DIVAR IP 7000 1U

DIP-7040-00N, DIP-7042-2HD, DIP-7042-4HD

BOSCH

en Installation Manual

Table of contents

1	**Safety precautions**	**5**
1.1	General safety precautions	5
1.2	Electrical safety precautions	6
1.3	ESD precautions	7
1.4	Operating precautions	7
1.5	Important notices	8
1.6	FCC and ICES compliance	8
2	**System overview**	**9**
2.1	Chassis features	9
2.2	Chassis components	9
2.2.1	Chassis	9
2.2.2	Backplane	10
2.2.3	Fans	10
2.2.4	Mounting rails	10
2.2.5	Power supply	10
2.2.6	Air shroud	10
2.3	System interface	10
2.3.1	Control panel buttons	11
2.3.2	Control panel LEDs	11
2.3.3	Power supply LEDs and overheat indicators	12
3	**Inserting hard disks**	**13**
4	**Rack installation**	**14**
4.1	Unpacking the system	14
4.2	Preparing for setup	14
4.2.1	Choosing a setup location	14
4.2.2	Rack precautions	14
4.2.3	General system precautions	15
4.2.4	Rack mounting considerations	15
4.3	Rack mounting instructions	16
4.3.1	Identifying the sections of the rack rails	16
4.3.2	Installing the inner rails	17
4.3.3	Assembling the outer rails	17
4.3.4	Installing the outer rails to the rack	18
4.3.5	Installing the chassis into the rack	19
4.3.6	Installing the chassis into a Telco rack	20
4.4	Turning on the system	20
5	**System setup - first steps**	**21**
5.1	Introduction	21
5.2	Setup instruction	21
5.3	Starting the Application	21
5.4	Using Bosch VMS Config Wizard	22
5.5	Using Bosch VMS Configuration Client	33
5.5.1	Assigning device IP addresses	33
5.5.2	Adding additional licenses	34
5.6	Using Bosch VMS Operator Client	34
6	**Installing additional drives**	**36**
6.1	Adding new drives to Windows Server	36

6.2	Creating a VHD iSCSI target for VRM	36
6.3	Adding and formatting the VHD as a VRM target	37
7	**Connecting to the internet**	**38**
7.1	Protecting the system from unauthorized access	38
7.2	Setting up port forwarding	38
7.2.1	Setting up port forwarding in DIVAR IP	38
7.2.2	Setting up port forwarding in the router	38
7.2.3	Example for port forwarding	38
7.3	Choosing an appropriate client	39
7.3.1	Remote connection with Operator Client	39
7.3.2	Remote connection with Video Security App	40
7.4	Installing an Enterprise Management Server	40
8	**Recovering the unit**	**41**
9	**Additional documentation and client software**	**42**
10	**Appendices**	**43**
10.1	Motherboard	43
10.1.1	Motherboard layout	43
10.1.2	Motherboard component overview	44
10.1.3	Motherboard features	46
10.1.4	Block diagram	48
10.2	Chipset overview	48
10.3	PC health monitoring	49
10.4	Power configuration settings	49
10.5	Power supply	50
10.6	Super I/O	50
10.7	iSCSI support	50
10.8	Overview of the Nuvoton BMC controller	51

1 Safety precautions

Observe the safety precautions in this chapter.

1.1 General safety precautions

Follow these rules to ensure general safety:

- Keep the area around the system clean and free of clutter.
- Place the chassis top cover and any system components that have been removed away from the system or on a table so that they won't accidentally be stepped on.
- While working on the system, do not wear loose clothing such as neckties and unbuttoned shirt sleeves, which can come into contact with electrical circuits or be pulled into a cooling fan.
- Remove any jewelry or metal objects from your body, which are excellent metal conductors that can create short circuits and harm you if they come into contact with printed circuit boards or areas where power is present.
- After accessing the inside of the system, close the system back up and secure it to the rack unit after ensuring that all connections have been made.
- The system is heavy when fully loaded. When lifting the system, two people at either end should lift slowly with their feet spread out to distribute the weight. Always keep your back straight and lift with your legs.

Warning!

Interruption of mains supply:
Voltage is applied as soon as the mains plug is inserted into the mains socket.
However, for devices with a mains switch, the device is only ready for operation when the mains switch (ON/OFF) is in the ON position. When the mains plug is pulled out of the socket, the supply of power to the device is completely interrupted.

Warning!

Removing the housing:
To avoid electric shock, the housing must only be removed by qualified service personnel. Before removing the housing, the plug must always be removed from the mains socket and remain disconnected while the housing is removed. Servicing must only be carried out by qualified service personnel. The user must not carry out any repairs.

Warning!

Power cable and AC adapter:
When installing the product, use the provided or designated connection cables, power cables and AC adaptors. Using any other cables and adaptors could cause a malfunction or a fire. Electrical Appliance and Material Safety Law prohibits the use of UL or CSA-certified cables (that have UL/CSA shown on the code) for any other electrical devices.

Warning!

Lithium battery:

Batteries that have been inserted wrongly can cause an explosion. Always replace empty batteries with batteries of the same type or a similar type recommended by the manufacturer. Handle used batteries carefully. Do not damage the battery in any way. A damaged battery may release hazardous materials into the environment.

Dispose of empty batteries according to the manufacturer's instructions.

Warning!

Handling of lead solder materials used in this product may expose you to lead, a chemical known to the State of California to cause birth defects and other reproductive harm.

Notice!

Electrostatically sensitive device:

To avoid electrostatic discharges, the CMOS/MOSFET protection measures must be carried out correctly.

When handling electrostatically sensitive printed circuits, grounded anti-static wrist bands must be worn and the ESD safety precautions observed.

Notice!

Installation should only be carried out by qualified customer service personnel in accordance with the applicable electrical regulations.

Disposal

Your Bosch product has been developed and manufactured using high-quality materials and components that can be reused.

This symbol means that electronic and electrical devices that have reached the end of their working life must be disposed of separately from household waste.

In the EU, separate collecting systems are already in place for used electrical and electronic products. Please dispose of these devices at your local communal waste collection point or at a recycling center.

1.2 Electrical safety precautions

Basic electrical safety precautions should be followed to protect you from harm and the system from damage:

- Be aware of the locations of the power on/off switch on the chassis as well as the room's emergency power-off switch, disconnection switch or electrical outlet. If an electrical accident occurs, you can then quickly remove power from the system.
- Do not work alone when working with high voltage components.
- Power should always be disconnected from the system when removing or installing main system components, such as the motherboard or memory modules. When disconnecting power, you should first turn off the system and then unplug the power cords from all the power supply modules in the system.
- When working around exposed electrical circuits, another person who is familiar with the power-off controls should be nearby to switch off the power if necessary.

- Use only one hand when working with powered-on electrical equipment. This is to avoid making a complete circuit, which will cause electrical shock. Use extreme caution when using metal tools, which can easily damage any electrical components or circuit boards they come into contact with.
- The power supply power cords must include a grounding plug and must be plugged into grounded electrical outlets. The unit has more than one power supply cord. Disconnect both power supply cords before servicing to avoid electrical shock.
- Mainboard replaceable soldered-in fuses: Self-resetting PTC (Positive Temperature Coefficient) fuses on the mainboard must be replaced by trained service technicians only. The new fuse must be the same or equivalent as the one replaced. Contact technical support for details and support.

Caution!
Mainboard Battery: There is a danger of explosion if the onboard battery is installed upside down, which will reverse its polarities. This battery must be replaced only with the same or an equivalent type recommended by the manufacturer (CR2032). Dispose of used batteries according to the manufacturer's instructions.

Caution!
DVD-ROM Laser: This system comes without a DVD-ROM drive but if added: To prevent direct exposure to the laser beam and hazardous radiation exposure, do not open the enclosure or use the unit in any unconventional way.

1.3 ESD precautions

Electrostatic Discharge (ESD) is generated by two objects with different electrical charges coming into contact with each other. An electrical discharge is created to neutralize this difference, which can damage electronic components and printed circuit boards. The following measures are generally sufficient to neutralize this difference before contact is made to protect your equipment from ESD:

- Do not use mats designed to decrease electrostatic discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- Use a grounded wrist strap designed to prevent static discharge.
- Keep all components and printed circuit boards (PCBs) in their antistatic bags until ready for use.
- Touch a grounded metal object before removing the board from the antistatic bag.
- Do not let components or printed circuit boards come into contact with your clothing, which may retain a charge even if you are wearing a wrist strap.
- Handle a board by its edges only. Do not touch its components, peripheral chips, memory modules or contacts.
- When handling chips or modules, avoid touching their pins.
- Put the mainboard and peripherals back into their antistatic bags when not in use.
- For grounding purposes, make sure your computer chassis provides excellent conductivity between the power supply, the case, the mounting fasteners and the mainboard.

1.4 Operating precautions

The chassis cover must be in place when the system is operating to assure proper cooling. Out of warranty damage to the system can occur if this practice is not strictly followed.

Note:
Please handle used batteries carefully. Do not damage the battery in any way. A damaged battery may release hazardous materials into the environment. Do not discard a used battery in the garbage or a public landfill. Please comply with the regulations set up by your local hazardous waste management agency to dispose of your used battery properly.

1.5 Important notices

	**Accessories** - Do not place this unit on an unstable stand, tripod, bracket, or mount. The unit may fall, causing serious injury and/or serious damage to the unit. Use only with the cart, stand, tripod, bracket, or table specified by the manufacturer. When a cart is used, use caution and care when moving the cart/apparatus combination to avoid injury from tip-over. Quick stops, excessive force, or uneven surfaces may cause the cart/unit combination to overturn. Mount the unit per the manufacturer's instructions.

1.6 FCC and ICES compliance

(only for U.S.A. and Canada)
This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer’s instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

2 System overview

DIVAR IP 7000 1U is an affordable, simple and reliable all-in-one recording, viewing and management solution for network surveillance systems of up to 64 channels (with 32 channels pre-licensed). Running the full Bosch VMS (Video Management System) solution and powered by Bosch VRM (Video Recording Manager) software, the DIVAR IP 7000 1U is an intelligent IP storage device that eliminates the need for separate NVR (Network Video Recorder) server and storage hardware.

The 1U unit combines advanced management and state-of-the-art recording management into a single cost-effective, plug and play IP recording appliance for IT-minded customers which are seeking for a state-of-the-art “second generation” NVR recording solution.

DIVAR IP 7000 1U features:

- Instant real time access to video
  View high quality HD video despite low or limited bandwidth connections. Dynamic Transcoding technology ensures that you can view your video immediately — anytime, anywhere.
- Easy installation
  DIVAR IP 7000 1U features wizard based set-up and centralized configuration to reduce installation times. All components are pre-installed and pre-configured. Simply connect to the network and turn on the unit — DIVAR IP 7000 1U starts recording straight out of the box.
- Access to Bosch VMS
  After starting the system, immediate access to the Bosch VMS management application is offered by a customized user interface. The ability to use one central user interface for configuration and operation management reduces installation and training requirements, and helps to keep ongoing system management costs low.

2.1 Chassis features

The chassis includes the following features:

- 4 slots for 4 SATA drives
- Graphic card (1x DVI, 1x Display Port output)
- One slim DVD-RW drive. This drive allows you to quickly install or save data.
- One internal USB Transcoder device
- Other onboard features are included to promote system health. These include various cooling fans, a convenient power switch and a reset button.

2.2 Chassis components

This chapter describes the most common components included with your chassis. For more information, see the installation instructions detailed later in this manual.

2.2.1 Chassis

The chassis includes 4 hard drive bays and supports a 1U backplane, fans and two power supplies.

2.2.2 Backplane

Each chassis comes with a 1U backplane. The backplane accepts SAS/SATA hard drives.

Warning!

Use caution when servicing and working around the backplane. Hazardous voltage or energy is present on the backplane when the system is operating. Do not touch the backplane with any metal objects and make sure no ribbon cables touch the backplane.

2.2.3 Fans

The chassis supports system fans that are 1U high and powered from the motherboard.

2.2.4 Mounting rails

The unit can be placed in a rack for secure storage and use. To setup your rack, follow the step-by-step instructions included in this manual.

2.2.5 Power supply

Each chassis model includes 2 high-efficiency power supplies (redundant). In the unlikely event your power supply fails, replacement is simple and can be accomplished without tools.

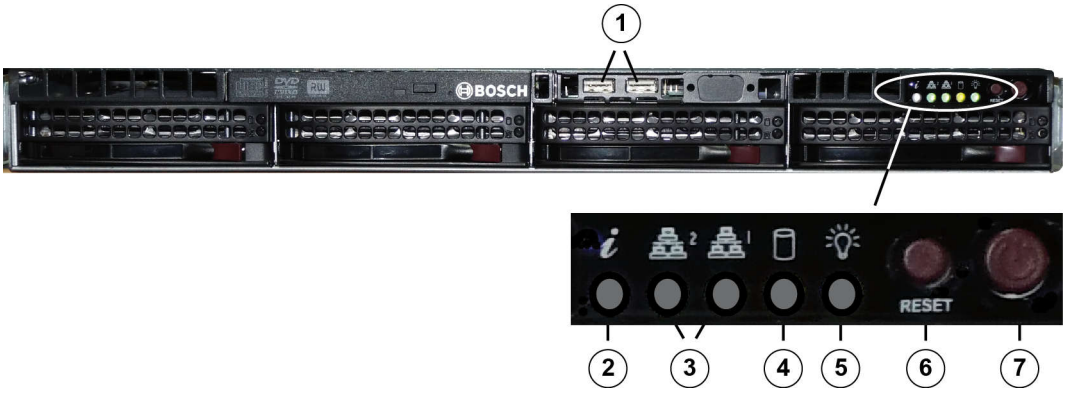
2.2.6 Air shroud

Air shrouds are shields, usually plastic, which conduct the airflow directly to where it is needed. Always use the air shroud included with your chassis.

2.3 System interface

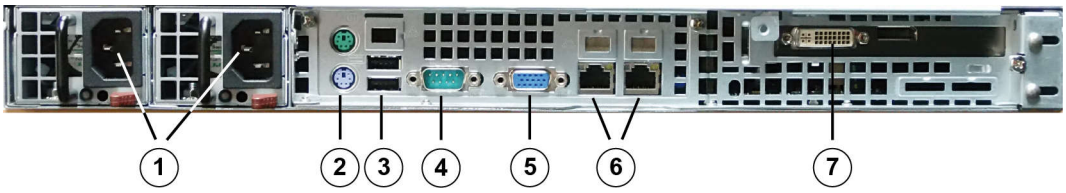
There are several LEDs on the front and rear of the chassis. The LEDs show the over-all status of the system and the activity and health of specific components.

Front view:



1	2x USB 2.0	**5**	Power
2	Failure information (not used)	**6**	Reset
3	NIC1/NIC2	**7**	Power on/off
4	HDD		

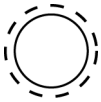
Rear view:



1	2x mains connection 100 – 240 VAC, 50 - 60 Hz **Note:** Connect both power cables.	**5**	Monitor (VGA) **Note:** Do not use!
2	2x PS/2 (mouse and keyboard)	**6**	2x NIC **Note:** Connect both NIC ports to the appropriate network switch.
3	2x USB 2.0	**7**	1x graphic card (1x Display Port, 1x DVI) **Note:** DVI port must be used for configuration.
4	Serial interface COM		

2.3.1 Control panel buttons

There are two push-buttons located on the front of the chassis. These are (in order from left to right) a reset button and a power on/off button.

–  **Reset**: The reset button is used to reboot the system.

–  **Power:** The main power switch is used to apply or remove power from the power supply to the server system. Turning off system power with this button removes the main power but keeps standby power supplied to the system. **Therefore, you must unplug system before servicing.**

2.3.2 Control panel LEDs

The control panel located on the front of the chassis has LEDs to provide you with critical information related to different parts of the system. This section explains what each LED indicates.

–  Information LED: not used

–  **NiC2**: A flashing LED indicates network activity on GLAN2.

–  **NIC1**: A flashing LED indicates network activity on GLAN1.

–  **HDD**: A flashing LED indicates IDE channel activity in the SAS/SATA drive, SCSI drive, and/or DVD-ROM drive activity.

–  **Power**: Indicates power is being supplied to the system's power supply units. This LED should normally be illuminated when the system is operating.

2.3.3 Power supply LEDs and overheat indicators

This chassis provides several options which may include hot-swappable, cold-swappable, and redundant power supplies. Some power supplies include an LED in the rear with the following definitions:

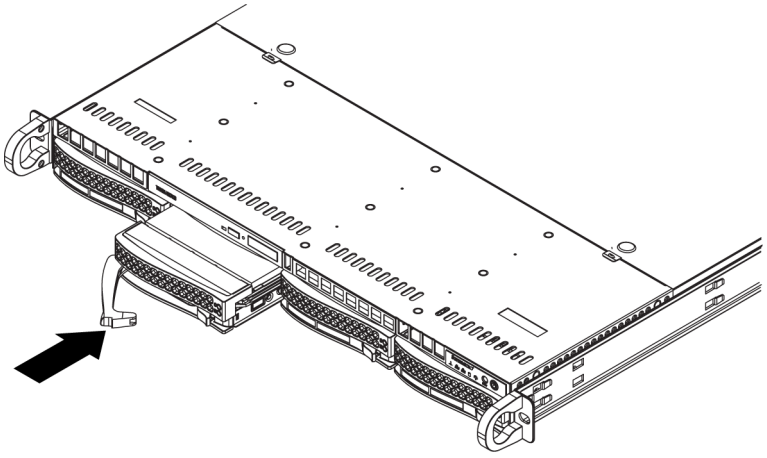
Power supply LEDs	
Solid green	Power supply is on.
Solid amber	The power supply is plugged in and turned off, or the system is off but in an abnormal state.

3 Inserting hard disks

This chapter describes the insertion of hard disks that are mounted in drive carriers to simplify their installation.

To insert the drive carrier:

- Insert the drive carrier into the chassis bay. Make sure that the drive carrier handle is completely closed.



Notice!

We recommend using the respective Bosch hard disk drives. The hard disk drives as one of the critical component are carefully selected by Bosch based on available failure rates. HDD – not delivered from Bosch – are not supported. Information on supported HDDs can be found in the datasheet in the Bosch Online Product Catalog.

See also:

– *Installing additional drives, page 36*

4 Rack installation

This chapter provides a quick setup checklist to get your chassis up and running. Following these steps in the order given should enable you to have the system operational within a minimum amount of time.

4.1 Unpacking the system

You should inspect the box the chassis was shipped in and note if it was damaged in any way. If the chassis itself shows damage, file a damage claim with the carrier who delivered it and notify the respective Bosch RMA desk.
You will also need it placed near at least one grounded power outlet.
Due to the weight of the system: After opening the top of the shipping box, one person should stand at either end and lift the disk array out together.
Be sure to read the safety precautions.

4.2 Preparing for setup

The box the system is shipped in includes a rack mount kit, which you will need to install the system into the rack.
Follow the steps in the order given to complete the installation process in a minimum amount of time. Read this section before you begin the installation procedure outlined in the sections that follow.

4.2.1 Choosing a setup location

- Situate the system in a clean, dust-free area that is well ventilated. Avoid areas where heat, electrical noise and electromagnetic fields are generated. Place the system near a grounded power outlet.
- Leave approximately 25 inches clearance in front of the rack to be able to open the front door completely.
- Leave approximately 30 inches of clearance in the back of the rack to allow for sufficient airflow and ease in servicing.
- Install the system only in a Restricted Access Location (dedicated equipment rooms, service closets and the like).

Notice!
This product is not suitable for use with visual display work place devices acccording to §2 of the the German Ordinance for Work with Visual Display Units.

4.2.2 Rack precautions

Warning!
To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- Ensure that the leveling jacks on the bottom of the rack are fully extended to the floor with the full weight of the rack resting on them.
- In single rack installations, attach stabilizers to the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- In multiple rack installations, couple the racks together.
- Always make sure the rack is stable before extending a component from the rack.
- Extend only one component at a time - extending two or more simultaneously may cause the rack to become unstable.

4.2.3 General system precautions

- Review the electrical and general safety precautions that came with the components you are adding to your chassis.
- Determine the placement of each component in the rack before installing the rails.
- Install the heaviest components on the bottom of the rack first, and then work up.
- Use a regulating uninterruptible power supply (UPS) to protect the system from power surges, voltage spikes if you want to keep your system operating in case of a power failure.
- Allow the SATA hard drives and power supply modules to cool before touching them.
- Always keep the rack's front door and all panels and components on the system closed when not servicing to maintain proper cooling.

See also:

- *Safety precautions, page 5*

4.2.4 Rack mounting considerations

Ambient operating temperature

If installed in a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature (Tmra).

Reduced airflow

Equipment should be mounted into a rack so that the amount of airflow required for safe operation is not compromised.

Mechanical loading

Equipment should be mounted into a rack so that a hazardous condition does not arise due to uneven mechanical loading.

Circuit overloading

Consideration should be given to the connection of the equipment to the power supply circuitry and the effect that any possible overloading of circuits might have on overcurrent protection and power supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Reliable ground

A reliable ground must be maintained at all times. To ensure this, the rack itself should be grounded. Particular attention should be given to power supply connections other than the direct connections to the branch circuit (i.e. the use of power strips, etc.).

4.3 Rack mounting instructions

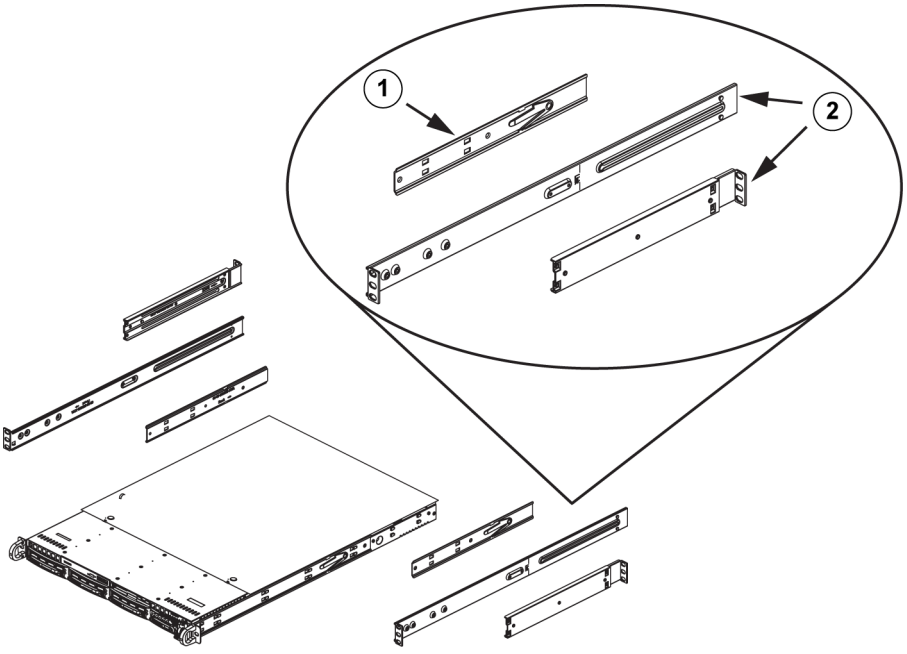
This section provides information on installing the chassis into a rack unit. There are a variety of rack units on the market, which may mean the assembly procedure will differ slightly. You should also refer to the installation instructions that came with the rack unit you are using.

Notice!
This rail will fit a rack between 26" and 33.5" deep.

4.3.1 Identifying the sections of the rack rails

The chassis package includes two rail assemblies in the rack mounting kit. Each assembly consists of two sections:

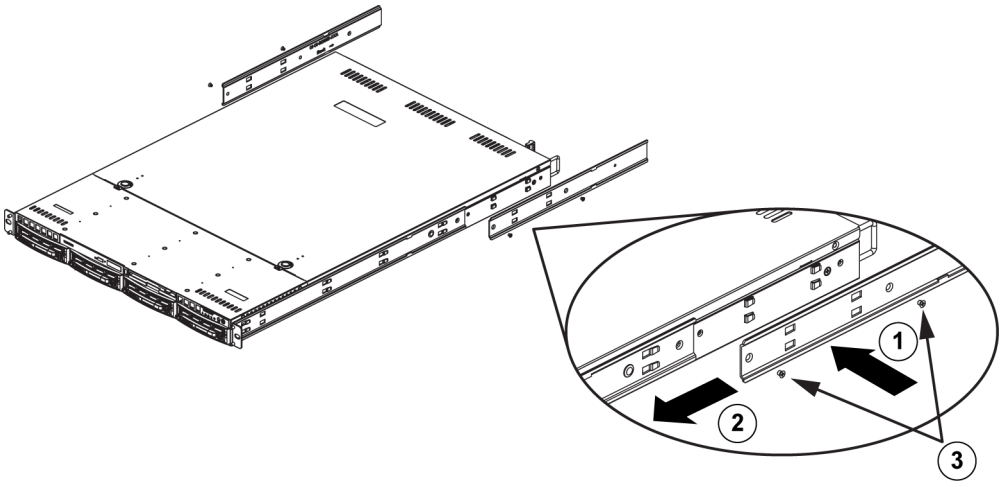
– an inner fixed chassis rail that secures directly to the chassis
– an outer fixed rack rail that secures directly to the rack itself.



1	Rail extension (inner rail is pre-installed on the chassis)
2	Outer rails

4.3.2 Installing the inner rails

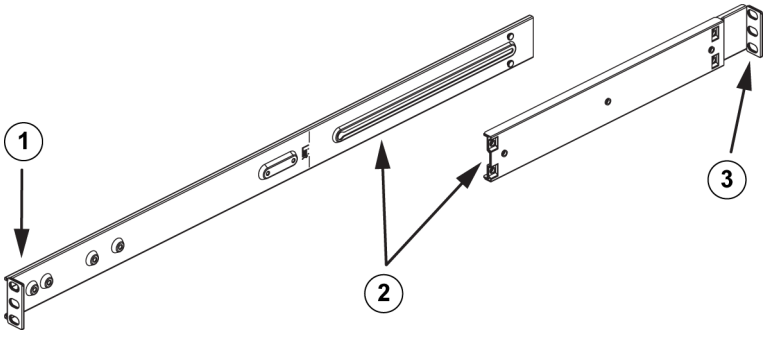
The chassis includes a set of inner rails which are in two sections: inner rails and inner rail extensions. The inner rails are pre-attached and do not interfere with normal use of the chassis if you decide not to use a server rack. Attach the inner rail extension to stabilize the chassis within the rack.



To install the inner rails:

1. Place the inner rail extensions on the side of the chassis aligning the hooks of the chassis with the rail extension holes. Make sure the extension faces "outward" just like the pre-attached inner rail.
2. Slide the extension toward the front of the chassis.
3. Secure the chassis with 2 screws as illustrated.
4. Repeat steps for the other inner rail extension.

4.3.3 Assembling the outer rails

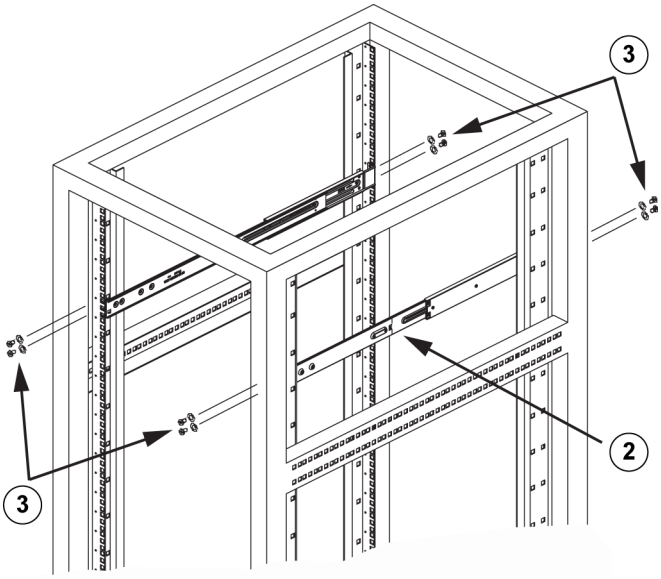


To assemble the outer rails:

1. Secure to the front of the rack.
2. Attach the two sections of the outer rail together.
3. Secure to the rear of the rack.

4.3.4 Installing the outer rails to the rack

Outer rails attach to the rack and hold the chassis in place. The outer rails extend between 30 inches and 33 inches.



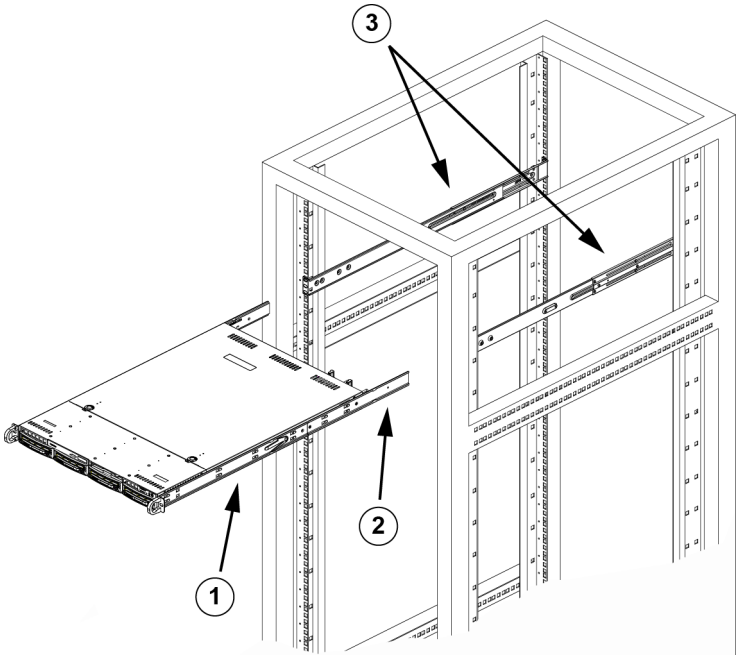
To install the outer rails to the rack

1. Attach the longer section of the outer rail to the outside of the shorter section of the outer rail. You must align the pins with the slides. Both ends of the outer rail must face the same direction in order to be secured to the rack.
2. Adjust both sections of the outer rail to the proper length so that the rail fits snugly within the rack.
3. Secure the longer section of the outer rail to the front of the rack with two M5 screws and the shorter section to the rear side of the rack with two M5 screws.
4. Repeat steps for the remaining outer rail.

See also:

– *Assembling the outer rails, page 17*

4.3.5 Installing the chassis into the rack



1	Inner rail	**3**	Outer rails
2	Rail extension		

To install the chassis into a rack

1. Confirm that chassis includes the inner rails and rail extensions. Also, confirm that the outer rails are installed on the rack.
2. Line chassis rails with the front of the rack rails.
3. Slide the chassis rails into the rack rails, keeping the pressure even on both sides (you may have to depress the locking tabs when inserting). When the system has been pushed completely into the rack, you should hear the locking tabs click.
4. (Optional) Insert and tightening the thumbscrews that hold the front of the system to the rack.

Warning!

Do not pick up the unit with the front handles. The handles are designed to pull the system from a rack only.

Warning!

Stability hazard

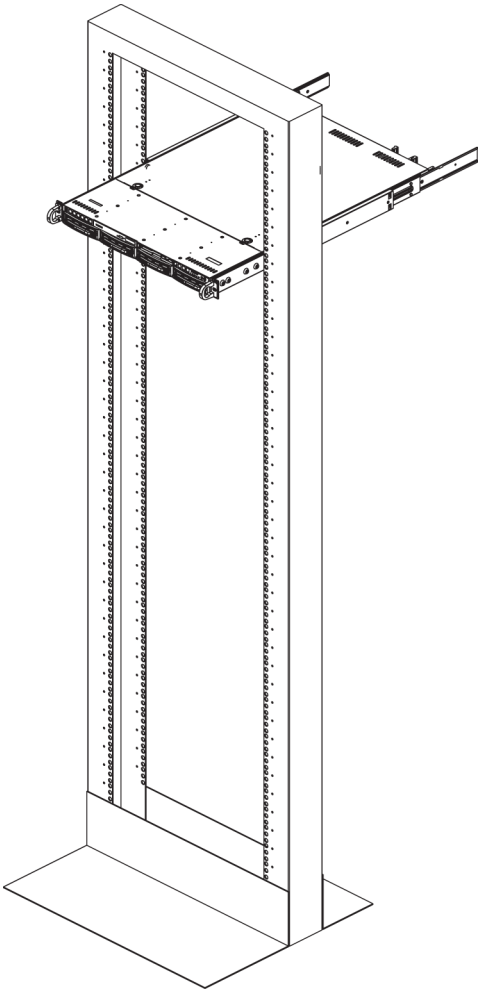
Before sliding the unit out for servicing make sure that the rack stabilizing mechanism is in place, or the rack is bolted to the floor. Failure to stabilize the rack can cause the rack to tip over.

See also:

– *Rack precautions, page 14*

4.3.6 Installing the chassis into a Telco rack

To install the chassis into a Telco type rack, use two L-shaped brackets on either side of the chassis (four in total). First, determine how far the chassis will extend out the front of the rack. Larger chassis should be positioned to balance the weight between front and back. If a bezel is included on the chassis, remove it. Then attach the two front brackets to each side of the chassis, then the two rear brackets positioned with just enough space to accommodate the width of the Telco rack. Finish by sliding the chassis into the rack and tightening the brackets to the rack.



4.4 Turning on the system

The last thing to be done is to provide input power to the system.

To turn on the system:

1. Plug the power cord from the power supply unit into a high-quality power strip that offers protection from electrical noise and power surges. We recommended using an uninterruptible power supply (UPS).
2. Press the power button on the control panel to turn on the system.

5 System setup - first steps

The following installation directive provides information on Installation and Configuration.
DIVAR IP systems are based on Windows Server 2008 R2 operating system.
This chapter is valid for DIVAR IP models that come with pre-installed hard drives. Empty units start into the DOM recovery menu on first start. The recovery process is described in the installation manual.
See also:
– *Recovering the unit, page 41*

5.1 Introduction

DIVAR IP systems are shipped with a pre-installed Configuration Wizard from factory.

5.2 Setup instruction

All DIVAR IP systems are preconfigured with a default IP address and with default iSCSI settings.
– IP Address: 192.168.0.200
– Subnet mask: 255.255.255.0
Observe the following:
– DIVAR IP needs to have an active network link during installation. Make sure that the network switch you are connecting to is powered on.
– The default IP address must not be occupied by any other device in the network. Make sure that the default IP addresses of existing DIVAR IP systems in the network are changed before adding another DIVAR IP.
– Determine whether the initial installation is on a DHCP network. If not then you must assign valid IP addresses to the video devices. Consult the local IT administrator to obtain a valid IP address range to be used with DIVAR IP and associated devices.
– The default iSCSI settings are optimized for use with Bosch VMS/VRM.

User with administrator rights:
– User: BVRAdmin
– Password: WSS4Bosch

Notice!
We strongly recommend not changing the user settings. Changing the user settings can result in malfunctioning of the system.

5.3 Starting the Application

DIVAR IP system is ready to go out of the box. The application provides a simple to install and intuitive to use solution for network surveillance systems.

To start the application:
1. Connect the unit and the cameras to the network.
2. Turn on the unit.
   The Windows Server 2008 R2 setup process starts.
3. Select the appropriate language for the installation, then click **Next**.
4. In the **Country or region**, **Time and currency** and **Keyboard layout** lists, click the appropriate item, then click **Next**.
   The Microsoft Software License Terms and the EULA (End User License Agreement) are displayed.
5. Accept the license terms, then click **Start**. Windows restarts.

6. After restart is finished, press CTR+ALT+DELETE. The Windows logon page is displayed.
7. Enter the default password **WSS4Bosch**.
8. After entering the password, a message is displayed that you must change the password before logging on the first time. To confirm, click **OK**.
9. Change the password.
   A series of scripts perform important setup tasks. This can take several minutes. Do not turn off the computer.
   The Bosch VMS default screen is displayed.
   Note: In case of password loss a system recovery must be performed as described in the installation manual. The configuration must be done from scratch or must be imported.
10. On the Bosch VMS default screen, double-click the **Bosch VMS Wizard** icon  to start the Configuration Wizard.
    The **Welcome** page is displayed.
11. Configure the system using the Configuration Wizard.

Notice!
If the IP addresses of devices that should be added don't fall within the same IP range as the DIVAR IP we recommend using the Bosch VMS Configuration Client. In all other cases use the Configuration Wizard.

Notice!
To perform administrative tasks, the BVRAdmin account can be entered when Bosch VMS default screen is displayed. To do so, press CTRL+ALT+DEL, then hold down SHIFT while clicking the **Switch User** option and keep SHIFT pressed for about five seconds.

Notice!
We strongly recommend not changing any operating system settings. Changing operating system settings can result in malfunctioning of the system.

See also:
- *Using Bosch VMS Config Wizard, page 22*
- *Using Bosch VMS Configuration Client, page 33*
- *Recovering the unit, page 41*

5.4 Using Bosch VMS Config Wizard

Intended use for Config Wizard is the quick and easy configuration of a smaller system. Config Wizard helps you to achieve a configured system including VRM, iSCSI system, cameras, recording profiles and user groups.
User groups and their permissions are configured automatically. You can add or remove users and set passwords.
Config Wizard can access Management Server only on the local computer.
You can save an activated configuration for backup purposes and import this configuration later. You can change this imported configuration after import.
Config Wizard adds the local VRM automatically.

Restrictions:
The following tasks cannot be done with the Configuration Wizard. Use Bosch VMS Configuration Client instead.
- adding additional license packages

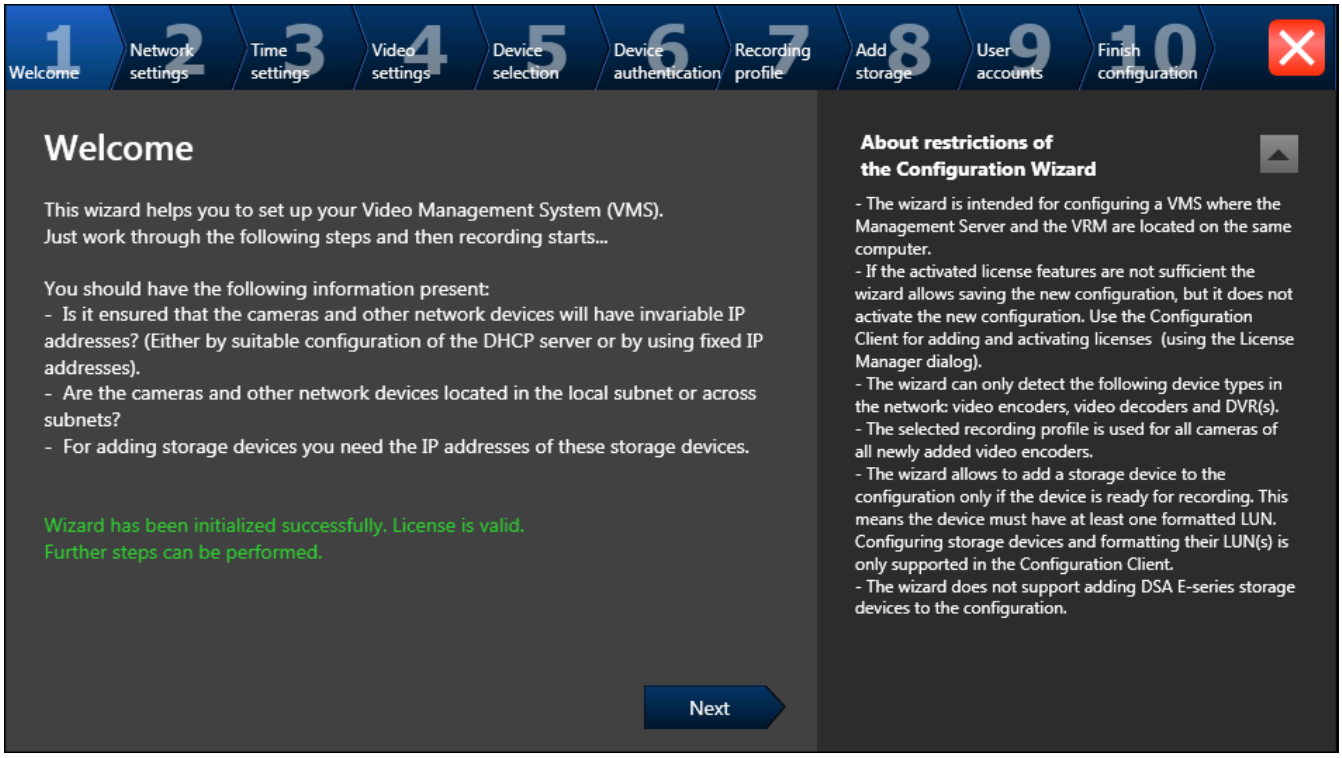
- adjusting schedules
- configuring systems with no or multiple VRM
- configuring external storage devices
- adding Video Streaming Gateway
- all advanced configurations beyond a basic setup (maps or alarms, for example)

For these tasks refer to the Bosch VMS manual (see*Additional documentation and client software, page 42*).

To achieve a quick configuration using the Configuration Wizard:

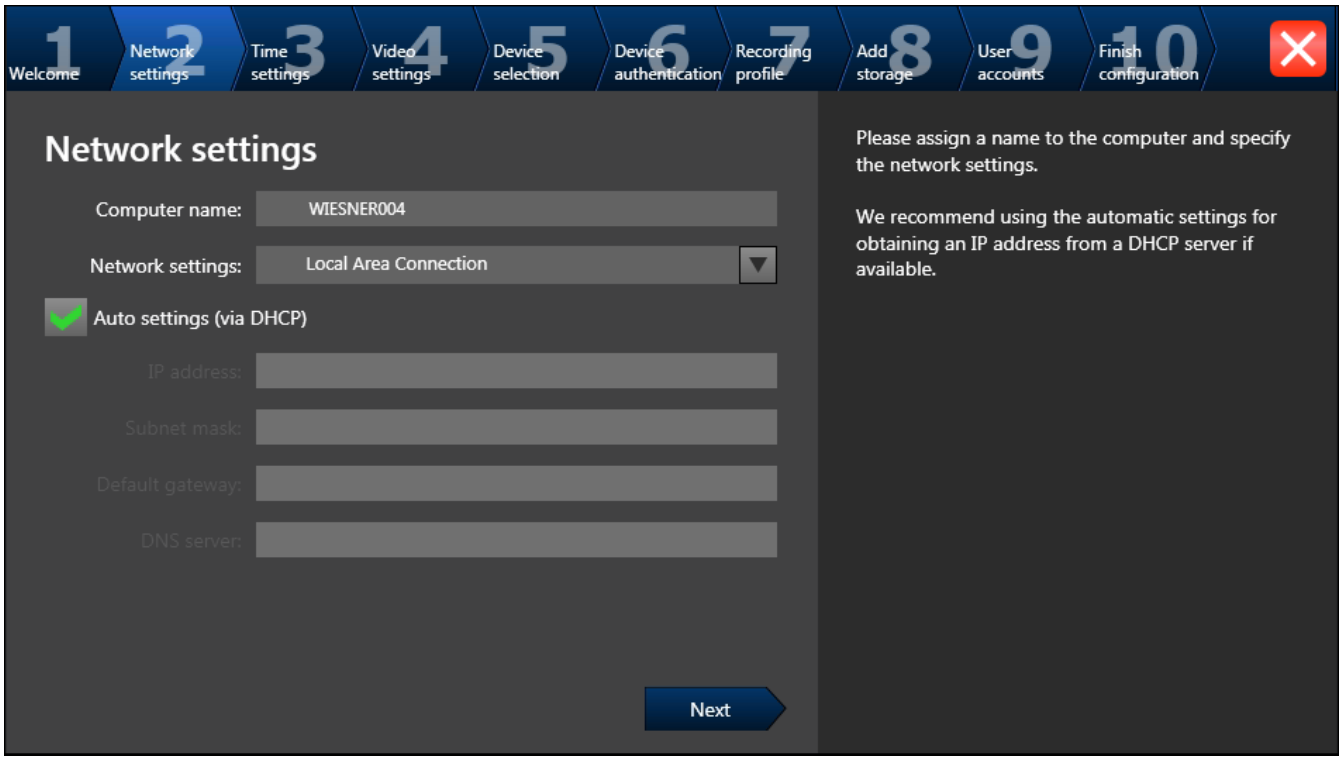
1. On the Bosch VMS default screen, double-click the **Bosch VMS Wizard** icon. The **Welcome** page is displayed.
2. Run-through the following pages of the wizard.

Welcome page



- Click **Next** button to continue.

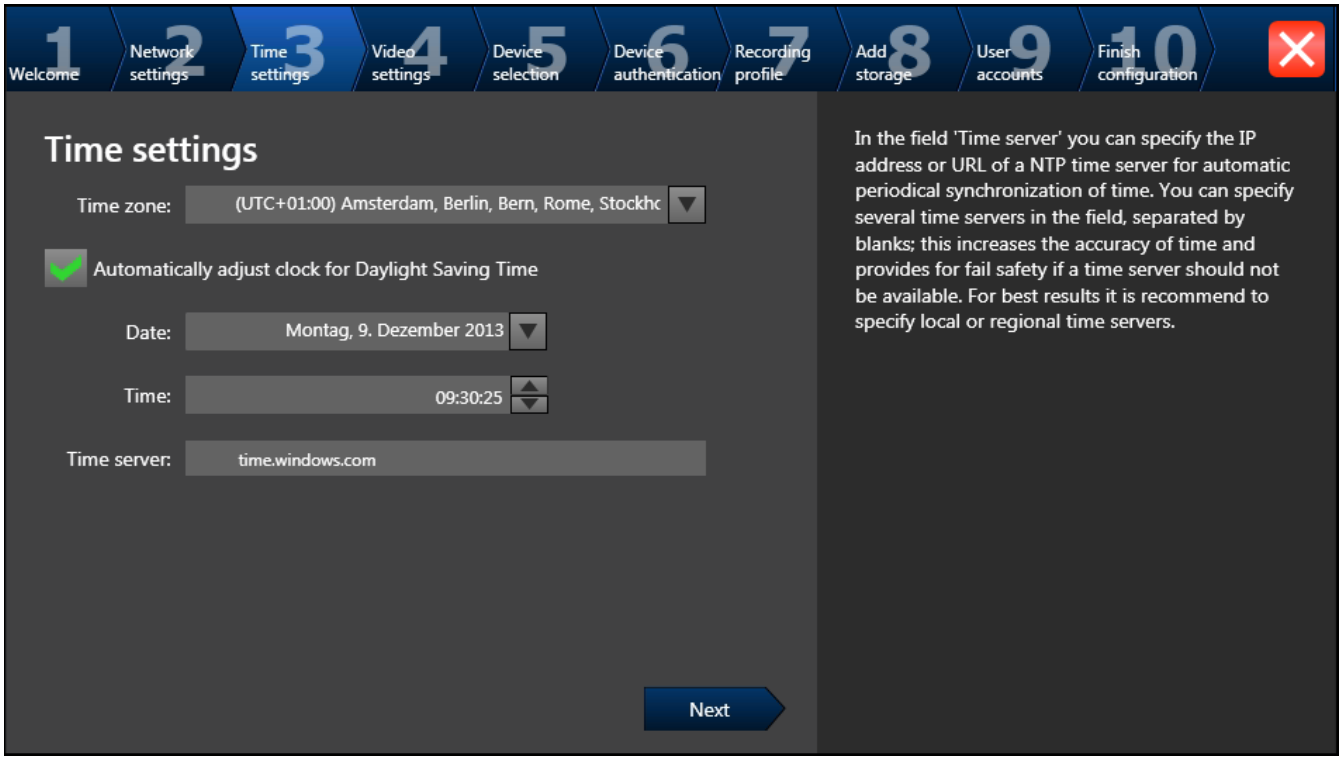
Network settings page



You configure the network settings of the operating system.
As soon as you click **Next** button, the settings are activated.
If you have changed any setting on this page, click **Reboot** to restart the system.

Notice!
If a DHCP server is employed in the network for the dynamic assignment of IP addresses, activate acceptance of IP addresses automatically assigned to the device.
Certain applications (VRM, Bosch Video Management System, Bosch Video Client, Configuration Manager) use the IP address for the unique assignment of the device. If using these applications, the DHCP server must support the fixed assignment between IP address and MAC address, and must be appropriately set up so that, once an IP address is assigned, it is retained each time the system is rebooted.

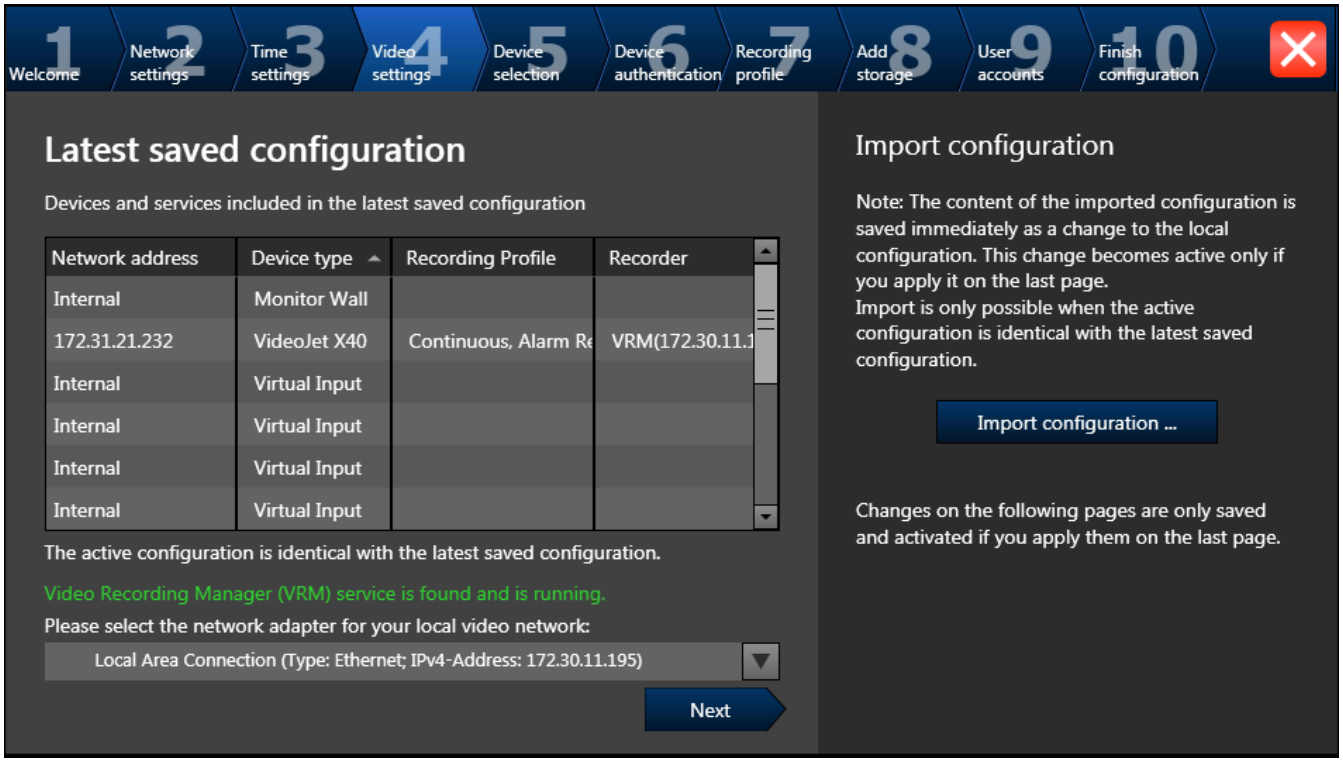
Time settings page



You configure the time settings of the operating system.

Note:
We highly recommend defining a time server in a video surveillance environment.

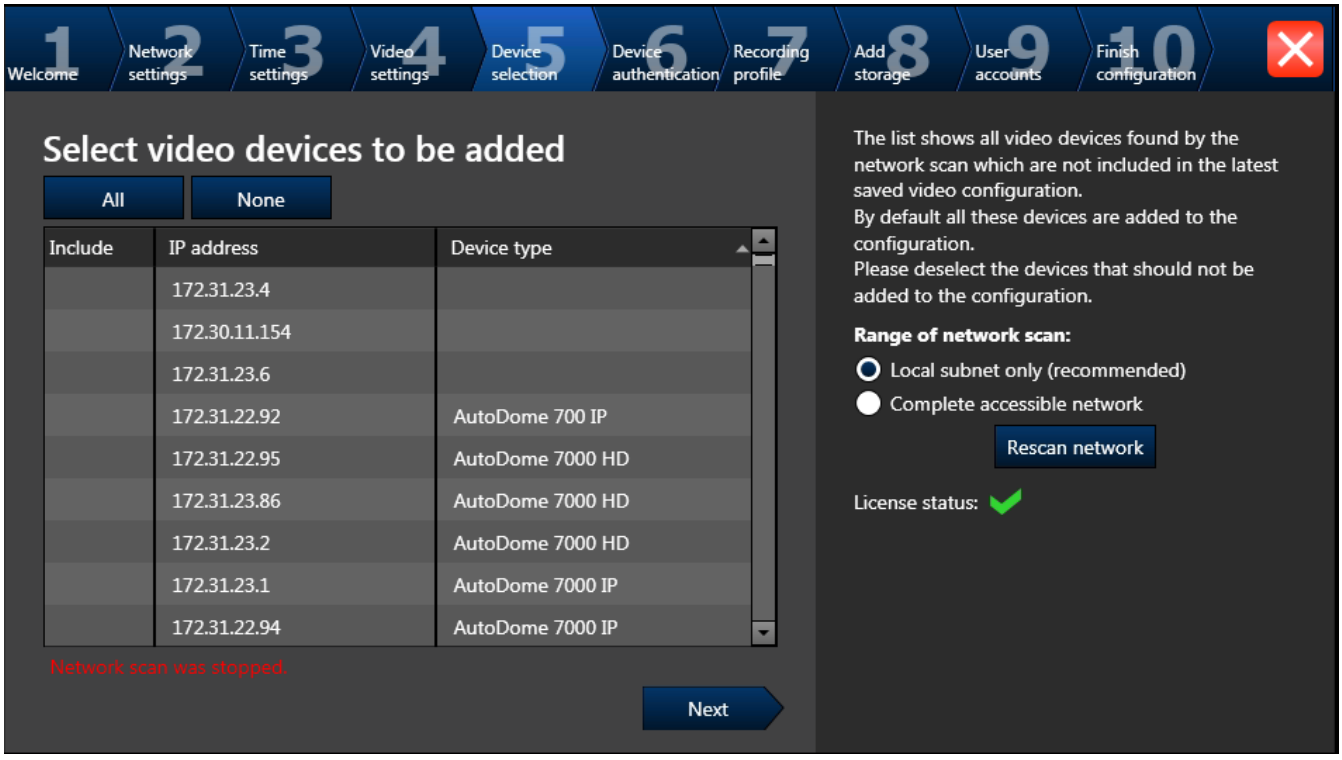
Video settings page



This page displays the devices and services that are included in the latest saved configuration. You can import a configuration.

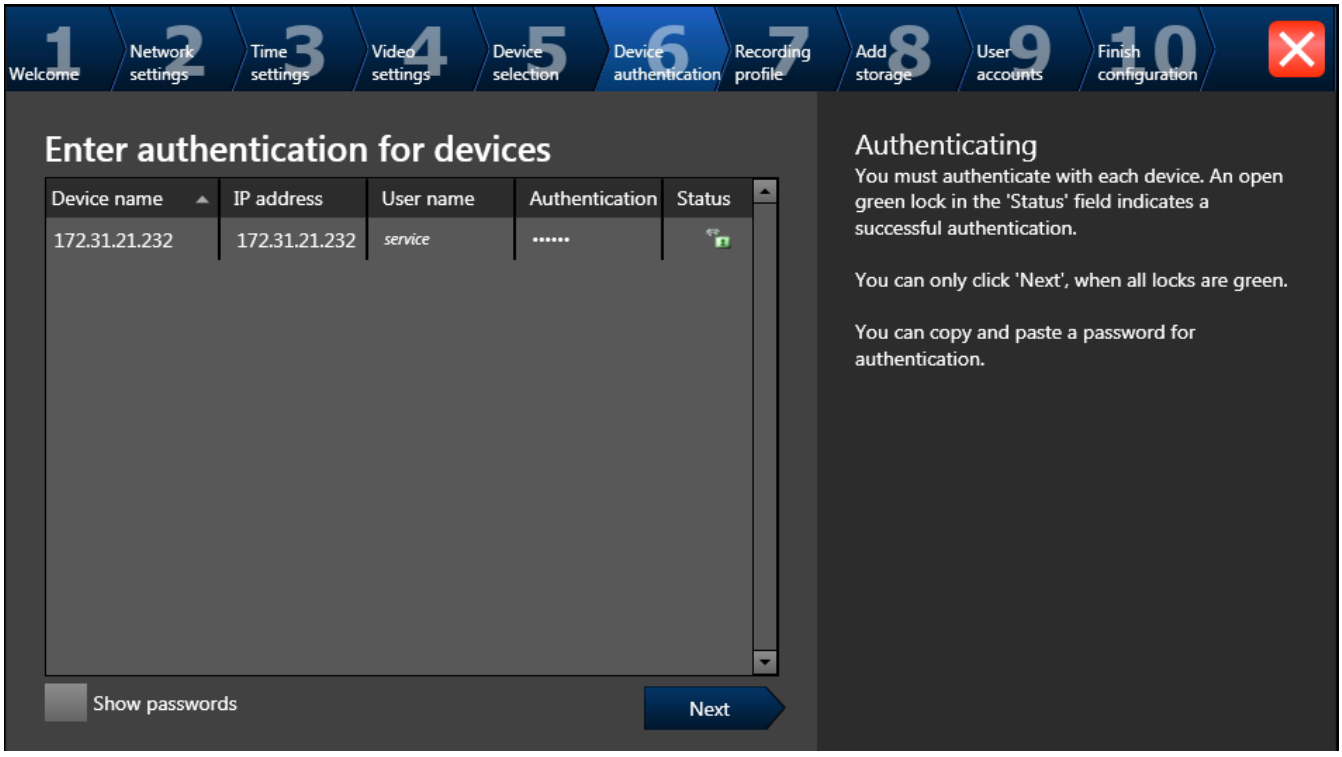
Note:
If the wizard fails in this step, close the wizard and start it again.

Device selection page



Note:
The scan for devices can take a time. You can cancel the scan. All devices that were already scanned, are displayed in the table.
This page displays all video devices that are not included in the latest saved configuration.
Deselect the devices that should not be added to the configuration, then click **Next**.

Device authentication page

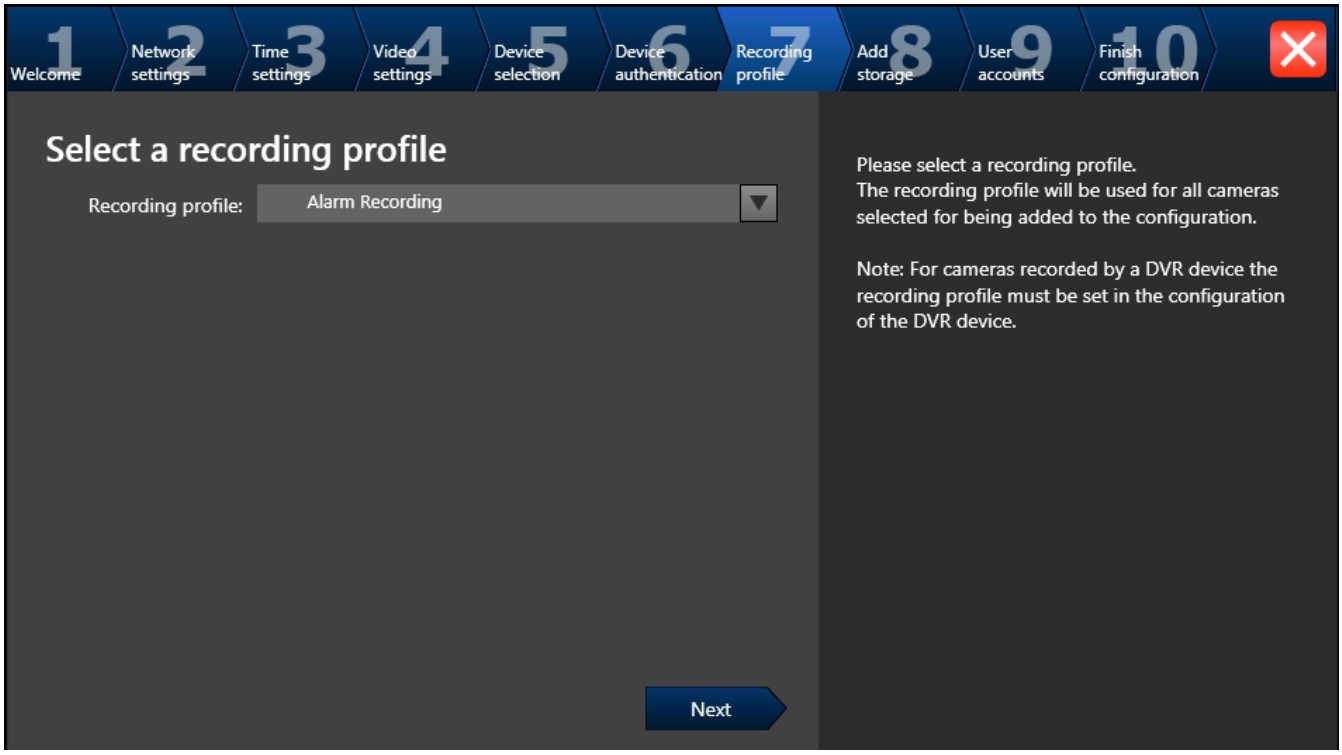


This page is used to authenticate at video devices protected by password. For easy authentication with the same password for multiple devices you can use the clipboard (CTRL +C, CTRL+V):

- Select a row with a successfully authenticated device (green lock is displayed), press CTRL+C, select multiple rows displaying a red lock and press CTRL+V).

Password check is performed automatically, when you do not enter a further character in the password field for a few seconds or you click outside the password field.

Recording profile page



For different profile assignments to different cameras you must execute Config Wizard multiple times.

Note:
Before selecting a recording profile observe the following:

– **Recording profile details**
All video devices use the default recording profile details.

Profile	Scheduled Time	Continuous	Pre-Alarm	Past alarm
Alarm Recording	Day/ Night/ Weekend	-	Normal Quality 10 Seconds	Good Quality 10 Seconds
Alarm Recording Night and Weekend	Night and Weekend	-	Normal Quality 10 Seconds	Good Quality 10 Seconds
Continuous , Alarm Recording	Day/ Night/ Weekend	Continuous Normal Quality	-	Good Quality 10 Seconds
Recording	Day/ Night/ Weekend	Continuous Normal Quality	-	-
Recording Night and Weekend	Night and Weekend	Continuous Normal Quality	-	-

To change these use the Bosch VMS Configuration Client.

– **Stream quality settings**
All video devices use the default settings for Stream 1 to record.

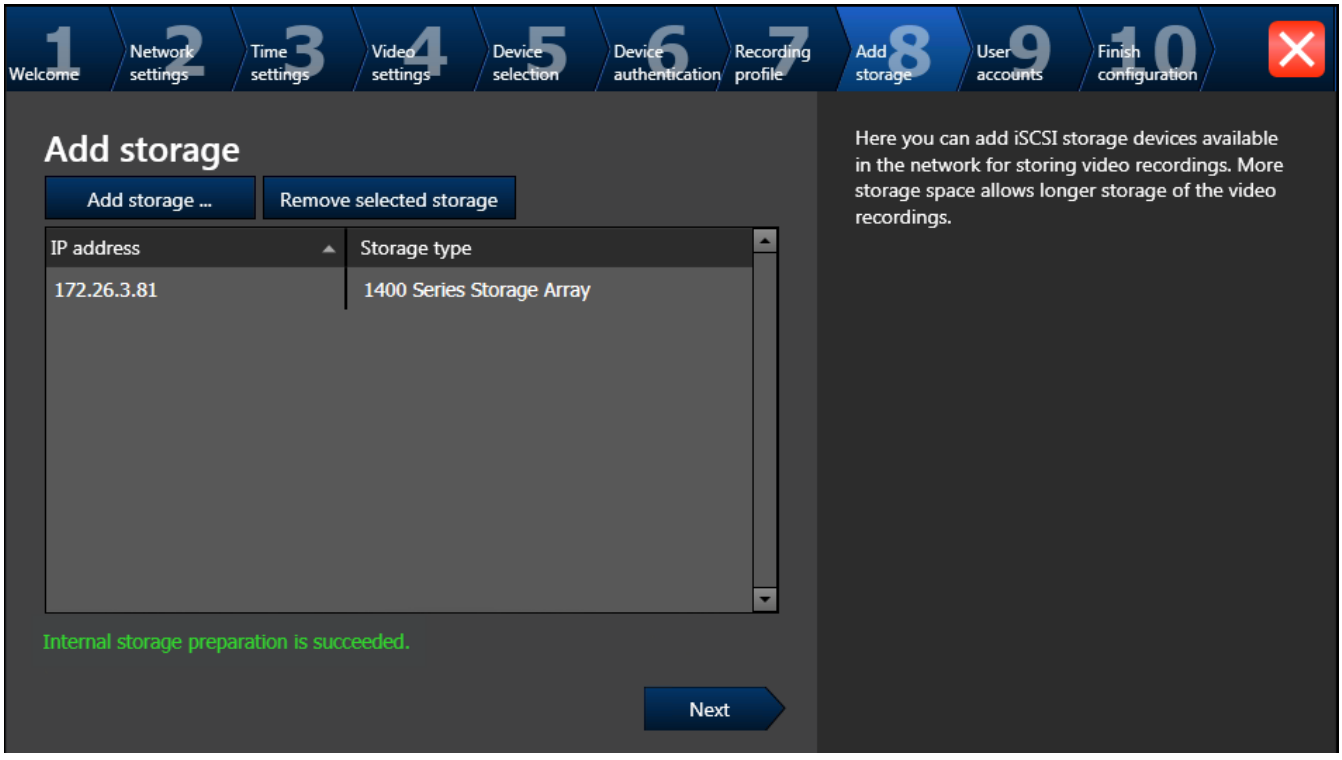
Name	SD Resolution	Frames per second(FPS)	Target Bit Rate	Maximum Bit Rate
Normal	CIF	7.5 IPS	512 Kbps	1024 Kbps
Good	2CIF	15 IPS	1024 Kbps	2048 Kbps
Excellent	4CIF	30 IPS	2048 Kbps	4096 Kbps
HD 720P	HD 720P	30 IPS	5000 Kbps	10000 Kbps
HD1080P	HD1080P	30 IPS	5000 Kbps	10000 Kbps

To change these use the Bosch VMS Configuration Client.

– **Schedule**

The default schedule is used for all recording profiles.
The Day schedule is active from 8 a.m. until 6 p.m., Monday through Friday.
The Night schedule is active from 6 p.m. until 8 a.m., Monday through Friday.
The Weekend schedule is active 24 hours a day for Saturday and Sunday.
To change the schedule use the Bosch VMS Configuration Client.

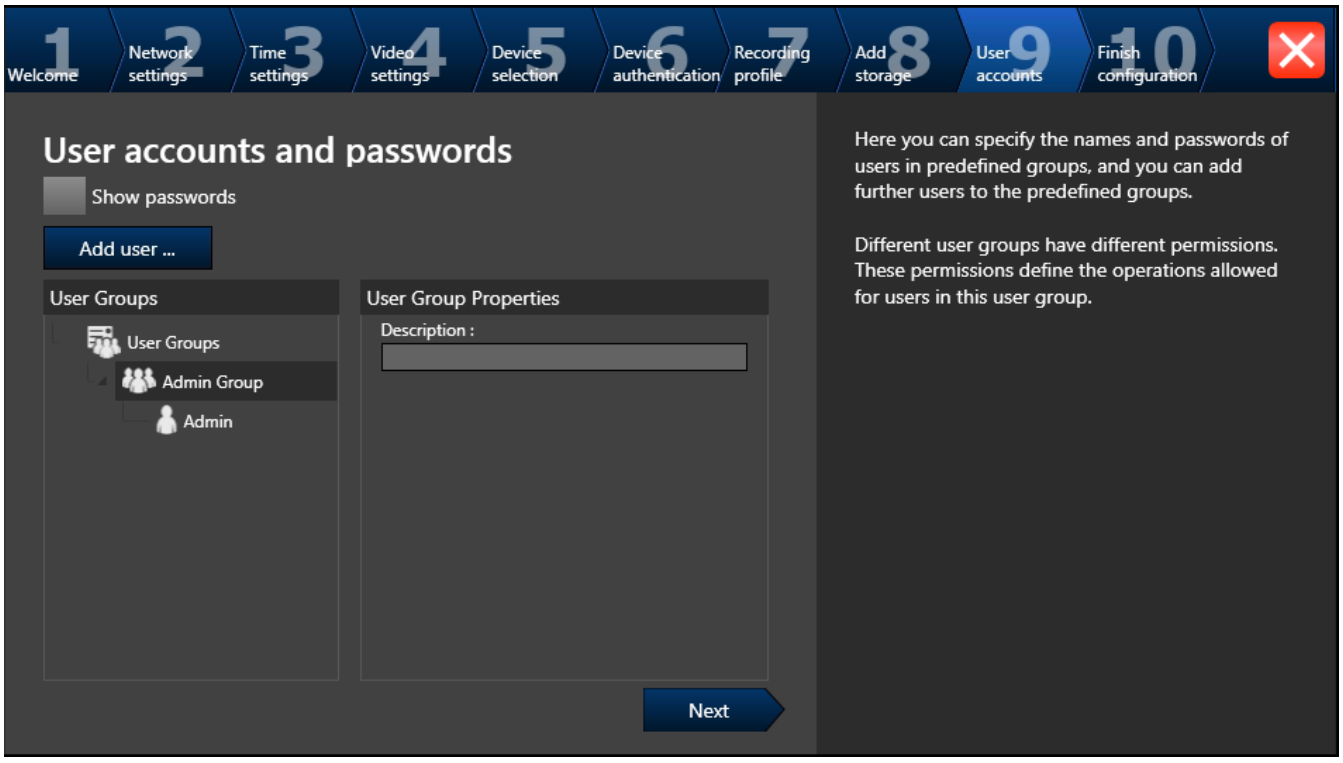
Add storage page



This page allows the addition of additional iSCSI storage devices
For limitations, refer to the datasheet available in the online catalog.

Notice!
If the wizard stops and the message appears, that the internal iSCSI storage is not ready for recording because the LUNs are not formatted, you must format the LUNs using Bosch VMS Configuration Client.
To format the LUNs, see Bosch VMS Configuration Manual, Chapter **Formatting a LUN**.

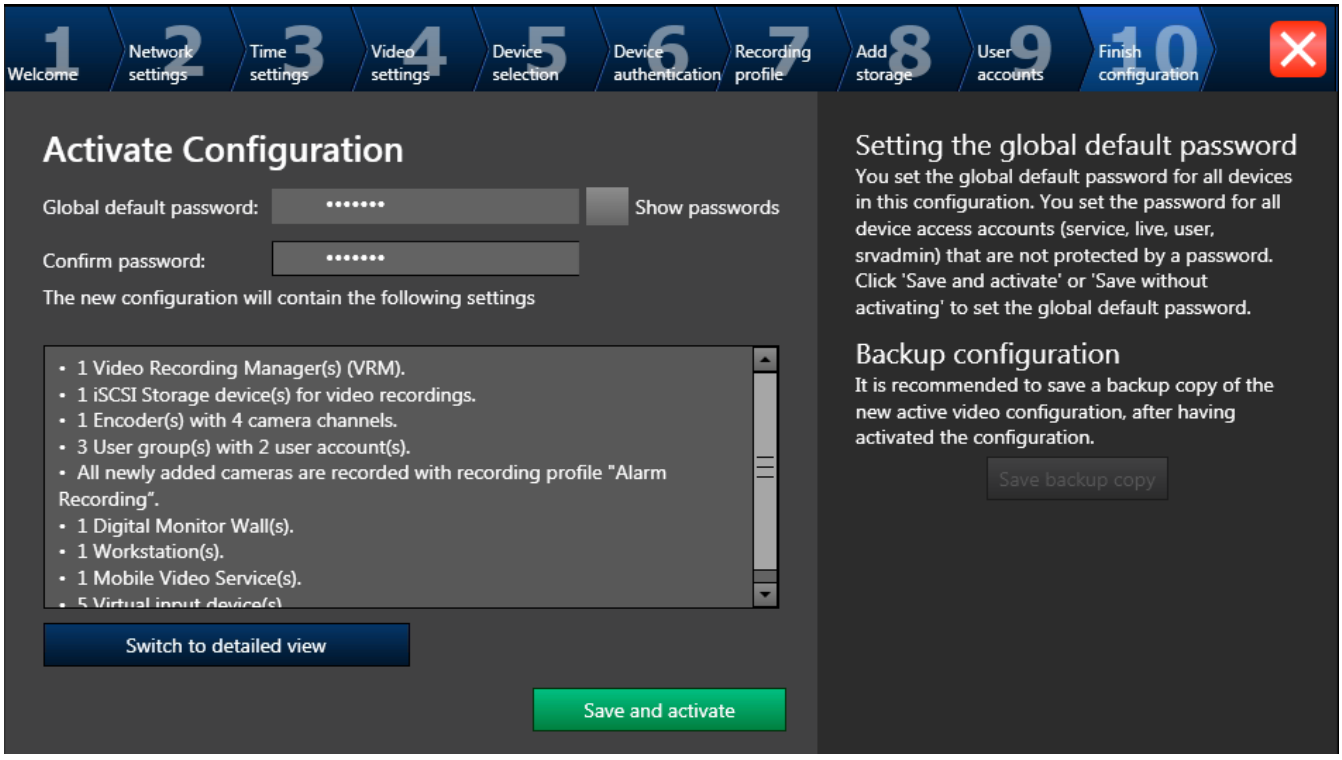
User accounts page



You can add users and passwords. Use Configuration Client to add user groups and to change permissions.

Notice!
We strongly recommend using password protection for all users defined in the system.

Finish configuration page



This page is used for providing a global default password for all devices that are not currently protected by a password.
After clicking **Save and activate** the configuration is activated.
After successful activation the **Activate Configuration** page is displayed again. Now you can store a backup of the configuration if desired: Click **Save backup copy**.

Notice!
We recommend saving the configuration after each change on an external storage media, for example, USB drive. After recovering the system you can import this backup copy.

5.5 Using Bosch VMS Configuration Client

5.5.1 Assigning device IP addresses

If the IP addresses of devices that should be added do not fall within the same IP range as the DIVAR IP, we recommend using the Bosch VMS Configuration Client.

To assign device IP addresses:

1. On the Bosch VMS default screen, double-click the Configuration Client icon to change device network settings. The application starts.
2. Enter the following, then click **OK**.
   User name: admin
   Password: no password required (if not set with the wizard)
   Connection: 127.0.0.1
3. On the **Hardware** menu, click **Initial Device Scan**.
   The application performs a network scan for all defaulted devices.
4. To assign all devices at once, click **Select All**, then right-click the selected devices, then click **SetIP Addresses**. The **Set IP Addresses** dialog box is displayed.

Note:
It is also possible to configure the devices individually with specific IP addresses based on MAC address.

5. Enter the starting IP address for the address range you want to use, click the **Calculate** tab, then click **OK**.
6. To restart the devices, click **OK**.
7. Close Configuration Client .

5.5.2 Adding additional licenses

You can add additional licenses using Configuration Client.

To activate the software:

1. Start Configuration Client.
2. On the **Tools** menu, click **License Manager...**.
   The **License Manager** dialog box is displayed.
3. Click to check the boxes for the software package, the features, and the expansions that you want to activate. For the expansions, enter the number of licenses.
   If you have received a Bundle Information file, click **Import Bundle Info** to import it.
4. Click **Activate**.
   The **License Activation** dialog box is displayed.
5. Write down the computer signature or copy and paste it into a text file.
6. On a computer with Internet access, enter the following URL into your browser:
   https://activation.boschsecurity.com
   If you do not have an account to access the Bosch License Activation Center, either create a new account (recommended) or click the link to activate a new license without logging on. If you create an account and log on before activating, the License Manager keeps track of your activations. You can then review this at any time.
   Follow the instructions to obtain the License Activation Key.
7. Return to the Bosch VMS software. In the **License Activation** dialog box, type the License Activation Key obtained from the License Manager and click **Activate**.
   The software package is activated.

5.6 Using Bosch VMS Operator Client

Use Bosch VMS Operator Client to verify the live, recording and playback functionality of DIVAR IP.

To verify live image functionality in the Operator Client

1. On the Bosch VMS default screen, double-click the Operator Client icon  . The application starts.
2. Enter the following and click **OK**.
   User name: admin
   Password: no password required (if not set with the wizard)
   Connection: 127.0.0.1
3. Click the live image icon. The Logical Tree with the cameras is displayed.
4. Select a camera and drag it to an image window. The image of the camera is displayed if the camera is assigned correctly.
   Note:
   Cameras in the image window with a red dot in the camera's icon are viewed live.

To verify recording functionality in the Operator Client

- Cameras in the Logical Tree with a red dot in the camera's icon are recording.

To verify playback functionality in the Operator Client

- The time line moves if the a camera is viewed in playback mode.

To perform further functionalities refer to the Bosch VMS manual.

Performance overview live

	4CIF		
	2.5 Mbit	**5 Mbit**	**10 Mbit**
Number of software monitors	20	13	9

	720p		
	2.5 Mbit	**5 Mbit**	**10 Mbit**
Number of software monitors	14	11	6

	1080p		
	2.5 Mbit	**5 Mbit**	**10 Mbit**
Number of software monitors	8	6	5

References to the manual are described in *Additional documentation and client software, page 42*.

6 Installing additional drives

After physical drive mounting has been performed, the following configurations must be performed for the drives to be accessible to both the operating system and Bosch Video Recording Manager (VRM).

- *Adding new drives to Windows Server, page 36*
- *Creating a VHD iSCSI target for VRM, page 36*
- *Adding and formatting the VHD as a VRM target, page 37*

See also:

- *Inserting hard disks, page 13*

6.1 Adding new drives to Windows Server

To add new drives to Windows server:

1. On the Bosch VMS default screen, press CTRL+ALT+DEL, then hold down SHIFT while clicking the **Switch User** option and keep SHIFT pressed for about five seconds.
   Note: To perform administrative tasks, the BVRAdmin account can be entered
2. In the taskbar, click **Server Manager**. The **Server Manager** window is displayed.
3. In the left pane, expand **Storage**, then click **Disk Management**.
   The added hard drisk appear as **Unallocated**.
4. Right-click the **Unallocated** disk, then click **New Simple Volume**.
   The **New Simple Volume Wizard** dialog box is displayed.
5. In the **Welcome** dialog box, click **Next**.
6. In the **Specify Volume Size** dialog box, allow all of the automatically allocated space and click **Next**.
7. In the **Assign Drive Letter or Path** dialog box, click **Assign the following drive letter**, enter the drive letter assigned to the new drive, then click **Next**.
8. In the **Format Partition** dialog box make sure the following settings are correct, then click **Next**.
   - **File system:** NTFS
   - **Allocation unit size:** Default
   - **Volume label:** New Volume
   - The **Perform a quick format** check box must be selected.
9. In the **Summary** dialog box, click **Finish**.
   The description of the new drive changes to **Healthy (Primary Partition)**.

6.2 Creating a VHD iSCSI target for VRM

To create a VHD iSCSI target for VRM:

1. On the Bosch VMS default screen, press CTRL+ALT+DEL, then hold down SHIFT while clicking the **Switch User** option and keep SHIFT pressed for about five seconds.
   Note: To perform administrative tasks, the BVRAdmin account can be entered
2. In the taskbar, expand **Microsoft iSCSI Software Target**, expand **iSCSI Targets**, then click the **TG0** icon.
   All existing virtual disks are displayed with their LUN numbers.
3. Right-click the **TG0** icon, then click **Create Virtual Disk for iSCSI Target**.
   The **Create Virtual Disk Wizard** dialog box is displayed.
4. I n the **Welcome** dialog box, click **Next**.
5. In the **File** dialog box, enter the path to the new virtual hard disks using the assigned drive letter of your newly installed drisks, then click **Next**.
   Note: The name you are creating must have the file extension *.VHD, for example **F:\VirtualDisk.vhd**.

6. In the **Size** dialog box, enter the size of the new virtual hard disks in the **Size of virtual disk (MB)** box, then click **Next**.
   Note:
   – If the total size of the new disk is displayed in gigabyte, multiply the value in the **Currently available free space** size by 1024.
   – If the total size of the new disk is displayed in terabyte, multiply the value in the **Currently available free space** by 1024 twice.
7. In the **Description** dialog box, enter the description of the new virtual disk, then click **Next**.
8. In the **Summary** dialog box, click **Finish**.
   In the right pane of the **Server Manager** window the new virtual disks are displayed.

6.3 Adding and formatting the VHD as a VRM target

To add and format the VHD as a VRM target:

1. On the Bosch VMS default screen, double-click the Configuration Client icon  to change device network settings. The application starts.
2. Enter the following, then click **OK**.
   User name: admin
   Password: no password required (if not set with the wizard)
   Connection: 127.0.0.1
3. In the Device Tree, expand **VRM Devices**, expand the VRM of the system, expand the configured **Pool**, expand the iSCSI of the system, then click the icon of the iSCSI target. The virtual disks are displayed with the state **unformatted**.
4. Select the **Format** check box.
5. Click the **Format LUN** tab, then click **OK** to format the selected LUNs.
   The formatting progress starts and when completed, the new disks will be displayed with the state **formatted**.
6. Close Configuration Client.

7 Connecting to the internet

This section describes the steps that are required to access the DIVAR IP system from the internet.

7.1 Protecting the system from unauthorized access

In order to protect the system from unauthorized access, we recommend that you follow strong password rules before connecting the system to the internet. The stronger your password, the more protected your system will be from unauthorized persons and malware.

7.2 Setting up port forwarding

In order to access a DIVAR IP system from the internet through a NAT/PAT capable router, port forwarding must be configured on the DIVAR IP system and on the router.

7.2.1 Setting up port forwarding in DIVAR IP

To set up port forwarding in DIVAR IP:

1. Make sure the system is fully configured with all devices.
2. On the Bosch VMS default screen, double-click the Configuration Client icon  . The application starts.
3. Enter the following, then click **OK**.
   User name: admin
   Password: no password required (if not already entered with the wizard)
   Connection: 127.0.0.1
4. On the **Settings** menu, click **Remote Access Settings**.
5. Select the **Enable Port Mapping** check box.
6. In the **Public network address** box, enter the static IP address your internet service provider assigned to you or alternatively enter a DNS name that is already configured in the dynamic DNS setting of your router.
7. In the **Private IP address** box, select the IP address.
8. Click **Show Port Forwarding**.
9. Save and activate the configuration.

7.2.2 Setting up port forwarding in the router

To set up port forwarding in the router (general):

1. The port forwarding rules shown on this page must be set at your internet router. For details, refer to the router manual.
2. Ignore the port forwarding entry that contains the IP address 127.0.0.1.
3. Set the following additional rule at your internet router instead:
4. **Private IP:** <IP address of DIVAR IP>
   Private Port: 443
   Public Port: 443

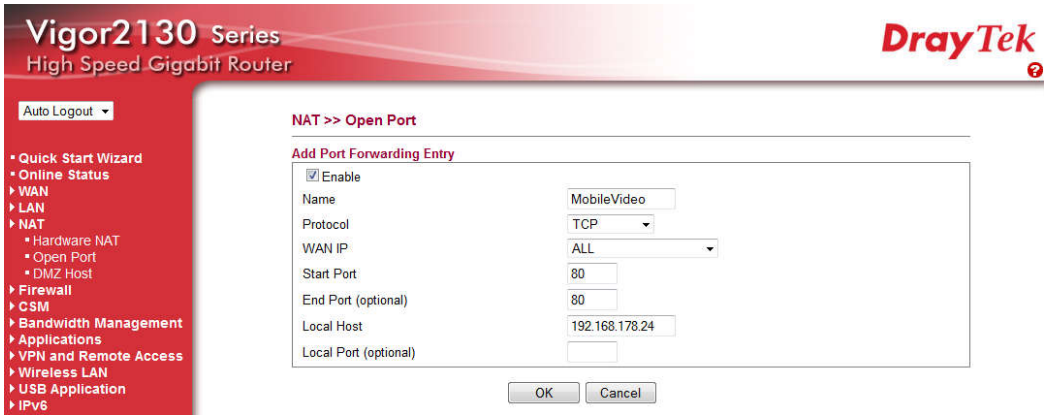
7.2.3 Example for port forwarding

The following example describes the port forwarding for a router of the VIGOR 2130 Series.

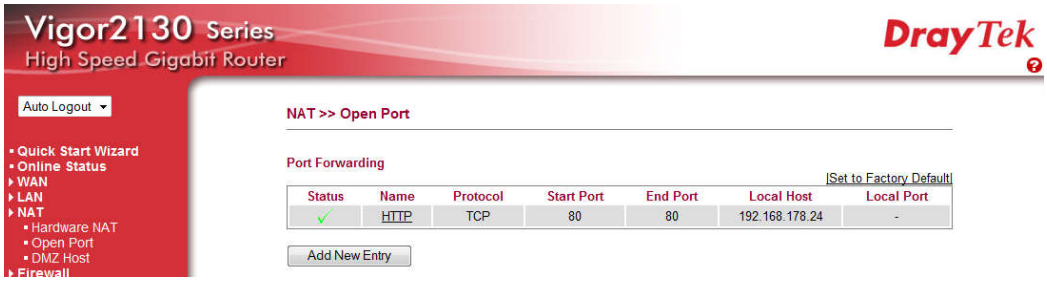
To configure port forwarding on the router:

1. Activate the port forwarding with the following steps:
   Enable the port forwarding.
   Enter a name for this port forwarding entry, for example **MobileVideo**.
   Select the protocol (**TCP**) and port to route to the Mobile Video Service computer.

In the **WAN IP** list, leave the default setting. This is router specific.
In the **Start Port** and **End Port (optional)** fields, enter **80** for unsecured access or **443** for secured access. Do not define a port range.
In the **Local Host** field, enter the static IP address or the local computer name, if you use DHCP.
In the **Local Port (optional)** field leave the default setting. It is router specific.



2. Click **OK**.
The following screenshot shows the results of your port forwarding settings.



3. Repeat this procedure for every entry of the port forwarding list shown in Configuration Client.
The DIVAR IP system can now be reached from the Internet.

7.3 Choosing an appropriate client

There are two supported clients that allow remote connections to a DIVAR IP system through the internet.

7.3.1 Remote connection with Operator Client

To make a remote connection with Bosch VMS Operator Client

1. Download the resource folder of the Bosch VMS installer using the following network share:
\\<IP address of DIVAR IP>\sources
2. Copy the **Setup** directory to the remote workstation that will be used for remote viewing.
3. In the **Setup** directory, right-click `setup.exe`, then click **Run as administrator** and accept the security message.
4. In the **Welcome** dialog box clear all check boxes except Operator Client.
5. Follow the installation process.
6. After finishing the installer successfully, start Operator Client using the desktop shortcut.

7. Enter the following, then click **OK**.
   User name: admin
   Password: enter user password
   Connection: enter public IP address or dynDNS name

7.3.2 Remote connection with Video Security App

To make a remote connection with Video Security App:

1. In Apple's App Store search for **Bosch Video Security**.
2. Install the Video Security app on your iOS device.
3. Start the Video Security app.
4. Select **Add**.
5. Enter the public IP address or dynDNS name (see Setting up port forwarding).
6. Make sure Secure Connection (SSL) is switched on.
7. Select **Add**.
8. Enter the following:
   User name: admin
   Password: enter user password

Notice!
Only use Bosch VMS Operator Client Video Security App in the version that matches DIVAR IP. Other clients or application software may work but are not supported.

7.4 Installing an Enterprise Management Server

For a central management of multiple systems you can install Bosch VMS Enterprise Management Server on a separate server.

To install Bosch VMS Enterprise Management Server on a separate server:

1. Download the resource folder of the Bosch VMS installer using the following network share:
   \\<IP address of DIVAR IP>\sources
2. Copy the **Setup** directory to the server that should act as an Enterprise Management Server.
3. In the **Setup** directory, right-click `setup.exe`, then click **Run as administrator** and accept the security message.
4. In the **Welcome** dialog box, clear all check boxes except **Enterprise Management Server** and **Configuration Client**.
5. Follow the installation instructions.
6. After finishing the installer successfully, start Configuration Client using the desktop shortcut.

Notice!
For Enterprise Management Server configuration refer to the Bosch VMS documentation.

8 Recovering the unit

Following procedure describes how to restore the factory default image.

To restore the unit to factory default image

1. Start the unit and press **F11** during the BIOS power-on-self-test.

Notice!

Make sure that a DVI monitor, a keyboard and a mouse are connected to the unit.

2. Select **SATA:4M-ATP Velocity MI SATA DO** in boot device menu.
   The Recovery menu is displayed.
3. Select one of the following:
   - **Initial Factory Setup (all data on the system will be lost)**
     (restores to factory default image and deletes all data on the HDDs)
     or
   - **System Recovery (back to Factory Defaults)**
     (restores to factory default image; data on the HDDs will not be deleted)

   Note:
   Windows performs the setup. The screen displays the percentage of the process.

Notice!

Do not turn off the unit during the process. This will damage the Recovery media.

4. The unit starts from the Recovery media. If the setup is successfull. press **Yes** to restart the system.
5. Windows performs the initial setup of the operating system. The unit restarts after Windows has completed the setup.
6. After the restart of the unit, the factory default settings are installed and the Windows logon screen is displayed.
   The factory default settings are:
   - IP address: 192.168.0.200
   - Subnet mask: 255.255.255.0
   - User: BVRAdmin
   - Password: WSS4Bosch

9 Additional documentation and client software

Documentation for Bosch Security System products can be found as follows:

- www.boschsecurity.com > select your region and your country > select **Product Catalog** > start a search for your product > select the product in the search results to show the existing documents.

And on the following network share:

- \\<IP address of DIVAR IP>\sources

10 Appendices

This chapter gives information for supporting and troubleshooting.

10.1 Motherboard

All graphics shown in this chapter were based upon the latest PCB Revision available at the time of publishing of the manual. The motherboard you've received can differ from the graphics shown in this chapter.

10.1.1 Motherboard layout

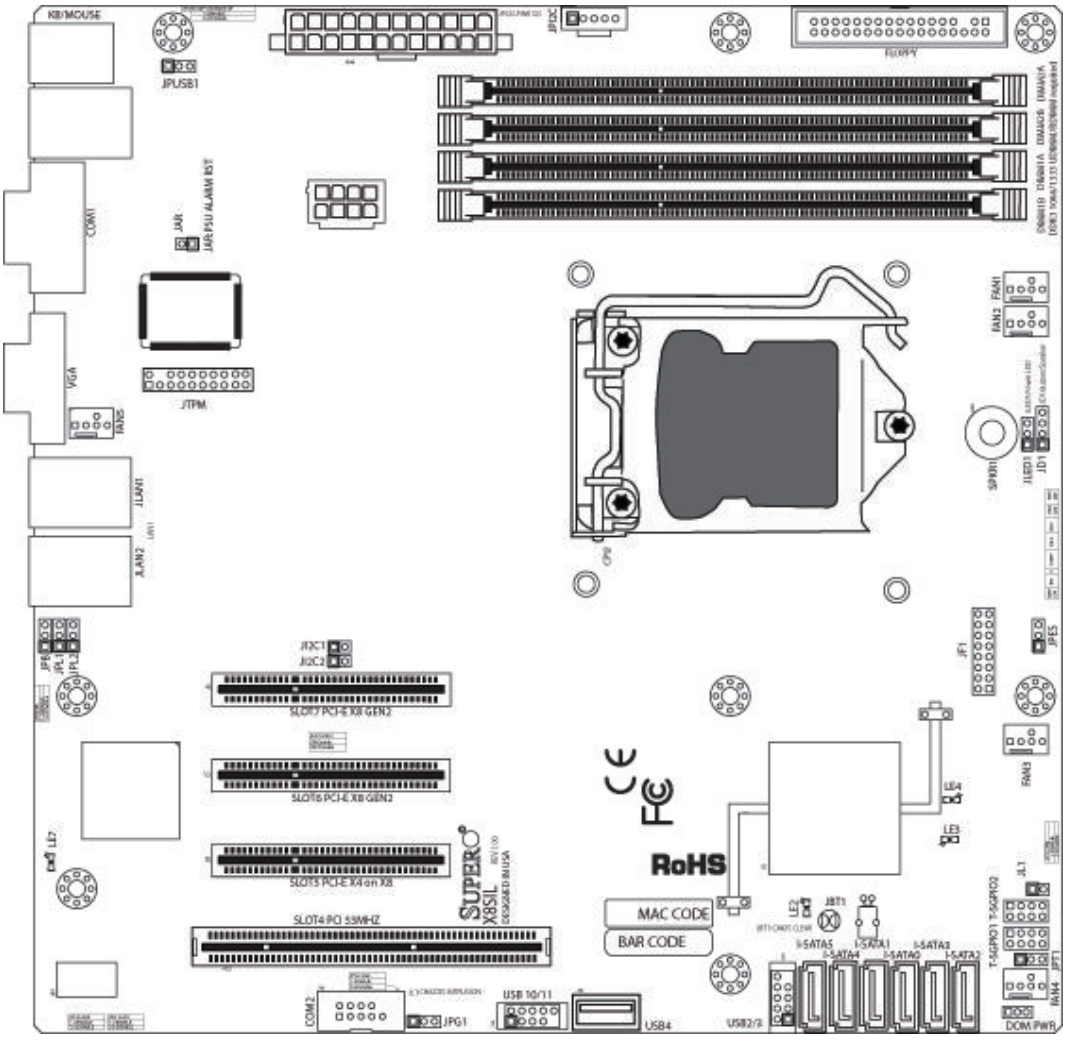


Figure 10.1: Motherboard layout

Important notes to the user:

- Jumpers not indicated are for testing only.
- When LE2 (Onboard Power LED Indicator) is on, system power is on. Unplug the power cable before installing or removing any components.
- All systems have a SATA DOM connected to Serial ATA ports (I-SATA-5) with a small power connector (DOM PWR).
- SATA-DOM: Is plugged in connector I-SATA-5 on the motherboard.

10.1.2 Motherboard component overview

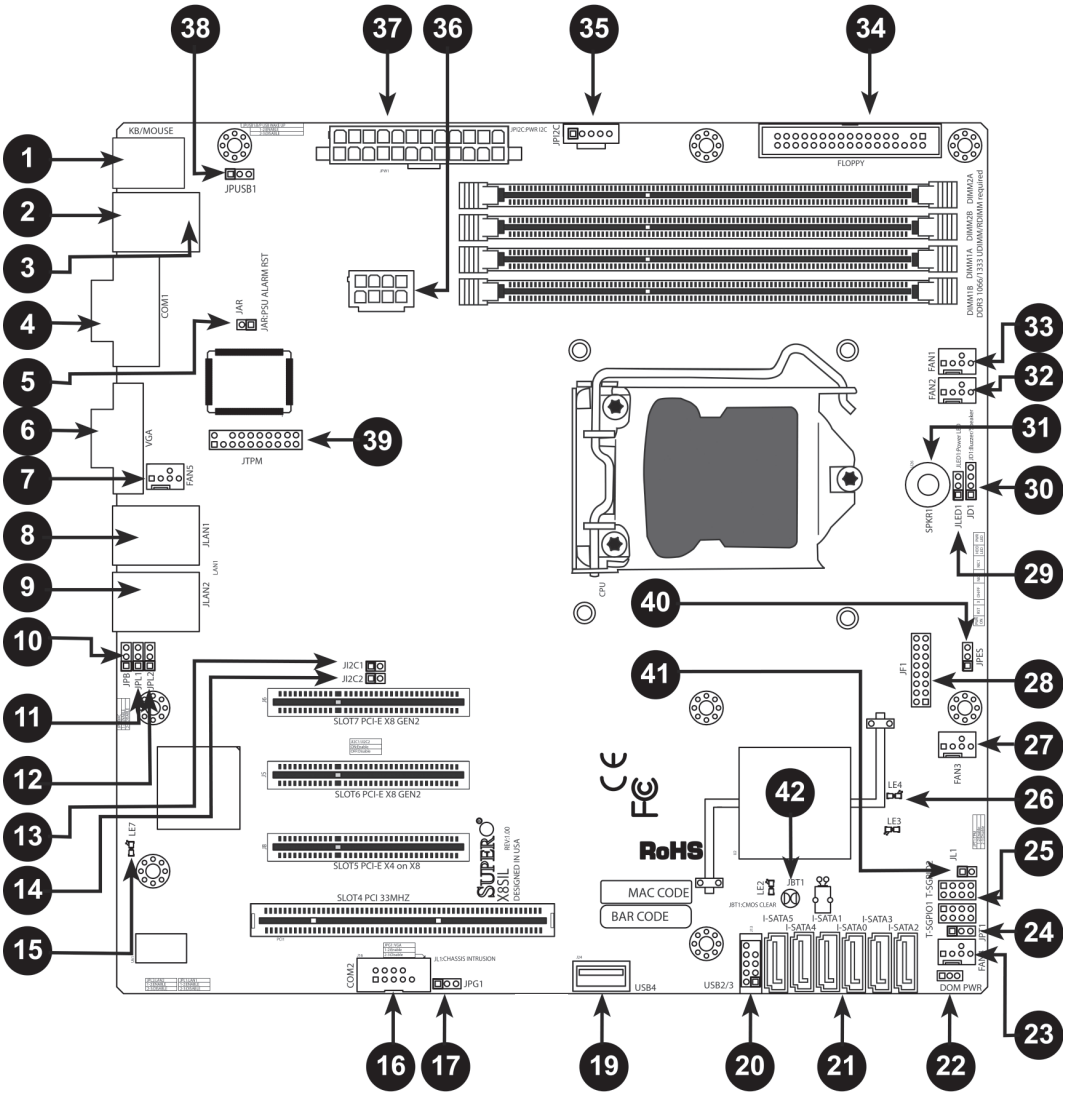


Figure 10.2: Motherboard – component overview

X8SIL/X8SIL-F/X8SIL-V jumpers

Number	Jumper	Description	Default
38	JPUSB1	BP USB0/1 Wake-up	Pins 1-2 (Enabled)
42	JBT1	CMOS Clear	
40	JPES	Energy Saving Feature	Pins 2-3 (Disabled)
13,14	JI2C1/JI2C2	SMB to PCI Slots	
17	JPG1	Onboard VGA Enable	Pins 1-2 (Enabled)
11,12	JPL1/JPL2	LAN1/LAN2 Enable	Pins 1-2 (Enabled)
24	JPT1	TPM Enable	Pins 1-2 (Enabled)
10	JPB	BMC Jumper	Pins 1-2 (Enabled)

X8SIL/X8SIL-F/X8SIL-V headers/connectors

Number	Connector	Description
4,16	COM1/COM2	COM1/2 Serial connection headers
33,32,27,23,7	Fans 1~5	System/CPU fan headers
34	Floppy	Floppy Disk Drive connector
5	JAR	Alarm Reset
30	JD1	Speaker header (Pins 3/4: Internal, 1~4:External)
28	JF1	Front Panel Control header
41	JL1	Chassis Intrusion header
29	JLED	Power LED Indicator header
37	JPW1	24-pin ATX main power connector (required)
36	JPW2	+12V 8-pin CPU power connector (required)
1	KB/Mouse	Keyboard/mouse connectors
8,9	LAN1~LAN2,	Gigabit Ethernet (RJ45) ports (LAN1/LAN2)
21	I-SATA 0~5	Serial ATA ports (X8SIL has 4 Serial ATA Ports)
2	IPMI	IPMI LAN Port (X8SIL-F Only)
35	JPI2C	PWR supply (I2C) System Management Bus
31	SPKR1	Internal speaker/buzzer
25	T-SGPIO-0/1	Serial General Purpose IO headers (for SATA)
3,20	USB0/1	Backplane USB 0/1
19	USB 4	Type A USB Connector
18	USB 10/11	Front Panel USB header (X8SIL-F Only)
22	DOM PWR	Disk-On-Module (DOM) Power Connector
39	JTPM	Trusted Platform Module (TPM) Header
6	VGA	Onboard Video Port

X8SIL/X8SIL-F/X8SIL-V LED indicators

Number	LED	Description	Color/State	Status
26	LE4	Onboard Standby PWR LED Indicator	Green: Solid on	PWR On
15	LE7	IPMI Heartbeat LED (X8SIL-F Only)	Yellow: Blinking	IPMI: Normal

10.1.3 Motherboard features

CPU	Single Intel Xeon 3400 series processor in an LGA1156 socket.	
Memory	Four (4) 240-pin, DDR3 SDRAM DIMM sockets with support for up to 16GB of UDIMM or up to 32GB of RDIMM memory (ECC/ DDR3 1333/1066/800 MHz memory only.)	
	Supports dual-channel memory bus	
	DIMM sizes	
	UDIMM	1 GB, 2 GB, and 4GB
	RDIMM	1 GB, 2GB, 4GB, and 8GB
Chipset	Intel 3420 Chipset (X8SIL-F/X8SIL-V)	
	Intel 3400 Chipset (X8SIL)	
Expansion Slots	Two (2) PCI Express 2.0 (x8) slot	
	One (1) PCI Express x4 (x8) slot	
	One (1) 32-bit PCI 33MHz slot	
Integrated Graphics	Matrox G200eW	
Network Connections	Two Intel 82574L Gigabit (10/100/1000 Mb/s) Ethernet Controllers for LAN 1 and LAN 2 ports.	
	Two (2) RJ-45 Rear IO Panel Connectors with Link and Activity LEDs	
	Single Realtek RTL8201N PHY to support IPMI 2.0 (X8SIL-F Only)	
I/O Devices	SATA Connections (X8SIL-F/X8SIL-V Only)	
	SATA Ports	Six (6)
	RAID (Windows)	RAID 0, 1, 5, 10
	RAID (Linux)	RAID 0, 1, 10
	SATA Connections (X8SIL Only)	
	SATA Ports	Four (4)
	Integrated IPMI 2.0 (X8SIL-F Only)	
	IPMI 2.0 supported by the WPCM450 Server BMC	
	Floppy Disk Drive	
	One (1) floppy drive interface (up to 1.44 MB)	
	USB Devices (X8SIL Only)	
	Two (2) USB ports on the rear IO panel	
	One (1) Type A internal connector	
I/O Devices (Continued)	USB Devices (X8SIL-F/X8SIL-V Only)	

	Two (2) USB ports on the rear IO panel
	Four (4) USB header connectors for front access
	One (1) Type A internal connector
	Keyboard/Mouse
	PS/2 Keyboard/Mouse ports on the I/O backplane
	Serial (COM) Ports
	Two (2) Fast UART 16550 Connections: one 9-pin RS-232 port and one header
	Super I/O
	Winbond Super I/O 83627DHG-P
BIOS	32 Mb SPI AMI BIOS SM Flash BIOS
	DMI 2.3, PCI 2.3, ACPI 1.0/2.0/3.0, USB Keyboard and SMBIOS 2.5
Power Configuration	ACPI/ACPM Power Management
	Main switch override mechanism
	Keyboard Wake-up from Soft-Off
	Internal/External moder ring-on
	Power-on mode for AC power recovery
PC Health Monitoring	CPU Monitoring
	Onboard voltage monitors for CPU core, +3.3V, +5V, +/-12V, +3.3V Stdby, +5V Stdby, VBAT, HT, Memory, Chipset
	CPU 3-Phase switching voltage regulator
	CPU/System overheat LED and control
	CPU Thermal Trip support
	Thermal Monitor 2 (TM2) support
	Fan Control
	Fan status monitoring with firmware 4-pin (Pulse Width Modulation) fan speed control
	Low noise fan speed control
System Management	PECI (Platform Environment Configuration Interface) 2.0 support
	System resource alert via Supero Doctor III
	SuperoDoctor III, Watch Dog, NMI
	Chassis Intrusion Header and Detection
CD Utilities	BIOS flash upgrade utility

	Drivers and software for Intel 3400/3420 chipset utilities
Other	ROHS 6/6 (Full Compliance, Lead Free)
Dimensions	Micro ATX form factor, 9.6" x 9.6"

10.1.4 Block diagram

The following graphic shows the block diagram of the motherboard.

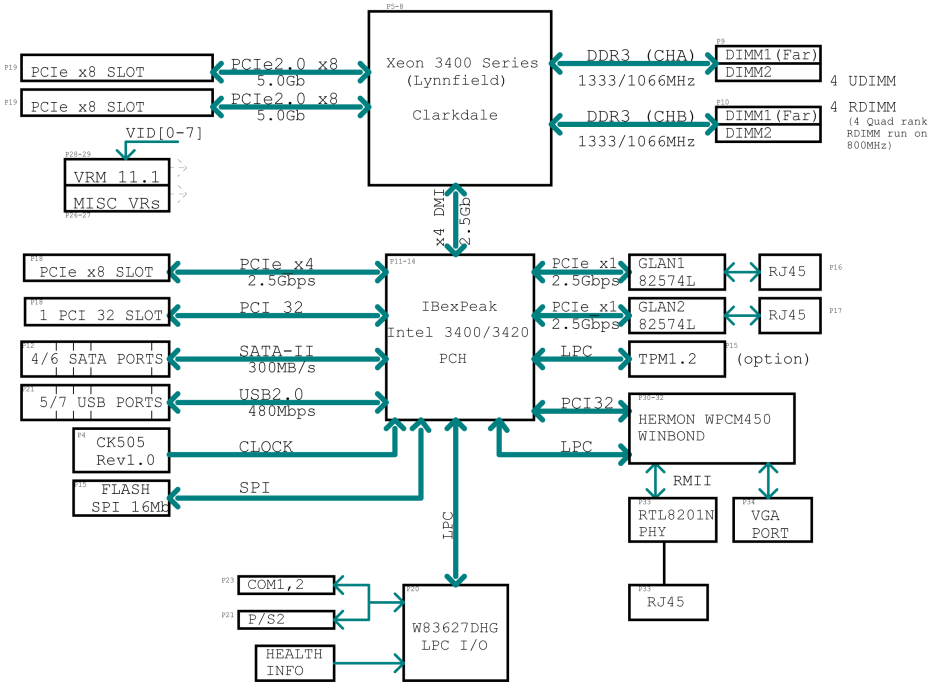


Figure 10.3: Block diagram

Notice!

This is a general block diagram and may not exactly represent the features on your motherboard. See the Motherboard Features pages for the actual specifications of each motherboard.

10.2 Chipset overview

The X8SIL/X8SIL-F/X8SIL-V supports the Intel Xeon 3400 processor series. Built upon the functionality and the capability of the single-chip Intel 3400 chipset, the X8SIL/X8SIL-F/X8SIL-V motherboard provides the performance and feature set required for single-processor-based systems with configuration options optimized for entry-level server platforms.The high-speed Direct Media Interface (DMI) featured in the Intel 3400/3420 chipset enables the X8SIL/X8SIL-F/X8SIL-V motherboard to offer a high-speed Direct Media Interface (DMI) for chip-to-chip true isochronous communication with the processor. This feature allows the X8SIL/X8SIL-F/X8SIL-V to achieve up to 10 Gb/s of software-transparent data transfer on each direction, achieving

better performance than comparable systems. The X8SIL/X8SIL-F/X8SIL-V also features a TCO timer (to enable the system to recover from a software/hardware lock), ECC Error Reporting, Function Disable and Intruder Detect.

Intel 3400/3420 chipset features

- Direct Media Interface (up 10 Gb/s transfer, Full Duplex)
- Intel Matrix Storage Technology and Intel Rapid Storage Technology
- Dual NAND Interface
- Intel I/O Virtualization (VT-d) Support
- Intel Trusted Execution Technology Support
- PCI Express 2.0 Interface (up to 5.0 GT/s)
- SATA Controller (up to 3G/s)
- Advanced Host Controller Interface (AHCI)

10.3 PC health monitoring

This section describes the PC health monitoring features of the X8SIL/X8SIL-F/X8SIL-V. These features are supported by an onboard System Hardware Monitor chip.

Recovery from AC power loss

BIOS provides a setting for you to determine how the system will respond when AC power is lost and then restored to the system. You can choose for the system to remain powered off (in which case you must hit the power switch to turn it back on) or for it to automatically return to a power on state. The default setting is Last State.

Onboard voltage monitoring

The onboard voltage monitor will scan the following voltages continuously: CPU core, +3.3V, +5V, +/-12V, +3.3V Stdby, +5V Stdby, VBAT, HT, Memory, Chipset. Once a voltage becomes unstable, it will give a warning or send an error message to the screen. Users can adjust the voltage thresholds to define the sensitivity of the voltage monitor by using SD III.

Fan status monitor with software

PC health monitoring can check the RPM status of the cooling fans via Supero Doctor III.

CPU overheat LED and control

This feature is available when the user enables the CPU overheat warning feature in the BIOS. This allows the user to define an overheat temperature. When this temperature reaches this pre-defined overheat threshold, the CPU thermal trip feature will be activated and it will send a signal to the buzzer and, at the same time, the CPU speed will be decreased.

10.4 Power configuration settings

This section describes the features of your motherboard that deal with power and power settings.

Slow blinking LED for suspend-state indicator

When the CPU goes into a suspend state, the chassis power LED will start blinking to indicate that the CPU is in the suspend mode. When the user presses any key, the CPU will wake-up and the LED indicator will automatically stop blinking and remain on.

BIOS support for USB keyboard

If the USB keyboard is the only keyboard in the system, it will function like a normal keyboard during system boot-up.

Main switch override mechanism

When an ATX power supply is used, the power button can function as a system suspend button. When the user presses the power button, the system will enter a SoftOff state. The monitor will be suspended and the hard drive will spin down. Pressing the power button again to wake-up the whole system. During the SoftOff state, the ATX power supply provides power

the system to keep the required circuitry "alive". In case the system malfunctions and you want to turn off the power, just press and hold the power button for 4 seconds. The power will turn off and no power will be provided to the motherboard.

10.5 Power supply

A stable power source is necessary for proper and reliable operation. It is even more important for processors that have high CPU clock rates of 1 GHz and faster.
The X8SIL/X8SIL-F/X8SIL-V accommodates ATX12V standard power supplies. Although most power supplies generally meet the specifications required by the CPU, some are inadequate. A 2-Amp of current supply on a 5V Standby rail is strongly recommended.
It is strongly recommended that you use a high quality power supply that meets ATX12V standard power supply Specification 1.1 or later. It is also required that the 12V 8-pin power connection (JPW2) be used for adequate power supply. In areas where noisy power transmission is present, you may choose to install a line filter to shield the computer from noise. It is recommended that you also install a power surge protector to help avoid problems caused by power surges.
DIVAR IP 7000 1U does not have a function to determine pre-failure of a power supply. The power supply will have the LED to show it is “OK” or “failed” by showing the color green or amber for the respective status. When the power supply fails, it shows amber, when it is functioning correctly it shows green.

10.6 Super I/O

The disk drive adapter functions of the Super I/O chip include a floppy disk drive controller that is compatible with industry standard 82077/765, a data separator, write pre-compensation circuitry, decode logic, data rate selection, a clock generator, drive interface control logic and interrupt and DMA logic. The wide range of functions integrated onto the Super I/O greatly reduces the number of components required for interfacing with floppy disk drives. The Super I/O supports two 360 K, 720 K, 1.2 M, 1.44 M or 2.88 M disk drives and data transfer rates of 250 Kb/s, 500 Kb/s or 1 Mb/s.
It also provides two high-speed, 16550-compatible serial communication ports (UARTs). Each UART includes a 16-byte send/receive FIFO, a programmable baud rate generator, complete modem control capability and a processor interrupt system. Both UARTs provide legacy speed with baud rate of up to 115.2 Kbps as well as an advanced speed with baud rates of 250 K, 500 K, or 1 Mb/s, which support higher speed modems.
The Super I/O provides functions that comply with ACPI (Advanced Configuration and Power Interface), which includes support of legacy and ACPI power management through a SMI or SCI function pin. It also features auto power management to reduce power consumption.

10.7 iSCSI support

The X8SIL/X8SIL-F/X8SIL-V motherboard supports the iSCSI Internet Protocol. iSCSI is an IP networking standard used to link and manage data storage, and transfer data across the internet and private intranets through long distance. iSCSI can be used to transmit data over local area networks (LANs), wide area networks (WANs), or the Internet. It can enable location-independent data storage and retrieval.
iSCSI allow clients to issue SCSI commands to remote SCSI storage devices and allow data centers to consolidate remote storage devices into storage arrays, giving an illusion of locally-attached disks to host servers. Unlike fiber-optic networks that require special cabling, iSCSI can run over long distance using existing networks.

For the X8SIL/X8SIL-F/X8SIL-V motherboard, iSCSI is supported on LAN 1. This can be enabled through the BIOS: Advanced => PCI/PnP Configuration => Onboard LAN1 Option ROM Select.

10.8 Overview of the Nuvoton BMC controller

The Nuvoton WPCM150 is a combined Baseboard Management Controller and 2D/VGA-compatible Graphics Core with PCI interface, Virtual Media and Keyboard, and a Keyboard/Video/Mouse Redirection (KVMR) module.
The WPCM150 interfaces with the host system via a PCI interface to communicate with the Graphics core. It supports USB 2.0 and 1.1 for remote keyboard/mouse/virtual media emulation. It also provides an LPC interface to control Super I/O functions and connects to the network via an external Ethernet PHY module or shared NCSI connections.
The Nuvoton BMC communicates with onboard components via six SMBus interfaces, fan control, Platform Environment Control Interface (PECI) buses, and General Purpose I/O (T-SGPIO) ports.
It also includes the following features:

– One X-Bus parallel interface for expansion I/O connections
– Three ADC inputs, Analog and Digital Video outputs
– Two serial for boundary scan and debug

There are two different versions of the Nuvoton BMC chip that are used in this product series. The Nuvoton WPCM150 (Manufacturer P/N WPCM150GA0BX5) which includes all of the features above, is the chip installed in the X8SIL motherboard. Another version, the Nuvoton WPCM450 (Manufacturer P/N WPCM450RA0BX) also has all the features as described above plus IPMI 2.0 support. This particular chip is installed in the X8SIL-F and X8SIL-V models. However, IPMI is supported only on the X8SIL-F motherboard.

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com