

Building Integration System V5.0

Table of contents

1	Using Help	6
2	General tips for BIS operators	8
2.1	Working with right-mouse-button menus	8
2.2	Customized and optional components	8
2.3	Regarding operators and authorization levels	8
3	System Overview	10
3.1	BIS single server systems	10
3.2	BIS multi-server systems	11
4	Logging On and Off	14
4.1	Logging onto BIS	14
4.2	Changing an operator password	14
4.3	Viewing updated interface pages	14
4.4	Logging off BIS	15
4.5	Forced restart due to configuration change	15
5	The Screen Display	19
5.1	Standard Screen Elements	19
5.2	Navigation Buttons	20
5.3	Message Display Field	21
5.4	Tool Bar	21
5.5	Location Tree	23
5.6	Additional Displays	24
5.7	BIS Smart client	25
5.7.1	Standard screen elements	25
5.7.2	Differences	26
6	Displaying Documents	28
6.1	Document Display	28
6.2	Location Overview/Location Plans	28
6.3	Layers	31
6.4	Zoom and Pan	32
6.5	Device Overview	33
6.6	Action Plans	37
6.7	Miscellaneous Documents	38
7	BIS Message Processing	39
7.1	Processing a BIS message	39
7.2	Standard features of a message	39
7.3	Optional/configurable features of a message	42
7.4	Notes on Workflow processing	42
7.5	Notes on deleting messages	42
7.6	Using the mobile client	43
7.6.1	Prerequisites and HTTPS certificates	43
7.6.2	Settings	44
7.6.3	Connecting the mobile client to the BIS server	45
7.6.4	Adding a shortcut icon to the screen of your mobile client	45
7.6.5	Logging out of the mobile client	46
7.6.6	Viewing, accepting and deleting messages	46
7.6.7	Push notification	46
7.7	Message processing in the Smart client	47
8	Using the BIS Smart Client	48






8.1	Logging in and out	48
8.1.1	Logging in to BIS	48
8.1.2	Logout of BIS	48
8.2	Changing password	48
8.3	Changing the interface language	49
8.4	Connection to BIS server	49
8.5	The screen display	49
8.5.1	Standard screen elements	49
8.5.2	Side navigation	50
8.5.3	Dashboard	51
8.6	Manual backup of workspaces and dashboards	52
8.7	BIS alarm processing	53
8.7.1	Processing an alarm	53
8.7.2	Standard features of an alarm	53
8.7.3	Searching for specific alarms	55
8.7.4	Filtering alarms	55
8.7.5	Action plans of an alarm	56
8.7.6	Notes on accepting and deleting alarms	56
8.8	Location overview	57
8.8.1	Purpose of the location overview	57
8.8.2	Patterns of the detector symbols	58
8.8.3	Giving commands to a selected detector	58
8.8.4	View or hide map layers	58
8.8.5	Viewing multiple maps	59
8.8.6	Map navigation aids	59
8.9	Devices overview	60
8.9.1	Purpose of the devices overview	60
8.9.2	Searching for specific devices	60
8.9.3	Giving commands to a selected device	61
8.9.4	Working with subdevices	61
9	Control	62
9.1	Controlling with BIS	62
9.2	Controlling from the Location Tree	62
9.3	Controlling from the Location Graphic	62
9.4	Controlling from the Device Overview	62
9.5	Controlling from an Action Plan	63
9.6	Controlling with Action Buttons	63
10	Operator Alarms	64
10.1	Operator Alarms	64
10.2	How to Trigger an Operator Alarm	64
11	Simulated Alarms	65
11.1	Simulated Alarms	65
11.2	How to Trigger a Simulated Alarm	65
12	Printing	67
12.1	Printing with BIS	67
12.2	Log Printing	67
12.3	Alarm Printing	67
12.4	Printing Manually	68
13	Sending Messages to Operators	69

13.1	Sending Messages to Operators	69
14	Event Log	71
14.1	Event Log contents and backup	71
14.2	Event Log User Interface	72
14.3	Managing Filters	73
14.4	Using Filters	75
14.5	Using Reports	76
15	Event Log Filters	79
15.1	Filter Overview	79
15.2	Filter Address	80
15.3	Filter Attributes	81
15.4	Filter Date/Time	82
15.5	Filter Event Type	84
15.6	Filter States	85
15.7	Filter Operators	85
15.8	Filter Access Control	86
15.9	Filter Visible Columns	88
	Glossary	90

1 Using Help




How to use this help file.

Tool bar buttons

Button	Function	Description
	Hide	Click this button to hide the navigation pane (Contents, Index and Search tabs), leaving only the help pane visible.
	Show	When the Hide button is clicked it is replaced by the Show button. Click this button open the Navigation pane.
	Back	Click this button to move back through the chain of topics most recently viewed.
	Forward	Click this button to move forward again through the same chain of topics
	Print	Click this button to print. Choose between "Print the selected topic," and "Print the selected heading and all subtopics".

Tabs

Contents

This tab displays a hierarchical table-of-contents. Click a book icon  to open it  and then click on a topic icon  to view the topic.

Index

This tab displays an index of terms in alphabetical order. Select a topic from the list or type in a word to find the topic(s) containing it.

Search

Use this tab to find any text. Enter text in the field and then click button: **List Topics** to find topics that contain all the words entered.

Resizing the help window

Drag the corner or edge of the window to the desired size.

Further conventions used in this documentation

- Literal text (labels) from the UI appears in **bold**.
E.g. **Tools, File, Save As...**
- Sequences of clicks are concatenated using the > character (the greater-than sign).
E.g. **File > New > Folder**
- Changes of control-type (e.g. menu, radio-button, check box, tab) within a sequence are indicated just before the label of the control.
E.g. Click menu: **Extra > Options > tab: View**
- Key combinations are written in two ways:

- <Ctrl> + <Z> means hold down the first key while pressing the second
- <Alt>, <C> means press and release the first key, then press the second
- The functions of icon buttons are added in square brackets after the icon itself.
E.g. [Save]

2 General tips for BIS operators

2.1 Working with right-mouse-button menus

You can activate a number of BIS displays, selections, and control functions in the operator interface using the right mouse button.

Use the right mouse button especially to trigger control functions (for example, detector reset, user alarm, and so on). Place the mouse pointer on one of the following elements:

- A certain location in the location tree (the selected control command for all detectors in your location's floor plan.
- An entry in the right-hand window of the devices overview
- A detector symbol for a floor plan in the locations overview



Notice!

The functions of the right mouse button depend on the configuration, scope of the system, and authorization level of the current operator. Different functions may be available to different operators.

2.2 Customized and optional components

This online help describes all BIS standard controls and their behavior. It is nevertheless possible for system administrators to create a BIS user interface that differs significantly from the default UI. Please contact your system administrators for documentation of highly customized BIS interfaces.

2.3 Regarding operators and authorization levels

Operation on Workstation PC

Only one BIS operator at a time can log on at a workstation PC. BIS can be configured so that one operator can log onto the system at several workstation PCs simultaneously.

Any number of operators per system can be configured. It is advisable, however, that not more than 10 operators log on simultaneously. A higher number of simultaneous operators will degrade system performance.

Operation from the BIS Login Server

Operators can also log onto the system at the login server PC directly. BIS works equally well from an operator workstation as from the server PC.

System Check

Operators who are logged onto the system can be identified via the device overview.

BIS can automatically trigger a message or execute an action when the last operator logs off the system.

Authorization Levels

BIS can be configured with any number of authorization levels.

Each authorization level can be customized for efficient message processing and safety administration.

Authorization levels govern the following:

- Control commands
- Individual addresses or address ranges
- Messages that are assigned according to specific states
- Configuration functions. Every page in the configuration has an individual authorization. An operator can be authorized, for example, to configure new detectors, but not new users.

Dual Authentication

For each authorization level it is possible to define whether dual authentication is required (i.e. whether two user logons are required to gain access to the system). In such cases, after the first authorized user has logged on, a second login window appears for a different user of the required authentication level.

3 System Overview

Building Integration System (BIS) is a comprehensive browser-based building management solution. It combines access control, building safety (fire, intrusion) and site-monitoring (CCTV) systems in a single user interface. Developed according to OPC (Open Platform Communications*) standards, BIS easily integrates OPC-compliant systems.

***) Note:** This is the new definition of the OPC acronym by the OPC foundation, as of November 2011.

System topologies: single vs. multi-server

- A **BIS single server system** contains one computer called the BIS Login Server, also known simply as the BIS server.
 - Each BIS server can act as a communications hub for zero or more connection servers and database servers, which are separate computers.
 - Either the BIS server runs OPC and database server software by itself, or this software runs on separate connection and database server computers. **Note:** As long as there is only one BIS server, the system is known as a single server system.
- A **BIS multi-server system** is where two or more BIS single-server systems cooperate in a network
 - The individual BIS servers in the network can be providers or consumers of each other's data, or both provider and consumer simultaneously.
 - Thus a multi-server system can be hierarchical or peer-to-peer in its structure.

3.1 BIS single server systems

Definition

A single server BIS system contains only one BIS login server (also known as the BIS server). It may run OPC servers itself, and it may contain zero or more Connection servers and Database server computers.

Illustration

BIS installations vary enormously in size and complexity. The following illustrates a small and a complex BIS single-server installation.



Figure 3.1: A small single server BIS system

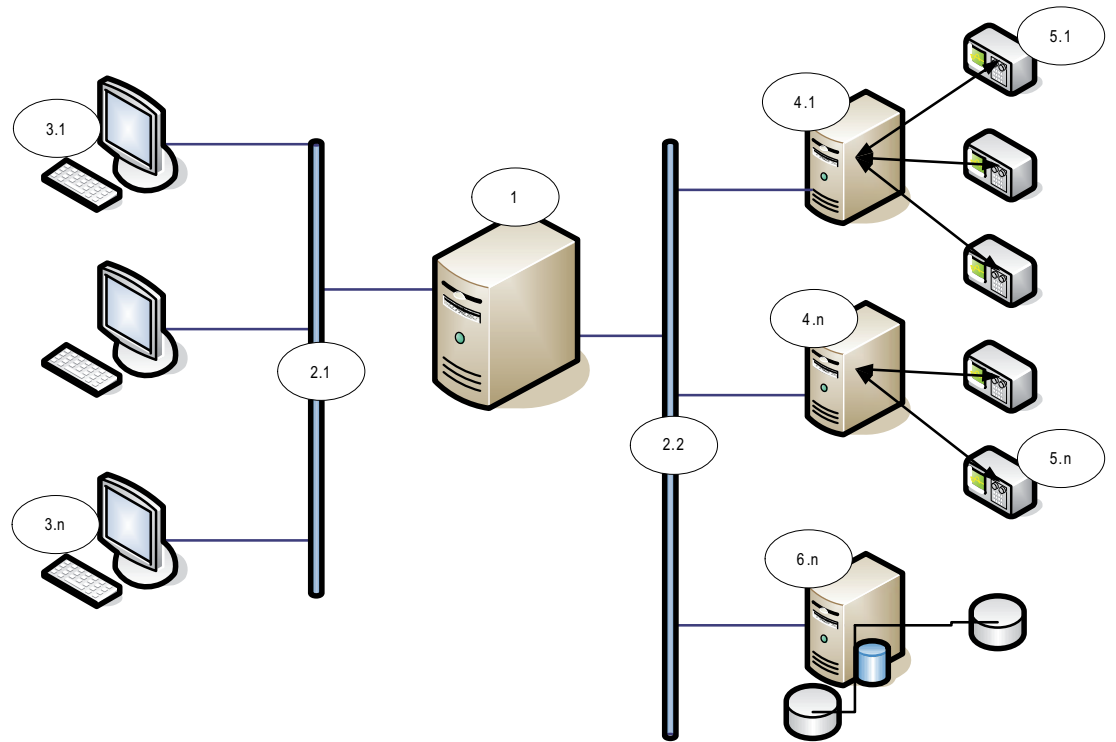


Figure 3.2: A complex single server BIS system

No.	Name	Function
1	BIS (Login) server	Runs the BIS application. The BIS server functions as an OPC client
2.1 to 2.n	Network(s)	Carries signals
3.1 to 3.n	BIS Client Workstation(s)	Runs the BIS user interface
4.1 to 4.n	Connection server(s)	Runs OPC server processes
5.1 to 5.n	OPC device(s)	Interacts with the outside world
6.1 to 6.n	Database server	Hosts BIS data for event log and engines

3.2 BIS multi-server systems

Definition

A multi-server BIS system is one in which two or more BIS single server systems share information. BIS multi-server systems can be organized as hierarchical or peer-to-peer networks.

Implementation overview

Participating BIS single-server systems can be providers of information, consumers of information, or both simultaneously.

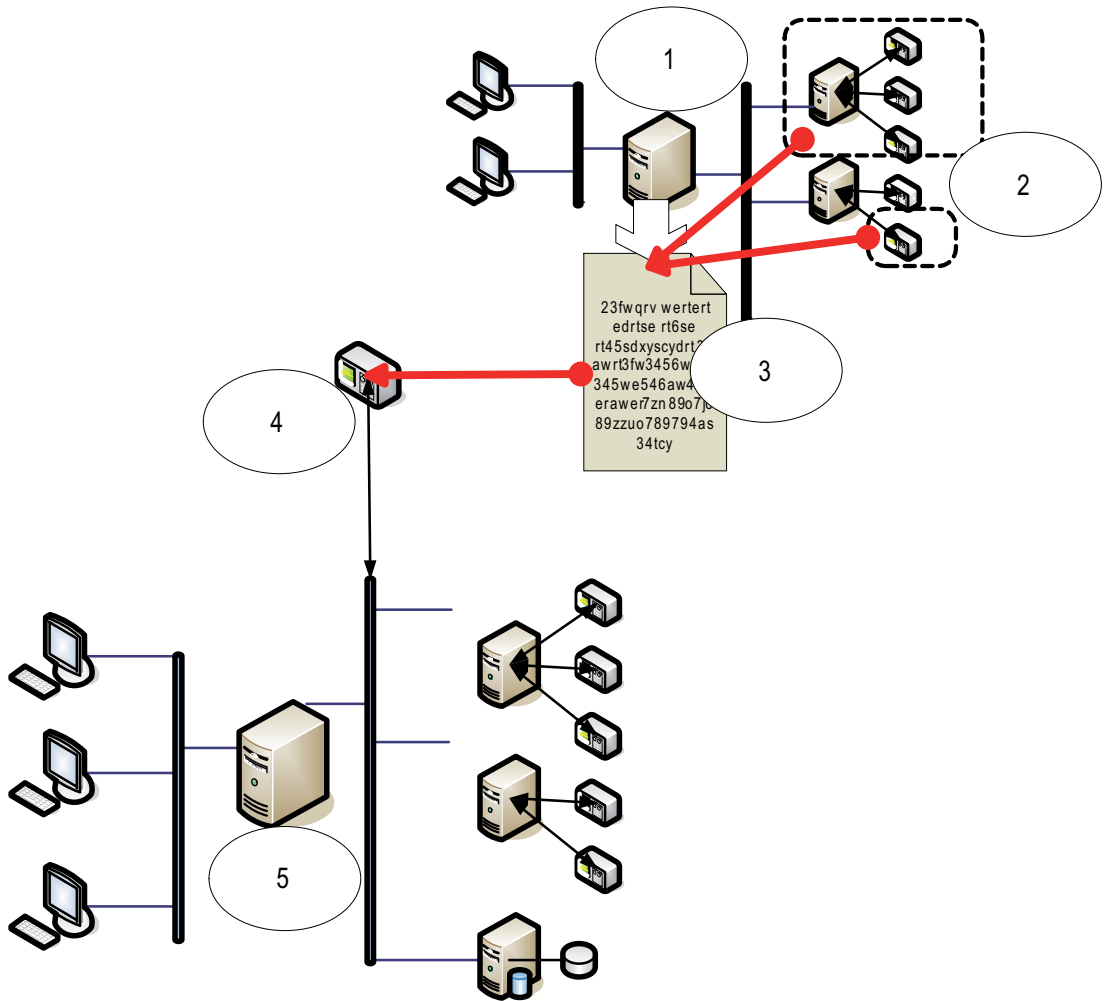
- The Provider server creates a configuration file that details exactly which information it should share with others.

- The Consumer server configures and browses the provider server as a remote OPC server.

Any or all of the information monitored by the provider can be passed to the consumer or consumers. Typically the information consists of OPC addresses, state-changes, commands and alarms.

Illustration

For simplicity, the following illustrates the interaction of one provider and one consumer server. The size and complexity of the multi-server BIS system is limited by the network traffic and the capacity of the consumer servers to process incoming data.



No.	Name	Function
1	The provider server	A kind of BIS server that provides information to other BIS single server systems
2	The subset of the addresses that the provider server should share	
3	The encrypted configuration file generated by the provider server	Describes the subset of information that the provider server should share

No.	Name	Function
4	An OPC server of type BIS Remote System	Acts as an interface between the provider server and the consumer server. It is configured on the consumer server using the encrypted configuration file, and then browsed like any other connection server.
5	The consumer server	This BIS server receives and processes information from its own devices, and those of connected provider servers

4 Logging On and Off

4.1 Logging onto BIS

If your system is not configured so that starts BIS automatically, perform the following procedure to log onto BIS from the workstation PC:

1. Start the Internet Explorer browser. If your administrator configured the home page of your browser to be BIS, then the BIS logon screen appears immediately. If not, enter the address of the BIS logon server as follows: `https://<Name of the BIS server>`
2. Enter your Operator name and password in the window and click the **OK** button. The entries are validated by the logon server, and the server checks your authorization level. The server then sends the start page to your workstation PC. The start page can vary depending on your authorization level.
If your BIS system uses **Windows authentication**, entering name and password may not be necessary.
If dual authentication is in operation a second login window appears for the second operator.

4.2 Changing an operator password

Prerequisites

The following procedure is for systems configured to use **BIS** authentication.

If your Windows and BIS passwords are identical, it is likely that the system is using **Windows authentication**. In this case, you can change your password in Windows, by pressing **CTRL-ALT-DEL** and clicking the **Change Password...** button.

Procedure

Perform the following procedure to change your operator password:

1. Start the Internet Explorer browser. The browser should be configured with BIS as the home page. If not, enter the address of the BIS logon server as follows:
`https://<Name of the BIS server>`
2. Enter your operator user name and password when prompted.
This is required in order to fetch the password policy from the BIS server.
3. Click the **Change password** button. In the Change password window, enter your operator name, old (current) password, and your new password twice.
4. BIS confirms that the password has changed.
Log onto BIS using your new password.

Notice!

This procedure only changes the password for the current operator's BIS user interface. It has no effect on the Configuration Browser passwords. For information on changing those passwords, please refer to **Changing the Configuration Password** in the **BIS Configuration online help**.

Please note: The password is case-sensitive, whereas the operator name is not.



4.3 Viewing updated interface pages


If you are informed that your operator interface pages have been updated, but you still see the old pages on the workstation PC, do the following:

1. From Internet Explorer, select the menu: **Tools > Internet Options...**, then click on the **Delete Files...** button.
2. Select the **Delete all offline content** check box.

3. Click the **OK** button.
4. Close the **Internet Options** window.
5. In Internet Explorer, select the menu **View/Refresh**.

4.4 Logging off BIS

Perform the following procedure to log off BIS:

- ▶ Close the operator interface by clicking .



Notice!

Logging off is only possible if all the pending messages have been processed and deleted, or moved to the workflow.

Your authorization level may prevent you from logging off the system until another operator has logged on. This ensures that at least one operator is always logged onto the system.

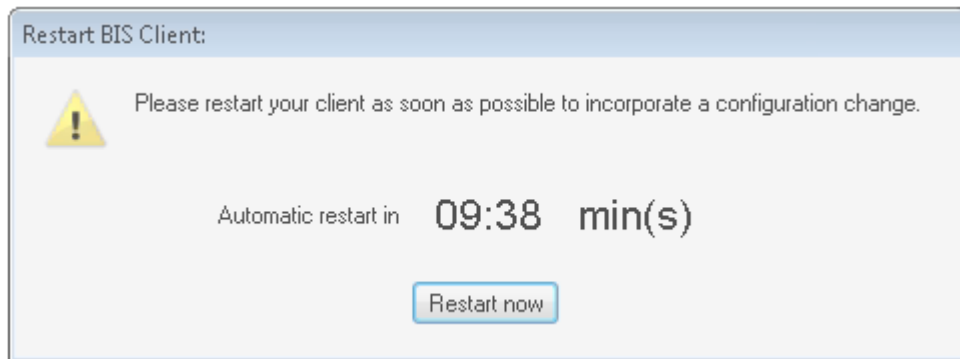
4.5 Forced restart due to configuration change

Reloading a modified running configuration

If the running configuration is changed by an administrator it must be reloaded for the changes to take effect. There are two options:

- Reload the configuration with immediate effect, disconnecting all operators at once.
Note: this was the default behavior up to and including BIS Version 3.0.
- Reload the configuration with delayed effect (10 minutes by default). This allows the operators a grace period in which to finish what they are doing and restart their clients manually.
Note: a major benefit of this option is that, in the case of two or more operators, at least one operator may be logged on at all times. That is, there is no longer any time in which the BIS Messages are not being monitored.

If the administrator chooses the second option, the operator will receive a persistent popup message giving the remaining time until client restart is forced. This is the **grace period**.



Availability of some configuration changes during the grace period

Purpose of the grace period is to ensure that a configuration change does not incapacitate all operators simultaneously, even for a short time. Operators can stagger their restarts to ensure that at least one is monitoring the system at all times.

To ensure the greatest possible system integrity the client restart should be performed as soon as possible after notification, and no mission-critical operations should be performed during the grace period.

Nevertheless the following table lists the main configuration additions, modifications and deletions that will be available to operators during the grace period, under the restrictions there described.

Changed object	Add	Modify	Delete
BIS operator	Visible in the client after clicking the Refresh button or folding/unfolding the relevant part of the device tree.	Property "Allowed to terminate client" is propagated to the client on the fly. All other properties visible in the client after clicking the Refresh button or folding/unfolding the relevant part of the device tree. If modified in the configuration the operator is immediately logged off without reloading the configuration.	If deleted from the configuration the operator is immediately logged off the client.
Device / Groups / Detectors and other BIS addresses	Visible in the client after clicking the Refresh button or folding/unfolding the relevant part of the device tree.	Changes of address are visible in the client after clicking the Refresh button or folding/unfolding the relevant part of the device tree. A client restart is required to display changed names reliably.	A client restart is required to remove deleted devices from the GUI. Until restart the deleted objects are marked with a # character.
Address lists	Visible in the client after clicking the Refresh button or folding/unfolding the relevant part of the device tree.	Changes of address are available. Note: Change of address list name requires client restart	Until restart the deleted objects are marked with a # character.
Graphic files / Named views / Layers	Detector mappings available. State changes are highlighted with the colors of the new states.	Not available. The old graphic file and layer information are not updated until after client restart	Not available. The old graphic file and layer information are not updated until after client restart

Changed object	Add	Modify	Delete
Action plan and Misc. documents	Newly created links to Action Plans and Misc. Documents are available.	If an Action Plan or Misc. Document is in use when its link is changed or deleted, then the old document persists until the operator has finished in it. The newly linked document will not appear until the next invocation.	If an Action Plan or Misc. Document is in use when its link is changed or deleted, then the old document persists until the operator has finished in it. A document that has been unlinked will not appear again.
Timer settings NB: <i>General settings >Timer (not the timer within jobs)</i>	Available	Available	Available
Counters and groups	Not available	Changes in participating address lists and state lists available. Changes in name and/or color require restart.	Counter remains visible but ceases to count
Associations (Jobs)	Available	Available	Available
BIS operator authorizations	(not directly visible in the client)	The following modifications available: <ul style="list-style-type: none"> - The property "Allowed to terminate client" - Modifications to addresses and address lists 	Authorization can only be deleted if no operator has it.
ACE user profiles	Available	Available	Available
ACE workstation profiles	Available	Available	Available
ACE areas	Available upon Refresh	Available upon Refresh	Available upon Refresh
ACE reader types, card configurations, PIN code configurations	Available	Available	Available
ACE divisions	Requires client restart	Requires client restart	Requires client restart

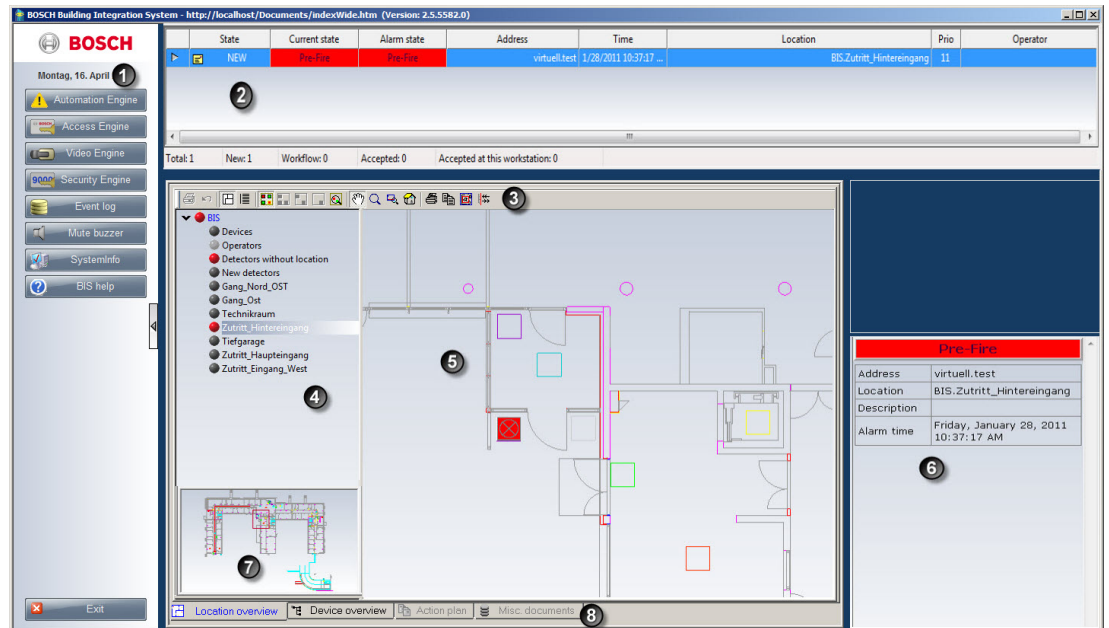
Changed object	Add	Modify	Delete
Index page	Requires client restart	Requires client restart	Requires client restart
Virtual devices	Available	Requires client restart	Requires client restart
Alarm print	Print template, state mapping, printer and layer information is updated for automatic alarm printing. All other features require client restart	Print template, state mapping, printer and layer information is updated for automatic alarm printing. Modified layer information is not available for manual printing.	Print template, state mapping, printer and layer information is updated for automatic alarm printing. All other features require client restart
Event log	Available	Available	Available
OPC and connection servers	Available upon Refresh	Requires client restart	Requires client restart

5 The Screen Display

5.1 Standard Screen Elements

The screen display explained in this section pertains to BIS's **default** configuration. Modified configurations can alter what you see on your BIS screens.

Depending on the system's configuration, some elements described here may not be present on your system, or may behave differently from the system's defaults.



Label Screen Element

- 1 *Navigation Buttons, page 20* Invoke BIS Engines and Event log, control the loudspeaker, get system information, invoke help or exit BIS. In previous versions these buttons were displayed by default horizontally across the top of the screen.
- 2 *Message Display Field, page 21* Displays incoming messages for processing by the system operator. This field has its own status bar, which summarizes the messages in the list.
- 3 *Tool Bar, page 21* Manipulates the Location and Device Overviews.
- 4 *Location Tree, page 23* Lists locations, but in effect any possible sources of BIS alarms/messages (locations, devices, detectors, operators) in a logical hierarchy.
- 5 **Document Display area:** the main pane for displaying floor plans, action plans, device hierarchies and Miscellaneous documents.
- 6 *Additional Displays, page 24:* A display which is configurable by the system administrator, typically used for showing details of a message selected in the Message Display field.
- 7 **Navigation pane:** As an aid to orientation, the pane shows the full extent of the currently loaded location graphic, and the red rectangle indicates the part of the graphic currently visible in the Document Display area.

- 8 **Tabs for display selection:** Tabs for switching between different display modes: **Location overview**, **Device overview**, **Action plan**, and **Miscellaneous documents**.

5.2 Navigation Buttons

Automation Engine



Click this button to switch to the Automation Engine. For more information, refer to the Automation Engine Operation Online Help.

Security Engine



Click this button to start the Security Engine (the Admin9000 module). For more information, refer to the Security Engine Operation Online Help.

Access Engine



Click this button to start the Access Engine. For more information, refer to the Access Engine Operation Online Help.

Video Engine



Click this button to start the Video Engine. For more information, refer to the Video Engine Operation Online Help.

Event Log



Click this button to open the Event Log. For more information see *Event Log, page 71*, *Event Log Filters, page 79* and the BIS Configuration help file.

Mute Buzzer



Click this button to mute the buzzer for 30 seconds. The buzzer is switched off when the message is accepted. If a new message arrives with the same or a higher priority however, the buzzer sounds again.

System Information (SystemInfo)



Click this button to view a summary of system information, including operator name, operator permissions, BIS version, server name, computer name, operating system, language, logon time.

BIS Help



Click this button to view the BIS Operation Online Help.

To print the online help, right-click on the opened help topic and click **Print...**

Exit



Click this button to log off the BIS Operator Interface.

5.3 Message Display Field

Incoming messages are displayed in a list for processing by the operator. In a default configuration the message fields are:

- The **State** of the message (New, Accepted, or Workflow). A blinking icon identifies new messages.
- The **Current state** and **Alarm state** of the triggering device (for example, **Master armed**)
- The **Address** of the triggering device
- The **Time** (actually date and time) of the message
- The **Location** of the triggering device
- The **Prio** (priority) of the message
- The **Operator** who accepted the message. This field is empty for all messages in states other than “Accepted”.



Notice!

A BIS system administrator can change which fields appear in the display, and in what order. This is done by editing the ActiveX controls in the .htm file which defines the main BIS screen for a particular configuration. For details please consult the BIS Configuration help file.

As operator you may see one or more additional fields, which can be configured by the BIS system administrator. These include:

- A **Brief text** which can be used for describing the triggering device
- A **Time Stamp** marking the time the message was accepted. This field is empty for all messages in states other than “Accepted”.
- The **Attributes** (either Custom or OPC attributes) of the message, e.g. user ID, message text etc.
- **Message (number)** and **Current State (number)**

5.4 Tool Bar



The tool bar offers a number of functions that affect the display:

Button	Description
	Prints the floor plan for the current alarm/message location.
	When traversing the location tree during message processing, this button takes you straight to the detector triggering the current alarm/message.
	Displays the location graphic
	Displays the detectors belonging to the currently selected element in the location tree (detector view).
	Displays all detectors of the currently selected element in the location tree, without filtering.



Displays those detectors of the currently selected element in the location tree which have the same **group** as the current message



Displays those detectors of the currently selected element in the location tree which have the same **state** as the current message



Displays only the detectors for the message currently selected in the message field.



Filters the displayed list of detectors by **state lists**, **address lists** and/or **addresses**. Two wildcards can be used in the address field:

* = The asterisk represents any number of characters, including zero.

? = The question mark represents exactly one character.

Notes:

- The search is case-sensitive.
- Select **<without filtering>** to switch off filtering based on the respective criterion
- Removing or adding a filter criterion causes an automatic refresh of the search results.
- Filters the displayed list of detectors, not the graphical view.
- Include detectors from sub locations in the search by selecting the check box marked **Include sub locations**. (detector view)
- The more detectors are present at a location, the longer the filtering process will take.



Move the visible section of the location display: left-click, hold and drag. Use the mouse wheel to zoom in and out.



Zoom the visible section of the location display left-click hold and drag up or down. Use the mouse wheel to zoom in and out



Zoom to selection.

Click and drag to select an area in the graphic, then click this button to zoom to the selected area.



Home view.

Reverts the display area back to the initial view.



Displays a dialog box for selecting layers to be hidden or displayed



Prints the location graphic (provided a print template has been set up). See BIS Configuration Guide online help "Alarm print" for details.

Note!

Macros in the print template will not be instantiated by information from the selected message.

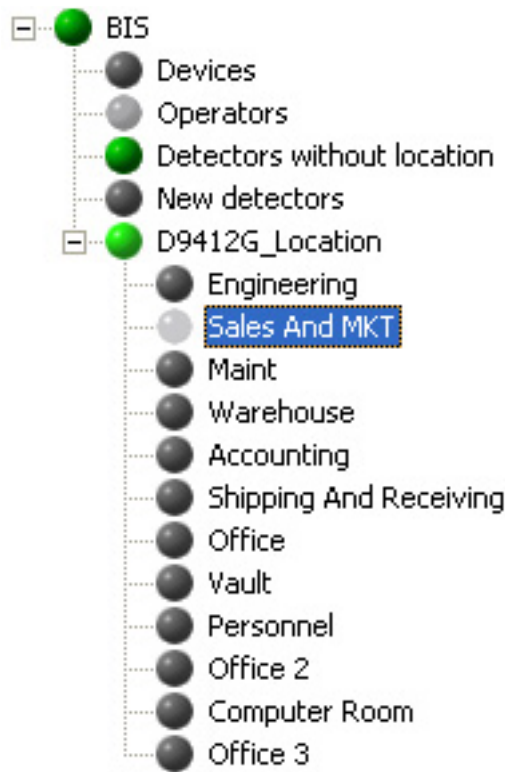


Toggles whether the Navigation Pane is displayed.



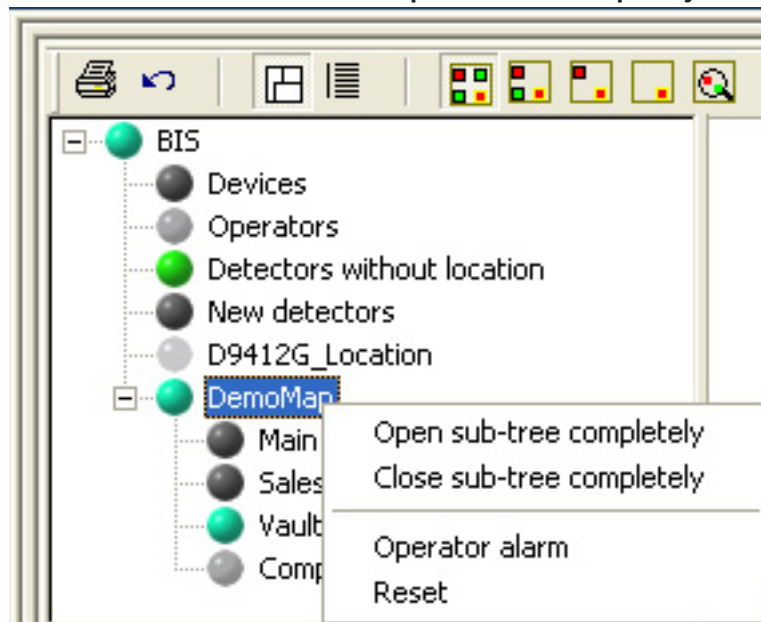
Toggles whether the Location Tree is displayed

5.5 Location Tree



Shows all connected systems and objects with their respective addresses and line states, as well as other elements identifiable in the system (for example, configured authorization levels).

You can open or close any location tree node, as well as all sub-nodes beneath a node. Right-click on a node and select either **Open sub-tree completely** or **Close sub-tree completely**.



5.6 Additional Displays

The standard BIS displays and controls in this area are as follows. Depending on the configuration your user interface may display customized screen elements. In this case please consult your system administrator for further information.

Counters

 On	12
 Off	0
 Ready/Standby	56
 Pre-Alarm	0
 Fire External	0

Counters show the number of objects currently in particular states. The sums of one or more line states are displayed for one or more objects, in different colors.

Counters can be defined per operator group, hence it is possible that different operators see different sets of counters.

For example, the device state counter **Open Windows Detector Area Warehouse** counts only the addresses of the windows (i.e. their magnetic contacts) in the warehouse, and only if these have the status **Open**. If the device state counter is 0 then it is determined that no window is open and that the operator can arm the intruder alarm for this area.

If you **double-click** on a device state counter, BIS lists those devices in that state within the location overview area. This can take some time if your system is very large.

Address	State	
 D9412G.D9412G...	Burglary Cancel	Pan...
 D9412G.D9412G...	Burglary Cancel	Pan...

Message Details

Closing Extend	
Address	D9412G.D9412G.Area_1.*
Location	BIS.D9412G_Location
Description	
Alarm time	Thursday, June 22, 2006 12:31:43 PM

If you click on a message in the message list, message details display in this area.

Action Buttons



(example)

The BIS screen interface is configurable to the operators' needs. This allows the system administrator to add action buttons (e.g. for switching to another camera display, opening telephone directories, starting an application etc.).

Depending upon the purpose of the action button, the operator may be prompted for additional information (e.g. addresses or other parameter values).

When adding an action button, the system administrator considers the following parameters:

- Button text (for example, **Escalator off**)
- Type of control to execute (for example, emergency switch off of all escalators)
- Authorization level required for the activation of the button (for example, technicians only)
- Message reference (the address of the object to control may be derived from the message)

All controls triggered through action buttons are entered in the Event Log, along with the operator's login name.

Action buttons can also be embedded in action plans which are invoked for the processing of a message. Action buttons can be configured so that:

- The action button **must** be pressed before the message can be deleted
- The action button can be pressed once or multiple times

Layer Buttons



(example)

These are optional components to determine the visibility of layers in the location plan.

5.7 BIS Smart client

As of BIS 4.9 the application offers a web-based Smart Client, which contains its own online documentation. You start both clients in a browser with the name of the BIS server:

HTTPS://<Name of BIS server>

The choice of browser determines which client starts:

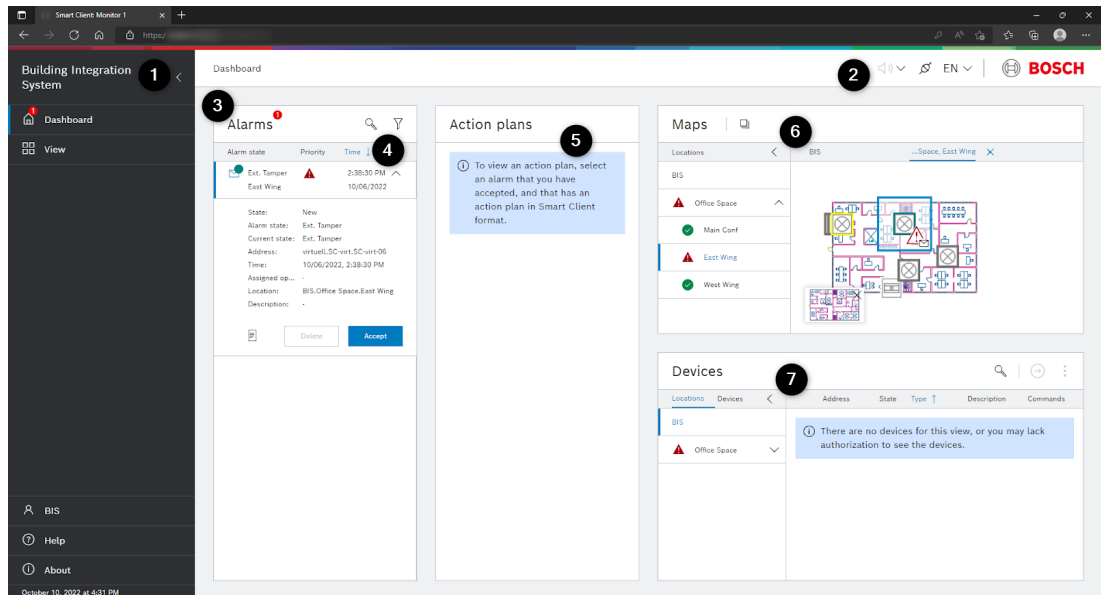
- **Internet Explorer:** Classic client
- **Mobile browser:** BIS Mobile client
- **Modern desktop web browser** (see table of browsers and their versions below): Smart client

Web Browser	Version
Google Chrome	90 or higher
Microsoft Edge	90 or higher
Mozilla Firefox	88 or higher

5.7.1 Standard screen elements

The screen display explained in this section is subject to possible BIS Smart Client customizations. Customization options can alter what you see on your screen.

This page explains the functions of possible standard screen elements of the BIS Smart Client user interface.



Label Screen Element

- 1 Side navigation: collapsible or expandable pane consisting of navigation menu items to load alarms and location maps, invoke customization options of the interface, get system help on using the BIS Smart Client, get system information or to exit BIS.
- 2 **Dashboard** title bar: consists of button to mute alarm sounds, showing real-time status of connection with BIS server and interface language selection.
- 3 Dashboard: consists of customizable collection of widgets, to display alarms, maps of system and objects, or alarm action plans.
- 4 Alarms widget (example): displays incoming alarms for processing by the operator.
- 5 Action plan widget (example): displays action plans associated with the alarms.
- 6 Map widget (example): displays alarms on location maps, and quick navigation using the location tree nodes.
- 7 Devices widget (example): displays where the devices are being placed.

5.7.2

Differences

The following differences apply to the Smart client, as compared with the Classic client:

Parallel processing

- To accept or delete multiple alarms simultaneously, select multiple alarms from the alarm list and right-click for the context menu.
- To send commands to multiple devices simultaneously, select multiple devices in the map and right-click for the context menu. The resulting context menu will contain only those commands that are common to all the devices that you have selected.

Sending commands to devices

- The Smart client monitors only devices that belong to locations that user has defined in the system. Typically these locations correspond to physical locations in the real world, and can be displayed in a map.

- The current version of Smart Client does not support commands where the commands require you to enter parameters in a popup window.

6 Displaying Documents

6.1 Document Display

The display container serves as the frame for the various types of document display. Which document types appear, and in what order, depends on the configuration:

- **Location overview** with possibly multi-layered location plans.
- **Device overview**
- **Action plan**
- **Miscellaneous documents**

Display by Priority

The system administrator of a BIS system uses the BIS Configuration Browser to associate message types with one or more documents in a prioritized list. When a message is received, the first document in that list will be displayed. The other documents in the list (if any) can be displayed by clicking them in the **Additional Display area**, see *Additional Displays, page 24*. Similarly, your system administrator specifies here which of the four document types are displayed at all.

Display Multiple Documents on the Screen

The BIS system administrator also configures the html files shown in the Document Display. Depending on the settings, you may be able to view more than one display container simultaneously.

Multiple Monitor Operation

In a multiple monitor environment, the various document types can be distributed across multiple monitors, so that they are visible to the operator at all times.



Notice!

If several messages are presented simultaneously during message processing, the document display always relates to the message just selected.

6.2 Location Overview/Location Plans

Location Overview/Location Plans (**optional component**)

The location overview is an important means of orientation in BIS.

What is the purpose of the location overview?

The location overview and the associated location plans show all locations:

- Locations at which detectors and sensors are placed
- Locations to which graphics, areas (named subareas of graphics, e.g. **South Entrance**), and message-dependent layers are assigned

You can always print location overviews, even without pending messages. The detectors placed there are displayed in the location plans with their current line states.

Why is one of the symbols blinking in the overview?

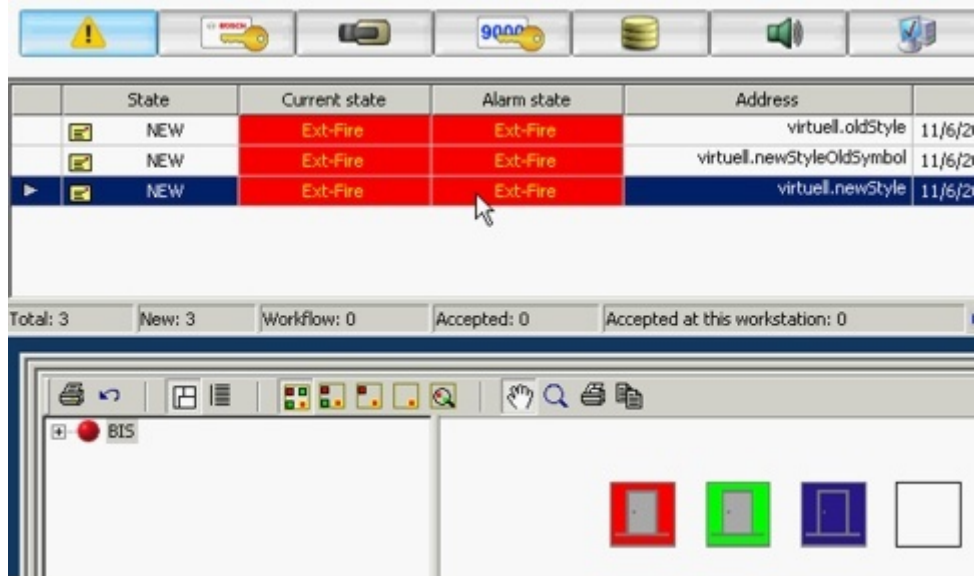
If you select an alarm message the related symbol **blinks** to make it easier to locate.

Depending on your system's configuration, the blinking symbol can stand for a single sensor, detector or a group of either.

Blink patterns of the detector symbols

The following settings are possible (individually or in combination):

- **Default setting:** background color blinks (depending on state of the detector symbol)
- Special setting 1: Frame and symbol of the detector blink on a green background
- Special Setting 2: Whole detector symbol blinks (frame, symbol and background)



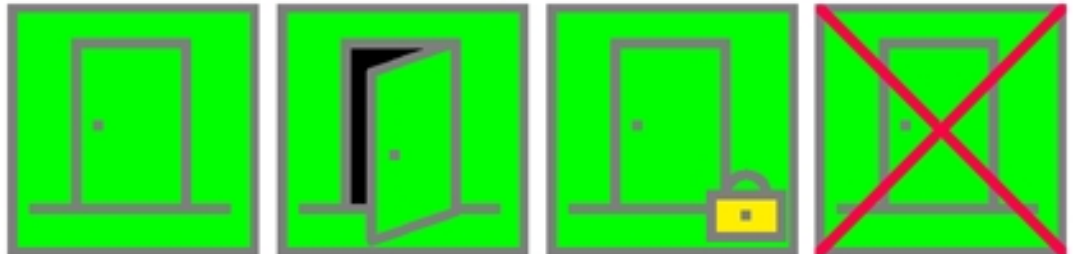
Notice!

Please contact your BIS administrator if you need to reconfigure these blink settings.

A detector symbol has changed, what has happened?

Your system may be configured so as to reflect state changes of detectors not only by sending messages and changing the color of the detector symbol, but by changing the symbols themselves.



For instance it is possible a door can be shown in the states closed, open, locked, etc.



During message processing

The location plan displayed during message processing always depends on the selected (or displayed) message. Navigation through the entire location tree and the associated location plans is also possible during message processing.

Message Display in the Location Overview

Button	Description
	Displays the detectors in a graphical floor plan, if configured (spatial view).
	Lists the detectors as they are organized (logical structure view).

**Notice!**

No distinction made between detectors, sensors and groups of either in the display. All detector points allocated to the location will be displayed, not just those having a hyperlink in the graphic.

Giving commands to a selected detector

There are two ways to send a command to a detector via the location overview:

1. Right-click the detector symbol. If your authorization is sufficient a context menu opens, which contains all the commands available for this detector and your authorization level. Left-click the desired command in the context menu, then, if required, enter any other required control parameters (e.g. **ON** or **OFF**) in the ensuing dialog box.
2. Alternatively, double-click the detector symbol to invoke the **Fast Access Command** defined in the **BIS Configuration Browser** for this detector type. The **Fast Access Command** is the default command among those listed for the detector type. If none has been defined then an explanatory error message appears.

**Notice!**

The list of commands is alphabetically sorted. The names of the commands can be edited using the BIS configuration browser. Placing an exclamation mark at the front of the command name promotes the command to the top of the list alphabetically, and simultaneously makes it the **Fast Access Command** for this detector type: **BIS Configuration Browser > Infrastructure > Detector Types > Commands > (Right click and edit the name of the command)**

Orientation aids in the location overview

To facilitate working with the location overviews, and assist in message processing, a number of orientation aids are provided.

**Notice!**

These orientation aids depend on your system configuration. Not all functions may be available in your system. See your system administrator for more information.

Buttons in the display header (Tool bar)

In both views (message display or location graphic), the header of the display container provides a tool bar:

Blinking elements in the location overview

If there is a message or state-change for a group, detector or sensor, the icons on the location map for that element will blink.

Navigation pane (7)

A navigation pane is always visible. The area shown in the main display is outlined in red in the navigation pane, thus helping you to locate alarms in relation to the entire site.

Controlling from the location overview

If so configured by the system administrator controls can be activated from the location tree as well as from the relevant location graphic.



Notice!

Controlling from the location overview is an optional feature and may not be enabled on your system. Contact your system administrator for more information.

6.3 Layers


Layers (**optional component**)

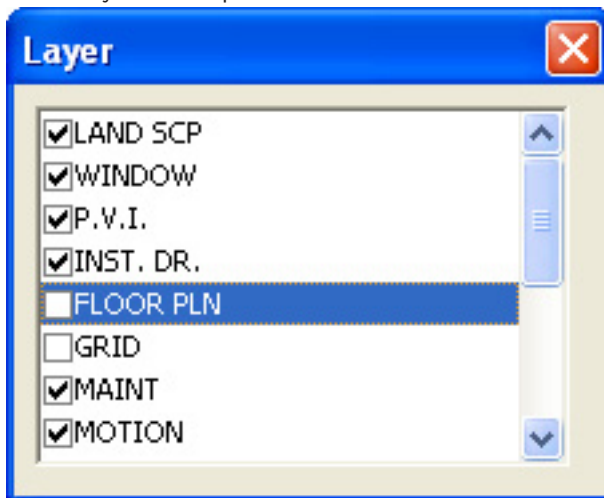
What are layers?

AutoCAD plans typically consist of separate images which overlie each other and are therefore own as layers. Each layer may contain specialized information (e.g. ventilation, plumbing, approach routes, escape routes, fire doors, positions of fire extinguishers etc.) and can be displayed in combination or separately as required. A location overview usually consists of many layers.

How are layers displayed?

Layers are always displayed with messages, and relate to the state and alarm location of the detector that generated the message. When a message is displayed, layers are also displayed during manual navigation.

To control which layers are shown, click  to open the **Layer** dialog. Then select and de-select layers as required.

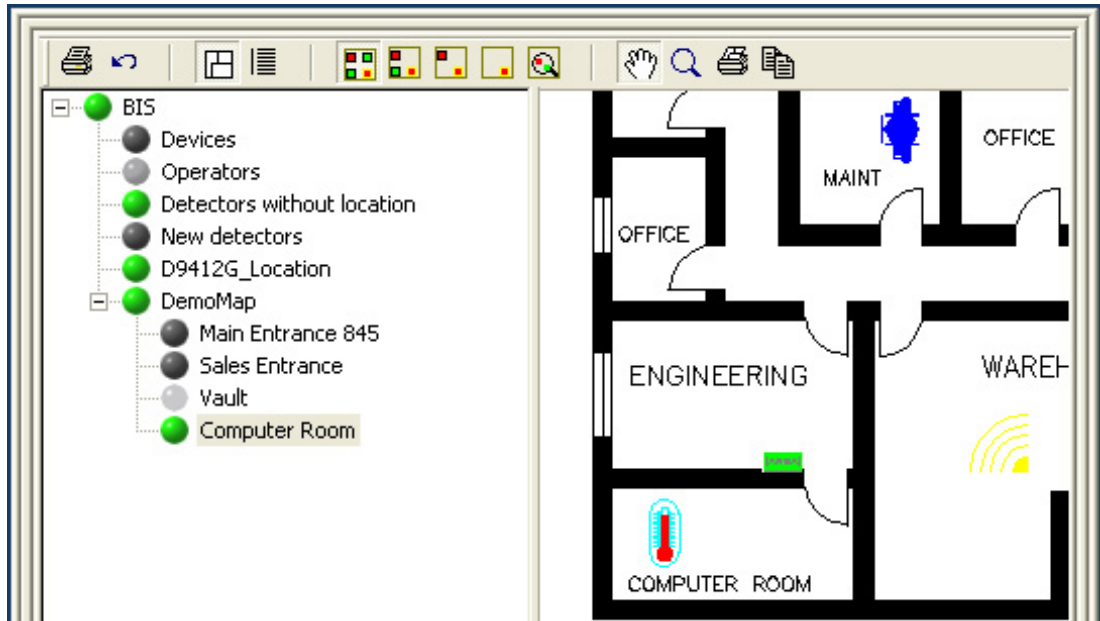


Layer buttons

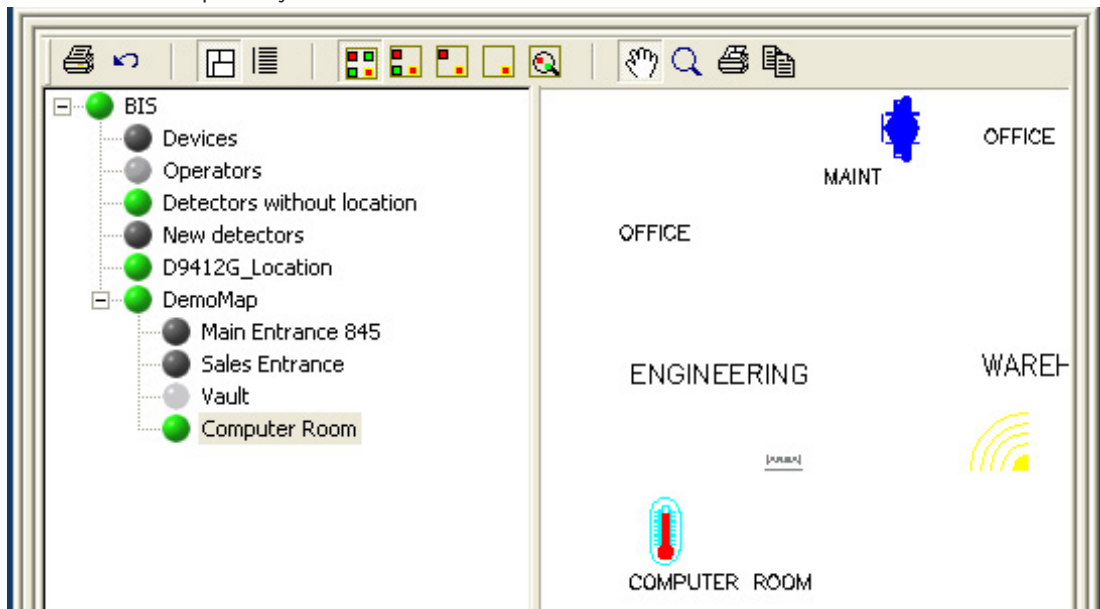
Your system administrator can also add a custom button to your operator screen that you can use to show and hide a specific layer. For example, you could use this button:



to show the floor plan layer:



or hide the floor plan layer:



Notice!

The display of layers and layer buttons is an optional feature and possibly not enabled on your system. Contact your system administrator for more information.



Notice!

Avoid multiple dash and underline characters in layer names e.g. ABBCC|--DFF and ABBCC|DFF__HHKK, as these can lead to compatibility problems between AutoCAD and the BIS client.

6.4

Zoom and Pan

Zoom and Pan (Graphic Navigation) **(optional component)**



Zoom and **Pan** allow enlargement or reduction (Zoom), or back and forth movement (Pan), of the graphic display. Use the mouse for smooth uninterrupted movement.

Zoom and Pan make it possible to rapidly navigate through the alarm locations, as well as to select individual images for display and printout.

Using Zoom and Pan

The function can be started during or outside of message processing, as follows:

1. Click and drag the graphic display in two dimensions
2. Click on the symbol in the tool bar

Button	Description
	Zoom: Enlarge or reduce the display.
	Pan: Move the display back and forth.



Notice!

The zoom and pan functions are optional features, and may not be enabled on your system. Contact your system administrator for more information.

6.5

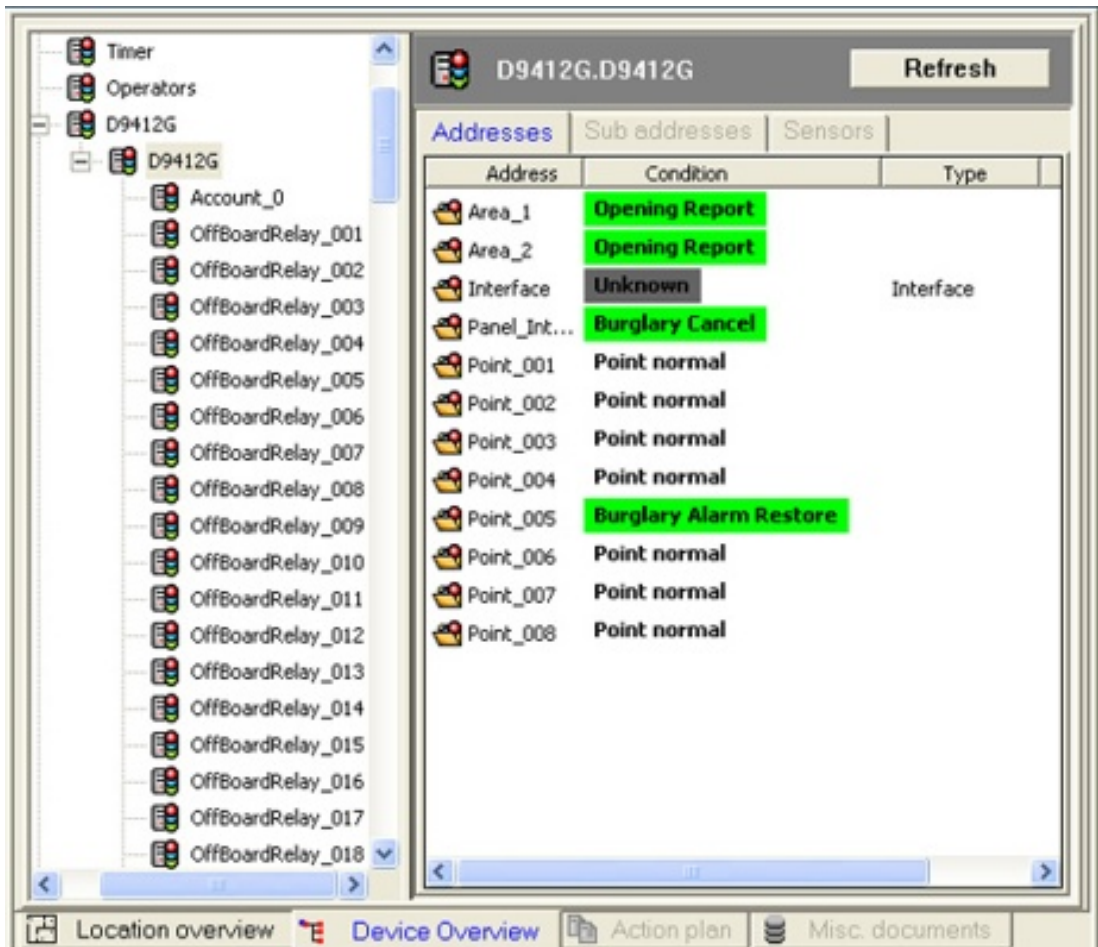
Device Overview

Device Overview (optional component)

Besides the location tree and the location plans, the device overview provides another orientation aid when using BIS.

What is the purpose of the device overview?

The device overview shows all connected systems and objects, with their addresses, states, and other elements identifiable in the system (for example, configured operators). The individual objects are sorted in this view not by location, but by connected devices (for example, “Building control” or “Timer”), and logical administrative units (for example, “Operator”).



Similar to the location overview, there is also a tree structure in the device overview. This tree structure, however, does not display the locations, but the logical levels of the contained systems and objects (the device levels). Where location plans are displayed in the locations overview, the device overview displays detector addresses pertaining to the selected level (with the current state), sensors, lists, groups, and so on.

If an element (such as a detector group) is selected in the device overview, the associated sub-elements (for example, detectors) can be selected in the list by double clicking. You can return to higher levels by double-clicking the back-arrow button.

The address overview is updated continuously.

Double-clicking on a counter causes BIS to display all devices with that state:

Address	State	
D9412G.D9412G...	Burglary Cancel	Pan...
D9412G.D9412G...	Burglary Cancel	Pan...

Calling the device overview

The device overview exists independently of a message display, and can be called during or outside of message processing.

- To call the device overview, click the **Device Overview** tab in the display container.
- Double-clicking on a counter also causes BIS to display all devices with that state from

the counter's state list.

Address	State	
 D9412G.D9412G...	Burglary Cancel	Pan...
 D9412G.D9412G...	Burglary Cancel	Pan...



Notice!

The device overview is an optional feature which requires configuration. It is possible that the device overview is not enabled for your system. Contact your system administrator for more information.

Sorting the device overview

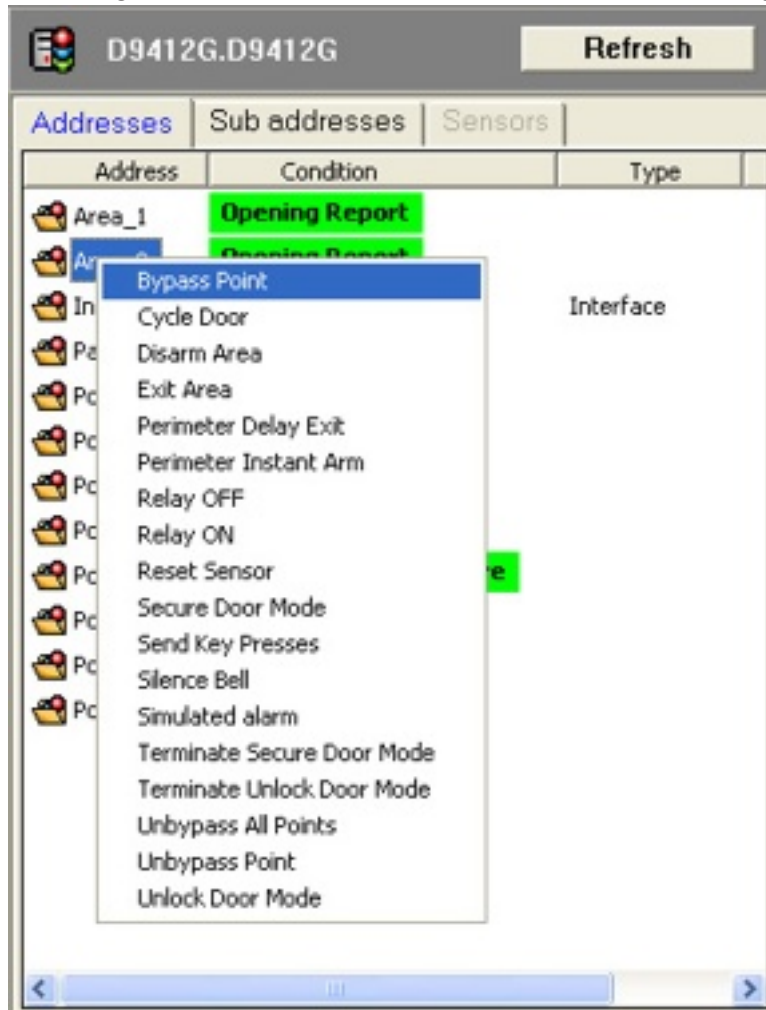
The contents of the overview can be sorted by clicking on the appropriate column heading (e.g. **Address, State, Type**).

Controlling devices from the device overview

There are two methods for giving commands to devices via the device overview:

Context Menu:

- Right-click the desired device. If your account is suitably authorized, a menu opens containing the commands that are available for this detector and your authorization level.



- Select the desired command using the left mouse button, and enter other control parameters as required (for example, **ON** or **OFF**).

New since BIS Version 2.3

- It is now possible to associate any URL with any detector type, and invoke a browser with that URL via the context menu. As only one URL can be invoked at a time, the context menu command is only available where detectors are selected singly, not multiply or from lists. Click **Show extended** in the context menu entry to invoke the URL. The association of detector and URL is performed in the Configuration Browser (see Configuration Browser online help). This feature is typically used to provide extra documentation for the detector type. If no URL has been associated, clicking **Show extended** will produce a dialog box where a URL can be entered manually.
- Similarly detector types can now be associated with BIS Reports. Click **Show Report** in the context menu of a detector in Location or Device Overview to invoke the report. See Configuration Browser online help for details on how to associate BIS Report types with detector types.

Fast access command

- A suitably authorized user can configure which of the device's commands will be executed when the corresponding button in the **Fast access command** column is clicked. If so configured then the same command will be executed when the user double-clicks on the device's icon in the Location overview.
- Place an exclamation mark at the front of the command name to promote the command to the top of the list alphabetically, and simultaneously make it the **Fast Access Command** for this detector type: **BIS Configuration Browser > Infrastructure > Detector Types > Commands > (Right click and edit the name of the command)**

Display of states in the device overview

The device overview shows not only the states of physical devices, but also of “virtual” devices such as address lists, servers, timers, command/event queues, operators etc.



Notice!

If an action is to be triggered on the status change of a device from the device overview, then system administrator needs to configure an appropriate association in **Configuration browser > General Settings > Associations**

See BIS Configuration Browser help for details.

State display of the address lists

In the device tree select **Devices > virtuell > Address lists**. The names of configured address lists appear in the device overview. The state of a complete address list is the highest prioritized state of all the current states of its sub addresses.

State display of the connection servers

In the device tree select **Devices > virtuell > Server**. The names of all connection server computers appear in the device overview. You can see from the displayed state whether the server is functioning correctly.

State display of the command and event queues: “System status”

In the device tree select **Devices > virtuell > System status**. The various queues of incoming messages and outgoing OPC commands appear in the device overview. Four states are used (state numbers 271-274, introduced with BIS 2.3); these are:

- **Normal** (green)

- **Warning** (yellow)
- **Critical** (orange)
- **Error** (red)



Notice!

With the **Error** state, the maximum number of entries has been reached, and any new incoming messages will be lost.

Three system status "devices" are visible by default.

These are

- **Commands to OPC servers** (how many OPC commands are waiting to be sent to OPC servers)
- **Offline Messages** (how many offline messages from OPC servers are waiting to be processed by BIS)
- **Eventlog entries** (how many messages are waiting to be written to the event log)
The queues for further OPC servers appear under the name **Data from** <OPC server name>

State display of the time-scheduled programs

In the device tree select **Devices** > **Timer**. The names of all time-scheduled programs appear in the device overview along with their current states.

State display of operators

In the device tree select **Devices** > **Operators**. The names of all configured operators appear in the device overview along with their current states: **logged on** or **logged off**.

6.6

Action Plans

Action Plans (optional component) are created in advance by system administrators, and not by the operator. Which document types appear, and in what order, depends on the configuration. For more information please consult the BIS Configuration online help.

Contents of an action plan

An action plan defines in detail what steps should be taken in the event of an alarm. The states triggering the messages are continuously monitored. The action of deleting a message is stored in the Event Log.

An action plan can contain active elements such as action buttons (see below) and macros, which are replaced by current data from the message every time the action plan is displayed (e.g. the time of day).

Displaying the action plan

An action plan is not displayed until an operator accepts the relevant message. This is to ensure that only one operator at a time executes the plan.

- If the action plan is uppermost in the list of documents configured to the message, then it appears in the display container as soon as the message is accepted.
- Else display it by clicking the **Action plan** tab, usually below the display container.

Action buttons in an action plan

An action plan can contain predefined, context-related action buttons. These are created by the system administrator with the following attributes:

- Label
- Authorization (the user groups allowed to click the button). If you are not authorized to use an action button it appears grayed out in the user interface.

- Message reference (address, state, automatic display)
- The commands to be executed

If an action plan contains **required/mandatory** buttons, its message cannot be deleted until these buttons have been clicked.

**Notice!**

A message cannot be deleted unless all required actions have been executed.

Action plans and Workflows

If a message requires the attention of different kinds of operator, it can be forwarded by right-clicking the message, selecting **Workflow** and then selecting another operator group from the popup list.

For example, an action plan for a stuck elevator might contain the action button **Intercom** to communicate with the elevator. This button would be authorized for all operator groups. In the same action plan another button **Reboot Elevator** would be authorized only for the location manager, and so be grayed out in the normal operator's UI. If the normal operator determines the alarm is genuine he may forward the message via Workflow to the location manager's group. When the location manager accepts the message he will be able to click the button **Reboot Elevator** from the action plan.

Another example: an operator can postpone processing of a non-urgent message, after accepting it, by forwarding it via Workflow to his own group. The Event Log records such actions in any case.

6.7

Miscellaneous Documents

Miscellaneous Documents (optional component)

In addition to the location overviews, device overviews, and action plans, the **Miscellaneous documents** category is another document type that can display during message processing.

This category includes any number of HTML documents.

Miscellaneous documents can contain macros, which are replaced at the time of message generation by current data from the message (for example, the date).

Examples for miscellaneous documents:

- Display of message-related first aid measures
- Retrieval of video images from webcams
- Links to databases (for example, a central hazardous substances database)
- Display of telephone or address books
- Calling documents from in-house applications (for example, SAP)
- Embedding active documents from external applications (for example, the analog value display of a pyrometer)

**Notice!**

These documents can also be part of an action plan.

Displaying miscellaneous documents


- Click the **Misc. documents** tab. All documents in this category are shown in a list field, and can be selected from that field.

7 BIS Message Processing

7.1 Processing a BIS message

How you process a message depends on the scope and configuration of your BIS system. There are only a few rules which are generally applicable.

- Ensure that you are familiar with any local rules and procedures for your site, that these are stored locally and can be consulted quickly in an emergency.

Step	Procedure
1. Suspend the acoustic signal while making a first assessment of the situation, or proceed to step 2	Click the  button.
2. Accept the message.	Double-click the message.
3. Assess the overall situation if faced with several simultaneous messages.	Browse through the lines of messages to find common reference points for the pending messages. This will help you to decide on the order of processing. Note: It may be helpful to sort the list by clicking on the header of the Priority or Time columns.
4. View documents.	Click in the documents list (if available) to view the documents. You may find important information that will help you process the message. For more details see <i>Displaying Documents, page 28</i>
5. Execute the required procedure.	Execute the steps listed in the message documents, particularly those in an action plan. See also <i>Action Plans, page 37</i>
6. If you require the actions of others, place the message in the workflow.	Right-click on the selected message and select Workflow from the context menu. A list of operator groups appears, to which you may pass the processing of the message. Select one of these. The action plan itself may specify to which user group you should pass the message, and when you should do this. The message then appears on the displays of all operators belonging to group you selected. See also <i>Notes on Workflow processing, page 42</i>
7. After processing, delete the message.	Right-click on the selected message and select Delete from the menu. Delete the message only if all specified steps have been executed. In case of messages with an action plan there may be certain mandatory actions (e.g. mandatory buttons to press) before the message can be deleted. See also <i>Notes on deleting messages, page 42</i>

7.2 Standard features of a message


The following section describes features which are standard to messages in a BIS installation.

Recipients

A message only appears in the message list of those operators who are authorized to process the message. The operator who accepts the message first is responsible for further processing. The message cannot be accepted by more than one operator.

Acoustic signals

When a message arrives, the system produces an audible signal, which can be turned off for

30 seconds by clicking the  button. The signal sounds again until the message has been accepted (acknowledged) by double-clicking the message.



Message states

Message State	Description
New	All the incoming messages that have not been accepted by any operator are marked NEW . These messages are displayed to all operators that are authorized to process them.
Accepted	All messages which have been accepted by any operator are marked ACCEPTED . In the Operator column, the name of the operator who accepted the message is displayed. Only this operator can delete the message or put it into the workflow.
Workflow	A message is marked WORKFLOW if it was accepted by another user, but was forwarded to your authorization level for further processing. All operators with your authorization level see the message on their own workstations, and may accept the message from there.

The Message Display Field

The message display field shows all messages that you are authorized to process.

- Sort the list by clicking on the header of the column by which you wish to sort.
- Select multiple messages by shift-clicking or control-clicking. An arrow in the left column marks the message you selected last.
- Details of the selected message may appear elsewhere on the screen, depending on how your user interface has been configured.
- If you are running a Multi-Server BIS installation, and a message arrives on your Consumer server from a Provider server, then the message display field prefixes the name of the Provider server to the Address field, and the background color of the message is gray, as seen in the following illustrations:

	State	Current state	Alarm state	Address	Time
	ACCEPTED	Ext-Fire	Ext-Fire	virtuell.test1	20.10.2014 10:47:21
	ACCEPTED	Emergency alarm	Emergency alarm	virtuell.test2	20.10.2014 10:52:07

Total: 2 New: 0 Workflow: 0 Accepted: 2 Accepted at this workstation: 1

Figure 7.1: Messages from a Provider server as seen locally on that Provider server, or one of its clients.

	State	Current state	Alarm state	Address	Time
	ACCEPTED	Ext-Fire	Ext-Fire	RemoteSites.TEST-HP8.virtuell.test1	20.10.2014 10:47:21
	ACCEPTED	Emergency alarm	Emergency alarm	RemoteSites.TEST-HP8.virtuell.test2	20.10.2014 10:52:07

Total: 2	New: 0	Workflow: 0	Accepted: 2	Accepted at this workstation: 1
----------	--------	-------------	-------------	---------------------------------

Figure 7.2: The same messages from a Provider server as seen remotely on a Consumer server, or one of its clients.

- An operator on the Consumer server can accept and process remote messages (messages from a Provider server) as if they were coming from any other Connection server .
- Whenever there are no messages, the message display field is hidden and replaced with a clock.
- The message pool can hold a maximum of 5000 messages (plus, if necessary, the Event log full message) regardless of the processing state of the messages.
- The status bar below the Message Display provides the following information:

Total: 3	New: 0	Workflow: 0	Accepted: 3	Accepted at this workstation: 3	
----------	--------	-------------	-------------	---------------------------------	--

- **Total** number of all messages in the list
- Number of **New** messages in the list
- Number of **Workflow** messages in the list
- Number of **Accepted** messages in the list
- Number of messages in the list **Accepted at this workstation**
- Icon **a-z**: Indicates whether the messages are currently sorted or not. If unsorted the icon is crossed out.



Notice!

To avoid confusion in the message list, new messages are always appended to the end of it. Because of this, a previously-sorted list may become unsorted. If this occurs, the flag **a-z** icon in the status bar is crossed out, as shown above.



Notice!

- If the alarm is configured to be handled exclusively, and was accepted from a Classic Client,
- the Classic Client that accepted the message can see the message
 - no other Classic Clients will show the message
 - all Smart Clients will show the message

The dwell time of a message

in general a message disappears from the message display field only when deleted.

Exception:

- If during message processing the same object issues a new message with **the same or higher priority**, the initial message is overwritten. For example, a fire detector detects dirt during its self-diagnostics check. If this detector shortly thereafter triggers a fire alarm, and the dirt message still has not been processed, the dirt message is overwritten by the fire alarm and disappears from the message display field.
- If another message with a lower priority arrives, the original message is not overwritten; the new message appears in addition to the original message.
- If the first message is already being processed when a new message arrives, it is not overwritten. The second message appears in addition to the original message.

7.3 Optional/configurable features of a message

The following section describes the commoner features which may or may not be part of your BIS installation, depending on how it is configured. For details on the many possibilities offered, please consult the BIS Configuration helpfile.

Message documents

When a message arrives, BIS displays any documents that are associated with it in the configuration (e.g. location plans, escape routes, action plans, instructions regarding hazardous substances). If more than one message is present in the message list, then it is those documents associated with the selected message that are displayed. For more information see *Displaying Documents, page 28*

Automatic events

When a message arrives, BIS may trigger events that are associated with it in the configuration (e.g. the printing of a specific document).



Notice!

If so configured, the system can also trigger automatic controls without generating messages.

Sequence-monitoring using timeouts

To help ensure that urgent messages are not overlooked or ignored, the configuration may include timeouts for message processing steps (e.g. the time taken to accept a message after it arrives). If a timeout occurs, a control or a new message may be triggered automatically.

Display of alarm location

The standard behavior is to show the location of the alarm immediately after a message arrives in the location tree. This behavior can be reconfigured by the administrator, e.g. so that the location tree shows the alarm location only after a message had been accepted.

7.4 Notes on Workflow processing

A workflow is the set of operator types to whom a certain message can be passed for further processing. Each message that has been placed in the workflow is then marked **WORKFLOW**.

- Messages can only be sent to a Workflow individually. Multiply-selected messages can not be put into a Workflow simultaneously.
- The configuration may specify escalation sequences for messages. These automatically forward messages to the workflow if the first operator group does not accept the message within a certain time limit. This helps ensure that urgent messages are not overlooked or ignored.

7.5 Notes on deleting messages

A message remains in the message display list until it is deleted, then it disappears from the list. You must distinguish between two types of messages.

- **Messages without an action plan** : These messages can be deleted at any time. You can select multiple messages of this type for simultaneous deletion by ctrl-clicking or shift-clicking them.
- **Messages with an action plan**: Action plans usually have mandatory actions which you must complete in the course of message processing. You cannot delete a message until all mandatory actions have been executed.

You must delete each of these messages separately.

Logging off BIS

As an operator, you can only log off a running BIS configuration when you have finished processing all the messages that you have accepted.

Information about the acknowledgement and deletion of messages, as well as the status of the associated action plans and miscellaneous documents, is automatically recorded in the Event Log, see *Event Log, page 71*.

7.6 Using the mobile client

Introduction

The mobile client is a browser-based application that connects to the BIS server and allows operators to perform the following tasks from portable devices:

- View, accept and delete alarms.
- Receive notifications over the internet from the BIS server, even if you have not opened the BIS server's web page. This is known as “push notification”.

Differences between desktop clients and mobile clients

The mobile client is intended to help operators to stay informed about alarms when they are not at their workstations. It provides a subset of the functionality of the desktop client. The main differences are:

- Its menus and commands are automatically displayed in the language that is set in the options of the browser, provided that this is one of the languages supported by BIS. The default language is English.
- Alarms are displayed in the language of the BIS installation.
- The colors and sounds are the defaults from the mobile client.
- It does not support the handling of BIS **Workflows, Action plans** and **Miscellaneous documents**.
- Mobile client operators can log out even if they have open alarms (alarms that they have accepted and not yet deleted). Such alarms remain assigned to the current operator for 30 minutes before being marked as **New** again, and offered for reassignment in the alarms list.

Supported browsers

The following web browsers are supported:

- Chrome (recommended)
- Firefox
- Edge

Notes: The Edge browser can be used for accepting and deleting messages, but does not support push notification. Apple iOS does not support push notification at all.

Technical specifications

- A single browser window can connect 1 operator to only 1 BIS server.
- The operator can have up to 5 concurrent sessions on separate tabs.

7.6.1 Prerequisites and HTTPS certificates

There are no configuration steps necessary in the BIS Configuration Browser. The mobile client is enabled by default.

For secure communications with the BIS server, CA certificates or self-signed certificates can be used. By default, BIS creates self-signed certificates, which need to be manually exported, imported and installed on the client devices.

Ensure that the filename extension `.CER` is defined as MIME type `application/x-x509-ca-cert` for the Default Web Site of the BIS server:

1. On the BIS server, start the Windows program **IIS Manager**
2. In the **Connections** column, open the page with the name of your BIS server and navigate to **Sites > Default Web Site**
3. In the main pane **MIME Types**, if file name extension `.cer` is not listed as MIME Type `application/x-x509-ca-cert` then add it as follows:
 - In the **Actions** column, click **Add...** and enter them in the **Edit MIME Type** popup.
 - Click **OK** and close **IIS Manager**.

Importing a self-signed certificate from the server to the client device

1. On the mobile client device open the certificate's URL in a browser.
 - For example, if your BIS server is called `BISSERVER1` then the URL will be `http://BISSERVER1/BISSERVER1.CER`
2. Save the certificate file in local computer storage **Trusted root** on your mobile client device.

Installing self-signed certificates onto mobile devices

Prerequisite: This section assumes that you have generated a self-signed certificate on the BIS login server, and placed it in the mobile's internal file storage.

Generic procedure

1. On your mobile device open the device settings and enter `certificate` to search for the certificates installation menu.
2. Select **Install certificate from storage** (or similarly named menu item, depending on your operating system).
3. Select the imported certificate and Install it.



Notice!

Note that the exact procedure will vary slightly from platform to platform, and version to version. If in doubt, consult the device's own online help.

7.6.2

Settings

Time and date formats

The time and date formats for the mobile client's alarm list and alarm details are configured in the following file:

```
<BIS Installation drive>\MgtS\SmartClient\BWC\config.json
```

The relevant lines, here shown with default settings, are:

```
"timeFormat_24hrs": "true"
```

and

```
"dateFormat": "dd/mm/yy"
```

- To change the time to 12 hour am/pm format, edit the line to: "timeFormat_24hrs": "false"
- To change the date to US format, edit the line to "dateFormat": "mm/dd/yy".
The system currently supports only these two date formats.
- If a time or date format is missing or invalid, then system uses the default settings.

After changing settings in this file, restart the mobile client.

7.6.3 Connecting the mobile client to the BIS server

1. Open the URL `https://MYSERVER/BWC` in the browser of your mobile device, where `MYSERVER` is the hostname of your BIS login server.
2. (First time only) Add the application's shortcut icon to the home screen of your mobile client. See the next section for more detailed instructions.
After performing this step, always launch the application from the shortcut icon.
3. On the Login screen, enter the username and password of a BIS operator, as defined in your configuration
 - The Home screen (Alarm list) opens.

7.6.4 Adding a shortcut icon to the screen of your mobile client

Introduction

For convenience, an application shortcut can be added to the home screen of your mobile client.

If you fail to add the shortcut icon the first time you open the URL, then you will no longer be prompted, and you will need to add the icon manually via the browser's menu.



Notice!

Note that the exact procedure will vary slightly from platform to platform, and version to version. If in doubt, consult the device's own online help.


Adding a shortcut icon using the Chrome browser

Prerequisite: You have entered the URL of your BIS login server for the first time in the browser's address bar.



1. Click the link **Add Building Integration System to Home screen** in the popup bar at the bottom of the screen
2. Click **Add** in the popup to confirm.
 - The shortcut icon is added to the screen.

Adding a shortcut icon using the Firefox browser

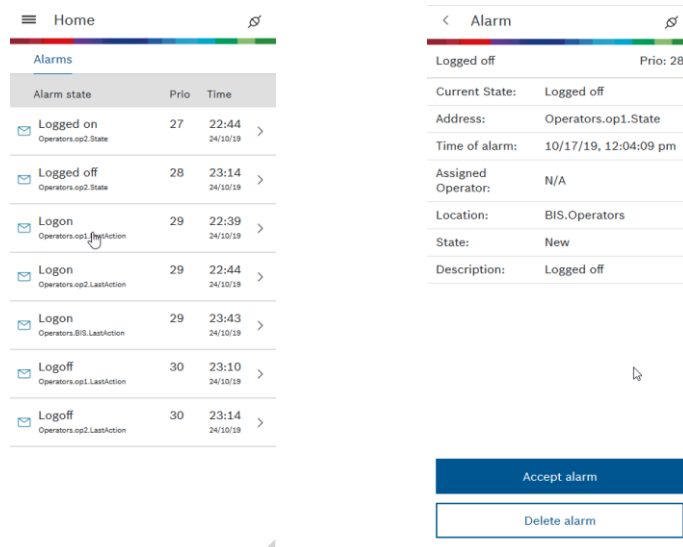
Prerequisite: You have entered the URL of your BIS login server for the first time in the browser's address bar.

1. Click the  icon at the top of the screen
 - The icon is displayed
2. Click **+ ADD TO HOME SCREEN** below the icon.
3. Click **Add** in the popup, to confirm
 - The shortcut icon is added to the screen.

7.6.5 Logging out of the mobile client

1. Click the **Menu** button 
2. Click **Log out** 

7.6.6 Viewing, accepting and deleting messages




1. On the Home screen the messages are sorted first in order of priority (highest to lowest), and then by timestamp (oldest to newest).
 - Messages that have been accepted by other operators will be read-only.
 - Messages that have been deleted by other operators will not appear.
2. Click inside any message to see a details screen.
3. On the message details screen:
 - Click **Accept** to accept the message, so that it becomes your responsibility to handle it. Other mobile operators will see your ownership in their mobile clients.
 - Click **Delete** to delete the message, after you have handled it. The message will disappear from all other mobile clients.

7.6.7 Push notification

Introduction

Push notification means that the mobile client receives messages from the BIS server even if the BIS server page is not currently opened in a browser.

Prerequisites

- The operator has permission to see the message.
- Push notification enabled in the settings menu ( (**Menu**) > **Settings**) of the BIS browser application.
 - **Note:** Push notification is enabled by default for all operators and every new session. If not desired it must be deactivated manually in the settings menu every time you open a session.

- The operating system and browser allow Push notification. For example, iOS Safari does not.

Operation

When a new alarm is triggered, the BIS server "pushes" a message to all mobile clients where the prerequisites are fulfilled:

Notification is sent only for **new** alarms, not the modification or handling of existing alarms. Each notification expires after 30 minutes.

The BIS server sends notification and logs out the operator automatically after 30 minutes of inactivity on the mobile client. Before that, after 27 minutes inactivity, it sends a warning to the mobile client to give the operator a chance to avoid the imminent logout.

A similar notification is sent if the BIS application stops, usually because of a configuration change. The operator then needs to log in again.

7.7

Message processing in the Smart client

The BIS Smart client contains its own online help. Consult this online help for details.

Message and alarm processing in the Smart client allows a degree of parallel processing:

- To accept or delete multiple alarms simultaneously, select multiple alarms from the alarm list and right-click for the context menu.
- To send commands to multiple devices simultaneously, select multiple devices in the map and right-click for the context menu. The resulting context menu will contain only those commands that are common to all the devices that you have selected.

8 Using the BIS Smart Client

8.1 Logging in and out

8.1.1 Logging in to BIS

To login to BIS from the workstation PC


1. Start the Microsoft Edge (Chromium-based), Google Chrome or Mozilla Firefox browser.
2. Enter the address of the BIS logon server as follows: `https://<Name of the BIS server>`
3. Enter your operator user name and password in the window.
4. Select **Login**.

The logon server validates your login entries, and checks your authorization level. The server then sends the start page to your workstation PC.

If the password check policy is enabled on BIS, logging in with credentials where the operator user name and the password is the same invokes a change password dialog. The BIS Smart Client prompts you to change your password so that it complies with the password policy which is specified on the dialog screen.


8.1.2 Logout of BIS

To logout of BIS

1. Go to **Operator** menu item  of the side navigation.
2. Select **Logout**.
3. A confirmation dialog will appear if you have unsaved changes (for example, changes to workspace or dashboard configuration). Select **Save** to save or **Discard** to discard the changes, following which you will be logged out of BIS.

8.2 Changing password

To change the password of the current operator

1. Go to **Operator** menu item  of the side navigation.
2. Select **Change password**.
3. In the ensuing dialog, enter the old password.
4. Enter the new password.
5. Confirm the new password.
6. Select **Save** to change the password, following which you will also be logged out of BIS. Otherwise, select **Cancel** to abort the change.



Notice!



The new password must comply with the policy as described in the dialog. You cannot save the password until it matches the specified requirements.

8.3 Changing the interface language

The operator can change the BIS Smart Client interface language by selecting the language from the language selection list on the **Dashboard** title bar. The interface language changes on the fly as you select different language code abbreviations from the language selection list.

8.4 Connection to BIS server

The connection icon on the **Dashboard** title bar indicates the connection status to the BIS server. The following possible status are:

Icon	Connection to BIS server
	Connection is good.
	Connection is lost. You are no longer connecting to the BIS server.

You may be disconnected for one of the following reasons:

- maximum number of users for the license has been reached
- BIS server unreachable
- general network issues
- others

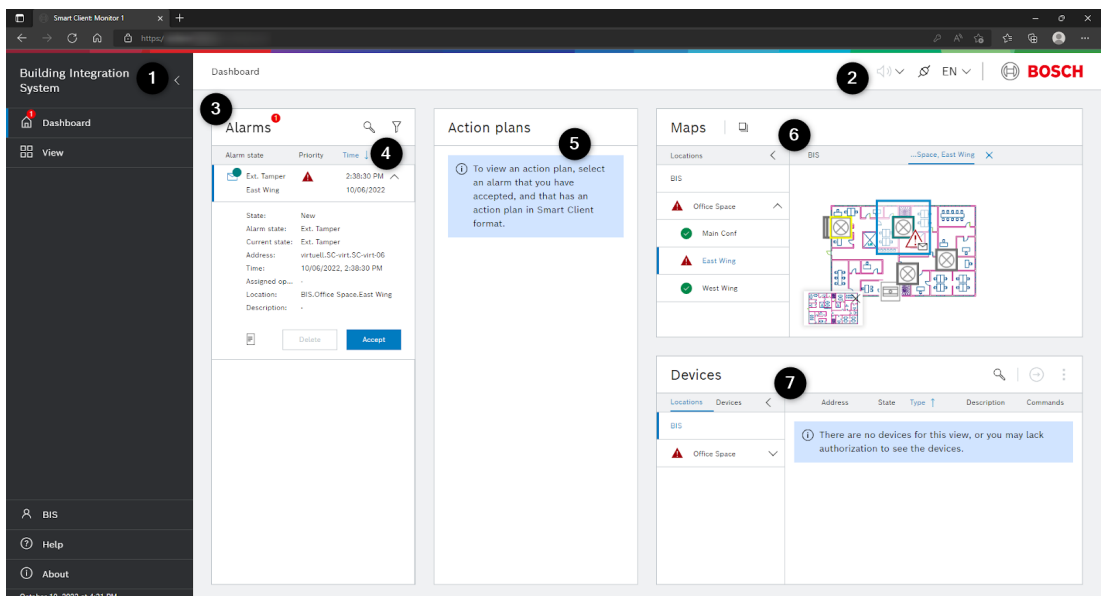
Check with your system administrator to resolve the issue.

8.5 The screen display

8.5.1 Standard screen elements

The screen display explained in this section is subject to possible BIS Smart Client customizations. Customization options can alter what you see on your screen.

This page explains the functions of possible standard screen elements of the BIS Smart Client user interface.




Label	Screen Element
1	Side navigation: collapsible or expandable pane consisting of navigation menu items to load alarms and location maps, invoke customization options of the interface, get system help on using the BIS Smart Client, get system information or to exit BIS.
2	Dashboard title bar: consists of button to mute alarm sounds, showing real-time status of connection with BIS server and interface language selection.
3	Dashboard: consists of customizable collection of widgets, to display alarms, maps of system and objects, or alarm action plans.
4	Alarms widget (example): displays incoming alarms for processing by the operator.
5	Action plan widget (example): displays action plans associated with the alarms.
6	Map widget (example): displays alarms on location maps, and quick navigation using the location tree nodes.
7	Devices widget (example): displays where the devices are being placed.

8.5.2


Side navigation

The side navigation consists of the following elements:

Dashboard

Select the **Dashboard** menu item  to invoke the dashboard, which can be customized to display any, or a combination of the following widgets: **Alarms, Maps, Action Plans** or **Devices**. If the dashboard of the specific monitor contains the alarm widget, the number appearing beside this button represents the number of unprocessed alarms.


View

Select the **View** menu item  to customize the dashboard and workspace.


Operator

Select the **Operator** menu item  to change password or logout from BIS.

Help

Select the **Help** menu item  to invoke the HTML help file for navigating and using the BIS Smart Client within the web browser.

About

Select the **About** menu item  to view a summary of system information, including the operator name, server name, server operating system, language, operator permissions, and BIS version.


Date and time

For display only. Shows the real-time date and time of the BIS Smart Client.


Collapsing and expanding the side navigation

The side navigation can be collapsed to minimize its view, leaving a larger display space for other information. The original view of the side navigation can be restored by expanding it again.

To collapse the side navigation

- ▶ Select the **Collapse** button  beside the Building Integration System title.
- ⇒ The side navigation collapses, taking up a smaller view on the display.

To expand the side navigation

- ▶ Select the **Expand** button .
- ⇒ The side navigation expands, providing a full view of the navigation buttons.




8.5.3

Dashboard

The dashboard is a browser window that an operator can configure to contain an assortment of widgets, which are reusable, modular user interface components. Examples of widgets include alarm widget that can display alarms, map widget for maps of systems and objects, action plan widget for alarm action plans or device widget for location of devices. Being customizable, the user interface may look different between individual dashboards.


Alarms widget

Incoming alarms are displayed in a list in the alarms widget for processing by the operator. The alarm fields are:

- The **Alarm state** of the alarm (new, accepted or forwarded) including location information. An unopened mail  indicates new alarms. An opened mail  indicates accepted alarms. A pointer on the right of an unopened mail  indicates forwarded alarms in a workflow.
- The **Priority** of the alarms, with warning signs varying in color from yellow for low priority to dark red for high priority.
- The **Time** (actually date and time) of the alarms

Select the alarm to expand it to display the details. This action also opens its location map in a tab on the map widget. The details of the alarm are:

- The **State** of the alarm (new, accepted or forwarded)
- The **Alarm state** of the triggering device
- The **Current state** of the triggering device
- The **Address** (location) of the triggering device
- The **Time** (actually date and time) of the alarm
- The **Assigned** operator, who accepted the alarm
- The **Location** of the alarm
- The **Description** of the alarm

If there is an action plan attached to the alarm, it appears with the  icon. To view the action plan in the action plan widget, accept the alarm. If there is no action plan widget on the dashboard, you will not be able to view the action plan.

Map widget

The map widget contains the location tree on the left and the location overview on the right. The location tree shows all connected systems and objects with their respective addresses and line states, as well as other elements identifiable in the system.

You can open any location tree node, as well as sub-nodes beneath a node. Opening the node displays the corresponding location map in the location overview area.

Selecting new alarms in the alarms widget open their corresponding maps in their respective tabs in the location overview.

Action plan widget

An action plan defines in detail what steps should be taken in the event of an alarm. The action plan of an alarm can only be viewed in the action plan widget. If such an action plan widget is not configured for the dashboard, you cannot view the action plan. For more information on the configuration of action plans, refer to the *BIS Configuration Guide*.

Device widget

The device widget contains the device tree on the left and devices overview list on the right. The device widget shows all connected systems and objects in their location, as well as other elements identifiable in the system.

You can view the device tree by location or by device type. Expanding the nodes will display all devices in the devices overview list corresponding to the location or device type.

8.6

Manual backup of workspaces and dashboards

User-created workspaces and dashboard layouts are not covered by the BIS integrated backup or restore tools. If you intend to create a significant number of workspaces or dashboards, you can back up and restore them manually using the *SQL Server Management Studio*.

To create a backup of workspaces and dashboard layouts

1. Launch *SQL Server Management Studio* and connect to the SQL Server instance for BIS (named "BIS" by default).
2. Go to **Databases** node, locate the **SmartClient.Shell** database.
3. Right-click the **SmartClient.Shell** database item, and select **Tasks > Back Up...** from the context menu.
4. Configure the backup parameters as suits your needs, then select **OK** to commence the backup.

To restore a backup of workspaces and dashboard layouts

1. Using *IIS Manager*, ensure that the Smart Client application is stopped. If needed, stop its application pool (**Server root > Application Pools > Smart Client Shell AppPool**).
2. Launch *SQL Server Management Studio* and connect to the DQL Server instance for BIS.
3. Go to **Databases** node, ensure that there is no **SmartClient.Shell** database item. Delete it if necessary. Note that this will remove any workspaces and dashboards that may have been created since the last backup.
4. Right-click the **Databases** node, and select **Restore Database...** from the context menu.
5. Locate the backup you created earlier (e.g., by specifying the backup file under **Source > Device**), and configure the restore parameters as needed.
6. Select **OK** to restore the **SmartClient.Shell** database from the backup.


- 7. Using **IIS Manager**, start the Smart Client application again by starting its application pool (see step 1).

8.7 BIS alarm processing

8.7.1 Processing an alarm

How you process an alarm depends on the scope and configuration of your BIS system. There are only a few rules, which are generally applicable.

- Ensure that you are familiar with any local rules and procedures for your site, which can be consulted quickly in an emergency.
- If an alarm arrives, keep calm.

Step #	Step	Procedure
1	Suspend the acoustic signal while making a first assessment of the situation.	Select the Mute once button  to mute once.
2	Assess the overall situation if faced with several simultaneous alarms.	Browse through the lines of alarms to find common reference points for the pending alarms. This will help you to decide on the order or processing. Note: it may be helpful to sort the list by clicking the header of Priority or Time columns.
3	View documents.	Select the alarm to view the map. You may find important information that will help you process the alarm.
4	Accept the alarm.	Select the alarm, and then select Accept .
5	Execute the required procedure.	View the action plan in the action plan widget. Execute the steps listed in the action plan.
6	After processing, delete the alarm.	Select the alarm, and then select Delete .


8.7.2 Standard features of an alarm



The following section describes features that are standards to alarms in BIS.

Acoustic signals

When an alarm arrives, the system produces an audible signal.

To mute the sound once (temporarily)

- ▶ On the **Dashboard** title bar, select the **Mute once** button  .
- or

1. On the **Dashboard** title bar, select the **Down** button  beside the **Mute once** button .
2. Select **Mute once**.

This mutes the sound temporarily until the operator refreshes the web browser, or applies a different workspace to the session.

Otherwise, the operator can also choose to mute the sound permanently.

To mute the sound permanently

1. On the **Dashboard** bar, select the **Down** button  beside the **Mute once** button .
2. Select **Mute permanently**.

This mutes the sound permanently for the session, until the operator logs off and logs in again.

Display of alarm location

When a new alarm arrives, select the alarm to show its location map in a tab in the location overview of the map widget. The map zooms into the object by using the named view that issues the alarm. If the map navigation pane is obscuring the view of this object, BIS Smart Client automatically collapses the map navigation pane into a tiny map icon.

Alarm states

Alarm State	Description
New	All alarms that have not been accepted by any operator are marked as new.
Accepted	All alarms that have been accepted by any operator are marked as accepted.
Forwarded	An alarm is marked as forwarded if it was accepted by another operator, but was forwarded to you for further processing.

Note: The colored circles tagged to the alarm icons are color codes of the device states. In BIS, the states of the device are differentiated by different color codes.

The alarm list

The alarm list shows all alarms.

- Sort the list by selecting the header of the column by which you wish to sort. The currently sorted field name is highlighted in a different color and an arrow indicating the sorting order. An upward pointing arrow indicates sorting in ascending order, and a downward pointing arrow indicates sorting in descending order. Selecting the header again will sort the list in the opposite order.
- Filter the list by selecting the filter criteria, or search the alarm using the search function.
- Select the alarm to expand and show more details. This also opens the location map in a tab in the display area of the map widget. The map zooms into the object that issues the alarm.

- The operator can accept and process the alarm.
- The highlighted number in the badge of the alarms widget represents the number of unprocessed alarms in the list.



Notice!

New alarms are always inserted according to the currently sorted field name.



Notice!

In the Smart Client, it is not possible to configure the alarm to be handled exclusively. If the alarm is configured as such in the Classic Client, and was accepted from a Smart Client,

- no Classic Clients will show the message
- all Smart Clients will show the message

The dwell time of an alarm

In general, an alarm disappears from the alarms list only when deleted.

Exception:


- If during alarm processing the same object issues a new alarm with the same or higher priority, the initial alarm is overwritten.
- If another alarm with a lower priority arrives, the original alarm is not overwritten; the new alarm appears in addition to the original alarm.
- If the first alarm is already being processed when a new alarm arrives, it is not overwritten. The second alarm appears in addition to the original alarm

8.7.3


Searching for specific alarms

You can search the alarm list for alarms that match your input text. You can enter any text in the search input field. This search is an incremental search that instantly filter possible matches as you type the search text in real-time.

To search for an alarm

1. On the **Alarms** title bar, select the **Search** button .
2. Enter the search text in the **Search** text area.

To clear the search result

- ▶ On the **Alarms** title bar, select the **Close** button .
- or
- ▶ Select the **Esc** key.
- ⇒ This clears the search result and shows all alarms in the list.

8.7.4

Filtering alarms

You can filter the alarm list to show only specific alarms based on selected criteria from the following categories:




- state
- priority

- time

To toggle the visibility of the filter categories

- ▶ On the **Alarms** title bar, select the **Filter** button  to hide or show the filter categories.

To filter the alarm list


1. On the **Alarms** title bar, select the **Filter** button  if the filter categories are not visible.
2. Select the **Expand** button  beside the category to expand it if it is not already expanded.
3. Select the desired criteria.
4. Select the **Collapse** button  beside the category to collapse it if you wish to hide the criteria of the specific category.
5. Repeat the steps above for all other filter categories if so desired.


As you select a criterion from the specific category, the number beside the category reflects the number of selected criteria for the category.

To hide the filter categories


- ▶ Select **Hide filters** (just below the **Alarms** title bar).

or

- ▶ On the **Alarms** title bar, select the **Filter** button .

⇒ The filters are hidden from view. The number appearing beside the **Filters** button  reflects the number of chosen filter criteria.


To clear the chosen filter criteria

1. On the **Alarms** title bar, select the **Filter** button  if the filter categories are not visible.
2. Select **Reset** (just below the **Alarms** title bar).

8.7.5

Action plans of an alarm

Action plans (optional component) are created in advance by system administrators, and not by the operator. An action plan defines in detail what steps should be taken in the event of an

alarm. An alarm with an action plan is indicated by the **Action plan** icon .

An action plan is not displayed until an operator accepts the relevant alarm. Select the alarm, and then select **Accept** to view the action plan in the action plan widget. This means that if your dashboard is not customized with the action plan widget, you will not be able to view the action plan.

8.7.6

Notes on accepting and deleting alarms

An alarm remains in the alarms display list until it is deleted, then it disappears from the list.

The alarm can be accepted to be processed. You must distinguish between two types of alarms.

- Alarms without an action plan: These alarms can be accepted and deleted individually at any time.
- Alarms with an action plan: Action plans usually have mandatory actions. You can accept but cannot delete these alarms.
 - If the dashboard contains an action plan widget, select **Accept** to accept the alarm and view the action plan in the action plan widget.
 - If the dashboard does not have an action plan widget, selecting **Accept** will not show the action plan. In the ensuing dialog, select **Accept** to accept the alarm without viewing the action plan, or **Cancel** to leave the alarm as new.

You can also select multiple alarms for processing at the same time if they do not have action plans. Alarms with action plans require special set of rules for processing.

To select multiple non-contiguous alarms

1. Select an alarm from the alarm list.
2. While pressing the **Ctrl** key, select another alarm from the alarm list.
3. Repeat for any other alarms that you wish to process together.

Note: All selected alarms are highlighted by a thin blue bar towards their left.

To select multiple contiguous alarms

1. Select the first alarm of the contiguous list from the alarm list.
2. While pressing the **Shift** key, select the last alarm of the contiguous list from the alarm list.

Note: All contiguously selected alarms are highlighted by a thin blue bar towards their left.

To process the selected alarms

1. Right-click any selected alarms.
2. Select **Accept** to accept or **Delete** to delete the alarms in the context menu.
3. In the ensuing confirmation dialog, select **Accept** to accept the alarms, or **Delete** to delete the alarms, or **Cancel** to abort the operation.

8.8 Location overview

8.8.1 Purpose of the location overview

The location overview and associated location maps show all locations:

- Locations at which detectors and sensors are placed
- Locations to which graphics, areas (named subareas of graphics, for example South Entrance), and alarm-dependent layers are assigned

The devices must be linked to a location for them to be viewed in the BIS Smart Client. The devices placed there are shown in the location maps with their current line states. Hover over the device icons to display their details.

If an alarm arrives, the top-level node, and the immediate parent node of the device will display an alert in the shape of a red triangle in the location tree.

8.8.2 Patterns of the detector symbols

The following settings are possible (individually or in combination)

- Colored frame around the symbol (dark grey in normal state, other colors in other states)
- Colored warning triangle beside the symbol
- Unopened mail, opened mail, or unopened mail with a pointer on the right beside the warning triangle to indicate status of the alarms (new, accepted or forwarded)

8.8.3 Giving commands to a selected detector

There are two ways to send a command to a detector via the location graphic map:

1. Right-click the detector symbol. If your authorization is sufficient, a context menu opens, listing the commands available for this detector. Select the desired command in the context menu.
 - Commands requiring input parameters will present a dialog where you can enter the desired value. The **OK** button is disabled by default. It is only enabled if the entered value is valid. Once enabled, you can proceed to invoke the command by selecting **OK**. Otherwise, select **Cancel** to abort.
 - Commands not requiring input parameters will execute immediately.
2. Alternatively, double-click the detector symbol to invoke the **Fast Access Command** defined in the **BIS Configuration Browser** for this detector type. The **Fast Access Command** is the default command among those listed for the detector types. If none has been defined, then an explanatory error message appears.

You can also select multiple detectors to send a command. Note that only common commands between the multiple detectors will be visible.

To select multiple detectors to send a common command

1. Select the detector symbol.
2. While pressing the **Ctrl** key, select the next detector symbol.
3. Repeat until all detectors that you desire are selected.
4. Right-click any detector symbol.
5. Select the desired command in the context menu.

8.8.4 View or hide map layers


The location maps are made up of multiple different layers. You can choose to view only layers that you wish to see by toggling the visibility of each layer in the location overview.




Notice!

BIS Smart Client remembers the layer selections for the last operator. To view all layers, reset the visibility of the map layers.


To toggle the visibility of the map layers

1. On the **Map** title bar, select the **Layers** button  to show the list of layers.
2. From the list of layers, select to show, or deselect to hide them on the fly.
3. Select **Hide layers** to hide the list of available layers.

The number next to **Hide layers** represents the number of layers currently hidden from view.

The **Layers** button  remain in blue color as long as there are layers that are deselected.

To reset the visibility of the map layers

1. On the **Map** title bar, select the **Layers** button  if the layers list is not visible.
2. Select **Reset** to make all layers visible again.

8.8.5

Viewing multiple maps

Selecting an object in location tree opens the associated map in the location overview area. You can also open multiple maps in their respective tabs in the location overview.

To open a map in its tab

1. Right-click the desired location object in the location tree.
2. Select **Open a new tab** from the context menu.



8.8.6

Map navigation aids

Using location overview to assist with alarm processing, BIS Smart Client provides a number of navigation aids for the graphical maps. This includes a map navigation pane and zoom, pan and tilt functions.

Map navigation pane

A map navigation pane is always available at the bottom left corner of the location overview. The area shown in the main display is outlined in blue in the navigation pane. This helps to locate alarms in relation to the entire site.

You can minimize this map navigation pane by selecting its collapse button . The map navigation pane then collapses into a tiny map icon . To expand the map navigation pane, simply select the tiny map icon.

Zoom, pan and tilt

Use the mouse to zoom in (close-up), zoom out (wide view) and panning (horizontal or vertical) of the location overview. Zoom and pan make it possible to navigate rapidly through alarm locations, as well as selected parts of the map for display and printout. Tilt makes it possible to angle the map to view it in a three dimensional perspective.

Move the mouse within the boundaries of the location graphic map until the pointer becomes




. Drag the location graphic to pan the map in two dimensions, horizontally or vertically.

Zoom in by scrolling the mouse wheel upwards; zoom out by scrolling the mouse wheel downwards. Tilt the location graphic map by selecting the **Shift** key and pan it at the same time.

To reset the map in two dimensions

- ▶ Select the node of the map in the location tree.
- or

- ▶ On the **Map** title bar, select the **Restore to initial view** button  .
- or
- ▶ Select the tab of the map.

8.9 Devices overview

8.9.1 Purpose of the devices overview

The devices widget shows the locations where the devices are being placed. The devices must be linked to a location for them to be viewed in the BIS Smart Client.

To view the devices by location

- ▶ Select **Locations** from the **devices** widget.

To view the devices by devices type

- ▶ Select **Devices** from the devices widget.

Expand the nodes from the tree to view the devices and their information in the devices overview list. Information of the devices include addresses, current line states, types, descriptions and available commands. Hover over the information to display their details.

If an alarm arrives, the top-level locations node, and the parent location node of the device will also display an alert in the shape of a red triangle in the device location tree.

To sort the devices overview list

- ▶ Select the header of the column by which you wish to sort. The selected sort column is highlighted in a different color with an arrow indicating the sorting order. An upward pointing arrow indicates sorting in ascending order, and a downward pointing arrow indicates sorting in descending order.


To toggle sorting order of the devices overview list

- ▶ Select the sorted header which is highlighted with an arrow. This will sort the list in the opposite order.


8.9.2 Searching for specific devices

You can search the devices list for devices that match your input text. You can enter any text in the search input field. This search is an incremental search that instantly filter possible matches as you type the search text in real-time.

To search for a device

1. On the **Devices** title bar, select the **Search** button  .
2. Enter the search text in the **Search** text area.

To clear the search result



- ▶ On the **Devices** title bar, select the **Close** button  .

or

- ▶ Select the **Esc** key.
- ⇒ This clears the search result and shows all devices in the list.

8.9.3 Giving commands to a selected device

There are a few ways to send a command to a device via the devices widget:

1. Select the **Fast Access Command**  of the device to invoke the command defined in the BIS Configuration Browser for this device type. The **Fast Access Command** is the default command among those listed for the device types. If none has been defined, the **Fast Access Command** is disabled.
2. Select the **Options**  of the device. If your authorization is sufficient, a context menu opens, listing the commands available for this device. Select the desired command in the context menu.
 - Commands requiring input parameters will present a dialog where you can enter the desired value. The **OK** button is disabled by default. It is only enabled if the entered value is valid. Once enabled, you can proceed to invoke the command by selecting **OK**. Otherwise, select **Cancel** to abort.
 - Commands not requiring input parameters will execute immediately.
3. Alternatively, right-click the device. If your authorization is sufficient, a context menu opens, listing the commands available for this device. Select the desired command in the context menu. If there are no commands defined for the device type, right-clicking the device shows the “no command” message.

You can also select multiple devices to send a command. Note that only common commands between the multiple devices will be visible.

To select multiple devices to send a common command

1. Select the device.
2. While pressing the **Ctrl** key, select the next device.
3. Repeat until all devices that you desire are selected.
4. Right-click any device.
5. Select the desired command in the context menu.

8.9.4 Working with subdevices

Some devices may have subdevices that represent additional aspects associated with the main device, for example, individual sensors. To view and work with subdevices, select the arrow next to the device name to reveal them.

9 Control

9.1 Controlling with BIS

Depending on the configuration, BIS offers several means of controlling connected devices (for example, bringing elevators to the ground floor, or closing gates). You can trigger control events in standby mode of the system, as well as during message processing.

Controls are executable in the following ways, as described in detail in the following sections:

1. From the location tree
2. From the location graphic (location plan)
3. From the devices overview
4. From an action plan (possible only during message processing)
5. From miscellaneous documents
6. Through buttons on the operator interface



Notice!

All control events can be entered in the Event Log with the name of the triggering operator.

9.2 Controlling from the Location Tree

If configured, controls can be activated from the location tree (for example, a reset or an operator alarm). Proceed as follows:

1. Right-click the desired location in the location tree. If your authorization is sufficient a menu opens.
2. Left click the desired command and enter other control parameters in the ensuing input box.

When controlling from the location tree, the commands always act on the relevant location, not on individual elements placed there.

9.3 Controlling from the Location Graphic

If configured, controls can be activated from the location graphic for individual elements (for example, the reset of a certain detector). Proceed as follows:

1. Select the desired location in the location tree. This displays the relevant location graphic.
2. Right-click an element in the location graphic (for example, a detector). If your authorization is sufficient a menu opens.
3. Left click the desired command and enter other control parameters in the ensuing input box.

You can activate controls from the location graphics in standby mode as well as in message mode.

9.4 Controlling from the Device Overview

If configured, controls can be activated from the device overview by right-clicking the device. Proceed as follows:

1. Click the **Device overview** tab in the display container.
2. Navigate through the structure tree of the device overview until you reach the desired unit. Details are listed.

3. Right-click the desired line in the overview. If the configuration is correct and the authorization is sufficient, a menu opens.
4. Left click the desired command and enter other control parameters in the ensuing input box.

The Device overview can also be used to create backups of the Event Log. For more details see *Event Log contents and backup, page 71*

**Notice!**

You can activate controls from the device overview in standby mode as well as in message processing mode.

9.5

Controlling from an Action Plan

Action plans are created by system administrators and not by the operator. For more information please consult the BIS Configuration online help. This section describes basic aspects of action plans (where suitably configured). Please see the following section for more details *Action Plans, page 37*

As action plans are always associated with a certain message, control events can be triggered from an action plan only during the processing of the message (i.e. after the operator has accepted the message).

Controls from an action plan are usually manually executed by clicking the appropriate Action buttons, see *Controlling with Action Buttons, page 63*. Nevertheless, system administrators may also configure automatic controls in the action plan.

Action plans and related processing are entered in the log book along with the messages which invoked them.

9.6

Controlling with Action Buttons

Action buttons are a basic but powerful kind of manual control in the system. They can activate general scripts via ActiveX as well as influencing the states monitored by the BIS state machine. See also *Action Plans, page 37*.

Action buttons are not necessarily message related and can be configured to appear in the BIS operator interface outside of action plans.

Examples of action buttons on the BIS operator interface:

- **Emergency OFF** action button stops the operation of escalators with one mouse click
- **Camera 1** through **Camera 4** action buttons switch the display to the appropriate camera at the matrix
- **Alarm simulation** action button simulates an alarm for testing and exercise purposes

10 Operator Alarms

10.1 Operator Alarms

An operator alarm is an alarm that is triggered manually by the operator in response to external information (e.g. a threat by telephone, or something the operator witnesses personally), and not automatically detected through a subsystem.

An operator alarm is like a normal alarm in that it is always linked to a specific message location and has a state change associated with it.

BIS handles the operator alarm like a normal alarm, that is, it executes controls defined for that alarm location, and makes state changes.

An operator alarm message must be handled by other operators like any other alarm.



Notice!

The operator alarm is an optional feature and may not be enabled on your system. Contact your system administrator for more information.

10.2 How to Trigger an Operator Alarm

Depending on the configuration, there are two ways to trigger an operator alarm:

- **By using action buttons on the operator interface**

The system administrator may place an action button with the **Operator alarm** function on the BIS UI. For more information please consult the BIS Configuration online help. Because the operator alarm must always be linked to a certain message location and state change, this information must be entered manually in a separate input box after clicking the button.
- **Through the right mouse button menu**

An operator alarm can also be triggered when the operator right clicks on a message location in the location tree.

11 Simulated Alarms

11.1 Simulated Alarms

Simulated alarms are useful for testing the Associations (If-Then rules) in a BIS configuration, to test the display of message documents, or to train operators in message processing. The simulated alarm command in fact simulates only a state. Whether a simulated alarm is in fact generated depends on whether an Association exists that is triggered by the simulated state.

Simulated alarms generate only a message on the screen, which must be accepted and processed by the operator even though they have no real consequences.

So that simulated alarms can be distinguished from real alarms, they are only visible in the message display field, See *Standard Screen Elements, page 19*

Simulated alarms have the same priorities as real alarms. They are processed the same way, and are sortable according to their priority and timestamps alongside real alarms. The only differences are:

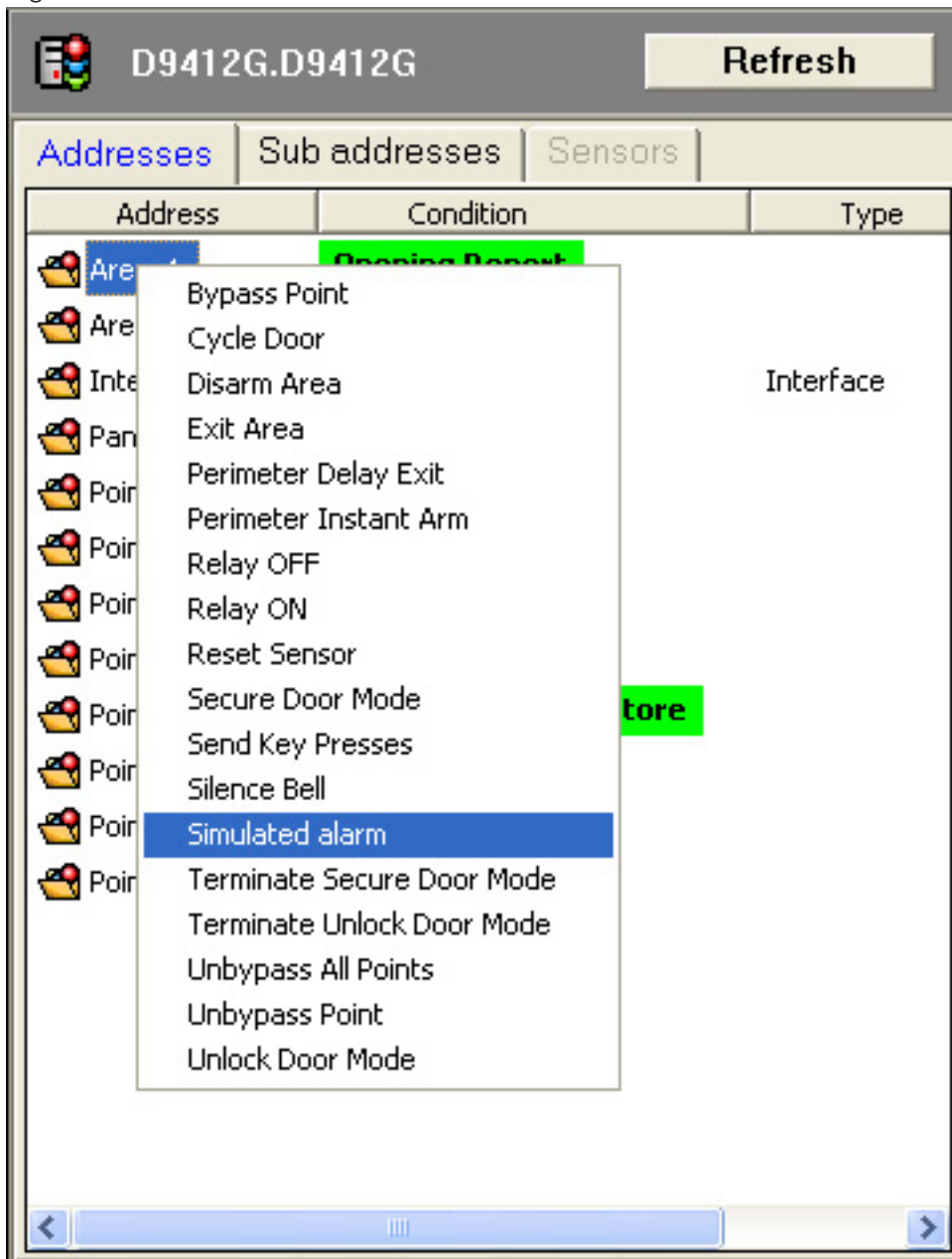
- The **Current State** of the alarm message is unaffected. The **Alarm State** is displayed in struck-through text in order to distinguish it from a real alarm.
- Simulated alarms produce only messages. They do not trigger any state-changes or commands

11.2 How to Trigger a Simulated Alarm

Simulated alarms can only be triggered through detector icons.

1. Select a location in the location overview, or a detector in the device overview.

2. Right-click the location or detector and select **Simulated alarm**.



3. Enter a state number in the ensuing dialog.
4. Note that an alarm message will only appear if the state change triggers an Association that generates an alarm. See the BIS Configuration online help for details.

12

Printing

12.1

Printing with BIS

The system administrator can configure different printers for the different events in BIS (for example, fault messages can be sent to a specific printer).

Printing can be started manually or automatically (i.e. by automatic printing rules in the BIS Configuration). See the BIS Configuration online help for details.

12.2

Log Printing

System configuration determines which events trigger printing, and which information is included in the printout. See the BIS Configuration online help for details.

The printer configured as the log printer must be accessible from the BIS login server, because printing events are controlled from there.

The system monitors the printing function. No manual override is possible on log printing.



Notice!

The printer **must** be configured to use the operating system's **printer spooler**. If this is not done, printing will not be asynchronous, resulting in reduced BIS server performance.

12.3

Alarm Printing

System configuration determines which alarm events trigger a special printout, and what information is included. The following is a brief summary of the possibilities. See the BIS Configuration online help for details.

The printer configured as the alarm printer must be accessible from every workstation. Printing can be started manually or automatically (i.e. by automatic printing rules in the BIS Configuration). See the BIS Configuration online help for details.



Notice!

The printer **must** be configured to use the operating system's **printer spooler**. If this is not done, printing will not be asynchronous, resulting in reduced BIS server performance.

Time of printout

For each alarm location and alarm state the system can be configured so that printing is automatic on the arrival, or alternatively upon acceptance of an alarm, and which location graphic should be printed with the message.

Macros in the document


If the documents to be printed contain macros, they are instantiated by current information at the time of printing (for example, the name of the operator who just logged in).

Layers in the document

If the location graphic to be printed contains **layers (e.g. the layer of the triggering detector)**, the configuration can individually include or exclude any layers from the printout.

12.4 Printing Manually

Printouts can be triggered manually on all printers configured as alarm printers.

1. Click  in the tool bar above the location overview.
2. Select the printer and its properties, then start the print job.

While printing from the location overview (graphic display), the graphic of the current alarm message is always printed. In all other cases, the currently displayed document is printed.

13 Sending Messages to Operators

13.1 Sending Messages to Operators

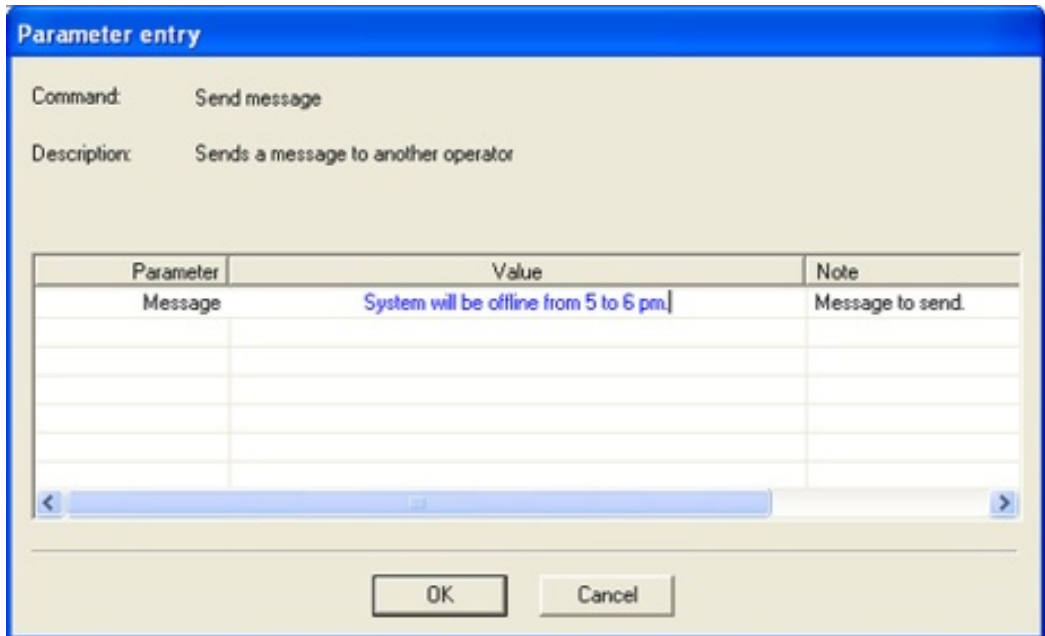
Within BIS logged-in operators can exchange short messages between their workstations. The command is called **Send message** and can be invoked from the context menus of operators, for example in the Location or Device overviews.

The following example describes how a message to any operator is triggered from the **Device overview**.

1. Select the **Operators** node in the device tree of the device overview. All configured operators are listed. You can identify, with the help of the status display, which operators are currently logged onto the system.
2. Right-click one of the logged-on operators. A menu appears, from which you select **Send message**.



3. In the entry dialog that appears, in the **Value** box, enter the text of the message you want to send to the operator, then click **OK** to send the message.



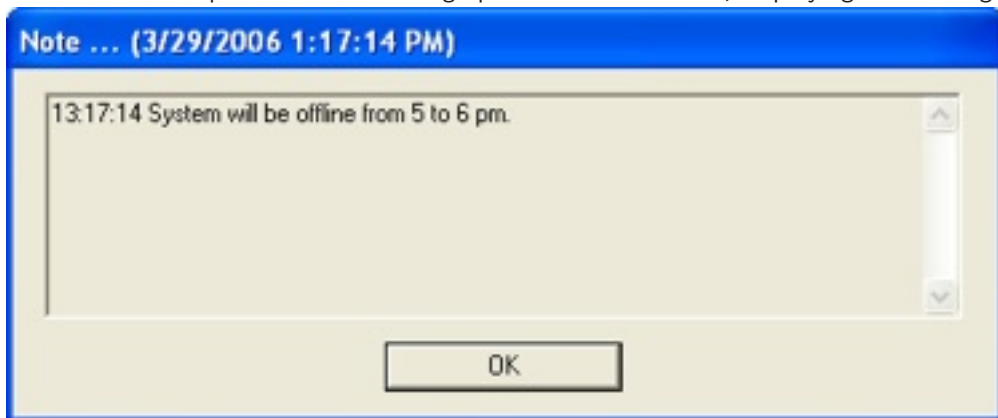
The image shows a 'Parameter entry' dialog box with a blue title bar. It contains the following information:

Command: Send message
Description: Sends a message to another operator

Parameter	Value	Note
Message	System will be offline from 5 to 6 pm.	Message to send.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

A small window opens on the receiving operator's workstation, displaying the message.



The image shows a 'Note ... (3/29/2006 1:17:14 PM)' window with a blue title bar. It displays the following text:

13:17:14 System will be offline from 5 to 6 pm.

An 'OK' button is located at the bottom of the window.

14 Event Log

14.1 Event Log contents and backup

All system events are logged in the Event Log. The type of entries stored in the Event Log is configurable.

Events in the Event Log can include:

- Operator logons and logoffs
- State changes
- Automatic and manual controls
- Message processing events



Notice!

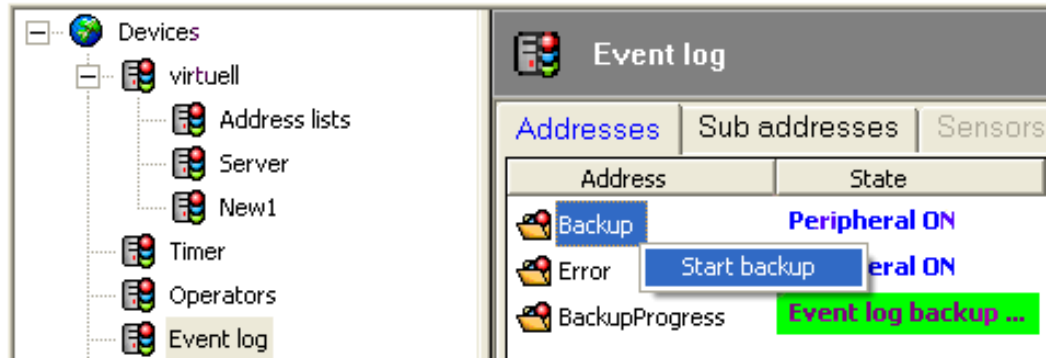
The system always logs configuration changes made with Admin9000. These changes are visible to every operator.

Security Engine card holders are part of the **common** division. These card holders are visible to every operator.

Backup of the Event Log

It is possible to backup the Event Log database from the Device Overview and from the BIS Manager.

- For backing up the Event Log from the BIS manager please consult the **BIS Configuration online help > BIS Manager > BIS Manager tabs > Event Log**
- To back up the Event Log from the Device Overview proceed as follows:
- From the BIS main screen click the **Device Overview** tab, then in the **Devices** hierarchy click **Event Log**, then in the main Document Display area right click on **Backup** and select **Start backup**.
- When prompted enter a valid path for the backup (see note below), the maximum number of backups allowed in that path, and 1 or 0 depending on whether already backed-up entries should be deleted (1) or not (0).



Notice!

From the Device Overview it is only possible to backup the Event Log database to a local or a valid UNC path (\\<servername>\<sharename>\<path>), **not** to a mapped drive. Moreover the BIS user process must have write-access to this UNC path, i.e. the same user/password combination must exist on \\<servername>.


Any drive letter which is used instead of a UNC path refers to a drive on the BIS login server, and not on the local machine (unless these happen to be identical).

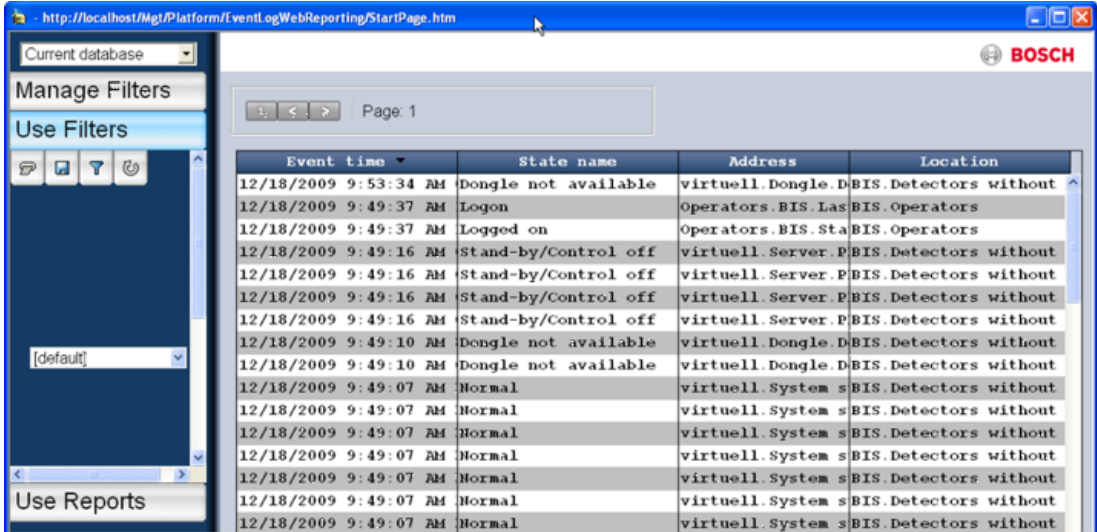
Hence if you wish to back up the Event Log to a local machine that is not the BIS login server you must use a UNC path.

From the BIS Manager it is however possible to backup to a mapped drive, provided the windows account under which the BIS Manager is running has write-access to this mapped drive.



14.2 Event Log User Interface

Click , in the navigation toolbar to start the Event Log application.



Event time	State name	Address	Location
12/18/2009 9:53:34 AM	Dongle not available	virtuell Dongle.D	BIS.Detectors without
12/18/2009 9:49:37 AM	Logon	Operators.BIS.Las	BIS.Operators
12/18/2009 9:49:37 AM	Logged on	Operators.BIS.Sta	BIS.Operators
12/18/2009 9:49:16 AM	Stand-by/Control off	virtuell.Server.P	BIS.Detectors without
12/18/2009 9:49:16 AM	Stand-by/Control off	virtuell.Server.P	BIS.Detectors without
12/18/2009 9:49:16 AM	Stand-by/Control off	virtuell.Server.P	BIS.Detectors without
12/18/2009 9:49:16 AM	Stand-by/Control off	virtuell.Server.P	BIS.Detectors without
12/18/2009 9:49:10 AM	Dongle not available	virtuell.Dongle.D	BIS.Detectors without
12/18/2009 9:49:10 AM	Dongle not available	virtuell.Dongle.D	BIS.Detectors without
12/18/2009 9:49:07 AM	Normal	virtuell.System.s	BIS.Detectors without
12/18/2009 9:49:07 AM	Normal	virtuell.System.s	BIS.Detectors without
12/18/2009 9:49:07 AM	Normal	virtuell.System.s	BIS.Detectors without
12/18/2009 9:49:07 AM	Normal	virtuell.System.s	BIS.Detectors without
12/18/2009 9:49:07 AM	Normal	virtuell.System.s	BIS.Detectors without
12/18/2009 9:49:07 AM	Normal	virtuell.System.s	BIS.Detectors without
12/18/2009 9:49:07 AM	Normal	virtuell.System.s	BIS.Detectors without

On the left panel of the window appear controls for changing database settings, setting filters and initiating searches:

- A control for selecting the **Database**
- **Manage Filters** button for adding, editing and deleting filters
- **Use Filters** button for applying the filters you have defined
- **Use Reports** button for running predefined or user-defined reports

The **Database** selector enables you to search other event log databases which may be present on your system. The default setting is the current database.






The **Manage Filters**, **Use Filters** and **Use Reports** buttons function as vertical tabs or “Outlook buttons”.

- The **Manage Filters** tab is closed by default when the Event Log is started. Clicking **Manage Filters** will display a set of horizontal tabs in which search filter settings can be configured, modified and saved. Saved filters can be invoked by name from the **Filter - Search** tab. Details about how to use the **Manage Filters** tab can be found under *Managing Filters, page 73: Creating and Modifying Filter Settings*

- The **Use Filters** tab is closed by default when the Event Log is started. This tab is used for invoking Event Log searches based on the named filters configured under the Reports tab, or invoking ad hoc searches. The results can be displayed here and saved for further processing. Details about how to use the **Use Filters** tab can be found under *Using Filters, page 75: Starting and refreshing searches*
- The **Use Reports** tab is open by default when the Event Log is started. This tab is used for invoking predefined or user-defined reports. The results are displayed here and can be saved for further processing. Details about how to use the **Use Reports** tab can be found under *Using Reports, page 76: Starting and refreshing reports.*

Navigating through the results

In the main pane of the dialog the results of the search are displayed in columns whose number and order are determined by the filter. When the Event Log is first invoked a new search is started based on the **default** filter, and the results displayed here. Note that if a button is gray it is not active. This is because the desired page has been reached or does not exist. Examples:

-  You are already on the first page of results.
-  Go to the first page of results.
-  Go back through the results by one page.
-  You are already on the first page of results.
-  Go forwards through the results by one page.

The text **Page <n>** to the right of these buttons indicates the number of the page currently displayed.

Formatting the time stamp

The format of the time stamp in the Event Log is determined by the Windows registry key `HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\International\Accept Language`

To change the format flexibly, delete this key if it exists, and set the format in browser's regional and language settings. To do this, navigate to:

Internet Explorer > Internet options > General tab > Appearance, Languages > Set Language Preferences


The Event log will take the language format that is uppermost.





14.3 Managing Filters

Click the **Manage Filters** Outlook button for a dialog page containing tabs for defining filter criteria.

The purpose of filters is to focus on the essential and exclude unnecessary event messages. The user interface supports the saving and reuse of filters you have defined and named. By contrast, the **Use Filters** Outlook button allows you to search with criteria defined on-the-fly.

A series of smaller buttons below the **Reports** button in the left-hand tool bar provide the following functions:

Button	Function	Description
	Add a new filter.	A new entry New Filter , appears in the list of filters below the buttons. This filter still lacks a definition.

	Save selected Filter	Saves the changes made to the selected filter.
	Copy selected filter	Creates a copy of the selected filter with all the settings of the original.
	Delete selected filter.	The selected filter is deleted; Note: No confirmation is requested. The default filter, with the black icon, can not be deleted.
	Revert to last saved filter data.	All changes made to filters since the last save (N.B. not just the last change) will be discarded. The last saved settings are reloaded.

Default filter

A default filter **[default]** is always present. It can be modified and renamed but not deleted. This filter is applied as soon as the Event Log is invoked, and contains the following settings:


- Date/Time:
 - a relative time filter covering the events of the past 2 hours
- Visible Columns:
 - Event time
 - State name
 - Address
 - Location



Notice!


The [default] filter appears at the top of the list, due to the alphabetic value of its first character. If you change the name its alphabetical position in the list will may also change, but it will remain recognizable by its black icon, whereas all other filters have blue icons.

Creating new filters

Click  to create a new filter called **New filter**. The tabs for defining the filter appear. Two text fields appear above the tabs: The fields **Filter** and **Description** allow you to change the default name and give the filter a descriptive explanation.



Notice!

A new or modified filter is marked with an asterisk * in the **Filter** field. At the same time the  button becomes active, enabling you to discard unsaved changes if desired.

The only predefined setting is that of **Visible columns** for the results list.


The columns are:


- Event time
- State name
- Address
- Location

For all other filter types there is no predefined setting.

Copying the current filter

To create variants of existing filters a copy function is available.

Select the filter whose settings you wish to copy and click . A copy of the filter is added to the end of the list, under the name **Copy of** <Name of original filter>.

Give the filter a new name and make the desired modifications. Save the filter using the  button.

14.4 Using Filters

Introduction

In the **Use Filters** menu, which is also displayed when the Event Log is invoked, you can search for (filter), print and save database entries. You can experiment with temporary changes to filters, and browse back and forth within filter results of the current session.








Notice!

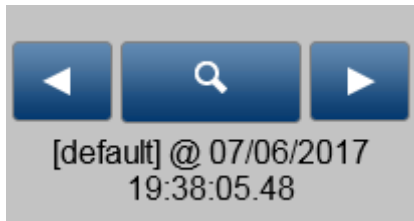
To prevent Event log from taking too much processing power from the system, searches will return a maximum of 10,000 records and then display a warning: **Maximum number of result rows exceeded.**



Workaround: Use a more restrictive filter to limit the number of results to 10,000 or fewer.

Procedure

1. In the BIS Client, click **Event Log**. The application appears in a separate window.
2. Select the desired database in the upper combo-box.
3. Select the desired filter from the drop-down list.
4. If desired, use the  button to check or temporarily change the selected filter. If you make a change the filter name will be marked with an asterisk.
5. Click the search button  to search the database using the filter in the drop-down list. If you modified this filter in the previous step, it will be marked with an asterisk.
 - To sort the results by the contents of a column (ascending or descending) click the column headers. **NOTE:** This causes the database query to be reissued using the new sort criteria, and does not simply re-sort the list of results already obtained.
 - To save temporary changes to filter settings click the **Manage Filters** menu. The changed filter will be marked with an asterisk, and you will need to click the  button to save, or the  button to discard, before you can use other filters.
 - To discard temporary changes to filter settings click the  button. The filter reverts to the settings last saved in the **Manage Filters** menu.

6. (Optional) Click the arrow buttons to the left and right of the search button to move back and forth within this session's history of search results. When you do this, the name of the filter used, and the date and time of its execution, is displayed along with the search button.




- Click the  button to save the results that are currently on the screen. They are saved to a CSV file where they can be further processed using Microsoft Excel. Note that the file name and file path are unmodifiable:
<Installation drive>:\MgtS\Export\BIS\lastResult.csv
Therefore ensure that any previous results that you wish to keep are saved under a different name before performing further exports.
 - **NOTE:** only the results are saved, not the filter settings. Filter settings can only be saved in the **Manage Filters** menu.
7. (Optional) To copy a line from search results, click in the desired line and press Ctrl-C. The line is copied to the Windows paste buffer and can be pasted from there into other applications.
8. (Optional) To print the results list click the  button. The layout is predefined and can not be changed. The first page of the printout gives details including the date and filter settings used. Ensure that the print version does not contain too many columns for the width of the output medium. Use the filter tab **Visible Columns** to choose which columns appear and in what order.

14.5 Using Reports

In the **Use Reports** Outlook button you can run predefined or user-defined reports.

Note, reports can not be created within BIS. Reports can be created by system administrators in the **MS Report Builder** tool outside of BIS. Please see the Report Builder tool's own online help for further details.

Once an administrator has created a new report and placed it in the BIS Reports default

directory, then click the refresh button  to include the new report on this Outlook button.

Predefined reports

The predefined reports available after the installation of BIS are:

Report name	Description
Distributed Events	A tabular report (new as of BIS 4.0)

	<ul style="list-style-type: none"> - Click this report to show events from the local BIS server and all the BIS servers that have been configured to participate in the Distributed Events report. The original server name for each event appears in the first column. The events are fetched and displayed based on the authorization of the operator who clicks to request the report. - The report will query the N most recent events from each of the configured BIS servers, where N is an integer (default 500, max 2000) set by the Distributed reports configuration tool in the Tools menu of the Configuration Browser. - Currently no filtering of event type takes place.
Events for ACE	<p>A tabular report.</p> <ul style="list-style-type: none"> - If Access Engine (ACE) is part of your BIS installation, then click this report to list those events relevant to access control.
Events list	<p>A tabular report.</p> <ul style="list-style-type: none"> - Click this report to show the last 2000 events
Events per device	<p>A graphical report.</p> <ul style="list-style-type: none"> - Click this button to show in a histogram the top 10 event-producing devices - Click one of the bars to show the Events list report for the respective device. - Click the back-arrow button in the toolbar (see Reports toolbar below) to return to the parent report.
Events per state	<p>A graphical report.</p> <ul style="list-style-type: none"> - Click this button to show in a histogram the top 10 most frequent states. - Click one of the bars to show the Events list report for all events which have this state. - Click the back-arrow button in the toolbar (see Reports toolbar below) to return to the parent report.
Events per time	<p>A graphical report.</p> <ul style="list-style-type: none"> - Click this button to show a graph of the number of events per day. The dates are shown along the horizontal axis of the graph. - Click one of the points on the graph, representing the number of events on that day, to zoom in on that day and display the number of events per hour. - Click again to zoom in on an hour and display the number of events per minute. - Click again to zoom in on a minute and display the number of events per second. - Click again to display the Events list report of the actual events listed for that second. - Click the back-arrow button in the toolbar (see Reports toolbar below) to return to the parent report.

Reports toolbar

The tool bar above the main window pane offers a number of ways to customize the display of the report results.

The screenshot shows a software interface for viewing event logs. At the top, there is a navigation bar with a back arrow, a page indicator '1 of 40', a forward arrow, a zoom level '75%', a search box with 'Find | Next', and an 'Export' button. Below this, a summary line reads 'Total number of events: 2000'. The main area is a table with columns: Event time, Address, Detector type, State name, and an empty column. The table contains several rows of event data. A dropdown menu is open over the 'Export' button, showing options: 'Select a format', 'Acrobat (PDF) file', 'Excel', and 'Word'. A sub-menu 'Export Formats' is also visible. Numbered callouts 1-7 point to various UI elements: 1 (back arrow), 2 (back arrow), 3 (75% zoom), 4 (search box), 5 (dropdown menu), 6 (refresh icon), and 7 (print icon).

Event time	Address	Detector type	State name	
08/14/2009 01:53:21 PM 297	virtuell.Server.PERITTAINGH.FPA	OPCServer	Stand-by/Control off	
08/14/2009 01:53:12 PM 767	virtuell.Dongle.Dongle	Dongle	Dongle available	
08/14/2009 01:53:11 PM 343	Operators.BIS.LastAction	Operator	Login	BIS
08/14/2009 01:53:11 PM 343	Operators.BIS.State	OperatorState	Logged on	BIS
08/14/2009 01:53:11 PM 063	virtuell.Event Log	Event log	Stand-by/Control off	
08/14/2009 01:53:11 PM 063	virtuell.Protocolprinting	Protocolprinting	Stand-by/Control off	
08/14/2009 01:53:10 PM 953	Times.Event log back up	Times	Times off	

1. Page forward and backward through the report
2. (Back-arrow) Return to a parent report after zooming in on details
3. Modify the display settings for the report from 10% to 500%, Whole Page or Page Width
4. Enter a search term to seek within the current report
5. Export the report to a different format for post-processing or printing, e.g. PDF, Excel or Word formats.
6. Refresh the report
7. Print the report

15 Event Log Filters

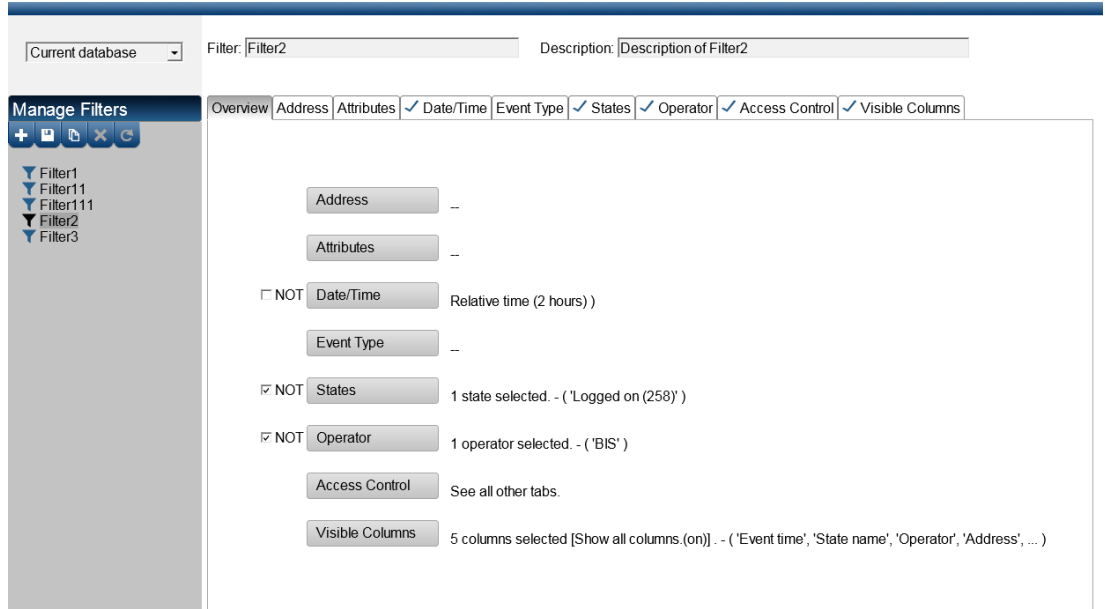
15.1 Filter Overview

Introduction

The **Overview** tab summarizes settings from the other tabs. Its entries are hyperlinks which take you directly to the corresponding tab.

Any tabs where changes have been made are marked with a green tick.

Building Integration System



Logical negation of filters using NOT

Each of the individual filter settings can be logically negated by selecting the **NOT** check box next to the hyperlinks.

A negated filter will allow all records to pass that do not have any of the values contained in that filter.

For example, a filter is defined to catch all records where the Operator is OP1 or OP2.

- Where the **NOT** check box is cleared, only records that contain the Operator name OP1 or OP2 will pass the filter.
- Where the **NOT** check box is selected, only records that do not contain the Operator name OP1 or OP2 will pass the filter.

Note that the **Access Control** filter tab holds a collection of different filters, and therefore cannot be negated with a simple NOT.

Notice!

Possibility of incompatible filters with backup databases

By default only filter criteria relevant to the current database are made available.

These criteria are not changed, however, when changing between a current and a backup database.

It is therefore possible in such cases to apply filters which are irrelevant to the current database, and thus yield "no search results".



15.2 Filter Address

The purpose of this tab is to allow the event log to be searched using device addresses. Because the number of addresses can be very large, this dialog provides its own special filters to narrow the focus to specific groups of addresses.

This dialog is divided into three areas:

- **Available Addresses** - to select special detector types and message types of interest to you. Each column represents a section of a device address which is normally divided by the “.” (period) character, e.g. **AccessEngine.Devices.DMS.State**
- **Free Input** - to enter search terms for other detector types that also should appear in the search results.
- **Selected Addresses** - The resulting list of addresses to be sought in the event log. This list should be regarded as a logical OR, i.e. any messages which contain **any** of the selected addresses in this list will be found when the search is started.

Available Addresses

Detector type: All

Filter:

1	2	3	4
AccessEngine	Devices	BPR HI-2	Event
AccessEngine	Devices	BPR HI-2	AddCheck
AccessEngine	Devices	BPR HI-1	State
AccessEngine	Devices	BPR HI-3	AddCheck
AccessEngine	Devices	BPR HI-2	State
AccessEngine	Devices	BPR HI-2	Sabotage
AccessEngine	Devices	BPR HI	State
AccessEngine	Devices	BPR HI	Sabotage
AccessEngine	Devices	BPR HI	Event

AccessEngine.Areas.Area

Free Input

Selected Addresses

1	2	3
AccessEngine	Areas	Area-7_04

Further filtering to find addresses of interest

1. Select the desired **Detector type** from the list- the default setting is **All**.
The list contains only those detector types which have generated event-log messages. A complete list of all detector types available to the system can be seen in the **Detector types** dialog in the Configuration Browser.
2. The addresses matching the detector type now appear the upper **Addresses** list

3. Use the text box **Filter**, if the list is still very long, to restrict even further the kinds of addresses to be included in the event log. The text entered should match the desired addresses either literally or by use of wildcards. The text itself is not case sensitive.
4. Click the **Apply** button to apply the filter and restrict the list. Overwrite the filter to change it, or click **Delete** to remove the filter and refresh the addresses list without it.

Use of wildcards

The wildcards which can be used are

- “*” (asterisk) for any character(s)
- “?” (question mark) for exactly 1 character
- “.” (period) for an address section boundary.

E.g. the address is matched by the filters
AccessEngine.Devices.DMS.State	AccessEngine.Devices.DMS.State accessengine* *.devices* *dMs* a*.*.state
Event log.Error	*Error event*

If the number of available addresses exceeds 200 then an additional control appears to facilitate scrolling through the list.



1. Select the desired entries in the **Addresses** list (multi-select using Ctrl-Click, Shift-Click etc).
2. Click the button **Add to selection** to add these to the **Selected Addresses** list in the lower part of the dialog window
3. Addresses to be found by using the **Free Input** text box. The wildcard syntax is the same as for the **Filter** box above. E.g. if you are interested in seeing all entries pertaining to operators then enter **operators.*** in the **Free Input** box and click the **Add to selection** button. To add more addresses simply overwrite the **Free Input** text and press **Add to selection** again.

Post hoc modifications

To modify a previously collected set of selected addresses, add new pairs as described above or delete unwanted pairs by selecting them in the **Selected Addresses** list and then clicking the **Delete** button below it.

15.3

Filter Attributes

The upper half of this dialog offers all **Available Attributes** along with their corresponding values in two selection lists.

Overview Address Attributes Date/Time Event Type States Operator Access Control Visible Columns

Available Attributes

Attributes:	Name ▲	Value ▲
	Alarm ID	BIS.Detectors without location
	Authorization	BIS.Operators
	Brief text	Video Systems.Detectors without location
	Command	Video Systems.Operators
	Location	
	Status	
	URL	

Selected Attributes

Attributes:	Name ▲	Value
	Location	Video Systems.Operators
	Location	BIS.Operators

AND
 OR

When an available attribute is selected in the left-hand list (Name) then the right-hand list (Value) becomes populated with its possible values.

To transfer attribute-value pairs from **Available** to **Selected Attributes** select a value in the right-hand list and then click the **Add to selection** button. Repeat the procedure as often as required to complete your set of selected attributes.

Post hoc modifications

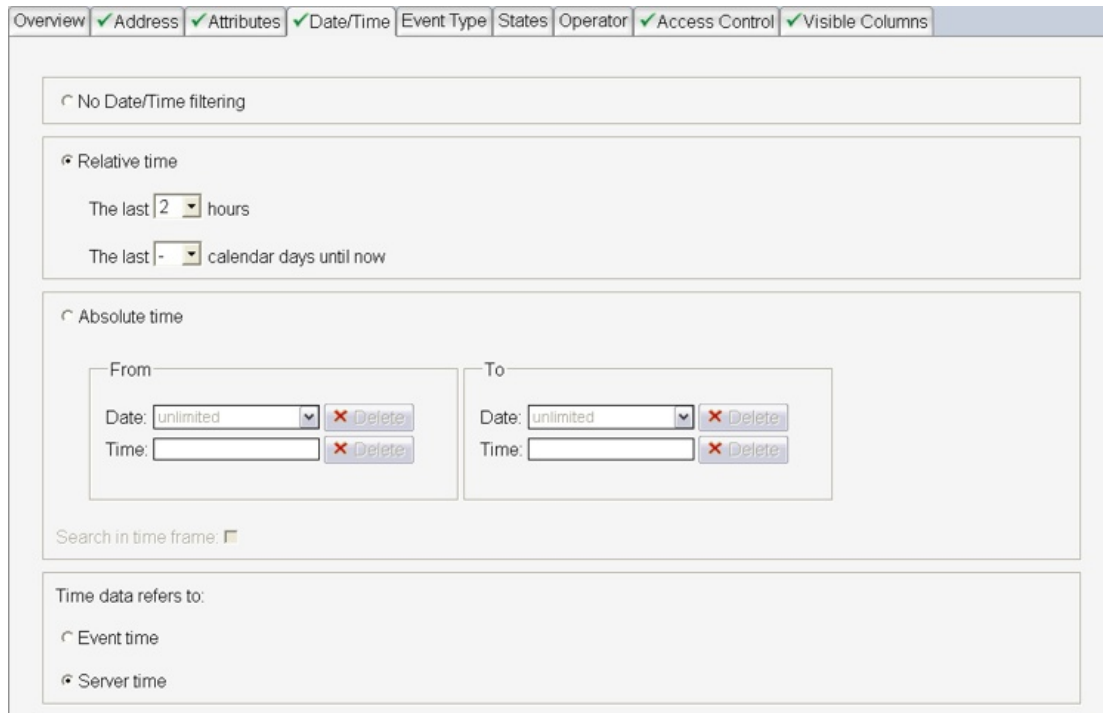
In order to modify the set of selected attributes add new pairs as described above, or delete unwanted pairs by selecting them in the **Selected Attributes** list and then clicking the **Delete** button below it.

Prior to version 2.3 the attributes in a search were combined by a logical **OR**. Since Version 3.0 they are combined by either a logical **AND** or logical **OR**, depending on the **AND/OR** radio button. To prevent self-contradictory filter criteria, the **Add to selection** button will only permit you to add multiple Attributes of the same name if the radio button is set to **OR**.

If a logical combination of attributes is negated on the Event log's main **Overview** tab, then only those records are retrieved from the Event Log that did not pass the original filter.

15.4 Filter Date/Time

Use this dialog tab to create time/date filters. These are especially beneficial in the case of event logs which span long periods of time.



- The following possibilities are available for date/time filtering. Note that the three kinds of time settings (None, Relative and Absolute) are mutually exclusive within any one search.
- **No Date/Time filtering** All events are shown as long as they are not excluded by other filters.
 - **Relative time** By default this option filters the events of the last 2 hours. This may be changed by setting **one** of the following 2 mutually exclusive options.
 - **The last ... hours** The combo-box contains the values 1 - 12 and 24.
 - **The last ... calendar days until now** The combo-box contains the values 1 - 7, 14, 21 and 28.
 - **Absolute time**
 - **From ... To**

The **Date** can be entered manually but it is recommended that to use the date-picker control which is accessible from the combo-box arrow button.

Time is entered manually. Double-digit values for Hour, Minute and Seconds are required.

Entries can be changed by overwriting them, or deleted via the **Delete** button.
 - **Search in time frame**

If this check-box is **not selected**, then the date/times entered are treated as **absolute** start and end times for the search. Example: Setting **From** 01.06.2008 - 08:00:00 **To** 05.06.2008 - 12:00:00 Result: All events between these two points in time will potentially be found by the search.

If this check-box is **selected**, then the two clock times are treated as a **time frame** for each day in the date range.

Example: as above

Result: All events occurring between 08:00:00 - 12:00:00 on each day of the date range 01.06.2008 to 05.06.2008 will potentially be found by the search.
 - **Time data refers to:**
 - **Event time**
 - **Server time**

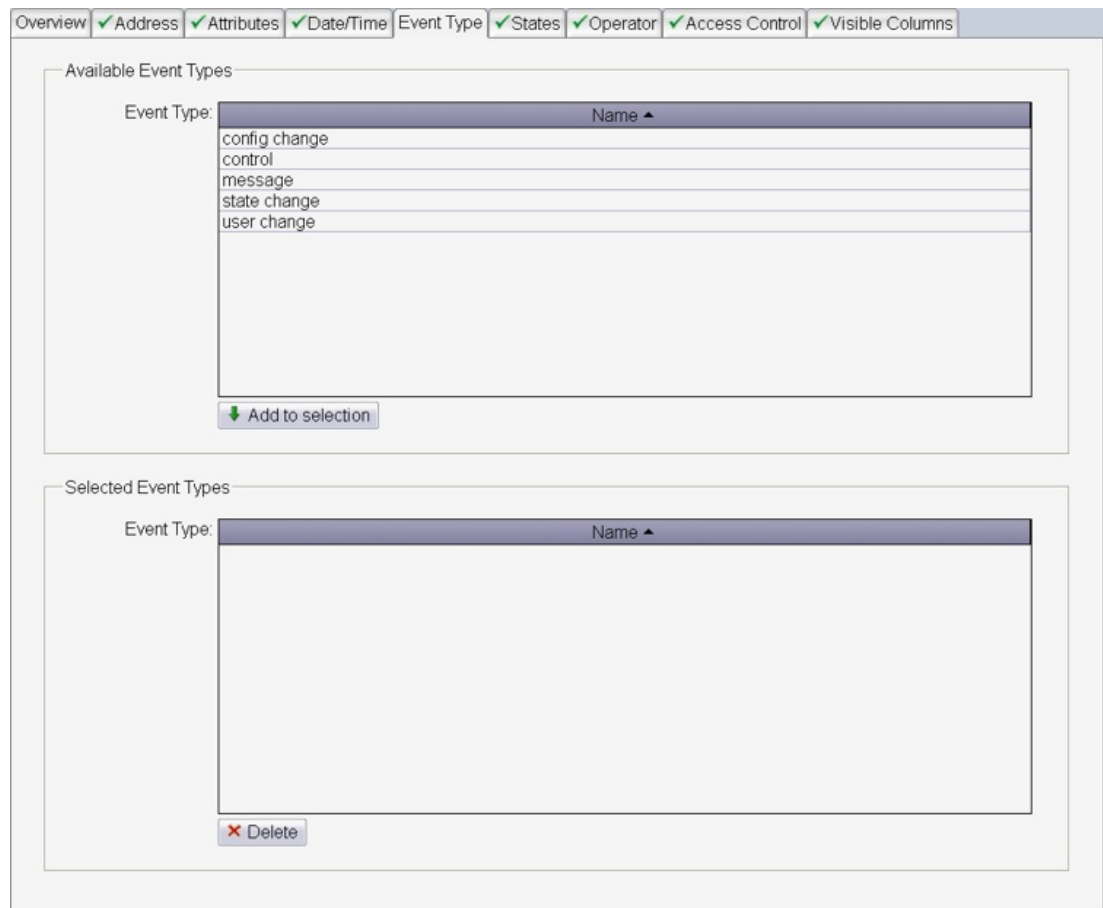
– Server time

Events are logged with two time stamps: one is the time of the occurrence and the other is the logging time on the server (i.e. in the database). These two time stamps may differ considerably, for instance, where devices which have been offline forward their buffered messages when they come back online hours later.

In general the **Event time** will be the more representative for the purposes of filtering, however in order to determine the downtime of particular devices it may be necessary to filter on **Server time**.

15.5 Filter Event Type

This tab lists **Available Event Types** from which those desired can be transferred to the lower **Selected Event Types** list, and thus included in the overall search filter.

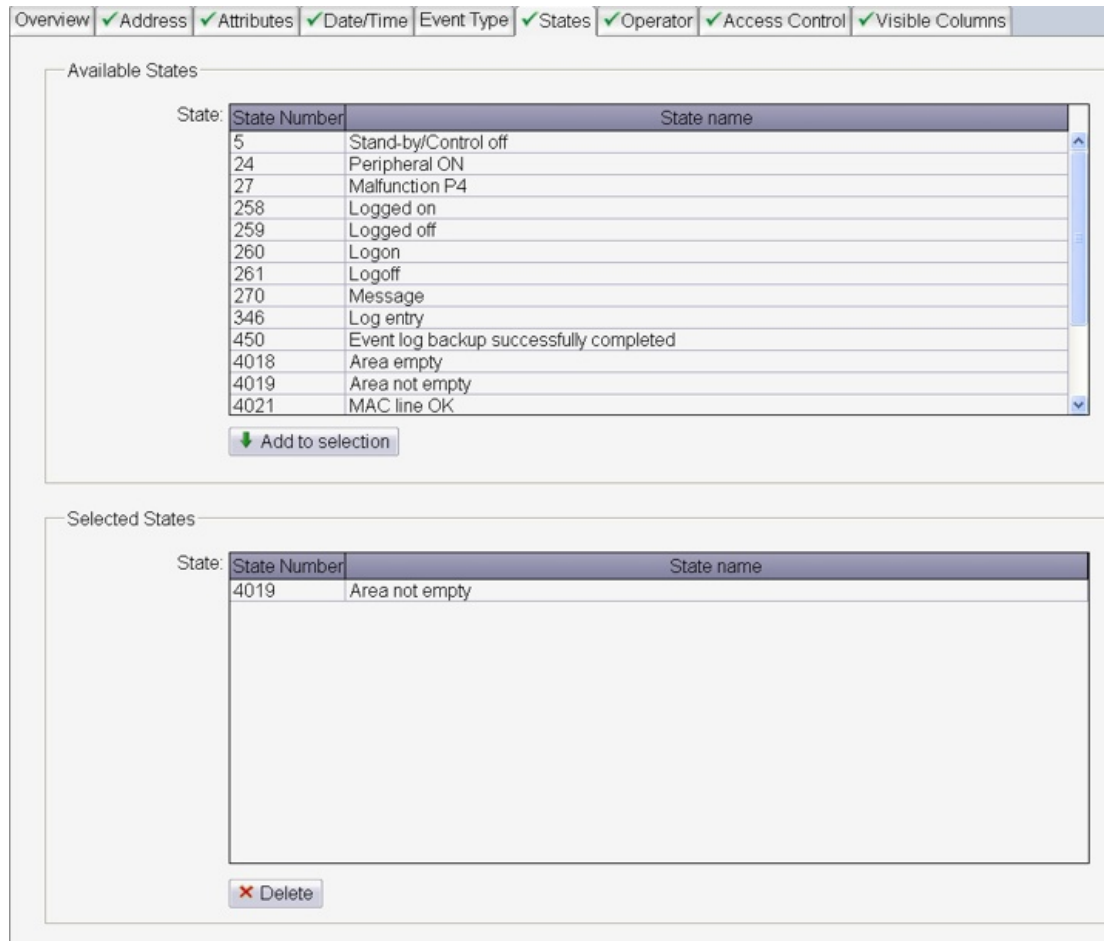


After making your choice of event types (multi-select using Ctrl-Click, Shift-Click etc.) click the **Add to selection** button to add them to the filter.

In order to modify the set of selected types add new ones as described above and delete unwanted types by selecting them in the **Selected Event Types** list and then clicking the **Delete** button below it.

15.6 Filter States

Event messages contain information about the current state of the device generating the message. Use this dialog tab to create filters based on such states.



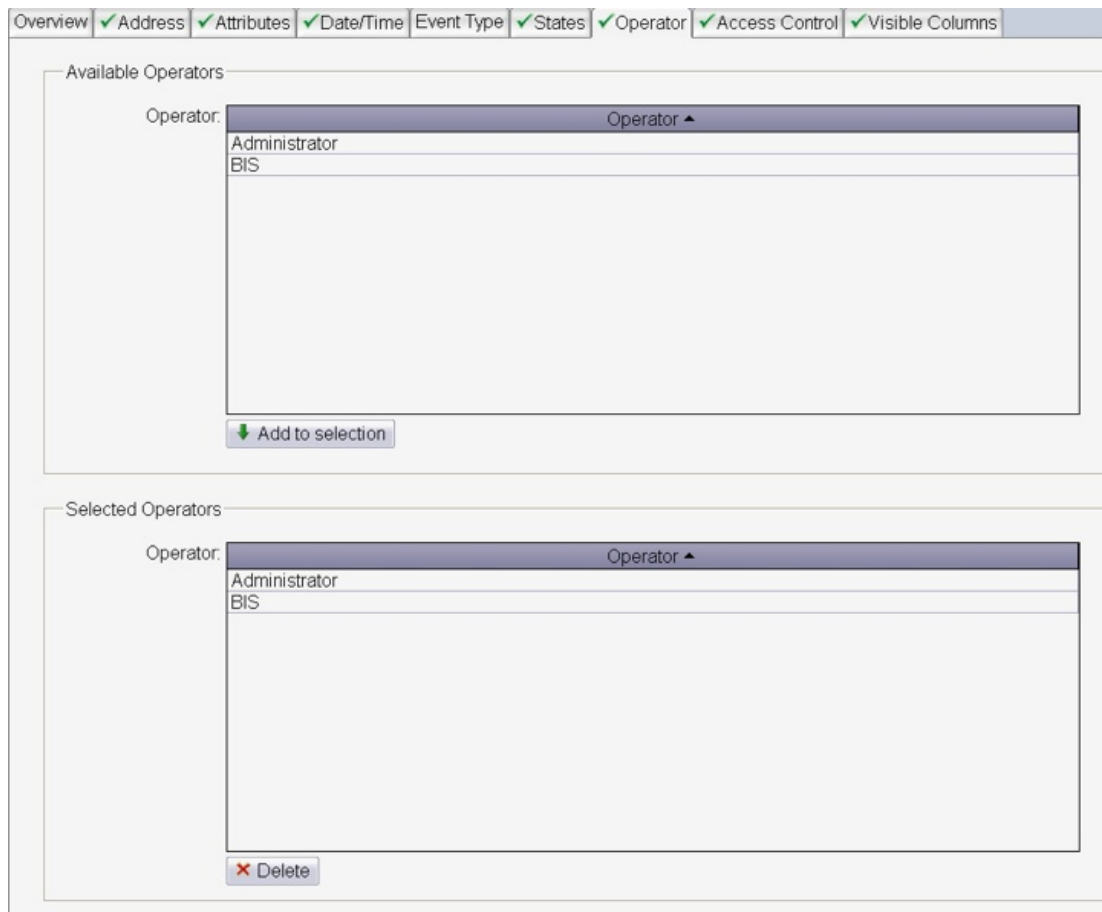
The list contains however only those states which have generated event-log messages. A complete list of all states available to the system can be seen in the **States dialog in the Configuration Browser**.

After making your choice of states (multi-select using Ctrl-Click, Shift-Click etc.) click the **Add to selection** button to add them to the filter.

In order to modify the set of selected states add new ones as described above and delete unwanted states by selecting them in the **Selected States** list and then clicking the **Delete** button below it.

15.7 Filter Operators

Every log-in and log-off plus every modification made to data is logged under the name of the respective operator. Use this dialog tab to create filters based on operator names, and thus discover his/her activities.



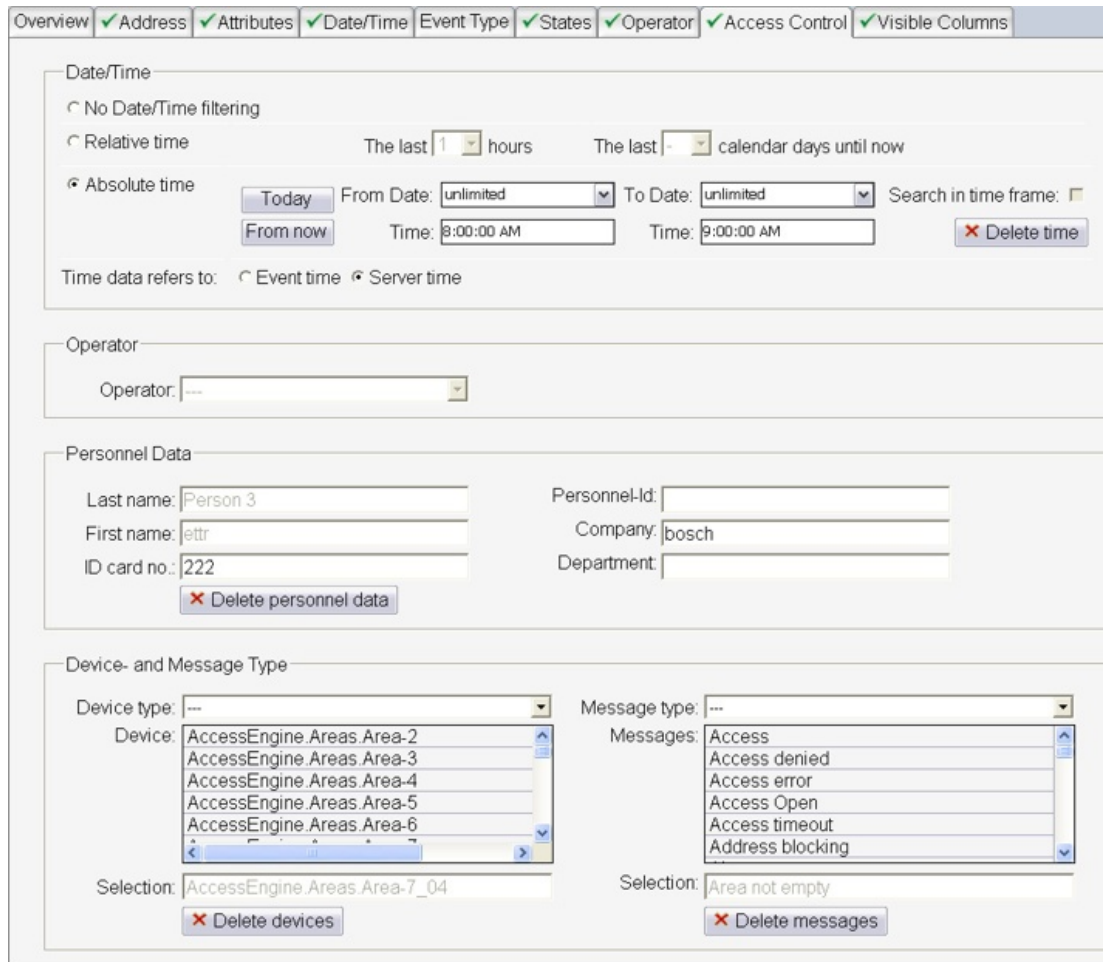
After making your choice of operators (multi-select using Ctrl-Click, Shift-Click etc.) click the **Add to selection** button to add them to the filter.

In order to modify the set of selected operators add new ones as described above and delete unwanted operators by selecting them in the **Selected Operators** list and then clicking the **Delete** button below it.

15.8 Filter Access Control

This dialog tab provides a convenient overview of most of the other filters and their settings (all except **Event Type**) and also allows you to set and/or modify them from a central location.

As soon as settings have been made on one of the other tabs (except **Visible Columns** and **Event Type**) they will also appear on this tab, and their tab headers will be marked with a green tick.



The following filter types are displayed here in separate areas:

- **Date/Time**
Shows the settings made on the **Date/Time** tab. Modifications made here are also reflected on the **Date/Time** tab. All options, input fields and displays of that tab also appear here. **Absolute time** contains two additional buttons for convenience:
 - The **Today** button sets **From Date** and **To Date** to the current date, and the times to midnight and 11:59 PM respectively.
 - The **From now** button sets **From Date** to the current date and the start time to the current time. The other two fields (**To Date** and end time) are cleared of input.
- In contrast to the **Date/Time** dialog tab the single **Delete time** button deletes both clock times.
- **Operator**
Shows the settings made on the **Operator** tab.
As long as only one or zero entries on the **Operator** tab has been selected, then this filter can also be modified from the **Access Control** tab. Otherwise this control is disabled and the following warning is displayed. More than one operator selected on Operator page
- **Personnel Data**
Shows the settings made on the **Attributes** tab, as long as only one entry was selected there, and as long as only the attributes NAME and FIRSTNAME are affected. Otherwise these fields are disabled.

In addition, and only here, further personnel data filters can be set: **ID card no., Personnel-ID, Company and Department.**

Note that using the **xDelete Personnel Data** button here will also delete attribute settings on the **Attributes** tab.

– **Device- and Message Type**

Shows the filter settings from the dialog tabs **Address** and **States** in the fields labeled **Selection** under the list boxes **Device** and **Messages**.

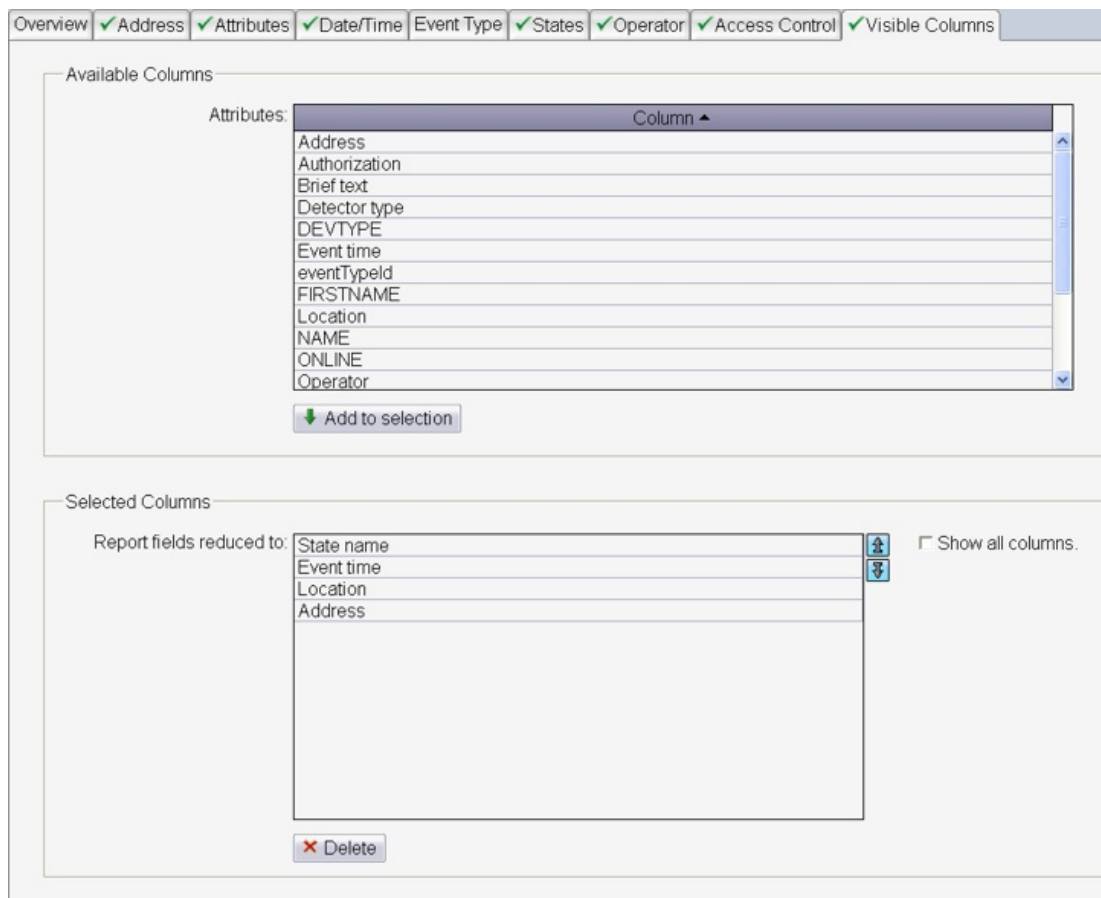
Use the combo-boxes **Device type** and **Message type** to reduce the list entries to a manageable number. Simply clicking on an entry in the list boxes will transfer it to the **Selection** text field.

Note that the **xDelete Devices** and the **xDelete Messages** buttons will remove the entire selection from the tabs **Address** and **States** respectively.



15.9 Filter Visible Columns

This dialog tab is not for creating filters but for configuring the display of the search results which were produced by applying those filters.

An event log message consists of a set of data divided into columns. Use this dialog to determine which columns (i.e. which data) you wish to view in the final search results.



The default visible columns are **Event time, State name, Address** and **Location**.

After making your choice of columns (multi-select using Ctrl-Click, Shift-Click etc.) click the **Add to selection** button to add them to the lower list **Report fields reduced to**. New entries are added at the end of the list. Change the order of the columns by selecting one or more column names and then moving them up or down using the  and  buttons.

Selecting the check box **Show all columns** does not alter the contents of the **Report fields reduced to** list, but does ensure that all remaining available columns appear in alphabetical order to the right of them in the search results.

After making your choice of columns (multi-select using Ctrl-Click, Shift-Click etc.) click the **Add to selection** button to add them to the filter.



Notice!

Report and print format

The maximum number of columns which can be viewed easily on most screens is five.

Move those columns which interest you most therefore to the top of the **Report fields reduced to** list (and hence to the leftmost columns in the search results).

Note that too many columns in a printout may lead to unexpected page-breaks.

In order to modify the set of selected columns that was already defined, add new ones as described above, and delete unwanted columns by selecting them in the **Selected Columns** list and then clicking the **Delete** button below it.

Note however that the column **Event time** is required and can not be deleted.

Glossary

BIS server

(Hardware) A computer where the BIS application is installed. Also known as a Login server.

Connection server

(Hardware) A computer that runs OPC server software with which external devices communicate by OPC protocol. The BIS setup program can be used to turn a Windows system into a potential Connection server.

Consumer server

(Hardware) The Consumer server is a BIS single server system that reads information from one or more other BIS single server systems by configuring them as OPC servers.

Database server

(Hardware) A computer that hosts BIS databases for the event log and (optional) engines.

Multi-server BIS system

A multi-server BIS system is one in which two or more BIS single server systems share information. BIS multi-server systems can be organized as hierarchical or peer-to-peer networks.

OPC client

A software program that reads data communications in OPC protocol written by OPC servers.

OPC server

A software program that converts the hardware communication protocol used by a device into the OPC protocol.

Provider server

(Computer) The Provider server is a BIS single server system that provides information to other BIS single server systems via OPC.

Single server BIS system

A single server BIS system contains only one BIS Login server (also known as the BIS server). It may run OPC server software itself, and may contain zero or more Connection server and Database server computers.

Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2023

Building solutions for a better life.

202304171641