



# CISCO VMS (MS)

DiVA Connect  
Installation manual



## About this manual

This manual describes the installation, start-up and configuration of the systems DiVA Connect. The information in this manual is intended for authorised service personnel and system administrators.

Further information on system operation can be found in the associated user manual.

## Style conventions

The following style conventions are used in this manual:



### Warning

Information is marked in this manner if its non-observance could endanger your health or the functional capability of the system.



### Notice

Additional important information is marked in this manner.

→ *The beginning of successive stages of operation is marked in this manner.*

The individual stages of operation are numbered in sequence.

Keyboard entries or text entries on the screen are denoted in this manner.

Menus, dialogue windows, buttons, etc. are distinguished by **bold type**.

## Service-Hotline

If you have any further questions about the system, please use our service hotline:.

Softwareversion: 4.00.013

Press date: July 2009 (1st edition)

Order number for this manual: KB313-05

### Publisher:

Cisco Systems GmbH  
Am Söldnermoos 17

85339 Hallbergmoos

- Adobe® are trademarks of Adobe Systems Incorporated
- Microsoft and Windows are registered trademarks of Microsoft Corporation
- DiVA® is a registered trademark of MAKU Information Technology Ltd.
- Other names and products not listed above are possibly trademarks or registered trademarks of the respective company

Copyright © Cisco Systems Ltd. 2009

All rights reserved. This document may not be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form, in whole or in part, without the prior written consent of Cisco Ltd.

Subject to technical alteration



<b>Introduction .....</b>	<b>5</b>	Configure holiday profiles .....	28
System description .....	5	Creating new devices .....	30
Explanation of terminology .....	6	Deleting devices .....	30
<b>General advice .....</b>	<b>7</b>	Configure MediaServer .....	31
Security advice .....	7	Configuring protocols .....	33
Important! .....	8	Configure data supplier .....	36
Cleaning .....	9	Setting up archives .....	37
Automatic logout .....	9	Deleting archives .....	40
Adobe Reader .....	10	Deleting archive data .....	40
Alarm recording .....	10	Configuring archive type standard .....	41
Pop-Up-Blocker .....	10	Configuring archive type alarm .....	44
Security settings for Internet Explorer 7 .....	10	Configuring track type pre/post alarm .....	46
<b>Start-up and administration.....</b>	<b>11</b>	Aborting pre/post alarm recording .....	48
System requirements .....	11	Enabling alarm (alarm, pre/post alarm) .....	48
Power supply .....	11	Multiview profiles.....	50
Operating conditions .....	11	Setting up branch manager.....	52
Browser setting (only IE 6) .....	13	Invoking branch manager .....	54
Product activation .....	13	Creating and displaying reference images .....	56
System parameters .....	15	Securing and exporting system data .....	59
Administrator login .....	15	Importing secure system data .....	61
System navigation .....	16	Carrying out software update .....	62
Explanation of user interface:.....	17	Network setup.....	63
Explanation of user interface:.....	18	Restarting the system .....	64
Setting up users .....	19	Logging out of the system .....	64
Changing user rights .....	23	Viewing system status information .....	65
Deleting users .....	23	Viewing configuration information .....	69
Unblock blocked users.....	24	Viewing log file.....	71
Create user groups .....	24	Log file messages .....	72
General system settings .....	25	<b>Index .....</b>	<b>73</b>
Time profiles.....	27		
Configuring existing time profile .....	27		
Create a new time profile.....	27		
Setting holiday profiles.....	28		



## System description

Security-critical areas are monitored and controlled with DiVA Connect.

The systems DiVAConnect fulfil the requirements of the German SP 9.7/5, "Installation tips for optimal room surveillance systems (ORUA)" according to the regulations for health and safety at work regarding banks (BGV C9) and was tested and certified by the Administrative Professional Association's expert committee.

### General functionality

The images created from the attached cameras are digitalised and stored. Each device is integrated via the network connection (Ethernet) in the available network. The data communication takes place via the TCP/IP protocol. Any number of devices can be integrated into the available network structure.

The configuration and service of the devices can be undertaken from any PC workstation integrated in the network.

Access to the software and therefore device settings is password-protected. The user access (user password) and administrator access (administrator password) are different.

# Introduction

## Explanation of terminology

Some terms, which are applied in this manual and in part in the menus as well, will be explained here in more detail.

### Address

Identification number for connected devices.

### Alarm

Archive type for a permanent recording. As soon as an alarm contact is triggered, a recording of a pre-assigned number of images before and after the alarm trigger occurs.

### ATM

Abbreviation for automated teller machine.

### DHCP

Abbreviation for Dynamic Host Configuration Protocol. Using a corresponding server, DHCP allows the dynamic allocation of an IP address in the network.

### DiVA

An abbreviation for digital video archive used in the manual for the DiVApro, DiVAplusSE and DiVAmicro devices.

### DNS

Abbreviation for Domain Name System.

Simplification of the administration in the network. The DNS is mainly used to convert domain names into IP addresses.

### EEC

Abbreviation for electrostatically endangered component.

### Event

An action is referred to as an event if it triggers a recording of camera images onto an archive.

### NSI

Abbreviation for Network Serial Interface

### Recorder

Archive type for an event- and transaction-controlled recording.

### Ring buffer

Images are stored on the archive until the maximum number of images has been reached. The next image then starts at the beginning and overwrites the images from the first taken (ring buffer principle).

### Archive

Series of successive images recorded from different cameras.

## Security advice

This section contains important security advice for the installation and operation of the system.

### Protection against unauthorised use

The system is protected against unauthorised use via a password function (user password and administrator password). However, you should still observe the following points during installation and operation:

- The system stores personal data subject to data protection. Data protection must be observed during operation of the system.
- Carefully store any data you have printed off or saved onto a data storage device.
- Information about the system may only be given to authorised persons
- Use the password function of the system in order to protect it from unauthorised access.

### Target groups

The installation, maintenance and repair of a device may only be carried out by authorised service personnel. In accordance with the german UVV "Kassen", the SP 9.7/5 "Installation guidelines for optical room surveillance equipment (ORÜA)" must be observed during installation and configuration of the system. Work on the system that might interfere with the recording process may only be carried out at times when no cash transactions are taking place, i.e. outside normal working hours or immediately after an assault on the bank branch.

## Advice on the application of extension components

- Only use extension components complying with the requirements and regulations on safety electromagnetic compatibility and telecommunication end device installations. The use of unsuitable extensions may constitute a breach of said regulations and cause system damage. If you are unsure about the application of extension components, ask the manufacturer for advice.
- **Advice on the application of video cameras**  
If the device is used in accordance with german UVV "Kassen", the manufacturer recommends the application of UVV "Kassen"-approved video cameras.



### **Important!**

All warnings and notices mentioned in this technical documentation and labelled on the products are to be observed carefully. The product may only be installed, put into operation and used in accordance with the regulations and in compliance with the instructions contained in this technical documentation. The operational reliability of the product requires professional and careful installation. Operation and use of the devices is restricted to trained personnel. Opening, repairing or altering the device can lead to the loss of operational reliability if not carried out by non-authorized persons or companies, and lead to the expiry of any warranty claims. The same applies to the use of replacement parts, integrated parts and accessories not approved by the manufacturer.

## Cleaning

### Cleaning the device

---



#### **Warning**

Do not use cleaning solvents to clean the device.

---

Use a dry cloth to clean the device.

### Cleaning the cameras

Regularly clean the lens surface of the camera lenses. Use a soft, dry cloth for cleaning.

### Automatic logout

If you are logged onto the system and there is no input for about 10 minutes, then for technical security reasons you will be logged out of the system after this time period.

### Adobe Reader

In order to be able to display archived images as full images, print and save to an external storage medium, the latest version of Adobe reader must be installed on the PC. This program can be downloaded for free from the following link:  
<http://www.adobe.de/products/acrobat/readstep.html>

### Alarm recording

During an alarm recording, it is not possible to configure the system. The **Restart** menu item in the main menu and the menu items **System, Devices, Network, Date/Time, Activation, Upload** in the sub manu are masked out.

### Pop-Up-Blocker

Deactivate all of the pop-up blockers on the browser to ensure trouble free operation of the DiVA system as follows:

#### Internet Explorer up to Ver. 6:

Tools -> Pop-up Blocker -> Turn Off Pop-up Blocker

#### Internet Explorer ab Ver. 7:

Extras -> Internetoptionen -> Sicherheit -> Stufe anpassen...  
-> Verschiedenes -> Popublocker verwenden -> Deaktivieren

#### Mozilla Firefox:

Tools -> Options -> Content -> Block Popup Windows  
(uncheck box)

### Security settings for Internet Explorer 7

Set the following security settings in IE from version 7 and onwards to optimise DiVA software's appearance and functionality:

#### Disable the grey address bar:

Internet Options -> Security -> Custom level... ->  
Miscellaneous-> Allow websites to open windows without  
address bar or status bar -> Enable

#### Allow archive downloads:

Tools -> Internet Options -> Security -> Custom level... ->  
Download -> Automatic prompting for file downloads -> Enable

#### Disable the phishing filter:

Tools -> Internet Options -> Security -> Custom level... ->  
Miscellaneous-> Use phishing filter -> Disable



#### Warning

Observe the safety tips in the **General advice** chapter without fail.

Carry out all installation work in the no-voltage state for each of the devices involved only.

Furthermore SP 9.7/5, "installation guidelines for optical surveillance systems" (ORÜA) from the regulations for safety and health at work (BGV) regarding banks must be observed.

Work on the system which impairs the recording operation may only be performed if no cash transaction is being carried out, i.e. outside working hours or immediately following a robbery.

---

## System requirements

Network: Ethernet

Protocol: TCP/IP

Workstation PC: smallest monitor resolution  
1024 x 768 TrueColor

Internet browsers: Internet Explorer 6.0 and higher  
Firefox 1.0 and higher

Recommended Internet browser: Internet Explorer 7.0 and higher  
Firefox 1.0 and higher




## Power supply

All devices belonging to the system be connected to a battery-driven power supply (UPS) wherever possible. All power supply cables must be brought centrally to the USB and connected there.

## Operating conditions

### Visual system status information using traffic lights

With the traffic lights you obtain visual status information of the system.

Colour of light	Meaning
 green	Error-free system function
 yellow	<ul style="list-style-type: none"> <li>▪ An pre/post alarm archive is active</li> <li>▪ At least one pre/post alarm archive is locked</li> <li>▪ There is an alarm recording on a alarm archive</li> <li>▪ No data has arrived from an ATM for more than 23 hrs. An entry will be made in the logfile.</li> </ul>
 red	<ul style="list-style-type: none"> <li>▪ A critical fault has occurred, e.g. camera error. An entry in the logfile follows.</li> <li>▪ An alarm archive is locked</li> <li>▪ After rebooting, initialisation takes longer than two minutes.</li> <li>▪ An pre/post alarm archive is no more free.</li> </ul>




### Notice

Click on the traffic lights for system status information and a more detailed fault description. Should an error occur in the system, the system status information will be shown immediately after logging in.

## Start-up and administration

Additional colour of light in the branch manager

Colour of light	Meaning
 orange	<ul style="list-style-type: none"><li>▪ At least one pre/post alarm archive is locked</li><li>▪ Alarm recording on an alarm archive</li></ul>

In addition to the above-stated visual status displays, locked alarm archives and pre/post alarm archives are displayed in orange shown in the system status under point **Archives**.

## Browser setting (only IE 6)



If, when using the operating system Windows XP SP2, you have problems downloading archives, you should carry out the following steps in Internet Explorer (Ver. 5.X and higher):

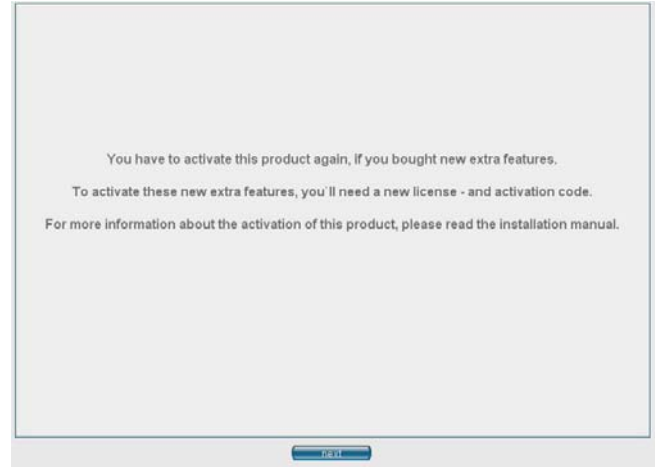
1. Click on **Tools/Internet options**.
2. Click on the **Security** tab.
3. Click on **Trusted Sites**.
4. Click on the **Sites ...** button.
5. Enter the IP address used by the device.

## Product activation

This must be activated when starting the system for the first time.

→ *How to activate the product:*

1. Start the web browser program (e.g. Microsoft Internet Explorer or Mozilla Firefox) installed on the workstation PC.
2. Enter the IP address of the desired system or select the corresponding bookmark (Bookmarks, Favourites).
3. When first starting the system, the **Product activation** menu will appear.  
For a product reactivation click on the **Admin./Settings** button  in the main menu  
and on the **Activation** button  in the sub menu.



**Fig. 1:** Notice for the product activation

4. Click on the **Next** button.
5. A warning will appear. To confirm, enter your password and click the **OK** button:



# Start-up and administration

6. In the following menu, the activation code must be entered. The device code is required to obtain an activation code. The activation code can be obtained by calling the service hotline, or from your reseller.

**Product activation**

Thank you for choosing our product.

To use this product, you have to activate it once.  
Please enter the activation code, you got from our website or from our Hotline, into the fields below

For more information about the activation of this product, please read the installation manual.

**Device code:** 0EHESS1 - 0NUNPT4 - 0SOR1IN - 003X5B5

**Activation code:**  -  -  -

OK

**Fig. 2:** Menu product activation

7. Confirm the entry by clicking **OK**.
8. The following message appears after correct entry:

**The product activation was successful.**  
**The program will restart in 5 seconds .**

( Please wait about 30 seconds to login until the system is initialized )

9. The system restarts after 5 seconds.
10. After restarting, you should wait a further 30 sec until you log into the system.

## System parameters

As administrator you have access to all adjustable device parameters. To protect against unauthorised access however, you must enter a password. The factory preset administrator password is "maku" (user name "admin").

We recommend changing the password. The password must have a minimum of 6 characters and a maximum of 20 characters.



### Notice

Entry is case sensitive.

---



### Warning

No access to the system is possible without entering the password. If you have forgotten the password, send the device to the manufacturer.

---

## Administrator login

To obtain access to the adjustable system parameters, you must first log in as the system administrator.

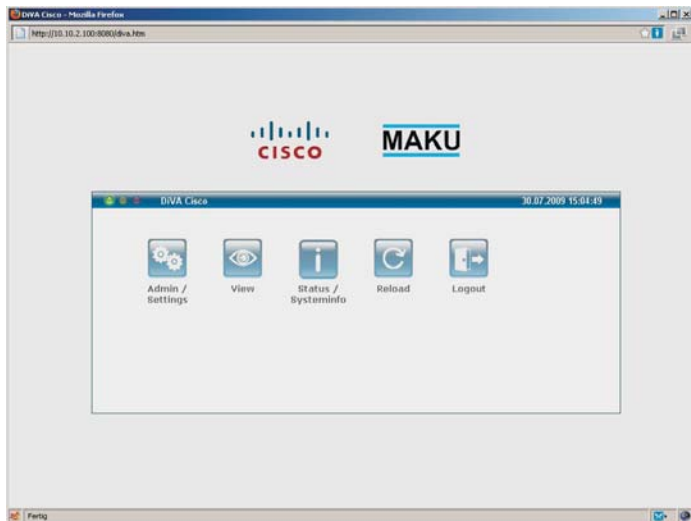
→ *How to carry out the login procedure:*

1. Start the web browser (e.g. Microsoft Internet Explorer or Mozilla Firefox) installed on the workstation PC.
2. Enter the IP address of the desired system or select the corresponding bookmark (Bookmarks, Favourites). If you want to call up and use the preset branch manager for login, then enter the IP address followed by the entry */links.htm*.  
**Example:** `http://192.168.90.81/links.htm`. (see page 52)
3. Enter the user name and the administrator password. The factory-made preset values are:  
user name = admin  
administrator password = maku
4. Confirm the administrator password entry by clicking the **OK** button. For the branch manager, click on the desired system. After correctly entering the administrator password, the main menu finally appears. If there are any errors in the system, you will first see the system status information for checking (see page 64).



## System navigation

### Main menu

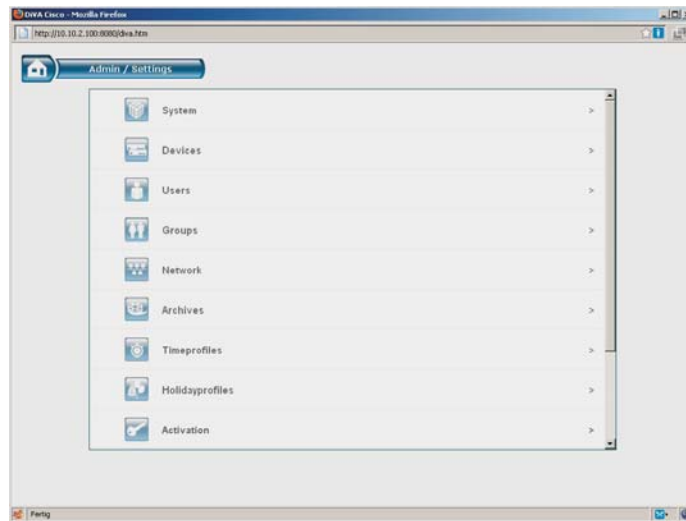


**Fig. 3:** Main menu

The system is divided into one main menu (see fig. 3), and a number of sub-menus.

By clicking on an item listed in the main menu, you will be directed to a sub-menu (see fig. 4). By clicking on an item listed in a sub-menu, you will be directed to the settings menu, where individual settings can be changed.

Exceptions are the main menu items **restart** and **logout**, which are executed immediately following a security enquiry.



**Fig. 4:** Sub menu

### Navigation menu



**Fig. 5:** Navigation menu

The system features a user-friendly navigation menu. Whichever menu has been clicked on is displayed in order of priority above the other menus.

By clicking on one part of the navigation menu, you will be directed to the relevant sub-menu.

By clicking on this button,  you will always be directed back to the main menu.

## Explanation of user interface:

(Main menu: View)

Transaction data field

Image display field

Camera selection menu

The screenshot displays the DIWA Cisco web interface in a Mozilla Firefox browser window. The interface is divided into several sections:

- Transaction data field:** A red box highlights the area containing a home icon and a list of transaction data. The list includes:
  - GAA
  - Permanent
  - Suspicion record
  - ORUA 1Below the list, the following details are shown:
  - Start date: 30.07.2009
  - Start time: 06:41:58
  - End date: 30.07.2009
  - End time: 15:05:40
- Image display field:** A red box highlights a large video feed showing three people in a tunnel-like setting. Below the video, there is a section labeled "Zugehörige Daten:" with a small blue icon to its right.
- Camera selection menu:** A red box highlights a vertical menu on the right side of the interface with the following items:
  - 30.07.2009
  - 15:05:40
  - Axis 210
  - Permanent
- Image search menu and tools buttons:** A red box highlights the bottom section of the interface, which includes navigation buttons (back, forward, home, stop), an "Interval: 1 Image" dropdown, and various tool icons for search, zoom, and other functions.

## Explanation of user interface:

### Image display field

In the image display field archive images from the cameras chosen in the camera selection menu and the archives are displayed.

### Transaction data field

In the transaction data field the transaction data corresponding to the displayed archive images are displayed in the image display field.

### Camera selection menu

Here you should select the camera, the archive and the image interval in the image display field.

### Image search menu



In this menu you can search for archived images.

### Tools-Buttons

Use the buttons to utilise various functions (navigation, archive, application etc.)

### Configuration switch

In the configuration menu, functions, user rights etc. can be switched on or off by activating the switch:








Switch	Explanation
	Turn on function, user rights, etc.
	Turn off function, user rights, etc.








## Tools-Buttons

The buttons turn blue as soon as the mouse cursor passes over them.

If a button stays grey, the function is unavailable.

## Explanation of the Buttons:




Button	Explanation
	<b>Start search</b> Enter the search criteria in the fields and then click this button.
	<b>Delete search fields</b> For a new search, the search fields should be deleted.
	<b>Single images forwards/backwards</b> Entered images as below forwards/backwards
	<b>Stop automatic image search</b>
	<b>Scroll forwards/backwards</b> Entered images as below automatically forwards/backwards. Left-click repeatedly to slow down the display at up to three levels. Right-click to increase it again. (Factor: 1 - 0.75 - 0.5 - 0.25).
	<b>Download image archive</b>
	<b>Print image</b>

Button	Explanation
	<b>Display a results list for a full text or event search</b>
	<b>Back to search dialogue</b>
	<b>To process overview</b>
	<b>Retrieve preview image bar</b>
	<p><b>Markers to isolate the image archive to be backed up</b></p> <p>These markers can be used to precisely determine the start and end of the image archive to be backed up</p>
	<b>Search for the previous or next process</b>
	<b>Search for the previous or next image within the process (possible to change camera)</b>

## Setting up users

Up to 50 further users can be set up in addition to the "admin" default user. Rights can be allocated for each user different user

→ *How to set up a new user:*

1. Click on the **Admin./Settings** button  in the main menu and on the **user** button  in the sub menu.
2. To create a new user, click on the button  in the subsequent menu.
3. The new user configuration menu appears.
4. Enter a user name and password.
5. Select a time profile for the login if necessary.
6. Select a group if necessary.
7. Set the user rights by activating the switches.
8. Confirm the entries by clicking **OK**.

**General**

Name:

Password:

Confirm password:

Login only while:

Is member of:

Network speed limitation:

**User rights**

Administrator:

Operator:

Hardware configuration:

Archive:

Users:

User can change password:

Network configuration:

View reference images:

Save reference images:

Info / Status:

Live images:

Saved images:

View data:

View logfile:

Unlock alarm archives:

**Fig. 6:** Menu *Setting up users*

## General

- **User name**  
The user name must have at least 1 character and no more than 20 characters.
- **Password**  
The password must have at least 6 characters and no more than 20 characters.



### Notice

All characters are allowed for user name and password except € ; ~ & " #.

Care must be taken with upper and lower cases when entering the user name.

---

- **Login only during the time profile**  
Here you select a predefined time profile (see page 27). A login for this user is then only possible during the time that is defined there. This function is not active for an administrator.
- **Is member of**  
Select a previously configured group (see page 24) for the user.
- **Network speed limitation**  
The preset maximal network load is active.

## User rights

Those rights denoted by an plus (+) are administrator rights.

- **Administrator**  
If the user is an administrator, he or she may activate the switch. With that, the administrator rights will be selected automatically. t

## ▪ **Operator**

If the user is an operator, he or she may activate the switch. With that, the user rights for an operator will be selected automatically.

## ▪ **Hardware configuration +**

All functions of the **configuration** menu item may be carried out, such as assigning the camera names. This option should however only be selected by the administrator.

## ▪ **Archives +**

The user may create, change and/or delete archives in the archive administration. This right can only function if the **hardware configuration** user right (see page 21) has also been activated.

## ▪ **User +**

All functions of the **user** menu item may be carried out, such as creating new users and assigning user rights. This option should however only be selected by the administrator.



### **Warning**

Remember that any user authorized to set up a new user can freely set up a new user with all authorization rights.

If several users with administrator rights attempt to log in at the same time, only the first user will be granted access to the system. When selecting user rights, you should carefully consider which rights should be allowed to each individual user.

---

## ▪ **User can change password**

The set-up user has the possibility to change his or her password.

## ▪ **Network configuration +**

The user may alter the network configuration. This right can only be carried out if the **hardware configuration** user right (see page 21) has also been activated.

## ▪ **View reference images**

Users can only see the reference images created in pre/post alarm, but cannot create them. Apart from that, only users with the corresponding rights can call up the **Quick Check** function.

## ▪ **Save reference images**

The user may create reference images for pre/post alarm. This right can only be carried out with the rights **view reference image**, **live images** and **stored images**.

## ▪ **Info/Status**

The system status information can be viewed and printed.

## ▪ **Live images**

Access to the live image function (view live images) is enabled.

## ▪ **Saved images**

All saved images may be browsed, viewed and printed.

## ▪ **View data**

All stored images with corresponding data may be browsed, viewed and printed.

## ▪ **View logfile**

The logfile can be viewed and printed.

## ▪ **Unlock alarm archives**

The user may re-enable an alarm that appears in the system status information (contact event) and archives administration (alarm archive).



## Notice

As soon as the **hardware configuration** and/or **user setup** and/or **archive administration** and/or **network configuration** rights are assigned to a user, he will be listed as an administrator with the corresponding symbol



. Should a user have none of these rights, he will be



listed as a normal user with the symbol

## Overview of user rights



User right	Admin. right	permitted action
Hardware configuration	yes	- complete system configuration - reorganising archives - display configuration overview
Users	yes	Administering users and user rights
Live images	no	Live images may be viewed.
Saved images	no	Saved images may be browsed, viewed and printed.
View data	no	Saved images <b>with</b> data may be browsed, viewed and printed.
Archives	yes	- <b>archives</b> menu item ( <b>hardware configuration</b> user right must be set). - Enabling of pre/post alarm archives
Info/Status	no	Viewing and printing the system status informations
User can change password	no	May change password.
View logfile	no	Viewing and printing the logfile
Network configuration	yes	Configuring network ( <b>hardware configuration</b> user right must be set.)

User right	Admin. right	permitted action
Unlock alarm archives	no	Enabling an alarm archive
View reference images	no	- Viewing of reference images - Execution of quick check.
Save reference images	no	- Creation of reference images in pre/post alarm mode ( <b>live images</b> and <b>save images</b> user rights are necessary.) - Execution of quick check..
Network speed limitation	no	Set network speed limit is active for this user.

## Changing user rights

The user rights can be subsequently changed.



→ *How to change the user rights:*

1. Click on the **Admin./Settings** button  in the main menu and on the **user** button  in the sub menu.
2. The **users** menu appears.
3. Click on the user whose rights you want to change.
4. In the **user administration** menu, change the user rights. If the password is to remain unchanged, then leave the password and password confirmation fields empty.
5. Confirm the entries by clicking the **OK** button.

## Deleting users

Users can be completely deleted.

→ *How to delete a user:*




1. Click on the **Admin./Settings** button  in the main menu and on the **user** button  in the sub menu.
2. The **users** menu appears.
3. Click on the user you want to delete.
4. The **user administration** menu appears.
5. Click the **delete** button in order to delete the user from the **users** menu.



## Unblock blocked users

If a user is blocked (as a result of entering an incorrect password too many times), they may be unblocked by an administrator.

→ *How to unblock a user:*

1. Click on the **admin/settings** button  .  
in the main menu, and on the **user** button  in the sub-menu.
2. The **user** menu will appear.
3. Click on the blocked user  you would like to unblock.
4. The **user settings** menu will appear.
5. Click on the **unlock** button to unblock the user.






### Notice

Administrators are automatically unblocked after a system restart.  
Normal users will only be unblocked after a system restart if, in the general system settings (see page 25), the switch beside the **save blocked users** function is not activated.

## Create user groups

User groups can be configured which are only permitted to retrieve live images from certain cameras, and may only access certain archives (for image searches).

→ *How to configure a user group:*

1. Click on the **admin/settings** button  .  
in the main menu, and on the **groups** button  in the sub-menu.
2. To create a new group, click on the  button in the menu that appears
3. The configuration menu for a new group will appear.
4. Under **group name**, give the group a unique name.
5. Under **available cameras**, select the cameras from which this group is permitted to view live images.
6. Under **accessible archives**, select the archives to which this group may have access, that is, the archives within which this group may perform images searches. If archives are added at a later time, the **all archives** function will be deactivated.
7. Confirm the changes by clicking **OK**.



## General system settings

Assign a name to each system and select the desired menu language. Additionally you can specify the time format, date format and user functions. Furthermore you can specify different system based functions (report errors after x minutes delay, open new browser window for multiview, all-logout function).

General	
Systemname:	DVA Cisco
Language:	English
Format	
Date format:	DD.MM.YYYY
Time format:	24 hours
Users	
Concurrent users:	3
The user will be locked after: wrong logins	3
Save locked users:	<input checked="" type="checkbox"/>
Misc	
Report errors after:	0 minutes delay
Admin can suspend all users:	<input checked="" type="checkbox"/>
Open new browser window for multiviews:	<input checked="" type="checkbox"/>

**Fig. 7: Menu System settings**

→ How to set the general system settings:

1. Click on the **Admin./Settings** button  in the main menu and on the **user** button  in the sub menu.
2. The **system** menu appears.
3. Enter a system name in the **system name** entry field. The system name cannot exceed 20 characters.
4. Select the menu **language** by clicking on the drop down box.
5. Select the **date format** by clicking on the drop down box.
6. Select the **time format** (24 or 12 hours) by clicking on the drop down box..
7. Under **users** in the dropdown menu **simultaneous users**, specify the number of users who can log in simultaneously.
8. In the selection window **The user will be locked after X wrong logins**, select the maximum number of incorrect login attempts.
9. Activate the user right **save locked users**, so that users (not administrators) remain blocked even after a system restart.
10. In the **Issue fault report after:** field under **other**, enter a value in minutes.



### Notice

As the system sends requests to the camera inputs on a low priority basis, the camera input display may require up to approx. one minute to update.

---



11. With the **All logout** function, the address bar of the browser can be used to log out all users logged in to the system, by entering the IP address of the DiVA system, followed by **/all/logout\_all\_users.htm**. Activate the **All logout** function.
12. Activate the function **open new browser window for multiviews**, if the multiview profile is to be opened in a new window, rather than in the DiVA window.
13. Confirm this entry by clicking on **OK**.

## Time profiles

In order to set the opening hours for the foyer and recording periods among other things, you have the opportunity to define ten various time profiles.

### Configuring existing time profile




→ How to configure an existing time profile:

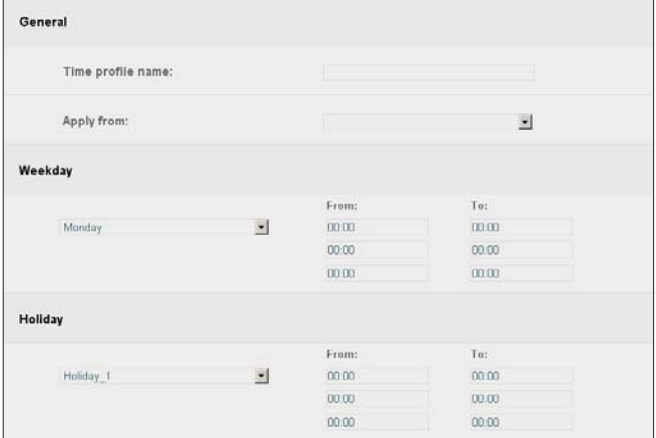
1. Click on the **Admin./Settings** button  in the main menu and on the **time profile** button  in the sub menu.
2. To configure an existing time profile click on a time profile.
3. Alter the values as described in **creating a new time profile** (see next page).
4. Confirm your entries by clicking **OK**.

### Create a new time profile

To use personal, user-defined time profiles, they must be newly created.

→ How to create a new time profile:

1. Click on the **Admin./Settings** button  in the main menu and on the **time profile** button  in the sub menu.
2. To create a new time profile, click on the button  in the subsequent menu.



General		
Time profile name:	<input type="text"/>	
Apply from:	<input type="text"/>	
Weekday		
Monday	From:	To:
	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>
Holiday		
Holiday_1	From:	To:
	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>

Fig. 8: Menu time profile

3. Provide a term for the time profile to be created in the **name** field.

4. If applicable select an existing time profile that you wish to take over in the **take over from** field.
5. In the **weekday** field, select the day for which you wish to set the opening hours. Up to three time intervals are available for that purpose.  
If applicable select the entry **all** in the field **weekday** in order to designate directly the same time interval for all weekdays.
6. If applicable, define up to four types of public holiday with up to three individual time intervals in the **public holidays** field.
7. Confirm your entries by clicking **OK**.



## Notice

The time intervals cannot be configured to extend beyond a particular day.

### For example:

A time interval from 10pm in the evening until 6am the following morning must be divided into two time intervals:




Weekday		
all	From:	To:
	22:00	23:59
	00:00	06:00
	00:00	00:00

## Setting holiday profiles

The holidays can be individually set and also backed up on a data carrier in order to import them to another system. Up to 21 holiday profiles can be created.

## Configure holiday profiles

→ *How to configure an existing and new holiday profile:*

1. Click on the **Admin./Settings** button  in the main menu  
  
and on the **holiday profile** button  in the sub menu.
2. To configure an existing holiday profile click on a holiday profile.
3. To create a new time profile, click on the button  in the subsequent menu.
4. Assign a distinct term for the holiday profile in **name**.
5. To make the profile the current profile, check the **used** box. Only one holiday profile can be set to **used**. Profiles that were previously designated as **used** will be automatically deactivated.
6. In the **setting holiday profile** menu, enter a date and a name and select the desired public holiday type that you previously defined in a time profile.

Name:  Used:

Date:	Name:	Category:	Date:	Name:	Category:
		Holiday_1			Holiday_1
		Holiday_1			Holiday_1
		Holiday_1			Holiday_1
		Holiday_1			Holiday_1
		Holiday_1			Holiday_1
		Holiday_1			Holiday_1
		Holiday_1			Holiday_1
		Holiday_1			Holiday_1
		Holiday_1			Holiday_1
		Holiday_1			Holiday_1
		Holiday_1			Holiday_1
		Holiday_1			Holiday_1
		Holiday_1			Holiday_1
		Holiday_1			Holiday_1
		Holiday_1			Holiday_1

Fig. 9: Menu *holiday profile settings*

7. Confirm the entries by clicking **OK**.

## Creating new devices


In the **devices** menu, the following devices may be created and configured:

MediaServer with camera feeds, data interfaces and protocols.

→ *How to configure a new device:*



1. Click on the **Admin./Settings** button  in the main menu

and on the **devices** button  in the sub menu.

2. To create a new device, click on the button  in the subsequent menu.
3. The **device selection** menu appears.
4. Click on the device you want to connect.
5. Configure the connected device:  
For configuration a **MediaServer** see page 31.  
For configuration a **protocol** see page 33.  
For configuration a **data interface** (e.g. NSI Gateways) see page 36.
6. You can also configure the device later by clicking the **devices** item in the menu structure.

## Deleting devices




→ *How to delete a devices:*

1. Click on the **Admin./Settings** button  in the main menu  
and on the **devices** button  in the sub menu.
2. In the menu structure click on the device to be deleted.
3. In the menu that appears click on the **delete** button to remove the device from the system.
4. Finally confirm the changes by clicking **OK**.

## Configure MediaServer

The DiVA Connect system can be operated on a media server. For this, the media server must be created and correctly configured.


→ How to configure a new device:

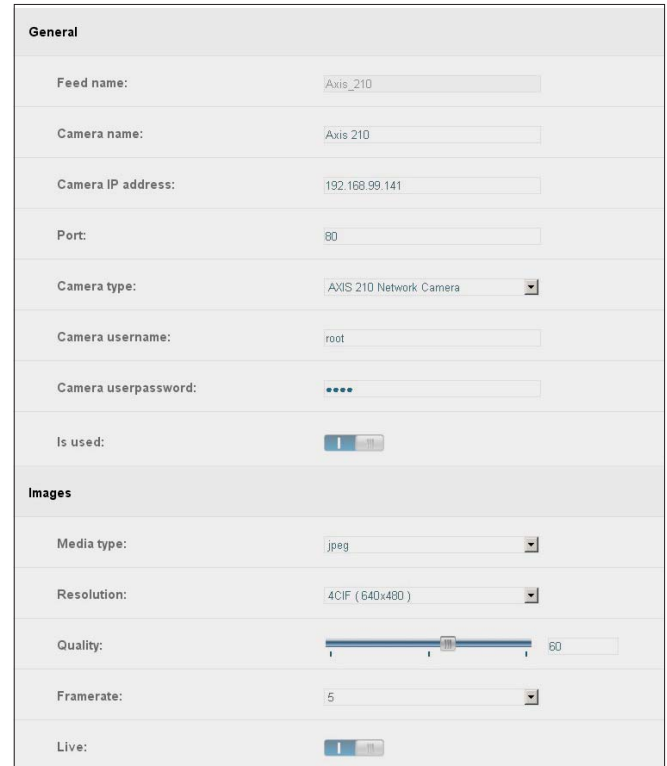
- In the main menu, click on the **admin/settings** button  and in the sub-menu on the **devices** button .
- Click on the button  to configure the media server.



**Fig. 10:** Menu *Configure MediaServer*

- Under **general**, assign a name to the media server.
- Enter the host IP/name, and the port from which the media server can be accessed.

- Configure the cameras which are connected to the media server by clicking on the button , and adding a camera channel.



**Fig. 11:** Menu *camera feed*



## Start-up and administration

6. Under **general**, enter a name for the **feed**, a **camera name**, the **camera IP address** and the **port** from which the camera can be accessed.
7. Select the **camera type**, and enter the **camera user name** and the **camera user password**.
8. In order to be able to use the camera, the camera must be activated with the **used** switch.
9. The images to be recorded by the camera are configured under **images**.
10. From the dropdown menus, select the appropriate **media type** (JPEG), **resolution** (320x240, 640x480, or 1280x1024), the **image quality** (0-100) and the **frame rate**.
11. To enable live images from the camera to be viewed, the **live** switch must be activated.
12. Confirm your entries by clicking on **OK**.

## Configuring protocols

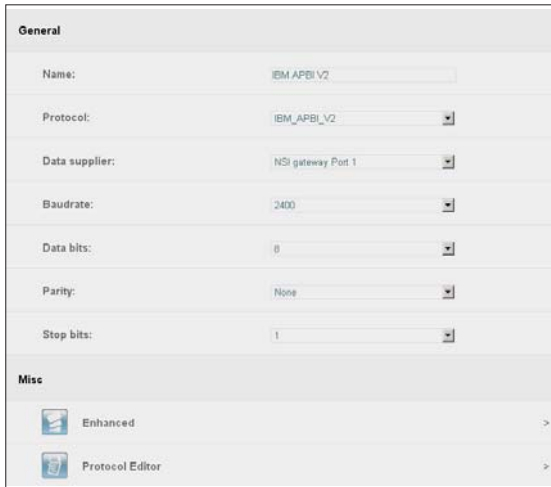
To be able to operate a GAA on a data interface, for example, (eg. NSI gateway), the transfer parameters and the appropriate protocol must be set, and a unique name entered.

→ *How to configure a protocol:*

1. Click on the **Admin./Settings** button  in the main menu

and on the **devices** button  in the sub menu.

2. To configure a protocol click on the **protocol** button .



The screenshot shows a configuration window with the following fields and options:



- General**
  - Name: IBM APBI\_V2
  - Protocol: IBM\_APBI\_V2
  - Data supplier: NSI gateway Port 1
  - Baudrate: 2400
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
- Misc**
  - Enhanced >
  - Protocol Editor >

**Fig. 12:** Menu **Protocol**

3. Assign a distinct term for the data interface in **name**.

4. Select a **protocol** (see also **protocol editor** page 35).
5. The following message appears:



6. First click on the further parameters before clicking on the **enhanced** button .
7. In **data supplier**, select the COM Port of the device (NSI Gateway) aus.
8. Set the transfer parameters **bits per second, data bits, parity** and **stop bits**.
9. Click on the **enhanced** button .
10. If a protocol cannot be modified by clicking the **enhanced** button, then the **not available!** message will appear.
11. If you have selected a protocol that can be modified, then the following menu will appear:

Photostep configuration: IBM

Photostep: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Portrait:

Cash dispenser:

Collect:

New transaction triggered by:

Analysis of TAN

Analysis of photosteps

Fig. 13: Menu **Protocol/Enhanced**

12. Select a common protocol in the **protocol default** menu.
13. If necessary modify the photo steps. When a change is made to the photo steps, the display in the **photo steps default** selection menu changes automatically to **user-defined**.
14. For the desired photo step (from 1 to 16) click on the **Portrait** and/or **security** radio button to generate corresponding images for this photo step.  
A portrait image for photo step 3 as well as a security image for photo step 11 is generated as shown by the example in Fig. .
15. To use photo steps to generate data to be applied, click the **collect** radio button. You can also use photo steps for generation when no portrait or security has been selected.
16. Click according to choice in the **TAN evaluation** radio button if a new related procedure (through recognition of a change in TAN) should be triggered, or **evaluation of the**

**photo steps** radio button if a new related procedure should be triggered (through recognition of a photo step which is smaller or the same as a preceding photo step).



### Notice

Some computer centres do not provide TANs. In this case, **evaluation of the photo steps** should be selected.

17. Finally confirm the configuration by clicking **OK**. The changed settings are automatically adopted in the programming code of the protocol editor (see page 35).

## Protocol editor

If none of the protocols in the protocol selection are right for the ATM, then you have the opportunity to alter or reset the protocols. The protocol editor is available for the purpose.



### Warning

The alteration of a protocol should only be carried out in consultation with the service hotline since the storage of an altered protocol is irreversible. Moreover, Java programming knowledge is required.

→ How to create or change an ATM protocol:

1. Click on the **protocol editor** button



```

Name: IBM_APBI_V2

////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
// Protokoll Interpreter IBM-APBI //
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////

import java.io.*;

public class IBM_APBI_V2 extends gsaProtocolHelper
{
    // Diese Werte werden aus dem FotoStep-Dialog übernommen
    //
    private String portrait = "";
    private String geldfach = "";
    private String collect = "";
    private String unetan = "";

    private final String VERSION = "IBM-APBI_V2 Protokollinterpreter";

    private String STX = chr( 0x02 );
    private String ETX = chr( 0x03 );
    private String strAnsStatus = new String( chr(02)+"1111"+chr(31)+"101000"+chr(31)+chr(31)+chr
    private String strAnsACK = new String( chr(02) + chr(06) + chr(10) + chr(03) + chr(15) );
    private String strAnsNAK = new String( chr(02) + chr(21) + chr(10) + chr(03) + chr(28) );

    private int actStep; //Aktueller Step
    private int lastStep = 16; //Step auf Max Step
    private String photoStep = ""; //Step löschen
    private String gsaDaten = ""; //Daten löschen
    private String lastTan = ""; //letzte TAN merken
    
```

Fig. 14: Menu **protocol editor**

2. In the **name** field, enter a distinct term for the changed or new protocol.



### Warning

If the name is not changed, then the selected protocol will be overwritten.

3. Alter the protocol accordingly.
4. Finally confirm the protocol change by clicking **OK**



### Notice




After confirming by clicking **OK**, the **please wait** message will appear in a JAVA output window. After approx. 1 minute, the **compiling successful** message appears. Only then is the JAVA protocol applicable.

## Configure data supplier

Data supplier (e.g. NSI Gateway) are automatically recognised and appear in the device list with their MAC address as identification.

Currently only a NSI gateway can be configured. A unique name must be given to the data interface. Apart from that, the contacts connected need to be configured.

→ *How to configure an NSI gateway:*

1. Click on the **Admin./Settings** button  in the main menu  
and on the **devices** button  in the sub menu.
2. To configure a NSI Gateway click on the **NSI gateway** button .
3. Enter a unique handle (such as NSI GAA 1) for the NSI gateway in the **Name** field.
4. The MAC address will automatically appear in the **MAC address** field. However, you can also alter this manually.
5. To configure the contacts enter a name and select the contact type (NC or NO).
6. To using the input contacts the **use** switch must be turned on.



### Notice

Only report contacts can be connected and configured.

7. Confirm your entries by clicking **OK**.

General	
Name:	<input type="text" value="NSI gateway"/>
Mac - Address:	<input type="text" value="00:09:ba:03:00:61"/>
Input contact 1	
Name:	<input type="text" value="Kontakt 1"/>
Type:	<input type="button" value="NC"/>
Is used:	<input checked="" type="checkbox"/>
Input contact 2	
Name:	<input type="text" value="Kontakt 2"/>
Type:	<input type="button" value="NO"/>
Is used:	<input type="checkbox"/>




**Fig. 15:** Menu *Data supplier*

## Setting up archives

You can divide the system hard drive into a max. of 50 archives. Since it is possible to configure each archive individually, you achieve different ring buffer capacities. For each alarm and standard archive the image resolution and the image and archive sizes can be individually determined. For each pre/post alarm archive all important parameters can be set.




Before saving the images and data the database target must be specified:

→ *How to specify the database target:*

1. Click on the **Admin./Settings** button  in the main menu and on the **archives** button  in the sub menu.
2. To specify the database click on the database button .
3. Confirm the entries by clicking on **OK** and confirm the following warning by entering your password and clicking on the OK button:



## Archives icons

Icon	Meaning	Explanation
	Standard archive	An event- and transaction-controlled recording in the ring buffer ensues.
	Alarm archive	Records permanently. As soon as an alarm contact is triggered however, only a pre-determined number of images are recorded. Subsequently, the archive is locked and no further recordings occur
	Pre/post alarm archive	An archive that in accord with the german BGV (banks) records for pre/post alarm mode

## Explanation of alarm or standard archive type:

**Fig. 16:** Menu *configure alarm/standard archive*

## Name

Provide a name so that the track is uniquely identified.

# Start-up and administration

## Size of archive in MB

You set the track size manually using the slider. The maximum value is automatically displayed on the scale.

## Explanation for pre/post alarm archive type:

General	
Archive name:	<input type="text"/>
Number of alarm archives:	<input type="text" value="3"/>
Number of cameras:	<input type="text" value="2"/>
Thereof IP Cameras:	<input type="text" value="0"/>
Pre/post alarm archive	
Before alarm:	<input type="text" value="15"/> minutes <input type="text" value="2"/> Pics / s
After alarm:	<input type="text" value="15"/> minutes <input type="text" value="2"/> Pics / s
Suspicion record.	
Suspicion recording ( number of images ):	<input type="text" value="1000"/>

Fig. 17: Menu **Setting up pre/post alarm archive**

## Name

Provide a name so that the track is uniquely identified.

## Number of alarm Archives

State the number of alarm archives.

## Number of cameras

State the number of cameras (min. 1).



### Notice

Please note that at least two cameras are required for a pre/post alarm recording pursuant to the german UVV "Kassen".

## There of IP cameras

If IP cameras are also assigned to the pre/post alarm archive, the number of cameras should also be entered here. This will allow the difference in image size of the IP cameras to be taken into account for the archive size.

## Before alarm (minutes)

Enter the number of minutes that should be recorded before the alarm trigger (min. 15 minutes and max. 30 minutes).

## Interval

Select the interval to determine how many per images per second should be made prior to the alarm. You can choose between 1 image/second and 2 images/second.

## After Alarm (minutes)

Enter the number of minutes that should be recorded after the alarm trigger (min. 15 minutes and max. 30 minutes).




## Interval

Select the interval to determine how many per images per second should be made after the alarm. You can choose between 2 image/second and 4 images/second.

## Suspicion recording (number of images)

Enter the number of images that can recorded in total after a suspicion trigger (1000 images is recommended).

→ *How to configure a new archive:*

1. Click on the **Admin./Settings** button  in the main menu and on the **archives** button  in the sub menu.
2. To create a new archive, click on the button  in the subsequent menu according to the archive type.
3. Select one of the **alarm, standard** or **pre/post alarm** archive types.
4. In the **General** menu (see Fig. 16) enter a archive name in the **name** field.
5. With the slider, choose an archive size
6. If you have chosen the **pre/post alarm** archive type, then the menu for setting up an pre/post alarm archive appears (see Fig. 17).
7. Enter a distinct term in **name** for the pre/post alarm archive.
8. Enter values for **number of alarm tracks, number of cameras, there of IP Cameras, before alarm (minutes), after alarm (minutes) and suspicion (number of images)**.
9. Confirm by clicking **OK**



### Warning



The size of an configured archive cannot be revised at a later stage. Archives can only be deleted and subsequently recreated.

---



## Deleting archives

→ *How to delete archives:*

1. Click on the **Admin./Settings** button  in the main menu and on the **archives** button  in the sub menu.
2. Click on the archive to be deleted.
3. In the menu that subsequently appears click on the **delete** button.
4. Once confirmed, the archive with the stored images is deleted.  
Exception: Pre/post alarm archives.  
Here, a warning appears:



In order to permanently delete the pre/post alarm archive, enter your password and then click on the **OK** button..





### Notice

In some circumstances, a system restart is required after a track is deleted. A note to this effect will appear in the message to be confirmed.

## Deleting archive data

The data from an standard archive can be manually deleted. An automatic delete can be configured in the respective track (see page 43).

→ *How to delete the archive data manually:*

1. Click on the **Admin./Settings** button  in the main menu and on the **archives** button  in the sub menu.
2. Click on the archive to be the data deleted.
3. Click on the **delete data** button.
4. Confirm the warning by clicking **OK** in order to delete the deleted for good.



### Warning

The data cannot be recovered !

## Configuring archive type standard



### Warning

Before implementing this item, you must have setup the camera feeds on the MediaServer (siehe Seite 31).

For image recording on the previously set standard archive (see page 37) it must be configured with events to trigger image recording. Up to eight various pre-defined events can be allocated for each archive. For each event, you can select the cameras that should record images when the event is triggered. Additionally, the time duration of the event must be defined.

### Camera allocation menu:

Trigger event:	Trigger device:	Axis 210
ATM portrait	IBM APBII V2	<input checked="" type="checkbox"/>
ATM cash dispenser	IBM APBII V2	<input checked="" type="checkbox"/>
		<input type="checkbox"/>
		<input type="checkbox"/>
		<input type="checkbox"/>
		<input type="checkbox"/>
		<input type="checkbox"/>
		<input type="checkbox"/>

Fig. 18: Menu **Camera allocation**

### Archive

The name of the chosen archive appears in this field, which you can also change if necessary.

### Trigger event

Here, an event is selected which triggers the image recording. There is a choice of different events:

- **ATM portrait:** A connected ATM with portrait camera
- **ATM cash dispenser:** A connected ATM with security camera



### Notice

Each connected ATM should be configured to a separate archive.

If an ATM only has an inbuilt portrait camera, then the events **ATM portrait** **and** **ATM cash dispenser** must be allocated to the same camera since the transaction data is transmitted and recorded with the event **ATM cash dispenser**.

Furthermore, the events **ATM portrait** and **ATM cash dispenser** may only be assigned **once** in each case to an address in the complete event allocation.

- **Contact:** A connected message contact (NSI Gateway)
- **Permanent:** Permanent recording of camera images

## Trigger device

Here the associated address, camera or the associated device is selected for the chosen event. The address set here must agree with the address set on the device.

For the events **ATM portrait** and **ATM cash dispenser**, the protocols are available in each case, in the way that they were configured in the **protocol** menu (see page 33).

For the **contact** event, the contacts are available, in the way that they were configured at the NSI Gateway (see page 36).

## Columns with camera names

Here you can only select cameras that are defined as **used** in the camera feeds menu in the MediaServer device configuration (see page 34).

By clicking on the camera name, you will see a preview image of the camera connections.

## Retention time x days

The archive data can be automatically deleted after the entered number of days.



### Warning

Once you have carried out this function on an archive, you will not be able to reverse it.

## Device filter

Select the device whose cameras are to be shown to select them for events.

## Time control:

Trigger event:	Trigger device:	Delay:	Interval / Fps:	Quantity:	Time control:	
ATM portrait	IBM APBi V2	00:00:00	00:01:00	Interval	2	offen
ATM cash dispenser	IBM APBi V2	00:00:00	00:01:00	Interval	2	offen
		00:00:00	00:01:00	Interval	2	geschlossen
		00:00:00	00:01:00	Interval	2	geschlossen
		00:00:00	00:01:00	Interval	2	geschlossen
		00:00:00	00:01:00	Interval	2	geschlossen
		00:00:00	00:01:00	Interval	2	geschlossen
		00:00:00	00:01:00	Interval	2	geschlossen

Fig. 19: Menu **Event allocation/Time control**

## Delay

The delay for the beginning of the recording is set here. The delay begins after the event trigger.

## Interval

Set the time interval between successive images in a recording.



### Notice

The time input is given in the form minutes:seconds:hundredths of seconds

Alternatively, you can also enter a value in frames/second.

## Image

Here the number of images are entered which should be recorded after the end of the event trigger.





### Hinweis


The value of 2 images is the minimum for contact events, since otherwise the event repeats itself for as long as is technically possible. This is independent of the interval setting.

## Time control

Here the time profile (see page 27) is allocated, for which the cameras can record when an event trigger occurs. Time profiles must first be created before they can be selected.

→ *How to allocate an event to an archive:*

1. Click on the **Admin./Settings** button  in the main menu and on the **archives** button  in the sub menu.
2. Click on the archive, to which you wish to allocate events.
3. Place a check in the **Retention time x days** field and enter a value, so that the data on this archive is deleted after reaching the entered number of days.
4. Click on the **event** column and select the event from the drop down menu in each case.
5. Click on the **Trigger device** column and select the address, the contact, the camera or the device for this event from the drop-down menu.
6. Click on the radio button for the cameras in order to allocate these to the event. To view a preview image of the camera, click on the camera name.
- 7.

Click on the **time control** button **Zeitsteuerung** .

To change the **camera allocation** again, click on the button .

8. Click on the **interval** input window and enter a value for the interval, for which the image recording should take place. The smallest value that can be set is 00:00:04 (see page point 13). Alternatively, you can also enter a value in frames/second.
9. Click on the **image** input window and enter a value for the number of images which should be recorded after the end of the event trigger. A maximum of 25 images for an interval of 00:00:04 is possible (see page point 13).
10. Click on arrow in the **time control** selection window and select a previously configured time profile (see page 27) from the resulting drop-down menu.
11. Confirm and save the entries by clicking **OK**.

## Configuring archive type alarm

Permanent recordings are made on a previously set alarm archive (see page 37). However as soon as an alarm contact is triggered, only an certain prespecified number of images are recorded.

Subsequently, the archive is locked and no further recording takes place. A fault contact must be allocated to this archive and the duration of the image recording must be set.

General	
Archive name:	<input type="text" value="Alarm1"/>
Interval:	<input type="text" value="00:01:00"/> Interval ▾
Timeprofile:	<input type="text" value="geschlossen"/> ▾
Alarm	
Address:	<input type="text" value="Kontakt 2"/> ▾
Quantity:	<input type="text" value="2"/>
Available cameras	
Axis 210:	<input type="checkbox"/> <input checked="" type="checkbox"/>

**Fig. 20:** Menu *alarm archive*

### Archive name

The name of the chosen archive appears in this field, which you can also change if necessary.

### Interval

Time interval for successive images in a image recording.

### Time profile

Here the time profile (see page 27) is entered for which the cameras can record when an alarm trigger occurs.



### Address

Contact which triggers the alarm.

### Quantity

Total number of images to be recorded after an alarm trigger.

→ *How to configure an alarm archive:*

1. Click on the **Admin./Settings** button  in the main menu and on the **archives** button  in the sub menu.
2. Select the alarm archive to be configured.
3. Enter a value in the **interval** selection window. The smallest value that can be set is 00:00:04. Alternativ können Sie auch einen Wert für Bilder/Sek. eingeben.
4. In the **address** selection window, choose the address with the report contact, which should trigger the alarm recording.
5. From the **timeprofile** drop-down menu, select a previously configured time profile (see page 27)
6. In the **quantity** input window, enter a value for the number of images to be recorded after an alarm trigger.
7. Choose the recording **cameras** by activate the switches.
8. Confirm and save the entries by clicking **OK**.



### Notice

The archive is locked after an alarm recording and can only be overridden by carrying out the **enable alarm** procedure (see page 48). All track images are deleted and a new recording begins.

---

## Configuring track type pre/post alarm

Permanent recordings are made on previously set pre/post alarm archive (see page 37). However, as soon as an alarm contact is triggered, recording only takes place for a certain prespecified time (min. 15 minutes and max. 30 minutes) before and after the alarm trigger. After that, the pre/post alarm archive is locked and no further recording takes place. If several pre/post alarm archives are set up, then there is an automatic switch to the following track. Even for a suspicion trigger, a set number of images are recorded. Therefore contacts must be allocated for the alarm and suspicion cases that trigger the recordings.



### Warning

Do not connect the contacts for the alarm and suspicion triggers until the pre/post alarm archive has been configured, or rather, ensure that the contacts are inactive, since otherwise an alarm will be triggered directly after contact allocation.

---

### Archive name

The name of the chosen archive appears in this field which you should also alter here if necessary.

### Alarm contact

Select a contact to trigger the alarm.

### Password

For an alarm abort, i.e. dealing with the appropriate archive during an alarm trigger, a password is required, which you must provide here.

### Suspicion contact

Select a contact to trigger suspicion recording.

### Suspicion interval

Time interval between successive images in a image recording.

### Quantity

Enter the number of images which should be recorded after a suspicion trigger.

### Available cameras

Choose at least two camera for the recording.

**General**

Archive name: ORQA

**Alarm**

Alarm contact: Kontakt 2

Password:

Confirm password:

**Suspicion record.**

Suspicious contact: Kontakt 2

Interval: 00:01:00 Interval



Quantity: 30

**Available cameras**

Axis 210:

**Fig. 21:** Menu *Pre/post alarm archive configuration*

→ How to configure an pre/post alarm archive:

1. Click on the **Admin./Settings** button  in the main menu and on the **archives** button  in the sub menu.
2. Select the pre/post alarm archive to be configured.
3. In the **alarm contact** drop-down menu, select the contact which should trigger the alarm recording.



4. Provide a password for a possible alarm abort and enter this again for confirmation in **password confirmation**.
5. In the **suspicion contact** drop-down menu, select the contact which should trigger the suspicion recording.
6. Enter a value in the **interval** selection window. The smallest value that can be set is 00:00:04. Alternatively, you can also enter a value in frames/second.
7. In the **quantity** selection window, enter a value for the number of images to be recorded after a suspicion trigger.
8. Choose the recording **cameras** by activate the switches.
9. Confirm the entries by clicking **OK**.



### Aborting pre/post alarm recording

After an pre/post alarm is triggered, only limited work in the system is possible during the alarm recording. After an alarm trigger, the system logs itself out automatically. In the status display, the "alarm recording is running!" pre/post alarm status appears. Only the pre/post alarm archive appears in the archive administration. The pre/post alarm can only be cancelled by a password request.

→ *How to abort an pre/post alarm recording:*

1. Click on the **Admin./Settings** button  in the main menu and on the **archives** button  in the sub menu.
2. Click on the pre/post alarm archive.
3. Enter a previously provided password (see page 46) to abort the alarm recording.
4. Confirm the password and hence the abort of the alarm recording by clicking **OK**.

### Enabling alarm (alarm, pre/post alarm)

#### Enabling Alarm



Alarm archives locked after an alarm trigger must be enabled for a new recording.



#### Notice

Alarm archives can only be enabled if you possess the **enable alarm** user right.

→ *How to enable an alarm archive:*

1. Click on the **Admin./Settings** button  in the main menu and on the **archives** button  in the sub menu.
2. Click on the alarm archive to be enabled.
3. The **alarm archive** menu appears.
4. Click the **unlock** button.



5. All images are deleted and a new permanent recording begins until an alarm is triggered again.



#### Warning

Nothing can be accessed when an alarm track is enabled. All archived images are deleted.

## Enabling pre/post alarm

An pre/post alarm archive locked after an alarm trigger must be enabled before a new recording can be made.



### Notice



Pre/post alarm archives alarms can only be enabled if you possess the **archives** user rights..



### Warning

Nothing can be accessed when an pre/post alarm archive is enabled. All archived images are deleted.

→ How to enable an pre/post alarm archive:

1. Click on the **Admin./Settings** button  in the main menu and on the **archives** button  in the sub menu.
2. Click on the pre/post alarm archive
3. The **pre/post alarm archive** menu appears.
4. In **locked pre/post alarm archives** press the **unlock** button on the pre/post alarm archives to be enabled.



5. Click on the **unlock** button.
6. All images are deleted and a new permanent recording begins until an alarm is triggered again.

## Multiview profiles

As soon as more than one camera with live image rights is configured in the system (see page 30), you have the option of configuring a multi-view display as desired, and storing it in a multi-view profile. Up to 50 multi-view profiles can be stored.



### Notice

You will only have access to the live image mode if the **live image** option in the user configuration has been activated by the administrator, and if you are assigned to the **live image group** that is permitted to view live images from this camera.

In addition, the **live image** option must be assigned in the camera configuration.




Please note that live images are not to be accessible from safe deposit box surveillance cameras on the grounds of privacy law.

If you are denied access to live images from a particular camera, the following image shall appear::



You can only save and delete multi-view profiles if you possess administrator rights.

→ How to create and edit a multiview profile:

1. In the main menu, click on the **admin/settings** button  and in the sub-menu on the **multiview** button .
2. To edit an existing multiview profile, click on the relevant multiview profile in the menu.
3. To create a new multiview profile, click on the button  in the menu.
4. Depending on the system configuration (see page 26), a new window will open, or the **multiview profile** will be displayed in the current window.

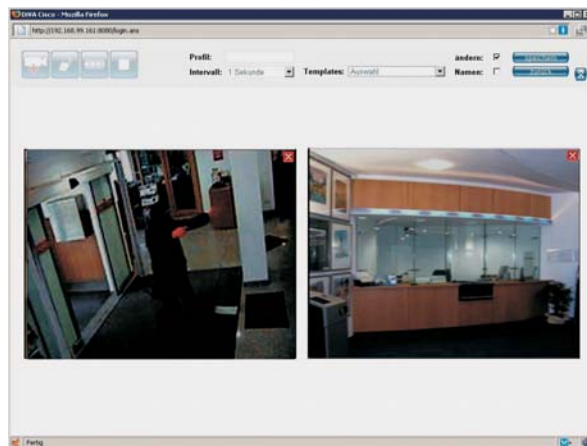


Fig. 22: Multiview








## Notice

If the multiview profile is open in the current window, and you close the window via the browser button , you will be logged out of the system.

If the **multiview profile** opens in a new window, and the configured window size of the selected multiview profile is larger than the maximum display resolution, you will receive an error message. To adjust the resolution, contact the administrator.

5. Under **profile**, assign the multiview profile a unique name.
6. If the system is configured so that multiview profiles open in a new window (see page 23), the resolution of the window may be adjusted to suit the display resolution. In the **size** dropdown menu, select a resolution for the multiview window.
7. Under **templates**, select a pre-configured multiview profile. If a configuration has been performed previously, all camera images will be deleted after a confirmation prompt.
8. The camera images will be assigned in the matrix according to the template selected.
9. Manual camera images may also be added to the profile. For this, click on the button .  
A multiview profile may contain a maximum of twelve camera images, plus one additional camera image which may be set as **VARIABLE** (see item 16).
10. A camera image which has been recently added is outlined in green.
11. Check the **change** box to edit the camera images. The camera images may be scaled, moved or deleted. In addition, the camera in the camera image can be selected.
12. To move the camera image onto the matrix, click on the image. The cursor will change to an arrow/cross . Hold down the left mouse button, and drag the image to the desired location. The menu bar will fade for as long as the left mouse button is held down.
13. The images will automatically be placed on a grid. This will allow you to place the images more easily.
14. To scale the images, press the ctrl key while holding down the left mouse button. The cursor will change into a diagonal double-arrow . You can now scale the image continuously.
15. To change the camera in the camera image, click on the camera image. The camera selection menu will appear. Select the desired camera.
16. If necessary, set one camera image to **VARIABLE**. As soon as you click on another camera image, this image will also appear in the camera image, set to **VARIABLE**. The image interval in the camera image is set to 0.25 seconds with the **VARIABLE** setting, and cannot be changed.
17. Click on an individual camera image to delete it . This button will only appear if the **change** box has been checked. .

18. To display the camera name in the camera image, check the "name" box.
19. To delete all camera images, click on the button .
20. To view live images from the cameras, click on the button .  
Under **interval**, select the desired live image interval.
21. To stop live images, click on the button .
22. To hide the configuration menu, click on the icon .  
To show the menu again, click on the icon .
23. To save the configured multiview profile, click on the **save** button.
24. To delete a previously saved multiview profile, click on the **delete** button.
25. To return to the start without making changes to the multiview profile, click the **back** button, or close the multi-view profile that was opened in the new window.

## Setting up branch manager

The branch manager gives you the opportunity to log into several systems via **one** menu terminal without having to know further IP addresses in each case. You can also log into each system from any workstation within your network using just a single user name and password entry.

Note however that here you must be set up as a user with your own password on the target system. The status of all systems in each case can be displayed by means of an advanced function.

To be able to use the branch manager functions, these must first be set up.

→ *How to set up the branch manager*

1. Click on the **Admin./Settings** button  in the main menu

and on the **branch manager** button  in the sub menu.



### Notice

You can only set up the branch manager if you have the user right **hardware configuration**. Take care during the programming that you confirm your entries within 10 minutes approx. Otherwise an automatic logout occurs (see page 9) and your entries will not be saved.

---

```

File# 1
* DiVAConnect1:192.168.1.3
* DiVAConnect1:192.168.1.4
>
File# 2
* DiVAConnect1:SSL192.168.1.5
* DiVAConnect1:192.168.1.6
    
```

**Fig. 23:** Menu *branch manager setup*

2. Bearing in mind the following entry conditions, enter the names and IP addresses of the systems
  - 1st line:  
Name of branch  
Subsequent lines:  
System identifier with associated IP address. A semi-colon must be placed between the identifier and the IP address, whereby **no** empty space may be placed after the semi-colon.  
**Example:** *DiVA 1:192.168.90.81*
  - > means: set a new **column** in the menu.  
This character must be entered on a separate line.

- >> means: set a new **row** in the menu.  
This character must be entered on a separate line.
- \* means: system status display.  
This character must be entered before the system identifier in order to receive a status report.


An empty space must be placed between the \* and the identifier.


**Example:** \* *DiVA 1:192.168.90.81*

- - means: no system status display.  
An empty space must be placed between the - and the identifier.  
**Example:** - *DiVA 1:192.168.90.81*

- **STATUS** means: An abbreviated system information report can be retrieved in the branch manager. The following information, among other things, will be displayed:  
Id no, system name, system time, software version, device reports (eg. System OK or camera error).

A space must be placed between STATUS and the IP address.

An info symbol  appears as a symbol that system information may be displayed via the branch manager.  
For example: \* *DiVApro:STATUS 192.168.90.81*

- After the last character on each line, the button  must be pressed.  
Even after the last line!



## Notice

For a faultless function in the branch manager, the above described entry syntax must be exactly adhered to.

The colours of the status display (red, orange and green) have the same significance as those in the system status information of the user interface (see page 11) .

The status display is not updated until the branch manager is again retrieved, or until the page is reloaded in the browser.  
(In Internet Explorer, this occurs automatically after 8 min.)

3. Confirm the entries by clicking **OK**.

## Invoking branch manager

→ *How to invoke the branch manager:*

1. Start the browser installed on the workstation PC (e.g. Internet Explorer or Firefox).
2. Enter the IP address of the desired system, followed by the entry */links.htm*.

**Example:** *192.168.90.81/links.htm*



**Fig. 24:** *Branch manager*

3. By entering the user name and password and subsequently clicking on the corresponding system you will be logged in.



## Notice

To log in, you will need user name and password for the corresponding system.

The entry fields for the user name and password can be deleted by clicking the **delete** button.

4. To display system information of a system via the branch manager, click on the symbol

5. The most important system information will then be displayed in the upper left of the branch manager. To leave the information display, click outside the information window.



### Notice

System information will only be shown if a user name and password have been entered. These users must be authorised on the system, and possess the user rights for **hardware configuration** and/or **system status enquiries**.

In addition, the systems must be accessible, and must be systems of the new DiVA system platform, and have a software version from 3.05.086 installed.

---



## Creating and displaying reference images

For the monthly performance check in accordance with the German UVV "banks", the image contents from all holdup cameras must be inspected. New reference images can be created with the system every month and compared with available reference images.





### Notice

You can only create and display reference images if the user setup options **set reference images**, **check reference images**, **live images**, **stored images** have been activated for you by the system administrator. Available reference images cannot be deleted, just overwritten!

To create reference images, you will need to be allocated to a live-image group that is authorised to view live images from the reference image camera. Otherwise, the live image from this camera will only be shown for a maximum of two minutes.

## Creating reference images

→ How to create, review and store new reference images:

1. Click on the **Admin./Settings** button  in the main menu  
and on the **reference image** button  in the sub menu.
2. The **reference images** menu is opened.
3. With a simulator create a reference image from all holdup cameras in accordance with the German UVV "banks".
4. For this purpose, select a holdup camera from the **camera** drop-down menu and click on the **live** button. You now see the live image of the camera in the display **live** field.



### Notice

The live image is refreshed every second.

5. Wait until the simulator is positioned at the correct distance by the auxiliary (see Fig. 25)



Fig. 25: Menu reference images

6. To store reference images five storage spaces per camera are available in the **reference image allocation** field.  
Click on the **store reference image 1** button, for example, to store the displayed live image as the first reference image.
7. To print out the image, select this by clicking the small preview image.

8. The selected preview image is displayed in the **reference image display field**.
9. To print out the image click on the **print image** button.
10. A new window is opened in Acrobat Reader, in which the image is displayed in the highest quality. To print the image, use the print dialogue of Acrobat Readers.
11. Review the displayed or printed image according to the following criteria:  
**The defined structures of the simulator (Model C or model 2) must be clearly discernible as single black and white bars.**  
 Correct the camera position or the display window in case the aforementioned conditions are not fulfilled.



### Notice

The reviewed images may not be improved using image editing procedures.

12. For all other holdup cameras installed, create the reference images with the corresponding simulators. Store the images, in each case as reference image for the selected camera name.
13. Finally pass the reference images over to an authorised member of staff from the financial institute so that they can be archived.



## Display reference images

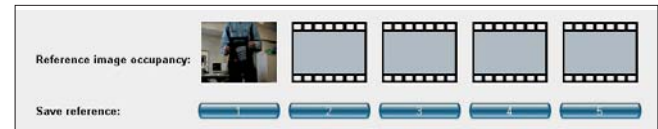


### Notice

You can only view reference images if the admin has enabled the options for **viewing reference images**, **live images** and **saved images** in the user settings for you.

→ *How to let the stored reference images be displayed:*

1. Click on the **Admin./Settings** button  in the main menu  
 and on the **reference image** button  in the sub menu.
2. The **reference images** menu is opened.
3. Select a holdup camera from the **camera** drop-down menu.
4. The stored images are displayed as preview images in the **reference image allocation** field. The most recent reference image created last is surrounded by a red dashed-border box. The creation date is shown for each reference thumbnail image. Moving the mouse cursor over the thumbnail will also show you the time that the image was saved.



5. Click on a preview image.
6. The selected preview image is displayed as a reference image with date/time in the **reference** field.

### Comparing live image with stored reference image

The displayed live image can also be compared with a stored reference image directly on the screen.

→ *How to compare the live image with a stored reference image:*

1. In the **camera** drop-down menu, select a holdup camera.
2. Click on the **live** button to display the live image of the selected camera.



#### Notice

The live image is refreshed every second.

3. Click on the preview image of a stored reference image. The stored reference image is now displayed in the image display field **reference** with date and time. You can now directly carry out the comparison between the live and reference images.

## Securing and exporting system data

Export and secure the set parameters on a data storage medium. The system configuration (system name, camera settings, devices, event allocations) and the authorisations as well the set public holidays, time profiles and multiview profiles can all be protected against loss and overwriting, reproduced and re-imported according to requirements.

### Exporting system configuration



#### Notice

After successfully starting up secure the system parameters on a data storage medium that can be write-protected. Leave the data storage medium with the system parameters directly on site at the customer service area without fail.


Note that all settings which were made in the chapter on **setting up archives** (see page 37) have not been secured. You should therefore make a note of these without fail or print off the configuration information (see page 68).

Also, the Java scripts are not secured and should likewise be secured, e.g. by making notes or using the intermediate save function with a text editor.

→ *How to export the system configuration to a data storage medium:*

1. Click on the **Admin./Settings** button  in the main menu


and on the **download** button  in the sub menu.

2. Click on the **configuration download** button 
3. Choose **save file** .... (can vary according to the browser being used).
4. Select a file path or data storage medium.
5. Save the system parameters file (DIVA.cfg) under the system name.

### Exporting user rights

The user parameters (user names and rights) can be exported to a data storage medium in order to secure them or import them to another system if necessary.


→ *How to export the authorisations to a data storage medium*

1. Click on the **download user rights** button 
2. Choose **save file** .... (can vary depending on browser used).
3. Choose a file path or data storage medium.
4. Save the authorisations file (user.cfg) under a distinct name

## Exporting holidays

The holiday settings can be exported to a data storage medium in order to secure them or import them to another system if necessary.


→ *How to export the public holiday settings to a data storage medium:*

1. Click on the **download holidays** button 
2. Choose **save file** .... (may vary depending on browser used).
3. Choose a file path or data storage medium.
4. Save the public holidays file (holidays.cfg) under a distinct name

## Exporting time profiles

Time profile configurations can be exported to a storage device for data backup or importing on another system, as required.


→ *How to export time profile configurations to a storage device:*

1. Click on the **download time profiles** button 
2. Select **Save as...** (may vary depending on your browser)
3. Select a storage path or storage device.
4. Save the time profile file (timeprofiles.cfg) using a unique filename.

## Exporting multiview profile

The multiview profiles configuration can be exported to a data storage medium in order to secure them or import them to another system if necessary.

→ *How to export the multiview profiles configuration to a data storage medium:*

1. Click on the **download multiview profiles** button 
2. Select **Save as...** (may vary depending on your browser)
3. Select a storage path or storage device.
4. Save the multiview profile file (multiviewprofiles.cfg) using a unique filename.

## Exporting the internal system log file

An internal system log file can be exported for troubleshooting purposes.

However, you should only do this in consultation with the hotline.

## Importing secure system data



### Warning

Before uploading the system parameters, ensure that you have knowledge of the user identification of the system configuration to be imported (e.g. name and password of the system administrator to be imported).



### Warning

After performing a restart, you must enter the user name and password which were provided in the system configuration to be imported. Ensure that you have knowledge of this user identification (e.g. name and password of the system administrator to be imported).

→ *How to import the system configuration secured on the data storage system, authorities, public holidays:*

1. Click on the **Admin./Settings** button  in the main menu

and on the **upload** button  in the sub menu.



The image shows a button labeled 'Upload' on the left and a search field on the right with a 'Durchsuchen...' button next to it.

2. Click on the **browse...** button.
3. Select the desired parameter file from the data storage medium.



### Notice

The system can tell apart the types of parameters (system, user, holidays or multiview profile) by means of the file

4. Click on the **OK** button.
5. Confirm the message, which appears after the system parameter file, user parameter file or public holidays file has been loaded, with **OK** in order to activate the parameters.
6. After browsing, confirm the message with **OK**.

## Carrying out software update

To profit from software improvements and new functions, the procedure for carrying out software updates has been deliberately designed in a simple manner.

---





### Warning

Before carrying out a software update secure the system and user parameters on a data storage medium (e.g. diskette or similar)

---

→ *How to carry out a software update:*

1. Click on the **Admin./Settings** button  in the main menu  
  
and on the **upload** button  in the sub menu.
2. Click on the **browse** button.
3. Select the file (\*.upd) with the software update from the corresponding storage medium.
4. Confirm the entry with **OK**.
5. Confirm the message, which appears after loading the software update, likewise with **OK in order to** finally carry out the update.
6. After carrying out the update confirm the message with **OK**.



### Notice

A software update last approx. 1 minutes.

---

## Network setup

You can deal with various settings for the network.

<b>Default gateway</b>	
Host IP/Name:	<input type="text" value="10.10.2.90"/>
<b>HTTP Port</b>	
HTTP Port:	<input type="text" value="8088"/>
<b>Network speed limitation</b>	
Netw. speed limit ( bytes/sec. ):	<input type="text" value="500000"/>
<b>Network adaptor for external devices</b>	
Network adaptor:	<input type="text" value="eth1.0"/>
Range start:	<input type="text" value="192.168.98.10"/>
Range end:	<input type="text" value="192.168.98.100"/>

**Fig. 26:** Menu **Network setup**

### Default Gateway

The system can be assigned a **host/IP name**. The system can then be recognised as a server under this name in a Windows network.

### HTTP Port

The port number for the HTTP server is entered here (standard value = 8088).




### Network speed limitation (Bytes/sec.)

A value for the limit of the net load can be entered. The net load of the system can be limited to 199 Bytes/sec, even for users from other subnets.

### Network adaptor for external devices

An IP address pool can be determined for configured network adaptors for external devices, which the system grants if network capable devices are connected.

→ *How to set the network:*

1. Click on the **Admin./Settings** button  in the main menu
- and on the **upload** button  in the sub menu.
2. Click on the **options** button  to change general network settings.
3. Under **host/IP name**, assign a name to the system so that it can be recognised as a server in a network.
4. In the field **network speed limit**, enter the size of the reduction.
5. If necessary, configure the IP address pool of the network adaptors for additional devices.
6. Confirm the entries by clicking on **OK**.





## Notice

If the net load limit is to be effective for a user, then the **net load limit** entry in the **user setup** dialogue must be activated. If this is the case, then the registration procedure at the module is delayed until the user and password are checked. The network settings first become active after restarting.

## Restarting the system


After changes have been made to the system (e.g. changes of the network settings or for maintenance works), the system must be restarted.



## Notice

You can only access the **Restart** menu item if the system administrator has activated the **Hardware configuration** option in the user installation for you. A system restart is not possible during an alarm recording.

→ *How to restart the system:*

1. Click on the **Restart** button  in the main menu
2. You will be asked if you really want to restart the system.
3. Click **OK**. All users will now be logged off automatically. Subsequently, the system will be restarted. This may take up to 4 minutes.





## Notice

The image recording is interrupted during the restarting process.

## Logging out of the system





You also have the option of logging out of the system manually.

→ *How to restart the system:*

1. Click on the **Logout** button  in the main menu.
2. Confirm the message by clicking **OK**. All users are automatically logged out. The system is subsequently restarted.
3. Alternatively you can log out of the system by closing the browser window. Simply close the browser window by clicking . No security request takes place here!.

## Viewing system status information

All relevant system information is automatically collected and stored on the hard drive of the module. The system status information is divided into four blocks.



-  The white area contains general information about the system..
-  The red area contains information about severe errors in the system.
-  The orange area contains information about locked recording archives and pre/post alarms.
-  The yellow area contains information about errors in the system which, although not severe, nonetheless need to be observed.



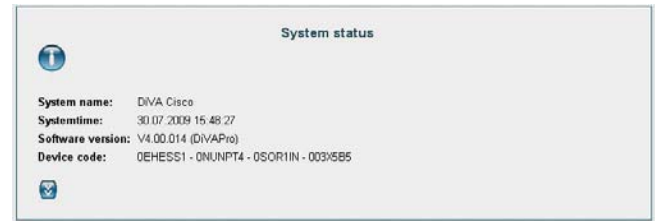
### Notice

You can only view the system status information if the **view system status** and/or **hardware configuration** user setup options have been activated for you by the system administrator.



→ How to view the system status information:

1. Click on the **Status/Systeminfo** button  in the main menu and on the **system status** button  in the sub menu or click on the system status display (traffic light). The system status information is displayed.

2. The white section is displayed in long form by default. If errors occur in the system, then these are displayed in the red, orange or yellow section; the white section then appears in shortened form.



**Fig. 27:** General system status in shortened form.

3. To see the extended status information of the white section (see Fig. 28), click on the button . To close this again, click on the button .
4. To leave the system status information, click on any item in the navigation bar.

### System status information displayed in the white area in shortened form:

- System name
- System time
- Software version
- Device code

# Start-up and administration

System status information displayed in the white area in extended form:

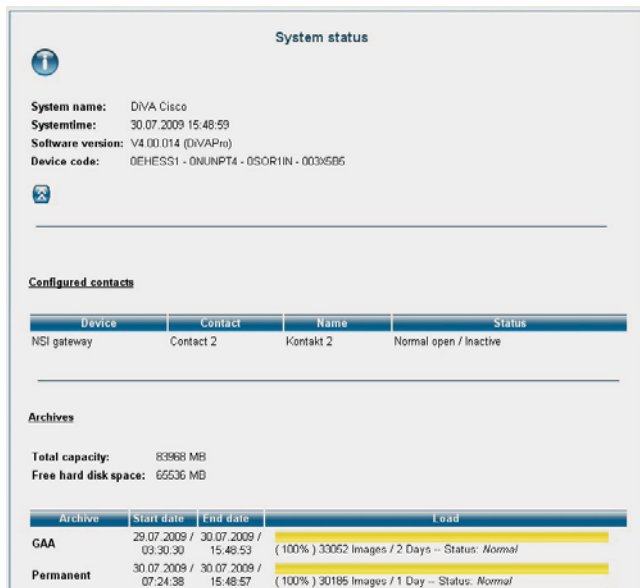


Fig. 28: General system status in extended form.

- All statements from the shortened form.

Statements about the status of the configured contacts:

**Device, contact, name, status:**

The status shows whether the contact was configured as breaker or maker and whether this is active or inactive.

Statements about the archives:

**total capacity and available free hard disk space:**

This shows how full the system hard drive is.

**Start date:** Point in time for the first recorded image on the archive.

**End date:** Point in time for the last recorded image on the archive.

**Load:**

**Yellow:** Used part of the track with percentage statement of the load, statement of the time period in days in which the track was used and statement about the recorded images.

**Green:** Unused part of the track

**Orange:** Locked alarm archive and/or pre/post alarm archive.

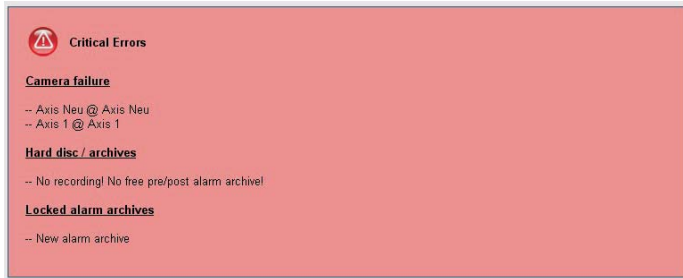
**Archive status:**

Alarm archive locked, Alarm triggered, Normal, Active, Free or Alarm locked.

**Pre/Post alarm archive status:**

**Normal:** No pre/post alarm recordings are being carried out.

## System status reports in the red area



**Fig. 30:** System status info in the red area

### Hard drives/archives

This shows whether alarm recordings are running or for displayed reasons cannot run:

- No alarm recording! No free track!

### Locked alarm archives

This lists alarm archives locked after an alarm recording. These must be enabled for a new recording.

### Camera error

Here cameras are listed which have a fault.

### Device error

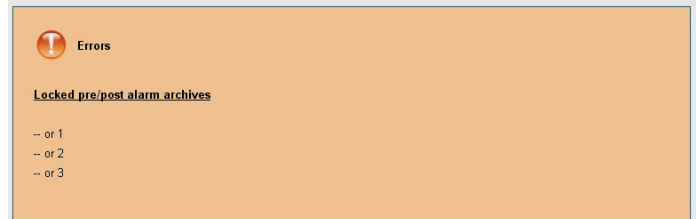
Here devices are listed which have a fault.



### Warning

If a fault is permanently displayed, then customer service should be informed.

## System status reports in the orange area:



**Fig. 29:** System status info in the orange area

### Hard drives/archives

This shows if pre/post alarm is on.

### Locked pre/post alarm archives

This lists pre/post alarm archives locked after an alarm recording. These must be enabled for a new recording.

### Archives for which alarms are triggered

Alarm archives for which an alarm is triggered are displayed here.

## System status reports in the yellow area:

### Device info

- If no transaction data has been transferred at a data interface for 23 hours, then this is displayed with the name of the data interface and the protocol.



### Notice

Note that the system status information is only a snapshot of the system and is not automatically refreshed.

---

## Viewing configuration information

All relevant, **configurable** system data are automatically collected and stored on the hard drive of the module.

The following information is displayed (see Fig. 32 and 31):

- **General system information**  
system name, system time, software version, device code
- **Network configuration**  
HTTP Port, Host name,
- **Hard drive information:**  
Total space, free space
- **Statements about the configured archives**  
Name, load, archive size, start date, end date, time period, type, status
- **Statements about the event allocations of the archives**  
archive name, event, address, camera allocation, delay, interval, images, time control.
- **Statements about connected cameras**  
Connection, Name of the camera, device to which the camera is connected, whether live images may be invoked, quality of the camera images.
- **Statements about the connected devices.**  
Device type; name of the device; software version of the device (if available); additional information
- **Configured contacts**  
Device, contact, name, status, event type
- **Group**  
Group name, live images allowed for cameras listed, available archives





- **Time profiles** (prprofile name, days, time period (from ... to))
- **Holiday profiles**  
Name, profiles in use
- **Multiview profiles**  
Name, used cameras, resolution, interval




### Notice

You can only view this configuration information if the **view system information** user setup option has been activated for you by the system administrator.

→ *How to can view the configuration information:*

1. Click on the **Status/Systeminfo** button  in the main menu and on the **config info** button  in the sub menu
2. To print out the configuration information click on the button  .  
(Recommended printer setting: DIN A4 landscape format).
3. To leave the configuration information again, click on the button .

**System configuration**



**System**

System information	
System name:	DIVA Cisco
Systemtime:	04.08.2009 16:28:28
Software version:	V4.00.014 (DIVAPro)
Device code:	0EHESS1 - 0NUNPT4 - 0SOR1N - 003x5B5

---

**Network**

General	
HTTP Port:	8080
DIVA Hostname:	-----

---

**Hard drive**

Harddisk info	
Total capacity:	83968 MB
Free hard disk space:	77312 MB

---

**Archives**

Archive	Images	Archive size	Start date	End date	Time range	Category	Status
1) GAA	44221 (100%)	1000 MB	02.08.2009 / 16:01:45	04.08.2009 / 16:28:23	3 Days	Standard	Normal

---

**Event selection**

Archive 1: GAA

Trigger event	Address	Camera selection	Delay	Interval	Images	Time control
ATM portrait	IBM APBI V2	Axis 210	00:00:00	00:01:00	2	open
ATM cash dispenser	IBM APBI V2	Axis 210	00:00:00	00:01:00	2	open

---

**Connected cameras**


Connection	At device	Name	Live	Quality
	MediaServer	Axis 210	yes	-----

Fig. 32: Configuration information part 1

**Connected devices**

Devicetype	Name	Version	Information
Mediaserver	MediaServer	-----	-----
NSI Gateway	NSI gateway	-----	-----
Protocol	IBM APBI V2	IBM_APBI_V2	( Last recording: 04.08.2009 16:28:23 )

---

**Configured contacts**

Device	Contact	Name	Status	Event category	User trap
NSI gateway	Contact 1	Kontakt1	Normal close / Inactive	-----	-----
NSI gateway	Contact 2	Kontakt2	Normal close / Active	-----	-----

---

**Time profiles**

Profile 1: geschlossen

Days	From	To	From	To	From	To
Monday	00:00	00:00	00:00	00:00	00:00	00:00
Tuesday	00:00	00:00	00:00	00:00	00:00	00:00
Wednesday	00:00	00:00	00:00	00:00	00:00	00:00
Thursday	00:00	00:00	00:00	00:00	00:00	00:00
Friday	00:00	00:00	00:00	00:00	00:00	00:00
Saturday	00:00	00:00	00:00	00:00	00:00	00:00
Sunday	00:00	00:00	00:00	00:00	00:00	00:00
Holiday_1	00:00	00:00	00:00	00:00	00:00	00:00
Holiday_2	00:00	00:00	00:00	00:00	00:00	00:00
Holiday_3	00:00	00:00	00:00	00:00	00:00	00:00
Holiday_4	00:00	00:00	00:00	00:00	00:00	00:00

Profile 2: offen

---

**Licensefeatures**

Feature	Standard features
Mediaserver	yes
NSI gateways	10
Protocols	10
Image journal	yes
Pre/post alarm archive	yes
Branch manager	yes



Fig. 31: Configuration information part 2

## Viewing log file




All login procedures and error messages, e.g. camera fault, are stored in a log file (see Fig. 33).



### Notice

You can only view the log file if the **view log file** user option has been activated for you by the system administrator.

→ *How to view the log file:*

1. Click on the **Status/Systeminfo** button  in the main menu and on the **logfile** button  in the sub menu
2. To leave the configuration information again, click on the button .

System name: DIVA Cisco

```

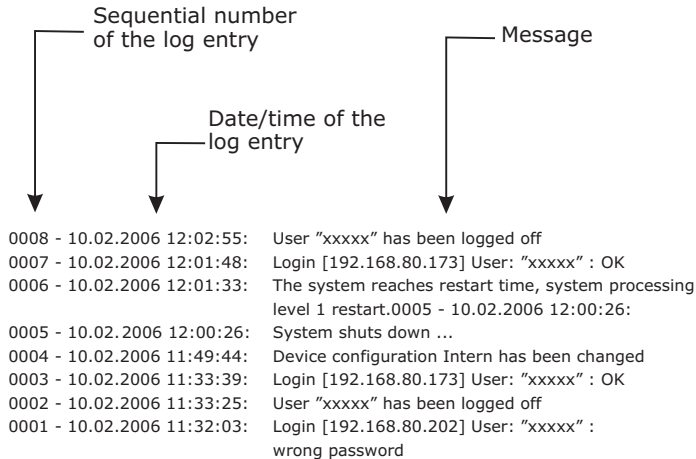
0197 - 05.08.2009 10:52:50: User admin: Pre/post alarm archive Alarm1 reset
0196 - 05.08.2009 10:52:01: Alarm set on archive Alarm1
0195 - 05.08.2009 10:52:00: User admin: Pre/post alarm archive Alarm1 reset
0194 - 05.08.2009 10:51:31: Login [192.168.99.250] User: admin : OK
0193 - 05.08.2009 10:47:52: User "admin"has been logged-off.
0192 - 05.08.2009 10:44:32: Login [192.168.99.250] User: admin : OK
0191 - 05.08.2009 05:00:12: Alarm set on archive Alarm1
0190 - 05.08.2009 05:00:10: The system reaches restart time, system processing level 1 restart.
-----
0189 - 04.08.2009 18:30:19: User "admin"has been logged-off.
0188 - 04.08.2009 18:28:24: Login [192.168.99.250] User: admin : OK
0187 - 04.08.2009 17:47:01: User "admin"has been logged-off.
0186 - 04.08.2009 17:38:49: Login [192.168.99.250] User: admin : OK
0185 - 04.08.2009 17:33:18: User time out admin was logged-off due to an user time out.
0184 - 04.08.2009 17:22:12: Login [192.168.99.250] User: admin : OK
0183 - 04.08.2009 17:09:33: User time out admin was logged-off due to an user time out.
0182 - 04.08.2009 16:59:30: Login [192.168.99.250] User: admin : OK
0181 - 04.08.2009 16:56:44: User time out admin was logged-off due to an user time out.
0180 - 04.08.2009 16:46:42: Login [192.168.99.250] User: admin : OK
0179 - 04.08.2009 14:02:35: User "admin"has been logged-off.
0178 - 04.08.2009 13:59:23: User admin: Event selection Alarm1 changed
0177 - 04.08.2009 13:59:12: User admin: Event selection Alarm1 changed
0176 - 04.08.2009 13:58:47: User admin: Create new archive
0175 - 04.08.2009 13:57:43: Login [192.168.99.250] User: admin : OK
0174 - 04.08.2009 13:56:03: System started (V4.00.014)
0173 - 04.08.2009 13:55:47: Login [192.168.99.250] User: admin : OK
0172 - 04.08.2009 13:55:46: User admin: Archive Alarm1 deleted
0171 - 04.08.2009 13:47:57: User admin: Event selection Alarm1 changed
0170 - 04.08.2009 13:45:42: Login [192.168.99.250] User: admin : OK
0169 - 04.08.2009 12:45:32: User time out admin was logged-off due to an user time out.
    
```

**Fig. 33:** Logfile



## Log file messages

### Example for configuration result:



### Other possible log file messages:

**Message:** 0003 - 10.06.2006 12:26:20:  
Error occurred: camera 2b defect  
0002 - 10.06.2006 12:25:37:  
Error occurred: camera 1a fault  
Cameras have a fault

**Meaning:**

**Message:** 0005 - 10.06.2006 12:33:33:  
Error removed: Camera 2b  
0004 - 10.06.2006 12:33:26:  
Error removed: Camera 1a

**Meaning:** Cameras are running without fault again

**Message:** 0008 - 10.06.2006 13:00:20:  
Error occurred: gateway GAA1 MSB0  
Error removed: gateway GAA1 MSB0  
Gateway GAA1 MSB0 has a fault

---

### Meaning:



#### Notice

If the address of the NSI Gateway is changed during operation, the error also occurs!  
Pulling out the ATM plug from the gateway does not lead to an error message.

---

If the system network plug is pulled out during operation, no error message will appear. If the network plug is pushed back in, then the following message appears:

0025 - 10.06.2006 13:57:41: System has started

---



#### Notice

If during operation the system is disconnected from the network and subsequently re-connected, then no error message appears.

---

**Message:** 0098 - 07.06.2006 13:45:23:  
Alarm triggered on track alarm

**Meaning:** A fault contact has triggered an alarm on the "alarm" track and an alarm has been recorded.

**Message:** 0099 - 07.06.2006 13:55:45:  
Locked alarm track alarm has been enabled.

**Meaning:** The alarm track has been evaluated and subsequently enabled for the next alarm recording.  
All images have been deleted.

- A**
- Acrobat Reader.....10
  - address .....44
  - administrator .....15,20
  - administrator password .....15
  - adress.....42
  - after Alarm .....38
  - alarm .....6,37,46,48
  - alarm recording .....10
  - alarm track .....44
  - Archive .....6
  - Archive name.....46
  - ATM.....6
  - ATM cash dispenser.....41
  - ATM portrait.....41
- B**
- before alarm .....38
  - Blocked users.....24
  - branch manager.....52,54
  - buttons .....18
- C**
- camera error.....67
  - cameras .....46
  - changing user rights.....23
  - cleaning .....9
  - Cleaning the cameras.....9
  - cleaning the device .....9
  - configuration information ....69
  - Configuration switch.....18
  - configure a new track.....39
  - Configure holiday profiles .....28
- D**
- Configuring protocols .....33
  - contact.....41
  - creating reference images...56
- D**
- date format.....25
  - delay .....42
  - Deleting devices .....30
  - deleting users .....23
  - device .....42
  - device error .....67
  - DHCP.....6
  - display reference images ....57
  - displaying reference images 56
  - DiVA Hostname .....63
  - DNS.....6
  - Download image archive ....18
- E**
- EEC .....6
  - enabling alarm .....48
  - event .....6,41
  - existing time profile .....27
  - Exporting multiview profile..60
  - exporting public holidays ....60
  - Exporting user rights .....59
- G**
- general system settings .....25
- I**
- image .....43
  - image display field .....18
  - image search menu.....18
  - images after suspicion trigger .....46
  - Important.....8
  - importing secure system data .....61
  - Info/Status .....21
  - internal satellite .....6
  - interval .....44,47
  - invoking branch manager...54
  - IP address .....13,15,52
- L**
- language .....25
  - Live images .....21
  - log file messages .....72
  - logfile.....21
  - login .....20
  - login procedure .....15
- M**
- MediaServer.....31
  - Multiview profiles.....50
- N**
- Name .....37 - 38
  - net load.....63
  - Network adaptor.....63
  - network setup .....63
  - Network speed limitation ....20
  - NSI .....6
- P**
- password.....20
  - Passwort für Alarmabbruch .46
  - permanent.....41
  - power supply .....11
  - preview image.....57
  - Print image .....18
  - product activation .....13
  - Protocol.....11
  - protocol editor.....35
- R**
- recorder .....6
  - reference image allocation ..56
  - Restarting the system .....64
  - ring buffer .....6
- S**
- secure the set parameters .59
  - security advice.....7
  - Service-Hotline.....1
  - Setting holiday profiles .....28
  - setting up branch manager .52
  - setting up tracks.....37
  - single images forwards/backwards.....18
  - software update .....62
  - Software-Update .....62
  - start search .....18
  - stop automatic image search .....18
  - suspicion .....38,46 - 47
  - suspicion interval.....46
  - system description.....5
  - system name .....25

# Index

system parameters .....15  
system status information...65

## T

target groups .....7  
time control.....43 - 44  
time format.....25  
Time profiles .....27  
Tools-Buttons.....18  
track type PAT.....46  
traffic lights .....11  
transaction data field.....18

## U

UPS .....11  
user groups .....24  
user interface .....17 - 18  
user name.....15,20  
user rights .....22  
User rights.....20

## V

viewing log file .....71  
visual status information.....11

## W

workstation PC .....11



**Publisher:**

Cisco Systems GmbH  
Am Söldnermoos 17

85339 Hallbergmoos

Art.-No. KB313