DIVUS®
Show it. Control it.

DIVUS OPTIMA

Version 1.2.1 – rev. 1493

GENERAL INFORMATION

DIVUS GmbH
Pillhof 51
I-39057 Eppan (BZ)

We reserve the right to make changes to the manual without prior notification.

We assume no responsibility for any errors or omissions that may appear in this document.

We do not assume liability for the flawlessness and correctness of the programs and data contained on the delivered discs.

You are always welcome to inform us of errors or make suggestions for improving the program.

The present agreement also applies to special appendices to the manual.

This manual can contain terms and descriptions, which improper use by third can harm the copyrights of the author.

Please read the manual before beginning and keep the manual for later use.

The manual has been conceived and written for users who are experienced in the use of PCs and automation technology.

This version of the manual is based on the following version(s):

- DIVUS TOUCHZONE image R4.8

- DIVUS OPTIMA v. 1.2.1 rev. 1493

Our General Terms and Conditions apply, which can be downloaded here:

https://www.divus.eu/en/general-conditions

CONVENTIONS

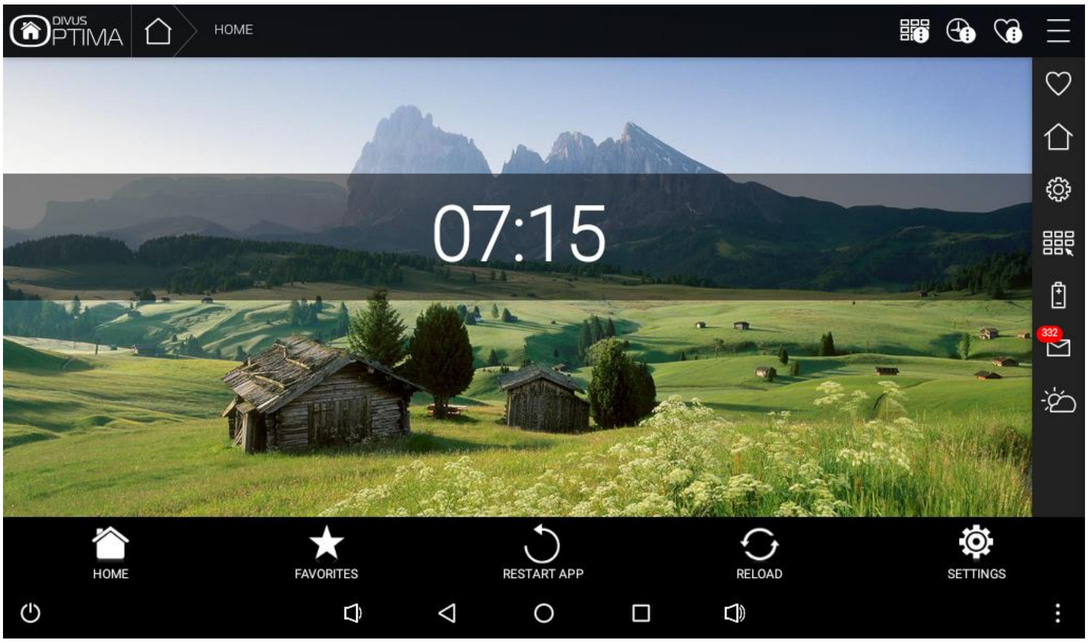
[KEYS]	Keys that are to be pressed by the user are given in square brackets, e.g. [CTRL] or [DEL]
`COURIER`	On-screen messages are given in the Courier font, e.g. `C:\>`
`COURIER BOLD`	Keyboard input to be made by the user are given in Courier bold, e.g. **`C:\>DIR).`**
„…“	Names of buttons to be pressed, menus or other onscreen elements and product names are given within double quotes. (e.g. “Configuration”).
PICTOGRAMS	In this manual the following symbolic are used to indicate particular text blocs.
⚠	Caution! A dangerous situation may arise that may cause damage to material.
i	Hint Hints and additional notes
NEW	New New features

The terms “**DIVUS** TOUCHZONE” and “**DIVUS** TZ” or simply “TZ” all point out the same product.

INDEX

1 Introduction

The DIVUS OPTIMA app is designed to be used together with KNX CONTROL and acts as a web app, which optimizes and displays the content in fullscreen. The app allows an easier access compared to regular browsers. Not only controlling the lights is possible, but also HVAC control, irrigation, scenarios, shutter functions, energy management and much more. With DIVUS OPTIMA you can control your house from your hand.



This manual will not describe the contents of KNXCONTROL/visualization, neither its navigation nor OPTIMA features. Information regarding DIVUS KNXCONTROL can be found in the corresponding DIVUS OPTIMA user/administration manuals, available on the DIVUS website: www.divus.eu

This app is intended to be used on DIVUS TOUCHZONE only, in this manual all examples are based on DIVUS TOUCHZONE with Android 6. For smartphones, tablets and other devices the app DIVUS OPTIMA MOBILE should be used.

Further information about the app DIVUS OPTIMA can be requested by contacting the technical support of DIVUS.

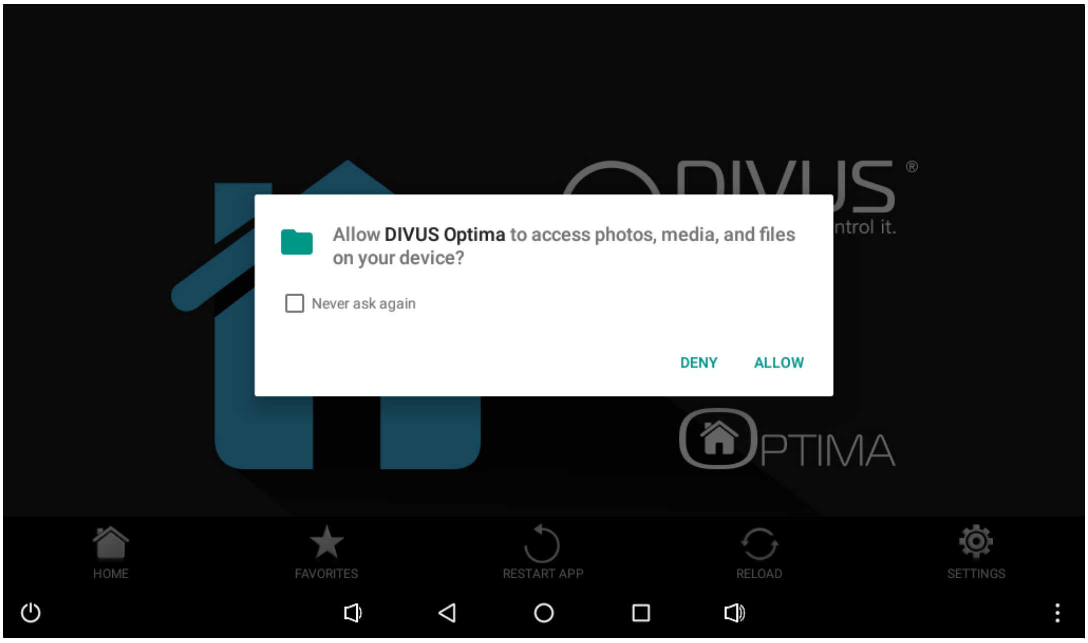
1.1 PREREQUISITES

DIVUS OPTIMA requires Android 2.2 (API 8) or higher to run, the app will be unable to install on devices running a lower Android version.

A DIVUS KNXCONTROL device is required in order to use the app.

1.2 FIRST START

If your device supports DIVUS OPTIMA, when launching the app, on some versions of Android some runtime permissions are asked and have to be manually allowed: DIVUS OPTIMA asks to access media on the device, this is required e.g. for logging purposes.

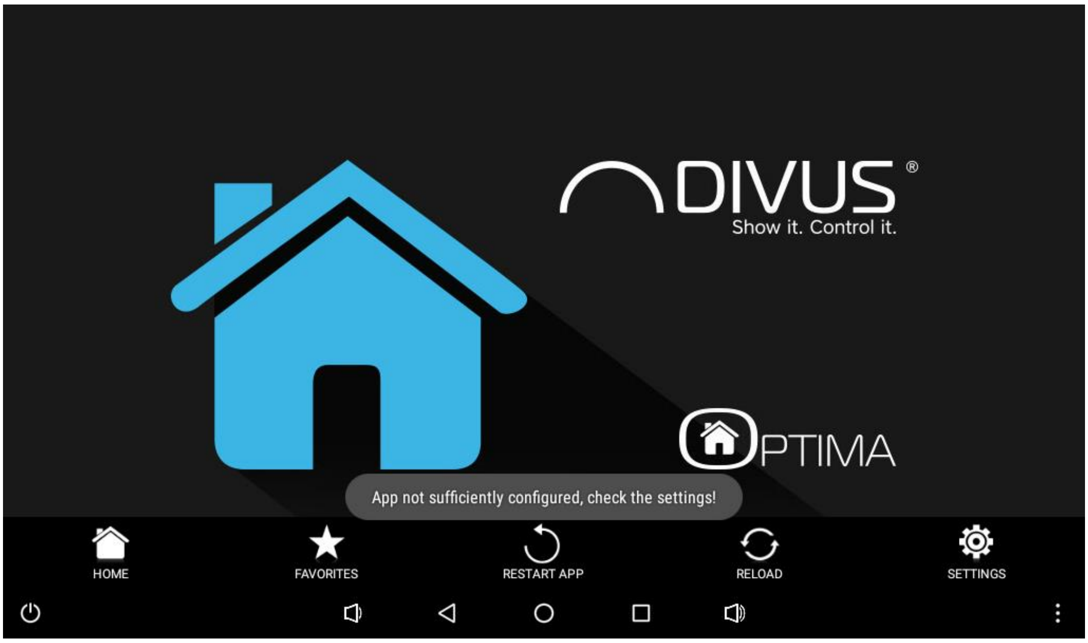


Allow **DIVUS Optima** to access photos, media, and files on your device?

☐ Never ask again

As long as some permissions are not granted, these missing permissions are asked at every start of the main view of the app until granted or denied permanently. When these permissions are not granted some functions of the app may not work! If the user decides to permanently deny these permissions then this dialog should not show up anymore. These permissions can also be granted/revoked manually in the settings on the applications management page of DIVUS OPTIMA.

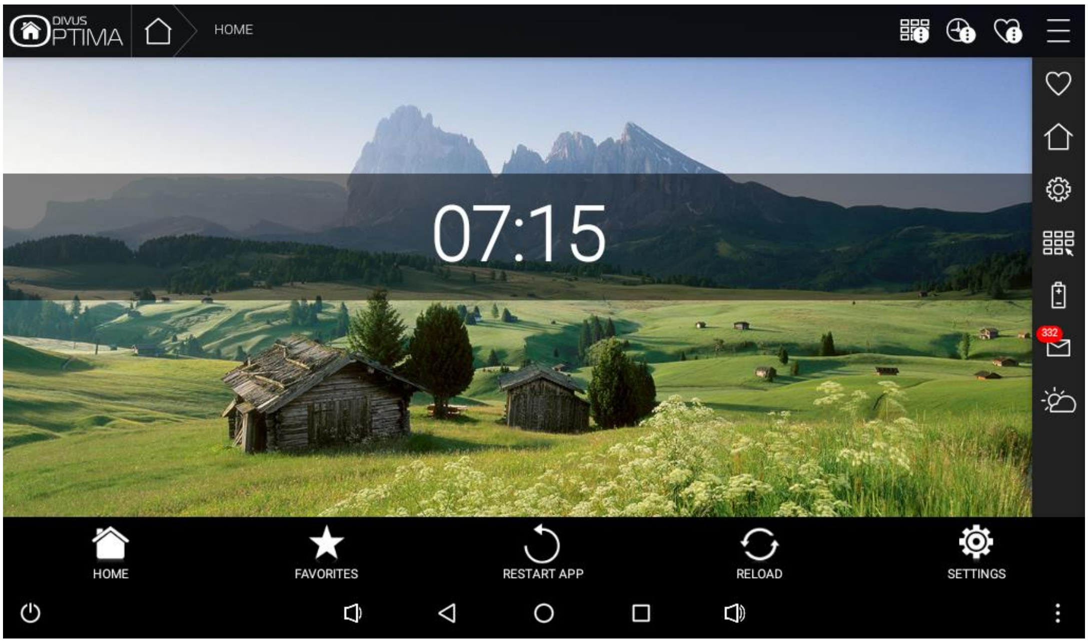
After the prompt for the permissions, when launching the app you will find the following empty screen, as no server is yet configured. A corresponding message will also be shown on the screen.



App not sufficiently configured, check the settings!

2 Main view

The main view of DIVUS OPTIMA consists of the main screen displaying the currently configured visualization from the DIVUS KNXCONTROL device, and on bottom a toolbar which contains additional controls.

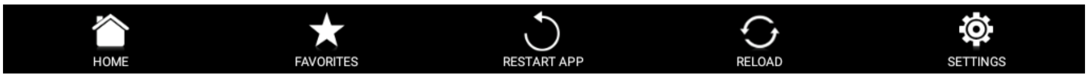


The content of the visualization shown on screen is loaded from the server and displayed as received, no content is generated by the app itself. Thus, the content may vary due to server-side configuration, user account and device used during access.

Additionally there are some controls in the menu of the app, accessible through the virtual or hardware MENU key of the device. The first button allows to open the app settings (similar to the corresponding button in the toolbar), the other button opens a dialog containing general information about the app.

2.1 TOOLBAR

At the bottom of the main view there is a toolbar containing various functions, mostly related to navigation through the visualization.



From left to right, the buttons are as follows:

- HOME

  This button will load the main screen of the visualization, which is usually displayed as the very first page after a successful login.

- FAVORITES

  This button will load the favorites page of the visualization.

- RESTART APP

  This button will delete the cached data, terminate the app and restart it after a short delay. This is a sure way in order to get up-to-date content from the server.

- RELOAD

  This button will simply reload the content of the visualization, however cached data is kept.

- SETTINGS

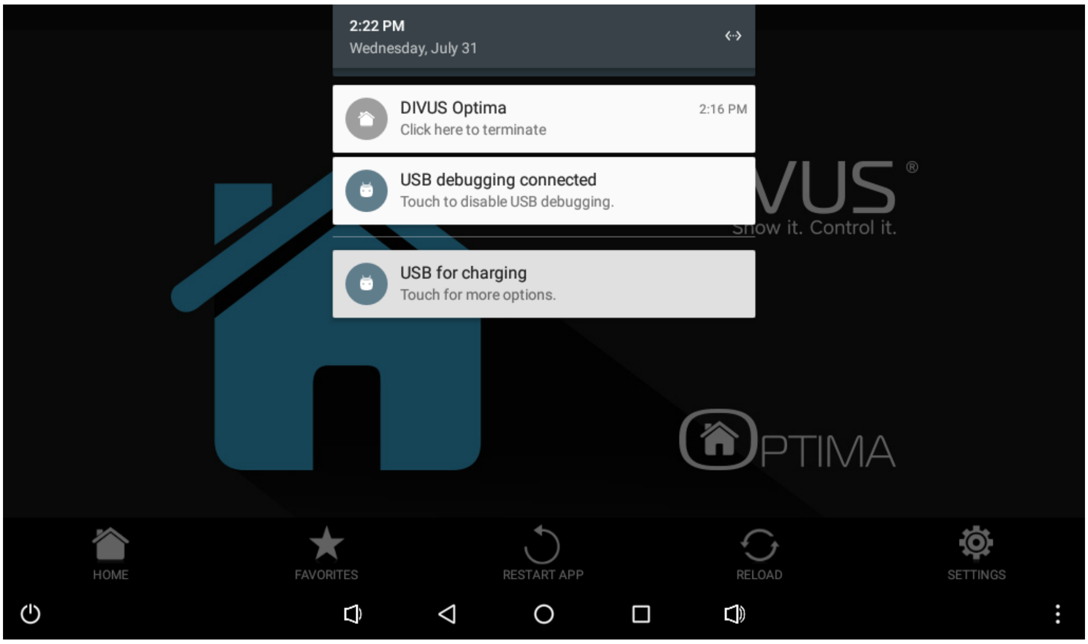
  This button is used in order to open the settings of the app, where DIVUS OPTIMA can be configured.

The single buttons or even the whole toolbar can be hidden, as will be explained later in the manual.

Access to the settings can be password protected, thus allowing to change the settings of the app only to authorized personnel. The password can be set in the settings, by default no password is set. When no password is set then the access to the settings is unprotected, and no password prompt is shown.

2.2 BACKGROUND SERVICE

In order to improve user experience and reduce loading times the app makes use of service running in background which runs separately from the user interface. The main task of the background service is loading of the visualization from the DIVUS KNXCONTROL device and react to network changes if required. While the service is running the following notification is visible:



2:22 PM
Wednesday, July 31

DIVUS Optima 2:16 PM
Click here to terminate

USB debugging connected
Touch to disable USB debugging.

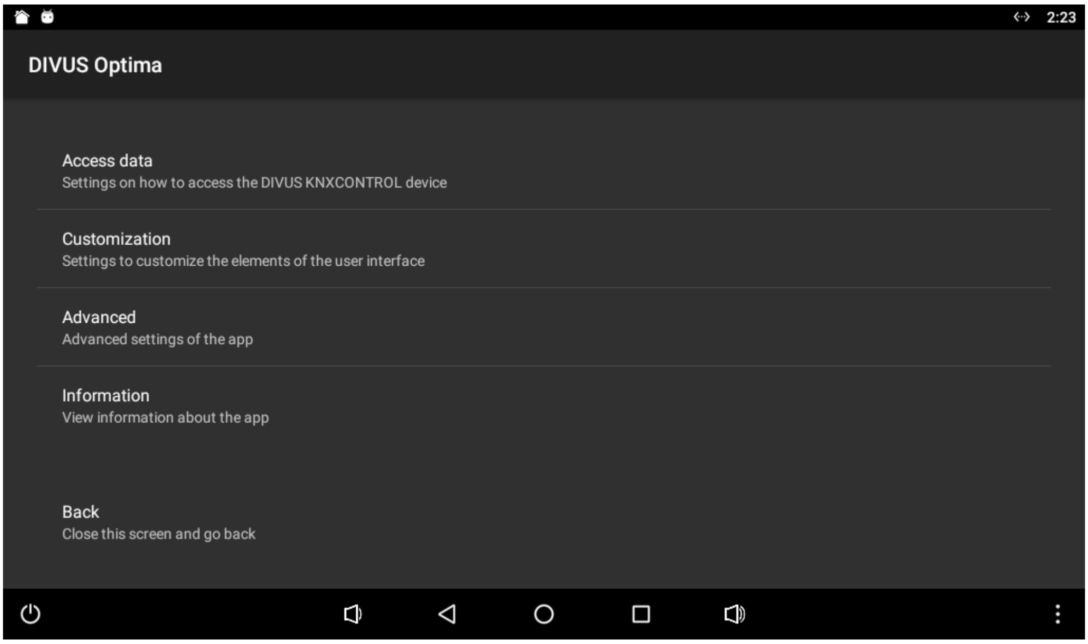
USB for charging
Touch for more options.

By clicking on this notification the background service and the whole app itself is terminated.

⚠ A service running in background may drain the battery quickly. If this is a concern it is advised to manually close the app through the notification whenever the app is not used.

3 Settings

The settings are accessible through the app menu, or through the dedicated button in the toolbar. There are various settings in the app which are grouped into various categories, as visible in the following screenshot:



Access data
Settings on how to access the DIVUS KNXCONTROL device

Customization
Settings to customize the elements of the user interface

Advanced
Advanced settings of the app

Information
View information about the app

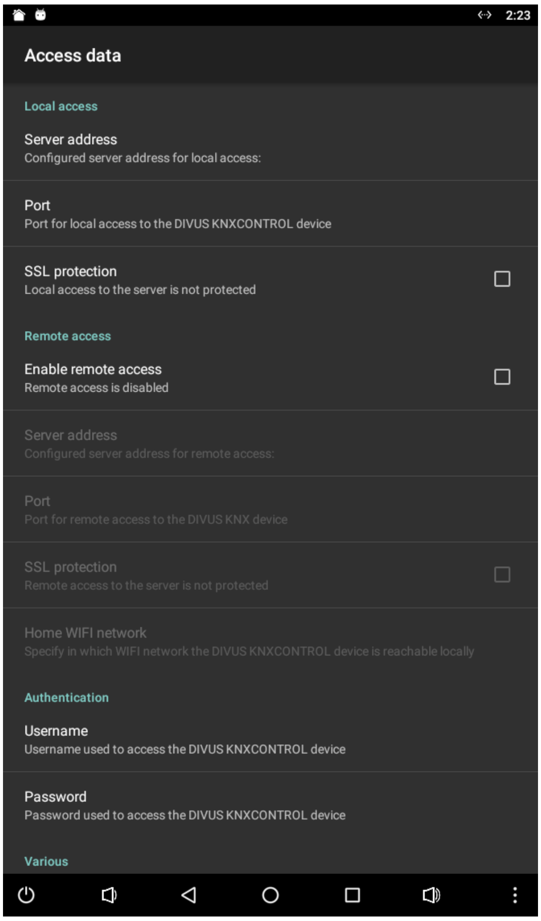
Back
Close this screen and go back

The various settings will be discussed in detail in the next sections of the manual.

The last option allows to close the settings and go back to the main view, adopting the new configuration.

3.1 ACCESS DATA

This category holds various settings required to access the DIVUS KNXCONTROL device.



2:23

Access data

Local access

Server address
Configured server address for local access:

Port
Port for local access to the DIVUS KNXCONTROL device

SSL protection ☐
Local access to the server is not protected

Remote access

Enable remote access ☐
Remote access is disabled

Server address
Configured server address for remote access:

Port
Port for remote access to the DIVUS KNX device

SSL protection ☐
Remote access to the server is not protected

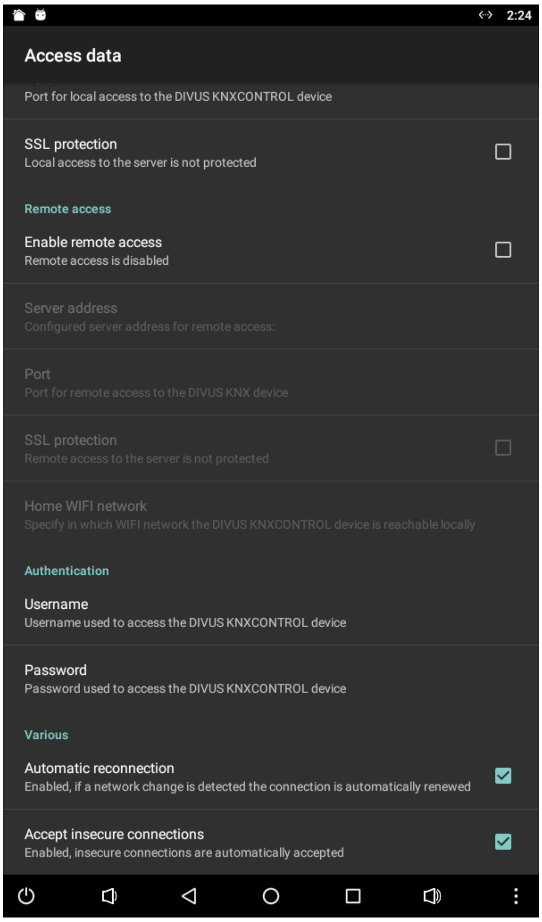
Home WIFI network
Specify in which WIFI network the DIVUS KNXCONTROL device is reachable locally

Authentication

Username
Username used to access the DIVUS KNXCONTROL device

Password
Password used to access the DIVUS KNXCONTROL device

Various



2:24

Access data

Port for local access to the DIVUS KNXCONTROL device

SSL protection ☐
Local access to the server is not protected

Remote access

Enable remote access ☐
Remote access is disabled

Server address
Configured server address for remote access:

Port
Port for remote access to the DIVUS KNX device

SSL protection ☐
Remote access to the server is not protected

Home WIFI network
Specify in which WIFI network the DIVUS KNXCONTROL device is reachable locally

Authentication

Username
Username used to access the DIVUS KNXCONTROL device

Password
Password used to access the DIVUS KNXCONTROL device

Various

Automatic reconnection ☑
Enabled, if a network change is detected the connection is automatically renewed

Accept insecure connections ☑
Enabled, insecure connections are automatically accepted

These settings are divided into various sections: local access, remote access, authentication and various.

3.1.1 LOCAL ACCESS

Here various setting for the local access to the DIVUS KNXCONTROL device can be configured.

First of all, the server address of the DIVUS KNXCONTROL device can be specified. Clicking on this setting will open a dialog which will perform a 5 seconds scan in order to discover devices in the currently connected network. After this scan the IP addresses of the found devices are listed, clicking on an address will select this DIVUS KNXCONTROL device for the local server address. Alternatively the server address can also be typed manually in the below text-box.

The next option allows to set the port to be used to connect to the server, by default 80. If SSL protection is enabled then in most cases also the port has to be adapted, usually 443.

As mentioned before, the last option allows to enable/disable SSL protection, disabled by default. Without SSL protection a regular HTTP connection is used, when enabled then HTTPS is used. If enabled, then additional certificates may be required on the device.

It’s also possible to access the server through port-forwarding, in this case the corresponding router address and port have to be used instead of address/port of the physical DIVUS KNXCONTROL device.

3.1.2 REMOTE ACCESS

This section holds various settings regarding remote access to the DIVUS KNXCONTROL device.

The first option allows to enable/disable remote access, disabled by default. Remote access is intended for situations where the DIVUS KNXCONTROL device should be accessed from various networks which may be local or remote and thus require different access data. Enabling this setting will unlock the other options related to remote access.

The next options specify the address and port of the DIVUS KNXCONTROL device to connect to when in a remote network. For the remote access the server address/port has to be entered manually.

Similar to local access, also for remote access it’s possible to enable/disable SSL protection, disabled by default. Without SSL protection a regular HTTP connection is used, when enabled then HTTPS is used. If enabled, then additional certificates may be required on the device.

The next options allows to configure how to handle the various WIFI networks. Clicking this option will open a prompt which ask for permission to access the device location, which is required in order to scan the currently reachable WIFI networks. If this permission is denied then the WIFI networks cannot be scanned. Next a dialog which will show the currently visible WIFI networks is displayed, where it will then be possible to select multiple WIFI networks and mark them as “home WIFI network”. When connected to a WIFI network marked as home WIFI network the local access data is used, else the remote access data. Alternatively the WIFI network SSIDs can also be typed manually, separated by a “;”.

It’s also possible to access the server through port-forwarding, in this case the corresponding router address and port have to be used instead of address/port of the physical DIVUS KNXCONTROL device.

Local/remote access while connected to a WIFI network is handled through the corresponding “home WIFI network” setting. Ethernet connection will always use the local access data, whereas mobile data will always use remote access data.

3.1.3 AUTHENTICATION

This section holds various settings regarding authentication used when connecting to the DIVUS KNXCONTROL device.

Access to the DIVUS KNXCONTROL device is protected by username/password, which have to be added in the corresponding settings in order to access the visualization. This access data is used both for local and remote access. Should the provided login data be wrong, then loading the visualization will stop during the authentication step and the username/password can be entered manually. Should the access data be valid, then the app will perform the login automatically and directly load the visualization without further user input.

ℹ Contents of the visualization may differ between different username/password.

3.1.4 VARIOUS

This section holds miscellaneous settings regarding the server access.

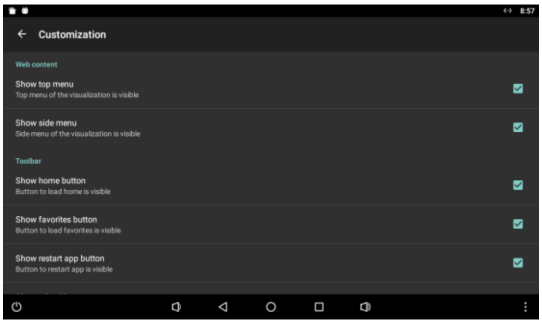
The first option allows to enable automatic reconnection on network changes, enabled by default. When enabled the app will listen for network changes and should a change be detected, then the app reloads again the content of the visualization and also handles switching between local/remote access data. When the automatic reconnection is disabled the app will not reload any content and retain the current loaded data.

⚠ With disabled automatic reconnection it can happen that the app may still display the visualization, but is no more functional as access to the DIVUS KNXCONTROL device may no more be possible.

The next option configures if the app should automatically accept all insecure connections, enabled by default. When disabled and trying to access an insecure connection, then the app will display a dialog which will require manual user input to either proceed or abort loading. If this option is enabled, then the app automatically accepts all insecure connections without user interaction.

3.2 CUSTOMIZATION

This category holds various settings regarding the customization of the app in its general appearance.



8:57

Customization

Web content

Show top menu
Top menu of the visualization is visible ☑

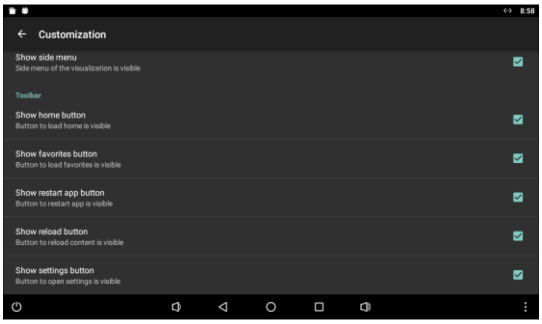
Show side menu
Side menu of the visualization is visible ☑

Toolbar

Show home button
Button to load home is visible ☑

Show favorites button
Button to load favorites is visible ☑

Show restart app button
Button to restart app is visible ☑



8:58

Customization

Show side menu
Side menu of the visualization is visible ☑

Toolbar

Show home button
Button to load home is visible ☑

Show favorites button
Button to load favorites is visible ☑

Show restart app button
Button to restart app is visible ☑

Show reload button
Button to reload content is visible ☑

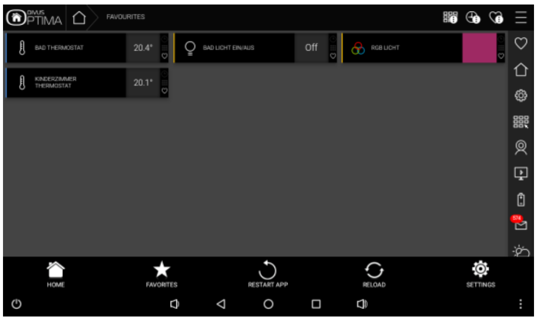
Show settings button
Button to open settings is visible ☑

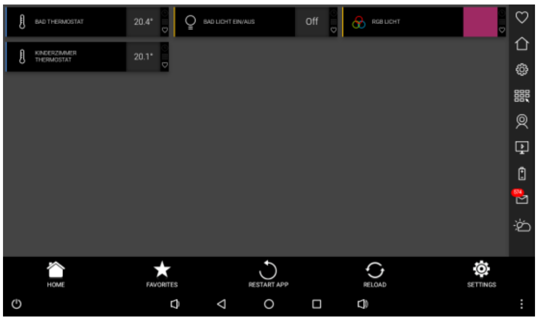
These settings are divided into various sections: web content and toolbar.

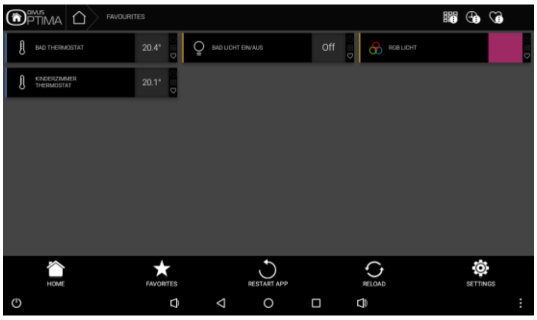
3.2.1 WEB CONTENT

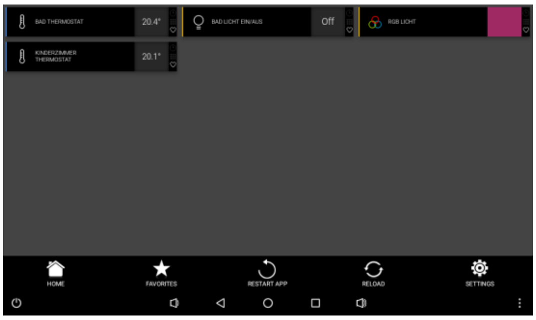
Here various settings for visibility of various web content elements can be configured.

The first option configures whether the top menu in the visualization is visible, by default set to visible. Should this be disabled then the top menu in the visualization is no more visible. The other option configures whether the side menu of the visualization is visible, by default set to visible. Should tis be disabled, then the side menu of the visualization is no more visible. The following screenshots show the various possible configurations:









When both menus are set to not be visible, then the visualization will have the most space to display on screen. However, the navigation elements of the menu will no more be accessible.

3.2.2 TOOLBAR

Here the visibility of the various toolbar elements can be configured.

- Show home button

  Configures whether the home button in the toolbar is visible or not, by default set to visible.

- Show favorites button

  Configures whether the favorites button in the toolbar is visible or not, by default set to visible.

- Show restart app button

  Configures whether the restart app button in the toolbar is visible or not, by default set to visible.

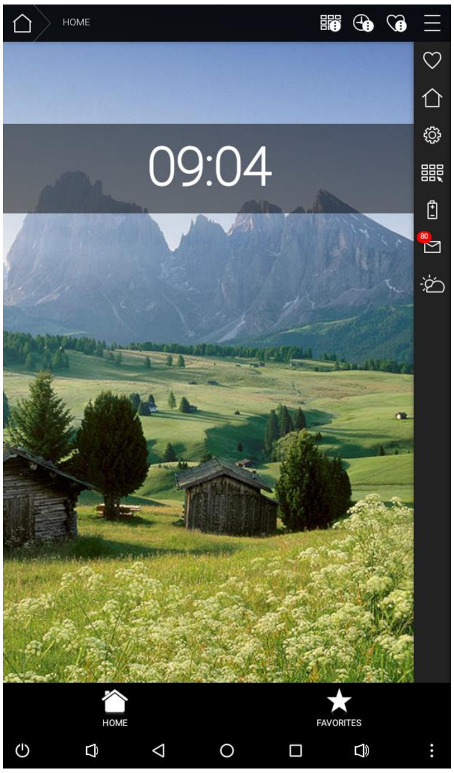
- Show reload button

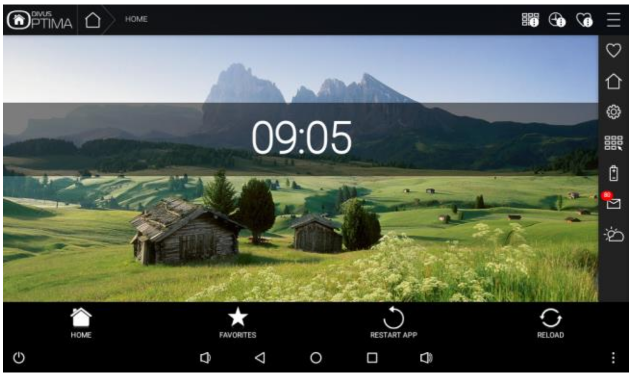
  Configures whether the reload button in the toolbar is visible or not, by default set to visible.

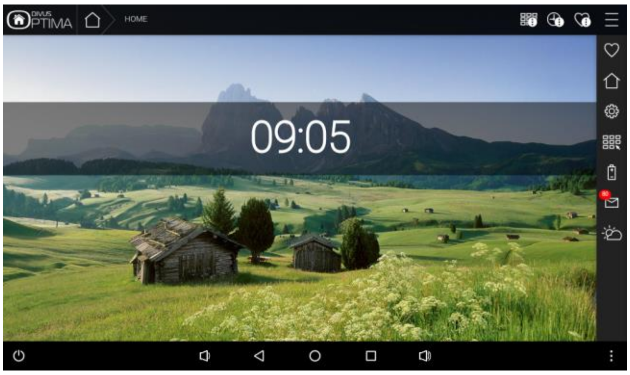
- Show settings button

  Configures whether the settings button in the toolbar is visible or not, by default set to visible.

The elements in the toolbar will always try to fill the whole width of the toolbar as best as possible, depending on the screen size, device orientation and number of visible elements. Below are a few examples of possible combinations:





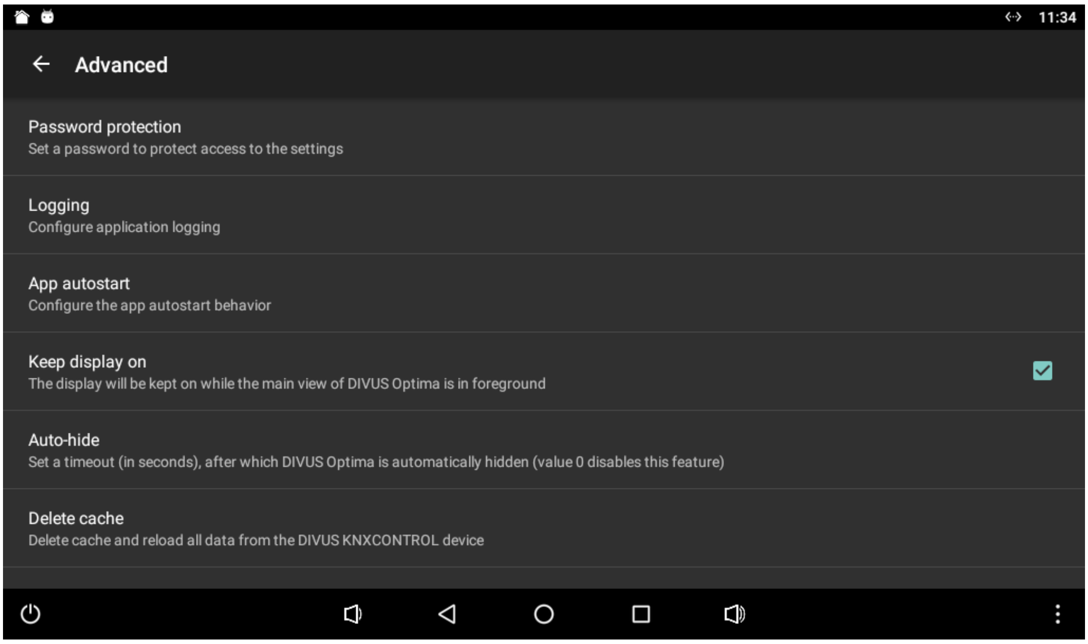


If all elements are set to be invisible, then the whole toolbar will become invisible, giving the visualization a bit more space on screen to display its elements.

⚠ When the settings button is set to invisible, it’s still possible to open the settings through the menu of the hardware/virtual MENU key of the device. However, not all devices possess a MENU key. If the settings button is set to invisible and the device does not posses a MENU key, then access to the settings of the app is permanently lost, unless the app itself is reset.

3.3 ADVANCED

This category holds various advanced settings of the app.



Advanced

Password protection
Set a password to protect access to the settings

Logging
Configure application logging

App autostart
Configure the app autostart behavior

Keep display on ☑
The display will be kept on while the main view of DIVUS Optima is in foreground

Auto-hide
Set a timeout (in seconds), after which DIVUS Optima is automatically hidden (value 0 disables this feature)

Delete cache
Delete cache and reload all data from the DIVUS KNXCONTROL device

As mentioned before in this manual, the first option allows to configure a password to protect access to the settings from unauthorized personnel. Clicking on this setting will open a dialog through which a new password can be set, after providing the current password and repeating the new password twice. When a password is set, a prompt will be displayed when trying to open the settings, and access to the settings is granted only by providing the correct password. By default no password is set and access to the settings is unrestricted.

The next option opens a sub-menu with various configuration regarding logging. By default logging is enabled and information about the app operations are logged to a file, when logging is disabled then no information is recorded. The next option allows to manually send the logs to DIVUS, which can be required for technical assistance. The next option allows to periodically send the logs automatically to DIVUS, this setting is intended for long-term support and should only be enabled when told to do so by the DIVUS team. Finally, the last setting allows to delete the currently logged data.

The next option opens a sub-menu where it’s possible to configure the app autostart behaviour. By default app autostart is disabled and thus the app will not start automatically once the device is started, requiring manual start of the app. When enabled, then an additional setting becomes available which allows to set a delay when the app autostart should be performed, after the device has completed boot. Two types of autostart are available: background and foreground. Foreground is a regular autostart in which the app will come in foreground and load the contents. The background autostart is less intrusive and only starts the background service which will in turn load the visualization in background, thus when opening the app the first time the contents are already loaded.

The next option may modify the power management behaviour of the device while the app is open. By default “keep display on” is enabled, thus while the main view of the app is in foreground it will prevent the device from turning off the screen. When this setting is disabled, then the screen may turn off as configured in the power management settings of the device.

The next option allows to configure an auto-hide for the app, by default set to 0 and thus disabled. Clicking this option will open a dialog in which it will be able to insert a timeout (in seconds). If a timeout is set, while the main view is open and hasn’t been actively used by the user for the set time, then the app will automatically close once this time has run out. Only the main view of the app is closed, background service will still be running and loaded data is kept.

The last option allows to manually delete all cached data and force a reload of the web content. When clicking on this setting the procedure is started immediately, and when going back to the main view the content is already loading.

3.4 INFORMATION

This last category holds some general information about the app. In the first part there are general information about the app: app version, copyright and privacy policy. The second part contains contact information in order to contact DIVUS in case of technical assistance: homepage, e-mail and telephone number.