bosch video recorder 400 series manual

File Name: bosch video recorder 400 series manual.pdf
Size: 4815 KB
Type: PDF, ePub, eBook
Category: Book
Uploaded: 1 May 2019, 12:22 PM
Rating: 4.6/5 from 776 votes.

Status: AVAILABLE

Last checked: 3 Minutes ago!

In order to read or download bosch video recorder 400 series manual ebook, you need to create a FREE account.

Download Now!

eBook includes PDF, ePub and Kindle version

Register a free 1 month Trial Account.
Download as many books as you like (Personal use)
Cancel the membership at any time if not satisfied.
Join Over 80000 Happy Readers

Book Descriptions:

We have made it easy for you to find a PDF Ebooks without any digging. And by having access to our ebooks online or by storing it on your computer, you have convenient answers with bosch video recorder 400 series manual . To get started finding bosch video recorder 400 series manual , you are right to find our website which has a comprehensive collection of manuals listed.
Our library is the biggest of these that have literally hundreds of thousands of different products represented.

Book Descriptions:

bosch video recorder 400 series manual

Available in basic and advanced versions, the 400 Series features a highly reliable embedded design that minimizes maintenance and operational costs. The basic version provides one audio input, while the advanced version has four audio inputs and a DVD writer. System Overview The Bosch 400 Series takes advantage of the latest H.264 compression technology that allows for more efficient video compression. This reduces the amount of storage and bandwidth needed while also producing better image quality. The 400 Series records multiple video and audio signals while simultaneously providing live multiscreen viewing and playback. Comprehensive search and playback functions provide quick recall and viewing of recorded video. Recording Ease of use is key to the 400 Series design. Simply connect the cameras, apply power, and the unit begins recording automatically. All recording takes place in the background with no operator intervention required. The use of H.264 compression reduces the file size of recordings by as much as 30% compared to standard MPEG4, without sacrificing image quality. Recording at 2CIF and 4CIF resolution is also possible by reducing the recording image rate settings. The recording rate and quality are individually configurable per channel for maximum flexibility. The recording archives are split into two partitions. Alarm recordings input and motion are stored on one partition, while continuous recordings are stored on a separate one. An overwrite mode can be selected separately for each partition if required. PTZ devices, including the Bosch AutoDome Modular and AutoDome Easy II, are supported. Video Recorder 400 Series 4Channel realtime H.264 recording View and record video in CIF, 2CIF, or 4CIF resolution. Builtin web viewer for remote viewing, playback, control, and configuration. Supports VGA and analog monitor output up to 1280x1024. Dual streaming for local recording and remote viewing.All models have extensive alarm. Video Video recording.http://dafangtour.com/fckeditor/userimages/complete-landman-training-manual-reviews.xml

- **bosch video recorder 400 series manual, bosch video recorder 400 series manual download, bosch video recorder 400 series manual pdf, bosch video recorder 400 series manual free, bosch video recorder 400 series manual instructions.**

Video Standard SVGA Record Rate IPS. This can cause fire or electrical shock.Any change or modification of the equipment, not expressly approved by Bosch, could void the warranty or, in the case of an authorization agreement, authority to operate the equipment. This symbol means that electronic and electrical appliances, which have reached the end of their working life, must be collected and disposed of separately from household waste material. SELV circuits should only be connected to other SELV circuits. Video loss Video loss is inherent to digital video recording; therefore, Bosch Security Systems cannot be held liable for any damage that results from missing video information. To minimize the risk of lost digital information, Bosch Security Systems recommends multiple, redundant recording systems, and a procedure to back up all analog and digital information. All rights reserved. Trademarks All hardware and software product names used in this document are likely to be registered trademarks and must be treated accordingly. Both versions operate in a similar manner. The illustrations in this manual show the 4channel version. The 8channel version has 4 additional video channels and 4 additional alarm inputs. The shipping carton is the safest container in which to transport the unit. Save it and all packing materials for future use. Take note of the locations of the cooling vents in the units enclosure and ensure that they are not obstructed. Connect to your network via the RJ45 Ethernet port. Connect a “Bosch RS232 to Biphase converter” to the RS232 port if required. 3.1.3 Powering up Switch on all connected

equipment. The default User ID is ADMINISTRATOR, the default password is 000000 six zeros.Date format Select from three date formats which show either the month MM, the day DD, or the year YYYY first. Date Fill in the current date.http://www.gastleads.com/userfiles/complete-learn-to-play-bass-manual.xml

IP address, Subnet Fill in the IP, subnet mask, gateway addresses, and DNS server mask, and Gateway addresses when DHCP is not enabled.For service purposes, use a nullmodem cable to connect the serial port of the PC to the unit. The Baud rate can be selected in the menu system. No user serviceable parts inside. Refer all servicing to qualified service personnel. Opening the top cover will void the warranty.Click the Monitor B button.Press the enter key to display the Cameo Menu.While in zoom mode, move the mouse pointer to select the area of the picture to be displayed.Press the stop key to switch back to live viewing. An alarm also switches the unit back to live viewing.Within this period of video the event search results can be found.Within this period of video the smart search results can be found.Click Hard disk to see more information about the hard disks.Note Only Bosch hard disks with a signature can be used. If the hard disk is not certified, it cannot be used for recording. The latest alarm status message is always shown.Each of these groups has a set of dropdown submenus which provide access to a screen where the values and functions can be selected and changed.Note Disabling channels will allow increasing the frame rate or resolution on the remaining enabled channels.Postevent Postevent recording duration can be set between 10 seconds and 10 minutes, or set to Follow the alarm state.Select the VGA Output to match the best VGA resolution on the used VGA monitor monitor A.Click Clear All to delete the selected area.Select Manual to require the operator to press the Acknowledge key to acknowledge an alarm.There is no logon user ID or password to protect a camera live image.More Email Settings To Enter up to three email addresses that outgoing email should be sent to.Although the structure is the same, menus and settings behave differently because of the Web Browser.Click and hold the up and down arrows for tilt.Press ESC to exit Full Screen.

Click Step backward to move the image back one frame. Hold it down to continue stepping at a maximum rate of 3 images per second.This window shows details of the video frame shown in the cameo when it was clicked. Exit button Click the Exit button to stop using the Archive Player. Its the ideal solution for a wide range of applications including shopping centers, car parks, financial institutions, city centers and crowd surveillance.The 700 Series provides everything you need to store and manage your surveillance video in a single, easytoinstall box. And installation wizards and automatic IP address assignment, helps you to reduce installation time by up to 50% compared to traditional PCbased IP video solutions.Its the ideal solution for a wide range of applications including shopping centres, car parks, financial institutions, city centres and crowd surveillance. The 700 Series provides everything you need to store and manage your surveillance video in a single, easytoinstall box. And installation wizards and automatic IP address assignment, helps you to reduce installation time by up to 50% compared to traditional PCbased IP video solutions. Its embedded design is also more secure than PC based IP systems. Dedicated to IP with up to 32 H.264 IP camera support with the straightforward easeofuse of a traditional analogue recorder. Speedy installation with fully automatic assigning of H.264 IP cameras. Protect your recorded video from hard drive failures with on board RAID4. Easy to service and expand up to 8 terabytes of internal storage with front replaceable hard drives. Record text data together with associated video e.g. from an ATM machine, license plate reader or cash register. Searching on text data allows fast retrieval of the associated video and provides legal evidence in the event of fraudEquipped with four frontreplaceable HD drives, RAID4, H.264 IP camera support and extensive integration features e.g.

https://labroclub.ru/blog/3g-pentron-manual

with license plate recognition systems, the Divar 700 Series Recorder is ideal for demanding CCTV applications. The 700 Series superior image quality and compression gets the most out of CCTV

images. Features. Both recorders have. Auto discovery and assignment of IP devices. Four frontaccessible hard drivesOnboard RAID4 support. Record text data from e.g. an Automatic Teller MachineATM, license plate reader. External storage option. Optional second Gigabit port. Advanced event handling. Integration with thirdparty management software using VideoSDK. Divar 700 Series H.264 Hybrid Recorder. Hybrid recording of up to 16 analogue cameras and up to 16 additional H.264 IP cameras. Divar 700 Series H.264 Network Recorder. Up to 32 H.264 IP cameras. Benefits. The Divar Hybrid Recorder 700 Series digital recorder supports up to 8 or 16 analogue cameras and up to 16 H.264 IP video streams. It's easy to expand your system with our scalable Divar Network Recorder 700 Series, supporting up to 32 H.264 IP cameras. You can increase storage easily using infield updates without having to call out an engineer. The very high level of easeofuse of the 700 Series even makes attaching an optional external storage array a matter of seconds. Human operators have been relied on to make decisions about who to admit and deny based on levels of authorisation and the appropriate credentials. But the access control business, like many industries before it, is undergoing its own digital transformation; one where the protection of premises, assets and people is increasingly delivered by interconnected systems utilising IoT devices and cloud infrastructure to offer greater levels of security and protection. Modern access control solutions range from simple card readers to two factor authentication systems using video surveillance as a secondary means of identification, right through to complex networks of thermal cameras, audio speakers and sensors.

These systems, connected through the cloud, can be customised and scaled to meet the precise requirements of today's customer. And it's the ease of cloud integration, combined with open technologies and platforms that is encouraging increasing collaboration and exciting developments while rendering legacy systems largely unfit for purpose. Remote management and advanced diagnostics. Cloud technology and IoT connectivity means remote management and advanced diagnostics form an integral part of every security solution.Cloud technology and IoT connectivity means remote management and advanced diagnostics form an integral part of every security solution. For example, as the world faces an unprecedented challenge and the COVID19 pandemic continues to cause disruption, the ability to monitor and manage access to sites remotely is a welcome advantage for security teams who might otherwise have to check premises in person and risk breaking social distancing regulations. The benefits of not physically having to be on site extend to the locations within which these technologies can be utilised. As an example, within a critical infrastructure energy project, access can be granted remotely for maintenance on hard to reach locations. Advanced diagnostics can also play a part in such a scenario. When access control is integrated with video surveillance and IP audio, realtime monitoring of access points can identify possible trespassers with automated audio messages used to deter illegal access and making any dangers clear. And with video surveillance in the mix, high quality footage can be provided to authorities with realtime evidence of a crime in progress. Comprehensive protection in retail. Within the retail industry, autonomous, cashierless stores are already growing in popularity. The use of connected technologies for advanced protection extends to many forwardlooking applications.

Customers are able to use mobile technology to selfscan their chosen products and make payments, all from using a dedicated app. From an access control and security perspective, connected doors can be controlled to protect staff and monitor shopper movement. Remote management includes tasks such as rolling out firmware updates or restarting door controllers, with push notifications sent immediately to security personnel in the event of a breach or a door left open. Remote monitoring access control in storage. In the storage facility space, this too can now be entirely run through the cloud with remote monitoring of access control and surveillance providing a secure and

streamlined service. There is much to gain from automating the customer journey, where storage lockers are selected online and, following payment, customers are granted access. Through an app the customer can share their access with others, check event logs, and activate notifications. With traditional padlocks the sharing of access is not as practical, and it's not easy for managers to keep a record of storage locker access. Online doors and locks enable monitoring capabilities and heightened security for both operators and customers. The elimination of manual tasks, in both scenarios, represents cost savings. When doors are connected to the cloud, their geographical location is rendered largely irrelevant. They become IoT devices which are fully integrated and remotely programmable from anywhere, at any time. This creates a powerful advantage for the managers of these environments, making it possible to report on the status of a whole chain of stores, or to monitor access to numerous storage facilities, using the intelligence that the technology provides from the data it collects. Open platforms power continuous innovation.

All of these examples rely on open technology to make it possible, allowing developers and technology providers to avoid the pitfalls that come with the use of proprietary systems. The limitations of such systems have meant that the ideas, designs and concepts of the few have stifled the creativity and potential of the many, holding back innovation and letting the solutions become tired and their application predictable. Proprietary systems have meant that solution providers have been unable to meet their customers' requirements until the latest upgrade becomes available or a new solution is rolled out. This use of open technology enables a system that allows for collaboration, the sharing of ideas and for the creation of partnerships to produce groundbreaking new applications of technology. Open systems demonstrate a confidence in a vendor's own solutions and a willingness to share and encourage others to innovate and to facilitate joint learning. An example of the dynamic use of open technology is Axis' physical access control hardware, which enables partners to develop their own cloudbased software for control and analysis of access points, all the while building and expanding on Axis' technology platform. Modern access control solutions range from simple card readers to two factor authentication systems using video surveillance as a secondary means of identification. Opportunities for growth. Open hardware, systems and platforms create opportunities for smaller and younger companies to participate and compete, giving them a good starting point, and some leverage within the industry when building and improving upon existing, proven technologies. This is important for the evolution and continual relevance of the physical security industry in a digitally enabled world.

Through increased collaboration across technology platforms, and utilising the full range of possibilities afforded by the cloud environment, the manufacturers, vendors and installers of today's IP enabled access control systems can continue to create smart solutions to meet the everchanging demands and requirements of their customers across industry. As the industry moves towards the mass adoption of interconnected physical security devices, end users have found a plethora of advantages, broadening the scope of traditional video surveillance solutions beyond simple safety measures. Thanks in part to these recent advancements, our physical solutions are at a higher risk than ever before. With today's ever evolving digital landscape and the increasing complexity of physical and cyberattacks, it's imperative to take specific precautions to combat these threats. Video surveillance systems. Cybersecurity is not usually the first concern to come to mind. When you think of a video surveillance system, cybersecurity is not usually the first concern to come to mind, since digital threats are usually thought of as separate from physical security. Unfortunately, these two are becoming increasingly intertwined as intruders continue to use inventive methods in order to access an organisations assets. Hacks and data breaches are among the top cyber concerns, but many overlook the fact that weak cybersecurity practices can lead to physical danger as well.

Organisations that deploy video surveillance devices paired with advanced analytics programs often leave themselves vulnerable to a breach without even realising it. While they may be intelligent, IoT devices are soft targets that cybercriminals and hackers can easily exploit, crippling a physical security system from the inside out. Physical security manufacturers.

Whether looking to simply gain access to internal data, or paralyse a system prior to a physical attack, allowing hackers easy access to surveillance systems can only end poorly. In order to stay competitive, manufacturers within the security industry are trading in their traditional analogue technology and moving towards interconnected devices. Due to this, security can no longer be solely focused on the physical elements and end users have taken note. The first step towards more secured solutions starts with physical security manufacturers choosing to make cybersecurity a priority for all products, from endpoint to edge and beyond. Gone are the days of end users underestimating the importance of reliability within their solutions. Manufacturers that choose to invest time and research into the development of cyberhardening will be ahead of the curve and an asset to all. Wireless communication systems. Integrators also become complicit in any issues that may arise in the future. Aside from simply making the commitment to improve cyber hygiene, there are solid steps that manufacturers can take. One simple action is incorporating tools and features into devices that allow end users to more easily configure their cyber protection settings. Similarly, working with a third party to perform penetration testing on products can help to ensure the backend security of IoT devices. This gives customers peace of mind and manufacturers a competitive edge. While deficient cybersecurity standards can reflect poorly on manufacturers by installing vulnerable devices on a network, integrators also become complicit in any issues that may arise in the future. Cybersecurity services. In addition, we've all heard of the bans, taxes and tariffs the U.S. government has recently put on certain manufacturers, depending on their country of origin and cybersecurity practices. Lawsuits aside, employing proper cybersecurity standards can give integrators a competitive advantage.

With the proliferation of hacks, malware, and ransomware, integrators that can ease their clients cyberwoes are already a step ahead. By choosing to work with cybersecurityfocused manufacturers who provide clients with vulnerability testing and educate end users on best practices, integrators can not only thrive but find new sources of RMR. Education, collaboration and participation are three pillars when tackling cybersecurity from all angles. For dealers and integrators who have yet to add cybersecurity services to their business portfolios, scouting out a strategic IT partner could be the answer. Unlocking countless opportunities. Becoming educated on the topic of cybersecurity and its importance for an organisation is the first step. Physical security integrators who feel uncomfortable diving headfirst into the digital realm may find that strategically aligning themselves with an IT or cyber firm will unlock countless opportunities. By opening the door to a partnership with an ITfocused firm, integrators receive the benefit of cybersecurity insight on future projects and a new source of RMR through continued consulting with current customers. In exchange, the IT firm gains a new source of clients in an industry otherwise untapped. This is a win for all those involved. While manufacturers, dealers and integrators play a large part in the cybersecurity of physical systems, end users also play a crucial role. Commonplace cybersecurity standards. Below is a list of commonplace cybersecurity standards that all organisations should work to implement for the protection of their own video surveillance solutions. Always keep camera firmware up to date for the latest cyber protections. Change default passwords, especially those of admins, to keep the system locked to outside users. Create different user groups with separate rights to ensure all users have only the permissions they need.

Set an encryption key for surveillance recordings to safeguard footage against intruders and prevent hackers from accessing a system through a backdoor. Enable notifications, whether for error codes or storage failures, to keep up to date with all systems happenings. Check the web server log on a

regular basis to see who is accessing the system. Ensure that web crawling is forbidden to prevent images or data found on your device from being made searchable. Avoid exposing devices to the internet unless strictly necessary to reduce the risk of attacks.Benefits over facial recognition systems Typical security staff response would be to monitor the video wall while reviewing the footage and making a verbal announcement throughout the mall so the staff can keep an eye out for her. There is no telling how long it will take, while every second feels like hours under pressure. As more time passes, the possible areas where the child can be will widen, it becomes more timeconsuming to search manually, and the likelihood of finding the child decreases. What if we can avoid all of that and directly search for that particular girl in less than 1 second Artificial neural networks are improving every day and now enable us to search for a person across all selected camera streamsWith Artificial Intelligence, we can. Artificial neural networks are improving every day and now enable us to search for a person across all selected camera streams in a fraction of a second, using only one photo of that person. The photo does not even have to be a full frontal, passporttype mugshot; it can be a selfie image of the person at a party, as long as the face is there, the AI can find her and match her face with the hundreds or thousands of faces in the locations of interest. The search result is obtained in nearly real time as she passes by a certain camera. Distinguishing humans from animals and statues.

The AI system continuously analyses video streams from the surveillance cameras in its network, distinguishes human faces from nonhuman objects such as statues and animals, and much like a human brain, stores information about those faces in its memory, a mental image of the facial features so to speak. When we, the system user, upload an image of the person of interest to the AI system, the AI detects the faces in that image along with their particular features, search its memory for similar faces, and shows us where and when the person has appeared. We are in control of selecting the time period up to days and place cameras to search, and we can adjust the similarity level, i.e., how much a face matches the uploaded photo, to expand or finetune the search result according to our need. Furthermore, because the camera names and time stamps are available, the system can be linked with maps to track and predict the path of the person of interest. AI Face Search is not Face Recognition for two reasons it protects people’s privacy, and it is lightweight. Protecting people’s privacy with AI Face Search. All features of face recognition can be enabled by the system user, such as to notify staff members when a person of interest is approaching the store AI Face Search is not Face Recognition for two reasons it protects people’s privacy, and it is lightweight. First, with AI Face Search, no names, ID, personal information, or lists of any type are required to be saved in the system. The uploaded image can be erased from the system after use, there is no face database, and all faces in the camera live view can be blurred out postprocessing to guarantee GDPR compliance. Second, the lack of a required face database, a live view with frames drawn around the detected faces and constant face matching in the background also significantly reduces the amount of computing resource to process the video stream, hence the lightweight. Face Search versus Face Recognition. AI Face Search.

Face Recognition. Quick search for a particular person in video footage. Identify everyone in video footage. Match detected faces in video stream to target faces in an uploaded image. Match detected faces in video stream to a database. Do not store faces and names in a database. Must have a database with ID info. Automatically protect privacy for GDPR compliance in public places. May require additional paperwork to comply with privacy regulations. Lightweight solution. Complex solution for largescale deployment. Main use locate persons of interest in a large area. Main use identify a person who passes through a checkpoint. Of course, all features of face recognition can be enabled by the system user if necessary, such as to notify staff members when a person of interest is approaching the store, but the flexibility to not have such features and to use the search tool as a simple Googlelike device particularly for people and images is the advantage of AI Face Search.Because Face Search is not based on face recognition, no faces and name identifications are

stored. Advantages of AI Face Search. Artificial Intelligence has advanced so far in the past few years that its facial understanding capability is equivalent to that of a human. The AI will recognise the person of interest whether he has glasses, wears a hat, is drinking water, or is at an angle away from the camera. In summary, the advantages of Face Search. High efficiency a target person can be located within a few seconds, which enables fast response time. High performance high accuracy in a large database and stable performance, much like Google search for textbased queries. The simpletouse interface requires minimal training and no special programming skills. Highcost saving the time saving and ease of use translate to orders of magnitude less manual effort than traditionally required, which means money saving. Scalability AI can scale much faster and at a wider scope than human effort.

AI performance simply relies on computing resource, and each Face Search appliance typically comes with the optimal hardware for any system size depending on the customer need, which can go up to thousands of cameras. Privacy AI Face Search is not face recognition. For face recognition, there are privacy laws that limits the usage. Because Face Search is not based on face recognition, no faces and name identifications are stored, so Face Search can be used in many public environments to identify faces against past and realtime video recordings. AI Face Search match detected faces in video stream to target faces in an uploaded image. Common use cases of AI Face Search. In addition to the scenario of missing child in a shopping mall, other common use cases for the AI Face Search technology include. Retail management Search, detect and locate VIP guests in hotels, shopping centres, resorts, etc.School campus protection With the recent increase in number of mass shootings in school campuses, there is a need to identify, locate and stop a weapon carrier on campus as soon as possible before he can start shooting. Face Search will enable the authorities to locate the suspect and trace his movements within seconds using multiple camera feeds from different areas on campus. Only one clear image of the suspect’s face is sufficient. In the race of technology development in response to business needs and security concerns, AI Face Search is a simple, lightweight solution for airports, shopping centres, schools, resorts, etc.By Paul Sun, CEO of IronYun, and Mai Truong, Marketing Manager of IronYun According to a recent survey, 60% of shoppers are afraid of going grocery shopping, with 73% making fewer trips to physical stores. Returning to the workplace is also causing unease, as 66% of employees report feeling uncomfortable about returning to work after COVID19.