QUICK INSTALLATION GUIDE

Raritan® Dominion® KX II-101 KVM-over-IP

PEPPERL+FUCHS

Table of Contents

I. Introduction 2

II. Raritan Dominion KX II-101 KVM-over-IP Switch 2
Device Interfaces 2
Application Setup 4

III. Preparing VisuNet RMs 5
Set IP Address of RM 5
Add KVM Switch to Trusted Sites 5
Create KVM Profile and Connect to KVM Switch 7

IV. Congifuring the KVM Switch 8
Change Username/Password 8
Enable Direct Port Access 8
Set up Date and Time 9
Create a Self-Signed Certificate 10
Import a Self-Signed Certificate 11

Introduction

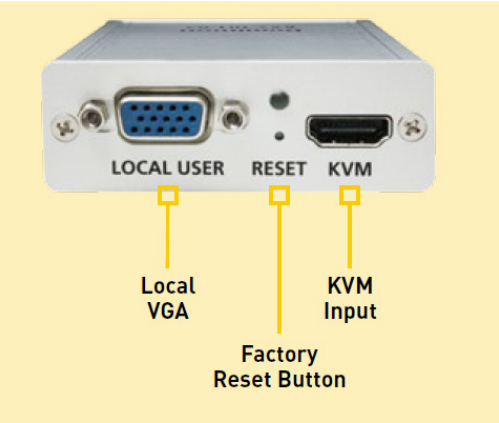
The VisuNet RM Shell 4.1.1 (or newer) embeds a software client that allows connection to Raritan® KVM-over-IP switches. The KVM-over-IP client allows a point-to-point connection between a VisuNet Remote Monitor and a Host PC to be set up in the safe area. The local host PC can be shared and remotely operated by a second user on the remote monitor in the hazardous location.

In this quick installation guide, the configuration of the RM Shell 4.1.1 (or newer) and the Raritan Dominion® KX II-101 KVM-over-IP switch is described; it is available as an accessory (DKX2-101-V2, #547998).

Raritan® Dominion® KX II-101 KVM-over-IP Switch

Device Interfaces

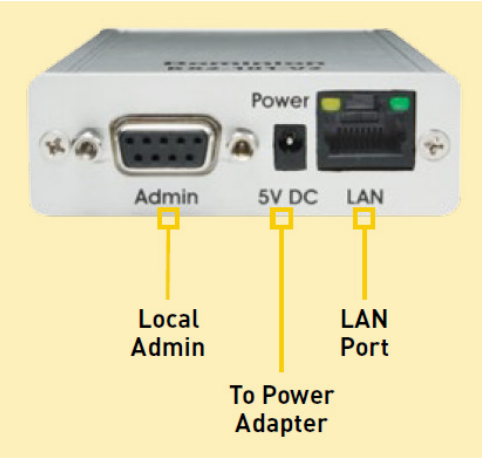
The Raritan Dominion KX II-101 KVM-over-IP switch (KVM switch) has multiple interfaces that are used to connect a VisuNet Remote Monitor / Box Thin Client (RM) to a local Host PC:



KVM Cable
VGA, PS/2, USB from Target Server

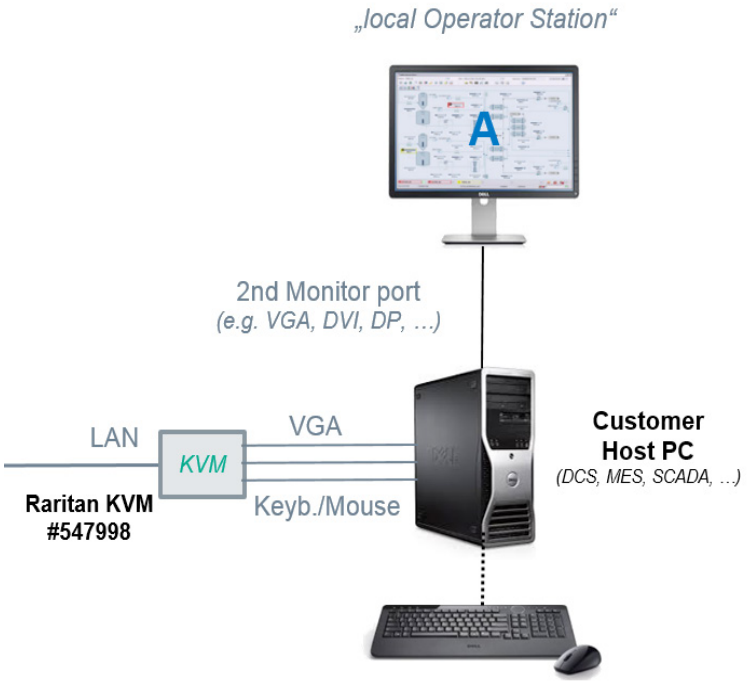
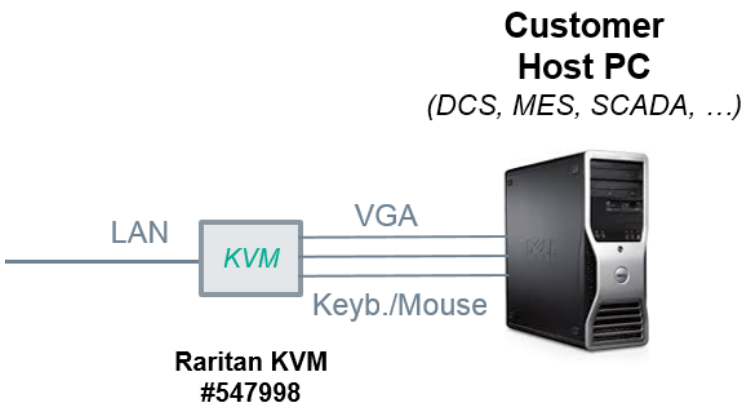
- **Local VGA:** This is a VGA port that can be used to connect an optional, local monitor to the KVM switch and share the transmitted video signal from a host PC.
- **Factory Reset Button:** This button allows the configuration of the KVM switch to be reset.
- **KVM Input:** This is the interface for the KVM cable that provides all interfaces that must be connected to the host PC.
  - **VGA:** Connect the VGA interface to the VGA port of the host PC to transmit the video signal to the KVM switch. (If the Host PC only has digital interfaces like display port, HDMI, DVI, please use a digital-to-analog signal converter.)
  - **USB:** Connect the USB interface to a USB port of the host PC to forward the keyboard/mouse to the host PC.
  - (**PS/2:** You can also use the PS/2 ports to forward the keyboard/mouse to the host PC.)

Pepperl+Fuchs Group www.pepperl-fuchs.com
Germany: +49 621 776 2222 pa-info@de.pepperl-fuchs.com
USA: 330 486 0002 pa-info@us.pepperl-fuchs.com
Singapore: +65 67799091 pa-info@sg.pepperl-fuchs.com



- (**Local Admin**: Serial port for local administration of a host PC — this interface is not relevant for VisuNet Remote Monitors.)
- **To Power Adapter:** This is the interface to power the KVM switch.
- **LAN Port:** This is the Ethernet port that must be connected with the RM.

There are multiple setup options for the KVM switch:

Connection with Local Monitor (connected to host PC): Use this setup if you want to operate the host PC locally and via an RM that is connected via LAN. *(recommended setup)*	
Connection without Local Monitor: Use this setup if you do not want to locally operate the host PC but only want to operate the host PC via an RM that is connected via LAN.	

Application Setup

In addition to the local setup of the KVM switch and the host PC, there are also multiple options for connecting the KVM switch to an RM and integrating the KVM switch into a network:

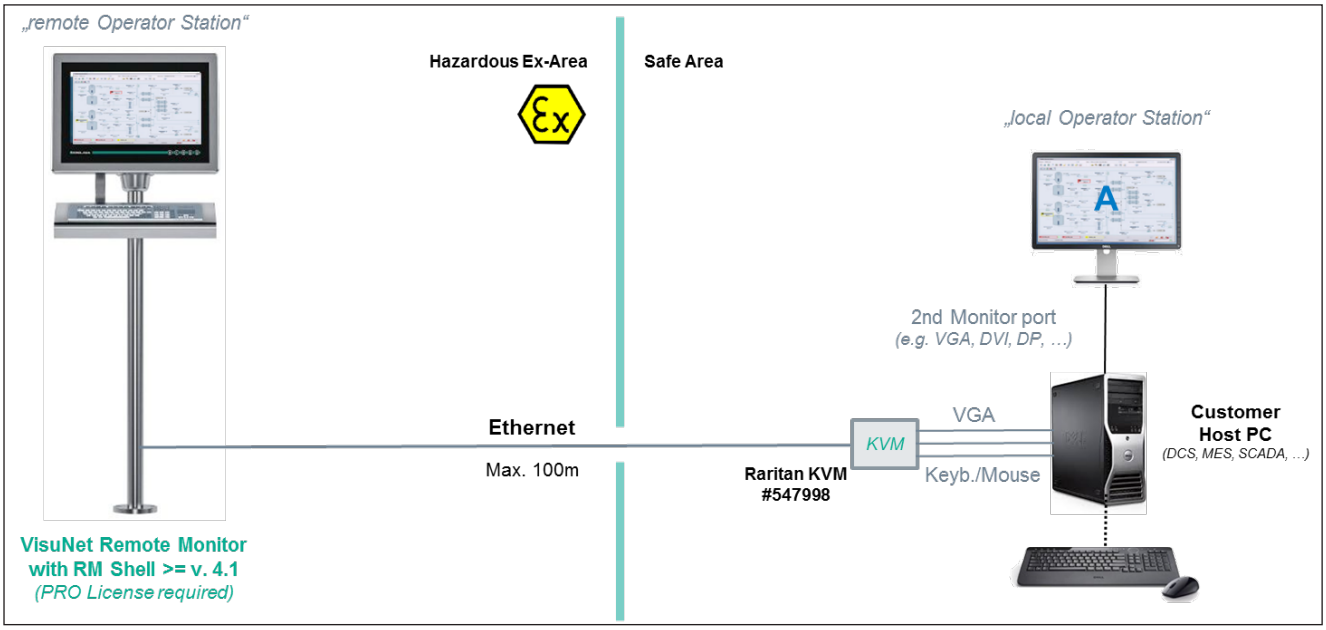


Figure 1: RM and KVM switch (point-to-point)

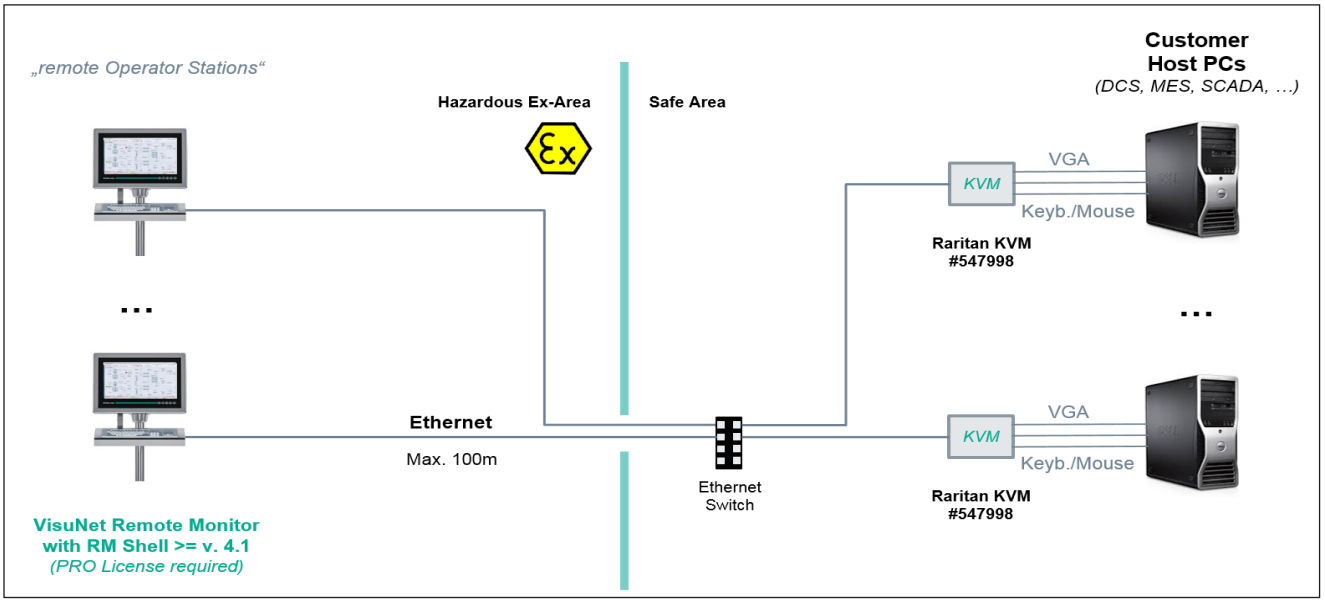


Figure 2: RMs and KVM switches (Ethernet switched)

PEPPERL+FUCHS
Pepperl+Fuchs Group
www.pepperl-fuchs.com
Germany: +49 621 776 2222
pa-info@de.pepperl-fuchs.com
USA: 330 486 0002
pa-info@us.pepperl-fuchs.com
Singapore: +65 67799091
pa-info@sg.pepperl-fuchs.com

Preparing VisuNet Remote Monitors / Box Thin Clients

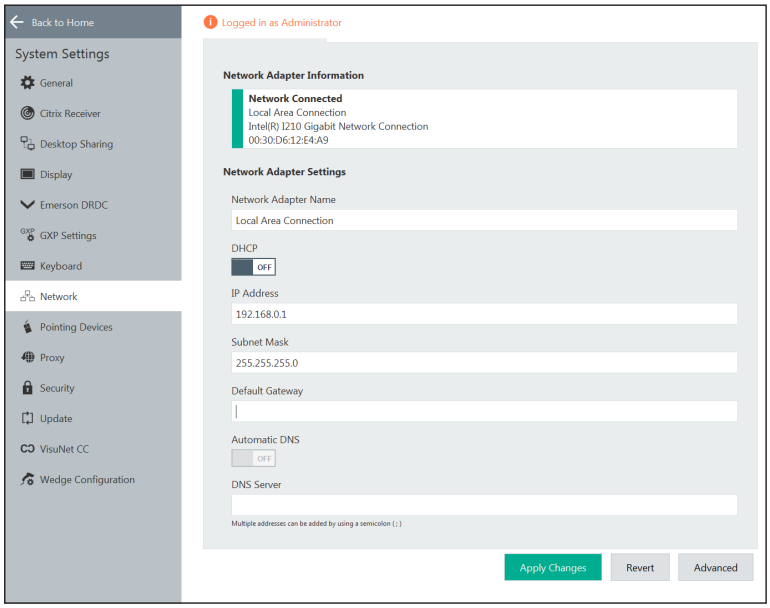
In this section, the steps for a direct connection between an RM and a KVM switch are described. Before you can connect with a VisuNet RM Shell KVM profile to a host PC, you need to configure the KVM switch.

Note: The following steps describe the configuration of the KVM switch from an RM. The setup can also be performed from a standard PC.

Set IP Address of RM

First, change the IP address of the RM to a static IP address that is within the IP address range of the KVM switch (192.168.0.xxx).

("Sytem Settings" app ➔ Network ➔ IP Address)

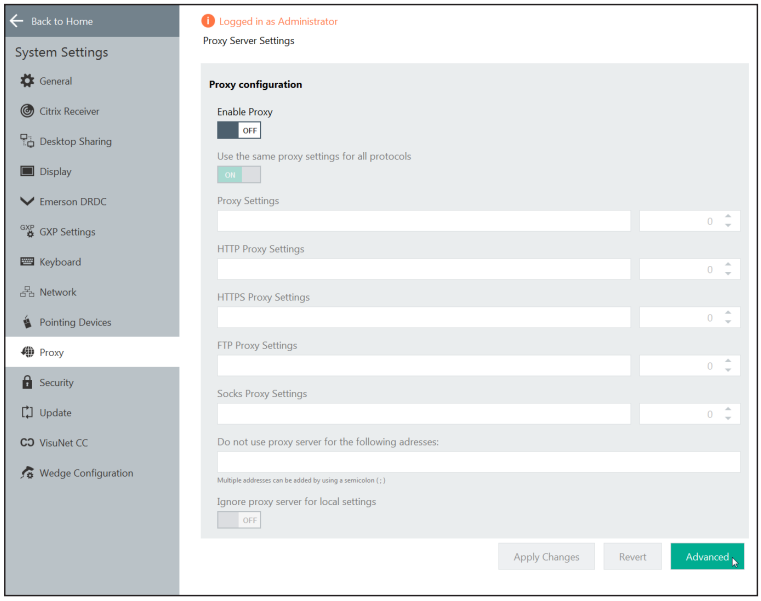


Add KVM Switch to Trusted Sites

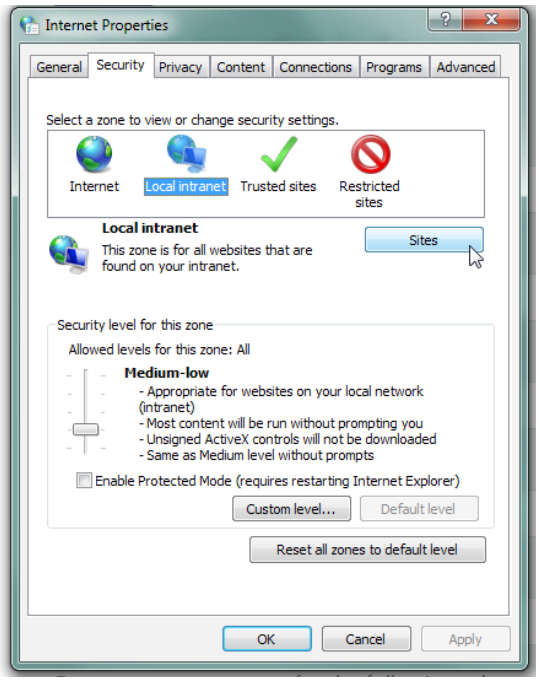
Especially when you use a point-to-point connection to the KVM switch, the certificate-based communication can pose a problem since the certificate cannot be properly validated. To overcome this problem, we recommend that the KVM switch be added to the trusted intranet zone and that the the security settings are losened. This allows a direct connection to be established without warning pop-ups.

Note: If you are using a multiport KVM switch that is maintained by IT and has a valid certificate installed, you can skip the following steps.

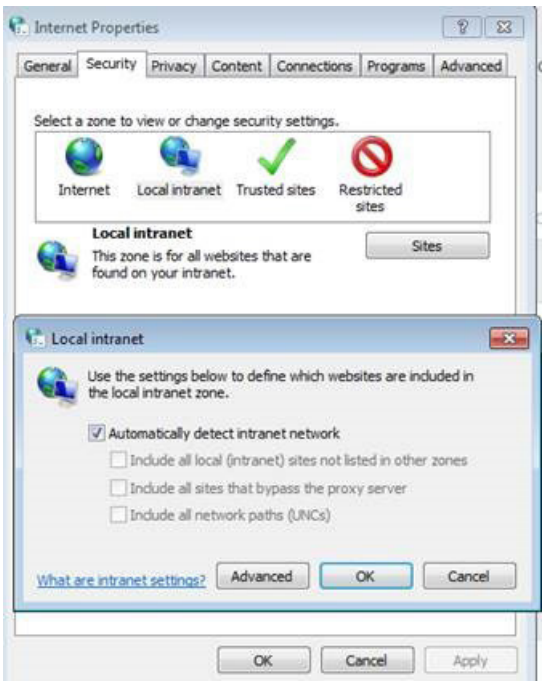
1. Open Internet Properties in RM Shell.
   b. (Log in as Adminstrator)
   c. Go to "System Settings" app ➔ Proxy ➔ Click on "Advanced"

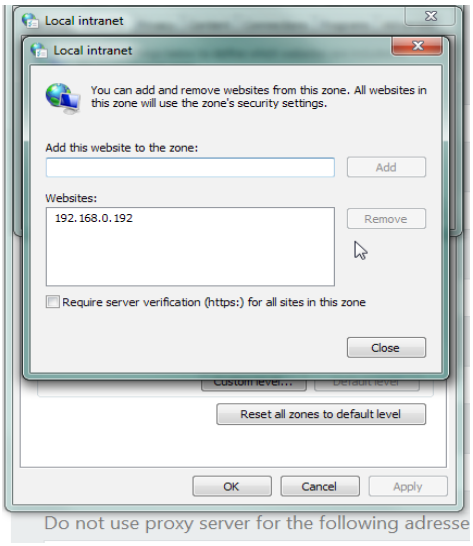


2. Add IP address of KVM switch (Default: 192.168.0.192) to the "Local intranet" zone.
   - Select the "Security" tab and the zone "Local intranet."
   - Click on "Sites."



   - Click on the "Advanced" button and add the IP address of the KVM switch to the list (default IP: 192.168.0.192). Deselect the option "Require server verification (https:) for all sites in this zone" if set.



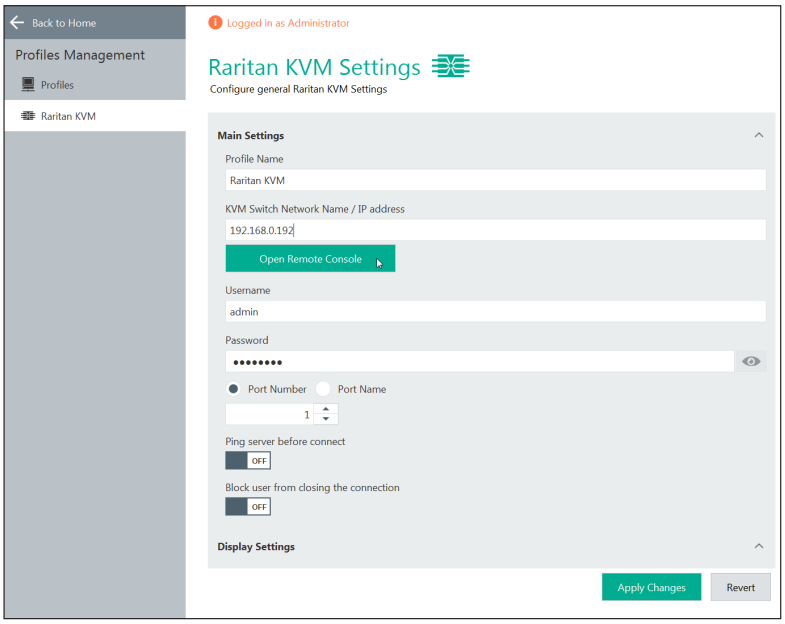


3. Change certificate settings in the "Advanced" tab.
   Disable the following two settings:
   - "Check for publisher's certificate revocation"
   - "Warn about certificate address mismatch"
4. Apply changes by pressing "OK" and reboot RM.

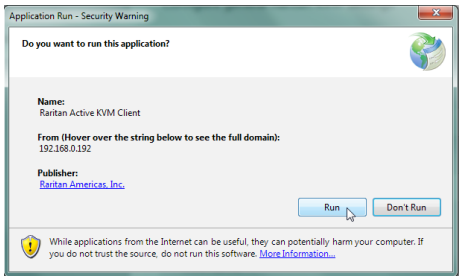
Create KVM Profile and Connect to KVM Switch

After the system has rebooted, you need to create a KVM profile and establish a connection to the KVM switch to setup the proper settings on the switch.

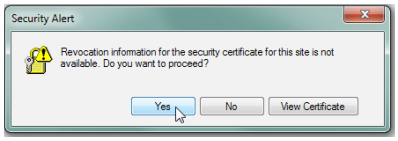
1. Go to "Profile Management" and create a new KVM profile.
2. Configure the new profile with the following parameters:
   a. Profile Name: Use a meaningful name for the connection (e.g. Raritan KVM)
   b. KVM Switch Network Name / IP address: IP Address of Raritan switch (factory default: 192.168.0.192)
   c. Username: Enter username, stored on KVM switch (factory default: admin)
   d. Password: Enter password of KVM switch user (factory default: raritan)
   e. Port number: Select port of KVM switch you want to use (factory default: 1)



1. Open the connection initially by pressing "Open Remote Console." A connection to the KVM switch will be established and you will be prompted to choose whether you want to run the client application.
   a. Press "Run" to download the KVM client application onto the RM.



   b. Two security alerts will pop up that will ask you if you would like to proceed with the following settings. Press "Yes" to accept.



The connection will finally be established, the KVM switch will be loaded, and the login window will appear.

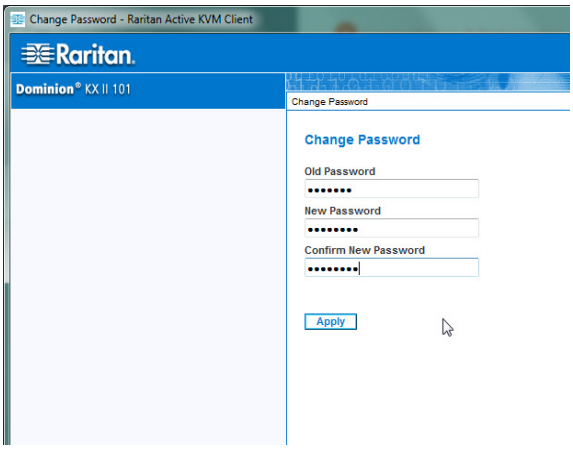
Configuring the KVM Switch

In this section, the configuration steps are described that are required to establish a connection from an RM to a KVM switch.

Change Username/Password

When you log in for the first time to the KVM switch, you will be prompted to change the default username and password (admin / raritan).

Use a strong password to increase system security.

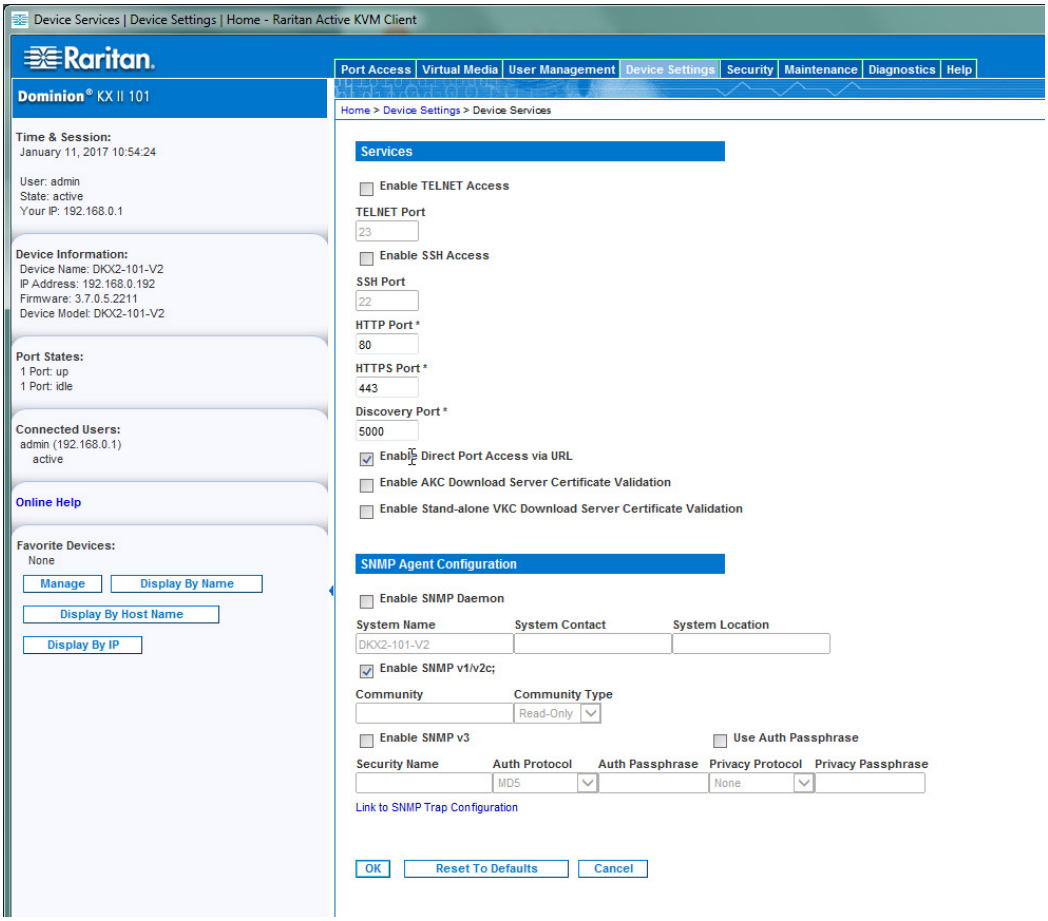


Note: If you change the username or password, please also update the username and password stored in the Raritan KVM profile on the RM.

Enable Direct Port Access (DPA)

The RM Shell requires DPA to be activated on the KVM switch.

- Navigate to “Device Settings ➔ Device Services” and enable "Enable Direct Port Access via URL."

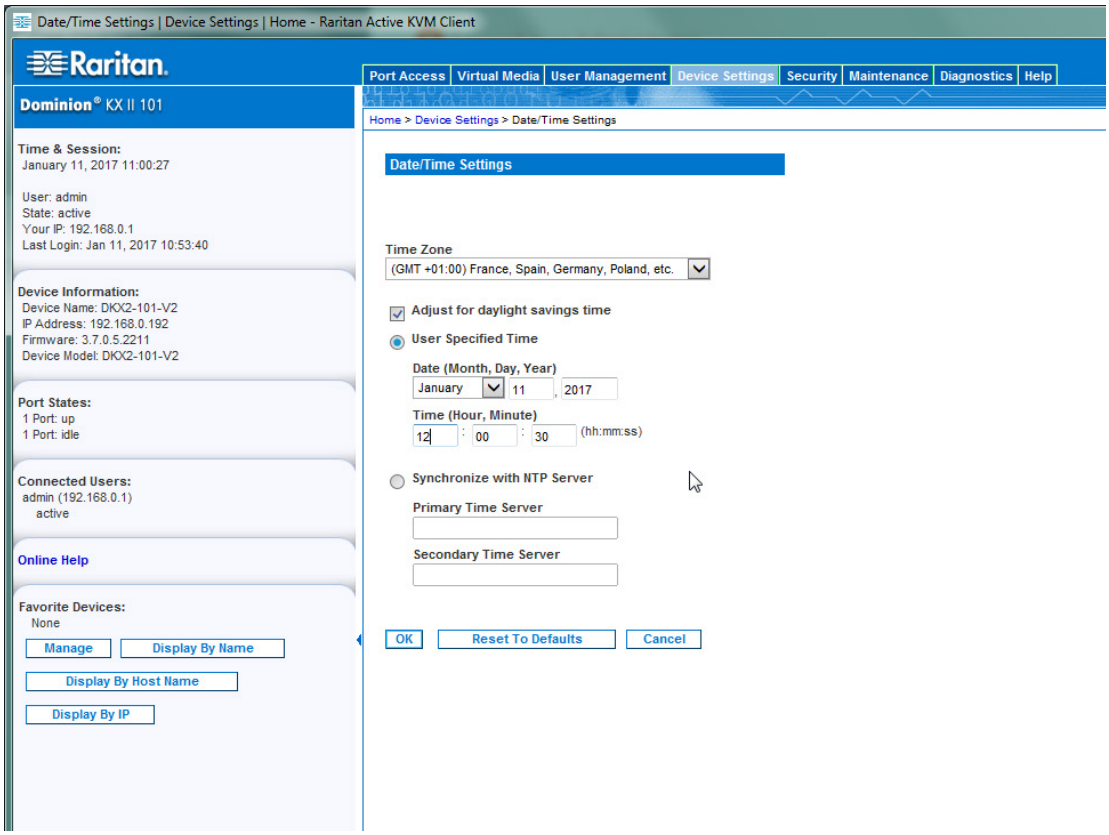


PEPPERL+FUCHS
Pepperl+Fuchs Group www.pepperl-fuchs.com
Germany: +49 621 776 2222 pa-info@de.pepperl-fuchs.com
USA: 330 486 0002 pa-info@us.pepperl-fuchs.com
Singapore: +65 67799091 pa-info@sg.pepperl-fuchs.com

Set up Date and Time

Check the KVM switch time.

- Navigate to "Device Settings ➔ Date/Time" and update the date and time.



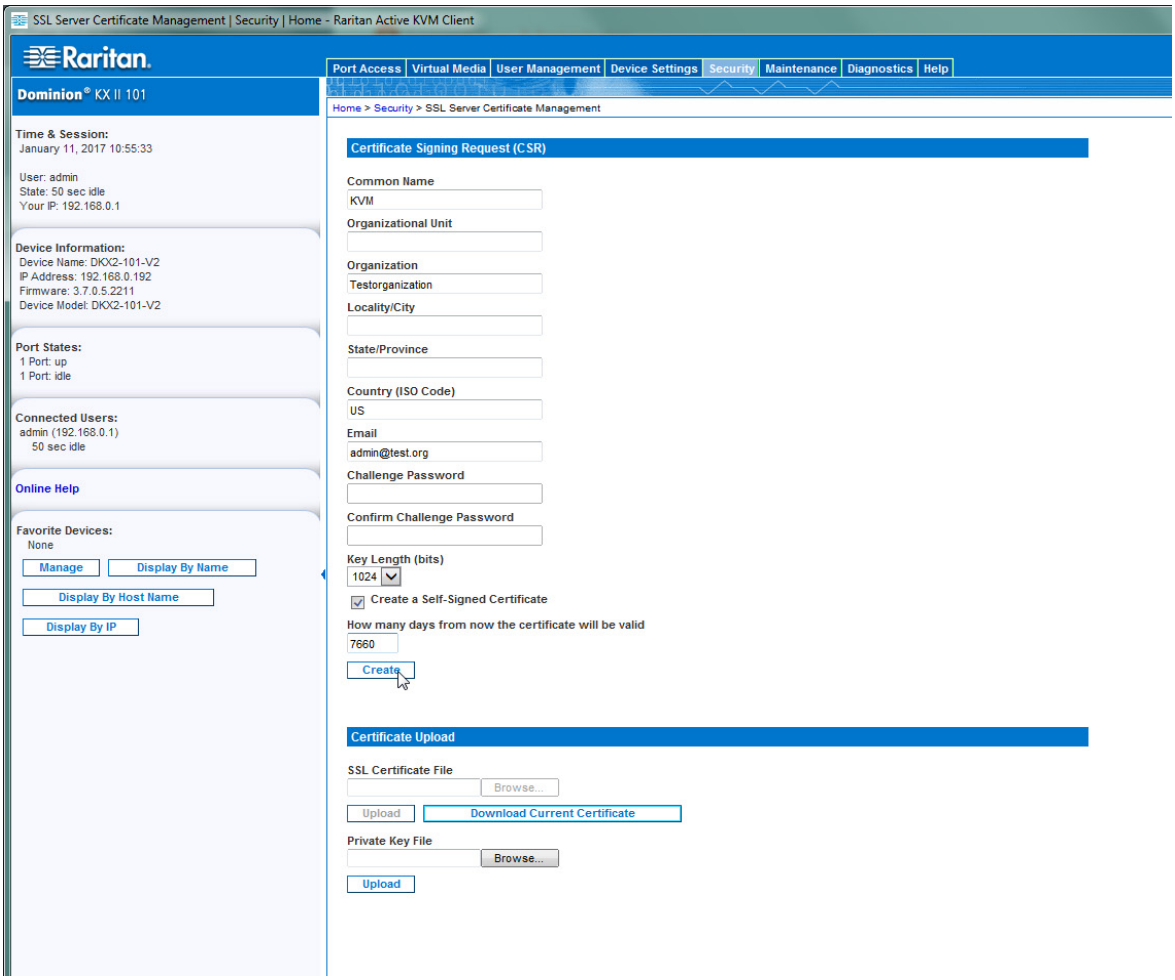
IMPORTANT: The times on the RM and KVM switch must match!

Create a Self-Signed Certificate

Note: This step is only required if you do not have a valid "company certificate" that can be used on the KVM switch.

IMPORTANT: A self-signed certificate should only be used when a direct connection between an RM and a KVM switch is established and when the RM is not connected to a company intranet or Internet.

1. Navigate to "Security ➔ Certificate" and create a new certificate with your organization information. (If you have a certificate available, you can upload it via "Certificate upload.")

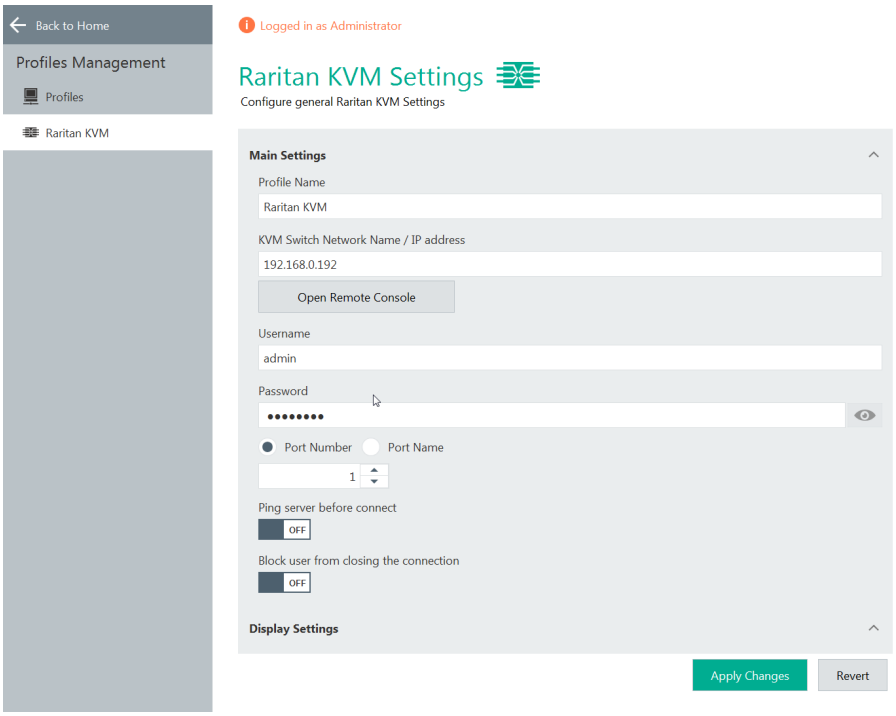


2. Click "Create" to create the certificate. You will be prompted to choose whether you want to create a self-signed certificate. Click "OK."
3. After the Certificate has been created successfully on the KVM switch, reboot the device. Navigate to "Maintenance ➔ Reboot."
4. Close the Remote Console window.
5. Update the username and password of the KVM profile settings.
6. Apply the changes.

Import a Self-Signed Certificate

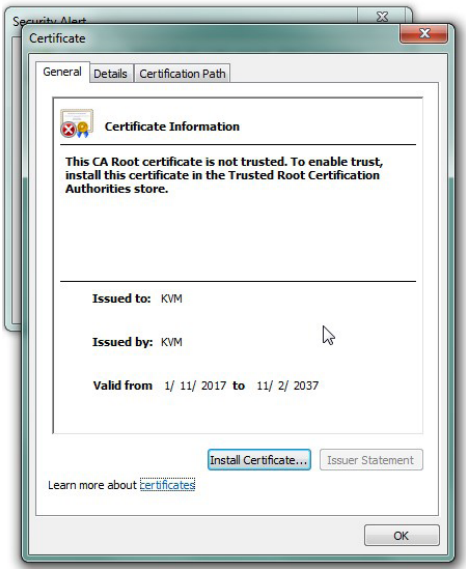
When you have created a self-signed certificate on the KVM switch, you need to import the created certificate into the RM Shell.

1. Open the KVM profile settings on the RM.
2. Connect to the KVM switch by pressing "Open Remote Console"

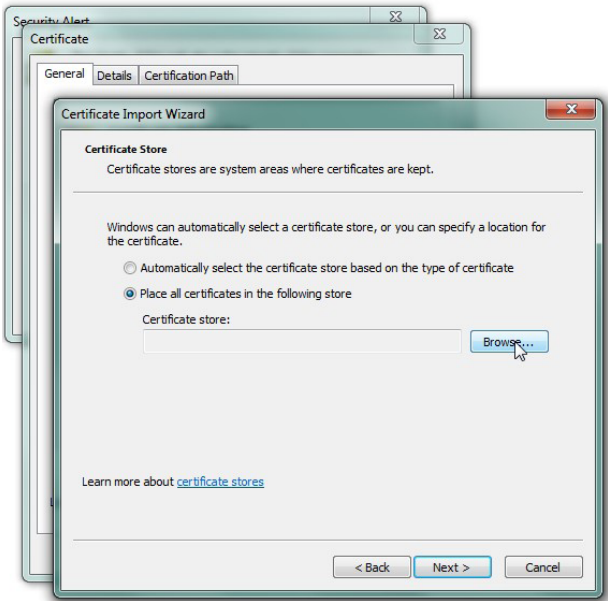


3. When the connection is established, you are prompted with a security alert that the integrity of the connection cannot be verified. Open the certificate by clicking "View Certificate."

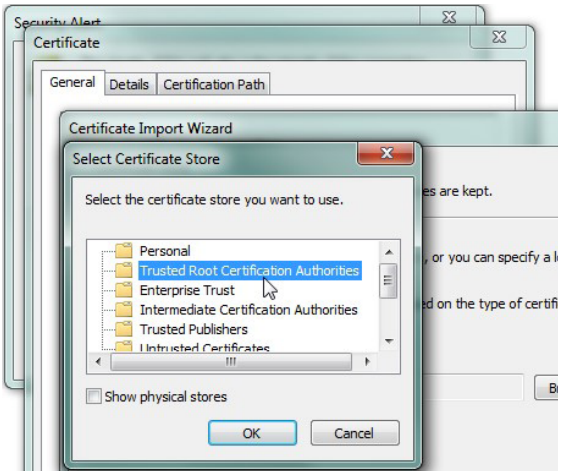
4. Now you need to import the certificate into the Trusted Root Certificate Authorities Store.
   a. Click on "Install Certificate." A new window opens.



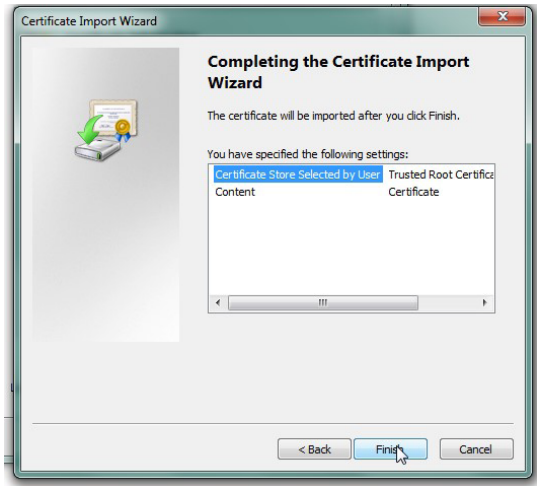
   b. Select "Place all certificates in the following store" and press "Browse."

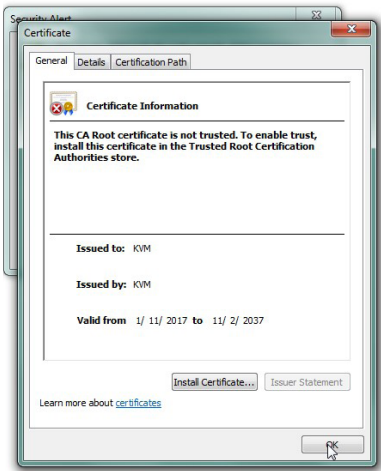


   c. Select the folder "Trusted Root Certification Authorities" and press "OK."

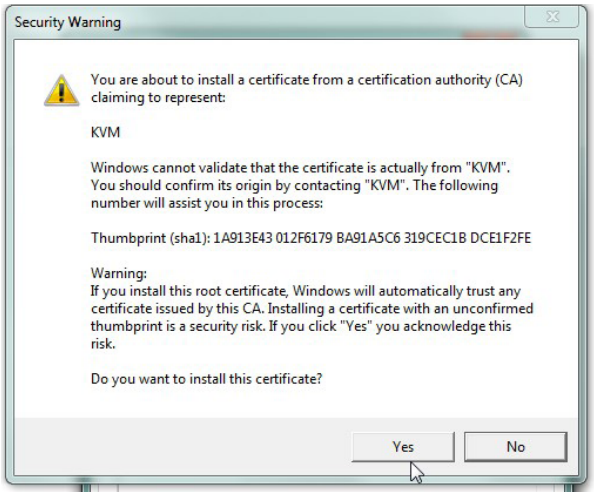


d. Import the certificate by pressing "Finish." Close the window by pressing "OK."

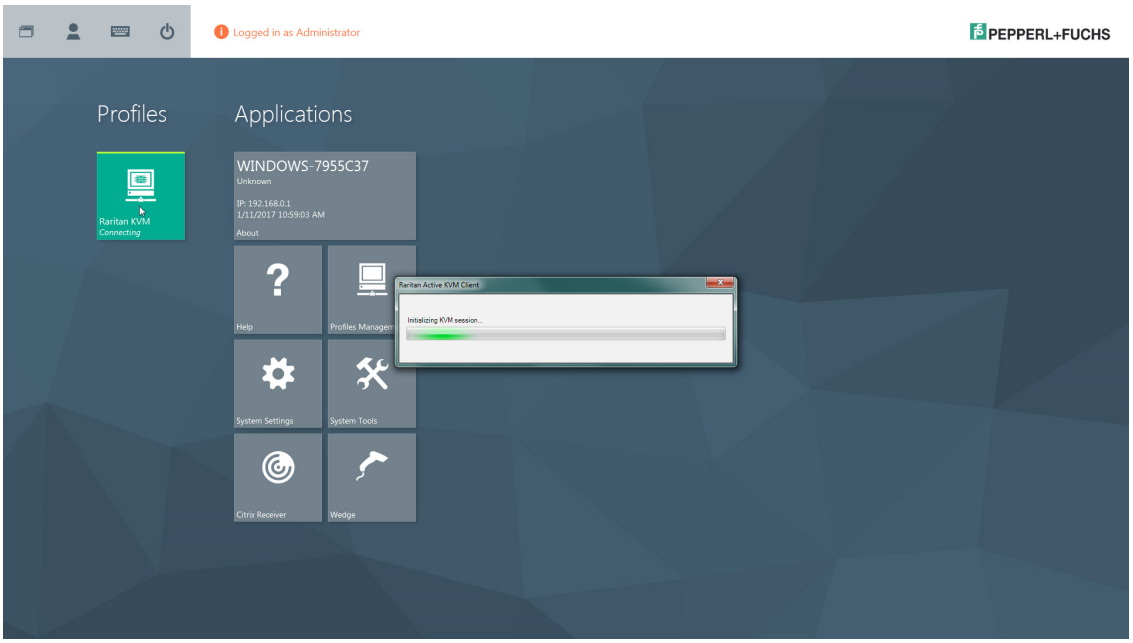




e. A security warning pops up and asks if you really want to install the certificate. Accept by pressing "Yes." The certificate has now been successfully imported.



5. After you have imported the certificate, close the Remote Console window.
6. The KVM switch and KVM profile are now configured, and operators can start them by clicking the profile on the home screen of the RM Shell.



Your automation, our passion.

Explosion Protection

- Intrinsically Safe Barriers
- Signal Conditioners
- Fieldbus Infrastructure
- Remote I/O Systems
- HART Interface Solutions
- Wireless Solutions
- Level Measurement
- Purge and Pressurization Systems
- Industrial Monitors and HMI Solutions
- Electrical Explosion Protection Equipment
- Solutions with Explosion Protection

Industrial Sensors

- Proximity Sensors
- Photoelectric Sensors
- Industrial Vision
- Ultrasonic Sensors
- Rotary Encoders
- Positioning Systems
- Inclination and Acceleration Sensors
- AS-Interface
- Identification Systems
- Logic Control Units
- Connectivity

PEPPERL+FUCHS

www.pepperl-fuchs.com

Printed in Germany · TDOCT-5540_ENG 01/17 00