



Select by location		Select by alarm		Select by stream info		Select by time	
Site	AL	Stream name		Stream name		From	To
Status	AL	Stream name		Stream name		13/03/2026	11:42:00
Status	Active	Clear	Location	File	Stream	Description	
☒	Clear	Mar 12 20:01:44	Mar 12 20:01:48	LiveSite129probe	IP TV	NC-239.255.1.66	No signal
☒	Clear	Mar 08 07:11:20	Mar 08 07:11:24	LiveSite129probe	IP TV	NC-239.255.1.66	No signal
☒	Active	Mar 05 09:33:42		LiveSite129probe	IP TV	SVT8_SVT24 HD	No signal
☒	Active	Mar 05 09:33:42		LiveSite129probe	IP TV	SVT1 HD	No signal
☒	Active	Mar 05 09:33:42		LiveSite129probe	IP TV	ZDF HD	No signal
☒	Active	Mar 05 09:33:42		LiveSite129probe	IP TV	NRK3_Super HD	No signal
☒	Active	Mar 05 09:33:42		LiveSite129probe	IP TV	NRK2 HD	No signal
☒	Active	Mar 05 09:33:42		LiveSite129probe	IP TV	NRK1 HD	No signal
☒	Active	Mar 05 09:33:42		LiveSite129probe	IP TV	TLC Sverige HD	No signal
☒	Active	Mar 05 09:33:42		LiveSite129probe	IP TV	TLC Norge HD	No signal
☒	Active	Mar 05 09:33:42		LiveSite129probe	IP TV	TLC Danmark	No signal
☒	Active	Mar 05 09:33:41		LiveSite129probe	IP TV	TLC Austria	No signal



VBC Controller User's Manual

Applies to software release v7.0.0

April 2026

Current documents are always found in the log-in area of the **www.bridgetech.tv** site. Refer to section 1.3 of this document for more information.

VBC Controller User's Manual
Revision f0b6d2f2 (2026-04-16)

Copyright © Bridge Technologies Co AS. Bentsebrugata 20, NO-0476, Oslo, Norway.
All rights reserved.

This publication can contain confidential, proprietary, and confidential trade secret information. No part of this document may be copied, photocopied, reproduced, translated, or reduced to any machine-readable or electronic format without prior written permission from Bridge Technologies Co AS. CE-marked in accordance to low voltage directive (LVC) 73/23/EEC and EMC directive 89/336/EEC. Compliant to requirements for US and Canada. Designed for CSA approval. Bridge Technologies Co AS continuously improves on products and reserves the right to modify the specifications without prior notice. Information in this document is subject to change without notice and Bridge Technologies assumes no responsibility or liability for any errors or inaccuracies.

The BRIDGE, BRIDGE TECHNOLOGIES and BRIDGETECH name, logo and all other related logos are registered trademarks of BRIDGE TECHNOLOGIES Co AS.

All other products or services mentioned in this document are identified by the trademarks, service marks, or product names as designated by the companies who market those products. Inquiries should be made directly to those companies. This document may also have links to third-party web pages that are beyond the control of Bridge Technologies. The presence of such links does not imply that Bridge Technologies Co AS endorses or recommends the content on those pages. Bridge Technologies acknowledges the use of third-party open source software and licenses in some products.

This product can include software developed by the following people and organizations with the following copyright notices:

- Curl. Copyright © Daniel Stenberg and many contributors. All rights reserved.
 - Dropbear. Contains software copyright © 2008 Google Inc. All rights reserved.
 - OpenSSL Project for use in the OpenSSL Toolkit. (<https://www.openssl.org/>).
- Copyright © The OpenSSL Project. Copyright © Eric A. Young, Tim J. Hudson All rights reserved.

All trademarks and registered trademarks mentioned herein are the property of their respective owners.



Contents

Contents	3
1 INTRODUCTION	8
1.1 Sites and Blades	8
1.2 Users and Access	8
1.3 How to Use This Manual	9
2 INSTALLATION AND INITIAL SETUP	11
2.1 System Requirements	11
2.2 First-time Installation	11
2.2.1 Obtaining and preparing the installation media	11
2.2.2 Deploying in a virtualized environment	12
2.2.3 Obtaining and installing pre-built virtual images	12
2.2.4 Installing from provided installation media	12
2.3 Maintaining the underlying Operating System	18
2.4 Verifying Correct Initial Setup and Software Activation	19
2.5 Initial Setup Troubleshooting	20
2.6 Upgrading From a Previous Version	20
2.6.1 Using the User Interface	21
2.6.2 Using a full reinstall	21
2.7 Accessing the User Interface	21
2.8 Firewall Configuration	22
2.9 Network configuraiton	23
2.10 License Details	23
2.11 Accessing the administrative interface	23
2.12 Deactivating	23
3 REMOTE DATA WALL	24
3.1 Introduction to the Remote Data Wall	24
3.2 Accessing the Remote Data Wall	24
4 MASTER VBC	26
4.1 Introduction to the Master VBC	26
4.2 Configuring access rights	26
5 THE VBC GRAPHICAL USER INTERFACE	28
5.1 Login	29
5.2 Alarms	29
5.3 Blade alarms	30



5.4	Streams	31
5.4.1	Streams Performance Indicator	33
5.4.2	Streams Configuration	34
5.4.3	Streams Status	36
5.4.4	VBC Live Mosaic requirements	36
5.5	Expert	36
6	EXPERT VBC GRAPHICAL USER INTERFACE	38
6.1	Login	39
6.2	Live	40
6.3	Monitoring	41
6.3.1	Monitoring — Top Level	41
6.3.2	XML Alarms	46
6.3.3	Monitoring — Site	46
6.3.4	Monitoring — Blade	48
6.3.5	Monitoring — All sites	48
6.4	Blade alarms	51
6.5	Graphics view (Graphics option)	55
6.6	Stream view	57
6.6.1	Stream names, class and interface	58
6.6.2	Stream view — Selected	59
6.6.3	Selected Stream Compare MediaWindow	63
6.6.4	Selected Stream Compare ETR	65
6.6.5	Selected Stream Compare Streamdata	66
6.7	Thumbs view	68
6.8	Service view (Transport Stream Service View option)	70
6.8.1	Service view — Thumbs	71
6.8.2	Service view — Selected	72
6.8.3	Selected TS Service Compare ETR	74
6.9	Map	76
6.10	RDP	77
6.11	RDW	79
6.11.1	RDW — Canvases	79
6.11.2	RDW — Devices	80
6.11.3	RDW — Tags	81
6.11.4	Canvas Configurator	82
6.11.5	Remote Data Wall Widgets	84
6.11.5.1	Web Widget	84
6.11.5.2	Textbox Widget	84
6.11.5.3	Thumbnail Widget	84
6.11.5.4	Loudness Widget	85
6.11.5.5	Media Window Widget	85
6.11.5.6	Alarms Widget	85
6.11.5.7	RF Graph Widget	85
6.11.5.8	Clock Widget	86
6.11.5.9	Slide Widget	86
6.11.5.10	Countdown Widget	86
6.11.5.11	Graphics Widget	86
6.11.5.12	Stream View Widget	86



6.11.5.13 Redundancy Widget	87
6.11.5.14 MicroTimeline Widget	87
6.11.5.15 OTT Graph Widget	87
6.11.5.16 OTT Status Widget	87
6.11.5.17 Constellation Widget	87
6.11.5.18 RF Data Widget	87
6.11.5.19 Map Widget	88
6.11.5.20 Canvas Control Widget	88
6.11.5.21 Tag Control Widget	88
6.12 Equipment	89
6.12.1 Equipment — Edit device	91
6.12.2 Equipment — Management	93
6.13 Alarm setup	100
6.13.1 Alarm setup — Message Fwd	102
6.13.2 Alarm setup — Scheduling	107
6.14 Timeline (requires Archive Server)	111
6.14.1 Choosing what to inspect	111
6.14.2 Navigating in time	111
6.14.3 Persistent layout	112
6.14.4 Audio silence in the timeline	112
6.15 Reports	114
6.15.1 Reports — Manual Report	115
6.15.2 Reports — Report list	116
6.15.3 Reports — Auto reports	117
6.15.4 Reports — Import logo	118
6.15.5 Reports — The PDF Report	118
6.15.6 Reports — The HTML Report	122
6.16 Ext. Reports	124
6.16.1 Ext. Reports — Manual extended report	125
6.16.2 Ext. Reports — Extended report list	127
6.16.3 Ext. Reports — Auto extended reports	128
6.16.4 Ext. Reports — PDF Report	130
6.16.5 Ext. Reports — Alarm poll and report status	133
6.16.6 Ext. Reports — Setup storage	135
6.17 Main — Sites and Users	136
6.17.1 Sites and Users — Sites	136
6.17.2 Sites and Users — Users	137
6.17.3 Sites and Users — User groups	138
6.18 Main — Logs	140
6.18.1 Logs — Logs	140
6.18.2 Logs — Settings	141
6.19 Main — Snapshots	142
6.20 Main — Alarm statistics	144
6.21 Main — Stream groups	145
6.22 Main — Service groups	146
6.23 Main — Archive Setup	147
6.23.1 Archive server	147
6.23.2 Connecting the Archive server	147
6.23.3 Configuration	148



6.23.4 Alarms	148
6.24 Main — Gfx. View Setup (Graphics option)	149
6.24.1 Configure diagrams	149
6.24.2 Setup and data mapping	150
6.25 Main — General	153
6.25.1 General — Clear	153
6.25.2 General — Connections	154
6.25.3 General — Preferences	155
6.25.4 General — Authentication	156
6.25.5 General — Sync	157
6.26 Main — About	158
6.26.1 About — Release info	158
6.26.2 About — License	159
6.26.3 About — Technologies	161
6.26.4 About — Credits	162
6.26.5 About — System	163
6.26.6 About — Data	165
6.26.7 About — Software	165
A Appendix: Separate Probe and Network Interfaces	167
B Appendix: The VBC Files	168
C Appendix: The VBC System Services	170
D Appendix: Example Site Configuration	172
E Appendix: Getting the Thresholds Right	174
F Appendix: Probe Versus VBC Alarms	176
G Appendix: Syslog forwarding	178
H Appendix: Troubleshooting	179
I Appendix: Backing up the VBC	180
I.1 Backing up the VBC	180
I.2 Restoring the VBC from backup	180
I.3 Restoring the nightly backup	180
I.4 Obtaining the backup script from a newer version	181
J Appendix: On-line License Activation	182
J.1 Introduction	182
J.2 Requirements	182
K Appendix: Software Maintenance	184
L Appendix: Software Upload	185
L.1 Obtain the software image	185
L.2 Backup the VBC configuration and data	185
L.3 Transfer the image to the VBC and save	186



L.4	Wait while the software is being saved	187
L.5	Verify the new image	187
L.6	Software upload troubleshooting	187
M	Appendix: Network configuration	188
M.1	Web-based configuration	188
M.2	Command-line based configuration	189
M.3	Further reading	192
N	Appendix: Enabling NTP time synchronization	193



1 INTRODUCTION

The VBC Controller is a server-side software application that offers central management of Bridge Technologies devices. Operating devices through the VBC is considerably more convenient and powerful than operating each device independently.

When managing a large digital television system there is a need to easily monitor the overall system status. Deploying the VBC Controller as part of the system enables the user to view the system status at-a-glance and the VBC's drill-down functionality makes it easy to locate the problem source and examine details on the devices themselves.

Through the VBC the user can perform tasks such as building a hierarchical equipment view, view aggregate alarm and status messages, get aggregate status per TV stream and compare measurements across devices.

The VBC supports alarm export for integration into an NMS system.

The VBC server runs in a Linux environment. The VBC client is simply a web browser pointed towards the VBC server.

1.1 Sites and Blades

The VBC Controller supports a hierarchical equipment view. At the top of the chain are sites. A site is a number of devices that logically or physically belong together. These devices are also called blades. Each device has an IP address and its own web interface that can be reached directly or via the VBC.

For systems deploying microVB units a Micro Device Controller (MDC) can be added to the VBC as a device. MDC will then report monitoring statistics to the VBC on behalf of all the microVBs.

1.2 Users and Access

The VBC Controller supports a role based user interface where a user is given full or limited access to a selection of the devices. Setup of system wide configurations, such as user setup, is performed by the pre-configured user admin.

The *admin* user is hard-coded inside the VBC and is the only user-defined when the VBC is installed. The *admin* user is the only user that has access to the system-wide setup views. Put another way, the *admin* can do everything a regular user can do and more.

Beware! You can easily do a lot of damage by accident as the *admin* user, so logging in as *admin* is not recommended for performing regular tasks.

When logging in, the user name for the *admin* user is always **admin** and the default password is **elvis**. **Please change the password for this user after installing the system.**

There is no limit to the number of active users or to the number of active users of the same account. Each client will work independently of the others, only affected by changes to global settings usually done by the *admin* user.

The VBC uses a standard web mechanism called cookies to identify users. A cookie is a piece of data that the VBC returns to the browser when the user logs in. The browser will automatically provide this cookie



in all subsequent requests towards VBC. The cookie allows the VBC to remember the state for all users who are logged in – so that it knows which sites the user has access to etc. Generally all windows or tabs from the same browser application will appear to the VBC as the same user – since they will all forward the same cookie.

The *admin* grants each user access to one or more sites. When logging in, the client's access will be limited to the sites associated with the login name. The client will only have access to devices belonging to these sites.

Each user belongs to one user group. The access rights for the users is controlled in the user groups. Here the user can be limited to read only access, allowed the TS service view, doing RDP etc.

The user interface provided by the VBC is dynamic in the sense that almost all pages are generated differently for each user. The **Stream view** will, for instance, only list streams that are monitored by probes that are included at the sites that the user has access to.

1.3 How to Use This Manual

This User's Manual is valid for software version 7.0.0 of the VBC Controller.

Throughout this manual the term stream is often used rather than unicast or multicast. One stream may consist of one or more services, and refers to one IP stream received as a uni- or multicast or over an SRT connection (for Ethernet input) or one transport stream (ITU.T J.83 Annex A/B/C QAM, DVB-T/T2 COFDM, 8VSB, DVB-S/S2, ASI). When the term multicast is used in this manual, it explicitly refers to a stream arriving over the network as a multicast or unicast, including unicasts that use the SRT protocol.

Chapter 2 **INSTALLATION AND INITIAL SETUP** explains how to install the software on a server.

Chapter 3 **REMOTE DATA WALL** introduces the Remote Data Wall.

Chapter 4 **MASTER VBC** provides an overview of the Master VBC feature.

Chapter 5 **THE VBC GRAPHICAL USER INTERFACE** describes the graphical user interface (GUI) as seen when pointing a web browser to the VBC Controller's IP address.

Chapter 6 **EXPERT VBC GRAPHICAL USER INTERFACE** describes the expert view, which is used to configure and dive deeper into the features of the VBC.

A **Appendix: Separate Probe and Network Interfaces** describes how to set up the VBC as a bridge between the probe and management networks.

B **Appendix: The VBC Files** summarizes the files that are installed and created by the VBC.

C **Appendix: The VBC System Services** lists the Linux processes used by the VBC.

D **Appendix: Example Site Configuration** contains an example on how to configure VBC sites.

E **Appendix: Getting the Thresholds Right** explains how to set up VBC thresholds.

F **Appendix: Probe Versus VBC Alarms** describes the alarm handling in the probes versus the VBC Controller.

G **Appendix: Syslog forwarding** gives an example on how to use the Syslog forward feature with an external syslog service.

H **Appendix: Troubleshooting** lists some hints troubleshooting VBC Controller issues.

I **Appendix: Backing up the VBC** describes how to create a backup of the VBC and how to restore it later.



J Appendix: On-line License Activation outlines the on-line license activation procedure.

K Appendix: Software Maintenance briefly describes software maintenance licenses and how they are used.

L Appendix: Software Upload explains how to upgrade the VBC software.

M Appendix: Network configuration gives a brief introduction to the server OS network configuration.

N Appendix: Enabling NTP time synchronization provides some basic information about setting up time synchronization.

Note that current version of the User's Manual can be found on the <https://www.bridgetech.tv/> website. Log in as end user: **customer** with password: **xmas4u**. Additional technical documentation is also found at the same location.



2 INSTALLATION AND INITIAL SETUP

2.1 System Requirements

Please refer to the web site at <https://support.bridgetech.tv/> for the currently recommended hardware. The load on the VBC server will increase for increasing number of concurrent users and with more sites and blades, and the VBC's responsiveness is dependent on server specifications.

The VBC Live Mosaic feature requires requires additional CPU and networking resources on the VBC server and a client PC with sufficient resources to decode multiple video services at once. The amount of resources required on the VBC is highly dependent on the number of streams and their compression characteristics. Please read the documentation at <https://support.bridgetech.tv/> for the currently recommended hardware.

It may be a good investment to use high performance server hardware in order to handle future system extensions.

Supported platforms:

- Ubuntu 24.04 LTS for x86_64

2.2 First-time Installation

Make sure that the server hardware or virtual environment matches the requirements. Download the appropriate installation image from the end-user area on <https://www.bridgetech.tv/> and then follow the procedure outlined below.

This manual details installation on Ubuntu Server 24.04 LTS. For more details, please refer to the Ubuntu Server installation guide¹.

2.2.1 Obtaining and preparing the installation media

Obtain the latest installation ISO image. The same installation media is used for Ubuntu Server and Ubuntu Server Pro installations. If you have an Ubuntu Pro subscription, you can enter the subscription details during the installation procedure.

To install from a USB mass storage device, transfer the downloaded image to the device using a tool such as **dd** (macOS, Unix, Linux), **Rufus**² (Windows) or **Etcher**³ (macOS, Windows, Linux). The Ubuntu documentation⁴ has a step-by-step guide on how to create a bootable USB stick, just remember to use the ISO file you just downloaded and not the one linked from the guide.

Once the USB device is prepared, please continue to chapter 2.2.4. For installation in a virtualized environment, please continue to chapter 2.2.2.

¹<https://ubuntu.com/server/docs/how-to>

²<https://rufus.ie/>

³<https://etcher.io/>

⁴<https://ubuntu.com/tutorials/create-a-usb-stick-on-ubuntu>



2.2.2 Deploying in a virtualized environment

It is also possible to deploy the software in a virtualized environment. For optimal performance, check the processor configuration of **cores per socket** on your host server and use the same configuration setting of cores per virtual sockets on the virtual machine.

To install the software in the virtualized environment, please attach the downloaded ISO image to a virtual DVD-ROM unit and follow the steps in chapter 2.2.4. We recommended **disabling** any 'Easy install', 'Unattended install' or similarly worded option, and *not* selecting the operating system type when initially creating the new virtual machine instance in your virtualization environment. These options may override the installation instructions included in the provided installation image, causing an incomplete installation.

2.2.3 Obtaining and installing pre-built virtual images

Pre-built images for VMware (vSphere/Workstation/Player) are provided in OVA (Open Virtualization Format Archive) format. These images contains a system already installed according to the steps below, with VMware Tools already installed and activated.

To deploy the image, you need to import it to the virtualization host, please refer to the documentation of your virtualization environment for more details on how to do this.

If installed in a VMware vSphere environment, the machine should report back its network configuration to the host environment. Please allow some time for it to do so, and then continue to chapter 2.3.

2.2.4 Installing from provided installation media

The installation media will install Ubuntu Linux Server 24.04 LTS on the server. The disks will be formatted and all contents lost. Make sure that any important data on the server has been backed up before beginning the procedure.

1. Boot the server and make sure that the primary boot device is set appropriately.

The installer will run, showing a screen similar to the one depicted in figure 2.1. Some of the steps described in the Ubuntu Server installation guide will be skipped over, with the appropriate settings applied. Please follow the on-screen prompts to install the system:

2. First select the language in which to run the installer, and then which keyboard layout to use to navigate the installer, selecting 'Done' to continue.

Please note that all screenshots and descriptions in this installation manual describe the English user interface, but all settings should be available independent of the language selected.

3. Configure your network devices as needed to reach the internet, see figure 2.2.

If a proxy is required on your network to reach the internet, provide the address in the next step. The connection will be tested and once ready, select 'Done' to continue.

The installer will be able to run without an internet connection, in this case select 'Continue without network'.

Post-installation network configuration can be performed using the **nmtui** utility, please refer to M Appendix: Network configuration for details.

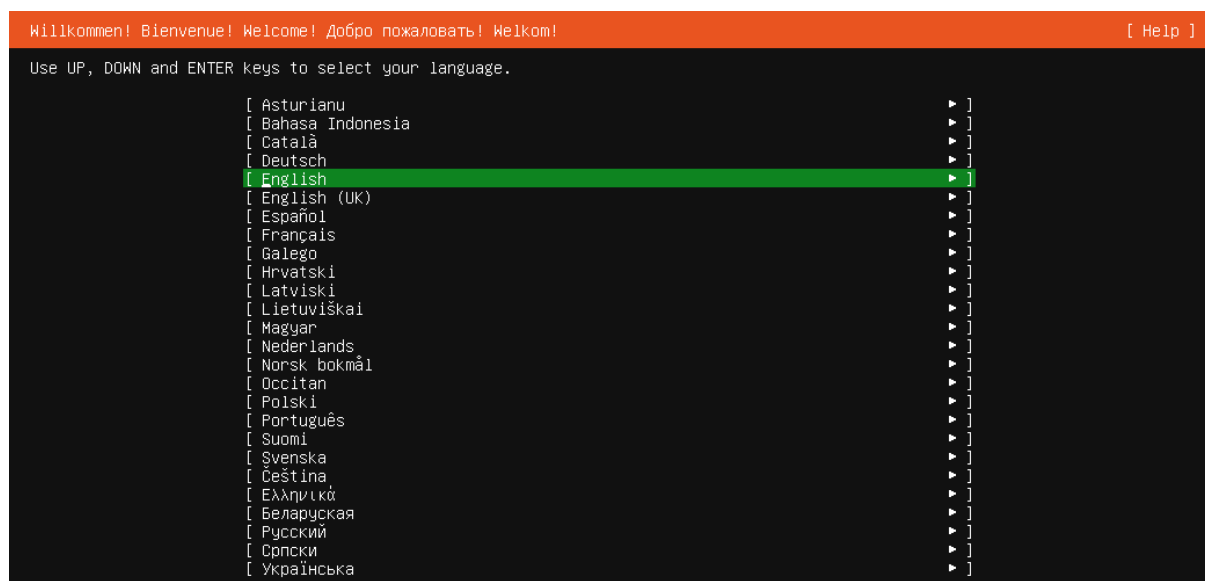


Figure 2.1: Welcoming screen

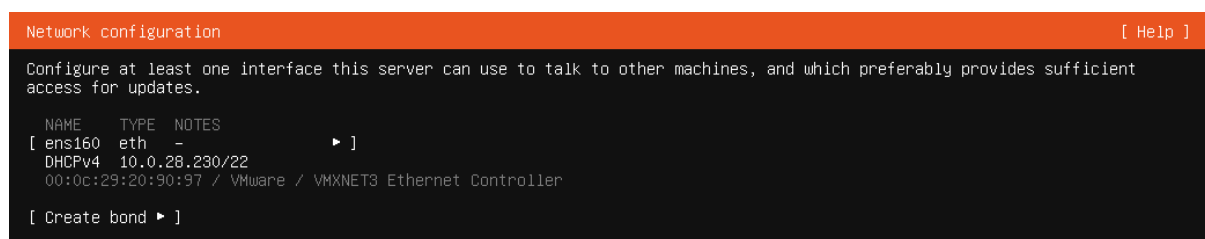


Figure 2.2: Network configuration

4. Next, configure the partitioning. We recommend selecting 'Custom storage layout' (figure 2.3) and configuring the partitioning manually, as the automatic partitioning often leaves parts of the hard disk unused.

We recommend not using a swap partition when using the Software Probe, as this can interfere with the real-time operation of the software.

If you are installing on a system with pre-existing partitions, volumes and/or RAID devices, you will need to select 'Delete' on each of these in turn to remove them before continuing. If you are unable to remove specific partitions, highlight the disk itself and select 'Reformat' to clear all partitions on the disk. When installing from USB, the USB device will be displayed in this list. It will be marked as 'in use' and cannot be deleted.

- For the drive intended for the OS, select 'Use As Boot Device'. Compare figure 2.4.
- Select 'free space' on the same device. In the pop-up menu, select 'Add GPT Partition' and create a partition of 1G, formatted as xfs at mount point /boot. Select 'Create' to create the partition, see figure 2.5.
- Again, select 'free space', open the pop-up menu and select 'Add GPT partition'. Leave the Size field blank (to assign the maximum available), set format to 'Leave unformatted' and select 'Create' to create the partition, see figure 2.6.
- Select 'Create volume group (LVM)', selecting the partition created in the previous step. Select 'Create' to create the LVM volume group, see figure 2.7.

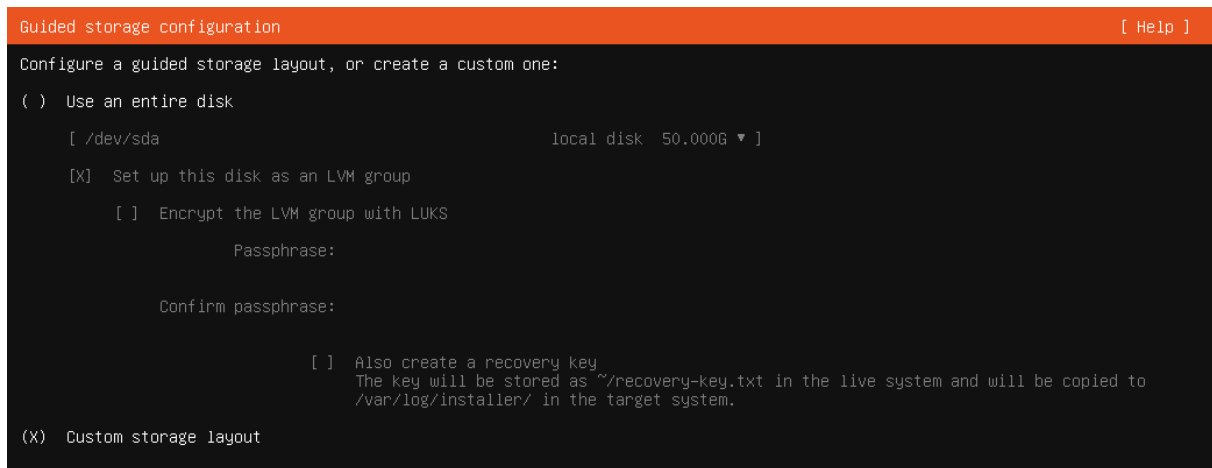


Figure 2.3: Select 'Custom storage layout'

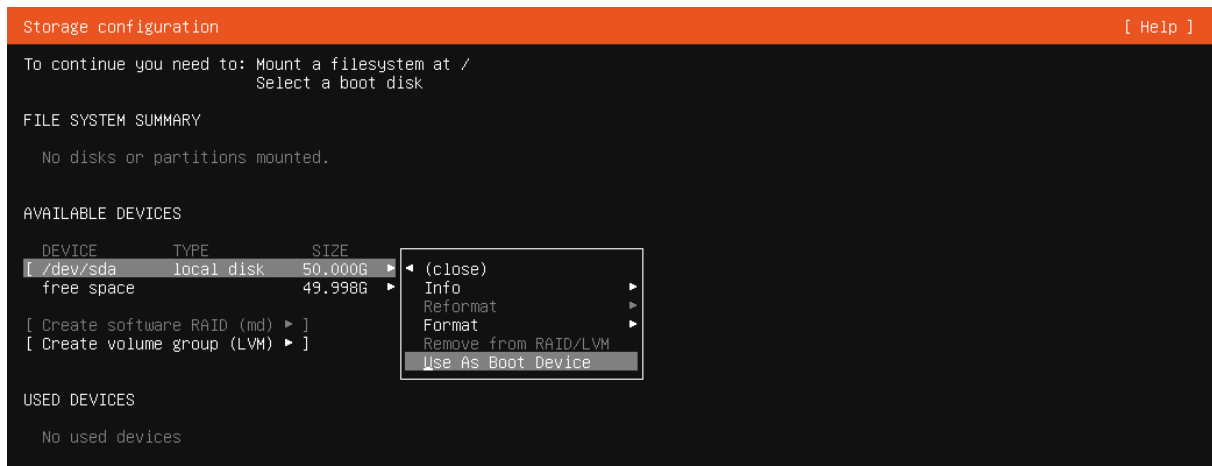


Figure 2.4: Select boot device



Figure 2.5: Create boot partition



Adding GPT partition to /dev/sda

Size (max 48.997G):

Format:

Mount:

Figure 2.6: Create space for volume group

Create LVM volume group

Name:

Devices:

/dev/sda	50.000G
local disk	
[X] partition 3	48.997G
unused partition of local disk	

Size: 48.996G

☐ Create encrypted volume

Passphrase:

Confirm passphrase:

☐ Also create a recovery key:
The key will be stored as
~/recovery-key-{name}.txt in the live system
and will be copied to /var/log/installer/ in
the target system.

Figure 2.7: Create volume group



Figure 2.8: Create root volume

- Select 'free space' under the 'NN (new)' device (where *NN* is the name you gave it in the previous step). Select 'Create Logical Volume'. Name it 'root', leaving the size field blank (to assign the maximum available), and setting format to 'xfs'.
The configuration should look similar to figure 2.8. Select 'Create' to create the logical volume.
 - The storage configuration should look similar to figure 2.9. Accept it by selecting 'Done'.
Confirm that you want to apply the changes by selecting 'Continue'.
5. Next, create the administrative user and password, see figure 2.10. This is used later to log in to the administrative interface.
 6. If you have an Ubuntu Pro subscription, enter it here, as seen in figure 2.11. Otherwise, select 'Skip for now'.
To attach an Ubuntu Pro subscription later, enter `pro attach` at the command line and follow the on-screen prompts.
 7. To be able to log in remotely to the system, select 'Install OpenSSH server' in the SSH configuration screen depicted in figure 2.12.
You can import SSH keys to enable password-less installation using the 'Import SSH key' feature if the system has internet connectivity and you have an account with any of the supported services. Please note that you will still need to have set a password to use the Cockpit administrative interface.
 8. The installation will now start. Once finished, there will be a button at the bottom of the screen saying 'Reboot Now'. Remove the installation media and ensure that the system boots up properly.
The default installation does not provide any graphical user interface environment, and only a minimal set of command-line tools. Please refer to the Ubuntu Server documentation about how to unminimize it if necessary.
We do not recommend running a graphical user interface environment on a system running the Software Probe.



Storage configuration [Help]

FILE SYSTEM SUMMARY

MOUNT POINT	SIZE	TYPE	DEVICE TYPE
[/	18.996G	new xfs	new LVM logical volume ▶]
[/boot	1.000G	new xfs	new partition of local disk ▶]
[/opt/btech/probe/storage/recordings	30.000G	new xfs	new LVM logical volume ▶]

AVAILABLE DEVICES

No available devices

[Create software RAID (md) ▶]
[Create volume group (LVM) ▶]

USED DEVICES

DEVICE	TYPE	SIZE
[probe (new)	LVM volume group	48.996G ▶]
recordings	new, to be formatted as xfs, mounted at /opt/btech/probe/storage/recordings	30.000G ▶]
root	new, to be formatted as xfs, mounted at /	18.996G ▶]
[/dev/sda	local disk	50.000G ▶]
partition 1	new, BIOS grub spacer	1.000M ▶]
partition 2	new, to be formatted as xfs, mounted at /boot	1.000G ▶]
partition 3	new, PV of LVM volume group probe	48.997G ▶]

[Done]
[Reset]
[Back]

Figure 2.9: Finishing partitioning setup

Profile configuration [Help]

Enter the username and password you will use to log in to the system. You can configure SSH access on a later screen, but a password is still needed for sudo.

Your name:

Your servers name:
The name it uses when it talks to other computers.

Pick a username:

Choose a password:

Confirm your password:

Figure 2.10: Create a log-in profile

Upgrade to Ubuntu Pro [Help]

Upgrade this machine to Ubuntu Pro for security updates on a much wider range of packages, until 2034. Assists with FedRAMP, FIPS, STIG, HIPAA and other compliance or hardening requirements.

[About Ubuntu Pro ▶]

() Enable Ubuntu Pro

(X) Skip for now

You can always enable Ubuntu Pro later using the 'pro attach' command.

Figure 2.11: Enable Ubuntu Pro

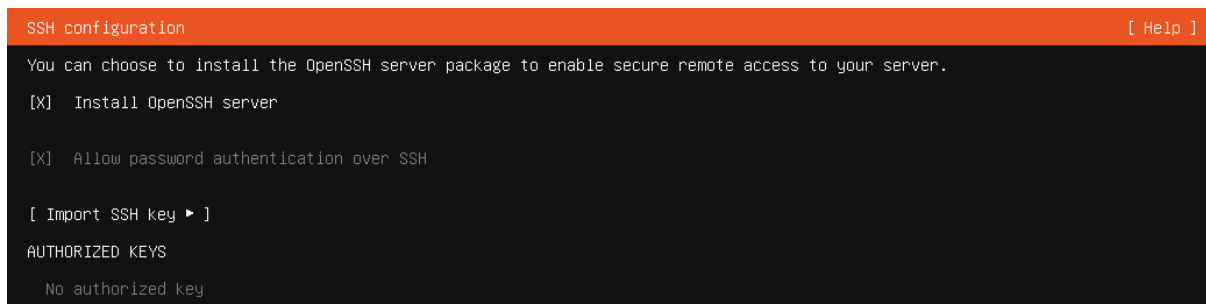


Figure 2.12: SSH configuration

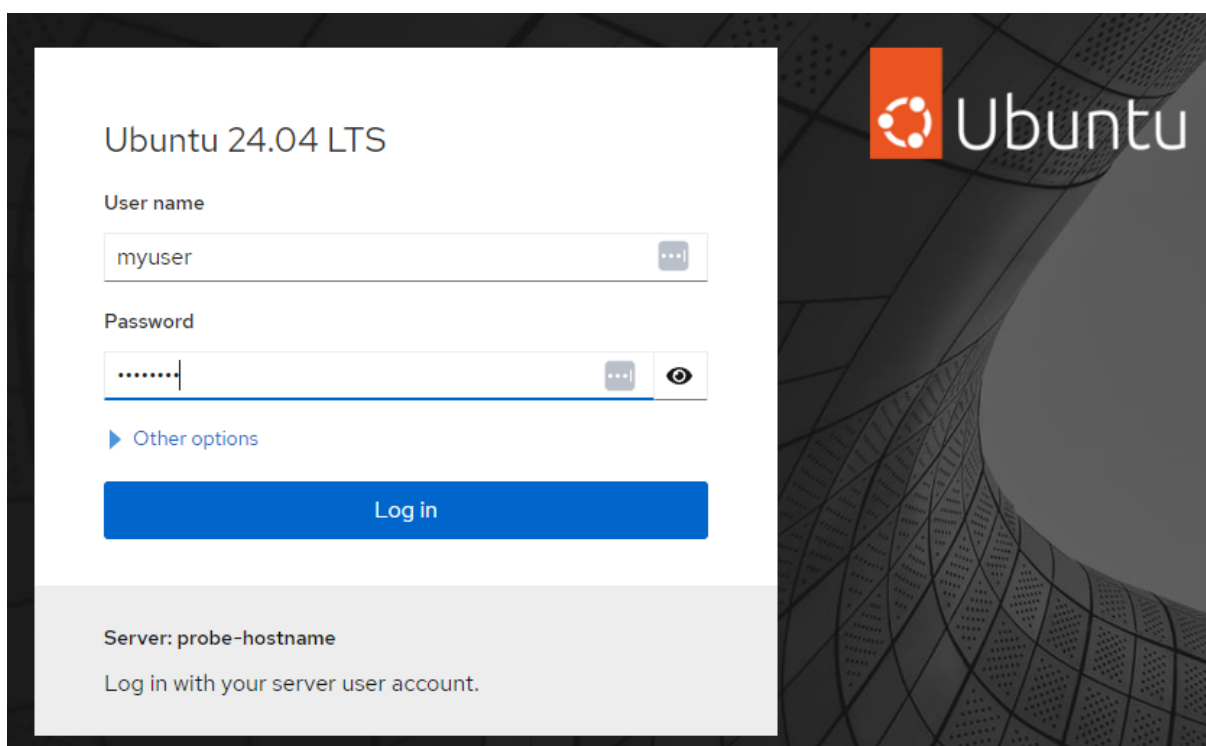


Figure 2.13: Cockpit administrative interface

2.3 Maintaining the underlying Operating System

The software installed on the system is using Ubuntu Linux Server as its base system. For information on how to maintain the operating system, including how to update it to install security patches, please refer to the Ubuntu Server system documentation.

An overview of Ubuntu Server documentation can be found at <https://ubuntu.com/server/docs/how-to>

The supported base operating system versions for VBC Controller are detailed in chapter 2.1. We recommend keeping the base operating system updated; any known incompatibilities will be published in the release notes.



2.4 Verifying Correct Initial Setup and Software Activation

Once the software has been installed and restarted all further configuration takes place through the web interface.

When logging in to the pre-built images and the VB330 Appliance, the default password for the **admin** user is **elvis**. The same password is used for logging in remotely using Secure Shell (ssh) and the Cockpit administrative interface.

1. Launch a web browser application on the management system. One of the following browsers are recommended:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Apple Safari

2. Enter the selected IP address in your web browser to access the Software Activation page. If your host is using dynamic addressing, you can log in to the account created during installation and issue the command **ip addr** to display the address assigned to the system.

If you get a HTTPS certificate warning, just accept it.

The network settings should have been set when the operating system was installed. If the web browser is unable to reach the web server, check the server's network settings in the operating system.

3. The Cockpit administrative interface should be displayed inside the browser. Cockpit is password-protected and uses the system accounts for logging in. The page displayed should look similar to figure 2.13.
4. Most operations require that you obtain administrative access by clicking the button at the top of the screen after having logged in. When using the command shell (terminal), use the **sudo** command to run programs with administrative access.

If you have enabled the root account by setting a password for it, it will automatically have administrative access.
5. If this is a new server, and you need to obtain license keys for the purchased products, please contact your sales representative.
6. The VBC Controller is not enabled by default on the newly installed server. To enable it, click the icon next to its name. This will open a detailed view with display details of the installed software, such as the installed version. If you have a license key that you want to enable and have not yet done so, enter the key in the field labeled **Apply license key** and click the **Add license** button.
7. Click the button labeled **Activate** and wait for it to finish. An activation message will be shown upon completion. If successful, the VBC Controller should now be activated, and you will be presented with a link to the user interface. The next time you access the server using a web browser, you should be taken automatically to the enabled software.

Please note that it may take some additional time before the user interface of the activated product becomes available. If you receive an error trying to access it, please wait for a few minutes before trying again.



To return to the Cockpit administrative interface to make changes, open the **About — License** tab in the VBC Controller user interface and click the link labeled **Manage server**.

It is **strongly recommended** that the system time is configured to be synchronized against an external NTP server. Please refer to N Appendix: Enabling NTP time synchronization for more information on configuring time synchronization.

2.5 Initial Setup Troubleshooting

If you are having trouble bringing up the Software Activation interface, or the VBC Controller web based management interface, verify the following:

- Verify that the client machine and the VBC Controller are configured on the same subnet and that they have different addresses, or, if you use different subnets, verify that the routing and gateways are set correctly on both the client machine and the VBC Controller.
- Make sure that the IP address of the gateway and the network interface are not the same.
- Verify that the appropriate Ethernet link indicators of the PC and the VBC Controller are lit.
- Verify that web browser proxy settings are not interfering.
- Verify that local firewall settings on the PC are not interfering.
- Try rebooting the server and make sure all services start as expected.
- Clear the browser's cache.
- Verify that the web server is running, by entering the command

```
systemctl status nginx
```

on the server's command line. If it is not running properly, check the system logs for hints by typing

```
journalctl -u nginx
```

- If you can reach the Cockpit administrative interface, but the VBC Controller GUI is not working, enter the command `vbchello` on the server's command line to verify that the VBC services are running. If services are not running, try re-installing the VBC.

Please refer to M Appendix: Network configuration for more information on server network configuration using the Cockpit administrative interface.

2.6 Upgrading From a Previous Version

We strongly recommend backing up the VBC files before upgrading to a new version of the VBC Controller, or when switching to Ubuntu 24.04 LTS. The backup procedure is described in I Appendix: Backing up the VBC of this manual.



To upgrade to this release of the VBC Controller, your system must meet the system requirements.

VBC Controller version 7.0.0 will be able to upgrade VBC version 6.4 or later only. For systems running older versions of VBC or older versions of the operating system, or to switch to Ubuntu 24.04 LTS, you must first backup the system by following the procedure described in I Appendix: Backing up the VBC. Install the new system using the instructions for new installations as described in chapter 2.2 and then restore the backup on the new system. This is described in section 2.6.2 Using a full reinstall.

2.6.1 Using the User Interface

Please refer to chapter 6.26.7 and L Appendix: Software Upload for details on how to install the upgrade image.

2.6.2 Using a full reinstall

Sometimes it is necessary to upgrade the system by doing a full reinstall. This must be done when:

- Upgrading from VBC before version 6.4
- Upgrading from a system running CentOS Linux, Rocky Linux or Red Hat Enterprise Linux to Ubuntu 24.04 LTS.
- Moving the VBC to a new server

The procedure for upgrading by doing a full reinstall is as follows:

- First back up the old machine by using the procedure described in I Appendix: Backing up the VBC. Make sure to use the backup script from the new SW version when doing the backup and store the backup in a safe location.
- Install the new system using the instructions for new installations as described in chapter 2.2.
- Restore the backup on the new system as described in I Appendix: Backing up the VBC.

Please note that classic license keys are no longer supported. Please see section 6.26.2 About — License on how to obtain the current hardware key and classic product license key and contact your sales representative to obtain a new license key before moving to a newer operating system.

2.7 Accessing the User Interface

Once the software has been installed and activated all further configuration takes place through the web interface.

The following web browsers are supported for the management interface:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Apple Safari

The login view should be displayed inside the browser. This should look similar to figure 2.14. If you have problems accessing the user interface, refer to chapter 2.5 for troubleshooting.



Current user
You are currently logged out

Login

Name

Password

Login

Figure 2.14: The VBC Controller Graphical User Interface

2.8 Firewall Configuration

If you have firewalls active, the following ports need to be enabled:

<i>Protocols and ports</i>	
Web (TCP port 80/443 and 8080)	Required. For serving clients. Port 8080 is only used if MDC is part of the VBC configuration.
Web tunneling to probes (TCP port 80/443 and 8080)	Required. The VBC will intercept and forward http (web) requests from clients towards probes on port 80 (http) or 443 (https). Port 8080 is only used if MDC is part of the VBC configuration.
Probe polling (XML over TCP port 80 or 443)	Required. Every 60 seconds, the VBC server requests measurements from the probes. Also used to verify if probes are alive.
On-line license proxy (TCP port 8443)	Required unless the probes can access the licensing service directly. When the probes are on a restricted network, they will use the proxy serving on this port to connect to the licensing service. The port needs only to be open towards the probe network.
SNMP traps and consultation (UDP ports 161 and 162)	To be able to receive SNMP traps or consult the VBC MIB.
NTP (TCP port 123)	Used for time synchronization if the probes have been configured with the VBC IP address. It is strongly recommended that the server running the VBC software, and the equipment controlled by it, be synchronized against an external NTP server. Refer to N Appendix: Enabling NTP time synchronization for more details.
Device auto-detection (UDP port 2011)	Used by the VBC to auto-detect devices.



ftp (TCP port 21)	Required if probes are to be software upgraded from the VBC server.
Secure Shell and telnet (TCP ports 22 and 23)	Useful to perform health checks etc. towards probes.

For more details on how to configure the network, please refer to A Appendix: Separate Probe and Network Interfaces.

2.9 Network configuraiton

The VBC Live Mosaic feature requires an additional dedicated Data port (DATA NIC) for receiving multicast or SRT transport streams for live transcoding. The input streams should not be received on the management interface. Some additional configuration may be required to ensure VBC Live will join multicast and SRT stream sources on the correct interface.

This is done by adding the data port IP address to the UDP_URL_SUFFIX environment variable in the configuration file:

```
/etc/opt/btech/vbclive/vbclive.conf
```

For example if the IP address of the DATA NIC is 10.0.20.30, then the UDP_URL_SUFFIX should be set to:

```
UDP_URL_SUFFIX="?localaddr=10.0.20.30&overrun_nonfatal=0&fifo_size=50000000"
```

After editing and saving the file restart the VBC Live transcoder processes with:

```
sudo systemctl restart vbc.live_worker_agent.service
```

2.10 License Details

After the unlicensed VBC Controller software is installed, it will revert to being an element manager with no access to licensed features and with no alarm features.

To obtain a license, please contact your your Bridge Technologies reseller, who will return a **Product License Key** which entered in the **About — License** view.

2.11 Accessing the administrative interface

To return to the administrative interface after activating the VBC Controller, you can either navigate to the **About — License** view and follow the **Manage sever** link, or navigate your web browser to the address <https://<IP>/admin>, where <IP> is the IP address (or host name, if using DNS) of the server.

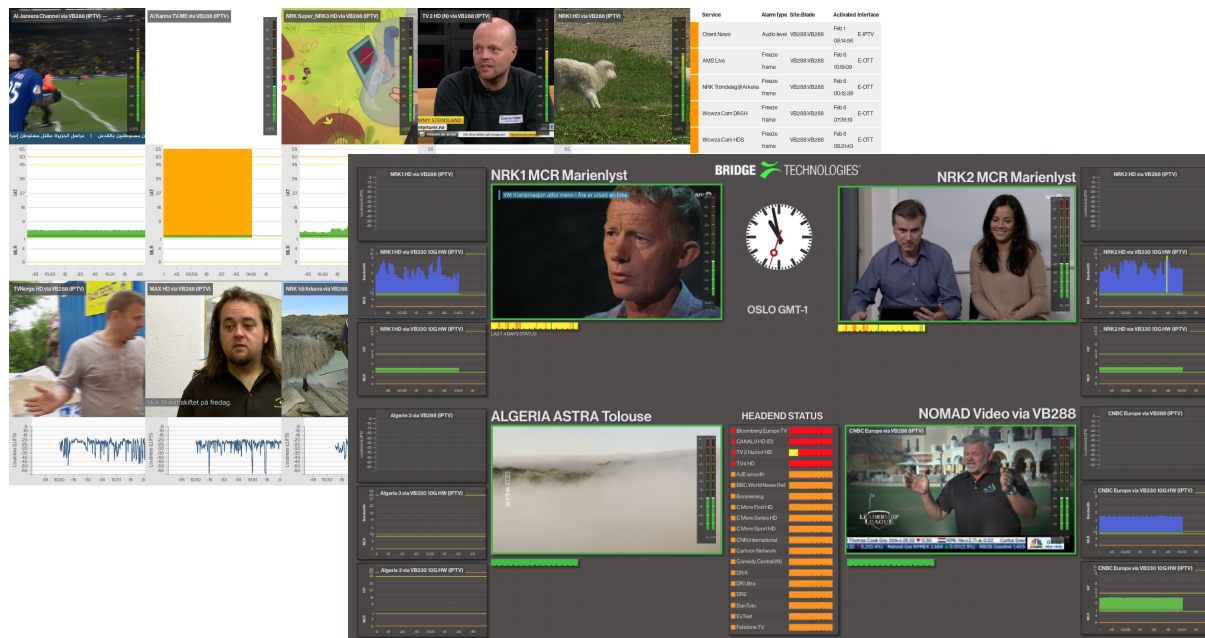
2.12 Deactivating

To deactivate VBC Controller, you must first access the administrative interface (see the previous section) and make sure that it is not set to the default. Expand the product details heading and click the **Remove as default** button.

Once this is done, access the VBC Controller user interface and de-activate it from the **About — License** view.



3 REMOTE DATA WALL



This chapter gives a quick introduction on how to use the Remote Data Wall feature of the VBC Controller.

3.1 Introduction to the Remote Data Wall

Remote Data Wall (RDW) gives the opportunity to quickly and easily create a visual representation of network activity using a web browser window. Depending on the size or complexity of the network being monitored, RDW can spread from a single screen to multiple screens in a videowall format – but requires no specialist skills to install.

The Remote Data Wall can be configured to display mosaics from the selected streams, as well as alarm lists and other important information from within the system. A configured mosaic is called a *canvas* and is configured in the **RDW — Canvases** view. Please see chapter 6.11.5 below for more information on the available widgets.

3.2 Accessing the Remote Data Wall

The Remote Data Walls can be reached by entering `<IP address>/rdw/` in a browser's URL field. All connected browser windows are displayed as *devices* in the **RDW — Devices** view. By default, the canvas named **Default** is used for new devices. It is possible to select which RDW canvas is to be displayed on a specific device in this view. Each canvas can be displayed on any number of devices.

It is not possible to use the same browser session as a Remote Data Wall display device as the one you are using to access the configuration interface.

The RDW can also be reached through the Devices list clicking the link at the bottom of the screen, as shown in the picture below.



Device 63	Testing ▼	Identify
Connect a new device by opening http://10.0.28.110/rdw in a web browser.		

Go to chapter 6.11 for details on how to configure the Remote Data Wall.



4 MASTER VBC

This chapter gives a quick introduction on how to use the Master VBC feature of the VBC Controller.

4.1 Introduction to the Master VBC

There is a limit to the number of blades one single VBC server can handle. The load on the VBC server depends on several factors, including the amount of alarm processing, the number of blades and the total number of streams. The MASTER-OPT license option allows multiple VBC servers to be managed by one top-level VBC Controller. When the VBC Controller is equipped with the Master license, it allows sub-VBCs to be added from the **Equipment** view and will fetch information from the sub-VBCs (also called external VBC or remote VBCs).

A regular VBC Controller becomes a Master VBC Controller by installing the MASTER-OPT license for the number of requested blades. This blade count should exceed the aggregate number of blades from all the sub-VBCs.

The Master VBC Controller can be licensed to support thousands of blades. The license details and blade count can be seen from the **About — License** view.

From the user's perspective the differences between a regular VBC Controller and a Master VBC Controller are the following:

- The **Monitoring — All Sites** view shows status for any site, any VBC Controller.
- The *External site alarm* is raised for any sub-VBC having alarms.
- Seamless click-through to sub-VBCs from alarms and the **All Sites** view

4.2 Configuring access rights

In order to avoid login requests when accessing the Sub-VBCs from within the Master VBC the same user account must exist on the Sub-VBC, with the **Allow access without login** flag checked in the **Main — Sites and Users — Users** User setup view. If TACACS+ authentication is enabled in the **Main — General — Authentication** view, the same constraints applies to the VBC user selected to be used for TACACS+ authenticated logins.

Authentication

Tacacs+

Tacacs+ parameters

Server IP address	10.0.28.118	Tacacs+ server IP address
Secret		Used to encrypt communication - must match setting on Tacacs+ server
Default local user	TAC default ▼	This user account will be used by default for all Tacacs+ authenticated users
Auth-key	VBUserLevel	Key to be used to authorize user access level if enabled on Tacacs+ server
Access level 1	ReadOnly ReadOnly ▼	Select local user account to match value assigned by Tacacs+ server for Auth-key
Access level 2	ReadWrite ReadwriteUser ▼	Select local user account to match value assigned by Tacacs+ server for Auth-key
Access level 3	Admin admin ▼	Select local user account to match value assigned by Tacacs+ server for Auth-key

Apply



In the below screenshot the *TAC* user needs to be identically defined on the Master VBC and the Sub-VBCs. The Sub-VBCs must have the flag **Allow access without login** checked for the user.

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

ALARM SETUP

REPORTS

EXT. REPORTS

MAIN

SITES AND USERS

LOGS

SNAPSHOTS

ALARM STATISTICS

STREAM GROUPS

SERVICE GROUPS

GFX. VIEW SETUP

GENERAL

NETWORK

ABOUT

SitesUsersUser groups

User	Info		
ReadOnly	Restricted access to 4 sites	Edit	Delete
ReadwriteUser	Normal access to 4 sites	Edit	Delete
TAC default	Normal access to 2 sites	Edit	Delete
admin	Admin access to 5 sites	Edit	Delete

Edit user

NameTAC default

Password.....

User groupNormal

Force stream-groupAll streams

Allow access without login☒

Monitoring-page displays stream-groups☒

Stack Monitoring-page vertically☐

Show number of Probes in StreamView☒

Show interface in StreamView☐

Available sites

[Unassigned]

[Autodetected]

rfsite

serversite

MANGLE

Accessible sites

julesite

site 12

Apply changes



5 THE VBC GRAPHICAL USER INTERFACE

The VBC web interface is reached by pointing a web browser to the IP address of the VBC Controller as shown in the screenshot above. The following web browsers are recommended:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Apple Safari

The web application runs on PCs, iPads, and Android devices. iPhones are currently not supported.

The user interface is divided into an Operational View and an Expert View. Configuration options are accessible through the Expert View.

The navigation menu is located in the top left corner and can be made visible or hidden by clicking the navigation menu button, which is indicated with three horizontal lines (≡) and accessible from any page. The navigation menu consists of several different icons that will help you navigate to the preferred view. These views are documented below.

The navigation menu consists of **Login**, **Alarms**, **Blade alarms**, **Streams** and **Expert** view.

Alarms, Blade alarms and Streams share a text-based **search filter** located at the top of the page. The search filter remains active across the views, enabling efficient navigation when the VBC monitors a large number of streams.

The legacy views, **Stream view**, **Thumbs view** and **Service view** can be found in the **Expert** View.

Tool-tips are available for most buttons and labels. To access tool-tip information simply navigate your cursor towards a button or a label and leave it hovering for a second or two.

The VBC web interface can be displayed in a dark or a light theme, where the dark theme is the default. Pressing the theme selector at the bottom left of the user interface switches between these two modes. The display mode is remembered across sessions, until the browser's session data is cleared. In this User's Manual, screenshots are taken using the light theme, to be friendlier on the environment when printing.

Note that different web browsers behave differently with respect to memory leaking, and if the VBC GUI should be available at all times the browser should be selected carefully. A browser memory leak manifests itself as the browser responding more and more slowly, and this is corrected by closing down the application and restarting.



5.1 Login

Current user
You are currently logged out

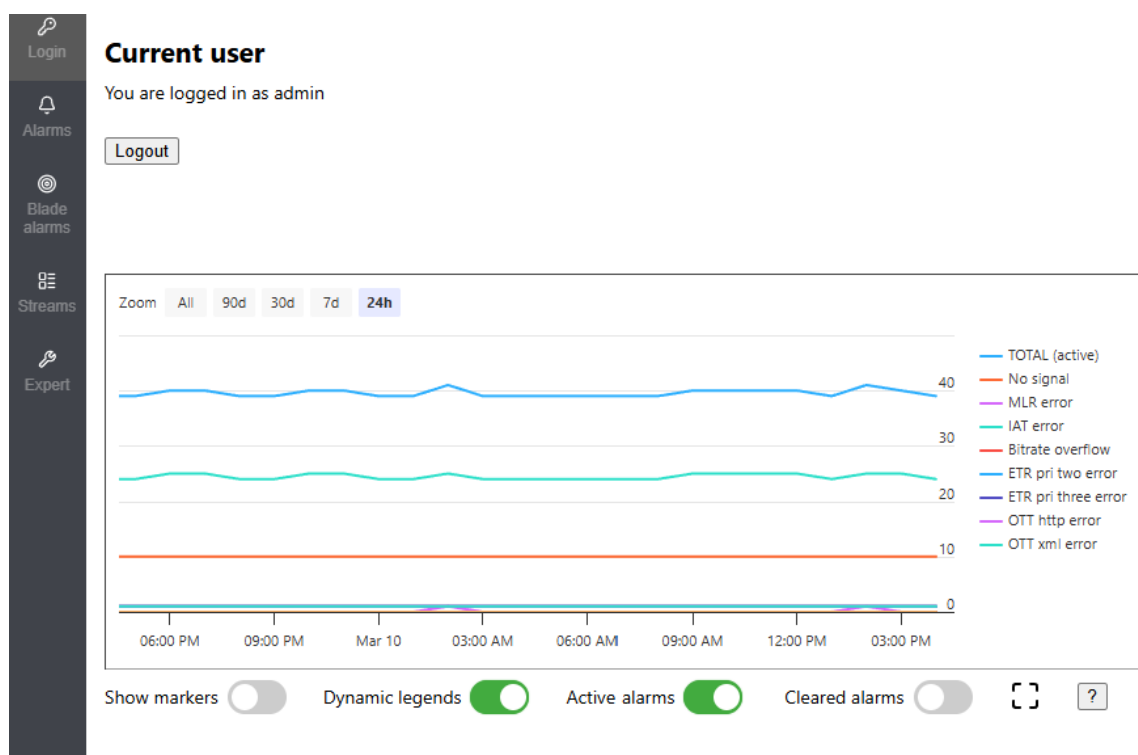
Login

Name

Password

Login

Users are required to log in to get access to the VBC Controller. Only the *admin* user can add new users – this is explained in the chapter 1.2 of this manual.



After a user has logged in, the menu-tree changes to reflect the new options.

Users will stay logged in until they actively log out or their session times out (by navigating the browser away from the VBC application).

5.2 Alarms

The **Alarm** view displays a list of active VBC alarms across all sites.



Login							
Alarms							
Blade alarms							
Streams							
Expert							

	Status	Active		Location	Iface	Stream	Description
🔍	🔴	Major	2026-03-10 07:52:04	LiveSite:129probe	IPTV	NRK1 HD	No signal NRK1 HD
🔍	🔴	Major	2026-03-10 07:52:04	LiveSite:129probe	IPTV	NRK2 HD	No signal NRK2 HD
🔍	🔴	Major	2026-03-10 07:52:04	LiveSite:129probe	IPTV	NRK3_Super HD	No signal NRK3_Super HD
🔍	🔴	Major	2026-03-10 07:52:04	LiveSite:129probe	IPTV	SVT1 HD	No signal SVT1 HD
🔍	🔴	Major	2026-03-10 07:52:04	LiveSite:129probe	IPTV	SVTB_SVT24 HD	No signal SVTB_SVT24 HD
🔍	🔴	Major	2026-03-10 07:52:04	LiveSite:129probe	IPTV	TLC Austria	No signal TLC Austria
🔍	🔴	Major	2026-03-10 07:52:04	LiveSite:129probe	IPTV	TLC Danmark	No signal TLC Danmark
🔍	🔴	Major	2026-03-10 07:52:04	LiveSite:129probe	IPTV	TLC Norge HD	No signal TLC Norge HD
🔍	🔴	Major	2026-03-10 07:52:04	LiveSite:129probe	IPTV	TLC Sverige HD	No signal TLC Sverige HD
🔍	🔴	Major	2026-03-10 07:52:04	LiveSite:129probe	IPTV	ZDF HD	No signal ZDF HD
🔍	🟡	Error	2026-03-10 07:52:04	LiveSite:129probe	IPTV	Animal Planet HD	IAT error Animal Planet HD
🔍	🟡	Error	2026-03-10 07:52:04	LiveSite:129probe	IPTV	BBC BRIT HD	IAT error BBC BRIT HD

The purpose is to get an overview of the current state. The alarms are not aggregated. The list can be sorted on Status, Activation time, Location, Interface and Stream.

An info button opens a pop-up that presents relevant blade alarms for the selected VBC alarm. Blade alarms are explained in chapter 5.3.

Configuration is done in the LIVE view that can be found under the **Expert** menu in chapter 6.2.

5.3 Blade alarms

The **Blade alarms** view displays a list of active and cleared alarms present in devices' individual alarm lists.

Login

Alarms

Blade alarms

Streams

Expert

Select by location

Site

All

Blade

All

Select by alarm

☐ Show only Active alarms

VBC alarm

No signal

Select by stream info

Stream name

Service name

Select by time

From

01/01/1999 00:00:00

To

13/03/2026 11:34:00

	Status	Active	Cleared	Location	Iface	Stream	Description	
🔍	🟢	Cleared	Mar 12 20:01:44	Mar 12 20:01:48	LiveSite:129probe	IPTV	NC_239.255.1.66	No signal
🔍	🟢	Cleared	Mar 08 07:11:20	Mar 08 07:11:24	LiveSite:129probe	IPTV	NC_239.255.1.66	No signal
🔍	🔴	Active	Mar 05 09:33:42		LiveSite:129probe	IPTV	SVTB_SVT24 HD	No signal
🔍	🔴	Active	Mar 05 09:33:42		LiveSite:129probe	IPTV	SVT1 HD	No signal
🔍	🔴	Active	Mar 05 09:33:42		LiveSite:129probe	IPTV	ZDF HD	No signal
🔍	🔴	Active	Mar 05 09:33:42		LiveSite:129probe	IPTV	NRK3_Super HD	No signal
🔍	🔴	Active	Mar 05 09:33:42		LiveSite:129probe	IPTV	NRK2 HD	No signal
🔍	🔴	Active	Mar 05 09:33:42		LiveSite:129probe	IPTV	NRK1 HD	No signal
🔍	🔴	Active	Mar 05 09:33:42		LiveSite:129probe	IPTV	TLC Sverige HD	No signal
🔍	🔴	Active	Mar 05 09:33:42		LiveSite:129probe	IPTV	TLC Norge HD	No signal
🔍	🔴	Active	Mar 05 09:33:42		LiveSite:129probe	IPTV	TLC Danmark	No signal
🔍	🔴	Active	Mar 05 09:33:41		LiveSite:129probe	IPTV	TLC Austria	No signal

Items found in database: 12

Blade alarms are reported immediately when the probes detect an alarm condition. The VBC alarms are based on error-seconds reported by probes. The relationship between blade alarms and VBC alarms is described in documents available in the **Alarm setup** page in the Expert View (requires admin login).

Note that only alarms that are enabled in devices will be present in the **Blade alarms** view.

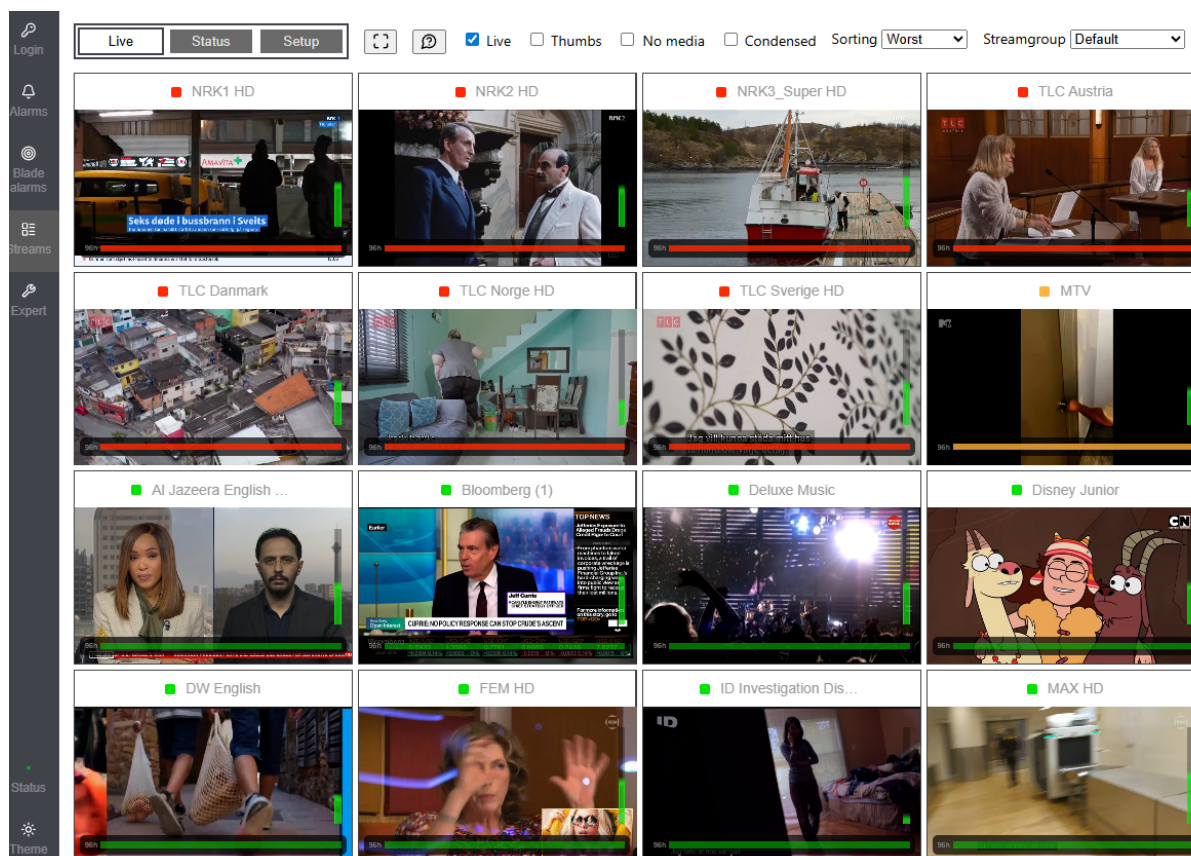
The list of alarms can be filtered by utilizing the **Options** in the top menu. It is possible to toggle between displaying all alarms and only active alarms. Description of the configuration can be found in the Expert view under section 6.4.



5.4 Streams

The **Streams** view displays video and alarms from multiple streams for confidence monitoring. It can be used to create a mosaic wall of live-decoded and/or thumbnail-decoded streams.

Each tile can display video, audio bar, and alarm history. The alarm graph shows the aggregated alarm status, combining alarms from all probes monitoring the stream.



The **Streams** view provides operational efficiency:

- Viewing options : select between Mosaic (Live and Thumbs) or List View (Condensed).
- Sorting options : choose from predefined sorting methods.
- Stream Groups : switch between predefined sets of streams.

Use the following buttons to:

 Open fullscreen mode. Press  to leave fullscreen.

 Show information about the Streams view.

The Mosaic wall can be populated with any combination of streams available to the VBC by toggling “Live”, “Thumbs”, and “No Media” check-boxes. To mimic the traditional Stream View, toggle the Condensed check-box on. The check-boxes for “Live”, “Thumbs”, and “No Media” have no effect in this mode.



The following table describes the display options:

<i>Streams view display options</i>	
Live	Tiles with live video and alarm history.
Thumbs	Tiles with still pictures and alarm history.
Condensed	List of streams with alarm history.

The following table describes the sorting and filtering options:

<i>Streams view sorting options</i>	
Sorting	Sort streams based on predefined categories: Name, Interface, Worst and Best.
Streamgroup	Toggle between predefined stream groups. Configure at Main — Stream groups .

The **Condensed** view lists the streams together with their alarm history. The **Streams** view can be tailored for each operator by combining predefined selections.

One key use case is the Penalty Box feature, available through the **Sorting** options, which automatically orders streams by alarm severity.

NRK1 HD	2	NRK2 HD	2
NRK3_Super HD	2	SVT1 HD	2
SVTB_SVT24 HD	2	TLC Austria	2
TLC Danmark	2	TLC Norge HD	2
TLC Sverige HD	2	ZDF HD	2
Animal Planet HD	1	BBC BRIT HD	1
BBC Earth HD	1	DASH	1
Discovery Science (1)	1	Eurosport Norge HD	1
FOLX MUSIC TELEVISION (1)	1	Fritz	1
FTV UHD	1	HISTORY HD	1

Detailed mode is available for each stream through stream selection. When a stream is selected, a new page lists all Probes receiving that particular stream.



Login

Alarms

Blade alarms

Streams

Expert

NRK Super _ NRK3 HD

Probe list - NRK Super _ NRK3 HD

Interface	Probe	Site	96h	Stream
IPTV	VB220-258-246	Terrestrial+ASI		NRK Super _ NRK3 HD
IPTV	VB330 - HW	Central HE		NRK Super _ NRK3 HD@eth0
IPTV	Appliance Server	Central HE		NRK Super _ NRK3 HD
IPTV	VB220-SW	Cloud IP Probe		NRK Super _ NRK3 HD
IPTV	JPEG-XS	JPEG-XS		NRK Super _ NRK3 HD

Alarms - NRK Super _ NRK3 HD

Active	Cleared	Location	Iface	Stream	Description	
	2026-03-11 01:18:03	2026-03-11 01:30:02	Cloud IP Probe:VB220-SW	IPTV	NRK Super _ NRK3 HD	QoE video NRK Super _ NRK3 HD
	2026-03-11 01:18:03	2026-03-11 01:25:03	JPEG-XS:JPEG-XS	IPTV	NRK Super _ NRK3 HD	QoE video NRK Super _ NRK3 HD
	2026-03-11 01:18:03	2026-03-11 01:25:03	Central HE:Appliance Server	IPTV	NRK Super _ NRK3 HD	QoE video NRK Super _ NRK3 HD
	2026-03-09 01:18:03	2026-03-09 01:26:02	JPEG-XS:JPEG-XS	IPTV	NRK Super _ NRK3 HD	QoE video NRK Super _ NRK3 HD

It is possible to drill down to a specific probe using a link that navigates directly to the **Stream overview** page in the Probe's **Expert** view. Live-decoded streams display an audio icon in the thumbnail for audio playback.

NRK

Live ☒ Thumbs ☐ No media ☐ Condensed Sorting Best Streamgroup Default

NRK Super _ NRK3 ...

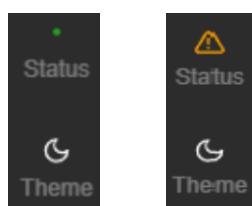
NRK Tegnspråk

NRK2 HD

The main license supports a limited number of Live streams; refer to the License Options section for details.

5.4.1 Streams Performance Indicator

Live decoding performance depends heavily on server capabilities and the characteristics of the streams being decoded. See section **VBC Live Mosaic requirements** for additional guidance.





A performance indicator is shown in the lower section of the main left menu to notify the operator if the client has detected any performance issues. If the Streams page experiences low frame rates for multiple streams, the status icon will show a warning indicating that the client (typically CPU, GPU, or networking) is struggling to keep up. Limiting the number of live streams can reveal whether the issues are front-end related.

5.4.2 Streams Configuration

Configure the **Streams** view on the **Setup** tab. All live video displayed in the Streams view is generated by the VBC server. In order to do that, the VBC server must have access to all the streams, either as multicasts, unicasts or as SRT streams. The URLs configured in the Live Setup page must match streams available on the VBC server.

Type	Name	Video setup	URL source	URL	Joined	#
RDP	129probe_1	Enabled	Manual	srt://10.0.30.129:3301?mode=caller		
RDP	129probe_2	Enabled	Manual	srt://10.0.30.129:3302?mode=caller		
Probe	AI Jazeera English HD	Enabled	Device config	udp://239.255.2.39:5500	*	1
Probe	Animal Planet HD	Unconfigured	Device config	udp://239.255.2.22:5500	*	1
Probe	BBC BRIT HD	Unconfigured	Device config	udp://239.255.2.23:5500	*	2
Probe	BBC Earth HD	Unconfigured	Device config	udp://239.255.2.18:5500	*	2
Probe	BBC World News Europe HD (1)	Unconfigured	Device config	udp://239.255.1.27:5500	*	1
Probe	Bloomberg (1)	Enabled	Device config	udp://239.255.1.14:5500	*	1
Probe	CNBC (1)	Unconfigured	Device config	udp://239.255.1.15:5500	*	1

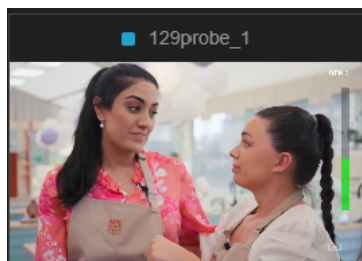
The Setup page is only available for users with admin rights. Other users will not see the three tabs described below:

Streams view options	
Live	Displays the Live view.
Status	Displays resource usage.
Setup	Displays configuration page to add streams.

Select the **Setup** tab to open up the configuration page. The Setup page provides multiple filtering mechanism to ease configuration of streams. Streams can be found through information from the Probe or added locally to the VBC. For the VBC Live option, the streams must be received by the VBC server itself. Transmission methods are multicast, SRT or RDP.

Streams that are received by a Probe are listed and the operator can select which streams to join for live decoding. Join enables active monitoring of the stream. Another way of receiving streams monitored by the Probes, is to transmit the stream from the Probe to the VBC via RDP. There is a search option that displays only RDP feeds.

Alarm history is shown as a 96h alarm-graph in the tile as long as the stream-name in the Live Setup page matches the stream-name used by probes monitoring the stream.



Streams that are not monitored by any Probes can be received by multicast or SRT. The filter option named “Local” displays only streams that are received by the VBC server. These streams have a blue icon, no alarm history and are only visible to users with admin rights if the **Streamgroup** is set to **Default**. A blue icon is also shown for streams that are monitored by Probes, but the Video Setup state is set to “On hold”.

Sorting options for the setup page

Configured	Displays all configured streams.
Joined	Displays streams that are currently joined and monitored by one or more probes.
Not joined	Displays streams that are configured but not monitored by one or more probes.
RDP engine	Displays RDP configurations obtained from Probes.
Locals	Displays streams that are only joined on the VBC server, not on a Probe.

The Video Setup column let the operator choose to pause (“On hold”), enable (“Enabled”), or disable (“Unconfigured”) individual streams. The URL source can be overwritten by the operator by choosing the override option in the URL source column. The URL column displays the current source of the stream.

Streams configurations

Type	Information about how the stream is joined: Probe, RDP, Local
Name	Stream name. Manual override option for some Types.
Video setup	Control if a stream is being monitored: “On hold”, “Enabled”, or “Unconfigured”.
URL source	Option to manually override URL.
URL	Pre-filled or manually entered by setting URL source to “Override”.
Joined	Indication if stream is currently joined and monitored by one or more probes.
Number	Number of probes currently monitoring the stream.



5.4.3 Streams Status

Login

Alarms

Blade alarms

Streams

Expert

LiveStatusSetup?

Resource usage for each server

Worker	System CPU	Transcoders CPU	Idle CPU	System MEM	Transcoders MEM	Free MEM
probe	17.1 %	8.6 %	82.9 %	15.99 GB	1.17 GB	13.26 GB

Resource usage for each transcoded stream

Worker	Stream name	CPU	MEM	MEM
probe	NRK1 HD	37.2 %	0.95 GB	5.9 %
probe	SW330_1	9.2 %	0.10 GB	0.6 %
probe	hw4_1	21.3 %	0.11 GB	0.6 %

Select the Status tab to open the status page. This page displays the resource usage (CPU and Memory) for each stream and for each transcoded stream. This information is available only to users with admin rights.

Server health can be monitored through resource usage, helping operators configure streams without exceeding server capacity.

Status information

System CPU	How much CPU the system uses in total (all functionality including transcoding).
Transcoder CPU	How much CPU is used to transcode streams for Live View. This number is included in the System CPU number.
Idle CPU	Idle time (100%–System).
System MEM	Max system memory.
Transcoder MEM	Memory used by transcoders.
Free MEM	Available memory.

5.4.4 VBC Live Mosaic requirements

The VBC Live Mosaic functionality is restricted by a License. The input streams must be received on the data interface. Refer to the Network configuration chapter for details. Live decoding performance depends heavily on server capabilities and the characteristics of the input streams.

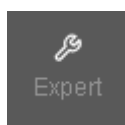
Rule of Thumb

Reference: One AVC 720p50/1080i25 4:2:0 8 bit stream requires 1 modern Intel Xeon Gold physical CPU core.

- AVC 4:2:2 10bit requires 2× the reference
- HEVC 4:2:0 8bit requires 2× the reference
- HEVC 4:2:2 10bit requires 3× the reference

Please contact <https://bridgetech.tv/support/> for further details.

5.5 Expert



Selecting **Expert** in the main menu opens the Expert Graphical User Interface, which gives access to VBC Controller configuration and additional features.

The contents of the Expert Graphical User Interface is described in detail in chapter 6.



6 EXPERT VBC GRAPHICAL USER INTERFACE

#	Sev	Activated	Cleared	Site Name	Description
1	■	2026-03-26 20:03:02		Processing.VB330-Recording	IAT error DigiTV
2	■	2026-04-09 12:44:04		Processing.10 TIMES	ETR pri one error STREAMS:10
3	■	2026-04-09 13:23:05		Ingest.19 TIMES	ETR pri one error STREAMS:10
4	■	2026-04-09 12:46:04		Processing.10 TIMES	ETR pri two error STREAMS:10
5	■	2026-04-09 13:23:05		Ingest.19 TIMES	ETR pri two error STREAMS:10
6	■	2026-04-09 13:05:04	2026-04-09 13:23:02	Ingest.19 TIMES	ETR pri two error STREAMS:10
7	■	2026-04-09 13:02:05	2026-04-09 13:23:02	Ingest.20 TIMES	ETR pri one error STREAMS:10
8	■	2026-04-09 12:49:04	2026-04-09 13:15:02	Processing.10 TIMES	MLR error STREAMS:10
9	■	2026-04-09 12:49:04	2026-04-09 13:15:02	Ingest.20 TIMES	MLR error STREAMS:10
10	■	2026-04-09 13:03:05	2026-04-09 13:05:02	Ingest.20 TIMES	ETR pri two error STREAMS:10
11	■	2026-04-09 13:02:05	2026-04-09 13:03:02	Ingest.19 TIMES	ETR pri two error STREAMS:10
12	■	2026-04-09 12:44:04	2026-04-09 13:02:02	Ingest.13 TIMES	ETR pri two error STREAMS:10
13	■	2026-04-09 12:58:06	2026-04-09 13:02:02	Ingest.14 TIMES	ETR pri one error STREAMS:10
14	■	2026-04-09 12:44:04	2026-04-09 12:58:02	Ingest.13 TIMES	ETR pri one error STREAMS:10
15	■	2026-04-09 12:44:04	2026-04-09 12:45:02	Processing.9 TIMES	ETR pri two error STREAMS:9
16	■	2026-04-09 12:43:06	2026-04-09 12:44:02	Processing.9 TIMES	ETR pri one error STREAMS:9
17	■	2026-04-09 12:43:06	2026-04-09 12:44:02	Processing.6 TIMES	ETR pri two error STREAMS:6
18	■	2026-04-09 12:43:06	2026-04-09 12:44:02	Ingest.9 TIMES	ETR pri two error STREAMS:8
19	■	2026-04-09 12:35:04	2026-04-09 12:44:02	Ingest.12 TIMES	ETR pri one error STREAMS:10
20	■	2026-04-09 12:35:04	2026-04-09 12:43:02	Processing.3 TIMES	ETR pri two error STREAMS:3

The **Expert** view provides access to more in-depth analysis and to the VBC Controller configuration options. It can be reached by selecting the **Expert** option in the navigation menu in the top left corner of the screen.

The Expert UI can be navigated by using the tree menu, which is always located next to the navigation menu. The menu contains more entries for the *admin* than the menu for regular users. Some menu items are nested, in particular the site and blade sub-menu entries are provided to allow quick access to the last visited site and blade.

Note: Some of the screenshots in this section are taken from a previous software release. While the look of these pages has changed, the information displayed and documentation is still valid for this release.



6.1 Login

Login

Alarms

Blade alarms

Streams

Expert

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

REPORTS

EXT. REPORTS

MAIN

User login

License info

Activated

Current user

You are currently logged in as: **demo**

Logout

Login history for demo:

#	Username	IP-address	Login time	Logout time
1	demo	10.0.28.159	2026 Mar 16 13:08:03	(active)
2	demo	172.20.0.199	2026 Mar 12 11:13:56	(active)
3	demo	10.0.28.254	2026 Mar 16 07:34:55	2026 Mar 16 11:53:06 [Vo]
4	demo	10.0.28.9	2026 Mar 16 08:16:52	2026 Mar 16 08:36:33
5	demo	10.0.28.66	2026 Mar 16	2026 Mar 16 08:20:07

Alarm statistics - sum of active and cleared alarms for each hour

Zoom All 90d 30d 7d 4d 24h 4h

Users are required to log in through the main **Login** view. Please see chapter 5.1 on page 29 for details.

The Expert view provides login history and alarm statistics for all sites.

The **Logout** button will log the user out, and the main **Login** page will be displayed.



6.2 Live

	Active alarms all sites							
LOGIN	Fields...	Filter alarms...	Page 1	Page -1	Page +1	Page +5		
LIVE								
MONITORING	#	Sev	Status	Activated	Dt	Site:Name	Interface	Description
BLADE ALARMS	1	Major	2020 Nov 2 11:08:20	157m	VB330:Core	IPTV	No signal ATV Test	
GRAPHICS VIEW	2	Major	2020 Oct 25 03:01:21	8d	DVB-T2-VB252-T2	IPTV	No signal NRK1	
STREAM VIEW	3	Major	2020 Oct 25 03:01:21	8d	DVB-T2-VB252-T2	IPTV	No signal T2MI	
THUMBS VIEW	4	Major	2020 Nov 2 11:08:20	157m	VB330:Core	IPTV	No signal Test-Cuba	
SERVICE VIEW	5	Major	2020 Nov 2 13:38:20	433s	V6.0 RELEASE-VB330 SW v6	IPTV	QoE audio test0	
MAP	6	Major	2020 Nov 2 13:39:21	372s	V6.0 RELEASE-VB330 SW v6	IPTV	QoE video test0	
RDP	7	Major	2020 Nov 2 13:39:21	372s	V6.0 RELEASE-VB330 SW v6	IPTV	QoE video test1	
RDW	8	Major	2020 Nov 2 13:39:21	372s	V6.0 RELEASE-VB330 SW v6	IPTV	QoE video test2	
EQUIPMENT	9	Error	2020 Oct 25 03:01:21	8d	VB330:Core	IPTV	IAT error Disney Channel (D)	
ALARM SETUP	10	Error	2020 Oct 25 03:01:21	8d	DASH QoS (VB220:OTT-VB2)	IPTV	IAT error Disney Channel (D)	
TIMELINE	11	Error	2020 Oct 25 03:01:21	8d	VB330:Core	IPTV	IAT error Disney Channel (N)	
REPORTS	12	Error	2020 Oct 25 03:01:21	8d	DASH QoS (VB220:OTT-VB2)	IPTV	IAT error Disney Channel (N)	
EXT. REPORTS	13	Error	2020 Oct 25 03:01:21	8d	VB440 test:VB440	IPTV	IAT error Matrox 2 Video@Primary	
MAIN	14	Error	2020 Oct 25 03:01:21	8d	V6.0 RELEASE-VB440 v6.0	IPTV	IAT error Matrox 2 Video@Primary	
	15	Error	2020 Oct 25 03:01:21	8d	VB440 test:VB440	IPTV	IAT error Matrox 2 Video@Secondary	
	16	Error	2020 Oct 25 03:01:21	8d	V6.0 RELEASE-VB440 v6.0	IPTV	IAT error Matrox 2 Video@Secondary	
	17	Error	2020 Nov 2 09:32:21	4h	VB220-VB272-VB272 DVB S-	IPTV	MLR error CNBC Europe	
	18	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101	
	19	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101a	
	20	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101aa	
	21	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101ab	
	22	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101ac	
	23	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101ad	
	24	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101ae	
	25	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101af	
	26	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101ag	
	27	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101ah	
	28	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101ai	
	29	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101b	
	30	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101c	
	31	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101d	
	32	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101e	
	33	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101f	
	34	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101g	
	35	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101h	
	36	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101i	
	37	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101j	
	38	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101k	
	39	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101l	
	40	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101m	
	41	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101n	
	42	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101o	
	43	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101p	
	44	Error	2020 Oct 25 03:01:21	8d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200_101q	

The alarm list in the **Live** view displays all currently un-aggregated active VBC alarms. The list is identical to the list in the **Monitoring** view, except that cleared alarms are not included and alarms are not aggregated.



6.3 Monitoring

The VBC provides monitoring at three different levels. Top-level monitoring allows the user to get an overview picture of the complete system; site monitoring provides details about one selected site and blade monitoring allows the user to monitor a specific device.

6.3.1 Monitoring — Top Level

LOGIN

LIVE

MONITORING

SITE

BLADE

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDV

RDW

EQUIPMENT

ALARM SETUP

TIMELINE

REPORTS

EXT. REPORTS

MAIN

Status for all sites

Ok	Err	Now	Site
0	0		ATest
0	1		DASH QoS (VB220)
0	1		DVB-T2
1	0		HLS QoS (VB120)
1	0		MCR
2	0		MicroVB-MDC
1	0		QTT Manager
0	1		QTT QoS (VB288)
0	2		V6.0 RELEASE
0	1		VB120-VB252
1	0		VB220-VB252-252
0	1		VB220-VB252-252
0	1		VB220-VB272
0	0		VB243
1	0		VB273
0	1		VB288
1	2		VB330
0	1		VB440 test
1	0		VB50

Streamgroup status

	[All streams]
	AJZ
	ASJ
	COFDM
	Content checked
	Demo
	HD Services
	HeadEnd
	NRK 1 HD
	NilsTest
	OTT
	Premium
	SD Services
	Thor5 - C11
	Training
	YLETV
	satellite

Alarms all sites

Fields...	Filter alarms...	Clear alarms	Page 1	Page -1	Page +1	Page +5		
#	Sev	Status	Activated	Cleared	Dt	Site Name	Interface	Description
1	Major		2020 Oct 25 03:01:23		8d	DVB-T2 2 TIMES	IPTV	No signal STREAMS:2
2	Major		2020 Nov 2 11:08:32		166m	VB330 2 TIMES	IPTV	No signal STREAMS:2
3	Major		2020 Nov 2 13:53:21		107s	V6.0 RELEASE-VB330 SW v6	IPTV	QoE audio test0
4	Major		2020 Nov 2 13:54:36		32s	V6.0 RELEASE-3 TIMES	IPTV	QoE video STREAMS:3
5	Error		2020 Oct 25 03:01:24		8d	VB440 test:2 TIMES	IPTV	IAT error STREAMS:2
6	Error		2020 Oct 25 03:01:24		8d	V6.0 RELEASE-2 TIMES	IPTV	IAT error STREAMS:2
7	Error		2020 Nov 2 05:32:32		8h	DASH QoS (VB220 2 TIMES	IPTV	IAT error STREAMS:2
8	Error		2020 Nov 2 09:08:31		4h	VB330 2 TIMES	IPTV	IAT error STREAMS:2
9	Error		2020 Nov 2 05:32:32		8h	VB330 2 TIMES	IPTV	MLR error STREAMS:72
10	Error		2020 Nov 2 09:32:21		4h	VB220-VB272-VB272 DVB S-	IPTV	MLR error CNBC Europe
11	Error		2020 Nov 2 13:55:02		6s	VB288 2 TIMES	E-OTT	OTT alignment STREAMS:2
12	Error		2020 Nov 2 11:41:40		133m	QTT QoS (VB288):2 TIMES	OTT	OTT http error SL01
13	Error		2020 Oct 31 22:20:33		39h	V6.0 RELEASE-2 TIMES	OTT	OTT http error STREAMS:2
14	Error		2020 Nov 2 13:21:39		33m	VB330 4 TIMES	OTT	OTT http error STREAMS:4
15	Error		2020 Nov 2 11:39:42		135m	VB288 2 TIMES	OTT	OTT transport error STREAMS:2
16	Error		2020 Nov 2 13:10:32		44m	VB330 2 TIMES	OTT	OTT transport error STREAMS:2
17	Error		2020 Oct 26 12:51:20		7d	V6.0 RELEASE-VB330 SW v6	OTT	OTT transport error NASA TV
18	Error		2020 Nov 2 11:40:40		134m	VB288 3 TIMES	OTT	OTT xml error STREAMS:3
19	Error		2020 Nov 2 11:44:32		130m	DASH QoS (VB220 3 TIMES	OTT	OTT xml error STREAMS:3
20	Error		2020 Nov 2 13:47:21		467s	VB330 Core	OTT	OTT xml error Test 3
21	Error		2020 Oct 25 03:01:24		8d	VB330 72 TIMES	IPTV	RTP drops STREAMS:72
22	Error		2020 Nov 2 13:53:21		107s	VB440 test-VB440	IPTV	RTP drops Matrox 2 Video@Secondary
23	Error		2020 Nov 2 13:53:21		107s	V6.0 RELEASE-VB440 v6.0	IPTV	RTP drops Matrox 2 Video@Secondary
24	Warning		2020 Oct 25 03:01:24		8d	VB440 test:9 TIMES	IPTV	Bitrate overflow STREAMS:9
25	Warning		2020 Oct 25 03:01:24		8d	V6.0 RELEASE-9 TIMES	IPTV	Bitrate overflow STREAMS:9
26	Warning		2020 Nov 2 09:33:20		4h	VB220-VB272-VB272 DVB S-	IPTV	Bitrate underflow T2M1 Container
27	Warning		2020 Oct 25 03:01:21		8d	VB330 Core	IPTV	Bitrate underflow NASA UHD 2022-7
28	Warning		2020 Nov 2 09:32:21		4h	VB220-VB272-VB272 DVB S-	IPTV	Bitrate underflow PLPO
29	Warning		2020 Oct 25 03:01:21		8d	VB220-VB252-252-VB252	COFDM2	ETR interface error RIKSTV-MUX4-CH30
30	Warning		2020 Oct 25 03:01:21		8d	VB220-VB272-VB272 DVB S-	SAT2	ETR interface error TP37 UHD
31	Warning		2020 Nov 2 13:53:40		88s	VB220-VB252-252-2 TIMES	COFDM1	ETR pri one error STREAMS:2
32	Warning		2020 Nov 2 13:54:36		32s	VB220-VB272-2 TIMES	IPTV	ETR pri one error STREAMS:2
33	Warning		2020 Nov 2 13:54:36		32s	VB330 4 TIMES	IPTV	ETR pri one error STREAMS:4
34	Warning		2020 Oct 30 10:26:33		3d	VB330 2 TIMES	IPTV	ETR pri other error STREAMS:2
35	Warning		2020 Nov 2 13:54:36		32s	VB120-VB262-7 TIMES	IFACES:3	ETR pri three error STREAMS:7
36	Warning		2020 Oct 25 03:01:21		8d	VB330 Core	IPTV	ETR pri three error NRK1 HD (RTP)
37	Warning		2020 Oct 25 03:01:21		8d	DASH QoS (VB220-OTT-VB272	IPTV	ETR pri three error MPTS TV 2
38	Warning		2020 Oct 25 03:01:21		8d	VB220-VB252-252-VB252	COFDM2	ETR pri three error RIKSTV-MUX4-CH30
39	Warning		2020 Nov 1 23:23:38		14h	VB120-VB262-2 TIMES	IPTV	ETR pri two error STREAMS:2
40	Warning		2020 Nov 2 09:32:21		4h	VB220-VB272-VB272 DVB S-	IPTV	ETR pri two error CNBC Europe
41	Warning		2020 Oct 25 03:01:21		8d	VB220-VB252-252-VB252	COFDM2	ETR pri two error RIKSTV-MUX4-CH30
42	Cleared		2020 Nov 2 13:44:11	2020 Nov 2 13:55:02	10m	VB288-VB288	E-OTT	OTT alignment Bipbop
43	Cleared		2020 Nov 2 13:53:48	2020 Nov 2 13:54:22	34s	VB288 2 TIMES	E-OTT	OTT alignment STREAMS:2
44	Cleared		2020 Nov 2 13:43:21	2020 Nov 2 13:54:20	11m	VB288-VB288	OTT	OTT http error Wowza Cam SS

The top level **Monitoring** page displays status for each site and a top level alarm list. The color of the bulb indicates the severity of the most severe active alarm for a device that belongs to the site.

The layout of this page can be changed in the user setting described in the **Sites and Users — Users** menu.

The following color codes are used for bulbs:

Color codes in bulbs	
Green	No active alarms (or only alarms set to severity OK)
Yellow	The most serious active alarm is a warning
Orange	The most serious active alarm is an error
Red	The most serious active alarm is a major error (typically No Signal)
Black	At least one device has a fatal error (typically cannot be reached)

The same color codes are used for alarms.

The severity of different alarms can be customized globally by the *admin* user, in the **Alarm setup** view.

VBC Controller User's Manual v7.0.0 © Bridge Technologies Co AS

41



The user can select which alarms to show and hide in the **Filter alarms** view. The setting is reset to the default when the user logs in the next time. Clicking **Clear alarms** will wipe all the cleared alarms from the alarm list. The alarm list is reset the next time the user logs in.

To avoid reporting too many alarms, the alarm list in the **Monitoring** page merges similar alarms within a site. This is called **alarm aggregation** and is not performed for any other alarm list except the SNMP alarm list. Alarm aggregation is not performed across sites. Hence similar alarms in different sites are never merged.

The following table shows examples of alarm aggregation:

Raw alarm	Aggregated alarm
SiteA:BladeX No signal BBC SiteA:BladeY No signal BBC	SiteA:2 TIMES No signal BBC
SiteB:BladeX No signal BBC SiteB:BladeY No signal NRK SiteB:BladeZ No signal BBC	SiteB:3 TIMES No signal STREAMS:2

The N TIMES aggregation indicates that N alarm messages were merged. The STREAMS:M aggregation indicates that in total M different stream names were reported in the raw messages.

In the VBC, all probe alarms are based on error-seconds measurements reported by probes, compared against error thresholds defined for the same probe. Extractor alarms reflect the current device status.

In order to view probe alarms that may possibly correspond to a VBC alarm, click the blue information icon ⓘ associated with the VBC alarm. A pop-up view shows individual **Blade alarms** that match the VBC alarm in time and type of alarm. Note that the time on the probes and the VBC should be synchronized in order for this functionality to work correctly, refer to N Appendix: Enabling NTP time synchronization for more details. Also note that alarms must be enabled probe GUI, otherwise they will not be displayed in the pop-up view. Please refer to the probe manual for more information. As there is not a one-to-one relationship between probe and VBC alarms, there will often be a number of probe alarms that can cause a VBC alarm to be raised. This means that the list of probe alarms can have many entries compared to the VBC alarm text.

Blade alarms

Select by location

Site:

US-HE

Blade:

All

Select by alarm

☐ Show only Active alarms

VBC alarm:

OTT xml error

Select by stream info

Stream name:

stream...

Service name:

service...

PID:

PID...

Select by time

From:

25/03/2024 01:10:00

To:

25/03/2024 02:25:00

Alarms active in interval are shown

Sev	Status	Time	Site	Blade	Interface	Stream	VBC alarm	Description
		Cleared Mar 25 02:24:09 - Mar 25 02:24:13	US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1920x1080: Lagging behi...
		Cleared Mar 25 02:24:09 - Mar 25 02:24:13	US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1280x720: Lagging behi...
		Cleared Mar 25 02:24:08 - Mar 25 02:24:12	US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1920x1080: Lagging behi...
		Cleared Mar 25 02:24:08 - Mar 25 02:24:12	US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 640x360: Lagging behin...
		Cleared Mar 25 02:24:08 - Mar 25 02:24:12	US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1280x720: Lagging behi...
		Cleared Mar 25 02:24:08 - Mar 25 02:24:12	US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 480x272: Lagging behin...
		Cleared Mar 25 02:24:03 - Mar 25 02:24:07	US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1920x1080: Lagging behi...
		Cleared Mar 25 02:24:03 - Mar 25 02:24:07	US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1280x720: Lagging behi...
		Cleared Mar 25 02:24:02 - Mar 25 02:24:07	US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1920x1080: Lagging behi...
		Cleared Mar 25 02:24:02 - Mar 25 02:24:07	US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 640x360: Lagging behin...
		Cleared Mar 25 02:24:02 - Mar 25 02:24:07	US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1280x720: Lagging behi...
		Cleared Mar 25 02:24:02 - Mar 25 02:24:06	US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 480x272: Lagging behin...
		Cleared Mar 25 02:23:57 - Mar 25 02:24:01	US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1920x1080: Lagging behi...
		Cleared Mar 25 02:23:57 - Mar 25 02:24:01	US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1280x720: Lagging behi...
		Cleared Mar 25 02:23:56 - Mar 25 02:24:00	US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1920x1080: Lagging behi...
		Cleared Mar 25 02:23:56 - Mar 25 02:24:00	US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 640x360: Lagging behin...
		Cleared Mar 25 02:23:56 - Mar 25 02:24:00	US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1280x720: Laaqing behi...

Gaps in database affecting current selection: 0

Total records: 4936/100000

Note: Only alarms generated by devices are displayed in this list. Disabled device alarms are not available.



The status bar at the bottom of the alarm list shows information about the number of records in the database and the number of records in the current filter. Please refer to **Blade alarms** for more details.

The table below lists all VBC alarm messages; note that this is the behavior when using default thresholds (refer to E Appendix: Getting the Thresholds Right for a description on how to calibrate thresholds):

<i>Message</i>	<i>Description</i>
No contact	This alarm is raised if the VBC is unable to obtain status from a particular probe. The probes are polled every 60 seconds, so if raised, this alarm will stay active until poll contact is achieved.
External site alarm	This alarm will be raised if a remote VBC has alarms for this site. The details can be checked by accessing the remote VBC.
No signal	This alarm indicates that during the last 60 seconds poll interval the probe experienced at least 3 seconds of no signal.
RTP drops	This alarm indicates that during the last hour the number of error-seconds experienced by probe exceeded the threshold (default 5 seconds).
MLR error IAT error Bitrate overflow Bitrate underflow	These alarms indicate that during the last hour the number of error-seconds experienced by the probe exceeded the threshold (default 20 seconds).
ETR pri one error ETR pri two error ETR pri tree error ETR pri other error ETR interface error	These alarms indicate that during the last hour the number of ETR error-seconds experienced by the probe exceeded the threshold (default 250 seconds).
OTT transport error OTT http error OTT xml error	These alarms indicate that during the last hour the number of OTT error-seconds experienced by the probe or extractor exceeded the threshold (default 60 seconds).
System alarm	The device has a system alarm. This can for instance be a alarm indicating missing time synchronization or missing power to one of the power supplies.
Scrambling state	This alarms indicate that during the last poll period a VB288 Objective QoE Content Extractor has detected that either the signal is scrambled while expecting it not to be or vice versa. The VB288 allows the configuration of these alarms per stream.
OTT alignment	Reported by the probe or VB288 if the profiles for an OTT service are not aligned with regard to the sequence number, suggesting that the picture is not synchronized between the profiles.
Caption availability	This alarm indicates that a service with closed caption monitoring had less caption services than specified in its threshold.
Caption quality	This alarm indicates that a quality issue with one or more of the caption services extracted from a service with closed caption monitoring.



QoE video	This alarm indicates a problem with the video quality. This can be a too low MOS score, freeze-frame or color-freeze condition for a stream that has this detection enabled.
QoE audio	According to threshold settings, a stream was either too silent, too loud or out of phase for a too long period.
Archive error	This alarm indicates the Archive server has active errors such as low disk space or too many configured streams.
Archive warning	This alarm indicates the Archive server has active warnings such as disk space less than 50%.

Please note that the alarm window can be changed from the default 1 hour as assumed in the above explanations. For shorter alarm windows the number of error seconds required are scaled accordingly.

Clicking one of the site-names will open the **site status** page.

The user may select what fields should be present in the alarm list by clicking the **Fields...** button. Removing some fields may be convenient when using a screen with low resolution.

Alarm field selection

Field	Display in alarm list
#	☒
Sev	☒
Status	☒
Activated	☒
Cleared	☒
Duration	☒
Site:Name	☒
Interface	☒
Description	☒

Apply

Select fields to be displayed in alarm list

The user may select to remove some alarm types from the alarm list by clicking the **Filter alarms...** button. This affects the graphical user interface for the current user only. By re-enabling alarms that have been previously filtered these alarm instances will re-appear in the alarm log.



LOGIN
LIVE
MONITORING
SITE
BLADE
BLADE ALARMS
GRAPHICS VIEW
STREAM VIEW
THUMBS VIEW
SERVICE VIEW
MAP
RDP
RDW
EQUIPMENT
ALARM SETUP
TIMELINE
REPORTS
EXT. REPORTS
MAIN

Alarm setup user

Reported by Probes

Message	Display in alarm list	Severity level
No signal	☒	Major
RTP drops	☒	Error
MLR error	☒	Error
IAT error	☒	Error
Bitrate overflow	☒	Warning
Bitrate underflow	☒	Warning
ETR pri one error	☒	Warning
ETR pri two error	☒	Warning
ETR pri three error	☒	Warning
ETR pri other error	☒	Warning
ETR interface error	☒	Warning
OTT transport error	☒	Error
OTT http error	☒	Error
OTT xml error	☒	Error
System alarm	☒	Major
Caption availability	☒	Error
Caption quality	☒	Error
QoE video	☒	Major
QoE audio	☒	Major

Reported by Extractor

Message	Display in alarm list	Severity level
Freeze frame	☒	Error
OTT alignment	☒	Error
Scrambling state	☒	Error

Reported by VBC

Message	Display in alarm list	Severity level
No contact	☒	Fatal
Archive Error	☒	Major
Archive Warning	☒	Error
External site alarm	☒	Major

Apply

Select alarm messages that are to be displayed in alarm lists for the current user

The user may clear out the alarm list by clicking the **Clear alarms** button. This hides the cleared alarms from the alarm list for the current user for this session, if the user logs out and in again the full alarm list will be displayed.

The **Page** buttons allow the user to view the navigate the alarm list and go back and forth in the list of alarms.



6.3.2 XML Alarms

The un-aggregated top level alarms are available as XML via a static URL. The URL is obtained by replacing the `/vbc` part of the regular VBC URL with `/vbc/static/alarms_exp.xml` – see example below.

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

ALARM SETUP

TIMELINE

REPORTS

EXT. REPORTS

MAIN

Active alarms all sites

Fields... Filter alarms... Page 1 Page -1 Page +1 Page +5

#	Sev	Status	Activated	Dt	Site/Name	Interface	Description
1	Major	2020 Nov 2 15:28:20	22h	VB330:Core	IPTV	No signal NASA UHD backup	
2	Major	2020 Oct 25 03:01:21	9d	DVB-T2:VB252-T2	IPTV	No signal NRK1	
3	Major	2020 Oct 25 03:01:21	9d	DVB-T2:VB252-T2	IPTV	No signal T2MI	
4	Major	2020 Nov 2 11:08:20	26h	VB330:Core	IPTV	No signal Test-Cuba	
5	Major	2020 Nov 3 13:53:21	494s	V6.0 RELEASE-VB330 SW v6	IPTV	QoE audio test0	
6	Major	2020 Nov 3 13:55:21	374s	V6.0 RELEASE-VB330 SW v6	IPTV	QoE video test0	
7	Major	2020 Nov 3 13:55:21	374s	V6.0 RELEASE-VB330 SW v6	IPTV	QoE video test1	
8	Major	2020 Nov 3 13:55:21	374s	V6.0 RELEASE-VB330 SW v6	IPTV	QoE video test2	
9	Error	2020 Oct 25 03:01:21	9d	VB330:Core	IPTV	IAT error Disney Channel (D)	
10	Error	2020 Oct 25 03:01:21	9d	DASH QoS (VB220:OTT-VB2)	IPTV	IAT error Disney Channel (D)	
11	Error	2020 Oct 25 03:01:21	9d	VB330:Core	IPTV	IAT error Disney Channel (N)	
12	Error	2020 Oct 25 03:01:21	9d	DASH QoS (VB220:OTT-VB2)	IPTV	IAT error Disney Channel (N)	
13	Error	2020 Nov 3 01:37:21	12h	VB440 test:VB440	IPTV	IAT error Matrox 2 Video@Primary	
14	Error	2020 Nov 3 01:37:21	12h	V6.0 RELEASE-VB440 v6.0	IPTV	IAT error Matrox 2 Video@Primary	
15	Error	2020 Nov 3 01:37:21	12h	VB440 test:VB440	IPTV	IAT error Matrox 2 Video@Secondary	
16	Error	2020 Nov 3 01:37:21	12h	V6.0 RELEASE-VB440 v6.0	IPTV	IAT error Matrox 2 Video@Secondary	
17	Error	2020 Nov 2 15:31:21	22h	VB330:Core	IPTV	IAT error NASA UHD 2022-7	
18	Error	2020 Nov 3 06:53:20	7h	VB220-VB272:VB272 DVB S-	IPTV	MLR error CNBC Europe	

← → ↺

vbc.bridgetech.tv/vbc/static/alarms_exp.xml

🔍 ☆

This XML file does not appear to have any style information associated with it. The document tree is shown below.

<?xml version="1.0" encoding="UTF-8" ?><alarmlist crc="512feae" release="2020 Nov 3 13:55:05"><msg n="1" status="Fatal" activated="2020 Oct 25 03:01:21" duration="816824" site="(Unassigned)" blade="Thomas thumbs" interface="" descr="No contact with blade" stream="" /><msg n="2" status="Major" activated="2020 Nov 2 15:28:20" duration="80805" site="VB330" blade="Core" interface="IPTV" descr="No signal" stream="NASA UHD backup" /><msg n="3" status="Major" activated="2020 Oct 25 03:01:21" duration="816824" site="DVB-T2" blade="VB252-T2" interface="IPTV" descr="No signal" stream="NRK1" /><msg n="4" status="Major" activated="2020 Oct 25 03:01:21" duration="816824" site="DVB-T2" blade="VB252-T2" interface="IPTV" descr="No signal" stream="T2MI" /><msg n="5" status="Major" activated="2020 Nov 2 11:08:20" duration="96405" site="VB330" blade="Core" interface="IPTV" descr="No signal" stream="Test-Cuba" /><msg n="6" status="Major" activated="2020 Nov 3 13:53:21" duration="104" site="V6.0 RELEASE" blade="VB330 SW v6.0" interface="IPTV" descr="QoE audio" stream="test0" /><msg n="7" status="Major" activated="2020 Nov 3 13:55:21" duration="104" site="V6.0 RELEASE" blade="VB330 SW v6.0" interface="IPTV" descr="QoE video" stream="test1" /><msg n="8" status="Major" activated="2020 Nov 3 13:55:21" duration="104" site="V6.0 RELEASE" blade="VB330 SW v6.0" interface="IPTV" descr="QoE video" stream="test2" /><msg n="9" status="Error" activated="2020 Oct 25 03:01:21" duration="816824" site="VB330" blade="Core" interface="IPTV" descr="IAT error" stream="Disney Channel (D)" /><msg n="10" status="Error" activated="2020 Oct 25 03:01:21" duration="816824" site="DASH QoS (VB220:OTT-VB2)" blade="OTT-VB220" interface="IPTV" descr="IAT error" stream="Disney Channel (D)" /><msg n="11" status="Error" activated="2020 Oct 25 03:01:21" duration="816824" site="VB330" blade="Core" interface="IPTV" descr="IAT error" stream="Disney Channel (N)" /><msg n="12" status="Error" activated="2020 Oct 25 03:01:21" duration="816824" site="DASH QoS (VB220:OTT-VB2)" blade="OTT-VB220" interface="IPTV" descr="IAT error" stream="Disney Channel (N)" /><msg n="13" status="Error" activated="2020 Nov 3 01:37:21" duration="44264" site="VB440 test" blade="VB440" interface="IPTV" descr="IAT error" stream="Matrox 2 Video@Primary" /><msg n="14" status="Error" activated="2020 Nov 3 01:37:21" duration="44264" site="V6.0 RELEASE" blade="VB440 v6.0" interface="IPTV" descr="IAT error" stream="Matrox 2 Video@Primary" /><msg n="15" status="Error" activated="2020 Nov 3 01:37:21" duration="44264" site="VB440 test" blade="VB440" interface="IPTV" descr="IAT error" stream="Matrox 2 Video@Secondary" /><msg n="16" status="Error" activated="2020 Nov 3 01:37:21" duration="44264" site="V6.0 RELEASE" blade="VB440 v6.0" interface="IPTV" descr="IAT error" stream="Matrox 2 Video@Secondary" /><msg n="17" status="Error" activated="2020 Nov 2 15:31:21" duration="80624" site="VB330" blade="Core" interface="IPTV" descr="IAT error" stream="NASA UHD 2022-7" /><msg n="18" status="Error" activated="2020 Nov 3 06:53:20" duration="25305" site="VB220-VB272" blade="VB272 DVB S-S2" interface="IPTV" descr="MLR error" stream="CNBC Europe" /></alarmlist>

In this example the two screenshots show the same alarms.

The XML alarm list provides integrators with an additional way of automating alarms export from the VBC – now integrators can choose between SNMP and XML alarm integrations.

The `release` attribute in the XML document is updated every time the VBC refreshes the alarm list and the `crc` attribute will only change when the alarm list changes.

Refer to **Alarm setup** for a description on how alarms are also available via the MIB and SNMP traps.

Please refer to the document **Eii External Integration Interface** for detailed information about Eii.

6.3.3 Monitoring — Site

The **Site** monitoring page provides information about the selected site. Each device is presented in a list with indication about the device type and IP address. The status of each blade is indicated by the color of a status bulb. For all non-green blade bulbs there should be corresponding entries in the alarm list.

The alarm list will only show alarms for the selected site.



Site status for VB330

Filter 

#	Status	Site	Name	Type	Model	IP address
1		VB330	Core	probe	VB330	10.0.205.104
2		VB330	VB330 - L2TPenc	probe	VB330	10.0.205.14
3		VB330	VB330-Redundant	probe	VB330	10.150.100.226

VBC alarms

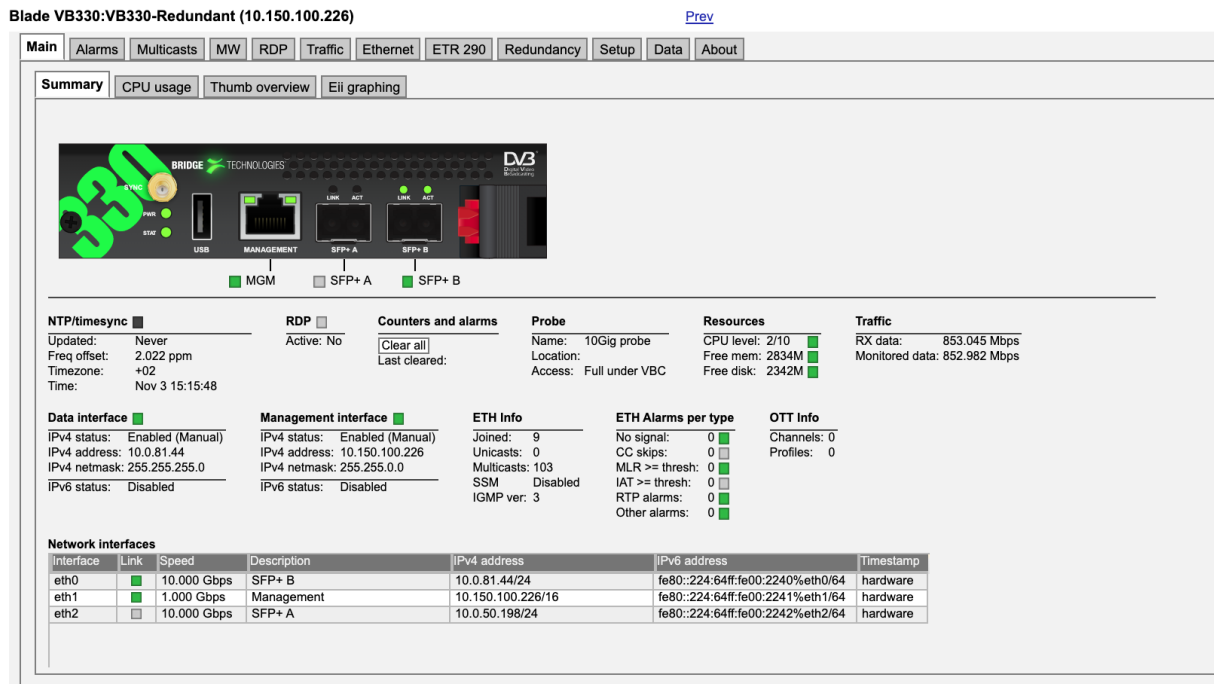
[Clear alarms](#) [Page 1](#) [Page -1](#) [Page +1](#) [Page +5](#)

#	▲	Sev	Status	Activated	Cleared	Dt	Site:Name	Interface	Description
1			Major	2020 Nov 2 15:28:20		22h	VB330:Core	IPTV	No signal NASA UHD backup
2			Major	2020 Nov 2 11:08:20		26h	VB330:Core	IPTV	No signal Test-Cuba
3			Error	2020 Oct 25 03:01:21		9d	VB330:Core	IPTV	IAT error Disney Channel (D)
4			Error	2020 Oct 25 03:01:21		9d	VB330:Core	IPTV	IAT error Disney Channel (N)
5			Error	2020 Nov 2 15:31:21		22h	VB330:Core	IPTV	IAT error NASA UHD 2022-7
6			Error	2020 Oct 25 03:01:21		9d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200__101
7			Error	2020 Oct 25 03:01:21		9d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200__101a
8			Error	2020 Oct 25 03:01:21		9d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200__101aa
9			Error	2020 Oct 25 03:01:21		9d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200__101ab
10			Error	2020 Oct 25 03:01:21		9d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200__101ac
11			Error	2020 Oct 25 03:01:21		9d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200__101ad
12			Error	2020 Oct 25 03:01:21		9d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200__101ae
13			Error	2020 Oct 25 03:01:21		9d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200__101af
14			Error	2020 Oct 25 03:01:21		9d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200__101ag
15			Error	2020 Oct 25 03:01:21		9d	VB330:VB330 - L2TPenc	IPTV	MLR error NC_ff3e_40_2a03_7400_200__101ah

Clicking one of the device name links opens up the **Blade** monitoring page through which the regular device graphical user interface is accessed.



6.3.4 Monitoring — Blade



The **Blade** monitoring page provides information about one blade. The top part of the page is the device's own web interface pages, similar to those that can be reached by accessing the device directly. The bottom part of the page contains the VBC alarm list for the selected blade.

If the blade cannot be reached from the VBC server, the top half of the page will be empty for approximately 30 seconds, after which an error message will be displayed. In this situation the blade's bulb status icon is usually black in the **Site** monitoring page, provided that the default 'No contact' alarm severity *Fatal* is used.

When accessing a probe through the VBC, the probe's built-in access control feature is disabled and the VBC decides if the user is going to have full access or simply read-only access.

Clicking one of the alarm entries will automatically select the corresponding page in the device.

If a Micro Device Controller (MDC) is part of the VBC configuration, the regular MDC user interface is accessed in a similar way as other blades, by clicking the site device link associated with the blade.

6.3.5 Monitoring — All sites

The **All sites** view is visible when using the Master VBC feature. Please refer to chapter 4 for details.



LOGIN	Now	Local site	Server	External site	Blades	Now	Loc
LIVE		secondaries	MASTERVBC	julesite	7		
MONITORING		secondaries	MASTERVBC	serversite	7		
SITE		secondaries	MASTERVBC	rfsite	16		
BLADE		secondaries	MASTERVBC	s1	1		
ALL SITES		secondaries	MASTERVBC	secondaries	2		
BLADE ALARMS		secondaries	MASTERVBC	Single_remote	1		
GRAPHICS VIEW		secondaries	vbc207	julesite	7		
STREAM VIEW		secondaries	vbc207	serversite	7		
THUMBS VIEW		secondaries	vbc207	rfsite	16		
SERVICE VIEW		secondaries	vbc207	s1	1		
MAP		secondaries	vbc207	secondaries	2		
RDP		secondaries	vbc207	Single_remote	1		
RDW		Single_remote	VBC215	julesite	7		
EQUIPMENT		Single_remote	VBC215	serversite	5		
ALARM SETUP		Single_remote	VBC215	rfsite	16		
REPORTS							
EXT. REPORTS							
MAIN							

SYSTEM IS RUNNING
LOW ON DISK FREE

Sort

Name ▼

Filter

[1-51](#) [52-102](#) [103-153](#) [154-204](#) [205-255](#) [256-306](#) [307-357](#) [358-408](#) [409-459](#) [460-510](#) [511-](#)

This view presents summary information for all the sites reported by Sub-VBCs registered in the **Equipment** view. The Sub-VBC is registered just like a regular blade and is given a name (shown as *Server*) and assigned to one of the Master VBCs sites (shown as *Local site*). The name of the Sub-VBC sites are reported in the *External site* column and the site's number of blades are found in the *Blades* column.

Clicking on the *External site* name will seamlessly present the Sub-VBC page inside the Master VBC.



LOGIN

LIVE

MONITORING

SITE

BLADE

ALL SITES

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

ALARM SETUP

REPORTS

EXT. REPORTS

MAIN

Blade Single_remote:VBC215 (10.0.28.215)

LOGIN

LIVE

MONITORING

SITE

BLADE

ALL SITES

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

Site status for serversite

#	Status	Site	Name	Type	Model	IP address
1		serversite	VB288_5_5	extractor	VB7880	10.0.30.144
2		serversite	VB288_Lab	extractor	VB7880	10.0.30.188
3		serversite	VB288_master	extractor	VB7880	10.0.31.146
4		serversite	swprobe181	probe	VProbe	10.0.31.181
5		serversite	swprobe182	probe	VProbe	10.0.31.182

VBC alarms

#	Sev	Status	Activated	Cleared	DI	Site Name	Interface	Description
1		Fatal	Feb 10 11:26:26		103m	serversite:swprobe182		No contact with blade
2		Major	Feb 10 11:25:50		104m	serversite:VB288_5_5	E-OTT	QoE audio Silent Both
3		Major	Feb 10 11:25:50		104m	serversite:VB288_master	E-OTT	QoE audio Silent Both
4		Major	Feb 10 11:25:50		104m	serversite:VB288_5_5	E-OTT	QoE video Silent Black
5		Major	Feb 10 11:25:50		104m	serversite:VB288_master	E-OTT	QoE video Silent Black
6		Major	Feb 10 11:25:50		104m	serversite:VB288_5_5	E-OTT	QoE video Silent Green
7		Major	Feb 10 11:25:50		104m	serversite:VB288_master	E-OTT	QoE video Silent Green
8		Major	Feb 10 11:26:30		22m	serversite:VB288_master	E-OTT	QoE video Silent Green

VBC alarms

#	Sev	Status	Activated	Cleared	DI	Site Name	Interface	Description
1		Major	Feb 10 11:25:48		103m	Single_remote:VBC215		External site alarm
2		Cleared	Feb 10 11:25:19	Feb 10 11:25:34	15s	Single_remote:VBC215		External site alarm
3		Cleared	Feb 8 13:10:49	Feb 10 11:25:19	46h	Single_remote:VBC215		No contact with blade
4		Cleared	Feb 8 12:50:01	Feb 8 13:08:19	18m	Single_remote:VBC215		No contact with blade
5		Cleared	Feb 8 09:30:16	Feb 8 12:50:01	3h	Single_remote:VBC215		External site alarm
6		Cleared	Feb 8 09:30:07	Feb 8 09:30:16	9s	Single_remote:VBC215		No contact with blade
7		Cleared	Feb 8 09:25:34	Feb 8 09:30:07	273s	Single_remote:VBC215		External site alarm
8		Cleared	Feb 8 09:23:35	Feb 8 09:25:27	112s	Single_remote:VBC215		External site alarm
9		Cleared	Feb 8 09:19:43	Feb 8 09:23:28	225s	Single_remote:VBC215		External site alarm
10		Cleared	Feb 8 09:14:01	Feb 8 09:19:36	335s	Single_remote:VBC215		External site alarm



6.4 Blade alarms

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

ROW

EQUIPMENT

REPORTS

EXT. REPORTS

MAIN

Select by location

Site: All

Blade: All

Select by alarm

☐ Show only Active alarms

VBC alarm: All

Select by stream info

Stream name: stream...

Service name: service...

PID: PID...

Select by time

From: dd/mm/yyyy --:--:--

To: 14/04/2023 10:13:28

Alarms active in interval are shown

Sev	Status	Time	Site	Blade	Interface	Stream	VBC alarm	Description
0	Event	Apr 14 10:13:07	SW-VB220	SW220	IPTV	Deluxe Music	MLR error	MLR >= error-threshold (35 >= 8)
0	Event	Apr 14 10:13:07	SW-VB220	SW220	IPTV	Deluxe Music	RTP drops	RTP Packet drops:5
0	Event	Apr 14 10:12:52	SW-VB220	SW220	IPTV	Deluxe Music	RTP drops	RTP Packet drops:1
0	Event	Apr 14 10:12:40	VB220-VB24...	ASI-Redund...	IPTV	Sonlife	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Cleared	Apr 14 10:12:39 - Apr 14 10:12:40	VB220-VB24...	ASI-Redund...	IPTV	Gospel Channel Europe	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:37	VB220-VB24...	ASI-Redund...	IPTV	Gospel Channel Europe	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:35	VB220-VB24...	ASI-Redund...	IPTV	Sonlife	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Cleared	Apr 14 10:12:34 - Apr 14 10:12:35	VB220-VB24...	ASI-Redund...	IPTV	Gospel Channel Europe	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:32	VB220-VB24...	ASI-Redund...	IPTV	Gospel Channel Europe	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:30	VB220-VB24...	ASI-Redund...	IPTV	Sonlife	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:29	VB220-VB24...	ASI-Redund...	IPTV	Gospel Channel Europe	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:27	VB220-VB24...	ASI-Redund...	IPTV	Gospel Channel Europe	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:25	VB220-VB24...	ASI-Redund...	IPTV	Sonlife	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:24	SW-VB220	SW220	IPTV	Deluxe Music	MLR error	MLR >= error-threshold (14 >= 8)
0	Event	Apr 14 10:12:24	SW-VB220	SW220	IPTV	Deluxe Music	RTP drops	RTP Packet drops:2
0	Cleared	Apr 14 10:12:24 - Apr 14 10:12:25	VB220-VB24...	ASI-Redund...	IPTV	Gospel Channel Europe	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:22	VB220-VB24...	ASI-Redund...	IPTV	Gospel Channel Europe	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:20	VB220-VB24...	ASI-Redund...	IPTV	Sonlife	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Cleared	Apr 14 10:12:19 - Apr 14 10:12:20	VB220-VB24...	ASI-Redund...	IPTV	Gospel Channel Europe	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:17	VB220-VB24...	ASI-Redund...	IPTV	Gospel Channel Europe	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:15	VB220-VB24...	ASI-Redund...	IPTV	Sonlife	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:14	VB220-VB24...	ASI-Redund...	IPTV	Gospel Channel Europe	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:12	VB220-VB24...	ASI-Redund...	IPTV	Gospel Channel Europe	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:10	VB220-VB24...	ASI-Redund...	IPTV	Sonlife	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:09	VB220-VB24...	ASI-Redund...	IPTV	Gospel Channel Europe	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:09	SW-VB220	SW220	IPTV	Deluxe Music	MLR error	MLR >= error-threshold (28 >= 8)
0	Event	Apr 14 10:12:09	SW-VB220	SW220	IPTV	Deluxe Music	RTP drops	RTP Packet drops:4
0	Event	Apr 14 10:12:07	VB220-VB24...	ASI-Redund...	IPTV	Gospel Channel Europe	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Cleared	Apr 14 10:12:07 - Apr 14 10:12:10	VB330	Appliance S...	OTT	VodTest2	OTT transport error	Video: avc1.640032 1920x1080...
0	Event	Apr 14 10:12:05	VB220-VB24...	ASI-Redund...	IPTV	Sonlife	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Cleared	Apr 14 10:12:04 - Apr 14 10:12:05	VB220-VB24...	ASI-Redund...	IPTV	Gospel Channel Europe	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:02	VB220-VB24...	ASI-Redund...	IPTV	Gospel Channel Europe	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:12:00	VB220-VB24...	ASI-Redund...	IPTV	Sonlife	Bitrate underflow	Bitrate underflow (0 < 0.1)
0	Event	Apr 14 10:11:59	VB220-VB24...	ASI-Redund...	IPTV	Gospel Channel Europe	Bitrate underflow	Bitrate underflow (0 < 0.1)

Gaps in database affecting current selection: 1000 Total records: 100000/100000 Note: Only alarms generated by devices are displayed in this list. Disabled device alarms are not available.

The **Blade alarms** view displays a list of active and cleared alarms present in devices' individual alarm lists. These alarms are not affected by VBC threshold settings, i.e. they reflect the current device alarm status, only limited by the one minute alarm poll rate. Note that only alarms that are enabled in devices will be present in the **Blade alarms** view.

Blade Alarms	
①	Click the blue information icon to view a detailed alarm description
Sev	A bulb indicating the alarm severity
Status	The alarm status: <i>Active</i> , <i>Cleared</i> or <i>Event</i>
Time	The time the alarm was raised by the device. For cleared alarms the time span of the alarm is shown, i.e. the time the alarm was raised and the time it was cleared.
Site	The site(s) where this the device that raised the alarm is located
Blade	The name(s) of the device that raised the alarm. Can be multiple names if the same device is added to multiple sites
Interface	The interface receiving the stream causing the alarm
Stream	The name of the stream having the alarm
VBC alarm	The VBC alarm name
Description	The device alarm description

By default all blade alarms from sites the user has access to are displayed in the Blade Alarms list. However a number of filtering options makes it easy to search the list for specific alarms:



<i>Blade Alarms Filtering</i>	
Site	Select a site from the drop-down menu to view alarms originating from the selected site only.
Blade	Select a device from the drop-down menu to view alarms originating from the selected device only. Please note that you need to select the site before selecting the blade.
Show only active alarms	Check this box to view active alarms only. Events and cleared alarms are not displayed.
VBC alarm:	Select a VBC alarm name from the drop-down menu to view that alarm type only.
Stream name	Type a text string + <Enter> to only view alarm list entries matching the specified stream name. The search is case insensitive and matching starts from the beginning of the string.
Service name	Type a text string + <Enter> to only view alarm list entries matching the specified service names. The search is case insensitive and matching starts from the beginning of the string. Only applicable for streams that carry service names. It is common not to transmit this information Single Program Transport Streams (SPTS) which often used in IPTV systems. Service names are transmitted in tables in the transport streams such as Service Description Table (SDT) for DVB systems or Virtual Channel Tables (VCT) for ATSC systems.
PID	Type a PID number + <Enter> to view alarm list entries with matching PID number only. Note that this is only relevant for ETR alarms that are associated with a specific PID.
From	Select a date and time from the drop-down (if supported, otherwise type it manually on the form YYYY-MM-DDTHH:MM:SS) to specify a time window defined by the From and End time . Make sure you define both date and a time for the value to be used. All alarms that were active during this time window will be displayed. Define From only to view all blade alarms raised after the specified time plus alarms that were active at the specified time.
To	Select a date and time from the drop-down (if supported, otherwise type it manually on the form YYYY-MM-DDTHH:MM:SS) to specify a time window defined by the From and To . Make sure you define both date and a time for the value to be used. All alarms that were active during this time window will be displayed. Define To only to view all blade alarms that were active before the specified time.

Click on a element in the blade alarm list to seem more detailed information about that specific alarm.



Details for blade alarm

Profile_1 [1280x720 - H264] Transport error: Download duration 127% >= 100% chunk dur. (40.70.71.156)

Status: Cleared
Severity: Error
Alarm type: OTT
VBC alarm name: OTT transport error
Blade IP: 10.0.205.104
Site(s): VB330
Blade name(s): Core
Interface: OTT
Stream: SS Internet Example
Service name: 1280x720 - H264
PID:
Raise time: Nov 4 13:11:49
Raise description: Profile_1 [1280x720 - H264] Transport error: Download duration 127% >= 100% chunk dur. (40.70.71.156)
Raise sequence no: 528643
Raise trap: aty=OTT|stn=SS Internet Example|aid=2501|sid=1|sna=1280x720 - H264|Profile_1 [1280x720 - H264] Transport error: Download duration 127% >= 100% chunk dur. (40.70.71.156)
Clear time: Nov 4 13:12:18
Clear description: Profile_1 [1280x720 - H264] Transport error: Download duration 127% >= 100% chunk dur. (40.70.71.156)
Clear sequence no: 528645
Clear trap: aty=OTT|stn=SS Internet Example|aid=2501|sid=1|sna=1280x720 - H264|Profile_1 [1280x720 - H264] Transport error: Download duration 127% >= 100% chunk dur. (40.70.71.156)

Blade Alarm Details

Status	The alarm status: <i>Active</i> , <i>Cleared</i> or <i>Event</i>
Severity	The alarm severity as configured in the Alarm setup page on the device
Alarm Type	The type of alarm such as ETH, ETR, OTT or SYS
VBC alarm name	The name corresponding to this alarm in the VBC. As an example, the ETR alarm Continuity counter error corresponds to the VBC alarm ETR pri one error
Blade IP	The IP address of the device which have reported this alarm
Site(s)	The sites where this device have been registered. Normally a device is registered to one site but in some situations it can also be useful to add it to multiple sites
Blade name(s)	The name the device have been assigned in the Equipment view. If the same device is registered to multiple sites then all the different names the device have been assigned is shown here
Interface	The interface receiving the stream causing the alarm
Stream	The name of the stream having the alarm
Service name	The name of the service affected by the alarm. Only applicable for ETR alarms and only when the stream contain service name information
PID	The Packet ID of the PID affected by the alarm. Only applicable for ETR alarms
Raise time	The time the alarm was raised by the device
Raise description	The description of the alarm when it was raised
Raise sequence no	The sequence number of the alarm message as sent by the device when it was raised
Raise trap	The trap alarm text sent by the device when raising the alarm. The format of this text field is described in the document SNMP trap format
Clear time	The time the alarm was cleared by the device
Clear description	The description of the alarm when it was cleared. For some alarms this may be different from the raise description (updating the number of detected MLR errors etc.)



Clear sequence no	The sequence number of the alarm message as sent by the device to clear the alarm
Clear trap	The trap alarm text sent by the device when clearing the alarm. The format of this text field is described in the document SNMP trap format

The status bar at the bottom of the alarm list shows information about the number of records in the database and the number of records in the current filter.

In some cases the VBC might be missing possible blade alarms. Click on the ⓘ icon to bring up detailed information about the reasons for the missing blade alarms.

Alarm fetching issues			
Time	Issue	Blade IPA	Lost blade alarms
2023 Apr 13 13:39:21	Blade restart has caused gaps in alarms from blade	10.0.205.9	n/a
2023 Apr 10 02:55:23	Blade restart has caused gaps in alarms from blade	10.150.0.176	n/a
2023 Apr 9 16:25:17	Blade restart has caused gaps in alarms from blade	10.150.0.176	n/a
2023 Apr 4 10:05:02	Blade restart has caused gaps in alarms from blade	10.0.205.9	n/a
2023 Apr 3 21:49:27	Blade restart has caused gaps in alarms from blade	10.150.0.176	n/a
2023 Apr 3 14:01:47	Blade restart has caused gaps in alarms from blade	10.150.0.167	n/a
2023 Apr 3 13:51:07	Blade restart has caused gaps in alarms from blade	10.150.0.167	n/a
2023 Apr 3 13:30:54	Blade restart has caused gaps in alarms from blade	10.0.205.228	n/a
2023 Apr 3 13:29:25	Blade restart has caused gaps in alarms from blade	10.0.205.120	n/a
2023 Apr 3 13:23:11	Blade restart has caused gaps in alarms from blade	10.0.205.200	n/a
2023 Apr 3 13:17:38	Blade restart has caused gaps in alarms from blade	10.0.205.41	n/a
2023 Apr 3 12:52:37	Blade restart has caused gaps in alarms from blade	10.0.205.193	n/a
2023 Apr 3 12:51:05	Blade restart has caused gaps in alarms from blade	10.0.205.216	n/a



6.5 Graphics view (Graphics option)

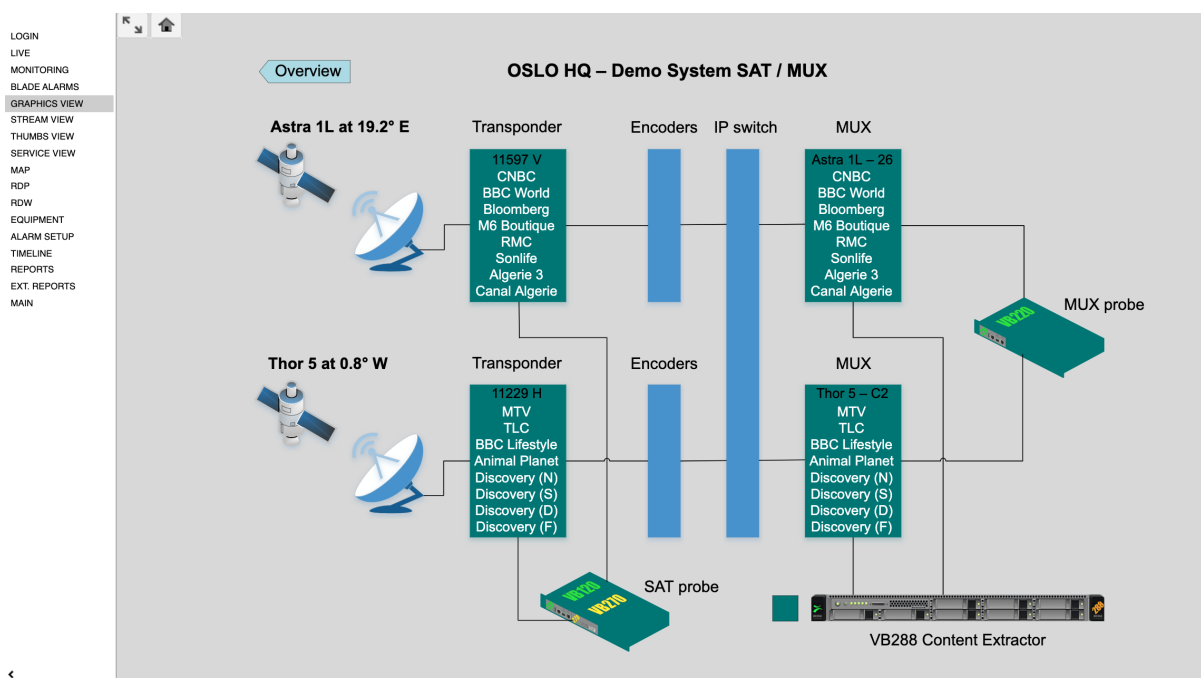


Figure: Simulation of a network monitored by Bridge Technologies equipment.

Graphics view will display diagrams, where the diagram objects are used to show the current alarm status of the VBC elements: Site, Blade, Stream or Stream group.

The operator designs diagrams and generate the diagram files in the Scalable Vector Graphics (.svg) format, which is an open standard and is supported by all modern browsers. Graphics View currently support importing of .svg files generated by Microsoft Visio® and Inkscape.

When generating diagram files the objects can be hyperlinked to a VBC blade view, VBC selected stream view, or to other uploaded diagram files. To navigate to these diagram click the relevant areas of the diagram. This allows for instance to have a system overview diagram where you can see the different sites and then click in to see details for the headend or the different regional sites, overview of the channel status, list of transponders on the satellite etc.

In the example diagram above the box background colors are displaying the aggregated status of the stream group, the stream arrow colors are showing status of the individual streams, and the probes are showing the corresponding status color of the probe (Blade) in the VBC.

Use the following buttons to navigate the diagrams:



Click to view the diagram full screen, filling the entire browser window. You can additionally use the browser menus to make the graphics view fill the entire computer screen.



Click to return to the normal VBC GUI when in full screen mode



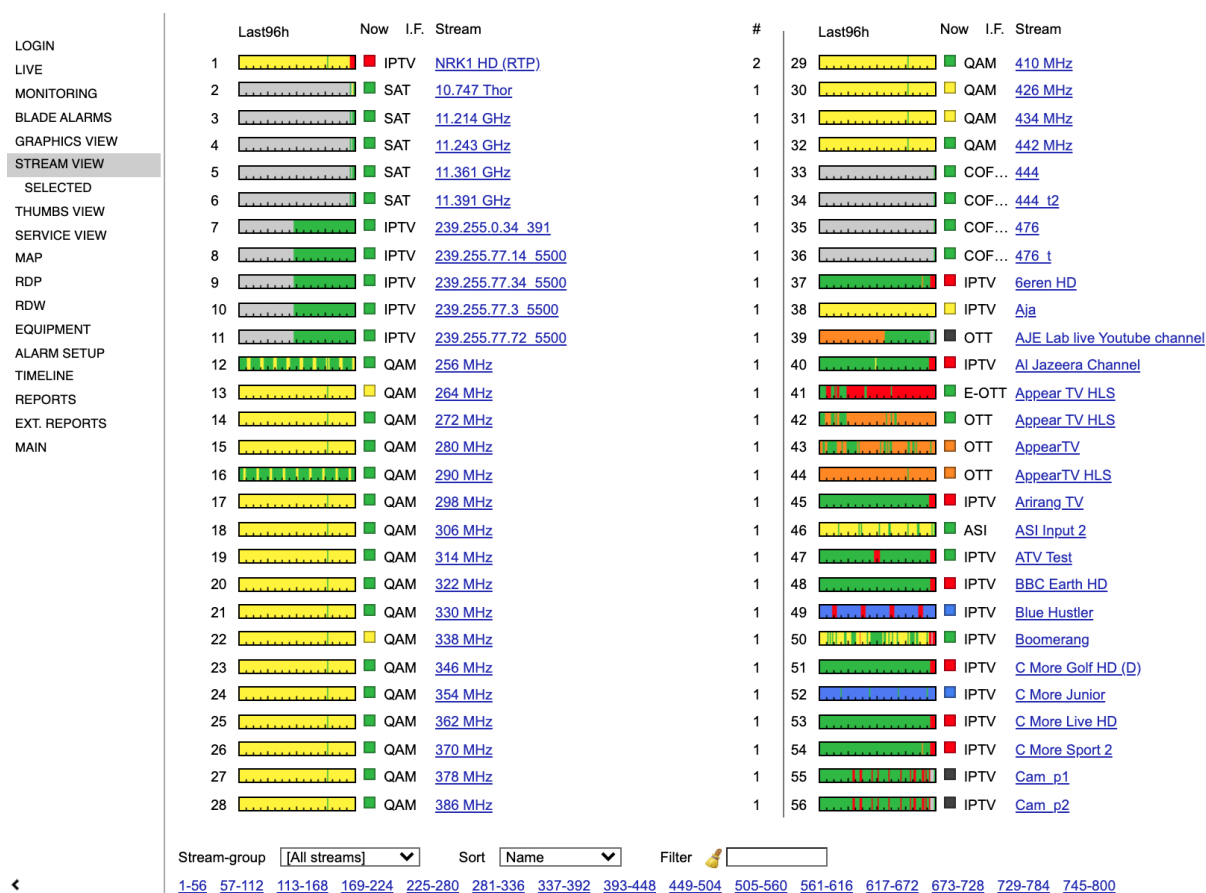
Click to go to the starting diagram (configured in the **Main — Gfx. View Setup** view). This is useful when you have multiple diagrams with hyperlinks for navigation.



Please refer to chapter 6.24 for details on how to configure the Graphics view.



6.6 Stream view



In the **Stream view** streams are by default presented in alphabetical order. For each stream the bulb shows the current status, and the 96-pixel MicroTimeline stream-bar shows the status for the last 96 hours (i.e. 4 days).

Each bulb-color corresponds to the aggregate status for all probes that belong to sites that the user has access to. The bulbs are updated every 60 seconds – which corresponds to the probe poll interval.

The stream bars reveal any VBC alarm that has been present during the last 4 days. The bars will automatically scroll one pixel to the left each hour with the rightmost pixels showing the status for the current hour. The bar color corresponds to the severity of alarms that have occurred. During periods when VBC alarms are masked due to VBC schedule settings, the bar color is blue. Note that this applies to VBC scheduling only, and not to probe or extractor scheduling. If scheduling applies part time of a one hour MicroTimeline period, it will be colored blue if there have been no alarms during the non-scheduled part of the period. Otherwise it will be colored according to alarm severity. Alarm severity is configured in the **Alarm setup** page.

The user selects whether all streams or only one stream group should be represented in the view. The selectable stream groups are available in the *Stream-group* drop-down menu. The stream groups are configured in the **Main — Stream groups** page.

The *Sort* drop-down menu allows stream sorting based on name, interface or current stream status severity.

The *Filter* field allows the user to specify a text string; only streams and sites with names matching the specified string will be displayed. If an extractor is part of the system, the VBC will also check against multicast addresses. This functionality is very useful to quickly locate a specific stream in a large system.



The number of streams presented on a page is only limited by the size of the display screen. Refreshing the screen after resizing the browser window will automatically fill up all of the available screen area. If there are more streams in the selected stream group than can be displayed in a single view the remaining streams may be monitored by clicking the numbered links at the bottom of the page.

Clicking a stream name brings up the **Selected** stream view.

6.6.1 Stream names, class and interface

Matrox 2 Video		Prev: Matrox 2 Audio		Next: Matrox 4 Ang		IPTV(Error-second) ▾					
#	Last 96h	Now	Interface	Probe	Class	NoSig	RTP	MLR	IAT	Overfl	Underfl
☐	1		IPTV	VB440 test:VB440	Primary	0	0	0	24h	24h	0
☐	2		IPTV	VB440 test:VB440	Secondary	0	23h	0	24h	24h	0

The stream name specified for Ethernet streams, OTT service and RF tuning setups are presented in the Stream View in VBC. Since by definition all stream names need to be unique on a single device we have added an optional class part to the stream name. This allows the same stream to be monitored several times on the same device and still have all instances reported separately to the VBC. For example, by naming three streams “BBC”, “BBC@main” and “BBC@backup”, all three streams will be treated as if the name was BBC alone. The class part is displayed in the **Stream view — Selected** list.

In addition to the class, the interface on which the stream was received is listed here. Streams received over RF or ASI are listed under their interface name. Multicasts are listed as *IPTV* when received on probes and as *E-IPTV* when received on extractors. OTT streams are listed as *OTT* when received on probes, or on extractors where OTT Active Testing has been enabled for the stream, and as *E-OTT* for the extractor QoE measurements.



6.6.2 Stream view — Selected

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

SELECTED

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

ALARM SETUP

TIMELINE

REPORTS

EXT. REPORTS

MAIN

Nat Geo HD (N)

Prev:[NRK 2](#)

Next:[Nat Geo Wild HD](#)

IPTV(Error-second) ▼



Bitrate: **10.67M**

Video: **10.34M clear**

Audio: **0.26M clear**

Teletext: n/a

Encoding: **yuv420p**

Size: **1920x1080**

Aspect: **16:9**

Service name: **Nat Geo HD (N)**

Stream: **Nat Geo HD (N)**

Address: **239.255.0.8:5500**

Extractor: [VB288](#)



Bitrate: **9.52M**

Video: **9.19M clear**

Audio: **0.26M clear**

Teletext: n/a

Encoding: **yuv420p**

Size: **1920x1080**

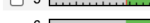
Aspect: **16:9**

Service name: **Nat Geo HD (N)**

Stream: **Nat Geo HD (N)**

Address: **239.255.0.8:5500**

Probe: [VB330 SW v6.0](#)

#	Last 96h	Now	Interface	Probe	NoSig	RTP	MLR	IAT	Overfl	Underfl
☐	1		IPTV	DASH QoS (VB220:OTT-VB220)	0	0	0	0	0	0
☐	2		IPTV	VB220-VB272:VB272 DVB S-S2	0	0	0	0	0	ETR
☐	3		IPTV	VB330:Core	19h	0	0	0	0	5s ETR
☐	4		IPTV	V6.0 RELEASE:VB330 SW v6.0	0	0	0	0	0	0 ETR
☐	5		IPTV	HLS QoS (VB120):VB120	0	0	0	0	0	0
☐	6		E-IPTV	VB288:VB288						

4 days 24 hours 60 minutes

[Compare MediaWindows](#)

[Compare streamdata](#)

[Compare ETR measurements](#)

VBC alarms for all sites

[Clear alarms](#) [First page](#) [Prev page](#) [Next page](#) [+5 page](#)

#	Sev	Status	Activated	Cleared	Dt	Site Name	Interface	Description
1	Warning	2020 Nov 5 17:27:20			12m	VB220-VB272:VB272 DVB...	IPTV	ETR pri one error Nat Geo HD (N)
2	Cleared	2020 Nov 5 17:24:21	2020 Nov 5 17:26:21	120s		VB220-VB272:VB272 DVB...	IPTV	ETR pri one error Nat Geo HD (N)
3	Cleared	2020 Nov 5 17:18:21	2020 Nov 5 17:23:20	299s		VB220-VB272:VB272 DVB...	IPTV	ETR pri one error Nat Geo HD (N)
4	Cleared	2020 Nov 5 17:04:20	2020 Nov 5 17:12:20	480s		VB220-VB272:VB272 DVB...	IPTV	ETR pri one error Nat Geo HD (N)
5	Cleared	2020 Nov 5 16:53:20	2020 Nov 5 17:02:20	540s		VB220-VB272:VB272 DVB...	IPTV	ETR pri one error Nat Geo HD (N)
6	Cleared	2020 Nov 5 16:48:21	2020 Nov 5 16:52:21	240s		VB220-VB272:VB272 DVB...	IPTV	ETR pri one error Nat Geo HD (N)
7	Cleared	2020 Nov 5 16:45:20	2020 Nov 5 16:47:20	120s		VB220-VB272:VB272 DVB...	IPTV	ETR pri one error Nat Geo HD (N)
8	Cleared	2020 Nov 5 16:39:20	2020 Nov 5 16:44:21	301s		VB220-VB272:VB272 DVB...	IPTV	ETR pri one error Nat Geo HD (N)
9	Cleared	2020 Nov 5 16:37:21	2020 Nov 5 16:38:21	60s		VB220-VB272:VB272 DVB...	IPTV	ETR pri one error Nat Geo HD (N)
10	Cleared	2020 Nov 5 16:20:20	2020 Nov 5 16:35:20	15m		VB220-VB272:VB272 DVB...	IPTV	ETR pri one error Nat Geo HD (N)
11	Cleared	2020 Nov 5 16:11:21	2020 Nov 5 16:19:21	480s		VB220-VB272:VB272 DVB...	IPTV	ETR pri one error Nat Geo HD (N)
12	Cleared	2020 Nov 5 16:03:21	2020 Nov 5 16:10:20	419s		VB220-VB272:VB272 DVB...	IPTV	ETR pri one error Nat Geo HD (N)
13	Cleared	2020 Nov 5 15:57:21	2020 Nov 5 16:02:20	299s		VB220-VB272:VB272 DVB...	IPTV	ETR pri one error Nat Geo HD (N)
14	Cleared	2020 Nov 5 15:44:21	2020 Nov 5 15:56:20	12m		VB220-VB272:VB272 DVB...	IPTV	ETR pri one error Nat Geo HD (N)
15	Cleared	2020 Nov 5 15:22:21	2020 Nov 5 15:43:20	21m		VB220-VB272:VB272 DVB...	IPTV	ETR pri one error Nat Geo HD (N)

The **Selected stream** view lists measurements for all probes that are monitoring the selected stream. For each blade monitoring the stream, a 96-pixel MicroTimeline bar is displayed, showing the status for the last 96 hours (i.e. 4 days) for the stream on that blade, along with the selected error-second values, as described below. If one or more VB288 Objective QoE Content Extractors, or probes with the Content Extraction and Alarming option, are part of the VBC configuration and is monitoring the stream, a thumbnail picture and associated meta-data are displayed at the top of the page.

By selecting between two and ten probes (clicking the check box at the beginning of each line) and then clicking **Compare Media Windows for selected probes** the graphs for the probes are displayed in the **Selected stream compare MediaWindow** view. Note that this is only relevant for streams present on probe IPTV interfaces.

By selecting between one and five probes (clicking the check box at the beginning of each line) and then clicking **Compare Streamdata for selected probes**, the graphs for the probes are displayed in the **Selected stream compare Streamdata** view. This comparison can be done for IPTV, OTT and RF streams. The data shown depends on the stream type.

By selecting between one and five probes (clicking the check box at the beginning of each line) and then clicking **Compare ETR measurements for selected probes** selected ETR measurements for the probes are displayed in the **Selected stream compare ETR** view. Note that this is only relevant for streams that are ETR analyzed. ETR analyzed streams will have an additional link **ETR** in the rightmost column that when clicked will open up the probe's ETR page for the selected stream.

It is possible to jump between the streams by clicking the **Prev** and **Next** links at the top of the page. The



bulb displayed for each probe shows the probe's status for the selected stream. Clicking the probe name opens the probe's **Stream overview** page for the selected stream in the **Monitoring — Blade** view.

Thumbnail meta-data

<i>Parameter</i>	<i>Description</i>
Bitrate:	The total stream rate
Video:	The video bitrate and whether the component is scrambled or not
Audio:	The audio bitrate and whether the component is scrambled or not
Teletext:	The teletext bitrate and whether the component is scrambled or not
Encoding:	The video encoding format
Size:	The video picture size (video resolution)
Aspect:	The video aspect ratio
Service name:	The name of the service in the stream
Address:	The multicast IP address of the stream
Probe / Extractor:	The name of the blade delivering thumbnail and metadata; can be clicked

Each minute the VBC polls probes for information which is displayed in four categories selectable in the drop-down list in the top right hand corner.

IPTV(Error-second)

Selecting **IPTV(Error-second)** displays all IPTV error second parameters measured by the probe during the selected period¹ (last 4 days, 24 hours or 60 minutes). VBC alarms are based on the error second parameters, and the severity of the corresponding alarm is indicated by the colored bulb by the parameter name.

<i>Parameter</i>	<i>Description</i>
NoSig:	Number of seconds with no signal
RTP:	Number of seconds with RTP packet drops. This will always be zero if the stream is not encapsulated in RTP headers
MLR:	Number of seconds with packet drops in the TS layer (seconds when media loss rate is non-zero). This is equal to the number of error seconds with CC errors
IAT:	Number of seconds when the delay factor exceeds the threshold
Overfl:	Number of seconds when the bitrate exceeds the error-threshold
Underfl:	Number of seconds when the bitrate falls below the error-threshold

IPTV(Statistical)

Selecting **IPTV(Statistical)** shows all aggregate IPTV measurements that are not error-seconds measured by the probe during the selected period (last 4 days, 24 hours or 60 minutes).

¹Note that the MicroTimeline bar is not scaled, it always represents 96 hours.



<i>Parameter</i>	<i>Description</i>
OK-polls:	Number of times that the probe has been successfully polled
Failed-polls:	Number of times that VBC has failed to poll the probe. Each time VBC fails to poll a probe the No contact alarm is raised for one minute
Sum-MLR:	Number of TS packets lost in the MPEG2 transport stream. This is not the same as the number of CC errors (which would be the number of detected packet losses and not the packet count)
Sum-RTPdrop:	Number of RTP packets dropped

IPTV(Last minute)

Selecting **IPTV(Last minute)** shows parameters that are updated for each poll (i.e. each minute).

<i>Parameter</i>	<i>Description</i>
Signal:	For how long the probe has been receiving a signal for this stream. This is the same as the time since the last no-signal error second
Max-IAT:	The peak delay factor during the last minute. This is the same as the peak IAT during the last minute and is a measure of how much jitter is present in the signal
Max-bitr:	Peak bitrate during the last minute
Min-bitr:	Lowest bitrate during the last minute

ETR(Derived error-seconds)

Selecting **ETR(Derived error-seconds)** displays all ETR derived error second (DES, see description in next section) parameters measured by the probe during the selected period (last 4 days, 24 hours or 60 minutes). VBC alarms are based on the error second parameters, and the severity of the corresponding alarm is indicated by the colored bulb by the parameter name.

<i>Parameter</i>	<i>Description</i>
EtrPri1:	Number of seconds with ETSI TR 101 290 priority 1 errors
EtrPri2:	Number of seconds with ETSI TR 101 290 priority 2 errors
EtrPri3:	Number of seconds with ETSI TR 101 290 priority 3 errors
EtrOther:	Number of seconds with ETR 290 other errors
EtrIface:	Number of seconds with ETR 290 interface errors
Measured:	Displays for how long the stream has been ETR 290 measured by the probe, shown as a percentage of the selected measurement period

ES versus DES

For IPTV (Ethernet) streams that are continuously monitored the parameters are specified as ES(param) meaning the parameter reflects error-seconds directly. The ETR parameters are generally monitored round-robin, so to convert these measurements to error seconds per hour (or other time periods) they have to be extrapolated. For example, clicking the “60 minutes” for the ETR parameters will extrapolate all ETR measurements during the last 60 minutes so that they are comparable. As an example, if a stream is ETR monitored for only 3 minutes during the last 60 minutes, the number of error seconds measured



during this 3 minutes period is multiplied by 20 and the Measured % parameter will show 5 (since 5 % of 60 minutes equals 3 minutes).

OTT(Error-seconds)

For OTT streams, selecting **OTT(Error-seconds)** in the drop-down menu gives the following parameters:

<i>Parameter</i>	<i>Description</i>
OttTransport:	Number of seconds with OTT transport errors
OttHttp:	Number of seconds with OTT HTTP errors
OttXml:	Number of seconds with OTT XML errors

The OTT error second counters listed above have corresponding VBC alarms.

Probes and Extractors with the OTT Active Testing license detect a large number of OTT errors and maps each into one of these general categories. This mapping can be seen by navigating to a probe's **OTT** view and clicking the **Alarms** tab in the pop-up window.

QOE/CAP(Error-seconds)

If content monitoring is enabled, selecting **QOE/CAP(Error-seconds)** will show QoE and caption related parameters:

<i>Parameter</i>	<i>Description</i>
CapAvail:	Number of seconds with captions availability alarms
CapQual:	Number of seconds with captions quality alarms
QoeVideo:	Number of seconds with QoE video-related alarms, such as freeze-frame and MOS below average
QoeAudio:	Number of seconds with QoE audio-related alarms, such as audio silence or out of phase
SCTE35:	Number of seconds with SCTE 35-related alarms, such as SCTE35 event gap or too few SCTE35 placement opportunities
EBPIDR:	Number of seconds with EBP/IDR-related alarms, such as EBP PTS gap outside of threshold or EBP and IDR PTS unaligned

Probes with the Content Extraction and Alarming options, as well as Extractors, detect several QoE errors and map them into these general categories.

AGG(Aggregated per probe)

From version 6.3, probes will report the special aggregate channel “probe_aggregate_stats” on behalf of all the IPTV and OTT channels. This allows the VBC to compare the aggregate performance of two probes on a higher level. This is particularly useful if the probes are configured as main and backup. The total number of error-seconds for key metrics are reported across all streams for IPTV and OTT, in addition to the max and min net bitrates aggregated for all IPTV streams last minute.

No alarming is done for the aggregate channel.



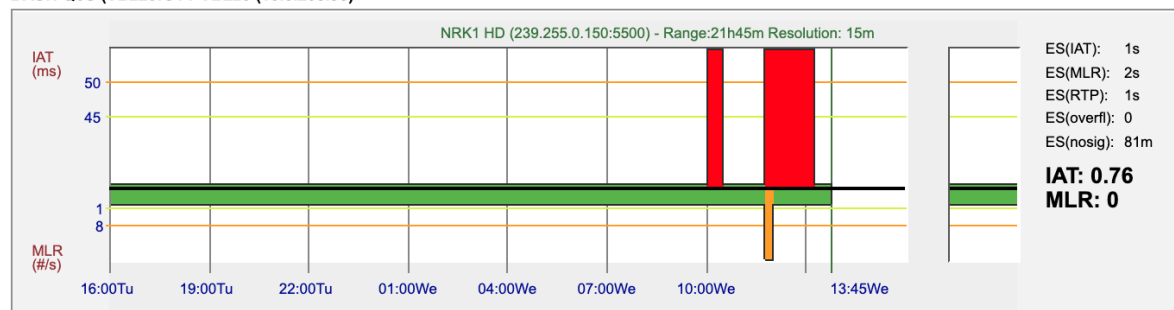
The AGG view is tailored to present the metrics reported for the “probe_aggregate_stats” streams. When plotting them (clicking **Compare streamdata**), a logarithmic scale is used in order to visualize totally different data types such as bit-rates and counters.

The following information is displayed:

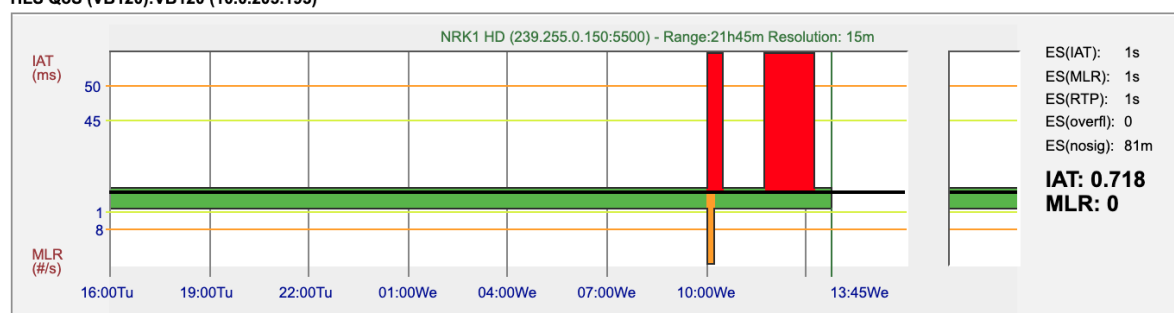
<i>Parameter</i>	<i>Description</i>
NoSig	Number of seconds with no signal, summed across all streams.
RTP	Number of seconds with RTP packet drops, summed across all streams.
MLR	Number of seconds with packet drops in the TS layer (seconds when media loss rate is non-zero), summed across all streams.
OttTransport:	Number of seconds with OTT transport errors, summed across all streams.
OttHttp:	Number of seconds with OTT HTTP errors, summed across all streams.
OttXml:	Number of seconds with OTT XML errors, summed across all streams.
Max-bitr:	Peak bitrate for all streams during the last minute, summed. Please note that this summed peak bitrate will not have occurred unless all the streams peaked at the same time, but it can give a good idea of what could be the edge case.
Min-bitr:	Lowest bitrate for all streams during the last minute, summed. Similar constraints apply as for Max-bitr above.

6.6.3 Selected Stream Compare MediaWindow

DASH QoS (VB220:OTT-VB220 (10.0.205.93))



HLS QoS (VB120):VB120 (10.0.205.193)



IAT:MLR BW:MLR IAT:RTP |< << >> >| 4 days 24 hours 8 hours 90 min running

Up to 10 probes can be compared in the **Selected stream compare MediaWindow** view. The high resolution version is used when only two probes are selected.



From the MediaWindow graph it is possible to compare packet jitter and CC errors in the streams. By comparing graphs it is possible to locate where packet jitter is introduced and where packet loss occurs. Refer to the probe manuals for more information about MediaWindow measurements.

The range of the graph can be set to a maximum of 4 days. For smaller ranges the scroll buttons may be used. It is also possible to view the bitrate graph by clicking the **BW:MLR** button. When the **IAT:RTP** button is clicked the graphs show packet jitter versus RTP packet loss. For SRT streams, clicking the **RTT:SRT** button shows SRT round-trip time and unrecoverable packet loss.

It is the probes that draw the MediaWindow graphs inside frames created by the VBC. If the probes are not time synchronized (using NTP) the graphs may appear unaligned and the time labels may be wrong. Refer to N Appendix: Enabling NTP time synchronization for more details.



6.6.4 Selected Stream Compare ETR

Overview (rfsite:41probe / QAM1 / 306 MHz (306.00 MHz, 256 QAM) ^

Stream overview

TS ID: 105
NW ID: 42499
Orig NW ID: 42499
Min. eff. bitr: 44.56 Mbps
Max. eff. bitr: 44.68 Mbps
Min. tot. bitr: 50.88 Mbps
Max. tot. bitr: 50.89 Mbps
Last update: 5 m, 31 s

Error statistics

Total monitoring time: 20 h, 34 m
ETR Priority 1: 1 m, 30 s
ETR Priority 2: 5 s
ETR Priority 3: 14 h, 46 m
No Signal: 54 s
CC Errors: 23 s
Interface errors: 15 m, 59 s
Other checks: No errors

Service alarms (rfsite:41probe / QAM1 / 306 MHz (306.00 MHz, 256 QAM) ^

Service/Alarm	Pid
1005 BBC Earth	

Services (rfsite:41probe / QAM1 / 306 MHz (306.00 MHz, 256 QAM) / ^

Service/Pid	Min bitrate	Max bitrate	CC	Max PCR
1005 BBC Earth	6.481 Mbps	12.287 M...	0	
3296 PMT	13.800 k...	16.296 k...	0	
3297 MPEG4 Video	6.192 Mbps	11.800 M...	0	74 ns
3298 MPEG1 Audio	267.712 ...	275.376 ...	0	
3299 Subtitling	2.960 kbps	61.440 k...	0	
3300 Subtitling	2.960 kbps	66.360 k...	0	
3301 Subtitling	1.504 kbps	67.432 k...	0	
3302 ECM	13.496 k...	16.568 k...	0	

Alarm graph (rfsite:41probe / QAM1 / 306 MHz (306.00 MHz, 256 QAM) ^

Check	Timeline
Alarm status	15:00Tu 21:00Tu 03:00We 09:00We

Show all Show errors < << >> > 24h 8h 90m

ETR Details (rfsite:41probe / QAM1 / 306 MHz (306.00 MHz, 256 QAM) v

Pri 1	Pri 2	Pri 3	Other	Interface
TS sync	Transport	NIT	CA syst.	Pre FEC BER
Sync byte	CRC	SI Rep	PID minbr.	Post FEC BER
PAT	PCR	Unref PID	PID maxbr.	MER
Continuity	PCR accr.	SDT	PID ch.	SNR
PMT	PTS	EIT	Serv. minbr.	Sig. str.
Miss.PID	CAT	RST	Serv. maxbr.	Center frequency
		TDT	Serv. ch.	Symbol rate
			MIP	T2MI
			Cont. ch.	Intf. ovfl.
			Gold TS	
			Time	

Overview (rfsite:41probe / QAM2 / GET TS-105 (306.00 MHz, 256 QAM) ^

Stream overview

TS ID: 105
NW ID: 42499
Orig NW ID: 42499
Min. eff. bitr: 42.22 Mbps
Max. eff. bitr: 44.94 Mbps
Min. tot. bitr: 50.86 Mbps
Max. tot. bitr: 50.91 Mbps
Last update: 47 s

Error statistics

Total monitoring time: 16 d, 4 h
ETR Priority 1: 5 h, 35 m
ETR Priority 2: 8 m, 52 s
ETR Priority 3: 15 d, 23 h
No Signal: 5 h, 14 m
CC Errors: 11 m, 50 s
Interface errors: 6 h, 28 m
Other checks: 18 m, 46 s

Service alarms (rfsite:41probe / QAM2 / GET TS-105 (306.00 MHz, 256 QAM) ^

Service/Alarm	Pid
1005 BBC Earth	

Services (rfsite:41probe / QAM2 / GET TS-105 (306.00 MHz, 256 QAM) / ^

Service/Pid	Min bitrate	Max bitrate	CC	Max PCR
1005 BBC Earth	863.448 ...	12.353 M...	7	
3296 PMT	13.536 k...	16.552 k...	0	
3297 MPEG4 Video	582.576 ...	11.808 M...	3	98 ns
3298 MPEG1 Audio	262.920 ...	278.400 ...	1	
3299 Subtitling	1.472 kbps	83.688 k...	0	
3300 Subtitling	1.472 kbps	83.456 k...	0	
3301 Subtitling	1.472 kbps	83.184 k...	0	
3302 ECM	13.368 k...	16.744 k...	0	

Alarm graph (rfsite:41probe / QAM2 / GET TS-105 (306.00 MHz, 256 QAM) ^

Check	Timeline
Alarm status	15:00Tu 21:00Tu 03:00We 09:00We

Show all Show errors < << >> > 24h 8h 90m

ETR Details (rfsite:41probe / QAM2 / GET TS-105 (306.00 MHz, 256 QAM) v

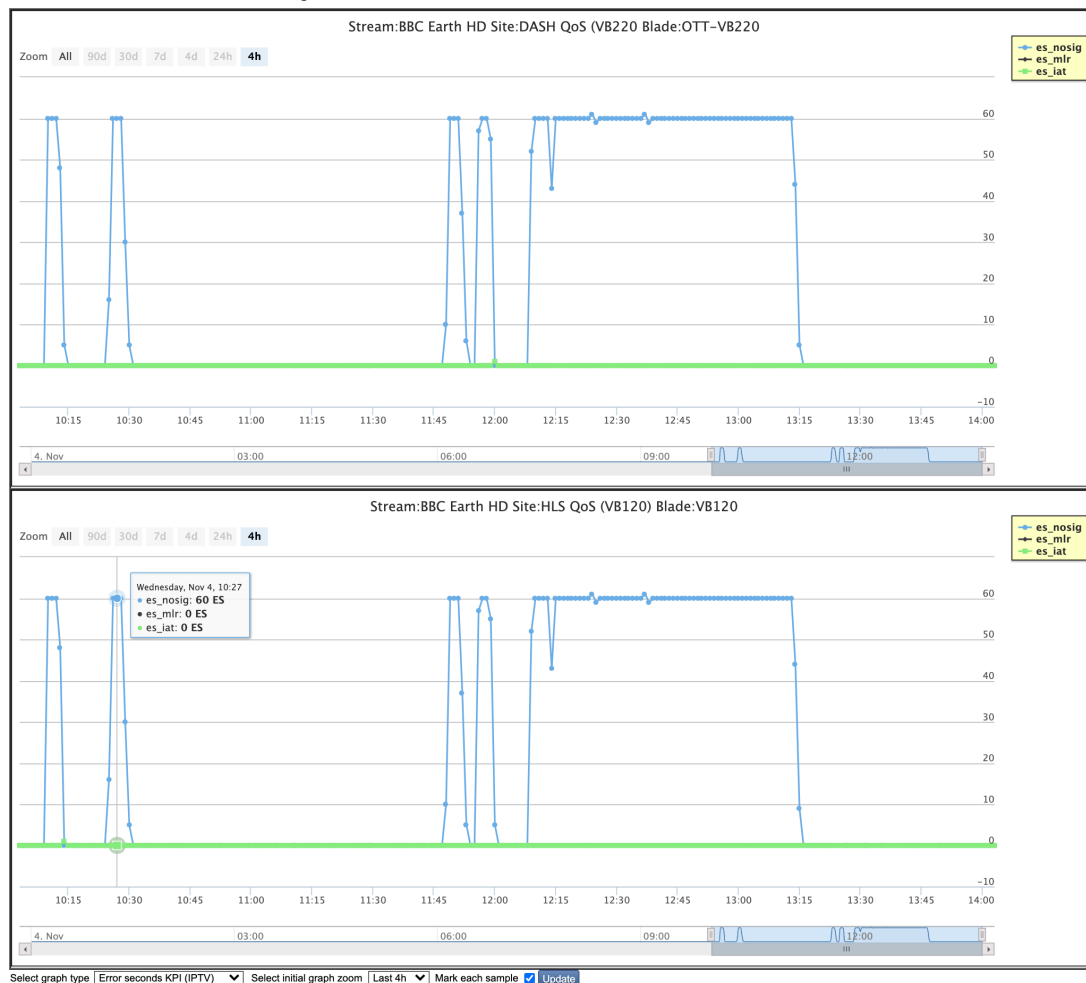
Pri 1	Pri 2	Pri 3	Other	Interface
TS sync	Transport	NIT	CA syst.	Pre FEC BER
Sync byte	CRC	SI Rep	PID minbr.	Post FEC BER
PAT	PCR	Unref PID	PID maxbr.	MER
Continuity	PCR accr.	SDT	PID ch.	SNR
PMT	PTS	EIT	Serv. minbr.	Sig. str.
Miss.PID	CAT	RST	Serv. maxbr.	Center frequency
		TDT	Serv. ch.	Symbol rate
			MIP	T2MI
			Cont. ch.	Intf. ovfl.
			Gold TS	
			Time	

Up to five streams may be compared across different probes and interfaces in the **Selected stream compare ETR** view.

Refer to the probe manual for a comprehensive description of the compare sub-views.



6.6.5 Selected Stream Compare Streamdata



This view is available for all Ethernet IPTV streams, OTT and RF streams. The data source is the stream-data in the database. The history available depends on the settings found under the **Disk tuning** link on the **About — System** page. The maximum history is two years. Note that the time needed to generate this page depends primarily on the speed on the VBC server, the history window of the database and the number of streams selected.

For 4h and 24h intervals data is plotted with minute resolution, for larger intervals 1 hour spacing is used.

Clicking the legends will toggle the visibility of each graph.

The user can customize the graphs by making selections in the menu-bar below the graphs and clicking Update.

The data that can be plotted depends on the type of the stream monitored. The available settings are:

<i>Graph type</i>	<i>Available parameters</i>
Error seconds KPI (IPTV streams)	Select among • Error seconds no signal • Error seconds media loss rate • Error seconds inter arrival time



Error seconds bitrate (IPTV streams)	Select among • Error seconds bitrate overflow • Error seconds bitrate underflow
Bitrates and DF (IPTV streams)	Select among • Max delay factor • Maximum bitrate • Minimum bitrate
Sum packet loss (IPTV streams)	Select among • Sum of media loss rate • Sum of RTP drops
RF parameters (for RF interfaces)	Select among • Signal level • Signal to noise ratio • Modulation error ratio
Error seconds KPI (OTT streams)	Select among • Error seconds quality • Error seconds availability • Error seconds transport • Error seconds http • Error seconds xml
Error seconds KPI (QOE)	Select among • Error seconds QoE video • Error seconds QoE audio • Error seconds captions availability • Error seconds captions quality
Aggregate probe info (AGG)	When selected for the “probe_aggregate_stats” stream, this graph displays a simple arithmetic sum of the statistics for all streams on the selected blade. Comparing the aggregate streams draws the graphs using a logarithmic scale. Please note that this graph does not display any meaningful data when selected for other stream types.
All	Displays all of the above in one graph

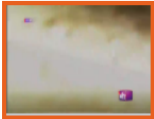
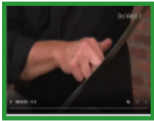
Select initial graph zoom: This specifies the initial zoom for all the graphs after the Update has been clicked. Each graph can be adjusted individually afterwards.

Mark each sample: Emphasize each database sample so that it is easy to spot holes in the database when the stream was not monitored.



6.7 Thumbs view

LOGIN
LIVE
MONITORING
BLADE ALARMS
GRAPHICS VIEW
STREAM VIEW
THUMBS VIEW
SERVICE VIEW
MAP
RDP
RDW
EQUIPMENT
ALARM SETUP
TIMELINE
REPORTS
EXT. REPORTS
MAIN

 Appear TV HLS OTT/10.150.0.167	 SL31 OTT/10.150.0.167	 SL69 OTT/10.150.0.167
 NRK3 DASH OTT/10.150.0.167	 SL32 OTT/10.150.0.167	 SL85 OTT/10.150.0.167
 SL01 OTT/10.150.0.167	 SL44 OTT/10.150.0.167	 SL86 OTT/10.150.0.167
 SL02 OTT/10.150.0.167	 SL48 OTT/10.150.0.167	 SL93 OTT/10.150.0.167
 SL03	 SL53	 SL99

Stream-group Sort Filter

[1-](#) [43-](#) [85-](#) [127-](#) [169-](#) [211-](#) [253-](#) [295-](#) [337-](#) [379-](#) [421-](#) [463-](#) [505-](#) [547-](#) [589-](#) [631-](#) [673-](#) [715-](#) [757-](#) [759-](#)

If one or more probes (software version 6.0.0 or later required) or more VB288 Objective QoE Content Extractors are part of the VBC configuration, the **Thumbs view** will present a thumbnail picture for each stream which is extracted.

The current stream status is indicated by the thumbnail picture's frame color. The MicroTimeline stream bar presenting stream status for the last 4 days is the same as in the **Stream view** page.

The line just below the stream name indicates whether it is an IPTV stream or a OTT stream. A stream will occur as many times as it is extracted on the supported blades. A stream will occur regardless of whether it is monitored by probes.

The number of streams presented on a page is only limited by the size of the display screen. Refreshing the screen after resizing the browser window will automatically fill up all of the available screen area.



Clicking a stream name brings up the **Stream view — Selected** view.

The selectable stream groups are available in the *Stream-group* drop-down menu. The user selects whether all streams or only one stream group should be represented in the view. The stream groups are configured in the **Main — Stream groups** page.

The *Sort* drop-down menu allows stream sorting based on name, interface or current stream status severity.

The *Filter* field allows the user to specify a text string; only streams where the stream name, multicast address or sites name matching the specified string will be displayed. This functionality is very useful to quickly locate a specific stream in a large system.



6.8 Service view (Transport Stream Service View option)

	Last96h	Now	I.F.	Service	#	Last96h	Now	I.F.	Service	#	Last96h	Now	I.F.	Service	#
LOGIN	1		QAM			43		COF...	Eurosport	3	85		IPTV	MTV 80s	1
LIVE	2		QAM	3sat	1	44		QAM	Eurosport 1	1	86		QAM	MTV 80s	1
MONITORING	3		IPTV	4K Universe	3	45		QAM	Eurosport Norge	2	87		SAT	MTV HD	1
BLADE ALARMS	4		ASI	a.tv HD	1	46		QAM	Eurosport Pluss 1	1	88		SAT	MTV HD Austria	1
GRAPHICS VIEW	5		IPTV	Al Jazeera Channel	1	47		QAM	Eurosport Pluss 2	1	89		QAM	MTV Hits	1
STREAM VIEW	6		QAM	Animal Planet	1	48		QAM	Eurosport Pluss 3	1	90		QAM	MTV Live	1
THUMBS VIEW	7		ASI	BB-MV-LokalTV	1	49		QAM	Eurosport Pluss 4	1	91		ASI	münchen.tv HD	1
SERVICE VIEW	8		QAM	BBC Brit	2	50		QAM	Eurosport Pluss 9	1	92		IPTV	Nasa TV UHD	4
MAP	9		IPTV	BBC BRIT HD (N)	2	51		QAM	Eurosport Pluss10	1	93		QAM	Nat Geo	1
RDP	10		QAM	BBC Earth	2	52		QAM	Eurosport Pluss11	1	94		IPTV	Nat Geo HD (N)	2
RDW	11		COF...	BBC WORLD NEWS	1	53		QAM	Eurosport Pluss12	1	95		QAM	Nat Geo Wild	1
EQUIPMENT	12		COF...	BBC World News	3	54		QAM	Fashion TV	1	96		COF...	National Geographic	4
ALARM SETUP	13		QAM	BBC World News	1	55		COF...	FEM	3	97		IPTV	NDR FS NDS HD	1
REPORTS	14		SAT	BDL VoD	1	56		QAM	FEM	1	98		QAM	NHK	1
EXT. REPORTS	15		SAT	Beate Uhse HD	1	57		IPTV	FEM HD	1	99		IPTV	Nick Jr.	1
MAIN	16		QAM	Boomerang	1	58		QAM	Food	1	100		QAM	Nick Jr.	1
	17		SAT	Boomerang	1	59		COF...	FOX	1	101		IPTV	Nickelodeon (N)	1
	18		IPTV	BR Fernsehen Nord HD	1	60		QAM	FOX	1	102		IPTV	Nickelodeon (S)	1
	19		IPTV	BR Fernsehen Süd HD	2	61		IPTV	FOX HD (N)	1	103		IPTV	NickToons	1
	20		QAM	C More First	1	62		QAM	France 2	1	104		QAM	Norway Live	1
	21		QAM	C More Hits	1	63		QAM	France 24	1	105		QAM	NRJ	1
	22		QAM	C More Series	1	64		QAM	France 24 English	1	106		QAM	NRK Alltid klassisk	1
	23		IPTV	C More Sport 1 HD	1	65		COF...	Frikkanalen	3	107		QAM	NRK Alltid Nyheter	1
	24		QAM	C More Stars	1	66		QAM	Ginx	1	108		SAT	NRK Alltid Nyheter	2
	25		COF...	CANAL+ First	3	67		QAM	God TV	1	109		SAT	NRK Folkemusikk	1
	26		COF...	CANAL+ Hits Sport	3	68		IPTV	Gospel Channel Europe	1	110		QAM	NRK Jazz	1
	27		COF...	CANAL+ Sport1	3	69		SAT	Handystar TV HD	1	111		SAT	NRK Jazz	2
	28		SAT	Channel21 HD	1	70		COF...	History	1	112		SAT	NRK Klassisk	1
	29		IPTV	CNBC Europe	1	71		QAM	History Channel	1	113		QAM	NRK mP3	1
	30		QAM	Colors	1	72		QAM	HISTORY2	1	114		SAT	NRK mP3	2
	31		IPTV	Cubavision Internacional	1	73		IPTV	HyperDeck - 1920X108...	1	115		QAM	NRK P1 Buskerud	1
	32		COF...	Discovery	1	74		QAM	ID	1	116		SAT	NRK P1 Buskerud	2
	33		QAM	Discovery	1	75		IPTV	ID Investigation Discovery	1	117		QAM	NRK P1 Finnmark	1
	34		IPTV	Discovery HD (N)	2	76		IPTV	Kunskapskanalen HD	1	118		SAT	NRK P1 Finnmark	2
	35		IPTV	Disney Channel	2	77		IPTV	Kunskapskanalen HD - T...	1	119		QAM	NRK P1 Hedmark/Oppl...	1
	36		IPTV	Disney Junior	2	78		IPTV	Kunskapskanalen HD - T...	2	120		QAM	NRK P1 Hordaland	1
	37		QAM	Disney Junior	1	79		ASI	Lokal-TV-Portal HD	1	121		SAT	NRK P1 Hordaland	2
	38		IPTV	Disney XD	1	80		IPTV	Matkanalen	1	122		SAT	NRK P1 Innlandet	2
	39		QAM	DR1	2	81		QAM	Matkanalen	1	123		QAM	NRK P1 Møre og Romsdal	1
	40		QAM	EPG DL HD PVR	1	82		IPTV	MAX HD	1	124		SAT	NRK P1 Møre og Romsdal	2
	41		QAM	EPG DL HD Zapper	1	83		QAM	MH.C	17	125		QAM	NRK P1 Nordland	1
	42		QAM	Euronews	1	84		IPTV	MTV	1	126		SAT	NRK P1 Nordland	2
Service group [All services] Sort [Name] Filter															
1-126 127-252 253-378 379-504 505-630 631-756 675-800															

In the optional **Service view** transport stream services are presented in alphabetical order as default. For each service the bulb shows the current status and the 96-pixel MicroTimeline stream-bar shows the status for the last 96 hours (i.e. 4 days). For services to be shown in the **Service view** the corresponding stream must be ETR 290 monitored in one or more probes and must have a service name signaled in the transport stream (in Service Description Table (SDT) for DVB systems or Virtual Channel Tables (VCT) for ATSC streams).

Note that the MicroTimeline is updated per stream and not per service. Thus all services that are part of the same stream will have the same MicroTimeline. The **Extended reports** functionality can generate service based PDF reports where the status is filtered per service (and optionally aggregated over different sites).

Each bulb color corresponds to the aggregate status for all probes that belong to sites that the user has access to. The bulbs are updated every 60 seconds – which corresponds to the probe poll interval.

The service bars reveal any alarm that has been present during the last 4 days. The bars will automatically scroll one pixel to the left each hour with the rightmost pixels showing the status for the previous full hour. The bar color corresponds to the severity of alarms that have occurred.

The number of services presented on a page is only limited by the size of the display screen. Refreshing the screen after resizing the browser window will automatically fill up all of the available screen area. If



there are more services in a system than can be displayed in a single view the remaining services may be monitored by clicking the numbered links at the bottom of the page.

The user chooses to display all services in the system or limit the display to one service group. The selectable service groups are available in the *Service group* drop-down menu. The service groups are configured in the **Main — Service groups** page.

The *Sort* drop-down menu allows service sorting based on name, interface or current stream status severity.

The *Filter* field allows the user to specify a text string; only services with names matching the specified string will be displayed. This functionality is very useful to quickly locate a specific stream in a large system.

Clicking a service name brings up the **Selected Service View**, allowing further inspection of a service.

6.8.1 Service view — Thumbs



Service group [All services] ▼ Sort Name ▼ Filter

1- 36- 71- 106- 141- 176- 211- 246- 281- 316- 351- 386- 421- 456- 491- 526- 561- 596- 631- 666- 701- 736- 766-
35 70 105 140 175 210 245 280 315 350 385 420 455 490 525 560 595 630 665 700 735 770 800

The **Service view — Thumbs** view is identical to the regular **Thumbs view**, except that individual thumbs will be displayed for each service within an MPTS (Multi Program Transport Stream).



6.8.2 Service view — Selected

NRK Super / NRK3 HD

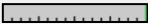

Prev:[NRK Super](#) Next:[NRK Super / NRK3 lydtekst](#)

Bitrate: **9.26M** Encoding: **yuv420p** Address: **239.255.0.152:5500**

Video: **8.42M clear** Size: **1280x720** Extractor: [VB288](#)

Audio: **0.07M clear** Aspect: **16:9**

Teletext: **0.30M** Service name: **NRK Super / NRK3 HD**

#	SID	Interface	Stream	Stream last 96h	Now	Probe
☐	1	1041	IPTV	NRK Super NRK3 HD		VB330:Core
☐	2	1041	SAT1	Main		VB273 :VB273 Redundant
☐	3	1041	SAT2	Spare		VB273 :VB273 Redundant

[Compare ETR measurements for selected services](#)

The **Selected Service View** lists MicroTimeline bars for all probes and interfaces that are ETR 290 monitoring the selected service. If a probe monitors the same service for several inputs there will be one entry in the list for each interface. If one or more VB288 Objective QoE Content Extractors, or probes with the Content Extraction and Alarming option, are part of the VBC configuration and is monitoring the service, a thumbnail picture and associated meta-data are displayed at the top of the page.

Selecting one to five locations and clicking the **Compare ETR measurements for selected services** will open the **Selected TS Service Compare ETR** view. Clicking the stream name opens the stream in the **Stream view — Selected** view. Clicking the probe name opens the probe's **Stream overview** page for the selected stream in the **Monitoring — Blade** view.

Thumbnail meta-data

<i>Parameter</i>	<i>Description</i>
Bitrate:	The total stream rate
Video:	The video bitrate and whether the component is scrambled or not
Audio:	The audio bitrate and whether the component is scrambled or not
Teletext:	The teletext bitrate and whether the component is scrambled or not
Encoding:	The video encoding format
Size:	The video picture size (video resolution)
Aspect:	The video aspect ratio
Service name:	The name of the service in the stream
Address:	The multicast IP address of the stream
Probe / Extractor:	The IP address of the probe or extractor delivering thumbnail and metadata; can be clicked

<i>Parameter</i>	<i>Description</i>
#	The probe number
SID	The service ID of the monitored service. This can differ between different sites if the service ID is remapped in the system



Interface	The type of probe interface that carries the stream containing the monitored service
Stream	The name of the stream carrying the service, as defined in the probe
Stream last 96h	The MicroTimeline bar for the stream that contains the selected service for the given probe and interface
Now	A bulb indicating the current status for the stream that contains the selected service for the given probe and interface
Probe	A link to the Blade view for the probe that has performed the service measurements



6.8.3 Selected TS Service Compare ETR

Overview (VB330:Core / Ethernet / NRK Super_NRK3 HD (239.255.0. ^

Stream overview

TS ID: 172
NW ID: NA
Orig NW ID: NA
Min. eff. 2.49 Mbps
bitr: 11.23
Max. off: 11.23

Error statistics

Total monitoring
time: 15 d, 3 h
ETR Priority 1: 3 h, 8 m
No Signal: 3 h, 7 m
CC Errors: 32 s
Interface

Service alarms (VB330:Core / Ethernet / NRK Super_NRK3 HD (239.2 ^

Service/Alarm	Pid
1041 NRK Super / NRK3 HD	

Services (VB330:Core / Ethernet / NRK Super_NRK3 HD (239.255.0.1 ^

Service/Pid	Min bitrate	Max bitrate	CC	Max ...
1041 NRK Super / NRK3	2.404 M...	11.375 ...	0	
440 PMT	5.624 kbps	13.112 k...	0	
1118 MPEG4 Video	1.584 M...	10.289 ...	0	-121....
3113 AAC LATM Audir	62.040 k...	83.480 k...	0	
4124 AC3 Audio	456.136 ...	467.432 ...	0	
6585 Subtitling	2.768 kbps	83.368 k...	0	
6116 Teletext	291.824 ...	306.608 ...	0	
6586 Subtitling	2.520 kbps	132.024 ...	0	

Alarm graph (VB330:Core / Ethernet / NRK Super_NRK3 HD (239.255.0.1 ^

Check	Timeline
Alarm status	15:00Tu 21:00Tu 03:00We 09:00We

ETR Details (VB330:Core / Ethernet / NRK Super_NRK3 HD (239.255.0.1 ^

Pri 1	Pri 2	Pri 3	Other	Interface
TS sync	Transport	NIT	CA syst.	T2MI
Sync byte	CRC	SI Rep	PID minbr.	IAT
PAT	PCR	Unref PID	PID maxbr.	MLR
Continuity	PCR accr.	SDT	PID ch.	RTP
PMT	PTS	EIT	Serv. minbr.	Intf. ovfl.
Miss.PID	CAT	RST	Serv. maxbr.	
		TDT	Serv. ch.	
			MIP	
			Cont. ch.	
			Gold TS	
			Time	

Overview (VB273 :VB273 Redundant / SAT1 / Main (1.094 GHz) / 10 ^

Stream overview

TS ID: 70
NW ID: 70
Orig NW ID: 70
Min. eff. 52.74 Mbps
bitr: 53.73
Max. off: 53.73

Error statistics

Total monitoring
time: 13 m, 28 s
ETR Priority 1: 23 s
No Signal: No errors
CC Errors: 23 s
Interface

Service alarms (VB273 :VB273 Redundant / SAT1 / Main (1.094 GHz) / 10 ^

Service/Alarm	Pid
1041 NRK Super / NRK3 HD	

Services (VB273 :VB273 Redundant / SAT1 / Main (1.094 GHz) / 104 ^

Service/Pid	Min bitrate	Max bitrate	CC	Max ...
1041 NRK Super / NRK3	2.515 M...	11.293 ...	9	
440 PMT	6.016 kbps	8.984 kbps	0	
1118 MPEG4 Video	1.610 M...	10.280 ...	2	134 ns
3113 AAC LATM Audir	63.472 k...	72.192 k...	0	
4124 AC3 Audio	451.904 ...	464.752 ...	1	
6585 Subtitling	2.776 kbps	6.040 kbps	0	
6116 Teletext	295.728 ...	303.224 ...	1	
6586 Subtitling	2.880 kbps	69.648 k...	0	
630 DSM-CC	78.264 k...	81.496 k...	1	

Alarm graph (VB273 :VB273 Redundant / SAT1 / Main (1.094 GHz) / 104 ^

Check	Timeline
Alarm status	02:00We 08:00We 14:00We 20:00We

ETR Details (VB273 :VB273 Redundant / SAT1 / Main (1.094 GHz) / 104 ^

Pri 1	Pri 2	Pri 3	Other	Interface
TS sync	Transport	NIT	CA syst.	Post LDPC-BCH
Sync byte	CRC	SI Rep	PID minbr.	MER
PAT	PCR	Unref PID	PID maxbr.	SNR
Continuity	PCR accr.	SDT	PID ch.	Sig. str.
PMT	PTS	EIT	Serv. minbr.	Pkt. err.
Miss.PID	CAT	RST	Serv. maxbr.	Center frequency
		TDT	Serv. ch.	Symbol rate
			MIP	T2MI
			Cont. ch.	Eb/N0
			Gold TS	EVM
			Time	Intf. ovfl.

Up to five transport stream services may be compared across different probes and interfaces in the **Selected TS Service Compare ETR** view.

74

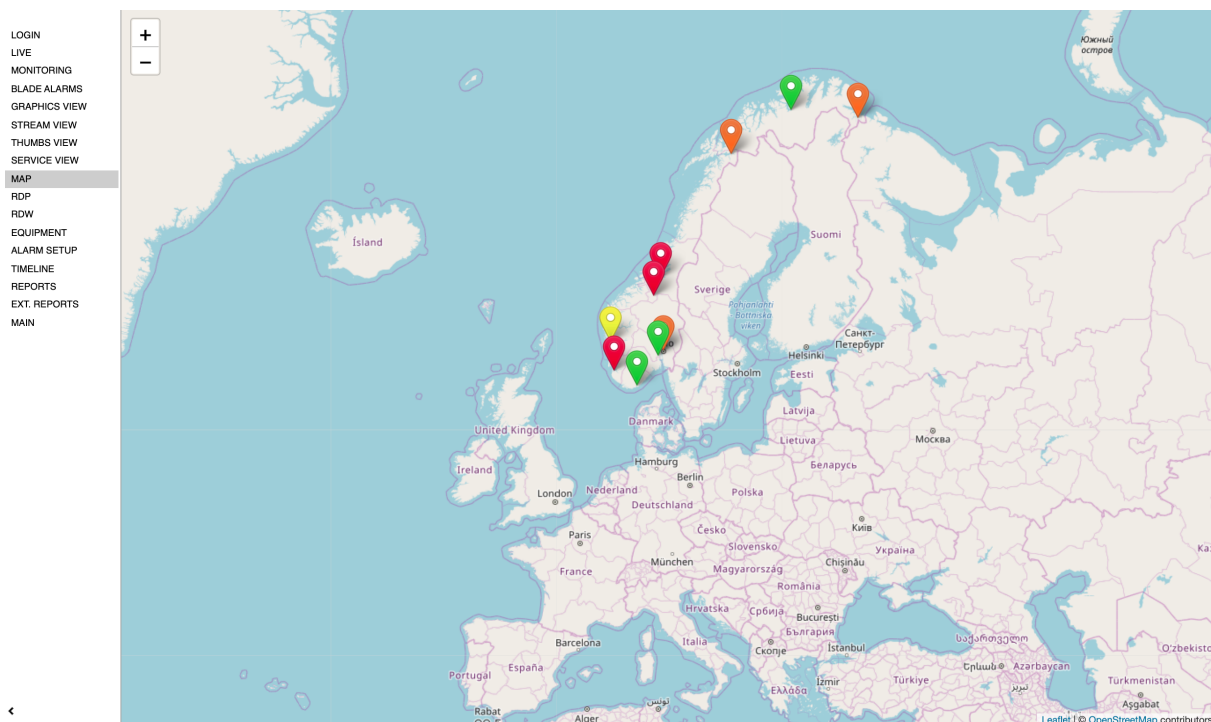
VBC Controller User's Manual v7.0.0 © Bridge Technologies Co AS



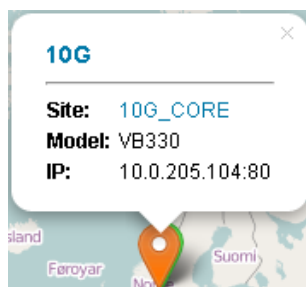
Refer to the probe manual for a comprehensive description of the compare sub-views.



6.9 Map



The map feature displays a geographic overview of blades that have a geographic location configured. Each blade is represented by a pin. The color of the pins shows the status of the devices.



Clicking a pin will display more information about that blade, such as name, site and IP and makes it possible to access the blade details.

The geographical location of a blade is configured in the **Equipment** view.

Note that the Map feature requires an Internet connection to reach the map server.



6.10 RDP

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

ALARM SETUP

TIMELINE

REPORTS

EXT. REPORTS

MAIN

Return Data Path (RDP)

Start	Stop	RDP	Site	Blade	IP address	Engine	Forw interface	Stream addr:port:ssm	Dest addr:port
Start	Stop		HLS QoS (VB120)	VB120	10.0.205.193	1	data	239.255.0.59:5500:10.0.81.15	172.20.1.115:1234
Start	Stop		HLS QoS (VB120)	VB120	10.0.205.193	2	management	239.255.0.10:5500:10.0.81.16	0.0.0.0:1234
Start	Stop		VB120-VB262	VB262	10.0.205.41	1	data	239.255.0.4:5500:0.0.0.0	10.20.30.40:1234
Start	Stop		VB120-VB262	VB262	10.0.205.41	2	management	(not relevant)	10.20.30.40:1234
Start	Stop		VB220-VB272	VB272 DVB S-S2	10.0.205.200	1	data	(not relevant)	10.20.30.40:1234
Start	Stop		VB220-VB272	VB272 DVB S-S2	10.0.205.200	2	management	(not relevant)	10.20.30.40:1234
Start	Stop		VB220-VB252-252	VB252	10.0.205.120	1	management	(not relevant)	172.20.1.76:5500
Start	Stop		VB220-VB252-252	VB252	10.0.205.120	2	data	0.0.0.0:0.0.0.0	10.20.30.40:1234
Start	Stop		VB220-VB242-256	ASI-COFDM	10.0.205.223	1	management	239.255.0.17:5500:0.0.0.0	10.20.30.40:1234
Start	Stop		VB220-VB242-256	ASI-COFDM	10.0.205.223	2	management	(not relevant)	10.20.30.40:1234
Start	Stop		DASH QoS (VB220)	OTT-VB220	10.0.205.93	1	management	239.255.0.153:5500:10.0.81.13	172.20.1.97:1234
Start	Stop		DASH QoS (VB220)	OTT-VB220	10.0.205.93	2	management	239.255.0.4:5500:10.0.81.13	10.20.30.40:1234
Start	Stop		VB273	VB273 Redundant	10.0.205.228	1	data	(not relevant)	10.20.30.40:1234
Start	Stop	✓	VB273	VB273 Redundant	10.0.205.228	2	management	0.0.0.0:0.0.0.0	10.20.30.40:1234
Start	Stop		VB330	Core	10.0.205.104	1	management	239.255.0.76:5500:10.0.81.15	172.20.1.112:1234
Start	Stop		VB330	Core	10.0.205.104	2	data	239.255.0.35:5500:0.0.0.0	10.0.123.213:391
Start	Stop		VB50	VB50	10.0.205.27	1	management	0.0.0.0:0.0.0.0	10.20.30.40:1234
Start	Stop		VB50	VB50	10.0.205.27	2	management	0.0.0.0:0.0.0.0	10.20.30.40:1234
Start	Stop		VB330	VB330 - L2TPenc	10.0.205.14	1	data	0.0.0.1:-2147438584:0.0.0.0	232.1.2.3:5500
Start	Stop		VB330	VB330 - L2TPenc	10.0.205.14	2	management	233.233.233.233:3509:200.200.160.160	0.0.0.0:5500
Start	Stop	✓	DVB-T2	VB252-T2	10.0.205.216	1	data	0.0.0.0:0.0.0.0	192.168.100.60:1234
Start	Stop	✓	DVB-T2	VB252-T2	10.0.205.216	2	data	(not relevant)	192.168.100.60:1235
Start	Stop		VB440 test	VB440	185.102.108.142	1	data	0.0.0.0:0.0.0.0	10.20.30.40:1234
Start	Stop		VB440 test	VB440	185.102.108.142	2	data	0.0.0.0:0.0.0.0	10.20.30.40:1234
Start	Stop		VB330	VB330-Redundant	10.150.100.226	1	management	239.255.0.20:5500:10.0.81.15	192.168.100.61:1234
Start	Stop		VB330	VB330-Redundant	10.150.100.226	2	management	0.0.0.0:0.0.0.0	10.20.30.40:1234
Start	Stop		[Unassigned]	device1	10.0.30.220	1	data	(not relevant)	239.255.7.77:1234
Start	Stop		[Unassigned]	device1	10.0.30.220	2	data	(not relevant)	239.255.8.88:5500
Start	Stop		V6.0 RELEASE	VB330 SW v6.0	10.0.205.9	1	ens160	239.255.0.150:5500:10.0.81.13	10.20.30.40:1234
Start	Stop		V6.0 RELEASE	VB330 SW v6.0	10.0.205.9	2	ens160	0.0.0.0:0.0.0.0	10.20.30.40:1234
Start	Stop		V6.0 RELEASE	VB440 v6.0	185.102.108.142	1	data	0.0.0.0:0.0.0.0	10.20.30.40:1234
Start	Stop		V6.0 RELEASE	VB440 v6.0	185.102.108.142	2	data	0.0.0.0:0.0.0.0	10.20.30.40:1234

Active RDP

Only one active RDP ☐

Stream to forward: address: port: ssm:

Destination: address: port:

Relay settings: Interface:

Update dialog from selected probe

Apply dialog to selected probes

The RDP view allows users to obtain control and overview of the RDP configuration and RDP status of individual probes in a system. This makes it easy to avoid stream corruptions that might otherwise occur due to several probes forwarding a stream to the same destination address.

The return data path list shows the RDP configuration of the probes in a system:

Return Data Path (RDP)	
Parameter	Description
[Start]	Click the Start button to start RDP forwarding for the corresponding probe
[Stop]	Click the Stop button to stop RDP forwarding for the corresponding probe
RDP	If RDP forwarding is active for a probe, the corresponding RDP field will display a checkmark (✓)
Site	The site associated with a probe. Click the site link to open the site view
Name	The probe name. Click the probe name link to open the probe view
IP address	The probe IP address
Engine	The probes have 2 independent RDP engines, this column shows the engine number
Forw. interface	Shows which probe Ethernet interface the RDP stream will be used to forward the stream
Stream addr:port:ssm	The address of the stream to be forwarded. The format is <i>IP-address:port number:Source Specific Multicast</i>
Dest addr:port	The destination address that the stream should be forwarded to. The format is <i>destination IP address:port number (interface gateway IP address)</i>



Active RDP

It is possible to define that only one RDP forwarding can be active at any time. Enabling RDP forwarding for a probe will then stop RDP forwarding for all other probes, to avoid possible stream interference due to several probes forwarding to the same address. Mark the checkbox and click the **Apply** button to activate this functionality.

RDP probe settings – only Ethernet

It is possible to define and upload RDP settings to a probe. This is done by setting parameters, selecting a probe by highlighting a row in the RDP probe list and clicking the **Apply to selected probes** button. It is also possible to select several rows to upload identical settings to several probes.

The RDP probe settings are:

<i>RDP probe settings – only Ethernet</i>		
	<i>Parameter</i>	<i>Description</i>
Stream to forward:	address:	The IP address of the multicast or unicast to be forwarded
Stream to forward:	port:	The port number of the multicast or unicast to be forwarded
Stream to forward:	SSM:	The source IP address for a Source Specific Multicast
Destination:	address:	The RDP destination IP address
Destination:	port:	The RDP destination port number
Relay settings:	Interface:	From the drop-down menu select the interface the RDP streaming should use: <i>Data interface</i> or <i>Management interface</i>

It is also possible to copy probe settings to the RDP probe settings dialogue field by highlighting a row in the RDP probe list and clicking the **Update from selected probe** button.



6.11 RDW

6.11.1 RDW — Canvases

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

ALARM SETUP

TIMELINE

REPORTS

EXT. REPORTS

MAIN

Canvases (10) | Devices (22) | Tags (0)

+ New Canvas

+ New Carousel

Filter

Edit

Clone

Remove

Name	Owner	Carousel
default	admin	
tutorial	admin	
Satellite Ingress / Redundancy Switching	demo	
Headend / Datacenter	demo	
IP Media Monitoring	admin	
Terrestrial Distribution	demo	
Broadband Cable	demo	
OTT / Multiscreen	demo	
QTT QoS & QoE	QTT	
test_1	demo	

The **RDW — Canvases** view creates, edits, or removes canvases for the current user, or all users if logged in as **admin**. Please refer to chapter 3 for more information on the Remote Data Wall feature.

You can filter the list of canvases by searching for name or owner in the **Filter** box.

Canvases	
Name:	Name of this canvas. Clicking the name opens the canvas configurator.
Owner:	Name of the user who owns this canvas.

To create a new canvas, click the **New Canvas** button and enter the name of the new canvas.

To change the name or owner of a canvas, first click the **Edit** button on the top right.

To remove a canvas, click the **Remove** button on the top right, then click the **Remove** button for the canvas you want to remove.



6.11.2 RDW — Devices

Canvases (10)		Devices (22)		Tags (0)		
All Devices		Recent	Connected	Inactive	Edit Remove	
Name	Canvas to show	Commands		Status	Status Last Updated	Auto reload
RT	default	Identify	Reload	Inactive	2 years ago	03:00
HS	default	Identify	Reload	Inactive	a year ago	03:00
Hugo Lap	default	Identify	Reload	Inactive	a year ago	03:00
hugo pc	IP Media Monitoring	Identify	Reload	Inactive	9 months ago	03:00
Peter office	default	Identify	Reload	Inactive	9 months ago	03:00
Reception Sofa Left	QTT QoS & QoE	Identify	Reload	Connected	11 hours ago	03:00
Reception Sofa Right	IP Media Monitoring	Identify	Reload	Connected	11 hours ago	03:00
Device 218	default	Identify	Reload	Inactive	2 months ago	03:00
Device 219	default	Identify	Reload	Inactive	2 months ago	03:00

The **RDW — Devices** lets the user change canvas, identify, or reload devices connected to its canvases. Please refer to chapter 3.2 for more information on how to connect devices to the Remote Data Wall.

It is not possible to use the same browser session as a Remote Data Wall display device as the one you are using to access the configuration interface.

There are four ways of filtering the know devices.

All Devices show all devices that are, or has been connected to the server at one point.

Recent show all devices that are connected, or was disconnected within the last day.

Connected show all devices that are connected now.

Inactive show all devices that has been disconnected for more than one day.



<i>Devices</i>	
Name:	Name of this device.
Canvas to show:	Name of the canvas to show on this device
Commands:	Identify displays the device name on the device. Reload forces the device to reload the canvas
Status:	Show the current status of the device, it can be <i>Connected</i> , <i>Disconnected</i> , or <i>Inactive</i>
Status Last Updated:	Last time the device was connected
Auto reload:	Show if and when the device will automatically reload

To change the name or reload time of a device, first click the **Edit** button on the top right.

To remove old devices, click the **Remove** button on the top right, then click the **Remove** button for the device you want to remove.

6.11.3 RDW — Tags

Canvases (10)Devices (22)Tags (3)

Show AllHide All

Visible

mcr-picture ×slideshow ×

Hidden

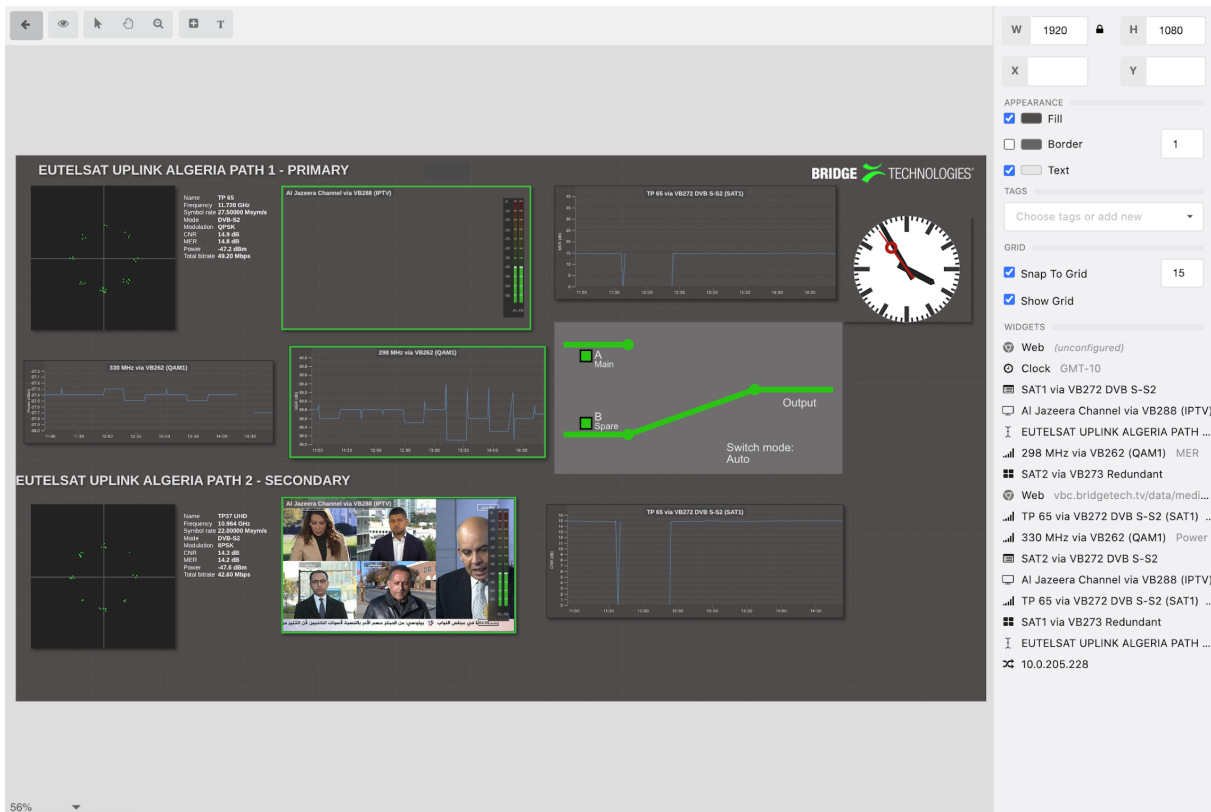
mcrpicture ×

The **RDW — Tags** view lets the user quickly hide canvases or widgets that have been tagged with specific tags.

Pressing the **Show All** button, makes all the tags visible. Pressing the **Hide All** button, makes all tags hidden. To move a single tag between visible and hidden, press the × next to its name.



6.11.4 Canvas Configurator



The **Canvas Configurator** lets the user configure a canvas by setting the size and color of the background, adding and placing widgets, and more.

It has three main areas; the toolbar at the top of the screen, the canvas and widget options on the right of the screen, and the canvas itself, where the widgets are placed.

Toolbar			
Function	Button	Key	Description
Preview		F	Toggle preview mode, where you can see how the canvas would behave on a client device
Select and Move		V	This tool can be used to select one or multiple widgets. Click a widget to select it or drag a box to select multiple widgets. Holding the shift button while clicking adds or removes the clicked widget to the selection. To move the selected widgets, drag them in place, or use the arrow keys. Selected widgets can be copied with Ctrl+C and pasted with Ctrl+V . Pressing the Delete key will delete all selected widgets from the canvas. Click the canvas background to deselect everything.
Pan		Alt	By either selecting this tool, or holding Alt , you can click and drag to move the viewpoint
Zoom		Z	This tool allows you to zoom in where you click. Holding Shift while clicking will zoom out instead.



Add Widget		W	This tool lets you add new widgets to the canvas. Either click the widget you want, or type its name and press enter, then drag out a box for the widget. This adds the widget to the canvas, and to the current selection.
Text		T	With this tool selected, click a Textbox widget to be able to edit it. With text selected, press Ctrl+B to make it bold , Ctrl+I to make it <i>italic</i> or Ctrl+U to make it <u>underlined</u> .

When changing widget options, only select *one* widget at a time. To change the options of the canvas, deselect all widgets.

Common options

Size and Position

W	Sets the width of the widget or canvas
H	Sets the height of the widget or canvas
X	Sets the horizontal position within the canvas
Y	Sets the vertical position within the canvas

Appearance

Fill	Sets the background color
Border	Sets the border color and width
Text	Sets the text color
Drop shadow	Adds a shadow on the bottom and right side of the widget

Tags

Add or remove tags from the canvas or selected widget. These tags can be used to hide sensitive information at the press of a button. To change the visibility of the tag, use the **RDW — Tags** view or the Tag Control Widget.

Canvas options

Grid

Snap To Grid	Makes the widgets snap to the grid size set
Show Grid	Makes the grid lines visible in the configurator

Widgets

This shows a list of all widgets. They can be selected here, and if some widgets are overlapping you can change the order in this list to change which will be rendered on top



<i>Widget options</i>	
<i>Plaque</i>	
Display	Selects the position of the plaque. Off removes it
Text	Sets the content of the plaque

6.11.5 Remote Data Wall Widgets

Each widget has its own options which differ from widget to widget. To edit these, it is important to only select one widget at a time.

6.11.5.1 Web Widget

The web widgets allows for embedding any web page or image on the RDW canvas.

<i>Options</i>	
URL	URL to the web page or image to load
Scale	Sets the zoom level of this page or image
Refresh	Sets if and how often the page or image is reloaded
Allow scripts	Sets if the page is allowed to run JavaScript
Allow progressive loading	Sets if the page is allowed to download additional data

6.11.5.2 Textbox Widget

The Textbox widget can be used to add static text to the RDW canvas.

<i>Options</i>	
Size	Sets the font size
Alignment	Sets the text alignment; one of <i>Left</i> , <i>Center</i> , or <i>Right</i>

6.11.5.3 Thumbnail Widget

The thumbnail widgets lets you display updating thumbnails from your multicasts and OTT channels.

<i>Options</i>	
Channel	Select a Multicast stream or OTT channel to display thumbnails from
Service	If the selected stream is a MPTS, you can select a specific service
Profile	If you selected a OTT channel and multiple profiles are available, you can select one
Show status border	Add a colored border that reflects the VBC alarms status for selected channel
Size	Sets the size of the image. <i>Contain</i> keeps the aspect ratio of the source, filling in black bars where needed; <i>Cover</i> resizes the image to make sure the image is fully visible; <i>Original</i> displays the image in its original size
Loudness	Turns on the selected audio meter for the selected channel, if available



6.11.5.4 Loudness Widget

The loudness widget displays audio values from your multicasts and OTT channels. It can either be a graph over the last couple of minutes, or a audio meter showing the current value. For a vertical meter, drag the box out high and thin. For a horizontal meter, drag the box out low and wide. For a graph, drag the box out high and wide.

<i>Options</i>	
Channel	Select a Multicast stream or OTT channel to display audio samples from
Service	If the selected stream is a MPTS or has multiple audio PIDs, you can select a specific service
Profile	If you selected a OTT channel and multiple profiles are available, you can select one
Show status border	Add a colored border that reflects the VBC alarms status for selected channel
Retention	Sets how much data the graph should display
Scale	Sets the where the graph or meter caps the values
Mode	Sets if the meter should show RMS or LUFS values

6.11.5.5 Media Window Widget

The media window widget shows media window data from your multicast streams.

<i>Options</i>	
Channel	Select a Multicast stream to display media window data from
Show status border	Add a colored border that reflects the VBC alarms status for selected channel
Plot	Sets which of the three available plots to display
Retention	Sets how much data the graph should display

6.11.5.6 Alarms Widget

The alarms widgets show the active VBC alarms, sorted by severity.

<i>Options</i>	
Filter	Filter list of alarms to only show streams which include this in the stream name
Source	Selects whether to display the VBC Controller alarm list, or that from a blade

6.11.5.7 RF Graph Widget

The RF graph widgets can display RF data from your tuners.

<i>Options</i>	
Channel	Select a Tuning to display RF data from
Data to display	Sets which data to display; Either <i>CNR</i> , <i>MER</i> , or <i>Channel Power</i>
Unit	Sets which unit to convert the values to
Scale	Sets the where the graph caps the values



Retention	Sets how much data the graph should display
------------------	---

6.11.5.8 Clock Widget

The clock widgets shows the time in the configured timezone.

<i>Options</i>	
Clock type	Sets what kind of clock to display
Timezone	Sets which timezone this clock should display
Minute offset	Sets the offset in minutes from the selected timezone

6.11.5.9 Slide Widget

The slide widgets can be used to create a slideshow of images hosted on any web server.

<i>Options</i>	
Animation	Sets what kind of animation to use between two images
Duration	Sets how long each image is displayed before changing
URL	Enter valid URLs for the images you want in the slideshow

Each image URL is added to a list. Use the arrows to change the order of the slides and the cross to delete them from the list.

6.11.5.10 Countdown Widget

The countdown widget can be used to count down to important events. When the countdown reaches zero, it turns red and starts counting up.

<i>Options</i>	
Title	Optional title text which will be displayed above the countdown
Deadline	Sets what date and time to count down to

6.11.5.11 Graphics Widget

The graphics widgets can display diagrams from the Graphics View.

<i>Options</i>	
Diagram	Sets which Graphics View diagram to display

6.11.5.12 Stream View Widget

The stream view widget shows the VBC Stream View.

<i>Options</i>	
Stream group	Sets if the widget displays all stream, or only streams in the selected stream group



6.11.5.13 Redundancy Widget

The redundancy widget displays the redundancy status from probes with a redundancy card.

Options

Probe	Set which probe to display redundancy status from
--------------	---

6.11.5.14 MicroTimeline Widget

The MicroTimeline widget shows the four day status of a single channel.

Options

Channel	Select a channel to display alarm history for
----------------	---

Show status border	Add a colored border that reflects the VBC alarms status for selected channel
---------------------------	---

6.11.5.15 OTT Graph Widget

The OTT graph widget shows the OTT alarm history for one channel.

Options

Channel	Select a channel to display alarm history for
----------------	---

Profile	If multiple profiles are available, you can select one
----------------	--

Show status border	Add a colored border that reflects the VBC alarms status for selected channel
---------------------------	---

6.11.5.16 OTT Status Widget

The OTT status widget shows the alarm history and OTT profile status for all OTT channels.

Options

Blade	Select a blade to show channels from, or “All blades” for every channel
--------------	---

Filter	Filter list of channels to only show channels which include this in the name
---------------	--

History	Set what retention you want for the history graphs
----------------	--

Min. severity	Filter away channels without at least this alarm severity in the selected history
----------------------	---

6.11.5.17 Constellation Widget

The constellation widget shows a constellation diagram for a single interface from a probe with one or more RF cards.

Options

Interface	Set which interface to show the constellation diagram for
------------------	---

6.11.5.18 RF Data Widget

The RF data widget shows RF data for a single interface from a probe with one or more RF cards.



Options

Interface	Set which interface to show the RF data for
------------------	---

6.11.5.19 Map Widget

The map widget shows the VBC Map view with all your blades

6.11.5.20 Canvas Control Widget

The canvas control widget is an interactive widget meant for a tablet or PC browser. It lets you control what canvas is shown on a given device.

Options

Device	Select which device this widget controls
---------------	--

Canvas	Select which canvases are available for selection
---------------	---

6.11.5.21 Tag Control Widget

The tag control widget is an interactive widget meant for a tablet or PC browser. It lets you control if canvases or widgets tagged with a single tag should be visible or hidden. This is an alternative to the way of changing tag visibility described in **RDW — Tags**.

Options

Tag	Select which tag this widget controls
------------	---------------------------------------

Show text	What label to use on the show button
------------------	--------------------------------------

Hide text	What label to use on the hide button
------------------	--------------------------------------



6.12 Equipment

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDW

RDW

EQUIPMENT

ALARM SETUP

TIMELINE

REPORTS

EXT. REPORTS

MAIN

Equipment view

Standard

RF cards

License

Resource

Other

Filter

☐ Enabled
☐ Disabled
☐ Probes
☐ Extractors
☐ Unassigned

#	Enabl...	Site	Name	Type	Ver	IP address	Protocol	SW-version	Co...	
1	☒	HLS QoS (VB120)	VB120	VB120	4	10.0.205.193	HTTP	5.6.0-3-118-g0...	View	Edit
2	☒	VB120-VB262	VB262	VB220	4	10.0.205.41	HTTP	5.6.0-3-118-g0...	View	Edit
3	☒	VB220-VB272	VB272 DVB S-S2	VB220	4	10.0.205.200	HTTP	5.6.0-3-118-g0...	View	Edit
4	☒	VB220-VB252-252	VB252	VB220	4	10.0.205.120	HTTP	5.6.0-3-118-g0...	View	Edit
5	☒	VB220-VB242-256	ASI-COFDM	VB220	4	10.0.205.223	HTTP	5.6.0-3-118-g0...	View	Edit
6	☒	DASH QoS (VB220)	OTT-VB220	VB220	4	10.0.205.93	HTTP	5.6.0-3-118-g0...	View	Edit
7	☒	MicroVB-MDC	MDC Demo	MDC		51.15.36.0	HTTPS	4.1BETA13	View	Edit
8	☒	MicroVB-MDC	MDC Idle	MDC		163.172.169.248	HTTPS	n/a		Edit
9	☒	VB273	VB273 Redundant	VB220	4	10.0.205.228	HTTP	5.6.0-3-118-g0...	View	Edit
10	☒	VB288	VB288	VB288	288	10.0.205.77	HTTPS	5.6.0-5	View	Edit
11	☒	MCR	ARCHIVE	Archive	45	10.0.205.234	HTTP	6.0.0-RC1	View	Edit
12	☒	VB330	Core	VB330	100	10.0.205.104	HTTP	5.6.0-3-118-g0...	View	Edit
13	☒	VB50	VB50	VB50	4	10.0.205.27	HTTP	5.6.0-3-118-g0...	View	Edit
14	☒	VB330	VB330 - L2TPenc	VB330	100	10.0.205.14	HTTP	5.6.0-4	View	Edit
15	☒	DVB-T2	VB252-T2	VB120	4	10.0.205.216	HTTP	5.6.0-3-118-g0...	View	Edit
16	☒	VB243	VB243	VB220		10.150.100.224	HTTP	n/a		Edit
17	☒	VB330	VB330 SW	SWProbe		10.0.205.9	HTTP	n/a		Edit
18	☒	VB440 test	VB440	VB440	440	185.102.108.142	HTTPS	6.0.1-1-709-g9...	View	Edit
19	☒	VB330	VB330-Redundant	VB330	100	10.150.100.226	HTTP	5.6.0-3-118-g0...	View	Edit
20	☒	QTT QoS (VB288)	QTT Extractor	VB288	288	10.150.0.167	HTTP	5.6.0-3-55-g01...	View	Edit
21	☒	[Unassigned]	Thomas thumbs	MDC		10.0.30.88	HTTP	n/a		Edit
22	☒	QTT Manager	QTT manager	Custom		10.150.0.171	HTTP	n/a		Edit
23	☒	[Unassigned]	device1	VB20	4	10.0.30.220	HTTP	5.6.0-3	View	Edit
24	☒	V6.0 RELEASE	VB330 SW v6.0	VB330	86	10.0.205.9	HTTP	6.0.0-RC4	View	Edit
25	☒	V6.0 RELEASE	VB440 v6.0	VB440	440	185.102.108.142	HTTPS	6.0.1-1-709-g9...	View	Edit
26	☒	ATest	ATest1	VB288		10.0.205.55	HTTP	n/a		Edit
27	☒	ATest	ATest2	VB288		10.0.205.56	HTTP	n/a		Edit
28	☒	ATest	ATest3	VB288		10.0.205.57	HTTP	n/a		Edit
29	☒	ATest	ATestApp1	SWProbe		10.110.1.75	HTTP	n/a		Edit
30	☒	ATest	ATest4	VB288		10.0.205.58	HTTP	n/a		Edit
31	☒	ATest	ATest5	VB288		10.0.205.59	HTTP	n/a		Edit
32	☒	ATest	ATest6	VB288		10.0.205.60	HTTP	n/a		Edit
33	☒	ATest	ATest7	VB288		10.0.205.61	HTTP	n/a		Edit
34	☒	ATest	ATest8	VB288		10.0.205.62	HTTP	n/a		Edit
35	☒	ATest	ATest9	VB288		10.0.205.63	HTTP	n/a		Edit
36	☒	ATest	ATestApp2	SWProbe		10.110.7.1	HTTP	n/a		Edit
37	☒	ATest	ATestApp3	SWProbe		10.110.7.2	HTTP	n/a		Edit

Add new device

Delete selected devices

Edit selected devices

Export...

The **Equipment** view lists important properties for all the devices that the user has access to. It also provides a convenient way for the user to view each device's configuration and software version.

Various equipment can be added to the VBC Controller and used for monitoring the system. The different probe models and the VB288 can be added and used for monitoring the RF, IP and OTT signals. For systems deploying microVB units the Micro Device Controller (MDC) server can be added to the VBC equipment list. An archive server can be added to archive data for up to 3 months and provide timelines. For large systems it is also possible to nest other VBC servers inside a VBC as described in **Master VBC**.

The *admin* user also add, edit and delete devices, as well as distribute configurations to several devices and perform batch software upgrades of probes and extractors.

For each device the following information is available:

<i>Standard</i>	
#	The table list number
Enabled	If this table entry is checked the device is enabled in the VBC



Site	The name of the site that a device is assigned to. Note that a single device may be assigned to several sites
Name	The name of the device, as specified by the admin user when adding a device to a site
Type	Type of device (for instance 'VB120' or 'VB288')
Ver	The hardware version for this device, where available
IP address	The device's IP address
Protocol	The protocol used to connect to this device (HTTP or HTTPS)
SW-version	The software version of the device
Config	The device's configuration can be viewed by clicking its View link. The configuration XML file may be saved for back-up and copying purposes
<i>RF cards</i>	
Slot 1	The RF card present in slot one, if available
Board serial slot 1	Serial number for the RF card present in slot one, if available
Slot 2	The RF card present in slot two, if available
Board serial slot 2	Serial number for the RF card present in slot two, if available
<i>License</i>	
HW Key or System ID	The hardware key (hardware devices) or system ID (software devices); used to attach a license to the device
License text	A textual representation of the devices' current license options. If the text is too long to be displayed in the table cell, hover over the cell with your cursor to display the full string
<i>Resource</i>	
Uptime	Time since device started
NTP sync	Whether the device is syncing against a time-server
Time	Current device time
Temp	Device's temperature in Celsius
Disk free	Current amount of disk free
Min df	Minimum ever disk free (since power on)
Ram free	Current amount of free memory
Min rf	Minimum ever free memory (since power on)
SD free	Available space on flash card (if equipped with one); for software probes with the flash option, the amount of free space on the storage partition
<i>Other</i>	
Description	Description/Name as specified on device
Location	Location as specified on device
Serial	Serial number of device
Maintenance ends	Date the software maintenance ends
Maintenance left	Remaining time for software maintenance

A number of check box filtering options allow the user to view only selected devices in the equipment list,



the alternatives are: **Enabled**, **Disabled**, **Probes**, **Extractors** and **Unassigned**.

Note that auto-detected devices show up in the list as *unassigned*.

The *admin* user has more options in the **Equipment** page than regular users. In addition to viewing configurations and software versions the *admin* can add, edit and delete devices, as well as distribute configurations to several devices and perform batch software upgrades of probes and extractors.

Click the **Add new device** button to manually add a device to the equipment list. This will open the **Edit device** pop-up view.

Select an existing device and click **Edit selected devices** to open the **Edit device** view described below. Make changes to the device as appropriate and click the **Apply changes** button. It is also possible to edit multiple devices by selecting several devices at once.

Selecting one or more existing devices and clicking the **Delete selected devices** button will delete the device(s).

6.12.1 Equipment — Edit device

Parameter	Value	Description
IP address	10.0.205.120	A device is identified by its IP address
Name	VB258	The name describes the device to the user
Protocol	HTTP	HTTP (clear) or HTTPS (encrypted)
Port	80	This port is the WEB traffic port, usually 80
Site	VB220 - VB258	The site that this device is part of
Type	VB220(probe)	The type of device
URL		For custom devices this URL is used
Location	58.968817, 5.729088	Specify as latitude,longitude
Password		Specify probe's admin password if authentication is used
Enabled	☒	Disabled devices are inactive inside VBC
Syslog forward	☒	Enable forwarding alarms and events to syslog

Note that the same device may be added to more than one site. This is achieved by adding a new device with the same IP address.

☐ Fetch device name

Close Apply changes

Edit device

IP address	The device IP address
Name	Type a device name that will be used throughout the VBC user interface
Protocol	Select whether to use HTTP (clear) or HTTPS ² (encrypted) when connecting to the device
Port	Define the port to be used for the web traffic, normally 80 for HTTP and 443 for HTTPS

²HTTPS is supported in software version 5.3 and later



Site	Select the site that the device should be associated with. In some cases, it may be useful to add one device to multiple sites. This can be done in by creating several device entries with the same IP address and port
Type	Select the type and model of the device from the drop-down menu
URL	When a device of type Custom has been selected, it is possible to define a URL to access this device's GUI
Location	By entering the geographical location of the blade here, it will be visible in the Map view. The location is entered as decimal degrees latitude and longitude, comma-separated, with positive numbers indicating north and east, respectively
Password	If the device has been configured to use a password in Setup — Security — Authentication , provide the password for the 'admin' user of the device here to allow the VBC to access it
Enabled	If this checkbox is disabled, the device will not be active within the VBC GUI
Syslog forward	If this checkbox is enabled, the blade alarms and SCTE 35 events (if the probe has SCTE 35 enabled) will be forwarded to the VBC's syslog. Refer to G Appendix: Syslog forwarding for examples on how to integrate with an external syslog facility.
Fetch device name	If you check this checkbox, the VBC will update the Name field from the name configured on the device. This checkbox is automatically reset after use. To set the name of the connected devices from the names configured in this view, please use the General — Sync view.

When the new device has been defined, click the **Apply changes** button. Click the **Close** button to close the pop-up view.

Use the **Export...** button to create an XML report file listing all the devices.



6.12.2 Equipment — Management

LOGIN	Device configuration management:
LIVE	Copy settings between devices of same type
MONITORING	Copy stream list between any devices
BLADE ALARMS	Manual configuration file management:
GRAPHICS VIEW	Import configuration file
STREAM VIEW	Upload imported configuration file to devices
THUMBS VIEW	Device software and license management:
SERVICE VIEW	Import device software image
MAP	Upload software to devices
RDP	Upload licenses to devices
RDW	Manage files:
EQUIPMENT	Manage uploaded software and configuration files
MANAGEMENT	
ALARM SETUP	
TIMELINE	
REPORTS	
EXT. REPORTS	
MAIN	
◀	

The **Equipment — Management** view makes it possible to copy configuration between the connected devices and perform software upgrades.

Device configuration management — Copy settings between devices of same type

Copy settings between devices

STEP 1: Select source device

Source device VB120(10.0.205.193,probe) ▼

STEP 2: Select destination device(s)

Device	IP address	Sel	Status
VB120	10.0.205.193	☐	
VB262	10.0.205.41	☐	
VB272 DVB S-S2	10.0.205.200	☐	
VB252	10.0.205.120	☒	
ASI-COFDM	10.0.205.223	☐	
OTT-VB220	10.0.205.93	☐	
VB273 Redundant	10.0.205.228	☐	
Core	10.0.205.104	☐	
VB50	10.0.205.27	☐	
VB330 - L2TPenc	10.0.205.14	☐	
VB252-T2	10.0.205.216	☐	
VB440	185.102.108....	☐	
VB330-Redundant	10.150.100.2...	☐	
device1	10.0.30.220	☐	
VB330 SW v6.0	10.0.205.9	☐	

Select all Clear all

STEP 3: Click the following link to generate list of compatible sections

Update list of available sections

There are 27 sections available

STEP 4: Select sections that are to be copied - only compatible sections listed

Section	Sel	
Scheduling templates	☐	View
ETR thresholds	☐	View
PID thresholds	☐	View
Service thresholds	☐	View
VBC thresholds	☐	View
Ethernet thresholds	☒	View
Auto thresholds	☐	View
ASI 1 Setup	☐	View
Full Service Monitoring	☐	View
Alarms	☐	View
Multicasts	☐	View
Page names	☐	View

Select all Clear all

STEP 5: Click the following link to copy selected sections to selected devices

Copy selected sections

Clicking this link will open the **Copy settings between devices** pop-up view. The process of copying settings between devices involves five steps:



1. Select source device
2. Select one or more destination devices
3. Click the **Update list of available selections** link
4. Select the groups of settings that should be copied
5. Perform the actual copying by clicking the **Copy selected sections** link

The VBC will determine which settings are compatible between devices and update the selection list accordingly.

Device configuration management — Copy stream list between any devices

Copy stream lists

Source device: VB120(10.0.205.193,probe) ▼

Destination device(s)

Device	IP address	Sel	Status
VB120	10.0.205.193	☐	
VB262	10.0.205.41	☐	
VB272 DVB S-S2	10.0.205.200	☐	
VB252	10.0.205.120	☐	
ASI-COFDM	10.0.205.223	☐	
OTT-VB220	10.0.205.93	☐	
MDC Demo	51.15.36.0	☐	
VB273 Redundant	10.0.205.228	☒	
VB288	10.0.205.77	☐	
ARCHIVE	10.0.205.234	☐	
Core	10.0.205.104	☐	
VB50	10.0.205.27	☐	
VB330 - L2TPenc	10.0.205.14	☐	
VB252-T2	10.0.205.216	☐	
VB440	185.102.108...	☐	
VB330-Redundant	10.150.100....	☐	
QTT Extractor	10.150.0.167	☐	
Thomas thumbs	10.0.30.88	☐	
QTT manager	10.150.0.171	☐	
device1	10.0.30.220	☐	
VB330 SW v6.0	10.0.205.9	☐	

[Copy Ethernet Streamlist to selected devices](#)

Clicking this link will open the **Copy stream lists** pop-up view.

The stream (multicast) list is compatible between probes and extractors, and it is therefore possible to freely copy this list between these types of devices. Select source device and one or more destination devices and click the **Copy Ethernet streamlist to selected devices** link. Note that multicast join information is not included in this copying process.

The status of the copying process can be viewed in the Status field. Clicking the **View** link will open a pop-up view providing additional status information.



Manual configuration file management — Import configuration file

Clicking this link will open the **Import configuration file** pop-up view. The config file can either be downloaded from another probe and uploaded without change or have been manually edited as described on the next page. Select the configuration XML file to be imported and click the **Go!** button.

Manual configuration file management — Upload imported configuration file to devices

Clicking this link will open the **Upload imported configuration file to devices** pop-up view.

Select the configuration file to be uploaded and select the destination devices. Click the **Upload configuration file to selected devices** link to perform the configuration upload. The status of the upload process can be viewed in the Status field. Clicking the **View** link will open a pop-up view providing additional status information.



Device	IP address	Sel	Status
VB120	10.0.205.193	☐	
VB262	10.0.205.41	☐	
VB272 DVB S-S2	10.0.205.200	☐	
VB252	10.0.205.120	☐	
ASI-COFDM	10.0.205.223	☐	
OTT-VB220	10.0.205.93	☐	
MDC Demo	51.15.36.0	☐	
VB273 Redundant	10.0.205.228	☐	
VB288	10.0.205.77	☐	
ARCHIVE	10.0.205.234	☐	
Core	10.0.205.104	☐	
VB50	10.0.205.27	☐	
VB330 - L2TPenc	10.0.205.14	☐	
VB252-T2	10.0.205.216	☐	
VB440	185.102.108...	☐	
VB330-Redundant	10.150.100...	☐	
QTT Extractor	10.150.0.167	☐	
Thomas thumbs	10.0.30.88	☐	
QTT manager	10.150.0.171	☐	
device1	10.0.30.220	☐	
VB330 SW v6.0	10.0.205.9	☐	

Manually editing the configuration

It is possible to manually edit an XML configuration file. Use a valid configuration file (by clicking a **View** link of the **Equipment view**) and save it locally. Edit the file and make appropriate changes before saving it. Any CRC attribute in line 2 of the config file must be removed (i.e. remove text similar to `crc="b8a1fa3f"`). Import the file from the **Import configuration file** view. The file will then become selectable in the **Upload imported configuration file** pop-up view.

Note: Please make sure that the structure of the XML is not corrupted when manually editing the file. Any syntax errors in the file will cause errors when the file is imported to the devices.

Device software and license management — Import device software image

The simplest way of performing a software upgrade of probes and extractors is by importing a software file (with .tea or .tea2 extension) via the **Import device software image** pop-up view and then selecting the corresponding file from the drop-down selection list in the **Upload software to devices** pop-up view.

Import probe or extractor software file

Choose file No file chosen

Go!

Importing software allows admin to upload software to selections of devices in parallel.
Device software files have .tea or .tea2 extensions.
Software images are located under the /opt/btech/vbc/configs/vb2_software folder.



Clicking this link will open the **Import device software image** pop-up view. Select the required software file and click the **Go!** button. Software images for VB1, VB2, VB3, VB288 and Software Probe, as well as timezone definitions, can all be imported using this dialog. Software files have *.tea* or *.tea2* extensions.

When the software file has been successfully imported, it will become available as a selection in the drop-down selection menu in the **Upload software to devices** pop-up view.

An alternative to importing a software file is to copy the software file directly to the `/opt/btech/vbc/configs/vb2_software` folder on the VBC server. This is typically achieved using the **scp** command in a terminal shell. The software file will then become available for selection.

Device software and license management — Upload software to devices

Device	IP address	Sel	Status
VB120	10.0.205.193	☐	
VB262	10.0.205.41	☐	
VB272 DVB S-S2	10.0.205.200	☐	
VB252	10.0.205.120	☐	
ASI-COFDM	10.0.205.223	☐	
OTT-VB220	10.0.205.93	☐	
VB273 Redundant	10.0.205.228	☐	
VB50	10.0.205.27	☐	
VB252-T2	10.0.205.216	☐	
device1	10.0.30.220	☐	

Clicking this link will open the **Upload software to devices** pop-up view. Software image files previously imported from the **Import device software image file** pop-up view will be available for selection in the drop-down selection menu. Software image files located in the `/opt/btech/vbc/configs/vb2_software` folder will also be selectable.

The upgrade procedure will use the protocol and credentials configured in the **Edit device** view. When upgrading from a software version prior to 5.4, this requires access control to be disabled during the upgrade process, which is configured in the **Setup — Login** view in the probe or VB288.

For older hardware probes, you have to select between using HTTP – this requires access control to be disabled during the upgrade process, which is configured in the **Setup — Login** view – or a procedure based on FTP and telnet – this requires the corresponding protocols to be enabled in the **Setup — Security** view of the probe and to be allowed in the network (not being blocked by firewalls etc.).



If the access control or security settings of the target device is blocking the update, you will need to use the stand-alone software upgrade procedure as described in the User's Manual of the specific product.

Select a software image from the menu and select one or more destination devices. Click the **Software upgrade selected devices** link to perform the upgrade. The status of the upgrade process can be viewed in the Status field. Clicking the **View** link will open a pop-up view providing additional status information.

Do not power off devices that are being software upgraded. If a device is powered off during software upload it will need special service to recover.

Upgrading to a new major release requires a valid software maintenance license, please refer to K Appendix: Software Maintenance for more details. If the current software maintenance license does not cover the uploaded software version, the upgrade will be aborted and the current version is kept.

Click the **Clear status** link to clear the software upload status fields.

Device software and license management — Upload licenses to devices

Upload licenses to devices [X]

Upload licenses to devices

Select license key XML to import to devices:

No file chosen

This dialog can import license XML files exported from a device, or license XML files obtained from your dealer. The uploaded license keys will be submitted to the devices immediately after upload, as long as the device is enabled in the Equipment view, and can be reached by VBC.

Clicking this link will open the **Upload licenses to devices** pop-up view. Software licenses can be distributed as XML files, which can be imported using this dialog, if the licensed device is known by the VBC.

Select the required license XML file and click the **Go!** button to import the licenses. Once uploaded, the VBC will start uploading the license or licenses to the devices.

License files exported from a probe or an VB288 using the **About — License** or **Data — Configuration** views may also be imported using this dialog. This can be useful to recover a license after a factory reset.



Manage files — Manage uploaded software and config files

Manage uploaded software and configuration files

Files uploaded by users

Sel	File	Type	Size	Date
☐	eth_streamlist_ex (7).xml	Config file	86K	2018 Oct 30 09:29:38
☐	330_full_config.xml	Config file	247K	2019 Dec 11 11:26:15
☐	Probe_hw4____hw4gbprobe-550-4-03May19.tea	Probe software	17283K	2019 Jun 28 10:26:48
☐	Probe_hw4____hw4gbprobe-550-6-28Aug19.tea	Probe software	17185K	2019 Sep 4 16:18:35
☐	Probe_hw4____hw4gbprobe-560-0-28Feb20.tea	Probe software	17440K	2020 Feb 28 16:10:22
☐	Probe_hw4____hw4gbprobe-560-1-23Mar20.tea	Probe software	17457K	2020 Mar 25 08:23:26
☐	Probe_hw4____hw4gbprobe-560-2-04Mar20.tea	Probe software	17477K	2020 May 6 14:21:16
☐	Probe_hw4____hw4gbprobe-560-3-17Jun20.tea	Probe software	17179K	2020 Jun 18 15:19:36
☐	Probe_hw4____hw4gbprobe-560-3-118-g048c306082-31Aug20.tea	Probe software	17115K	2020 Aug 31 15:20:25
☐	Extractor_pc____vb288-550-4-03May19.tea	Extractor software	28605K	2019 May 3 14:59:46
☐	Extractor_pc____vb288-560-0-28Feb20.tea	Extractor software	29596K	2020 Feb 28 16:10:11
☐	Extractor_pc____vb288-560-1-23Mar20.tea	Extractor software	29608K	2020 Mar 25 08:23:14
☐	Extractor_pc____vb288-560-2-04May20.tea	Extractor software	29621K	2020 May 6 14:22:15
☐	Extractor_pc____vb288-560-3-17Jun20.tea	Extractor software	29628K	2020 Jun 18 15:20:34
☐	Extractor_pc____vb288-560-3-118-g048c306082-31Aug20.tea	Extractor software	29760K	2020 Aug 31 15:20:07
☐	10GProbe_hw10g____10gbprobe-550-4-03May19.tea	10G probe SW	15810K	2019 May 3 14:59:32
☐	10GProbe_pc____swprobe-550-4-03May19.tea	10G probe SW	16212K	2019 May 3 14:59:40
☐	10GProbe_pc____swprobe-560-0-28Feb20.tea	10G probe SW	21040K	2020 Feb 28 16:10:01
☐	10GProbe_hw10g____10gbprobe-560-0-28Feb20.tea	10G probe SW	16213K	2020 Feb 28 16:10:27
☐	10GProbe_pc____swprobe-560-1-23Mar20.tea	10G probe SW	21112K	2020 Mar 25 08:22:55
☐	10GProbe_hw10g____10gbprobe-560-1-23Mar20.tea	10G probe SW	16233K	2020 Mar 25 08:23:42

Delete selected files

Clicking this link will open the **Manage files** pop-up view. Mark files that should be removed from list and click the **Delete selected files**. Deleted files will no longer be available in drop-down menus throughout the menu system.



6.13 Alarm setup

Alarm setup

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

ALARM SETUP

MESSAGE FWD

SCHEDULING

REPORTS

EXT. REPORTS

MAIN

Alarm setup Alerts

Alarm setup

#	Alarm message	Severity level	Origin	Window	Reset
1	No contact	Fatal (black) ▼	VBC	1	1
2	External site alarm	Major (red) ▼	VBC	1	1
3	No signal	Major (red) ▼	Probe	1	1
4	RTP drops	Error (orange) ▼	Probe	60	5
5	MLR error	Error (orange) ▼	Probe	60	5
6	IAT error	Error (orange) ▼	Probe	60	5
7	Bitrate overflow	Warning (yellow) ▼	Probe	60	5
8	Bitrate underflow	Warning (yellow) ▼	Probe	60	5
9	ETR pri one error	Warning (yellow) ▼	Probe	60	15
10	ETR pri two error	Warning (yellow) ▼	Probe	60	15
11	ETR pri three error	Warning (yellow) ▼	Probe	60	15
12	ETR pri other error	Warning (yellow) ▼	Probe	60	15
13	ETR interface error	Warning (yellow) ▼	Probe	60	15
14	OTT transport error	Error (orange) ▼	Probe	60	5
15	OTT http error	Error (orange) ▼	Probe	60	5
16	OTT xml error	Error (orange) ▼	Probe	60	5
17	System alarm	Major (red) ▼	Probe	1	1
18	Scrambling state	Error (orange) ▼	Extractor	1	1
19	Caption availability	Error (orange) ▼	Probe	60	5
20	Caption quality	Error (orange) ▼	Probe	60	5
21	QoE video	Major (red) ▼	Probe	60	5
22	QoE audio	Major (red) ▼	Probe	60	5
23	Archive Error	Major (red) ▼	Archive	1	1
24	Archive Warning	Error (orange) ▼	Archive	1	1
25	SCTE 35	Major (red) ▼	Probe	60	5
26	QTT error	Error (orange) ▼	QTT manager	1	1

Apply

[Understanding probe alarms](#) [Understanding VBC alarms](#) [Details of the VBC alarm model](#)

In the **Alarm setup** view, the *admin* user can change the severity level for any alarm.

Changing the severity level for alarms will impact the color of bulbs, stream-bars and alarms. The alarm lists present all active alarms sorted on severity, with black alarms top and green alarms bottom. Setting severity level to **OK (green)** will make sure those alarms do not impact bulbs or stream bars but they will still be present in the alarm lists.

The severity level is also used for the SNMP alarm list and traps.

The alarm setup view also allows the *admin* user to configure the alarm window and alarm reset time for each VBC alarm.

An overall system controller like the VBC Controller should not raise instantaneous alarms, as this for a large system might lead to a multitude of alarms toggling on and off, leading to an untidy user interface difficult to interpret. VBC alarms are therefore based on error second measurements summed over an alarm window period (sliding window). When the number of error seconds counted over the alarm window period exceeds the user-defined threshold for that alarm type the VBC will raise an alarm. The



alarm window and alarm reset time for 'No contact', the VB288 Objective QoE Content Extractor alarms and the Archive server alarms are fixed at 1 minute alarm windows. The default alarm window period is 1 minute for 'No signal' and 60 minutes for remaining alarms.

The alarm reset period is the number of consecutive minutes, without any new error seconds, needed to clear an active alarm.

Clicking the document links will open guides describing how to set thresholds for probes and the VBC. It is highly recommended to read these in order to correctly configure the alarm thresholds and alarm windows.

Alerts

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

ALARM SETUP

MESSAGE FWD

SCHEDULING

REPORTS

EXT. REPORTS

MAIN

Alarm setup

Alerts

#	Alarm message	Alert	Severity	Origin	Description
1	No contact	☒	Fatal	VBC	Activated if probe cannot be reached by VBC
2	External site alarm	☐	Major	VBC	Child VBC has active alarm for site
3	No signal	☐	Major	Probe	Activated if too much signal loss
4	RTP drops	☐	Error	Probe	Activated if too much RTP drops
5	MLR error	☐	Error	Probe	Activated if too much transport stream packet loss
6	IAT error	☐	Error	Probe	Activated if too much IP packet jitter
7	Bitrate overflow	☐	Warning	Probe	Activated if bitrate is too high
8	Bitrate underflow	☐	Warning	Probe	Activated if bitrate is too low
9	ETR pri one error	☐	Warning	Probe	Activated if too much ETR priority 1 errors
10	ETR pri two error	☐	Warning	Probe	Activated if too much ETR priority 2 errors
11	ETR pri three error	☐	Warning	Probe	Activated if too much ETR priority 3 errors
12	ETR pri other error	☐	Warning	Probe	Activated if too much ETR extended tests errors
13	ETR interface error	☒	Warning	Probe	Activated if too much ETR interface errors
14	OTT transport error	☐	Error	Probe	Activated if OTT transport fails
15	OTT http error	☐	Error	Probe	Activated if OTT HTTP connection errors
16	OTT xml error	☐	Error	Probe	Activated if errors in manifest files etc
17	System alarm	☒	Major	Probe	A device is experiencing an active system alarm
18	Scrambling state	☐	Error	Extractor	A stream has an unexpected clear/scrambled status
19	Caption availability	☐	Error	Probe	Caption data not available
20	Caption quality	☐	Error	Probe	Caption data contain errors
21	QoE video	☐	Major	Probe	One or more video content alarms are active
22	QoE audio	☐	Major	Probe	One or more audio content alarms are active
23	Archive Error	☐	Major	Archive	Archive server error
24	Archive Warning	☐	Error	Archive	Archive server warning
25	SCTE 35	☐	Major	Probe	One or more SCTE 35 content alarms are active
26	QTT error	☐	Error	QTT manager	The QTT manager has detected an error

Apply

- Selected alarms may have visual and audible notification subject to user settings
- Web browsers will by default block audio. For desktop and Android devices clicking into the WEB interfaces may enable audio.

In the **Alerts** view, VBC alerts can be enabled for selected VBC alarms. Whenever a new VBC alarm is raised with the Alert flag enabled, the alarm will trigger the following response in the web browser:

- The screen will flash 3 times (provided visual alerts are enabled for the current user)
- An alarm sound will play (provided audible alerts are enabled for the current user)

Note that autoplay of audio (and video) is disabled in modern web browsers, and the ability to play audio from applications varies and may be changing.



On Windows, macOS and Linux, Google Chrome has been found to be working after clicking into the GUI. Audio alerts may be muted when the VBC interface is running in the background. To enable audio for the VBC application in Google Chrome, click the lock icon next to the URL field in the web browser, select **Site settings**, and set **Sound** to *Allow*.

The iPad browser seem to block this kind of audio regardless of settings.

6.13.1 Alarm setup — Message Fwd

The VBC allows the *admin* to customize how alarms are to be generated and forwarded to 3rd party systems, either by SNMP or by email.

Alarms to forward

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

ALARM SETUP

MESSAGE FWD

SCHEDULING

TIMELINE

REPORTS

EXT. REPORTS

MAIN

Alarms

SNMP traps

Email setup

#	Alarm message	Forward	Email group	Severity	Origin	Description
1	No contact	☒	Do not forward	Fatal	VBC	Activated if probe cannot be reached by VBC
2	No signal	☒	Do not forward	Major	Probe	Activated if too much signal loss
3	RTP drops	☒	Do not forward	Error	Probe	Activated if too much RTP drops
4	MLR error	☒	Do not forward	Error	Probe	Activated if too much transport stream packet loss
5	IAT error	☒	Do not forward	Error	Probe	Activated if too much IP packet jitter
6	Bitrate overflow	☒	Do not forward	Warning	Probe	Activated if bitrate is too high
7	Bitrate underflow	☒	Do not forward	Warning	Probe	Activated if bitrate is too low
8	ETR pri one error	☒	Do not forward	Warning	Probe	Activated if too much ETR priority 1 errors
9	ETR pri two error	☒	Do not forward	Warning	Probe	Activated if too much ETR priority 2 errors
10	ETR pri three error	☒	Do not forward	Warning	Probe	Activated if too much ETR priority 3 errors
11	ETR pri other error	☒	Do not forward	Warning	Probe	Activated if too much ETR extended tests errors
12	ETR interface error	☒	Do not forward	Warning	Probe	Activated if too much ETR interface errors
13	Freeze frame	☒	Do not forward	Error	Extractor	Video has been detected as frozen
14	OTT transport error	☒	Do not forward	Error	Probe	Activated if OTT transport fails
15	OTT http error	☒	Do not forward	Error	Probe	Activated if OTT HTTP connection errors
16	OTT xml error	☒	Do not forward	Error	Probe	Activated if errors in manifest files etc
17	OTT alignment	☒	Do not forward	Error	Extractor	OTT profiles are unaligned
18	Archive Error	☒	Do not forward	Major	Archive	Archive server error
19	Archive Warning	☒	Do not forward	Error	Archive	Archive server warning
20	External site alarm	☒	Do not forward	Major	VBC	Child VBC has active alarm for site
21	System alarm	☒	Do not forward	Major	Probe	A device is experiencing an active system alarm
22	Scrambling state	☒	Do not forward	Error	Extractor	A stream has an unexpected clear/scrambled status
23	Caption availability	☒	Do not forward	Error	Probe	Caption data not available
24	Caption quality	☒	Do not forward	Error	Probe	Caption data contain errors
25	QoE video	☒	Do not forward	Major	Probe	One or more video content alarms are active
26	QoE audio	☒	Do not forward	Major	Probe	One or more audio content alarms are active

Apply

Only selected alarms are forwarded as SNMP traps.

Only those alarms that have **SNMP forwarding** checked will be part of the VBC's SNMP alarm list and thus forwarded as traps. When the **Monitoring** alarm list is updated, the SNMP alarm list is also updated if:

1. The alarm type has been selected for SNMP forwarding
2. The site that reports the alarm matches the selection in *Site to use for SNMP alarms* (selected in the **Alarm setup — Message fwd — SNMP Traps** view)

When the SNMP settings have been changed, the *admin* may want to rebuild the SNMP alarm list completely to get rid of alarms that are no longer relevant. This can be achieved by selecting *Clear* in the *Clear alarm lists* frame in the **Main — General** view.



The VBC's alarm MIB describes all the details of the trap and alarm lists formats. The MIB can be obtained from your Bridge Technologies reseller. The SNMP alarm list is only available through the SNMP MIB.

Alarms can also be forwarded by email to pre-defined email groups. Define email groups using the **Email setup** tab, and select the groups that are to receive the alarm in the **Email group** column of the specific alarm.

One email will be sent per the VBC alarm. Alarm aggregation is not performed for the email alarms. It is possible to also include the blade alarms from the device causing the alarms in the email - this will contain more specific information about the alarms than what the VBC alarms does.

SNMP Traps

Alarms

SNMP traps

Email setup

SNMP alarms
Site to use for SNMP alarms <all sites>
Enable trap aggregation ☒
Parameterize trap text ☒
Community string
Year in trap time ☐
Trap dest 1:
Trap dest 2:
Trap dest 3:
Trap dest 4:

Apply

- Specify trap destinations different from 0.0.0.0 to forward traps.
- When selecting another site to use for SNMP alarms, select **Clear alarm lists** in the **General** menu to rebuild alarm-list.
- Check **Enable trap aggregation** to avoid getting too many simultaneous SNMP traps.

Sometimes it is desirable to switch off alarm aggregation for the SNMP traps in order to get more precise alarms. The drawback is that during alarm storms the VBC will end up sending hundred of traps instead of just a dozen.

Consider the case where there is one site with one probe monitoring 100 streams and there is a signal loss for all streams. If *Enable trap aggregation* is disabled there will be one trap per stream of the format "Sitename:Bladename No signal streamname". If *Enable trap aggregation* is enabled there will only be only one alarm with format "Sitename:Bladename No signal Streams:100". Thus enabling trap aggregation reduces the number of traps from 100 to 1 in this case.

User properties

Site to use for SNMP alarms	Select which sites should generate alarm traps. By default all sites will be selected
Enable trap aggregation	Select if traps should be aggregated



Parameterize trap text	When the Parameterize trap text check-box is ticked the VBC SNMP traps will be parameterized. Refer to separate documentation on trap text format
Community string	The VBC SNMP community string can be changed
Year in trap time	If enabled, dates in SNMP traps include the year number
Trap dest 1–4	The IP address of the trap destination

By default the SNMP agent address is 127.0.0.1. The agent address can be changed in two ways:

1. Adding an entry for the VBC server in the server's own `/etc/hosts` file, for example adding the line `10.20.30.40 vbcserver` where 10.20.30.40 is the IP address to be used and vbcserver is the hostname of the VBC server.
2. Specifying the IP address of the agent directly when the `log_splitter` process is started. This is achieved by adding `-i 10.20.30.40` as args to the `log_splitter` process.

To do this, run `sudo systemctl edit vbc.log_splitter.service` from the command-line prompt and add these lines:

```
[Service]
ExecStart=
ExecStart=/opt/btech/vbc/bin/log_splitter -l 0 -p 161 -i 10.20.30.40
```

For both 1) and 2) the VBC needs to be restarted after applying the change by running **`systemctl restart vbc.log_splitter`**



Email setup

Alarms	SNMP traps	Email setup
--------	------------	--------------------

Email groups

Name	Recipient list	Comments
Alarm Group	example@mail.com	
Alarm group2	alarm@example.com	Development

Email Groups: 2

Protocol settings

Postpone mail send (sec):

Number of attempts:

Mail send interval (ms):

Mail max age (sec):

The **Email setup** view lists the email recipients can be set up to receive SNMP alarms. The email recipients are configured on this page and then selected on the **Alarms** tab.

A number of global parameters can be configured:

Protocol settings	
Postpone mail send (sec):	Number of seconds to wait after alarm status has changed before sending email. A value of 180 should ensure that relevant blade-alarms are included (if they have been enabled for the email group).
Number of attempts:	Number of attempts to try to send email before deleting it from the queue.
Mail send interval (ms):	Minimum time between email-sending of alarms – to control network load.
Mail max age (sec):	Delete emails if they have been in the send queue for longer than this time.

Remember to click **Apply** after modifying the global email parameters for the new parameters to take effect.

Click the **Add new** button to add a new email group to the list. This will open the **Edit email group**



pop-up view.

Edit email group [X]

Edit

Group name:

Recipient list:

Description:

Message text:

Add blade alarms ☐

Email group

Group name:	This names the email group so that it can be selected in the recipient drop-down.
Recipient list:	A comma-separated list of recipient email addresses.
Description:	A description of the group.
Message text:	A message to be included in every email.
Add blade alarms:	If checked also relevant blade-alarms will be included in the email, otherwise only VBC alarms are included.

When the new email group has been defined, click the **Apply changes** button. Click the **Close** button to close the pop-up view.

Highlighting an existing email group and clicking **Edit selected** will open the Edit email group pop-up view described above. Make the appropriate changes and click the **Apply changes** button.

Highlighting one or more existing email groups and clicking the **Delete selected** button will delete the email group(s).

The settings for the outgoing email server is configured in **Main — General — Connections — Outgoing mail server** view.

Please note that the alarm emails may end up being caught by spam filters. Please make sure that exception rules are added if needed so that these messages are not classified as spam. A correct mail server setup is needed in order to send out the alarm emails.



6.13.2 Alarm setup — Scheduling

Setup

Overview

Alarm scheduling

Stream	Comments	Enabled	All days	Mon	Tue	Wed	Thu	Fri	Sat	Sun
CANAL+ SPORT EXTRA	Transmission pause	✓	0000-0615,1845-2400							
CANAL+ FAMILY	Transmission pause	✓	0000-0615,1845-2400							
CANAL+ SPORT EXTRA	Pause in Transmission	✓	0000-0605,2300-2400							
DISNEY JUNIOR		✓	0000-0558,2158-2400							
DISNEY JUNIOR		✓	0000-0558,2158-2400							
NASA TV	test		0000-2400							
NICLODEON	Transmission pause	✓	0000-0459,1759-2400							
PLAYHOUSE_DISNEY		✓	0000-0605,2100-2400							
SVT1		✓		1931-1933	1931-1933	1931-1933	1931-1933	1931-1933		
SVT1	Insert of Local News	✓	1954-1956,1959-2003	1954-1956,1959-2003	1954-1956,1959-2003	1954-1956,1959-2003	1954-1956,1959-2003	1954-1956,1959-2003	1954-1956,1959-2003	1954-1956,1959-2003
SVT1	Insert of Local News	✓		0739-0822	0739-0822	0739-0822	0739-0822	0739-0822		
SVT1	Insert of Local News	✓		1708-1728,1747-1749	1708-1728,1747-1749	1708-1728,1747-1749	1708-1728,1747-1749	1708-1728,1747-1749		
SVT1	Insert of Local News	✓		0839-0920	0839-0920	0839-0920	0839-0920	0839-0920		
SVT1	Insert of local news	✓	1914-1916,1929-1931	0705-0708,0709-0711	0705-0708,0709-0711	0705-0708,0709-0711	0705-0708,0709-0711	0705-0708,0709-0711		
SVT1	Local News	✓		1808-1818	1808-1818	1808-1818	1808-1818	1808-1818		
SVT2	Insert of Local News	✓		0709-0719	0709-0719	0709-0719	0709-0719	0709-0719		
TV2_SPORT_4	Stop transmission night	✓	0000-0630							

Streams with alarm scheduling:17

- This page allows editing of **stream** based scheduling. **Service** and **PID** based scheduling are performed on probes.
- Streams with alarm filtering schedules will not generate VBC alarms during the filtered periods.
- Streams that need filtering of individual services or PIDs can do that on the probes (say one service in an MPTS generates alarms certain hours).
- The **Overview** TAB shows all scheduling settings for streams, services and PIDs.

Add new

Edit selected

Delete selected

The VBC scheduling functionality allows alarm masking at stream level during selected time intervals.

Scheduling Setup

In this view the user can define time windows during which alarms for a selected stream will be suppressed by the VBC. This enables alarm masking at times when it is known that a stream would otherwise generate non-relevant alarms, e.g. at times when a stream is not transmitted. Clicking the **Add new** button will open the **Edit alarm scheduling** pop-up view, allowing the user to define a scheduling scheme and associate it with a stream. Existing scheduling schemes may be edited by highlighting it and clicking the **Edit selected** button. A scheme may be deleted by highlighting it and clicking the **Delete selected** button.

The search field in the upper right corner of the view enables filtering on a text string; only list entries matching the specified text string will be visible.

Note that it is possible to associate more than one scheduling scheme for the same stream.

During times when a stream has alarm masking enabled, the stream's MicroTimeline will be colored blue. Note that this applies to VBC stream scheduling only, and not to scheduling performed at probe or extractor level.



Edit alarm scheduling

Edit

Stream

Enable ☒

Comment

Add user comment

Scheduling times

All days

Mon

Tue

Wed

Thu

Fri

Sat

Sun

Specify when alarms are to be filtered (i.e. ignored). Times are specified as hhmm-hhmm and can be comma separated.
Example: 0000-0258,2350-2400

Close

Apply changes

The alarm scheduling applies to the PDF reports as well with the limitation that a complete hour H is completely filtered if H:59 is filtered, otherwise not filtered at all. Hence if alarm scheduling is active at 13:59 for a stream, the report will mask all errors for that stream from 13:00 to 13:59.

The format of the scheduling period string is: HHMM:HHMM, HHMM:HHMM. As an example, masking errors from midnight to 6 in the morning and from 18.00 to 20.00 can be written as this: 0000-0600, 1800-2200.

<i>Parameter</i>	<i>Description</i>
Stream:	The name of the stream for which the scheduling applies
Comments:	A text string providing information about the scheduling scheme
Enabled:	An indication of whether the scheduling scheme is enabled or not
All days:	One or more scheduling periods that apply for all days during a week
Mon – Sun:	One or more scheduling periods that apply for the specified day



Scheduling Overview

Setup

Overview

All scheduling settings

Stream	Interface	Type	SID	PID	Ignore	Probe	Scheduling template	Scheduling
TP 65	SAT1	Pid	-	4176	Missing	10.0.205.200	Always	allDays(0000-2400)
TP 65	SAT1	Pid	-	4177	Missing	10.0.205.200	Always	allDays(0000-2400)
TVNorge HD	ETHERNET	Service	-1	-	All	10.0.205.104	Always	allDays(0000-2400)
TV 2 HD (N)	ETHERNET	Pid	-	0	Missing	10.0.205.104	Always	allDays(0000-2400)
TV 2 HD (N)	ETHERNET	Pid	-	0	Missing	10.0.205.104	Always	allDays(0000-2400)
NASA UHD	ETHERNET	Pid	-	0	Missing	10.0.205.104	Always	allDays(0000-2400)
NASA UHD	ETHERNET	Pid	-	0	Missing	10.0.205.104	Always	allDays(0000-2400)
Blue Hustler	(all)	Stream	-	-	-	(VBC)	-	allDays(0345-2400)
C More Junior	(all)	Stream	-	-	-	(VBC)	-	allDays(0000-07...
C More Kids	(all)	Stream	-	-	-	(VBC)	-	allDays(0000-07...
CANAL+ SPORT ...	(all)	Stream	-	-	-	(VBC)	-	allDays(0000-06...
CANAL+ _FAMILY	(all)	Stream	-	-	-	(VBC)	-	allDays(0000-06...
CANAL+ _SPORT...	(all)	Stream	-	-	-	(VBC)	-	allDays(0000-06...

Ignore empty filters

☒

Refresh

- This page shows all scheduling information entered on VBC (streams) and probes (services and PIDs)
- This page is updated when selecting the **Overview** TAB or when pressing the **Refresh** button. Probe changes are available to this page within two minutes.

This view displays an overview of all scheduled alarm masking defined in probes and the VBC. VBC scheduling applies at stream level, whereas probe scheduling applies at PID or service level.

When **Ignore empty filters** is checked only entries that can mask errors at certain times are included in the list. When this checkbox is not enabled all services and PIDs that are associated with service or PID threshold templates different from *Default* will be present in the scheduling list, irrespective of whether scheduling is actually enabled or not. If no scheduling applies for a service or PID present in the list, the corresponding **Scheduling template** field will read *Never*. Sorting by the **Scheduling template** column (by clicking the column heading) will group the enabled scheduling entries by the name of the scheduling template and may make navigation easier.

The search field in the upper right corner of the view enables filtering on a text string; only list entries matching the specified text string will be visible.

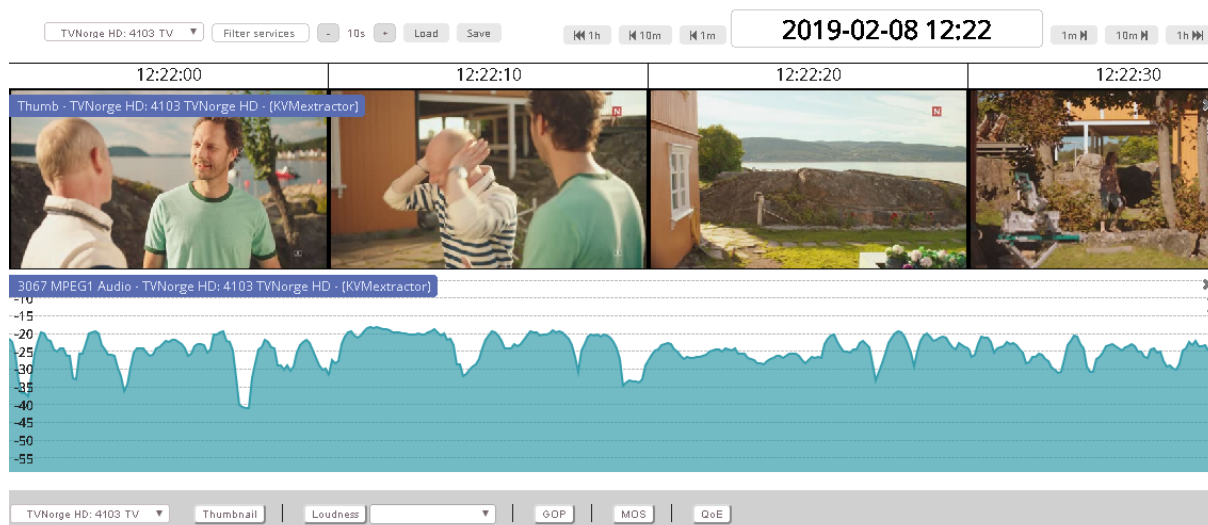
<i>Parameter</i>	<i>Description</i>
Stream:	The name of the stream for which the scheduling applies
Interface:	The probe interface on which the stream is received
Type:	The type of scheduling level: <i>stream</i> , <i>service</i> or <i>PID</i>
SID:	The service ID associated with a probe service scheduling scheme
PID:	The PID associated with a probe PID scheduling scheme
Ignore:	Lists the types of errors that are ignored. For a probe PID threshold template, scheduling is selected to apply for any of these errors: CC errors, missing PID errors, PCR errors, unreferenced PID errors or all errors. for a probe service threshold template, scheduled error masking can be done for EIT errors (problems with the EPG) or for all errors. If no scheduling applies for a PID in the schedule list, the field will display all types of errors and the associated Scrambling template field will read <i>None</i> .



Probe:	The IP address of the probe associated with the probe scheduling list entry. This can be clicked to access the device.
Scheduling template:	The probe scheduling template associated with the scheduling list entry (as defined in the probe Setup — Scheduling view). If no scheduling is enabled this field will read <i>None</i> .
Scheduling:	The scheduling time window(s) during which alarms are masked



6.14 Timeline (requires Archive Server)



The **Timeline** view requires an Archive Server, please refer to chapter 6.23 for details on how to configure the Archive Server. Select **Timeline** in the left hand menu, and the timeline should load in the right hand pane.

For information on the Timeline feature in the Software Probe version 6.0 and later, please refer to the Software Probe User's Manual.

6.14.1 Choosing what to inspect

To change which stream and service you are looking at, select the desired service from the drop down at the top left. Note that tracks that are already added will stay put to enable comparing services. If you do not want to have the old tracks there, click the small × in the top right of each track. You can filter which streams you see by typing part of the stream or service name into the filter box. The drop down should now only be populated by the matching streams or services. To clear the filter, just click on the × in the right hand part of the filter box.



In the bottom left you can select from which source you want to add tracks, and to the right of those you will find the different types of data stored from the selected device.

To remove a track, press the × located at the top right of the track you want to remove.

Some tracks can be resized by clicking on the vertical arrows located under the close button for the track.

6.14.2 Navigating in time



To navigate in time you have two options. Back and forth in time, and zoom in / out.

To go back and forth in time you can select the desired time from the time and date picker located at the center top. The time and date picker is most useful for large jumps in time, like if you want to look at



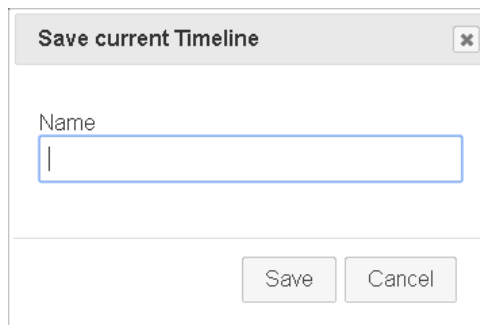
data from days/weeks/months back in time. Just select the correct date and time, and the timeline should automatically jump to that point in time.

The buttons to the left and right of the time-picker let you move in small increments in both directions, and are most suited for smaller adjustments in time.

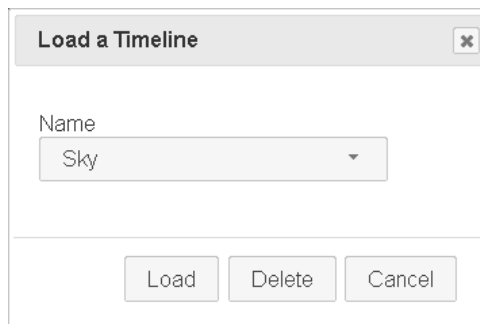
The last way to navigate in time is to drag the timeline in the direction you would want to move it. The timeline should smoothly glide with the dragging motion, and new data should pop up seamlessly.

To zoom in and out, use the + and – buttons located to the right of the filter box. Between the buttons the current zoom level is shown. The zoom level describes how much time is shown in one box.

6.14.3 Persistent layout



When you are happy with the widget layout, you may save the layout by pressing the **Save** button on the top of the screen and giving the layout an unique name. If you later want to update this layout, just save with the same name, and the new layout will override the old.



To load a previously saved layout, press the **Load** button on the top of the screen, find the layout you want in the list, and press the **Load** button. You can also delete layouts you no longer need from this view. Select the layout from the list, press the **Delete** button and confirm the deletion.

All the saved layouts are bound to the user currently logged in, so different users cannot see each others layouts.

6.14.4 Audio silence in the timeline

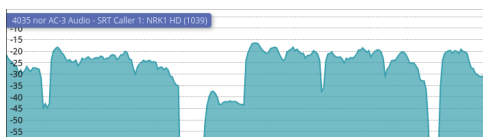
Audio loudness analysis on the probe is designed to monitor and analyze the loudness of audio streams continuously, however, in certain situations the probe may become overloaded resulting in an inability to keep up with the volume of incoming audio data configured for analysis. In such situations you may



notice missing audio analysis segments in the timeline. You can see an example of such a missing audio segment below:



The graphical representation of silent audio in the timeline is subtly different: notice that the thicker, darker line travels down the Y-axis towards an audio level of negative infinity (instead of abruptly disappearing from the segment). You can also see that upon audio returning from silence to once again being audible, the thick blue line travels up from negative infinity towards its new levels.





6.15 Reports

The fundamental measurements of the VBC reports are based on the parameters *availability*, *quality* and *timing*. The reports can be created for IPTV and OTT streams. To create reports for ETR measurements please use the **Ext. Reports** functionality.

<i>IPTV (Ethernet) streams</i>	
Availability	Availability refers to the presence of a stream. An availability of 100% means that there have been no signal disruptions for the complete interval that a stream has been monitored. The no-signal error seconds are measured directly by probes as ES(nosig).
Quality	Quality refers to the packet loss affecting a stream. A quality of 100% means that there has been no packet loss during the interval that the stream has been monitored. The packet loss is measured directly by the probes as ES(MLR).
Timing	Timing refers to the timing of a stream. Timing is based on error seconds just like availability and quality. However a difference is that the value leading to timing error seconds is not a boolean type. While it is straight forward to determine signal loss and packet loss, determining timing issues requires comparing a jitter measurement against a user specified threshold for IPTV streams. A jitter error-second is thus determined by comparing the IAT measurement against the IAT threshold defined as part of the Ethernet threshold template associated with the stream in the probe. Ethernet threshold templates are created in the probe's Multicasts — Ethernet thresh. view, and it is associated with a stream in the Multicasts — Streams — Edit view.
<i>OTT services</i>	
Availability	Availability refers to whether at least one profile for an OTT service is present. Otherwise error seconds are calculated and the availability parameters will drop to a lower value.
Quality	Quality error seconds are counted if not all profiles for a OTT service are present. 100% means that all profiles are present all the time.
Timing	Timing is not measured for OTT services in VBC version 7.0.0.

As an example, 10 error seconds during a period of 48 hours would be presented as 99.9942% for any of the parameters availability, quality or timing. The calculation is $100\% - \frac{10}{48 \times 60 \times 60} \times 100 = 99.99942\%$.

If you have site or stream names containing non-ASCII characters, you may need to select the report character set under **Main — General — Preferences**.



6.15.1 Reports — Manual Report

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

ALARM SETUP

TIMELINE

REPORTS

EXT. REPORTS

MAIN

Manual report

Report list

Auto reports

Import logo

Setup

Action:

Generate a manual report

Select sites to be included in report

Name	Include
VB330	☒
VB220-VB272	☒
VB273	☒
HLS QoS (VB120)	☒
VB120-VB262	☒

Select streamlists

[All streams]

 Select interfaces

IPTV only

Select FROM and TO dates (or use presets) - report can span from 1 day to 2 years

Preset

Last day

 From

2020-11-03

00h

 To

2020-11-04

00h

Select detail level of report - a full report will take longer to generate

Full report

 Include help page ☐

The trend graph average measurements for a specified period of time to emphasize changes over time

Auto select based on duration of report

 Include trend graphs for all streams ☐

Specify error second thresholds for each parameter to be used in report

Availability (%)

99.9700

 Quality (%)

99.9700

 Timing (%)

99.9700

The HTML document embeds links to the BLADE ALARMS page and is useful for smaller reports

Document type:

HTML

Generate manual report

The **Manual report** view allows the user to generate a report based on the parameters described below.

Note that parameter requirements for automatically generated reports are also specified in this view. Select the auto report period using the **Action** drop-down menu and set the parameters.

<i>Parameter</i>	<i>Description</i>
Site list	Only probes belonging to selected sites will contribute to the report.
Stream selection	The user may select to generate a report containing all streams in the system or only streams associated with one stream group. The stream groups are configured in the Main — Stream groups page.
Interfaces	Chose to create a report for IPTV (Ethernet) streams, OTT services or both.
Preset	Allows the user to select between a number of pre-defined report periods. The 'Report from' and 'Report to' fields are updated according to the selection. If the preset value Userdefined is selected, the user may manually determine the report period.
Report from	First date of the report. A report can span from 1 day to 2 years.
Report to	Last date of the report.
Report detail level	Choose whether to generate a full report, a report containing only erroneous streams or a report containing only summary information. When the check box is marked, a help page will be included in the report.



Trend graph interval	The trend graphs show progress over time by averaging all measurements for the selected interval (day, week or month) and plotting these values over time. When the check box is marked trend graphs for all streams will be included in the report.
Thresholds	Specify the availability, quality and jitter threshold percentages to be used in the report.
Document type	In addition to the PDF document type it is now possible to generate an HTML report. The HTML report will provide links to the Blade Alarms view with pre-populated search fields to look up relevant details.

When all parameters have been selected the report is generated by clicking the **Generate report** button.

When editing the settings for a automatic report the button **Apply changes** will save the settings and the button **Generate test report** will apply the settings and create a test report so that the settings can be tested.

6.15.2 Reports — Report list

Manual report Report list Auto reports Import logo Setup														
List of available reports														
Manual reports Automatic reports Fields...														
	Job	Origin	Generated	Type	Ifaces	User	From	To	Avail thr	Qual thr	Timing thr	Sites	Streamgroup	Doctype
View	1	Manual	2008 Sep 7 12:52:26	Full	IPTV	admin	2007-01-24	2008-09-06	99.9	99.9	99.9	7	[All streams]	PDF
View	4	Manual	2008 Sep 8 14:01:14	Erroneous	IPTV	headend	2008-06-09	2008-09-07	99.9	99.9	99.9	1	[All streams]	PDF
View	6	Manual	2008 Sep 8 14:11:59	Full	IPTV	admin	2008-08-31	2008-09-07	99.9	99.9	99.9	1	[All streams]	PDF
View	8	Manual	2008 Sep 8 14:12:44	Full	IPTV	admin	2008-09-07	2008-09-07	99.9	99.9	99.9	1	[All streams]	PDF
View	10	Manual	2008 Sep 8 16:42:44	Full	IPTV	admin	2008-09-06	2008-09-07	99.9	99.9	99.9	3	[All streams]	PDF
View	11	Manual	2008 Sep 8 16:43:13	Full	IPTV	admin	2008-08-29	2008-09-07	99.9	99.9	99.9	3	[All streams]	PDF
View	12	Manual	2008 Sep 8 17:53:06	Erroneous	IPTV	headend	2007-12-14	2008-09-07	99.9	99.9	99.9	1	[All streams]	PDF
View	13	Manual	2008 Sep 8 17:53:38	Full	IPTV	headend	2007-12-14	2008-09-07	99.9	99.9	99.9	1	[All streams]	PDF
View	14	Manual	2008 Sep 8 22:47:33	Erroneous	IPTV	headend	2008-09-07	2008-09-08	99.9	99.9	99.9	4	[All streams]	PDF
View	17	Manual	2008 Sep 9 10:55:24	Erroneous	IPTV	headend	2008-09-06	2008-09-08	99.9	99.9	99.9	4	[All streams]	PDF
View	21	Manual	2008 Sep 9 11:15:28	Full	IPTV	headend	2008-09-05	2008-09-08	99.9	99.9	99.9	4	[All streams]	PDF
View	23	Manual	2008 Sep 10 00:00:43	Full	IPTV	admin	2008-08-29	2008-09-09	99.9	99.9	99.9	1	[All streams]	PDF
View	28	Manual	2008 Sep 10 00:44:11	Full	IPTV	headend	2008-09-05	2008-09-08	95	98	99	4	[All streams]	PDF
View	502	Manual	2009 Oct 29 17:47:40	Full	IPTV	admin	2009-09-30	2009-10-30	99.0	99.5	99.5	10	[All streams]	PDF
View	506	Manual	2009 Nov 3 10:11:13	Full	IPTV	headend	2009-10-27	2009-11-03	90.5	90.5	90.9	1	Thumbs streams	PDF
View	507	Manual	2009 Nov 3 15:29:59	Full	IPTV	admin	2009-11-02	2009-11-03	99.0	99.5	99.5	6	[All streams]	PDF
View	510	Manual	2009 Nov 7 01:22:10	Full	IPTV	admin	2007-11-07	2009-11-07	99.0	99.5	99.5	12	[All streams]	PDF
Pending reports: 0 Progress current report: 100 % Terminated: 1555 Last report: Job 12857 issued 2020 Oct 29 11:44:28 failed step 1														
Delete selected														

The report list view provides a list of all reports that the logged-in user is allowed to view. The *admin* user has access to all reports while regular users can only view his own reports.

Newest reports will be presented at the bottom of the list (by default). Older reports with identical report parameters are removed when a new report is generated.

The status line at the bottom displays pending reports as well as terminated reports. A terminated report means that the report could not be generated likely because the report engine found an incomplete or inconsistent data set. Rather than doing a best effort report the report will be discarded and the 'Terminated' count increased. Click the **Fields...** button to select which fields should be present in the report list. Click the **Delete selected** button to delete one or more reports.



Manual report

Report list

Auto reports

Import logo

Setup

Report field selection

Field	Display in alarm list
Job	☒
Origin	☒
Generated	☒
Type	☒
Ifaces	☒
User	☒
From	☒
To	☒
Avail thr	☒
Qual thr	☒
Timing thr	☒
Sites	☒
Streamgroup	☒
Doctype	☒

Apply

Select fields to be displayed in report list

6.15.3 Reports — Auto reports

Manual report

Report list

Auto reports

Import logo

Setup

Automatic report generator

Type	Enable	When	Settings
Daily report	☐	Each day at 00:01	(empty - set from Manual report tab)
Weekly report	☐	Each Monday at 00:01	(empty - set from Manual report tab)
Monthly report	☐	Day 1 each month at 00:01	(empty - set from Manual report tab)
Email report	☐		Type in a comma separated list of recipients that should receive an email with the report

Apply changes

The VBC may automatically create reports daily, weekly or monthly, based on parameter requirements made by the user in the **Manual report** view.

If the enable daily report check-box is marked, a report will be created every day at time 00:01. Likewise generation of weekly and monthly reports can be enabled; the weekday and month day for the generation is specified by the user. Click the **Apply changes** button for changes to take effect.

Check the checkbox in the **Email report** row and enter the email address of a recipient, each of the checked report type will be emailed by their time of generation to the selected recipient(s). If there is more than one recipient, add a comma (',') between the addresses.



The mail server settings are found under **Main — General — Connections — Outgoing mail server**.

The Auto reports configuration will be individual to each user account registered on the VBC, so each user account may have its own configuration of the auto extended reports. This can be used to have multiple daily reports emailed every night etc.

The parameters for the report is located under the Settings column, these are set in the Manual extended report tab by selecting the Edit for the appropriate report for the Action setting.

6.15.4 Reports — Import logo

Manual report | Report list | Auto reports | **Import logo** | Setup

Import customer logo to be used in reports. The logo must be in JPEG format. Only admin can do this.

Import logo

Choose file No file chosen

Go!

Current logo:



BRIDGE TECHNOLOGIES™

In the Import logo tab the *admin* can import a custom logo that will be used in generated reports.

The aspect ratio of the logo should be OK inside the reports even if it is displayed with fixed width and height in this view.

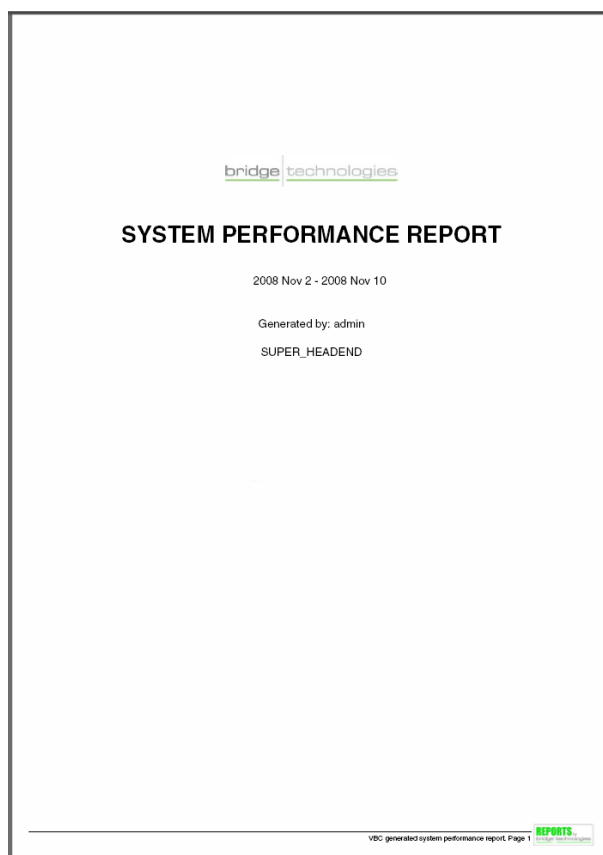
6.15.5 Reports — The PDF Report

The generated PDF reports contain the following information:

- Title page (page 1) describing who generated the report, report dates and contributing sites
- The summary page (page 2) containing measurements and trending across all streams and the SLA thresholds
- An optional help page describing the graphical elements of the report and showing the similarities between the VBC's report graph and the probe's MediaWindow graph
- The stream table listing all streams
- Per stream information (if requested) including optional trending graphs



The PDF report title page



The company logo can be imported.

The PDF report summary pages

Summary information

Report from	2015-Jan-03
Report to	2015-Feb-02
Days in report	30
User	admin
Streams	148
Stream-group	[All streams]
Number of sites	9
Stream-graph resolution	1h 0m
Report generated	2015 Feb 2 13:00:32
Report type	Full report
Show trending	Daily, all reported streams
Interfaces	ETHERNET, OTT

Sites:

HEADEND_CONTENT
HEADEND_CORE
OSLO_DVB-C
OSLO_DVB-S2
OSLO_DVB-T
OSLO_ASI
UK_DVB-T2
10G_CORE
OTT

The summary information grid shows overall information.



SLA all streams in report

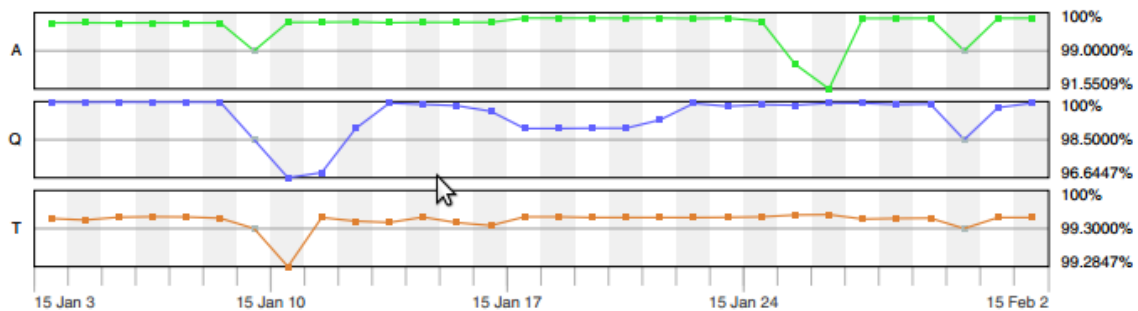
A, Q and J averaged for all streams in report. SLA is indicated as a line in the graph and max graph-value is 100%.

Availability:	99.402%	SLA=99.000%		PASS
Quality:	99.483%	SLA=98.500%		PASS
Timing:	99.480%	SLA=99.300%		PASS

The SLA overview shows how the reported streams perform compared to the SLA threshold values. If the measured parameter value is better than the SLA threshold the bulb icon associated with the parameter bar is green, otherwise it is red.

Trending for all streams in report

A, Q and J averaged for each interval for all streams and plotted. SLA is middle value.



The three trend graphs show how the parameter percentages develop over time. During each trend period (day, week or month) the number of error seconds are summed across all streams and the average is used to represent that trend interval. The labels are 100%, the user specified threshold and the all time low. If a measurement period is incomplete the associated value is indicated as a grey point located at the threshold line.

SLA thresholds

These threshold percentages were specified when report was generated

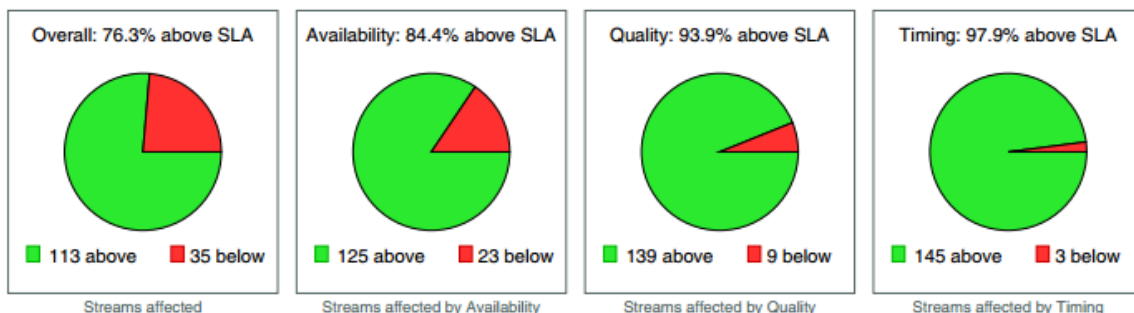
Parameter	%	Corresponding ES for 30 days	Corresponding ES for 1 day
Availability	99.0000	7h 12m	14m 24s
Quality	98.5000	10h 48m	21m 36s
Timing	99.3000	5h 2m	10m 4s

The threshold setting percentages are specified when the report is generated. This table also shows the corresponding number of error seconds for the entire reporting interval as well as for one day.



Streams above and below SLA thresholds

The error-seconds are summed for each stream and compared against SLA



The pie charts show how many streams fall below the threshold settings. In the above example there are 125 streams that are OK while 23 have an availability of less than the threshold setting. Hence 84.4% of the streams are OK with respect to availability.

The overall chart states how many streams are not affected at all – hence 113 of the streams are above the threshold settings for all parameters.

Stream table

The error-second figures equal the total sum of error-seconds divided by the number of probes (i.e. it is the average)

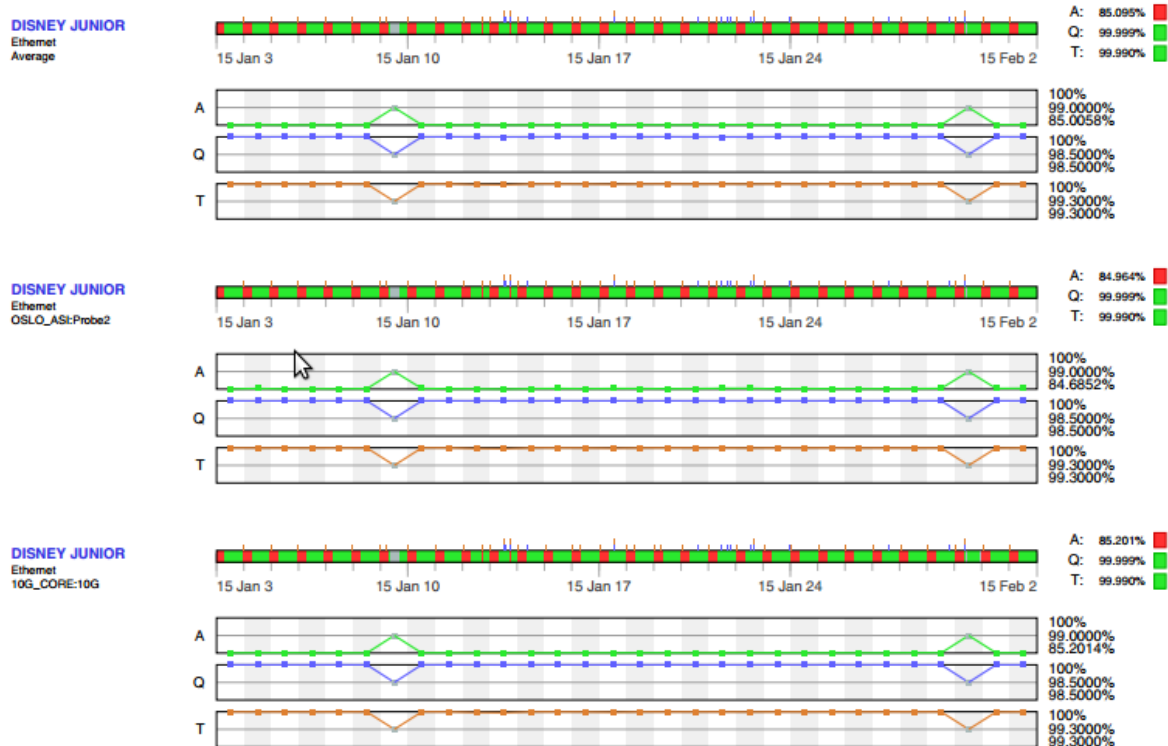
#	Stream and class	Iface	Avail (%)	ES (time)	Quality (%)	ES (time)	Timing (%)	ES (time)	Measured	Probes
1	1ST BALTIC MUSIC	Ethernet	0.0000	17h 0m	100.0000	0	100.0000	0	2% (17h 0m)	1
2	3sat	Ethernet	100.0000	0	99.9984	42s	99.9999	2s	98% (29d 15h)	2
3	6eren HD	Ethernet	100.0000	0	99.9992	20s	99.9978	57s	98% (29d 15h)	2
4	7eren	Ethernet	100.0000	0	99.9995	12s	99.9973	1m 9s	98% (29d 15h)	2
5	ALJAZEERA_INT	Ethernet	100.0000	0	99.9981	48s	100.0000	1s	98% (29d 16h)	3
6	ANIMAL_PLANET	Ethernet	99.9941	2m 30s	99.9994	16s	99.9853	6m 16s	98% (29d 16h)	2
7	Apple BipBop	OTT	100.0000	0	1.2360	7d 11h	100.0000	0	25% (7d 14h)	1
8	Apple Kenote	OTT	100.0000	0	98.8077	46m 30s	100.0000	0	9% (2d 17h)	1
9	Arirang TV	Ethernet	100.0000	0	99.9998	5s	99.9999	2s	98% (29d 15h)	2
10	BBB SS	OTT	100.0000	0	99.6241	2h 5m	100.0000	0	77% (23d 5h)	1

The stream table page lists all streams providing both error second and percentages for availability, quality and timing. The ES (time) values are an average based on measurements from all the probes monitoring the stream. The presented value is the total number of error seconds summed for each probe divided by the probe count.

A red bulb indicates that a parameter is outside the thresholds. The time the stream has been measured is stated, 100% means it was measured during the entire reporting interval. The number of probes that measured the stream is shown.



Per stream page



The stream graph is a graphical representation of the parameters quality, availability and timing over time. For each sample period (the sample period will depend on the range of the report) a color code is used to indicate if any of the quality (blue), availability (green) or timing (brown) parameters were affected for the stream. So it is sufficient for the stream to measure 1 error second during a specific sample period to color it accordingly. Conversely, the only way to have an all green bar is for the stream to measure 0 error seconds across the entire interval of the report. A grey color is used whenever no streams are measured. To the right of the stream graph are the status bulbs comparing the sum of error seconds against the user specified threshold.

For streams that are monitored on more than one probe, the average graph is drawn first followed by elementary probe measurements. The average graphs (the stream graph and the three trend graphs) are derived by summing the error-seconds of the elementary probe measurements and dividing by the number of probes. This averaging is performed according to the stream graph resolution (refer to the summary information) for stream graphs and for each trending interval for trend graphs.

6.15.6 Reports — The HTML Report

The HTML report is identical to the PDF report except that it contains hyperlinks which can be used to click into the **Blade Alarms** view to make the root-cause analysis of the errors in the report simpler. Note that the data in the **Blade Alarms** view is only temporarily available and will be replaced by more recent alarms as time passes. So the HTML report could be used to look into the details of current erroneous streams in a more interactive way than the PDF report allows. The PDF reports are more suitable to view trends and longer intervals and will smaller in size for the same content and thus more email-friendly.

Example HTML report with links to BLADE ALARMS:



Stream table

The error-second figures equal the total sum of error-seconds divided by the number of probes (i.e. it is the average)

#	Stream and class	Iface	Avail (%)	ES (time)	Quality (%)	ES (time)	Timing (%)	ES (time)	Measured	#P
1	NRK1 HD (RTP)	IPTV	100.0000	0	100.0000	0	100.0000	0	41% (10h 0m)	1
2	001 ABR CamHD HLS	OTT	100.0000	0	92.4694	45m 11s	100.0000	0	41% (10h 0m)	2
3	002 ABR CamHD CMAF	OTT	100.0000	0	91.4611	51m 14s	100.0000	0	41% (10h 0m)	2
4	003 ABR CamHD DASH	OTT	100.0000	0	91.9306	48m 25s	100.0000	0	41% (10h 0m)	2
5	004 ABR CamHD SS	OTT	100.0000	0	91.8361	48m 59s	100.0000	0	41% (10h 0m)	2
6	005 ABR CamHD HDS	OTT	100.0000	0	92.9028	42m 35s	100.0000	0	41% (10h 0m)	2

Clicking the link next to the red bulb for the **005 ABR Cam HD HDS** streams brings up the **Blade Alarms** view:

Blade alarms

Select by location

Site: All

Blade:

Select by alarm

☐ Show only Active alarms

VBC alarm: All

Select by stream info

Stream name: 005 ABR CamHD

Service name:

PID:

Select by time

Start time: 2020 Feb 25 00:00:00

End time: 2020 Feb 26 00:00:00

Alarms active in selected period will be shown

i	Sev	Status	Time	Site	Blade	Interface	Stream	VBC alarm	Description
1		Cleared	Feb 26 00:00:03 - Feb 26 00:00:22	rfsite	211-COF...	OTT	005 ABR CamHD HDS	OTT transport error	Profile_5 [750 kbps] Transport error: F...
2		Cleared	Feb 26 00:00:03 - Feb 26 00:00:22	rfsite	211-COF...	OTT	005 ABR CamHD HDS	OTT transport error	Profile_4 [2500 kbps] Transport error: ...
3		Cleared	Feb 26 00:00:03 - Feb 26 00:00:22	rfsite	211-COF...	OTT	005 ABR CamHD HDS	OTT transport error	Profile_3 [5000 kbps] Transport error: ...

For the **Blade Alarms** view to be reachable in this way the user setting for the admin user needs to have the option **Allow access without login** checked. The URL to be used for the VBC server is specified in the **General — Preferences** view as **Hostname in reports**. The default is 127.0.0.1.



6.16 Ext. Reports

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

ALARM SETUP

TIMELINE

REPORTS

EXT. REPORTS

MAIN

Manual extended reportExtended report listAuto extended reportsAlarm poll and report statusSetup storage

VB330	☐
VB220-VB272	☐
VB273	☐
HLS QoS (VB120)	☐
VB120-VB262	☐
VB220-VB242-256	☐
DASH QoS (VB220)	☐
VB220-VB252-252	☐
MCR	☐
MicroVB-MDC	☐
VB273	☐
VB288	☐
VB50	☐

Checks to be included in the report

Name	Chec...
☐ No signal	1100
☐ RTP packet drop	1250
☐ RTP duplicates	1260
☐ RTP out of order	1270
☐ CC skips	1350
☐ MLR >= err-thresh	1420
☐ MLR >= warn-thresh	1430
☐ IAT >= err-thresh	1400
☐ IAT >= warn-thresh	1410
☐ Bitrate overflow	1600
☐ Bitrate underflow	1610
☐ TS sync	3000
☐ Sync byte	3001

DeleteAdd group- Select preset -

All available checks

Name	Chec...
☐ No signal	
☐ RTP drops	
☐ MLR error	
☐ IAT error	
☐ Bitrate overflow	
☐ Bitrate underflow	
☐ ETR pri one error	
☐ ETR pri two error	
☐ ETR pri three error	
☐ ETR pri other error	
☐ ETR interface error	
☐ OTT transport error	
☐ OTT http error	

Select streams to be included in extended report [All streams]

Select services to be included in extended report [All services]

Select a time preset or choose 'User defined' to specify FROM and TO dates manually - extended report can span from 1 day to 2 years

Preset [Last 7 days] From [2020-10-28] To [2020-11-05]

Select detail level of extended report - a full report will take longer to generate

[All streams]

Select how the entities in the report should be sorted

[Site->Blade->Interface->Stream]

Specify error thresholds for parameters to be used in the extended report

Threshold (%) [99.0000]

Generate manual extended report

The extended reports section gives the user the ability to generate reports based on the raw **Blade Alarms** from the probes and extractors added to the VBC Controller. These reports will provide information about alarm status for all the different stream alarms reported by the devices connected to the VBC. This can be IPTV alarms, ETR alarms (both for MPTS or SPTS streams), RF alarms, OTT and content alarms. The reports are based entirely on the probe and extractor alarms, to get the alarm graphs “green” the alarm thresholds on the devices have to be changed.

Both the status of streams as well as the status of individual services in MPTS/SPTS and individual profiles in OTT can be shown in the report.

The reports can be created manually or automatically on a daily, weekly or monthly basis and emailed to a list of recipients.

All probes and extractors should run the latest software for the extended reports to work correctly. The network connection between the VBC server and the probes and extractors must work well. If the connection is down the VBC may not get all device alarms thus making the extended report incorrect. See the section **Ext. Reports — Alarm poll and report status** for how to check the status of alarm and report



data fetching from the devices in the system. If you have site or stream names containing non-ASCII characters, you may need to select the report character set under **Main — General — Preferences**.

6.16.1 Ext. Reports — Manual extended report

In the **action** section choose what type of report template should be modified (daily, weekly or monthly) or select **Generate Manual Report**.

Press the check box for each **site** that should be included in the selected report.

Checks to be included in the report		All available checks	
Name	Chec...	Name	Chec...
☐ No signal	1100	☒ No signal	
☐ RTP packet drop	1250	☒ RTP drops	
☐ RTP duplicates	1260	☒ MLR error	
☐ RTP out of order	1270	☒ IAT error	
☐ CC skips	1350	☒ Bitrate overflow	
☐ MLR >= err-thresh	1420	☒ Bitrate underflow	
☐ MLR >= warn-thresh	1430	☒ ETR pri one error	
☐ IAT >= err-thresh	1400	☒ ETR pri two error	
☐ IAT >= warn-thresh	1410	☒ ETR pri three error	
☐ Bitrate overflow	1600	☒ ETR pri other error	
☐ Bitrate underflow	1610	☒ ETR interface error	
☐ TS sync	3000	☒ OTT transport error	
☐ Sync byte	3001	☒ OTT http error	

Select which alarm data to be included in the report. To add checks drag either entire groups of checks or individual checks from the list of available checks on the right to the list of included checks on the left of the screen. The normal multi-select with Shift+Mouse or Ctrl+Mouse can be used. Checks which are added to a group will be plotted as one entity in the graph and the status of each check in the group is joined to produce one graph. If one of the checks are alarming in a period of time then the group will have an error in that period.

To add a custom group click the **Add group** button. To delete a check or a group of checks select the items and press **Delete** button. To rename an existing group double click the name of the group. It is not possible to rename a check directly but the same effect can be achieved by adding a group and adding one single check to that group. This makes it possible for instance to plot 'TS sync' as 'Signal availability'.

Some checks such as MOS below threshold are carried out for different stream types (IPTV and OTT) and they have different alarm ID's. These will show up as two different entries in the list. If you want to create a report with these alarms merged as one, create a group with that name and drag the two checks to that group.

The drop-down can be used to select between the following presets:

Predefined options for report data	
All checks:	All stream checks supported by the probes and extractors are plotted. The checks are plotted individually.
All VBC alarms:	Groups all the checks according to the VBC Controller alarm definition. The checks are plotted as groups.
All IPTV checks:	All IPTV checks supported by the probes. The checks are plotted individually.



All OTT checks:	All OTT checks supported by the probes. The checks are plotted individually.
All ETSI TR 101 290 checks:	All the checks specified the ETSI TR 101 290 specification. The checks are plotted individually.
All probe ETR 290 checks:	All the probe checks under ETR290. This includes all the ETSI TR 101 290 defined checks, the ETR priority other checks and the RF checks. The checks are plotted individually.
All ETR 290 interface checks:	All of the interface checks such as signal level, MER, SNR and bit error rate. The checks are plotted individually.
ETR 290 groups for Finland:	The checks grouped to fit Finnish government regulations.

Select which stream group to generate the report for or select **[All streams]** to generate the report for all streams. Please note that if there are no streams in the specified stream group on the selected site the report will be empty. The stream groups are configured in the **Main — Stream groups** page.

Select which service group to generate the report for or select **[All services]** to generate the report for all services. For a stream report this will then show all streams containing the services listed in the service group. Please note that if there are no services in the specified stream group on the selected site the report will be empty. Only reports that include service information can be filtered by service groups, i.e. it is not possible to use service filtering when creating a report with detail level set to All streams or Merged streams. The service groups are configured in the **Main — Service groups** page.

If both a stream group and a service group are specified, the report will contain only the services listed in the stream group that also contains (one or more of) the services in the specified service group.

The time span may be switched between **Today**, **Yesterday**, the **last 7, 30, 90 or 180 days**. Or the user may set a **User defined** interval including up to 2 years of report data. Please note that reports can take a long time to generate if a lot of data is to be included in the report.

The level of detail can be switched between:

All streams – This selection will display the status for all the streams monitored at the selected sites and display them individually. Generating such a report can take a long time and the number of pages may become high.

Merged streams – This selection will generate a report where the data for the streams are merged. If the same stream is monitored at different probes/sites and/or at different interfaces on one probe the measurement results will be merged showing the overall status of the stream. If the monitored stream has errors at one probe it will become red in the merged stream graph.

All streams and services – This selection will gather data from all of the streams and all of the services that are a part of the transport streams.

Merged streams and services – This selection generate a report based on all of the streams and their services and merge it all into one section.

All services – This selection will gather data from all of the services inside the monitored transport streams.

Merged services – This selection will gather data from all services in all of the monitored transport streams and then merge the data together.

The entities in the report can be sorted in different ways. Select one of the following in the drop-down:



- Site -> Blade -> Interface -> Stream
- Stream -> Site -> Blade -> Interface
- Stream -> Interface -> Site -> Blade

Set the **error threshold** for the alarm checks in the extended report, the threshold is based on percentage. If the selected report is of type a **Manual extended report** or **Daily, weekly or monthly report** the apply or generate button must be pressed for the settings to take action.

6.16.2 Ext. Reports — Extended report list

Manual extended reportExtended report listAuto extended reportsAlarm poll and report statusSetup storage

List of available extended reports

Manual extended reportsAutomatic extended reportsFields...

	Job	Origin	Generated	Type	Sorting	User	From	To	Thresh	Sites	Streamgroup	Servicegroup
View	1	Manual	2013 Oct 31 14:37:48	All streams	Site->Blade->Interface->Stream	admin	2013-10-24	2013-10-31	99.0000	16	[All streams]	[All services]
View	8	Manual	2013 Nov 4 15:44:47	All streams	Site->Blade->Interface->Stream	admin	2013-10-28	2013-11-04	99.0000	16	[All streams]	[All services]
View	11	Manual	2013 Nov 6 09:43:20	All streams	Site->Blade->Interface->Stream	admin	2013-10-30	2013-11-06	99.0000	1	[All streams]	[All services]
View	12	Manual	2013 Nov 6 09:44:31	All streams	Site->Blade->Interface->Stream	admin	2013-10-30	2013-11-06	99.0000	3	[All streams]	[All services]
View	13	Manual	2013 Nov 6 16:40:55	All streams	Site->Blade->Interface->Stream	jee	2013-10-07	2013-11-06	99.0000	11	[All streams]	[All services]
View	20	Manual	2013 Nov 7 10:19:58	All streams	Site->Blade->Interface->Stream	admin	2013-10-31	2013-11-07	99.0000	15	[All streams]	[All services]
View	22	Manual	2013 Nov 7 11:18:36	All streams	Site->Blade->Interface->Stream	admin	2013-11-06	2013-11-07	99.0000	15	[All streams]	[All services]
View	23	Manual	2013 Nov 7 14:17:50	All streams	Site->Blade->Interface->Stream	jee	2013-10-31	2013-11-07	99.0000	11	[All streams]	[All services]
View	24	Manual	2013 Nov 7 14:30:50	All streams	Site->Blade->Interface->Stream	jee	2013-11-06	2013-11-07	99.0000	3	[All streams]	[All services]
View	73	Manual	2013 Nov 27 21:36:30	All services	Site->Blade->Interface->Stream	admin	2013-11-26	2013-11-27	99.0000	1	[All streams]	[All services]
View	76	Manual	2013 Nov 28 09:16:06	All services	Site->Blade->Interface->Stream	admin	2013-11-21	2013-11-28	99.0000	1	[All streams]	[All services]
View	111	Manual	2013 Dec 12 16:50:33	All services	Site->Blade->Interface->Stream	admin	2013-12-05	2013-12-12	99.0000	5	[All streams]	[All services]
View	148	Manual	2013 Dec 27 17:55:46	All services	Site->Blade->Interface->Stream	admin	2013-12-20	2013-12-27	99.0000	4	[All streams]	[All services]
View	149	Manual	2013 Dec 27 18:01:15	All services	Site->Blade->Interface->Stream	admin	2013-11-27	2013-12-27	99.0000	4	[All streams]	[All services]
View	150	Manual	2013 Dec 27 18:01:59	All services	Site->Blade->Interface->Stream	admin	2013-11-27	2013-12-27	99.0000	15	[All streams]	[All services]
View	151	Manual	2013 Dec 27 18:06:43	All services	Stream->Site->Blade->Interface	admin	2013-11-27	2013-12-27	99.0000	15	[All streams]	[All services]
View	152	Manual	2013 Dec 27 18:06:55	All services	Stream->Interface->Site->Blade	admin	2013-11-27	2013-12-27	99.0000	15	[All streams]	[All services]
View	153	Manual	2013 Dec 27 18:20:51	All streams	Site->Blade->Interface->Stream	demo	2013-12-26	2013-12-27	99.0000	10	[All streams]	[All services]
View	154	Manual	2013 Dec 27 18:21:03	All streams	Site->Blade->Interface->Stream	demo	2013-12-20	2013-12-27	99.0000	10	[All streams]	[All services]
View	155	Manual	2013 Dec 27 18:21:15	All streams	Site->Blade->Interface->Stream	demo	2013-11-27	2013-12-27	99.0000	10	[All streams]	[All services]
View	156	Manual	2013 Dec 27 18:21:19	All streams	Stream->Site->Blade->Interface	demo	2013-11-27	2013-12-27	99.0000	10	[All streams]	[All services]
View	157	Manual	2013 Dec 27 18:21:25	All streams	Stream->Interface->Site->Blade	demo	2013-11-27	2013-12-27	99.0000	10	[All streams]	[All services]
View	180	Manual	2014 Jan 6 08:00:42	All services	Stream->Interface->Site->Blade	admin	2014-01-03	2014-01-06	99.0000	15	[All streams]	[All services]
View	181	Manual	2014 Jan 6 10:24:15	All services	Stream->Interface->Site->Blade	admin	2014-01-05	2014-01-06	99.0000	4	[All streams]	[All services]

Pending extended reports: 0Progress current extended report: 100 %Terminated: 1211Last extended report: Job 3677 issued 2020 Oct 29 11:16:06 successful

Delete selected

The extended report list contains all the extended reports generated by the VBC; both the manually and/or automatically generated PDF documents. The list is split up into two tables that may be switched between by pressing the buttons; **Manual extended reports** or **Automatic extended reports**.

The fields in each table may be changed by pressing the **Fields..** button, if there is a field that is not important to have in the tables it can be removed by pressing the corresponding checkbox.

The fields shown in the table are generally the parameters entered in in the **Manual extended Report** tab, except for **Job** number and **Sites**.

Job – a value that gets incremented each time a report is generated this is a global variable for **Manual extended reports** and **Automatic extended reports**.

Sites – the number of sites included in the report.

Press **View** to download and open the corresponding report.



6.16.3 Ext. Reports — Auto extended reports

Manual extended report Extended report list **Auto extended reports** Alarm poll and report status Setup storage

Automatic extended report generator

Type	Enable	When	Settings
Daily extended report	☐	Each day at 01:00	(empty - set from Manual extended report tab)
Weekly extended report	☐	Each Monday at 01:00	(empty - set from Manual extended report tab)
Monthly extended report	☐	Day 1 each month at 01:00	(empty - set from Manual extended report tab)
Email report	☐		Type in a comma separated list of recipients that should receive an email with the report

Apply changes

The automatic extended reports tab gives the opportunity to select when and how often the an extended report will be automatically generated.

Click the checkbox and select at what intervals the report should be generated, daily, weekly or monthly. For weekly reports the day of the week when the report are to be generated can be specified. Similarly for a monthly report the day of the month can be specified. The reports will be generated at 01.00 on the selected day(s).

Check the checkbox in the **Email report** row and enter one or more email address, separated by comma. Each generated report will be emailed to the selected recipient(s).

The mail server settings are found under **Main — General — Connections — Outgoing mail server**.

The Auto reports configuration will be individual to each user account registered on the VBC, so each user account may have its own configuration of the auto extended reports. This can be used to have multiple daily reports with different settings etc.

The parameters for the report is shown under the Settings column, these are set in the Manual extended report tab by selecting the Edit for the appropriate report for the Action setting.



LOGIN
LIVE
MONITORING
BLADE ALARMS
GRAPHICS VIEW
STREAM VIEW
THUMBS VIEW
SERVICE VIEW
MAP
RDP
RDW
EQUIPMENT
ALARM SETUP
TIMELINE
REPORTS
EXT. REPORTS
MAIN

Manual extended reportExtended report listAuto extended reportsAlarm poll and report statusSetup storage

☐	MCR	☐
☐	MicroVB-MDC	☐
☐	VB273	☐
☐	VB288	☐
☐	VB50	☐
☐	DVB-T2	☐
☐	VB243	☐
☐	VB440 test	☐
☐	QTT QoE (VB288)	☐
☐	QTT Manager	☐
☐	VB220_ES	☐
☒	V6.0 RELEASE	☒
☐	ATest	☐

Checks to be included in the report

Name	Chec...
☐ No signal	1100
☐ RTP packet drop	1250
☐ RTP duplicates	1260
☐ RTP out of order	1270
☐ CC skips	1350
☐ MLR >= err-thresh	1420
☐ MLR >= warn-thresh	1430
☐ IAT >= err-thresh	1400
☐ IAT >= warn-thresh	1410
☐ Bitrate overflow	1600
☐ Bitrate underflow	1610
☐ TS sync	3000
☐ Sync byte	3001

DeleteAdd group- Select preset -

All available checks

Name	Chec...
☐ ETR pri one error	
☐ TS sync	3000
☐ Sync byte	3001
☐ PAT	3002
☐ Continuity	3003
☐ PMT	3004
☐ Missing PID	3005
☒ ETR pri two error	
☒ ETR pri three error	
☒ ETR pri other error	
☒ ETR interface error	
☒ OTT transport error	
☒ OTT bit error	

Select streams to be included in extended report [All streams]

Select services to be included in extended report [All services]

Select a time preset or choose 'User defined' to specify FROM and TO dates manually - extended report can span from 1 day to 2 years

Preset [Last 7 days] From [2020-10-28] To [2020-11-05]

Select detail level of extended report - a full report will take longer to generate

[All streams]

Select how the entities in the report should be sorted

[Site->Blade->Interface->Stream]

Specify error thresholds for parameters to be used in the extended report

Threshold (%) [99.0000]

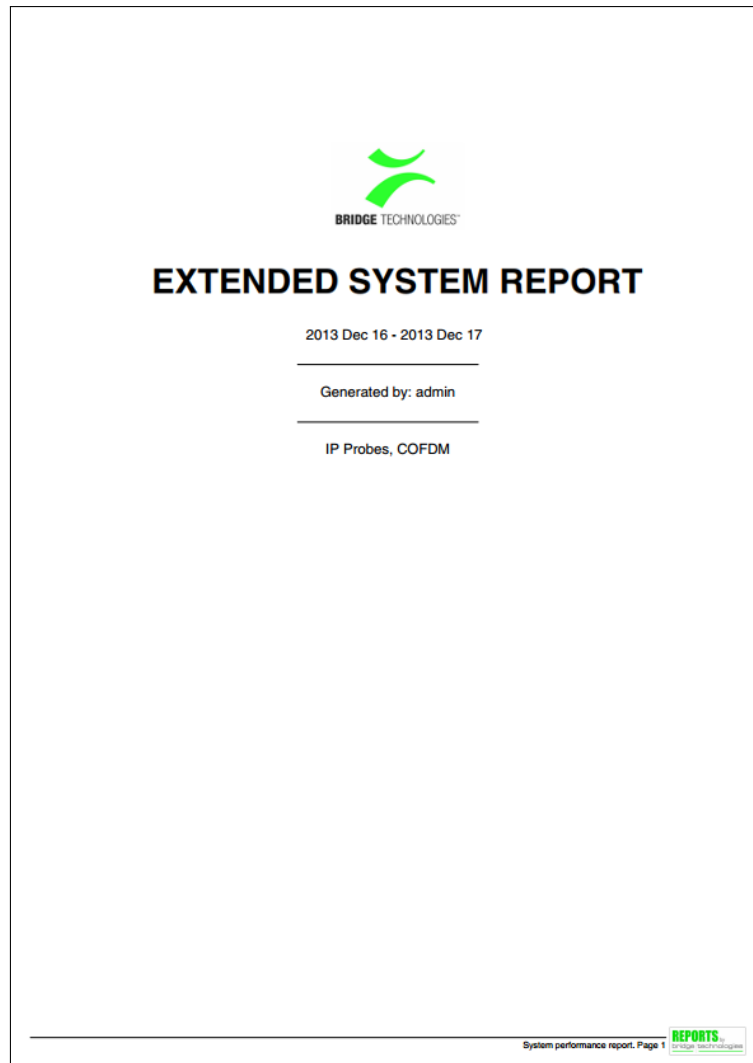
Generate manual extended report



6.16.4 Ext. Reports — PDF Report

The PDF report title page

The front page of the PDF report, a company logo may be imported.





The PDF report summary page

Summary information		Sites:	
Report from	2019-Jan-16	VB330	VB50
Report to	2019-Feb-15	VB220-VB272	DVB-T2
Days in report	30	VB273	VB243
User	admin	VB120	Tokyo
Stream group	[All streams]	VB120-VB262	
Service group	[All services]	VB220-VB242-256	
Number of sites	16	VB220-OTT	
Stream-graph resolution	1h 0m	VB220-VB252-252	
Report generated	2019 Feb 15 10:08:27	MCR	
Report type	Merged streams	MicroVB-MDC	
		VB273	
		VB288	

SLA thresholds				
All reporting are done based on 1 hour time periods. The number of error seconds (ES) allowed before marking a 1 hour period as red is shown below. The other time periods are shown for reference. These threshold percentages were specified when report was generated				
Parameter	SLA %	Maximum ES per 1 hour	ES for 1 day	ES for 30 days
ETR pri one error	99.5000	18s	7m 12s	3h 36m
TS sync				
Sync byte				
PAT				
Continuity				
PMT				
Missing PID				
Content errors	99.5000	18s	7m 12s	3h 36m
Freeze-frame detected				
Color-freeze detected				
MOS below threshold				
Audio silence detected				
Audio too loud detected				

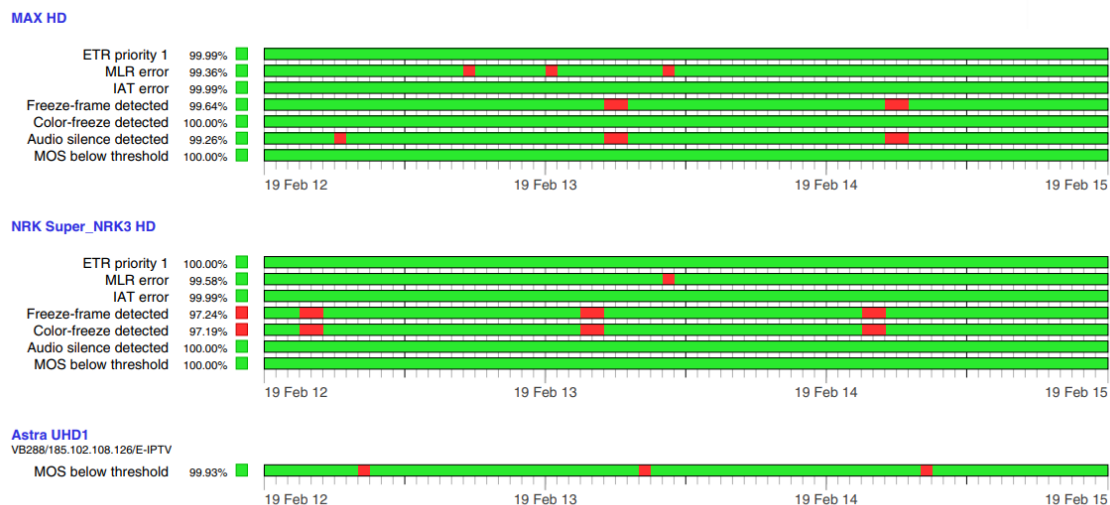
Extended system report Page 2

This page of the extended report shows a short summary about the specific report, sites and SLA thresholds.

The SLA thresholds shows which of the different probe and extractor alarms that are included, how many corresponding error-seconds for the number of days specified and corresponding error-seconds for 1 day and 1 hour. The report will always use the 1 hour period to determine if a part of the graph should be colored red. If the checks are added into one groups then this page will show which probe and extractor alarms are used for each of the groups.



The PDF report Alarm-graph page



The alarm-graph plots the status of the different alarms over the time period specified. The report is based on 1 hour periods and if the alarm has been active for more than the specified threshold during that period the graph will be colored red. A threshold of 99% coloring the graph red.

If several checks are joined together in group the graph will be colored red if one (or more) of those checks are in violation of the threshold.

The alarm-graphs will show entire streams or single services depending on what selected for detail level. Alarms that are grey all the time are disabled in the probes or extractors. When generating the report it is possible to omit checks which are not of interest or to group several checks together.



6.16.5 Ext. Reports — Alarm poll and report status

Manual extended report Extended report list Auto extended reports Alarm poll and report status Setup storage								
#	Blade type	IP address	Uptime	Seq no	Last alarm poll time	Alarm poll status	Last report gen...	Report gen. status
1	probe	10.0.30.220	4456053	3	Nov 4 23:26:42	Successfully fetched alarm list	Nov 4 23:00:00	Report data generated successfully
2	probe	10.0.205.9	36055	1045	Nov 4 23:26:45	Successfully fetched alarm list	Nov 4 23:00:00	Report data generated successfully
3	probe	10.0.205.14	40609	76	Nov 4 23:27:10	Successfully fetched alarm list	Nov 4 23:00:00	Report data generated successfully
4	probe	10.0.205.27	40576	2	Nov 4 23:26:42	Successfully fetched alarm list	Nov 4 23:00:00	Report data generated successfully
5	probe	10.0.205.41	36610	1571	Nov 4 23:26:51	Successfully fetched alarm list	Nov 4 23:00:00	Report data generated successfully
6	extractor	10.0.205.77	2652592	55823	Nov 4 23:26:41	Successfully fetched alarm list	Nov 4 23:00:00	Report data generated successfully
7	probe	10.0.205.93	5651471	572705	Nov 4 23:27:08	Successfully fetched alarm list	Nov 4 23:00:00	Report data generated successfully
8	probe	10.0.205.104	1345939	543479	Nov 4 23:26:57	Successfully fetched alarm list	Nov 4 23:00:00	Report data generated successfully
9	probe	10.0.205.120	40622	8260	Nov 4 23:27:28	Successfully fetched alarm list	Nov 4 23:00:00	Report data generated successfully
10	probe	10.0.205.193	36605	315	Nov 4 23:26:46	Successfully fetched alarm list	Nov 4 23:00:00	Report data generated successfully
11	probe	10.0.205.200	38189	12534	Nov 4 23:26:35	Successfully fetched alarm list	Nov 4 23:00:00	Report data generated successfully
12	probe	10.0.205.216	34251	8	Nov 4 23:27:00	Successfully fetched alarm list	Nov 4 23:00:00	Report data generated successfully
13	probe	10.0.205.223	35885	86	Nov 4 23:27:23	Successfully fetched alarm list	Nov 4 23:00:00	Report data generated successfully
14	probe	10.0.205.228	36713	250	Nov 4 23:26:55	Successfully fetched alarm list	Nov 4 23:00:00	Report data generated successfully
15	archive	10.0.205.234	0	0	Never	Error parsing alarms: Expected ""...	Never	No report generation performed yet
16	extractor	10.150.0.167	5993819	2284531	Nov 4 23:26:57	Successfully fetched alarm list	Nov 4 23:00:00	Report data generated successfully
17	custom	10.150.0.171	0	0	Never	Error parsing alarms: Error readin...	Never	No report generation performed yet
18	probe	10.150.10...	40598	43	Nov 4 23:26:59	Successfully fetched alarm list	Nov 4 23:00:00	Report data generated successfully
19	probe	185.102.1...	0	0	Never	Error parsing alarms: Expected ""...	Never	No report generation performed yet

The alarm poll and report status section will provide information about the last report generation from the VBC, if a device was unreachable or the VBC succeeded in getting the alarm, this section will tell what went wrong or not.

<i>Alarm poll and report status</i>	
#:	Number of the blade
Blade type:	Device type, either probe or extractor
IP address:	The IP of the selected device
Uptime:	Uptime in minutes
Seq no:	Sequence number of the last alarm message received
Last alarm poll time:	What the time was when the VBC fetched the alarm list from the device
Alarm poll status:	Status of the alarm poll, did the VBC manage to fetch the alarm list from the device
Last report:	When was the latest report data generated for the selected device. This should normally be done once every hour.
Report gen. status:	Provides information on the status of the last report data generation. If the device has a too old SW version for the report generation to work it will be shown here.

Press the blue information symbol to open a popup with detailed information about the device and a list of the alarms it supports.



Alarm overview for device						
Summary		Configured alarms				
Device IP:	10.0.205.14	Alarm name	Alarm group	Alarm category	Alarm type	Alarm severity
Device type:	probe	TS sync	ETR	Priority 1	Stream	red
Last alarm poll time:	Nov 4 23:28:10	Sync byte	ETR	Priority 1	Stream	red
Alarm poll status:	Successfully fetched alarm list	PAT	ETR	Priority 1	Stream	red
		Continuity	ETR	Priority 1	Pid	red
Last report gen. time:	Nov 4 23:00:00	PMT	ETR	Priority 1	Pid	red
		Missing PID	ETR	Priority 1	Pid	red
Report gen. status:	generated successfully	Transport	ETR	Priority 2	Stream	red
		CRC	ETR	Priority 2	Stream	red
		PCR	ETR	Priority 2	Pid	red
		PCR accur.	ETR	Priority 2	Pid	red
		PTS	ETR	Priority 2	Pid	red
		CAT	ETR	Priority 2	Stream	red
		NIT	ETR	Priority 3	Stream	red
		SI Rep Rate	ETR	Priority 3	Stream	red
		Unref PID	ETR	Priority 3	Stream	red
		SDT	ETR	Priority 3	Stream	red
		EIT	ETR	Priority 3	Stream	red
		RST	ETR	Priority 3	Stream	red
		TDT	ETR	Priority 3	Stream	red
		MGT	ETR	Priority 3	Stream	red
		VCT	ETR	Priority 3	Stream	red
		PIM/PNM	ETR	Priority 3	Stream	red
		RRT	ETR	Priority 3	Stream	red

Alarm overview for device

Alarm name:	The name of the alarm.
Alarm group:	The alarm group the alarm belongs to.
Alarm category:	The alarm category the alarm belongs to. Not applicable to all alarm types.
Alarm type:	The alarm type specifies what is affected by the error. The alarms can be for the entire System , affecting an entire Stream , or Substream affecting a service in a transport stream or a profile in OTT or affect a single PID in a transport stream.
Alarm severity:	The alarm severity of this alarm as configured in the device.
VBC alarm:	The VBC alarm name for this device alarm. This does not apply to device alarms that are not mapped to a VBC alarm.
Alarm poll status:	Status of the alarm poll, did the VBC manage to fetch the alarm list from the device.
Last report:	When was the latest report data generated for the selected device. This should normally be done once every hour.
Report gen. status:	Provides information on the status of the last report data generation. If the device has a too old SW version for the report generation to work it will be shown here.



6.16.6 Ext. Reports — Setup storage

Manual extended report

Extended report list

Auto extended reports

Alarm poll and report status

Setup storage

Blade alarm and report settings
Keep alarms for: 1 month ▼
Keep extended report data for: 2 years ▼
Delete reports after: Never ▼

Apply

- Up to 1 000 000 alarms are stored in the blade alarm database. The alarms are kept for the time specified here.
- More alarms in the log database results in longer processing times
- The stored alarms will be deleted for a probe if that probe is deleted from the system, deactivated or when the IP address of the probe is changed
- Up to 2 years of report data is stored in the database based on the configuration

The setup storage section lets the user set the time of how long alarm data should be saved, it may be set up to a maximum of one month, if there is a lot of alarm data in the database it may take longer time to use the **Blade Alarms** GUI. The database can keep up to 1 000 000 alarms. The extended reports data can be kept for up to two years.



6.17 Main — Sites and Users

6.17.1 Sites and Users — Sites

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDW

RDW

EQUIPMENT

ALARM SETUP

TIMELINE

REPORTS

EXT. REPORTS

MAIN

SITES AND USERS

LOGS

SNAPSHOTS

ALARM STATISTICS

STREAM GROUPS

SERVICE GROUPS

ARCHIVE SETUP

ARCHIVE DURATIONS

GFX. VIEW SETUP

GENERAL

NETWORK

ABOUT

SitesUsersUser groups

Name	Description	Edit	Delete
VB330	10G HW Probe	Edit	Delete
VB220-VB272	DVB S-S2	Edit	Delete
VB273	Redundant DVB S-S2	Edit	Delete
HLS QoS (VB120)	Probe	Edit	Delete
VB120-VB262	DVB Cable	Edit	Delete
VB220-VB242-256	ASI-COFDM Pairing	Edit	Delete
DASH QoS (VB220)	OTT	Edit	Delete
VB220-VB252-252	COFDM DUAL	Edit	Delete
MCR	Archive	Edit	Delete
MicroVB-MDC	MicroVB	Edit	Delete
VB273	Redundant	Edit	Delete
VB288	Extractor	Edit	Delete
VB50	DVB-T/T2, ISDB-T	Edit	Delete
DVB-T2		Edit	Delete
VB243	VB242-VB243	Edit	Delete
VB440 test		Edit	Delete
QTT QoS (VB288)		Edit	Delete
QTT Manager		Edit	Delete
VB220_ES	IP Probe	Edit	Delete
V6.0 RELEASE	Release end of October 2020	Edit	Delete
ATest	Archiving	Edit	Delete

Site properties

Name

VB120-VB262

Description

DVB Cable

Add new

From the **Site setup** page it is possible to add new sites. Existing sites can be deleted or renamed. Choose the site name with care since it will be used to identify alarm messages and devices across the VBC.

The site name can be changed without affecting the measurements. Hence changing a site name will only change the label when presenting the data and not affect the data themselves.

Getting the balance right between the number of sites and the number of devices in each site is important. Small systems usually only require one site while larger systems will benefit from defining more sites. As a rule of thumb, the number of sites should be similar to the number of devices in each site. The opposite is to have all the device at only one site or to have one site for each device. Note that a site does not necessarily mean a physical site location but can also be a logical location in the signal chain.

Refer to D Appendix: Example Site Configuration for an example configuration.



6.17.2 Sites and Users — Users

Sites

Users

User groups

User

Info

admin	Admin access to 2 sites	Edit	Delete
nils	Normal access to 1 sites	Edit	Delete

Edit user

Name

nils

Password

.....

User group

Normal

Force stream-group

[All streams]

Enable alarm alerts

Visual and audible

Allow access without login

☐

Monitoring-page displays stream-groups

☒

Stack Monitoring-page vertically

☐

Show number of Probes in StreamView

☒

Show interface in StreamView

☐

Available sites

[Unassigned]
[Autodetected]
Secondary

Accessible sites

Main

Apply changes

In the **User setup** page, only accessible to the *admin* user, users can be added, deleted or updated. All users have a name, a password and a list of sites they can access. In addition a user can have full or limited access to the sites, depending on the **User group** assigned to the user. The *admin* user will always have access to all sites.

User properties

Name:	The user name
Password:	The user password for login
User group:	User groups with different access rights are defined in the User group view. Select a user group from the drop down menu.
Force stream-group:	If assigned a stream group, then only that stream group is available in views such as Stream view and Reports .
Enable alarm alerts:	Will alert as requested for new VBC alarms which have alerts enabled in the Alarm setup view.
Allow access without login:	Enable this setting to allow the user to access this VBC Controller from a Master VBC. See chapter 4.2 for more details.
Monitoring page displays stream-group status:	Select if the <i>Stream group status</i> field should be displayed in the Monitoring view



Stack Monitoring page vertically:	Select if the <i>Status for all sites</i> and <i>Stream group status</i> fields should be stacked vertically in the Monitoring view. When a large number of stream groups have been defined, it may be necessary not to stack these fields, for all <i>Stream group status</i> timelines to be visible in the view.
Show number of probes in Stream view:	Select if the number of probes monitoring each stream should be displayed in the Stream view
Show interface in Stream view:	Select if the type of interface associated with a stream should be displayed in the Stream view
Available sites:	All defined sites become available for selection in this sub-window
Accessible sites:	Click the arrows to make a selection of sites that the user should have access to

When access rights have been defined, click the **Add new** button to add a new user. If the access rights of an existing user have been modified, click the **Apply changes** button.

The passwords defined here controls access to the VBC user interface. The administrative interface uses the system accounts, please refer to chapter 2.4 for details.

6.17.3 Sites and Users — User groups

SitesUsers**User groups**

#	Group-name	Read-only	Probe access	TS service view	RDP from VBC	Manage all devices	Manage unassigned devices	Manage devices for own sites
1	Admin	☐	☒	☒	☒	☒	☒	☒
2	Normal	☐	☒	☒	☐	☐	☐	☒
3	Privileged	☐	☒	☒	☒	☒	☒	☒
4	Restricted	☒	☒	☒	☒	☐	☐	☐
5	User1	☐	☒	☒	☐	☐	☐	☒
6		☐	☒	☒	☐	☐	☒	☒
7		☒	☐	☒	☒	☒	☒	☒
8	Reports	☐	☐	☐	☐	☐	☐	☐
9	Test	☒	☒	☒	☐	☐	☐	☐
10		☒	☐	☒	☐	☐	☐	☐

Apply

Reset all groups to default settings

- One user group is associated with each user and specifies what features are available.
- Some features not listed here are only available for the admin user.
- The Admin user group cannot be changed, neither can the group names of the four first groups.

The *admin* user can define access rights for up to ten different user groups. Four pre-defined user groups will often be sufficient, but the *admin* user can create an additional six user groups. The pre-defined user groups *Normal*, *Privileged* and *Restricted* can be edited, but the *Admin* user group cannot be altered. Note



that some access rights, such as editing users, are only available to the admin user. Hence a user in the Admin user group will not have all the access rights that the admin user has.



6.18 Main — Logs

6.18.1 Logs — Logs

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

ALARM SETUP

TIMELINE

REPORTS

EXT. REPORTS

MAIN

SITES AND USERS

LOGS

SNAPSHOTS

ALARM STATISTICS

STREAM GROUPS

SERVICE GROUPS

ARCHIVE SETUP

ARCHIVE DURATIONS

GFX. VIEW SETUP

GENERAL

NETWORK

ABOUT

LogsSettings

Log export

Select date and time to generate log from:2020-Aug-0700:00

Or generate log with only active alarms☐

Search filters

All these texts must match: (AND)Any of these texts must match: (OR)

Export as HTML

Export as XML

Clear search filters

- The generated log will be from the selected time for all sites that user has access to
- The historic report will contain only cleared alarms
- The log database is the cleared alarms for the last last **90** days and the database window can be changed by the admin user
- The log database is currently **782033** lines which corresponds to **362** new alarms every hour
- The server performance is heavily affected by alarm processing, so keeping the number of alarms low is key to improve performance and response times

In the **Logs** view it is possible to export an alarm log listing all cleared alarms from all sites the current user has access to. The log start time is selected using the drop-down menus, and the export is activated by clicking the *Export HTML* or *Export XML* links.

By using the filtering functionality it is possible to select that only alarm entries matching specific text strings should be exported. Text string requirements specified in the three leftmost entry fields should all be fulfilled for an alarm entry to be exported (logical AND function). At least one of the text string requirements specified in the three rightmost entry fields should be fulfilled for an alarm entry to be exported (logical OR function).

Clicking one of the *Export* links will present up to approximately 10000 alarms in a pop-up window. Clicking the *Clear search filter* link will clear the search filter entry fields.

The number of days the log is kept is set in **Logs — Settings**.



6.18.2 Logs — Settings

Logs

Settings

Log settings

Keep history: 90 days ▼

Apply

- This parameter specifies how long to keep past alarms available for log export in the Logs menu
- More alarms in the log database results in longer processing times

The **Logs — Settings** view allows the user to specify for how long alarm history should be stored and available for export in the Logs view. Note that a large number of alarms stored in the database will result in longer processing times.



6.19 Main — Snapshots

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

ALARM SETUP

TIMELINE

REPORTS

EXT. REPORTS

MAIN

SITES AND USERS

LOGS

SNAPSHOTS

ALARM STATISTICS

STREAM GROUPS

SERVICE GROUPS

ARCHIVE SETUP

ARCHIVE DURATIONS

GFX. VIEW SETUP

GENERAL

NETWORK

ABOUT

Restore snapshotAdd snapshotImport snapshot

List of available snapshots

Manual snapshotsAutomatic snapshotsImported snapshots

Name	Size	Description
snapshot_2020-03-26 15:23:23_manual.tgz	89.58 MB	Secondary Cleanup 260320
snapshot_2020-06-25 13:04:23_manual.tgz	89.63 MB	RDW
snapshot_2020-09-09 04:11:36_manual.tgz	89.69 MB	test
snapshot_2020-03-25 12:37:42_manual.tgz	89.58 MB	Primary Cleanup 250320

Restore blade-configs from snapshot: ☒ Restore selected snapshot

Status last snapshot restore: [View](#)

- Restoring a snapshot will restore all VBC settings and data except for long-term data such as report- and alarm-data.
- Blade configs are restored from snapshot if checkbox is selected - this will overwrite the probes current config.

A snapshot is a recording of all settings for both the VBC and for probes and extractors. A snapshot does not contain long-term data, such as alarms, stream data and reports, because that would make the snapshots too big to be useful.

The system takes automatic snapshots every night and keeps them for 30 days. When restoring a snapshot the user can select whether to also restore the blade configurations.

It is possible to export a snapshot from one VBC and restore it on another VBC. This is useful in order to synchronize two VBC servers. This operation can be performed manually, as well as via scripting. The two VBC servers need to be running the same version. The maximum supported size of a snapshot import is presently 25 Mbyte.

An example script for synchronizing two VBCs can be found in the following location of an installed VBC: /opt/btech/vbc/bin/sync_main_and_backup

The 6.4 release version of this script is listed below and has explanatory text embedded.

```
#!/bin/bash
#
# Please run this script in a separate folder with write access.
# This script detects changes to the MAIN_VBC and copies them to the BACKUP_VBC.
# The snapshot mechanism is used, as documented in the EII document available from site.
# The script must be run on the MAIN_VBC, as it needs to be able to access
# the created snapshot files.
#
# These parameters must be updated:
MAIN_VBC="10.0.30.99"
BACKUP_VBC="10.0.28.215"
```



```
DELAY=60

while true
do

date
echo "Time for syncing backup VBC"

echo "Step 1: Create a snapshot for scripted export"
wget -q http://$MAIN_VBC/vbc/snapshots?create="For copying to backup VBC" -O status1.xml
if grep -q "success=\"false\"" status1.xml ; then echo "FAILED - see status1.xml for details"; fi

# Keep the last two archives
cp snapshot.tgz prev_snapshot.tgz > /dev/null 2>&1

echo "Step 2: Obtain snapshot"
cp /opt/btech/vbc/configs/snapshots/snapshot_scripted.tgz snapshot.tgz

echo "Step 3: Check if it has changed"

# remove previously extracted snap, then extract current snapshot
rm -r current_ss > /dev/null 2>&1
mkdir current_ss > /dev/null 2>&1
tar xzf snapshot.tgz -C current_ss

# remove files which are not significant
rm current_ss/opt/btech/vbc/sites/channelstatus_extr.xml
rm current_ss/opt/btech/vbc/sites/channelstatus.xml
rm current_ss/opt/btech/vbc/sites/status.xml
rm -r current_ss/opt/btech/vbc/configs/lastminute/

# Compare to see if snapshot content has changed or first time
if [ ! -d prev_ss ] || ! diff -r current_ss prev_ss; then
    echo "Step 4: Post snapshot to backup server"
    wget -q --post-file=./snapshot.tgz http://$BACKUP_VBC/vbc/core/data/snapshot -O status4.html
    if grep -q INVALID status4.html; then echo "FAILED - see status4.html for details"; fi

    echo "Step 5: Request backup server to restore imported snapshot"
    # Note that providing restore=1&restoreBladeConfigs=1 will restore the blade configs from the snapshot as well
    wget -q "http://$BACKUP_VBC/vbc/snapshots?restore=1" -O status5.xml
    if grep -q "success=\"false\"" status5.xml ; then echo "FAILED - see status5.xml for details"; fi

# rotate
    rm -r prev_ss > /dev/null 2>&1
    mv current_ss prev_ss
else
    echo "No change"
fi

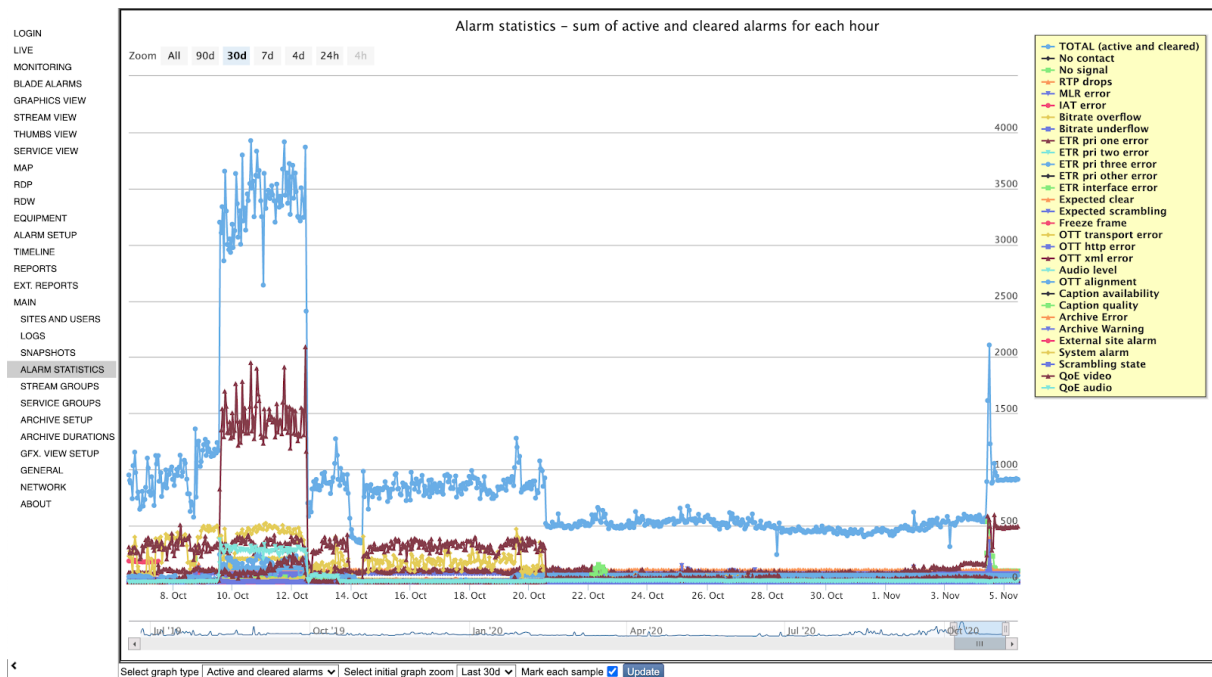
echo "Done"

sleep $DELAY

done
```



6.20 Main — Alarm statistics



The alarm graph is useful for trending the alarm counts over periods of time. This could be useful for a number of purposes, including

- identifying patterns to when alarm storms happen.
- determining the need to perform more tuning of thresholds and scheduling.
- lowering the load on the VBC server — lowering the number of alarms in a system will considerably lower the load on the server.

The alarm counts are provided per hour for the last 30 days. After 30 days they are aggregated per day, until they are deleted after two years.

Available graph types

Active alarms only	Plots the number of active alarms 15 minutes after each hour. Systems with many continuous alarms will show a consistently high number of active alarms.
Cleared alarms only	Counts the number of times alarms were cleared during each hour. In systems with lots of transient alarms this number will be high.
Active and cleared alarms	Aggregates the counts for the Active and Cleared alarm graphs.

Note that when 24 hours are aggregated into a one-day value, the peak value is used. The TOTAL graph is the sum of all elementary alarm counts in the graph. The TOTAL value is not stored in the database, but is derived from the values in the graph. For day aggregated values, the TOTAL graph will likely show a higher value than before aggregation, since after aggregation it sums the peak values across the entire day, and not per hour.



6.21 Main — Stream groups

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

ALARM SETUP

TIMELINE

REPORTS

EXT. REPORTS

MAIN

SITES AND USERS

LOGS

SNAPSHOTS

ALARM STATISTICS

STREAM GROUPS

SERVICE GROUPS

ARCHIVE SETUP

ARCHIVE DURATIONS

GFX. VIEW SETUP

GENERAL

NETWORK

ABOUT

Stream setup

Name	Description		
[All streams]	All streams. Cannot be edited.		
AJZ		Edit	Delete
ASI		Edit	Delete
COFDM	DVB-T multiplexes	Edit	Delete
Content checked		Edit	Delete
Demo	Demo	Edit	Delete
HD Services		Edit	Delete
HeadEnd		Edit	Delete
NRK 1 HD		Edit	Delete
NilsTest		Edit	Delete
OTT	OTT headEnd	Edit	Delete
Premium	Must be monitored	Edit	Delete
SD Services		Edit	Delete
Thor5 - C11	freq: 11372V, 24500, FEC7/8	Edit	Delete
Training		Edit	Delete
YLETV	Testing for Digita	Edit	Delete
satellite	monitorizar satellite	Edit	Delete

Stream properties

Name

Description

Make available to all users ☐

Available streams

NRK1 HD (RTP)

10.747 Thor

239.255.77.14_5500

239.255.77.34_5500

239.255.77.3_5500

239.255.77.72_5500

256 MHz

264 MHz

272 MHz

280 MHz

290 MHz

298 MHz

Selected streams

⇒

⇐

Add new

Each individual user may arrange the system's streams in different stream groups, the configuration being unique to each user. The MicroTimeline for each stream group in the **Monitoring** page then makes it simple to get an overview of the current and historical status for each group. The user can also select to view MicroTimelines for streams belonging to one particular stream group in the **Stream view**, and it is possible to create reports including selected stream groups only. Each stream group has a name and description assigned to it, and streams are selected by clicking an available stream and moving it to the 'Selected stream' window by clicking the arrow button. When stream selections have been made, the stream group is generated by clicking the **Add new** button.

For the admin user stream-groups can be edited on behalf of all users by checking the *Make available to all users* check box.



6.22 Main — Service groups

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDV

RDW

EQUIPMENT

ALARM SETUP

TIMELINE

REPORTS

EXT. REPORTS

MAIN

SITES AND USERS

LOGS

SNAPSHOTS

ALARM STATISTICS

STREAM GROUPS

SERVICE GROUPS

ARCHIVE SETUP

ARCHIVE DURATIONS

GFX. VIEW SETUP

GENERAL

NETWORK

ABOUT

Service group setup

Name	Description		
[All services]	All services. Cannot be edited.		
ComHem		Edit	Delete
NRK Channels		Edit	Delete
Radio services	All radio services	Edit	Delete
Test	Test	Edit	Delete
Viasat_4	on DVB-T muxes	Edit	Delete

Service group properties

NameBBC

DescriptionAll services

Make available to all users☐

Available services

3sat

4K Universe

Al Jazeera Channel

Animal Planet

Anirang TV

BB-MV-LokalTV

BDL VoD

Beate Uhse HD

Boomerang

C More First

C More Hits

C More Series

More...

Selected services

BBC BRIT HD (N)

BBC Brit

BBC Earth

BBC WORLD NEWS

BBC World News

Add new service group

Each individual user may arrange the system's services in different service groups, the configuration being unique to each user. For the admin user service groups can be made available to all users by checking the *Make available to all users* check box.

Each service group has a name and description assigned to it, and services are selected by clicking an available service and moving it to the 'Selected services' window by clicking the arrow button. When service selections have been made, the service group is generated by clicking the **Add new** button.

The service groups are used in the **Service view** pages to be able to easily filter the display to only show the selected services. This makes it easy to filter the display to show status for instance for all radio channels, all channels from a specific broadcaster or all channels from a specific country. When generating **Ext. reports** the report can be made to show status for a specific group of services. In some countries government regulations say that a PDF report should be created each week and sent to the authorities. The report should be limited to a set important national channels.



6.23 Main — Archive Setup

The Archive server is a stand alone server, but it needs VBC to be configured. When configured, the Archive server goes out to the various devices, and pulls data into the storage back-end. Later, to review the data stored, one uses the **Timeline** view on the VBC to inspect the data. Refer to chapter 6.14 for details on the Timeline view.

6.23.1 Archive server

The Archive server runs on a separate machine, but can on small installations run on the same machine as other software.

The Archive server is no longer being sold, and we instead recommend using the **Timeline** feature of the Software Probe.

License

The archive server comes with a license defining how many streams one can assign to it. Each unique stream name count as one stream. You can archive the same stream, from multiple sources, using only one slot of the license. If you are archiving a stream named XYZ and XYZ HD they will count as two streams. To avoid that you can give them different class names, as XYZ@SD and XYZ@HD.

For N streams an ARCHIVE-SERVER-N license is required. The number of aggregated services which is used to scale the server hardware does not correspond to the N in the license. 100 probes archiving the same 5 streams only requires a ARCHIVE-SERVER-5 license, but the hardware would need to be scaled for 500 services.

Network requirements

The Archive server needs to be able to access the VBC Controller server over either port 80 (http) or 443 (https) to retrieve its configuration.

The Archive server also needs to be able to access all probes that it has been configured to read information from through port 80 (http) without authentication (i.e., **Setup — Security — Authentication** must have **Authentication method** set to **Disabled**).

6.23.2 Connecting the Archive server

Setup Data About

Archive Server

VBC address: HTTP example.com

Apply

[Change network configuration](#)

Alarms:

To configure the Archive server, select the host name and protocol (http or https) it should use to connect to the correct VBC server.

On the VBC server, add the archive server as a new device, as described in chapter 6.12. Please note that you can only add one archive server per VBC server.



6.23.3 Configuration

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

ALARM SETUP

TIMELINE

REPORTS

EXT. REPORTS

MAIN

SITES AND USERS

LOGS

SNAPSHOTS

ALARM STATISTICS

STREAM GROUPS

SERVICE GROUPS

ARCHIVE SETUP

ARCHIVE DURATIONS

GFX. VIEW SETUP

GENERAL

NETWORK

ABOUT

Archive Stream Setup

Stream Name	Interf...	Blade	Thumbnails	Closed Capti...	Audio Loudn...	Media Window	EPG	VMAF	Edit
test2	IPTV	VB330 SW v6.0	✓		✓	✓			Edit
test1	IPTV	VB330 SW v6.0	✓		✓	✓			Edit
test0	IPTV	VB330 SW v6.0	✓		✓	✓			Edit
Wowza Cam SS	OTT	VB288	✓						Edit
Viasat 4 HD	IPTV	VB288	✓		✓				Edit
TV 2 HD (N)	IPTV	VB288	✓		✓				Edit
Smooth Stream Test	OTT	VB288	✓		✓				Edit
Nat Geo HD (N)	IPTV	VB288	✓		✓			✓	Edit
NRK1 HD	IPTV	VB288	✓		✓				Edit
NRK 1@Akamai	OTT	VB288	✓		✓			✓	Edit
Hyperdeck_p1@main	IPTV	VB330 SW v6.0	✓			✓			Edit
GOLD905 PREM	OTT	VB288	✓		✓			✓	Edit
CamHD_p1@main	IPTV	VB330 SW v6.0	✓			✓			Edit
NRK3 DASH	OTT	QTT Extractor	✓						Edit
AppearTV	OTT	QTT Extractor	✓						Edit
SL99	OTT	QTT Extractor	✓						Edit
SL86	OTT	QTT Extractor	✓						Edit
SL01	OTT	QTT Extractor	✓						Edit
BipBopQTT	OTT	QTT Extractor	✓						Edit
SL93	OTT	QTT Extractor	✓						Edit
SL85	OTT	QTT Extractor	✓						Edit
SL69	OTT	QTT Extractor	✓						Edit
SL66	OTT	QTT Extractor	✓						Edit
SL60	OTT	QTT Extractor	✓						Edit
SL53	OTT	QTT Extractor	✓						Edit
SL48	OTT	QTT Extractor	✓						Edit
SL44	OTT	QTT Extractor	✓						Edit
SL32	OTT	QTT Extractor	✓						Edit

Streams in use: 49 of 500

Add new stream

Delete selected

Edit selected

To configure what you want to archive you must go into the VBC, select MAIN, and then ARCHIVE SETUP. From that view you can add new streams to archive, remove streams, or edit what to archive.

To configure how long to store the different kinds of data, you must go into MAIN and then select ARCHIVE DURATION.

6.23.4 Alarms

There are three kinds of alarms, one for having too many streams configured, and one for when the disk is filling up. If too many streams have been configured, the Archive server will stop archiving more data. To fix that, either add more streams via a new license, or change the configuration to decrease the number of configured streams.

When you get an alarm saying the disk is getting full, you can change the configuration to keep it for a shorter duration, or add more disk to the server.



6.24 Main — Gfx. View Setup (Graphics option)

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

ALARM SETUP

TIMELINE

REPORTS

EXT. REPORTS

MAIN

SITES AND USERS

LOGS

SNAPSHOTS

ALARM STATISTICS

STREAM GROUPS

SERVICE GROUPS

ARCHIVE SETUP

ARCHIVE DURATIONS

GFX. VIEW SETUP

GENERAL

NETWORK

ABOUT

Current network diagram

Default network diagram DemoSystemSatMux.svg

Background color #dddddd

Apply

Edit network diagram

#	Enabl...	Filename	Description	Bg color	View box	scaling	
1	☒	no_diagram_present.svg	Please change th...			Scaled centered	Edit
2	☒	BridgetechNetwork.svg				Scaled centered	Edit
3	☒	menu2.svg				Scaled centered	Edit
4	☒	map.svg	Map over Norway...			Scaled centered	Edit
5	☒	Headend_content.svg	Extractors			Scaled centered	Edit
6	☒	DemoSetup.svg	NAB Demo System			Scaled centered	Edit
7	☒	Network_diagram.svg				Scaled centered	Edit
8	☒	Network_diagram_strip...				Scaled centered	Edit
9	☒	menu3.svg				Scaled centered	Edit
10	☒	USA_map.svg				Scaled centered	Edit
11	☒	channels.svg				Scaled centered	Edit
12	☒	vbc_netdiagram_button...	Heavily compress...	#ffffff		Scaled centered	Edit
13	☒	Ukraine_regions_map.svg				Stretched	Edit

Add new

Delete selected

Edit selected network diagrams

The **Main — Gfx. View Setup** is used to configure the diagrams available in the **Graphics View** and the Graphics Widget in the Remote Data Wall.

6.24.1 Configure diagrams

The diagram objects must be configured in Microsoft® Visio or Inkscape before uploaded to the VBC. There are some small differences in the two programs on how to do this, as shown in the table below.

NB! The mappable drawing objects must have closed perimeters (due to color fill).

Microsoft Visio	
Configuration	How to
Make an object in diagram alarm status mappable	In Data — Define Shape Data set Label to “displayCurrentStatus” and Value to “*/*/*/*”
Make click-through to another diagram	Set the objects hyperlink to “name of another diagram.svg”
Make click-through to VBC selected blade	Set the objects hyperlink to “displayBlade=<VBC blade name>” (do not include the <> characters in the actual string)
Make click-through to VBC selected stream view	Set the objects hyperlink to “displayStreamView=<VBC stream name>” (do not include the <> characters in the actual string)



Export .svg file	Export — Change File Type — Save As “SVG Scalable Vector Graphics (*.svg)”
<i>Inkscape</i>	
<i>Configuration</i>	<i>How to</i>
Make an object in diagram alarm status mappable	In Object Properties set Label to “displayCurrentStatus:*/*/*/*”
Make click-through to another diagram	Set the objects hyperlink (Href:) to “name of another diagram.svg”
Make click-through to VBC selected blade	Set the objects hyperlink (Href:) to “displayBlade=<VBC blade name>” (do not include the <> characters in the actual string)
Make click-through to VBC selected stream view	Set the objects hyperlink (Href:) to “displayStreamView=<VBC stream name>” (do not include the <> characters in the actual string)
Export .svg file	Save file as type “Inkscape SVG (*.svg)”

Note: The special string “*/*/*/*” is a wildcard for any mapping combination of “Site/Blade/Stream/Streamgroup”.

To set mapping directly in drawing simply replace * with the corresponding name in VBC.

The settings in the table above will make diagram objects configurable in the Graphics view pop-up window **Configure data mapping for diagram**. After a diagram object has been configured/mapped properly, the graphic element in the diagram will display color codes according to the current alarm status of the element.

<i>Color codes</i>	
Blue:	The graphic element has not been configured to a Site, Blade, Stream or Stream group.
Green:	The configured element has no alarms triggered.
Yellow:	Warning alarm on the configured element.
Orange:	Error alarm on the configured element.
Red:	Major alarm on the configured element.
Black:	Fatal alarm on the configured element.

6.24.2 Setup and data mapping

Uploading of drawing

To upload a drawing, click on **Main — Gfx. View Setup**. Then choose **Add new** or **Edit selected** to get to the configuration pop-up windows **Edit network diagram** and **Configure data mapping for diagram**.

<i>Edit network diagram</i>



File name:	Filename of the uploaded file.
Description:	A given description of the selected file.
Background color:	The background color should be written as either a text string, e.g “dimgrey” or as a hexadecimal color, e.g “#12a628”
Enabled:	Is the selected network diagram enabled?
View box:	The diagram will use this view box entry instead of the one specified in the .svg file.
Scaling:	Select the type of scaling wanted on the uploaded .svg file.

Click **Upload diagram file** to add a new network diagram. Then choose a .svg file from your computers file system and click the **Go!** button. The import status will show when the diagram is successfully uploaded (or in case of error state the cause). Close the **Upload diagram** pop-up and click **Configure data mapping**.

Edit network diagram

#	Enabl...	Filename	Description	Bg color	View box	scaling	
46	✓	USA_map_blank_south....				Scaled centered	Edit
50	✓	32 CableInputSVG.svg		0000		Scaled centered	Edit
56	✓	Test 1c(inkscape).svg				Scaled centered	Edit
63	✓	GfxViewDemo.svg				Scaled centered	Edit
94	✓	DemoSystemSatMux.svg				Scaled centered	Edit
96	✓	MUX_Astra_1L_26.svg				Scaled centered	Edit
97	✓	MUX_Thor_5_C2.svg				Scaled centered	Edit
98	✓	DemoSystemOverview....				Scaled centered	Edit
107	✓	TrueVisionsSatMuxes....				Scaled centered	Edit
109	✓	DemoSystemExample.svg				Scaled centered	Edit
123	✓	Olli_USA.svg	Olli test	c0c0c0		Scaled centered	Edit
124	✓	Olli_SD.svg	Olli test	00ffff		Scaled centered	Edit
125	✓	alarms.svg				Scaled centered	Edit

Add new **Delete selected** **Edit selected network diagrams**

Added diagram

Configure data mapping for diagram

SVG object ID	OK	Set ...	Site	Blade	Stream	Stream group	
group294-641			HEADEND_CORE	Probe1	[Match any stream]	[No mapping]	Edit
group68-254			OSLO_DVB-S2	P2	[Match any stream]	[No mapping]	Edit
shape46-144			OSLO_DVB-S2	P2	Astra 11597 V - SAT	[No mapping]	Edit
shape49-162			OSLO_DVB-S2	P2	Thor 11229 H - SAT	[No mapping]	Edit
shape60-212			[Match any site]	[Match any blade]	[Match any stream]	Astra 1L - 26	Edit
shape610-903			HEADEND_CO...	Extractor288	[Match any stream]	[No mapping]	Edit
shape63-230			[Match any site]	[Match any blade]	[Match any stream]	Thor5 - C2	Edit

Edit selected objects

Diagram preview

OSLO HQ - Demo System SAT / MUX

Edit network diagram

Parameter	Value	Description
File name	DemoSystemSatMux.sv	Upload new file to change
Description		Description of the diagram
Background color		The background color to use when displaying the page
Enabled	☒	Only enabled diagrams can be used
View box		If specified the diagram will use the specified view box instead of the one specified in the .svg file
Scaling	Scaled centered	Specifies how the diagram is scaled

Close **Apply changes** **Upload diagram file** **Configure data mapping**

Configure data mapping for diagram

SVG object ID:	The id of the object in the selected .svg file.
OK:	Checked if the object is correctly mapped to an element.
Set man.:	Checked if the selected object was configured manually in pop-up Edit object data mapping .
Site:	The name of the selected site.
Blade:	The name of the selected probe or extractor.
Stream:	The name of the selected stream. Including interface if individual stream selected, only stream name in case of aggregated stream status.
Stream group:	The name of the selected stream group.
Edit:	Press the edit link to change the settings of the selected object.



The diagram will be displayed in a preview window. Diagram objects are selected from the table in the pop-up **Configure data mapping for diagram**. Selected objects in the table will start blinking pink and yellow in the diagram preview window. The selected object(s) are then mapped to VBC elements Site, Blade, Stream or Stream group by choosing from drop-down selectors in the separate **Edit object data mapping** editing window.

Note: Mapping of a Stream group will override any other mapping combination of Site/Blade/Stream. Leave Stream group on [No mapping] for other mappings.

To choose an aggregated stream status, simply select [Match any site/blade] + the desired stream from the drop-downs. For mapping of a blade specific stream status select the desired Site, Blade and Stream. Remember to click **Apply changes**.



6.25 Main — General

The **General** page contains system affecting parameters that the *admin* should treat carefully. Clearing stream view data or alarm lists will however not affect Reports data.

6.25.1 General — Clear

LOGIN

LIVE

MONITORING

BLADE ALARMS

GRAPHICS VIEW

STREAM VIEW

THUMBS VIEW

SERVICE VIEW

MAP

RDP

RDW

EQUIPMENT

ALARM SETUP

TIMELINE

REPORTS

EXT. REPORTS

MAIN

SITES AND USERS

LOGS

SNAPSHOTS

ALARM STATISTICS

STREAM GROUPS

SERVICE GROUPS

ARCHIVE SETUP

ARCHIVE DURATIONS

GFX. VIEW SETUP

GENERAL

NETWORK

ABOUT

Clear

Connections

Preferences

Authentication

Sync

Clear streams

Clear

Clearing the streams will clear 4 days of history for all streams including the 96 MicroTimeline graphs and error second statistics. The Report feature is not affected.

Clear alarm lists

Clear

Clearing the alarms will flush all visible alarm lists and allow them to rebuild completely. The log files are not affected. The SNMP alarm list is also rebuilt and traps are sent accordingly.

Clear streams

If the Stream view history has been polluted (for whatever reason – maybe a problem that caused lots of errors has been solved) and the *admin* wants to clear the 4 days of stream history, he can click the appropriate Clear button. The last clear-time is presented inside the frame.

Note that after clearing, the stream bars will take 4 days to fully rebuild.

Clear alarm lists

To clear all the alarm lists (except currently active alarms) click the Clear button. The alarm history will be gone but active alarms will start to re-appear. The last clear-time is presented inside the frame.

If the SNMP settings have been changed, clearing the alarm lists will immediately rebuild the SNMP alarm list and send clear-traps for alarms that are no longer applicable.



6.25.2 General — Connections

Clear

Connections

Preferences

Authentication

Sync

Connection

ID web connections by IP address ☒ If checked, a client is identified by IP address AND the returned cookie (default). If cleared, only the cookie is used. VBC requires clients to have cookies enabled in their browser.

Apply

Identification

System name

System name used to identify server

Organization

Name of organization owning server

System contact

Contact person for this server

System location

Physical location of server

The information here will be used to identify the system over SNMP, and when using the license activation interface.

Apply

Outgoing mail server

Mail server:

localhost

Mail port:

25

Sender addr:

The mail server, port number and sender address used for distributing the automatic reports.

Apply

Connection

ID web connections by IP address: A VBC user may be recognized by the system either by a browser cookie only or by the combination of his IP address and the browser cookie (default).

Identification

System name: Each system can be assigned a user-defined name. It is part of the system's MIB. The name is also used for identifying the system when activating the license on-line, see J Appendix: On-line License Activation for more details.

Organization: The name of the organization (usually the company name) that is running the system. This name is only used for identifying the system when activating the license on-line.

System contact: The system contact is part of the system's MIB, and this parameter is relevant for SNMP use only. It is used to identify the contact person responsible for this system.

System location: The system location is part of the system's MIB. It is used to identify the physical location of the system.
This name is also used for identifying the system when activating the license on-line.

Outgoing mail server

To get the VBC to send alarms and reports by email to recipients an outgoing mail server must be configured.

If the configuration is a domain name, such as mail.example.com, make sure that the DNS settings on the server are configured properly.

Please note that VBC requires an SMTP server that allows it to send email without authentication or encryption. If a more complicated email setup is required, it is possible to install a Mail Transport Agent



(MTA) directly on the VBC server and set up the VBC to connect to it, by setting the outgoing server to localhost. Please refer to the system documentation³ for details on setting up a local MTA.

Please note that the emails may end up being caught by spam filters. Please make sure that exception rules are added if needed so that these messages are not classified as spam.

6.25.3 General — Preferences

Clear Connections Preferences Authentication Sync

Various

Max link:

Reporting character set:

Date format:

Time zone:

License activation proxy:

Hostname in reports:

Autofit pages: ☒

Apply

Provide links to this number of items in Stream View, Service View and Thumbs View (default: 400).

Select character set for non-ASCII strings in reports

Select the date format to use in VBC

Set time-offset relative to UTC time

URL for proxy server (http://proxy.host:port)

Hostname (or IP address) of VBC used in HTML reports for linking to BLADE ALARMS page

Reorganize content and hide less important fields to fit smaller screens

Various

Max link:	The number of links in the Stream view, Service view and Thumbs view, where maximum is 999 and 100 is the minimum. 400 is default.
Reporting character set:	This selects which character set is to be used for reports for non-ASCII characters, i.e., letters outside the A–Z range. The default choice is Multi-lingual , which covers most non-ideographic languages. When using site, stream or service names that contain ideographic characters, you can select the appropriate character set and style from one of Simplified Chinese , Traditional Chinese , Japanese and Korean .
Date format:	The date format used in the user interface can be changed here. Dates exported through machine-readable interfaces are not affected by this setting.
Time zone:	By setting the time zone the VBC Controller time can be offset from the reference NTP time. Please note that this changes the global time zone on the system running the VBC Controller.
License activation proxy:	When using on-line activation, the VBC needs to be able to connect to the license activation server. If the VBC is not connected directly to the Internet, you can add the URL to a proxy server that it can use here. If not configured, the VBC will try to use the local proxy installed on the host.
Hostname in reports:	The specified IP address or hostname specified here will be used in HTML report to reach the Blade Alarms view when clicking links in the report.
Autofit pages:	If enabled, some content is re-organized and some less important fields hidden, to fit smaller screens.

³<https://ubuntu.com/server/docs/how-to>



6.25.4 General — Authentication

Authentication

The authentication in the VBC Controller can be set to *Local users* (the default) or *Tacacs+*. Local users are configured using the **Main — Sites and Users — Users** view and makes it possible to define different access levels for different users.

Authentication method

Tacacs+ When accessing the VBC with a web browser, users needs to authenticate themselves with a username and password. These need to match the pre-defined **admin** user, a user available on the Tacacs+ server configured through the **Tacacs+** view, or any of the users configured in the **Main — Sites and Users — Users** view.

Local users When accessing the VBC with a web browser, users needs to authenticate themselves with a username and password. These need to match either the pre-defined **admin** user, or any of the users configured in the **Main — Sites and Users — Users** view. This is the default setting.

The message entered in the **Login message** text field will be displayed to the user in the **Login** view before logging in.

Tacacs+

This view is used to configure a Tacacs+ server for user authentication. For this to be used, Tacacs+ authentication must be selected in the **Authentication** view.



To use Tacacs+ authentication, the IP address of the Tacacs+ server must be specified, along with the secret key used to encrypt the communication between the Tacacs+ server and the VBC server. The same key must also be specified as part of the Tacacs+ server configuration.

The VBC server does not relate to the Tacacs+ accounts directly. The VBC only receives a reply from the Tacacs+ server whether the login was successful or not. If the login was successful the user will proceed into the VBC Controller as if he had logged directly into VBC as the *Local user* specified in this view, meaning that all Tacacs+ authenticated users will use the same local user account.

We recommend using HTTPS when using authentication, as this combines authentication with encryption. Using authentication with HTTP is not considered very secure since it is possible to sniff the un-encrypted communication and possibly reverse engineer the scrambling of login details.

<i>Tacacs+ parameters</i>	
Server IP address	IP address of the Tacacs+ server used for authentication.
Secret	Configures a fixed string used to encrypt the communication with the server.
Default local user	The VBC user account used when logging in using Tacacs+ authentication.
Auth-key	Defines which key in the Tacacs+ authentication response to use to determine the user access level. The value of this key is compared to the Access level below.
Access level 1–3	Up to three different Tacacs+ access levels can be configured to map to different local user accounts, allowing different authenticated users to have different access levels. The value configured here is matched with the value of the Auth-key configured above.

6.25.5 General — Sync

Clear

Connections

Preferences

Authentication

Sync

Sync device names

Sync

Synchronizes the blade name of active devices from the device name specified in the Equipment page

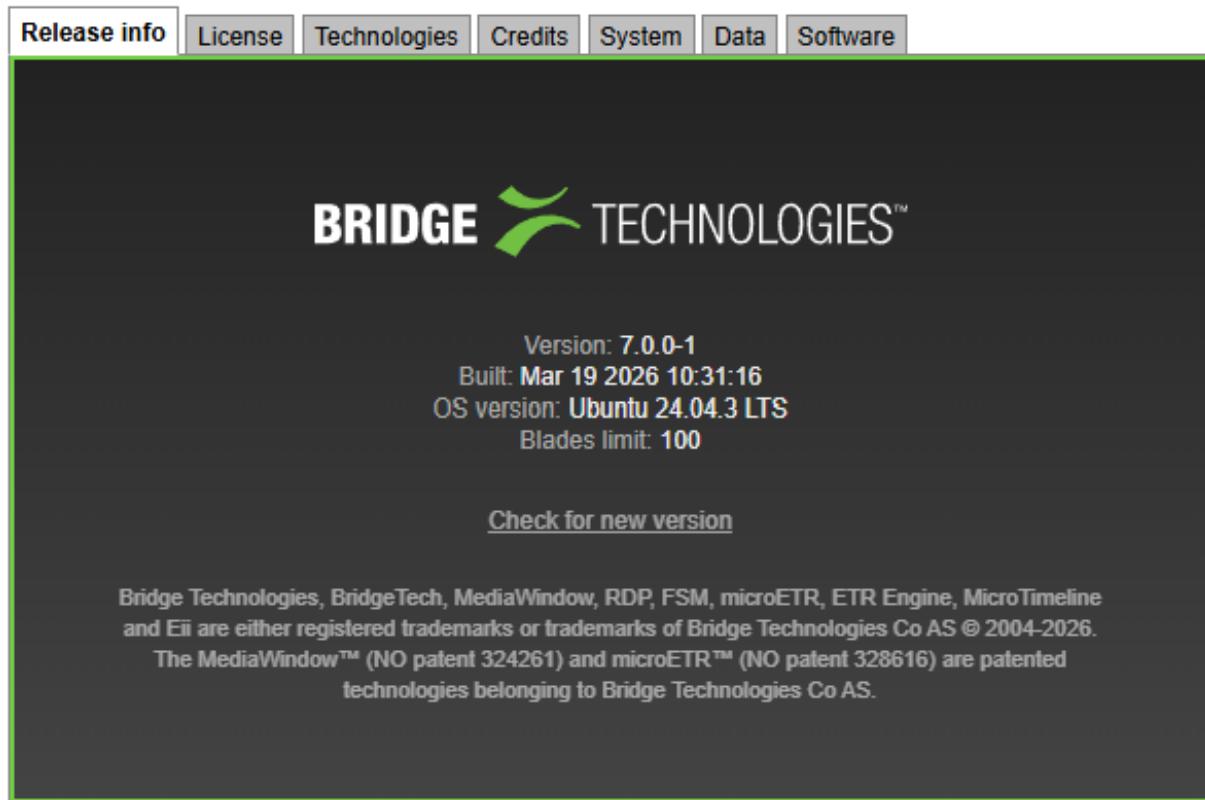
This view can be used to synchronize the connected devices with the device names configured in the **Equipment** view. When pressing the **Sync** button, the connected devices will have their device names updated with the information stored on the server.

To update the name in the **Equipment** view from the device, use the **Fetch device name** feature in the **Edit device** view.



6.26 Main — About

6.26.1 About — Release info



This view shows the product name, software version, the software build date and the version of the underlying operating system for the VBC Controller.

If the system has been able to contact the license activation server, you can click the **Check for new version** link to see whether a new software release is available. For more information on on-line license activation, see J Appendix: On-line License Activation.



6.26.2 About — License

Release info

License

Technologies

Credits

System

Data

Software

Available options

Installed	Option code	Option name	Details
✓	VBC-1000	VBC license for up to 1000 networked blades	i
✓	TSSV-OPT	Transport Stream Service View	i
✓	GRFX-OPT	Graphics Display Extensions Package	i
✓	RDW-OPT	Remote Data Wall	i
	MASTER-OPT	Master VBC	i

Current license details

VBC status: Permanent
System ID: 564D6FD4-B8F3-1170-067D-186F8D005206
Hardware key: 0044-731E-46F9-276E-BEA3
Current license: Verified
Production date: 2019 Feb 21

License key

Product license key:

The license has been activated on-line and will be verified periodically.
Note: Changing the feature license key will restart the main process!

Manage license activation

The current license does not require on-line activation.

If you release the license, you will need to enter the license key again to re-activate it.

Manage server

Access the administrative interface:
[Manage server](#)
If you deactivate the software, you will need to use the administrative interface to re-enable it.
☒ Activate VBC

The **License** view displays the currently active license. The license includes the number of blades supported by the VBC and whether the **Transport Stream Service View**, **Graphic Display Extensions Package Remote Data Wall** and **Master VBC** options are available. By clicking the blue information icon associated with each option it is possible to view option details.

The license key is activated towards a license server. Depending on the license properties, the activation might need to be updated periodically. The key is transferable between systems running the same software, as long as the license is not permanently assigned to a system. The system identifier is used to identify the system. The **Current license** field will display information on when the license key was last activated and possibly when it needs to be activated again. Click the **Renew** button to immediately renew the license with the license server.

Click the **Release** button to remove the current license, making it available to another host. Please make sure you have the license key available before you do this, as you must enter it again on the system you wish to transfer the license to. If you have lost the license key, contact your dealer to retrieve it. Make sure you include all details from this page in your request.

Please refer to J Appendix: On-line License Activation for more information on how to use on-line activated licenses. This appendix also describes how to renew the license when the VBC Controller cannot connect to the Internet.

Please refer to K Appendix: Software Maintenance for more details on software maintenance licenses.

Click the **Manage server** link to access the Cockpit administrative interface, see chapter 2.4 for more information.



To disable the VBC Controller, uncheck the **Activate software** checkbox and click the **Change** button. You cannot do this if it has been set as the default software through the administrative interface (which is done by default the first time you activate the software), you will need to remove it as the default before disabling VBC Controller. See chapter 2.12 for more details.

Current license details

VBC status:	This shows information about the current status of the license. Activated indicates a license has been activated successfully, and Permanent indicates a non-transferable on-line activated license. Demo license indicates a time-limited license, and also indicates the time remaining. Not activated means that the system does not have a valid license; if the status says Not activated yet, the system has a valid license but the system time is set incorrectly to a time before the activation. If the status says activation period has expired, the system has a valid license, but the activation period has expired, either because the system has not been able to renew the license or because the system time is set to be into the future. Element Manager mode is enabled if the VBC Controller does not have a valid license, or if the software maintenance license does not cover the installed version. Please refer to J Appendix: On-line License Activation for more information on how to use on-line activated licenses.
System ID:	The unique ID used to identify the system. This is a property of the system hardware, and will remain even if reinstalling the system. This ID is used to tie the license to the system. In the unlikely event that the hardware is missing this information, a number will be generated and the word “overridden” will be shown after the number.
Current license:	Verified indicates that the current license was read properly; when using a license that is not permanent, the time the license was last verified against the license activation server is also displayed. Off-line indicates that the current license has not been verified against the license activation server. The message will also include information about when the license activation must be renewed to avoid losing access to the license. Checked indicates that the system does not have an activated license, and includes the time when the status was last checked with the license activation server. Unknown is displayed if the activation status could not be determined, this is often because the system time is configured incorrectly.
Production date:	Displays the date when the system was produced.
Software maintenance period:	Displays the end date of software maintenance for the currently attached license. Please refer to K Appendix: Software Maintenance for more details on software maintenance licenses.



6.26.3 About — Technologies

Release infoLicenseTechnologiesCreditsSystemDataSoftware

periods of time to identify and eliminate problems.



Gold TS Protection makes monitoring for digital services much quicker to set up, and fault-tracking much faster, more accurate and secure. Gold TS Protection includes all the checks specified in the ETR290 standard, but goes much further to include testing for critical conditions missed by ETR290.



External Integration Interface (Eii) is a well defined interface allowing easy integration of Bridgetech probes into a 3rd party network management system (NMS). Measurement data and alarms from the probes can be accessed by the NMS through SNMP traps and/or XML files, enabling development of a customized graphical user interface that could comprise equipment from several manufacturers. The Eii interface is described in a document that is open and available.



Full Service Monitoring (FSM) allows easy validation of any server reachable by the probe via Ethernet. The servers may be probed by either sending an ICMP echo request packet (also known as ping) or performing an HTTP get request. The FSM feature thus allows the operator to verify that vital system components like remote VoD, CA and middleware servers are active, ensuring correct overall system performance. In the event of a server not being reachable, the operator will be notified by an alarm so that the problem may be corrected.



The MicroETR is a unique way of visualizing the complex results of ETSI TR 101 290 analysis in a simple icon. The MicroETR provides an at-a-glance overall status report for an MPEG transport stream, whether it be an Ethernet, ASI, QAM, COFDM or Satellite signal. Already by viewing the icon, the user will get an indication as to what signal impairments are present in the stream, and by clicking the icon he can further drill down to examine the analysis results in full detail. Many MicroETR icons can be displayed in a single view, in fact only limited by screen size, thus enabling easy yet advanced in-depth monitoring of a complete system.



The probes use the patented MediaWindow GUI to display the composite KPI IAT:MLR as it develops over time, providing a unique at-a-glance presentation of network behavior. In a single view both packet jitter and packet loss are presented, with colors that indicate the severity of errors present in the signal. Both current and historical errors are shown, and this enables the user to get an overview of what is actually going on in the IPTV network. Both packet jitter and packet loss in the network may lead to artifacts noticeable to the end users, and it is of vital importance for the operator to gain control over these parameters. The MediaWindow makes it simple to examine the network performance in order for the operator to correct current or

The **Technologies** view lists some of the technologies available in the Bridge Technologies product family.



6.26.4 About — Credits

Release infoLicenseTechnologiesCreditsSystemDataSoftware

Contains software licensed under the [GNU General Public License](#) version 2. Please contact your dealer to receive copies of the source code for these parts.

Contains software from the cURL project licensed under the [cURL license](#).

Contains software based on the [pugixml library](#). pugixml is copyright © 2006-2015 Arseny Kapoulkine.

Contains software based on the [json.hpp library](#). json.hpp is copyright © 2013-2019 Niels Lohmann.

Contains the jQuery library from the [JS Foundation](#), licensed under [the MIT license](#). Copyright JS Foundation and other contributors.

Contains software from the libpqxx project, licensed under [the BSD license](#). Copyright © 2001-2017 Jeroen T. Vermeulen.

Contains software from the Go project licensed under the [Go library license](#) identifying the following contributors:
Copyright © 2009-2018 The Go Authors. Copyright © 2013 Dario Castañé. Copyright © 2012 Rodrigo Moraes. Copyright © 2012 fsnotify Authors. All rights reserved.

Contains software licensed under [the MIT license](#).
From the lib/pq project: Copyright © 2011-2013, 'pq' Contributors. Portions Copyright © 2011 Blake Mizerany.
From the nu7hatch/gouuid project: Copyright © 2011 by Krzysztof Kowalik
From the jinzhu/copier project: Copyright © 2015 Jinzhu.
From the nhooyr/websocket project: Copyright © 2018 Anmol Sethi.

Contains software licensed under the [Apache License](#) version 2.0.
CoreOS Project
Copyright 2018 CoreOS, Inc
This product includes software developed at CoreOS, Inc. (<http://www.coreos.com/>).

The German railway station and 7-segment clock widgets contain code by [Rüdiger Appel](#) licensed under the [Creative Commons 3.0 license](#) (CC BY 3.0).

The report generator contains the Noto and Noto CJK fonts licensed under the [SIL Open Font License](#).

The RDW contains the Liberation Sans font licensed under the [SIL Open Font License](#).

The timeline contains code by [Font Awesome](#) licensed under the [Creative Commons 4.0 license](#) (CC BY 4.0) and the [SIL Open Font License](#).

The toolbar contains code licensed under the [Apache License](#) version 2.0.

This view shows information about the software included with the VBC Controller.



6.26.5 About — System

Release info
License
Technologies
Credits
System
Data
Software

NTP/timesync
Updated: 737 secs ago Freq offset: -2.950 ppm Time: Aug 29 10:58:33

VBC services

Service	Status	Started	Usr	Sys	Memory
nginx	Running	2024-08-23 11:14:01	0%	0%	13M
sogi-wrapper	Running	2024-08-23 15:15:10	0%	0%	3M
vbc.alarmdataweb	Running	2024-08-23 15:15:12	0%	0%	12M
vbc.bladealarmsweb	Running	2024-08-23 15:15:12	0%	0%	6M
vbc.database	Running	2024-08-23 11:12:03	0%	0%	30M
vbc.devdetect	Running	2024-08-23 15:15:11	0%	0%	5M
vbc.etreporting	Running	2024-08-23 15:15:11	0%	0%	5M
vbc.ewe	Running	2024-08-23 15:15:12	0%	0%	45M
vbc.licenseproxy	Running	2024-08-23 15:15:10	0%	0%	19M
vbc.log_splitter	Running	2024-08-23 15:15:13	0%	0%	17M
vbc.pollalarms	Running	2024-08-23 15:15:13	0%	0%	21M
vbc.pollarchive	Running	2024-08-23 15:15:11	0%	0%	5M
vbc.polldata	Running	2024-08-23 15:15:11	0%	0%	19M
vbc.pollpocket	Running	2024-08-23 15:15:11	0%	0%	5M
vbc.pollstatus	Running	2024-08-23 15:15:13	0%	0%	67M
vbc.pollthumbs	Running	2024-08-23 15:15:13	0%	0%	46M
vbc.pollvbc	Running	2024-08-23 15:15:12	0%	0%	13M
vbc.proxy	Running	2024-08-23 15:15:13	0%	0%	17M
vbc.rdw	Running	2024-08-23 15:15:13	0%	0%	19M
vbc.reporting	Running	2024-08-23 15:15:12	0%	0%	5M
vbc.snmp2xml	Running	2024-08-23 15:15:12	0%	0%	25M
vbc.streamdata	Running	2024-08-23 15:15:12	0%	0%	15M
vbc.streamdataweb	Running	2024-08-23 15:15:12	0%	0%	6M
vbc.syslogger	Running	2024-08-23 15:15:13	0%	0%	22M

Disk status
RAID status: **No supported RAID found**
Installation directory: 82% free (100G)
Temporary directory: 82% free (100G)

Server response time
Static request: 22ms **Redo**
Jittery values may be caused by browser overhead, network latency or heavy load

Database conversion
Progress: Complete

Suspend alarms and measurements
Suspend VBC ☐ **Apply**
When suspended, alarms will eventually clear and no new measurements are obtained

Links
[Benchmark VBC server...](#)
[Disk tuning...](#)
[Debug...](#)
[System status \(XML\)...](#)

The **System** view displays a snapshot of the current status of the system, to ensure correct VBC Controller operation.

The **NTP/timesync** section indicates whether the VBC clock is locked to an external time reference signal. If time synchronization is not enabled, a warning message is displayed in the menu column.

It is strongly recommended that the server running the VBC software, and the equipment controlled by it, be synchronized against an external NTP server. Refer to N Appendix: Enabling NTP time synchronization for more details.

We recommend using the standard operating system tools for configuring the system clock, and to use Chrony as the network time client. Please refer to the operating system instructions⁴ for further details on how to configure the date and time.

The **VBC services** overview displays the VBC services that are required. All the VBC services listed should have status *Running* or *Disabled* if the corresponding feature is not licensed or available. The current CPU and memory usage is also displayed. More information about the different services can be found in C Appendix: The VBC System Services.

Disk status displays free disk space to give the user some overview of disk resources available. It will additionally display the status of the RAID system, if supported. If no RAID system is installed, the message “No supported RAID found” will be displayed in red. The same message will be displayed if a RAID system is installed but not detected, as the installed software is unable to differentiate between the two cases.

Server response time is determined upon entering the **System** view. When the **Redo** button is clicked, a new request is sent to the web server.

⁴<https://ubuntu.com/server/docs/how-to>



Clicking the **Benchmark VBC server...** link will open a new window, allowing the user to check VBC server performance. Some typical benchmark times are listed as a reference.

Release info

License

Technologies

Credits

System

Data

Software

Benchmark

This benchmark test will execute a typical VBC scenario and is a good indication of the performance of the server. The performances of both CPU and the filesystem will influence the result. The benchmark will benefit considerably from having at least two cores; having more than two cores should not make any significant impact. Some of the VBC processes are suspended while the benchmark is running and the benchmark will usually take less than two minutes to complete.

Status

Execution time for benchmark test: 25.9s
Performed: 2019 May 2 15:27:25

Typical values

Platform	Result
Dell desktop PC, Intel Core 2 2.13GHZ, SATA disk	44.2s
VM-Ware (1 core) hosted on Dell desktop PC, Intel Q6600 quad core 2.4GHZ, SATA disk	100.4s
VM-Ware (2 cores) hosted on Dell desktop PC, Intel Q6600 quad core 2.4GHZ, SATA disk	45.9s
IBM 2u Rack server, Intel Xeon E5520 2.26GHZ Quad Core, SAS disk	33.1s

Begin benchmarking

Clicking the **Disk tuning...** link in the **About — System** page allows the user to configure for how long data should be stored on the disk. Storing data for long periods means that a large amount of disk space is required. Estimated disk usage is calculated based on the current configuration, and numbers are rounded to the nearest MB.

Release info

License

Technologies

Credits

System

Data

Software

Disk tuning

Disk tunings

Days to keep 1h resolution streamdata (1-730)

720

This is used when generating the stream PDF report and plotting graphs

Days to keep 1m resolution streamdata (1-40)

30

This is used when plotting graphs for shorter intervals

Based on individual device configurations there appears to be **500** streams reported from probes. Based on the selected intervals above this corresponds to a disk usage estimate of **59G**. The individual contributions are as follows: 16G(per hour data), 42G(per minute data).

Apply

Clicking the **Debug...** link allows the user to generate a document containing debug information that may be useful if VBC misbehavior is reported. This file should be sent along with a description of the misbehavior.



Clicking the **System status (XML)...** link generates an XML document with a short description of the system status.

6.26.6 About — Data

Release info License Technologies Credits System **Data** Software

Import data

[Streamgroups](#)

Import files will have extension .xml

The file submit dialogue below will not work for post requests requiring additional arguments.
See EII documentation for supported imports and exports.

No file chosen

Stream group configuration can be exported as XML documents. This is achieved by clicking one of the links inside the **Data** frame. A new browser window pops up containing the selected XML document. The browser will allow the contents of the page to be saved to file.

Restoring the stream group configuration is just as simple. Just click the **Browse** button and select the file that contains the XML document. Then click the **Go!** button and the information in the XML document will be applied.

To import documents that have been manually edited the CRC attribute at the very top of the document must be deleted (i.e. delete `crc="..."` from the file). This will bypass the checksum verification mechanism.

Please refer to the document **Eii External Integration Interface** for detailed information about XML import and export.

6.26.7 About — Software

Release info License Technologies Credits System Data **Software**

Import VBC software

VBC software files have the extension .tea

No file chosen

Please read 2.6 Upgrading From a Previous Version before updating using this interface.



The software section allows the VBC Controller to be upgraded to a newer software version. Select the **.tea** file from the local PC and click **Go!** to copy the software to the VBC. When the upload is complete, clicking the **Update software** button will begin the upgrade procedure. The latest version of the VBC software can be found in the End User area at <https://www.bridgetech.tv/>.

A more detailed description on the software update procedure can be found in L Appendix: Software Upload

Release info License Technologies Credits System Data **Software**

Software image uploaded successfully

42855360 bytes saved to disk

Update software

Software update in progress

Writing ...

Updating:  25%

-- Do not power off --

The system will automatically restart on completion

Status updated: 2/3/2020, 1:28:13 PM

Upgrading to a new major release requires a valid software maintenance license, please refer to K Appendix: Software Maintenance for more details. If the current software maintenance license does not cover the uploaded software version, the upgrade will be aborted and the current version is kept.



A Appendix: Separate Probe and Network Interfaces

The VBC Controller can act as a bridge between the user network and the data network.

There are a few important differences between accessing a probe directly from a client and accessing it via the VBC application. Accessing the device directly means pointing the client's web browser to the IP address of the device. This only works if the IP address of the device is reachable from the client's PC. This is not necessarily the case since often the probes and the clients are on different network segments. Accessing a probe via the VBC means that the client can reach a probe provided the client can reach the VBC server and the VBC server can reach the probe. This can be achieved even if the probes and clients are on different network segments since the VBC application can act as an HTTP tunneling device utilizing two network devices.

Conversely, if the probes are on a network which cannot reach the Internet, they must still be able to connect to the VBC host to be able to contact the on-line licensing service to be able to activate licenses on-line.

The full list of network ports that need to be available can be found in chapter 2.8 Firewall Configuration.



B Appendix: The VBC Files

A majority of the files that are part of the VBC Controller application are located in the `/opt/btech/vbc` folder. This table summarizes important files and folders.

<i>Disk location</i>	<i>Description</i>
/opt/btech/vbc/	Root folder for the VBC application (all subsequent locations are relative to this)
bin	The VBC binaries and some settings files
cb	Static parts of the VBC web interface
configs	Contains blade configurations, thresholds and software uploaded by users
database*	All PostgreSQL relational database files
database_backup	Nightly backup of the database files
doc	Documentation and sample files
etc	Version information
etrreports	PDF extended report files
ewecookies	Internal state files used by the ewe service
lib	System libraries and scripts
log	Folder containing various diagnostic log files
networkdiagrams	Graphics option files uploaded by users
poll	Scratch area for parameter gathering from blades
pollarchive	Scratch area for parameter gathering from the Archive Server
reports	PDF report files
rdw	Configuration and data for the RDW
settings	Configuration settings for alarms, user groups and scheduling
sites	Site configurations and some status files
thumbs	Thumbnail pictures obtained from probes and extractors

Note that future versions of the VBC may have different files, folders and file formats.

Log files

In the VBC all log files will be truncated regularly. No log files are allowed to grow beyond their limitations. The log files are located under the `/opt/btech/vbc/log` folder.

The log files limitations are:

<i>Log file</i>	<i>Limitation</i>	<i>Description</i>
actual.log	30,000 lines	Contains the raw event/alarm log. The log is truncated daily.
eachsite/allsites.log	20,000 lines	This is the aggregated alarm list presented in the Monitoring page.



eachsite/<site>.log	2,000 lines	This is the site alarm list presented in the Monitoring — Site page. This log is also used to present the alarm list for a selected stream in the Stream view and Thumbs View .
eachblade/<blade>.log	2,000 lines	This is the blade alarm list presented in the Monitoring — Site — Blade page.
eachsite/history.log	10,000 lines	Contains the past alarm history and is used for exporting the alarm history in the Logs view.



C Appendix: The VBC System Services

The VBC Controller application consists of a number of Linux system services:

<i>Service</i>	<i>Description</i>
ewe	The main application serving dynamic HTTP requests
ewews_ks	A stateless web server talking to the ewe process
devdetect	Detects blades (probes, extractors and Archive Servers) that have been configured to register automatically with the VBC
etrreporting	Generates extended PDF reports as described in chapter 6.16
log_splitter	Builds site, blade and stream log files from alarm files and SNMP data
pollalarms	Collects blade alarms for presentation in the Blade alarms view
pollarchive	Collects data from a configured Archive Server for use with the Timeline view
polldata	Aggregates XML data from blades for use with the RDW
pollpocket	Collects data from configured PocketProbe applications
pollstatus	Polls blades every 60 seconds and raises alarms
pollthumbs	Collects thumbnail pictures and metadata from probes and extractors
pollvbc	Collects alarm information from configured VBC sub-sites
proxy	Used by the RDW to present information from attached blades
rdw	Server process for the RDW
reporting	Generates regular PDF reports as described in chapter 6.15
snmp2xml	Generates the XML document available via the alarms_exp.xml page
streamdata	Collects probe data for generating stream based reports
vbclive	Serves the VBC Live Mosaic view described in chapter 5.4
postgresql	The freely available PostgreSQL application that implements the relational database used by the VBC processes
licenseproxy	A small HTTP proxy that is used to allow blades to activate licenses on-line through the VBC server, without themselves having direct Internet access; see J Appendix: On-line License Activation for more details
dbinstall	Transient service used for creating the initial VBC database, and updating it when upgrading the software

All these services need to run simultaneously for the VBC to work. They will automatically restart if they terminate unexpectedly, although that should not happen under normal circumstances. The command **vbchello** can be used to verify that all the necessary services are running, and their status is also available from the **Main — About — System** view.

The commands **vbcstart** and **vbcstop** are available to start and stop the VBC services, respectively. Diagnostics are logged using the system journal, and can be retrieved using the command **journalctl -u vbc.<service>**

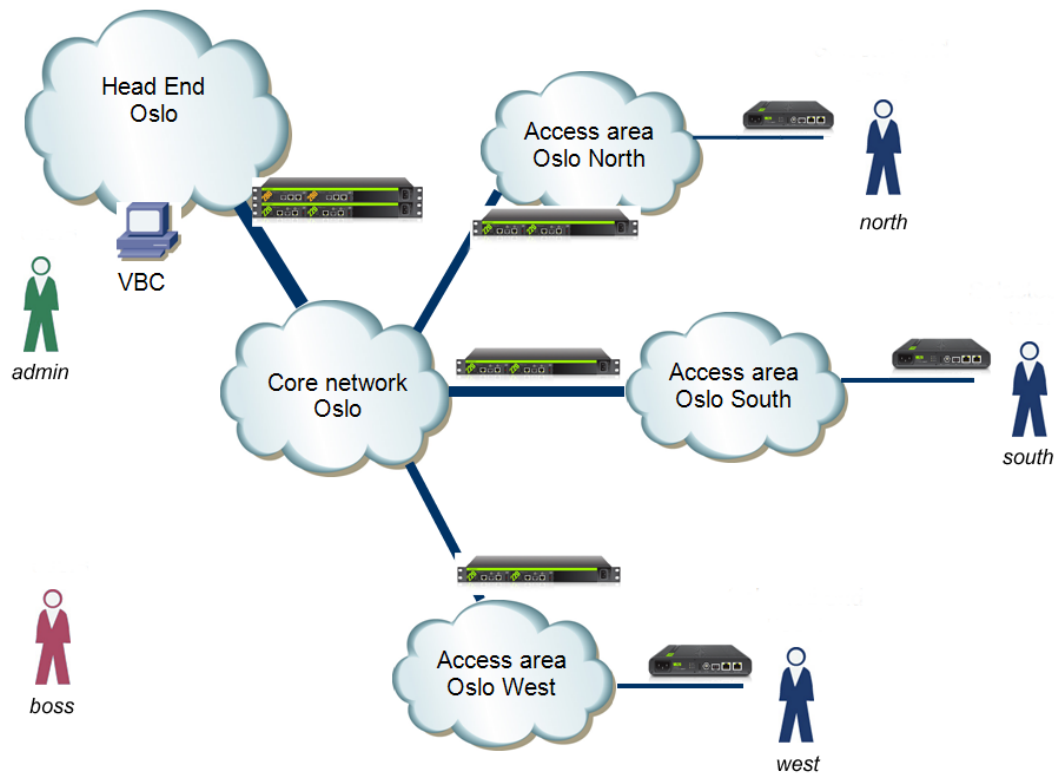


The service declaration files are stored in the `/usr/lib/systemd/system` directory. To override the declaration, for instance to change command-line parameters or logging options, copy the corresponding file to the `/etc/systemd/system` directory and make changes to the copy.



D Appendix: Example Site Configuration

This is an example configuration for a relatively small system that could serve as a template for larger systems. Probes have been deployed at strategic points in the network.



The following sites (7) and users (5) could be defined:

<i>Site</i>	<i>Device name</i>	<i>Blade</i>	<i>USER admin</i>	<i>USER north</i>	<i>USER south</i>	<i>USER west</i>	<i>USER boss</i>
HeadEnd	HE probe 1	VB220	Full	r/o	r/o	r/o	r/o
	HE probe 2	VB220					
	HE content	VB288					
AccessOsloNorth	AccessN probe 1	VB220	Full	Full			r/o
	AccessN probe 2	VB220					
AccessOsloSouth	AccessS probe 1	VB220	Full		Full		r/o
	AccessS probe 2	VB220					
AccessOsloWest	AccessW probe 1	VB220	Full			Full	r/o
	AccessW probe 2	VB220					
UserOsloNorth	UserN	VB20	Full	Full			r/o
UserOsloSouth	UserS	VB20	Full		Full		r/o
UserOsloWest	UserW	VB20	Full			Full	r/o

Note that in the table the blades column shows the actual hardware – in the **Equipment** view, these blades will have blade names and management IP addresses assigned to them.



The *admin* user has full access to all sites in addition to *admin*-specific rights like defining sites and devices in the system.

The *north*, *south* and *west* users have full access to probes monitoring the input and output signals of their respective regional sites. In addition they can view the output of the central head-end, thus enabling them to see if errors present in the signal at their regional site were also present at the output of the central head-end.

The *boss* user has read-only access to all sites and can view alarms present at all sites. He may also create reports covering some or all monitoring locations.

It may in some cases be useful to add one device to multiple sites. This can be done in the **Equipment** view by adding the same device IP address multiple times.



E Appendix: Getting the Thresholds Right

In order to customize the alarm thresholds in the VBC Controller it is necessary to understand exactly how VBC decides to raise an alarm as per the following:

1. The VBC obtains error-second statistics from each probe every minute
2. The VBC obtains VBC threshold settings from each probe when its configuration is changed.
Note that the number of error seconds counted by each probe depends on the different probe threshold settings. Probe thresholds include OTT thresholds, Ethernet thresholds, ETR thresholds, PID thresholds, Service thresholds and possibly RF thresholds. Refer to the probe manual for a comprehensive description of these threshold settings – only the VBC thresholds are considered in this appendix.
3. An alarm is raised if the number of error seconds summed for the last alarm window period exceeds the error-seconds threshold

Note that it is the probe's own VBC threshold settings that are used when comparing error-seconds against thresholds.

Alarms are cleared when the number of error seconds within the current alarm window no longer exceeds the alarm threshold or when there has been no error seconds during the last alarm reset period (whichever occurs first).

Step 1 – using default values

The probe's default threshold settings will raise alarms for a stream if there is:

<i>Error</i>	<i>Default threshold value</i>
No signal	5 seconds with no signal during the last poll period (60 seconds)
RTP drops	5 seconds with RTP drops during the last alarm window period
MLR error	20 seconds with MLR error (i.e. CC error) during the last alarm window period
IAT error	20 seconds with IAT error (jitter above 50ms) during the last alarm window period
Max bitrate	20 seconds with bitrate above 30 Mbit/s during the last alarm window period
Min bitrate	20 seconds with bitrate below 0.1Mbit/s during the last alarm window period
ETR Priority 1 error	250 seconds with ETR priority 1 errors during the last alarm window period
ETR Priority 2 error	250 seconds with ETR priority 2 errors during the last alarm window period
ETR Priority 3 error	250 seconds with ETR priority 3 errors during the last alarm window period
ETR other error	250 seconds with ETR other errors during the last alarm window period
ETR interface error	250 seconds with ETR interface errors during the last alarm window period
OTT transport error	60 seconds with OTT transport errors during the last alarm window period



OTT HTTP error	60 seconds with OTT HTTP errors during the last alarm window period
OTT XML error	60 seconds with OTT XML errors during the last alarm window period

These are sensible values for identifying streams with severe problems while at the same time avoiding too many alarms for minor disturbances in the signal.

Step 2 – identifying OK streams reporting alarms

After a while, maybe a few days or so, the stream-graphs and the alarm-lists will identify streams that exceed the threshold settings. Some of these streams may experience real trouble which requires more investigation. Others may be of a nature where alarms are being generated although the stream is OK – such as streams with expected signal breaks at regular intervals or streams with errors due to software multicasts wrapping frequently.

To change the threshold-setting for a particular stream, follow this procedure:

1. Identify a probe that includes the stream in its Stream list
2. Add a new threshold template in the probe's **Setup — VBC thresh.** view and select appropriate values
3. Edit the stream in the probe's **Multicasts — Streams** view and associate the stream with the new threshold template
4. Use the VBC's **Equipment** view to copy the new **Stream list** and **Thresholds** settings to all probes that include the stream in their stream list

VBC thresholds are associated with Ethernet multicasts in the **Multicasts — Streams — Edit** pop-up views, COFDM, QAM, SAT and ASI streams are associated with VBC thresholds in their respective interface setup views. For OTT the settings are found in the **OTT — Channels — Edit** pop-up view.

Stream lists and **Thresholds** can be freely copied between probes without affecting which streams are being monitored.

Step 3 – getting more alarms

For streams that are almost perfect, it might be worth considering tightening in the alarm thresholds to the maximum.

Setting the error-second threshold to a value of 1 tells VBC to raise the alarm for each occurrence of the error. The alarm will be cleared after the alarm reset time unless there are more errors.



F Appendix: Probe Versus VBC Alarms

The Probe alarms are independent of the VBC Controller alarms. The Probe has been designed to yield instantaneous alarms based on the current measurements. This typically results in lots of short-lived alarms that would be “too much” for the VBC to report, as the VBC may control a large number of Probes. The VBC therefore generates alarms based on error-second statistics gathered from Probes during a selectable time period defined by the *admin* user (default 60 minutes – sliding window).

Some the VBC alarms map to only one probe alarm type. Other the VBC alarms map to several probe or VB288 Objective QoE Content Extractor alarms. As an example, the VBC alarm ETR pri one error does alarming for the following probe alarms:

- TS sync
- Sync byte
- PAT
- Continuity
- PMT
- Missing PID

In order to view probe alarms that may possibly correspond to a VBC alarm, click the blue information icon ⓘ associated with the VBC alarm. A pop-up view shows individual **Blade alarms** matching the VBC alarm time and type. Note that the time on the probes and the VBC should be synchronized in order for this functionality to work correctly, refer to N Appendix: Enabling NTP time synchronization for more details. Also note that alarms must be enabled probe GUI, otherwise they will not be displayed in the pop-up view. Please refer to the probe manual for more information. As there is not a one-to-one relationship between probe and VBC alarms, there will often be a number of probe alarms that can cause a VBC alarm to be raised. This means that the list of probe alarms can have many entries compared to the VBC alarm text.

The full list of probe (and VB288 Objective QoE Content Extractor) alarms are available in the VBC's **Blade alarms** view.

Site	Blade	Interface	Stream	VBC alarm	Description
US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1920x1080: Lagging behi...
US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1280x720: Lagging behi...
US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1920x1080: Lagging behi...
US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 640x360: Lagging behin...
US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1280x720: Lagging behi...
US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 480x272: Lagging behin...
US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1920x1080: Lagging behi...
US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1280x720: Lagging behi...
US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 640x360: Lagging behin...
US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1280x720: Lagging behi...
US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 480x272: Lagging behin...
US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1920x1080: Lagging behi...
US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1280x720: Lagging behi...
US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 640x360: Lagging behin...
US-HE	SW-330	OTT	Bloomberg-West	OTT xml error	Mixed: avc1,mp4a 1280x720: Lagging behi...

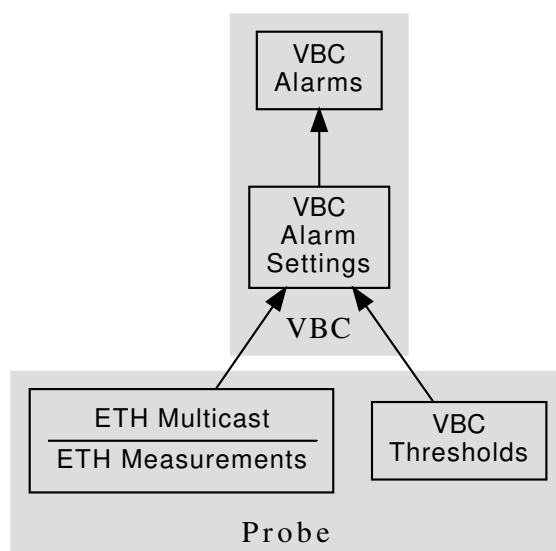


Figure F.1: VBC alarming based on Probe measurements



G Appendix: Syslog forwarding

The VBC Controller can collect blade alarms and SCTE 35 events from connected blades and make them available to the local syslog facility. This is enabled by checking the **Syslog forward** checkbox in the **Equipment — Edit device** view. The information is forwarded under the syslog identifier **syslogger**. In a default installation, the information is collected in the systemd journal and can be inspected using the **journalctl** command:

```
journalctl -t syslogger
```

To forward the collected messages to a remote syslog facility, the *rsyslog* tool can be used¹. The default configuration of rsyslog will create a number of local log files in the `/var/log` directory; to configure it to forward the messages to a remote syslog, we can create a configuration snippet in the `/etc/rsyslog.d` directory.

For instance, to forward all the messages from the **syslogger** service using UDP to a server at IP address 10.20.30.40 and port 514, using the RFC 5424 format, we save the following snippet at `/etc/rsyslog.d/syslogger.conf` and restart rsyslog by issuing the command **systemctl restart rsyslog**:

```
# Save as /etc/rsyslog.d/syslogger.conf to forward to 10.20.30.40:514
if ($programname == "syslogger") then {
    action(type="omfwd" target="10.20.30.40" port="514" protocol="udp"
        template="RSYSLOG_SyslogProtocol23Format")
}
```

For further information, please refer to the rsyslog documentation².

¹This tool is not installed by default, but can be added by issuing the command **sudo apt install rsyslog**.

²<https://www.rsyslog.com/doc/>



H Appendix: Troubleshooting

Please also see chapter 2.5 Initial Setup Troubleshooting.

Multiple browser windows towards the VBC

The VBC Controller has been designed to allow multiple users to log in and work independently of each other. Opening up two windows from the same browser application towards the VBC may not work as intended since the VBC will not be able to distinguish them as login is requested only once.



I Appendix: Backing up the VBC

We strongly recommend backing up the VBC files before upgrading to a new version of the VBC Controller, or when upgrading to a new release of the OS.

The backup–restore procedure is also useful when migrating the VBC configuration to another server. The procedure should work across different Ubuntu Linux, Rocky Linux, CentOS Linux or Red Hat Enterprise Linux versions, even across 32-/64-bit OSes.

The backup–restore procedure described in this appendix below is valid for VBC version 4.9.0 and later.

I.1 Backing up the VBC

To create an archive file called `/tmp/vbc_backup.tgz` containing all the VBC data including the database, type the following command in a terminal shell on the VBC server (as the root user):

```
/opt/btech/vbc/bin/vbc_copy /tmp/vbc_backup.tgz
```

Note: If running on VBC version 5.1 or earlier, the path to the script should instead be `/opt/btech/bin/vbc_copy`).

If the backup file is to be restored on a server running a newer version of the VBC, you must use the version of the `vbc_copy` script from the newest version. See the section **Obtaining the backup script from a newer version** below for details on how to obtain the file.

Now copy the `tgz` file to a safe place, such as a USB FLASH drive or a CD/DVD.

I.2 Restoring the VBC from backup

Make sure the `vbc_backup.tgz` file is in the `/tmp` folder. Then type the following command in a terminal shell (as the root user):

```
/opt/btech/vbc/bin/vbc_copy_restore /tmp/vbc_backup.tgz
```

Note: If running on VBC version 5.1 or earlier, the path to the script should instead be `/opt/btech/bin/vbc_copy_restore`).

I.3 Restoring the nightly backup

A nightly backup of the VBC database is generated automatically every night by a cron script. The two latest backups are kept in the `/opt/btech/vbc/database_backup` directory, under the file names `backup.current.gz` and `backup.old.gz`.

To restore a nightly backup, simply run the restore script, pointing it to the nightly backup file instead:

```
/opt/btech/vbc/bin/vbc_copy_restore /opt/btech/vbc/database_backup/backup.current.gz
```




I.4 Obtaining the backup script from a newer version

If the target system is running a newer version of VBC than the one the backup was taken from, you should always use the version of the backup script from the target release (i.e. the newest one).

The **vbc_copy** script can be copied from the newer VBC using scp:

```
scp /opt/btech/vbc/bin/vbc_copy root@<IP-address-of-other-server>:/tmp/
```

You can also extract the **vbc_copy** script from the upgrade package. Running the following command will extract the **vbc_copy** script to the current directory. Replace **vbc.tea** with the actual filename of the downloaded file:

```
/opt/btech/vbc/bin/tengff -e vbc.tea -f vbc_copy -kvbc
```



J Appendix: On-line License Activation

J.1 Introduction

The VBC Controller uses licenses which are activated and updated periodically over the Internet, without the need for human intervention. The license is only tied to the VBC when it is used and is periodically renewed. To transfer the software to a new host, the license can simply be released from the software and applied to an instance running on a different server.

Please make sure you have the license key available before you release the license, as you must enter it again on the system you wish to transfer the license to. The license key is *not* displayed in the VBC user interface.

If you have lost the license key, contact your dealer to retrieve it. Make sure you include all details from the **Main — About — License** view in your request.

When the VBC Controller sends the on-license activation over the Internet, it includes some basic information to verify the VBC Controller. This includes a basic hardware footprint, as well as parts of the SNMP identification data configured in the **Main — General — Connections** view.

J.2 Requirements

The VBC needs to be able to contact the license server either directly or via a proxy server, as described below. If proxy connectivity also is not available, an off-line activation procedure is available as well.

The VBC must also be configured with a correct date and time. Please refer to N Appendix: Enabling NTP time synchronization for more information on configuring time synchronization.

Direct access to activation server

To activate the license automatically, the VBC needs to be configured with a valid DNS server address (see M Appendix: Network configuration) which is able to look up the host name `license.microanalytics.org`. The VBC needs to be able to contact the host this name resolves to using HTTPS on port 443.

Using an arbitrary proxy server

The VBC Controller can be configured to use an arbitrary proxy server to connect to the licensing server. By adding the URL to a proxy server in the **Main — General — Preferences** view, the VBC will automatically attempt to use this proxy if a direct connection fails.

Off-line activation procedure

If the VBC network is completely disconnected from the Internet, it is still possible to activate the license using the off-line activation procedure. When using this, the license will be tied to the system and will not be transferable to another server. The off-line activation procedure needs to be repeated whenever there is a need to have the license feature set upgraded. If the activated VBC license is not **Permanent** –



which is typically the case in cloud deployments or in pure software installations – the off-line activation procedure has to be repeated a minimum of once per year.

Click the **Renew license off-line** button to start the off-line activation procedure.

Renew license off-line
Perform the following steps to renew the license:
1. Please verify that the system time is set correctly (time is now 2020-11-02 14:37:30 UTC).
2. [Download the license request document to your computer.](#)
3. Upload the license request document to the license activation interface by visiting <https://license.microanalytics.org/offline>
4. Upload the license document received from the license activation interface:

Välj fil Ingen fil har valts

Go!

Please note: If the system is restarted prior to completing step 4, you must start over from step 2.

License details

Follow the steps described in the dialog to renew or activate the license. To abort the procedure, click the **License details** button to return to the previous screen.

First, download the license request document from the VBC Controller to the computer you are browsing from. Once the file has been downloaded, connect the computer to the Internet if not already connected, and open the link to the off-line license manager¹.

Activate license
Please upload the license request document (.bin) here:

Choose File No file chosen

If you are activating a new system and need to claim a license, enter the license key here:

License key to claim, if any

Leave empty to renew an existing or pre-allocated license.

Request license

Select the .bin file that was downloaded in the first step, and optionally add a license key if the system you are activating did not already have a license attached. Once done, click the **Request license** button and save the license document file to the computer.

If needed, re-connect to the VBC network, return to the **Renew license off-line** view, select the .pem file that was generated by the license manager and press **Go!**

The license should now be added to the system. If this is a new or different license, the software will restart. Use the **License details** view to verify that the license was applied correctly.

¹<https://license.microanalytics.org/offline>



K Appendix: Software Maintenance

Purchasing yearly software maintenance enables future feature protection and guarantees access to the latest software for Bridge Technologies equipment and the VBC Controller. The latest version of the VBC software can be found in the End User area at <https://www.bridgetech.tv/>.

The software maintenance can be purchased for a three or five year period, typically initially purchased together with the system itself, during which new major releases can be installed.

The current software maintenance periods of all blades monitored by the VBC are displayed in the **Equipment** view, see chapter 6.12.

The current software maintenance period for the VBC Controller itself is displayed in the **About — License** view, see chapter 6.26.2 for more details. For an overview of software maintenance periods for multiple units, please refer to the **Equipment** view on the VBC Controller server.

For renewals, contact the local partner the system have been purchased from or Bridge Technologies directly at: sales@bridgetech.tv, with the title “**se-maintenance**”.

Use the **Equipment — Device software** view to update the software on monitored blades, please refer to chapter 6.12.2.

Use the **About — software** view to update the VBC software, please refer to chapter 6.26.7. While this procedure should only allow upgrades allowed by the currently activated software maintenance license, it is possible to do a manual upgrade to such a version. If the new software version detects that it is not properly licensed, the VBC starts in element manager mode.



L Appendix: Software Upload

Please read 2.6 Upgrading From a Previous Version first.

The process of performing a software upload to the VBC involves the following steps:

1. Obtain the software image.
2. Backup the VBC configuration and data.
3. Transfer the image to the VBC using the software upload functionality in the **About — Software** view or by using ssh, and save the new software image on the system.
4. Wait while the software is being saved.
5. Verify the new image.

L.1 Obtain the software image

The image will have a **.tea** extension and is distributed in a compressed ZIP archive together with the readme file detailing changes for this patch release.

Please study the **readme** file to be aware of any important information related to your current software patch. Subsequent patch details may indicate that significant bugs were identified and resolved after your current version and indicate where special care is recommended.

You can find the current version number under **About — Release**.

When upgrading to a new major version, please also study the release notes and **readme** files for all versions between your currently installed major version and the one you are upgrading to, as there might be important changes that you need to be aware of.

If you require any assistance understanding the release notes or readme files please contact your first line support service.

If you would rather re-install the system from scratch instead of using the upgrade procedure, please refer to chapter 2.

L.2 Backup the VBC configuration and data

We strongly recommend backing up the VBC files before upgrading to a new version of the VBC Controller, or when upgrading to a new release of the OS. The backup procedure is described in I Appendix: Backing up the VBC of this manual.



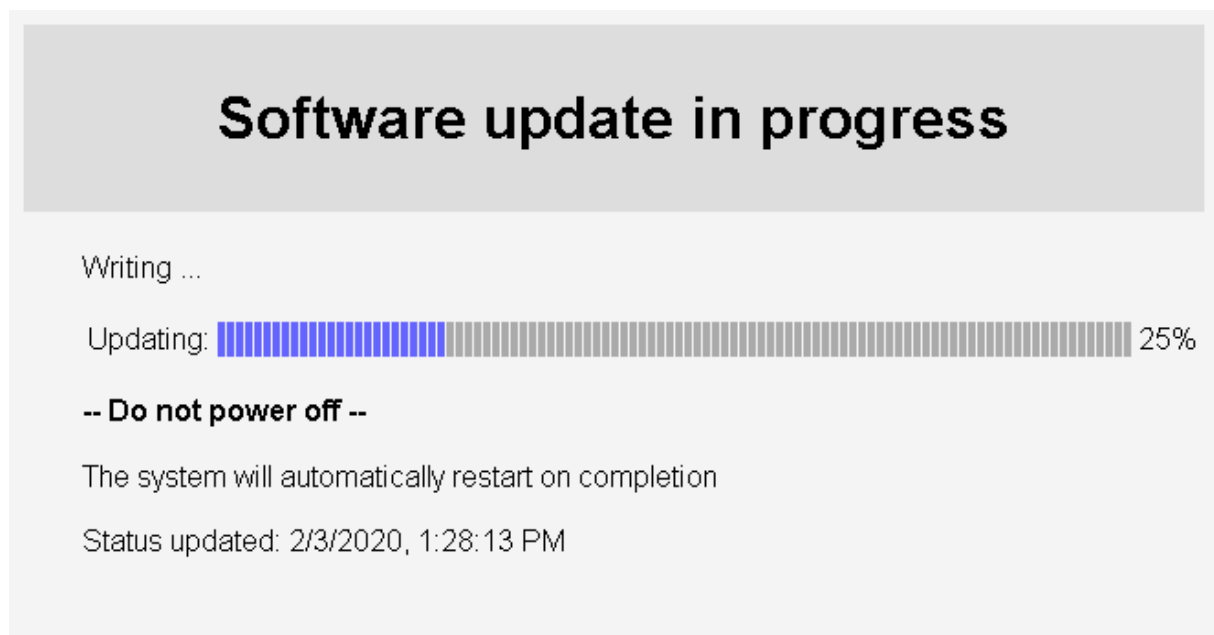
L.3 Transfer the image to the VBC and save

Using the software upload functionality in the About view

From the **About — Software** view select the software image file to be uploaded and click the **Go!** button. When the software has been successfully transferred to the VBC click the **Update software** button and confirm.



Progress bars are displayed to show the software update status.



Note that the VBC will restart when the new software has been installed, and the VBC's user interface will be unresponsive until restart has completed.

Using scp/sftp and ssh

Using a Secure Shell (ssh) client, such as PuTTY¹, first transfer (scp/sftp) the software image to the system.

Next, log in to the system shell to get a command prompt. If you copied the file as the same user you are logging in as, the file should be in the directory you just logged in to. If not, navigate to the directory you uploaded to using the **cd** command.

¹<https://www.chiark.greenend.org.uk/~sgtatham/putty/>



Copy the downloaded file to the `/var/opt/btech/vbc` directory and issue the command `/opt/btech/vbc/bin/vbc_upgrade` to begin the upgrade procedure.

```
cd /path/to/download
sudo cp filename.tea /var/opt/btech/vbc
sudo /opt/btech/vbc/bin/vbc_upgrade
```

L.4 Wait while the software is being saved

This will take a few minutes. The VBC software will then restart automatically. The VBC should state that the software image has been saved successfully.

When using the alternate method do not disconnect the ssh session before the software upgrade is completed.

L.5 Verify the new image

Connect a browser towards the VBC and verify the version and build time in the **About — Release info** view.

L.6 Software upload troubleshooting

If the upgrade is rejected, verify that the software version you are trying to upload is covered by software maintenance. Refer to K Appendix: Software Maintenance for more details.

If the system running the VBC is not connected to the internet, the software upload progress may in some cases be blocked by the PackageKit software trying to refresh its software package database. If this happens, it is recommended to disable the internet-based package repositories.

To make it possible for the system to receive security and bug fix updates, it is in this case recommended to replace these internet-based package repositories with locally hosted mirrors and update the configuration accordingly. Use the **Software Updates** view in the Cockpit administrative interface.

If the web interface does not appear to work correctly straight after upgrading the VBC it may be because the web browser is using files that are cached. Files may be cached for up to one hour in the web browser. To fix the issue, clear the cache manually:

Google Chrome: Settings — Privacy and security — Delete browsing data — Cached images and files

Mozilla Firefox: Settings — Privacy & Security — Cookies and Site Data — Clear Data — Temporary cached files and pages

Microsoft Edge: Settings — Privacy, search and services — Clear browsing data — Choose what to clear — Cached images and files

A log file from the last upgrade process can be inspected by manually by logging in to the system and opening the file `/opt/btech/vbc/log/upgrade.log` manually.



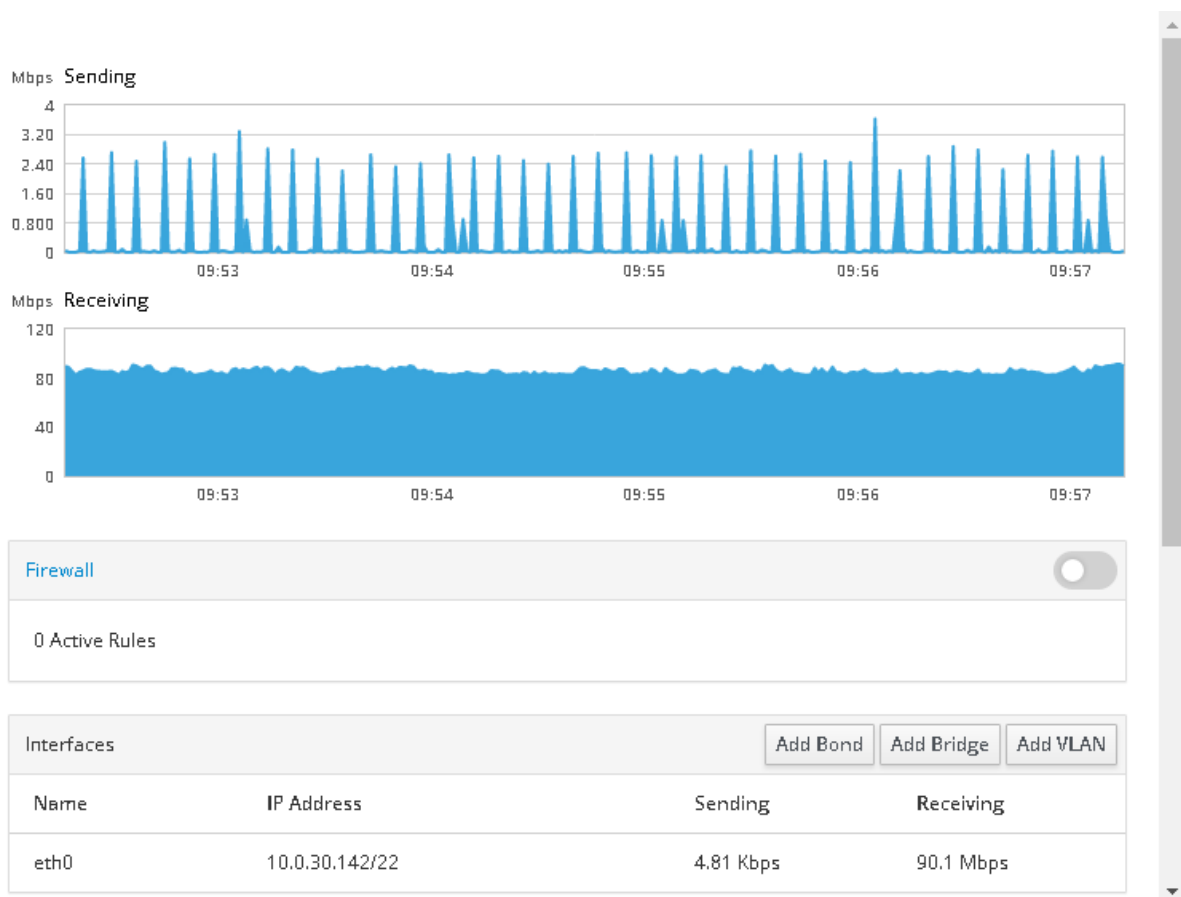
M Appendix: Network configuration

M.1 Web-based configuration

The system ships with a web-based network configuration module. If you are unable to access the system using the web interface, you will need to use the system console. Please see section M.2 for details on how to use the command-line based configuration tool from the console.

To access the web-based configuration module, open the Cockpit administrative interface, as described in section 2.4. The Cockpit administrative interface uses the same log-in credentials as the system accounts.

Click on the **Network** heading to open the network configuration.



For more information on how use Cockpit, please refer to the Cockpit documentation¹.

If you make changes here that causes you to lose web access to the server, you may need to use the command-line tools as described below.

¹<https://cockpit-project.org/documentation.html>

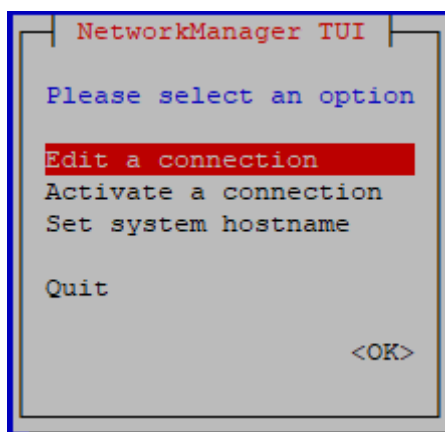


M.2 Command-line based configuration

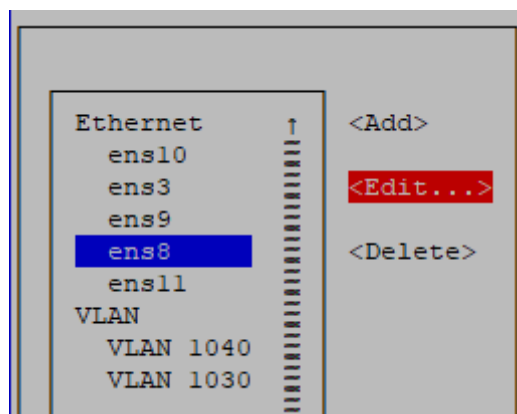
Changes to network configuration, adding new interface devices and VLANs can be done with the **nmtui** tool. Simply type **sudo nmtui** whilst logged into the server command shell². Navigate the nmtui menus using the cursor (arrow) keys and Enter to select.

Editing Network interface configuration

To edit a connection first select **Edit a connection** from the nmtui menu:



Select the interface to be edited and then select **Edit...** from the menu.



Make the necessary changes to IPv4 and IPv6 configuration.

²If the **nmtui** tool is not available on your system, you can install it by issuing the command **sudo apt install network-manager**



Edit Connection

Profile name `ens8`
Device `ens8 (0C:C4:7A:EB:16:0B)`

= **ETHERNET** <Show>

= **IPv4 CONFIGURATION** <Manual> <Hide>

Addresses `40.40.40.40/24` <Remove>
<Add...>

Gateway `40.40.40.1`

DNS servers <Add...>
Search domains <Add...>

Routing (No custom routes) <Edit...>

☒ Never use this network for default route
☐ Ignore automatically obtained routes
☐ Require IPv4 addressing for this connection

= **IPv6 CONFIGURATION** <Automatic> <Show>

☒ Automatically connect
☒ Available to all users

<Cancel> <OK>

Selecting **Automatically connect** will ensure the interface is connected next time the system boots.

Sometimes it is desirable to select **Never use this interface for default route**, particularly if additional interfaces are only used for monitoring multicast traffic or when setting up a native interface for adding VLANs.

After making changes select **OK** to return the previous menu. Generally, network configuration changes will take effect the next time the interface is activated. This can be done by deactivating and reactivating the interface from the **Activate a connection** menu in nmtui or with the command line **ifdown ifname** followed by **ifup ifname**.

Adding new and VLAN interfaces

To add a new interface, in the nmtui main menu select **Edit a connection** followed by **Add** and select the interface type from the menu. Typically this is **Ethernet** but may also be used to create VLAN interfaces. Advanced configurations such as Bond and Bridge may be selected if they are required.

To find the system assigned name for a newly added hardware device use the command line **ifconfig** or search in the output of the **dmesg** tool. It can be helpful to keep the nmtui **Profile name** for the device the same as the device name itself, for example:



Profile name `ens55`
Device `ens55`

= ETHERNET <Show>

= IPv4 CONFIGURATION <Automatic> <Show>

= IPv6 CONFIGURATION <Automatic> <Show>

☒ Automatically connect

☒ Available to all users

<Cancel> <OK>

To add a VLAN interface from nmtui main menu select **Edit a connection** followed by **Add**. Scroll to the bottom of the list and select VLAN:

Select the type of connection you wish to create.

Wi-Fi ↑

Bond |||||

Bridge |||||

Team □

VLAN ↓

<Cancel> <Create>

Edit the settings for the VLAN interface. The Device field should contain the name of the physical interface to be used for this VLAN and the VLAN number, for example `ens8.1040` means VLAN `1040` on interface `ens8`. The parent and VLAN ID fields should correspond to the values in the name field. In our example `ens8` is the parent and `1040` is the VLAN. Other settings are the same as for normal IPv4/6 interfaces.



Edit Connection

Profile name VLAN 1040

Device ens8.1040

= VLAN

Parent ens8

VLAN id 1040

Cloned MAC address

MTU (default)

<Hide>

= IPv4 CONFIGURATION <Manual>

Addresses 10.0.40.163/24 <Remove>

<Add...>

Gateway

DNS servers <Add...>

Search domains <Add...>

Routing (No custom routes) <Edit...>

☒ Never use this network for default route

☐ Ignore automatically obtained routes

☐ Require IPv4 addressing for this connection

<Hide>

= IPv6 CONFIGURATION <Automatic>

☒ Automatically connect

☒ Available to all users

<Show>

<Cancel> <OK>

After entering the configuration for the VLAN interface select **OK** to return the previous menu, then select **Back** and finally **Activate a connection** to activate the newly created VLAN interface.

M.3 Further reading

For more documentation, please refer to the *Introduction to networking*³.

³<https://ubuntu.com/server/docs/introduction-to-networking>

192

VBC Controller User's Manual v7.0.0 © Bridge Technologies Co AS



N Appendix: Enabling NTP time synchronization

It is strongly recommended that the server running the VBC software, and the equipment controlled by it, be synchronized against an external NTP server.

If not set up correctly, alarms may be displayed with incorrect timestamps and comparison between different probes may show up out of alignment.

NTP synchronization against public servers on the Internet is usually enabled automatically if they were detected during the operating system installation. It is possible to change the servers to use, for instance to set it to use a local NTP server, by changing the configuration in the file `/etc/chrony.conf` manually.

If time synchronization is not enabled, a warning message is displayed in the menu column.

The VBC Controller will also itself act as NTP server. Setting the VBC IP address in the **Setup — Routing** view in the probe or VB288 user interface will automatically add it as a time synchronization source. It is also possible to list the VBC IP address manually in the **Setup — Params** view.

For more details on how to configure Chrony, please refer to *How to serve the Network Time Protocol with Chrony*¹.

¹<https://ubuntu.com/server/docs/how-to-serve-the-network-time-protocol-with-chrony>