Remote Portal Guide

inside.Docupedia Export

Author: Froehle Nikolas (ST/SRM2-EU)

Date: 15-Feb-2018 13:11

Table of Contents

1 Overview

1.1 Introduction

The Remote Portal is part of Bosch's Cloud-based Services and supports plug-and-play remote access and services via the cloud. Services are provided via the Remote Portal's browser interfaces or as part of domain-specific applications or solutions.

Below is a short overview of features and services provided by the Remote Portal. More details can be found in the respective sections of this documentation.

1.2 Getting started

Registration at the Remote Portal and use of Remote Portal features are free of charge. For typical use one account should be created per company. Managing additional users and controlling access is then done using Remote Portal features described below.

Some services described below may require licenses for activation.

1.3 Supported devices

Remote Portal supports the following devices:

Device type	Devices
Fire alarm system	FPA-5000
Intrusion alarm system	B- and G-series
Video system	DIVAR IP 2000 DIVAR IP 5000 DIVAR hybrid DIVAR network IP cameras

1.4 Remote Portal features

1.4.1 System hierarchy

Remote Portal allows freely grouping systems and nesting groups of groups. This allows to define a hierarchy for devices, e.g. by customer or installation location, limit access for a set of devices or aggregate status of multiple devices.

1.4.2 User and access management

Remote Portal allow fine-grained control to the portal and access to devices and services by means of additional users and association of these users with systems, groups of systems and services.

1.4.3 Health monitoring

The Remote Portal provides various health checks on devices registered to the portal, including status of connection device-cloud and device functionality. The Remote Alert services allow sending notifications to one or more users when health issues arise.

1.5 Services

1.5.1 Remote Connect

Remote Connect allows connecting devices to the Remote Portal and is required for access via client software or use of further services.

With the exception of DIVAR network or hybrid devices the connection can be established without network configuration on site (see system requirements for details). DIVAR network and hybrid provide limited support for Remote Connect and require local network configuration as detailed in the device's manual.

Licensing of Remote Connect varies by product, see licensing for details.

1.5.2 Remote Alert

Remote Alert monitors system health and allows sending of notifications (SMS, E-mail) to users based on various triggers.

Remote Alert is available as part of Remote Connect service.

1.5.3 Remote Maintenance

Remote Maintenance assists in performing maintenance tasks on compatible devices and systems. Remote Maintenance is currently available for FPA-5000, for additional details please also visit http://www.boschsecurity.com/remoteservice-fire/.

Remote Maintenance is available as part of the Fire Remote Service license bundle, for details see licenses.

1.5.4 Camera Counter Reports

Camera Counter Reports are available on IP cameras capable of essential or intelligent video analytics connected directly to the Remote Portal. Camera Counter Reports poll counters from one or more cameras and store their values for up to 30 days.

The stored data can be visualized in the Remote Portal or exports as CSV data for further processing.

Camera Counter Reports are licensed with a 1-year license, see licensing for details.

2 System requirements

2.1 Browsers

The browser-based interfaces of Remote Portal are best viewed with a modern browser such as Firefox, Chrome or Internet Explorer. JavaScript must be enabled.

2.2 Device firmware support

To utilize all features and services of the Remote Portal the following firmware versions (or later) are recommended:

Fire Alarm System		Intrusion System		Video System	
Device	**Min. firmware**	**Device**	**Min. firmware**	**Device**	**Min. firmware**
FPA-5000	2.14	B-/G-Series	3.02	DIVAR IP 5000 (2000)	3.60.0051
Security Gateway	1.00			DIVAR hyrid, DIVAR network	1.00
				IP cameras	6.40

2.3 Client software

Compatible client software can establish device connections using Remote Portal credentials and via Internet. Local access to devices remains unaffected. The following client software versions (or later) are recommended.

Fire Alarm System		Intrusion Alarm System		Video System		
Client	**Min. version**	**Client**	**Min. version**	**Client**	**Version**	**Device Support**
RPS (FSP-5000-RPS)	4.8	RPS	6.02	Web-interface (direct access via Remote Portal)	Up-to-date version of: ▪ Firefox ▪ Google Chrome ▪ Microsoft Internet Explorer The Bosch Video SDK for configuring VCA can be used with Internet Explorer 11 and Firefox ESR 45.8 or later.	• DIVAR IP 2000 • DIVAR IP 5000 • IP cameras
		RSC (iOS, Android)	2.7	Video Security Client (1)	1.5.0.13	• DIVAR IP 5000 (2000)
				Video Security App (1)	2.1.1	• DIVAR IP 5000 (2000)
				To connect using Remote Portal Video System clients must have access to ports 443 and 42090.		

(1) Compatibility update for IP cameras planned 2017

2.4 Internet connection

Use of Remote Portal services requires the following Internet access for devices:

Fire Alarm System		Intrusion Alarm System		Video System	
Device	**Network requirements**	**Device**	**Network requirements**	**Device**	**Network requirements**
FPA-5000	• Connection to security gateway • Local IP via DHCP or static assignment • Access to public Internet on port 443.	B-/G-Series	• Local IP via DHCP or static assignment • Access to public Internet on port 443.	DIVAR IP 5000 (2000)	• Local IP via DHCP or static assignment • Access to public Internet on port 443. • Use of video functionality requires access to port 42000.
Security Gateway	• Local IP via DHCP or static assignment • Access to public Internet on port 443.			DIVAR hyrid, DIVAR network	• Fixed IP on network • Port forwarding according to manual • Public IPv4 address
				IP cameras	• Local IP via DHCP or static assignment • Access to public Internet on port 443. • Access to the Certificate Revocation List under http://36.mcg.escrypt.com/crl on port 80 • Use of video functionality requires access to ports 42000.
					Bandwidth of the Internet connection must be sufficient to support video streaming. Video streams should be configured to a bitrate suitable for the available bandwidth.

3 Portal guide

3.1 System hierarchy

3.1.1 Overview

To facilitate management of larger number of systems and allow fine-grained access control to these systems the Remote Portal provides a simple but powerful grouping mechanism. Grouping can be done by administrators of the account and provides the following functionality explained in greater detail below:

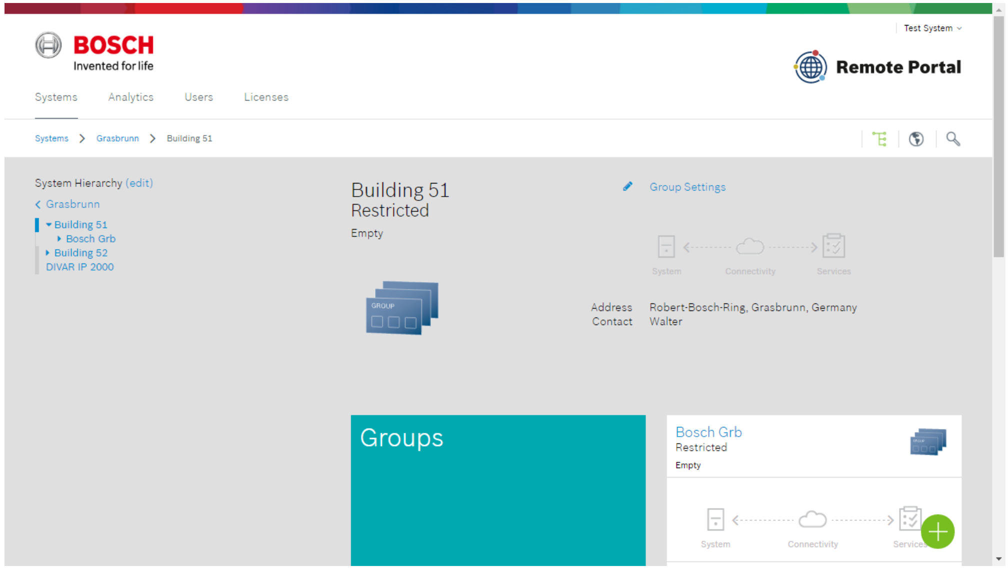
- Defining a system hierarchy
- Limiting access to groups and systems
- Aggregating status information of contained systems and groups

System hierarchy

The system hierarchy of the Remote Portal allows systems and groups to reside either at the top level of the hiearchy or nested in one or more groups below. There is no limit to the the depth of the nesting or combination of elements at any level.

The Remote Portal displays the hierarchy as a tree structure (giving access to the whole hierarchy, shown on left of screen) and by displaying the system and group cards of the current level on the right-hand side of the screen. Use the tree to navigate to any group or level of the hierarchy and cards to drill down in the hierarchy from current level.

> The tree display can be toggled by clicking on the tree symbol in the navigation toolbar above the main content area.



Address Robert-Bosch-Ring, Grasbrunn, Germany
Contact Walter

The system hierarchy can be edited by selecting "edit" in the tree navigation area. This function is available to administrators of the portal only.

With edit mode active elements of the tree can be rearranged in the existing group hierarchy. New groups can be added for a selected level by selecting the green "+" button and providing basic information for this group. This information can be updated by selecting "Group settings" at any later point in time.

Access control

By default any system within the Remote Portal can be accessed by administrators or technicians via browser or programming software. Access for customers must be granted explicitly.

Customizing technician access

Technician access can be customized by system or for a set of systems by adding a "Technician" account to a system or group respectively. This also automatically removes unrestricted access to these systems and groups. Unlimited access is restored again when all technicians are removed from a system and group.

For details on the permissions technician access grants see the users section of this document.

Granting access

Adding a technician to a group grants access to all systems of this group **and** the systems of any nested group. Access rights accumulate from top to bottom of the hierarchy, explained by this example:

```
Group 1 - Technician A, B
        System 1-1
        System 1-2

        Group 2 - Technician C
                System 2-1
                System 2-2 - Technician D
```

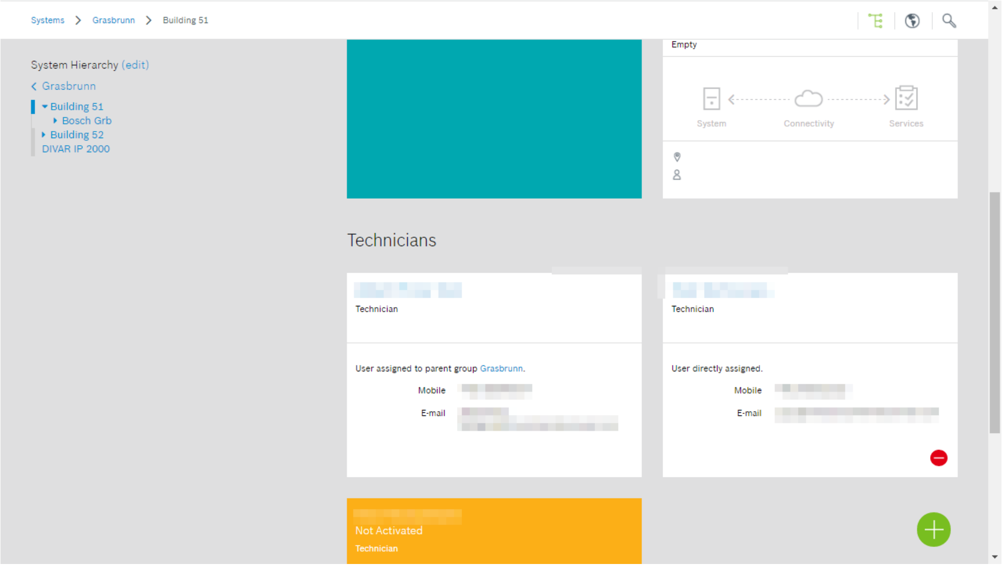
For this example technicians A and B can access systems 1-1, 1-2, 2-1 and 2-2, whereas technician C can only access systems 2-1 and 2-2 and technician D only systems 2-2.

Resulting access rights are shown at every level, as an example system 2-2 would all technicians having access, matching the example's configuration.

Removing access

Removal of access can be only be done at the highest level that a particular technician has access. In the example, access for technician A would need to be removed at group 1's level, though the technician is also shown in lower levels. Removal of access, where applicable, is shown via a red "-" button.

> Removal of the last "Technician" account at a particular level will reinstate unrestricted access of all technicians.



Systems > Grasbrunn > Building 51

System Hierarchy (edit)

< Grasbrunn

- Building 51
  - Bosch Grb
- Building 52
- DIVAR IP 2000

Empty

Technicians

[redacted]
Technician

User assigned to parent group Grasbrunn.

Mobile [redacted]

E-mail [redacted]

[redacted]
Technician

User directly assigned.

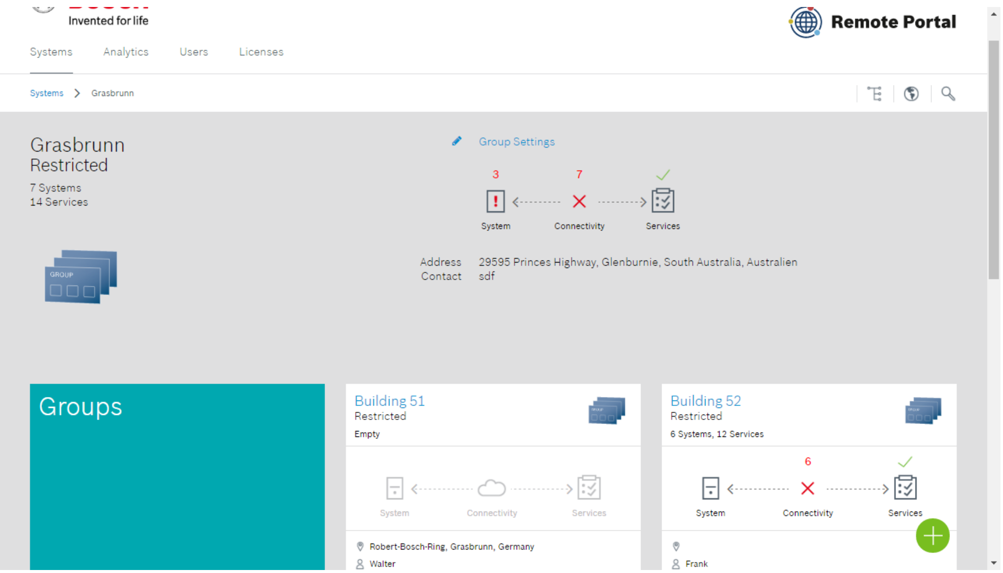
Mobile [redacted]

E-mail [redacted]

[redacted]
Not Activated
Technician

Status aggregation

Nesting systems in a group hierarchy leads to aggregation of status information of all the systems within a group, independent of nesting level. A group always displays the aggregate status of all systems (in particular system health, connectivity status or service status), with trouble states "bubbling" up to the top of group and displayed using the status icons. This provides a quick way to verify health of a large number of systems contained in a group and in case of error drilling down to affected systems by clicking through cards displaying active trouble states.



Grasbrunn
Restricted
7 Systems
14 Services

Address 29595 Princes Highway, Glenburnie, South Australia, Australien
Contact sdf

Building 51
Restricted
Empty
Robert-Bosch-Ring, Grasbrunn, Germany
Walter

Building 52
Restricted
6 Systems, 12 Services
Frank

3.2 Users

3.2.1 Users

Overview

The Remote Portal provides three different user types with which you can control access and use of portal and connected devices.

Administrators

"Administrators" accounts have full access to all features of the portal. Typically there will be only a select number of administrators to perform tasks such as adding new users, activating services or changing access rights on systems.

Technicians

"Technicians" account are used to perform tasks such as adding new devices, performing remote configuration or system maintenance. Technicians will use the Remote Portal and client software such as RPS.

Customers

"Customers" are typically accounts created for end customers. Customers typically will use client software, such as the video security app, to connect and use devices or can be created as users which receive notifications via SMS and Email.

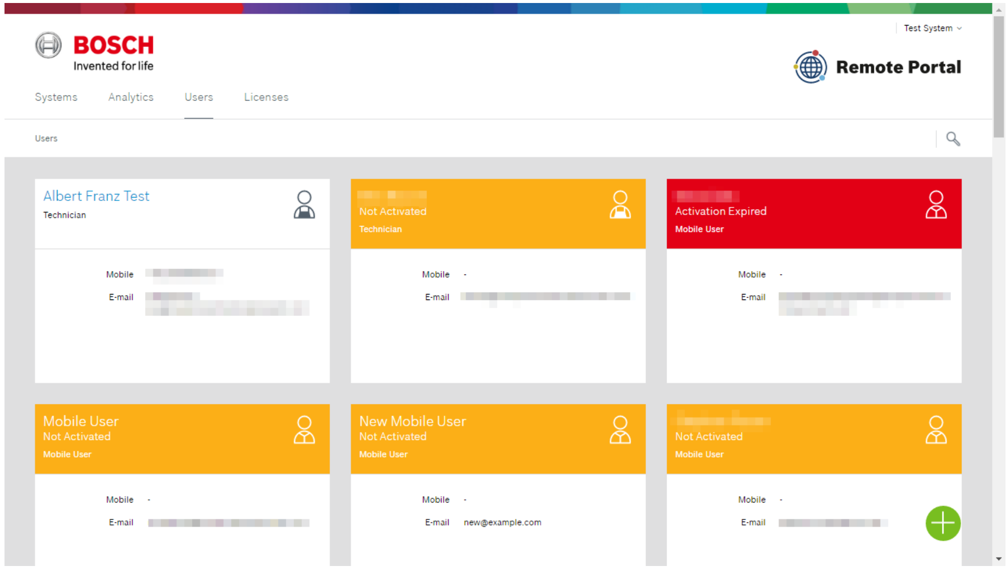
Are more detailed comparison of the different users can be found in the table below:

User type	Portal use	Device use			Service use
		Video System	Intrusion Alarm System	Fire Alarm System	
Administator	• Log into portal, change account data, reset password. • Add / remove additional users. • View device lists. • Manage licenses.	• Add / remove devices to account. • Configure camera counter reports • Use mobile apps to connect to DIVAR.	• Use RPS to claim panels (via Cloud ID) and perform remote configuration. • List panels.	- Use RPS to connect to all panels registered in account.	• All services
Technician	• Reset password at Remote Portal • Log in for service configuration and use	• Add devices to account (using device wizard / configuration) • Configure counters in report • Add / remove customers to report	• Use RPS to claim panels (via Cloud ID) and perform remote configuration	- Use RPS to connect to panels granted access registered in account.	(After access granted by administrator) • "Remote Connect" for configuration purposes • "Remote Maintenance" to perform service tasks

Customer	• Reset password at Remote Portal • Log in for camera counter reports and viewers.	• Use mobile apps to connect to DIVAR. • View camera counter reports • Configure viewers	• Use RSC app via cloud connection (requires access profile installed on device).			• Camera counter reports • Viewers
All users		• Use connect... URL ("Permalink") with device password.				• "Remote Alert" – Receive status notifications via email and SMS

Managing users

Users are managed by selecting the "Users" tab from the top navigation bar. From there you can add, edit and remove user accounts and get an overview of a user's access to systems and services.



Albert Franz Test
Technician
Mobile [redacted]
E-mail [redacted]

[redacted]
Not Activated
Technician
Mobile -
E-mail [redacted]

[redacted]
Activation Expired
Mobile User
Mobile -
E-mail [redacted]

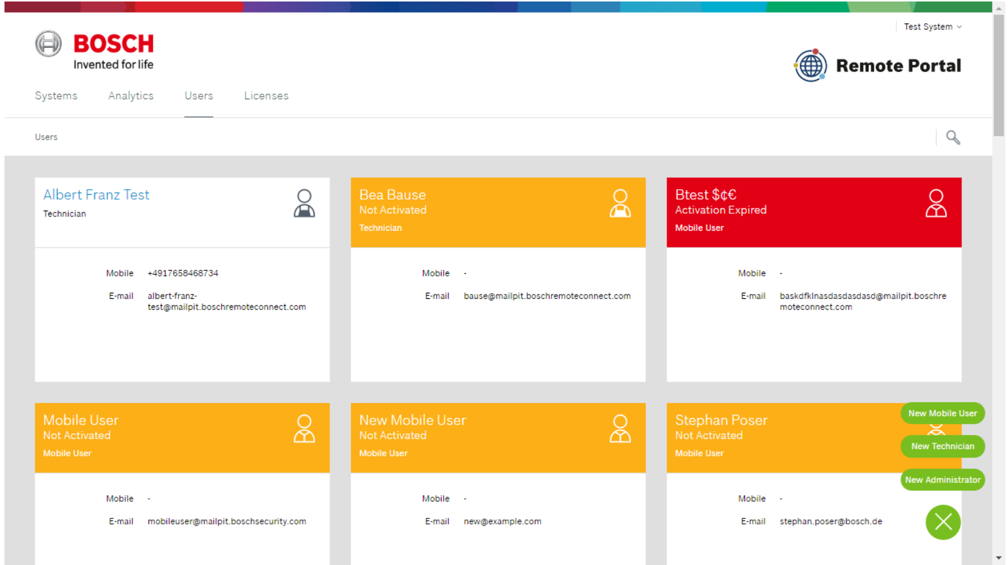
Mobile User
Not Activated
Mobile User
Mobile -
E-mail [redacted]

New Mobile User
Not Activated
Mobile User
Mobile -
E-mail new@example.com

[redacted]
Not Activated
Mobile User
Mobile -
E-mail [redacted]

Adding users

To add users select the "Users" tab in the top navigation bar, select the green "+" button and choose the type of user you wish to add. See the table above for an explanation of user types.



Albert Franz Test
Technician
Mobile +4917658468734
E-mail albert-franz-test@mailpit.boschremoteconnect.com

Bea Bause
Not Activated
Technician
Mobile -
E-mail bause@mailpit.boschremoteconnect.com

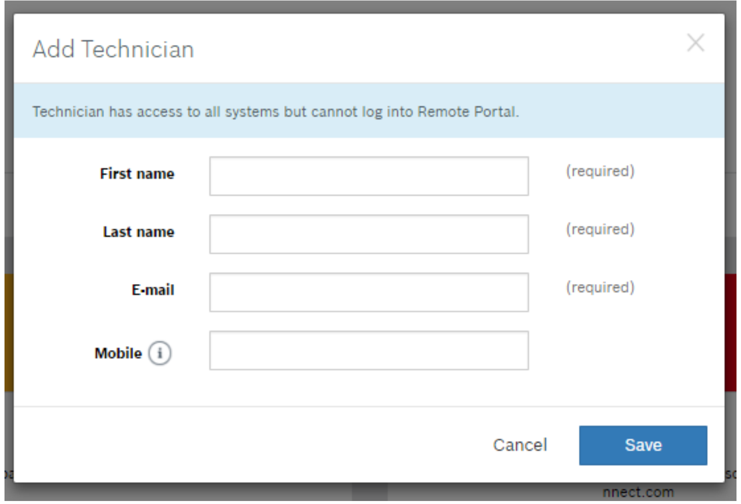
Btest $¢€
Activation Expired
Mobile User
Mobile -
E-mail baskdfklnasdasdasdasd@mailpit.boschremoteconnect.com

Mobile User
Not Activated
Mobile User
Mobile -
E-mail mobileuser@mailpit.boschsecurity.com

New Mobile User
Not Activated
Mobile User
Mobile -
E-mail new@example.com

Stephan Poser
Not Activated
Mobile User
Mobile -
E-mail stephan.poser@bosch.de

Provide a basic set of information for the user you are creating and click "Save":

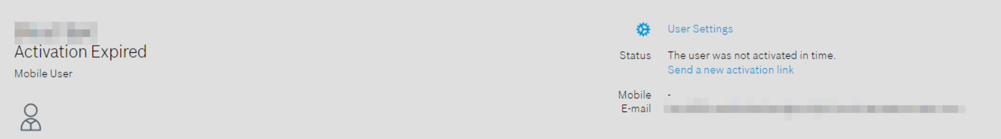


Add Technician

Technician has access to all systems but cannot log into Remote Portal.

First name		(required)
Last name		(required)
E-mail		(required)
Mobile ⓘ		

Newly created users receive an automated email from the system to confirm email address and set a custom password. Until this step has been taken by the user the user is in "Not activated" state and is highlight in yellow on the Users overview page. The activation link is valid for ten days, if a user does not confirm the email address within that time frame the link will expire and the the user is shown highlighted in red. You can request a new link to be sent for this user by clicking on the user's card and from there clicking on "Send a new activation link".



[redacted]

Activation Expired

Mobile User

User Settings

Status The user was not activated in time.
Send a new activation link

Mobile -
E-mail [redacted]

Until a user's email is verified the user cannot login to the Remote Portal. However a user's account can be seen and, for example, assigned to devices.

Editing users

User information (name, email address and mobile phone number) can be edited by selecting a user's card and clicking on "User Settings".

> Changing email address is done immediately and may disrupt existing logins from client software, e.g. RPS

Deleting users

Users can be deleted by selecting the user's card and clicking on "User Settings". Select "Delete" and confirm by selecting "Delete" again.

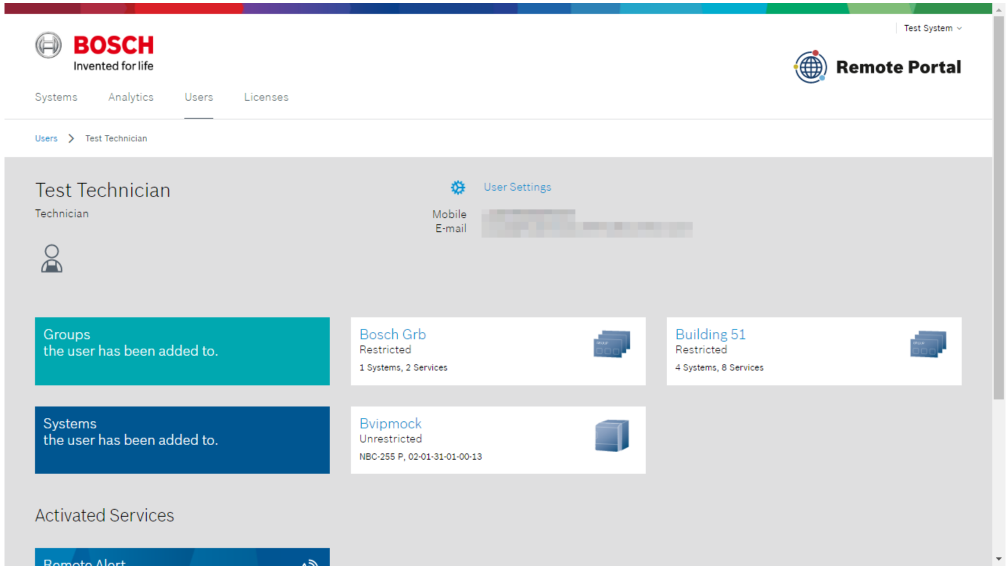
Deleted users are deleted immediately and cannot be recovered. Any access to devices or the portal associated with this user is revoked immediately.

Reviewing access to systems and services

Select a user's card to review access to systems and services.

Groups and Systems

The groups and systems section shows all groups and systems to which a user has been granted access. To modify access rights, select the respective group or system and remove the user from there.



Test Technician
Technician

User Settings
Mobile [redacted]
E-mail

Groups
the user has been added to.

Bosch Grb
Restricted
1 Systems, 2 Services

Building 51
Restricted
4 Systems, 8 Services

Systems
the user has been added to.

Bvipmock
Unrestricted
NBC-255 P, 02-01-31-01-00-13

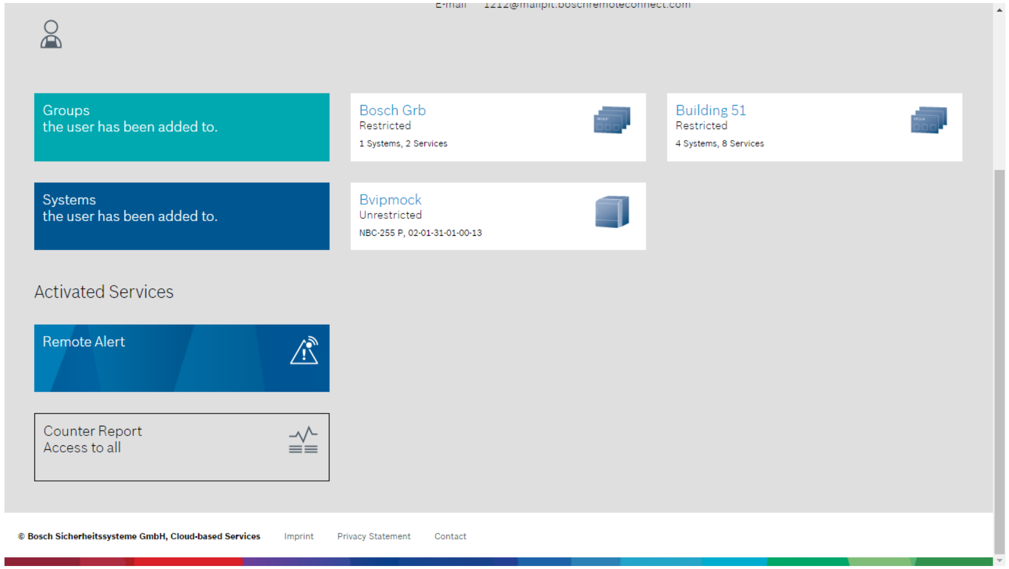
Activated Services

Remote Alert

Services

The services section lists all services that a user has access to and can utilize. To manage, as with Systems and Groups, click on the respective service and edit the user's settings as desired.

> Access to services is tied to access to a system. As an example a technician granted access use of "Remote Maintenance" service may also use the "Remote Connect" service. Verify the right user type is used grant only desired access rights to a system.



E-mail 1212@mailpit.boschremoteconnect.com

Groups
the user has been added to.

Bosch Grb
Restricted
1 Systems, 2 Services

Building 51
Restricted
4 Systems, 8 Services

Systems
the user has been added to.

Bvipmock
Unrestricted
NBC-255 P, 02-01-31-01-00-13

Activated Services

Remote Alert

Counter Report
Access to all

© Bosch Sicherheitssysteme GmbH, Cloud-based Services

3.3 Licenses

3.3.1 Overview

The table gives a high-level overview of functionality available without licenses vs. services requiring licenses and activation:

Domain	Device	Service	Licensing
Fire	FPA-5000	Remote Services Bundle: Remote Connect, Remote Maintenance, Remote Alert	Purchases of 1 year license via CTN First year included with purchases of security gateway.
Intrusion	B-/G-Series	Remote Connect	As part of intrusion installer services, sign-up at https://installerservices.boschsecurity.com/
Video	DIVAR hybrid / network	Remote Connect	Included with device purchase
	DIVAR IP 5000 (2000)	Remote Connect, Remote Alert	Included with device purchase
	IP cameras	Remote Connect, Remote Alert, Camera Viewers	Purchase of 1 year license
		Camera counter reports	Purchase of 1 year license

Ordering licenses

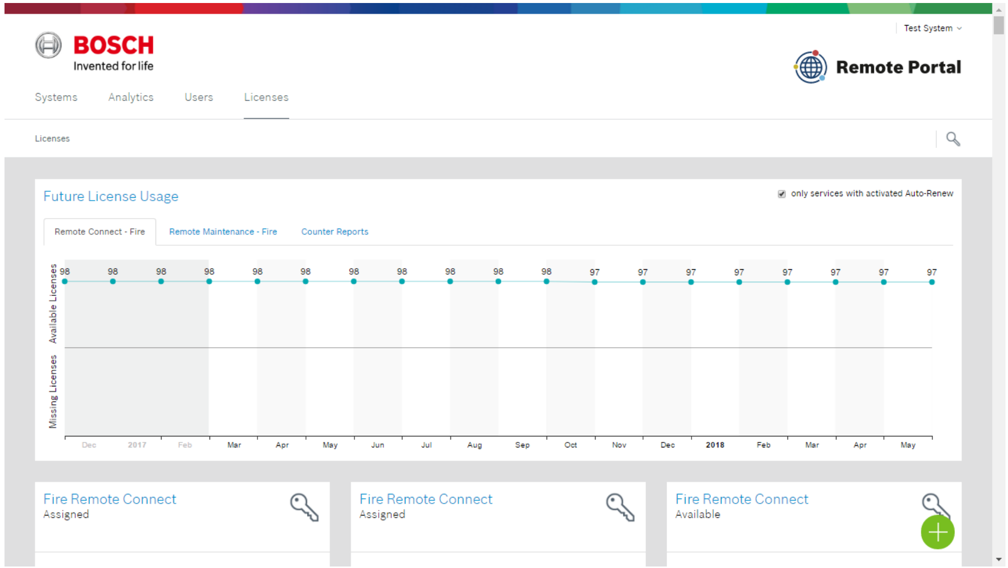
Dedicated licenses are ordered via a standard sales order to Bosch. Once order processing is completed a 16-digit license key is returned to the purchasing contact via email for each license order. This example shows an order of the FPA-5000 Remote Services license bundle licenses:

> *Dear customer,*
> *please follow the steps below to add your recently purchased licenses to your account:*
> *1. Log into your account at https://remote.boschsecurity.com*
> *2. Click the "Licenses" tab in the top bar.*
> *3. Click the "Add Licenses" button.*
> *4. Copy and paste the entire license information between the dashed lines to the browser dialog box and click "Add".*
> *----- license information (begin) -----*

> *Fire panel remote services bundle:*
> *1234: 1111-2222-3333-4444*
> *1235: 2222-3333-4444-5555*
> *1236: 3333-4444-5555-6666*
> *----- license information (end) -----*
>
> *Thank you for using Remote Services.*
> *Regards,*
> *Bosch Security Systems*

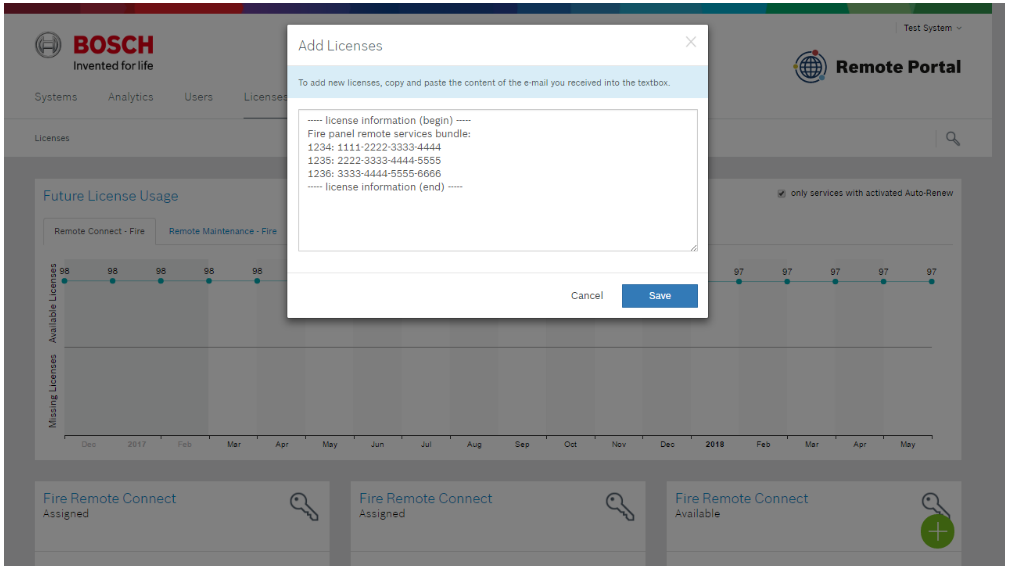
Adding licenses

Licenses must be added to a Remote Portal account before being ready for use. This is done by selecting the "License" tab, which is available for any administrator logged into the Remote Portal:



To add licenses to the active account select the green "+" button and copy and paste the license information provided into the presented dialog.

Note: The Remote Portal intelligently parses out licenses information from the information entered in the dialog, it is not necessary to apply special formatting or remove extra text. Multiple license codes can be added at once.



Add Licenses

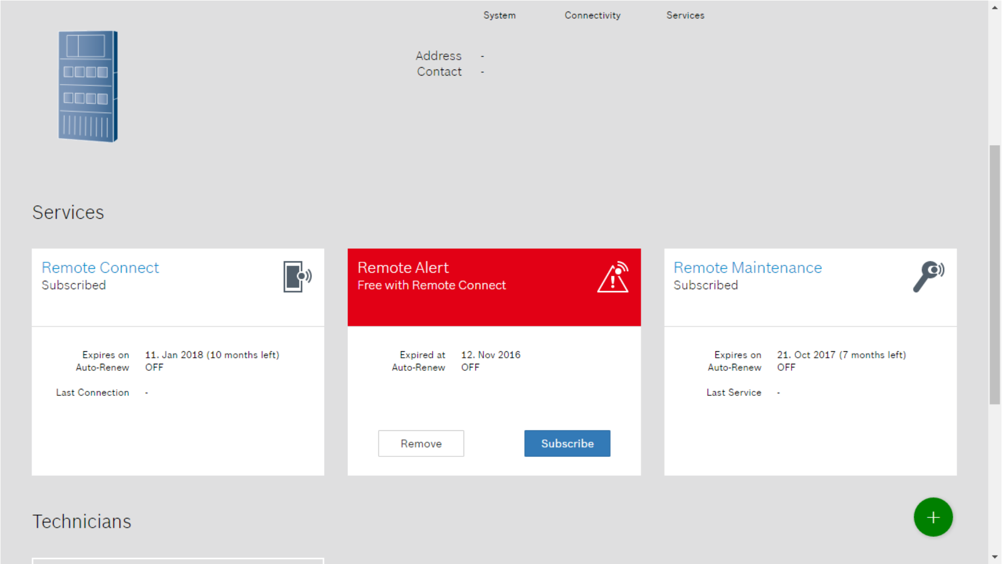
To add new licenses, copy and paste the content of the e-mail you received into the textbox.

```
----- license information (begin) -----
Fire panel remote services bundle:
1234: 1111-2222-3333-4444
1235: 2222-3333-4444-5555
1236: 3333-4444-5555-6666
----- license information (end) -----
```

Licenses added are saved in the Remote Portal for use, but only consumed when the corresponding is activated (manually or via auto-renewal). This allows having a stock of licenses in the Remote Portal for immediate use, without inactive licenses expiring inadvertently.

Using licenses / activating services

Subscribing to a service on device checks for availability of a suitable license in the Remote Portal account and converts if from an available license to a license subscribed to a device. License are assigned at random from stock available, a particular license's assignment can be checked from the license.



Address -
Contact -

Services

Remote Connect
Subscribed

Expires on 11. Jan 2018 (10 months left)
Auto-Renew OFF

Last Connection -

Remote Alert
Free with Remote Connect

Expired at 12. Nov 2016
Auto-Renew OFF

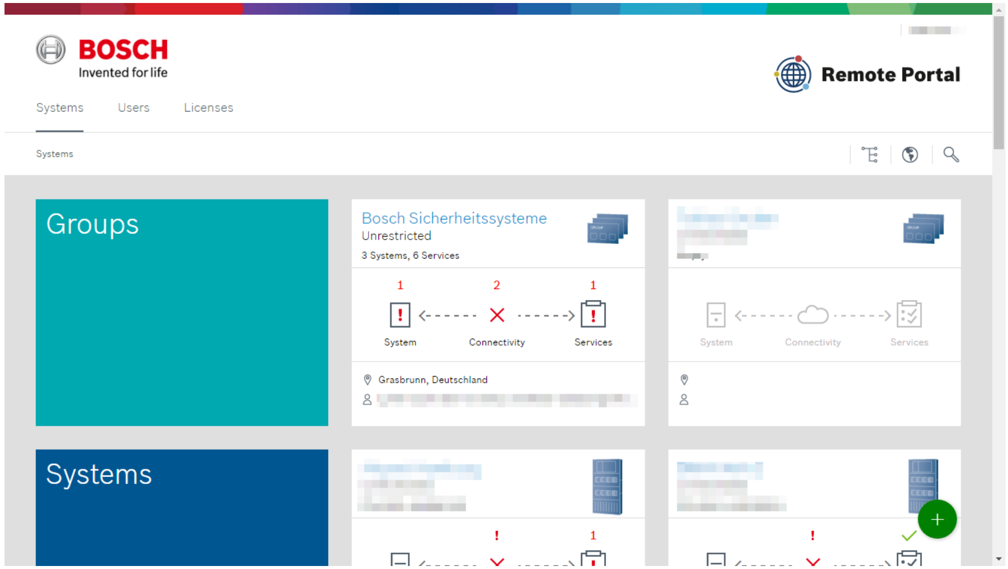
Remote Maintenance
Subscribed

Expires on 21. Oct 2017 (7 months left)
Auto-Renew OFF

Last Service -

Technicians

Remaining life-time of a license assigned to a service is shown in the sevice section of a device. Once the license expires the service is no longer available for use. License expiration is highlight in red in a device's service section and the systems overview screen at the services icon:

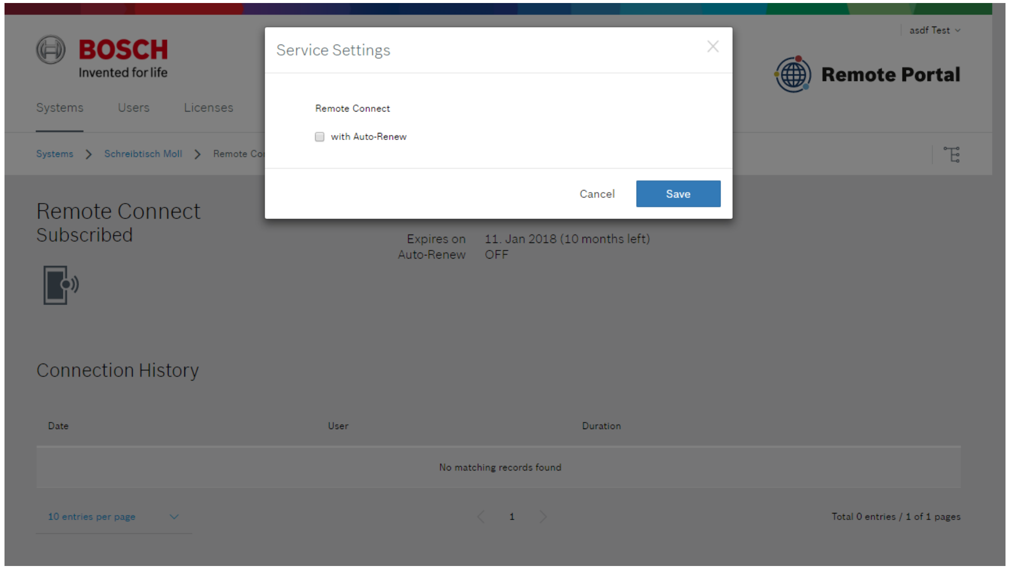


Bosch Sicherheitssysteme
Unrestricted
3 Systems, 6 Services

Grasbrunn, Deutschland

Auto-renewal

For convenience and to avoid service interruptions, services can be configured to auto-renew upon expiry. This can be done at time of service subscription or the service settings screen for a particular service:



Service Settings

Remote Connect

☐ with Auto-Renew

Remote Connect
Subscribed

Expires on 11. Jan 2018 (10 months left)
Auto-Renew OFF

Connection History

Date	User	Duration
No matching records found		

Total 0 entries / 1 of 1 pages

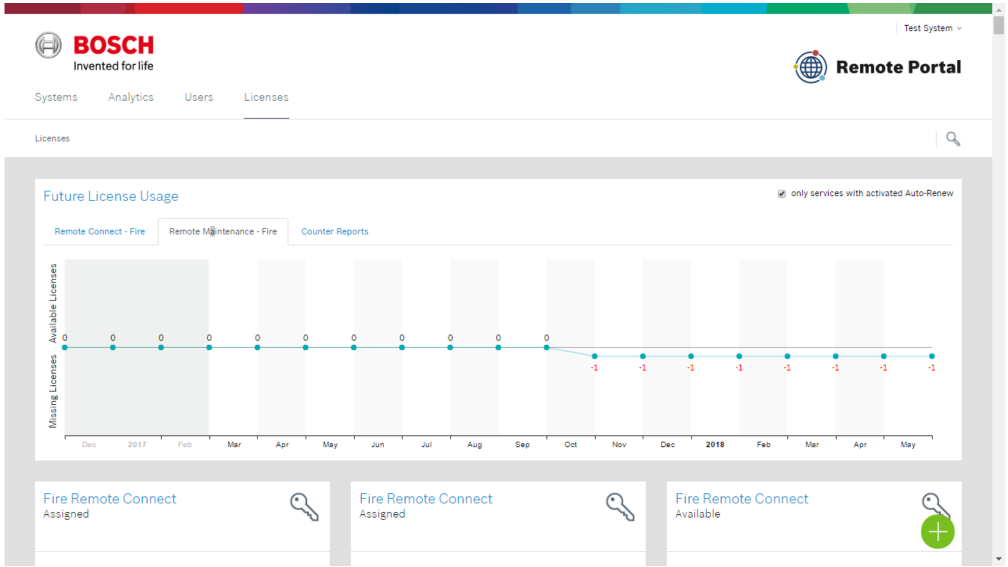
Auto-renewal requires a license to be available when renewal is due, otherwise renewal fails. Use the license management feature to plan for your license needs at regular intervals.

Managing licenses

The licenses tab provides the following information and actions to manage licenses:

Future License Usage

At the top of the screen current and predicted license usage is displayed, broken down by service / license type:



Based on the number of device subscribed, remaining lifetime of subscription and auto-renewal of service subscriptions the Remote Portal predicts when additional service licenses are needed, marking the estimated demand of licenses in red. Note that this estimation will change when additional devices are subscribed to a service.

Individual license status and maintenance

Individual licenses are shown below the license usage section of the screen and provide information on each purchased license:

- Status: available, assigned, expired
- For assigned licenses: Validity and assigned system

License that have not been assigned to a system yet (are in available state) can be removed from an account by clicking the trashcan symbol of the license. This allows you to transfer licenses to another account or make licenses unavailable for use.

License deletion is immediate and permanent. You must copy and save the license key presented in the warning dialog for later use.

4 Service guide

4.1 Remote Connect

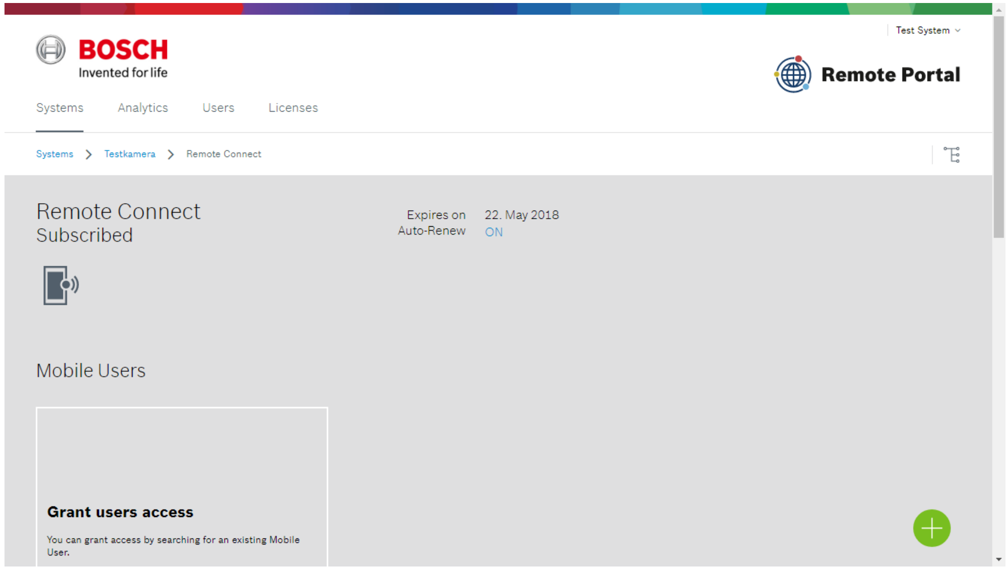
4.1.1 General

Remote Connect is the basic connectivity service provided by the Remote Portal which establishes a connection between system and cloud. Connection status of connected systems is automatically monitored and displayed in the system hierarchy. Additional information specific to systems is provided in later sections.

4.1.2 Customer access

Connections using client software can be managed by adding "Customer" account to the Remote Connect service of a system. Customers can access devices using client software or via the Remote Portal (in scope limited to viewing of e.g. camera counter reports).

To add a "Customer" account navigate to the Remote Connect service page of a system and select the green "+" button.



Remote Connect
Subscribed

Expires on 22. May 2018
Auto-Renew ON

Mobile Users

Grant users access

You can grant access by searching for an existing Mobile User.

Technician access is managed by means of the System hierarchy.

4.1.3 Additional services

Activation of additional services it outlined in the service description in later sections.

4.1.4 B-/G-series

Connection

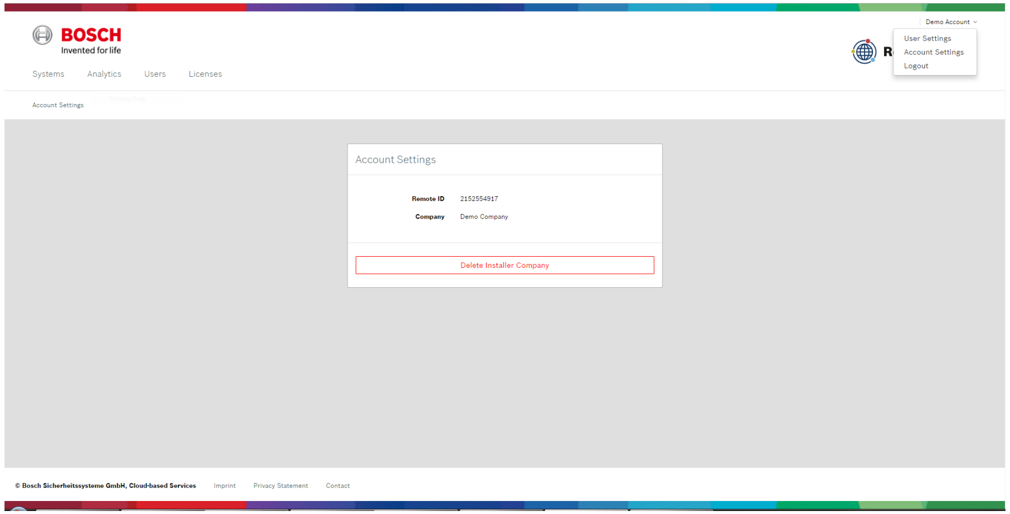
B-/G series panels automatically establish a secure connection to the Remote Portal (when cloud connection is enabled in the settings menu). To register a panel with a Remote Portal account the panel must be activated from RPS by use of its "Cloud ID". The cloud ID is provided in barcode and readable form as a sticker on the panel. To utilize cloud connection with these devices you must sign up with Bosch's installer services at https://installerservices.boschsecurity.com.

4.1.5 FPA-5000

Connection

FPA-5000 requires installation of a security gateway on-site which is configured to automatically establish a secure connection to the Remote Portal. The FPA-5000 must then be registered with a specific Remote Portal account by storing the account's Remote Portal ID in the panel.

The Remote Portal account's ID can be retrieved by logging into the account with an "Administrator"'s account and selecting "Account Settings" from the user account:



Account Settings

Remote ID 2152554917

Company Demo Company

Detailed configuration instructions are provided in the FPA-5000 manual.

Remote access

Administrators, technicians

Administrators and technicians assigned to a system can access the system using RPS. Details on RPS configuration for Remote Portal use are available in the RPS manual.

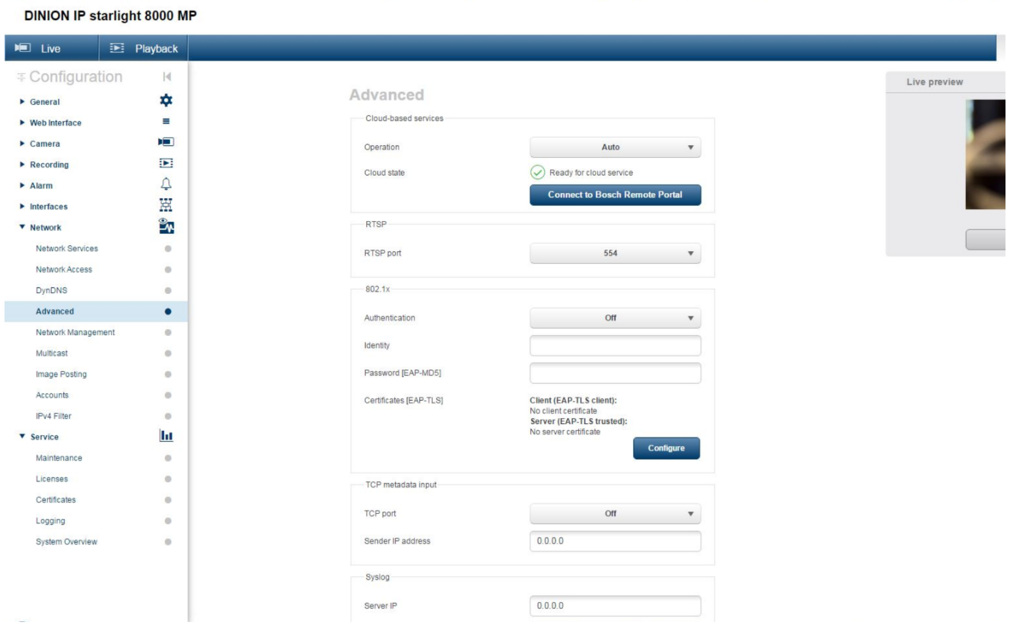
Customers

Customer access is not supported for FPA-5000.

4.1.6 IP cameras

Connection

IP cameras can be associated with a Remote Portal account through the device's configuration pages by selecting the *Advanced* menu of the *Network* section of the configuration pages. Connect the camera to your account by selecting "Connect ... " and providing credentials of an administrator or technician account.



Advanced

Cloud-based services

Operation: Auto

Cloud state: Ready for cloud service

Connect to Bosch Remote Portal

RTSP

RTSP port: 554

802.1x

Authentication: Off

Identity

Password [EAP-MD5]

Certificates [EAP-TLS]: **Client (EAP-TLS client):** No client certificate **Server (EAP-TLS trusted):** No server certificate

Configure

TCP metadata input

TCP port: Off

Sender IP address: 0.0.0.0

Syslog

Server IP: 0.0.0.0

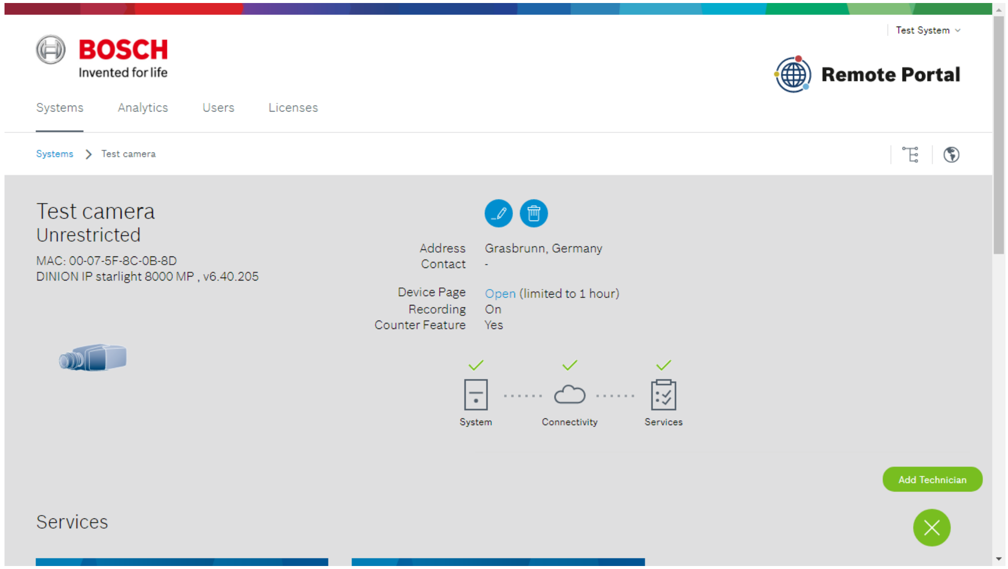
Ensure that camera date and time are set properly. Otherwise connection with the cloud will fail.
Using a time server is recommended to ensure that camera time remains properly after initial connection. Consult the camera's manual on details how to configure a time server.

After registration on device visit the Remote Portal to configure access or camera counter reports.

Remote access

Administrators, technicians

Administrators and technicians can access the camera's configuration pages directly from the Remote Portal using the "Device page" link on the system detail page. Access via this link is authenticated by the cloud and connects to the camera with "service" level.



Test camera
Unrestricted
MAC: 00-07-5F-8C-0B-8D
DINION IP starlight 8000 MP , v6.40.205

Address	Grasbrunn, Germany
Contact	-
Device Page	Open (limited to 1 hour)
Recording	On
Counter Feature	Yes

Connections to camera BVIP pages are limited to approximately one hour. To start a new session reload the system detail page and open the "Device page" link.

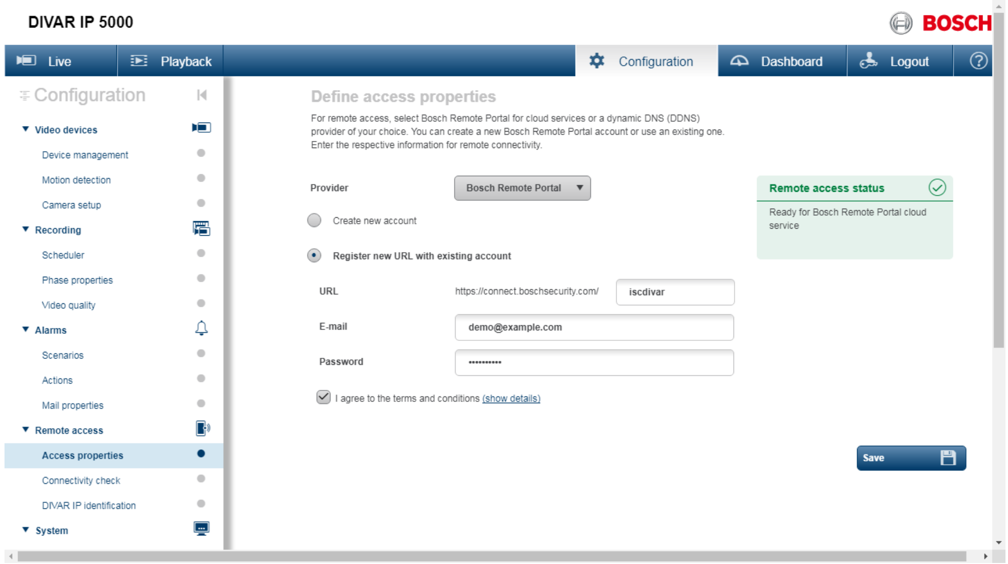
Customers

Customers with access to an IP camera (assigned via Remote Connect) can access Camera Counter Reports or Camera Viewers. See the service description for more details.

4.1.7 DIVAR IP 5000 (2000)

Connection

DIVAR IP 5000 (2000) can be registered with a Remote Portal account through the device's configuration pages, either as part of the setup wizard or (as shown) from the *Remote Access* section of the configuration page. Connect the DIVAR to your account by providing credentials of an "Administrator" or "Technician" account. The permalink URL allows logging into the device with local device credential at the selected URL.



Define access properties

For remote access, select Bosch Remote Portal for cloud services or a dynamic DNS (DDNS) provider of your choice. You can create a new Bosch Remote Portal account or use an existing one. Enter the respective information for remote connectivity.

Provider: Bosch Remote Portal ▼

○ Create new account

● Register new URL with existing account

URL: https://connect.boschsecurity.com/ iscdivar

E-mail: demo@example.com

Password: ••••••••••

☑ I agree to the terms and conditions (show details)

Remote access status ✓

Ready for Bosch Remote Portal cloud service

After registration on device visit the Remote Portal to configure Remote Connect for access using the Video Security Client or Video Security App (iOS).

4.1.8 DIVAR hybrid / network configuration

Connection

Full details on connection can be found in the DIVAR Operation Manual. To utilize Bosch Remote Portal follow these steps when configuring the device in the DDNS section:

1. Select the ‘Enable’ box.
2. Select Bosch Remote Portal as DDNS provider
3. Provide a unique name for this device. The domain "<name>.boschremoteconnect.com" will point back to the this device's public IP as long as the DDNS configuration is active.
4. In the account box provide "Administrator" or "Technician" credentials. For convenience a new Remote Portal account will be created for credentials that do not match an existing account.

Port forwarding

The access the system remotely the ports used by the apps must be forwarded to the system. This configuration is to be done on the network router that connects the local network of the recorder to the Internet.

It is recommended to forward the HTTPS, RTSP and TCP port and not the HTTP port for security reasons. The ports configured for these three services in the recorder settings need to be added to the port forwarding rules of the router pointing to the local network IP address of the recorder.

4.2 Remote Alert

4.2.1 Overview

Remote Alert monitors system health and allows sending of notifications (SMS, E-mail) to users based on configurable triggers. The table below summarizes available triggers and notifications types for different systems.

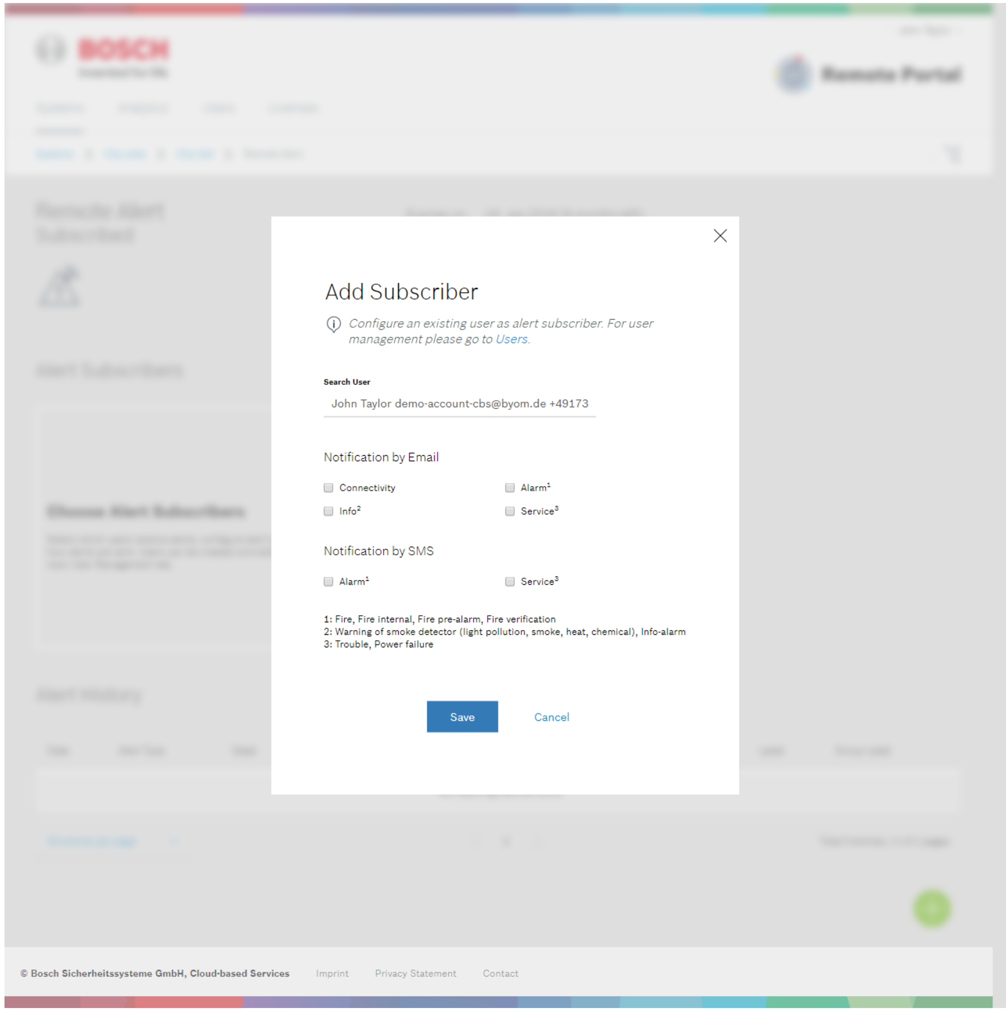
Remote Alert requires that Remote Connect is activated and available with a valid license for the system.

Fire Alarm System			Intrusion Alarm System			Video System		
Device	**Triggers**	**Notification**	**Device**	**Triggers**	**Notification**	**Device**	**Trigger**	**Notification**
FPA-5000	• Trouble • Alarm	• email • SMS	B-/G-Series	• Connection loss	• email	DIVAR IP 5000 (2000)	• Connection loss • Health status (summary as provided by system)	• email
Security Gateway	• Connection loss	• email • SMS				DIVAR hybrid, DIVAR network	• Connection loss	• email
						IP cameras	• Connection loss • Recording status	• email

Delivery of E-mail or SMS may fail for various reasons. Do not use Remote Alert applications for applications that require guaranteed delivery of notifications.

4.2.2 Configuration

Remote Alert is configured from the service detail page of each system. To start add a subscriber to Remote Alert using the green "+" button. Once a user is selected the Remote Portal will offer choosing the triggers and notification mechanism based on system type. The screenshot below is taken for a fire alarm system and varies slightly from other system types:



Add Subscriber

Configure an existing user as alert subscriber. For user management please go to Users.

Search User

John Taylor demo-account-cbs@byom.de +49173

Notification by Email

□ Connectivity □ Alarm[1]

□ Info[2] □ Service[3]

Notification by SMS

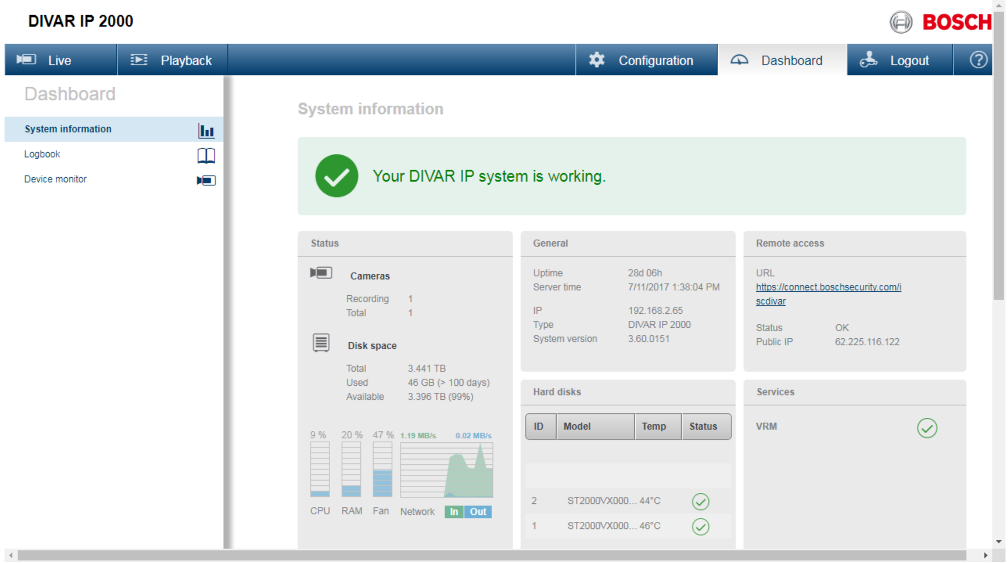
□ Alarm[1] □ Service[3]

1: Fire, Fire internal, Fire pre-alarm, Fire verification
2: Warning of smoke detector (light pollution, smoke, heat, chemical), Info-alarm
3: Trouble, Power failure

System specific notes

DIVAR IP 5000 (2000)

When enabling "Health Status" as a trigger for DIVAR IP the Remote Portal follows the overall status display of the DIVAR's dashboard. Notifications are sent when the dashboard changes from a green all-ok status to reported trouble.



System information

Your DIVAR IP system is working.

Status

Cameras

Recording	1
Total	1

Disk space

Total	3.441 TB
Used	46 GB (> 100 days)
Available	3.396 TB (99%)

9 % 20 % 47 % 1.19 MB/s 0.02 MB/s

General

Uptime	28d 06h
Server time	7/11/2017 1:38:04 PM
IP	192.168.2.65
Type	DIVAR IP 2000
System version	3.60.0151

Remote access

URL https://connect.boschsecurity.com/iscdivar

Status	OK
Public IP	62.225.116.122

Hard disks

ID	Model	Temp	Status
2	ST2000VX000...	44°C	✓
1	ST2000VX000...	46°C	✓

Services

VRM	✓

DIVAR hybrid / network

"Health status" on these devices monitors whether the device regularly update its public IP address. The grace period between missed updates and sending of alarms can be 30 minutes or more.

FPA-5000

For FPA-5000 triggers for critical system events can send SMS and e-mail. The table below details which event classes exist and whether notifications can be sent via e-mail or SMS for this class:

Event class	Description	E-Mail notification	SMS
Normal		✗	✗
Info	Warning of smoke detector (light pollution, smoke, heat, chemical), Info-alarm	✓	✗
Service	Trouble, Power failure	✓	✓
Alarm	Fire, Fire internal, Fire pre-alarm, Fire verification	✓	✓

For each triggering system event only the initial trigger within a 24 hour period will be sent, this reduces the number of message in case of larger event bursts.

Furthermore the Remote Portal limits total amount of SMS to 10 per day, per account. The portal alert history however always show all events, independent of whether a message was sent or not.

IP cameras

When enabling "Health Status" as a trigger for IP cameras the Remote Portal will monitor changes of recording status for this camera. Changes to recording status trigger a notification.

> Recording status changes are monitored for SD-card, direct-to-iSCSI or VRM-based recordings. When using other recording solutions status changes may not be visible to the Remote Portal.

4.3 Remote Maintenance

4.3.1 Overview

Remote Maintenance assists in performing maintenance tasks on compatible devices and systems. Remote Maintenance is currently available for FPA-5000.

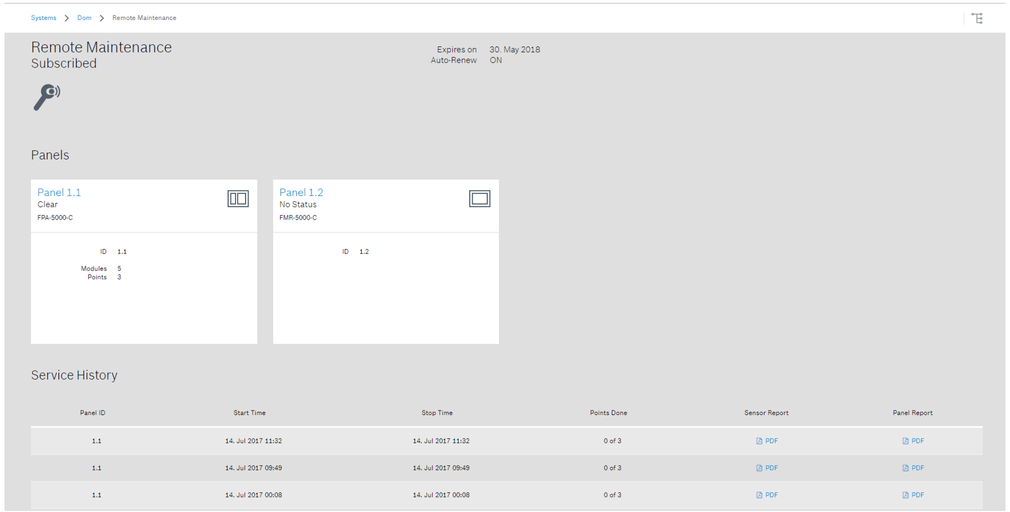
4.3.2 System hierarchy and status

Remote Maintenance shows the complete hierarchy and status of a FPA-5000 system. The hierarchy is updated live from the system and lists all panels, modules and points as running on site.

For all panels modules and points of the system the Remote Portal displays status information (Clear, Attention, Trouble). To quickly judge the health of a system this status information aggregates from points to modules to panels, in this way a technician can see at once at top level if there are any issues for system components.

The status of a system can be exported to PDF by selecting panel report or sensor report from the respective pages.

Panel structure



Remote Maintenance
Subscribed

Expires on 30. May 2018
Auto-Renew ON

Panels

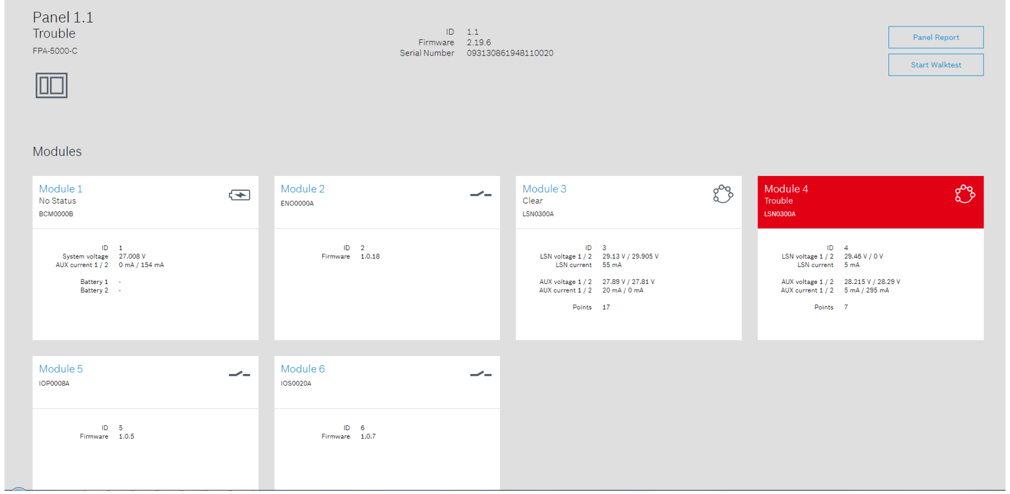
Panel 1.1
Clear
FPA-5000-C
ID 1.1
Modules 5
Points 3

Panel 1.2
No Status
FMR-5000-C
ID 1.2

Service History

Panel ID	Start Time	Stop Time	Points Done	Sensor Report	Panel Report
1.1	14. Jul 2017 11:32	14. Jul 2017 11:32	0 of 3	PDF	PDF
1.1	14. Jul 2017 09:49	14. Jul 2017 09:49	0 of 3	PDF	PDF
1.1	14. Jul 2017 00:08	14. Jul 2017 00:08	0 of 3	PDF	PDF

Module structure



Panel 1.1
Trouble
FPA-5000-C

ID 1.1
Firmware 2.19.6
Serial Number 093130861948110020

Modules

Module 1
No Status
BCM0000B

ID 1
System voltage 27.008 V
AUX current 1 / 2 0 mA / 154 mA

Battery 1 -
Battery 2 -

Module 2
ENO0000A

ID 2
Firmware 1.0.18

Module 3
Clear
LSN0300A

ID 3
LSN voltage 1 / 2 29.13 V / 29.905 V
LSN current 55 mA

AUX voltage 1 / 2 27.89 V / 27.81 V
AUX current 1 / 2 20 mA / 0 mA

Points 17

Module 4
Trouble
LSN0300A

ID 4
LSN voltage 1 / 2 29.46 V / 0 V
LSN current 5 mA

AUX voltage 1 / 2 28.215 V / 28.29 V
AUX current 1 / 2 5 mA / 295 mA

Points 7

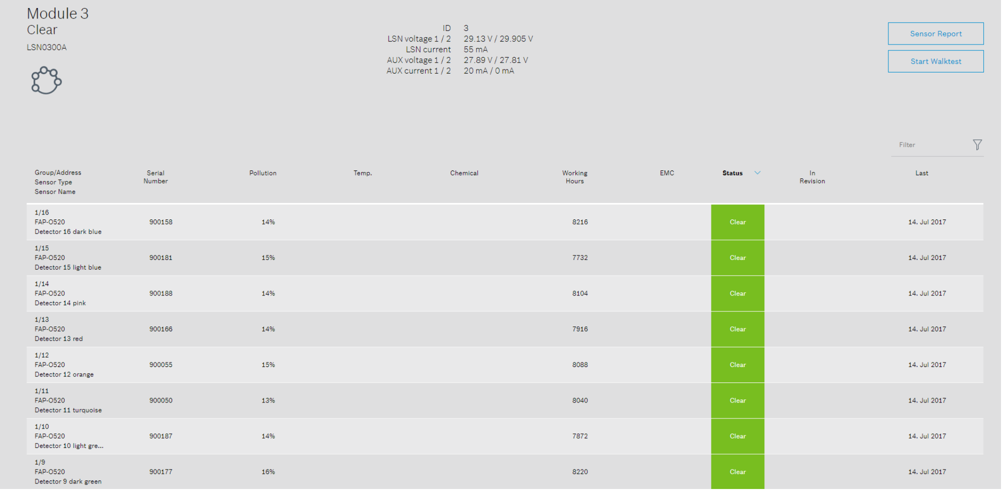
Module 5
IOP0008A

ID 5
Firmware 1.0.5

Module 6
IOS0020A

ID 6
Firmware 1.0.7

Point structure



Module 3
Clear
LSN0300A

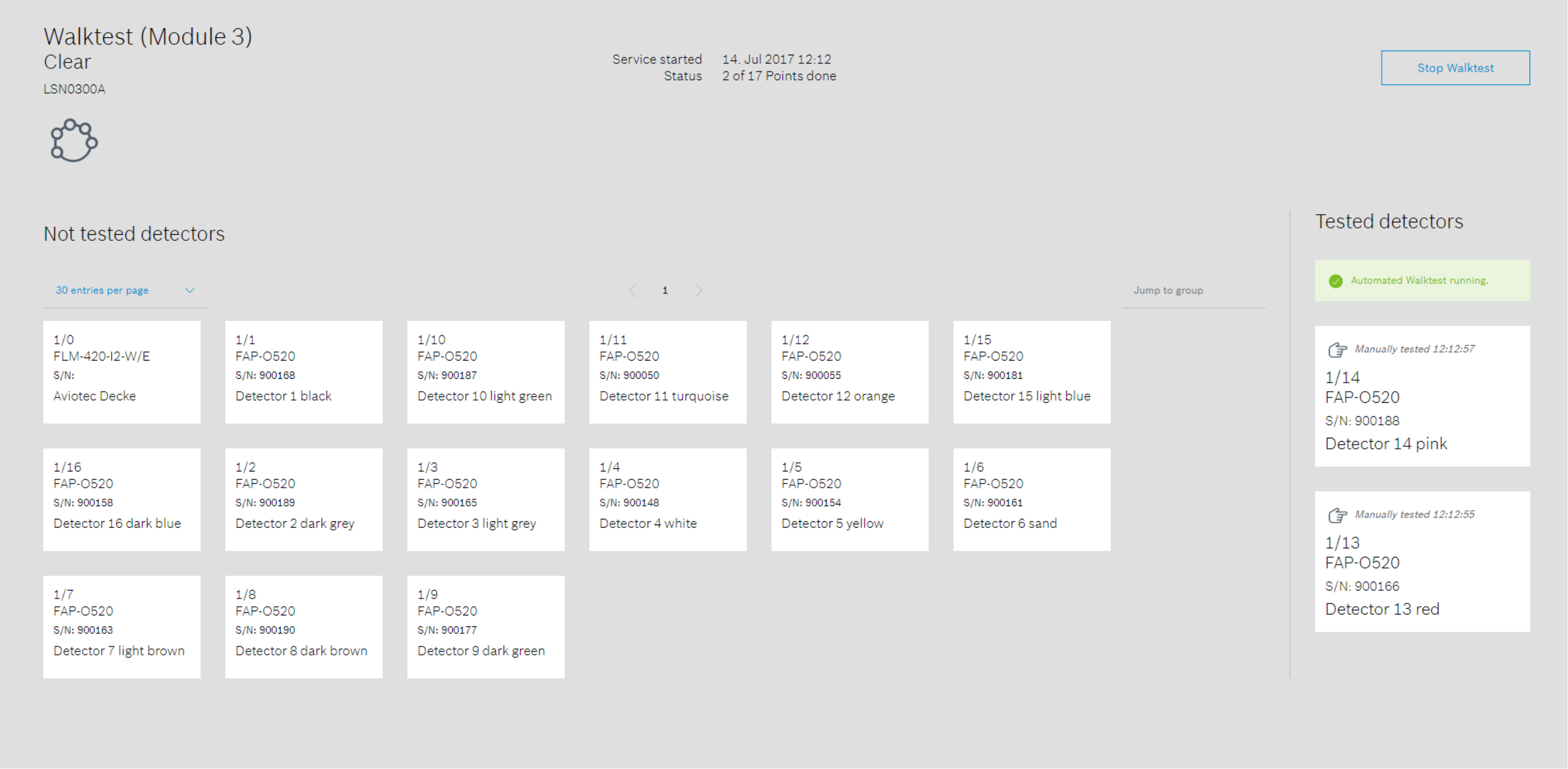
ID 3
LSN voltage 1 / 2 29.13 V / 29.905 V
LSN current 55 mA
AUX voltage 1 / 2 27.89 V / 27.81 V
AUX current 1 / 2 20 mA / 0 mA

Group/Address Sensor Type Sensor Name	Serial Number	Pollution	Temp.	Chemical	Working Hours	EMC	**Status**	In Revision	Last
1/16 FAP-O520 Detector 16 dark blue	900158	14%			8216		Clear		14. Jul 2017
1/15 FAP-O520 Detector 15 light blue	900181	15%			7732		Clear		14. Jul 2017
1/14 FAP-O520 Detector 14 pink	900188	14%			8104		Clear		14. Jul 2017
1/13 FAP-O520 Detector 13 red	900166	14%			7916		Clear		14. Jul 2017
1/12 FAP-O520 Detector 12 orange	900055	15%			8088		Clear		14. Jul 2017
1/11 FAP-O520 Detector 11 turquoise	900050	13%			8040		Clear		14. Jul 2017
1/10 FAP-O520 Detector 10 light gre...	900187	14%			7872		Clear		14. Jul 2017
1/9 FAP-O520 Detector 9 dark green	900177	16%			8220		Clear		14. Jul 2017

4.3.3 Walktest

The walktest service assists the revision on site. Walktests can be initiated either for a whole panel or for individual modules of the panel. When a walktest starts each point (e.g. smoke detector) is represented as a card. Cards put into revision mode are marked with a "R" and are ready for testing.

Cards are moved automatically from the left to the right side of the screen when the corresponding detector is tested successfully. This may take up to 30 seconds and requires that panel and mobile device are online and Remote Alert has been activated. If this does not apply, detector cards can be moved manually to the right pane by clicking on the cards. After finishing the revision a document is created and recorded in the history section and can be downloaded in PDF format.



Walktest (Module 3)
Clear
LSN0300A

Service started 14. Jul 2017 12:12
Status 2 of 17 Points done

Not tested detectors

1/0
FLM-420-I2-W/E
S/N:
Aviotec Decke

1/1
FAP-O520
S/N: 900168
Detector 1 black

1/10
FAP-O520
S/N: 900187
Detector 10 light green

1/11
FAP-O520
S/N: 900050
Detector 11 turquoise

1/12
FAP-O520
S/N: 900055
Detector 12 orange

1/15
FAP-O520
S/N: 900181
Detector 15 light blue

1/16
FAP-O520
S/N: 900158
Detector 16 dark blue

1/2
FAP-O520
S/N: 900189
Detector 2 dark grey

1/3
FAP-O520
S/N: 900165
Detector 3 light grey

1/4
FAP-O520
S/N: 900148
Detector 4 white

1/5
FAP-O520
S/N: 900154
Detector 5 yellow

1/6
FAP-O520
S/N: 900161
Detector 6 sand

1/7
FAP-O520
S/N: 900163
Detector 7 light brown

1/8
FAP-O520
S/N: 900190
Detector 8 dark brown

1/9
FAP-O520
S/N: 900177
Detector 9 dark green

Tested detectors

Automated Walktest running.

Manually tested 12:12:57
1/14
FAP-O520
S/N: 900188
Detector 14 pink

Manually tested 12:12:55
1/13
FAP-O520
S/N: 900166
Detector 13 red

4.4 Camera Counter Reports

4.4.1 General

Camera Counter Reports retrieve and store the values of camera VCA counters at regular intervals. The stored values can be visualized in the Remote Portal or exported to CSV files for further processing. Configuration of a report requires "Administrator" or "Technician" access to the Remote Portal and cameras to be used. Access to visualization and export can be granted to any customer.

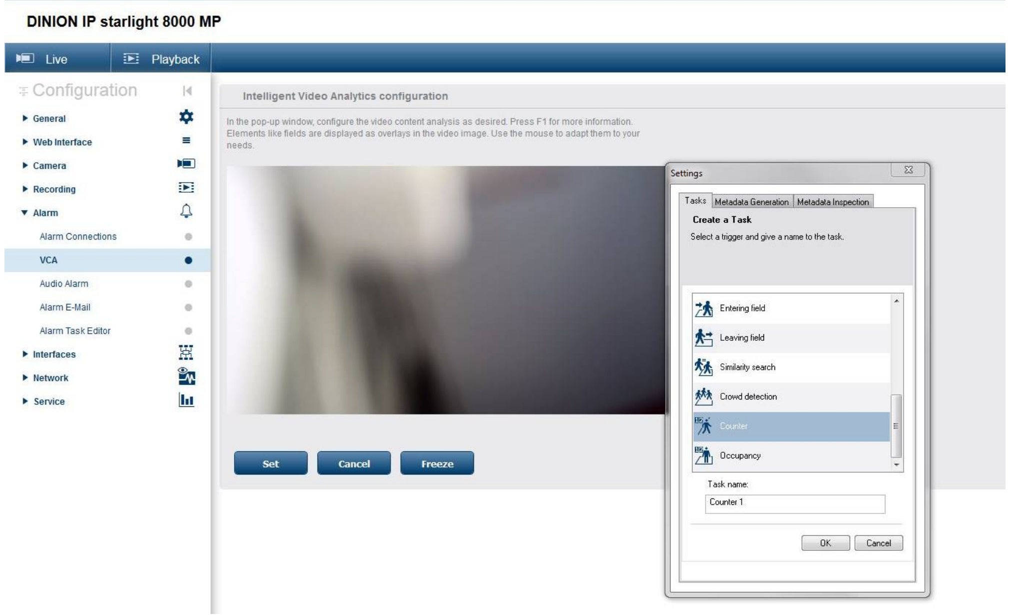
Creating a Camera Counter Report uses one license, see Licenses for more details.

4.4.2 Configuration

Camera configuration

Using cameras counters requires configuration of one or more VCA counting tasks on each camera. Follow the standard procedure for configuring cameras and setting up these tasks.

The task name given on camera will be used in the Remote Portal for configuration, preview or exporting.



DINION IP starlight 8000 MP

Intelligent Video Analytics configuration

In the pop-up window, configure the video content analysis as desired. Press F1 for more information. Elements like fields are displayed as overlays in the video image. Use the mouse to adapt them to your needs.

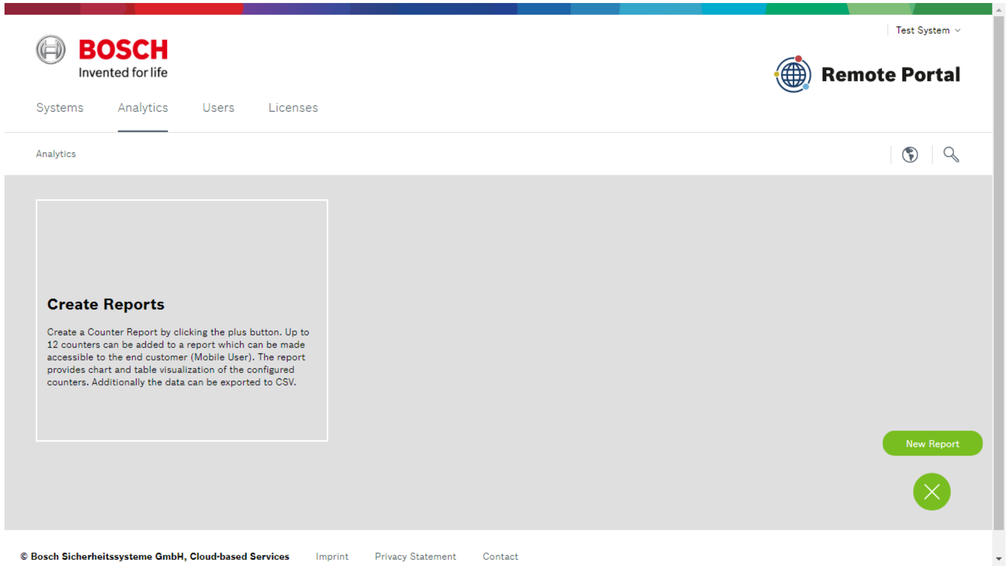
Create a Task

Select a trigger and give a name to the task.

Task name: Counter 1

Report configuration

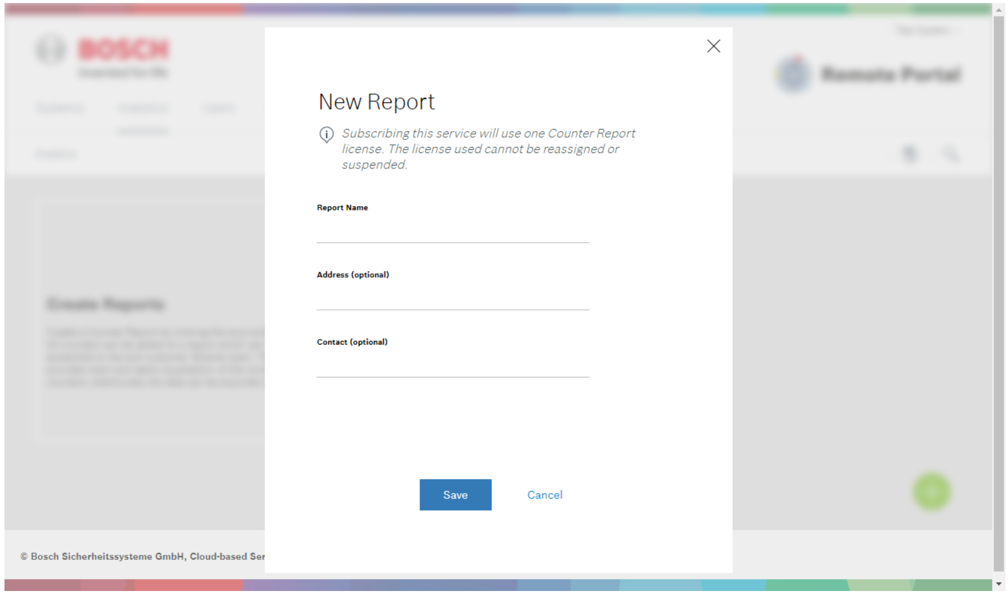
Camera Counter Reports are created and configured from the Analytics tab of the Remote Portal.



Create Reports

Create a Counter Report by clicking the plus button. Up to 12 counters can be added to a report which can be made accessible to the end customer (Mobile User). The report provides chart and table visualization of the configured counters. Additionally the data can be exported to CSV.

Select "New Report" and provide basic information as prompted:



New Report

Subscribing this service will use one Counter Report license. The license used cannot be reassigned or suspended.

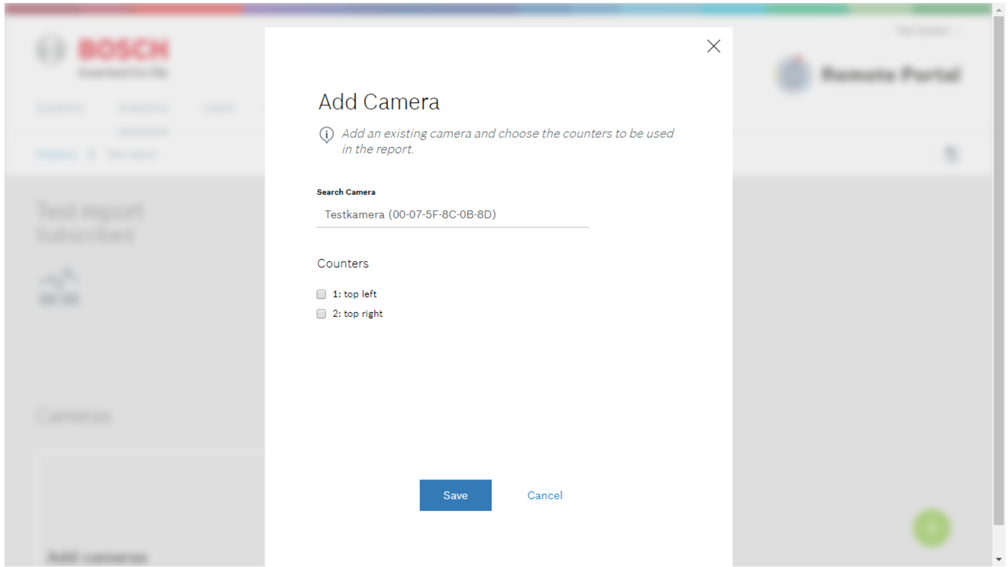
Report Name

Address (optional)

Contact (optional)

The first step after creating a report is to add cameras to the report. Press the green "+" button, select "Add camera" and search and select the camera by name or MAC address. The Remote Portal presents a list of counters that are available on camera, check each that you want to include in this report.

You can include multiple cameras in one report, up to a total of 12 counters.



Add Camera

Add an existing camera and choose the counters to be used in the report.

Search Camera

Testkamera (00-07-5F-8C-0B-8D)

Counters

□ 1: top left

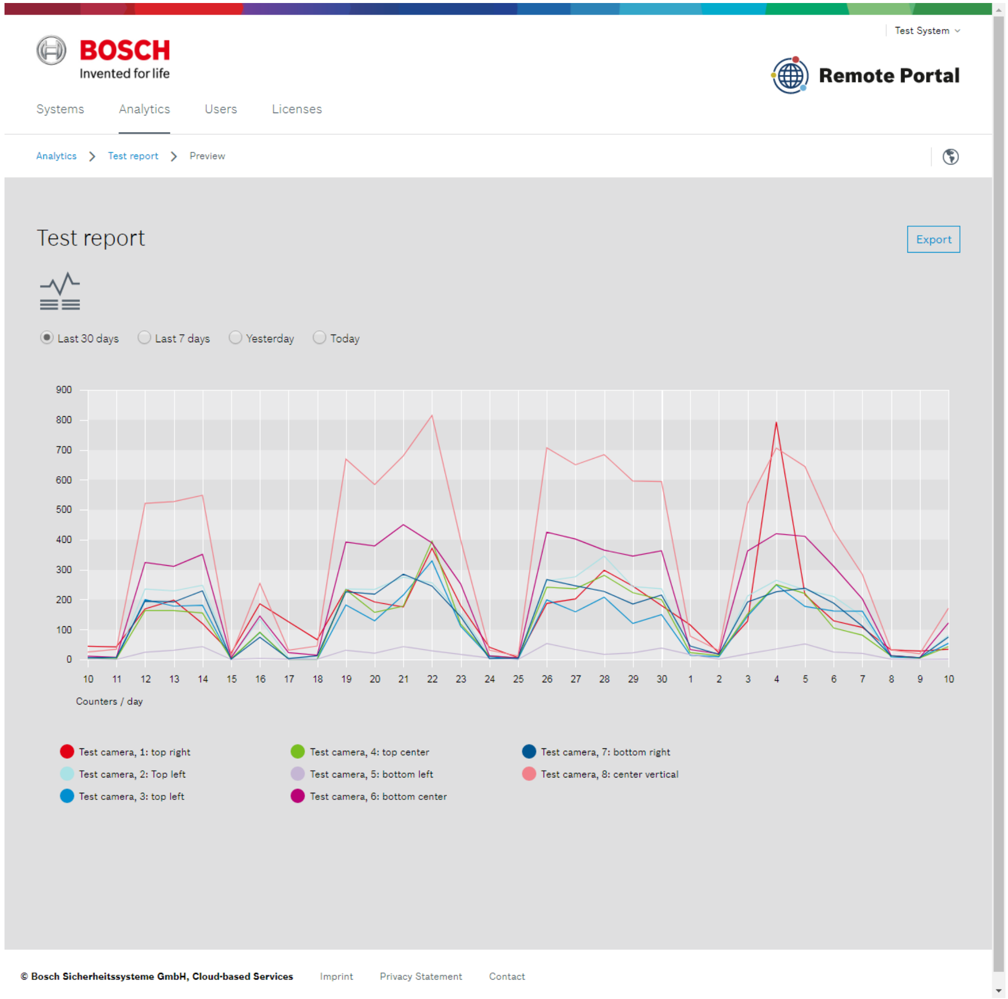
□ 2: top right

Counter values are retrieved approximately every 15 minutes. Until first update cycle has completed both Preview and Exports will not contain any data.

Preview

The Remote Portal provides basic visualization of collected counter data. For administrators and technicians this is available on the report's configuration page, for customers that where assigned the report directly from the start page after logging in.

For display with hour resolution (yesterday/today) time is displayed in local time. For displays with day resolution the value displayed is the sum value of this day.



Test report

● Last 30 days ○ Last 7 days ○ Yesterday ○ Today

900
800
700
600
500
400
300
200
100
0
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
1
2
3
4
5
6
7
8
9
10
Counters / day
Test camera, 1: top right
Test camera, 2: Top left
Test camera, 3: top left
Test camera, 4: top center
Test camera, 5: bottom left
Test camera, 6: bottom center
Test camera, 7: bottom right
Test camera, 8: center vertical
© Bosch Sicherheitssysteme GmbH, Cloud-based Services
Imprint
Privacy Statement
Contact

4.4.3 Export

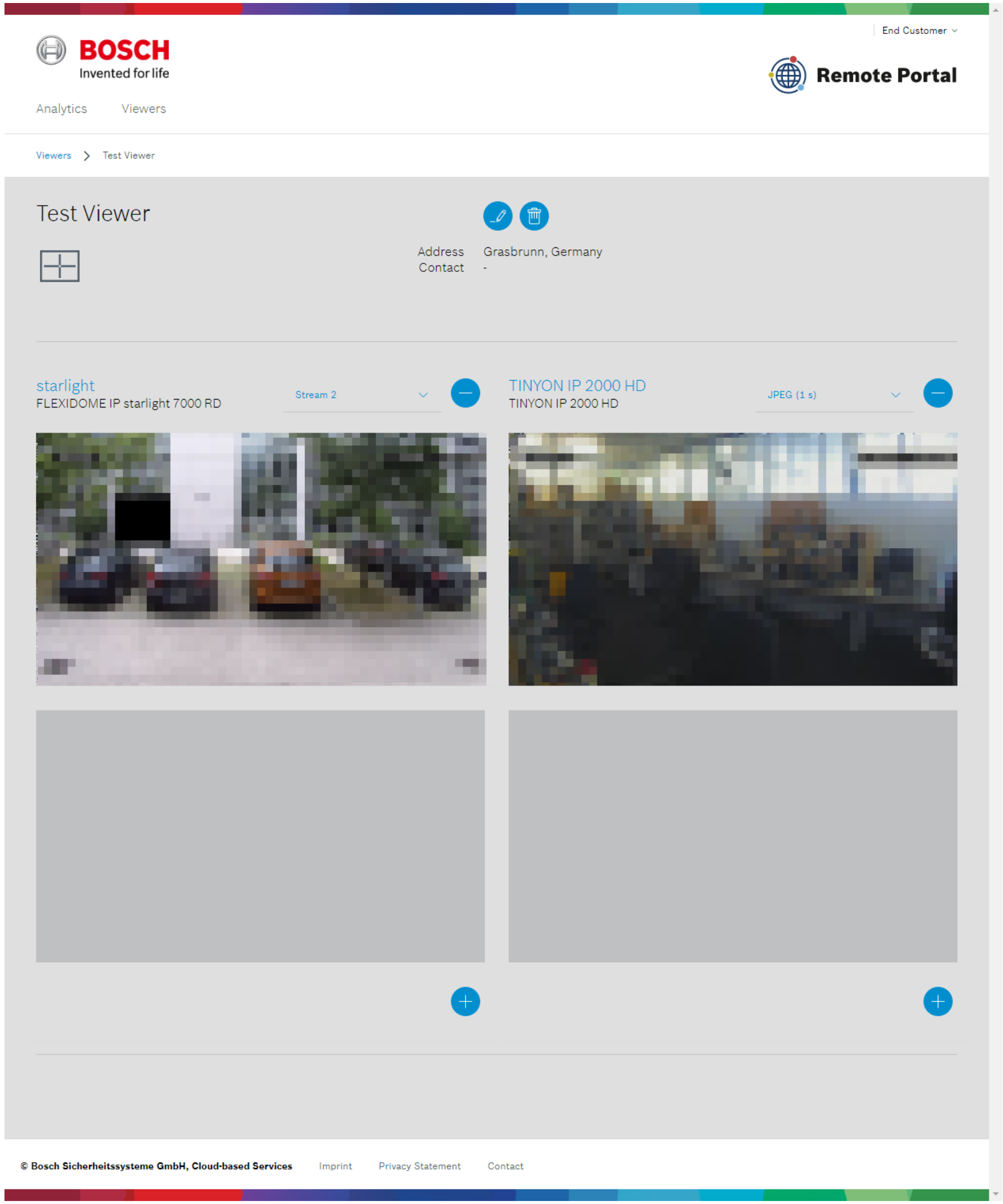
Select the "Export" button from the top right corner to export data in CSV format. Export always exports all available data.

Timestamps in exported data are always in UTC time zone. If required this can be changed to the proper time zone in post-processing.

4.5 Camera Viewers

4.5.1 General

Camera Viewers are a light-weight viewing tool that give end customer browser-based access to live images and video streams of cameras. Up to four cameras can be displayed with live streaming or JPEG polling.



Viewers > Test Viewer

Test Viewer

Address Grasbrunn, Germany
Contact -

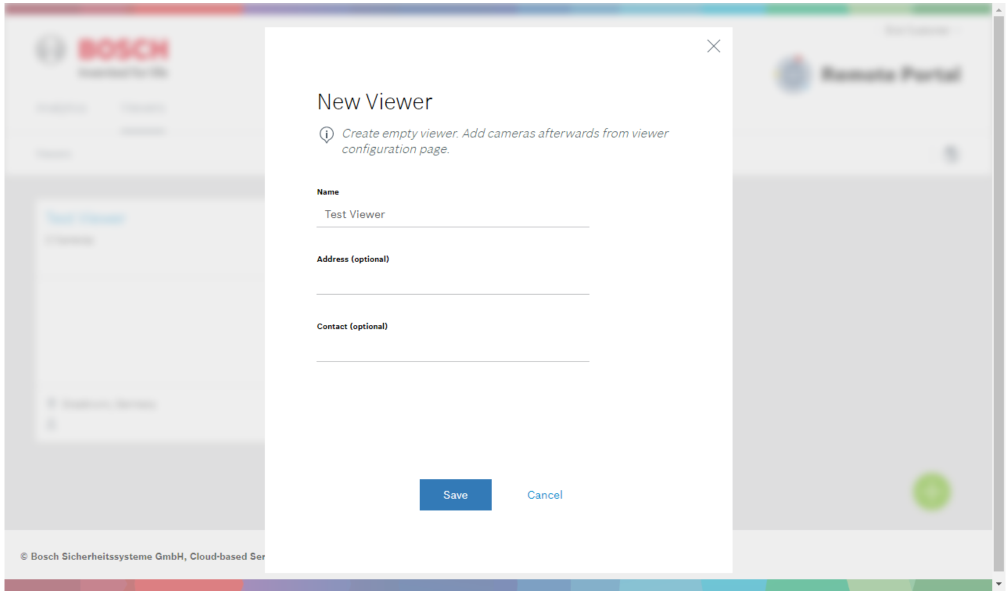
starlight
FLEXIDOME IP starlight 7000 RD
Stream 2

TINYON IP 2000 HD
TINYON IP 2000 HD
JPEG (1 s)

© Bosch Sicherheitssysteme GmbH, Cloud-based Services Imprint Privacy Statement Contact

4.5.2 Configuration

Camera Viewers are configured by end-customers from the "Viewers" tab of the Remote Portal. A new Camera Viewer can be created by selection the green "+" button and providing a name for the Viewer.



New Viewer

Create empty viewer. Add cameras afterwards from viewer configuration page.

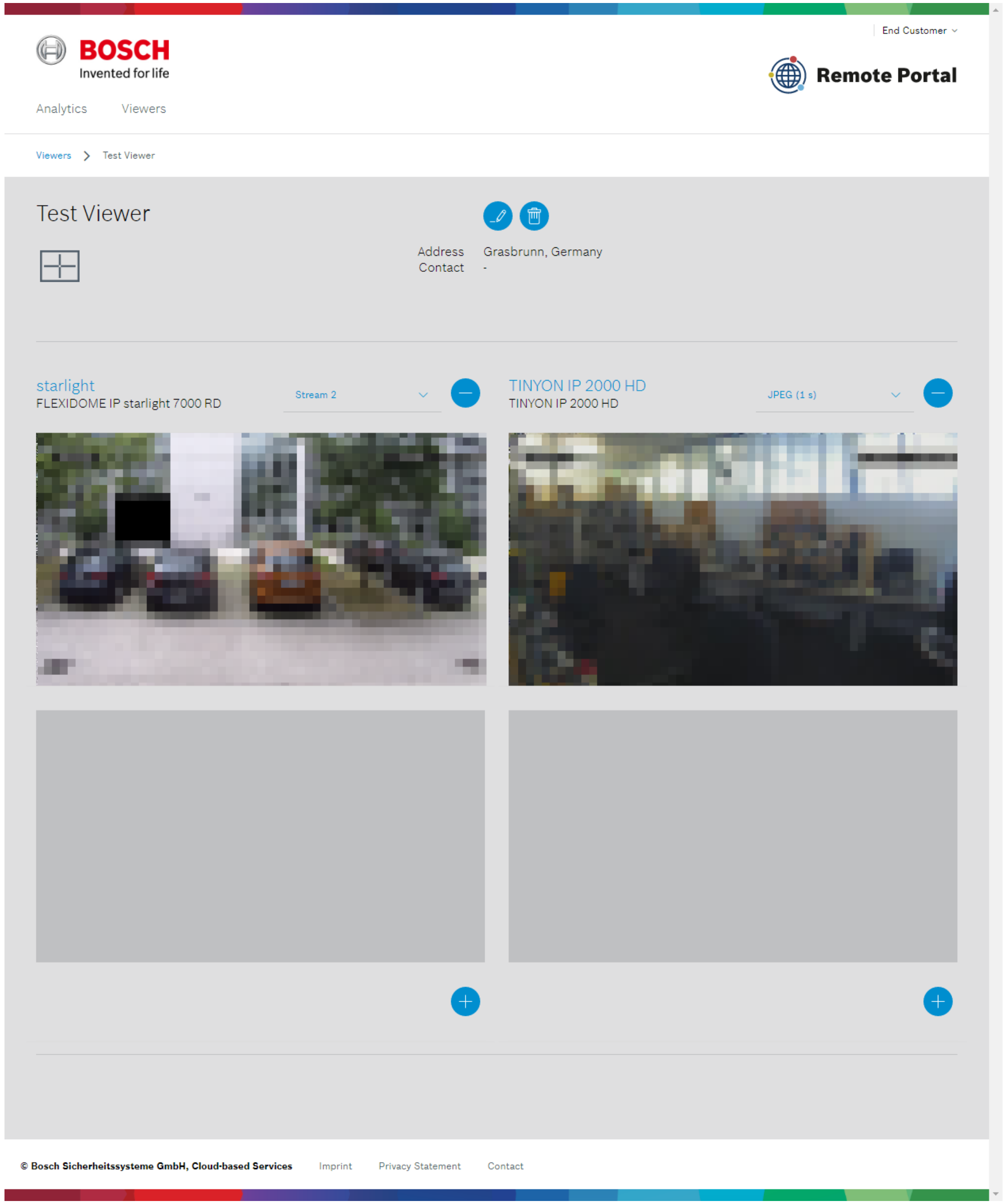
Name: Test Viewer

Address (optional):

Contact (optional):

Once a viewer is created cameras can be added and removed directly from the viewer itself. Note that a Customer is only able to cameras which are actively subscribed to Remote Connect and for which the "Customer" account has been attached to the Remote Connect service.

The screenshot below shows a Viewer configured with two cameras. Additional cameras could be added to bottom two grid positions by use of the blue "+" buttons, the top cameras could be remove by using the blue "-" button.



Viewers > Test Viewer

Test Viewer

Address Grasbrunn, Germany
Contact -

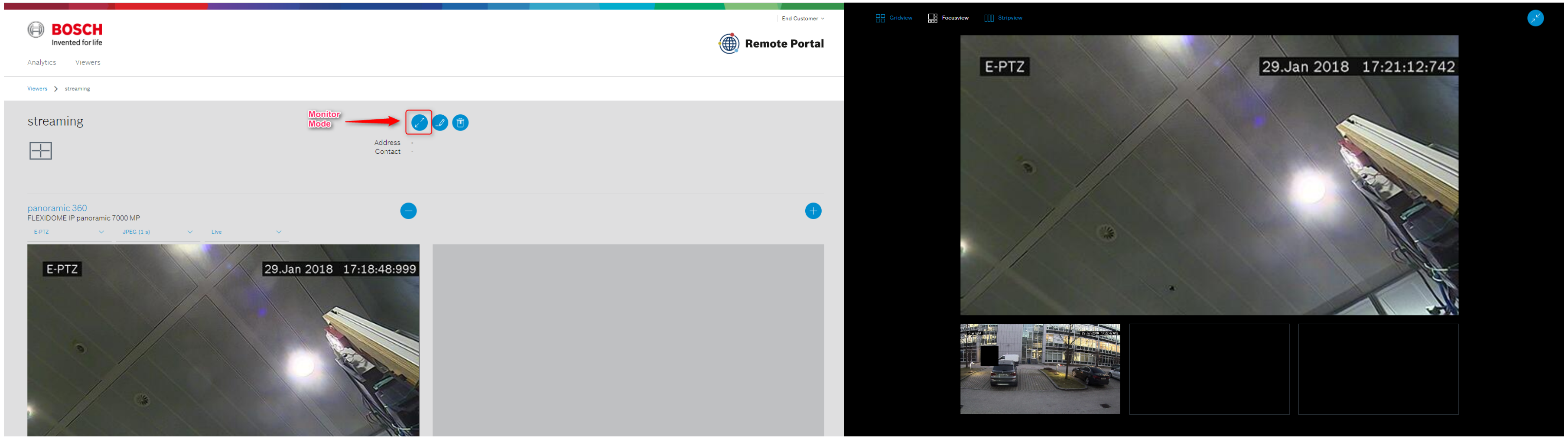
starlight
FLEXIDOME IP starlight 7000 RD
Stream 2

TINYON IP 2000 HD
TINYON IP 2000 HD
JPEG (1 s)

Camera Viewers are configured per customer and cannot be shared between multiple customers

4.5.3 Usage

Camera Viewers are accessed from the Remote Portal using the Customer account used for configuration. For "viewing only" the viewer can be put into monitor mode which removes most of the controls and maximizes the display size of images and videos. In monitor mode three different layouts can be configured: grid view, focus view and single view.

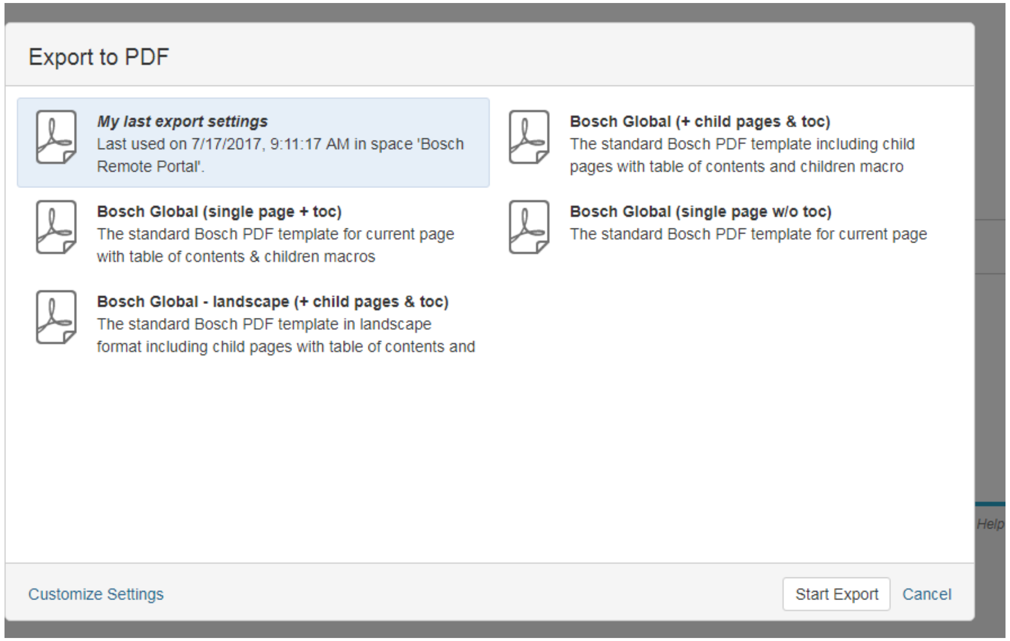


Camera Viewers display images and video streams via the cloud, even if the viewer is used on the same network as the cameras. For local applications installation of a desktop viewer such as BVC or Video Security client avoids consuming bandwidth on the Internet uplink or issues due to bandwidth fluctuations.

5 Tips and formatting guidelines

5.1 Hiding pages and exporting

- Attach label exclude to pages not to export, such as this one
- Select Bosch Global (child pages & toc) to export from Export to PDF menu



Export to PDF

My last export settings
Last used on 7/17/2017, 9:11:17 AM in space 'Bosch Remote Portal'.

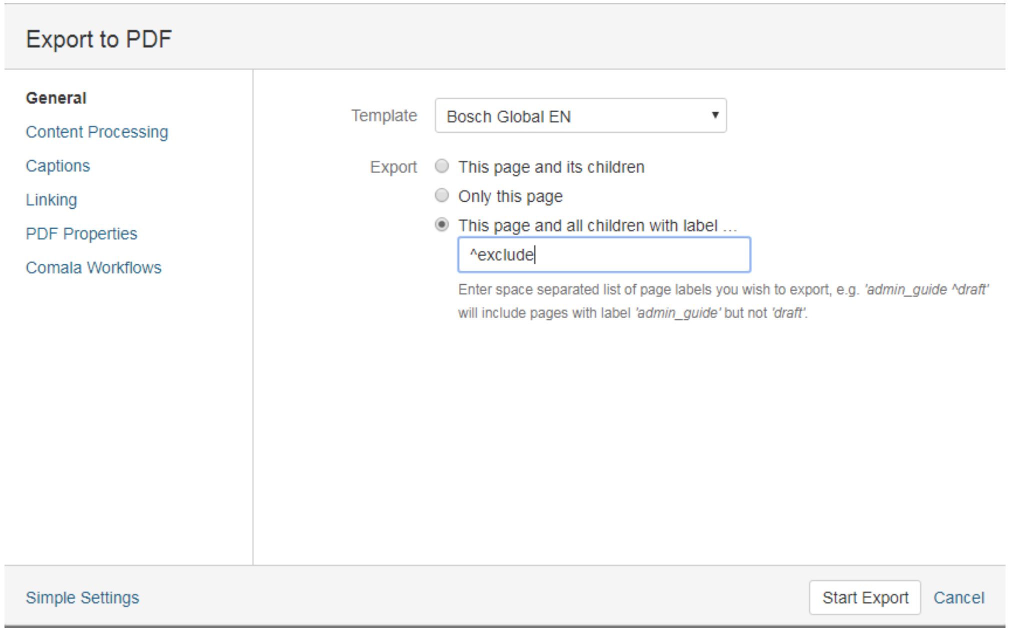
Bosch Global (+ child pages & toc)
The standard Bosch PDF template including child pages with table of contents and children macro

Bosch Global (single page + toc)
The standard Bosch PDF template for current page with table of contents & children macros

Bosch Global (single page w/o toc)
The standard Bosch PDF template for current page

Bosch Global - landscape (+ child pages & toc)
The standard Bosch PDF template in landscape format including child pages with table of contents and

- Select customize settings and limit pages to be excluded as shown (add {{ ^exclude}} to the last form field)



Template Bosch Global EN

Export
○ This page and its children
○ Only this page
● This page and all children with label ...

^exclude

Enter space separated list of page labels you wish to export, e.g. *'admin_guide ^draft'* will include pages with label *'admin_guide'* but not *'draft'*.

- Start Export

5.2 Terms

- Services are all capitalized: *Remote Connect*, not *remote connect* or *Remote connect*
- When context refers to a user or technician account, and not to a person of that role, capitalize and quote the term and add *account* to it, e.g. "User" account or "Technician" account. Otherwise use lower case.

5.3 Screenshots

- Take screenshots for 720p resolution, Chrome can does this via developer tools automatically including full length page screenshots
- Insert pictures and make preview image 500px wide.

5.4 Floating action button

- The floating action button is referred to as *green "+" button*

5.5 Wordings templates

Usage	Text	App note	Datasheet
Short description - Remote Connect	Enables connection between device, cloud and client software without network configuration on site. (*)	✓	✓
Short description - Remote Alert	Monitors system health and SMS or E-mail sends notifications to users based on configurable triggers.	✓	✓
Short description - Remote Maintenance	Collects and analyzes system data, assists in performing maintenance tasks on compatible devices and provides auto-generated maintenance reports.	✓	✓
Short description - Camera Counter Report	Retrieves and stores the values of camera VCA counters at regular interval and provides viewing and export via the Remote Portal.	✓	✓
Short description - Camera Viewer	Enables end customer browser-based access to live images and video streams of cameras.	✓	✓

6 Software clients guide

6.1 Video systems

6.1.1 Compatibility

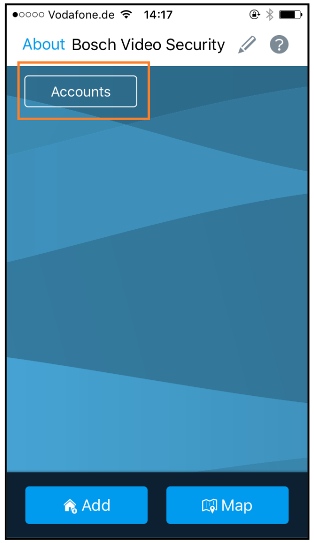
The table below lists software clients that are compatible for use with the Remote Portal managed users. Note that clients not listed may still be used for e.g. direct (local) connections but must configured individually.

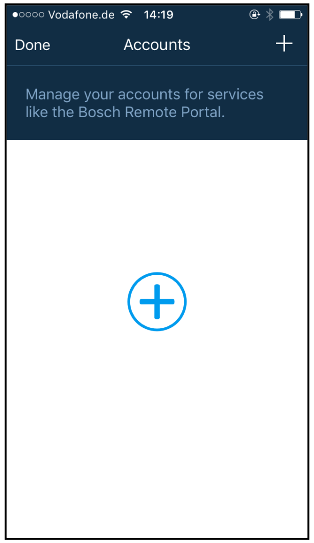
Client	Platform	Compatibility
Video Security App	iOS	DIVAR IP 5000 (2000)
Video Security Client	Windows	DIVAR IP 5000 (2000)

Configuration

Video Security App

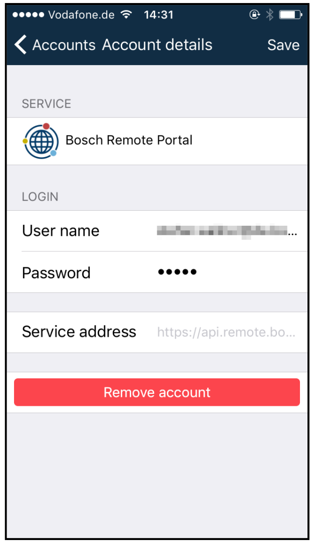
Download the "Video Security" app from the App Store and launch it. To establish connection to the Remote Portal select "Accounts" from the top left corner and tap "+" on the next screen:





Manage your accounts for services like the Bosch Remote Portal.

Provide Remote Portal credentials (Administrator or Customer) on the next screen. Leave "Service address" unchanged.



SERVICE

Bosch Remote Portal

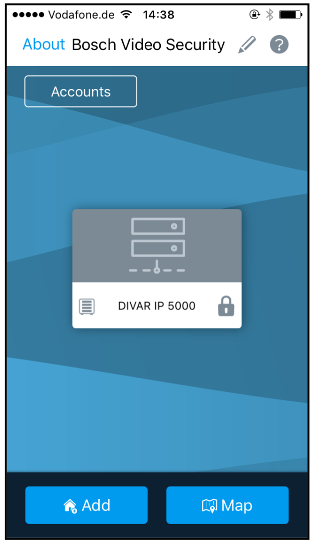
LOGIN

User name [redacted]

Password •••••

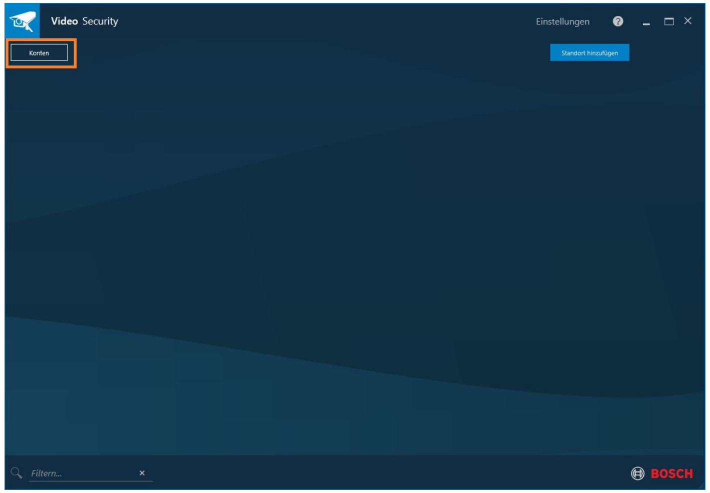
Service address https://api.remote.bo...

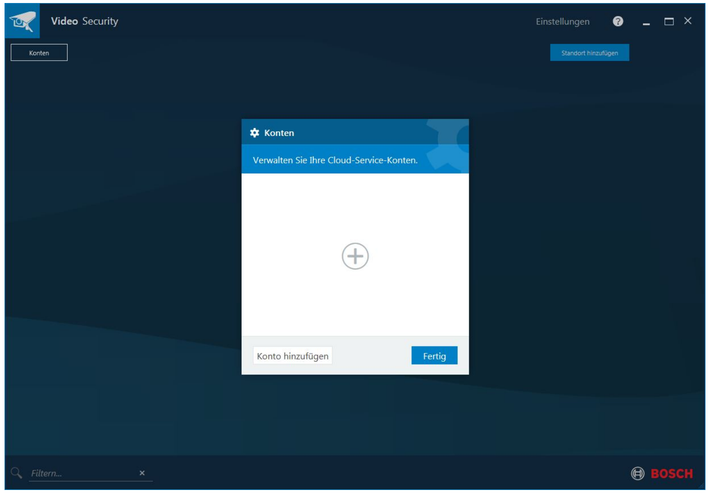
Select "Save". All devices that are accessible with the credentials provided will now be shown on home screen of the app and are ready for use.



Video Security Client

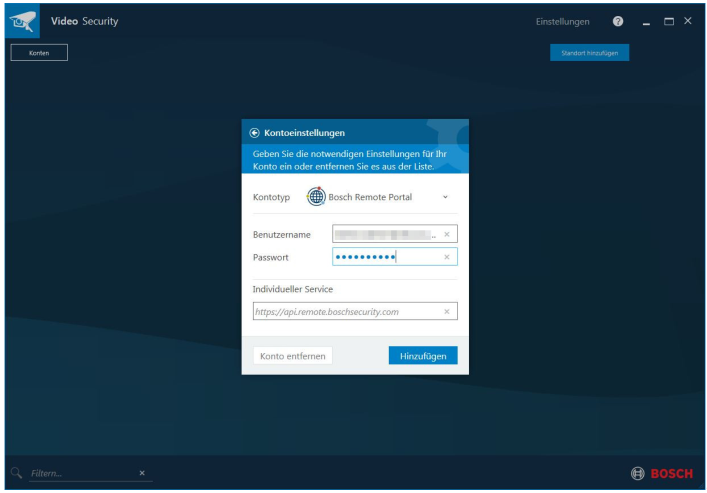
Video Security Client is available from the Bosch Downloadstore at https://downloadstore.boschsecurity.com. Select "Video Security Client" from the "Product Group" and download a suitable installation package. Install and launch the Video Security Client.





Verwalten Sie Ihre Cloud-Service-Konten.

Provide Remote Portal credentials (Administrator or Customer) on the next screen. Leave "Service address" unchanged.



Kontoeinstellungen

Geben Sie die notwendigen Einstellungen für Ihr Konto ein oder entfernen Sie es aus der Liste.

Kontotyp: Bosch Remote Portal

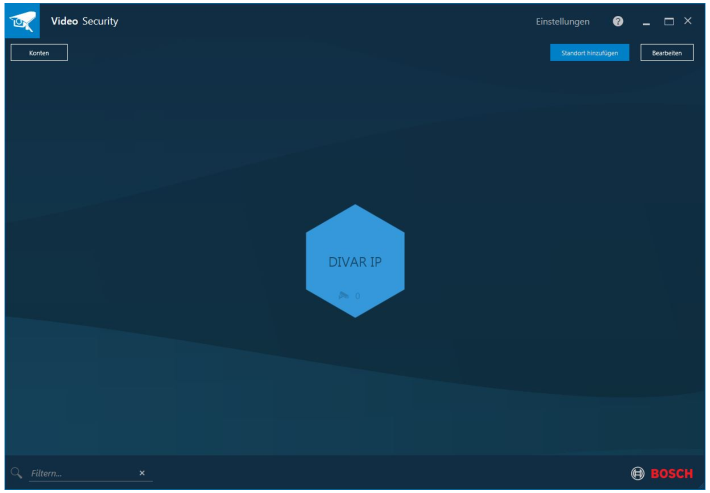
Benutzername: [redacted]

Passwort: ••••••••••

Individueller Service: https://api.remote.boschsecurity.com

,

Select "Add". All devices that are accessible with the credentials provided will now be shown on home screen of the Video Security Client and are ready for use.



Video Security
Einstellungen
Konten
Standort hinzufügen
Bearbeiten
DIVAR IP
Filtern...
BOSCH