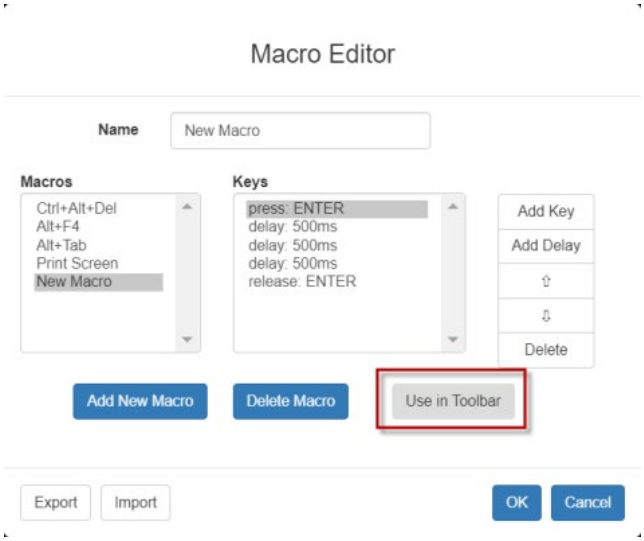


*Fig. 50 HKC **Input - Macro Editor - Use selected macro in Toolbar***

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

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

*Fig. 51 HKC **Toolbar - Macro in Toolbar***

7.3.3.3.3 Delete a Macro

To delete a macro, proceed as follows:

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

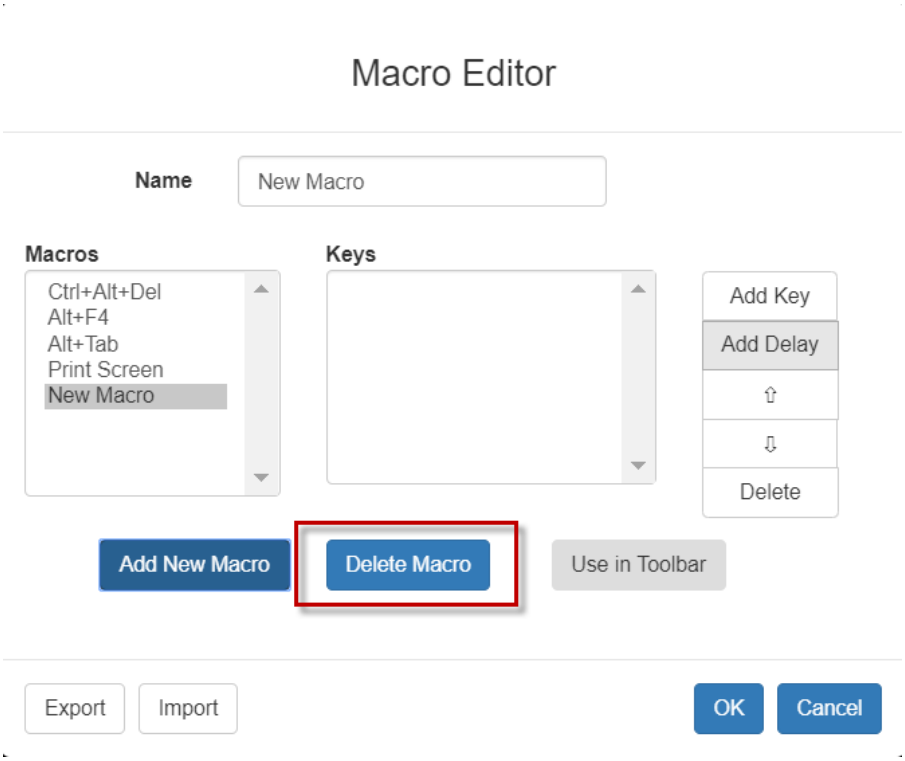


*Fig. 52 HKC **Input - Macro Editor - Delete Macro***

7.3.3.3.4 Import and Export Macros

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

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

To export and import macros:

1. Choose Input > Macro Editor.

   The list of macros created for your browser and SIRA Module displays in the Macro Editor dialog.
2. To export the list, click **Export**, then save the file.
3. Log in to the SIRA Module where you want to import the macros.
4. Click **Input > Macro Editor**.
5. Click **Import**, then click **Open to Import** and select the usermacros.xml file, and click **OK**.

   The macros found in the file display in the list.
6. Select the macros you want to import, then click **OK**.

Macro names must be unique. If a macro with the same name already exists, an error message appears. Click the **Edit** icon to rename the macro, then click the checkmark to save the name.

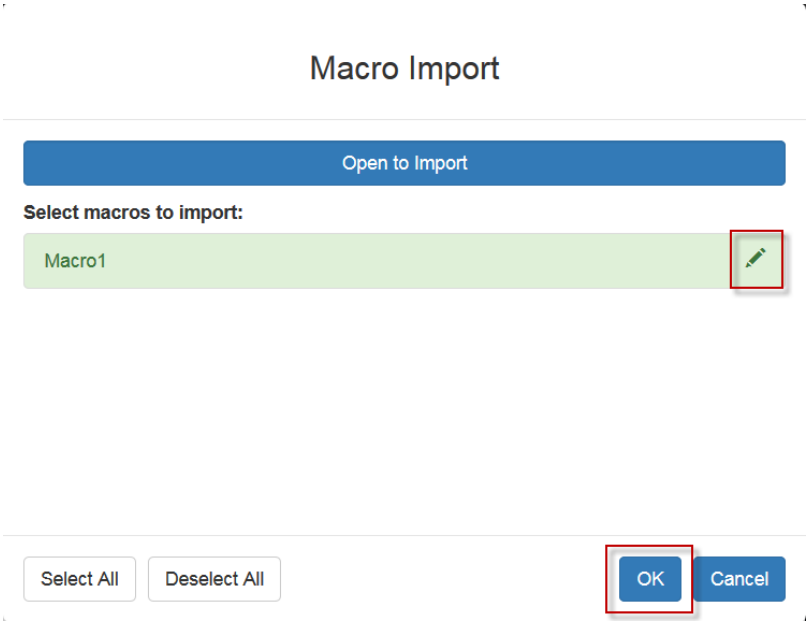


*Fig. 53 HKC **Input - Macro Editor - Import Macro***

7.3.3.4 Send Text to Target

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

To send text to target:

1. Click Input > Send Text to Target.

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

7.3.3.5 Mouse Modes

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

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

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

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

- Absolute (Mouse Synchronization)
- Intelligent (Mouse Mode)
- Standard (Mouse Mode) (see chapter 16.2, page 175 to avoid mouse disfunction)

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

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

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

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

7.3.3.5.1 Absolute

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

➡ Click **Input > Mouse Modes > Absolute**.

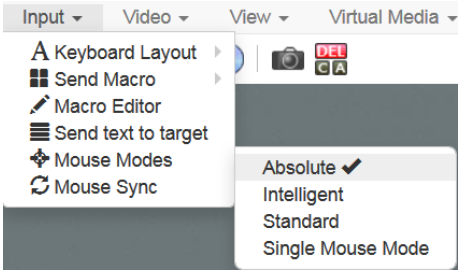


*Fig. 54 HKC **Input - Mouse Modes - Absolute***

7.3.3.5.2 Intelligent

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

➡ Click **Input > Mouse Mode > Intelligent**.

The mouse will synch (see chapter 7.3.3.7, page 80).

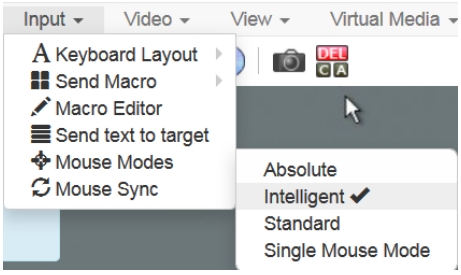


*Fig. 55 HKC **Input - Mouse Modes - Intelligent***

7.3.3.5.3 Standard

Standard Mouse mode uses a standard mouse synchronization algorithm. The algorithm determines relative mouse positions on the client and target. For the client and target mouse cursors to stay in synch, mouse acceleration must be disabled. Additionally, specific mouse parameters must be set correctly.

See source computer settings from chapter 16.2, page 175 to avoid mouse disfunction.

➡ Click **Input > Mouse Modes > Standard**.

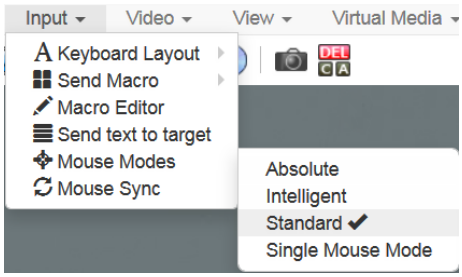


*Fig. 56 HKC **Input - Mouse Modes - Standard***

7.3.3.5.4 Single Mouse Mode

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

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

To enter Single mouse mode:

1. Click **Input > Mouse Modes > Single**.

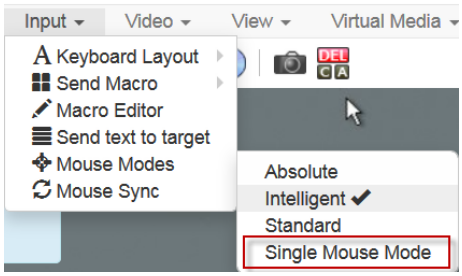


*Fig. 57 HKC **Input - Mouse Modes - Single Mouse Mode***

A message appears at the top of the client window:

2. Press Esc to show your cursor.

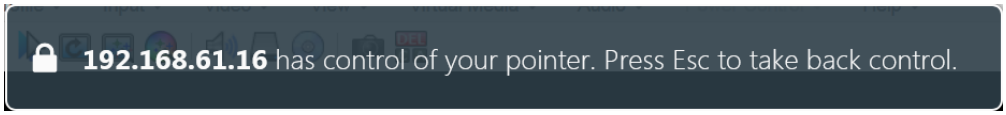


*Fig. 58 HKC **Input - Mouse Modes - Single Mouse Mode - Message***

To exit Single mouse mode:

➡ Press Esc.

Mouse mode changes back to dual mode.

7.3.3.6 Mouse Sync

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

To synchronize the mouse cursors, proceed as follows:

➔ Click **Inputs > Mouse Sync**.

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

7.3.3.7 Intelligent Mouse Synchronization Conditions

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

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

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

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

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

7.3.4 Video Menu

7.3.4.1 Refresh Screen

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

To force a refresh of the video screen:

- Choose Video > Refresh Video.

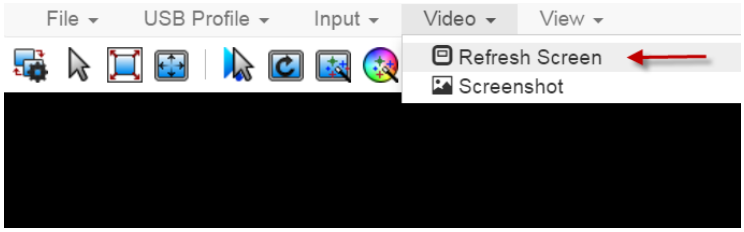


*Fig. 59 HKC **Video - Refresh Screen***

7.3.4.2 Screenshot

Take a screenshot of a target using the Screenshot command.

To take a screenshot of the target:

1. Choose **Video > Screenshot**.

   The screenshot file appears as a download to view or save. Exact options depend on your client browser.

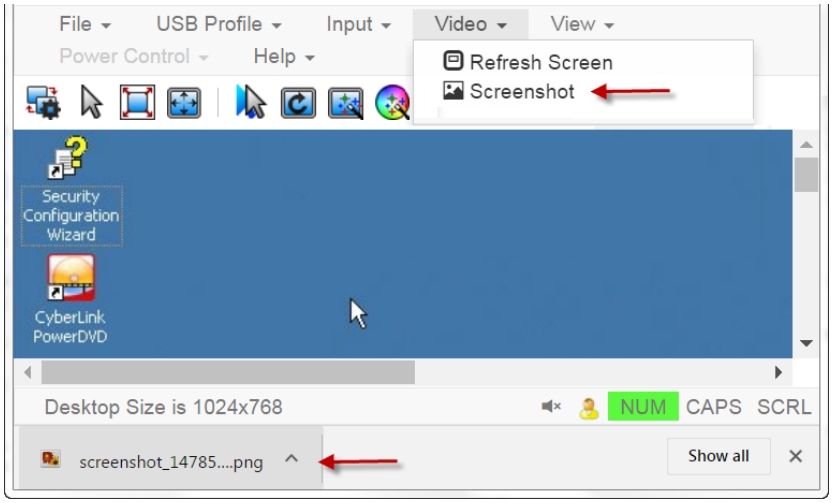


*Fig. 60 HKC **Video - Screenshot***

7.3.5 View Menu

The View Menu contains options to customize your HKC display.

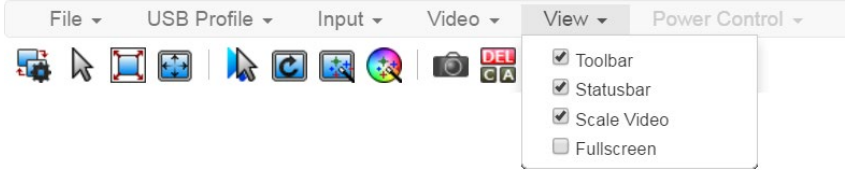


*Fig. 61 HKC **View***

Toolbar and Statusbar:

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

Scale Video:

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

Fullscreen:

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

- Press Esc to exit fullscreen.

7.3.6 Tools Menu

The Tools menu contains options for HKC target connection settings.

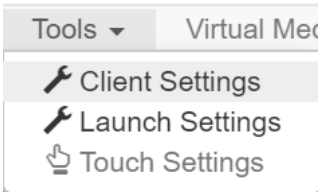


*Fig. 62 HKC **Tools***

Client Settings:

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

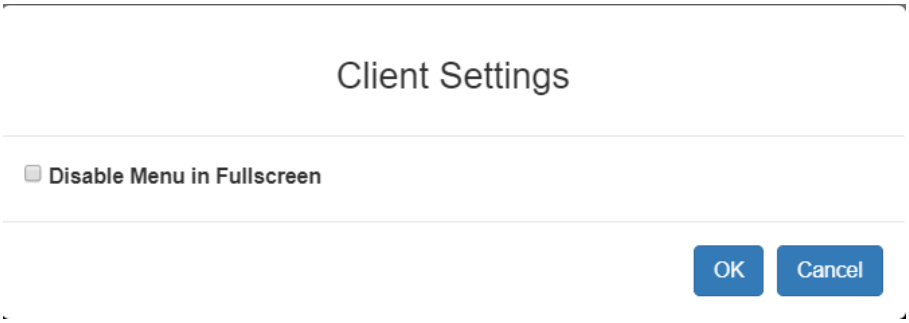


*Fig. 63 HKC **Tools - Client Settings***

Launch Settings:

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

Touch Settings - enabled for iOS clients:

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

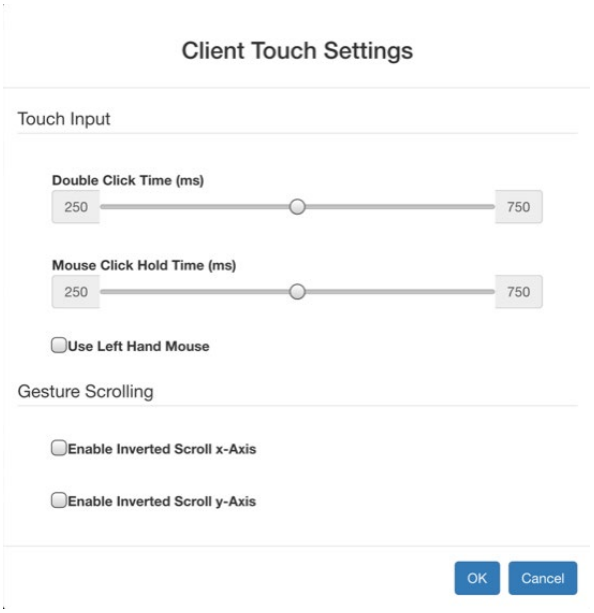


*Fig. 64 HKC **Tools - Launch Settings***

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

7.3.7 Virtual Media Menu

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

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

7.3.7.1 Connect Files and Folders

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

Supported browsers: Chrome, Firefox, Safari

File size limit: 4GB per file

To connect files and folders:

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

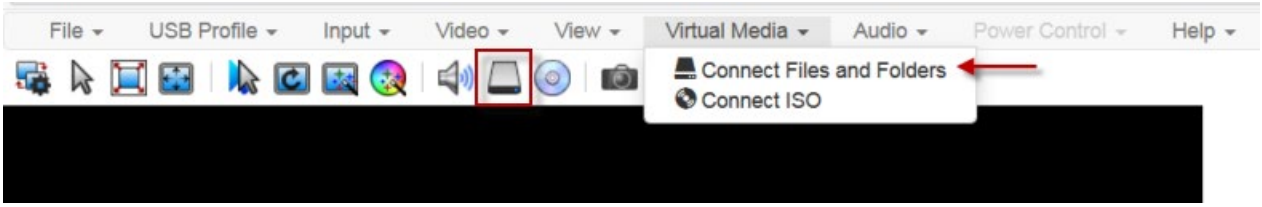


*Fig. 65 HKC **Virtual Media - Connect Files and Folders***

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

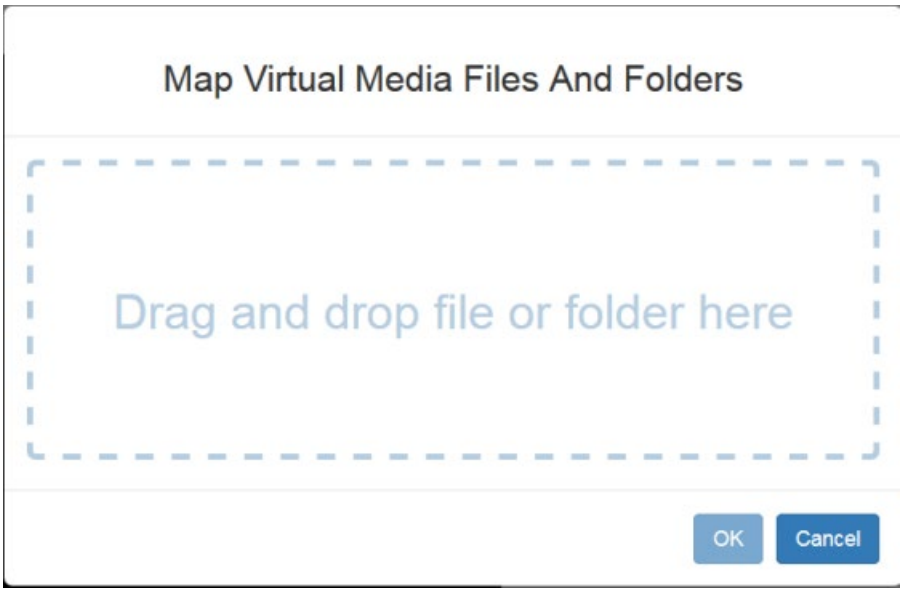


*Fig. 66 HKC **Map Virtual Media Files and Folders - Dialog***

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

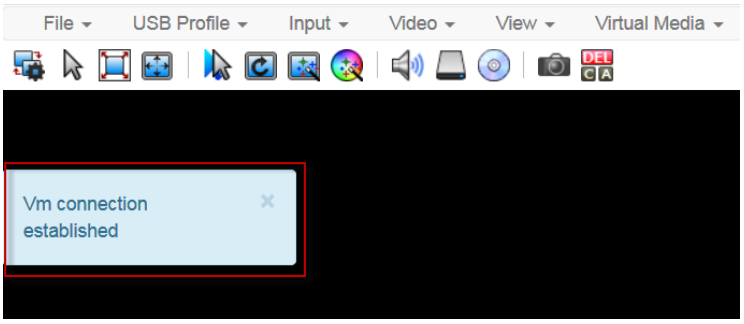


*Fig. 67 HKC **VM connection established - Dialog***

To disconnect files and folders:

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

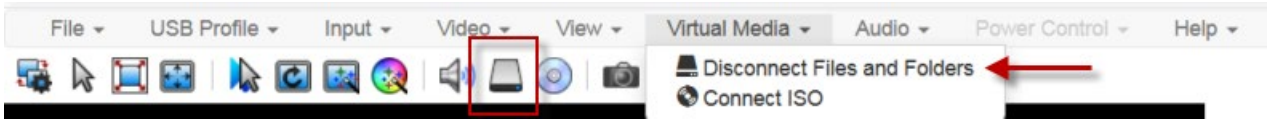


*Fig. 68 HKC **Virtual Media - Disconnect Files and Folders***

7.3.7.2 Connect ISO

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

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

To map virtual media image files:

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

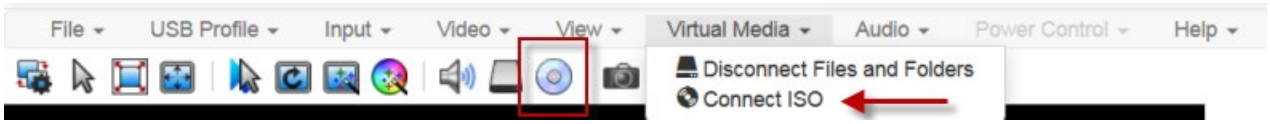


*Fig. 69 HKC **Virtual Media - Connect ISO***

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

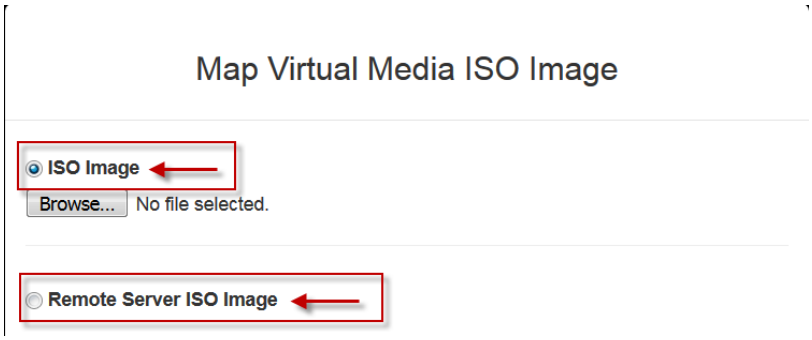


*Fig. 70 HKC **Virtual Media - Connect ISO - Map Virtual Media ISO Image***

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

- Select Remote Server ISO Image for ISO files on a remote server. Remote ISO files must be pre-configured by an administrator for the mapping to appear here. See Virtual Media File Server Setup (File Server ISO Images Only). Select the Hostname, then select the image file from the Image list. Enter the file server's username and password.

3. Click **OK** to map the selected file to the target.

   A message appears to show virtual media is connected.

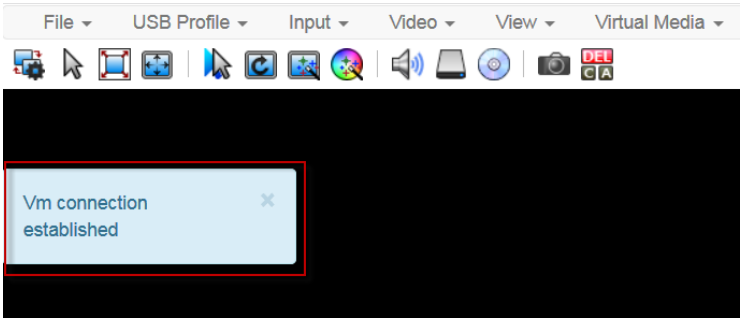


*Fig. 71 HKC **VM connection established - Dialog***

To disconnect ISO:

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

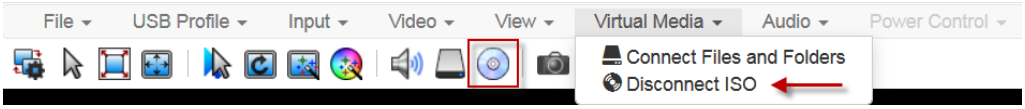


*Fig. 72 HKC **Virtual Media - Disconnect ISO***

7.3.8 Audio Menu

The Audio menu contains audio connection and settings.

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

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

7.3.8.1 Connect Audio

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

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

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

To connect audio:

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

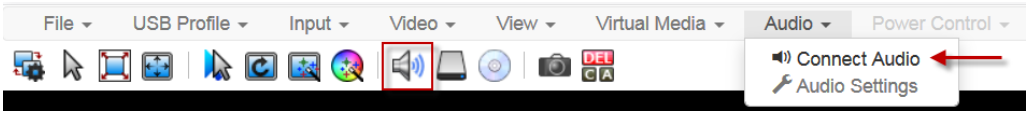


*Fig. 73 HKC **Audio - Connect Audio***

2. Tick the **Connect Playback Device** checkbox in the **Connect Audio Device** dialog.

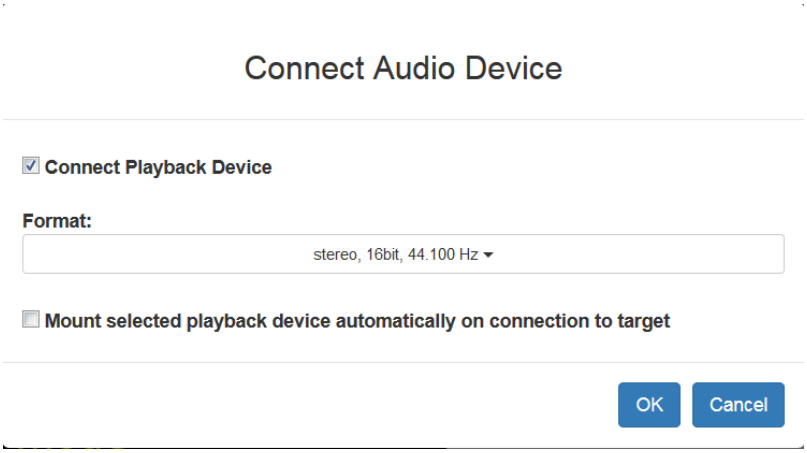


*Fig. 74 HKC **Audio - Connect Audio - Connect Audio Device - Dialog***

3. Tick the **Mount selected playback device automatically on connection to target** checkbox to enable the option.

   This setting will connect audio automatically the next time you connect to targets.
4. Click **OK**.

   A success message appears.

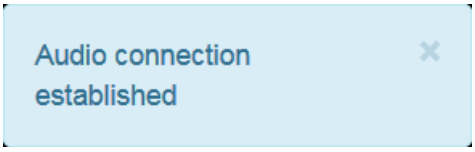


*Fig. 75 HKC **Audio - Connect Audio - Message***

To disconnect audio:

➡ Click **Audio > Disconnect Audio**, or click the matching icon in the toolbar.

7.3.8.2 Audio Settings

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

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

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

To configure audio settings, proceed as follows:

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

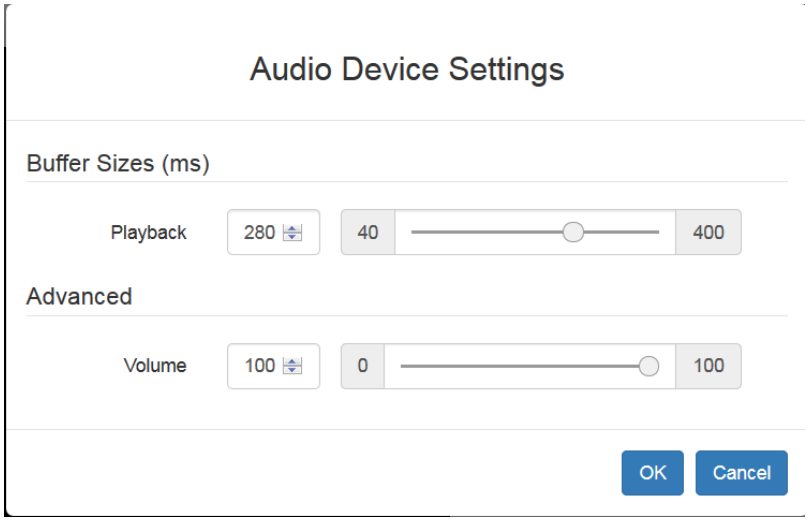


*Fig. 76 HKC **Audio - Audio Device Settings***

3. Click **OK**.

7.3.8.3 Auto Play in Safari

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

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

7.3.9 Using HKC on Apple iOS Devices

SIRA Module supports remote access to targets from Apple mobile devices with iOS 10.0 or higher, using a mobile version of HKC. Due to Apple iOS limitations, you may notice some differences in operation. See ***Limitations on Apple iOS Devices*** (on page 92).

7.3.9.1 Install Certificate on Apple iOS Device

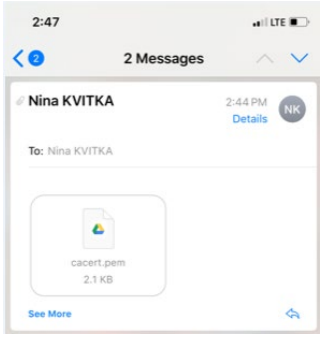
You must install a CA-signed certificate on your Apple iOS device before you can connect to SIRA Module. Access is prevented if only the default certificate is present. Depending on your browser, you may see an error such as "This Connection is Not Private".

When creating certificates, the certificate Common name should match the IP address/Hostname used to connect to the device.

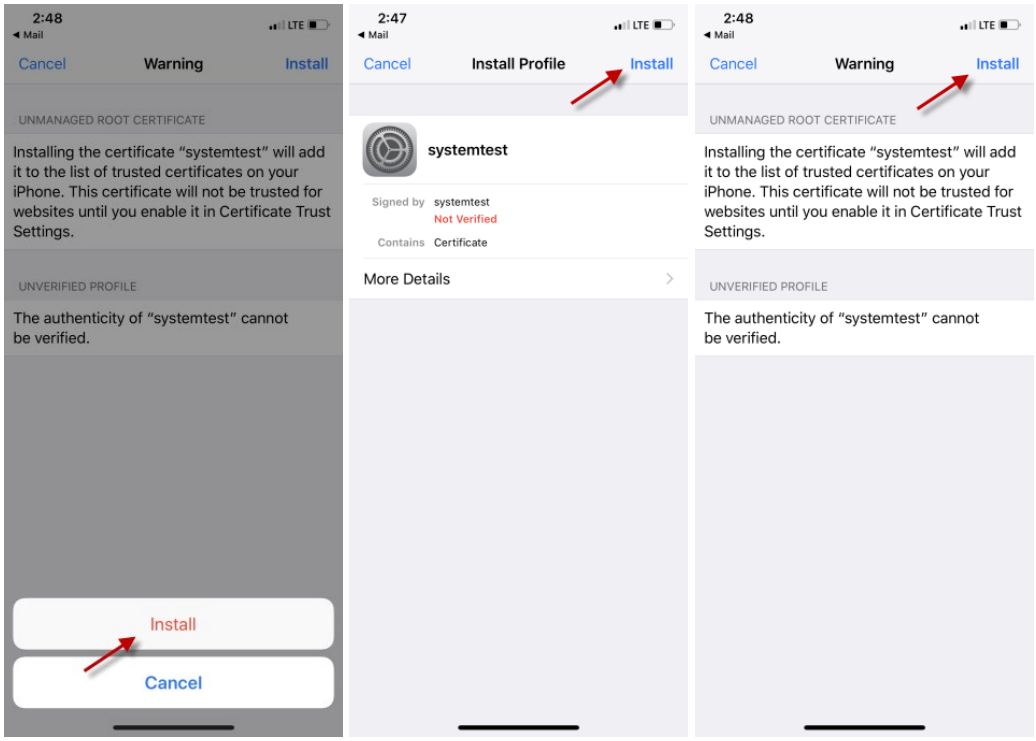
Install both the SIRA Module certificate and the CA certificate used to sign the SIRA Module certificate.

To install the certificate on an IOS device:

1. Email the certificate file to an email account that can be opened on the iOS device. Open the email and tap the attachment.

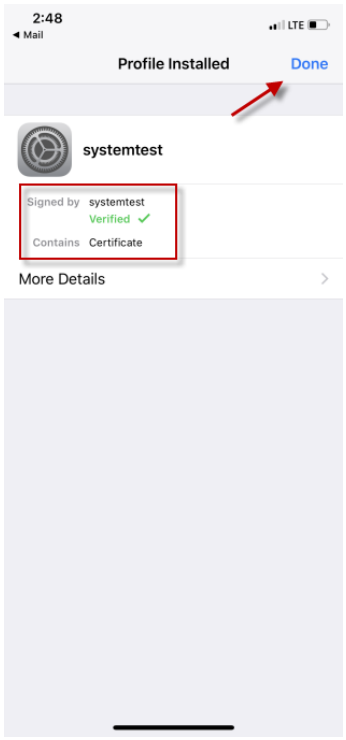


2. The certificate downloads as a "profile" that you have to install. You can have only one profile ready to install at a time. For example, if you download a profile and don't install it, and then download a second profile, only the second profile is available to be installed. If a profile is not installed within 8 minutes of downloading it, it is automatically deleted.
3. To install the profile, go to Settings, then tap Profile Downloaded.
4. Tap install, then follow prompts as presented to verify and Install.

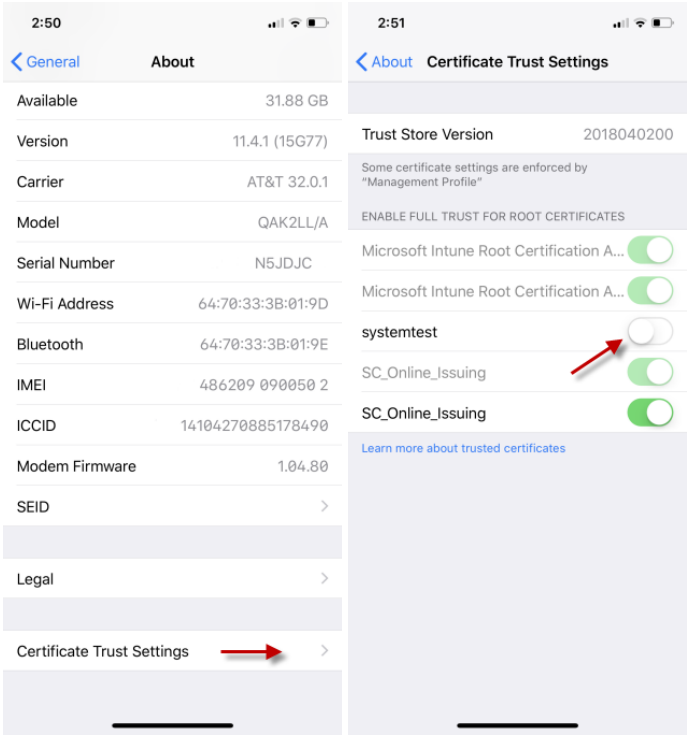


When complete the certificate is marked **Verified**.

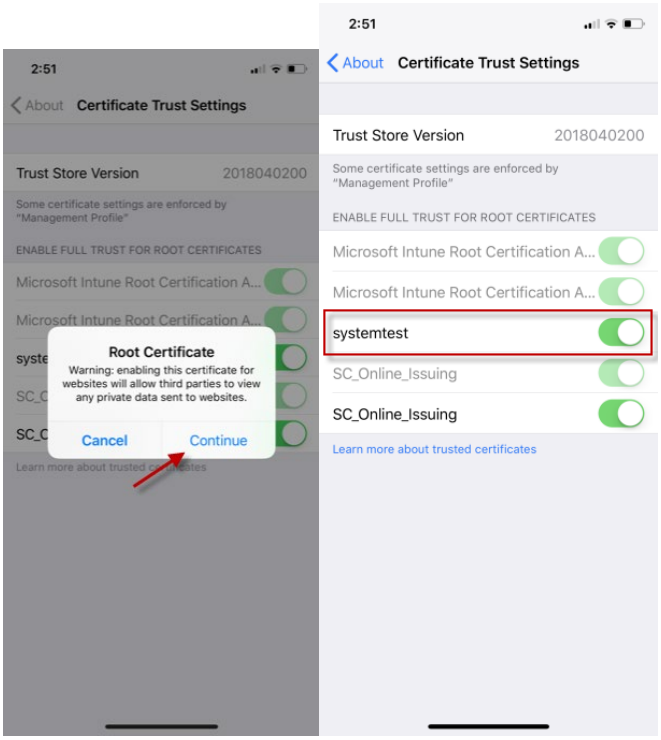
5. Tap Done.



6. To enable the certificate, go to **Settings > General > About**, then scroll all the way down.
7. Tap **Certificate Trust Settings**.



8. Tap the certificate that was installed earlier to enable.
   A warning appears.
9. Tap **Continue to enable**.
   The certificate slider displays green for enabled.



7.3.9.2 Touch Mouse Functions

Use the touchscreen equivalent for each mouse function. Some touch settings are configurable. See ***Tools Menu*** (on page 82).

Single Finger Touch	Mouse Equivalent
touch down - move - release	move mouse pointer
short tap	left click
double short tap	left double-click
short tap - touch down - hold for 250ms	mouse equivalent of Right Click"
short tap - touch down - move - release	hold down left mouse button and move, as in drag and drop or select

Two Finger Touch	Mouse Equivalent
touch down - move - release	move screen

7.3.9.3 Keyboard Access on Mobile

Keyboard access to the target is through a virtual keyboard, available on the toolbar. For all other actions requiring keyboard input, the IOS popup keyboard displays automatically.

7.3.9.4 Manage HKC iOS Client Keyboard Macros

The HKC iOS client includes a list of default macros. You can create additional macros using the HKC Macro Editor or import macros from a file. See ***Macro Editor*** (on page 73) and ***Import and Export Macros*** (on page 76).

To import macros when using an Apple iOS device, first export the file from HKC using a PC client. Add the file to a Cloud location to access from the IOS device for import.

7.3.9.5 Tools Menu

The Tools menu contains options for HKC target connection settings.

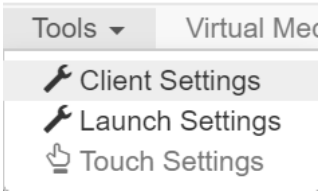


*Fig. 77 HKC **Tools***

Client Settings:

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

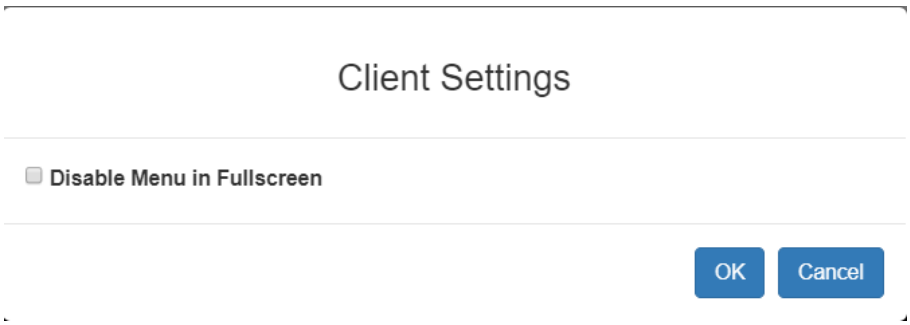


*Fig. 78 HKC on Apple **Tools - Client Settings***

Launch Settings:

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

Touch Settings - enabled for iOS clients:

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

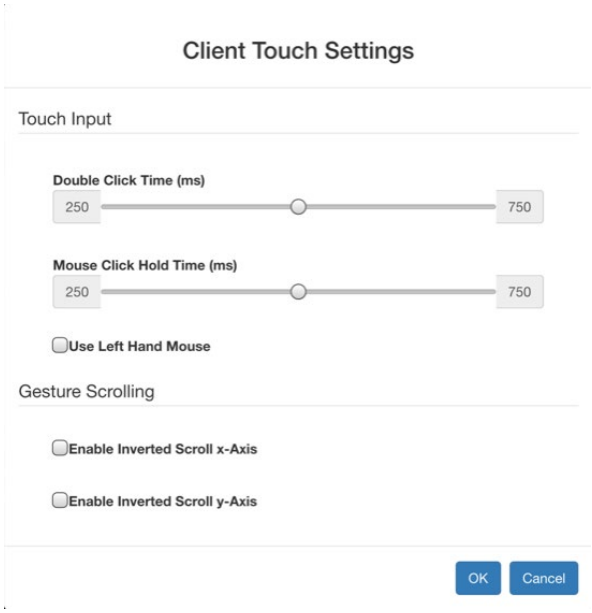


*Fig. 79 HKC on Apple **Tools - Client Touch Settings***

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

7.3.9.6 Limitations on Apple iOS Devices

Mobile access with iOS devices is supported for several Raritan products. Not all limitations apply to all products. Differences are noted.

- Target connections are closed after about one minute if the browser is in background, or if your iOS device enters Auto Lock mode
- Unable to create Macros for some special characters: F1-F12, ESC, Control, Alt, OS Meta keys and others. A selection of commonly used keys are available in the default Macro list. These keys can be edited. Additional keys such as F1-12 and arrows can be added using a Macro Import.
- In Safari on iOS, must refresh the connection to device after a KVM or Serial target launch in order to access menu options or serial targets. Not needed in Chrome on iOS.
- iOS does not support auto connect audio device to targets.
- On Ubuntu 14.04 target, no response to mouse click and hold on target items to simulate right clicking.
- Dual Target connection issues: Both target windows have to be closed separately. Only 1 port of a Dual target opened from Safari on iOS 11.x devices. (Dual targets not supported on KX4-101).
- Options "FullScreen" and "Resize window to fit screen" are not enabled/available on iOS.
- KB locale from the Client Virtual Keyboard must match input locale of device and OS locale of the target.
- iOS client target window does not have scrollbars. Unscaled video can be scrolled horizontally/vertically by sliding two fingers left/right or up/down. See ***Touch Mouse Functions*** (on page 91).
- On Safari, users are prompted to save passwords when switching from a target with a server VM connection to another target. These prompts can be turned off by unchecking the box "Usernames and passwords" in Safari > Preferences > AutoFill.
- On Safari, the onscreen keyboard includes word forecast. Selecting a forecast word adds a space at the end. For example, at login screen, selecting "admin" enters "admin ". Similar behavior occurs for VM File server Username and other areas.
- Cannot move menu option panels such as Connection Info.
- iOS On-Screen keyboard is displayed from all mouse clicks on the HTML admin page if keyboard "Go" is tapped to save setting changes instead of tapping the Save button.
- VKCS login occurs when refreshing login page after a reboot. This causes target connections to fail. To restore mobile HKC login, logout and enter the SIRA Module IP or hostname again. Issue is applicable to both iOS and PC Clients.
- The VM Files and Folders Option from the Virtual Media menu is disabled as not possible to drag and drop files to panel.
- Not all Accented letters are processed from iOS client.
- Macro files exported from iOS devices using Safari are automatically given the name "unknown" and need to be renamed with an xml extension to be imported to another client.
- Macro file export from Chrome on iOS devices is not possible due to issues with downloading data.
- Only characters support by target will be processed. There is no response from iOS characters such as ¥, § and … that are found on iPad keyboards.
- With the onscreen keyboard, selecting ' character or "Return" key, brings keyboard display back to first in list.

8 Port Access and Configuration

8.1 Port Access

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

Port Preview:

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

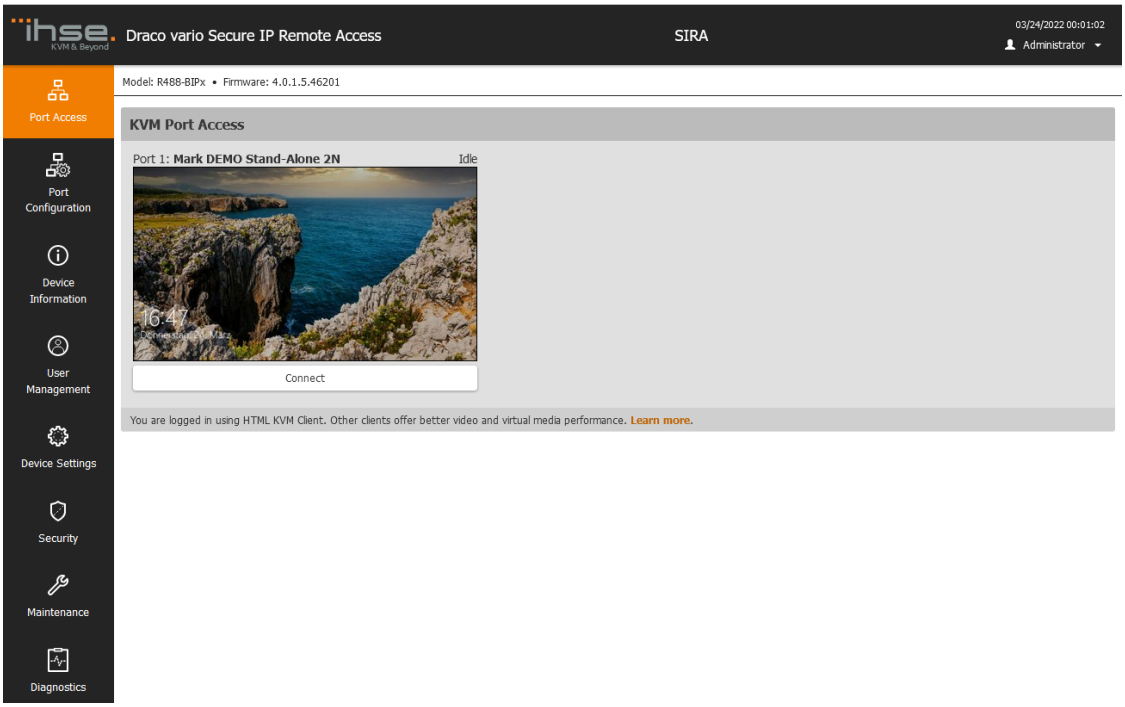


*Fig. 80 SIRA Configuration menu **Port Access - Port View***

Connect to the target:

➡ Click **Connect** to open a connection to the target.

For help with using the KVM clients, see chapter 7, page 36.

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

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

➡ Click **Port Configuration** to access all port configuration.

8.2.1 General

1. Enter a new name to rename the KVM port.
2. Click **Save**.

*Fig. 81 SIRA Configuration menu **Port Configuration - KVM Port 1 Settings - General***

➡ View the Current Port Status:

- Active, Idle
- Active, Busy: Connected, but PC Share is disabled, see chapter 12.3, page 152.
- Active, Connected: Connected, and PC Share is enabled.

8.2.2 Video Settings

1. Select **Enable VGA Mode** if the video input originates with a VGA or other analog source, through an HDMI adapter. In VGA mode, resolution is controlled on the video source device only.
2. Select the **Preferred Video Resolution**: The KX IV uses an EDID data structure to tell the target what video resolution is wanted. To change the video resolution on the target, change the **Preferred Video Resolution** to the new resolution.

   This should change the resolution when connecting to the target. If not, change the resolution on the target.

   - See **Supported Preferred Video Resolutions** (chapter 8.2.4, page 97) for a list of all supported resolutions.
   - If there is a specific EDID to load, see **Port Configuration: Custom EDIDs** (chapter 8.3, page 98).
3. Set the **Video Interface** to HDMI or DVI (no audio).
4. Set a longer **Cycle Time** if the target video is not responding properly to changes in preferred video resolution. Default is 200ms. A longer cycle time may allow the target to respond accurately to a new preferred video resolution.
5. Select **Enable Video Throttle** to cap the client frame rate at half the frame rate of the incoming video. This can be useful to reduce network bandwidth and CPU load on the client.
6. Click **Save** to apply all settings.

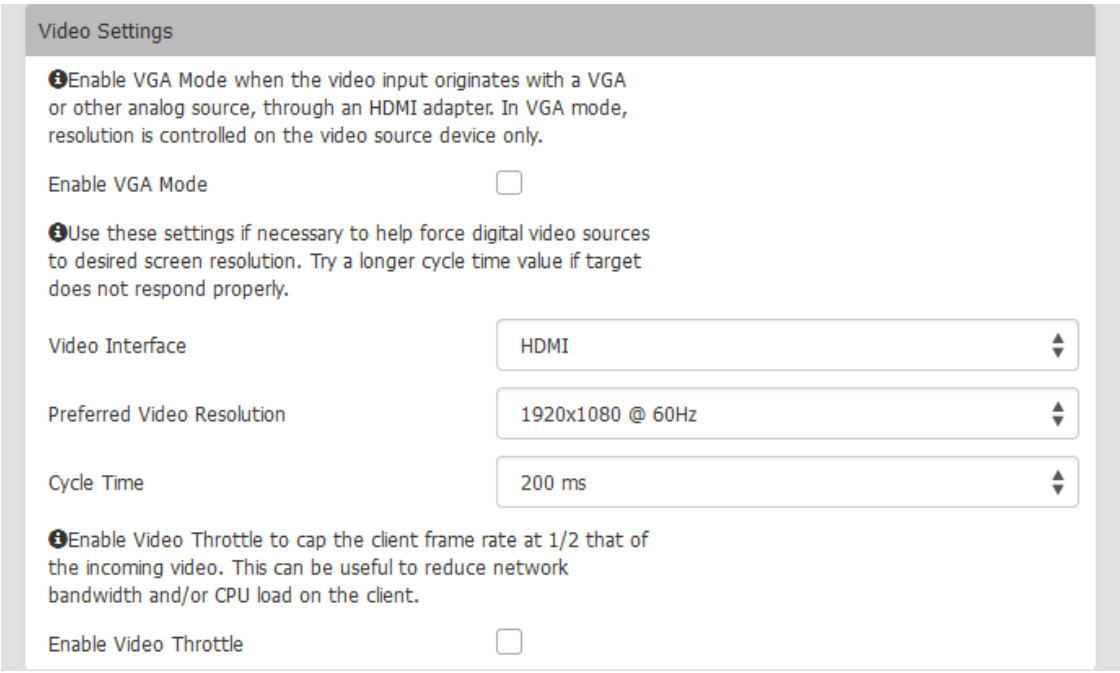


*Fig. 82 SIRA Configuration menu **Port Configuration - KVM Port 1 Settings - Video Settings***

8.2.3 Audio Settings

1. Tick the **Audio Compensation** checkbox to enable audio if there is no audio.
2. Reboot the SIRA Module after disabling this function to allow a new audio connection to another target computer.
3. Click **Save** to apply all settings.

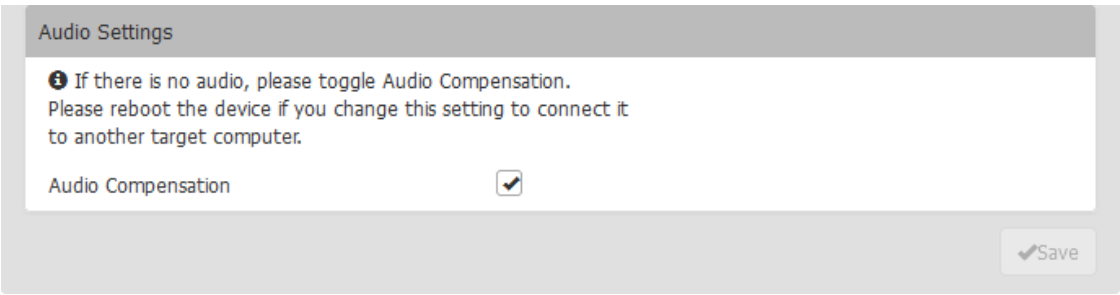


*Fig. 83 SIRA Configuration menu **Port Configuration - KVM Port 1 Settings - Audio Settings***

8.2.4 Supported Preferred Video Resolutions

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

Max. video resolution with frame rate:

- 1024x768@60Hz
- 1152x864@60Hz
- 1280x720@60Hz
- 1280x960@60Hz
- 1280x1024@60Hz
- 1360x768@60Hz
- 1440x900@60Hz
- 1400x1050@60Hz
- 1600x900@60Hz
- 1600x1200@60Hz
- 1680x1050@60Hz
- 1920x1080@60Hz (148.5MHz clock)
- 1920x1200@60Hz (Reduced Blanking 154MHz clock)
- 1920x2160@60Hz
- 2560x1440@60Hz
- 2560x1600@60Hz
- 3840x1080@60Hz
- 3840x1600@30Hz
- 3840x2160@30Hz

8.3 Port Configuration: Custom EDIDs

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

To upload a custom EDID:

1. Click **Port Configuration**.
2. Scroll down to **Custom EDIDs** and expand the menu.
3. Click **Browse** to go to the location of the `.rfp` EDID file, select it and click **Open**.
4. Click **Upload**.
5. Repeat these steps to add more files.
6. Once EDIDs are uploaded, they display in a list sorted by resolution.
7. Click **Show Description** to view the details.
8. Click the Delete icon to remove a file.

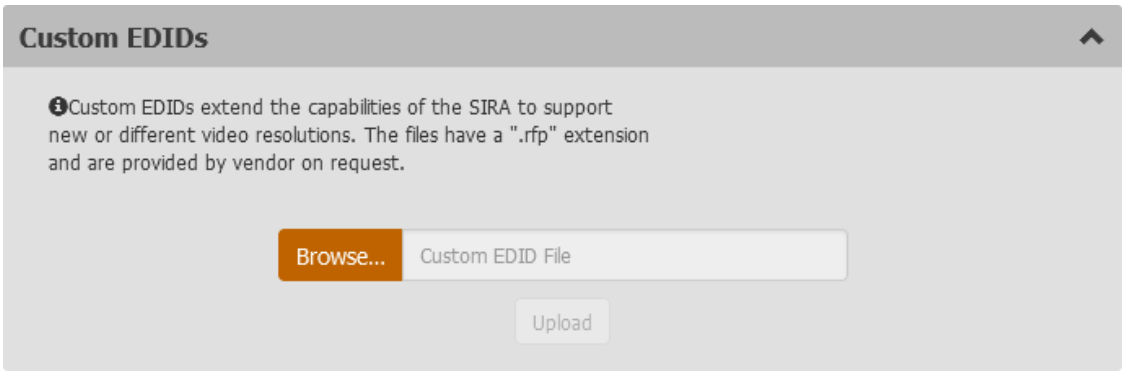


*Fig. 84 SIRA Configuration menu **Port Configuration - KVM Port 1 Settings - Custom EDIDs***

8.4 Port Configuration: Local Port Monitor EDID

If a local port monitor is attached to SIRA Module, a **Local Port Monitor EDID** section appears in the **Port Configuration** menu and the monitor's EDID is included in the **Preferred Video Resolution**. To use the local port monitor's EDID, select it as the **Preferred Video Resolution**.

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

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

To view Local Port Monitor EDID, proceed as follows:

1. Click **Port Configuration**.
2. Scroll down to **Local Port Monitor EDID**.
   The EDID of the currently attached local port monitor is listed.
3. Click **Show Description** to view the details.

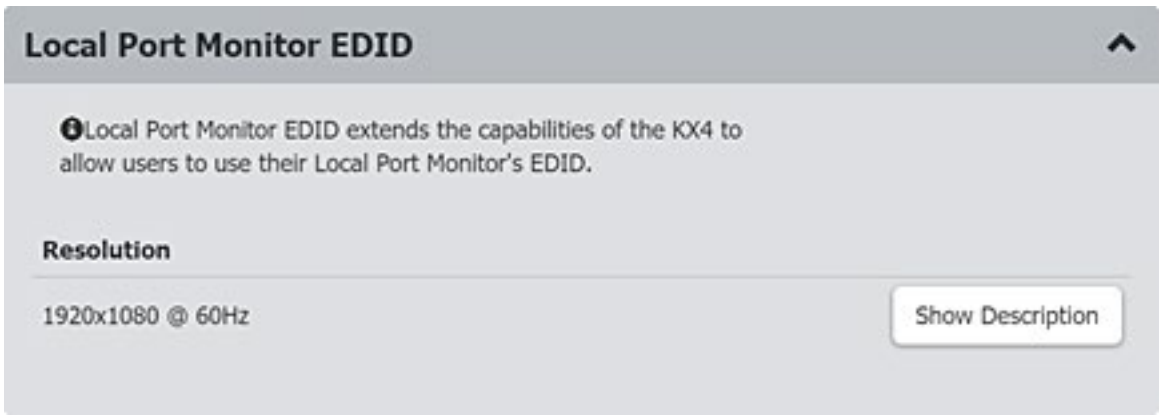


*Fig. 85 SIRA Configuration menu **Port Configuration - KVM Port 1 Settings - Local Port Monitor EDID***

8.5 Port Configuration: USB Connection Settings

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

To define USB connections for the target, proceed as follows:

1. Click **Port Configuration**.
2. Scroll down to USB Connection Settings.
3. Select the USB connection settings to be used:
   - 3.1. **Enable Absolute Mouse** - Clear the checkbox if the target does not support absolute mouse mode.
   - 3.2. **Use Full Speed** - Useful for BIOS that cannot accommodate High Speed USB devices. Clear the checkbox to allow negotiation to the target's highest USB speed capability.
   - 3.3. **Enumerate virtual media first before keyboard and mouse**: Useful to resolve issues when a target cannot detect USB mass storage at the BIOS.
4. Click **Save** to apply all settings.

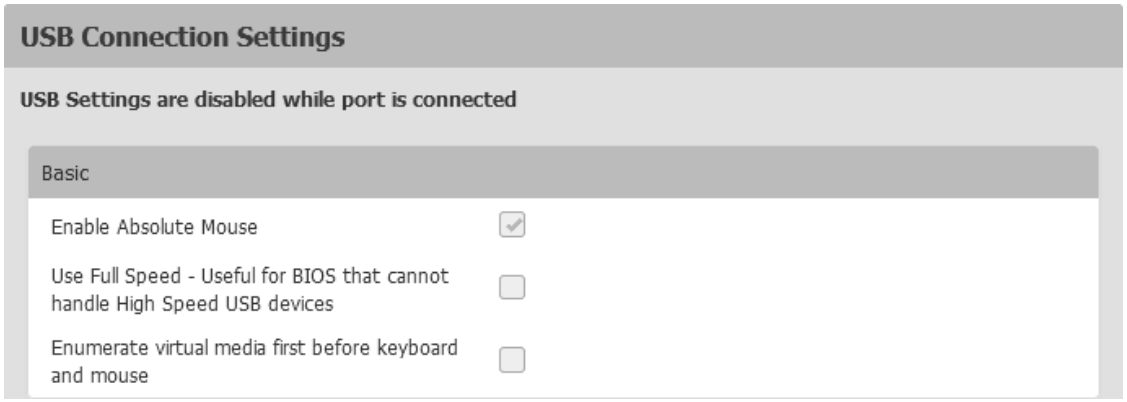


*Fig. 86 SIRA Configuration menu **Port Configuration - KVM Port 1 Settings - Custom EDIDs - Basic***

To set **Advanced** options as needed, proceed as follows:

1. Select the option for **Virtual Media Interface #1/2 Types**: Both interfaces cannot be set to CD-ROM or Removable Disk.
   - **Disabled**
   - **CD-ROM**
   - **Removable Disk**
   - **Auto** - can function as either **CD-ROM** or **Removable Drive** but not both at the same time
2. **Remove Unused VM Interface #1/2 From Device Configuration**: Tick this checkbox to remove the drive when VM is disconnected. Clear this checkbox to allow empty drives.
3. Click **Save** to apply all settings.

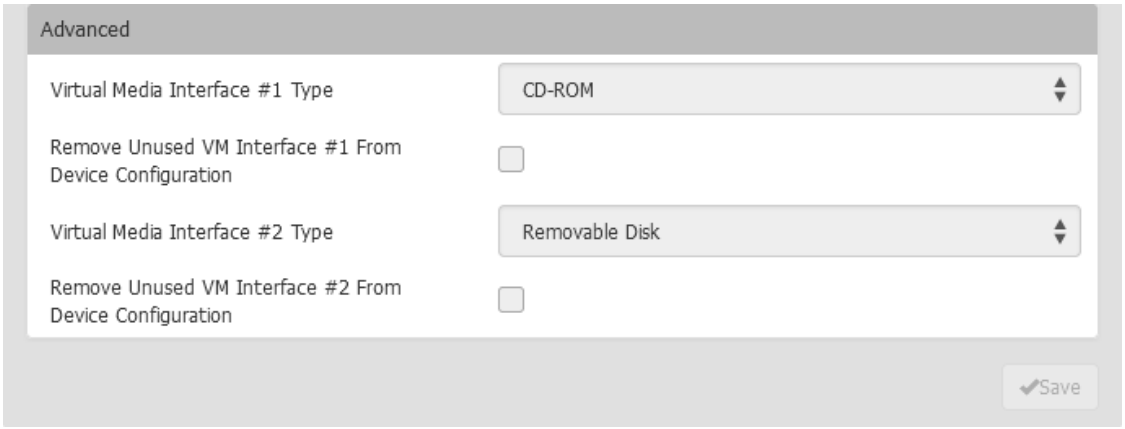


Fig. 87 *SIRA Configuration menu* ***Port Configuration - KVM Port 1 Settings - Custom EDIDs - Advanced***

9 Device Information

The **Device Information** displays name, system, and network details about the SIRA Module. In this menu the device can be renamed, and open source license information is displayed.

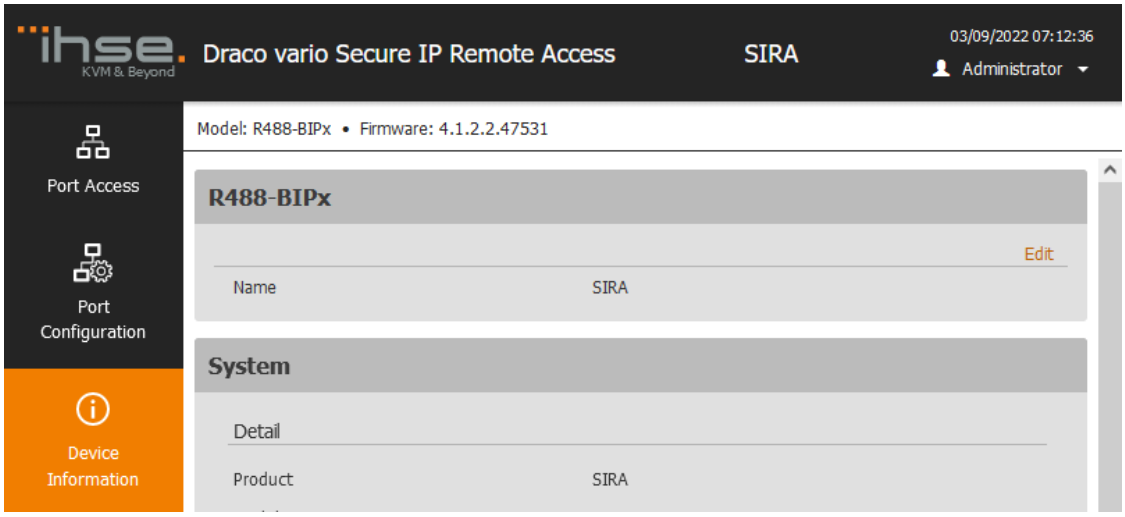


*Fig. 88 SIRA Configuration menu **Device Information - Submenu options***

To change the device name, proceed as follows:

1. Click **Device Information** in the tool bar.
2. Click **Edit** in the upper area.

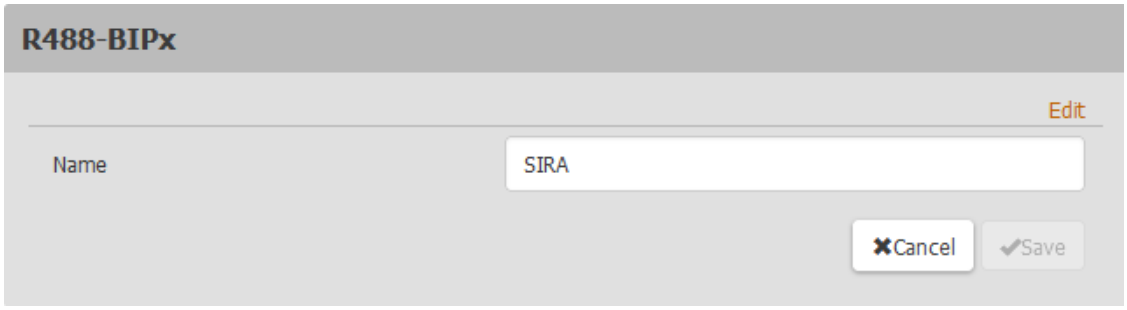


*Fig. 89 SIRA Configuration menu **Device Information - Changing the Name***

3. Enter a new name.
4. Click Save.

Under **System**, the **Detail** and the current **Status** is displayed:

Section	Content
Details	Product name, model, firmware version, hardware ID, and serial number
Status	Internal temperatures status, and local monitor status

*Fig. 90 SIRA Configuration menu **Device Information - System***

Network details

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

*Fig. 91 SIRA Configuration menu **Device Information - System***

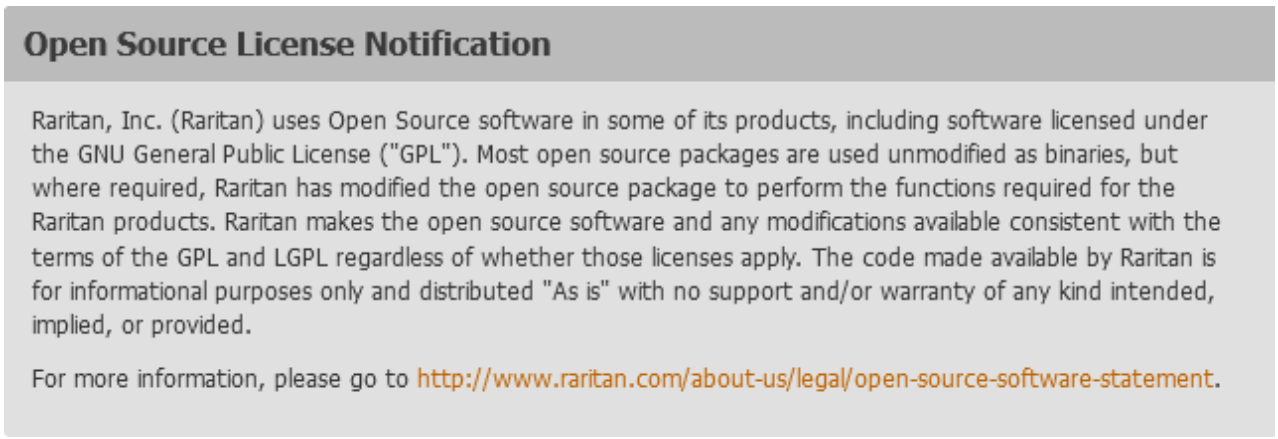


*Fig. 92 SIRA Configuration menu **Device Information - License***

10 Device Settings

To display the submenu options of the device settings, proceed as follows:

1. Click **Device Settings** to display the submenus.
2. Click **Network Services** to display the submenu of **Network Services**.

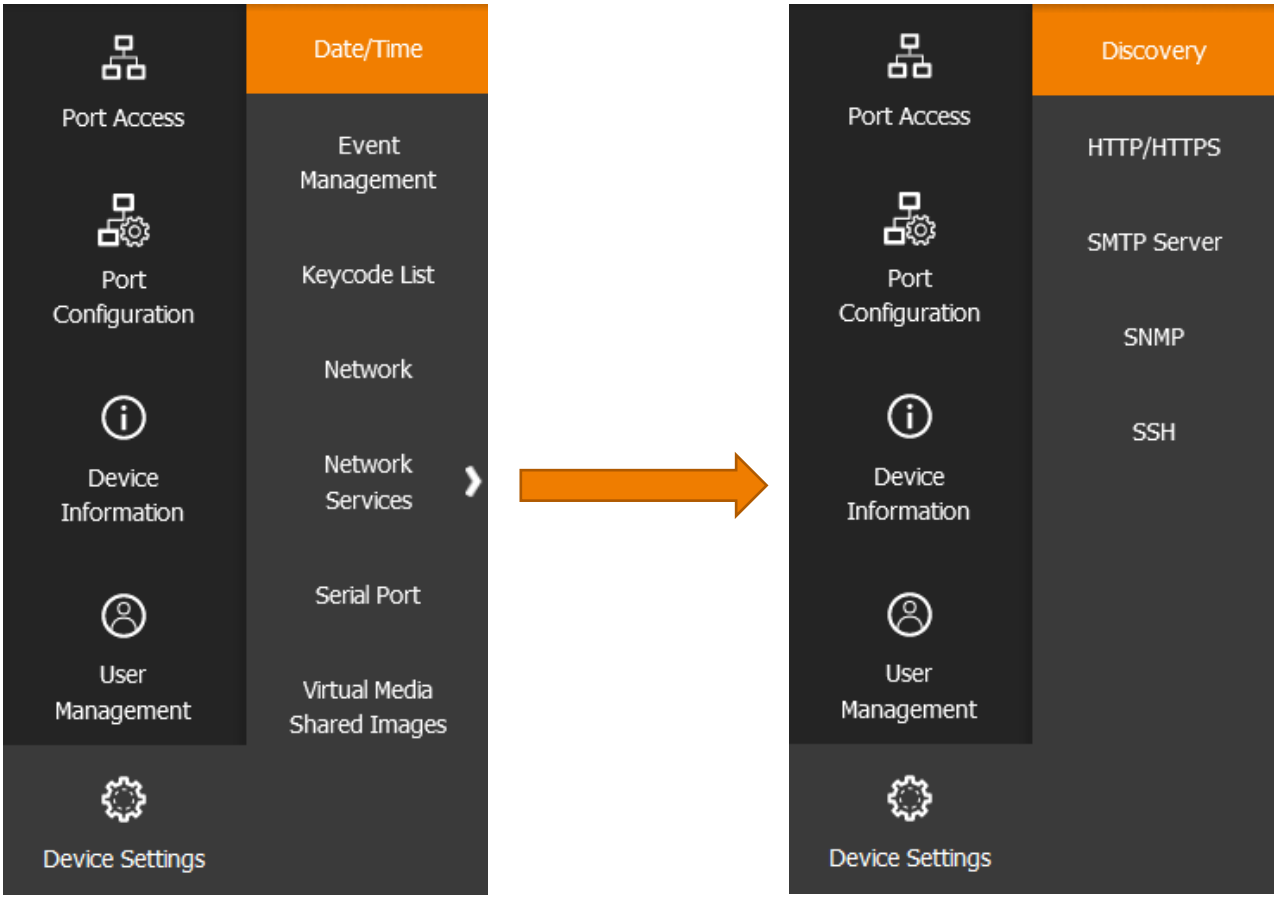


*Fig. 93 SIRA Configuration menu **Device Information - Submenu options***

10.1 Date and Time

Set the internal clock on the SIRA Module manually, or link to a Network Time Protocol (NTP) server.

The SIRA Module system date and time appears in the upper right corner of the web interface.

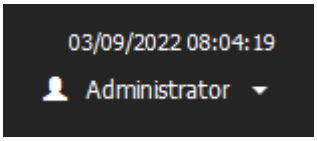


*Fig. 94 SIRA Configuration menu **Internal Clock***

To set the date and time, proceed as follows:

1. Click **Device Settings > Date/Time**.
   The **Date/Time** menu is displayed.

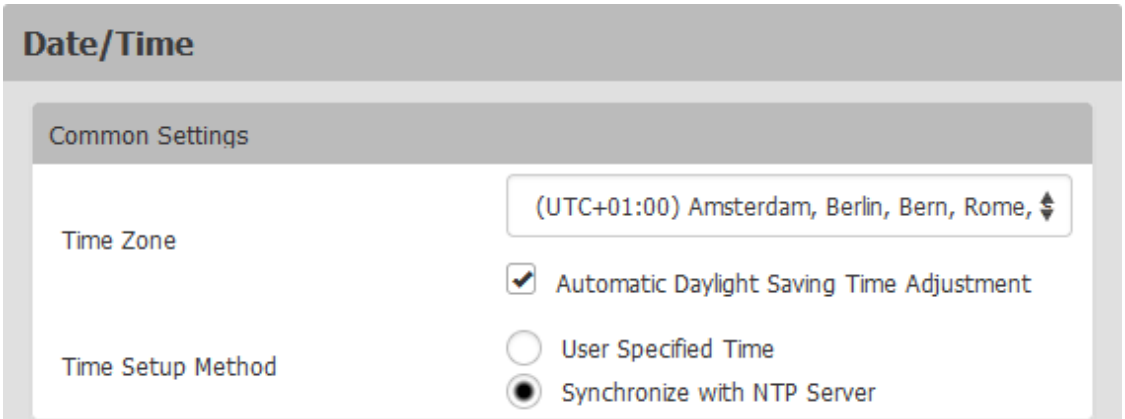


*Fig. 95 SIRA Configuration menu **Device Settings - Date/Time***

2. Select your **Time Zone**.
3. If your area participates in daylight saving time, verify the **Automatic Daylight Saving Time Adjustment** checkbox is selected.
4. Select the **Time Setup Method**:
   - **User Specified Time**: Set the time manually.
   - **Synchronize with NTP Server**: Use DHCP or set the NTP server manually

User Specified Time

1. Select **User Specified Time** under Common Settings.

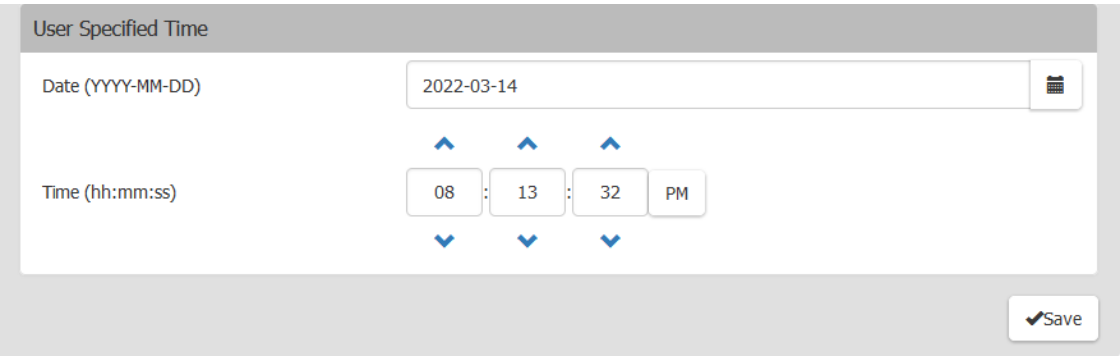


*Fig. 96 SIRA Configuration menu **Device Settings - Date/Time - User Specified Time***

2. Click the calendar icon to select the **Date**.
3. Enter the time in **Hours, Minutes and Seconds**.
4. Click **AM/PM** to toggle the setting for specifying AM or PM.
5. Click **Save** to apply all settings.

Synchronize with NTP Server using DHCP

1. Select **Synchronize with NTP Server** under Common Settings.

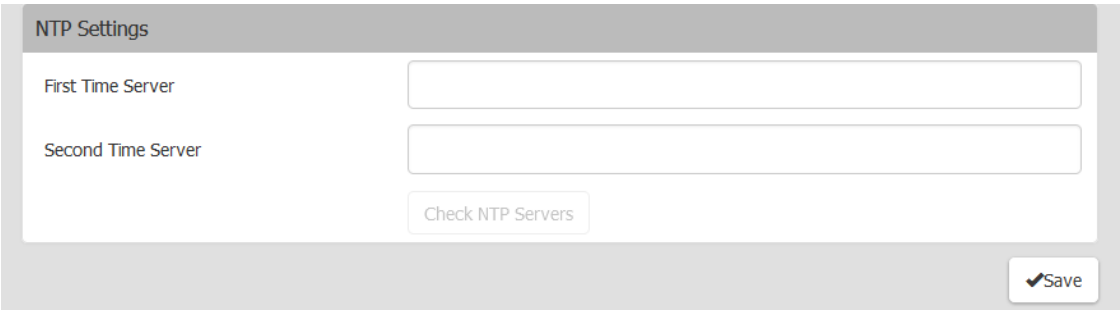


*Fig. 97 SIRA Configuration menu **Device Settings - Date/Time - Synchronize with NTP Server - with DHCP***

2. Leave the **First Time Server** and **Second Time Server** fields blank to use the DHCP-assigned NTP servers.

   DHCP-assigned NTP servers are available when either IPv4 or IPv6 DHCP is enabled (see chapter 10.4, page 117).
3. Click **Save** to apply all settings.

Synchronize with NTP Server

1. Select **Synchronize with NTP Server** under Common Settings.

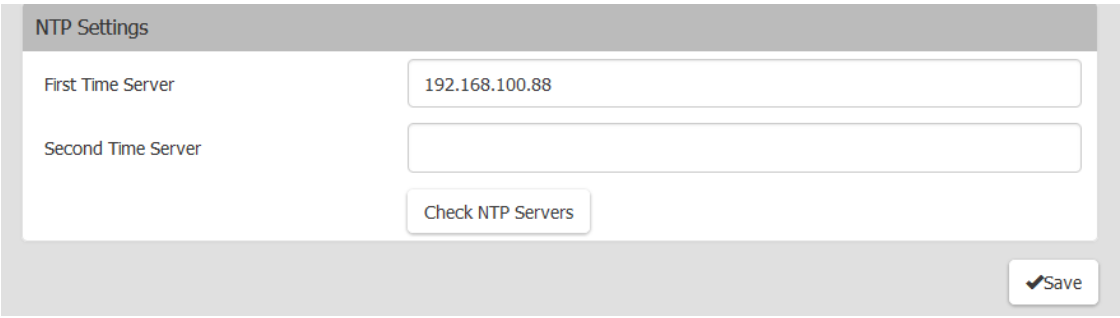


*Fig. 98 SIRA Configuration menu **Device Settings - Date/Time - Synchronize with NTP Server - without DHCP***

2. Enter the primary NTP server in the **First Time Server** field to specify NTP servers manually.

   A secondary NTP server is optional.
3. Click **Check NTP Servers** to verify.
4. Click **Save** to apply all settings.

10.2 Event Management

All supported events are logged in the system log by default. In this menu, additional actions can be created for any event, including sending an email, sending an SNMP notification, and forwarding a syslog message.

To display events and actions, proceed as follows:

1. Click **Device Settings > Event Management**.
   The **Event Management** menu shows events by **Category**.
2. Click a category to view individual events.

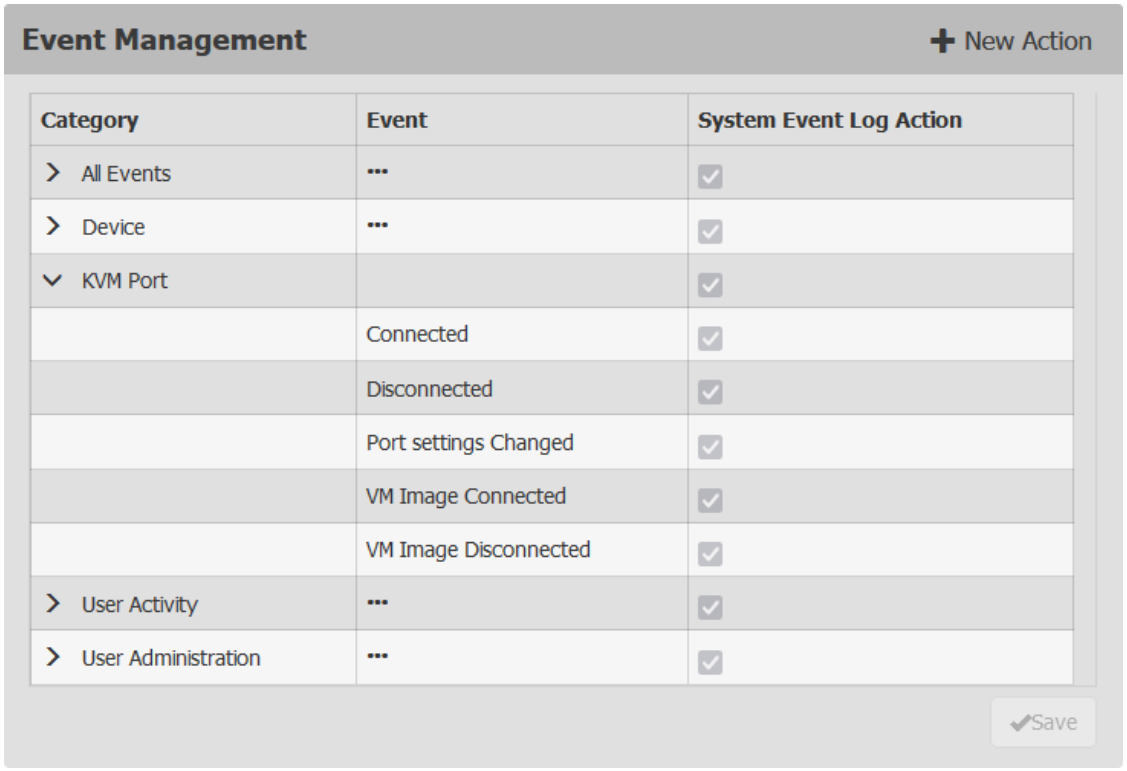


*Fig. 99 SIRA Configuration menu **Device Settings - Event Management***

Actions

There are three options available to create new actions. New actions are displayed in a new column in the Event Management list.

Action	Description
Send email	Use this action to send an email according to preconfigured SMTP settings or create actions with one or more customized SMTP settings.
Send SNMP notification	Use this action to send an SNMP notification to one or more SNMP servers.
Syslog message	Use this action to automatically forward event messages to the specified syslog server. Determine the syslog transmission mechanism you prefer when setting it up. SIRA Module may or may not detect syslog message transmission failure. Detected syslog failures and reasons are saved in the event log.

To assign an action to an event, see chapter 10.2.5, page 113.

10.2.1 Adding the Action Send Email

To add a **Send email** action, proceed as follows:

1. Click ➕ New Action.

   The **New Action** menu opens.

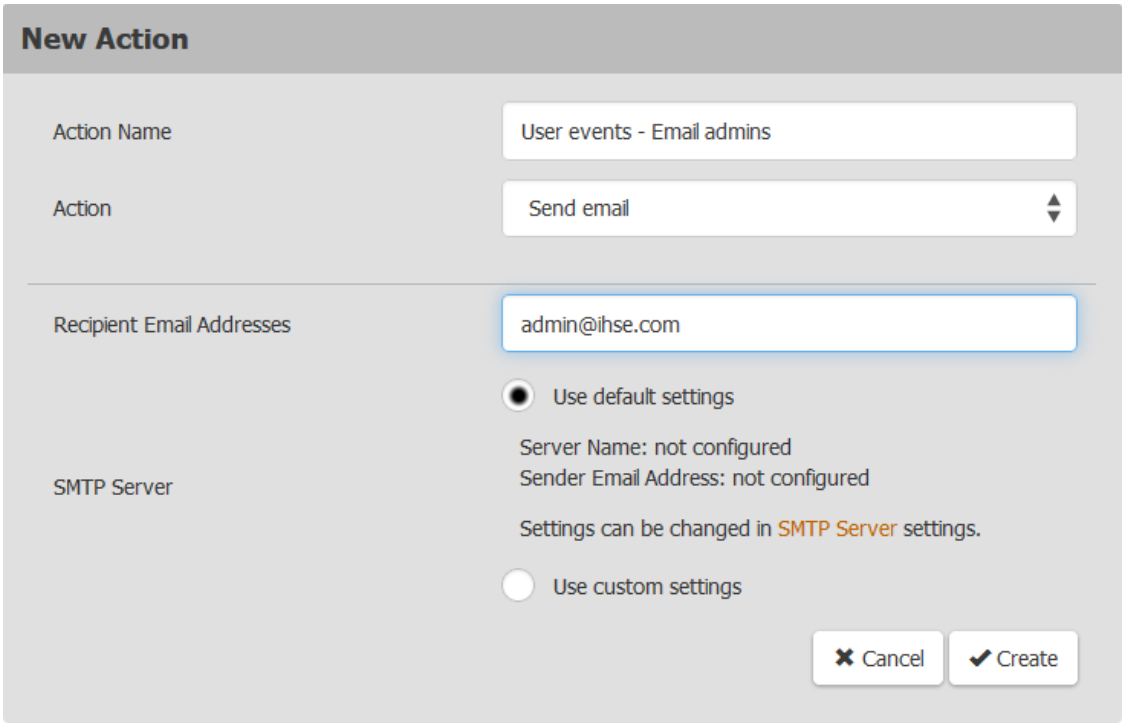


*Fig. 100 SIRA Configuration menu **Device Settings - Event Management - New Action - Send email***

2. Assign a name to this action.
3. Select **Send email** from the **Action** list.
4. Enter the email addresses of the recipients in the **Recipient Email Addresses** field. Use a comma to separate multiple email addresses.
5. Select one of two options for **SMTP Server** settings:
   5.1. **Use default settings**: By default, the SMTP server settings will be used to complete this action. To view or change those settings, click the **SMTP Server** hyperlink.
   5.2. **Use custom settings** to use a different SMTP server.

   The fields for customized SMTP settings appear (see chapter 10.5.3, page 122). 6. Click **Create**.

To assign an action to an event, see chapter 10.2.5, page 113.

10.2.2 Adding the Action SNMP Notifications

To create the **Send NMP notification** action, proceed as follows:

1. Click ➕ New Action.

   The **New Action** menu opens.
2. Select **Send SNMP notification** from the **Action** list.
3. Click in the **Notification Type** selection list to select the type of SNMP.
4. Follow the procedure below based on the selected notification type.

10.2.2.1 SNMP v2c notifications

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

1. Select **SNMPv2c Trap** from the **Notification Type** list.

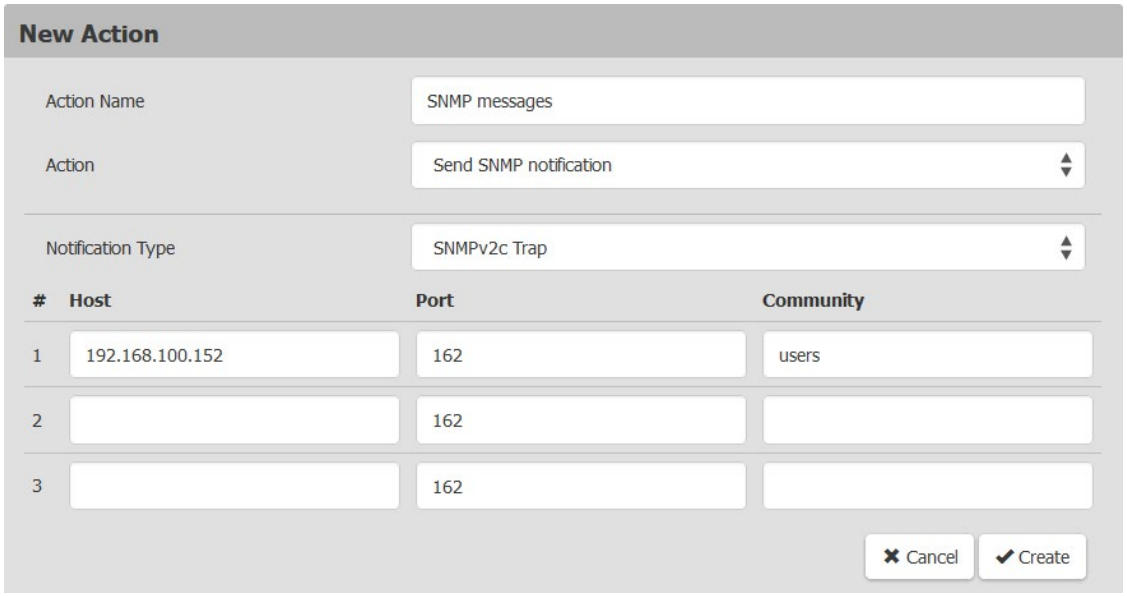


*Fig. 101 SIRA Configuration menu **Device Settings - Event Management - New Action - Send SNMP notification - SNMPv2***

2. Enter the IP address of the device(s) to be accessed in the **Host** fields.
   This is the address to which notifications are sent by the SNMP system agent.
3. Enter the port number used to access the device(s) in the **Port** fields.
4. Enter the SNMP community string to access the device(s) in the **Community** fields.
   The community is the group representing the SIRA Module and all SNMP management stations.
5. Click **Create**.

To assign an action to an event, see chapter 10.2.5, page 113.

10.2.2.2 SNMP v3 notifications

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

1. Select **SNMPv3 Trap** In the **Notification Type** field.

   The engine ID is prepopulated.

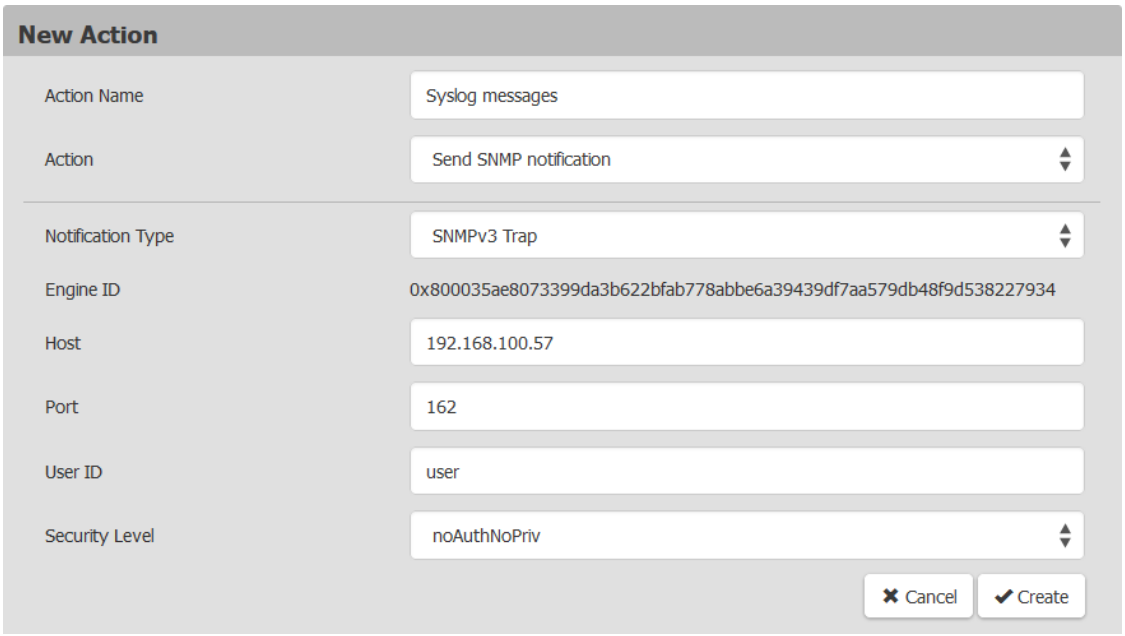


*Fig. 102 SIRA Configuration menu **Device Settings - Event Management - New Action - Send SNMP notification - SNMPv3***

2. Enter the following as needed:
   2.1. Enter the IP address of the device(s) to be accessed in the **Host** fields.

   This is the address to which notifications are sent by the SNMP system agent.

   2.2. Enter the port number used to access the device(s) in the **Port** fields.

   2.3. Enter the user ID for accessing the host in the **User ID** field. Make sure the User ID has SNMPv3 permission.

   2.4. Select one of the host security levels:

Security level	Next steps
noAuthNoPriv	➡ Select this if no authorization or privacy protocols are needed.
authNoPriv	➡ Select this if authorization is required but no privacy protocols are required. ➡ Select **MD5** or **SHA** in the **Authentication Protocol** list. ➡ Enter the authentication passphrase and confirm the authentication passphrase.
authPriv	➡ Select this if authentication and privacy protocols are required. ➡ Select **MD5** or **SHA** in the **Authentication Protocol** list. ➡ Enter the authentication passphrase and confirm the authentication passphrase. ➡ Select **DES** or **AES** in the **Privacy Protocol** list. ➡ Enter the privacy passphrase and confirm the privacy passphrase.

3. Click **Create**.

To assign an action to an event, see chapter 10.2.5, page 113.

10.2.3 Adding the Action Syslog Messages

To create the syslog message action, proceed as follows:

1. Click ➕ New Action.

   The **New Action** menu opens.

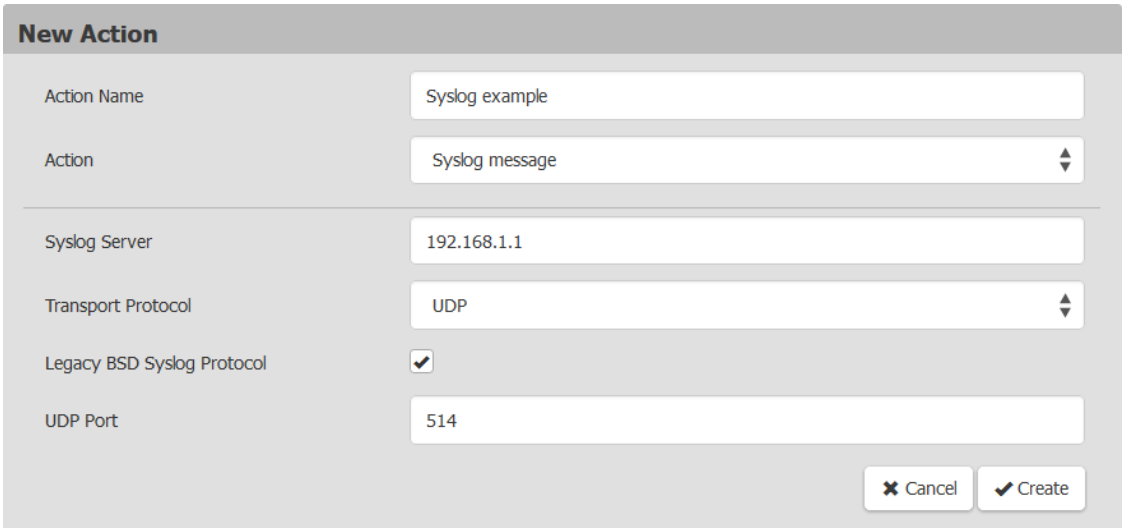


*Fig. 103 SIRA Configuration menu **Device Settings - Event Management - New Action - Send email***

2. Select **Syslog messages** from the **Action** list.
3. Specify the IP address to which the syslog is forwarded in the **Syslog Server** field.
4. Select one of the syslog protocols in the **Transport Protocol** field:

Transport protocol	Next steps
UDP	➡ Enter an appropriate port number (default 514). ➡ Select the **Legacy BSD Syslog Protocol** checkbox if applicable.
TCP	➡ Select if no TLS certificate is required. ➡ Enter an appropriate port number.
TCP+TLS	➡ Select if a TLS certificate is required. ➡ Enter an appropriate port number in the **TCP Port** field (default 6514). ➡ Click **Browse…** in the **CA Certificate** section to select and install the certificate file. After importing the certificate: click **Show** to view the installed certificate's content or click **Remove** to delete the installed certificate if it is inappropriate. **Note:** To allow event messages even if any TLS certificate in the selected certificate chain is outdated or not valid yet, tick the **Allow expired and not yet valid certificates** checkbox.

5. Click **Create**.

To assign an action to an event, see chapter 10.2.5, page 113.

10.2.4 Editing or Deleting an Action

Editing or deleting an action is described using the **Send SNMP notification** action as an example.

To edit or delete an action, proceed as follows:

1. Click the name of the action in the respective column.

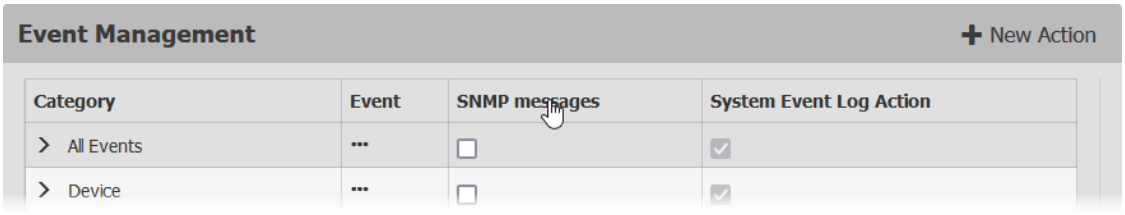


*Fig. 104 SIRA Configuration menu **Device Settings - Event Management - Selecting an Action***

The **Edit Action** menu opens.

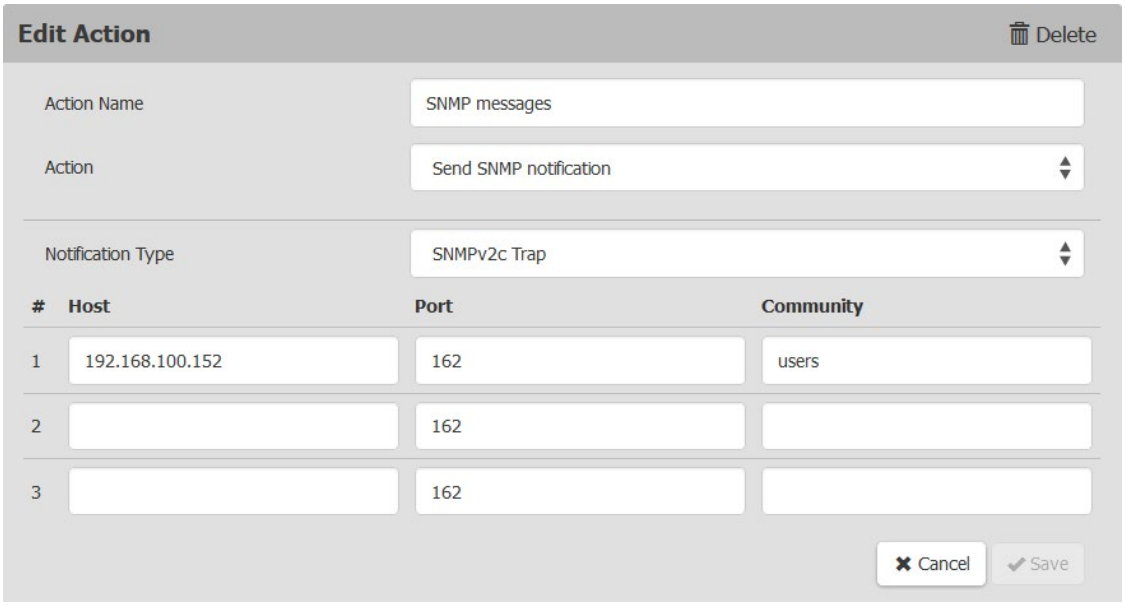


*Fig. 105 SIRA Configuration menu **Device Settings - Event Management - Edit Action***

2. To change settings:
   2.1. Change settings as needed.
   2.2. Click **Save** to save.
3. To delete the **Send SNMP notification** action:
   3.1. Click Delete to remove the action.
   A message appears.
   3.2. Click **Delete** to delete the action.

10.2.5 Assigning Actions

1. Click **Device Settings > Event Management**.

   The **Event Management** menu shows events by **Category**.

2. Click a category to view individual events.
3. Tick the respective checkboxes to assign the actions to events.

   In this example, an action named **User events - Email admins** has been added and assigned to all **User Activity** and **User Administration** events.

4. Click **Save**.

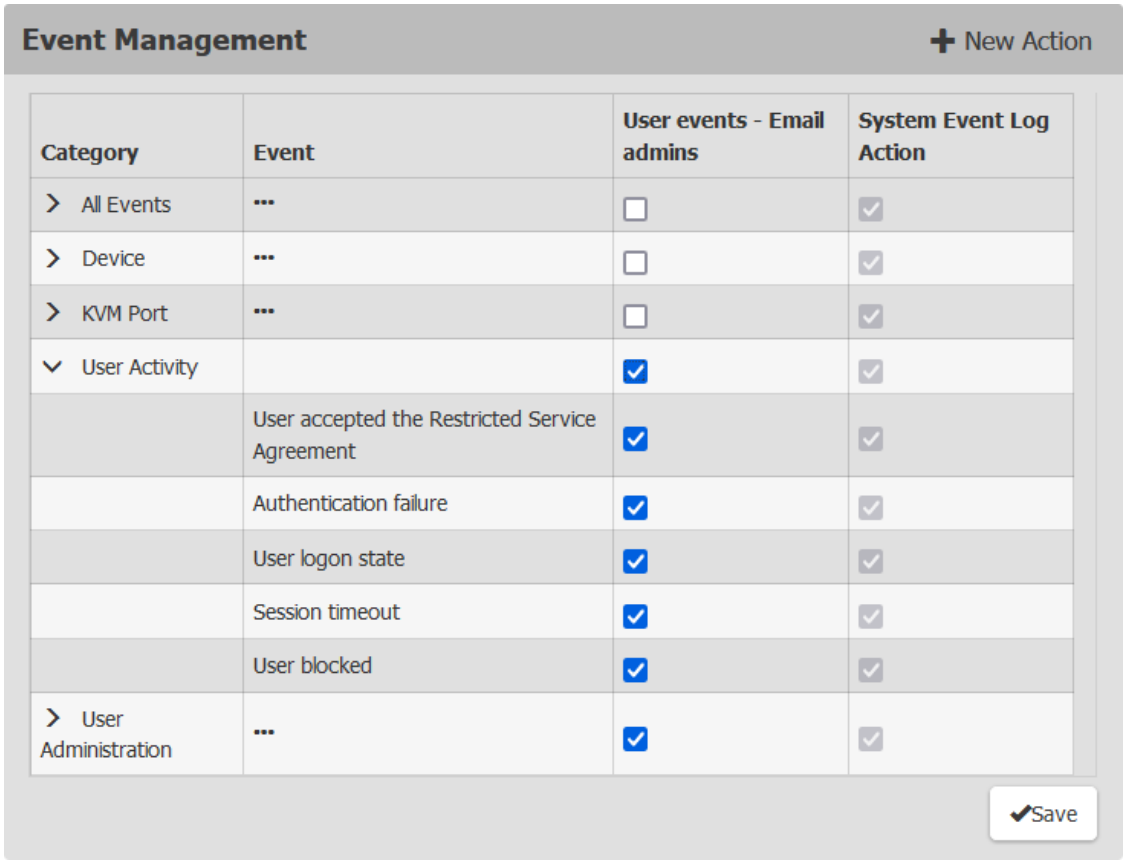


*Fig. 106 SIRA Configuration menu **Device Settings - Event Management - Assigning Action***

10.3 Keycode List

Use the **Keycode List** feature to create lists of keys to be blocked from being used. Assign the list to a user group to block the group from using those keys (see chapter 011.6, page 139).

Keycode lists are created by keyboard language type. The menu provides a list of keys that can be blocked for each keyboard type.

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

10.3.1.1 Adding a new Keyset

To add a new keyset, proceed as follows:

1. Click **Device Settings > Keycode List**.
   The **Keyboard Blocking** list is displayed.

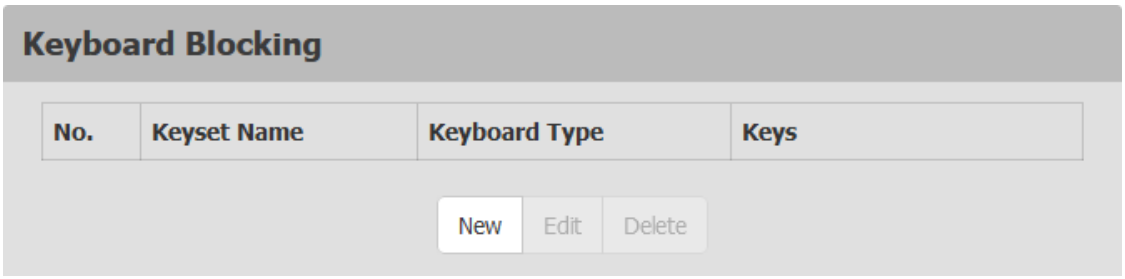


*Fig. 107 SIRA Configuration menu **Device Settings - Keycode list - Keycode Blocking***

2. Click **New**.
   The **New Keycode Setting** menu opens.

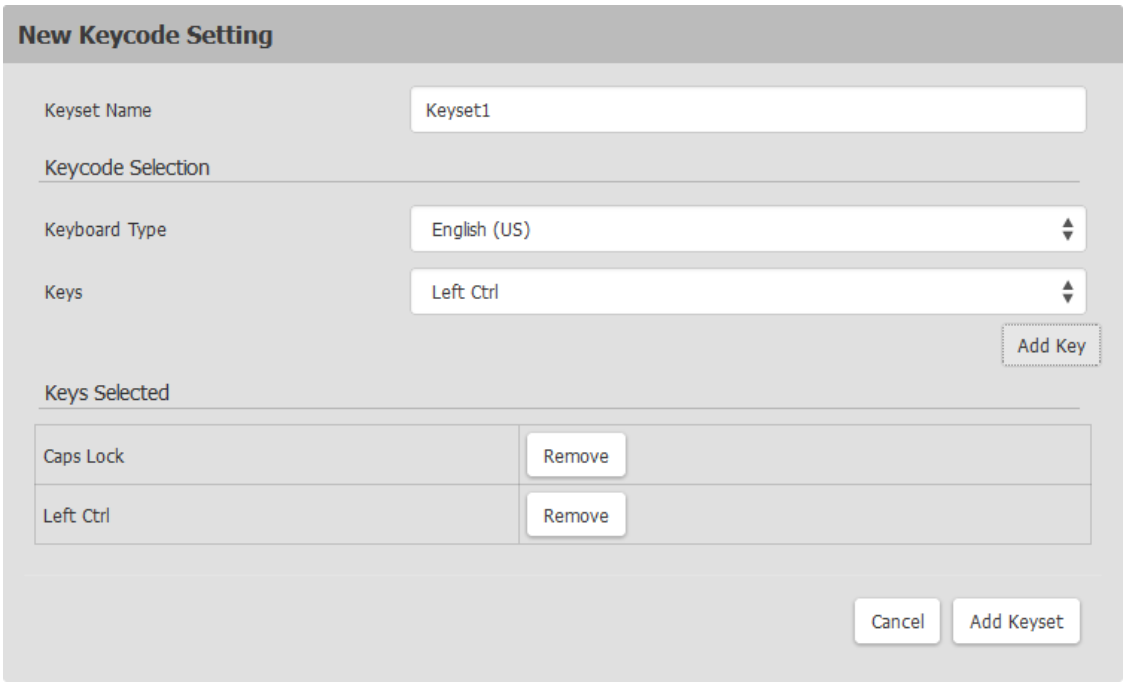


*Fig. 108 SIRA Configuration menu **Device Settings - Keycode List - New Keycode Setting***

3. Enter a **Keyset Name** to identify this list of keys to be blocked.
   The keyset name is used to assign the list to a user group (see chapter 11.5, page 139).
4. Select the keyboard type by language from the **Keyboard Type** list.
5. Select the key to be blocked from the **Keys** list.
6. Click **Add Key**.
   The added key appear in the **Keys Selected** list.
7. To add more keys, repeat steps 6 to 7.
8. Click **Add Keyset** when complete.

10.3.1.2 Changing a Keyset

To change a keyset, proceed as follows:

1. Click **Device Settings > Keycode List**.
2. Click a keyset by name to select it.
   The selected list is highlighted blue.

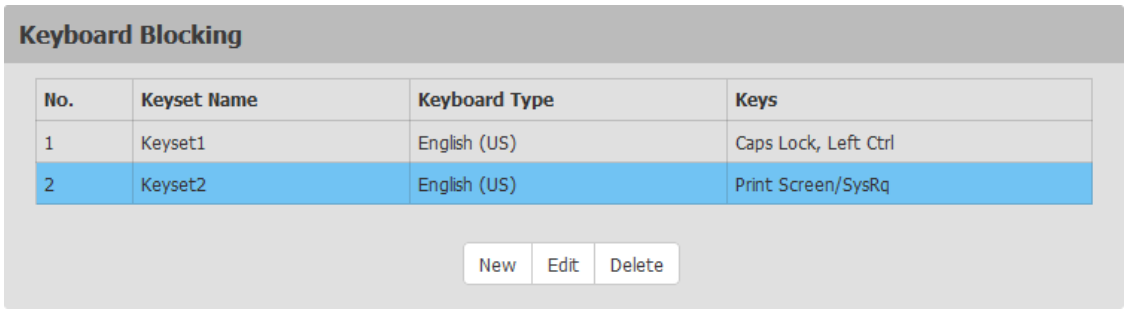


*Fig. 109 SIRA Configuration menu **Device Settings - Keycode List - Keycode Blocking***

3. Click **Edit** to change to the keyset.
   The **Edit Keycode Setting** is displayed.

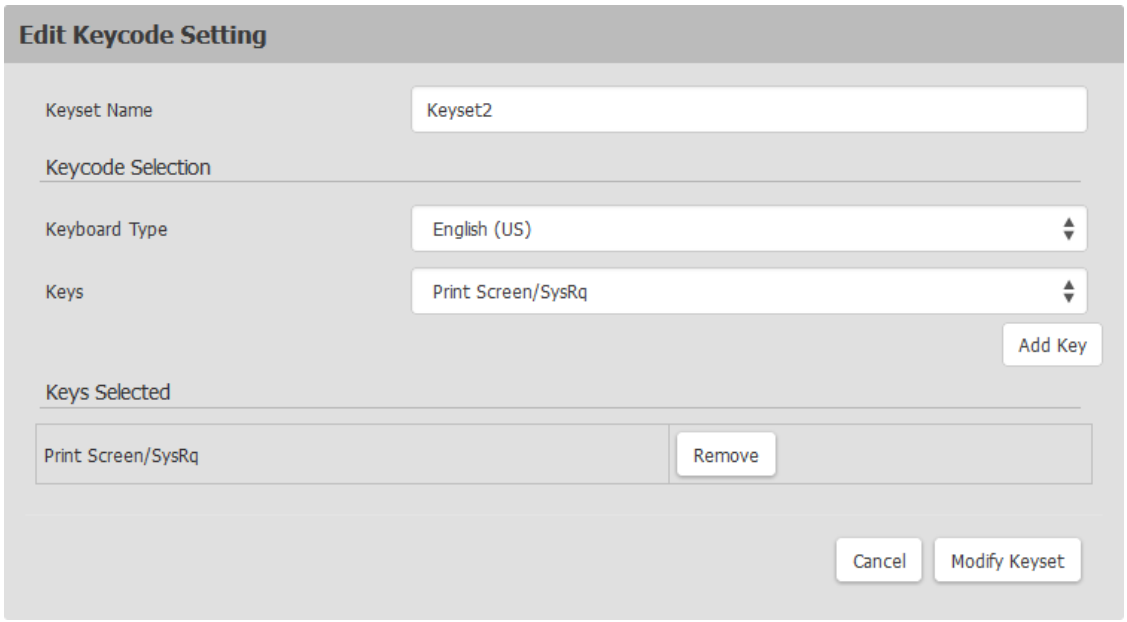


*Fig. 110 SIRA Configuration menu **Device Settings - Keycode List - Edit Keycode Setting***

4. Change settings as needed.
5. Click **Modify Keyset** to save the changes.

10.3.1.3 Deleting a Keyset

To delete a keyset, proceed as follows:

1. Click **Device Settings > Keycode List**.
2. Click a keyset by name to select it.
   The selected keyset is highlighted blue.

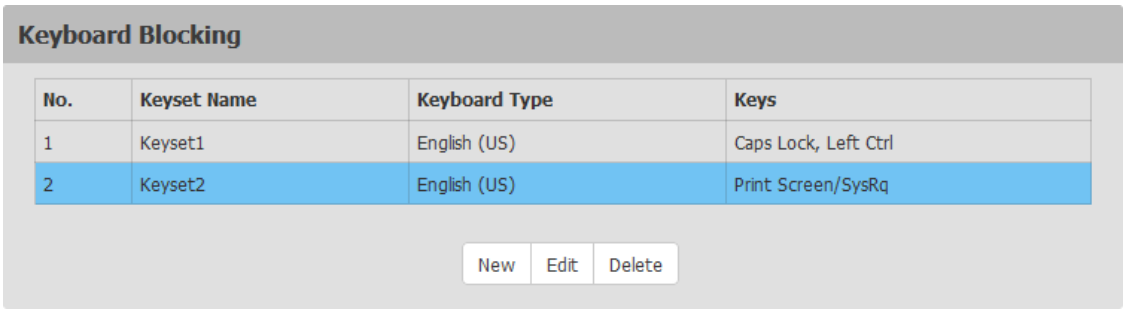


*Fig. 111 SIRA Configuration menu **Device Settings - Keycode List - Keycode Blocking***

3. Click **Delete** to remove the keyset.
   A **Keyset Deletion** message appears.
4. Click **Delete** to delete the selected keyset.

10.4 Network

The default network setting is 192.168.100.88/24 enabled for IPv4.

10.4.1 Configuring Ethernet Settings

To configure the network settings, proceed as follows:

1. Click **Device Settings > Network**.

   The **Network** menu is displayed.

Configuring IPv4 Settings

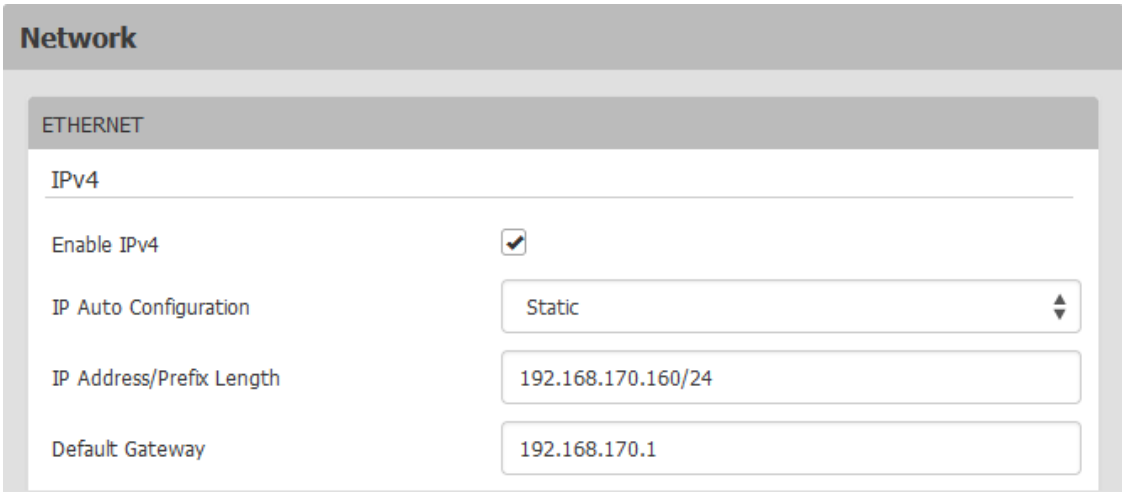


*Fig. 112 SIRA Configuration menu **Device Settings - Network - Ethernet***

The following settings can be configured:

Field/setting	Description	
Enable IPv4	Enable or disable the IPv4 protocol.	
IP Auto Configuration	Select the method to configure IPv4 settings.	
	DHCP	Auto-configure IPv4 settings via DHCP servers. Optionally specify the preferred hostname, which must meet the following requirements: • Auto-configure IPv4 settings via DHCP servers Consists of alphanumeric characters and/or hyphens • Cannot begin or end with a hyphen • Cannot begin with a number • Cannot contain punctuation marks, spaces, and other symbols • Maximum 253 characters
	Static	Manually configure the IPv4 settings. Assign a static IPv4 address, which follows this syntax **IP address/prefix length**. Example: 192.168.84.99/24

If DHCP is configured and the automatically assigned IP address is unknown, a local login is available (see chapter 16, page 175). After login the automatically assigned IP address is displayed in the **Device Information** menu (see chapter 9, page 101).

Configuring IPv6 Settings

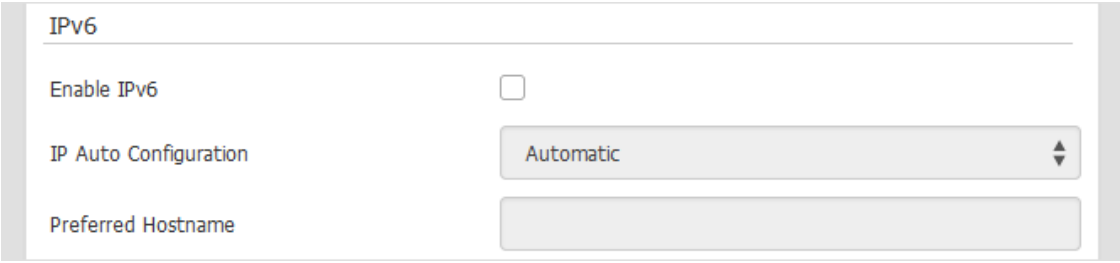


*Fig. 113 SIRA Configuration menu **Device Settings - Date/Time - User Specified Time***

The following settings can be configured:

Field/setting	Description	
Enable IPv6	Enable or disable the IPv6 protocol.	
IP Auto Configuration	Select the method to configure IPv4 settings.	
	Automatic	Auto-configure IPv6 settings via DHCPv6. Optionally specify the preferred hostname, which must meet the above requirements.
	Static	Manually configure the IPv6 settings. Assign a static IPv6 address, which follows this syntax **IP address/prefix length**. Example: fd07:2fa:6cff:1111::0/128

10.4.2 Configuring Interface Settings

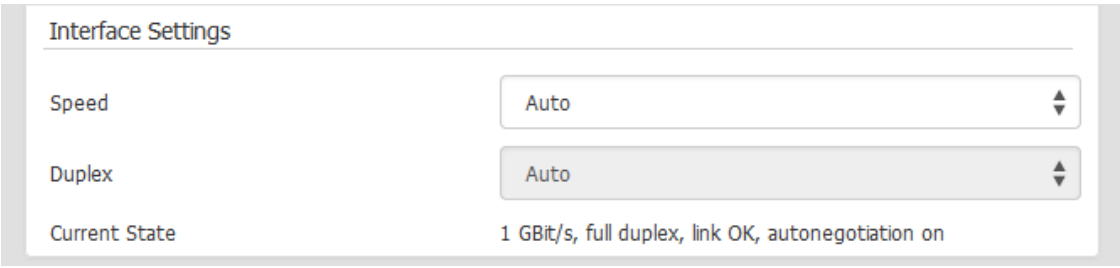


*Fig. 114 SIRA Configuration menu **Device Settings - Date/Time - User Specified Time***

The following settings can be configured:

Field/setting	Description	
Speed	Select a LAN speed.	
	Auto	System determines the optimum LAN speed through auto-negotiation.
	10 MBit/s	Speed is always 10 Mbps
	100 MBit/s	Speed is always 100 Mbps
	1 GBit/s	Speed is always 1 Gbps (1000 Mbps).

Field/setting	Description	
Duplex	Select a duplex mode.	
	Auto	The SIRA Module selects the optimum transmission mode through auto-negotiation.
	Full	Data is transmitted in both directions simultaneously.
	Half	Data is transmitted in one direction (to or from the SIRA Module) at a time.
Current state	Show the LAN's current status, including the current speed and duplex mode.	

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

Common Network Settings:

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

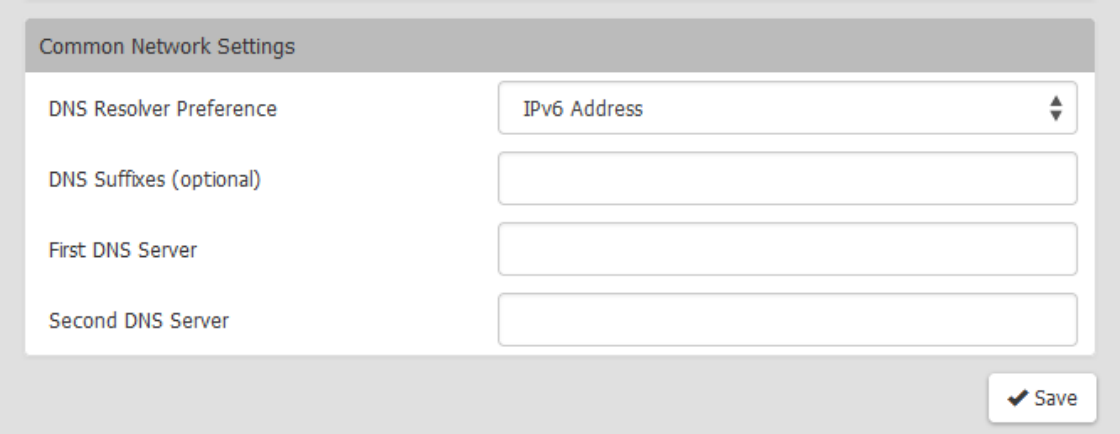


*Fig. 115 SIRA Configuration menu **Device Settings - Network - Common Network Settings***

Field/setting	Description
DNS Resolver Preference	Determine which IP address is used when the DNS resolver returns both IPv4 and IPv6 addresses. • IPv4 Address: Use the IPv4 addresses. • IPv6 Address: Use the IPv6 addresses.
DNS Suffixes (optional)	Specify a DNS suffix name if needed.
First/Second DNS Server	Manually specify static DNS server(s). • If any static DNS server is specified in these fields, it will override the DHCP-assigned DNS server. • If DHCP (or Automatic) is selected for IPv4/IPv6 settings, and there are NO static DNS servers specified, the SIRA Module will use DHCP-assigned DNS servers.

10.5 Network Services

The SIRA Module supports the following network communication services:

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

10.5.1 Discovery

The SIRA Module uses the default Discovery Port 5000 for communication with other products, such as the SIRA User Station. This port could also be used for a future central management solution. The port number can be changed if needed, but it cannot be changed while the device is under central management.

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

To change the default discovery port, proceed as follows:

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

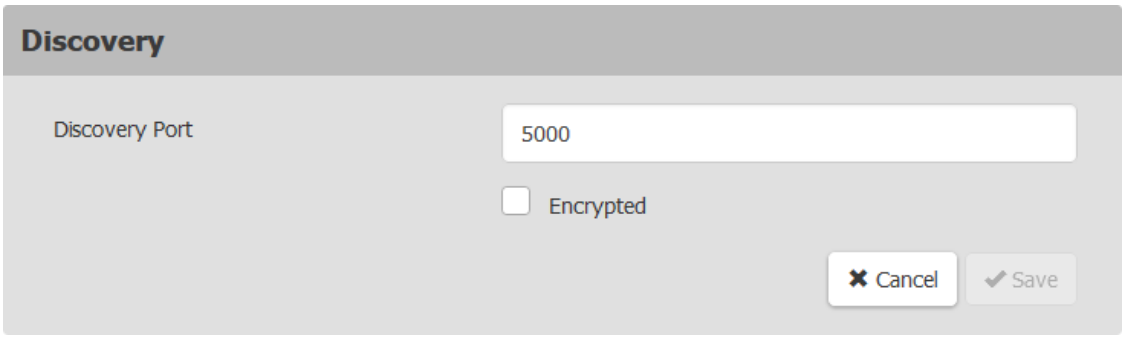


*Fig. 116 SIRA Configuration menu **Device Settings - Network Services - Discovery***

10.5.2 HTTP/HTTPS

The SIRA Module uses the default HTTP/HTTPS ports 80/443. You can change the default if needed. HTTP access will be redirected to HTTPS.

To change the default HTTP/HTTPS ports, proceed as follows:

1. Click **Device Settings > Network Settings > HTTP/HTTPS**.

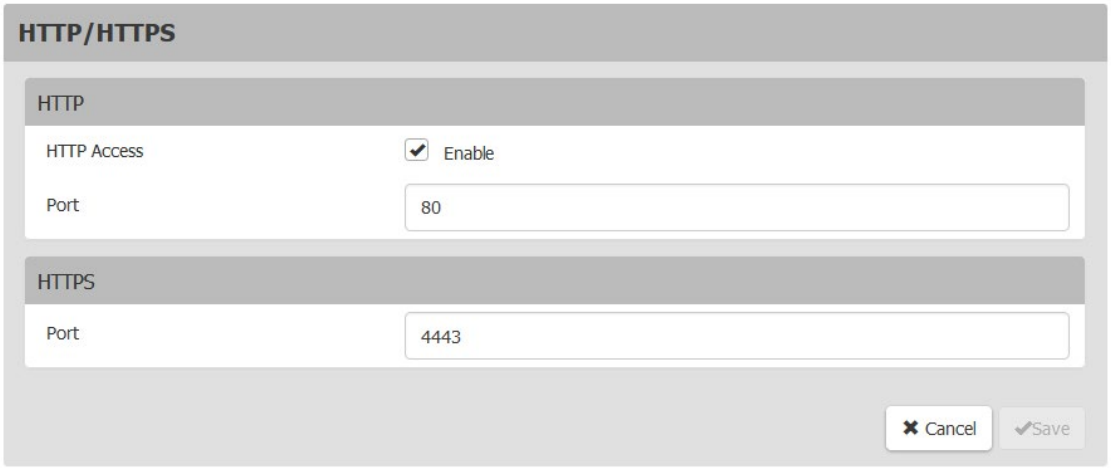


*Fig. 117 SIRA Configuration menu **Device Settings - Network Services - HTTP/HTTPS***

2. Tick the **HTTP Access** checkbox if HTTP needs to be enabled.

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

3. Enter the port numbers.
4. Click **Save**.

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

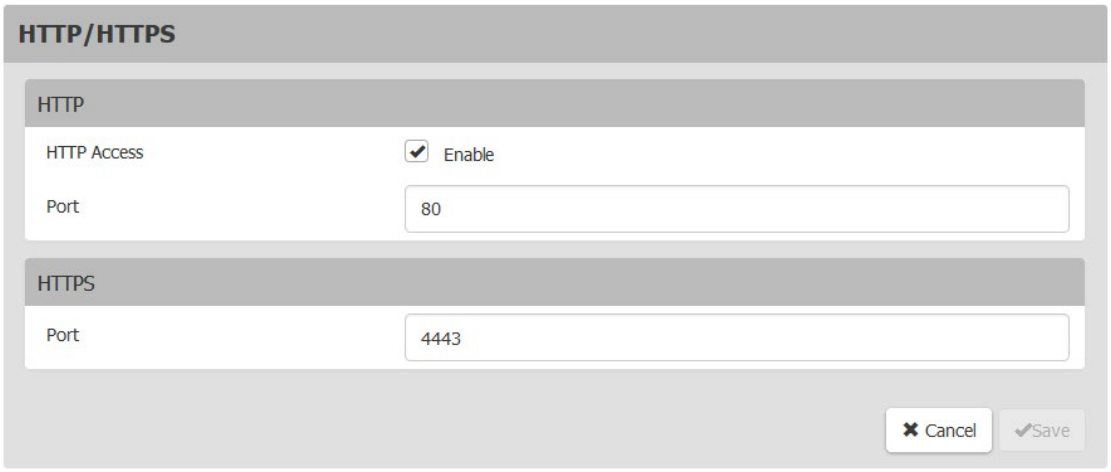


*Fig. 118 SIRA Configuration menu **Device Settings - Network Services - HTTP/HTTPS***

10.5.3 SMTP Server Settings

To send event emails, the event management has to be configured (see chapter 10.2.1, page 108).

If any email messages fail to be sent successfully, the failure event and reason are available in the event log (see chapter 13.2, page 162).

To set SMTP server settings, proceed as follows:

1. Click **Device Settings > Network Services > SMTP Server**.

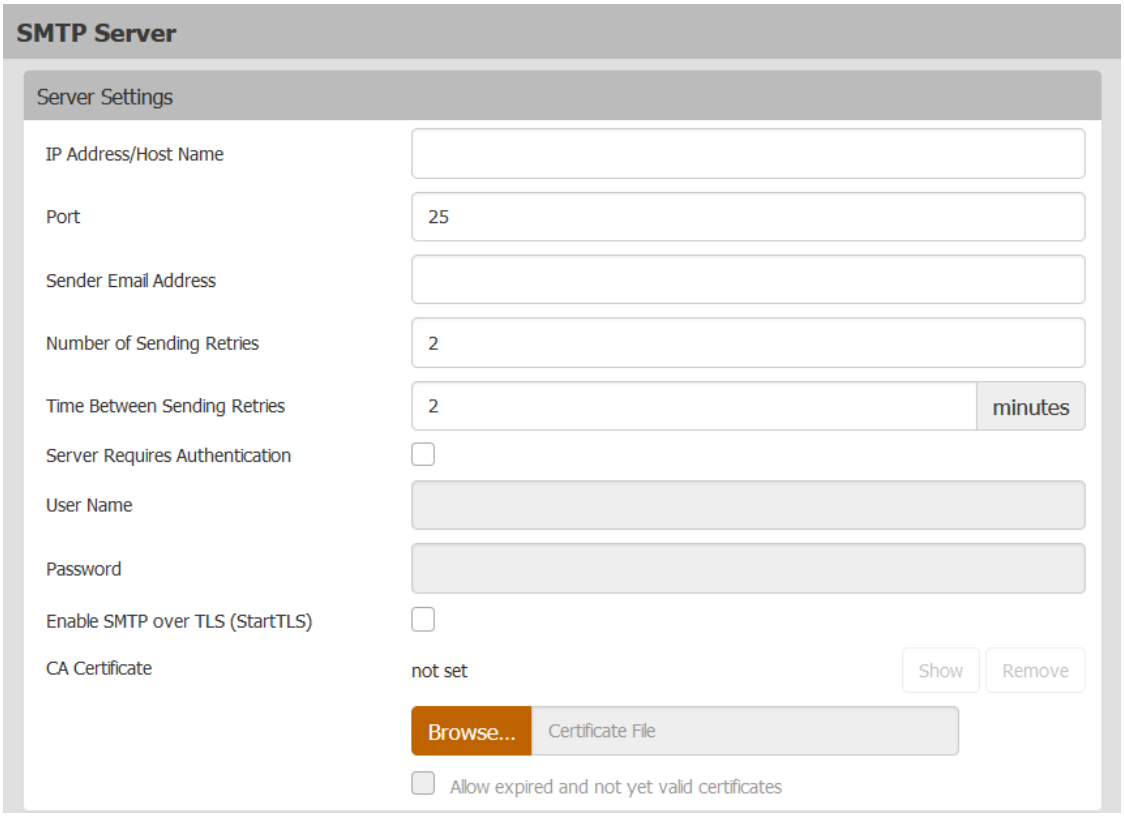


*Fig. 119 SIRA Configuration menu **Device Settings - Network Services - SMTP Server***

2. Enter the information needed:

Field	Description
IP address/host name	Enter the name or IP address of the mail server.
Port	Enter the port number (default 25).
Sender Email Address	Enter an email address for the sender.
Number of Sending Retries	Enter the number of email retries (default 2).
Time Between Sending Retries	Type the interval between email retries in minutes (default 2).
Server Requires Authentication	Tick this checkbox if your SMTP server requires password authentication, then enter the username and password.
User Name	Enter the username (case sensitive, input of minimum 4 up to 64 characters, no spaces allowed.
Password	Enter the password (case sensitive, input of minimum 4 up to 64 characters, spaces are allowed.
Enable SMTP over TLS (StartTLS)	Tick this checkbox if your SMTP server supports TLS.

Field	Description
CA Certificate	➡ Click **Browse…** in the **CA Certificate** section to select and install the certificate file. After importing the certificate: click **Show** to view the installed certificate's content or click **Remove** to delete the installed certificate if it is inappropriate. **Note:** To allow event messages even if any TLS certificate in the selected certificate chain is outdated or not valid yet, tick the **Allow expired and not yet valid certificates** checkbox.

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

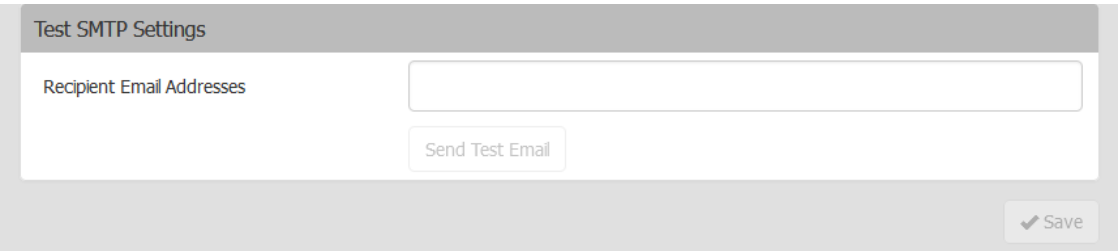


*Fig. 120 SIRA Configuration menu **Device Settings - Network Services - SMTP Server***

4. Click **Save**.

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

10.5.4 SNMP Settings

The SNMP communication between an SNMP manager and the SIRA Module can be enabled or disabled.

To configure SNMP communication, proceed as follows:

1. Click **Device Settings > Network Services > SNMP**.

*Fig. 121 SIRA Configuration menu **Device Settings - Network Services - SNMP***

2. Tick the **Enable SNMP v1 / v2c** and/or **Enable SNMP v3** checkbox to enable or disable the corresponding SNMP communication.
   2.1. The SNMP v1/v2c read-only access is enabled by default. The default **Read community string** is "public".
   2.2. Enter the string in the **Write community string** field to enable read-write access. Usually the string is "private".

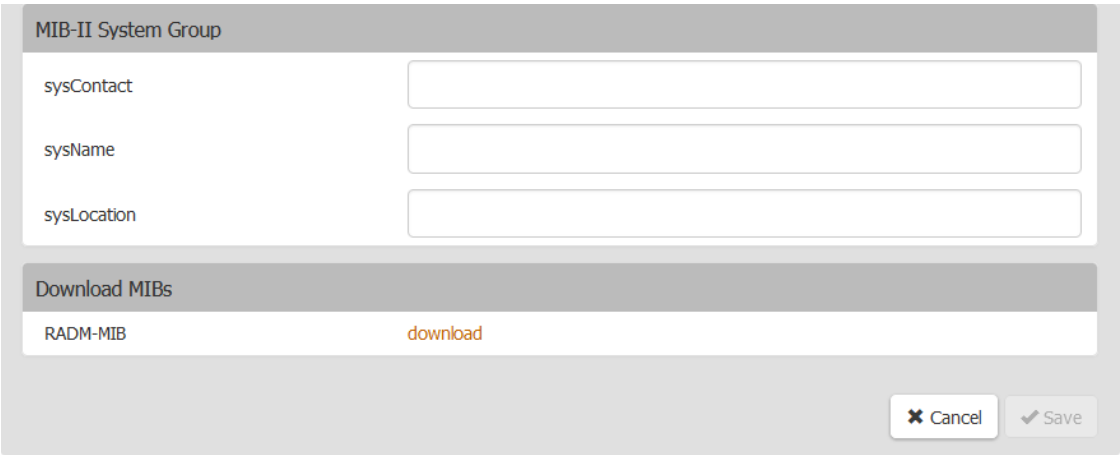


*Fig. 122 SIRA Configuration menu **Device Settings - Network Services - SNMP***

3. Enter the MIB-II system group information, if applicable.
   3.1. sysContact - the contact person in charge of the system
   3.2. sysName - the name assigned to the system
   3.3. sysLocation - the location of the system
4. Click the **download** link to get the SNMP MIB to use with your SNMP manager.
5. Click **Save**.

10.5.5 SSH Settings

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

To configure SSH settings, proceed as follows:

1. Click **Device Settings > Network Services > SSH**.

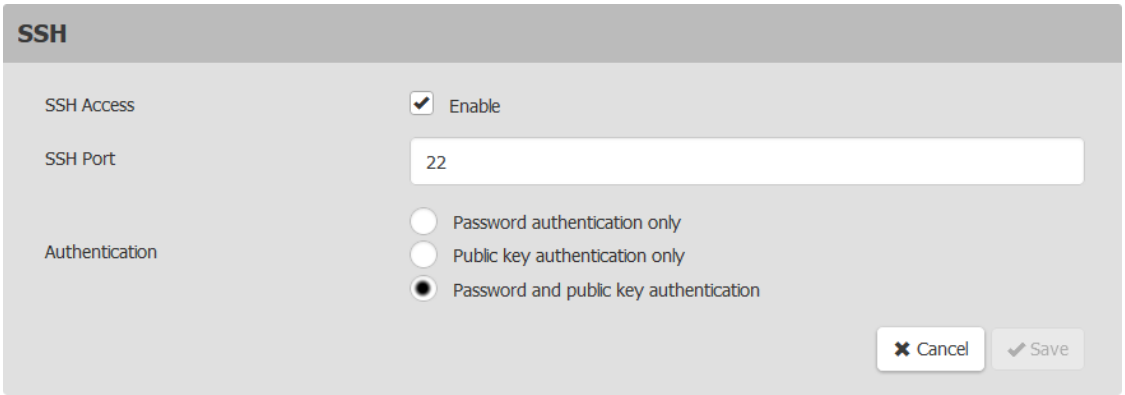


*Fig. 123 SIRA Configuration menu **Device Settings - Network Services - SSH***

2. Tick or clear the **SSH Access** checkbox, to enable or disable SSH access.
3. Enter a port number in the SSH Port field to change the default port 22.
4. Select one of the authentication methods.
   - **Password authentication only**: Enables password-based login only.
   - **Public key authentication only**: Enables public key-based login only.
   - **Password and public key authentication**: Enables both password and public key-based login, which allows either login authentication method to be used. This is the default setting.
5. Click **Save**.

If public key authentication is selected, a valid SSH public key have to be entered for each user profile to log in over the SSH connection (see chapter 11.6.4, page 141).

10.6 Virtual Media Shared Images

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

Requirements

➡ SMB/CIFS support is required on the file server.

10.6.1 Adding Virtual Media Share Settings

To designate file server ISO images for virtual media access, proceed as follows:

1. Click **Device Settings > Network Services > Virtual Media Shared Images**.
   The **Virtual Media Shared Images** list is displayed.

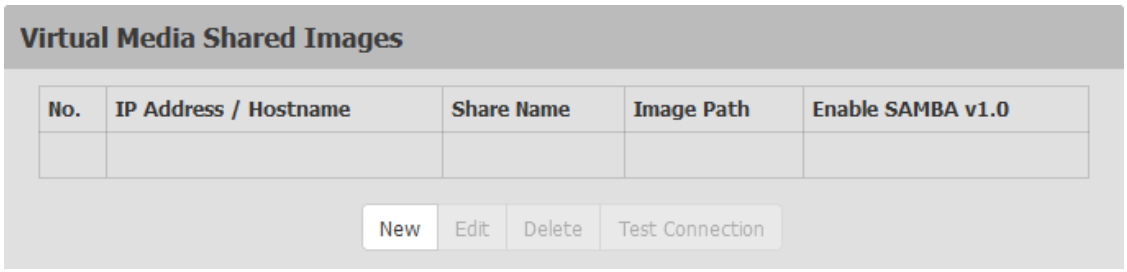


*Fig. 124 SIRA Configuration menu **Device Settings - Virtual Media Shared Images***

The following settings can be configured:

Field	Description
IP Address/Host Name	Host name or IP address of the file server. Up to 248 characters.
Share Name	Share name portion of the ISO image
Image Path	Full path name of the location of the ISO image. For example, /path0/image0.iso, \path1\image1.iso, and so on.
Enable Samba 1.0	Tick the Enable Samba 1.0 checkbox to allow SIRA Module to use an older Samba version. When cleared, Samba 3.0 is used.

2. Click **New** to add a shared image.

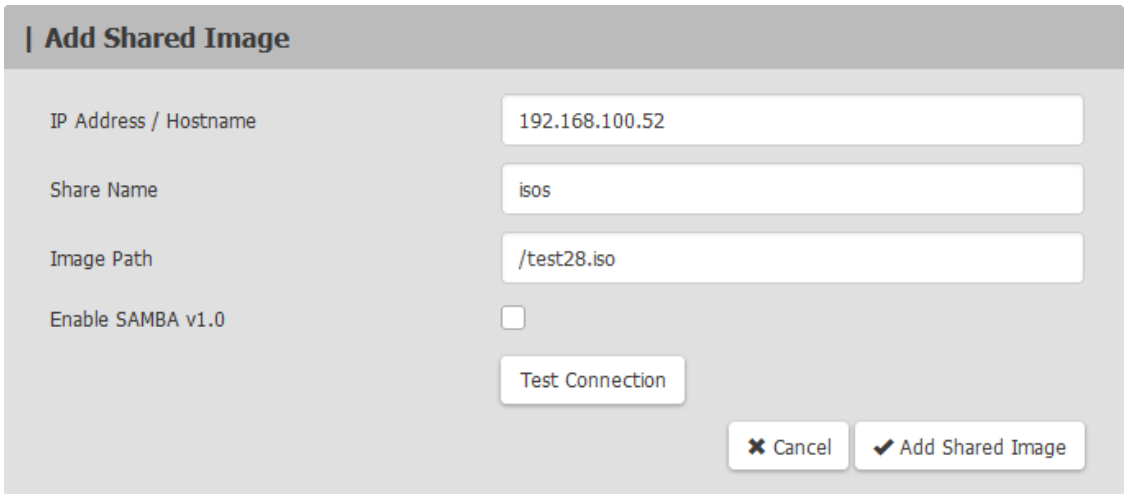


*Fig. 125 SIRA Configuration menu **Device Settings - Virtual Media Shared Images***

3. Enter information about the file server ISO images to be accessed:
   3.1. Enter the IP address or the hostname of the file server in the **IP Address / Host** Name field.
   3.2. Enter a name for the shared image in the **Share Name** field.

3.3. Enter the full path of the ISO image in the **Image Path** field.

3.4. Tick the Enable Samba v1.0 if an older Samba version should be used.

4. Click **Test Connection** to verify.

   A connection dialog appears.

5. Enter the username and password.

6. Click **Test** to perform the connection test.

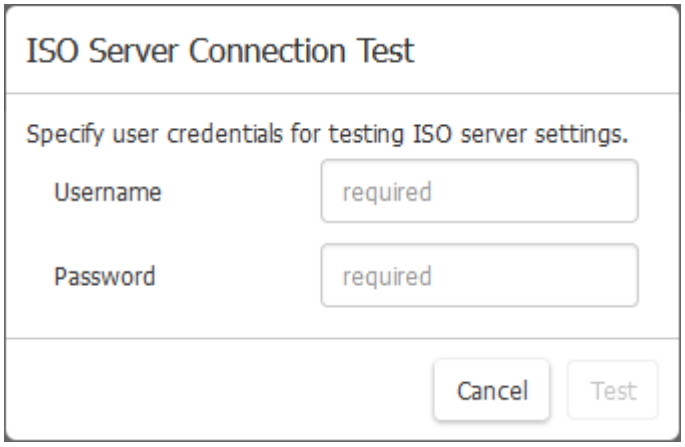


*Fig. 126 SIRA Configuration menu **Device Settings - Virtual Media Shared Images - Connection Test***

7. Click **Add Shared Image** in the **Add Shared Image** menu.

   The new virtual media shared image is listed in the **Virtual Media Shared Images** overview.

   All media specified here are now available for selection in the **Map Virtual Media CD/ISO Image** dialog (see chapter 7.1.10.3, page 60).

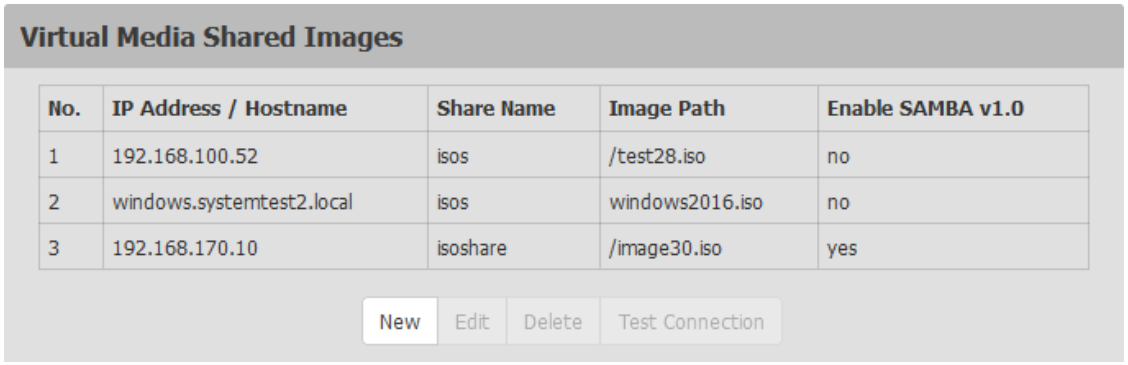


*Fig. 127 SIRA Configuration menu **Device Settings - Virtual Media Shared Images - Overview***

8. To add more file servers, repeat the same steps.

10.6.2 Changing Virtual Media Share Settings

To change virtual media share settings, proceed as follows:

1. Click **Device Settings > Network Services > Virtual Media Shared Images**.
2. Click virtual media share settings by name to select it.

   The selected virtual media share settings is highlighted blue.

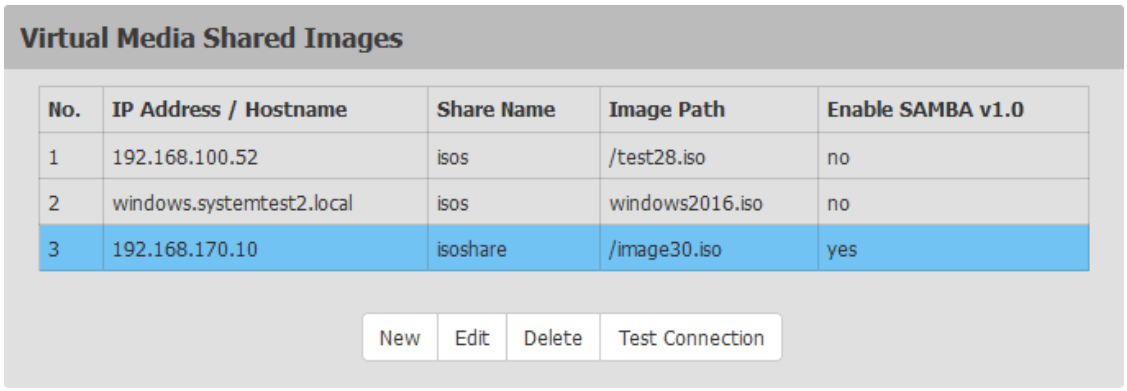


*Fig. 128 SIRA Configuration menu **Device Settings - Virtual Media Shared Images - Selection***

3. Click **Edit** to change to the virtual media share settings.

   The **Edit Virtual Media Share Settings** is displayed.

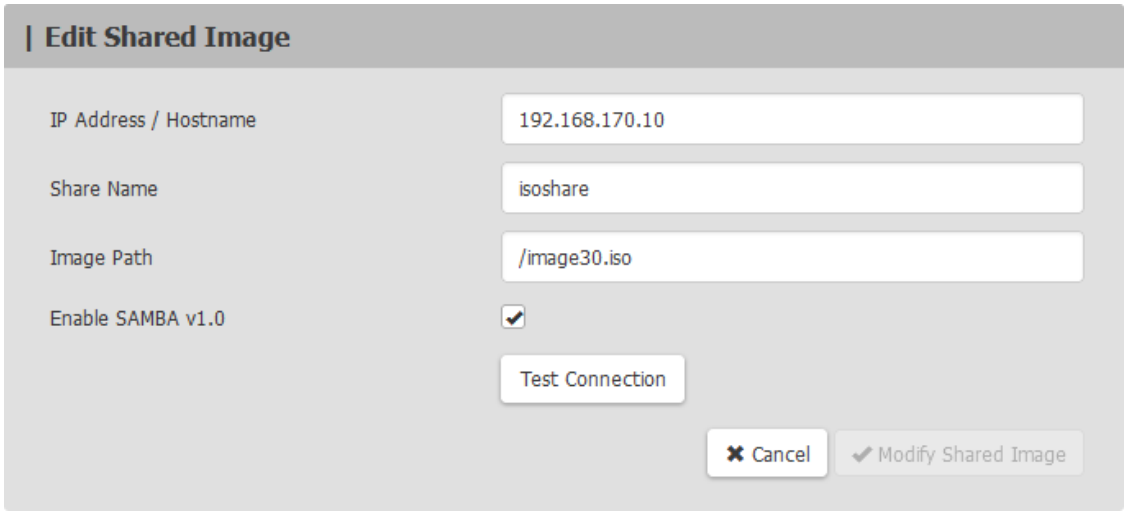


*Fig. 129 SIRA Configuration menu **Device Settings - Virtual Media Shared Images - Edit Virtual Media Share Settings***

4. Change settings as needed.
5. Click **Modify Shared Image** to save the changes.

10.6.3 Deleting Virtual Media Share Settings

To delete virtual media share settings, proceed as follows:

1. Click **Device Settings > Network Services > Virtual Media Shared Images**.
2. Click virtual media share settings by name to select it.

   The selected virtual media share settings is highlighted blue.

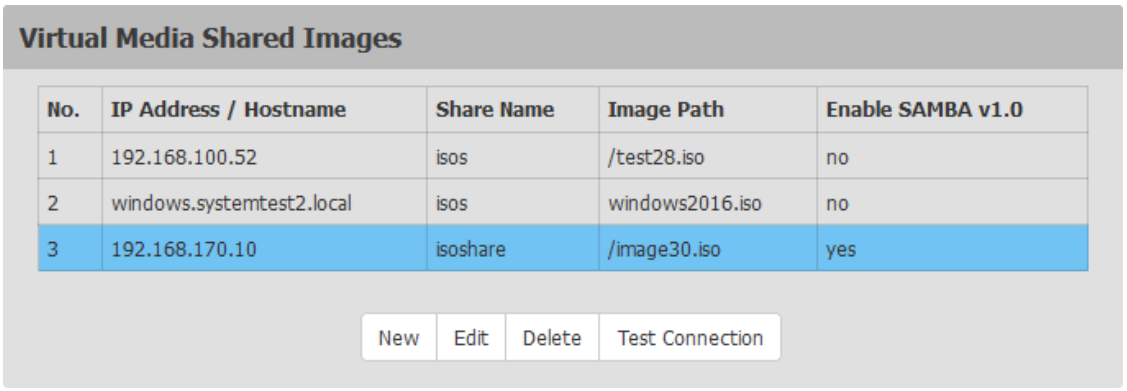


*Fig. 130 SIRA Configuration menu **Device Settings - Virtual Media Shared Images - Selection***

3. Click **Delete** to remove the virtual media share settings.

   A **Virtual Media Share settings deletion** message appears.
4. Click **Delete** to delete the selected virtual media share settings.

11 User Management

The SIRA Module can be configured for local or remote authentication. For other security settings related to user management, see **Security** chapter 11.6.4, page 141.

➡ Click **User Management** to view the submenu options.

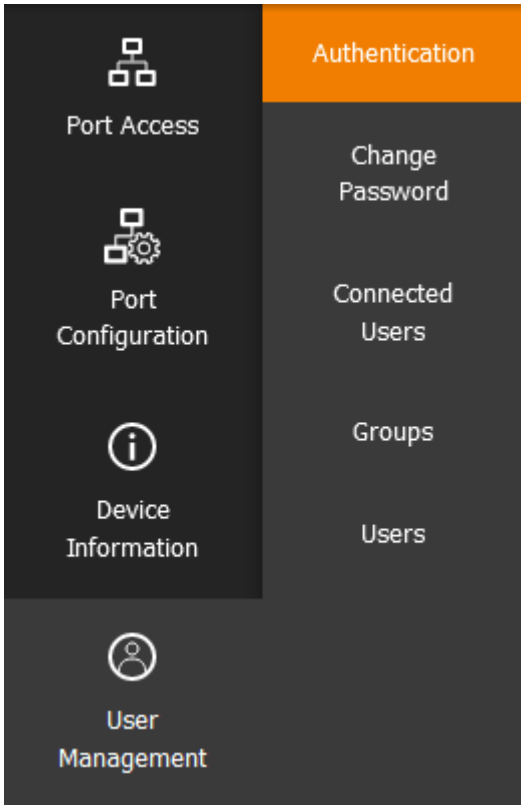


*Fig. 131 SIRA configuration menu **User Management - Submenu options***

11.1 Gathering LDAP/Radius Information

To configure external authentication, the following information about the external Authentication and Authorization (AA) server settings are required. If you are not familiar with these settings, consult your AA server administrator for help.

Radius authentication:

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

11.2 Configuring Authentication

IHSE uses TLS instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0.
➡ Ensure the network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

The SIRA Module supports:

- Local user database on the SIRA Module
- LDAP
- Radius

By default, the SIRA Module is configured for local authentication. Using this method, only needs to create user accounts (see chapter 11.6.3, page 141).

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

If you would like local authentication to be available as a backup method when external authentication is not available, create user accounts on the SIRA Module in addition to providing the external AA server data. Note that local and external authentication cannot be used simultaneously. When configured for external authentication, all SIRA Module users must have an account on the external AA server.

Local-authentication-only users will have no access when external authentication is enabled, except for the admin, who can always access the SIRA Module.

To select authentication type, proceed as follows:

1. Click **User Management > Authentication**.
   The **Authentication** menu is displayed.

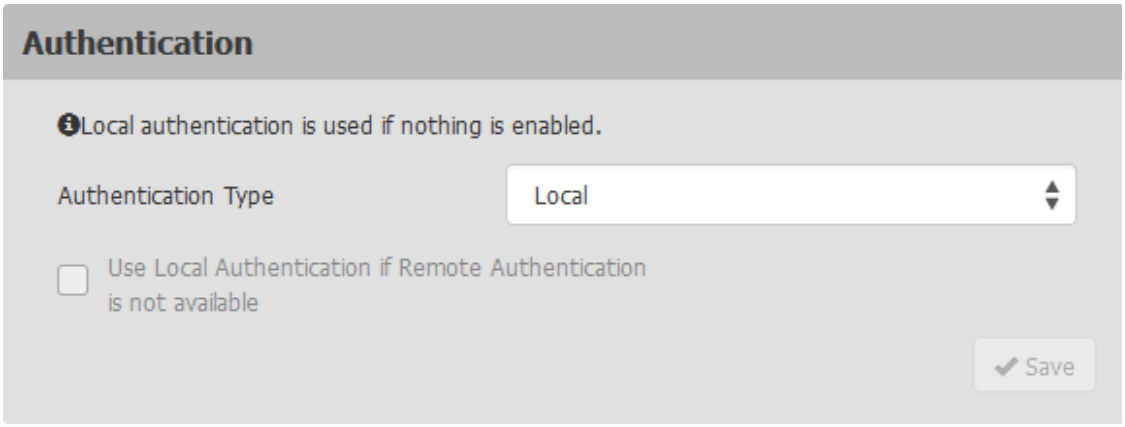


*Fig. 132 SIRA Configuration menu **User Management - Authentication - Authentication Type***

2. Select the desired **Authentication Type**:
   - Local
   - LDAP
   - Radius
3. Tick the **Use Local authentication if Remote Authentication is not available** checkbox to allow local authentication as a backup method when external authentication is not available, such as when the server is down.
4. Click **Save**.
   The selected authentication type is enabled.

For help with adding external servers, see **LDAP Authentication** chapter 11.3.1, page 130 and **Radius Authentication** chapter 11.3.3, page 134).
For help with adding users, see chapter 11.7.2, page 140).

11.2.1 LDAP Authentication

Gather the information to add LDAP servers to the SIRA Module (see chapter 11.1, page 129).

To add LDAP servers, proceed as follows:

1. Click **User Management > Authentication**.
2. Click **New** in the **LDAP Servers** section.

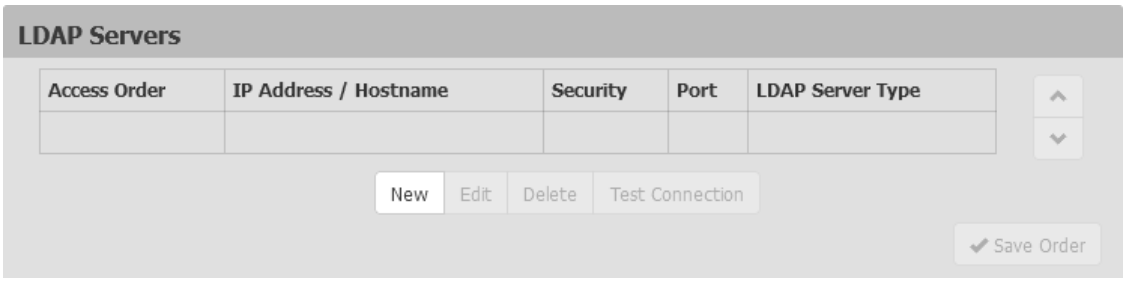


*Fig. 133 SIRA Configuration menu **User Management - Authentication - LDAP Servers***

The **Add LDAP Server** menu appears.

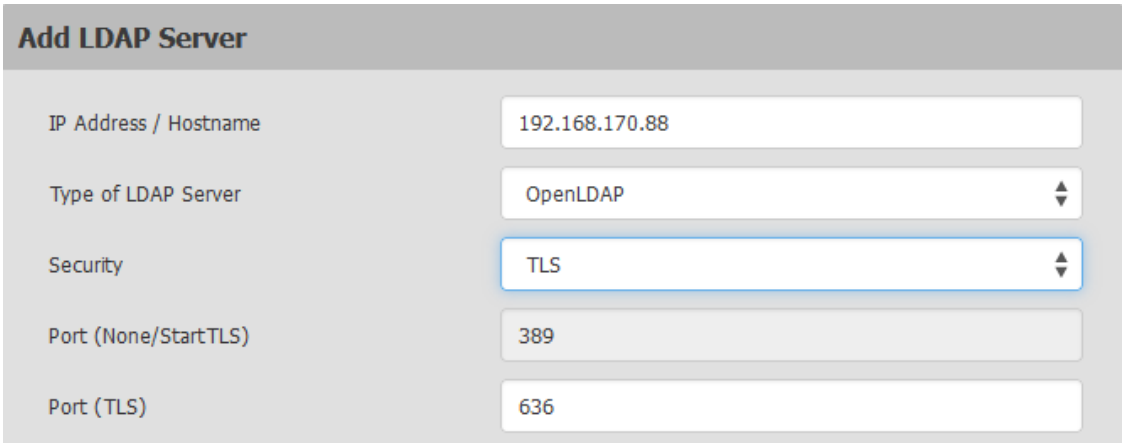


*Fig. 134 SIRA Configuration menu **User Management - Authentication - LDAP Servers - Add LDAP Server***

3. Enter the LDAP server details.

Field	Descprition
IP Address / Hostname	IP address or hostname of the LDAP/LDAPS server. Without encryption enabled, type either the domain name or IP address in this field but type the fully qualified domain name if encryption is enabled.
Type of LDAP Server	• OpenLDAP • Microsoft Active Directory **Note:** If using an OpenLDAP server, consult the LDAP administrator for the Bind Distinguished Name (DN) and password. If using a Microsoft Active Directory server, consult the AD administrator for the name of the Active Directory Domain.

Field	Descprition
Security	Type of LDAP Security: • StartTLS • TLS • None Using TLS encryption allows the SIRA Module to communicate securely with the LDAPS server. **Note:** If Secure LDAP is in use, consult the LDAP administrator for the CA certificate file.
Port (None/StartTLS)	Network port used by the LDAP server (default 389).
Port (TLS)	Configurable only when **TLS** is selected in the **Security** field. The default port is 636 or specify another port.

To manage the CA Certificate, proceed as follows:

1. Tick the **Enable verification of LDAP Server Certificate** checkbox if it is required to validate the LDAP server's certificate by the SIRA Module prior to the connection.

   If the certificate validation fails, the connection is refused.

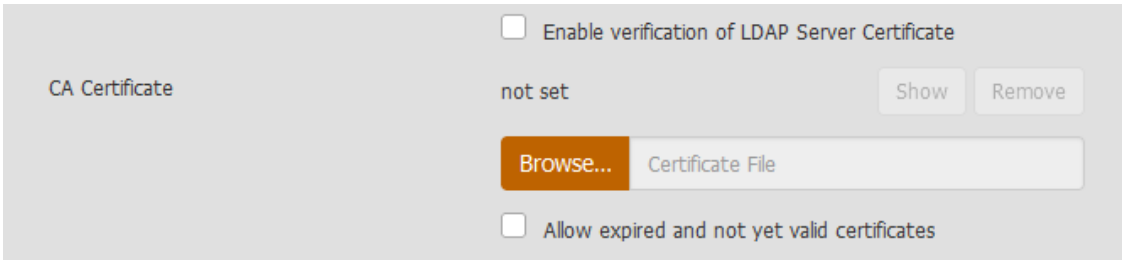


*Fig. 135 SIRA Configuration menu **User Management - Authentication - LDAP Servers - Add LDAP Server - CA Certificate***

2. Consult the AA server administrator to get the CA certificate file for the LDAPS server.
3. Click **Browse…** in the **CA Certificate** section to select and install the certificate file.

   After importing the certificate: click **Show** to view the installed certificate's content or click **Remove** to delete the installed certificate if it is inappropriate.
4. Tick the **Allow expired and not yet valid certificates** checkbox to allow event messages even if any TLS certificate in the selected certificate chain is outdated or not valid yet.

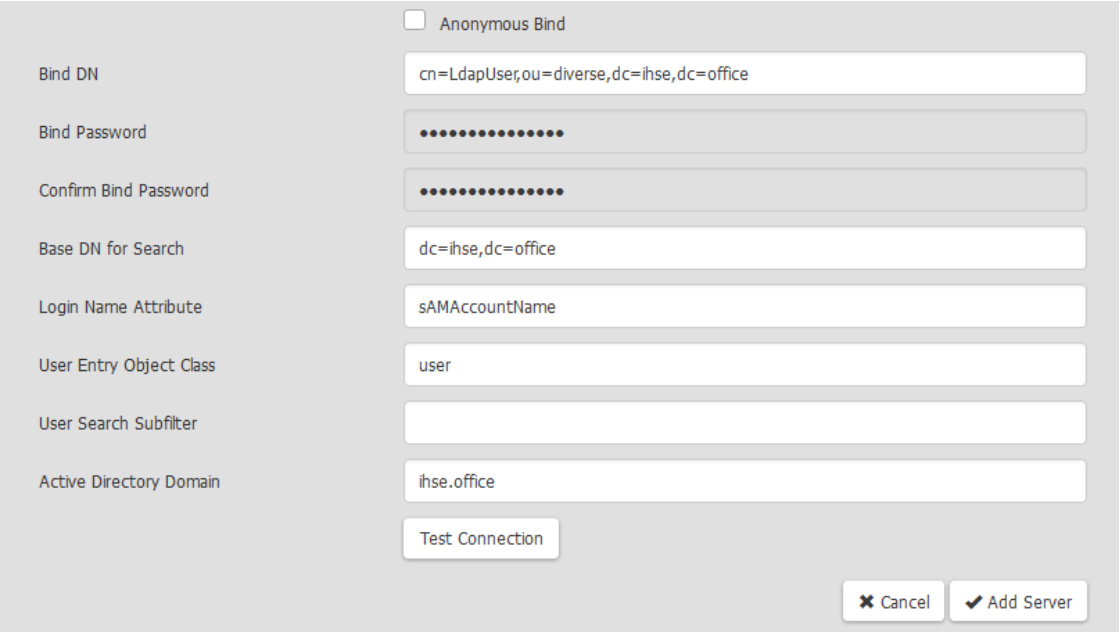


*Fig. 136 SIRA Configuration menu **User Management - Authentication - LDAP Servers - Add LDAP Server***

5. Enter the following data if required:

Field	Descprition
Bind DN	Bind Distinguished Name (DN) Required after clearing the Anonymous Bind checkbox. Distinguished Name (DN) of the user who is permitted to search the LDAP directory in the defined search base. **Note:** The Bind user must have access to the “memberOf” LDAP attribute. The “memberOf” attribute is used to get group memberships.
Bind Password	Required after clearing the Anonymous Bind checkbox.
Confirm Bind Password	Enter the Bind password.
Base DN for Search	The Base DN of the server (used for searching for users), the search base, which is the starting point of the LDAP search. Example: ou=dev,dc=example,dc=com
Login Name Attribute	The attribute (or AuthorizationString) of the LDAP user class which denotes the login name. Usually, it is the uid.
User Entry Object Class	The object class for user entries. Usually, it is inetOrgPerson.
User Search Subfilter	Search criteria (or BaseSearch) for finding LDAP user objects within the directory tree.
Active Directory Domain	The name of the Active Directory Domain. Example: testradius.com

6. Click **Test Connection** to check if the SIRA Module can connect with the server.

   A connection dialog appears.

7. Enter the username and password.

8. Click **Test** to perform the connection test.

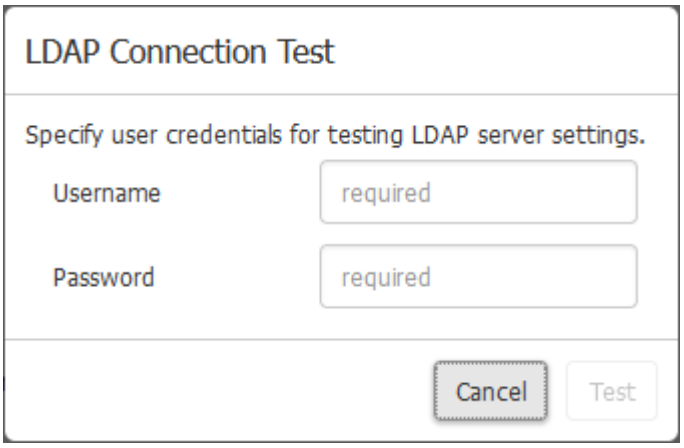


*Fig. 137 SIRA Configuration menu **User Management - Authentication - LDAP Servers - Add LDAP Server - Test Connection***

9. Click **Add Server** in the **Add Server** menu

   The new LDAP server is listed on the **Authentication** page under **LDAP Servers**.

10. To add more servers, repeat the same steps.
11. Click or on the **Authentication** page under **LDAP Servers** to set the order if having multiple servers.
12. Click **Save Order**.

To start using these settings, make sure **LDAP** is selected and saved in the **Authentication Type** field (see chapter 11.2, page 130).

11.2.2 Returning User Group Information from Active Directory Server

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

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

To enable your AD server on the SIRA Module, proceed as follows:

1. Using the SIRA Module, create special groups and assign proper permissions and privileges to these groups. For example, create groups such as KVM_Admin and KVM_Operator.
2. On the Active Directory server, create new groups with the same group names as in the previous step.
3. On the AD server, assign the SIRA Module users to the groups created in step 2.
4. From the SIRA Module, enable and configure the AD server properly (see chapter 11.2.1, page 131)

Important Notes

- The Group Name is case sensitive.
- The SIRA Module provides the following default groups that cannot be changed or deleted: **Admin** and **<Unknown>**. Verify that the Active Directory server does not use the same group names.

- If the group information returned from the Active Directory server does not match the SIRA Module group configuration, the SIRA Module automatically assigns the group of **<Unknown>** to users who authenticate successfully.
- If using a dial back number, the following case-sensitive has to be entered string: `msRADIUSCallbackNumber`.
- Based on recommendations from Microsoft, Global Groups with user accounts should be used, not Domain Local Groups.

11.2.3 Radius Authentication

Gather the information to add Radius servers to the SIRA Module (see chapter 11.1, page 129).

To add Radius servers, proceed as follows:

1. Click **User Management > Authentication**.
2. Click **New** in the **Radius Servers** section.

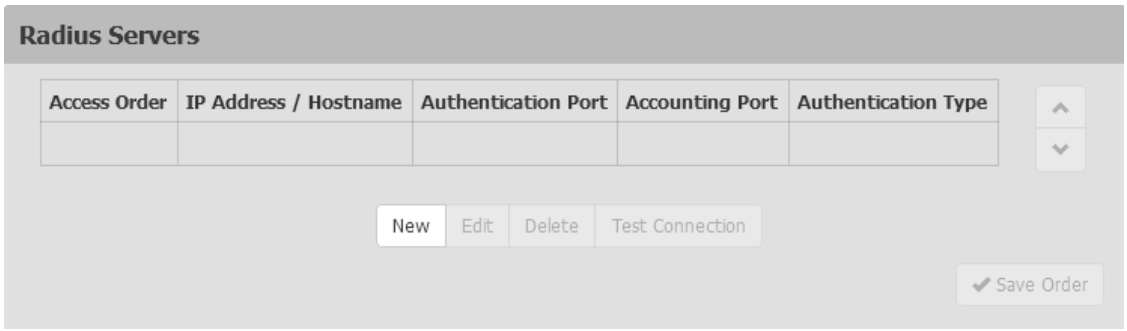


*Fig. 138 SIRA Configuration menu **User Management - Authentication - Radius Servers***

The **Add LDAP Server** menu appears.

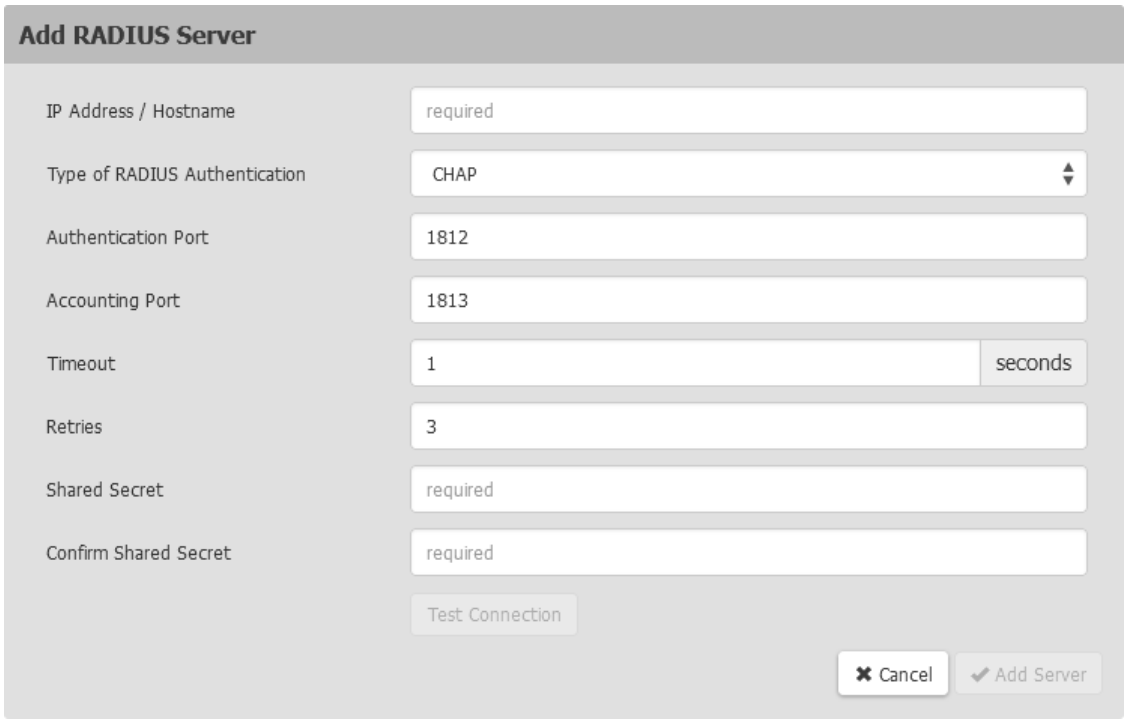


*Fig. 139 SIRA Configuration menu **User Management - Authentication - Radius Servers - Add Radius Server***

3. Enter the Radius server details.

Field	Descprition
IP Address / Hostname	The IP address or hostname of your Radius server.
Type of RADIUS Authentication	Select an authentication protocol. • PAP (Password Authentication Protocol) • CHAP (Challenge Handshake Authentication Protocol) • MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol Version 2) CHAP is generally considered more secure because the username and password are encrypted, while in PAP they are transmitted in the clear.
Authentication Port	Enter a new port number if necessary (default 1812).
Accounting Port	Enter a new port number if necessary (default 1813).
Timeout	Type the time period (in seconds) to establish contact with the Radius server before timing out.
Retries	Type the number of retries.
Shared Secret	Type the shared secret which is necessary to protect communication with the Radius server.
Confirm Shared Secret	Repeat the shared secret to confirm.

4. Click **Test Connection** to check if the SIRA Module can connect with the server.
   A connection dialog appears.
5. Enter the username and password.
6. Click **Test** to perform the connection test.

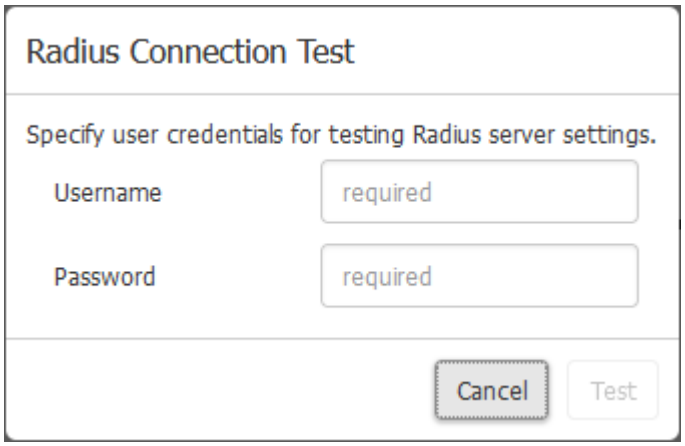


*Fig. 140 SIRA Configuration menu **User Management - Authentication - Radius Servers - Add Radius Server - Test Connection***

7. Click **Add Server** in the **Add Server** menu.
   The new Radius server is listed in the **Authentication** menu under **LDAP Servers**.
8. To add more servers, repeat the same steps.
9. Click or on the **Authentication** page under **LDAP Servers** to set the order if having multiple servers.
10. Click **Save Order**.
11. To start using these settings, make sure **Radius** is selected and saved in the **Authentication Type** field (see chapter 11.2, page 130).

11.2.4 Returning User Group Information via RADIUS

When a Radius authentication attempt succeeds, the SIRA Module determines the permissions for a given user based on the permissions of the user's group.

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

```
Raritan:G{GROUP_NAME}
```

11.3 Disabling External Authentication

To disable external authentication, proceed as follows:

1. Click **User Management > Authentication**.
2. Select **Local** in the **Authentication Type** drop-down menu.
3. Click **Save**.

   Local is enabled as authentication type.

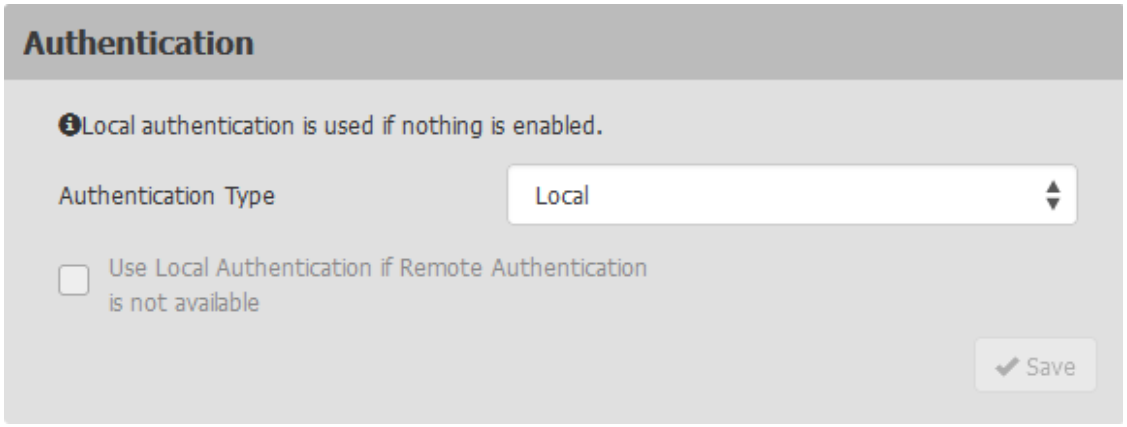


*Fig. 141 SIRA Configuration menu **User Management - Authentication - Authentication Type - Local***

11.4 Changing the Password

To change the password, proceed as follows:

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

*Fig. 142 SIRA Configuration menu **User Management - Authentication - Change Password***

11.5 Connected Users

Users that have logged in to the SIRA Module and their status can be checked. With administrator privileges, any user's connection can be terminated to the SIRA Module.

To view and manage connected users, proceed as follows:

1. Click **User Management > Connected Users**.

   A list of logged-in users is shown.

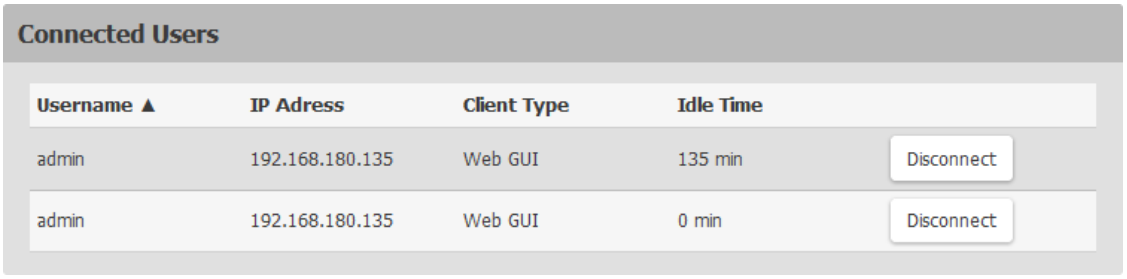


*Fig. 143 SIRA Configuration menu **User Management - Connected Users***

The following parameters can be configured:

Column	Description
Username	The login name of each connected user.
IP Address	The IP address of each user's host. For the login via a local connection (USB), **<local>** is displayed instead of an IP address.
Client Type	Web GUI: Refers to the web interface.
Idle Time	The length of time for which a user remains idle.

To disconnect users, proceed as follows:

1. Click **Disconnect** to disconnect any user.
2. Click **Disconnect** on the confirmation message.

   The user is forced to log out.

11.6 Users and Groups

The SIRA Module is shipped with one built-in administrator account: **admin**, which is ideal for initial login and system administration. This account cannot be deleted, and permissions cannot be changed, but the username and password can be changed.

All users must have a user account, containing the login name and password. Multiple users can log in simultaneously using the same login name.

Privileges are assigned at the Group level, therefore add groups, and assign users to groups. An admin group is created by default and has exclusive privileges (see chapter 11.6.1, page 139).

When a user is assigned to multiple groups with different privilege levels, the highest-level of access specified is allowed to the user. User group privilege changes take effect for the users in the group at the next login.

11.6.1 Admin Group Special Privileges

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

- Backup/Restore
- Disconnect Connected users
- Reset to Factory Defaults
- Diagnostics
- Enable SNMPv3 in the SNMP agent (SNMP gets and sets)
- Configure SNMPMv3 user parameters
  - Security Level
  - Authentication Protocol
  - Authentication Password
  - Privacy Password
  - Privacy Protocol

11.6.2 Adding Groups

To add groups, proceed as follows:

1. Click **User Management > Groups**.
2. Click  to add a group.

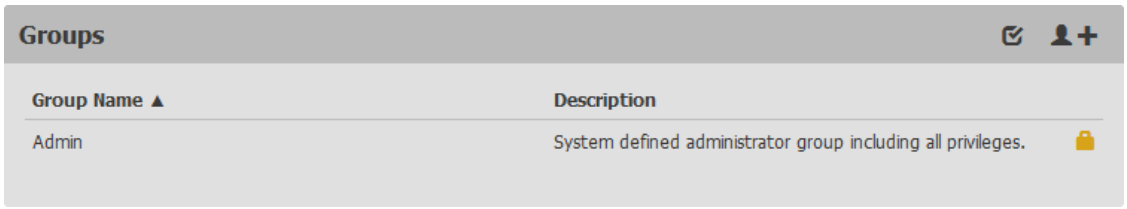


*Fig. 144 SIRA Configuration menu **User Management - Groups***

The **New Group** menu is shown.

*Fig. 145 SIRA Configuration menu **User Management - Groups - New Group - Settings***

3. Complete the **New Group** settings:

Field/setting	Description
Group Name	• 1 to 32 characters • Case sensitive • Spaces are permitted.
Description	• Enter a description of the group's role. • Up to 64 characters.

4. In the **Privileges** section select the **Privileges** assigned to this group. All tasks noted here as exclusions are available exclusively to the admin group (see chapter 11.6.1, page 139).

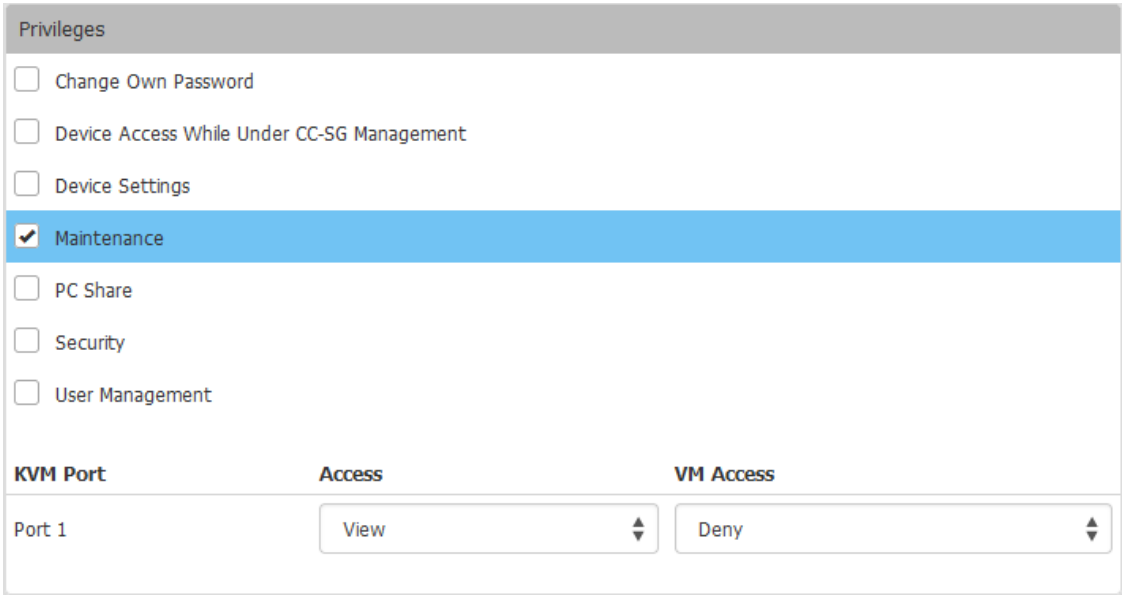


*Fig. 146 SIRA Configuration menu **User Management - Groups - New Group - Privileges***

Field/setting	Description	
Change Own Password	Allows users to change their password.	
Device Settings	All functions in the **Device Settings** menu except enable and configure SNMPv3.	
Maintenance	All functions in the **Maintenance** menu except **Backup/Restore** and **Reset to Factory Defaults**.	
PC Share	Simultaneous access to the same target by multiple users.	
Security	All functions in the **Security** menu.	
User Management	All functions in the User Management menu except Disconnect Users	
KVM Port	Access	• Deny • View • Control
	VM Access	• Deny • Read-only • Read-write

Some privileges require certain access permission. If the needed permissions are not set, an error message will appear.

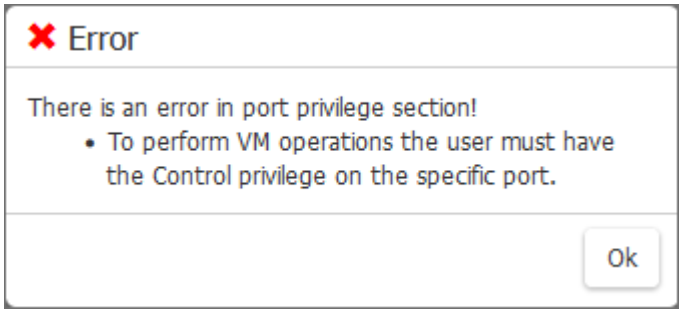


*Fig. 147 SIRA Configuration menu **User Management - Groups - New Group - Privileges - Error***

5. The **Restrictions** section has options for restricting client views and blocking keys.
   - Select **Hide Client Toolbar and Menu Bar** to remove these components from view for this group. Scaling and Client Hot Keys for **Single Mouse cursor** and **Full-Screen** will be available.
   - In the **Block Key Stroke** field, select a keycode list to restrict the users in this group from using the keys in the list (see chapter 10.3, page 113).

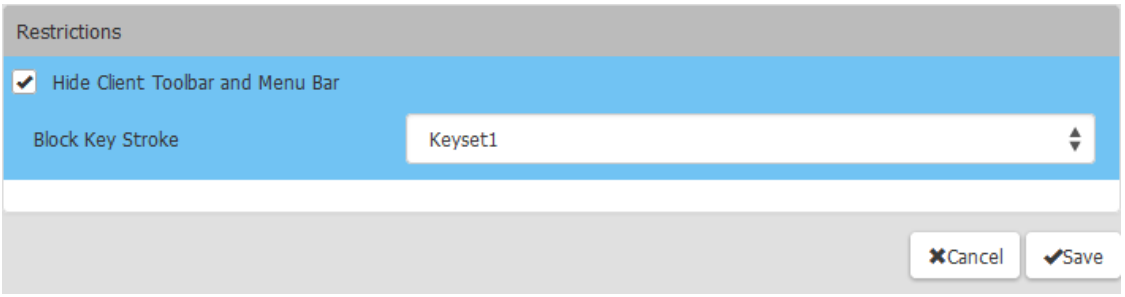


*Fig. 148 SIRA Configuration menu **User Management - Groups - New Group - Restrictions***

6. Click **Save**.
7. To assign these privileges and restrictions to users, select the group when you add or change users.

11.6.3 Deleting a Group

To delete a group, proceed as follows:

1. Click **User Management > Groups**.
2. Click to display the checkboxes for selecting the group to be deleted.

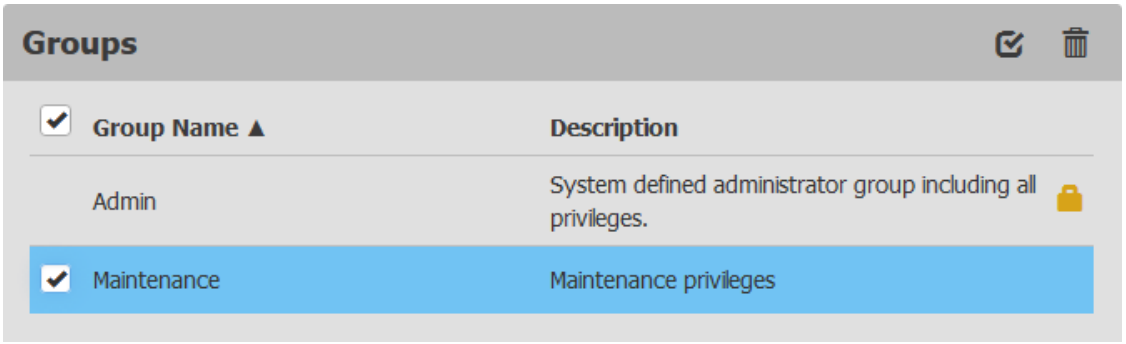


*Fig. 149 SIRA Configuration menu **User Management - Groups - Selection for deletion***

3. Tick the checkboxes of the group to be deleted.
4. Click .

   A **Group Deletion** message appears.
5. Click **Delete** to delete the selected group.

11.6.4 Adding and Assigning Users

Adding a User

To add a user, proceed as follows:

1. Click **User Management > Users**.
2. Click to add a user.

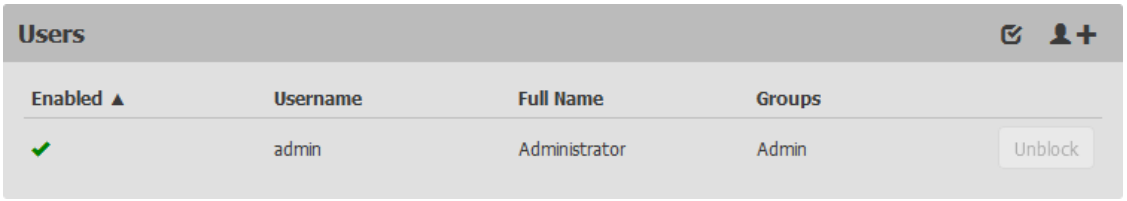


*Fig. 150 SIRA Configuration menu **User Management - Users***

The **New User** menu is shown.

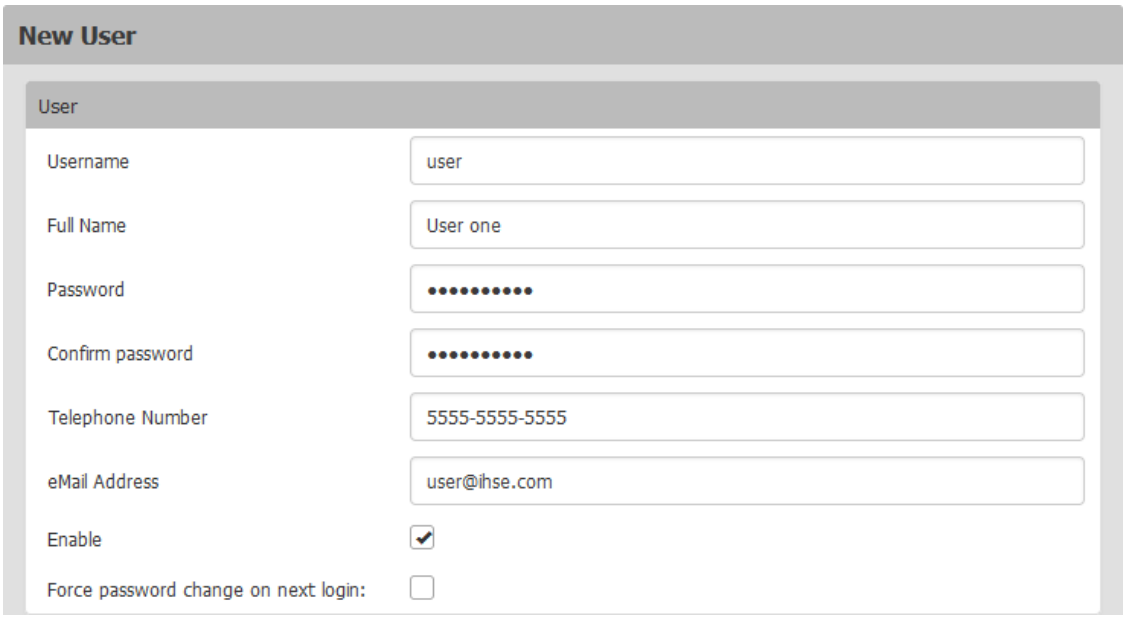


*Fig. 151 SIRA Configuration menu **User Management - Users - New User - User***

3. Complete the **New User** information:

Field/setting	Description
Username	The name the user enters to log in to the SIRA Module. • 4 to 32 characters • Case sensitive • Spaces are NOT permitted.
Full Name	The user's first and last names. • Up to 64 characters
Password Confirm Password	• Must contain at least one digit and one special character (e.g. !, #, $, +, =) • 8 to 64 characters • Case sensitive • Spaces and /-character are permitted.
Telephone Number	The user's telephone number.
eMail Address	The user's email address • Up to 128 characters • Case sensitive
Enable	When selected, the user can log in to the SIRA Module.
Force password change on next login	When selected, a password change request automatically appears the next time the user logs in.

4. The SSH public key is required when public key authentication for SSH is enabled (see chapter 10.5.5, page 124).
5. Open the SSH public key with a text editor.
6. Copy and paste all content in the text editor into the **SSH Public Key** field.

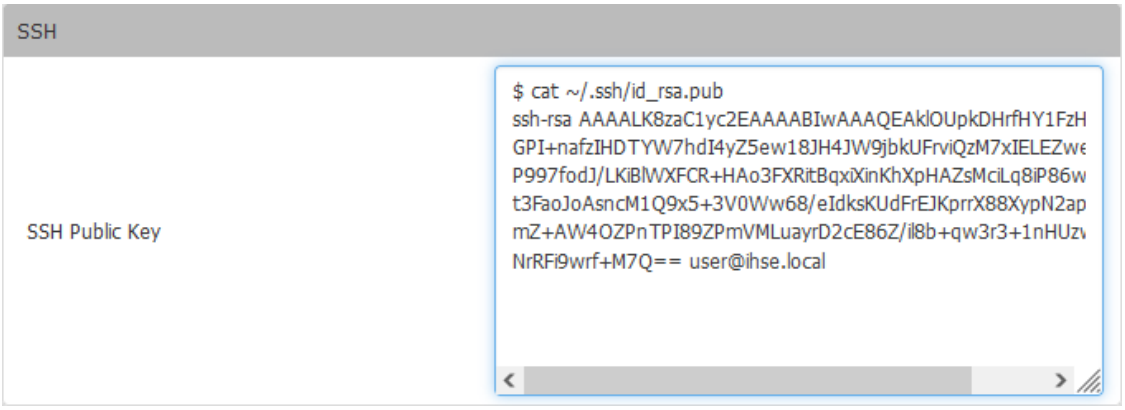


*Fig. 152 SIRA Configuration menu **User Management - Users - New User - SSH***

SNMPv3

The SNMPv3 access permission is disabled by default. This section appears when the permission is enabled in the SNMP settings, or when a user is part of the admin group.

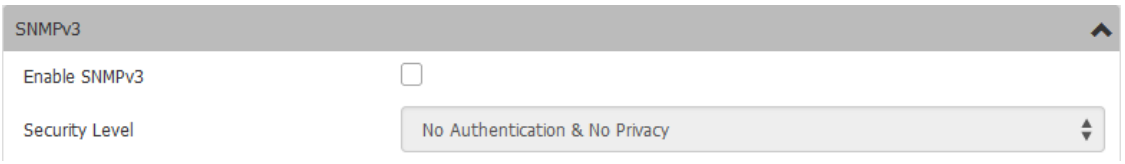


*Fig. 153 SIRA Configuration menu **User Management - Users - New User - SNMPv3***

7. Select the **Security Level** after enabling SNMPv3.

Field/setting	Description
Enable SNMPv3	Tick this checkbox when intending to permit the SNMPv3 access by this user. **Note:** The SNMPv3 protocol must be enabled for SNMPv3 access (see chapter 10.5.4, page 123).
Security Level	Click the field to select a preferred security level from the list: • **None**: No authentication and no privacy. This is the default. • **Authentication**: Authentication and no privacy. • **Authentication & Privacy**: Authentication and privacy.

Authentication Password

This section is configurable only when **Authentication** or **Authentication & Privacy** is selected.

*Fig. 154 SIRA Configuration menu **User Management - Users - New User - SNMPv3 - Authentication Password***

8. Enter the **Authentication Password** settings:

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

Privacy Password

This section is configurable only when **Authentication & Privacy** is selected.

*Fig. 155 SIRA Configuration menu **User Management - Users - New User - SNMPv3 - Privacy Password***

9. Enter the **Privacy Password** settings:

Field/setting	Description
Same as Authentication Password	Tick this checkbox if the privacy password is identical to the authentication password. To specify a different privacy password, clear the checkbox.
Password, Confirm Password	Type the privacy password if the **Same as Authentication Password** checkbox is cleared. The password must consist of 8 to 32 ASCII printable characters.

Protocol

This section is configurable only when **Authentication** or **Authentication & Privacy** is selected.

*Fig. 156 SIRA Configuration menu **User Management - Users - New User - User - SNMPv3 - Protocol***

10. Enter the **Protocol** settings:

Field/setting	Description
Authentication	Click this field to select the desired authentication protocol. Two protocols are available: • MD5 • SHA-1 (default)
Privacy	Click this field to select the desired privacy protocol. Two protocols are available: • DES (default) • AES-128

Assigning a User to a Group

1. In the **Groups** section, select the groups this user belongs to.
   Users have the privileges assigned to their groups.
2. Click **Save**.

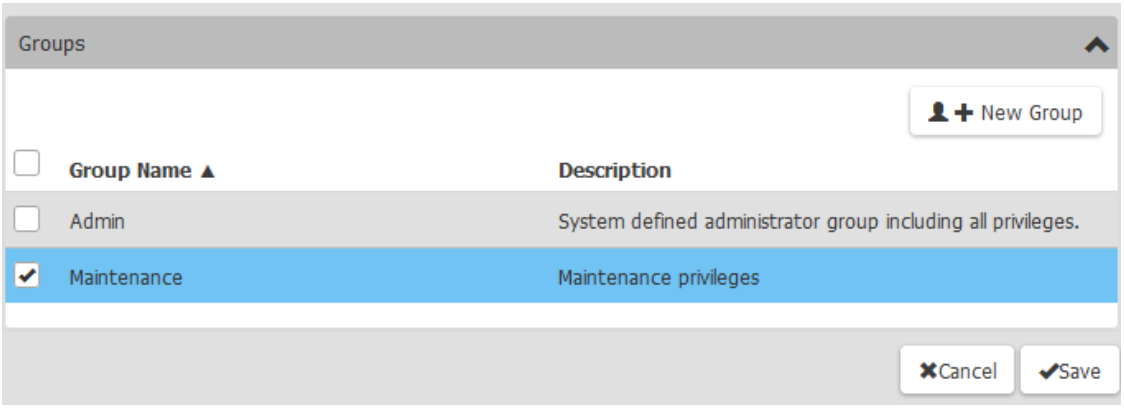


*Fig. 157 SIRA Configuration menu **User Management - Users - New User - Groups***

11.6.5 Changing a User

To change user settings, proceed as follows:

1. Click **User Management > Users**.
2. Click the user to be changed.

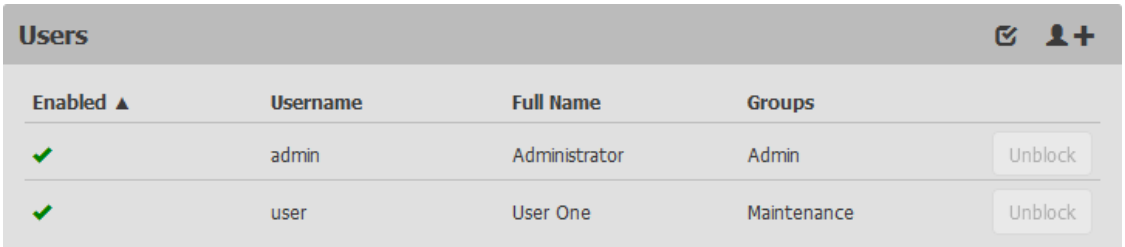


Fig. 158

3. Change the user information as needed.
4. Click **Save**.

11.6.6 Deleting a User

To delete a user, proceed as follows:

1. Click **User Management > Users**.
2. Click to display the checkboxes for selecting the users to be deleted.

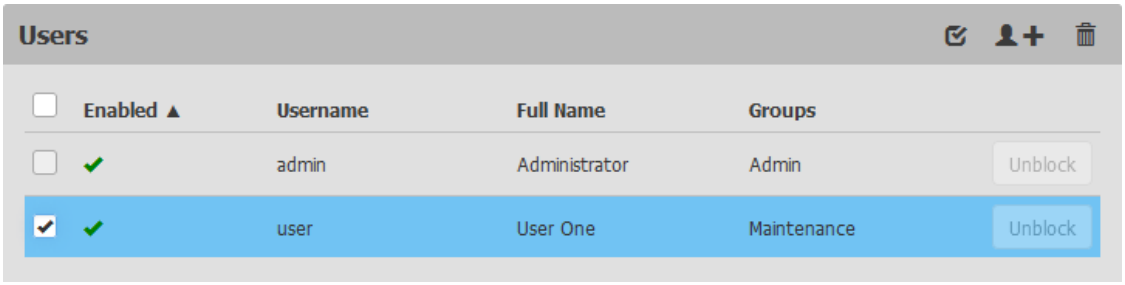


*Fig. 159 SIRA Configuration menu **User Management - Users - Selection for deletion***

3. Tick the checkboxes of the users to be deleted.
4. Click .

   A **User Account Deletion** message appears.
5. Click **Delete** to delete the selected users.

11.7 Settings for a SIRA CON LDAP Connection

To ensure functional SIRA CON LDAP connection, proceed as follows:

1. The Bind user must have access to the “memberOf” LDAP attribute. The “memberOf” attribute is used to get group memberships.

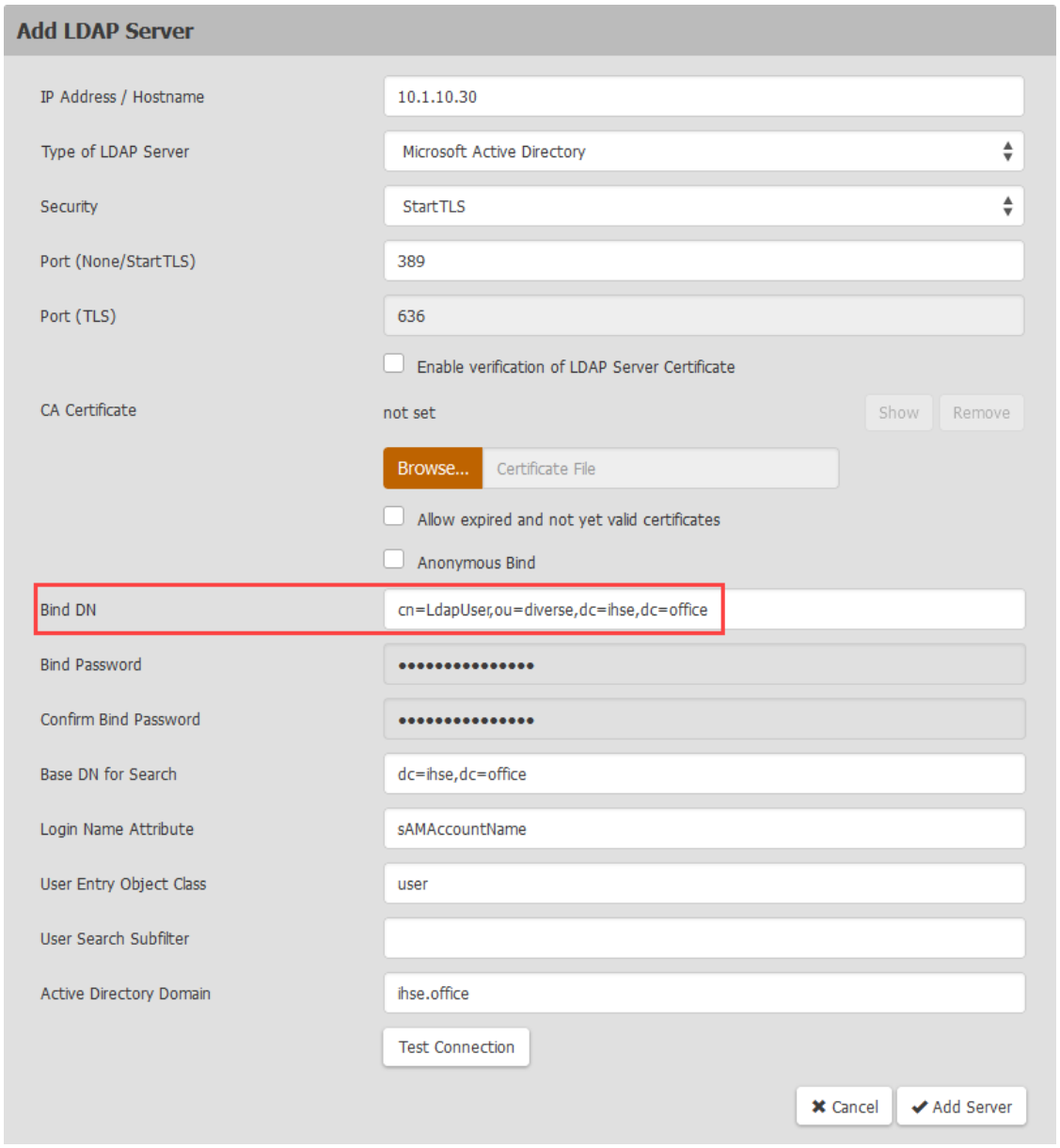


*Fig. 160 SIRA Configuration menu **User Management - Authentication - LDAP Servers - Add LDAP Server - LDAP Requirements***

2. Create at least one group at the SIRA CON manually, which has the exact same name as an existing LDAP group. All LDAP members of this group will get access to the SIRA CON.
3. Define the user rights of the LDAP users at the SIRA CON.

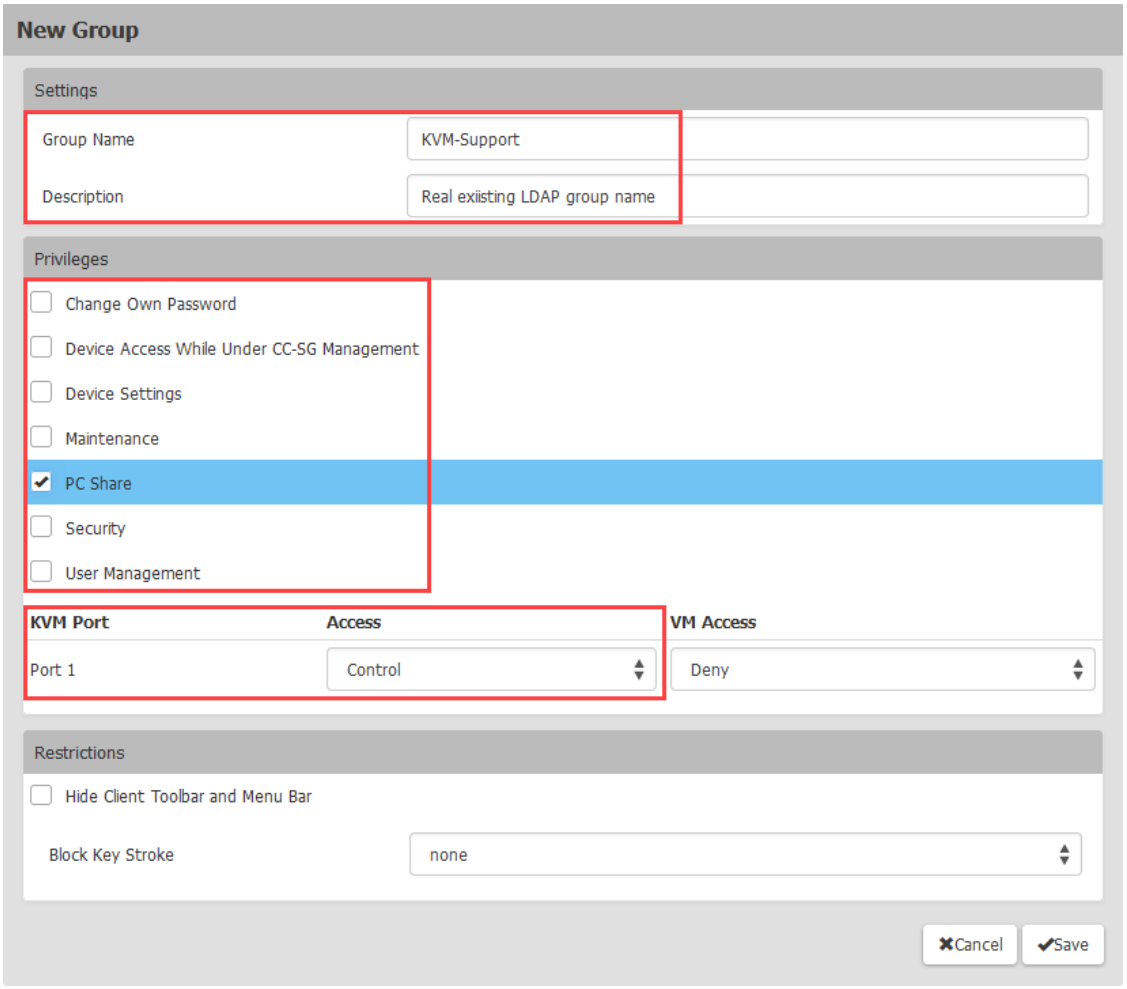


*Fig. 161 SIRA Configuration menu **User Management - Groups - New Group - LDAP Group Settings***

12 Security

12.1 Group Based Access Control

Group based access control rules are similar to IP access control rules, except that they are applied to members of a user group. Groups can thus be granted system permissions based on IP addresses.

The order of role-based access control rules is important, since the rules are executed in numerical order.

To create IPv4 or IPv6 group based access control rules, proceed as follows:

1. Click **Security > Group Based Access Control**.

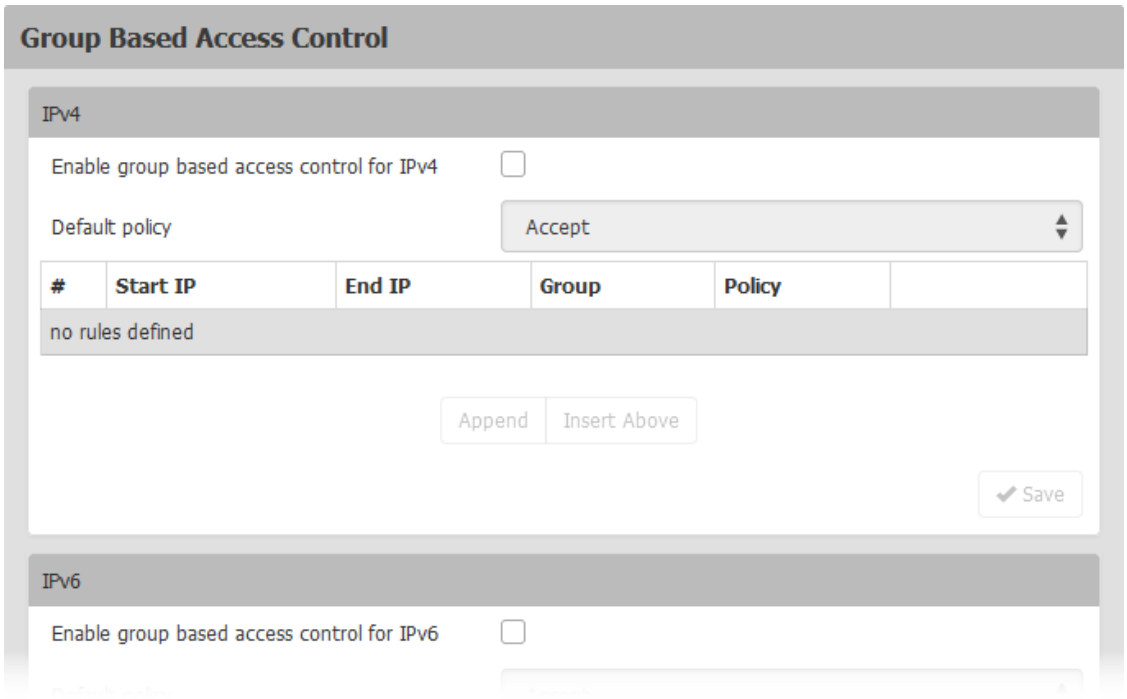


*Fig. 162 SIRA Configuration menu **Security - Group Based Access Control - Overview***

2. Tick the **Enable Group Based Access Control for IPv4** checkbox or scroll down to tick the checkbox for IPv6.
3. Determine the **Default Policy**:
   - Accept: Accepts traffic when no matching rules are present.
   - Deny: Rejects any user's login attempt when no matching rules are present.
4. Click **Append**.

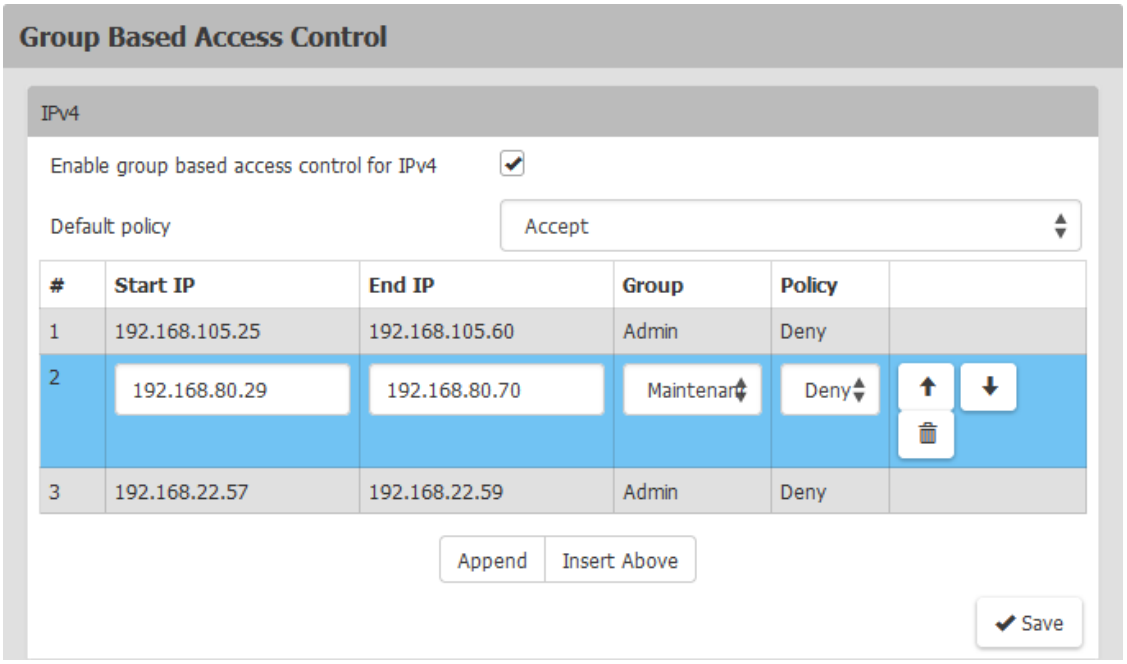


*Fig. 163 SIRA Configuration menu **Security - Group Based Access Control - Creating***

5. Create rules and put them in priority order:
   5.1. Enter **Start IP** and **End IP**, **Group** the rule applies to, and **Policy**.
   5.2. Click **Append** to add another rule.
   5.3. Select a rule and click **Insert Above** to add a rule above another.
   5.4. Click ↓ or ↑ on each rule to rearrange rules in order.
   5.5. Click 🗑 to delete a rule.
6. Click **Save**.
   Note that IPv4 and IPv6 rules are to be saved separately.

12.2 IP Access Control

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

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

To create IPv4 or IPv6 IP access control rules, proceed as follows:

1. Click **Security > IP Access Control**.
2. Tick the **Enable Group Based Access Control for IPv4** checkbox or scroll down to tick the checkbox for IPv6.

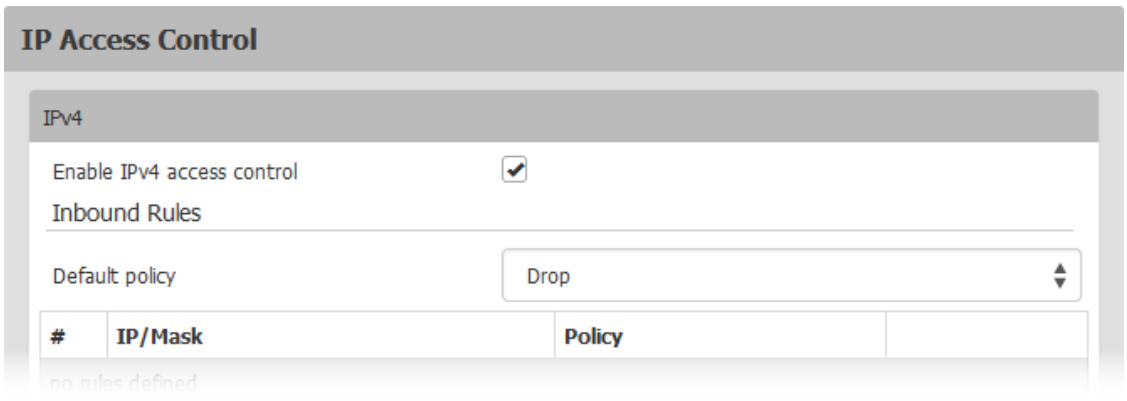


*Fig. 164 SIRA Configuration menu **Security - IP Access Control***

3. Go to the **Inbound Rules section** or the **Outbound Rules** section according to your needs.
   - Inbound rules control the data sent to the SIRA Module.
   - Outbound rules control the data sent from the SIRA Module.
4. Determine the **Default Policy**:
   - Accept: Accepts traffic from all addresses.
   - Drop: Discards traffic from all addresses, without sending any failure notification to the source host.
   - Reject: Discards traffic from all addresses, and an ICMP message is sent to the source host for failure notification.
5. Click **Append**.

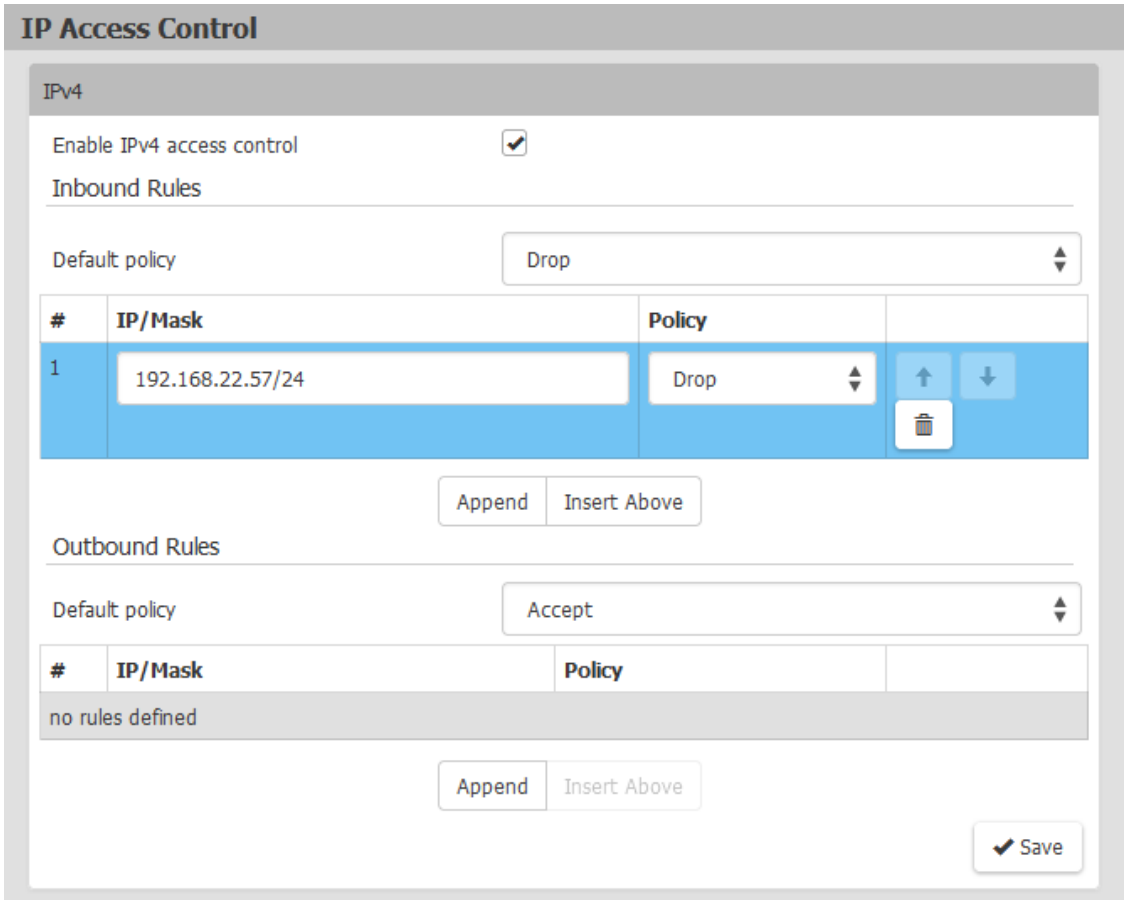


*Fig. 165 SIRA Configuration menu **Security - IP Access Control***

6. Create rules and put them in priority order:

6.1. Enter IP address and mask in the **IP/Mask** field.

6.2. Select **Policy**.

6.3. Click **Append** to add another rule.

6.4. Select a rule and click **Insert Above** to add a rule above another.

6.5. Click ↓ or ↑ on each rule to rearrange rules in order.

6.6. Click 🗑 to delete a rule.

7. Click **Save**.

   Note that IPv4 and IPv6 rules are to be saved separately.

12.3 KVM Security

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

To configure KVM security settings, proceed as follows:

1. Click **Security > KVM Security**.

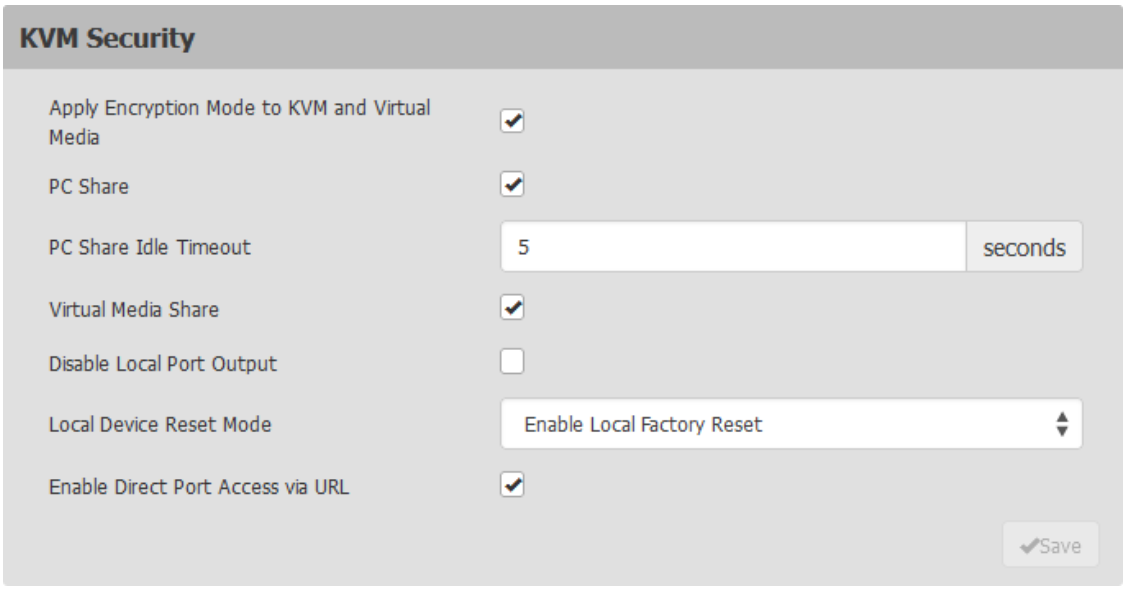


*Fig. 166 SIRA Configuration menu **Security - KVM Security***

2. Select options as needed.

Field/setting	Description
Apply Encryption Mode to KVM and Virtual Media	Tick this checkbox to use encryption for virtual media as well as KVM.
PC Share	Tick this checkbox to allow concurrent remote KVM access, enabling up to eight remote users to simultaneously log into one SIRA Module and concurrently view and control the same target through the device.
PC Share Idle Timeout	Set an idle time limit for users in PC Share mode. If a user has not moved the mouse or entered keyboard input and the timeout period expires, the user relinquishes control, and another user can access keyboard and mouse control of the target.
Virtual Media Share	This option is available only when PC Share mode is enabled. When selected, Virtual Media Share permits the sharing of virtual media and audio among multiple users, that is, several users can access the same virtual media or audio session. The default is disabled.

Field/setting	Description
Disable Local Port Output	Function not used.
Local Device Reset Mode	This option specifies which actions are taken when the hardware reset button on the device is depressed. Select one of the following options: ▪ **Enable Local Factory Reset** (default): Returns the SIRA Module device to the factory defaults (IP address by default 192.168.100.88). ▪ **Enable Local Admin Password Reset**: Resets the local administrator password only. The password is reset to "admin". ▪ **Disable All Local Resets**: No reset action is taken.
Enable Direct Port Access via URL	When selected, users can access the target directly by entering login credentials for the SIRA Module in a URL (see chapter 12.3.1, page 153).

3. Click **Save**.

12.3.1 Direct Port Access URL

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

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

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

Direct Access with Clients	Syntaxes for standard ports
VKCS	https://IPaddress/dpa.asp?username=username&password=password&port=1&client=vkcs
	https://IPaddress/dpa.asp?username=username&password=password&portname=port name&client=vkcs
AKC	https://IPaddress/dpa.asp?username=username&password=password&port=1&client=akc
	https://IPaddress/dpa.asp?username=username&password=password&portname=port name&client=akc
HKC	https://IPaddress/dpa.asp?username=username&password=password&port=1&client=hkc
	https://IPaddress/dpa.asp?username=username&password=password&portname=port name&client=hkc

12.4 Login Settings

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

To configure login settings, proceed as follows:

1. Click **Security > Login Settings**.

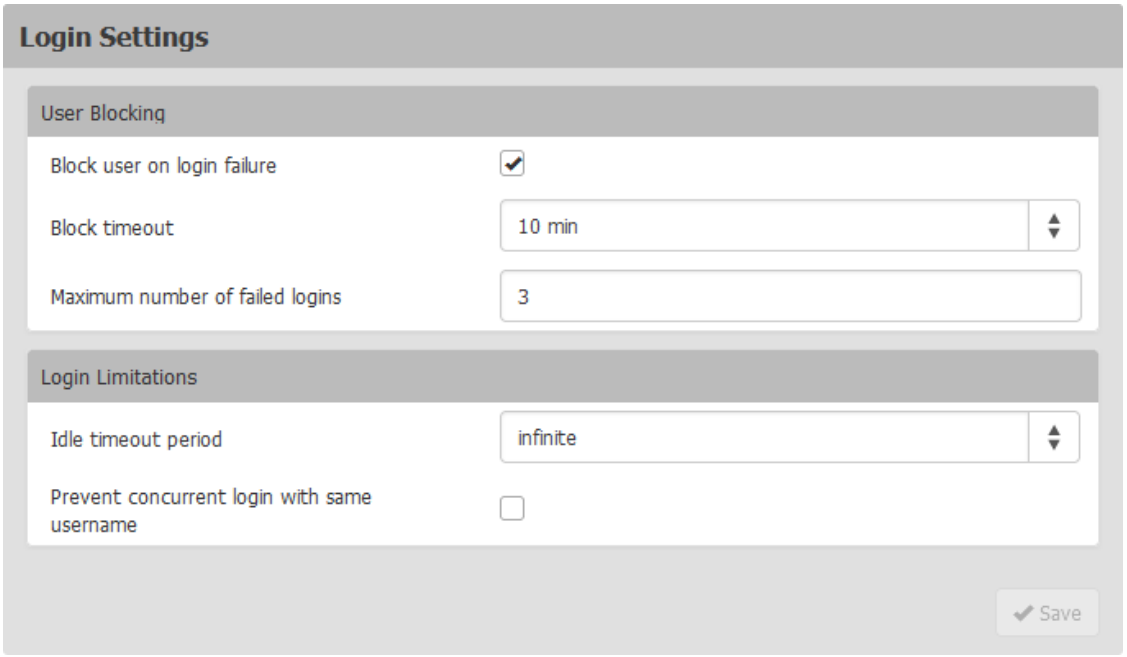


*Fig. 167 SIRA Configuration menu **Security - Login Settings***

2. Tick the **Block user on login failure** checkbox to block users for failed logins then configure the parameters.
   - **Block timeout**: Select the time period during which users with failed logins will be blocked from logging in
   - **Maximum number of failed logins**: Enter the number of failed login attempts that users can make before they are blocked.
3. Select a time in the **Idle timeout period** field to automatically logout users after an idle period.
4. Select **infinite** to allow idle users to remain logged in.
5. Tick the **Prevent concurrent login with same username** checkbox to prevent logins by more than one user with the same username. This setting does not apply to the default admin user.
6. Click **Save**.

12.5 Password Policy

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

To configure a password policy, proceed as follows:

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

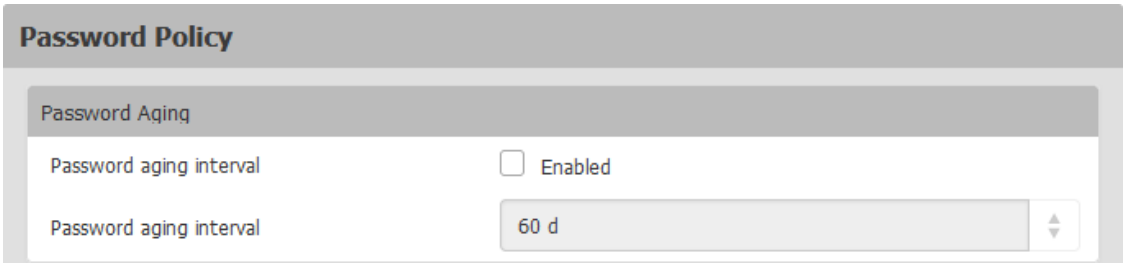


*Fig. 168 SIRA Configuration menu **Security - Security - Password Policy - Password Aging***

3. To enable strong passwords and set their parameters:
   - Tick the **Enabled** checkbox for Strong Passwords.
   - Set a **Minimum and Maximum password length**. Minimum is 8, maximum is 64.
   - Tick checkboxes to enforce at least one lower case, upper case, numeric, and/or special character.
   - Specify the **Password history size**, which controls how frequently passwords can be reused. Maximum is 12.

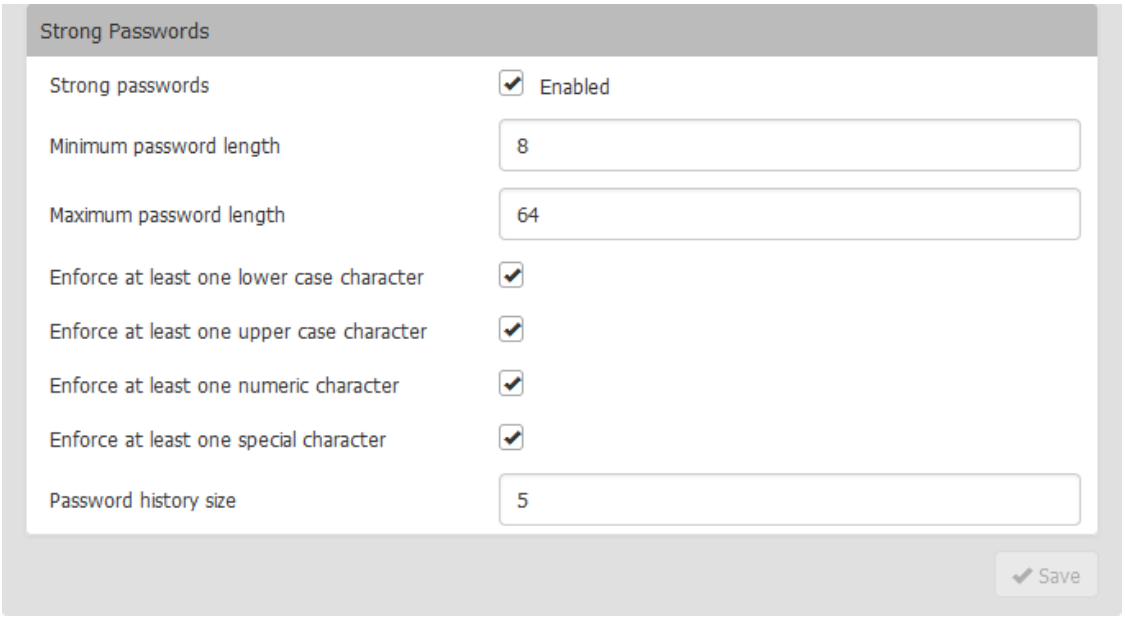


*Fig. 169 SIRA Configuration menu **Security - Password Policy - Strong Passwords***

4. Click **Save**.

12.6 TLS Certificate

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

The SIRA Module can generate a Certificate Signing Request (CSR) or a self-signed certificate using SHA-2.

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

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

When a self-signed certificate is created, the SIRA Module date and time are used to calculate the validity period. If the SIRA Module date and time are not accurate, the certificate's valid date range may be incorrect, causing certificate validation to fail (see Date and Time in chapter XX, page XX).

➡ Make sure your SIRA Module date/time is set correctly.

➡ The CSR must be generated on the SIRA Module

12.6.1 Viewing and Downloading the active TLS Certificate and Key

To view and download the active TLS certificate and key, proceed as follows:

1. Click **Security > TLS Certificate**.

   The active certificate details are displayed.

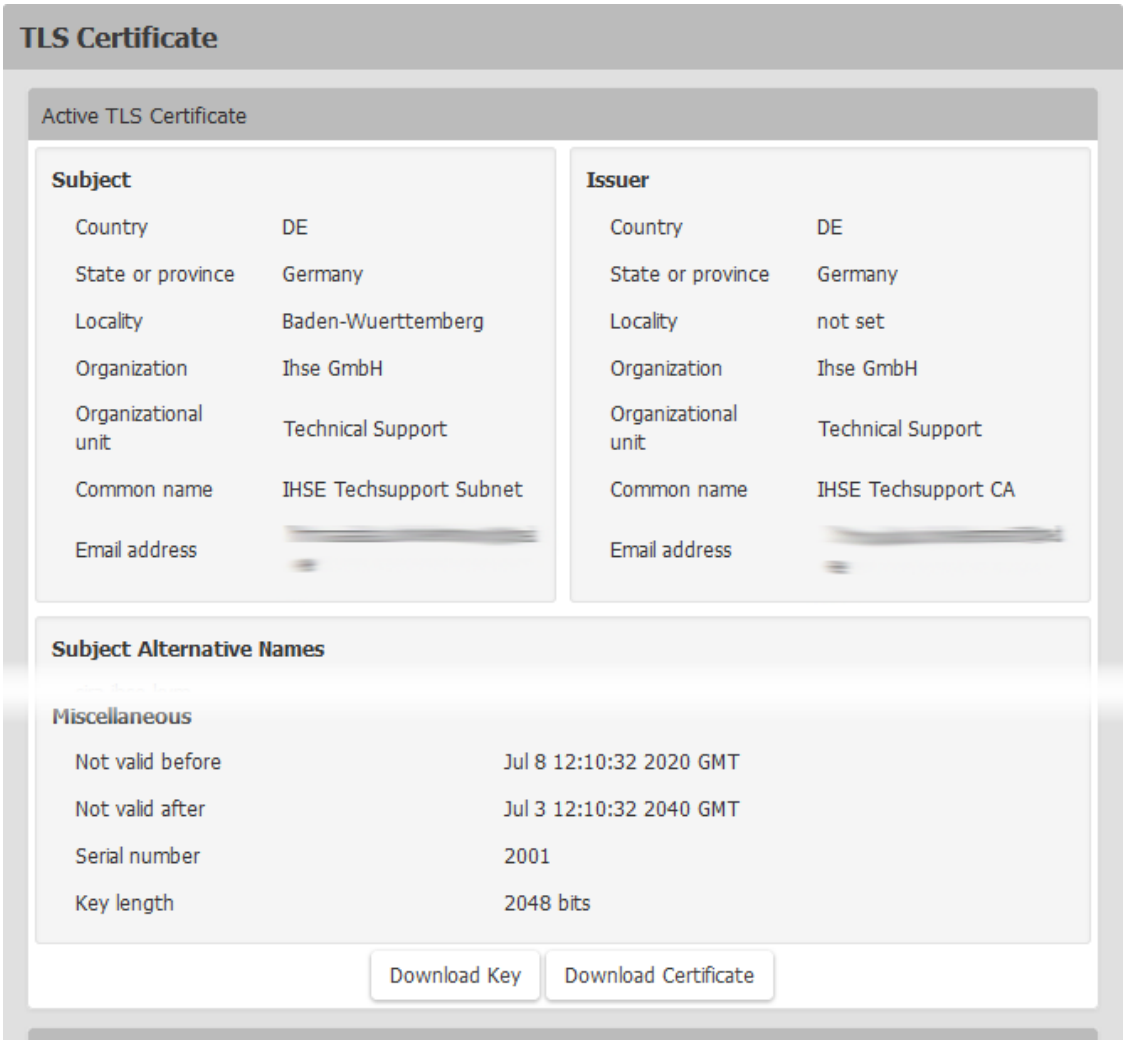


*Fig. 170 SIRA Configuration menu **Security - Login Settings***

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

12.6.2 Creating and Installing a new TLS Certificate

To create and install a new TLS certificate, proceed as follows:

1. Click **Security > TLS Certificate**.
2. Scroll down to the New TLS Certificate section.

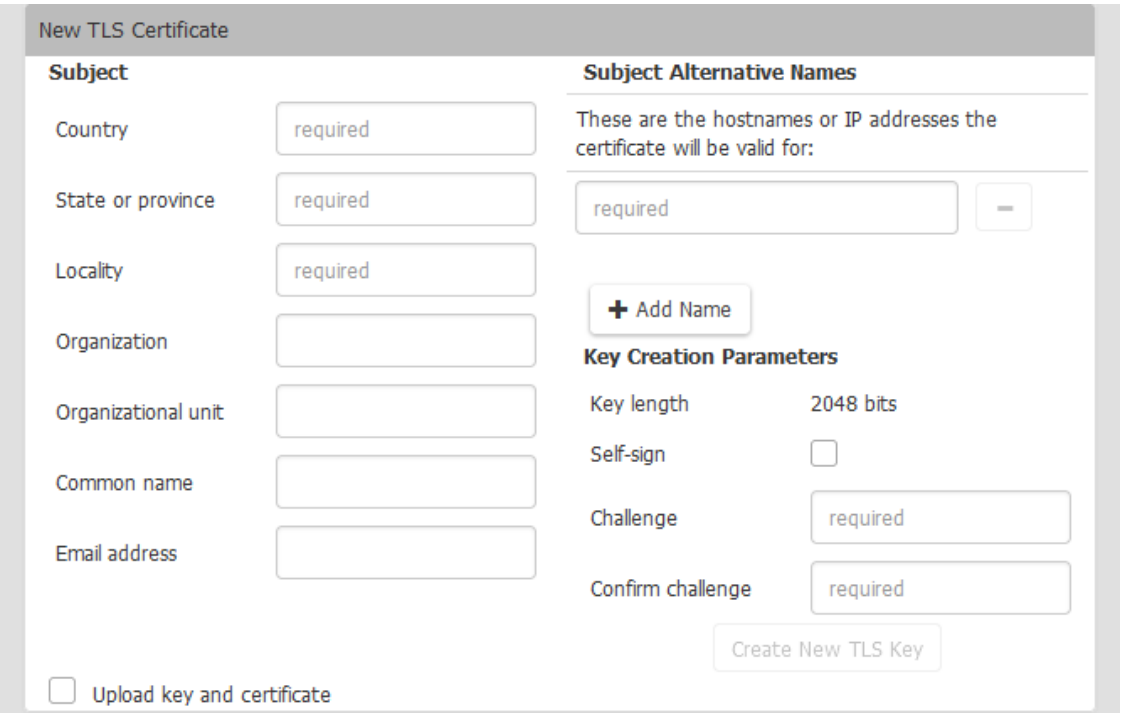


*Fig. 171 SIRA Configuration menu **Security - TLS Certificate - New TLS Certificate***

3. Complete the **Subject** fields:

Field	Description
Country	The country where the organization is located. This is the two-letter ISO code, e.g., DE for Germany, or US for the U.S.
State or province	The state or province where the organization is located.
Locality	The city where the organization is located.
Organization	The name of the organization to which the SIRA Module belongs.
Organizational unit	This field is used for specifying to which department within an organization the SIRA Module belongs.
Common name	The network name of the SIRA Module once it is installed on the network (usually the fully qualified domain name). The common name is identical to the name used to access the SIRA Module with a web browser, but without the prefix “http://”. In case the name given here, and the actual network name differ, the browser displays a security warning when the SIRA Module is accessed using HTTPS.
Email address	The email address of a contact person that is responsible for the SIRA Module and its security.

4. Add up to 10 **Subject Alternative Names** (SAN) by clicking the **Add Name** button, then enter the hostname or IP address in the field. SANs are the hostnames or IP addresses the certificate will be valid for.
5. To generate, do one of the following certification options:

Generating s self-signed Certificate

To generate self-signed certificate, proceed as follows:

1. Tick the **Self-Sign** checkbox under **Key Creation Parameters**.

When you select this option, the SIRA Module generates the certificate based on your entries, and acts as the signing certificate authority. The CSR does not need to be exported and used to generate a signed certificate.

2. Set the **Validity in Days**, which controls how many days until this certificate expires.

Ensure the SIRA Module date and time are correct. If the date and time are not correct, the certificate's valid date range may not be calculated correctly.

3. Click **Create New TLS Key**.

   When the page refreshes, new buttons appear in the **New TLS Certificate** section. These buttons allow to install, download, or delete the newly generated self-signed certificate and key.

4. Click **Install Key and Certificate**, to start using the new certificate.

   The page may refresh as the certificate loads.

Generating a CSR

To generate a CSR to send to the CA for certification, proceed as follows:

1. Enter a password in the **Challenge** and **Confirm challenge** fields under **Key Creation Parameters**.
2. Click **Create New TLS Key**.

   When the page refreshes, new buttons appear in the **New TLS Certificate** section. These buttons allow to download the CSR, download the key, or delete the CSR.

3. Click **Download Certificate Signing Request** to download the CSR.
4. Click **Download Key** to download the file containing the private key.
5. Send the CSR to a CA for certification.

   You will get the new certificate from the CA.

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

Uploading and Installing a Certificate

To upload and install a certificate, proceed as follows:

1. Return back to this page after getting the certificate from the CA to upload it to the SIRA Module.
2. After uploading, click **Install** to start using the new certificate.

   The page may refresh as the certificate loads.

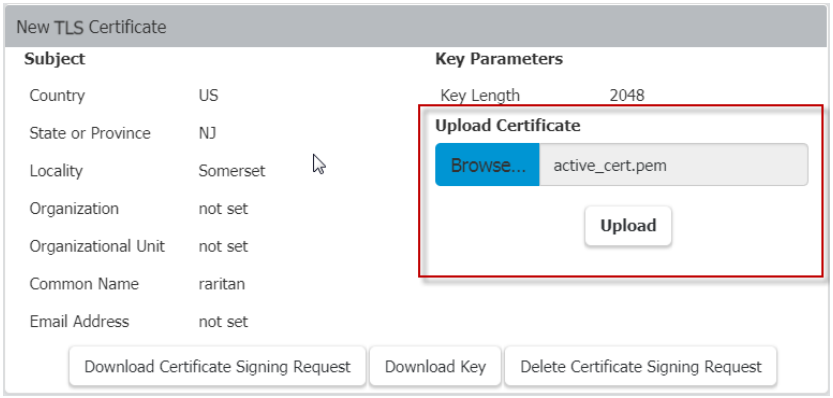


*Fig. 172 SIRA Configuration menu **Security - TLS Certificate - New TLS Certificate - Upload***

Uploading Key and Certificate

To upload a key and certificate, proceed as follows:

1. Click **Security > TLS Certificate** to activate the upload fields.
2. Scroll down to the **New TLS Certificate** section.
3. Tick the **Upload key and certificate** checkbox.
4. The browse and upload controls appear.

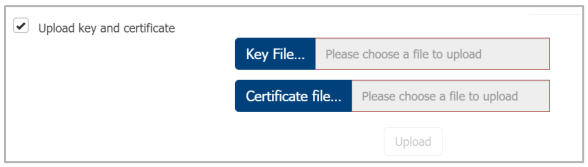


Fig. 173

12.7 Service Agreement

The Service Agreement page allows to enable an agreement that appears on the login page of the SIRA Module. Users must tick a checkbox on the agreement before logging in.

To configure the service agreement, proceed as follows:

1. Click **Security > Service Agreement**.

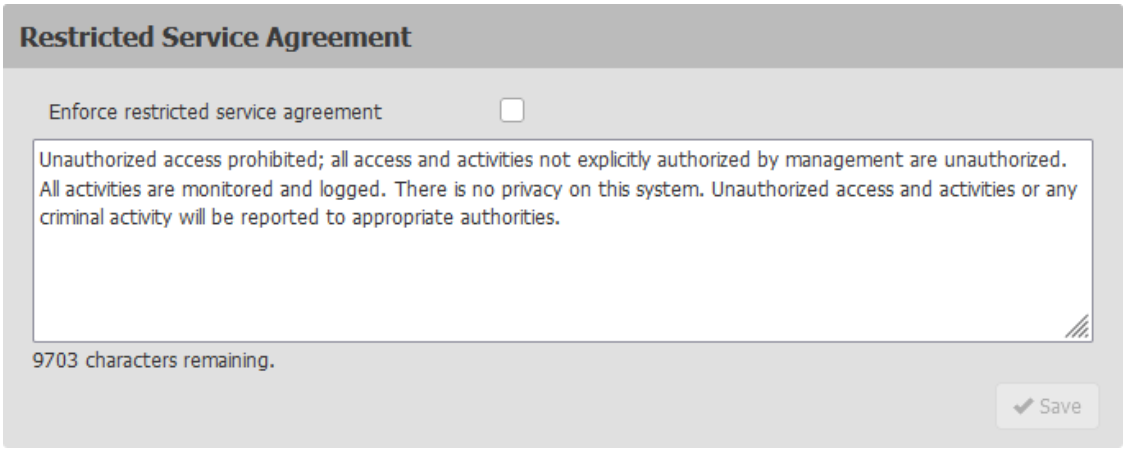


*Fig. 174 SIRA Configuration menu **Security - Service Agreement***

2. Tick the **Enforce Service Agreement** checkbox.
3. Enter the agreement text in the field.
4. Click **Save**.

   The login page will present the service agreement. Users must tick the checkbox before logging in.

13 Maintenance

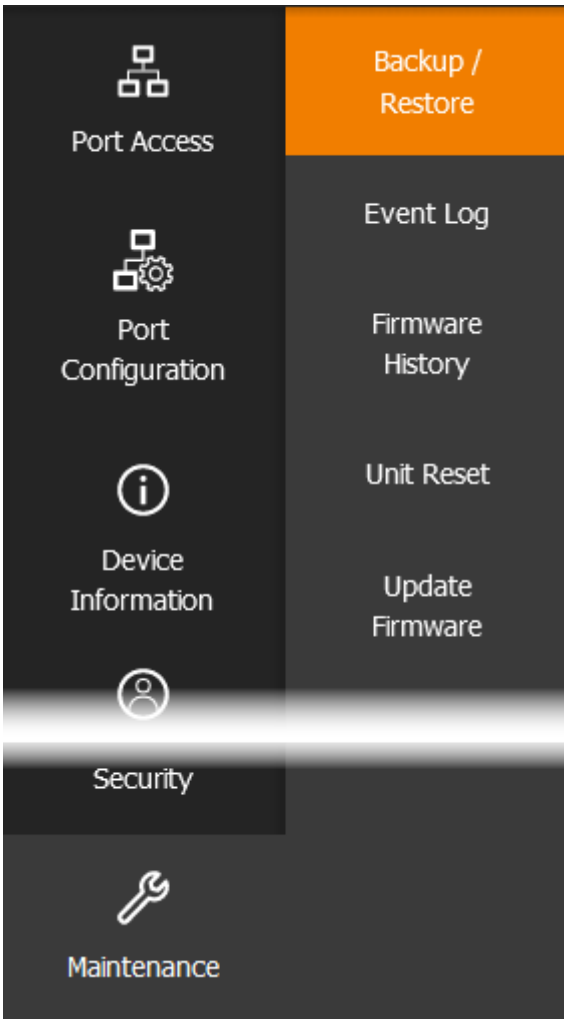


*Fig. 175 SIRA Configuration menu **Maintenance - Submenu***

13.1 Backup and Restore

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

Requirements

➡ You must be a member of the admin group to download a backup file, and to restore a SIRA Module with a backup file.

13.1.1 Saving Device Settings

To download the device settings backup file, proceed as follows:

1. Click **Maintenance > Backup/Restore**.

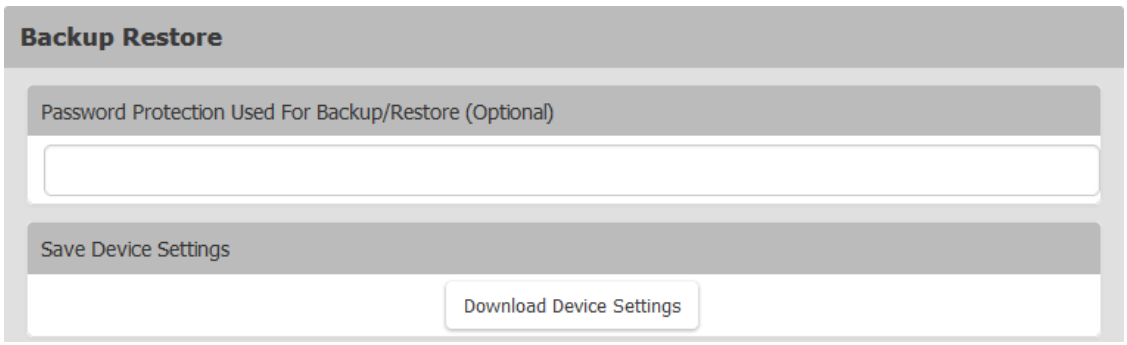


*Fig. 176 SIRA Configuration menu **Maintenance - Backup/Restore - Save Device Settings***

2. Enter a password in the **Password Protection Used For Backup/Restore (Optional)** field to password protect the backup file.
3. Click **Download Device Settings**.

   A query to open or save the `backup_settings.rfp` file appears.
4. Click **Save** to save the `backup_settings.rfp` file.

13.1.2 Restoring Device Settings

To restore the SIRA Module using a backup file, proceed as follows:

1. Click **Maintenance > Backup/Restore**.

   The **Backup Restore** menu opens.

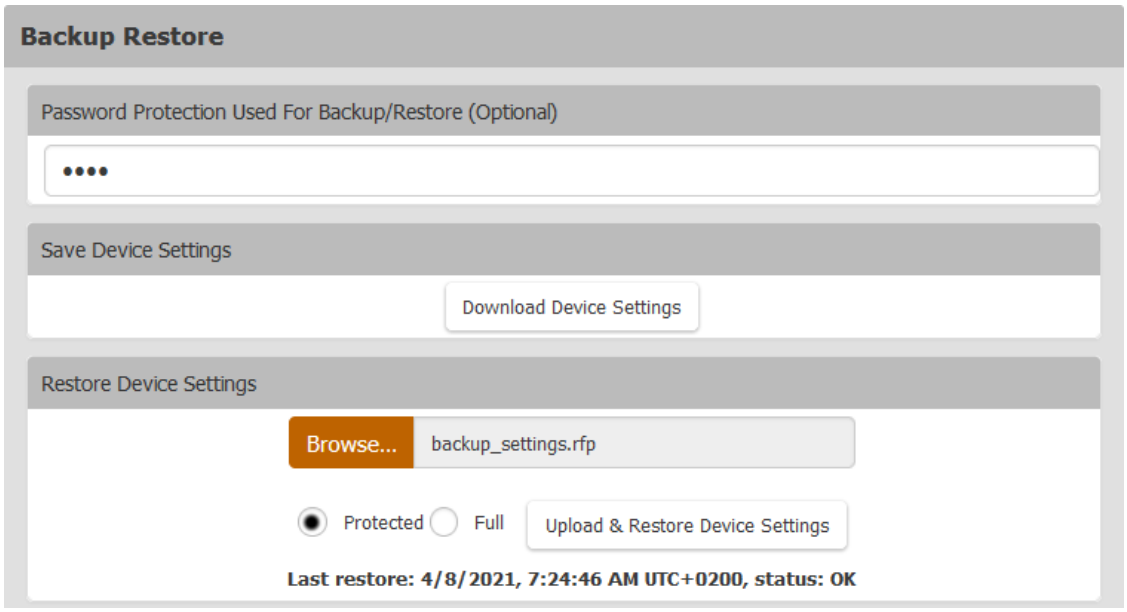


*Fig. 177 SIRA Configuration menu **Maintenance - Backup/Restore - Save Device Settings***

2. Click **Browse…** in the **Restore Device Settings** to select the backup file.
3. Select **Protected** or **Full**.
   - **Protected**: Restores all settings except for device specific settings: network information, names, preferred resolution.
   - **Full**: Restores everything.
4. If the file is password protected, enter the password in the **Password Protection Used For Backup/Restore (Optional)** field.
5. Click **Upload & Restore Device Settings** to upload the file.

6. Wait until the SIRA Module resets and the Login page re-appears, indicating that the restore is complete.

In a full restore, the IP address may have been changed.
➡ Start a new browser session to login to the new IP address.

13.2 Event Log

The SIRA Module captures certain system events and saves them in a local event log.

Over 2000 historical events that occurred on the SIRA Module in the local event log can be viewed. When the log size exceeds 256 KB, each new entry overwrites the oldest one.

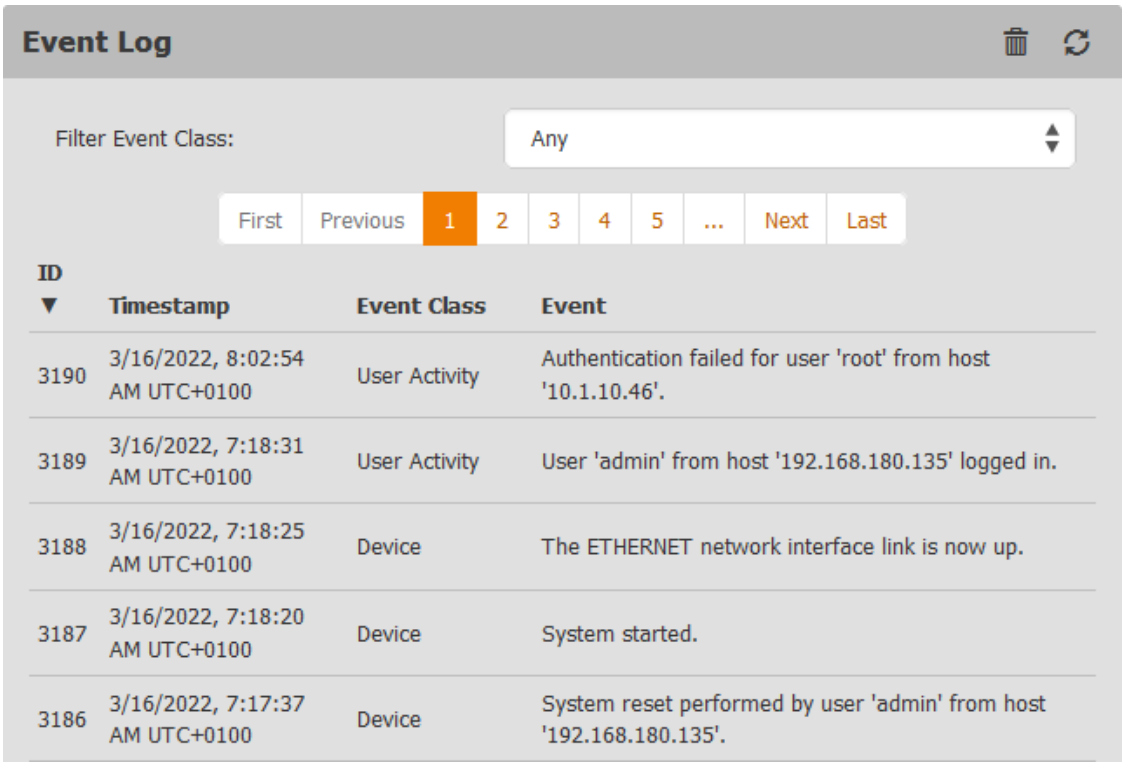


*Fig. 178 SIRA Configuration menu **Maintenance - Event Log***

Field/setting	Description
ID	ID number of the event
Timestamp	The timestamp in the event log is automatically converted to your computer's time zone. To avoid time confusion, apply the SIRA Module time zone settings to your computer or mobile device.
Event class	The event class can be filtered.
Event	Description of the event

To display the event log, proceed as follows:

1. Choose Maintenance > Event Log.
2. Click in the top-right corner to reload the event log.

To view by event category, proceed as follows:

➡ Select an option in the **Filter Event Class** field.

- Device
- KVM Port
- Serial Port (for further use only)
- User Activity
- User Administration

To clear the local event log, proceed as follows:

1. Click on the top-right corner.
2. Click **Clear Log** on the confirmation message.

13.3 Firmware History

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

To view the firmware update history, proceed as follows:

➡ Click **Maintenance > Firmware History**.

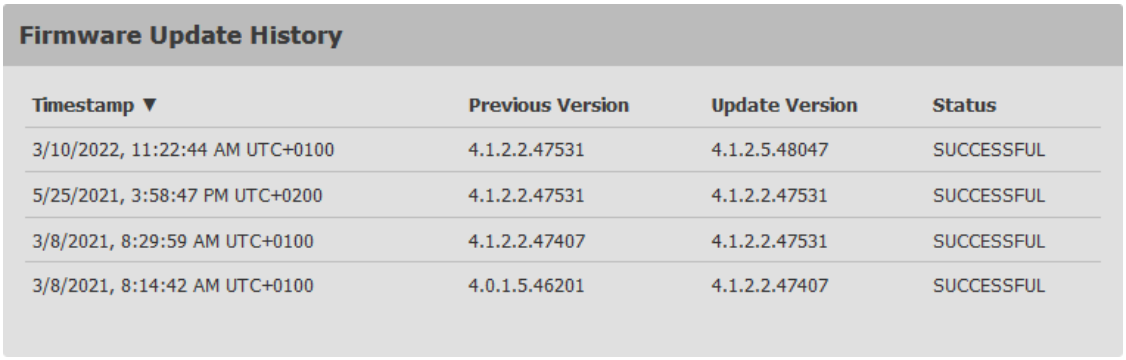


*Fig. 179 SIRA Configuration menu **Maintenance - Firmware History***

Each firmware update event consists of:

- Timestamp with update date and time
- Previous firmware version
- Update firmware version
- Update result

13.4 Unit Reset

13.4.1 Resetting the Unit

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

- Reboot Unit: Restarts the SIRA Module.

To reboot the device, proceed as follows:

1. Click **Maintenance > Unit Reset**.

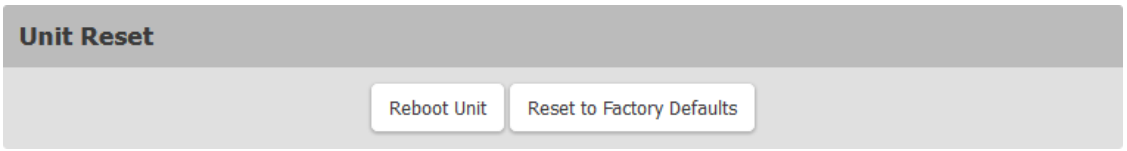


*Fig. 180 SIRA Configuration menu **Maintenance - Unit Reset***

2. Click **Reboot Unit**.
   A confirmation message appears.
3. Click **Reboot** to proceed.
   A countdown timer appears.

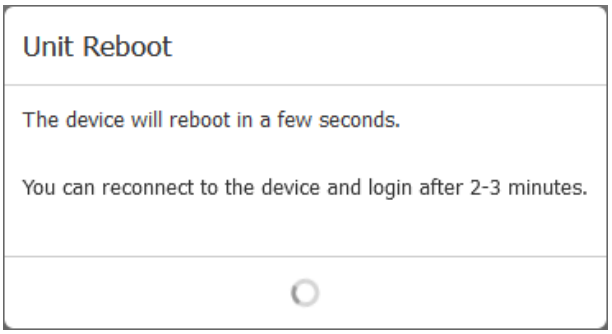


*Fig. 181 SIRA Configuration menu **Maintenance - Unit Reset***

When the restart is complete, the login dialog opens.

13.4.2 Resetting to Factory Default

Requirements

➡ Requires admin privilege.

To reset to factory defaults, proceed as follows:

1. Click **Maintenance > Unit Reset**.

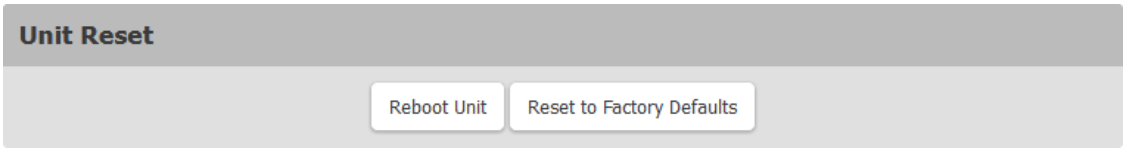


*Fig. 182 SIRA Configuration menu **Maintenance - Unit Reset***

2. Click **Reset to Factory Defaults**.
   A confirmation message appears.
3. Click **Factory Reset** to remove all customized settings and return the SIRA Module to the factory default settings.
   A countdown timer appears. It takes about two minutes to complete.
4. When the reset is complete, proceed with initial configuration (see chapter 6.2, page 32).

Other factory reset option

➡ Press reset hole carefully with a suitable reset tool for at least 5 seconds.
The device will reset and reboot.

13.5 Update Firmware

Firmware files are available on Raritan's Support page: www.raritan.com/support.

You must have the Maintenance privilege to update the SIRA Module firmware.

To update the firmware, proceed as follows:

1. Click **Maintenance > Update Firmware**.
2. Click **Browse** to go to the location of the firmware file.

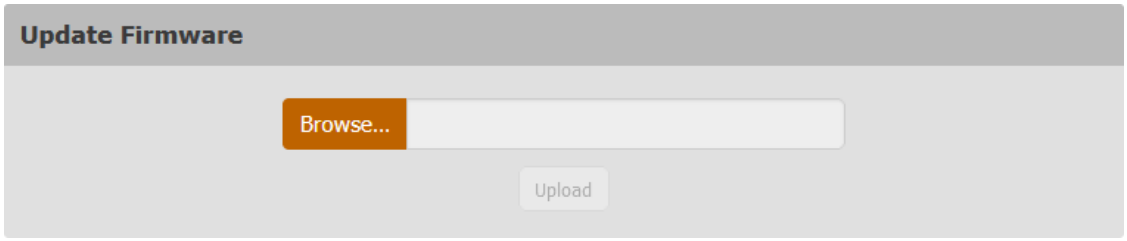


*Fig. 183 SIRA Configuration menu **Maintenance - Update Firmware***

3. Select an appropriate firmware file and click **Upload**.
   A progress bar appears to indicate the upload process.

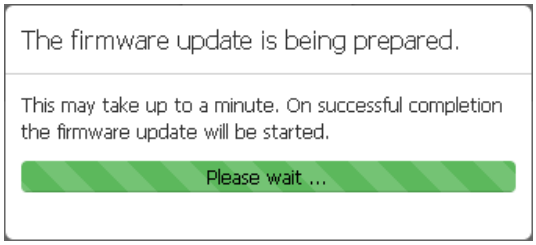


*Fig. 184 SIRA Configuration menu **Maintenance - Update Firmware - Upload progress***

4. Once complete, information of both installed and uploaded firmware versions as well as compatibility and signature-checking results are displayed.
   4.1. To cancel, click **Discard Upload**.
   4.2. To proceed with the update, click **Update Firmware**.

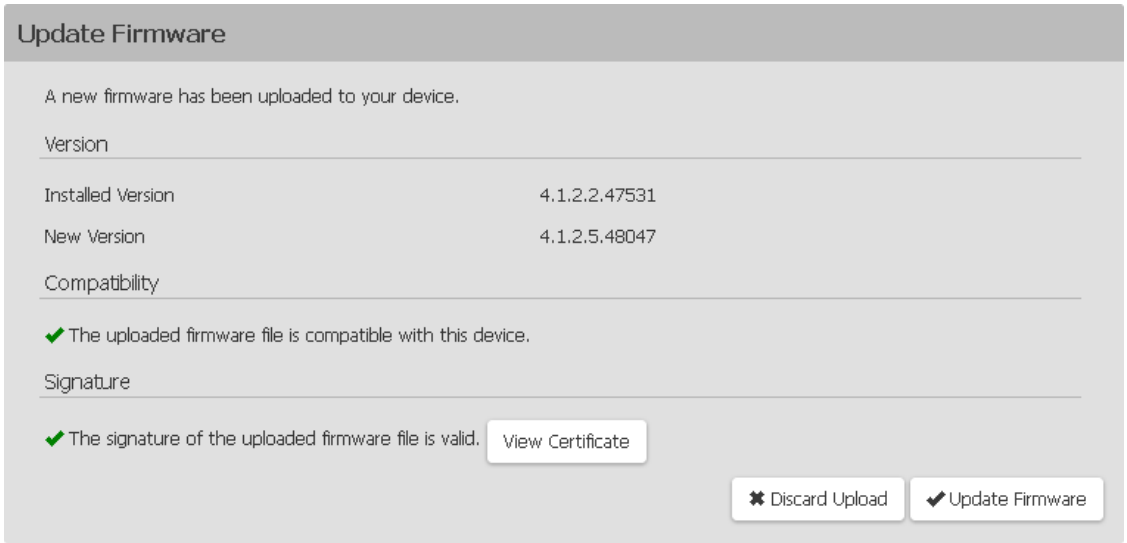


*Fig. 185 SIRA Configuration menu **Maintenance - Update Firmware - Firmware uploaded***

5. When the update begins, another progress bar appears.

The LAN port LED on the device fast-blinks green during update. The device will reboot automatically after completion of the update.

➡ Do NOT power off the SIRA Module during the update.

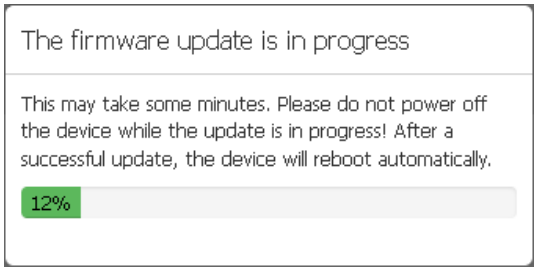


*Fig. 186 SIRA Configuration menu **Maintenance - Update Firmware - Update progress***

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

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

After updating, the SIRA Module MIB file may have changed. If using an SNMP manager, you may need to re-download the MIB file and make an update (see chapter 10.5.4, page 123).

Firmware Update completed with Warnings

The message **The firmware update completed with warnings** may appear before reboot if the update was completed while an iOS device was connected to the USB port on the SIRA Module. This warning does not indicate any problems or that the update failed.

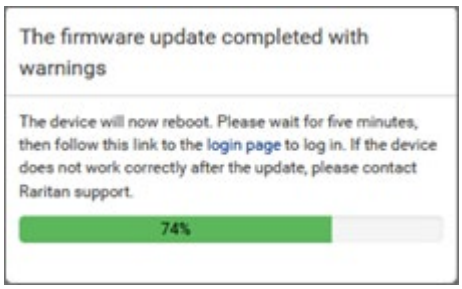


*Fig. 187 SIRA Configuration menu **Maintenance - Update Firmware - Update progress - Warning***

13.6 Dependencies Firmware for Draco SIRA CON

13.6.1 General Information

Basically, the IP part of the firmware of the Draco SIRA CON can be updated to newer versions and downgraded to older versions.

It is possible to skip versions and so it is not necessary to update step by step all interim versions between the current version and the target version.

13.6.2 Firmware File Encryption Change - Version 4.0 and 4.1

From version 4.0.x.xxxxx to version 4.1.x.xxxxx the encryption of the firmware file has changed, and both are not compatible.

If version **4.0.**x.xxxxx is installed, only firmware files that do not have the "-sec" suffix must be used, e.g., `kx-kx4-ihse-040102-47401.rfp`.

If version **4.1.**x.xxxxx is installed, only firmware files that have the "-sec" suffix must be used, e.g., `kx-kx4-ihse-040102-48047-sec.rfp`.

13.6.3 Update from Version 4.0 to Version 4.1 (special handling)

Because the versions 4.1.2.47531 and later are only available with the "-sec" suffix, you cannot directly update from version 4.0.x.xxxxx to one of these new versions.

If you want to go from current firmware version 4.0.x.xxxxx to the latest firmware version, you have to do one interim step.

1. Update to version 4.1.2.47401 using the firmware file `kx-kx4-ihse-040102-47401.rfp`.
2. Update to the latest version.

13.6.4 Downgrade from Version 4.1 to Version 4.0

A downgrade from version 4.1.x.xxxxx to version 4.0.x.xxxxx is not supported.

14 Virtual Media

14.1 Overview

The SIRA Stand-alone supports virtual media. Virtual media extends KVM capabilities by enabling targets to remotely access media from a client PC and network file servers.

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

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

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

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

14.2 Virtual Media Performance Recommendations

Additional studies of virtual media performance show that the SIRA Module virtual media performance can range up to 175 Mbit/s.

Reasons for Performance Limitations

- Writing to a virtual media drive connected to the KVM Client may be slower than reading from the drive.
- There may be performance variations across different USB drives.
- Network performance is also a factor.

Recommendations for Maximum Performance

➡ Turn off encryption. Encryption has a large effect on performance.

➡ Utilize a high-speed laptop/PC with AKC or VKC KVM Clients.

➡ Utilize the SIRA User Station (K488-UST).

14.3 Prerequisites for Using Virtual Media

14.3.1 SIRA Module Prerequisites

➡ For users requiring access to virtual media, the SIRA Module permissions must be set to allow access to the relevant port, as well as virtual media access (VM Access port permission) for the port. Port permissions are set at the group-level.

➡ For using **PC Share**, security settings must also be enabled in the **Security** settings menu (see chapter 12.3, page 152).

Optional

➡ A USB connection must exist between the device and the target.

➡ Correct USB connection settings have to be selected for the KVM target connected to the SIRA Module.

14.3.2 Client/Target Prerequisites

VM Prerequisites	Description
Client computer VM prerequisites	Certain virtual media options require administrative privileges on the computer (for example, drive redirection of complete drives). ➡ If using Windows, disable **User Account Control** or select **Run as Administrator** when starting Internet Explorer. To do this, click the **Start Menu**, locate IE, right-click and select **Run as Administrator**.
Target VM prerequisites	KVM targets must support USB connected drives.

14.4 Local Drives

The **Local Drive** option (see chapter 7.1.10.1, page 58) mounts an entire drive, which means the entire disk drive is mounted virtually onto the target. Use this option for hard drives and external drives only. It does not include network drives, CD-ROM, or DVD-ROM drives.

14.5 Supported Tasks

OTICE
Once connected to a virtual media drive, do not change mouse modes in the KVM client if 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.

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

14.6 Supported Types

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

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

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

14.7 Conditions when Read/Write is Not Available

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

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

14.8 Number of Supported Virtual Media Drives

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

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

To use virtual media, connect/attach the media to the client or network file server that are to be accessed from the target.

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

14.9 Virtual Media in a Linux Environment

14.9.1 Limitations and Requirements

Limitations and requirements	Description
Active system partitions	Active system partitions cannot be mounted from a Linux client. Linux Ext3/4 drive partitions need to be unmounted via umount /dev/<device label> prior to a making a virtual media connection
Mapped drives	Mapped drives from Linux clients are not locked when mounted onto connected targets.
Drive partitions	The following drive partition limitations exist across operating systems: • Windows® and Mac targets are not able to read Linux formatted partitions. • Windows and Linux cannot read Mac formatted partitions. • Only Windows Fat partitions are supported by Linux.
Root user permission requirement	The virtual media connection can be closed if mounting a CD-ROM from a Linux client to a target and then unmount the CD-ROM. ➧ To avoid these issues, you must be a root user.

14.9.2 Connect Drive Permissions

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

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

The drive is then available to connect to the target.

14.10 Virtual Media in a Mac Environment

14.10.1 Limitations and Requirements

Limitations and requirements	Description
Active system partitions	Virtual media cannot be used to mount active system partitions for a Mac client.
Drive partitions	The following drive partition limitations exist across operating systems: • Windows® and Mac targets are not able to read Linux formatted partitions. • Windows and Linux cannot read Mac formatted partitions. • Windows FAT and NTFS are supported by Mac. Mac users must unmount any devices that are already mounted to connect to a target. Use >diskutil umount /dev/disk1s1 to unmount the device and diskutil mount /dev/disk1s1 to remount it.

14.10.2 Connect Drive Permissions

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

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

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

14.11 Virtual Media File Server Setup

Use the **Virtual Media Shared Images** menu (see chapter 10.6, page 125) to designate the files server(s) and image paths that should be accessed using virtual media. File server ISO images specified here are available for selection in the **Remote Server ISO Image Hostname** and **Image** drop-down lists in the **Map Virtual Media CD/ISO Image** dialog (see chapter 7.1.10.3, page 60).

15 Diagnostics

15.1 Download Diagnostic

This function is for use by IHSE Field Engineers or when you are directed by IHSE Technical Support.

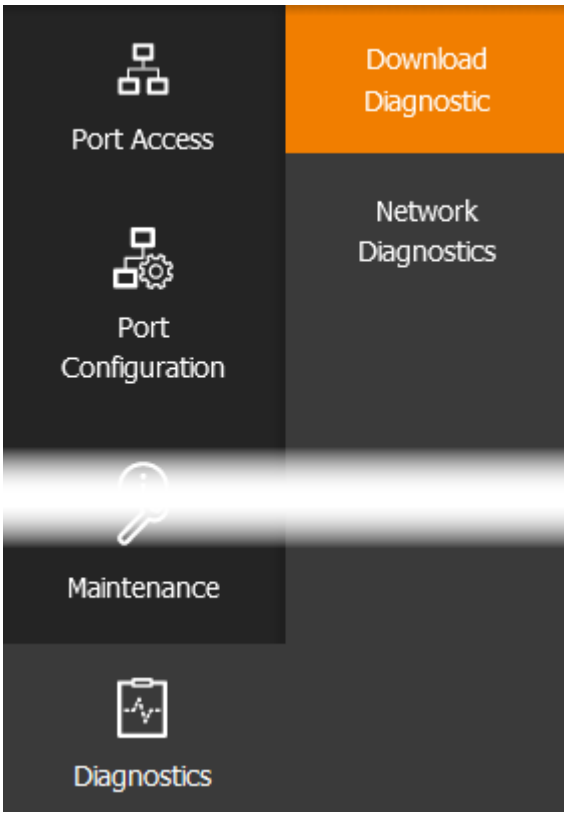


*Fig. 188 SIRA Configuration menu **Diagnostics - Submenu***

Requirements

➡ You must be a member of the admin group.

To download a diagnostic file to a client machine, proceed as follows:

1. Click **Diagnostics> Download Diagnostic**.

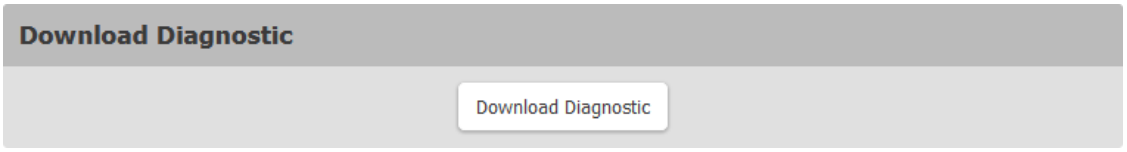


*Fig. 189 SIRA Configuration menu **Diagnostics - Download Diagnostics***

2. Click **Download Diagnostic**.
   After running the diagnostic, a query to open or save the compressed file (`.zip`) appears.
3. Click **Save** to save the `.zip` file.
4. Send this file as instructed by IHSE Technical Support.

15.2 Network Diagnostics

The SIRA Module provides the following tools diagnosing potential networking issues.

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

1. Choose **Diagnostics > Network Diagnostics**.

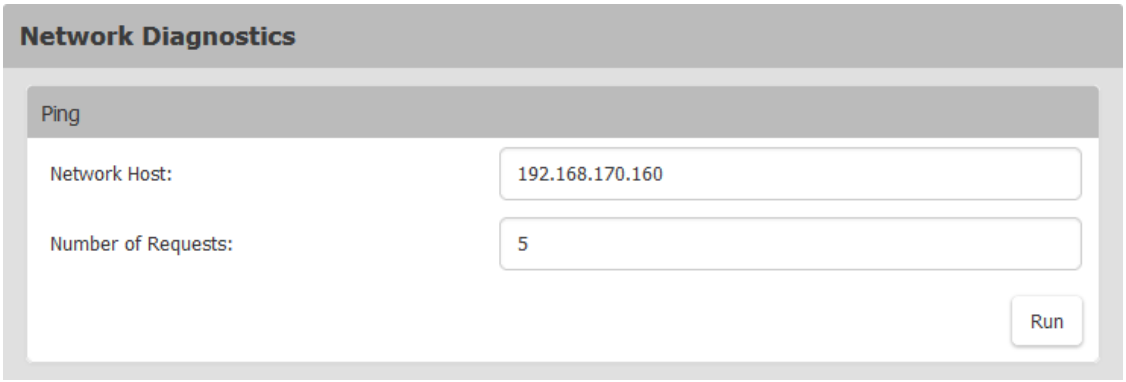


*Fig. 190 SIRA Configuration menu **Diagnostics - Network Diagnostics***

2. Perform any function below.

Ping:

1. Enter the IP address or hostname in the **Network Host** field.
2. Set the number of requests to be send (maximum 20).
   This determines how many packets are sent for pinging the host.
3. Click **Run** to ping the host.
   The Ping results are displayed.

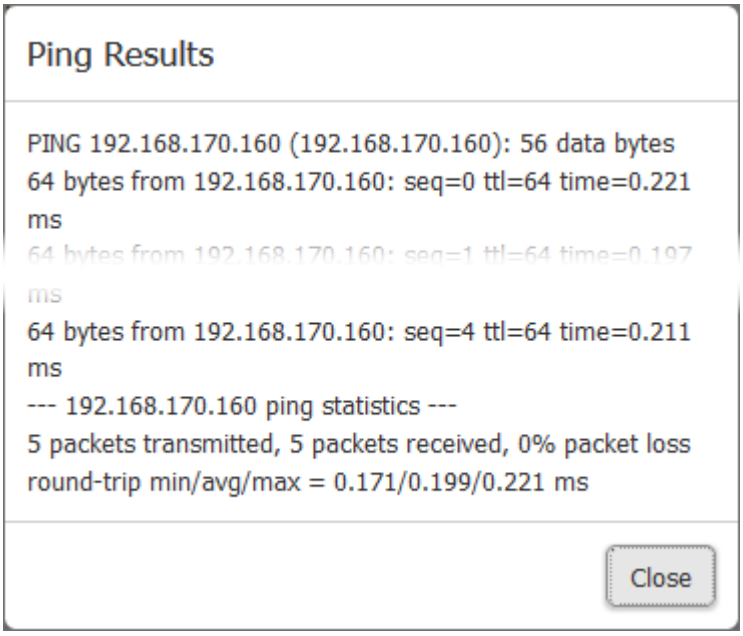


*Fig. 191 SIRA Configuration menu **Diagnostics - Network Diagnostics - Ping - Ping Results***

Trace Route

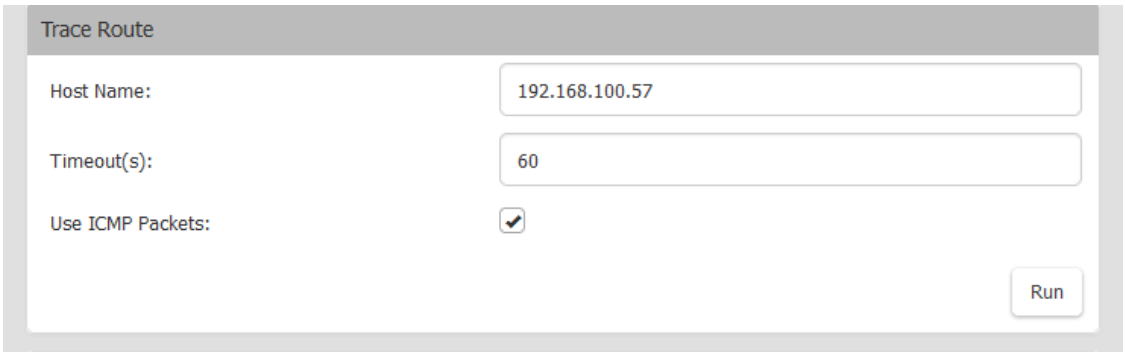


*Fig. 192 SIRA Configuration menu **Diagnostics - Network Diagnostics - Trace Route***

1. Enter the IP address or name of the host whose route is to be checked in the **Host Name** field.
2. Enter a timeout value in seconds in the **Timeout(s**) field to end the trace route operation (maximum 900 seconds).
3. Tick the **Use ICMP packets** checkbox to use the Internet Control Message Protocol (ICMP) packets to perform the trace route command.
4. Click **Run**.

   The **Trace Route** results are displayed.

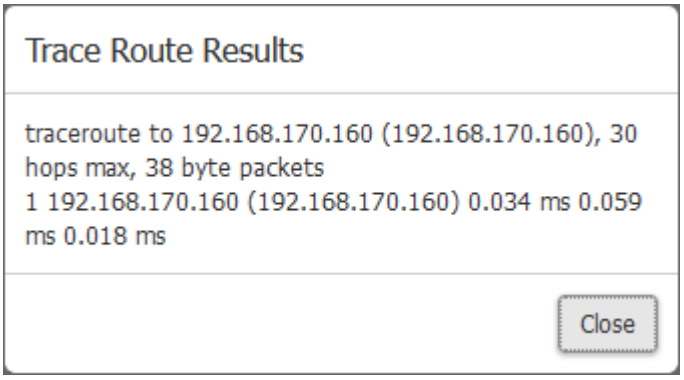


*Fig. 193 SIRA Configuration menu **Diagnostics - Network Diagnostics - Trace Route - Trace Route Results***

List TCP Connections:

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

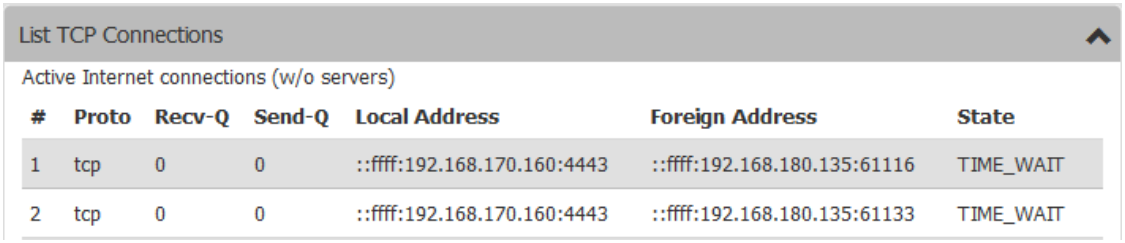


*Fig. 194 SIRA Configuration menu **Diagnostics - Network Diagnostics - List TCP Connections***

16 Troubleshooting

16.1 SIRA Module Connection

If DHCP is configured for the SIRA Module and/or the automatically assigned IP address is unknown, a local login is available. After login the automatically assigned IP address is displayed in the **Device Information** menu (see chapter 9, page 101).

To login to the SIRA Module locally via DHCP, proceed as follows:

1. Disable the wireless interface of the computer and make sure the computer is set to DHCP.
2. Connect a network cable between the computer network port and the LAN port of the SIRA Module.
3. Open a browser.
4. Enter the URL https://kvm.local.
   A login dialog appears.

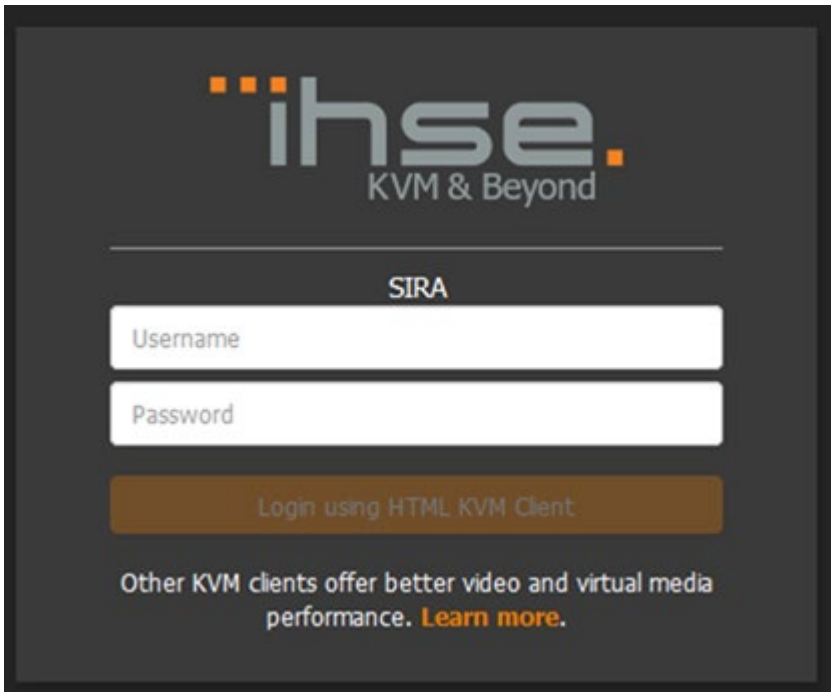


Fig. 195 SIRA Client - Login dialog

5. Enter the **Username** and **Password**.
   By default, the username is admin, and the password of the administrator is admin.
6. Click **Login using HTML KVM Client**.
7. To change to a static IP address, see chapter 10.4.1, page 117.

Re-connect the SIRA Module to the LAN after noting the automatically IP address or changing to a static IP address.

16.2 Mouse Settings and Mouse Synchronization

To get the **mouse synchronization** working while using the mouse mode "Standard", it is important to use the correct mouse settings at the source computer.

This is also important and necessary for **touch screens**, because touch screens require the mouse mode "Standard".

If the **Pointer Options** are not exactly set as shown in the picture below, the mouse synchronization does not work.

- The pointer speed has to be set exactly in the middle position.
- The **Enhanced pointer precision** option has to be disabled.

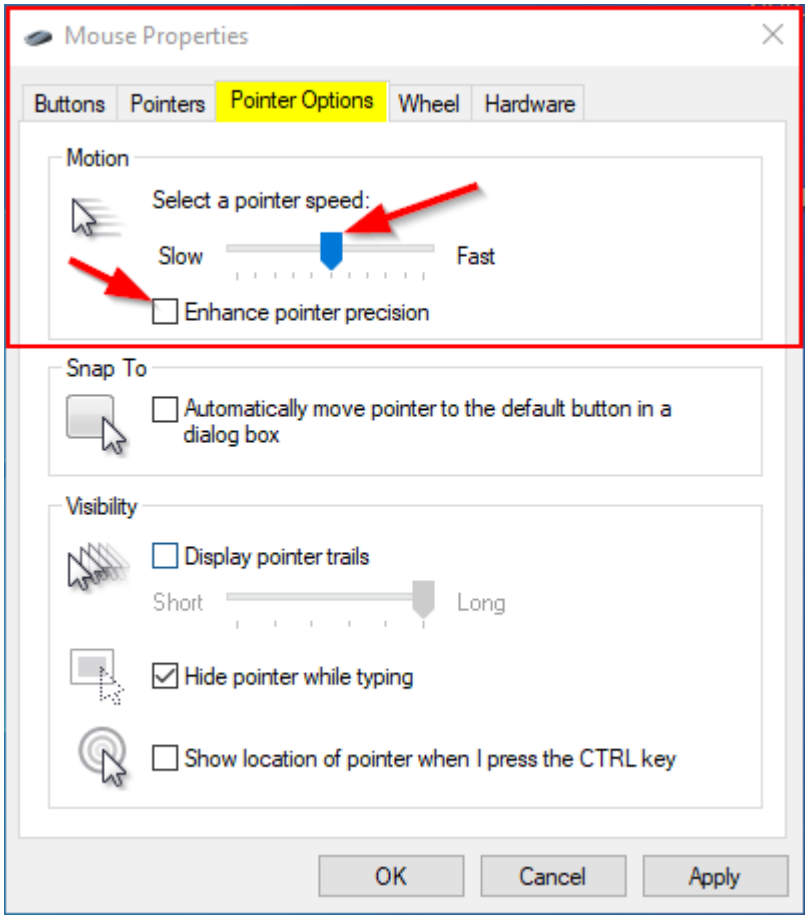


Fig. 196 Source computer - Mouse settings - Pointer options

17 Technical Data

17.1 TCP and UDP Ports Used

Definition	Port	Description
Listening TCP Ports	80	http access (configurable)
	443	https access (configurable)
	5000	SIRA K488 access (configurable)and for future use
	22	SSH access (if enabled, configurable)
	68	DHCP access (if DHCP is enabled)
Listening UDP Ports	162	SNMP access (if SNMP Agent is enabled)
	5001	For future use
TCP Ports Outgoing	398	LDAP authentication (if LDAP is enabled, configurable)
	636	LDAPS/StartTLS (if LDAPS/StartTLS is enabled, configurable)
	25	SMTP (email) (if enabled)
	445	SMB (Windows File System) access (Remote ISO image access)
UDP Ports Outgoing	514	Syslog (if enabled, configurable)
	5001	For future use
	1812	RADIUS authentication (if enabled, configurable)
	1813	RADIUS authentication (if enabled, configurable)

17.2 Interfaces

17.2.1 HDMI 1.4

Video

The audio/video interface can transmit monitor resolutions such as 1920 x 1200 @ 60 Hz, Full HD (1080p) or 4K30 (up to 3840 x 2160 @ 30 Hz). The data rate is limited to 165 MPixel/s and 8 bit.

Audio

Various audio formats can be transmitted through the interface

Parameter	Value
Standards	Stereo Linear Pulse Code Modulation (LPCM)
Bit depth	16 to 24 bit
Sample rate	32 to 192 kHz

3D

The interface is compatible to 3D. The 3D formats Side-by-Side and Top-and-Bottom can be transmitted.

HDCP coded content is currently not supported.

17.2.2 USB-HID

Our devices with USB-HID interface support a maximum of two devices with USB-HID protocol. Each USB-HID port provides a maximum current of 100 mA.

Keyboard

Compatible with most USB keyboards. Certain keyboards with additional functions may require custom firmware to operate. Keyboards with an integral USB Hub (Mac keyboards e.g.) are also supported, however, a maximum of two devices are supported.

Mouse

Compatible with most 2-button, 3-button and scroll mice.

Other USB-HID devices

The proprietary USB emulation supports certain other USB-HID devices, such as specific touch screens, graphic tablets, barcode scanners or special keyboards. However, support cannot be guaranteed for every USB-HID device.

Extension

If it is required to extend the USB-HID signals on CPU or console side (e.g. mounting requirement), the signals can be extended either via a 3.0 m A-B cable (247-U2) or a 3.0 m USB A-A extension cable (436-USB20). The compatibility to other extension cables cannot be guaranteed.

Only two USB-HID devices are supported concurrently, such as keyboard and mouse or keyboard and touch screen. A hub is allowed, but it does not increase the number of devices allowed.

To support other USB 'non-HID' devices, such as scanners, web cams or memory devices, use the USB 2.0 interfaces.

17.2.3 USB 2.0 (transparent)

The KVM-Extender with transparent USB 2.0 interface supports all types of USB 2.0 devices (without restriction). USB 2.0 data transfer is supported with USB high speed (max. 480 Mbit/s) or USB-embedded (up to 36/50/100 Mbit/s), depending on the add-on module.

Each USB embedded port provides a maximum current of 500 mA (high power). When using a USB high speed interface with 4 USB ports, respectively 2 connectors provides a maximum of 500 mA (high power) and 2 connectors a maximum of 100 mA.

17.2.4 Mini USB

This interface enables a customer specified communication with the KVM extender. The firmware could also be updated using this interface.

17.2.5 RJ45 (Network)

The communication of the Cat X devices requires a 1000BASE-T connection.

The cabling has to be done according to EIA/TIA-568-B (1000BASE-T) with RJ45 connectors at both ends. All four wire pairs are used in both directions. The cabling is suitable for a full duplex operation.

17.2.6 RJ45 (Interconnect)

Communication between Cat X devices requires a 1000BASE-T connection.

Connector wiring must comply with EIA/TIA-568-B (1000BASE-T), with RJ45 connectors at both ends. All four cable wire pairs are used

17.2.7 Fiber SFP Type LC (Interconnect)

Communication of fiber devices is performed via Gigabit SFPs that are connected to suitable fibers fitted with connectors type LC (see (see chapter 17.3.2, page 181).

NOTICE
The correct function of the device can only be guaranteed with SFPs provided by the manufacturer.

NOTICE
SFP modules can be damaged by electrostatic discharge (ESD). ➡ Please consider ESD handling specifications.

17.3 Interconnect Cable

17.3.1 Cat X

NOTICE

Transmission problems

Routing over an active network component, such as an Ethernet Hub, Router or Matrix, is not allowed. Operation with several patch fields is possible.

- ➡ Establish a point-to-point connection.
- ➡ Avoid routing Cat X cables along power cables.

NOTICE

Exceeding the limit of the device class

The use of unshielded Cat X cables with higher electromagnetic emissions / radiation can exceed the limit values for the specified device class.

- ➡ Correctly install shielded Cat X cable throughout interconnection, to maintain regulatory EMC compliance.

NOTICE

Exceeding limit values for electromagnetic radiation

The limit values for the electromagnetic radiation of the device are complied with if ferrites are mounted on both sides of all Cat X cables near the device. With installed ferrites, the devices meet the EU guidelines for electromagnetic compatibility. The operation of the devices without mounted ferrites leads to a loss of conformity with the EU directives.

- ➡ Mount ferrites on both sides of all Cat X cables near the device to maintain regulatory EMC compliance.

Type of Interconnect Cable

The SIRA Modules require interconnect cabling specified for Gigabit Ethernet (1000BASE-T). The use of solid-core (AWG24), shielded, Cat 5e (or better) is recommended.

Type of cable	Specification
Cat X installation cable AWG24	S/UTP (Cat 5e) cable according to EIA/TIA-568, standard 568-A or 568-B. Four pairs of wires AWG24. We recommend using standard 568-A, but standard 568-B is also supported.
Cat X patch cable AWG26/8	S/UTP (Cat 5e) cable according to EIA/TIA-568, standard 568-A or 568-B. Four pairs of wires AWG26/8. We recommend using standard 568-A, but standard 568-B is also supported.

The use of flexible cables (patch cables) type AWG26/8 is possible, however the maximum possible extension distance is halved.

Maximum Transmission Range for Video and USB-HID Signals (End-to-End Connection)

Type of cable	Maximum transmission range
Cat X installation cable AWG24	140 m (460 ft)
Cat X patch cable AWG26/8	70 m (230 ft)

17.3.2 Fiber

NOTICE

Transmission problems

Routing over an active network component, such as an Ethernet Hub, Router or Matrix, is not allowed. Operation with several patch fields is possible.

➡ Establish a point-to-point connection.

➡ Avoid routing Cat X cables along power cables.

Type of Interconnect Cable*

Type of cable	Specification
Single-mode 9 µm	• Two fibers 9 µm • I-V(ZN)H 2E9 (in-house patch cable) • I-V(ZN)HH 2E9 (in-house breakout cable) • I/AD(ZN)H 4E9 (in-house or outdoor breakout cable, resistant) • A/DQ(ZN)B2Y 4G9 (outdoor cable, with protection against rodents)
Multi-mode 50 µm	• Two fibers 50 µm • I-V(ZN)H 2G50 (in-house patch cable) • I/AD(ZN)H 4G50 (in-house or outdoor breakout cable, resistant)

* Cable notations according to VDE

Maximum Transmission Range for Video and USB-HID Signals (End-to-End Connection)

Type of cable	Maximum transmission range
Single-mode 9 µm	10,000 m (32,808 ft)
Single-mode 9 µm XV	5,000 m (16,404 ft)
Multi-mode 50 µm (OM3)	1,000 m (3,280 ft)
Multi-mode 50 µm	400 m (1,312 ft)

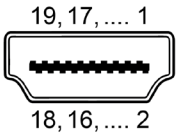
Using single-mode SFPs with multi-mode fibers, the ranges can be increased.

Type of Connector

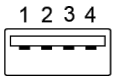
Connector	Type
Plug-in connector	LC-Connector

17.4 Connector Pinouts

17.4.1 HDMI

Connector	Pin	Signal	Pin	Signal
	1	T.M.D.S data 2 +	11	T.M.D.S clock GND
	2	T.M.D.S data 2 GND	12	T.M.D.S clock -
	3	T.M.D.S data 2 -	13	CEC
	4	T.M.D.S data 1 +	14	HEC data -
	5	T. M.D.S data 1 GND	15	DDC Input (SCL)
	6	DDC Input (SCL)	16	DDC Output (SDA)
	7	T.M.D.S data 1 -	17	DDC/CEC/HEC GND
	8	T.M.D.S data 0 GND	18	+5 V DC high impedance
	9	T.M.D.S data 0 -	19	Hot Plug recognition
	10	T.M.D.S clock +	-	

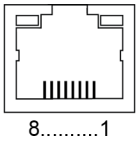
17.4.2 USB, Type A

Connector	Pin	Signal	Color
	1	+5 V (DC)	Red
	2	D -	White
	3	D +	Green
	4	GND	Black

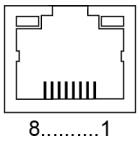
17.4.3 Mini USB, Type B

Connector	Pin	Signal	Color
	1	+5 V (DC)	Red
	2	Data –	White
	3	Data +	Green
	4	Not connected	-
	5	GND	Black

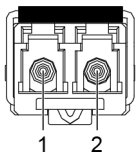
17.4.4 RJ45 (Network)

Connector	Pin	Signal	Pin	Signal
	1	D1+	5	D3-
	2	D1-	6	D2-
	3	D2+	7	D4+
	4	D3+	8	D4-

17.4.5 RJ45 (Interconnect)

Connector	Pin	Signal	Pin	Signal
	1	D1+	5	D3-
	2	D1-	6	D2-
	3	D2+	7	D4+
	4	D3+	8	D4-

17.4.6 Fiber SFP Type LC

Connector	Diode	Signal
	1	Data OUT
	2	Data IN

17.5 Power Supply, Current Draw and Power Consumption

17.5.1 Current Draw

	R488-BIPC	R488-BIPCR	R488-BIPS	R488-BIPSR	R488-BIPHHL
Current draw	2,100 mA	2,200 mA	2,100 mA	2,200 mA	1,600 mA

17.5.2 Power Consumption

	R488-BIPC	R488-BIPCR	R488-BIPS	R488-BIPSR	R488-BIPHHL
Power Consumption	13 W	13 W	13 W	13 W	10 W

17.6 Environmental Conditions and Emissions

Parameter	Value
Operating temperature	5 to 45 °C (41 to 113 °F)
Storage temperature	-25 to 60 °C (-13 to 140 °F)
Relative humidity	Max. 80% non-condensing
Operating altitude	Max. 2.500 m (7,500 ft)
Sound pressure level (SPL)	Max. 21 dBA per fan (474-6FAN)
Heat dissipation	Corresponds to power consumption in Watt (W)

17.7 Dimensions

	Dimension
Module	120 x 40 x 145 mm (4.7" x 1.6" x 5.7")

17.8 Weight

	R488-BIPC	R488-BIPCR	R488-BIPS	R488-BIPSR	R488-BIPHHL
Weight	217 g	223 g	233 g	264 g	110 g

17.9 MTBF

Specific MTBF values (mean time between failure) can be requested from the manufacturer’s technical support if required.

18 Technical Support

Prior to contacting support please ensure you have read this manual, and then installed and set-up your KVM Extender as recommended.

18.1 Support Checklist

To efficiently handle your request, it is necessary that you complete a support request checklist (Download). Please ensure that you have the following information available before you call:

- Company, name, phone number and email
- Type and serial number of the device (see bottom of the device)
- Date and number of sales receipt and name of dealer if necessary
- Issue date of the existing manual
- Nature, circumstances, and duration of the problem
- Components included in the system (such as graphic source/CPU, OS, graphic card, monitor, USB-HID/USB 2.0 devices, interconnect cable) including manufacturer and model number
- Results from any testing you have done

18.2 Shipping Checklist

1. To return your device, you need an RMA number (Return-Material-Authorization). Therefore, please contact your dealer.
2. Package your devices carefully. Add all pieces which you received originally. Preferably use the original box.
3. Note your RMA number visibly on your shipment.

Devices that are sent in without an RMA number will not be accepted. The shipment will be sent back without being opened; postage unpaid.

19 Glossary

The following terms are commonly used in this manual or in video and KVM technology.

Term	Description
AA server	Authentication and Authorization (AA) server
Cat X	Any Cat 5e (Cat 6, Cat 7) cable.
CA	Certificate Authentication
CON Device	Logical object that summarizes several EXT Units of physical extender modules (CON Units) to switch more complex sink systems via matrix.
CON Unit	Decoder extender module to connect to the console (monitor(s), keyboard, and mouse; optionally also with USB 2.0 devices).
Console	Monitor, keyboard, mouse, media control, external switching solution, etc.
CSR	Certificate Signing Request
CPU Device	Logical object that summarizes several EXT Units of physical extender modules (CPU Units) to switch more complex source systems via matrix.
CPU Unit	Encoder extender module to connect to a source.
DDC	Display Data Channel (DDC) is a serial communication interface between monitor and source. DDC enables data exchange via monitor cable and an automatic installation and configuration of a monitor driver by the operating system.
DisplayPort	A VESA standardized interface for an all-digital transmission of audio and video data. It is differentiated between the DisplayPort standards 1.1 and 1.2. The signals have LVDS level.
Dual-Head	A system with two video ports.
EDID	Extended Display Identification Data (EDID) is a metadata format (128 Byte) for display devices to describe their capabilities to a video source (e.g., graphics card).
Fiber	Single-mode or multi-mode fiber cables.
KVM	Keyboard, video, and mouse.
LPCM	LPCM (Linear Pulse Code Modulation) is a pulse modulation method, also known as an uncompressed data format. The LPCM method is used for converting analog audio into digital audio with evenly large value ranges.
Mini-DisplayPort	A VESA standardized interface for an all-digital transmission of audio and video data. It is differentiated between the DisplayPort standards 1.1 and 1.2. The signals have LVDS level.
Mini-XLR	Industrial standard for electrical plug connections (3 pole) for the transmission of digital audio and control signals.
MTBF	Mean Time Between Failure (MTBF) is measured in power-on hours and describes the system reliability.
Multi-Mode	50 µm multi-mode fiber cable.
RCA (Cinch)	A non-standard plug connection for transmission of electrical audio and video signals, especially with coaxial cables.
S/PDIF	Interface for electrical or optical transmission of digital stereo audio signals between different devices used in consumer electronics.
SFP	SFPs (Small Form Factor Pluggable) are pluggable interface modules for Gigabit connections. SFP modules are available for Cat X and fiber cables.
Single-Head	A system with one video port.

Term	Description
Single-Mode	9 µm single-mode fiber cable.
TOSLINK	Standardized fiber connection system for digital transmission of audio signals (F05 plug connection).
USB-HID	USB-HID devices (Human Interface Device) allow users to interact with computers. There is no need for a special driver during installation. When connecting, the message “New USB-HID device found” is reported. Typical USB-HID devices include keyboards, mice, graphics tablets and touch screens. Storage, video, and audio devices are not USB-HID devices.

20 Index

21 Table of Figures

22 Change Log

This table offers an overview about the most important changes available, such as new functions, changed configuration or operation.

Edition	Date	Chapter	New functions/changes
REV01.00	2022-03-24	-	Initial user manual