VideoBRIDGE Controller User's Manual

Applies to software release v5.5

Form 7657L • February 2019

VideoBRIDGE Controller User's Manual
Revision 0f39023 (2019-02-27)

Copyright
© 2019 Sencore, Inc. All rights reserved.
3200 Sencore Drive, Sioux Falls, SD USA
www.sencore.com
This publication contains confidential, proprietary, and 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 Sencore. Information in this document is subject to change without notice and Sencore Inc. assumes no responsibility or liability for any errors or inaccuracies. Sencore, Sencore Inc, and the Sencore logo are trademarks or registered trademarks in the United States and other countries. 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 Sencore. The presence of such links does not imply that Sencore endorses or recommends the content on those pages. Sencore acknowledges the use of third-party open source software and licenses in some Sencore products. This freely available source code can be obtained by contacting Sencore Inc.

About Sencore
Sencore is an engineering leader in the development of high-quality signal transmission solutions for the broadcast, cable, satellite, IPTV, and telecommunications markets. The company's world-class portfolio includes video delivery products, system monitoring and analysis solutions, and test and measurement equipment, all designed to support system interoperability and backed by best-in-class customer support. Sencore products meet the rapidly changing needs of modern media by ensuring the efficient delivery of high-quality video from the source to the home. More information about Sencore is available at the company's website, www.sencore.com.

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. (http://www.openssl.org/).
  Copyright © 1998-2017. The OpenSSL Project. All rights reserved.
- Webmin. Copyright © Jamie Cameron.

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

Contents

Contents 3

Document Revision History 8

1 INTRODUCTION 9
- 1.1 Sites and Blades . . . 9
- 1.2 Users and Access . . . 9
- 1.3 How to Use This Manual . . . 10

2 INSTALLATION AND INITIAL SETUP 12
- 2.1 System Requirements . . . 12
- 2.2 First-time Installation . . . 13
- 2.3 Deploying in a Virtualized Environment . . . 15
- 2.4 Verifying Correct Initial Setup and Software Activation . . . 15
- 2.5 Initial Setup Troubleshooting . . . 18
- 2.6 Upgrading From a Previous Version . . . 18
  - 2.6.1 Using an Installation Script . . . 19
  - 2.6.2 Using Software Activation . . . 19
  - 2.6.3 Using a full reinstall . . . 20
- 2.7 Accessing the User Interface . . . 20
- 2.8 Firewall Configuration . . . 21
- 2.9 License Details . . . 22
- 2.10 Accessing Software Activation interface . . . 23
- 2.11 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 Live . . . 31
5.3 Monitoring . . . 32
5.3.1 Monitoring — Top Level . . . 32
5.3.2 XML Alarms . . . 38
5.3.3 Monitoring — Site . . . 38
5.3.4 Monitoring — Blade . . . 40
5.3.5 Monitoring — All sites . . . 40
5.4 Blade alarms . . . 43
5.5 Graphics view (Graphics option) . . . 47
5.6 Stream view . . . 49
5.6.1 Stream names, class and interface . . . 50
5.6.2 Stream view — Selected . . . 51
5.6.3 Selected Stream Compare MediaWindow . . . 55
5.6.4 Selected Stream Compare ETR . . . 56
5.6.5 Selected Stream Compare Streamdata . . . 57
5.7 Thumbs view . . . 60
5.8 Service view (Transport Stream Service View option) . . . 62
5.8.1 Service view — Thumbs . . . 63
5.8.2 Service view — Selected . . . 64
5.8.3 Selected TS Service Compare ETR . . . 66
5.9 Map . . . 67
5.10 RDP . . . 68
5.11 RDW . . . 70
5.11.1 RDW — Canvases . . . 70
5.11.2 RDW — Devices . . . 71
5.11.3 RDW — Tags . . . 72
5.11.4 Canvas Configurator . . . 73
5.11.5 Remote Data Wall Widgets . . . 75
5.11.5.1 Web Widget . . . 75
5.11.5.2 Textbox Widget . . . 75
5.11.5.3 Thumbnail Widget . . . 75
5.11.5.4 Loudness Widget . . . 76
5.11.5.5 Media Window Widget . . . 76
5.11.5.6 Alarms Widget . . . 77
5.11.5.7 RF Graph Widget . . . 77
5.11.5.8 Clock Widget . . . 77
5.11.5.9 Slide Widget . . . 77
5.11.5.10 Countdown Widget . . . 78
5.11.5.11 Graphics Widget . . . 78
5.11.5.12 Stream View Widget . . . 78
5.11.5.13 Weather Widget . . . 78
5.11.5.14 Redundancy Widget . . . 78

5.11.5.15 MicroTimeline Widget . . . 79
5.11.5.16 OTT Graph Widget . . . 79
5.11.5.17 OTT Status Widget . . . 79
5.11.5.18 Constellation Widget . . . 79
5.11.5.19 RF Data Widget . . . 79
5.11.5.20 Map Widget . . . 80
5.11.5.21 Canvas Control Widget . . . 80
5.11.5.22 Tag Control Widget . . . 80
5.12 Equipment . . . 81
5.12.1 Equipment — Device list management . . . 83
5.12.2 Equipment — Device configuration management . . . 85
5.12.3 Equipment — Manual configuration file management . . . 87
5.12.4 Equipment — Device software and license management . . . 89
5.12.5 Equipment — Manage files . . . 92
5.13 Alarm setup . . . 93
5.13.1 Alarm setup — Message Fwd . . . 94
5.13.2 Alarm setup — Scheduling . . . 99
5.14 Timeline (requires Archive Server) . . . 103
5.14.1 Choosing what to inspect . . . 103
5.14.2 Navigating in time . . . 103
5.14.3 Persistent layout . . . 104
5.15 Reports . . . 106
5.15.1 Reports — Manual Report . . . 107
5.15.2 Reports — Report list . . . 108
5.15.3 Reports — Auto reports . . . 110
5.15.4 Reports — Import logo . . . 111
5.15.5 Reports — The PDF Report . . . 111
5.16 Ext. Reports . . . 116
5.16.1 Ext. Reports — Manual extended report . . . 117
5.16.2 Ext. Reports — Extended report list . . . 119
5.16.3 Ext. Reports — Auto extended reports . . . 120
5.16.4 Ext. Reports — PDF Report . . . 122
5.16.5 Ext. Reports — Alarm poll and report status . . . 125
5.16.6 Ext. Reports — Setup storage . . . 127
5.17 Main — Sites and Users . . . 128
5.17.1 Sites and Users — Sites . . . 128
5.17.2 Sites and Users — Users . . . 129
5.17.3 Sites and Users — User groups . . . 131
5.18 Main — Logs . . . 132
5.18.1 Logs — Logs . . . 132
5.18.2 Logs — Settings . . . 133
5.19 Main — Snapshots . . . 134
5.20 Main — Alarm statistics . . . 135

5.21 Main — Stream groups . . . 137
5.22 Main — Service groups . . . 138
5.23 Main — Archive Setup . . . 139
5.23.1 Archive server . . . 139
5.23.2 Enabling the Archive server . . . 139
5.23.3 Configuration . . . 139
5.23.4 System requirements . . . 140
5.23.5 Alarms . . . 140
5.24 Main — Gfx. View Setup (Graphics option) . . . 141
5.24.1 Configure diagrams . . . 141
5.24.2 Setup and data mapping . . . 143
5.25 Main — General . . . 146
5.25.1 General — Clear . . . 146
5.25.2 General — Connections . . . 147
5.25.3 General — Preferences . . . 149
5.25.4 General — Authentication . . . 150
5.26 Main — Network . . . 152
5.27 Main — About . . . 153
5.27.1 About — Release info . . . 153
5.27.2 About — License . . . 154
5.27.3 About — Technologies . . . 155
5.27.4 About — Credits . . . 155
5.27.5 About — System . . . 156
5.27.6 About — Data . . . 158

A Appendix: Separate Probe and Network Interfaces 159

B Appendix: The VBC Files 160

C Appendix: The VBC System Services 162

D Appendix: Example Site Configuration 164

E Appendix: Getting the Thresholds Right 166

F Appendix: Probe Versus VBC Alarms 169

G Appendix: Troubleshooting 171

H Appendix: Backing up the VBC 172
H.1 Backing up the VBC . . . 172
H.2 Restoring the VBC from backup . . . 172
H.3 Restoring the nightly backup . . . 173
H.4 Obtaining the backup script from a newer version . . . 173

I Appendix: On-line License Verification 174
I.1 Introduction 174
I.2 Requirements 174

J Appendix: Software Maintenance 177

K Appendix: Network configuration 178
K.1 Web-based configuration 178
K.2 Command-line based configuration 179

L Appendix: Enabling HTTPS 184

M Appendix: Enabling NTP time synchronization 188

Document Revision History

Date	*Version*	*Description*
February 2019	5.5	Updated manual to reflect changes in v5.5 software
February 2018	5.4	Updated manual to reflect changes in v5.4 software
February 2017	5.3	Updated manual to reflect changes in v5.3 software
March 2016	5.2	Updated manual to reflect changes in v5.2 software
February 2015	5.1	Updated manual to reflect changes in v5.1 software
January 2014	5.0	Updated manual to reflect changes in v5.0 software

1 INTRODUCTION

The VBC (VideoBRIDGE Controller) is a server-side software application that offers central management of Sencore VideoBRIDGE 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 VideoBRIDGE 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 VideoBRIDGE 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 VideoBRIDGE 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 menus. 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 5.5 of the VideoBRIDGE 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 uni- or multicast (for Ethernet input) or one transport stream (ASI, COFDM, QAM/VSB or QPSK/DVB-S2).

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 VideoBRIDGE Controller's IP address.

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 VideoBRIDGE Controller.

G Appendix: Troubleshooting lists some hints troubleshooting VideoBRIDGE Controller issues.

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

I Appendix: On-line License Verification outlines the on-line license verification procedure.

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

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

M 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 obtained from Sencore ProCare support by emailing procare@sencore.com.

2 INSTALLATION AND INITIAL SETUP

2.1 System Requirements

For demonstration purposes the minimum hardware requirements are:

- Quad-core 1.6 GHz CPU
- 4 Gbyte RAM minimum (remember to fill up all memory channels)
- 100 Gbyte writable disk space
- 10/100/1000T Ethernet Network Interface card(s) with support for CentOS Linux 7 or Red Hat Enterprise Linux 7

The recommended VBC server specifications for a medium sized system (20 blades or 8000 streams) are:

- Intel Quad-core 2.4 GHz CPU or better
- 16 Gbyte 1600 MHz DDR RAM (remember to fill up all memory channels)
- 500 Gbyte writable disk space
- 10/100/1000T Ethernet Network Interface card(s) with support for CentOS Linux 7 or Red Hat Enterprise Linux 7

The recommended VBC server specifications for a large system (60 blades or 24000 streams) are:

- Intel Xeon 1630 v4 (4 cores, 8 threads, 3.7 GHz) CPU
- 24 Gbyte 1600 MHz DDR 4 RAM (remember to fill up all memory channels)
- 1 Tbyte writable disk space
- 10/100/1000T Ethernet Network Interface card(s) with support for CentOS Linux 7 or Red Hat Enterprise Linux 7

The recommended VBC server specifications for a very large system (100+ blades) are:

- Intel Xeon 1630 v4 (4 cores, 8 threads, 3.7 GHz)
- 24 Gbyte 2400 MHz DDR 4 RAM (remember to fill up all memory channels)
- 2 × 1 Tbyte SAS, 15000 RPM in a Hardware RAID 1 configuration
  For even better performance SSD disks can be used instead, in a similar RAID 1 configuration
- 10/100/1000T Ethernet Network Interface card(s) with support for CentOS Linux 7 or Red Hat Enterprise Linux 7

It is important that the number of RAM modules matches the number of memory channels supported by CPU. For dual socket systems the number of required RAM modules doubles.

Example recommended CPU: Intel Xeon E5-1630 v4[1]:
For this system there are 4 memory channels. So, for single socket systems 4 × 16 Gbyte RAM modules could be fitted, and for a dual socket system 8 × 16 Gbyte RAM modules could be used.

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

Supported platforms:

- CentOS Linux release 7 (7.0–7.6) for x86_64
- Red Hat Enterprise Linux Server release 7 (7.0–7.6) for x86_64

2.2 First-time Installation

Make sure that the server hardware matches the requirements listed above and then follow the procedure outlined below.

1. Obtain the latest installation kickstart image from Sencore.

   Installation media is provided both for CentOS Linux and Red Hat Enterprise Linux. If you install the Red Hat Enterprise Linux version, you will need an active subscription for Red Hat Enterprise Linux server.

2. Insert the installation medium into the server:

   - For DVD-based installations, burn the downloaded ISO image to a DVD and insert into the server.
   - For USB-based installation, transfer the downloaded image to a USB mass storage device using a tool such as **dd** (Mac, Unix, Linux) or **USBWriter**[2] (Windows).
   - For installation in a virtualized environment, attach the downloaded ISO image to a virtual DVD-ROM unit.

     Note: Please read the advice on how to configure the virtual machine in section 2.3 to ensure optimal performance.

3. Boot the server and make sure that the primary boot device is set appropriately. If the system fails to boot from the medium, you may need to configure the boot loader for 'legacy BIOS mode'.

[1] https://ark.intel.com/content/www/us/en/ark/products/92987/intel-xeon-processor-e5-1630-v4-10m-cache-3-70-gh
html

[2] https://sourceforge.net/projects/usbwriter/

4. The installer will run, please follow the on-screen prompts to install the system, taking note of the following:

   - **IMPORTANT:** Leave 'Software selection' at 'Custom software selected'.
   - **IMPORTANT:** In the 'Installation Destination', the default partitioning will create a large `/home` partition, which is unused. To avoid this, use the 'I will configure partitioning' option. Then use the 'Click here to create them automatically' and manually reduce the size of (or remove) the `/home` partition, instead giving that space to the `/` partition.
   - We recommend that you configure network settings (IP address, gateway, DNS) within the installer. Post-installation network configuration can be performed using the **nmtui** utility, please refer to K Appendix: Network configuration for details.
   - The default installation does not provide any graphical user interface environment. This can be installed later if desired, please refer to the CentOS Linux[3] or Red Hat Enterprise Linux[4] documentation for more details.

5. At the end of the installation procedure, the server is rebooted. Remove the installation media and ensure that the system boots up properly.

6. If you installed the Red Hat Enterprise Linux server flavor, make sure you follow the instructions on how to subscribe the system to the Red Hat Customer Portal[5].

   If you install the CentOS Linux flavor, you may want to enable the Continuous Release repository[6] to be able to get access to security updates as quickly as possible.

7. 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.

   Continue to chapter 2.4 for details on how to enable the VideoBRIDGE Controller system.

The kickstart will install CentOS Linux 7 or Red Hat Enterprise Linux 7 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.

Note that new installations of VBC must use the kickstart install procedure.

[3] `https://wiki.centos.org/Manuals/ReleaseNotes/CentOS7`
[4] `https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/index.html`
[5] `https://access.redhat.com/solutions/253273`
[6] `https://wiki.centos.org/AdditionalResources/Repositories/CR`

2.3 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.

Please follow the steps from chapter 2.2 when installing the software in the virtualized environment. We recommended **disabling** any 'Easy 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.

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 described in the previous chapter, 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 with point 6 as described in the previous chapter.

When logging in to the console of the pre-built images, the default password for the **root** user is **elvis**. The same password is also used for logging in remotely using Secure Shell (ssh). **Please change the password for the root user after finishing the install**, log in and use the `passwd` command to do this.

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.

1. Launch a web browser application on the management system.

   Any web browser with support for JavaScript can be used to access the Software Activation interface, one of the following are recommended:

   - Google Chrome
   - Mozilla Firefox
   - Microsoft Edge
   - Microsoft Internet Explorer 11 or higher
   - Apple Safari

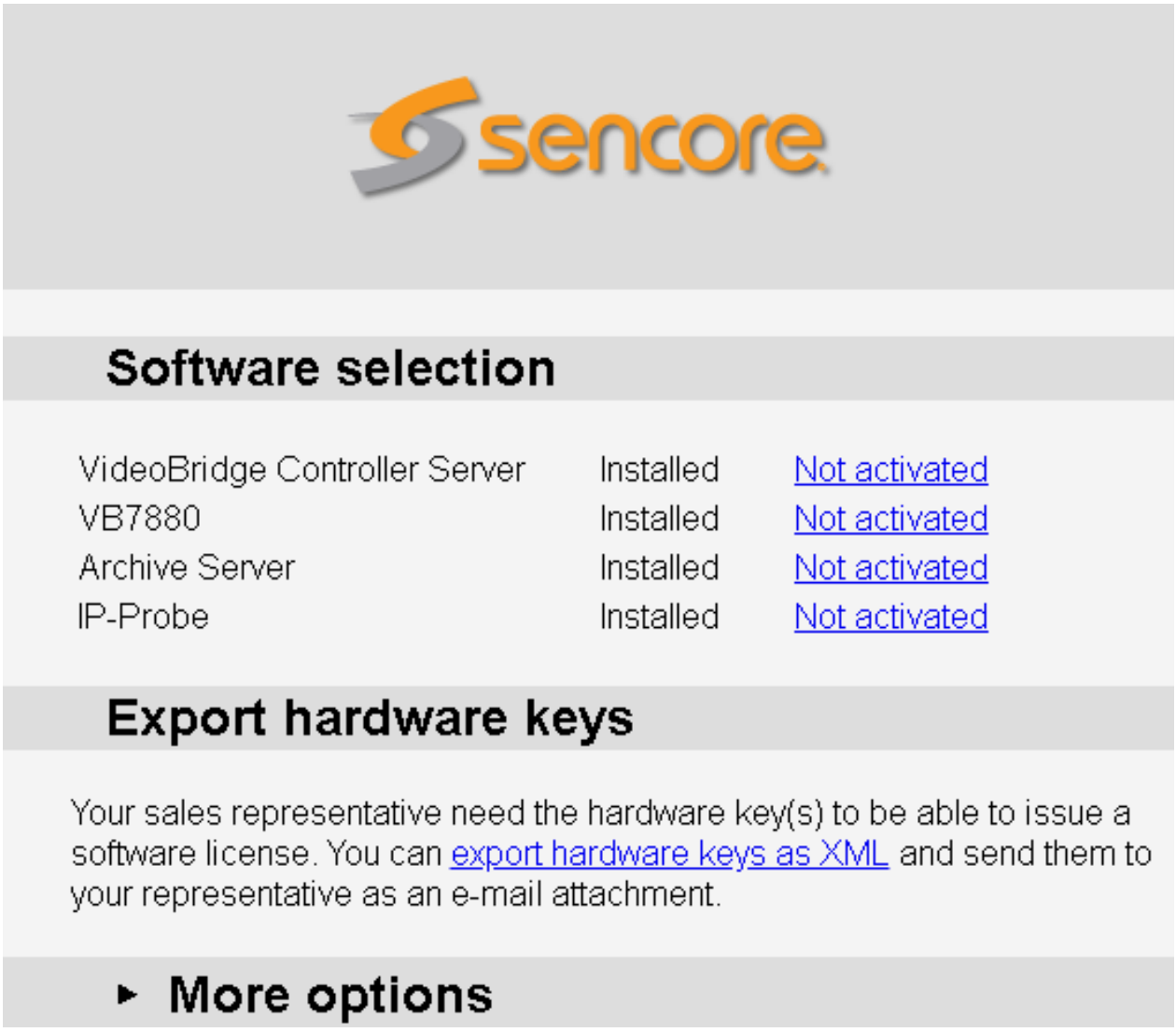


Figure 2.1: Software Activation

2. Type the IP address of the server in the browser URL field and press Enter.

   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 Software Activation view should be displayed inside the browser. Software Activation is password-protected, the user name is **admin** and the default password is **elvis**. The page displayed should look similar to figure 2.1.

   The password should be changed from the default. Expand the **More options** heading and follow the instructions under **Change password**[7].

4. If you already have an XML file with license keys for your system, click on the **More options** heading and upload this file under the **Import license keys** option. If you have the license key written down or in an e-mail, instead use the product page described below.

5. If this is a new server, and you need to obtain license keys for the purchased products, please click the link labeled **export hardware keys as XML** and send the downloaded file to your sales representative as an e-mail attachment.

6. The VideoBRIDGE Controller is not enabled by default on the newly installed server. To enable it, use the link labeled **Not activated** next to its name. This will take you to a page giving you the details of the installed software, such as the installed version and the hardware key. 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 software** and wait for it to finish. If successful, the VideoBRIDGE 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 Software Activation view to make changes, open the **About — License** tab in the VideoBRIDGE Controller user interface and click the link labeled **Manage installed software**.

By default, all web communication to and from the host running the VideoBRIDGE Controller is using un-encrypted HTTP communication. Please refer to L Appendix: Enabling HTTPS for information on how to enable HTTPS.

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

[7] If you forget the Software Activation password, you can reset it by logging in as root and issuing the command `/opt/btech/ssg/bin/reset_web_password`

2.5 Initial Setup Troubleshooting

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

- Verify that the client machine and the VideoBRIDGE 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 VideoBRIDGE 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 VideoBRIDGE 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 httpd
  ```

  on the server's command line. If it is not running properly, or you are seeing **DNS lookup failure** errors, try issuing the command

  ```
  echo "ServerName localhost" >> /etc/httpd/conf/httpd.conf
  ```

  and then restart the server by issuing the command

  ```
  systemctl restart httpd
  ```

- If you can reach Software Activation but the VideoBRIDGE 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 K Appendix: Network configuration for more information on server network configuration.

2.6 Upgrading From a Previous Version

We strongly recommend backing up the VBC files before upgrading to a new version of the VideoBRIDGE Controller, or when upgrading to a new release of the OS. The backup procedure is described in H Appendix: Backing up the VBC of this manual.

To upgrade to this release of the VideoBRIDGE Controller, your system must meet the system requirements described in chapter 2.1. If your system does not meet these requirements, the installation procedure will stop with an error message.

VideoBRIDGE Controller version 5.5 will be able to upgrade VBC version 5.2 or later only. Only systems running CentOS Linux or Red Hat Enterprise Linux 7.x can be upgraded. For systems running older versions of VBC or older versions of the operating system you must first backup the system by following the procedure described in H 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 2.6.3 Using a full reinstall.

VideoBRIDGE Controller version 5.3 was the last version with support for CentOS Linux or Red Hat Enterprise Linux release 6.x, 5.5 only supports release 7. The current version of the operating system can be found on the **About — Release info** tab in the user interface.

2.6.1 Using an Installation Script

Copy the installation script to the system. Log in as root and run the installation script by issuing the command

```
sh filename.run
```

(where *filename.run* is the name of the installation script). You will be presented with a menu with options to **I**nstall the software or **D**isplay the README file. Press the appropriate key and press Enter to begin.

This will upgrade the required files in `/opt/btech/vbc`, and restart the VBC server processes if the software was already activated.

If error messages appear while running the installer script, please check out the README file from the installer for additional information (available from the installer menu).

If the installation fails, try re-installing the system as described above.

2.6.2 Using Software Activation

It is also possible to upload the VBC using the Software Activation interface. Access Software Activation and expand the **More options** heading. Under the heading **Update software**, select

the software image file to be uploaded and click the **Update** button. The image will have a **.tea** extension. When the software has been transferred to the VBC, the **Update software** button to initiate the update.

If the VBC software was already activated, you will be transferred to a progress bar displaying the update status.

If the software was not activated, the upgrade will run in the background and you will be forwarded to the product page inside the Software Activation interface. Depending on how long the update takes, you may need to reload the product page again to verify that the software has been updated.

If the software upgrade fails, you can find a log describing the upgrade procedure by logging in to the VBC server and opening the file `/opt/btech/vbc/log/upgrade.log`

2.6.3 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 5.2
- Upgrading from a system running CentOS Linux or Red Hat Enterprise Linux release 6.x or older
- 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 H 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 H Appendix: Backing up the VBC.

Please note that the hardware key will change when the VBC is reinstalled on a new machine. Please see section 2.9 License Details on how to obtain the current hardware key and contact your sales representative to obtain a new license key.

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:

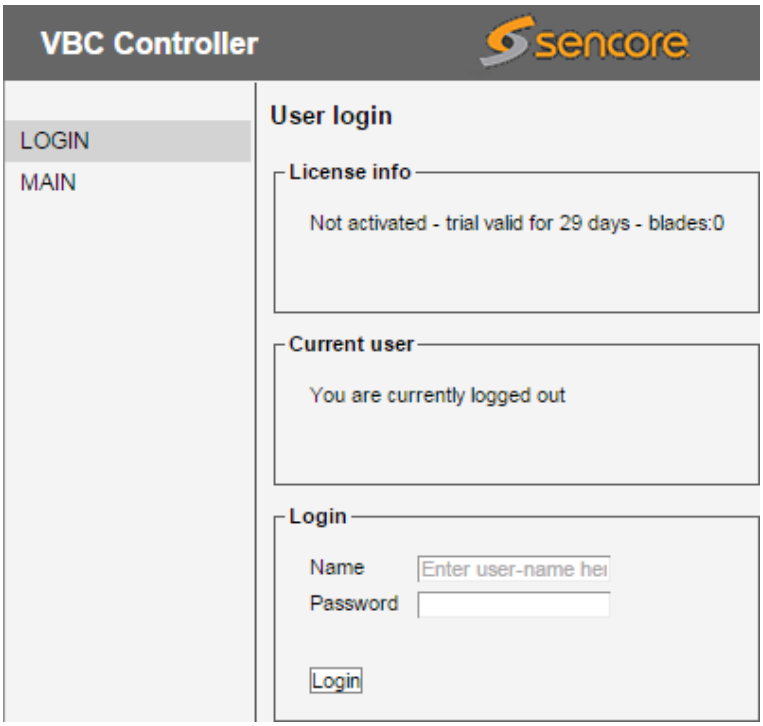


Figure 2.2: The VideoBRIDGE Controller Graphical User Interface

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Microsoft Internet Explorer 11 or higher
- Apple Safari

The login view should be displayed inside the browser. This should look similar to figure 2.2. If you have problems accessing the user interface, refer to chapter 2.5 for troubleshooting.

2.8 Firewall Configuration

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

Protocols and ports	
Web (TCP port 80 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 and 8080)	Required. The VBC will intercept and forward Web requests from clients towards probes on port 80. Port 8080 is only used if MDC is part of the VBC configuration.
Probe polling (XML over TCP port 80)	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 M 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 License Details

After the unlicensed VideoBRIDGE Controller software is installed, it will run in a trial mode for 30 days with unrestricted access to features. After this period, if a license key has not been obtained, the VBC will revert to being an element manager with no access to licensed features and with no alarm features.

To obtain a license the **Hardware key** displayed in the **About — License** view is given to Sencore, who will return a **Product License Key** which is submitted from the same view. The Hardware Key can also be seen in the Software Activation interface.

2.10 Accessing Software Activation interface

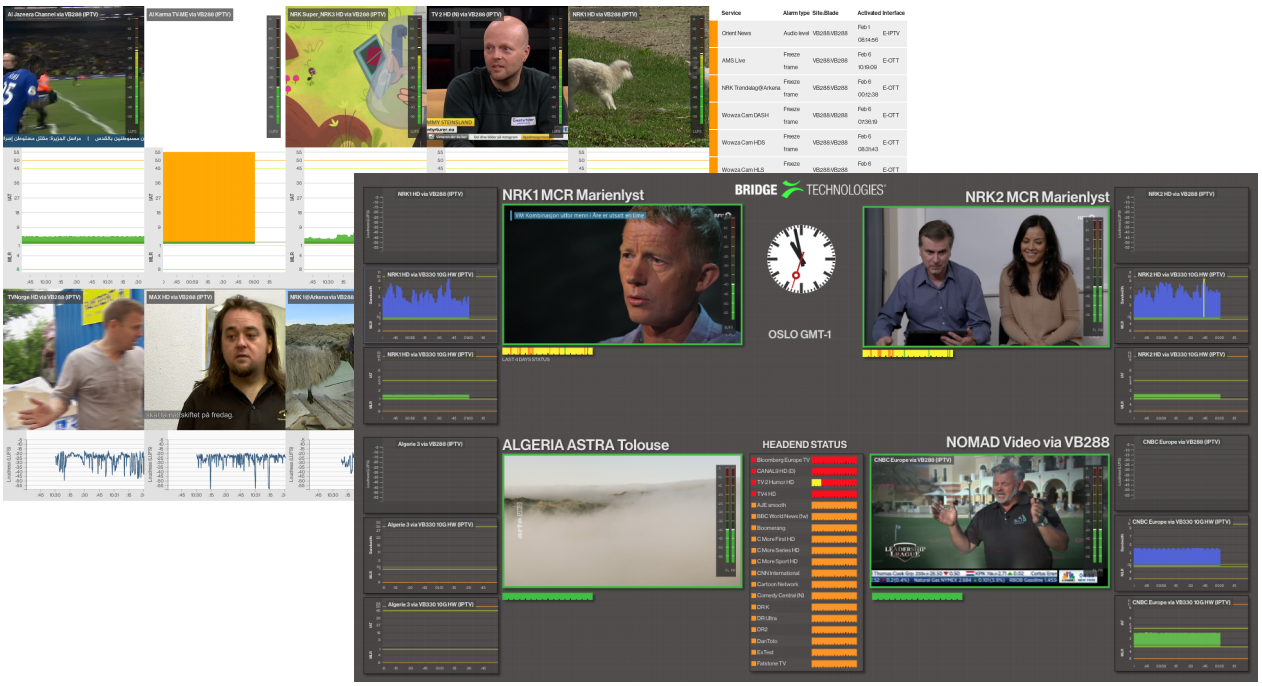
To return to the Software Activation view after activating the VideoBRIDGE Controller, you can either navigate to the **About — License** view and follow the **Manage installed software** link, or navigate your web browser to the address `http://<IP>/ssg`, where `<IP>` is the IP address (or host name, if using DNS) of the server.

2.11 Deactivating

To deactivate VideoBRIDGE Controller, you must first access the Software Activation interface (see the previous section) and make sure that it is not set to the default. Expand the **More options** heading and change the setting under **Set default software**.

Once this is done, access the VideoBRIDGE 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 VideoBRIDGE 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.

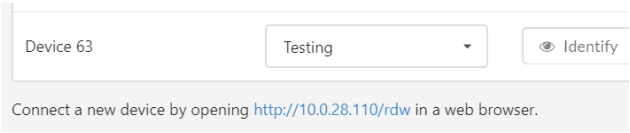
The Remote Data Wall can be configured to display mosaics from the selected streams, as well as alarm lists and other important information from within the system. A configured mosaic is called a *canvas* and is configured in the **RDW — Canvases** view. Please see chapter 5.11.5 below for more information 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.

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.



Go to chapter 5.11 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 VideoBRIDGE 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 VideoBRIDGE Controller. When the VideoBRIDGE Controller is equipped with the Master license, it allows sub-VBCs to be added from the **Equipment** menu and will fetch information from the sub-VBCs (also called external VBC or remote VBCs).

A regular VideoBRIDGE Controller becomes a Master VideoBRIDGE 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.

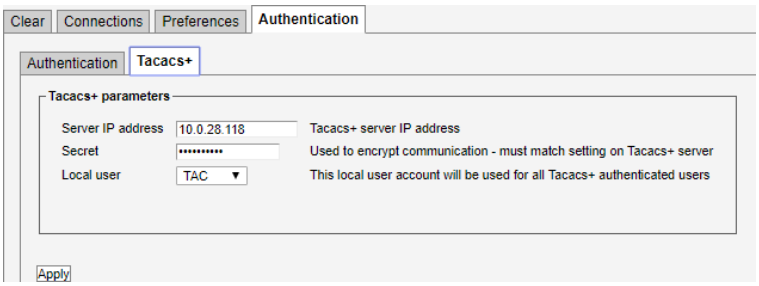
The Master VideoBRIDGE Controller can be licensed to support thousands of blades. The license details and blade count can be seen from the **About — License** view.

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

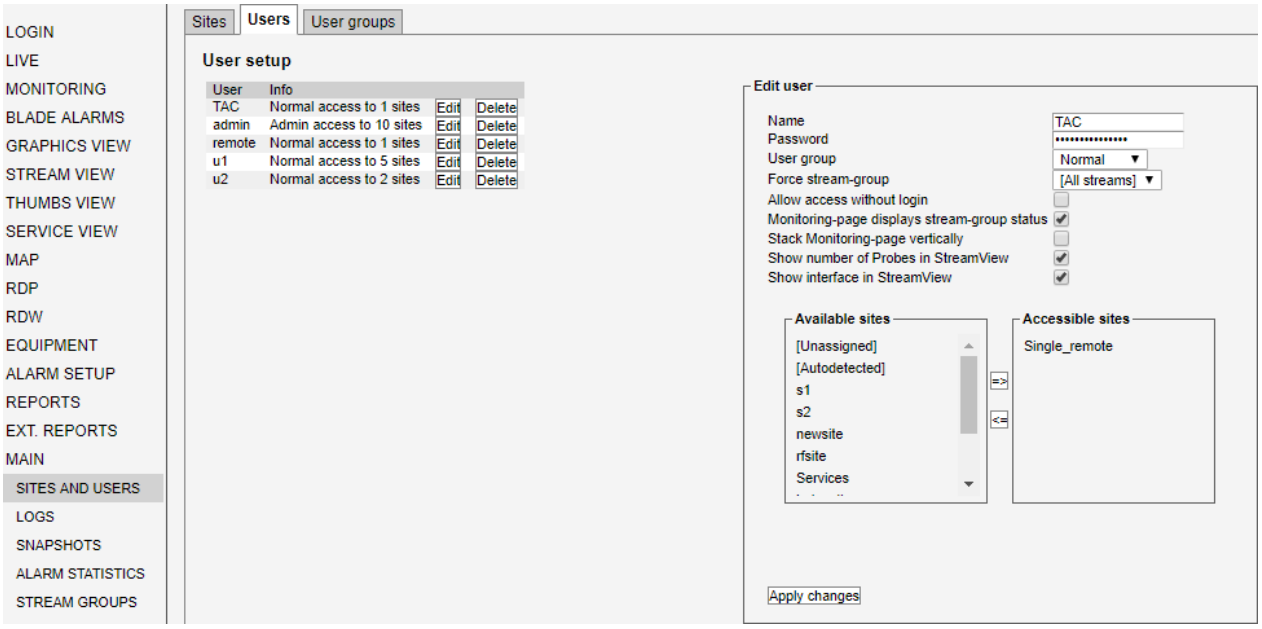
- The **Monitoring — All Sites** view shows status for any site, any VideoBRIDGE Controller.
- The *External site alarm* is raised for any sub-VBC having alarms.
- Seamless click-through to sub-VBCs from alarms and the **All Sites** view

4.2 Configuring access rights

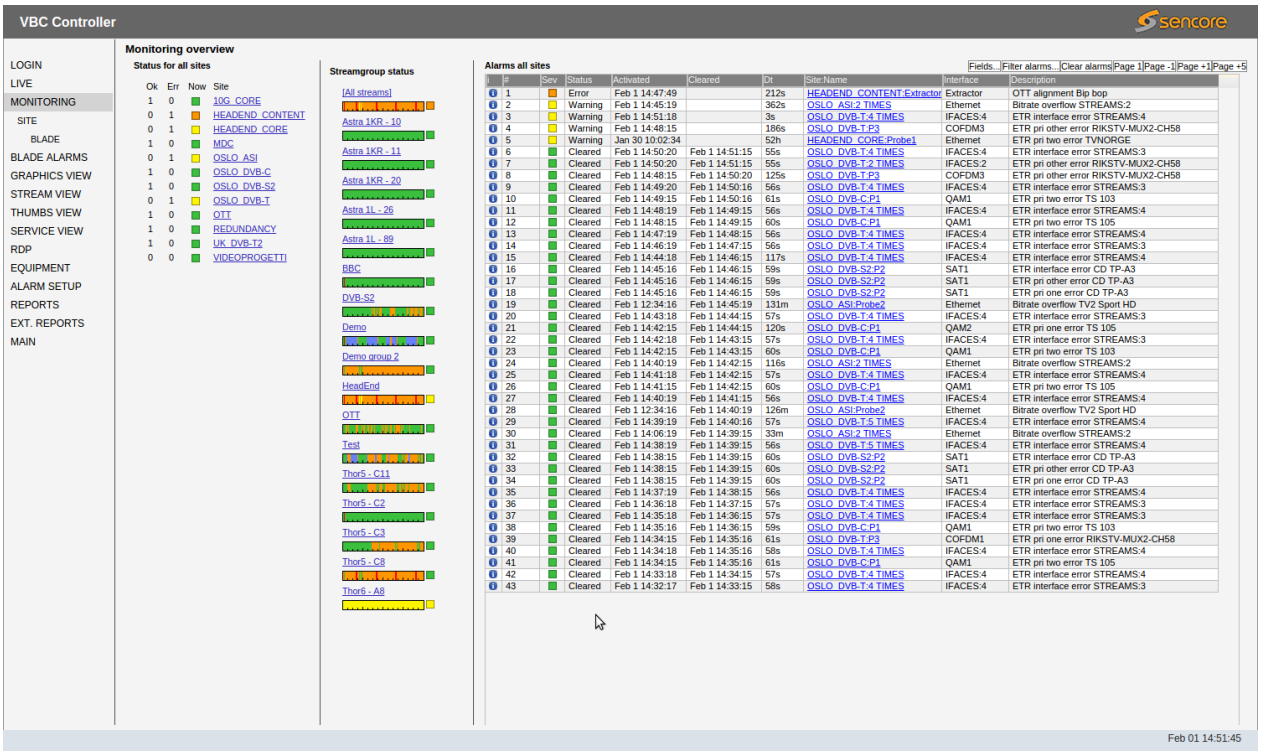
In order to avoid login requests when accessing the Sub-VBCs from within the Master VBC the The same user account must exist on the Sub-VBC, with the **Allow access without login** flag checked in the **Main — Sites and Users — Users** User setup view. If TACACS+ authentication is enabled, the same constraints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



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.



5 THE VBC GRAPHICAL USER INTERFACE



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

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Microsoft Internet Explorer 11 or higher
- Apple Safari

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.

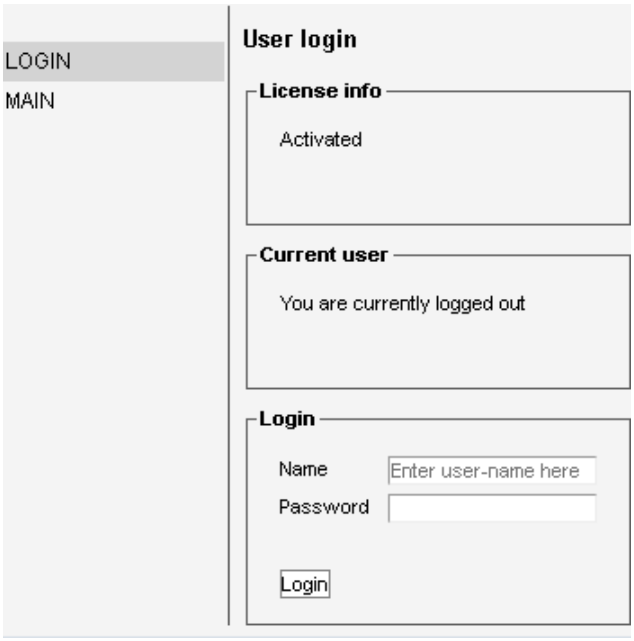
The interface is easy and intuitive to use. The tree menu is always located on the left hand side. The menu contains more entries for the *admin* than the menu for regular users. Some menu items are

nested, in particular the site and blade sub-menu entries are provided to allow quick access to the last visited site and blade.

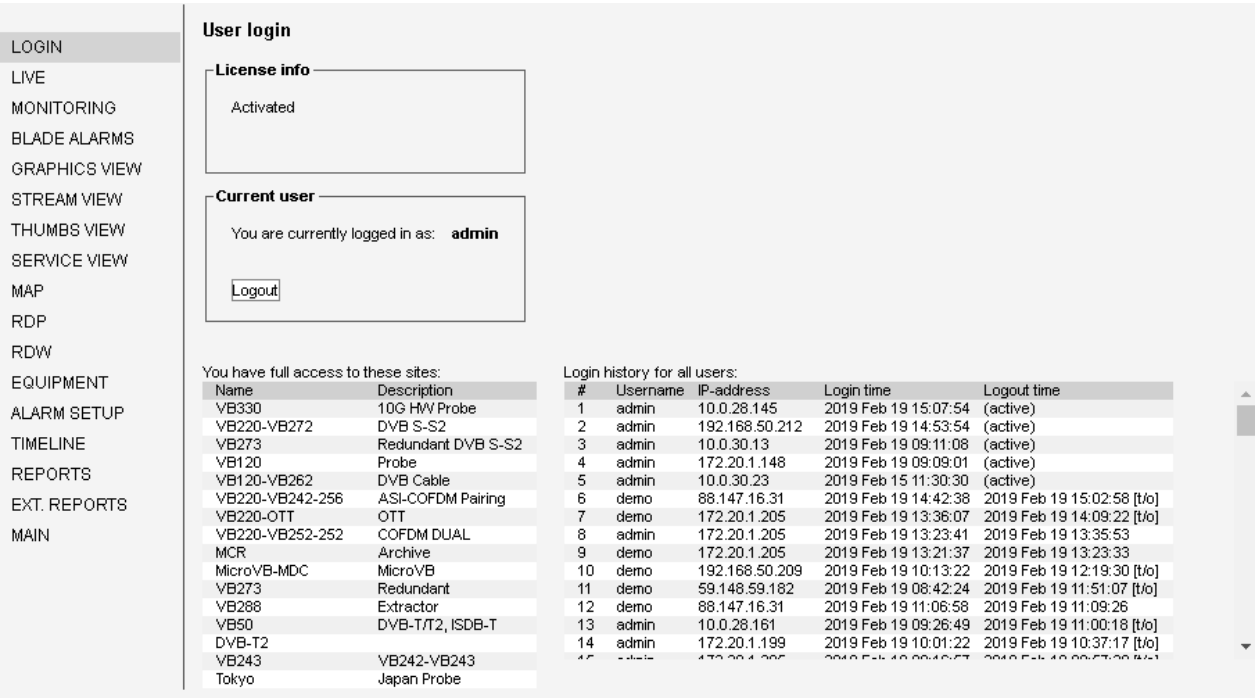
The web interface has been designed to be resizable in both vertical and horizontal directions with a minimum screen resolution of 1280×800 pixels. For operational use it is however highly recommended that a higher screen resolution is used. The **Stream view**, **Thumbs view** and **Service view** pages will automatically adapt to the current area of the browser window after it has been resized and the screen is refreshed.

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

5.1 Login



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

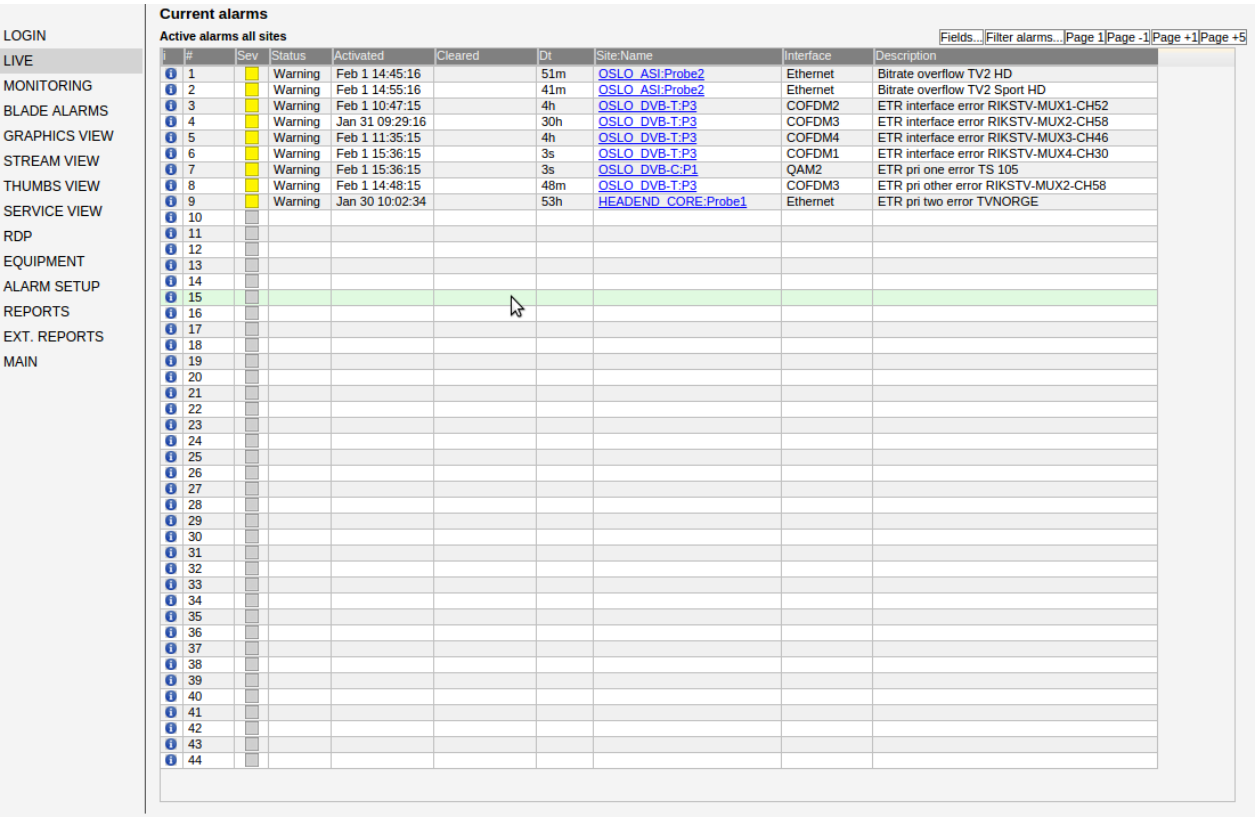


After a user has logged in, the menu-tree changes to reflect the new options.

A status-line lists all the sites that the user can access and states his access-rights (full or read-only). A login history for the user is also provided.

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 Live



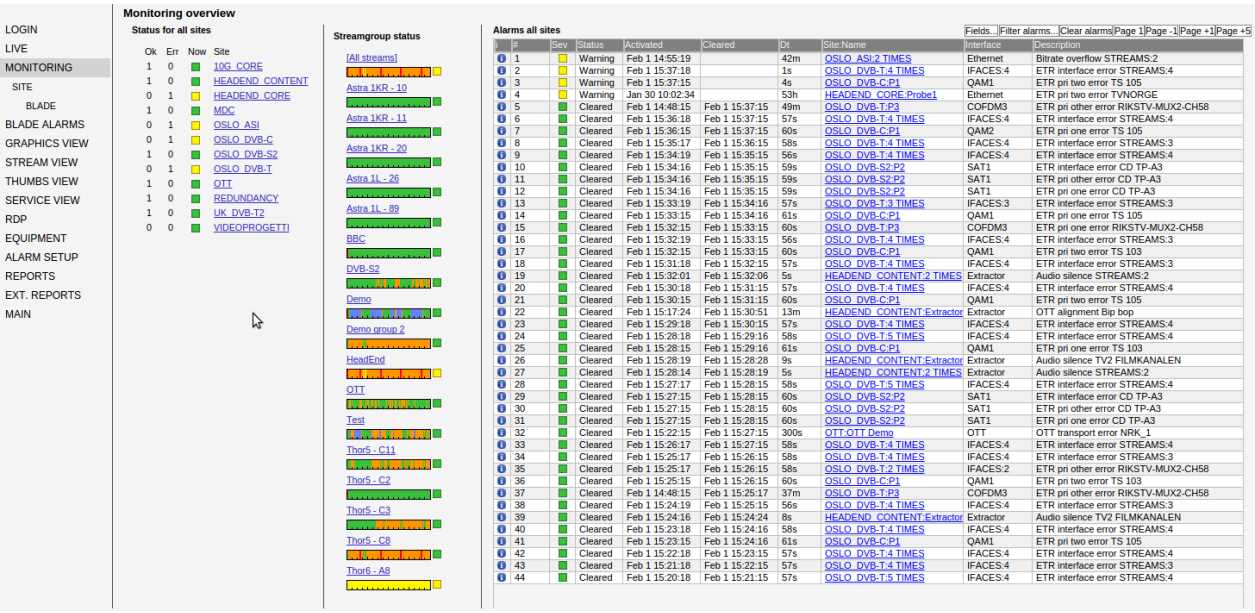
i	#	Sev	Status	Activated	Cleared	Dt	Site:Name	Interface	Description
	1		Warning	Feb 1 14:45:16		51m	OSLO_ASI:Probe2	Ethernet	Bitrate overflow TV2 HD
	2		Warning	Feb 1 14:55:16		41m	OSLO_ASI:Probe2	Ethernet	Bitrate overflow TV2 Sport HD
	3		Warning	Feb 1 10:47:15		4h	OSLO_DVB-T:P3	COFDM2	ETR interface error RIKSTV-MUX1-CH52
	4		Warning	Jan 31 09:29:16		30h	OSLO_DVB-T:P3	COFDM3	ETR interface error RIKSTV-MUX2-CH58
	5		Warning	Feb 1 11:35:15		4h	OSLO_DVB-T:P3	COFDM4	ETR interface error RIKSTV-MUX3-CH46
	6		Warning	Feb 1 15:36:15		3s	OSLO_DVB-T:P3	COFDM1	ETR interface error RIKSTV-MUX4-CH30
	7		Warning	Feb 1 15:36:15		3s	OSLO_DVB-C:P1	QAM2	ETR pri one error TS 105
	8		Warning	Feb 1 14:48:15		48m	OSLO_DVB-T:P3	COFDM3	ETR pri other error RIKSTV-MUX2-CH58
	9		Warning	Jan 30 10:02:34		53h	HEADEND_CORE:Probe1	Ethernet	ETR pri two error TVNORGE
	10								
	11								
	12								
	13								
	14								
	15								
	16								
	17								
	18								
	19								
	20								
	21								
	22								
	23								
	24								
	25								
	26								
	27								
	28								
	29								
	30								
	31								
	32								
	33								
	34								
	35								
	36								
	37								
	38								
	39								
	40								
	41								
	42								
	43								
	44								

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.

5.3 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.

5.3.1 Monitoring — Top Level



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** menu.

The user can select which alarms to show and hide in the **Filter alarms** menu. 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.

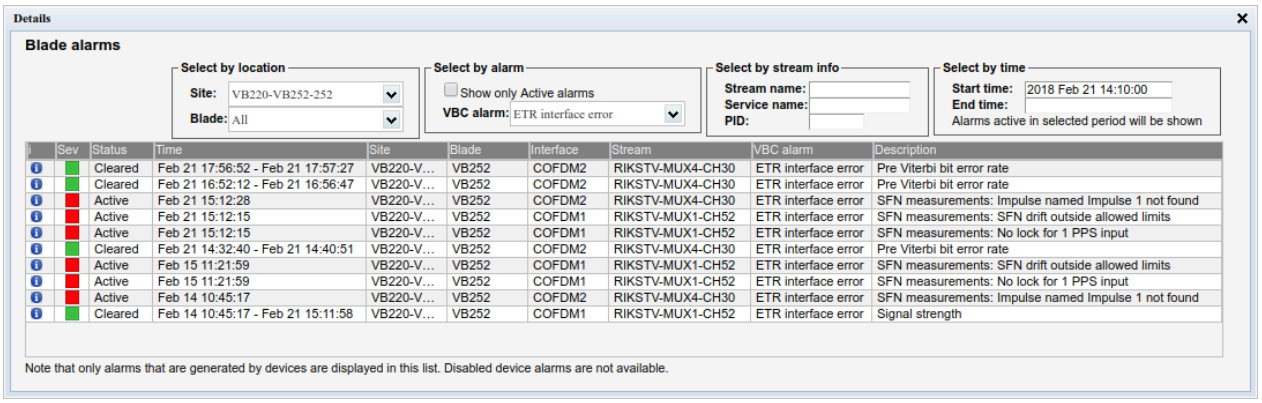
The following table shows examples of alarm aggregation:

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 M 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 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):

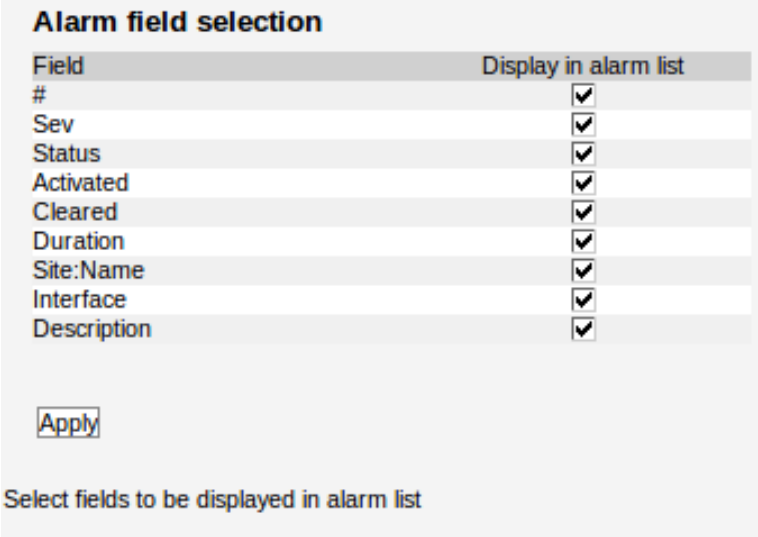
Message	*Description*
No contact	This alarm is raised if the VBC is unable to obtain status from a particular probe. The probes are polled every 60 seconds, so if raised, this alarm will stay active until poll contact is achieved.
External site alarm	This alarm will be raised if a remote VBC has alarms 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 VB7880 Advanced Content Extractor has detected that either the signal is scrambled while expecting it not to be or vice versa. The VB7880 allows the configuration of these alarms per stream.
OTT alignment	Reported by the VB7880 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 during the last poll period a VB7880 has detected that a service with closed caption monitoring had less caption services than specified in its threshold.
Caption quality	This alarm indicates that during the last poll period a VB7880 has detected a quality issue with one or more of the caption services extracted from a service with closed caption monitoring.
QoE video	This alarm indicates that during the last poll period a VB7880 Advanced Content Extractor has detected 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 on the VB7880 a stream was either too silent or too loud 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%.

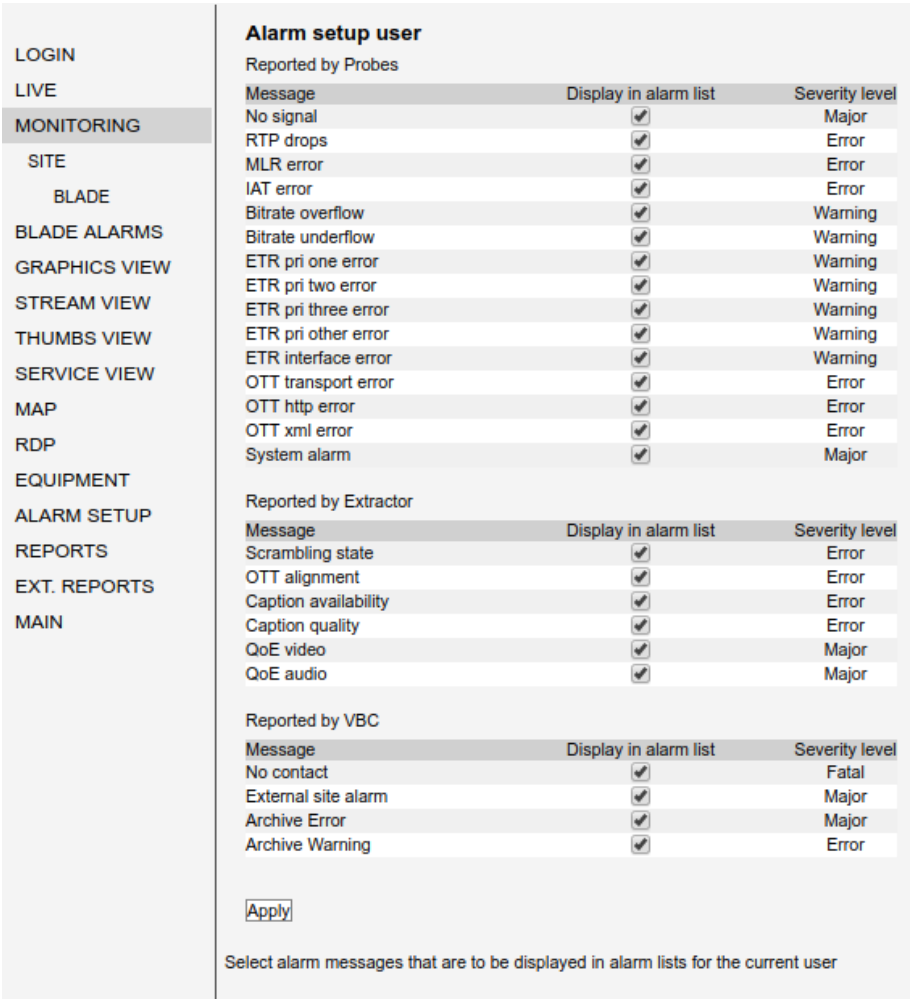
Please note that the alarm window can be changed from the default 1 hour as assumed in the above explanations. For shorter alarm windows the number of error seconds required are scaled accordingly.

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.



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.

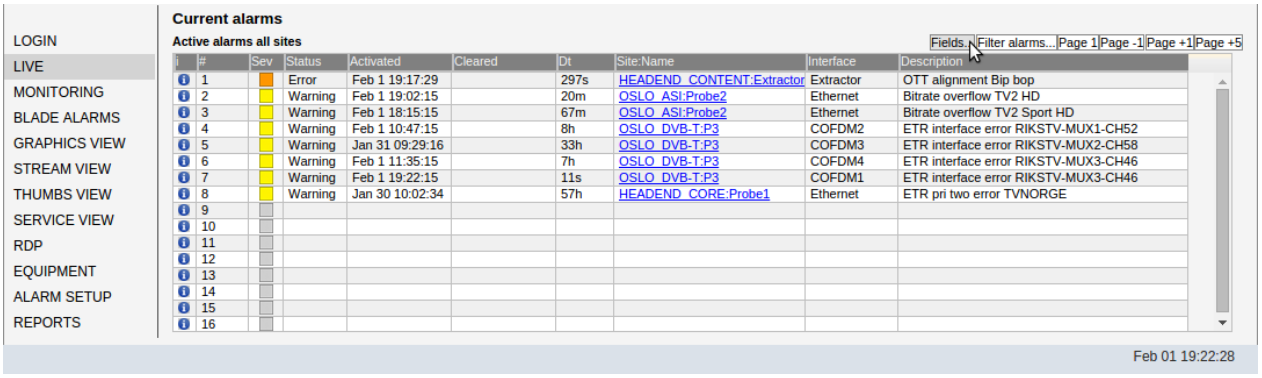


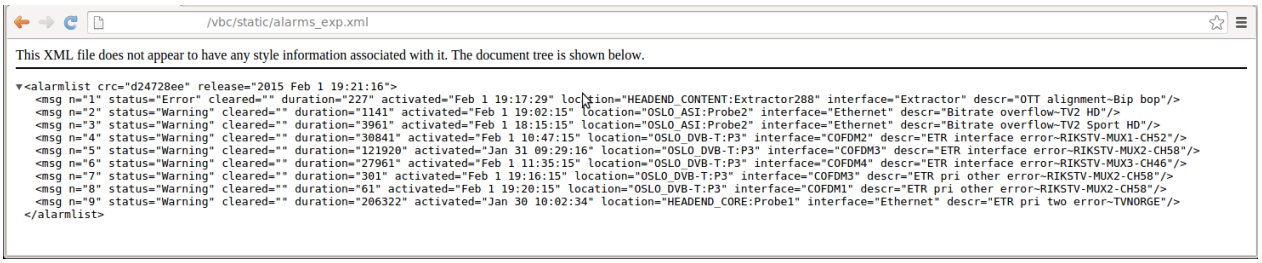
The user may clear out the alarm list by clicking the **Clear alarms** button. This hides the cleared alarms from the alarm list for the current user for this session, if the user logs out and in again the full alarm list will be displayed.

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

5.3.2 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.





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.

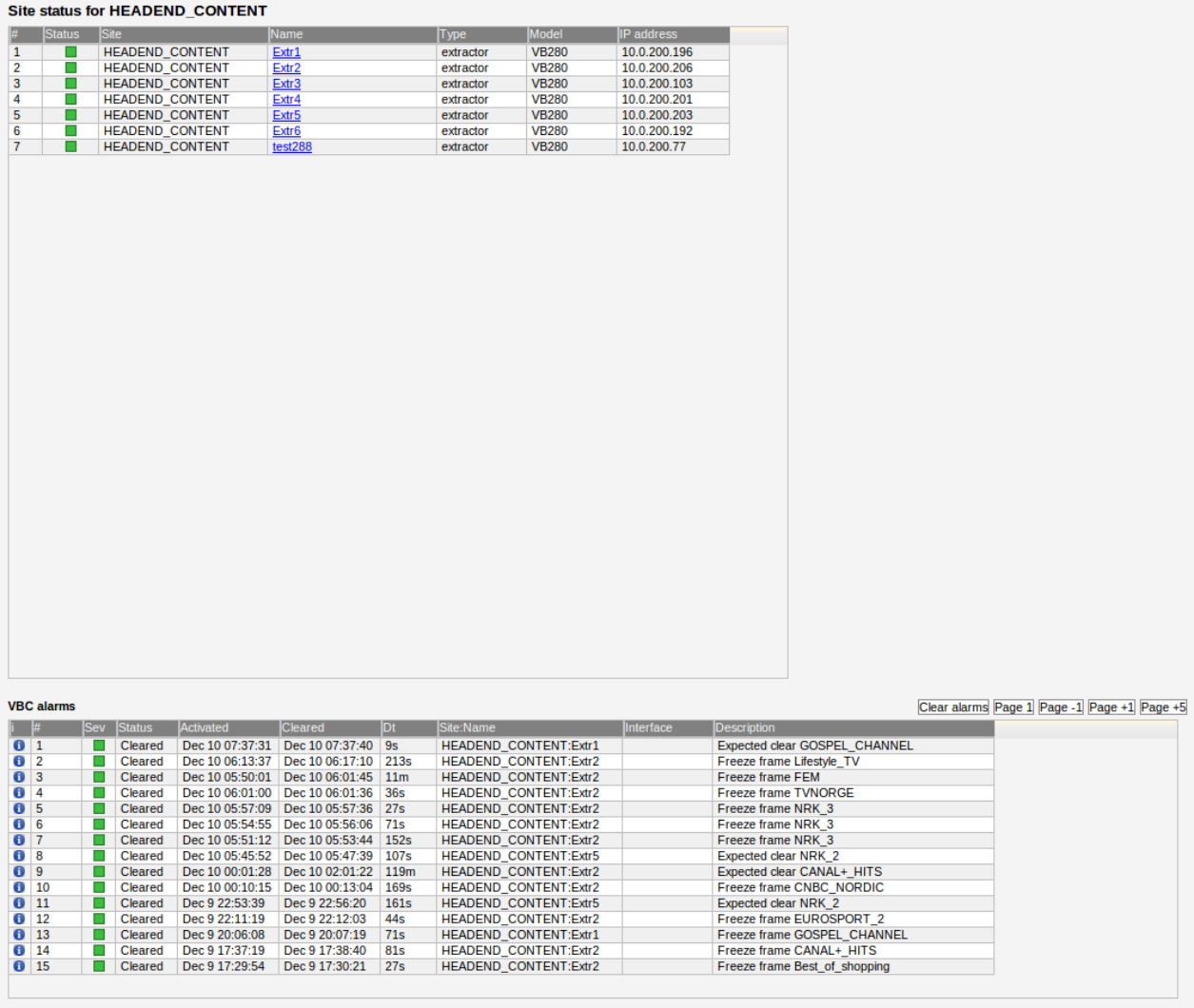
Refer to **Alarm setup** for a description on how alarms are also available via the MIB and SNMP traps.

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

5.3.3 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 HEADEND_CONTENT

#	Status	Site	Name	Type	Model	IP address
1		HEADEND_CONTENT	Extr1	extractor	VB280	10.0.200.196
2		HEADEND_CONTENT	Extr2	extractor	VB280	10.0.200.206
3		HEADEND_CONTENT	Extr3	extractor	VB280	10.0.200.103
4		HEADEND_CONTENT	Extr4	extractor	VB280	10.0.200.201
5		HEADEND_CONTENT	Extr5	extractor	VB280	10.0.200.203
6		HEADEND_CONTENT	Extr6	extractor	VB280	10.0.200.192
7		HEADEND_CONTENT	test288	extractor	VB280	10.0.200.77

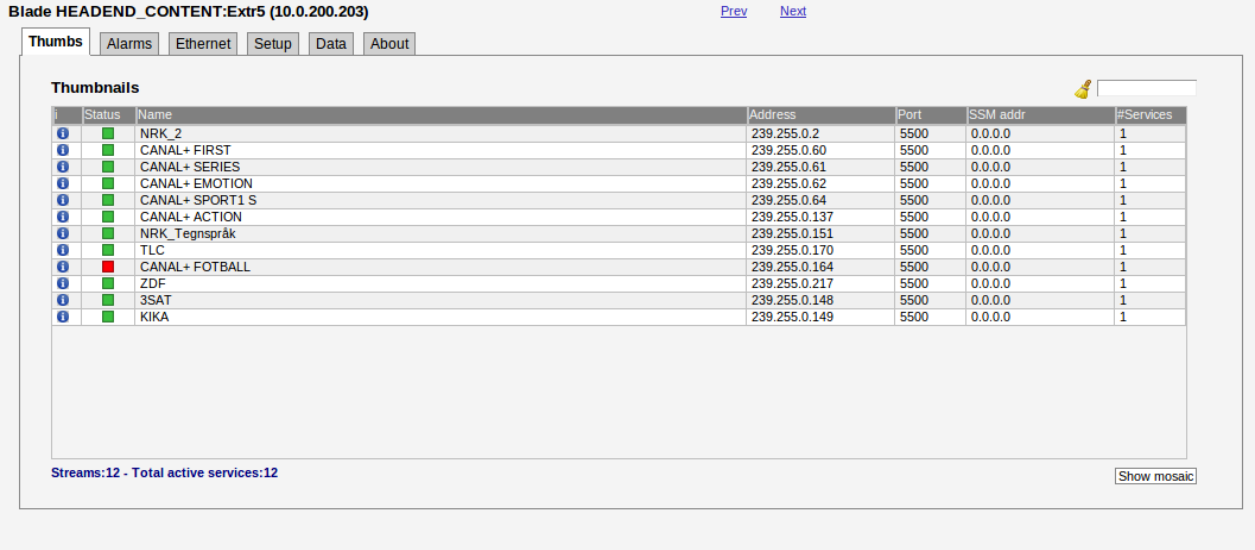
VBC alarms

Clear alarms | Page 1 | Page -1 | Page +1 | Page +5

i	#	Sev	Status	Activated	Cleared	Dt	Site:Name	Interface	Description
	1		Cleared	Dec 10 07:37:31	Dec 10 07:37:40	9s	HEADEND_CONTENT:Extr1		Expected clear GOSPEL_CHANNEL
	2		Cleared	Dec 10 06:13:37	Dec 10 06:17:10	213s	HEADEND_CONTENT:Extr2		Freeze frame Lifestyle_TV
	3		Cleared	Dec 10 05:50:01	Dec 10 06:01:45	11m	HEADEND_CONTENT:Extr2		Freeze frame FEM
	4		Cleared	Dec 10 06:01:00	Dec 10 06:01:36	36s	HEADEND_CONTENT:Extr2		Freeze frame TVNORGE
	5		Cleared	Dec 10 05:57:09	Dec 10 05:57:36	27s	HEADEND_CONTENT:Extr2		Freeze frame NRK_3
	6		Cleared	Dec 10 05:54:55	Dec 10 05:56:06	71s	HEADEND_CONTENT:Extr2		Freeze frame NRK_3
	7		Cleared	Dec 10 05:51:12	Dec 10 05:53:44	152s	HEADEND_CONTENT:Extr2		Freeze frame NRK_3
	8		Cleared	Dec 10 05:45:52	Dec 10 05:47:39	107s	HEADEND_CONTENT:Extr5		Expected clear NRK_2
	9		Cleared	Dec 10 00:01:28	Dec 10 02:01:22	119m	HEADEND_CONTENT:Extr2		Expected clear CANAL+_HITS
	10		Cleared	Dec 10 00:10:15	Dec 10 00:13:04	169s	HEADEND_CONTENT:Extr2		Freeze frame CNBC_NORDIC
	11		Cleared	Dec 9 22:53:39	Dec 9 22:56:20	161s	HEADEND_CONTENT:Extr5		Expected clear NRK_2
	12		Cleared	Dec 9 22:11:19	Dec 9 22:12:03	44s	HEADEND_CONTENT:Extr2		Freeze frame EUROSPORT_2
	13		Cleared	Dec 9 20:06:08	Dec 9 20:07:19	71s	HEADEND_CONTENT:Extr1		Freeze frame GOSPEL_CHANNEL
	14		Cleared	Dec 9 17:37:19	Dec 9 17:38:40	81s	HEADEND_CONTENT:Extr2		Freeze frame CANAL+_HITS
	15		Cleared	Dec 9 17:29:54	Dec 9 17:30:21	27s	HEADEND_CONTENT:Extr2		Freeze frame Best_of_shopping

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

5.3.4 Monitoring — Blade



i	Status	Name	Address	Port	SSM addr	#Services
		NRK_2	239.255.0.2	5500	0.0.0.0	1
		CANAL+ FIRST	239.255.0.60	5500	0.0.0.0	1
		CANAL+ SERIES	239.255.0.61	5500	0.0.0.0	1
		CANAL+ EMOTION	239.255.0.62	5500	0.0.0.0	1
		CANAL+ SPORT1 S	239.255.0.64	5500	0.0.0.0	1
		CANAL+ ACTION	239.255.0.137	5500	0.0.0.0	1
		NRK_Tegnspråk	239.255.0.151	5500	0.0.0.0	1
		TLC	239.255.0.170	5500	0.0.0.0	1
		CANAL+ FOTBALL	239.255.0.164	5500	0.0.0.0	1
		ZDF	239.255.0.217	5500	0.0.0.0	1
		3SAT	239.255.0.148	5500	0.0.0.0	1
		KIKA	239.255.0.149	5500	0.0.0.0	1

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 and the page will take approximately 10 seconds to load. 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.

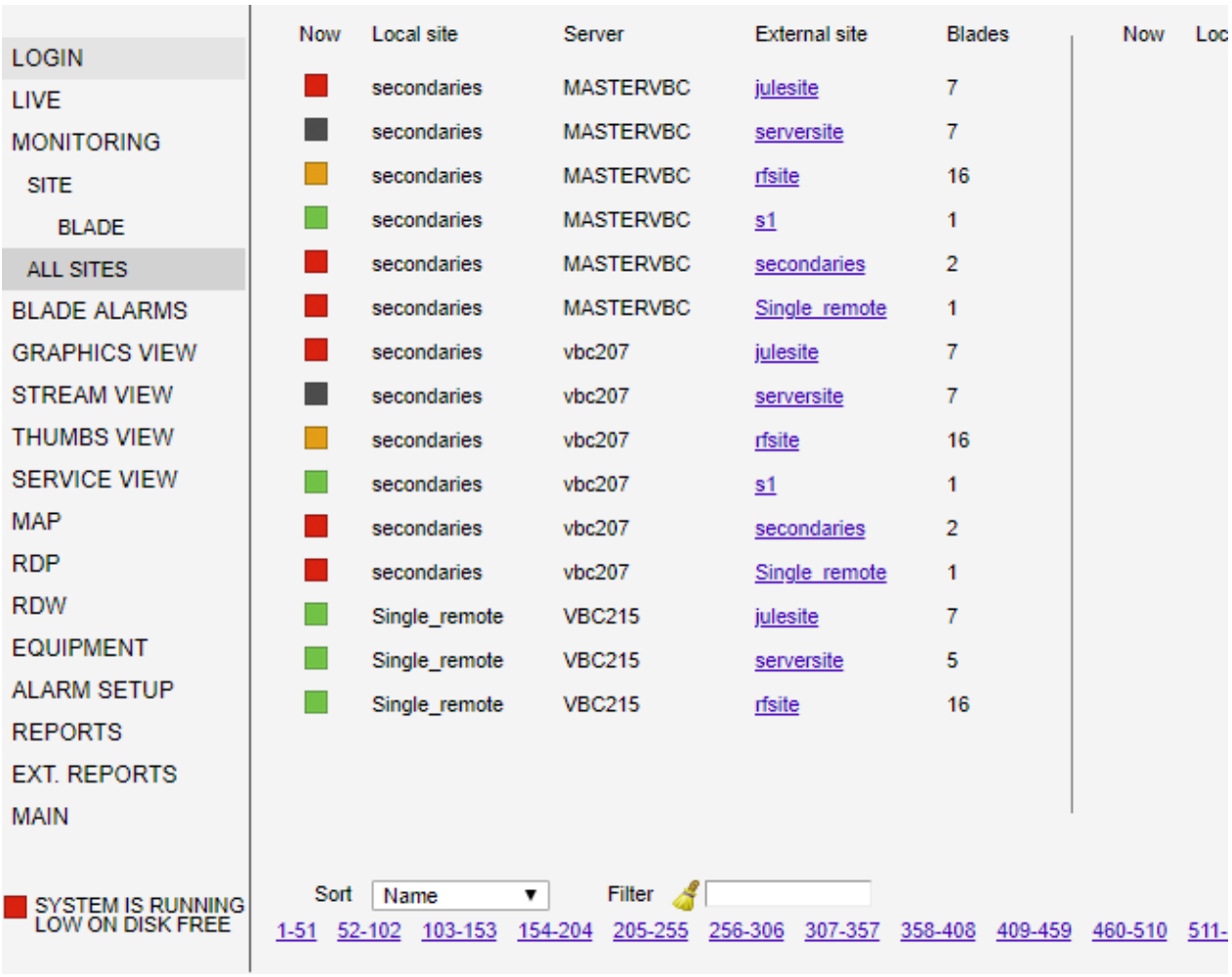
When accessing a probe through the VBC, the probe's built-in access control feature is disabled and the VBC decides if the user is going to have full access or simply read-only access.

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.

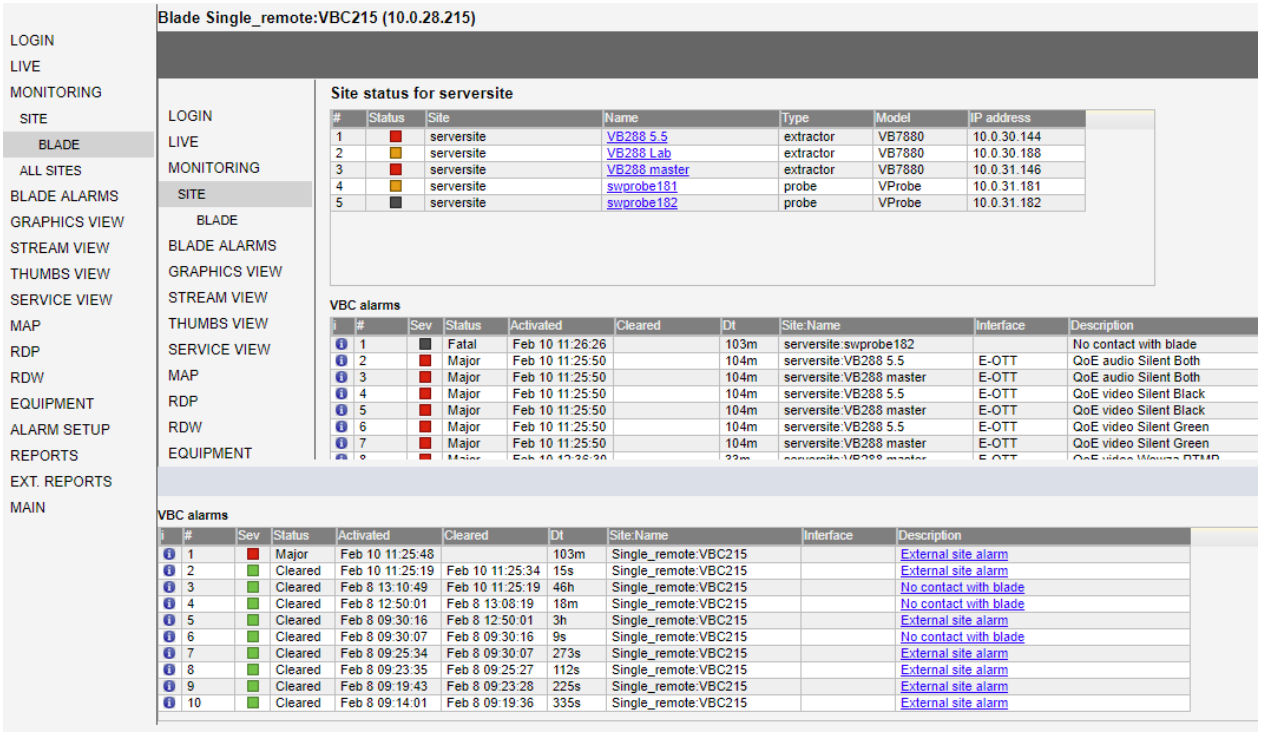
5.3.5 Monitoring — All sites

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

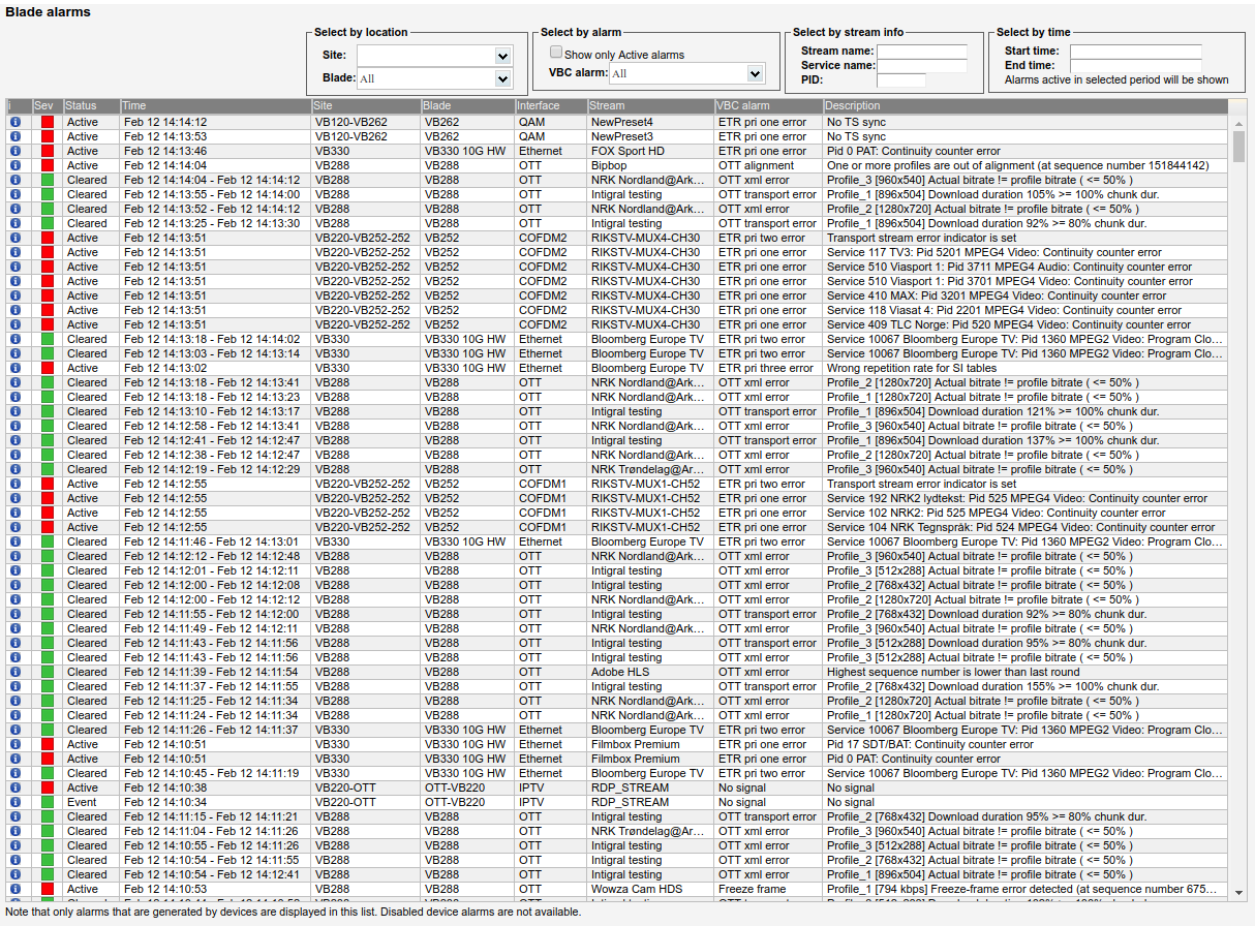


This view presents summary information for all the sites reported by Sub-VBCs registered in the **Equipment** view. The Sub-VBC is registered just like a regular blade and is given a name (shown as *Server*) and assigned to one of the Master'VBCs sites (shown as *Local site*). The name of the Sub-VBC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


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
ALARM SETUP
REPORTS
EXT. REPORTS
MAIN
LOGIN
LIVE
MONITORING
SITE
BLADE
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
i # Sev Status Activated Cleared Dt 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
VBC alarms
i # Sev Status Activated Cleared Dt 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

5.4 Blade alarms



i	Sev	Status	Time	Site	Blade	Interface	Stream	VBC alarm	Description
		Active	Feb 12 14:14:12	VB120-VB262	VB262	QAM	NewPreset4	ETR pri one error	No TS sync
		Active	Feb 12 14:13:53	VB120-VB262	VB262	QAM	NewPreset3	ETR pri one error	No TS sync
		Active	Feb 12 14:13:46	VB330	VB330 10G HW	Ethernet	FOX Sport HD	ETR pri one error	Pid 0 PAT: Continuity counter error
		Active	Feb 12 14:14:04	VB288	VB288	OTT	Bipbop	OTT alignment	One or more profiles are out of alignment (at sequence number 151844142)
		Cleared	Feb 12 14:14:04 - Feb 12 14:14:12	VB288	VB288	OTT	NRK Nordland@Ark…	OTT xml error	Profile_3 [960x540] Actual bitrate != profile bitrate (<= 50%)
		Cleared	Feb 12 14:13:55 - Feb 12 14:14:00	VB288	VB288	OTT	Intigral testing	OTT transport error	Profile_1 [896x504] Download duration 105% >= 100% chunk dur.
		Cleared	Feb 12 14:13:52 - Feb 12 14:14:12	VB288	VB288	OTT	NRK Nordland@Ark…	OTT xml error	Profile_2 [1280x720] Actual bitrate != profile bitrate (<= 50%)
		Cleared	Feb 12 14:13:25 - Feb 12 14:13:30	VB288	VB288	OTT	Intigral testing	OTT transport error	Profile_1 [896x504] Download duration 92% >= 80% chunk dur.
		Active	Feb 12 14:13:51	VB220-VB252-252	VB252	COFDM2	RIKSTV-MUX4-CH30	ETR pri two error	Transport stream error indicator is set
		Active	Feb 12 14:13:51	VB220-VB252-252	VB252	COFDM2	RIKSTV-MUX4-CH30	ETR pri one error	Service 117 TV3: Pid 5201 MPEG4 Video: Continuity counter error
		Active	Feb 12 14:13:51	VB220-VB252-252	VB252	COFDM2	RIKSTV-MUX4-CH30	ETR pri one error	Service 510 Viasport 1: Pid 3711 MPEG4 Audio: Continuity counter error
		Active	Feb 12 14:13:51	VB220-VB252-252	VB252	COFDM2	RIKSTV-MUX4-CH30	ETR pri one error	Service 510 Viasport 1: Pid 3701 MPEG4 Video: Continuity counter error
		Active	Feb 12 14:13:51	VB220-VB252-252	VB252	COFDM2	RIKSTV-MUX4-CH30	ETR pri one error	Service 410 MAX: Pid 3201 MPEG4 Video: Continuity counter error
		Active	Feb 12 14:13:51	VB220-VB252-252	VB252	COFDM2	RIKSTV-MUX4-CH30	ETR pri one error	Service 118 Viasat 4: Pid 2201 MPEG4 Video: Continuity counter error
		Active	Feb 12 14:13:51	VB220-VB252-252	VB252	COFDM2	RIKSTV-MUX4-CH30	ETR pri one error	Service 409 TLC Norge: Pid 520 MPEG4 Video: Continuity counter error
		Cleared	Feb 12 14:13:18 - Feb 12 14:14:02	VB330	VB330 10G HW	Ethernet	Bloomberg Europe TV	ETR pri two error	Service 10067 Bloomberg Europe TV: Pid 1360 MPEG2 Video: Program Clo…
		Cleared	Feb 12 14:13:03 - Feb 12 14:13:14	VB330	VB330 10G HW	Ethernet	Bloomberg Europe TV	ETR pri two error	Service 10067 Bloomberg Europe TV: Pid 1360 MPEG2 Video: Program Clo…
		Active	Feb 12 14:13:02	VB330	VB330 10G HW	Ethernet	Bloomberg Europe TV	ETR pri three error	Wrong repetition rate for SI tables
		Cleared	Feb 12 14:13:18 - Feb 12 14:13:41	VB288	VB288	OTT	NRK Nordland@Ark…	OTT xml error	Profile_2 [1280x720] Actual bitrate != profile bitrate (<= 50%)
		Cleared	Feb 12 14:13:18 - Feb 12 14:13:23	VB288	VB288	OTT	NRK Nordland@Ark…	OTT xml error	Profile_1 [1280x720] Actual bitrate != profile bitrate (<= 50%)
		Cleared	Feb 12 14:13:10 - Feb 12 14:13:17	VB288	VB288	OTT	Intigral testing	OTT transport error	Profile_1 [896x504] Download duration 121% >= 100% chunk dur.
		Cleared	Feb 12 14:12:58 - Feb 12 14:13:41	VB288	VB288	OTT	NRK Nordland@Ark…	OTT xml error	Profile_3 [960x540] Actual bitrate != profile bitrate (<= 50%)
		Cleared	Feb 12 14:12:41 - Feb 12 14:12:47	VB288	VB288	OTT	Intigral testing	OTT transport error	Profile_1 [896x504] Download duration 137% >= 100% chunk dur.
		Cleared	Feb 12 14:12:38 - Feb 12 14:12:47	VB288	VB288	OTT	NRK Nordland@Ark…	OTT xml error	Profile_2 [1280x720] Actual bitrate != profile bitrate (<= 50%)
		Cleared	Feb 12 14:12:19 - Feb 12 14:12:29	VB288	VB288	OTT	NRK Trøndelag@Ar…	OTT xml error	Profile_3 [960x540] Actual bitrate != profile bitrate (<= 50%)
		Active	Feb 12 14:12:55	VB220-VB252-252	VB252	COFDM1	RIKSTV-MUX1-CH52	ETR pri two error	Transport stream error indicator is set
		Active	Feb 12 14:12:55	VB220-VB252-252	VB252	COFDM1	RIKSTV-MUX1-CH52	ETR pri one error	Service 192 NRK2 lydtekst: Pid 525 MPEG4 Video: Continuity counter error
		Active	Feb 12 14:12:55	VB220-VB252-252	VB252	COFDM1	RIKSTV-MUX1-CH52	ETR pri one error	Service 102 NRK2: Pid 525 MPEG4 Video: Continuity counter error
		Active	Feb 12 14:12:55	VB220-VB252-252	VB252	COFDM1	RIKSTV-MUX1-CH52	ETR pri one error	Service 104 NRK Tegnspråk: Pid 524 MPEG4 Video: Continuity counter error
		Cleared	Feb 12 14:11:46 - Feb 12 14:13:01	VB330	VB330 10G HW	Ethernet	Bloomberg Europe TV	ETR pri two error	Service 10067 Bloomberg Europe TV: Pid 1360 MPEG2 Video: Program Clo…
		Cleared	Feb 12 14:12:12 - Feb 12 14:12:48	VB288	VB288	OTT	NRK Nordland@Ark…	OTT xml error	Profile_3 [960x540] Actual bitrate != profile bitrate (<= 50%)
		Cleared	Feb 12 14:12:01 - Feb 12 14:12:11	VB288	VB288	OTT	Intigral testing	OTT xml error	Profile_3 [512x288] Actual bitrate != profile bitrate (<= 50%)
		Cleared	Feb 12 14:12:00 - Feb 12 14:12:08	VB288	VB288	OTT	Intigral testing	OTT xml error	Profile_2 [768x432] Actual bitrate != profile bitrate (<= 50%)
		Cleared	Feb 12 14:12:00 - Feb 12 14:12:12	VB288	VB288	OTT	NRK Nordland@Ark…	OTT xml error	Profile_2 [1280x720] Actual bitrate != profile bitrate (<= 50%)
		Cleared	Feb 12 14:11:55 - Feb 12 14:12:00	VB288	VB288	OTT	Intigral testing	OTT transport error	Profile_2 [768x432] Download duration 92% >= 80% chunk dur.
		Cleared	Feb 12 14:11:49 - Feb 12 14:12:11	VB288	VB288	OTT	NRK Nordland@Ark…	OTT xml error	Profile_3 [960x540] Actual bitrate != profile bitrate (<= 50%)
		Cleared	Feb 12 14:11:43 - Feb 12 14:11:56	VB288	VB288	OTT	Intigral testing	OTT transport error	Profile_3 [512x288] Download duration 95% >= 80% chunk dur.
		Cleared	Feb 12 14:11:43 - Feb 12 14:11:56	VB288	VB288	OTT	Intigral testing	OTT xml error	Profile_3 [512x288] Actual bitrate != profile bitrate (<= 50%)
		Cleared	Feb 12 14:11:39 - Feb 12 14:11:54	VB288	VB288	OTT	Adobe HLS	OTT xml error	Highest sequence number is lower than last round
		Cleared	Feb 12 14:11:37 - Feb 12 14:11:55	VB288	VB288	OTT	Intigral testing	OTT transport error	Profile_2 [768x432] Download duration 155% >= 100% chunk dur.
		Cleared	Feb 12 14:11:25 - Feb 12 14:11:34	VB288	VB288	OTT	NRK Nordland@Ark…	OTT xml error	Profile_2 [1280x720] Actual bitrate != profile bitrate (<= 50%)
		Cleared	Feb 12 14:11:24 - Feb 12 14:11:34	VB288	VB288	OTT	NRK Nordland@Ark…	OTT xml error	Profile_1 [1280x720] Actual bitrate != profile bitrate (<= 50%)
		Cleared	Feb 12 14:11:26 - Feb 12 14:11:37	VB330	VB330 10G HW	Ethernet	Bloomberg Europe TV	ETR pri two error	Service 10067 Bloomberg Europe TV: Pid 1360 MPEG2 Video: Program Clo…
		Active	Feb 12 14:10:51	VB330	VB330 10G HW	Ethernet	Filmbox Premium	ETR pri one error	Pid 17 SDT/BAT: Continuity counter error
		Active	Feb 12 14:10:51	VB330	VB330 10G HW	Ethernet	Filmbox Premium	ETR pri one error	Pid 0 PAT: Continuity counter error
		Cleared	Feb 12 14:10:45 - Feb 12 14:11:19	VB330	VB330 10G HW	Ethernet	Bloomberg Europe TV	ETR pri two error	Service 10067 Bloomberg Europe TV: Pid 1360 MPEG2 Video: Program Clo…
		Active	Feb 12 14:10:38	VB220-OTT	OTT-VB220	IPTV	RDP_STREAM	No signal	No signal
		Event	Feb 12 14:10:34	VB220-OTT	OTT-VB220	IPTV	RDP_STREAM	No signal	No signal
		Cleared	Feb 12 14:11:15 - Feb 12 14:11:21	VB288	VB288	OTT	Intigral testing	OTT transport error	Profile_2 [768x432] Download duration 95% >= 80% chunk dur.
		Cleared	Feb 12 14:11:04 - Feb 12 14:11:26	VB288	VB288	OTT	NRK Trøndelag@Ar…	OTT xml error	Profile_3 [960x540] Actual bitrate != profile bitrate (<= 50%)
		Cleared	Feb 12 14:10:55 - Feb 12 14:11:26	VB288	VB288	OTT	Intigral testing	OTT xml error	Profile_3 [512x288] Actual bitrate != profile bitrate (<= 50%)
		Cleared	Feb 12 14:10:54 - Feb 12 14:11:55	VB288	VB288	OTT	Intigral testing	OTT xml error	Profile_2 [768x432] Actual bitrate != profile bitrate (<= 50%)
		Cleared	Feb 12 14:10:54 - Feb 12 14:12:41	VB288	VB288	OTT	Intigral testing	OTT xml error	Profile_1 [896x504] Actual bitrate != profile bitrate (<= 50%)
		Active	Feb 12 14:10:53	VB288	VB288	OTT	Wowza Cam HDS	Freeze frame	Profile_1 [794 kbps] Freeze-frame error detected (at sequence number 675…

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	
ⓘ	Click the blue information icon to view a detailed alarm description
Sev	A bulb indicating the alarm severity
Status	The alarm status: *Active*, *Cleared* or *Event*
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

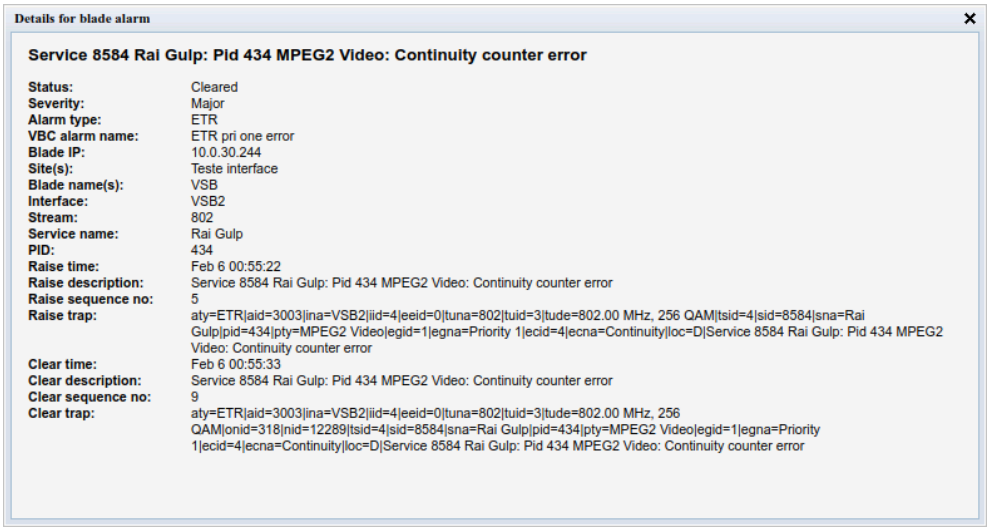
Interface	The interface receiving the stream causing the alarm
Stream	The name of the stream having the alarm
VBC alarm	The VBC alarm name
Description	The device alarm description

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:

Blade Alarms Filtering	
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.
Start time	Type a date and time (format example: Jun 21 14:31:17) + <Enter> to specify a time window defined by the **Start time** and **End time**. All alarms that were active during this time window will be displayed. Define a **Start time** only to view all blade alarms raised after the specified time plus alarms that were active at the specified time.

End time	Type a date and time (format example: Jun 21 14:31:17) + <Enter> to specify a time window defined by the **Start time** and **End time**. All alarms that were active during this time window will be displayed. Define an **End time** 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.



Blade Alarm Details	
Status	The alarm status: *Active*, *Cleared* or *Event*
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**

5.5 Graphics view (Graphics option)

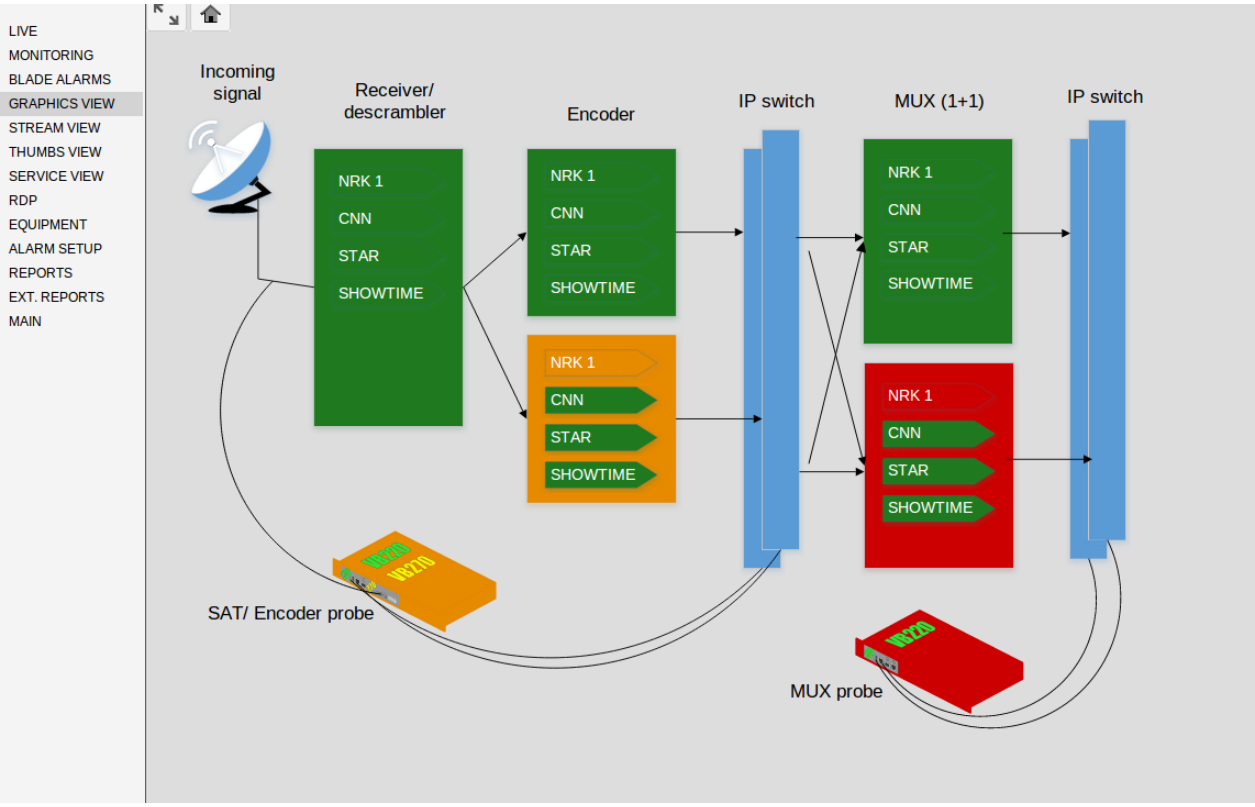


Figure: *Simulation of a network monitored by Sencore VideoBRIDGE equipment.*

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.

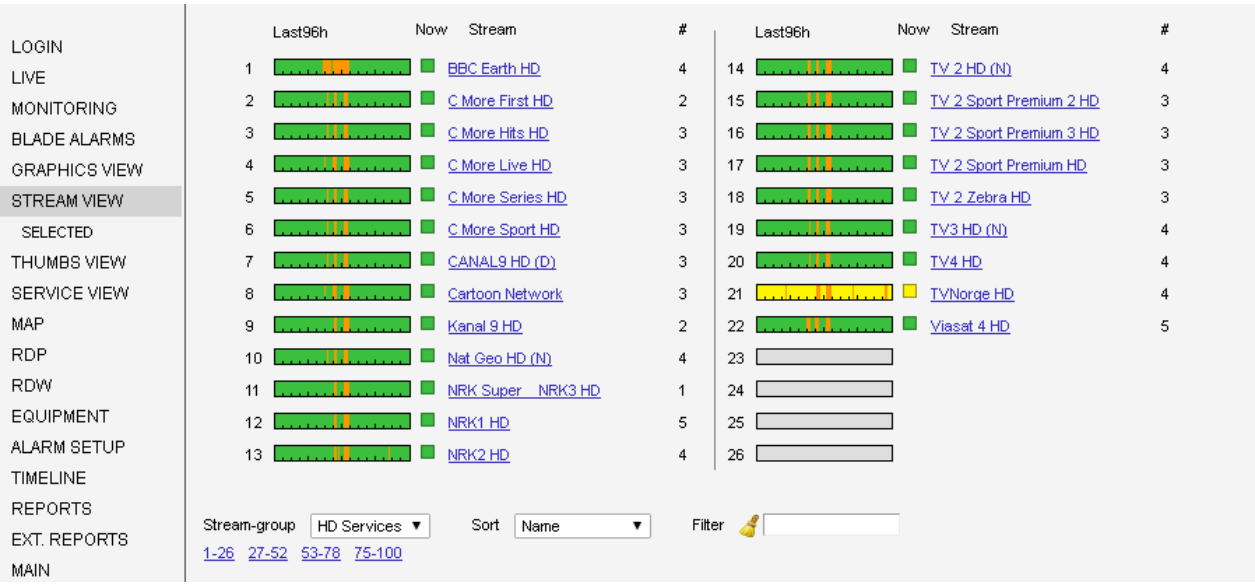
In the example diagram above the box background colors are displaying the aggregated status of the stream group, the stream arrow colors are showing status of the individual streams, and the probes are showing the corresponding status color of the probe (Blade) in the VBC.

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 5.24 for details on how to configure the Graphics view.

5.6 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.

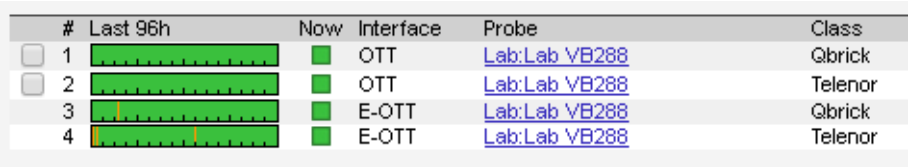
The Sort drop-down menu allows stream sorting based on name, interface or current stream status severity.

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.

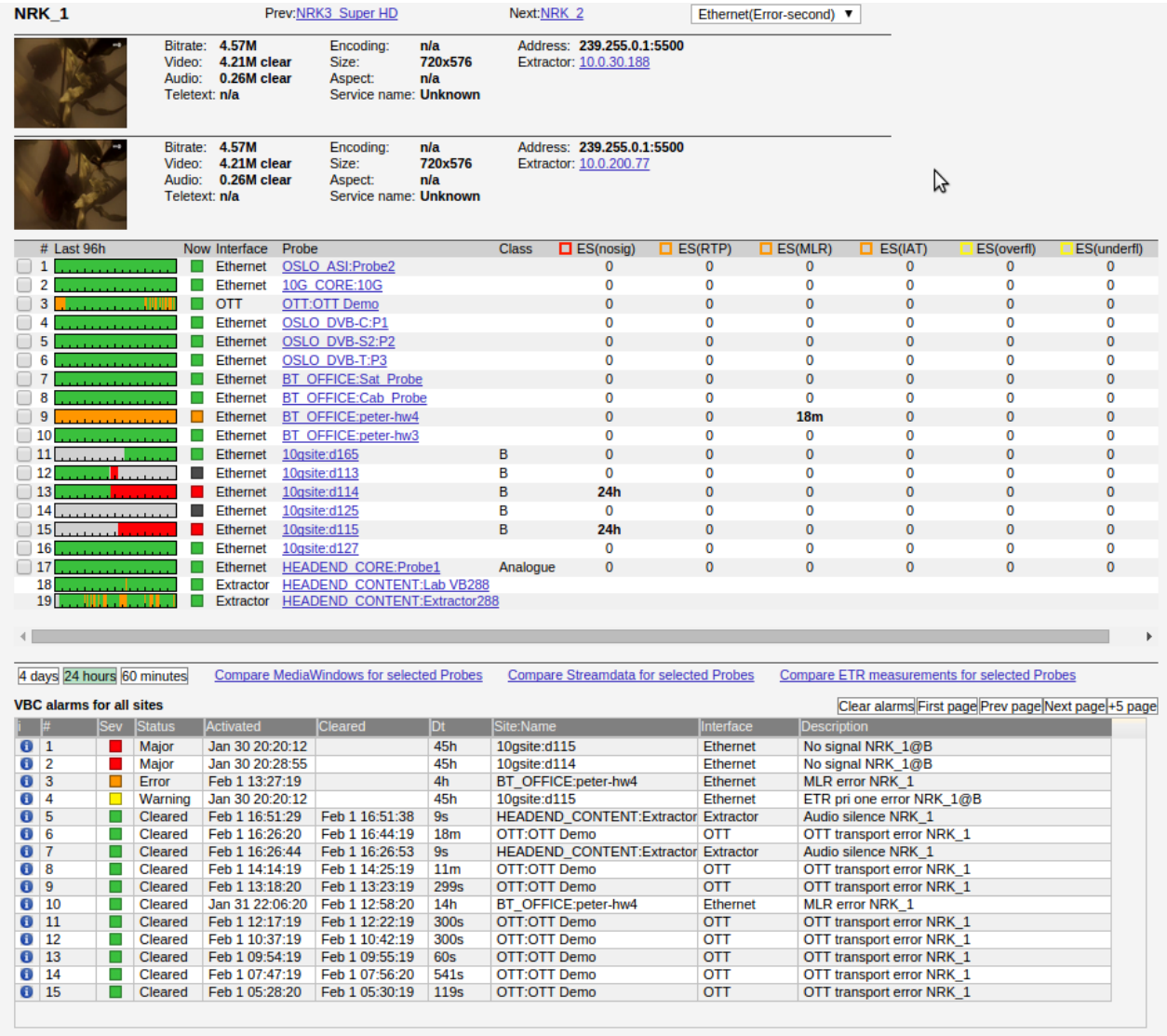
5.6.1 Stream names, class and interface



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.

5.6.2 Stream view — Selected



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 VB7880 Advanced Content Extractors 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 comparision 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.

Thumbnail meta-data

Parameter	*Description*
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
Extractor:	The IP address of the extractor 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 period[1] (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.

Parameter	*Description*

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

ES(nosig)	Number of seconds with no signal
ES(RTP)	Number of seconds with RTP packet drops. This will always be zero if the stream is not encapsulated in RTP headers.
ES(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.
ES(IAT)	Number of seconds when the delay factor exceeds the threshold.
ES(overfl)	Number of seconds when the bitrate exceeds the error-threshold.
ES(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).

Parameter	*Description*
sum(OK-polls)	Number of times that the probe has been successfully polled.
sum(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).

Parameter	*Description*
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.
cur(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.
cur(Max-bitr)	Peak bitrate during the last minute.
cur(Min-bitr)	Lowest bitrate during the last minute.

ETR

Selecting **ETR** 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.

Parameter	*Description*
DES(etrPri1)	Number of seconds with ETSI TR 101 290 priority 1 errors
DES(etrPri2)	Number of seconds with ETSI TR 101 290 priority 2 errors
DES(etrPri3)	Number of seconds with ETSI TR 101 290 priority 3 errors
DES(etrOther)	Number of seconds with ETR 290 other errors
DES(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

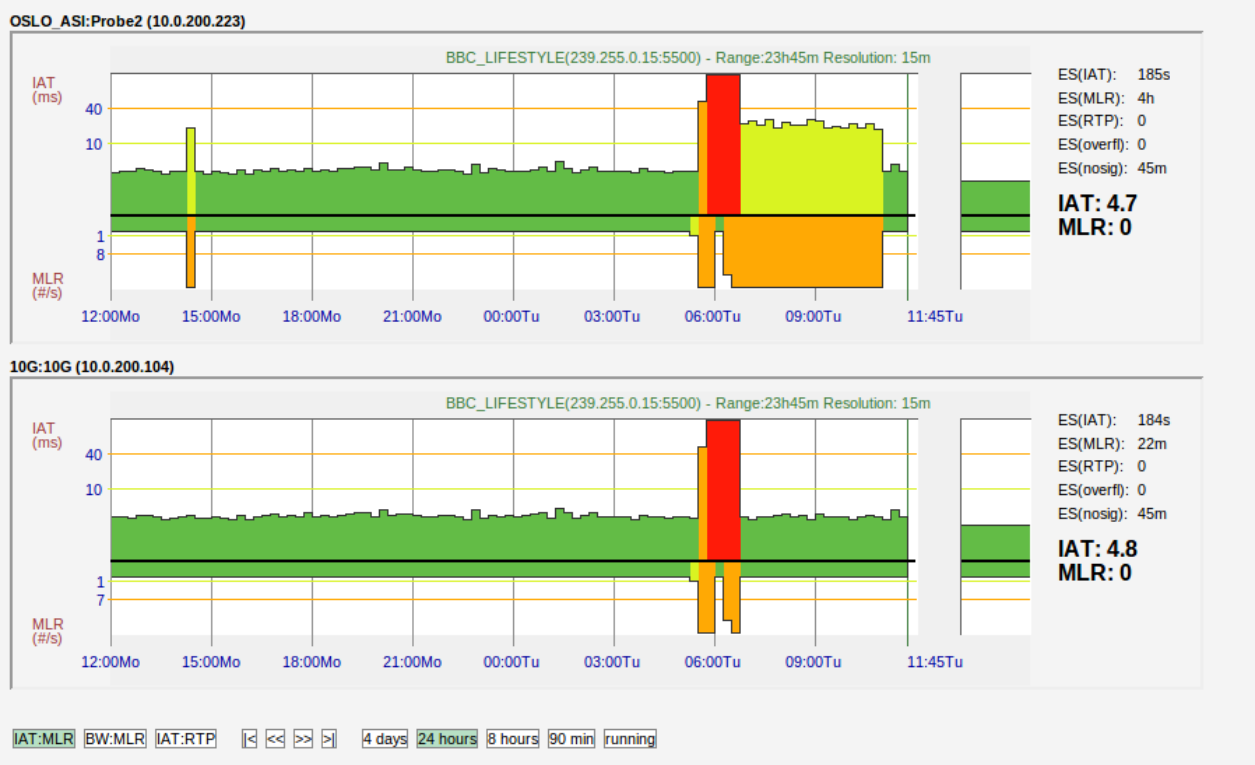
For OTT streams, selecting **OTT** in the drop-down menu gives the following parameters:

Parameter	*Description*
ES(Transport)	Number of seconds with OTT transport errors.
ES(Http)	Number of seconds with OTT HTTP errors.
ES(Xml)	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 menu and clicking the **Alarms** tab in the pop-up window.

5.6.3 Selected Stream Compare MediaWindow



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.

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

5.6.4 Selected Stream Compare ETR

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.

5.6.5 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:

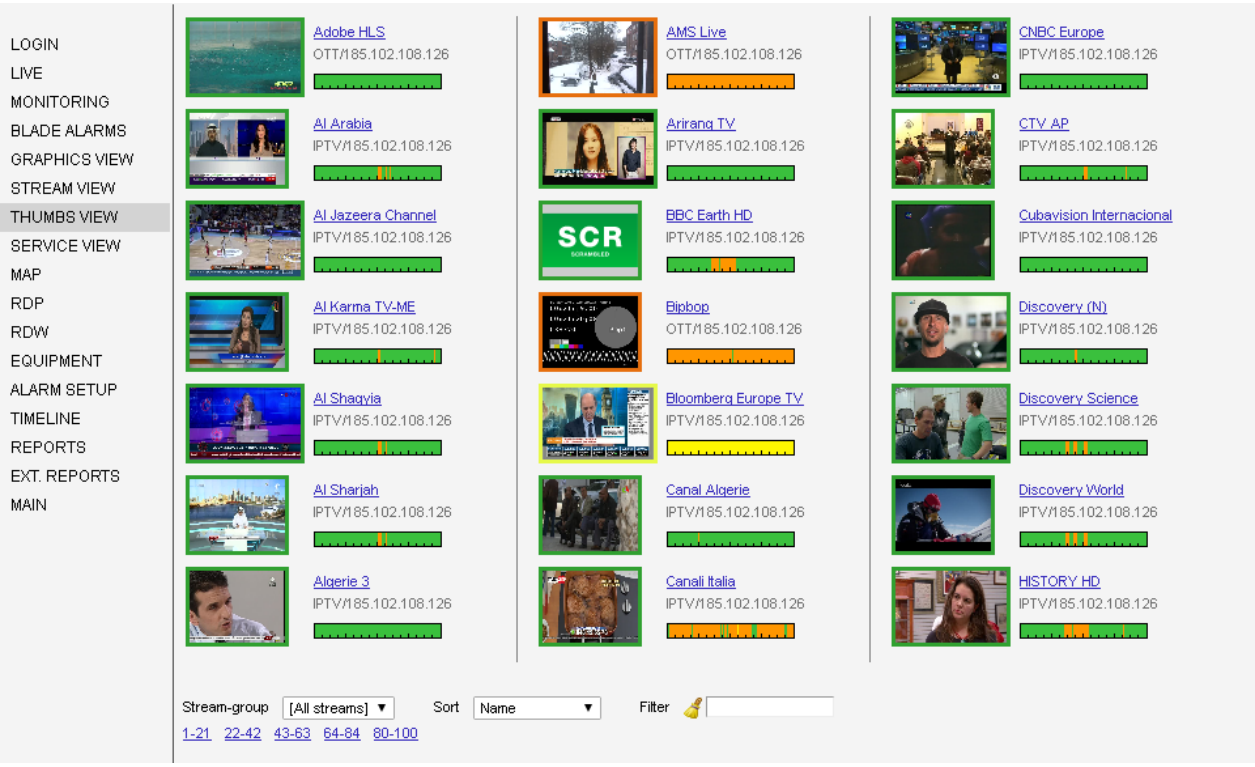
Graph type	*Available parameters*

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

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.

5.7 Thumbs view



If one or more VB7880 Advanced Content Extractors are configured as part of the VBC's setup, 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 VB7880s. 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.

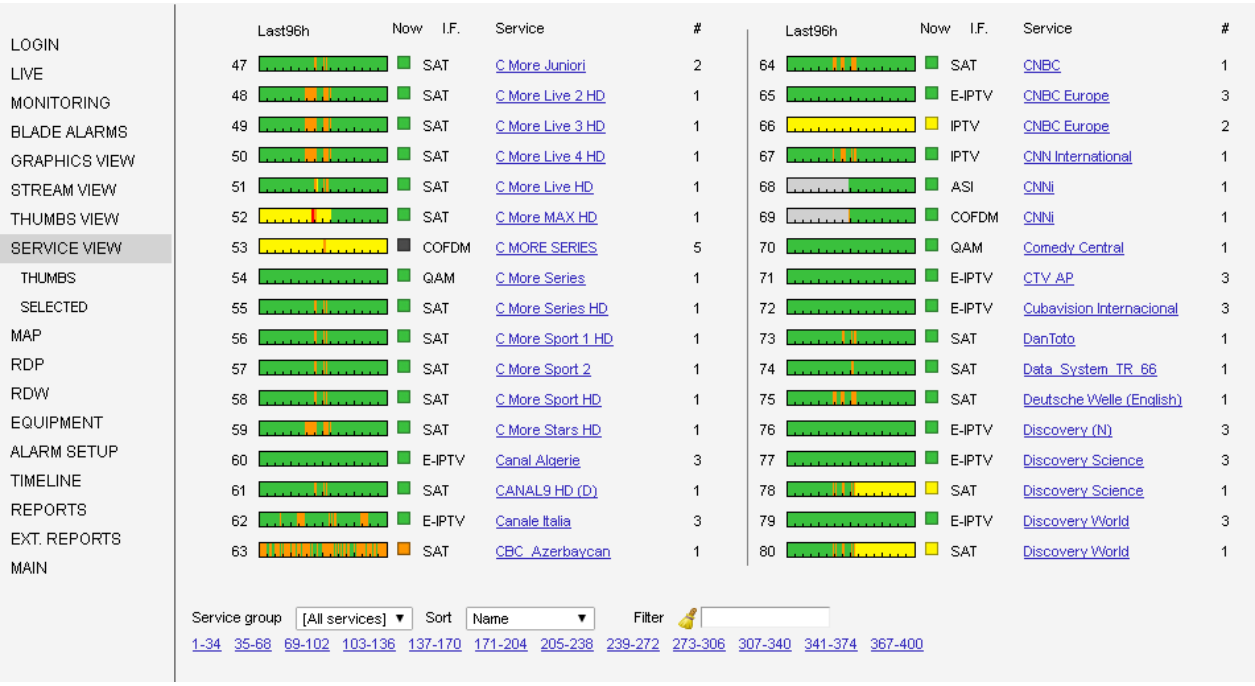
Clicking a stream name brings up the **Stream view — Selected** view.

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.

5.8 Service view (Transport Stream Service View option)



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

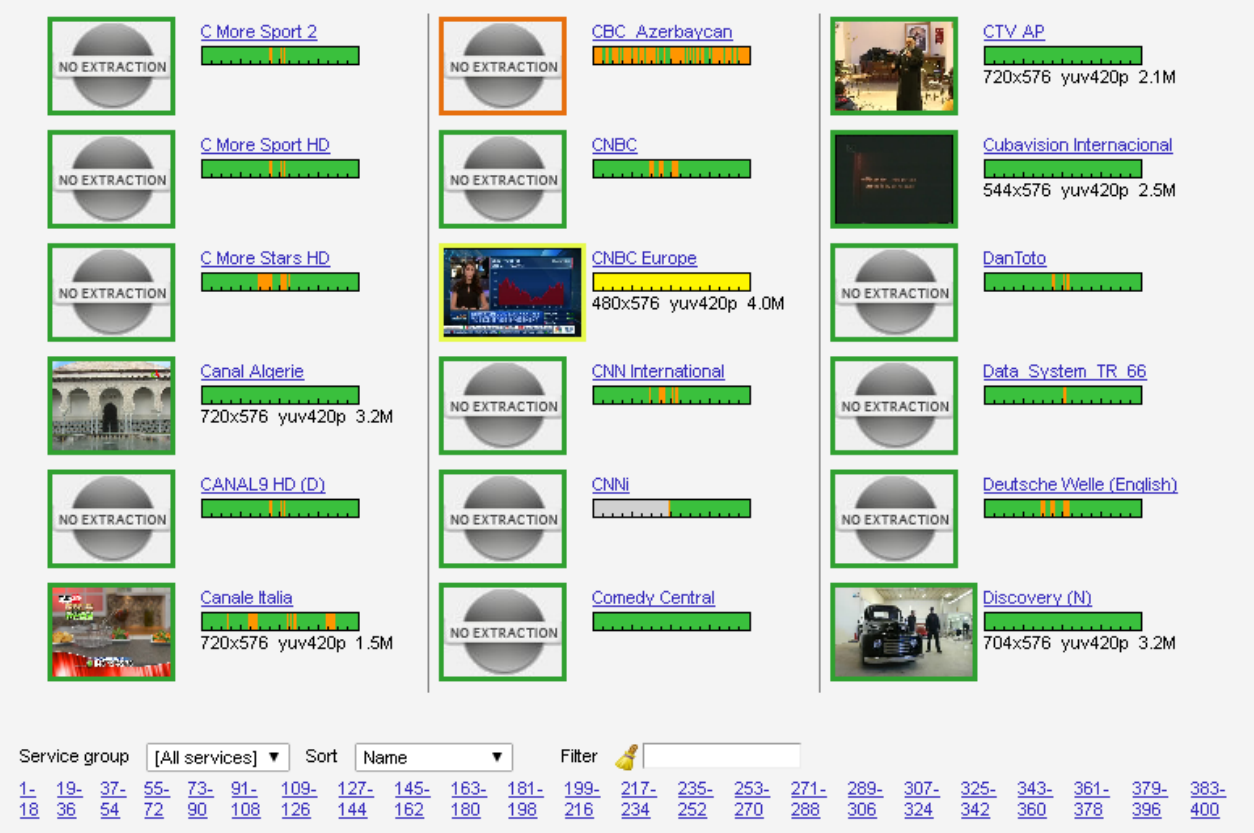
selectable service groups are available in the *Service group* drop-down menu. The service groups are configured in the **Main — Service groups** page.

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.

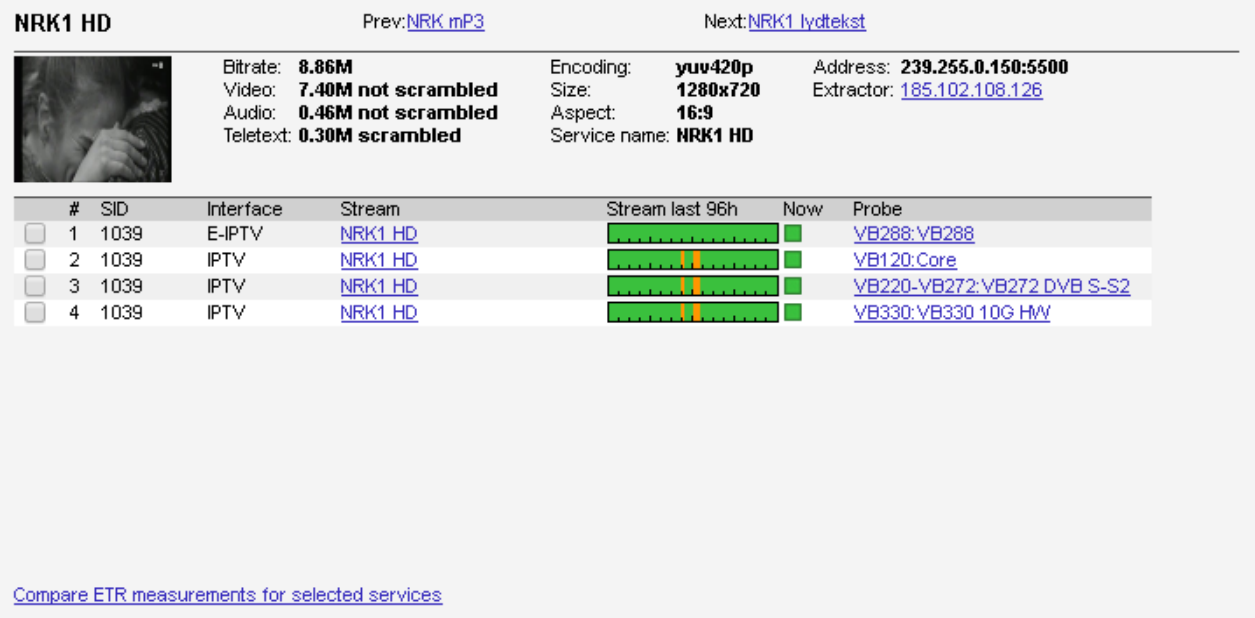
Clicking a service name brings up the **Selected Service View**, allowing further inspection of a service.

5.8.1 Service view — Thumbs



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).

5.8.2 Service view — Selected



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 VB7880 Advanced Content Extractors 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.

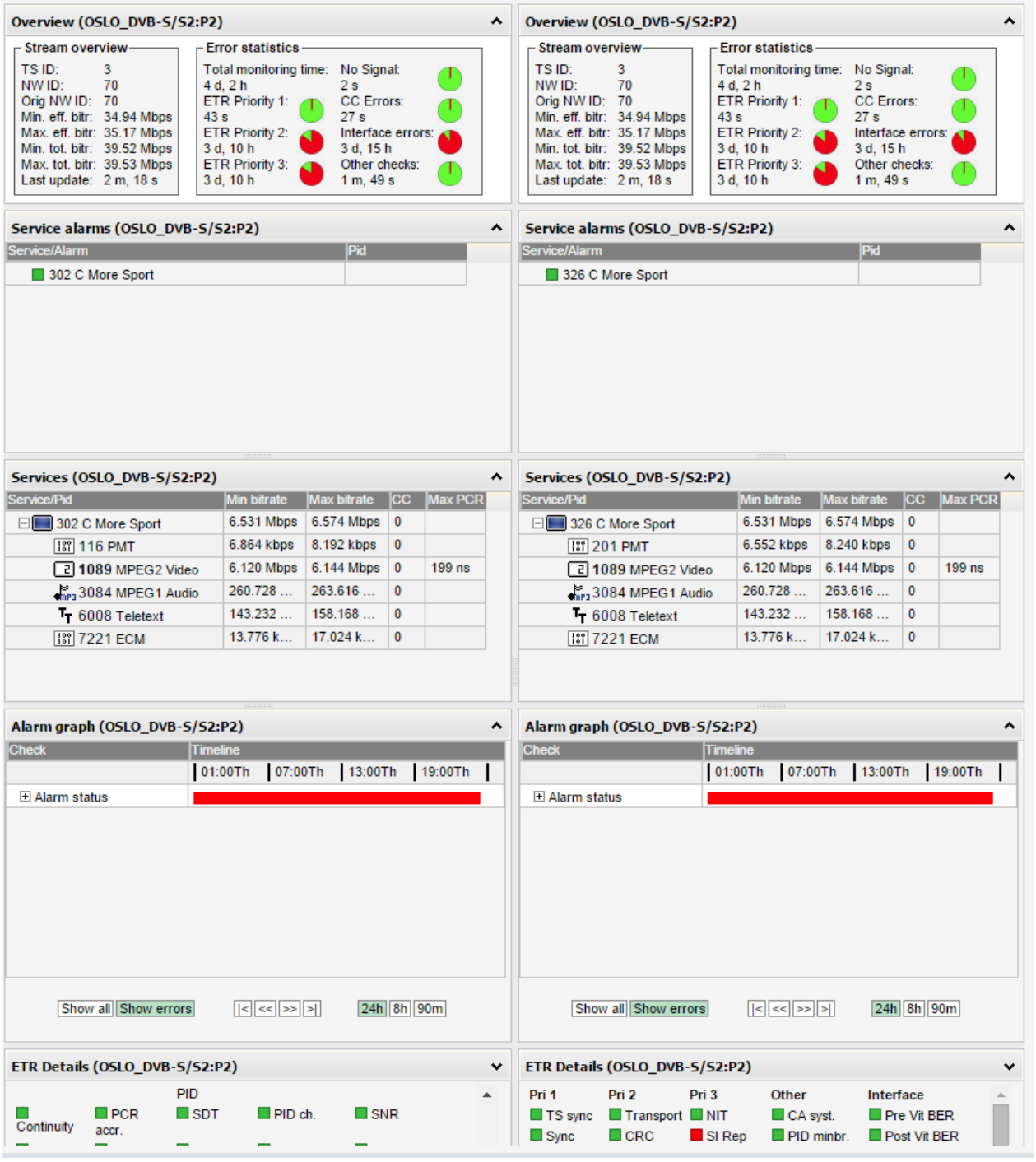
Selecting one to five locations and clicking the **Compare ETR measurements for selected services** will open the **Selected TS Service Compare ETR** view.

Thumbnail meta-data

Parameter	*Description*
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
Extractor:	The IP address of the extractor delivering thumbnail and metadata; can be clicked

Parameter	*Description*
#	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

5.8.3 Selected TS Service Compare ETR

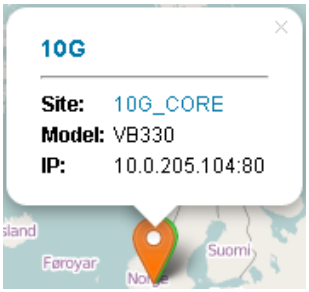


Up to five transport stream services may be compared across different probes and interfaces in the **Selected TS Service Compare ETR** view.

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

5.9 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.

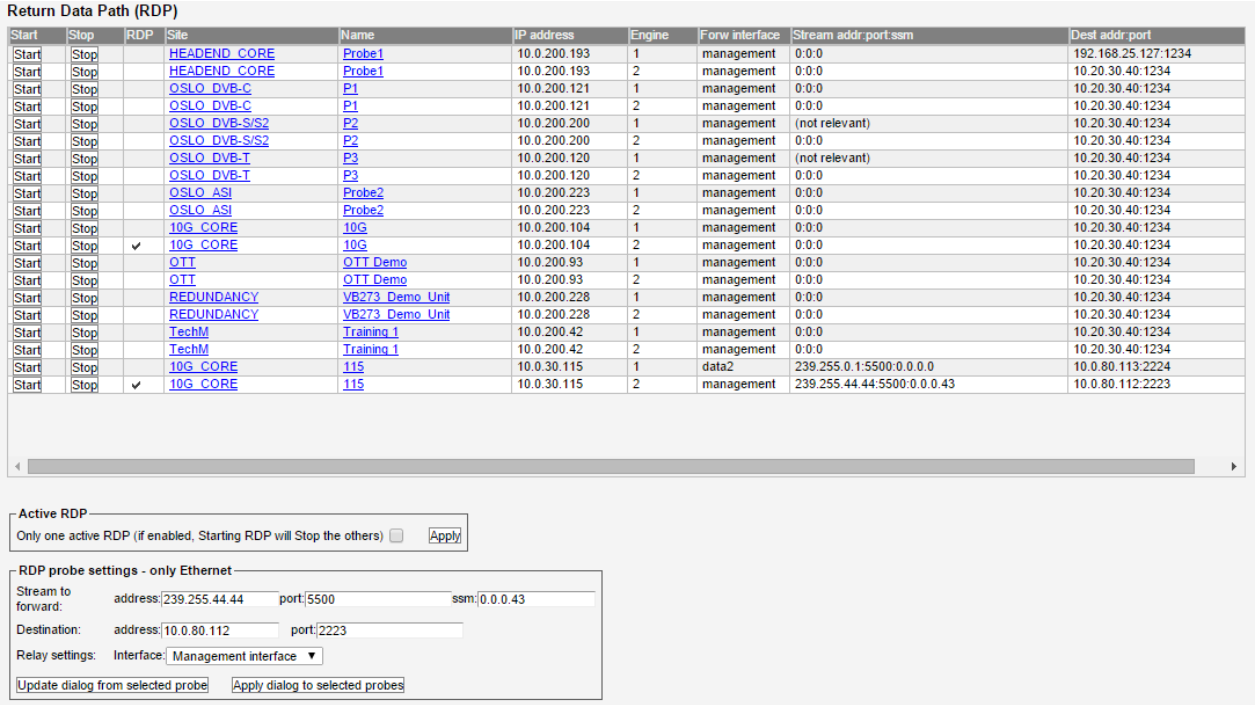


Clicking a pin will display more information about that blade, such as name, site and IP and makes it possible to access the blade details.

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.

5.10 RDP



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 *IP-address:port number:Source Specific Multicast*
Dest addr:port	The destination address that the stream should be forwarded to. The format is *destination IP address:port number (interface gateway IP address)*

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.

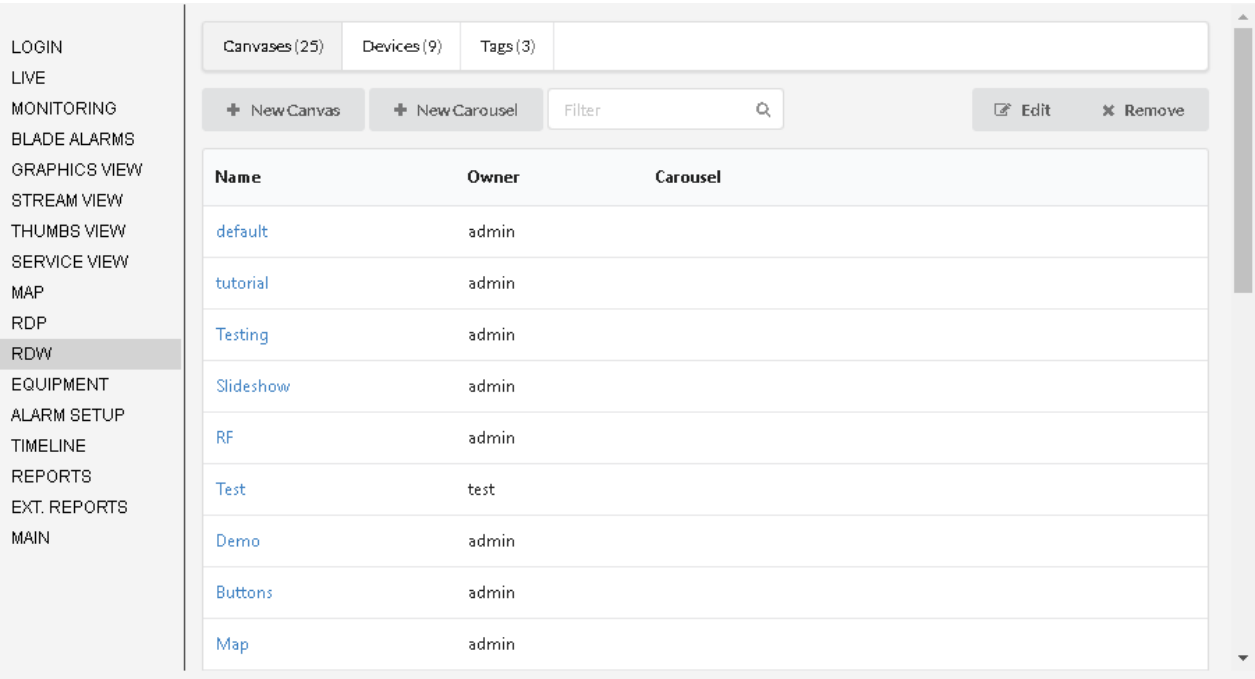
The RDP probe settings are:

RDP probe settings – only Ethernet		
	Parameter	***Description***
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: *Data interface* or *Management interface*

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.

5.11 RDW

5.11.1 RDW — Canvases



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.

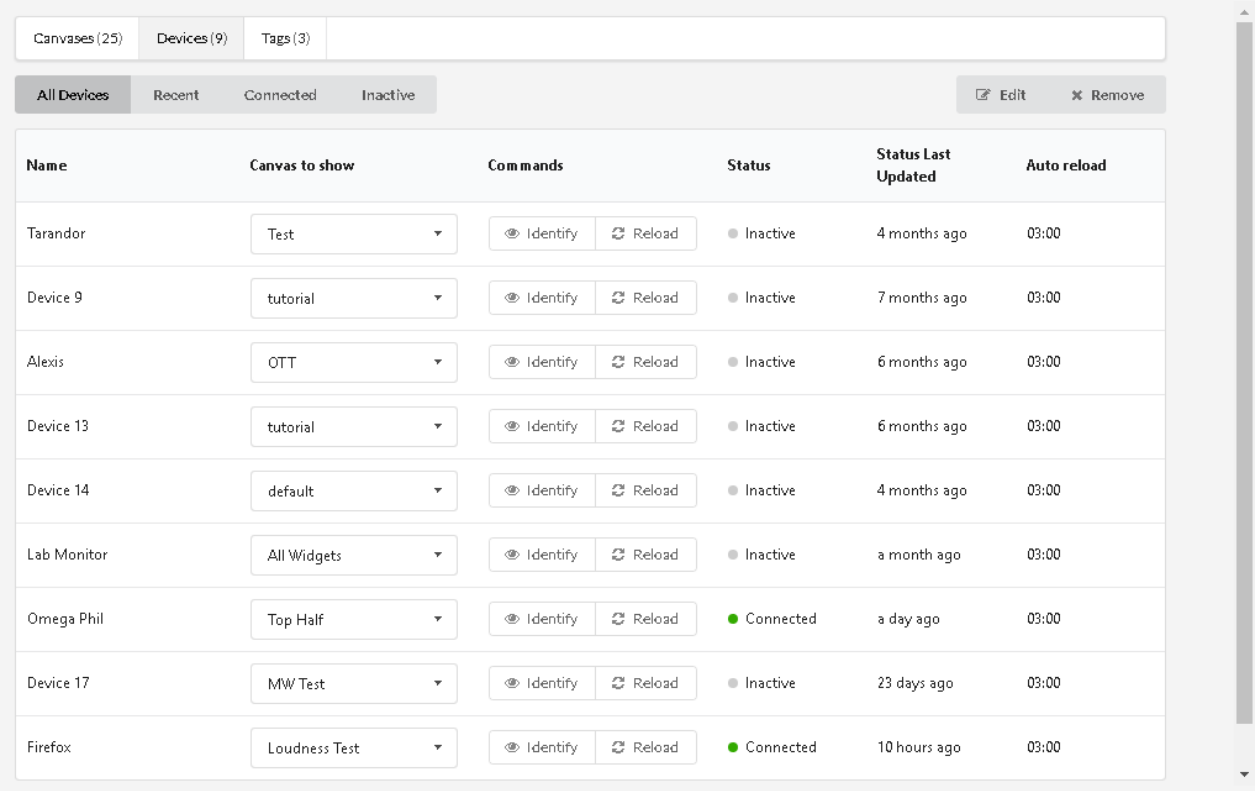
Canvases	
Name:	Name of this canvas. Clicking the name opens the canvas configurator.
Owner:	Name of the user who owns this canvas.

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.

5.11.2 RDW — Devices



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.

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.

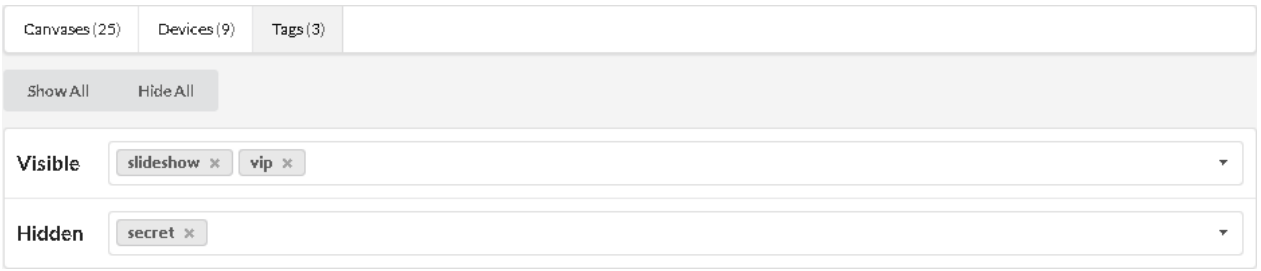
Devices	
Name:	Name of this device.
Canvas to show:	Name of the canvas to show on this device
Commands:	**Identify** displays the device name on the device. **Reload** forces the device to reload the canvas

Status:	Show the current status of the device, it can be *Connected*, *Disconnected*, or *Inactive*
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.

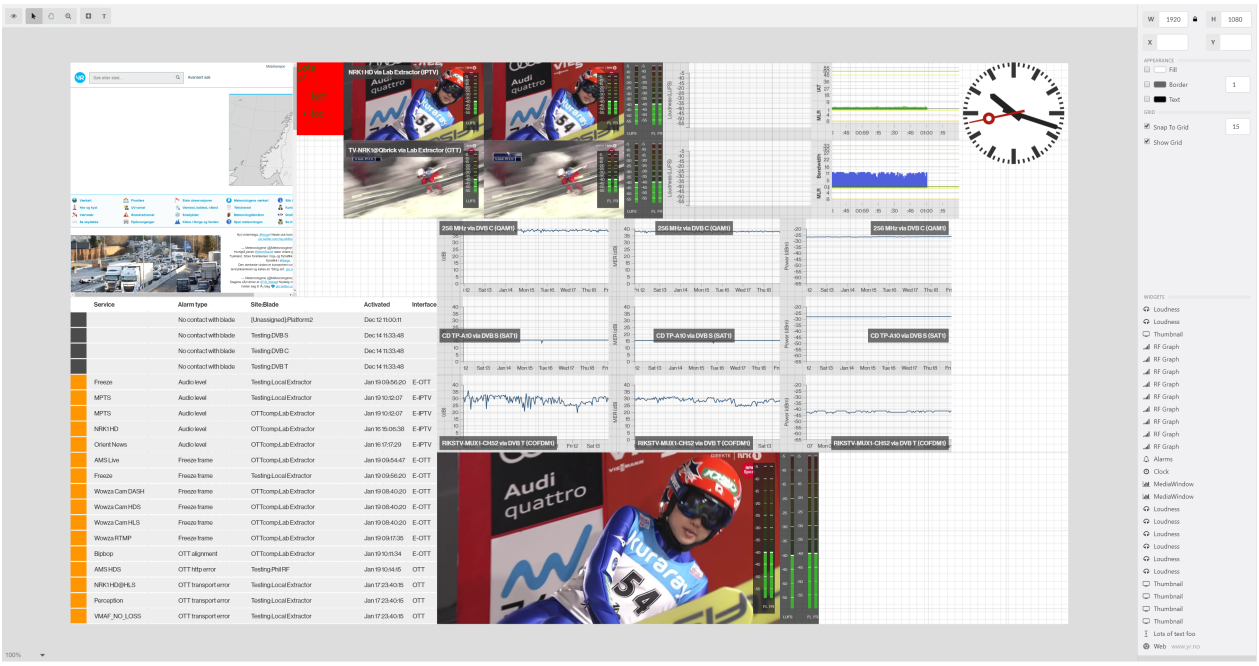
5.11.3 RDW — Tags



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.

5.11.4 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 by 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 *italic* or **Ctrl+U** to make it underlined.

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

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

5.11.5 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.

5.11.5.1 Web Widget

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

Options	
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

5.11.5.2 Textbox Widget

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

Options	
Size	Sets the font size
Alignment	Sets the text alignment; one of *Left*, *Center*, or *Right*

5.11.5.3 Thumbnail Widget

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

Options	
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. *Contain* keeps the aspect ratio of the source, filling in black bars where needed; *Cover* resizes the image to make sure the image is fully visible; *Original* displays the image in its original size
Loudness	Turns on the selected audio meter for the selected channel, if available

5.11.5.4 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.

Options	
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

5.11.5.5 Media Window Widget

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

Options	
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

5.11.5.6 Alarms Widget

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

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

5.11.5.7 RF Graph Widget

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

Options	
Channel	Select a Tuning to display RF data from
Data to display	Sets which data to display; Either *CNR*, *MER*, or *Channel Power*
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

5.11.5.8 Clock Widget

The clock widgets shows the time in the configured timezone.

Options	
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

5.11.5.9 Slide Widget

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

Options	
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.

5.11.5.10 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.

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

5.11.5.11 Graphics Widget

The graphics widgets can display diagrams from the Graphics View.

Options	
Diagram	Sets which Graphics View diagram to display

5.11.5.12 Stream View Widget

The stream view widget shows the VBC Stream View.

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

5.11.5.13 Weather Widget

The weather widget displays weather data fetched from yr.no .

Options	
Region	Sets which region to select locations from
Location	Sets the location to display weather data from
Unit	Sets the temperature unit (either Celsius or Fahrenheit)

5.11.5.14 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

5.11.5.15 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

5.11.5.16 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

5.11.5.17 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

5.11.5.18 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

5.11.5.19 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

5.11.5.20 Map Widget

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

5.11.5.21 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.

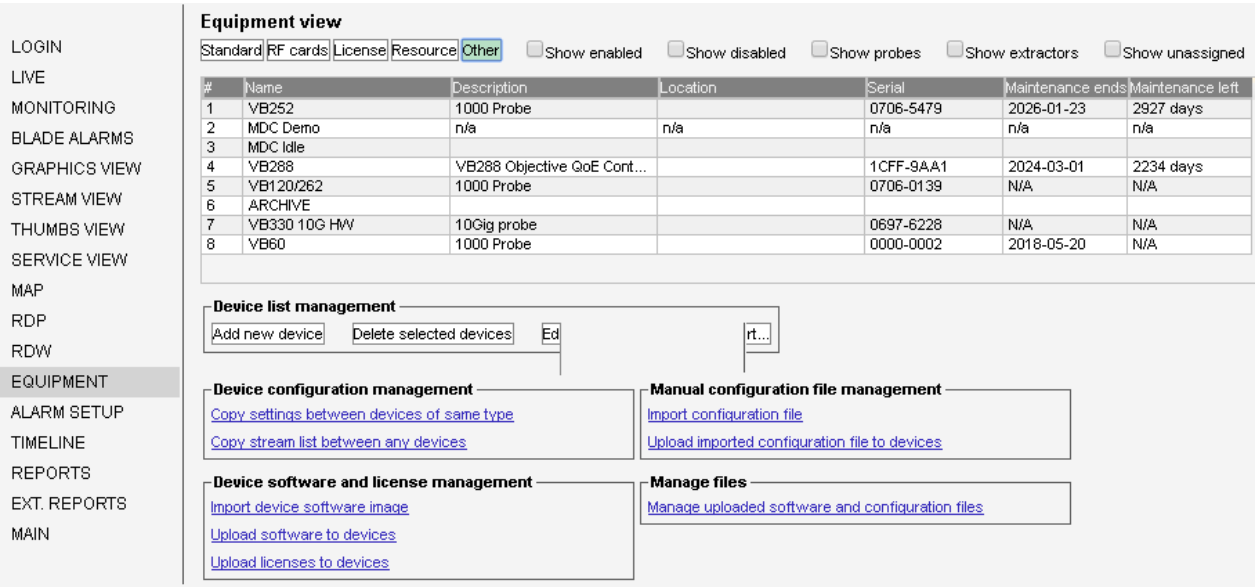
Options	
Device	Select which device this widget controls
Canvas	Select which canvases are available for selection

5.11.5.22 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

5.12 Equipment



The **Equipment** page 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 VideoBRIDGE Controller and used for monitoring the system. The different probe models and the VB7880 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:

Standard	
#	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 'VB7880')
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
	RF cards
Slot 1	The RF card present in slot one, if available
Slot 2	The RF card present in slot two, if available
	License
HW Key or System ID	The hardware key (hardware devices) or system ID (software devices); needed to generate a license for 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 the mouse pointer to display the full string.
	Resource
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)
	Other
Description	Description/Name as specified on device.
Location	Location as specified on devices
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: **Show enabled**, **Show disabled**, **Show probes**, **Show extractors** and **Show 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

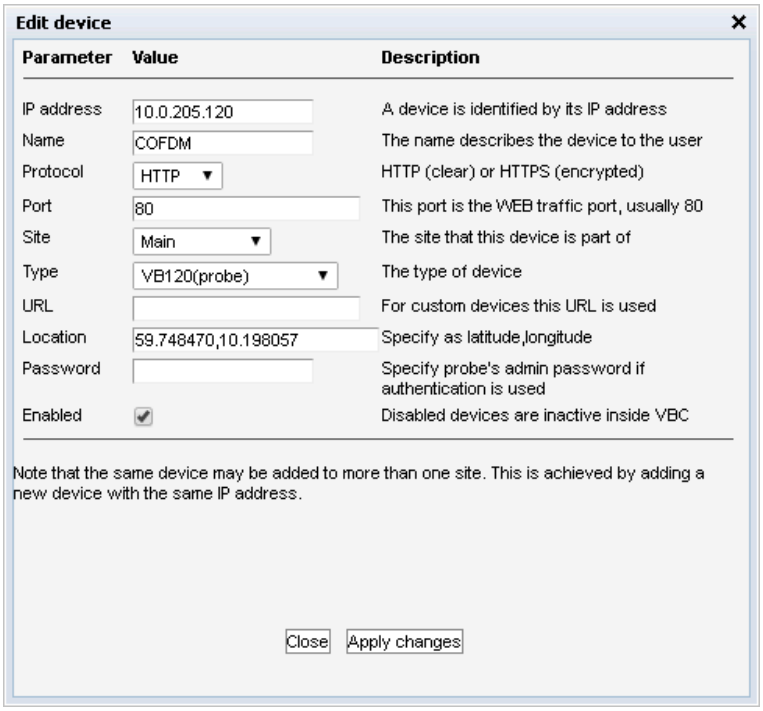
configurations and software versions the *admin* can add, edit and delete devices, as well as distribute configurations to several devices and perform batch software upgrades of probes and extractors.

5.12.1 Equipment — Device list management

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.

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



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

[2]HTTPS is supported in software version 5.3 and later

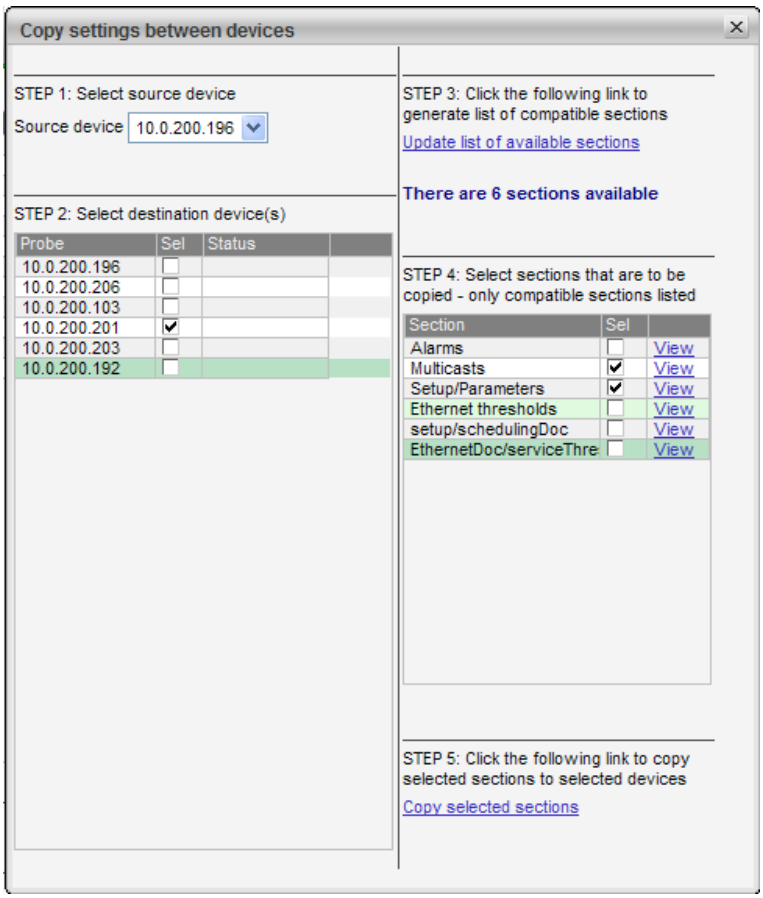
Port	Define the port to be used for the web traffic, normally 80 for HTTP and 443 for HTTPS
Site	Select the site that the device should be associated with. In some cases, it may be useful to add one device to multiple sites. This can be done in by creating several device entries with the same IP address 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

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.

5.12.2 Equipment — Device configuration management

Copy settings between devices of same type

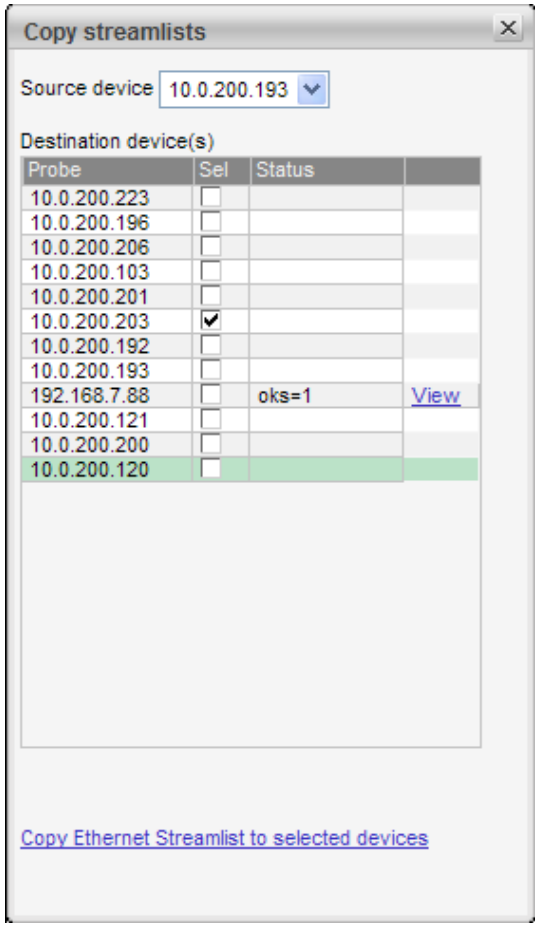


Clicking this link will open the **Copy settings between devices** pop-up view. The process of copying settings between devices involves five steps:

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.

Copy stream list between any devices



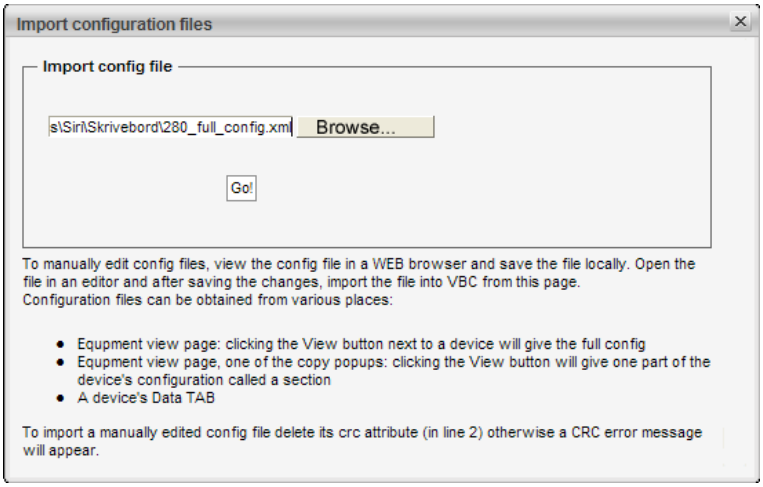
Clicking this link will open the **Copy stream lists** pop-up view.

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.

5.12.3 Equipment — Manual configuration file management

Import configuration file

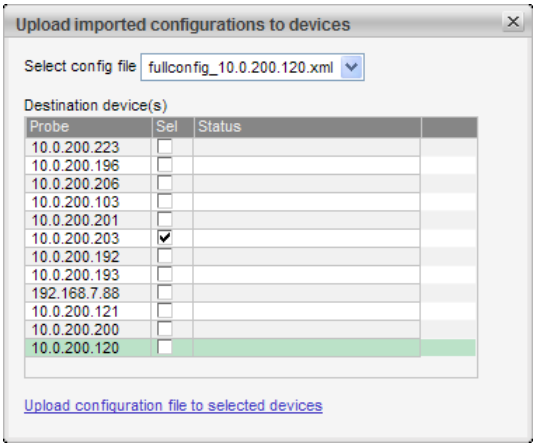


Clicking this link will open the **Import configuration file** pop-up view. The config file can either be downloaded from another probe and uploaded without change or have been manually edited as described on the next page. Select the configuration XML file to be imported and click the **Go!** button.

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.



Manually editing the configuration

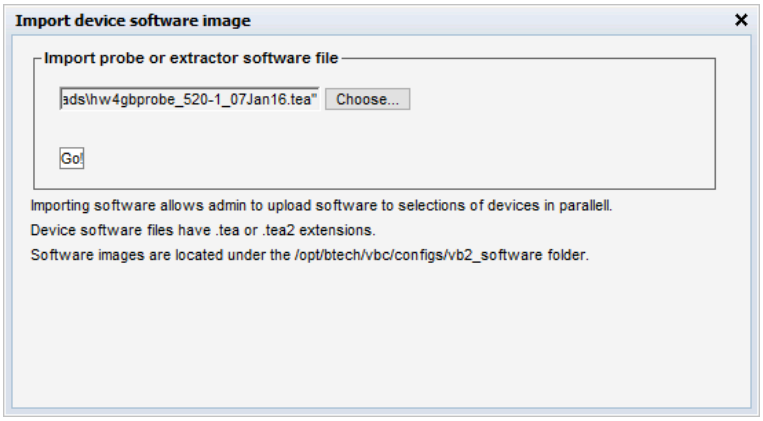
It is possible to manually edit an XML configuration file. Use a valid configuration file (by clicking a **View** link of the **Equipment view**) and save it locally. Edit the file and make appropriate changes before saving it. Any CRC attribute in line 2 of the config file must be removed (i.e. remove 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.

5.12.4 Equipment — Device software and license management

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 device software image

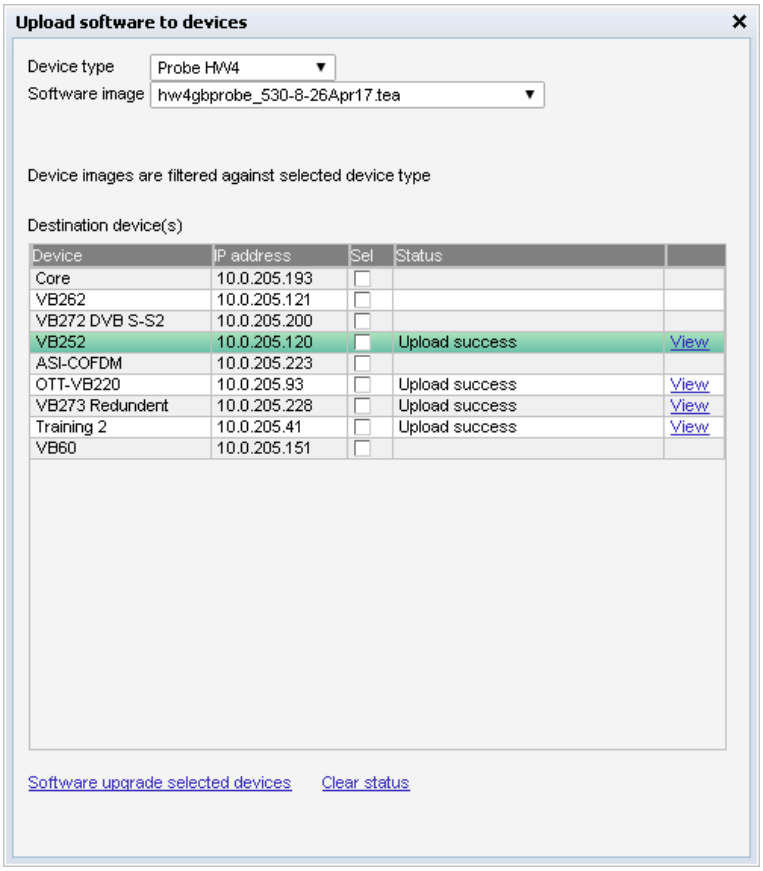


Clicking this link will open the **Import device software image** pop-up view. Select the required software file and click the **Go!** button. Software images for VB1xx, VB2xx, VB3xx, VB7880 and Software Probe can all be imported using this dialog. Software files have *.tea* or *.tea2* extensions.

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.

Upload software to devices



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 **Device list management** 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 VB7880.

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 J 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.

Upload licenses to devices

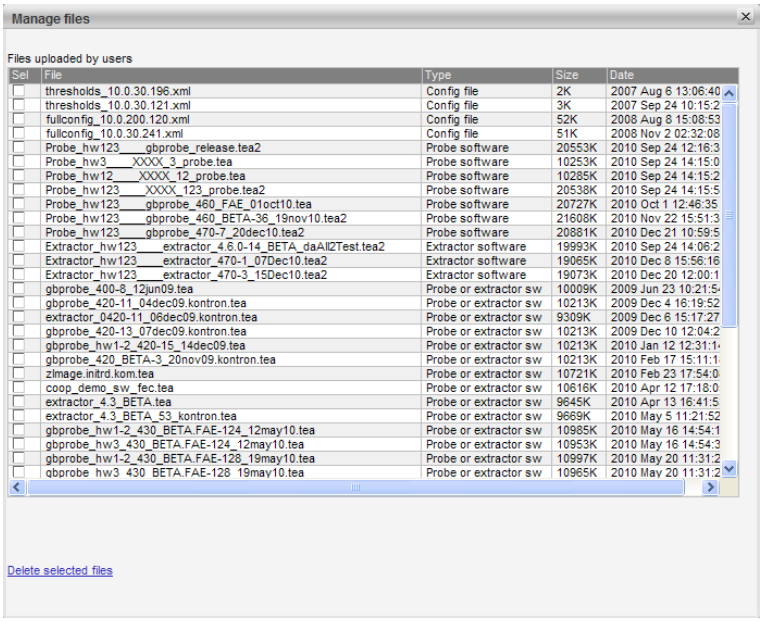
Clicking this link will open the **Upload licenses to devices** pop-up view. Software licenses can be distributed as XML files, which can be imported using this dialog, if the licensed device is known by the VBC.

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 VB7880 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.

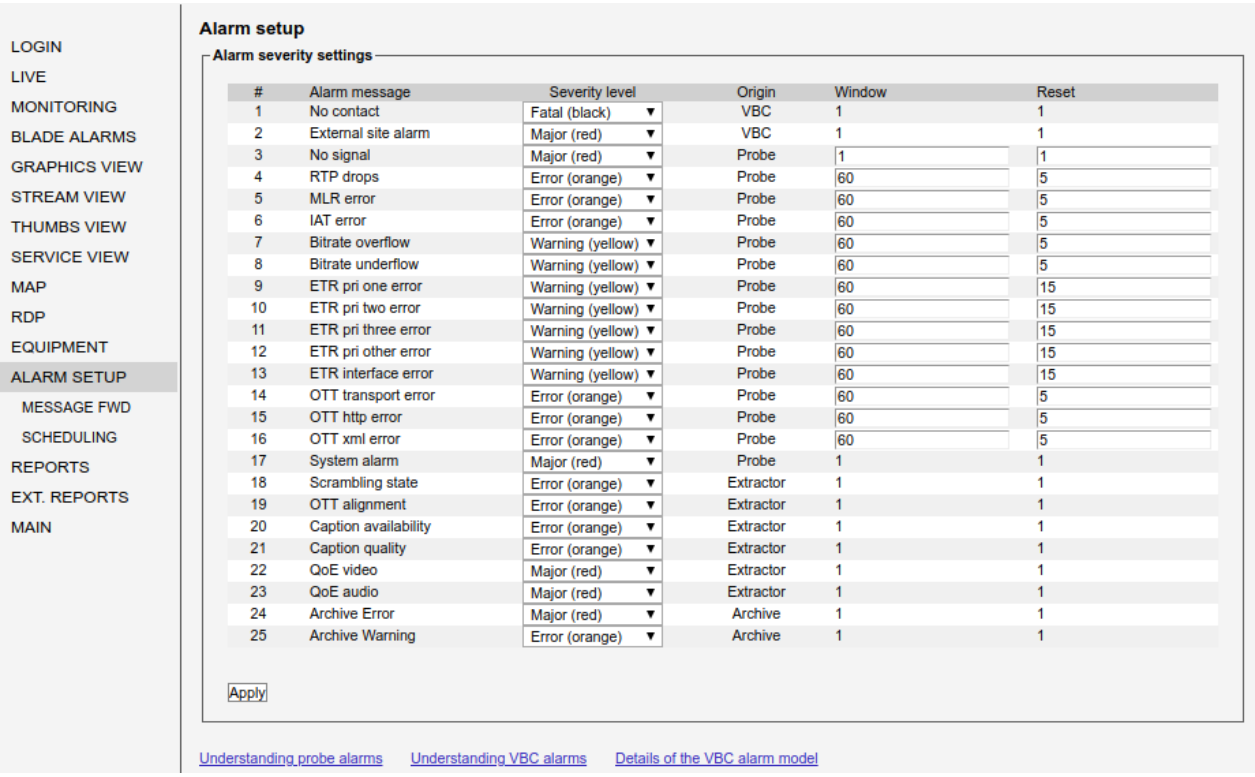
5.12.5 Equipment — Manage files

Manage uploaded software and config 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.

5.13 Alarm setup



In the **Alarm setup** menu 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 menu also allows the *admin* user to configure the alarm window and alarm reset time for each VBC alarm.

An overall system controller like the VideoBRIDGE 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 VB7880 Advanced 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.

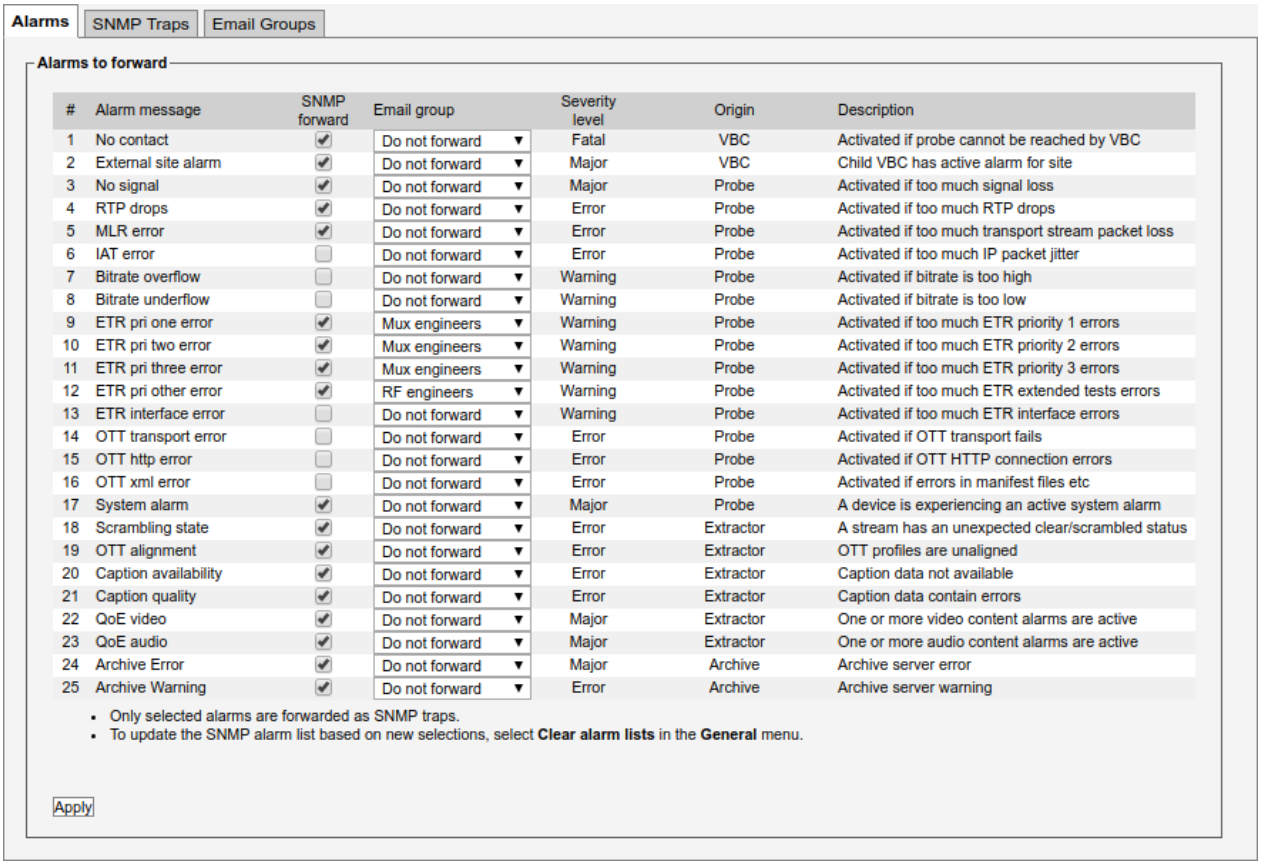
The alarm reset period is the number of consecutive minutes, without any new error seconds, needed to clear an active alarm.

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.

5.13.1 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



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

- Only selected alarms are forwarded as SNMP traps.
- To update the SNMP alarm list based on new selections, select **Clear alarm lists** in the **General** menu.

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)

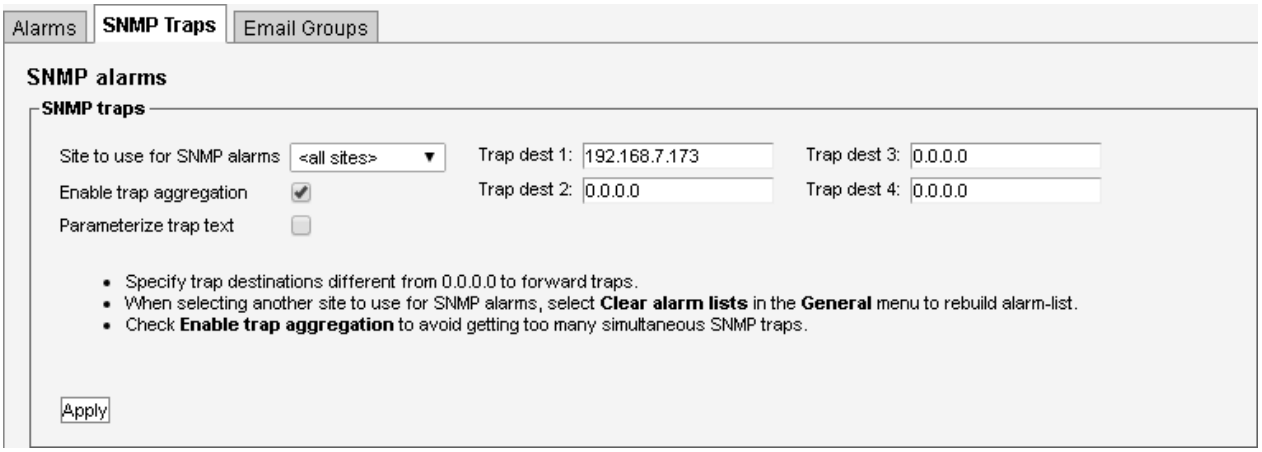
When the SNMP settings have been changed, the *admin* may want to rebuild the SNMP alarm list completely to get rid of alarms that are no longer relevant. This can be achieved by selecting *Clear* in the *Clear alarm lists* frame in the **Main — General** view.

The VBC's alarm MIB describes all the details of the trap and alarm lists formats. The MIB can be obtained from Sencore. 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 Groups** 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



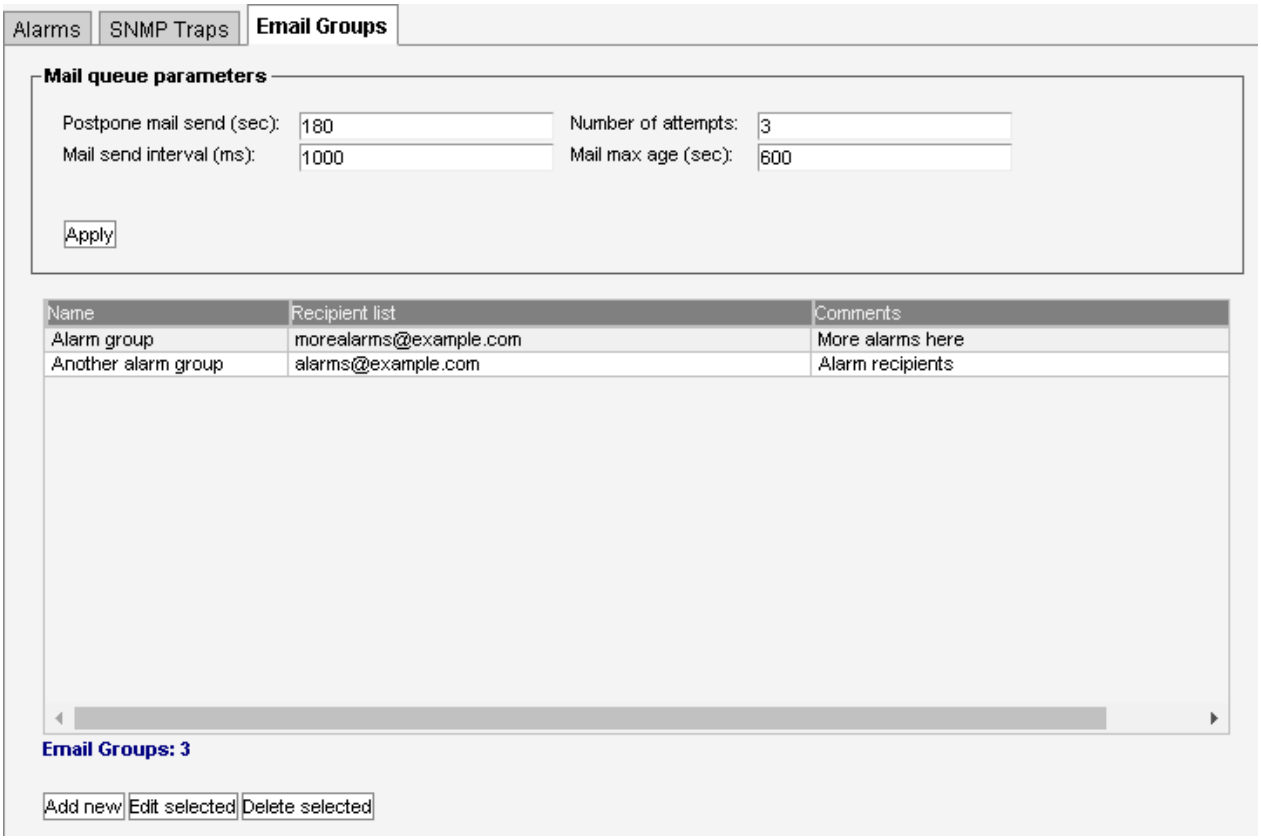
Sometimes it is desirable to switch off alarm aggregation for the SNMP traps in order to get more precise alarms. The drawback is that during alarm storms the VBC will end up sending hundred of traps instead of just a dozen.

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
Trap dest 1–4:	The IP address of the trap destination

Email Groups



The **Email Groups** page 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.

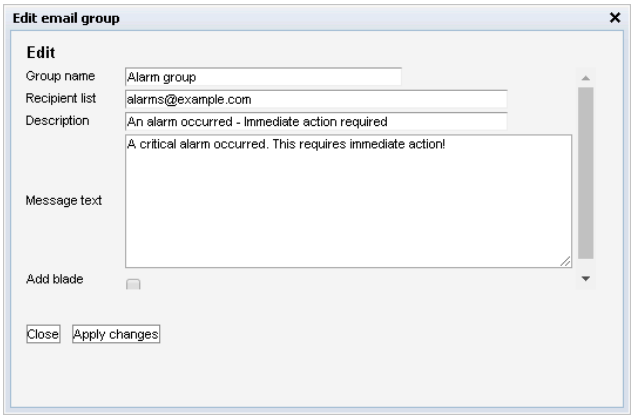
A number of global parameters can be configured:

Mail queue parameters	
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.



Email group	
Group name	This names the email group so that it can be selected in the recipient dropdown.
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.

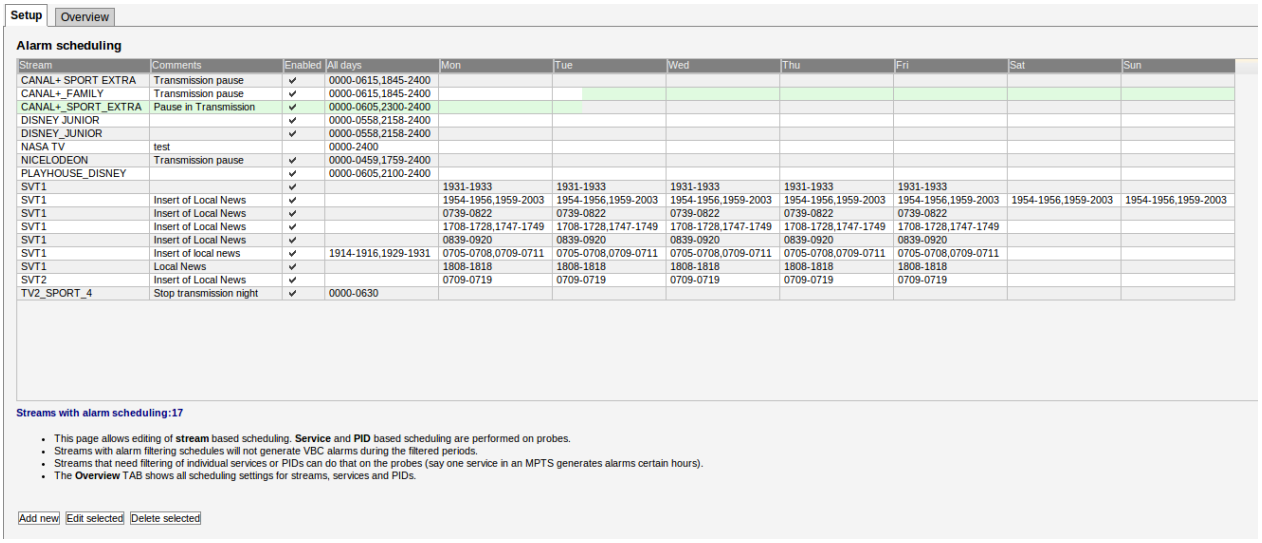
Highlighting an existing email group and clicking **Edit selected** will open the Edit email group pop-up menu described above. Make the appropriate changes and click the **Apply changes** button.

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.

5.13.2 Alarm setup — Scheduling



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

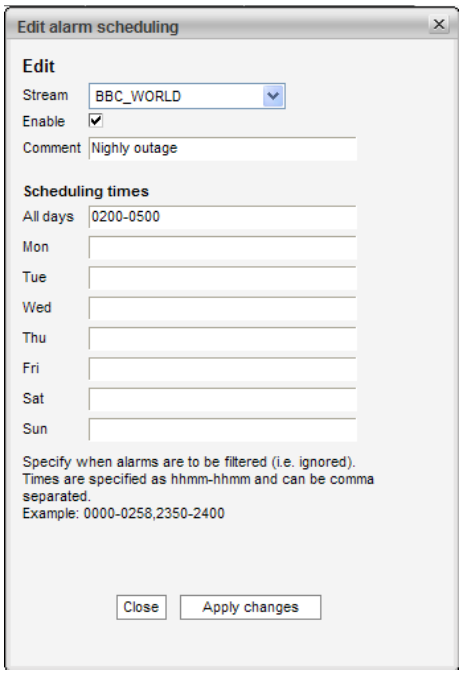
Scheduling Setup

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.

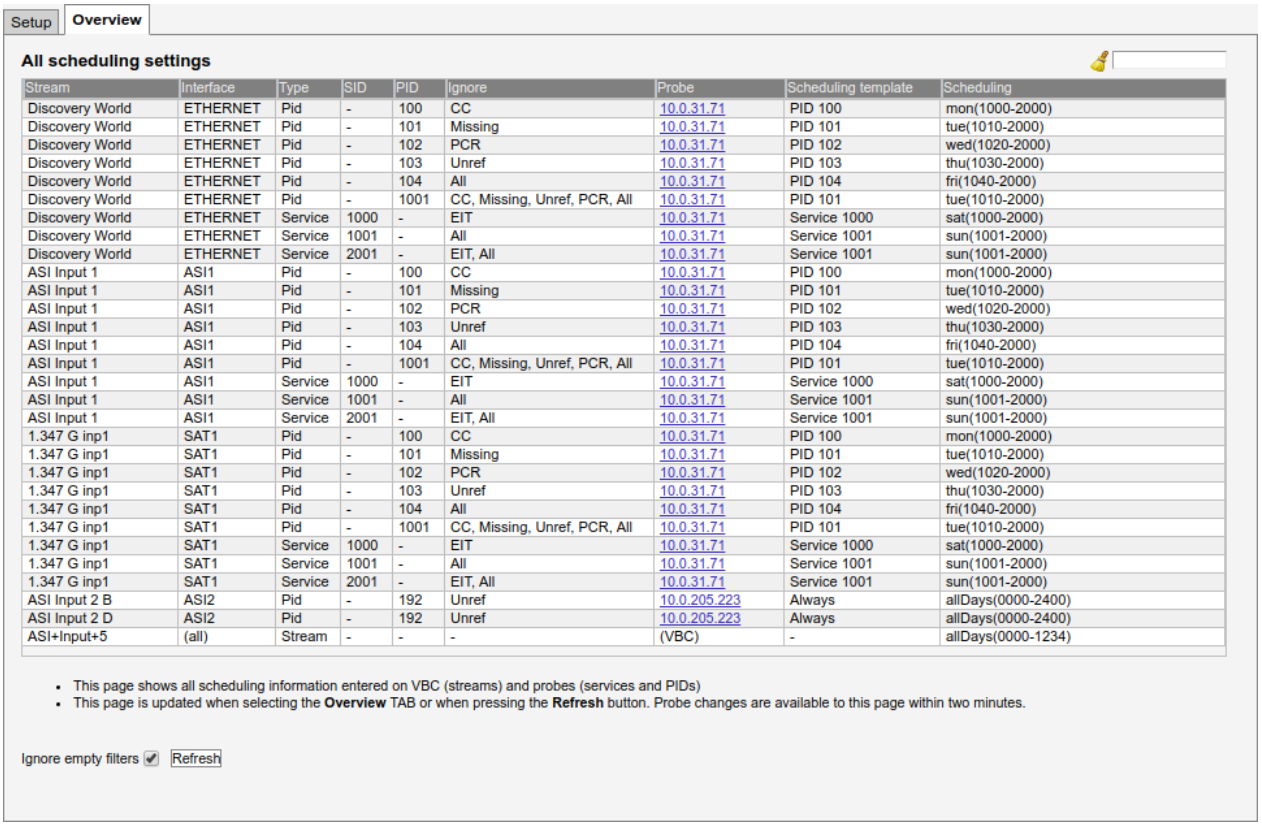


The alarm scheduling applies to the PDF reports as well with the limitation that a complete hour H is completely filtered if H:59 is filtered, otherwise not filtered at all. Hence if alarm scheduling is active at 13:59 for a stream, the report will mask all errors for that stream from 13:00 to 13:59.

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`.

Parameter	*Description*
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



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.

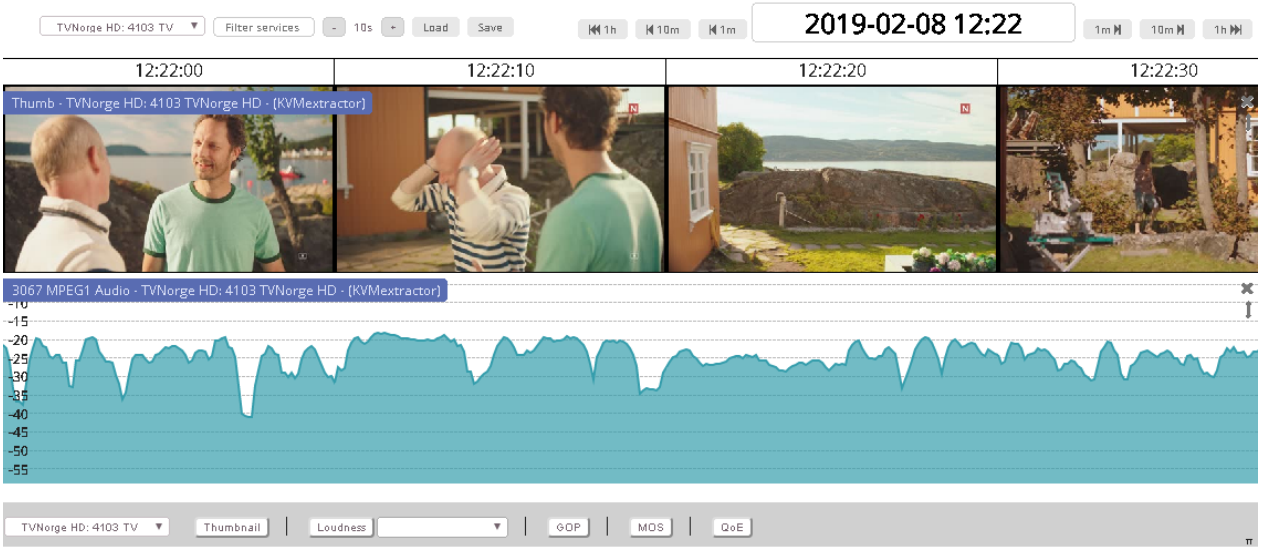
When **Ignore empty filters** is checked only entries that can mask errors at certain times are included in the list. When this checkbox is not enabled all services and PIDs that are associated with service or PID threshold templates different from *Default* will be present in the scheduling list, irrespective 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 bye 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.

Parameter	*Description*
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: *stream, service* or *PID*
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 *None*.
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 *None*.
Scheduling	The scheduling time window(s) during which alarms are masked

5.14 Timeline (requires Archive Server)



The **Timeline** view requires an Archive Server, please refer to chapter 5.23 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.

5.14.1 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.

5.14.2 Navigating in time

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

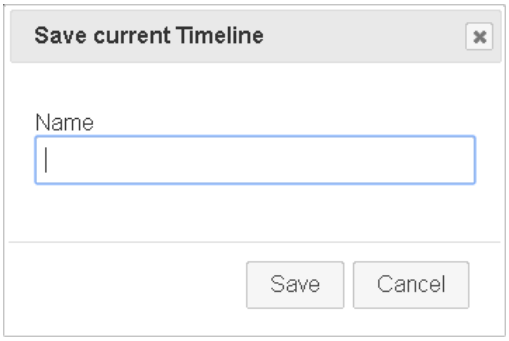
To go back and forth it time you can select the desired time from the time and date picker located at the center top. The time and date picker is most useful for large jumps in time, like if you want to look at data from days/weeks/months back in time. Just select the correct date and time, and the timeline 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.

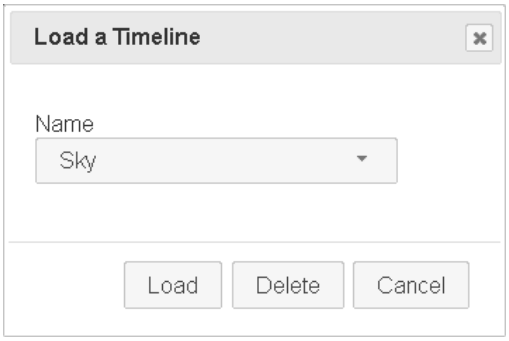
The last way to navigate in time is to drag the timeline in the direction you would want to move it. The timeline should smoothly glide with the dragging motion, and new data should pop up seamlessly.

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.

5.14.3 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.

5.15 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.

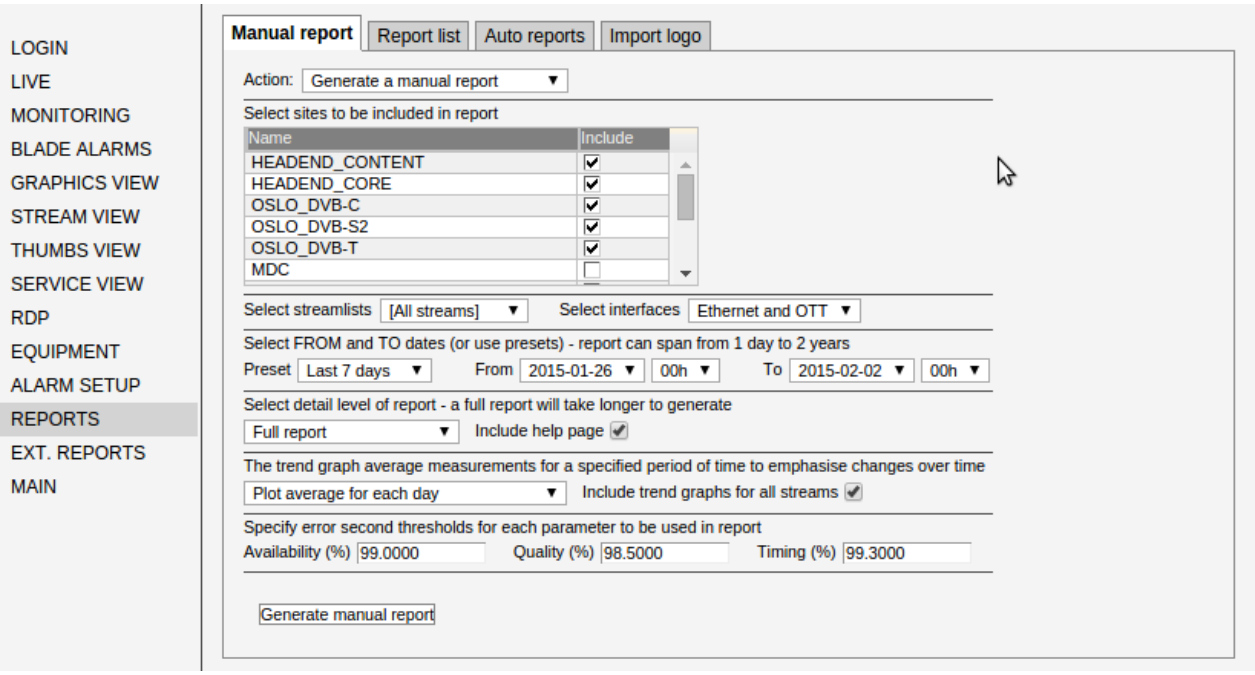
	IPTV (Ethernet) streams
Availability	Availability refers to the presence of a stream. An availability of 100% means that there have been no signal disruptions for the complete interval that a stream has been monitored. The no-signal error seconds are measured directly by probes as ES(nosig).
Quality	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.

	OTT services
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 5.5.

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 $100\% - \frac{10}{48\times60\times60} \times 100 = 99.99942\%$.

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

5.15.1 Reports — 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.

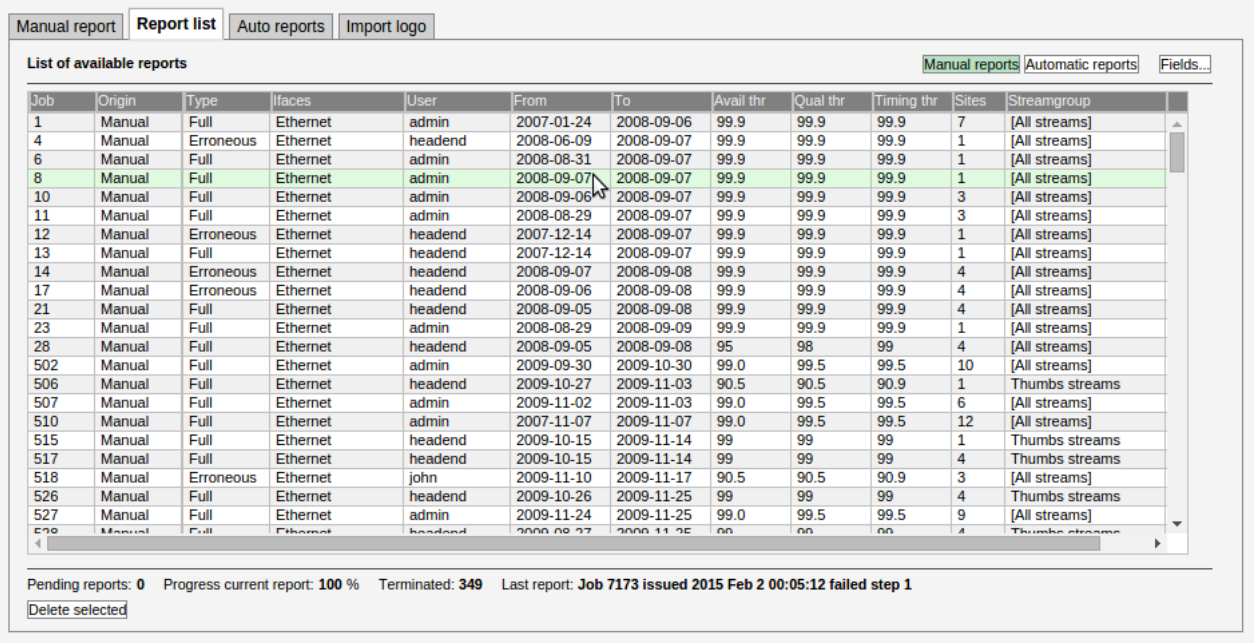
Parameter	*Description*
Site list	Only probes belonging to selected sites will contribute to the report.
Stream selection	The user may select to generate a report containing all streams in the system or only streams associated with one stream group. The stream groups are configured in the **Main — Stream 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.

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.

5.15.2 Reports — Report list

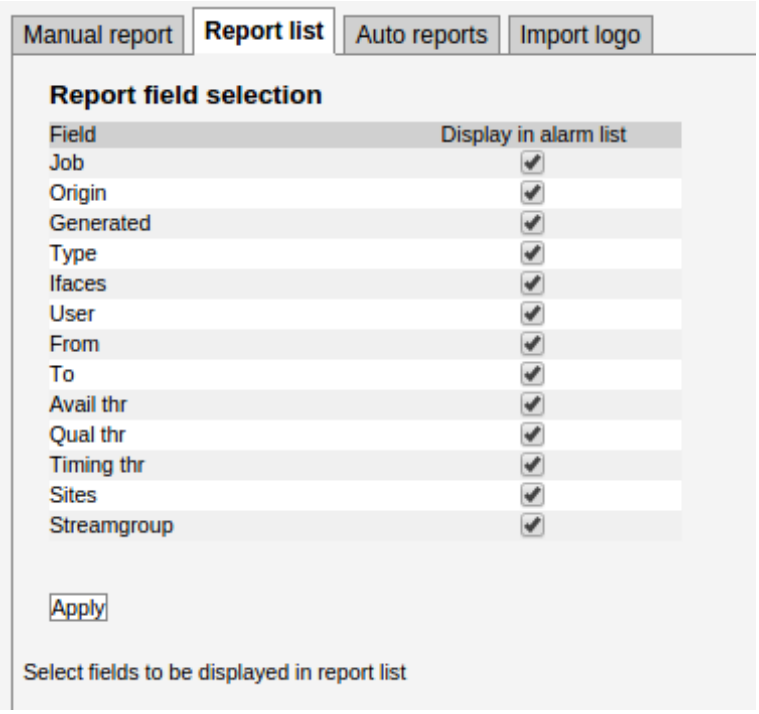


The report list menu provides a list of all reports that the logged-in user is allowed to view. The *admin* user has access to all reports while regular users can only view his own reports.

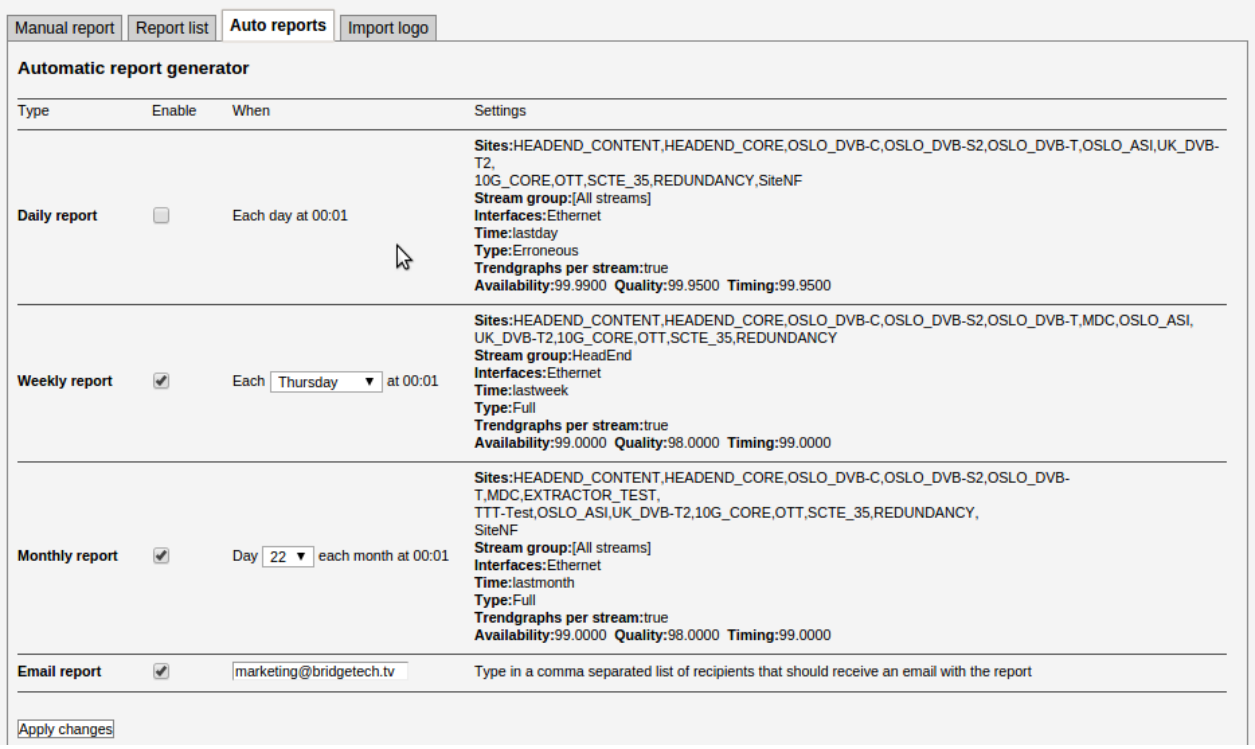
Newest reports will be presented at the bottom of the list (by default). Older reports with identical report parameters are removed when a new report is generated.

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.



5.15.3 Reports — Auto reports



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.

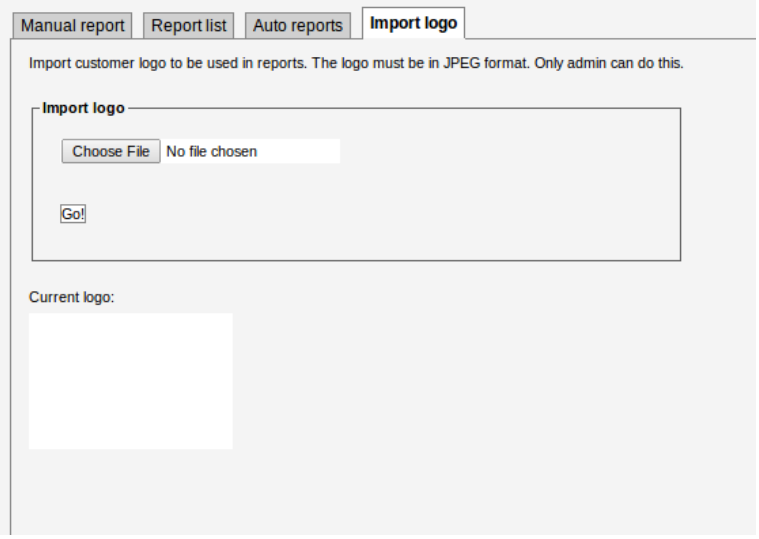
Check the checkbox in the **Email report** row and enter the email address of a recipient, each of the checked report type will be emailed by their time of generation to the selected recipient(s). If there is more than one recipient, add a comma (‘,’) between the addresses.

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.

5.15.4 Reports — Import logo



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

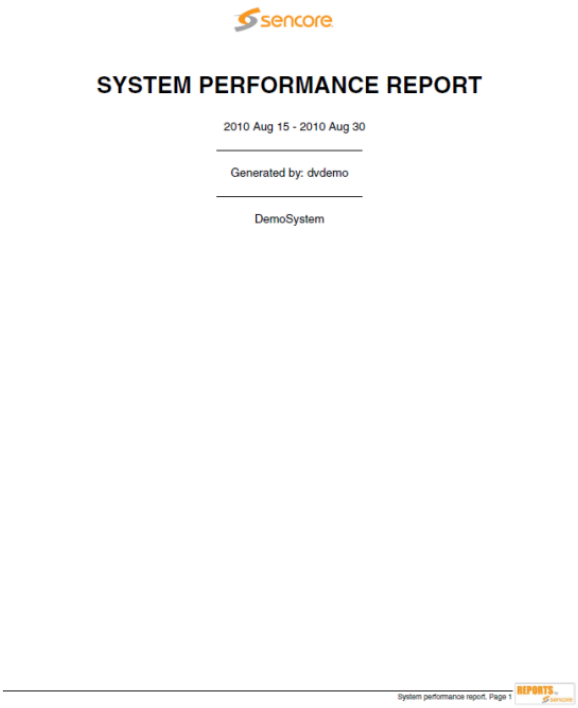
The aspect ratio of the logo should be OK inside the reports even if it is displayed with fixed width and height in this view.

5.15.5 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


sencore

SYSTEM PERFORMANCE REPORT

2010 Aug 15 - 2010 Aug 30

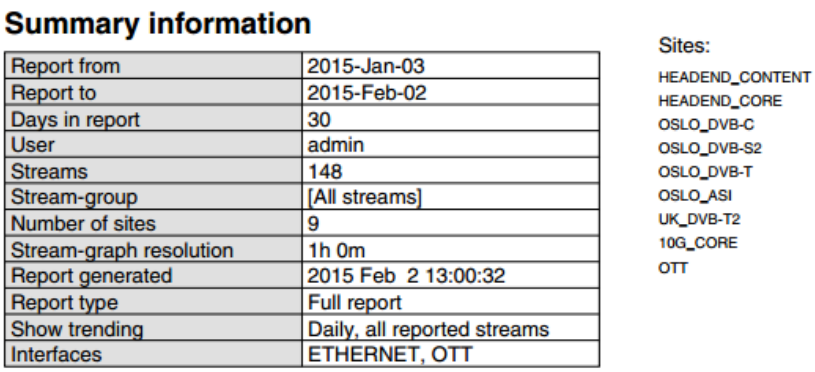
Generated by: dvdemo

DemoSystem

System performance report. Page 1

The company logo can be imported.

The PDF report summary pages



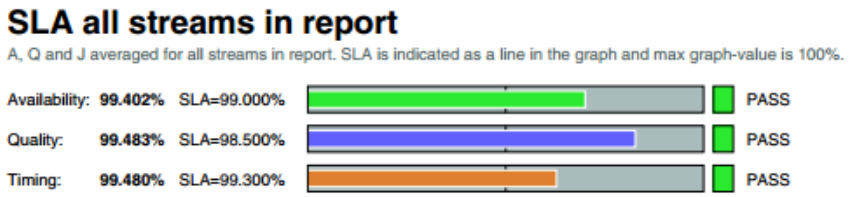
Summary information

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

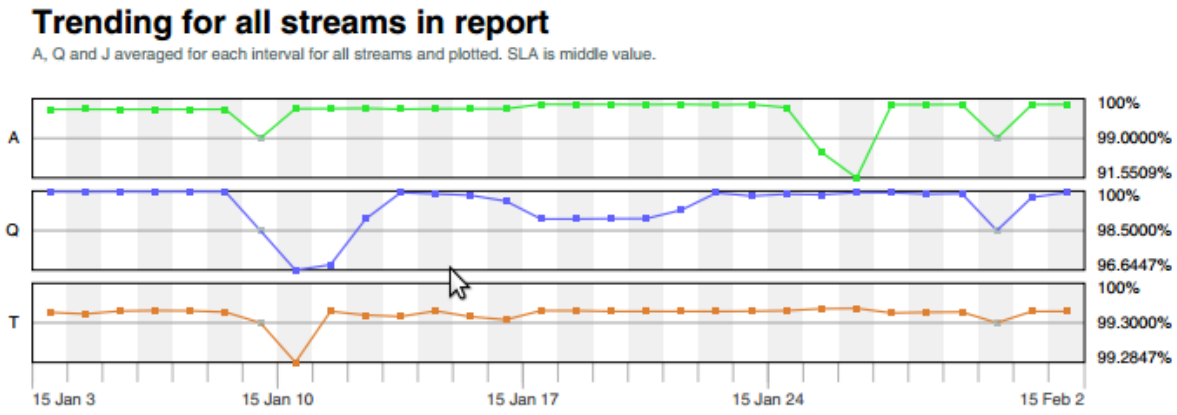
Sites:

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.



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.



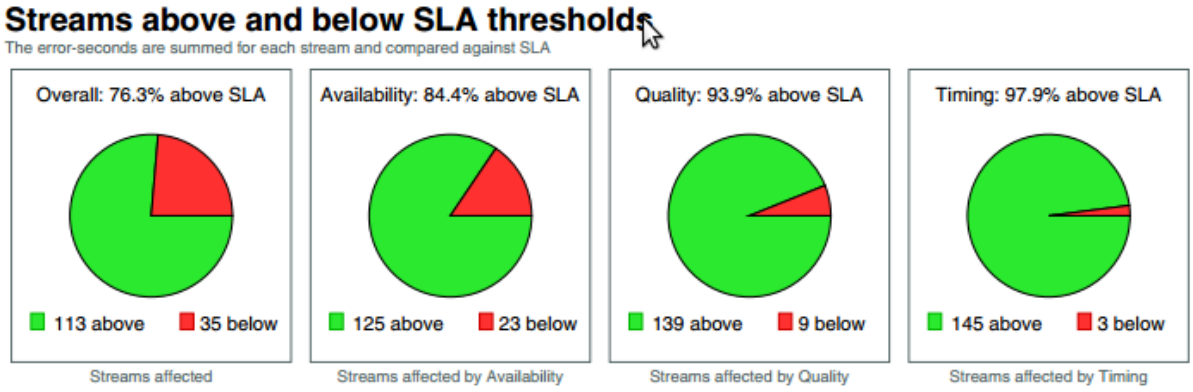
The three trend graphs show how the parameter percentages develop over time. During each trend period (day, week or month) the number of error seconds are summed across all streams and the average is used to represent that trend interval. The labels are 100%, the user specified threshold and the all 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.



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

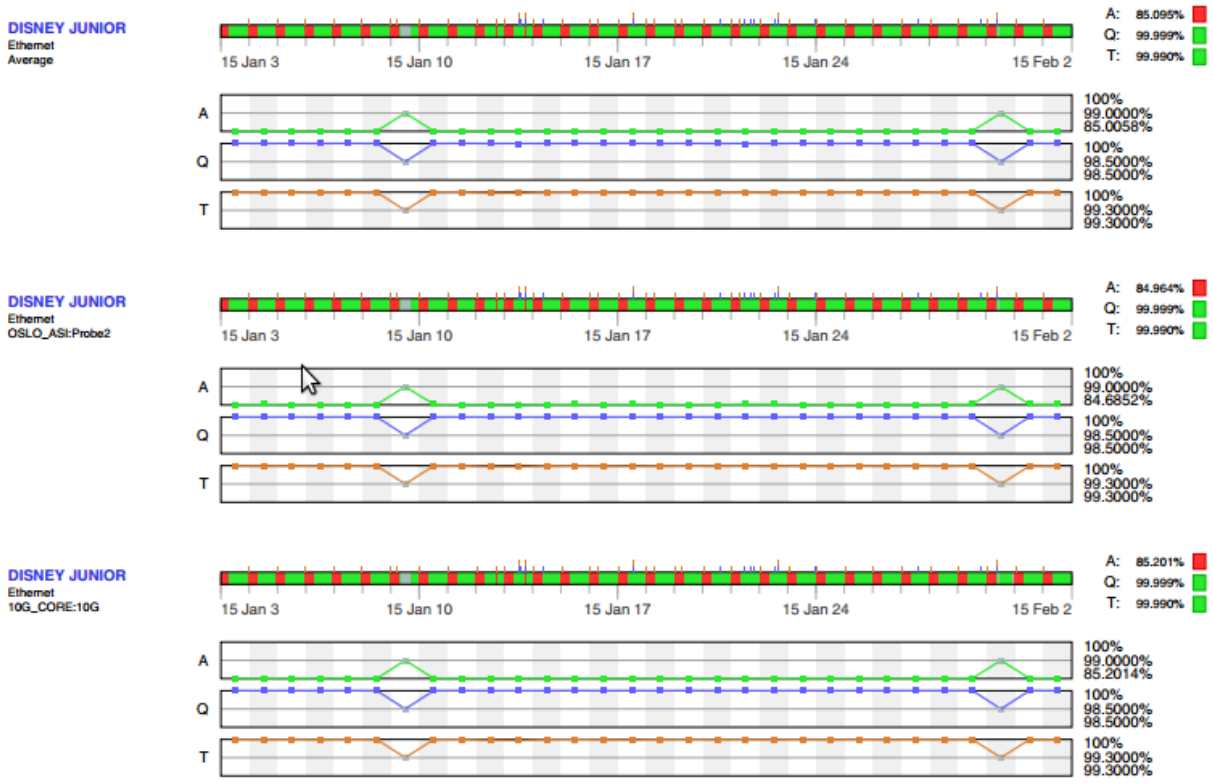
The error-second figures equal the total sum of error-seconds divided by the number of probes (i.e. it is the average)

#	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.

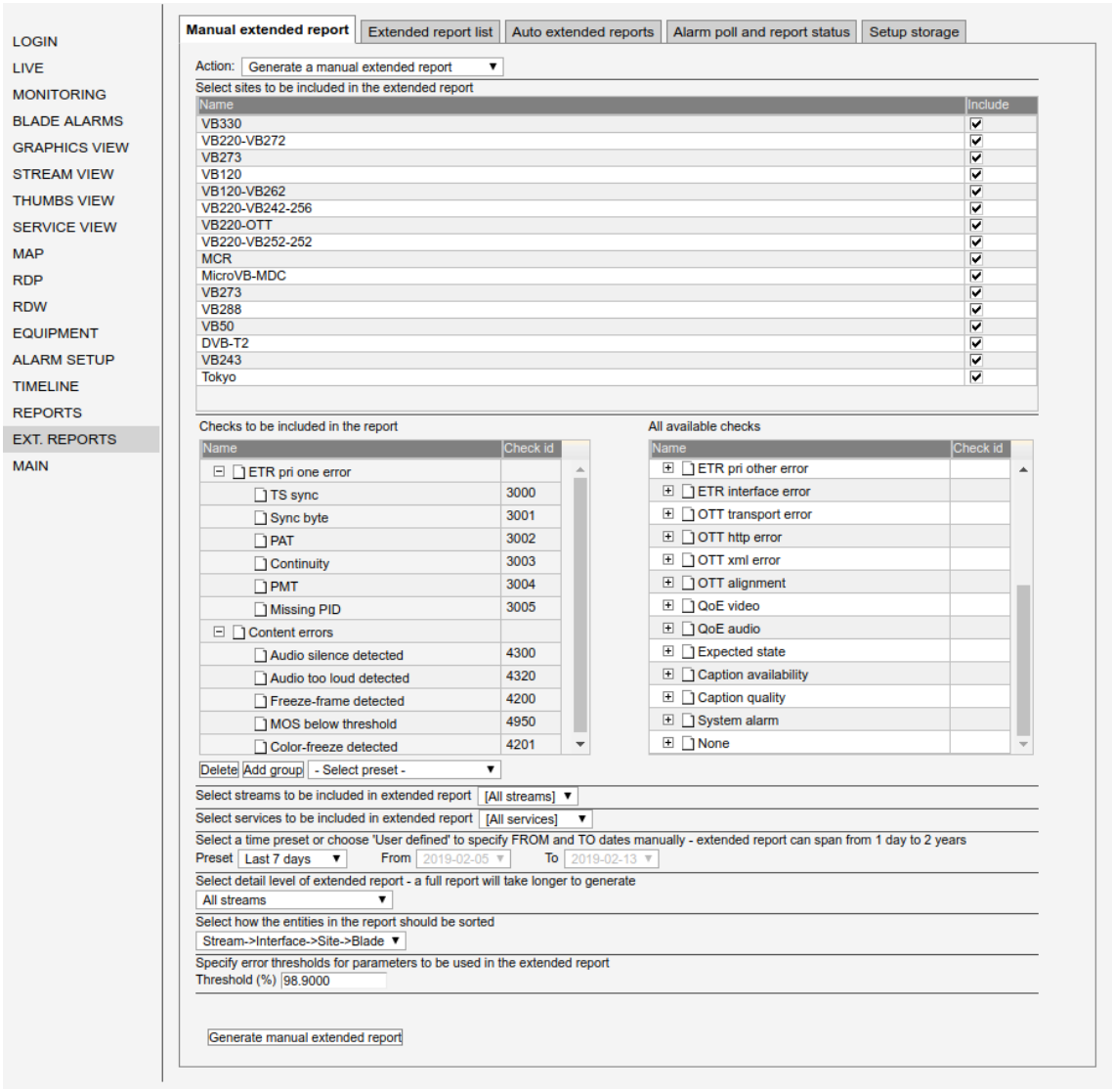
Per stream page



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.

5.16 Ext. Reports



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 VideoBRIDGE 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.

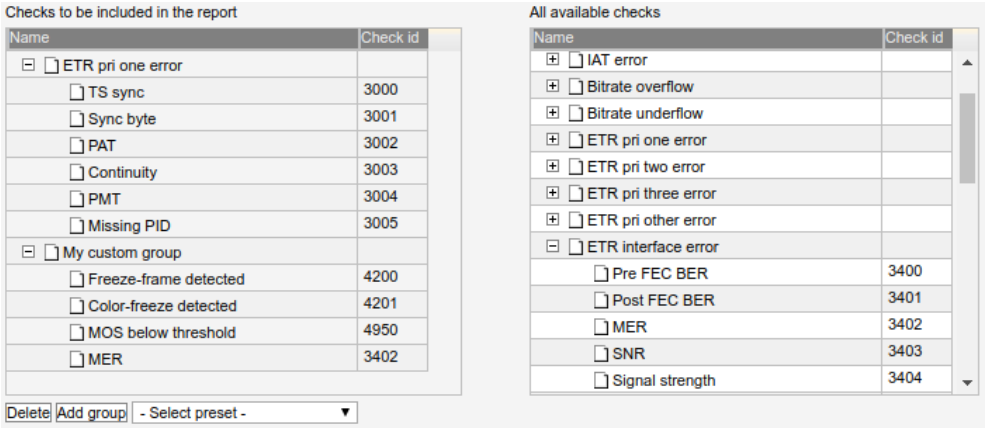
The reports can be created manually or automatically on a daily, weekly or monthly basis and emailed to a list of recipients.

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**.

5.16.1 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.



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 dropdown 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 VideoBRIDGE 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 services or Merged services. 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 a 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.

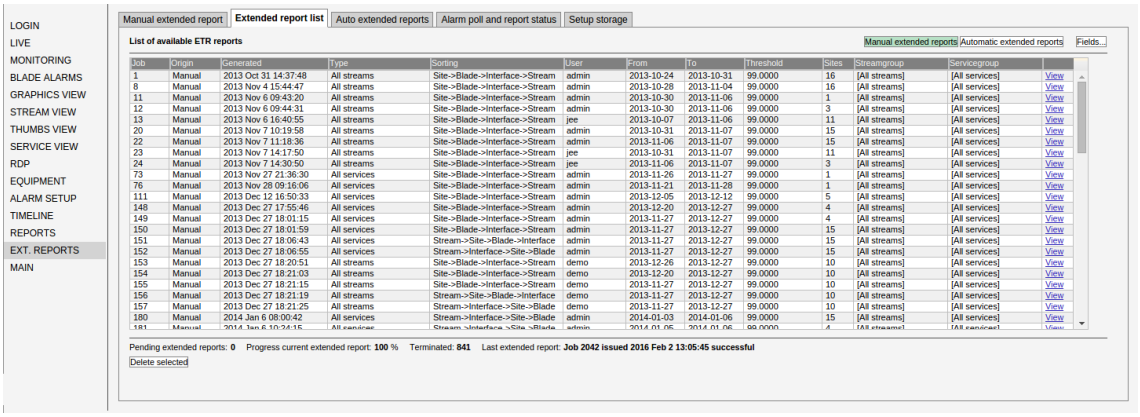
Merged services – This selection will gather data from all services in all of the monitored transport streams and then merge the data together.

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

- 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.

5.16.2 Ext. Reports — Extended report list



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.

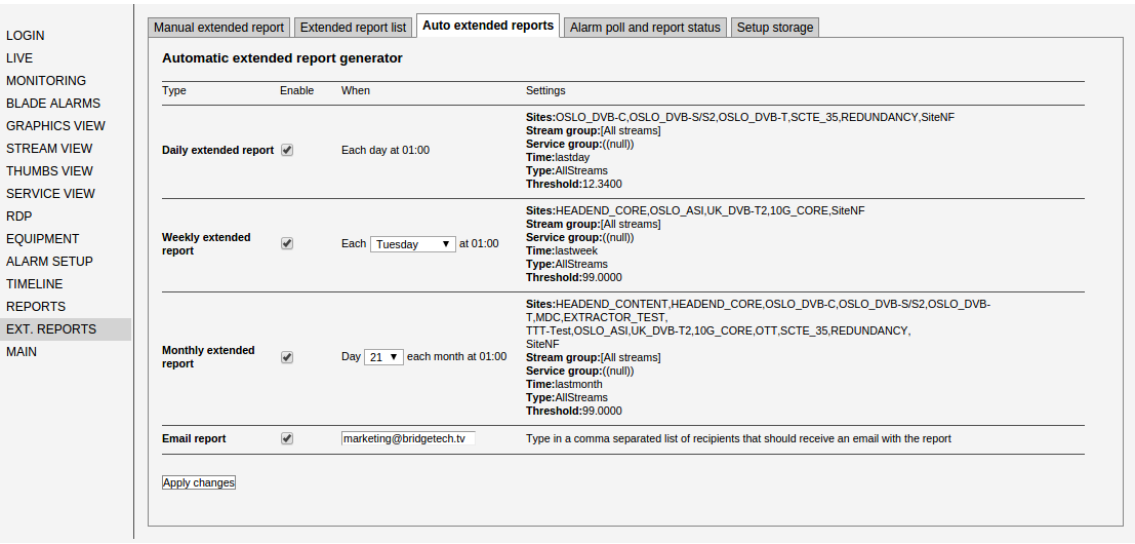
The fields shown in the table are generally the parameters entered in in the **Manual extended Report** tab, except for **Job** number and **Sites**.

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.

5.16.3 Ext. Reports — Auto extended reports



The automatic extended reports tab gives the opportunity to select when and how often the an extended report will be automatically generated.

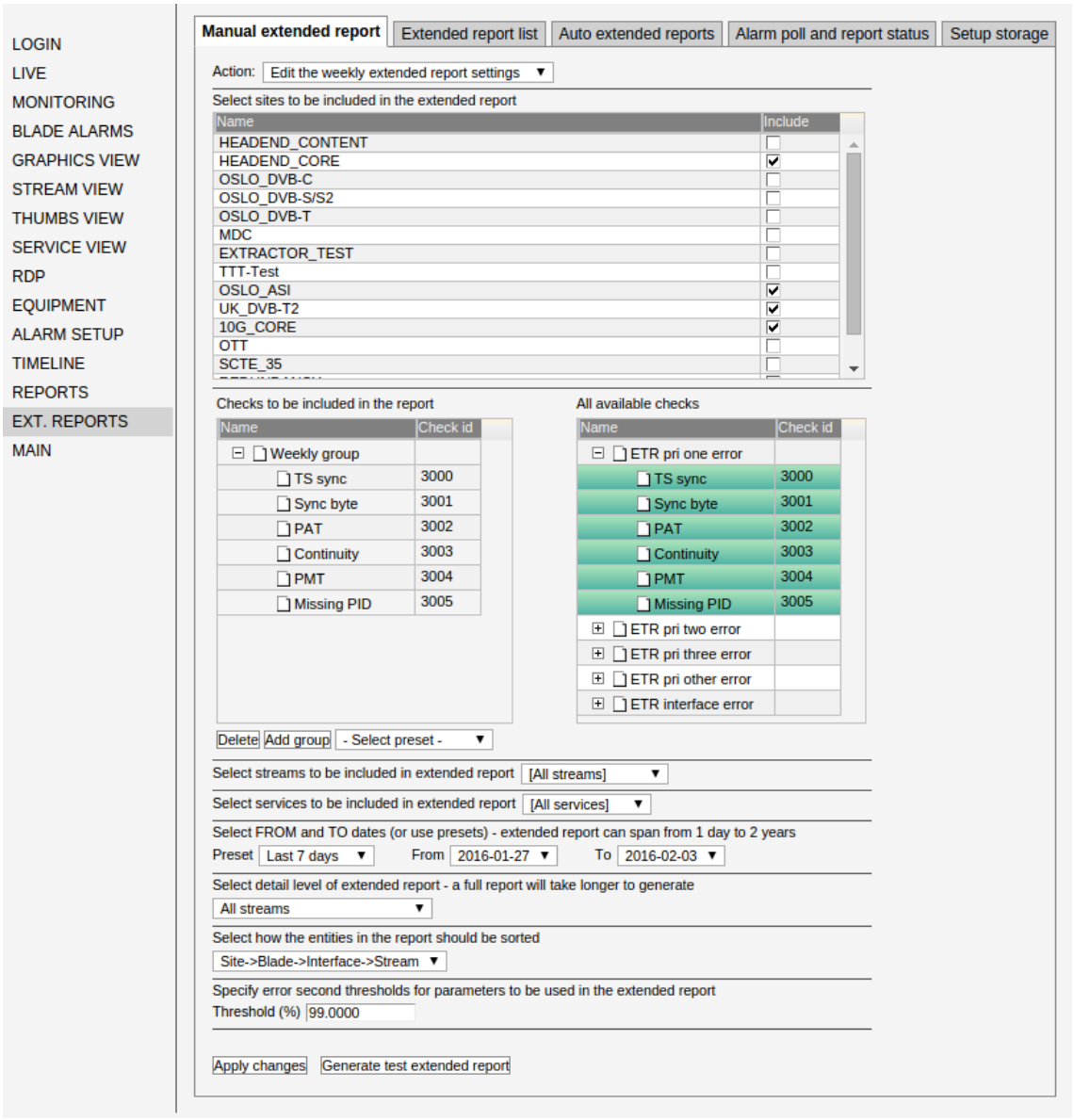
Click the checkbox and select at what intervals the report should be generated, daily, weekly or monthly. For weekly reports the day of the week when the report are to be generated can be specified. Similarly for a monthly report the day of the month can be specified. The reports will be generated at 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.

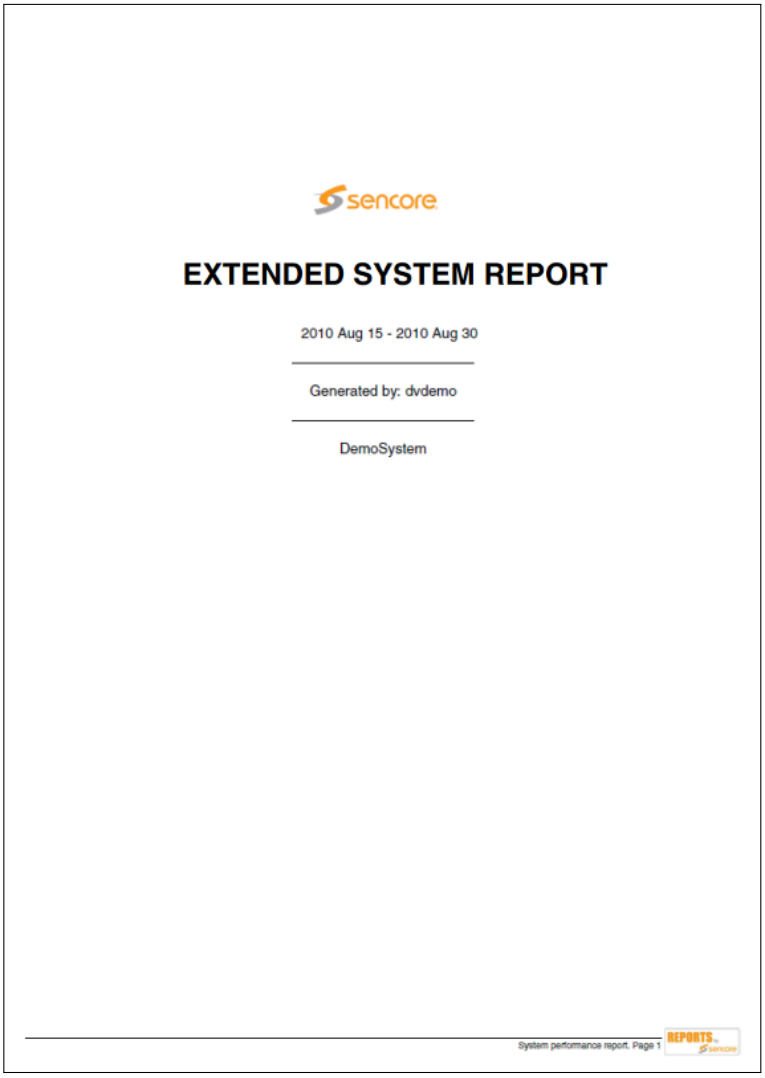
The parameters for the report is shown under the Settings column, these are set in the Manual extended report tab by selecting the Edit for the appropriate report for the Action setting.



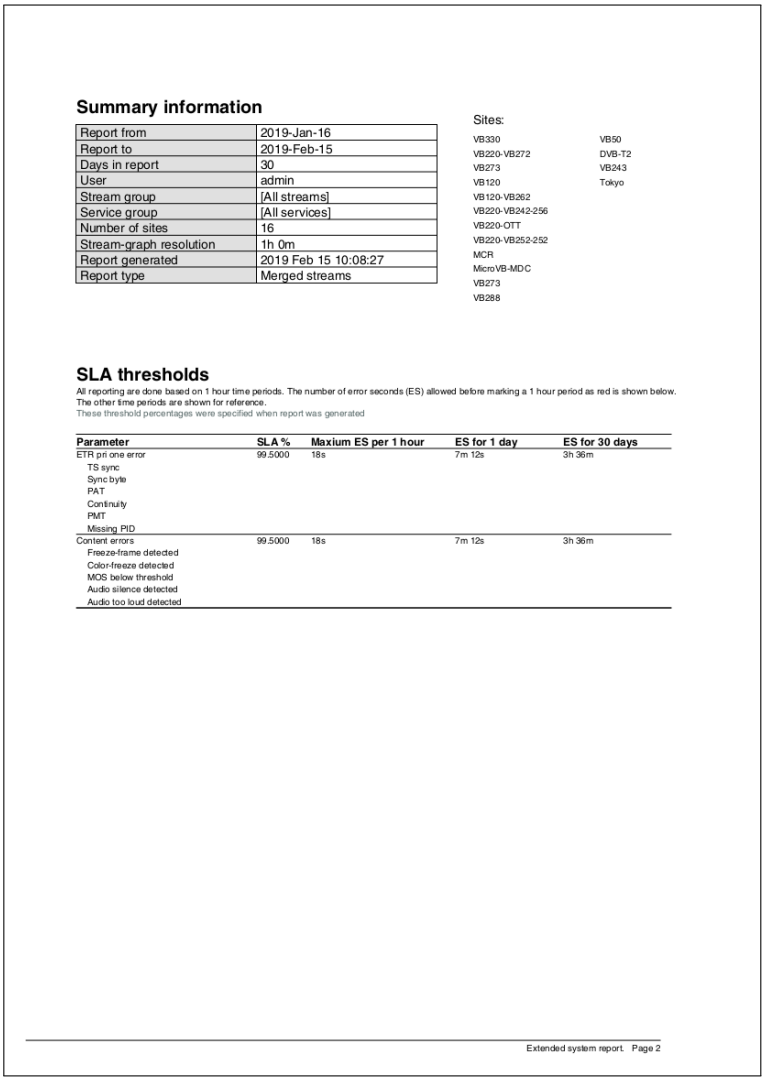
5.16.4 Ext. Reports — PDF Report

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

Report from	2019-Jan-16
Report to	2019-Feb-15
Days in report	30
User	admin
Stream group	[All streams]
Service group	[All services]
Number of sites	16
Stream-graph resolution	1h 0m
Report generated	2019 Feb 15 10:08:27
Report type	Merged streams

Sites:

VB330
VB220-VB272
VB273
VB120
VB120-VB262
VB220-VB242-256
VB220-OTT
VB220-VB252-252
MCR
MicroVB-MDC
VB273
VB288
VB50
DVB-T2
VB243
Tokyo

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 %	Maxium 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.

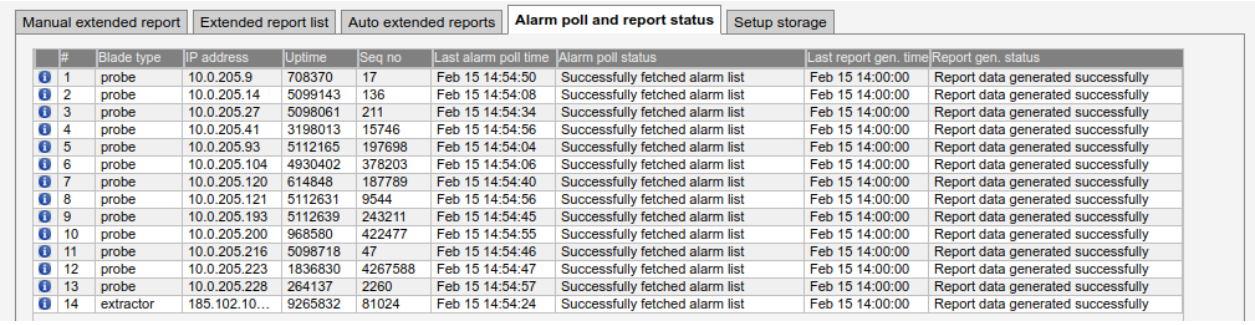
The PDF report Alarm-graph page

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 99coloring 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 probesor extractors. When generating the report it is possible to omit checks which are not of interest or to group several checks together.

5.16.5 Ext. Reports — Alarm poll and report status

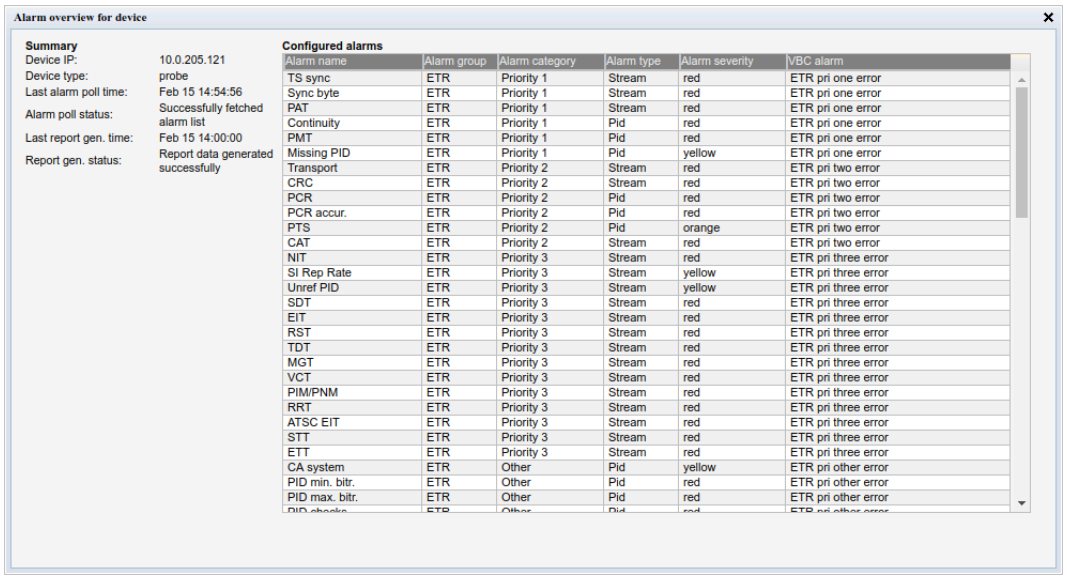


	#	Blade type	IP address	Uptime	Seq no	Last alarm poll time	Alarm poll status	Last report gen. time	Report gen. status
ⓘ	1	probe	10.0.205.9	708370	17	Feb 15 14:54:50	Successfully fetched alarm list	Feb 15 14:00:00	Report data generated successfully
ⓘ	2	probe	10.0.205.14	5099143	136	Feb 15 14:54:08	Successfully fetched alarm list	Feb 15 14:00:00	Report data generated successfully
ⓘ	3	probe	10.0.205.27	5098061	211	Feb 15 14:54:34	Successfully fetched alarm list	Feb 15 14:00:00	Report data generated successfully
ⓘ	4	probe	10.0.205.41	3198013	15746	Feb 15 14:54:56	Successfully fetched alarm list	Feb 15 14:00:00	Report data generated successfully
ⓘ	5	probe	10.0.205.93	5112165	197698	Feb 15 14:54:04	Successfully fetched alarm list	Feb 15 14:00:00	Report data generated successfully
ⓘ	6	probe	10.0.205.104	4930402	378203	Feb 15 14:54:06	Successfully fetched alarm list	Feb 15 14:00:00	Report data generated successfully
ⓘ	7	probe	10.0.205.120	614848	187789	Feb 15 14:54:40	Successfully fetched alarm list	Feb 15 14:00:00	Report data generated successfully
ⓘ	8	probe	10.0.205.121	5112631	9544	Feb 15 14:54:56	Successfully fetched alarm list	Feb 15 14:00:00	Report data generated successfully
ⓘ	9	probe	10.0.205.193	5112639	243211	Feb 15 14:54:45	Successfully fetched alarm list	Feb 15 14:00:00	Report data generated successfully
ⓘ	10	probe	10.0.205.200	968580	422477	Feb 15 14:54:55	Successfully fetched alarm list	Feb 15 14:00:00	Report data generated successfully
ⓘ	11	probe	10.0.205.216	5098718	47	Feb 15 14:54:46	Successfully fetched alarm list	Feb 15 14:00:00	Report data generated successfully
ⓘ	12	probe	10.0.205.223	1836830	4267588	Feb 15 14:54:47	Successfully fetched alarm list	Feb 15 14:00:00	Report data generated successfully
ⓘ	13	probe	10.0.205.228	264137	2260	Feb 15 14:54:57	Successfully fetched alarm list	Feb 15 14:00:00	Report data generated successfully
ⓘ	14	extractor	185.102.10...	9265832	81024	Feb 15 14:54:24	Successfully fetched alarm list	Feb 15 14:00:00	Report data generated successfully

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.

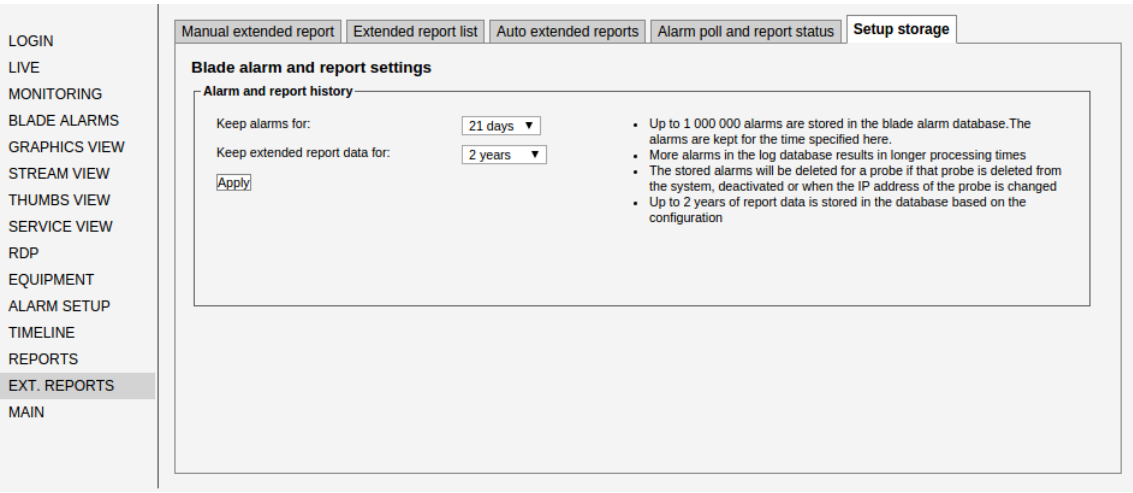
Alarm poll and report status	
#:	Number of the blade
Blade type:	Device type, either probe or extractor
IP address:	The IP of the selected device
Uptime:	Uptime in minutes
Seq no:	Sequence number of the last alarm message received
Last alarm poll time:	What the time was when the VBC fetched the alarm 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	
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 affect by the error. The alarms can be for the entire **System**, affecting a 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.

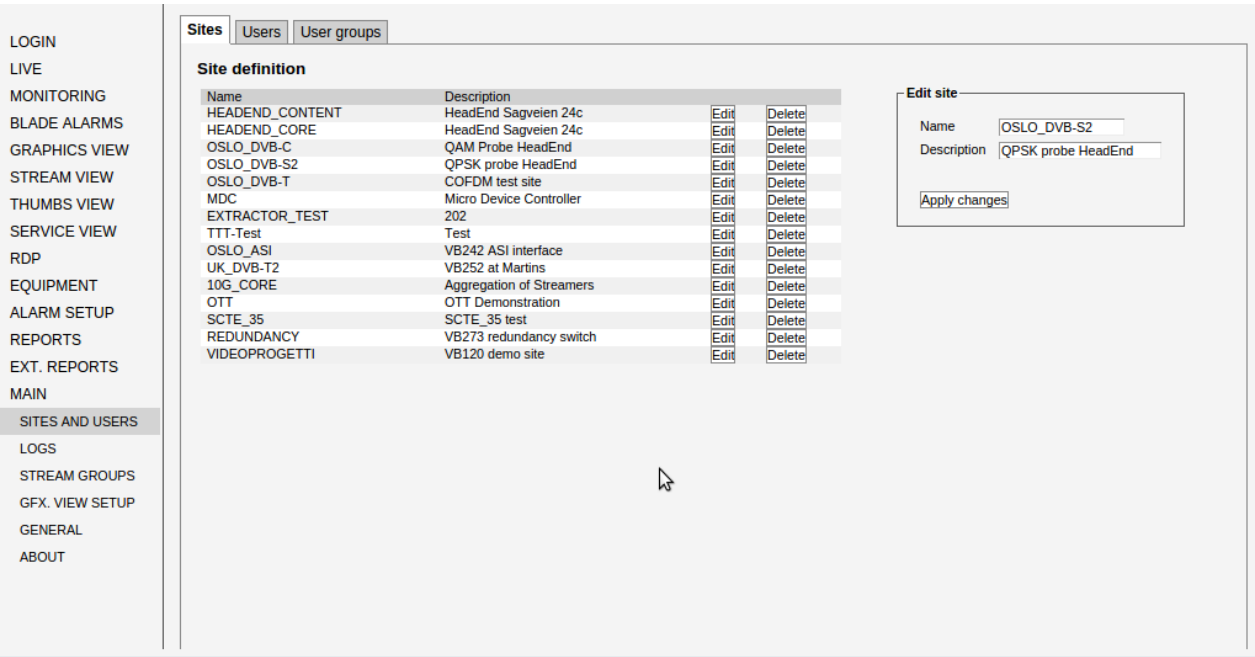
5.16.6 Ext. Reports — Setup storage



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 1 000 000 alarms. The extended reports data can be kept for up to two years.

5.17 Main — Sites and Users

5.17.1 Sites and Users — Sites



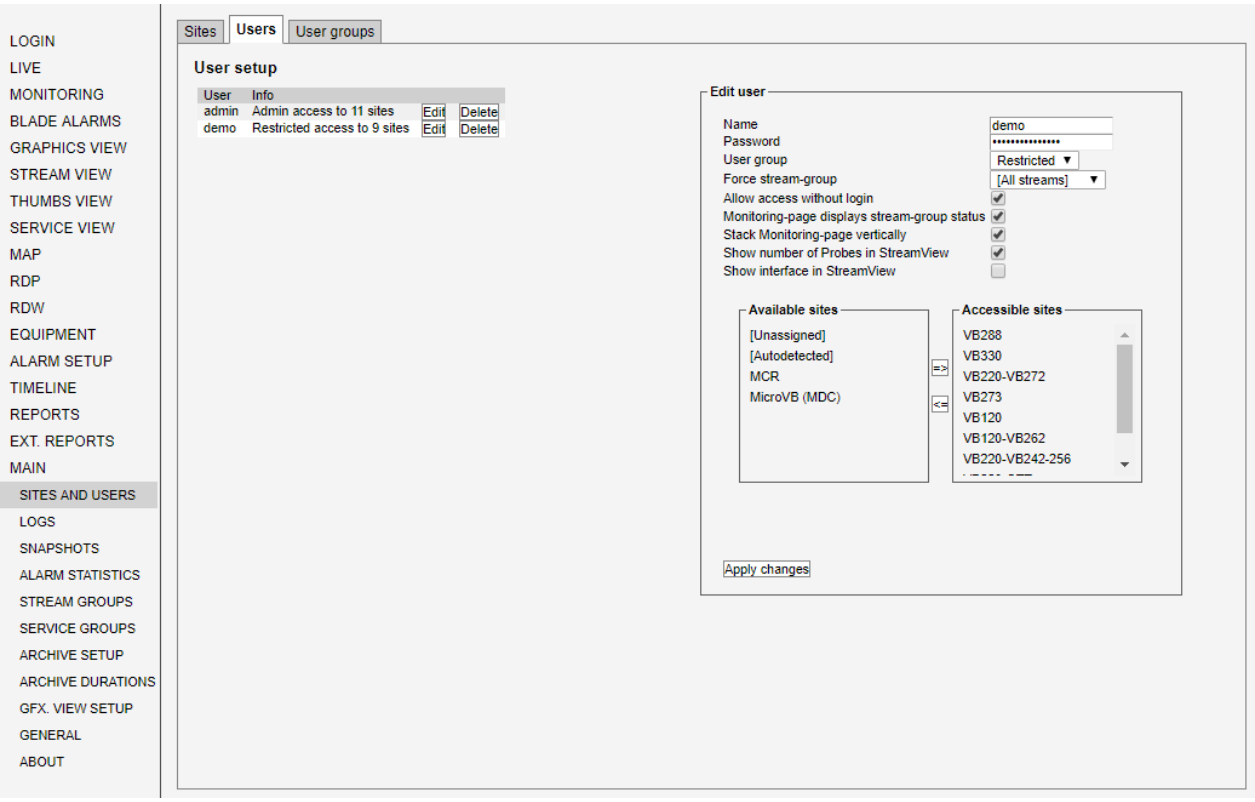
From the **Site setup** page it is possible to add new sites. Existing sites can be deleted or renamed. Choose the site name with care since it will be used to identify alarm messages and devices across the VBC.

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.

5.17.2 Sites and Users — Users



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.

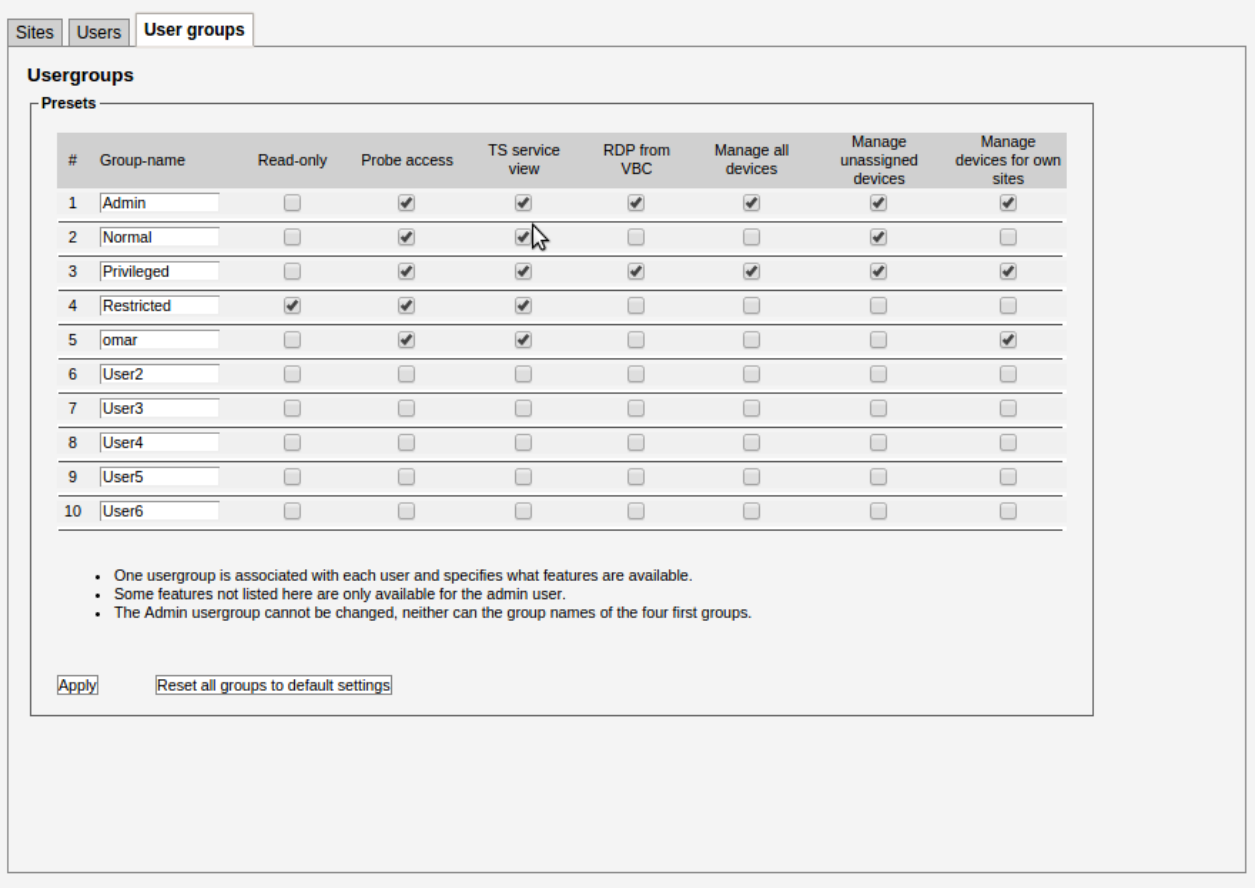
User properties	
Name:	The user name
Password:	The user password for login
User group:	User groups with different access rights are defined in the **User group** view. Select a user group from the drop down menu.
Force stream-group:	If assigned a stream group, then only that stream group is available in views such as **Stream view** and **Reports**.
Allow access without login:	Enable this setting to allow the user to access this VideoBRIDGE Controller from a Master VBC. See chapter 4.2 for more details.
Monitoring page displays stream-group status:	Select if the *Stream group status* field should be displayed in the **Monitoring** view

Stack Monitoring page vertically:	Select if the *Status for all sites* and *Stream group status* 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 *Stream group status* 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. To change the password for the Software Activation interface, please refer to chapter 2.4

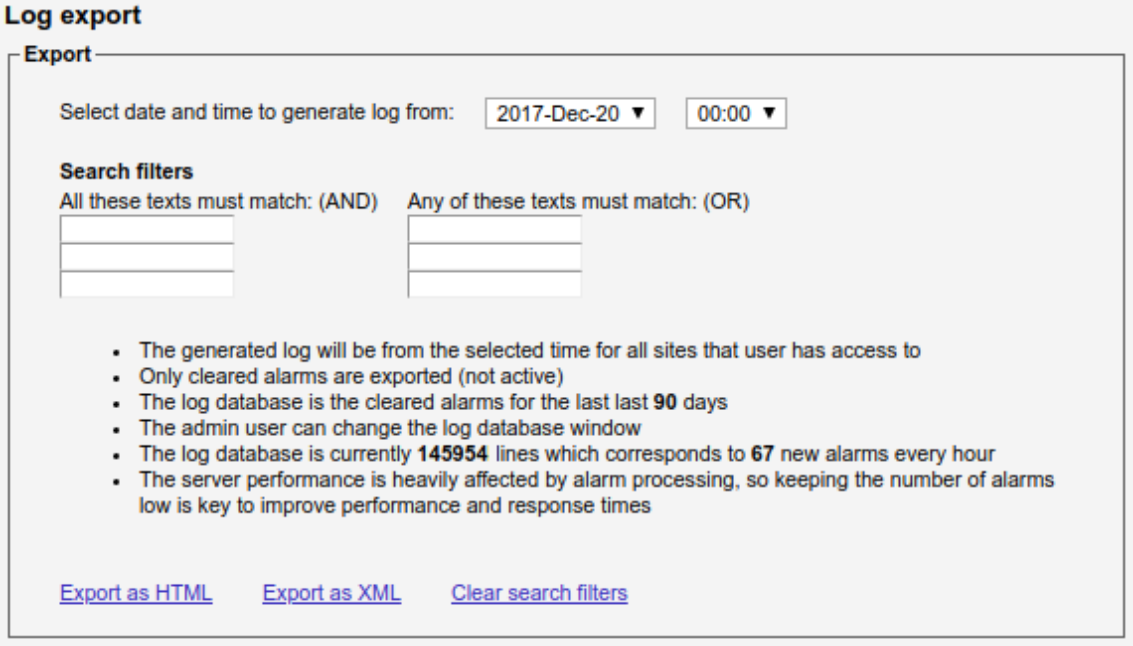
5.17.3 Sites and Users — User groups



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.

5.18 Main — Logs

5.18.1 Logs — Logs



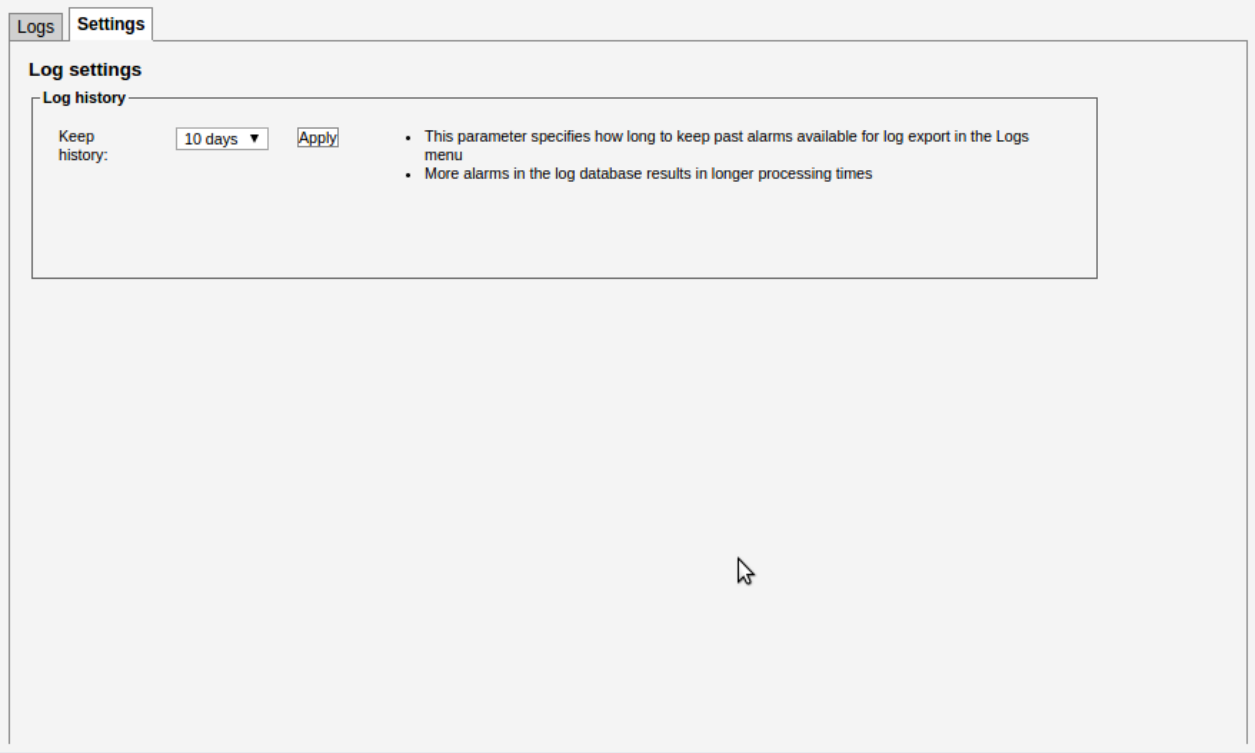
In the **Logs** view it is possible to export an alarm log listing all cleared alarms from all sites the current user has access to. The log start time is selected using the drop-down menus, and the export is activated by clicking the *Export HTML* or *Export XML* links.

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.

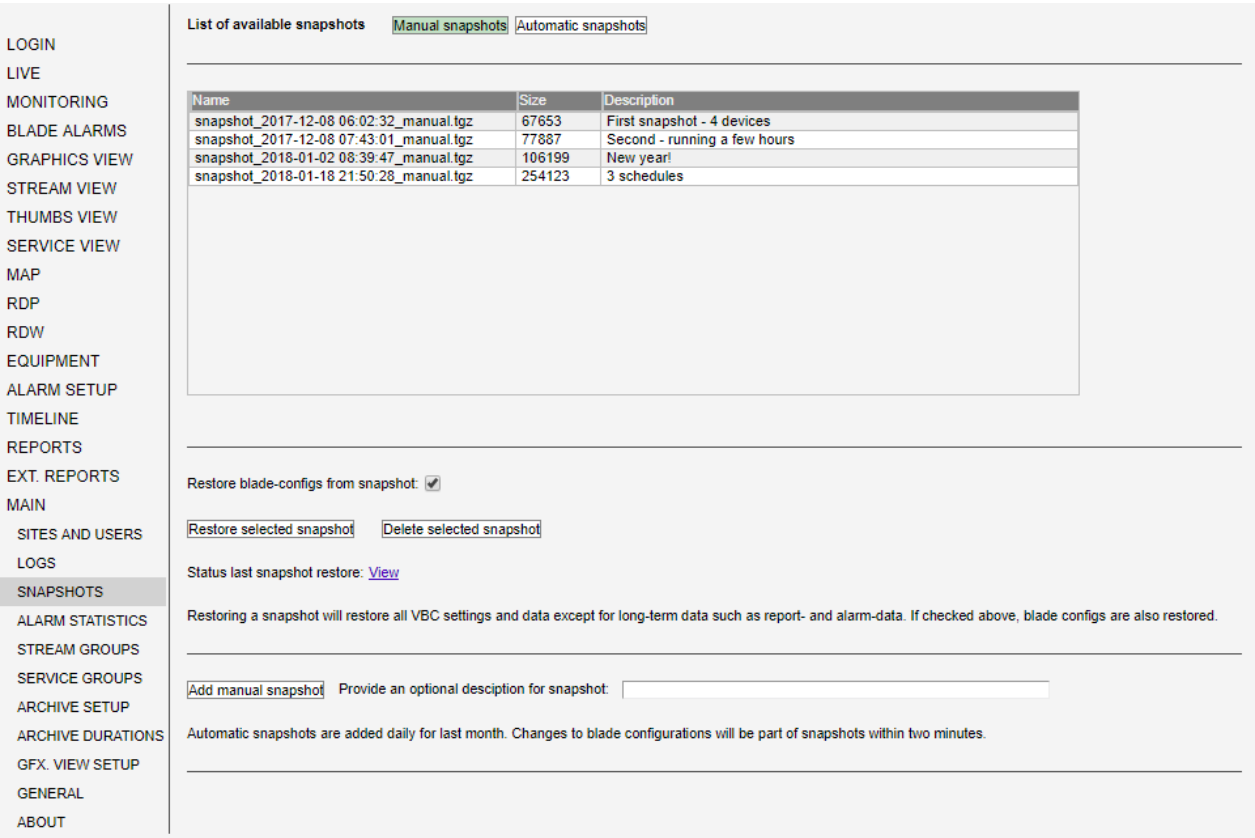
The number of days the log is kept is set in **Logs — Settings**.

5.18.2 Logs — Settings



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.

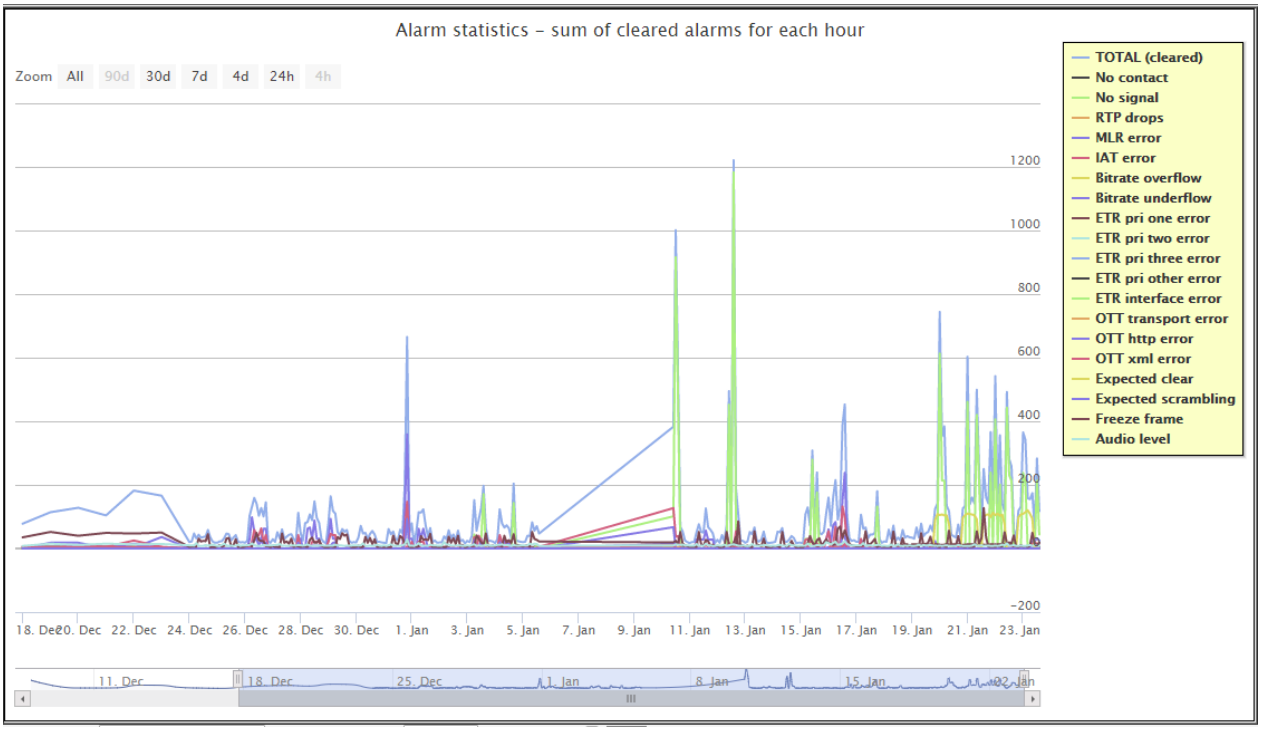
5.19 Main — Snapshots



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.

5.20 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

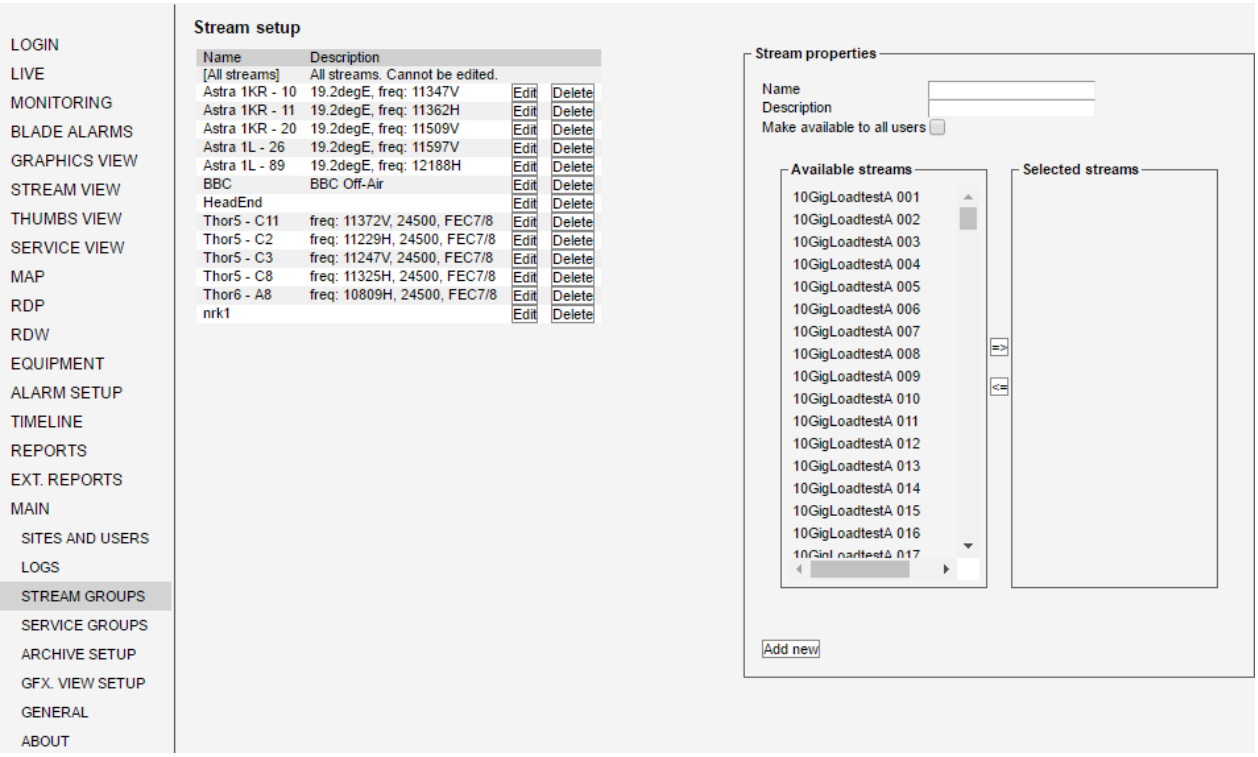
- identifying patterns to when alarm storms happen.
- determining the need to perform more tuning of thresholds and scheduling.
- lowering the load on the VBC server — lowering the number of alarms in a system will considerably lower the load on the server.

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.

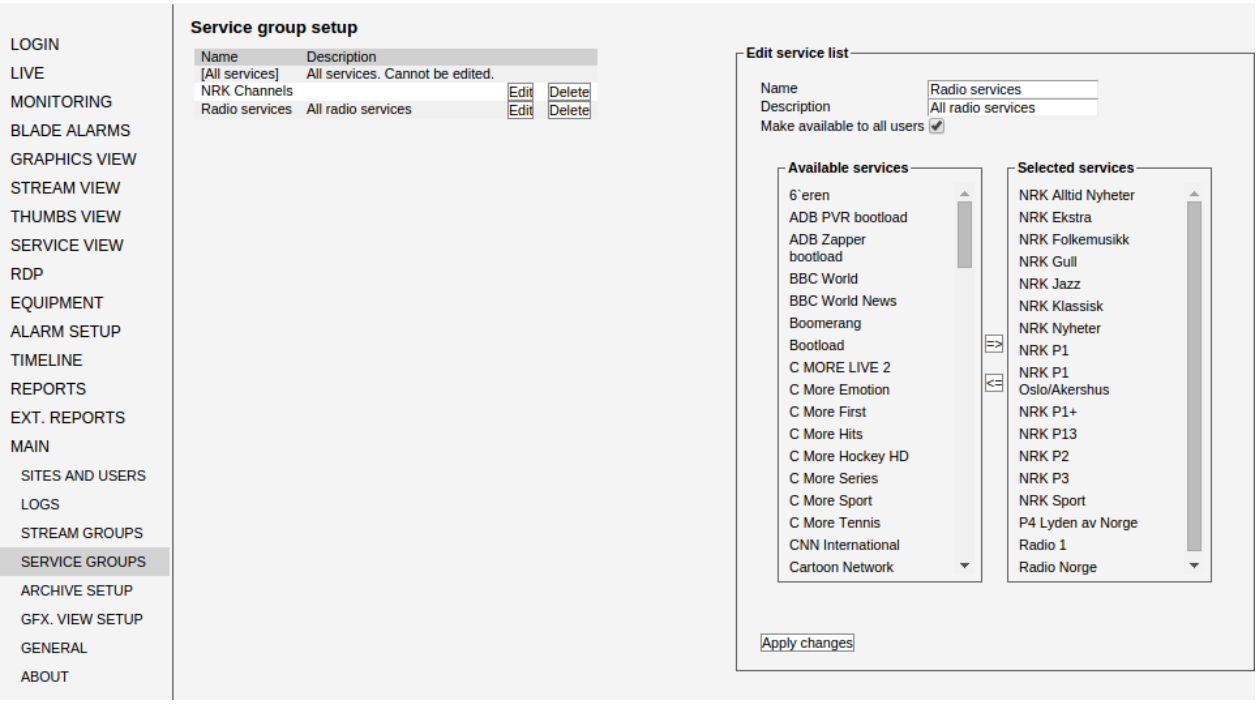
5.21 Main — Stream groups



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.

5.22 Main — Service groups



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.

5.23 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 backend. Later, to review the data stored, one uses the **Timeline** view on the VBC to inspect the data. Refer to chapter 5.14 for details on the Timeline view.

5.23.1 Archive server

The Archive server runs on a separate machine, but can on small installations run on the same machine as other software.

License

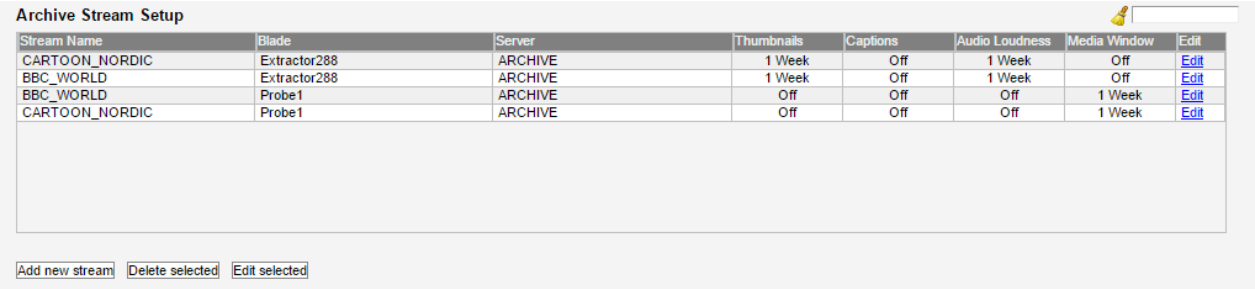
The archive server comes with a license defining how many streams one can assign to it. Each unique stream name count as one stream. You can archive the same stream, from multiple sources, using only one slot of the license. If you are archiving a stream named XYZ and XYZ HD they will count as two streams. To avoid that you can give them different class names, as XYZ@SD and XYZ@HD.

5.23.2 Enabling the Archive server

To enable the archive server, you need to activate it in the same manner as the VBC was activated in chapter 2.4. You then have to configure it to use the correct VBC server.

On the VBC server, add the archive server as a new device, as described in chapter 5.12. Please note that you can only add one archive server per VBC server.

5.23.3 Configuration



To configure what you want to archive you must go into the VBC, select MAIN, and then ARCHIVE SETUP. From that menu 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.

5.23.4 System requirements

The system requirements for the Archive server depend on how much data you want to archive and for how long. Maximum storage time is 3 months.

Server requirements, all parameters, 100 services aggregated for 3 months

- Intel Sandybridge generation CPU or newer
- 32 Gbyte RAM (DDR 4 recommended)
- 2 Tbyte available disk space (RAID 5 recommended)

Server requirements, all parameters, 1000 services aggregated for 3 months

- Intel Sandybridge generation CPU or newer
- 200 Gbyte RAM (DDR 4 recommended)
- 20 Tbyte available disk space (RAID 6 recommended)

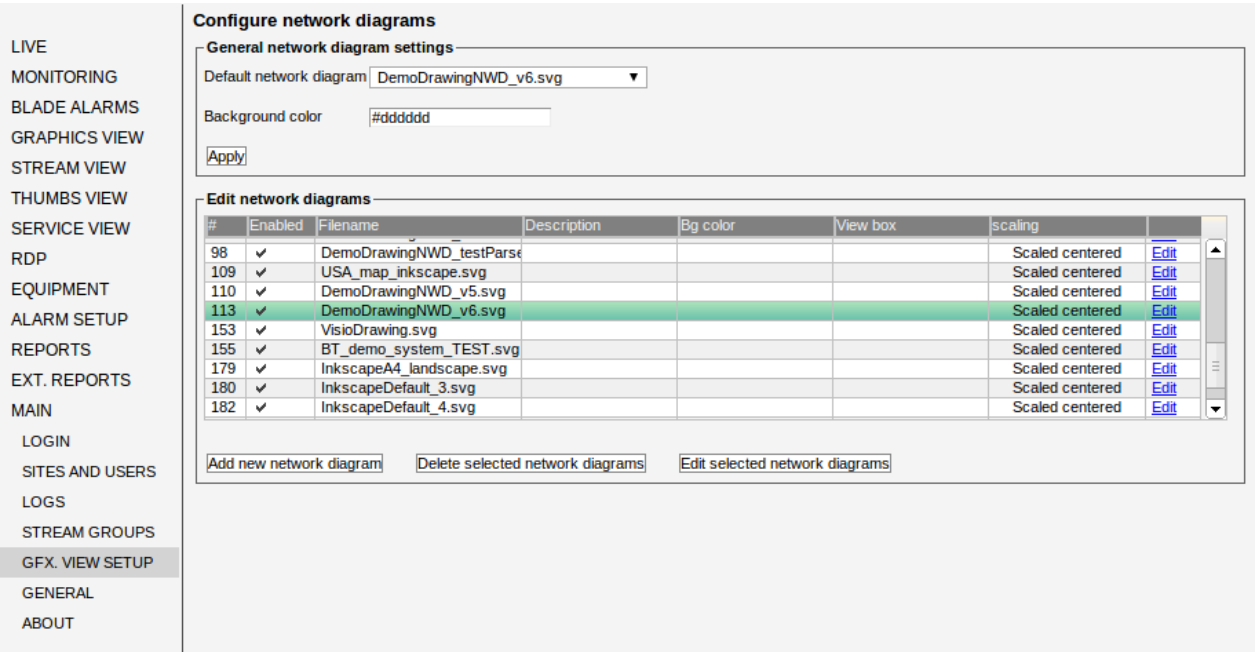
For N streams an ARCHIVE-SERVER-N license is required. The number of aggregated services which is used to scale the server hardware does not correspond to the N in the license. 100 probes archiving the same 5 streams only requires a ARCHIVE-SERVER-5 license, but the hardware would need to be scaled for 500 services.

5.23.5 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.

5.24 Main — Gfx. View Setup (Graphics option)



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.

5.24.1 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)"

Inkscape	
Configuration	*How to*
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.

Color codes	
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.

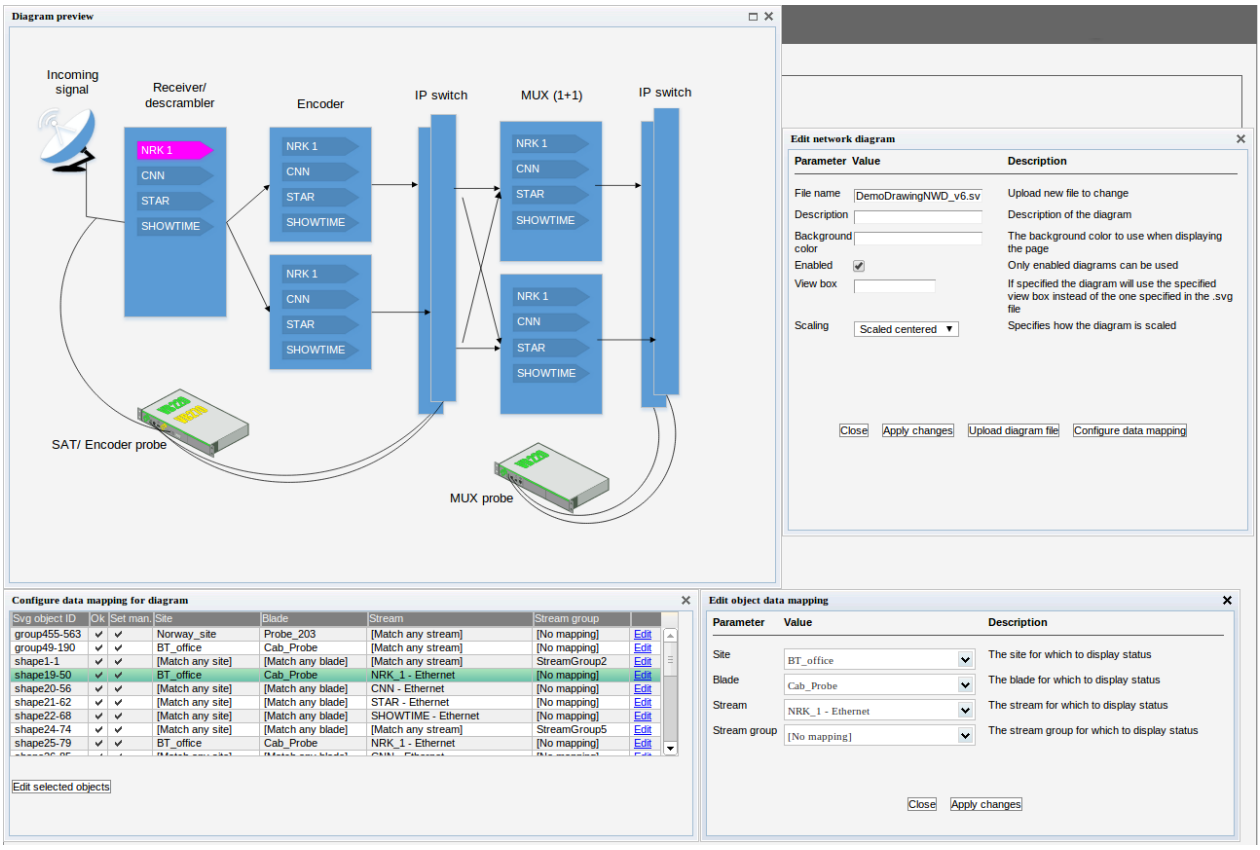
5.24.2 Setup and data mapping

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**.

Edit network diagram	
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**.



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 dropdown selectors in the separate **Edit object data mapping** editing window.

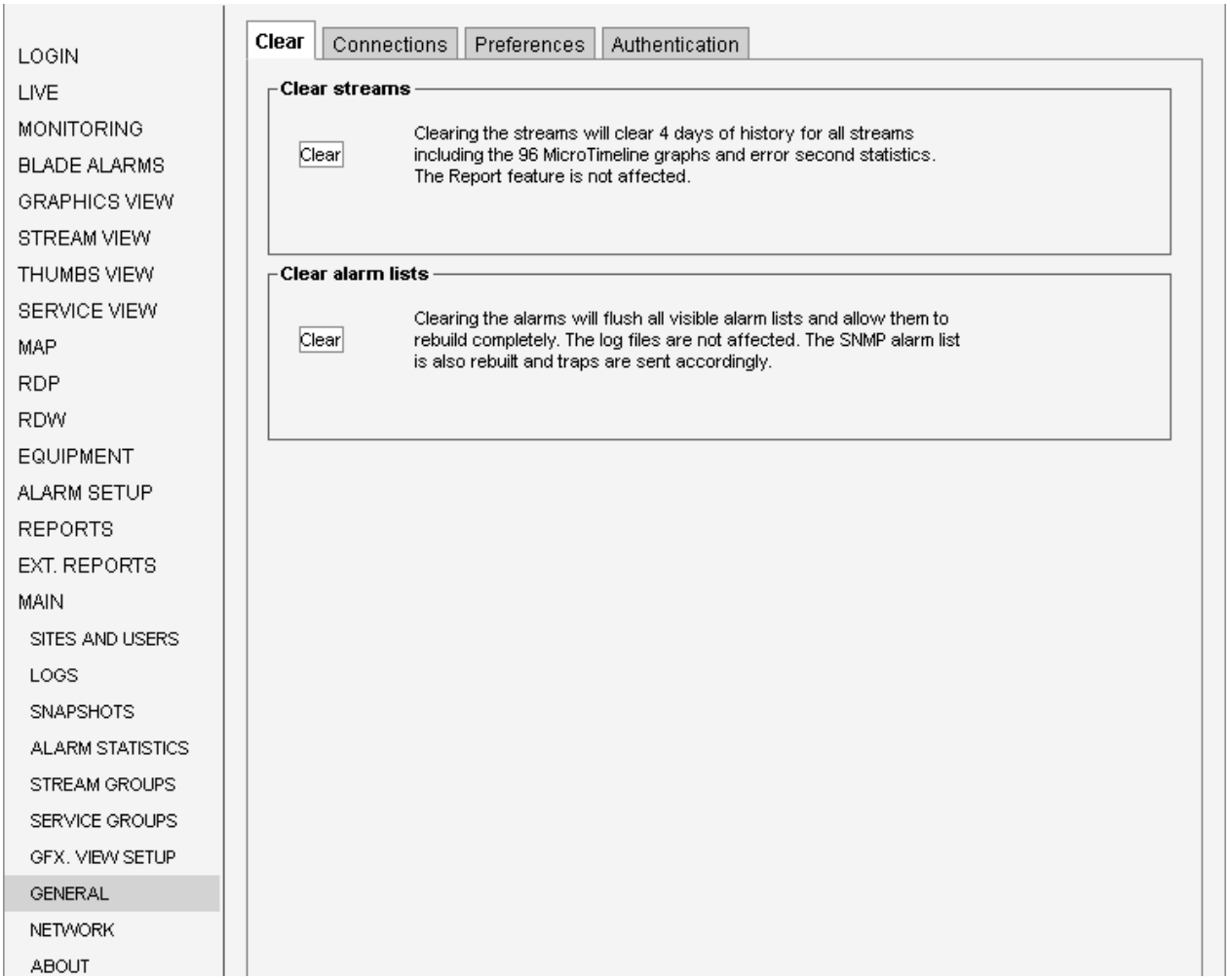
Note: Mapping of a Stream group will override any other mapping combination of Site/Blade/Stream. Leave Stream group on [No mapping] for other mappings.

To choose an aggregated stream status, simply select [Match any site/blade] + the desired stream from the dropdowns. For mapping of a blade specific stream status select the desired Site, Blade and Stream. Remember to click **Apply changes**.

5.25 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.

5.25.1 General — Clear



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.

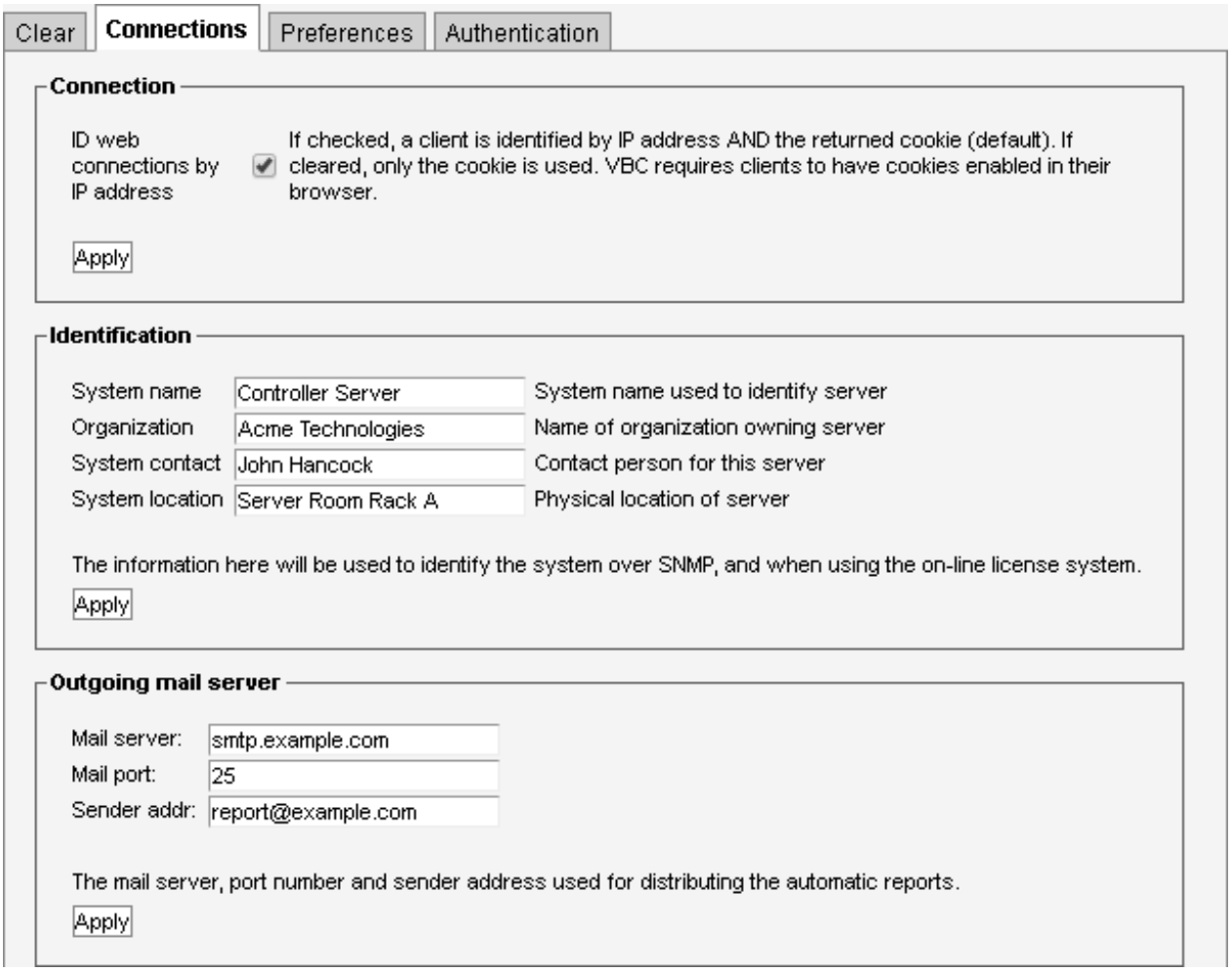
Note that after clearing, the stream bars will take 4 days to fully rebuild.

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.

5.25.2 General — Connections



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 verifying the license on-line, see I Appendix: On-line License Verification 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 verifying 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 verifying 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.

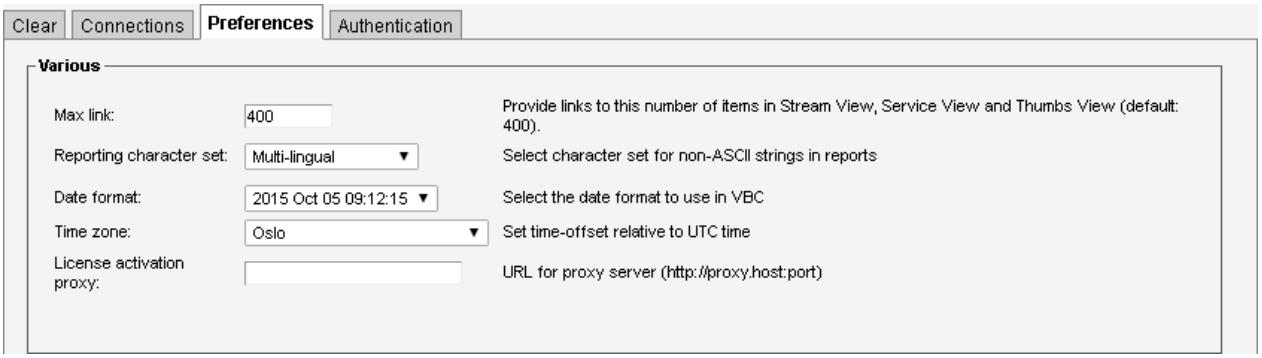
If the configuration is a domain name, such as `mail.example.com`, make sure that the DNS settings on the server are configured properly.

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 Administrator's Guide[3] 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.

[3] `https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/s1-email-mta`

5.25.3 General — Preferences



Various

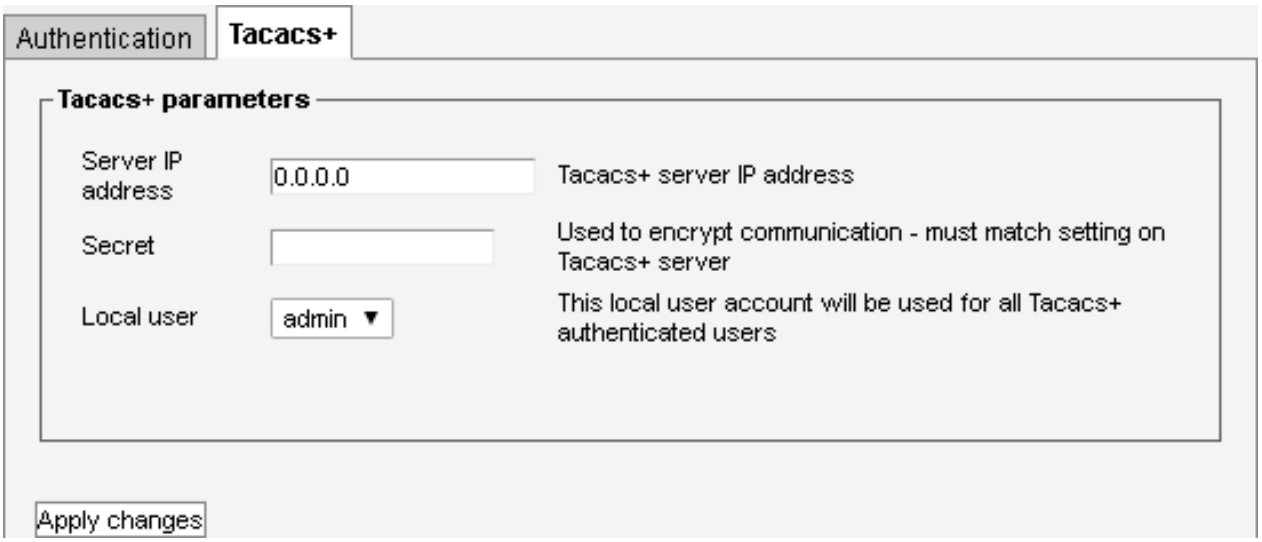
Various	
Max link:	The number of links in the Stream view, Service view and Thumbs view, where maximum is 999 and 100 is the minimum. 400 is default.
Reporting character set:	This selects which character set is to be used for reports for non-ASCII characters, i.e., letters outside the A–Z range. The 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 VideoBRIDGE Controller time can be offset from the reference NTP time. Please note that this changes the global time zone on the system running the VideoBRIDGE 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.

5.25.4 General — Authentication

Authentication

The authentication in the VideoBRIDGE 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.

Tacacs+



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.

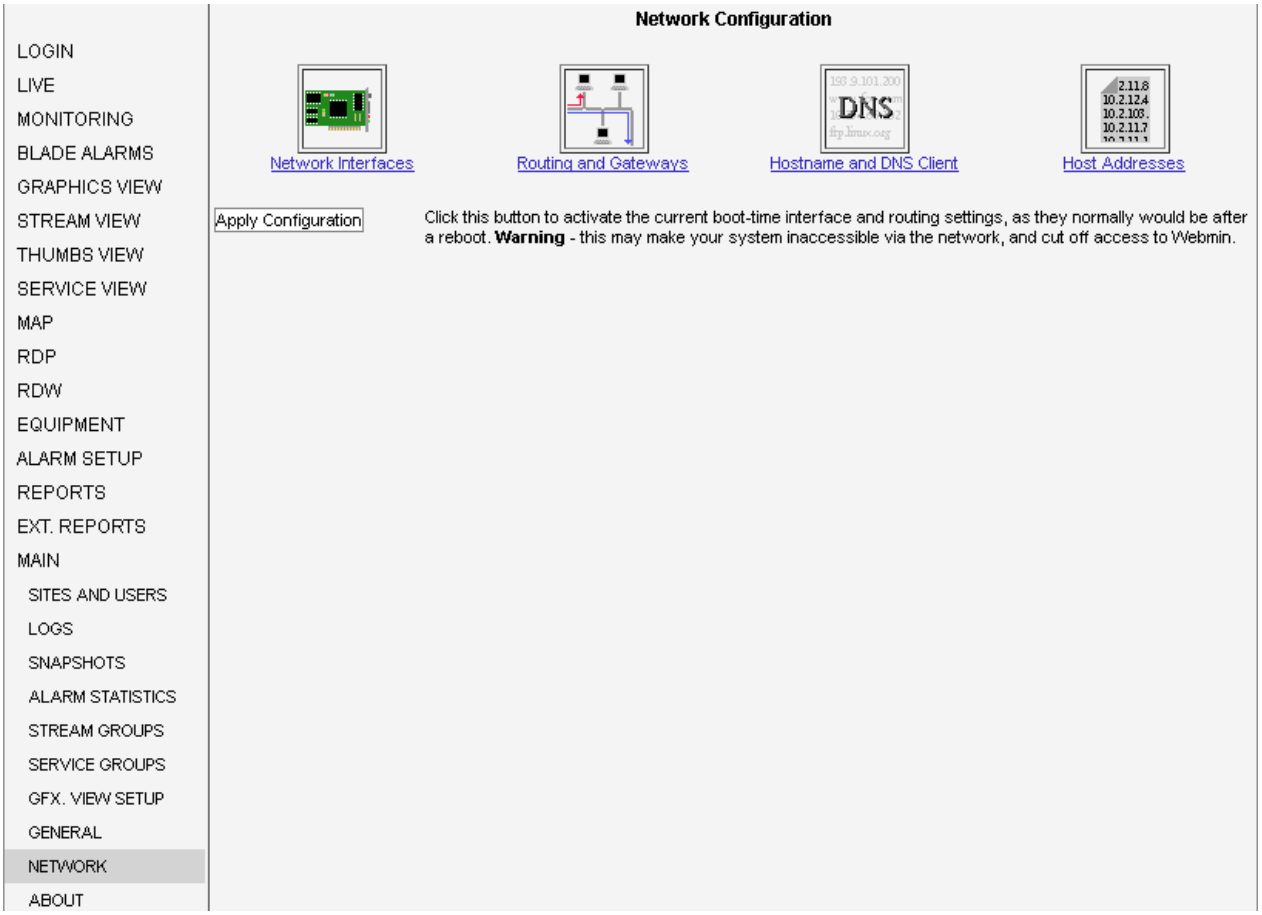
The VBC server does not relate to the Tacacs+ accounts directly. The VBC only receives a reply from the Tacacs+ server whether the login was successful or not. If the login was successful the user will proceed into the VideoBRIDGE Controller as if he had logged directly into VBC as the *Local*

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, see **Enabling HTTPS** for details on how to enable HTTPS for the VBC web server. 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 possible reverse engineer the scrambling of login details.

Tacacs+ parameters	
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
Local user	The VBC user account used when logging in using Tacacs+ authentication

5.26 Main — Network



The **Main — Network** view defines the Ethernet setup parameters for the network interfaces on the system hosting the VideoBRIDGE Controller.

This page uses the same log-in credentials as the Software Activation interface. Please refer to chapter 2.4 for details on Software Activation.

The configuration is divided into different sections, click the appropriate icon to access the different parts.

The web-based network configuration tool is based on WebMin. Further documentation is available in the WebMin documentation[4].

If you make changes here that causes you to lose web access to the server, please see K Appendix: Network configuration for how to configure the network using the command-line tools.

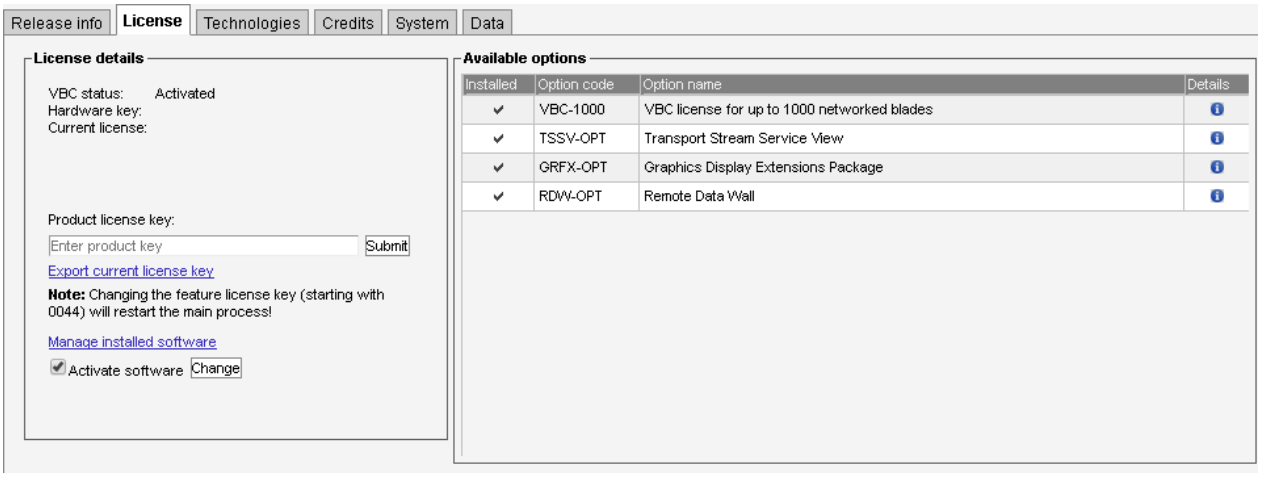
[4] https://doxfer.webmin.com/Webmin/Network_Configuration

5.27 Main — About

5.27.1 About — Release info

This view shows the software version, the software build date and the version of the underlying operating system for the VideoBRIDGE Controller.

5.27.2 About — License



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** and **Graphic Display Extensions Package** options are available. By clicking the blue information icon associated with each option it is possible to view option details.

The VideoBRIDGE Controller supports two different licensing schemes, on-line licenses and classic licenses. When using a classic license, a product license key is tied to the hardware key, which is the shorter of the two keys presented, in a non-transferrable manner. The license is installed once, and can also be exported in XML format from this page. This key can be imported using Software Activation, see chapter 2.4 for details.

When using an on-line license, the key is verified periodically towards a license server. The key is transferrable between systems running the same software, but only as long as on-line verification is supported. The longer system identifier is used to identify the system. The **Current license** field will display information on when the license key was last verified. 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.

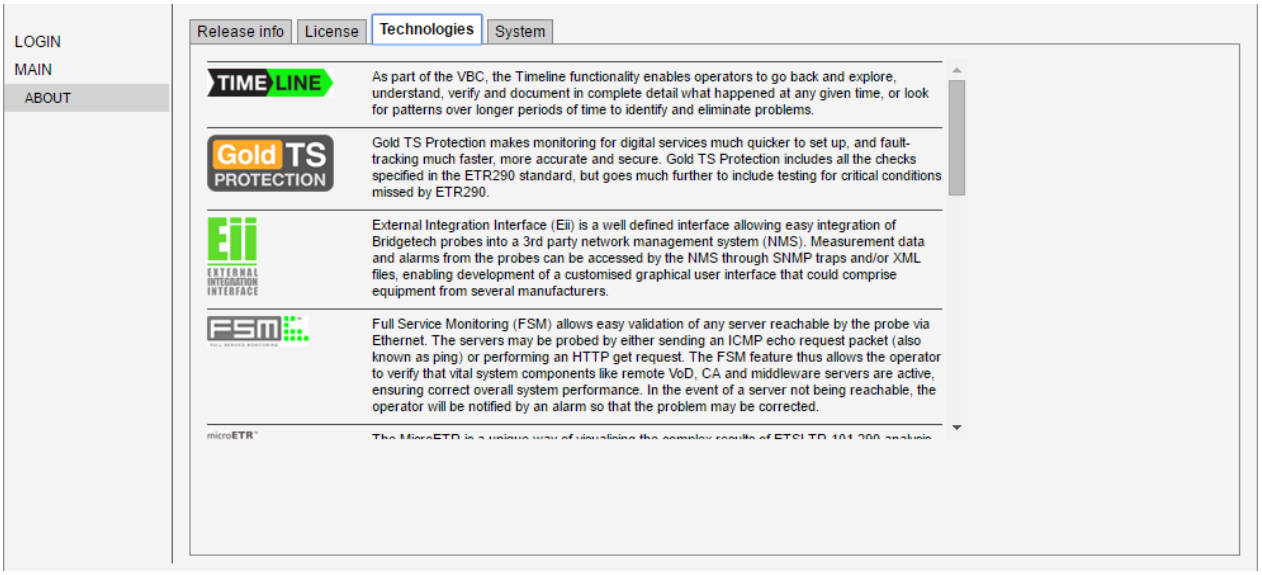
Please refer to I Appendix: On-line License Verification for more information on how to use on-line licenses. This appendix also describes how to renew the license when the VideoBRIDGE Controller cannot connect to the Internet.

Click the **Manage installed software** link to access the Software Activation interface, see chapter 2.4 for more information.

To disable the VideoBRIDGE 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 Software

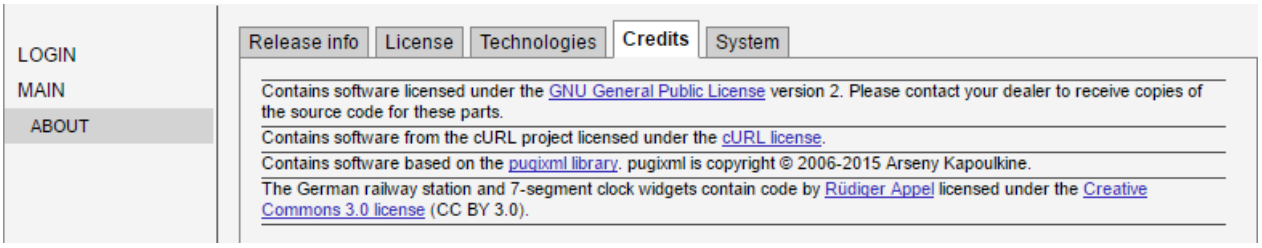
Activation interface (which is done by default the first time you activate the software), you will need to change the default back to **Software Activation** before disabling VideoBRIDGE Controller. See chapter 2.11 for more details.

5.27.3 About — Technologies



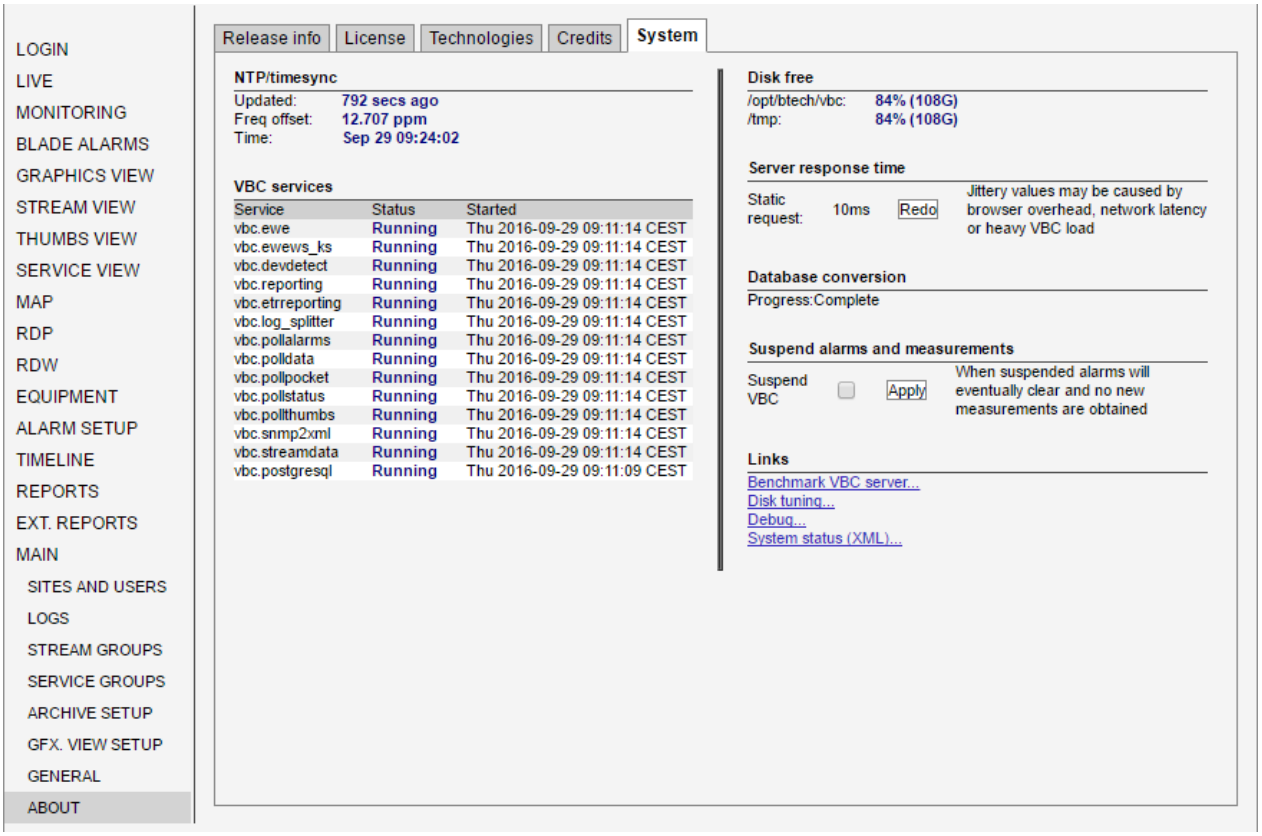
The **Technologies** view lists some of the technologies available in the Sencore VideoBRIDGE product family.

5.27.4 About — Credits



This view shows information about the software included with the VideoBRIDGE Controller.

5.27.5 About — System



The **System** view displays a snapshot of the current status of the system, to ensure correct VideoBRIDGE 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 M Appendix: Enabling NTP time synchronization for more details.

We recommend using the standard operating system tools for configuring the system clock. Please refer to the operating system instructions[5] for further details on how to configure the date and time.

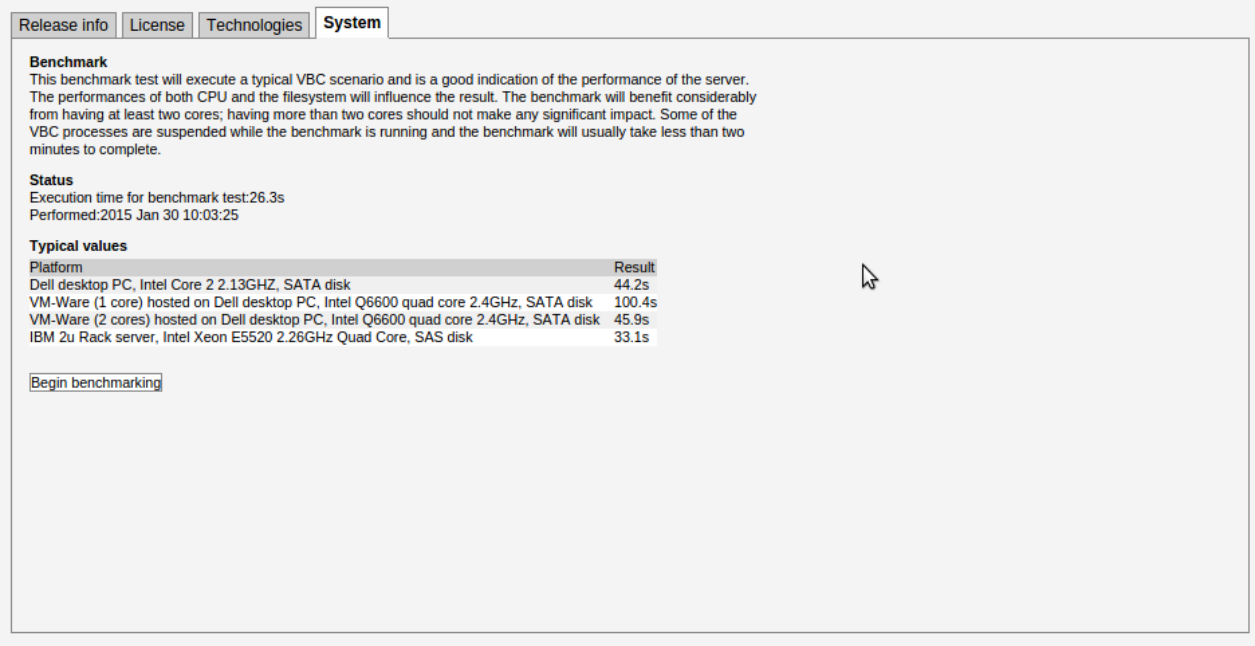
The **VBC services** overview displays the VBC services that are required. All the VBC services listed should have status *Running*. More information about the different services can be found in C Appendix: The VBC System Services.

Disk free displays free disk space to give the user some overview of disk resources available.

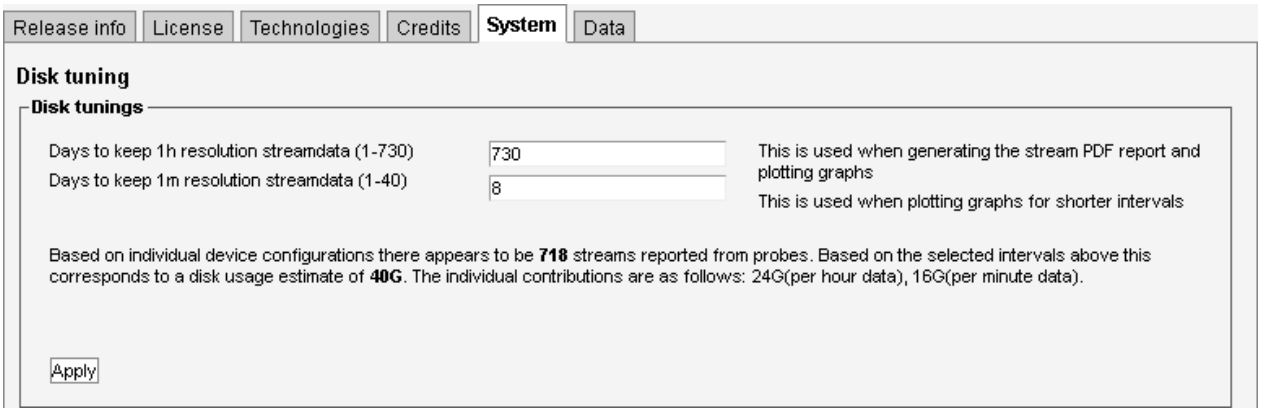
[5] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System_Administrators_Guide/chap-Configuring_the_Date_and_Time.html

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.

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.



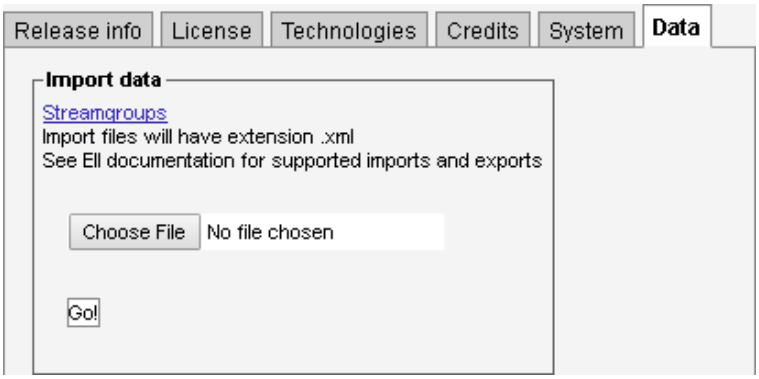
Clicking the **Disk tuning...** link in the **About — System** page allows the user to configure for how long data should be stored on the disk. Storing data for long periods means that a large amount of disk space is required. Estimated disk usage is calculated based on the current configuration, and numbers are rounded to the nearest MB.



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.

5.27.6 About — Data



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.

A Appendix: Separate Probe and Network Interfaces

The VideoBRIDGE 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.

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 VideoBRIDGE Controller application are located in the `/opt/btech/vbc` folder. This table summarizes important files and folders.

Disk location	*Description*
/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 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:

Log file	*Limitation*	*Description*
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 VideoBRIDGE Controller application consists of a number of Linux system services:

Service	*Description*
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 5.16
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 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 5.15
snmp2xml	Generates the XML document available via the alarms_exp.xml page
streamdata	Collects probe data for generating stream based reports
postgresql	The freely available PostgreSQL application that implements the relational database used by the VBC processes
licenseproxy	The freely available Tinyproxy application is used to allow blades to contact the on-line licensing service through the VBC server, so that they do not have to have direct Internet access; see I Appendix: On-line License Verification 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

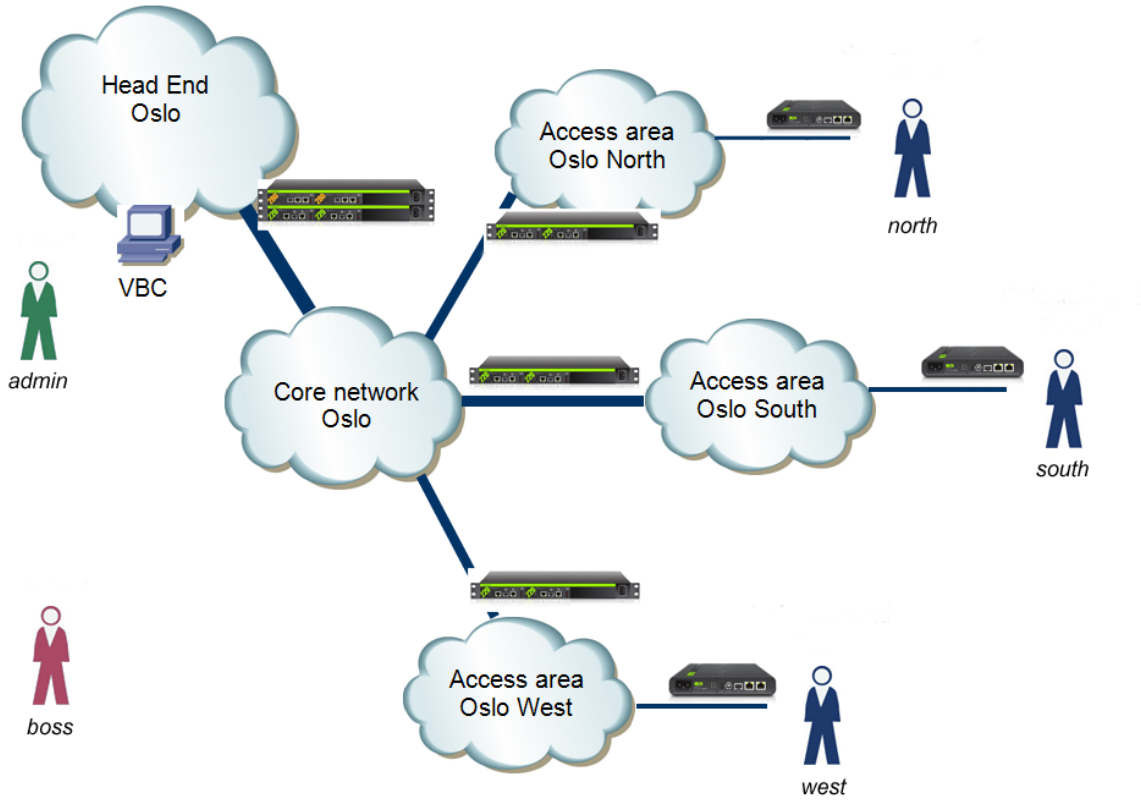
command **vbchello** can be used to verify that all the necessary services are running, and their status is also available from the **Main — About — System** view.

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:

Site	*Device name*	*Blade*	*USER admin*	*USER north*	*USER south*	*USER west*	*USER boss*
HeadEnd	HE probe 1	VB220	Full	r/o	r/o	r/o	r/o
	HE probe 2	VB220					
	HE content	VB7880					
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 VideoBRIDGE 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:

Error	*Default threshold value*
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.** menu and select appropriate values
3. Edit the stream in the probe's **Multicasts — Streams** menu and associate the stream with the new threshold template
4. Use the VBC's **Equipment** menu 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

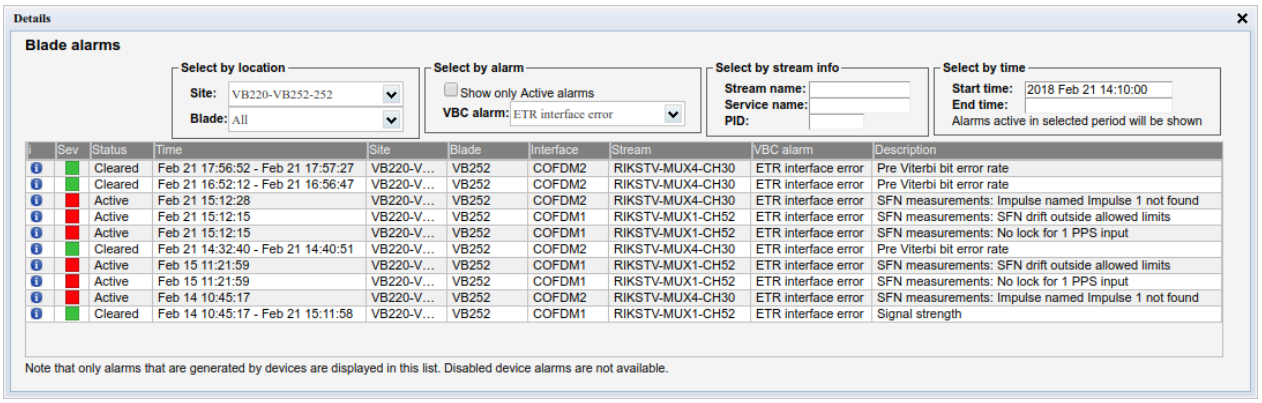
The Probe alarms are independent of the VideoBRIDGE Controller alarms. The Probe has been designed to yield instantaneous alarms based on the current measurements. This typically results in lots of short-lived alarms that would be “too much” for the VBC to report, as the VBC may control a large number 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 VB7880 Advanced 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 M 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 VB7880 Advanced Content Extractor) alarms are available in the VBC’s **Blade alarms** view.



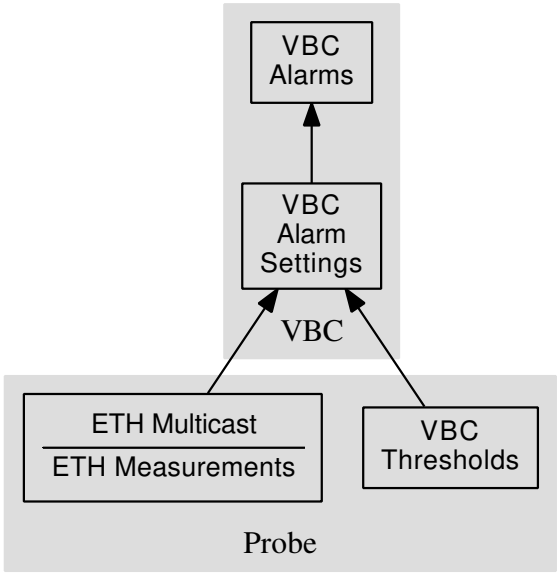


Figure F.1: VBC alarming based on Probe measurements

G Appendix: Troubleshooting

Please also see chapter 2.5 Initial Setup Troubleshooting.

Multiple browser windows towards the VBC

The VideoBRIDGE 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.

Please read the README.txt file that is part of the VBC software release for further troubleshooting.

H Appendix: Backing up the VBC

We strongly recommend backing up the VBC files before upgrading to a new version of the VideoBRIDGE 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 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.

H.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.

H.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`).

H.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
```

H.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 script (extension **.run**), by running it and selecting the "**E**xtract script" option. The **vbc_copy** script will be extracted to the home folder, i.e. the `/root` folder if running it as the root user.

If you have the **.tea** file, you first need to extract the upgrade script and invoke it by using the following commands. Replace **vbc.tea** with the actual filename of the downloaded file:

```
/opt/btech/vbc/bin/tengff -e vbc.tea -f vbc_release.sh -kvbc
bash vbc_release.sh
```

I Appendix: On-line License Verification

I.1 Introduction

The VideoBRIDGE Controller uses licenses which are verified 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 VideoBRIDGE Controller sends the on-license verification over the Internet, it includes some basic information to verify the VideoBRIDGE Controller. This includes a basic hardware footprint, as well as parts of the SNMP identification data configured in the **Main — General — Connections** view.

I.2 Requirements

Direct access to verification server

To be able to verify the on-line license, the VBC needs to be configured with a valid DNS server address (see K 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 (outgoing only).

If the VBC is configured in such a way that it is unable to perform this, it can be configured to use a proxy server as described below. If proxy connectivity also is not available, an off-line verification procedure is available as well, as described below.

Using an arbitrary proxy server

The VideoBRIDGE 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.

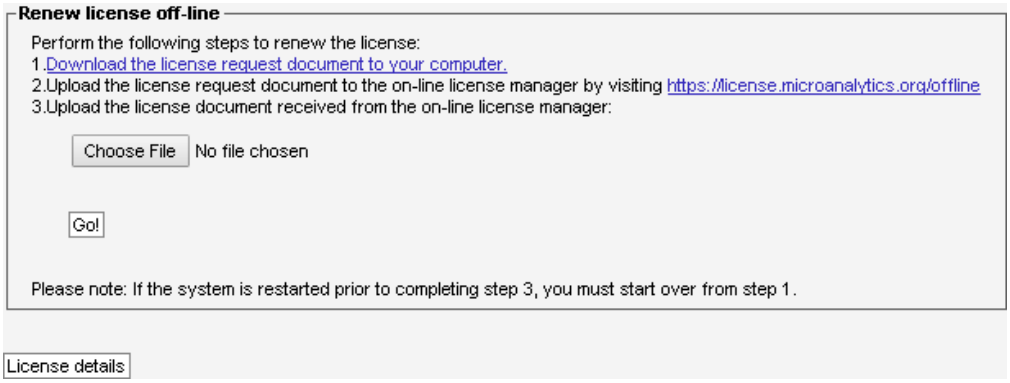
When installing the VBC software to a server, an instance of the Tinyproxy[1] software is automatically installed and configured to allow its connected blades to connect to (and only to) the licensing system as described in the previous section.

To configure Tinyproxy to, in turn, connect to an upstream proxy, edit the file `/etc/tinyproxy/vbc.conf` and see the instructions included in the file. When done, save the file and restart the service by typing **systemctl restart vbc.licenseproxy**

As long as the connected blades are configured with the address of this system in their **Setup — VBC** view, no further configuration should then be necessary for them to verify licenses.

Off-line verification procedure

If the network is completely disconnected from the Internet, it is still possible to verify the license using the off-line verification procedure. When using this, the license will be tied to the system and will not be transferable to another server. Click the **Renew license off-line** button to start the off-line verification procedure.

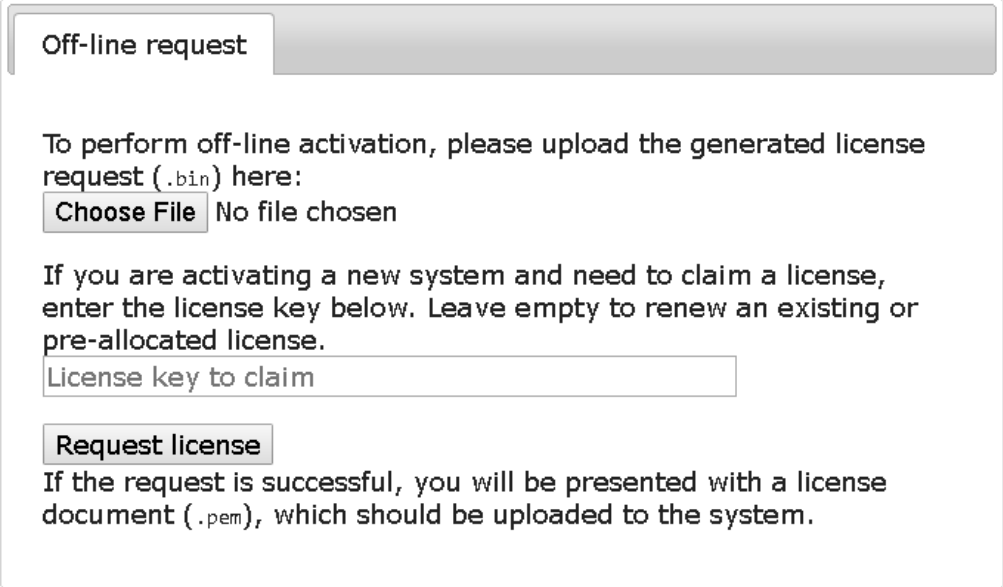


Follow the steps described in the dialog to renew or activate the license. To abort the procedure, click the **License details** button to return to the previous screen.

First, download the license request document from the VideoBRIDGE 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 manager[2].

[1] `https://tinyproxy.github.io/`

[2] `https://license.microanalytics.org/offline`



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.

J Appendix: Software Maintenance

Purchasing yearly software maintenance enables future feature protection and guarantees access to the latest software for Sencore VideoBRIDGE equipment.

The software maintenance can be purchased for a two or four 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 5.12.

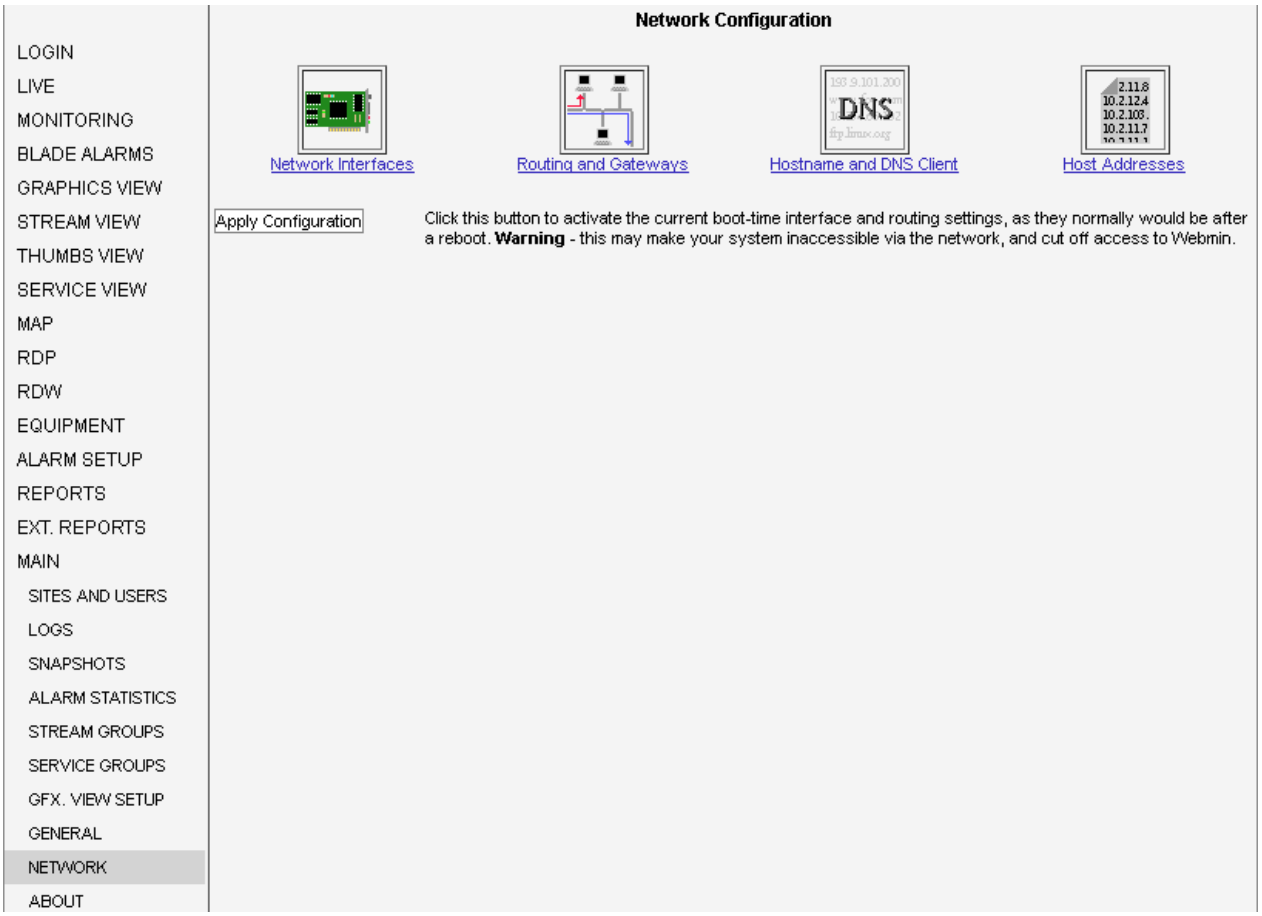
Use the **Equipment — Device software** view to update the software on monitored blades, please refer to chapter 5.12.4.

K Appendix: Network configuration

K.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 K.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 **Main — Network** view.



The web-based network configuration tool is based on WebMin. Further documentation is available in the WebMin documentation[1].

[1] https://doxfer.webmin.com/Webmin/Network_Configuration

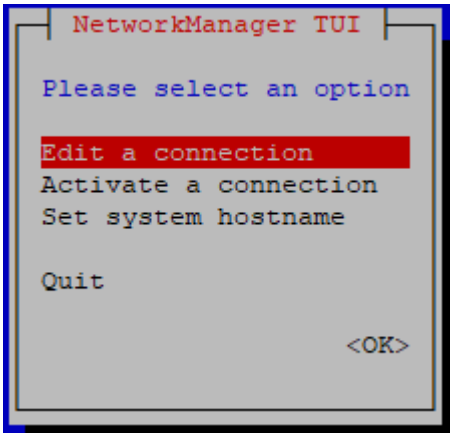
Another alternative is to install the Cockpit web-based interface, which can be used to configure most aspects of the system, including the network settings. Packages for Cockpit are available in the base CentOS/Red Hat Enterprise Linux distribution. For more information on how to install and use Cockpit, please refer to Getting Started With Cockpit[2].

K.2 Command-line based configuration

Changes to network configuration, adding new interface devices and VLANs can be done with the **nmtui** tool. Simply type **nmtui** whilst logged into the server command shell as root[3]. Navigate the nmtui menus using the cursor (arrow) keys and Enter to select. More documentation on using **nmtui** can be found in the Networking Guide[4].

Editing Network interface configuration

To edit a connection first select **Edit a connection** from the nmtui menu:

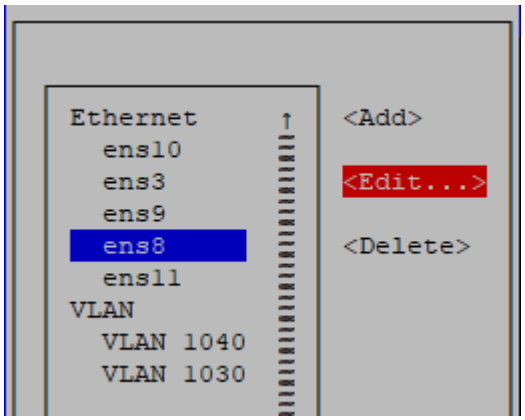


Select the interface to be edited and then select **Edit...** from the menu.

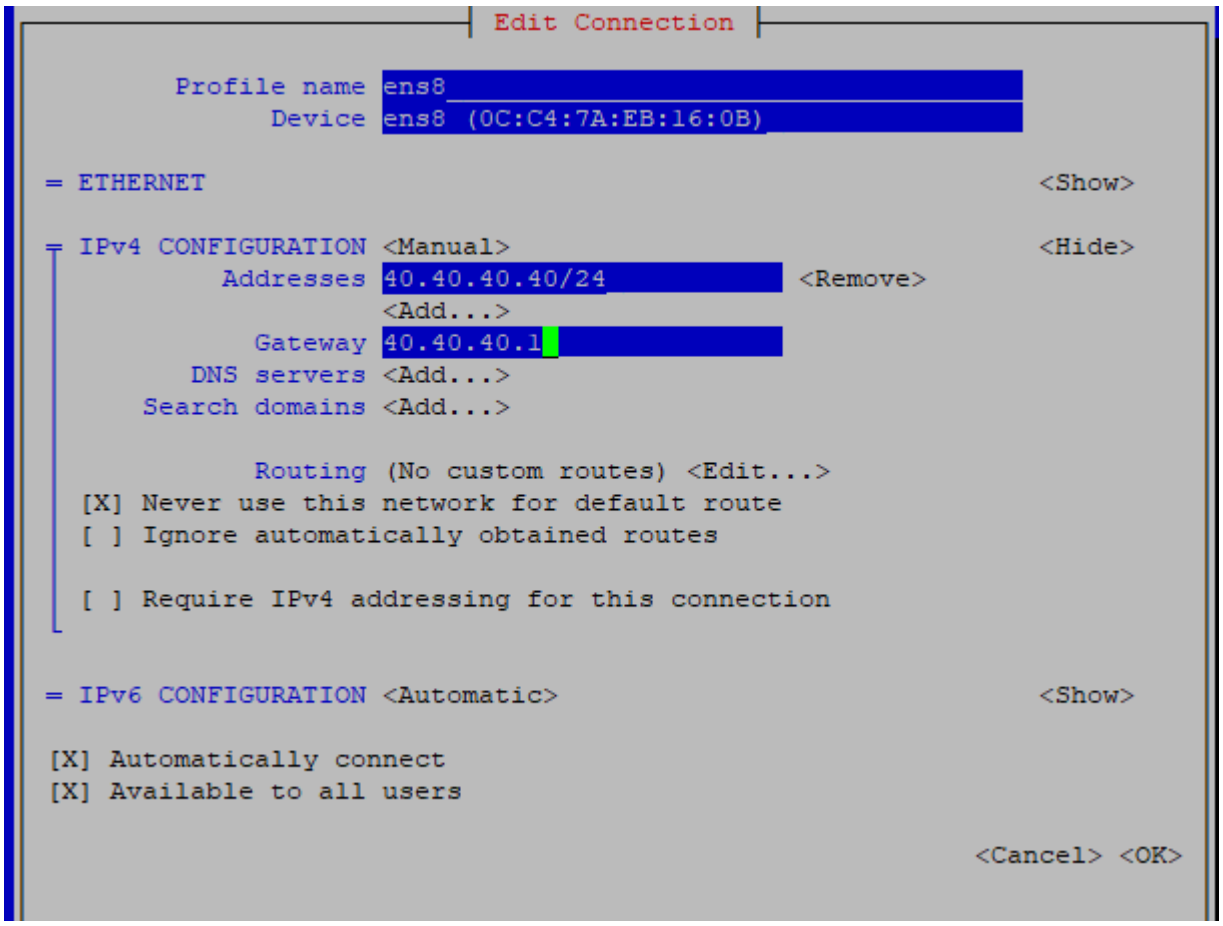
[2] https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/getting_started_with_cockpit/

[3] If the **nmtui** tool is not available on your system, you can install it by issuing the command **yum install NetworkManager-tui**

[4] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Networking_Guide/sec-Networking_Config_Using_nmtui.html



Make the necessary changes to IPv4 and IPv6 configuration.



Selecting **Automatically connect** will ensure the interface is connected next time the system boots.

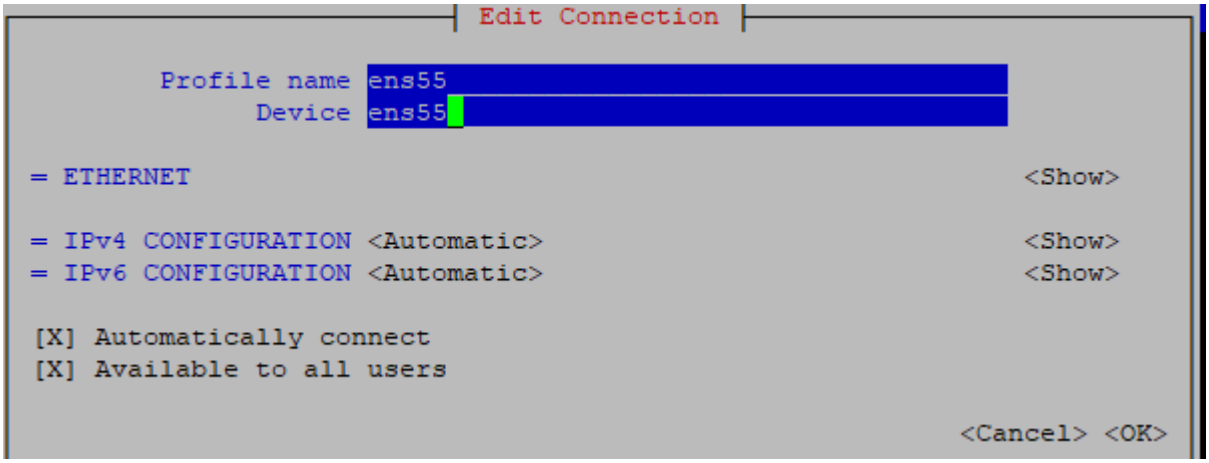
Sometimes it is desirable to select **Never use this interface for default route**, particularly if additional interfaces are only used for monitoring multicast traffic or when setting up a native interface for adding VLANs.

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**.

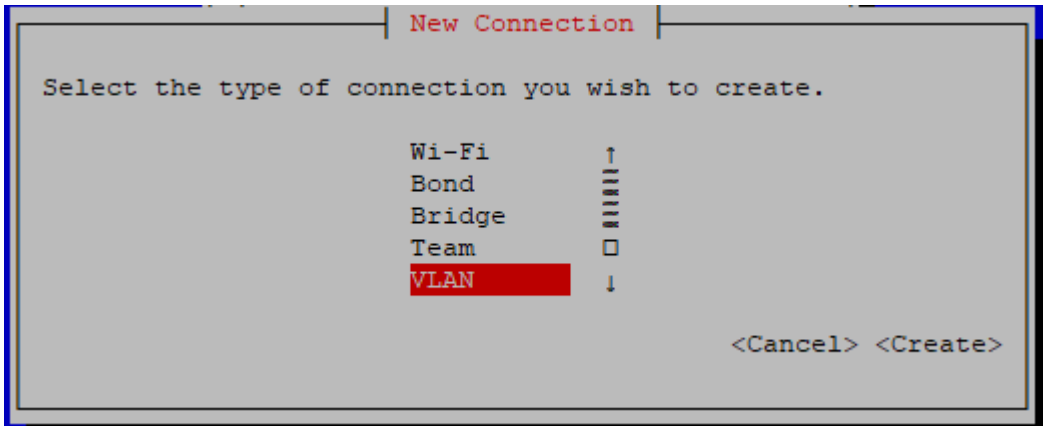
Adding new and VLAN interfaces

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.

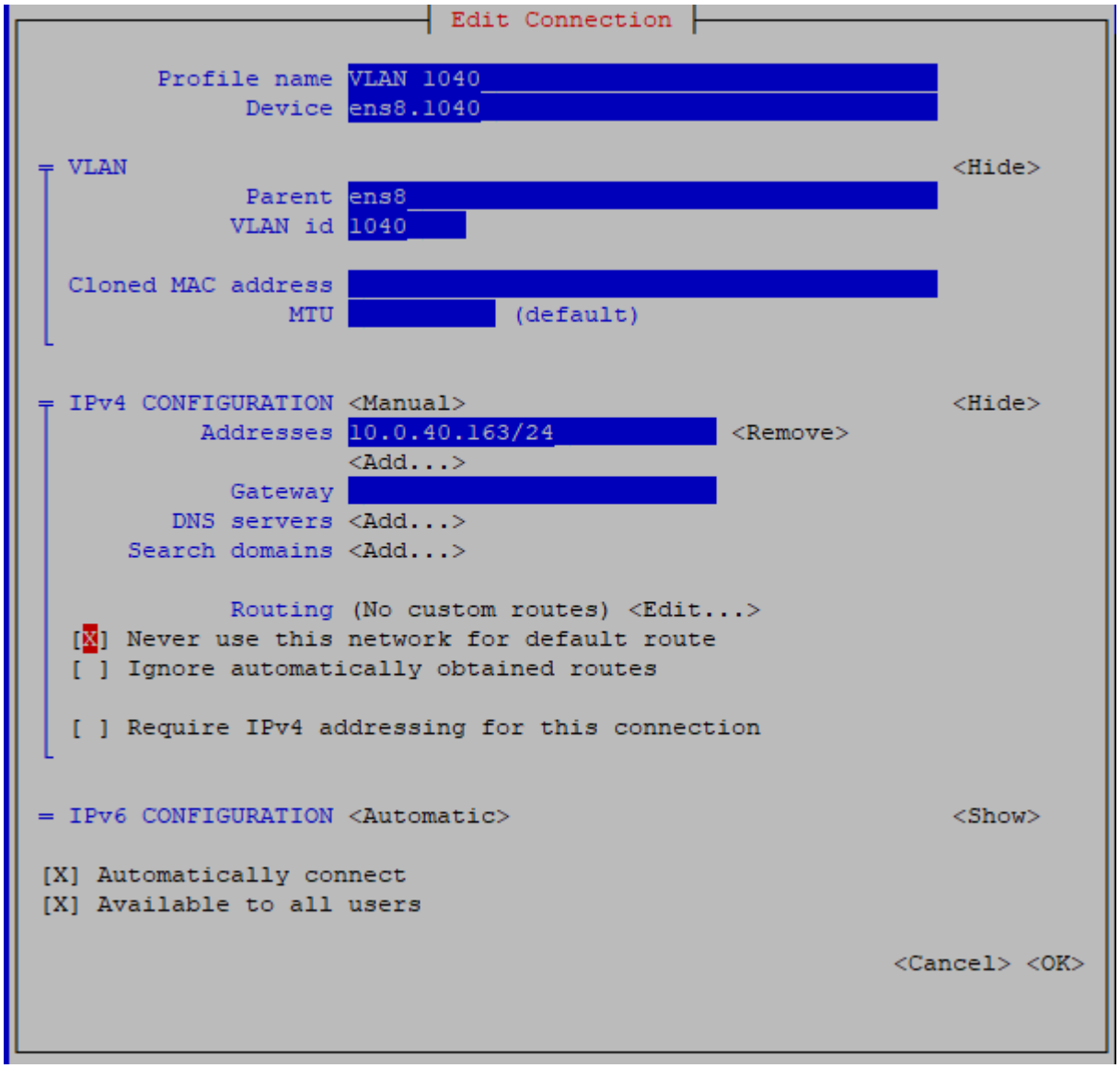
To find the system assigned name for a newly added hardware device use the command line **ifconfig** or search in the output of the **dmesg** tool. It can be helpful to keep the nmtui **Profile name** for the device the same as the device name itself, for example:



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:



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.



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.

L Appendix: Enabling HTTPS

By default, all web communication to and from the host running the VideoBRIDGE Controller is using un-encrypted HTTP communication. To enable HTTPS, the installed Apache server software needs to be configured appropriately.

The guide below is based on the guide from the CentOS Wiki[1]. To install packages, generate keys and update the Apache configuration, you will need to be root so you can either **su** to root or use **sudo** in front of the commands below.

If the system is available on a publicly visible host name, you can use EFF's Certbot to deploy a Let's Encrypt certificate. Please see the section **Using Certbot with Let's Encrypt** below.

> Installing packages requires an active Internet connection. If you are using Red Hat Enterprise Linux, you will need an active subscription to install packages.

Getting the required software

To enable SSL on Apache, you will need to install the `mod_ssl` package, if not installed already. To install the package, issue the following command:

```
yum install mod_ssl
```

Generating a certificate

If you have an internal certificate authority, use that to create a certificate. Otherwise follow the steps below to generate a self-signed certificate. Please note that modern browsers display a warning message when connecting to a web server running a self-signed certificate. This message can usually be suppressed by installing the certificate in the browser.

First generate a private key, which we call **ca.key**:

```
openssl genrsa -out ca.key 2048
```

Second, create a certificate signing request (CSR) in **ca.csr**:

```
openssl req -new -key ca.key -out ca.csr
```

[1] `https://wiki.centos.org/HowTos/Https`

Third, we self-sign the key:

```
openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt
```

We now have the necessary files, but we need to copy them to the correct locations in the file system:

```
cp ca.crt /etc/pki/tls/certs
cp ca.key /etc/pki/tls/private/ca.key
cp ca.csr /etc/pki/tls/private/ca.csr
```

Configuring the web server

The Apache SSL configuration file, **/etc/httpd/conf.d/ssl.conf**, needs to be updated to make use of the generated certificate. Open it using a text editor, for example:

```
vi +/SSLCertificateFile /etc/httpd/conf.d/ssl.conf
```

Change the paths to match where the Key file (**ca.crt**) and Certificate Key (**ca.key**) are stored. If you've used the method above, the configuration should be:

```
SSLCertificateFile /etc/pki/tls/certs/ca.crt
SSLCertificateKeyFile /etc/pki/tls/private/ca.key
```

We also need to forward the configuration from the HTTP host to the HTTPS host. This is done by adding the following line anywhere in the `VirtualHost` declaration in the **ssl.conf** file, you can for instance add this next to the lines above:

```
RewriteOptions Inherit
```

Quit and save the file and then restart Apache by issuing the command

```
systemctl restart httpd
```

All being well you should now be able to connect to the system using HTTPS. If there was an error, the command output should give you some hints on where to look.

Disabling HTTP access

To configure the server to redirect any access arriving over HTTP to the HTTPS server, the simplest way is to create the file `/etc/httpd/conf.d/001-http-to-https.conf`[2]:

```
cat <<'EOM' > /etc/httpd/conf.d/001-http-to-https.conf
RewriteEngine On
RewriteCond %{HTTPS} !=on
RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R,L]
EOM
```

After creating the file, restart Apache by issuing the command

```
systemctl restart httpd
```

If this does not work, please consult the Apache documentation or the Apache Wiki[3]. It is also possible to completely disable the HTTP port, if it is not needed.

Using Certbot with Let's Encrypt

If the system is available on a publicly visible host name, you can use EFF's Certbot to deploy a Let's Encrypt certificate. Some preparations are needed before running Certbot.

To enable SSL on Apache, you will need to install the `mod_ssl` package, if not installed already. To install the package, issue the following command:

```
yum install mod_ssl
```

Next, we need to configure Apache *VirtualHost* configurations for HTTP and HTTPS. The HTTPS one is configured in the Apache SSL configuration file, **/etc/httpd/conf.d/ssl.conf**, and needs to be updated slightly:

Open it using a text editor, for example:

```
vi +/VirtualHost /etc/httpd/conf.d/ssl.conf
```

Add the following line after the `<VirtualHost _default_:443>` line:

[2] `https://wiki.apache.org/httpd/RewriteHTTPToHTTPS`
[3] `https://wiki.apache.org/httpd/RedirectSSL`

```
RewriteOptions Inherit
```

Finally, we need to create a VirtualHost for the HTTP part, this one is kept simple and can be created by issuing the following command:

```
cat <<'EOM' > /etc/httpd/conf.d/002-http-virtualhost.conf
<VirtualHost _default_:80>
RewriteOptions Inherit
</VirtualHost>
EOM
```

Now the configuration should be ready for adding the Let's Encrypt certificate. Please follow the Certbot guide[4] for information on how to do that.

[4] https://certbot.eff.org/lets-encrypt/centosrhel7-apache

M 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 VideoBRIDGE Controller will also itself act as NTP server. Setting the VBC IP address in the **Setup — VBC** view in the probe or VB7880 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 configuring the date and time settings, please refer to the System Administrator's Guide, chapters *Configuring the Date and Time*[1] and *Using chrony*[2].

[1] `https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System_Administrators_Guide/chap-Configuring_the_Date_and_Time.html`

[2] `https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/sect-using_chrony`