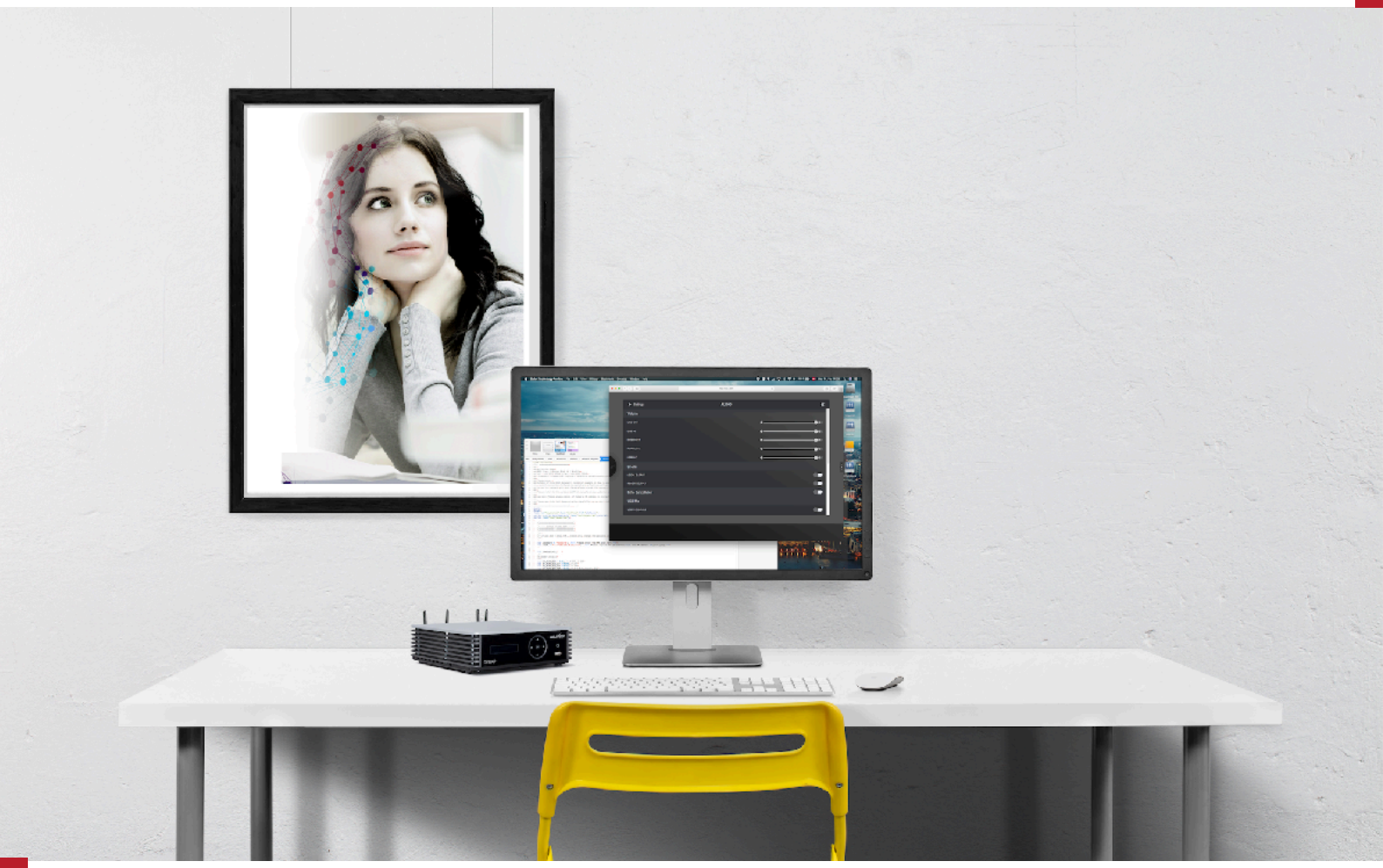
Cynap API

WolfProt

Developer's Guide

WOLFVISION



Foreword

Cynap, Cynap Core and Cynap Pure are our most innovative and outstanding systems. They offer a level and complexity of collaboration services which, so far, has never before been possible.

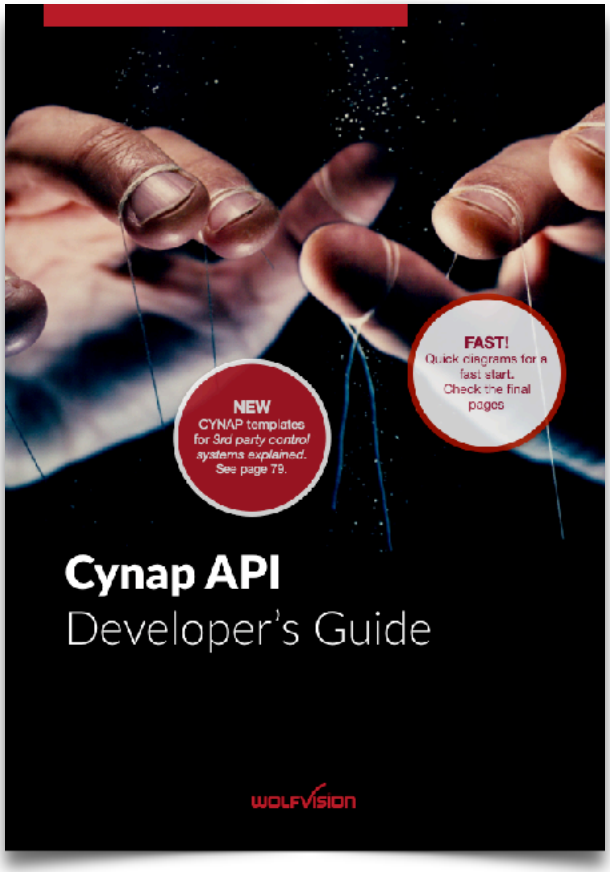
Cynap API, our command language for controlling Cynap, Cynap Core and Cynap Pure functions has been extended. It provides you with a sophisticated and versatile interface, enabling a broad range of options for customising your own installation.

These award-winning products are already considered to be a significant step forward in collaborative working and learning space design . With your added integration and customisation skills, I'm sure that you will create an outstanding setup!

Andreas Ganahl
Head of Innovation and Product Management

Table of Content

Structure



Part 1: Basics
How Cynap APIs work.

Part 2: Cynap devices
About Cynap services and their setup. Plus how the system (windows, file systems, etc.) works.

Part 3: Tutorials
Practical examples and tutorials on how to use WolfProt with Cynap and Cynap Core.

Part 4:Module for your 3rd party ctrl
Implementing 3rd party controllers layout and libraries provided by WolfVision.

Part 5: Troubleshooting
if you did everything right and it still doesn't work…

Part 6: Quick Guide
The fastest way to start coding with Cynap APIs

Networking Guides

For networking related topics please download **vSolution Cynap Network Integration** PDFs from our website.
| **Download**

Help file (available online and installed on every Cynap)

For general service description please read **vSolution Cynap Detailed Help Guide** from our website.
| **Visit help**

Cynap API Developer's Guide

1 Introduction

Cynap API (part of WolfProt protocol): A simple and fast way to operate Cynap from your 3rd party controller or from a customised webpage using web-sockets.

Our Cynap API command language aims to offer versatility and sophisticated access when it comes to develop your next room control integration.

The commands allow to use functions beyond the scope of its pre-defined user interface (e.g. setting a customised AirPlay PIN instead of having a randomised one generated by Cynap).

Our WolfProt APIs do work on all our products but this guide covers WolfProt integration on Cynap and Cynap Core.

About PJLink:
Cynap itself supports PJLink protocol to send out commands to PJLink controllable devices (e.g. monitors, projectors, etc.). WolfProt behaves similar to PJLink with its set and get command types.
Peripheral Commands on Cynap are not part of this documentation.
Read more about PJLink: PJLink English and head to the Hands On part where an example has been provided

1.1 Disclaimer

This manual is intended for Room Management System developers. Therefore it is assumed that you already have a good understanding of AMX/Crestron/Cue-system programming and integration (see http://www.howtoprogramcrestron.com/resources.html for Crestron integration or http://www.amx.com/products/NetLinxStudio.asp for AMX integration).

We strongly advise to adapt our demonstration modules to your customer needs before installing the provided demonstration template to improve its performance.

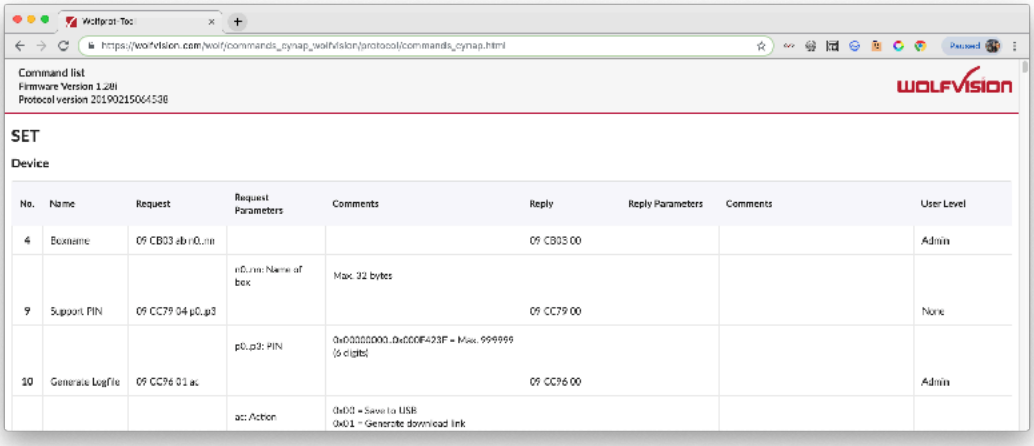
Knowledge of TCP/IP networking is beneficial. It is also assumed that your processor and touch panel/terminals are installed and do function correctly and reside on the same network (Wi-Fi or Ethernet) as Cynap.

Integration of Cynap and Cynap Core at customers site requires an in-depth knowledge of how Cynap and Cynap Cores are working.

1.2 Read more about Cynap APIs

If you're reading this document to find the latest commands in WolfProt, then please have a look here:

Cynap	https://wolfvision.com/wolf/commands_cynap_wolfvision/protocol/commands_cynap.html
Cynap Core	https://wolfvision.com/wolf/commands_cynap_wolfvision/protocol/commands_cynap_core.html
Changes in APIs	https://wolfvision.com/wolf/commands_cynap_wolfvision/protocol/changes_cynap.htm
All Visualizer products	https://wolfvision.com/wolf/protocol_command_wolfvision/protocol_command.htm#t=general_information%2Fabout.htm



HTML output of Cynap APIs on wolfvision.com

1.3 Help and Support

We do provide a number of support documents to help you integrate Cynap into your environment.

Please browse on the various download sections of our website, https://www.wolfvision.com or call us in case you need support.

Please make yourself familiar with the operations and installation procedures of Cynap by reading its *extensive HELP file* accessible through Cynap's *control center*.

We are, however, unable to support you with skills in programming languages needed to build your Room Management System solution.

For a quick start, WolfVision provides you with libraries and templates for AMX, Crestron and Extron (Extron Cynap/Cynap Core templates are developed by Extron and are available on their partner website). For more information please check part 5.

Part 1: Cynap API basics

Programmer, a machine that turns coffee into code.

How Cynap APIs work and how they respond.
Also, where to find the latest Cynap API command list.

2 Cynap API

Cynap API is based on WolfProt, the command language for all Wolfvision products.

At first it needs to be activated and configured (Enable and set Room Management System user).

The commands are divided into **GET** and **SET** commands. Commands require an authenticated user (if no user login password has been set, then the command automatically is granted user level access).

GET commands retrieve information from the devices; SET commands change settings or initiate a direct command. WolfProt commands are organised in request-reply pairs (SET/GET).
They start with a header, followed by the command, the length of the following parameters and the value of its parameters.

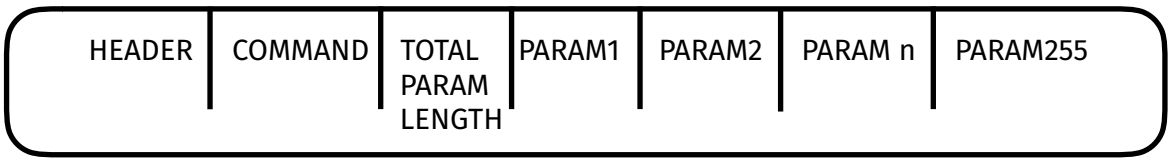
If you send a SET command you need to follow up with the appropriate GET command to check, if the SET command got executed. Return codes simply tells the agent that the command has or hasn't been received on Cynap/Visualizer.

Connection	**Ethernet or Wi-Fi, protocol is TCP/IP**
Cynap port - unencrypted	**50915**
Cynap port - encrypted	**50917**
WebSocket - unencrypted	**ws://{Cynap-IP}/xxx**
WebSocket - encrypted	**wss://{Cynap-IP}/xxx**

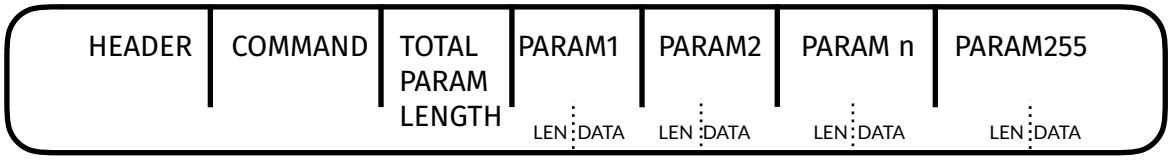
2.1 Cynap API Command Structure

There are no parameter delimiters, therefore some parameters need a prerequisite length of a parameter to function.

Command with no sizeof value in parameter
An example could be a command to mute audio



Command with custom size of parameter
Some parameters require an additional size value and it renders the parameters into required size and data value pair. (e.g. size of URL and the URL itself, etc.).
An example could be a command that opens a window with content type of browser and a URL



Please check each command, what kind of parameter and how the parameters are structured.

2.2 Header Definition

The header defines the size and the command mode. A GET commando queries values from the system and SET commands execute a defined function or change a configuration setting.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Reserved	**Reserved**	**Reserved**	**Reserved**	**0 Cmd 1 Byte**	**0 Len 1 Byte**	**0 Header 1 Byte**	**0 GET Cmd**
Reserved	**Reserved**	**Reserved**	**Reserved**	**1 Cmd 2 Byte**	**1 Len 2 Byte**	**1 Header 2 Byte**	**1 SET Cmd**

Commands requiring larger parameter sizes might need more allocated space which are being defined when using the command itself.

Get status command	Start with 08
Execute commands	Start with 09
Large execute commands (e.g. URL as a parameter)	Start with 0D

*(e.g. execute start video recording **09** CB 25 01 00)*

2.3 Return Codes

OK and ERROR reply bits that are not specified remain unchanged as in GET/SET command. The command 0xFF is reserved as an error code for an unknown command.

Return	Description	1	*Time out*
2	*Invalid command*	**3**	*Invalid parameter*
4	*Invalid length*	**5**	*Queue full (FIFO)*
6	*Firmware update error*	**7**	*Access denied*
8	*Authentication required*	**9**	*Busy*

For instance:

Start Video Recording	Command	Replies	
	09 CB 25 01 00	09 CB 25 00	*OK*
	09 CB 25 01 40	89 CB 25 03	*Invalid parameter*
	01 11 01 10	81 11 02	*Invalid command*

There are 10 return codes in total. The return codes are placed in Header Bit 7 in the return message. To know, if a command succeeded you need to send a get command to receive the status of your request.

The reply packet to each command tells you:
- on set commands: the command got executed
- on get commands: the status or parameters that have been set on Cynap

Otherwise you will receive an error code if you did violate the protocol.

Please be aware that if you don't get a reply packet after sending a set command, you're not violating the protocol but the socket is still expecting some additional values and waits forever for its completion.

Example: when sending a larger number on "parameter length" but not providing the necessary parameter (e.g. size of *cynap.net* of 9 chars as being 20 chars).

A common mistake is using the wrong AccessLevel; not being logged in at all or logged in as User when an Administrator log in is required.

Example:
Request the streaming resolution (Administrator log in required) and being connected to Cynap as User and issuing a GET command.

Request streaming resolution >> 08 CB 23 00

When logged in as Administrator you will receive one of:
- 08 CB 23 01 00 (Full HD)
- 08 CB 23 01 01 (HD)
- 08 CB 23 01 00 (qHD)
- 08 CB 23 01 00 (nHD)

When not logged in or logged in as User you will receive ERROR
- **88 CB 23 07**

Same happens with a SET command when you're not logged in as Administrator

Set streaming resolution >> 09 CB 23 01 00 (for Full HD)

When not properly logged in you will receive following hex values:
- 89 CB 23 07

Pro tip:
To quickly translate ASCII into hex use one of the many online hex converters -, your calculator might have a developer mode to calculate hexadecimal values.

2.4 How to read the Cynap API command list PDF

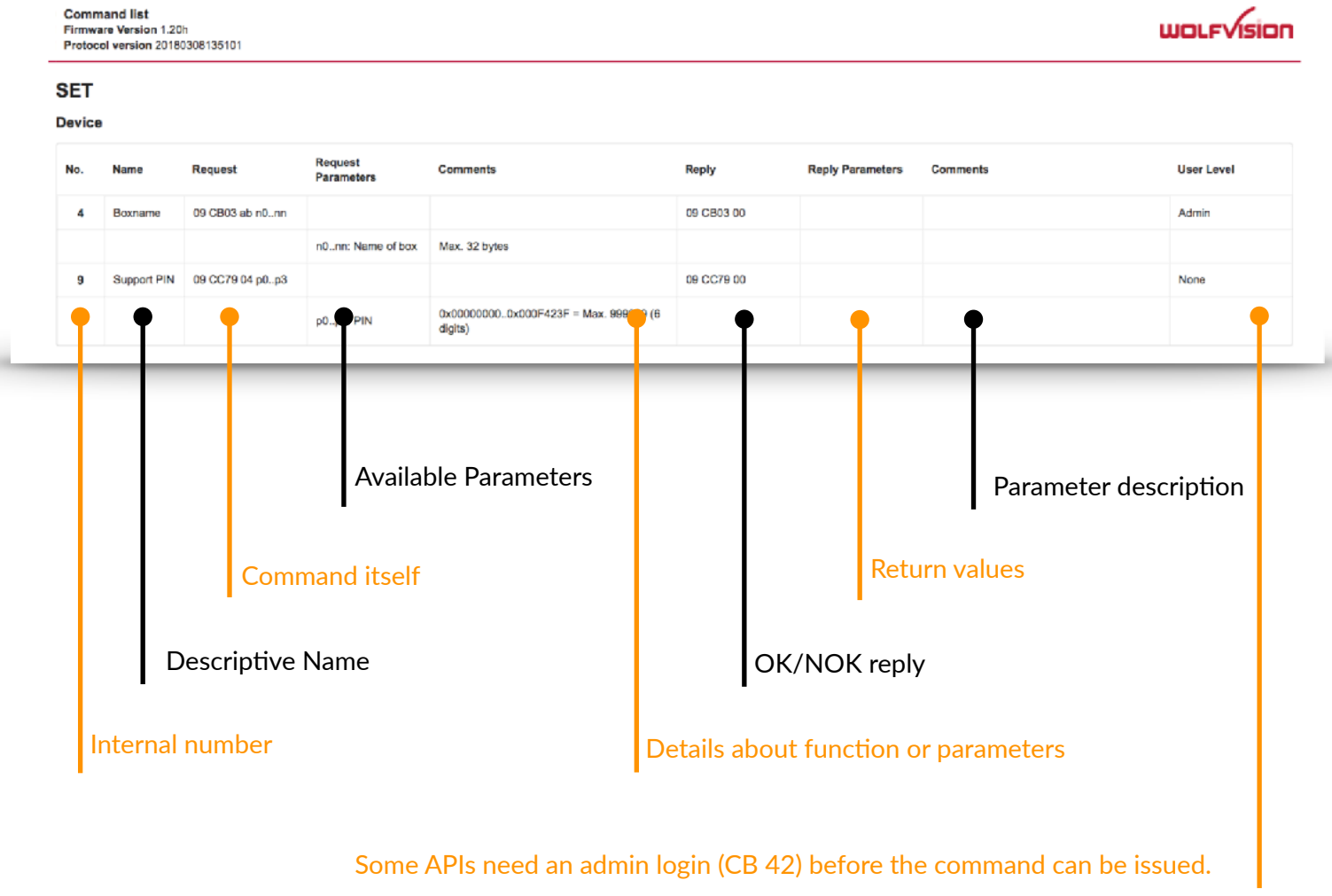
With each firmware update for Cynap, Cynap Core , and Cynap Purethere will be an updated Cynap API Command List PDF available on the Web.

Download link:
https://www.wolfvision.com/wolf/commands_cynap_wolfvision/protocol/commands_cynap.html

CB Remote (virtual remote control) consists of sending remote control commands by offering a button-function combined with a short press, long press and a long press-release.

09 CB01	**Start** of Request, containing command (e.g CB01 -> CB Remote control
02	**Followed** by the size of total following bytes as parameters, sometimes referred as AB in command list.
03 03	**Followed** by its parameters (sometimes additional length parameters are required (e.g. Password-size and password values).

Please make yourself familiar with the command structure before implementing new functionalities. For further insight of the Cynap APIs, please try to use some of the examples in the Hands-On-part of this document below.



Part 2: Cynap family specs and functions

3 Cynap

Cynap is a collaboration device which supports a large number of resources (videos, office formats or images), several input sources (on 2 HDMI in) on up to 4 windows as well as internal functions such as Recording/Streaming and Annotation, Whiteboard or WebRTC.

I won't go into details of all past, present and upcoming Cynap and Cynap Core features.

Please check our YouTube channel where all functions are being explained in detail.

Cynap functions explained:
https://www.youtube.com/user/WolfVisionVisualizer

3.1 Cynap specifications

System

Operating System	Linux
Memory	8GB
Internal storage	64GB
Output resolutions	Up to 4K UHD: 2160p60 (4.2.0), 2160p30 (4.4.4), 1080p60 (4.4.4), 1080p30 (4.4.4)
Compatible mobile device operating systems	iOS, Android, Mac OS, Windows, Windows Mobile, current HTML5 browser
Supported image file formats	GIF, JPEG, BMP, PNG
Supported document file formats	PDF, Word, PowerPoint, Excel, Text, HTML
Supported video file formats	AVI, WMV, MOV, MP4, DivX, MKV, M4V, OGV
Supported audio file formats	MP3, WMA, MKA, OGA, OGG
Supported mirroring protocols	AirPlay, Google Cast, Miracast (no HDCP support), vSolution Cast (up to 30 fps)
HDCP support	Yes, (HDCP 1.4)

Table 1: System specifications

Inputs and Outputs

Video input	HDMI x2 (HDMI 2.0)
HDBaseT 1.0 Input	x 1
Video output	HDMI x2 (HDMI 2.0)
HDBaseT 1.0 Output	x 1
Audio	Line in / Line out (3.5mm mini jacks)
USB ports	Rear USB 3.0 ports x4, front USB 2 port x1, FAT32 limited to 4 GB files

Table 2:Input/Outputs

3.2 Cynap functions

Features

Max. no. of devices simultaneously displaying content on screen	4
Max. simultaneous receiver connections via Capture app	Virtually unlimited (dependent on network infrastructure)
Wireless device mirroring	Yes
Streaming protocols	RTSP, RTP (Unicast/Multicast), RTMP (WebCasting FP)
Local video recording	Yes, 1080p, 30fps
Cloud services	Yes, Box, Google gDrive, Dropbox,
Access to network drives	Yes
Document and media player	Yes
Whiteboard and annotation	Yes
Presentation modes	Protected and open mode
On-screen content arrangement modes	Dynamic
Web conferencing	WebRTC
Dual screen modes	Yes
Integrated web browser	Yes
Customizable background image	Yes

Table 3: Cynap features

4 Cynap Core

Cynap Core offers most of Cynap functionalities.

For instance you are able to send a video stream to a Cynap Core but you are not able to receive a video stream from a Cynap Core since no stream output functionality has been implemented.

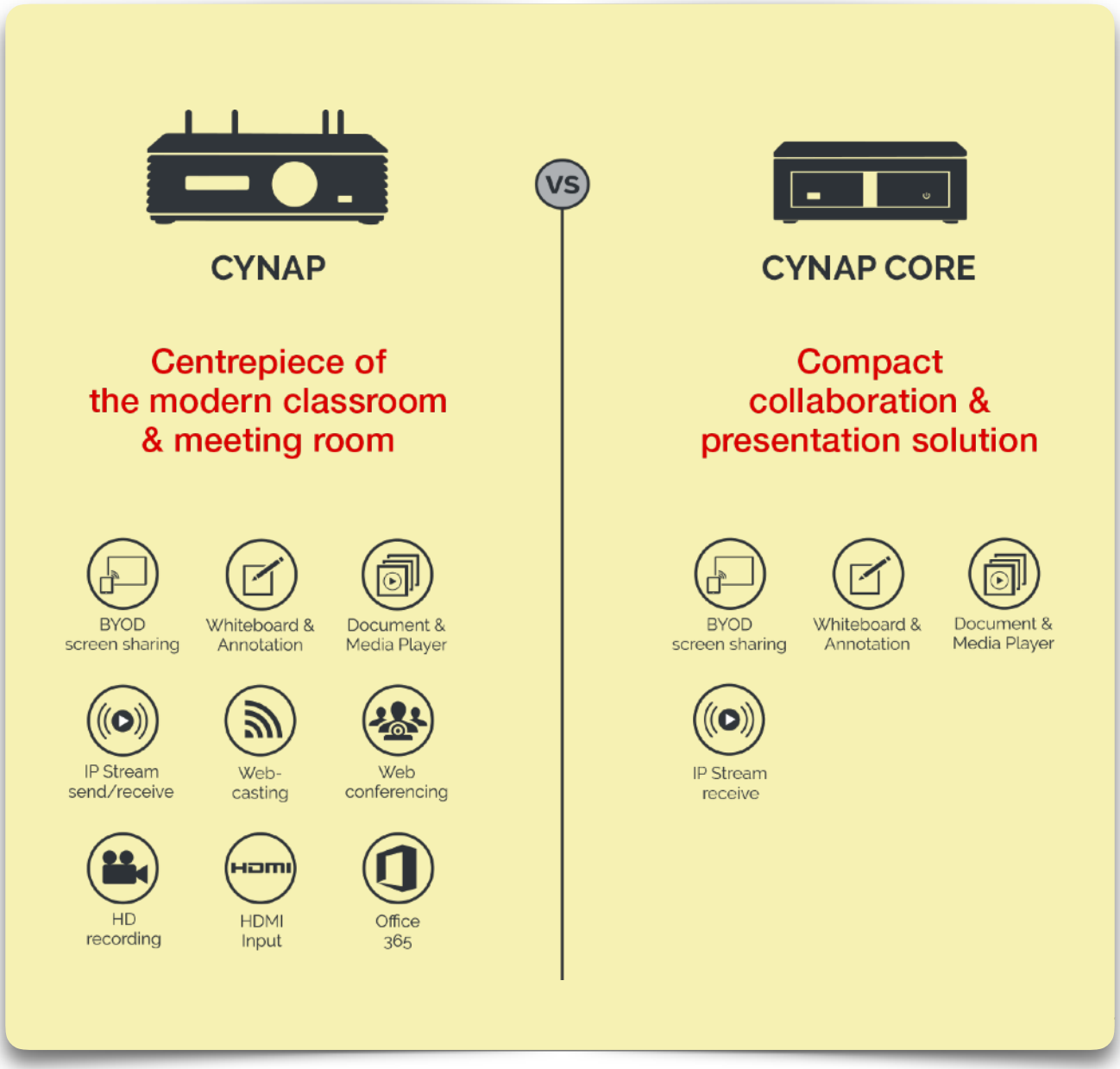
Templates for 3rd party controllers (room control systems/room managements systems) are available for all systems.

Commands haven’t been changed and you are able to use the same commands for Cynap or Cynap Core with the difference that some functions aren’t available on Cynap Core based on its limited functions and hardware configuration.

4.1 Cynap Core features

Document and media player	Yes
Compatible device operating systems	All iOS, Android, Mac OS, Windows, Windows Mobile devices, and all current HTML5 supported browsers
Supported mirroring protocols	AirPlay, Chromecast, Mirrorcast, vSolution Cast
Cloud services	Yes, Google Drive, Dropbox, Box, Jianguoyun, OneDrive, WebDAV protocol
Annotation and whiteboard	Yes
Integrated web browser	Yes
Max. no. of open windows	4
Max. resolution	2160p30

4.2 Comparison Cynap vs Cynap Core



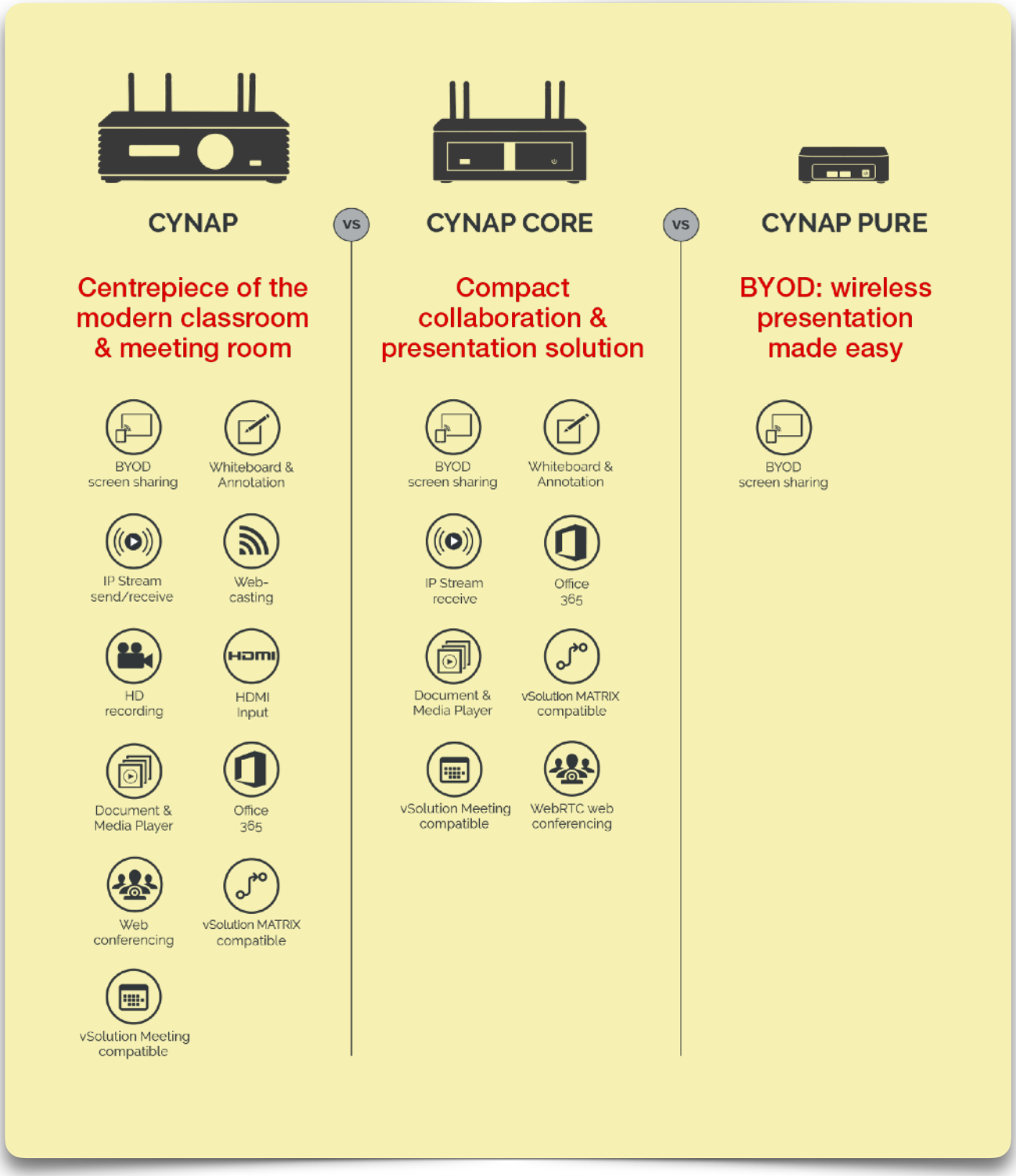
5 Cynap Pure

Cynap Pure offers the same Screen Sharing experience as on Cynap and Cynap Core.
Limited to screen sharing, the Pure still offers additional services not visible to the common user, for instance, you are able to use the Peripheral Controls to send PJLink commands or send Cynap API commands to control Cynap (e.g. standby, screensaver, WakeOnLAN, activating splash screen etc.)

5.1 Cynap Pure features

Compatible device operating systems	All iOS, Android, Mac OS, Windows, Windows Mobile devices, and all current HTML5 supported browsers
Supported mirroring protocols	AirPlay, Chromecast, Mirrorcast, vSolution Cast
Max. no. of open windows	4
Max. resolution	2160p30

5.1 comparison Cynap vs Cynap Core vs Cynap Pure



6 Connectivity

Wi-Fi standards	802.11 a/b/g/n/ac
Wi-Fi Bands	2.4 and 5 GHz
Data rate	Wireless up to 900Mbps
Network protocols	TCP/IP, FTP, HTTP, HTTPS, SNTP/NTP, RTP, RTSP, RTMP
IP configuration	DHCP, Static, network interface priority
Security encryption	WEP, WPA2, WPA Enterprise or IEEE 802.1x
Max. wireless coverage	Environment dependent
LAN ports	Yes, 2x 1GigE

Table 4: Network connectivity

Cynap supports WolfProt on all networking interfaces. To use it, you simply need to know the IP address of the networking interface you intent to use and also the proper port.

You are able to connect Cynap over a BSD socket or a WebSocket. Using WebSockets instead of BSD sockets offers simplified implementation methods if you want to encrypt access to Cynap using SSL. It also adds JavaScript as new method to control your Cynap or Cynap Core.

Before issuing a command you have to make sure that you're connected to Cynap and logged in as Room Management System user (open socket) or as an admin in case you need to change settings on the fly.

The second LAN port has been provided with a Room Control System in mind. In order to use it, you have to decide if you're binding Cynap into an existing network (LAN2-> set Interface mode to LAN) or if Cynap needs to handle IP addresses (LAN2->Interface mode to WolfVision Visualizer).

Cynap offers TLS encrypted connections – please make sure that you use the corresponding port (see Table 5: Firewall settings).
Cynap offers peripheral control to send specific commands on the attached network to a listening device (such as a projector); issued on startup or while Cynap's entering standby mode.

Cynap, once in standby mode, needs to be reactivated using Wake-On-LAN (sending a magic packet to Cynap's MAC address - LAN1 or LAN2).

6.1 Peripheral Control

Sending single commands to a remote unit (Visualizers and Cynaps included) allow for a very simple approach to start or shutdown a device.

You are able to send standardised commands (such as PJLINK) or device dependent commands (such as WolfProt) to be automatically sent while Cynap is booting up or shutting down.

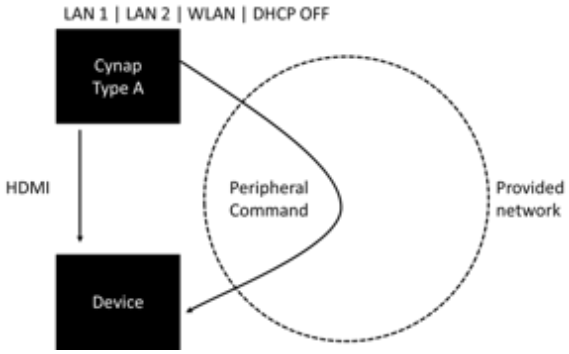
Simply enter the IP address of the device to be controlled along with its port number. Decide if a command is being issued on startup or while entering standby and then the command in hex format as well.

6.2 Integration options

Cynap offers 4 networking ports (3 usable and one solely reserved for Wi-Fi Direct/Miracast). LAN 1 and LAN 2 behave slightly different as LAN2 also supports Visualizer Ethernet Control support and, if activated as WolfVision port starts its own DHCP.

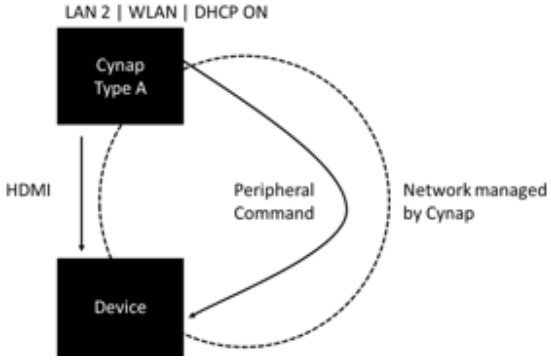
Networking port	Behaviour
Miracast	Wi-Fi only Wi-Fi direct – no support for peripheral control
LAN 1	Considered for being connected to company network DHCP client only
LAN 2	Considered for being connected to Visualizer and Room management system network DHCP client/server
WLAN	Wi-Fi network in client or access point mode DHCP client only
HDBaseT	Certified as Class A, Connected with LAN 2 and an activated DHCP server, a management connection could be established If managed device offers DHCP server functionality, LAN1 and LAN2 can be used (DHCP off)

Configuration 1: Cynap connected to existing customer network



Cynap and controlled device (such as a projector) reside on same network. IP´s on both devices are kept the same to successfully send command to device.

Configuration 2: Cynap providing its own Room Management System network

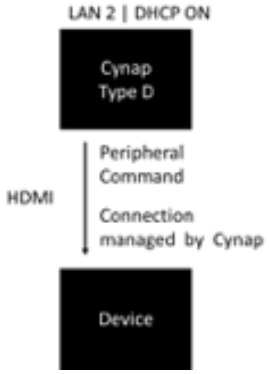


Cynap with DHCP ON creates a network for use with clients and managed devices.
LAN2 with Visualizer on or WLAN in Access point mode starts the DHCP.

Be aware that a Cynap in Access point mode can be detected and used by any device, whereas network access to the network on Ethernet port/ LAN 2 can be protected.

Only a very limited range of IPs is available when activating the DHCP on LAN 2 (from 172.31.255.202 to 172.31.255.210).

Configuration 3



Cynap supports HDBaseT Class A – therefore you are able to send USB, Data and HDMI traffic to your device on a single cable based connection.

On Cynap:
Connect LAN 2 with the HDBaseT Ethernet port.
Activate the DHCP server (Visualizer mode)

On HDBaseT connected device
Based on HDBaseT functionality add a HDBase IP/HDMI splitter.
Read IP Address

On Cynap:
Enter IP address in Peripheral Command settings.

6.3 Serial connectors

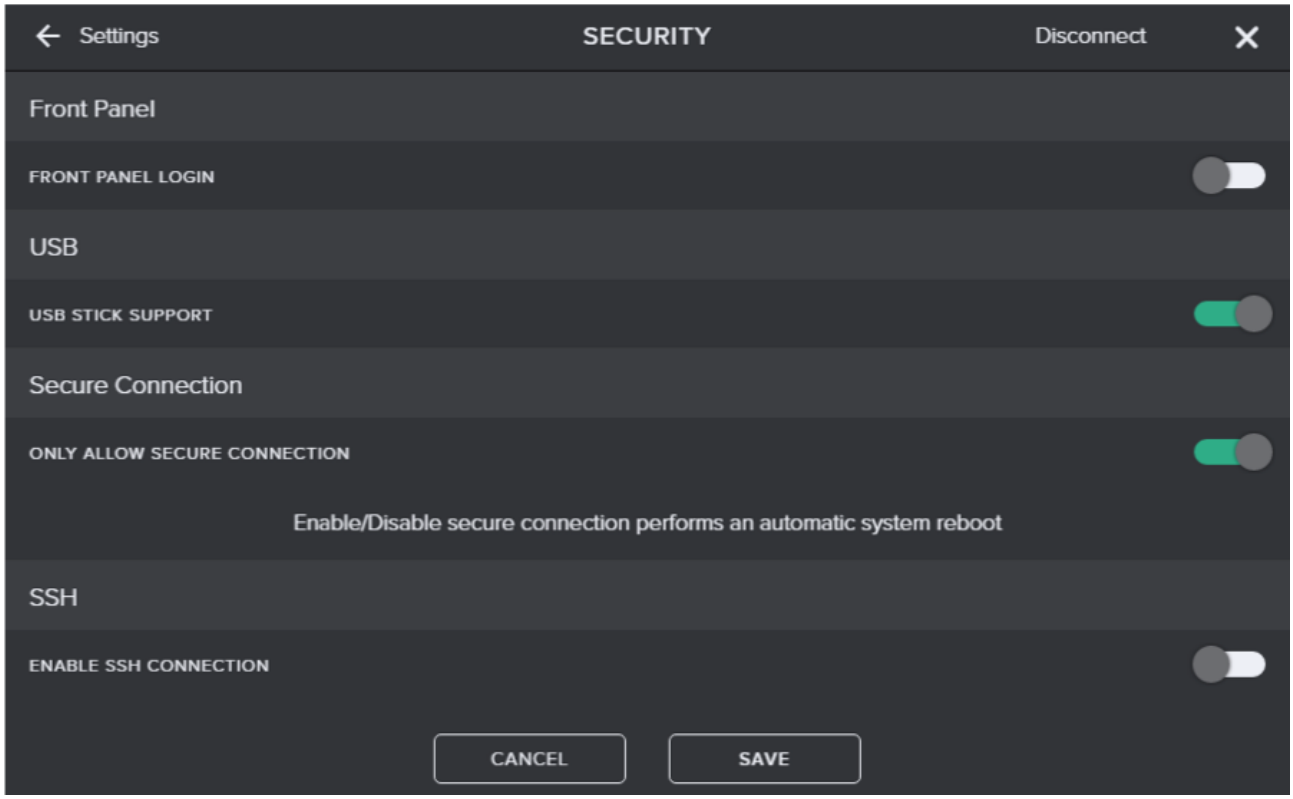
Cynap has no serial connector - to use your existing management system based on serial network, please make sure that you use a RS323-LAN adaptor to send commands to Cynap. Most work perfectly but before buying bulk please test them before purchase.

6.4 Cynap API and Visualizers

WolfProt has been extended and simplified for use with Cynap. CynapAPIs are available to control a Cynap connected Visualizer.

Cynap and Cynap Core offer both an unencrypted and encrypted socket connection at the same time.

You're able to force encrypted connections ***by switching on "Only allow secure connection"*** in the *security settings* in which case, the socket uses Port 50917 and blocks the connection on Port 50915.



6.5 Firewall settings

Port #		Feature	Description
50913	UDP/ TCP	WolfVision Device Discovery	Device Discovery (WOL, Wake-On-LAN) Port for WolfVision devices
50915	TCP	Cynap WolfProt	Communication between Room Management System and Cynap
50917	TCP	Cynap WolfProt protected by TLS	SSL encrypted connection to Cynap

Table 5: Firewall settings

6.6 Network information from the front panel

Function is limited to the Cynap as Cynap Core and Cynap Pure don't include a front panel.

Changing network settings for LAN1 and WLAN can be prevented by forcing a password check when applying network settings (SETTINGS—>SECURITY—>FRONT PANEL LOGIN).

1

Press Down Arrow-Key until you see **LAN Settings**

2

When you see LAN Settings, **press OK**

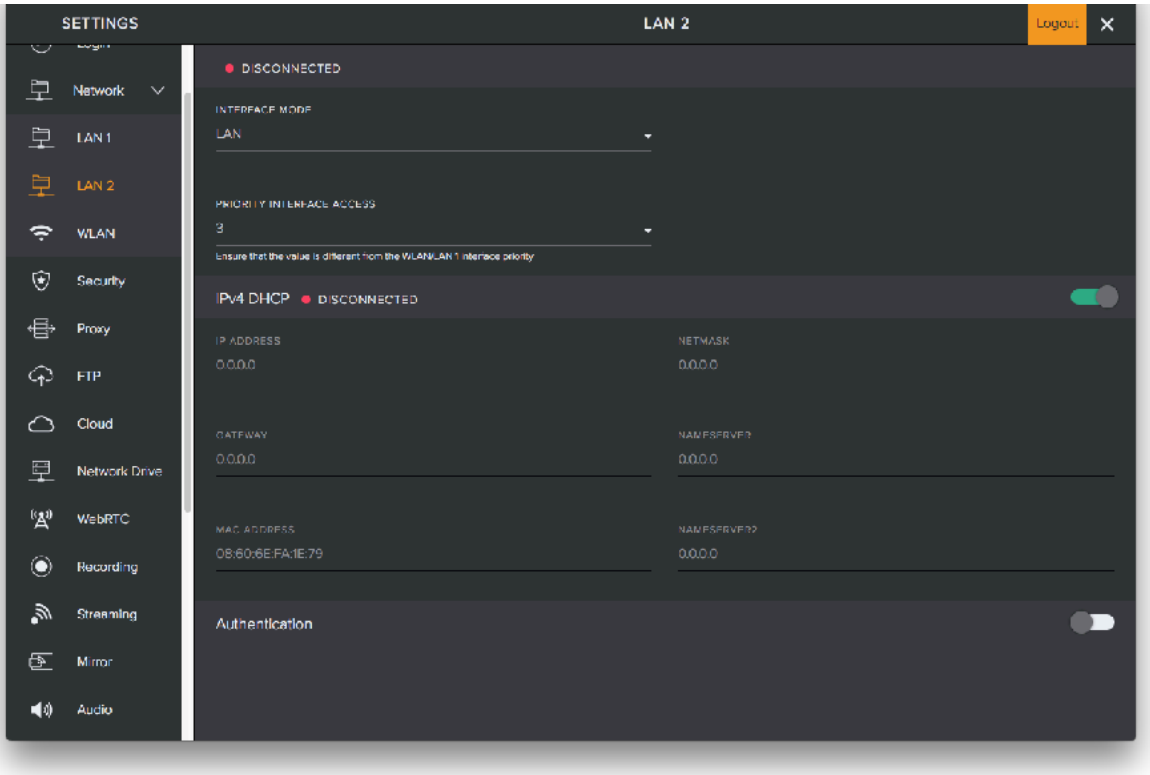
3

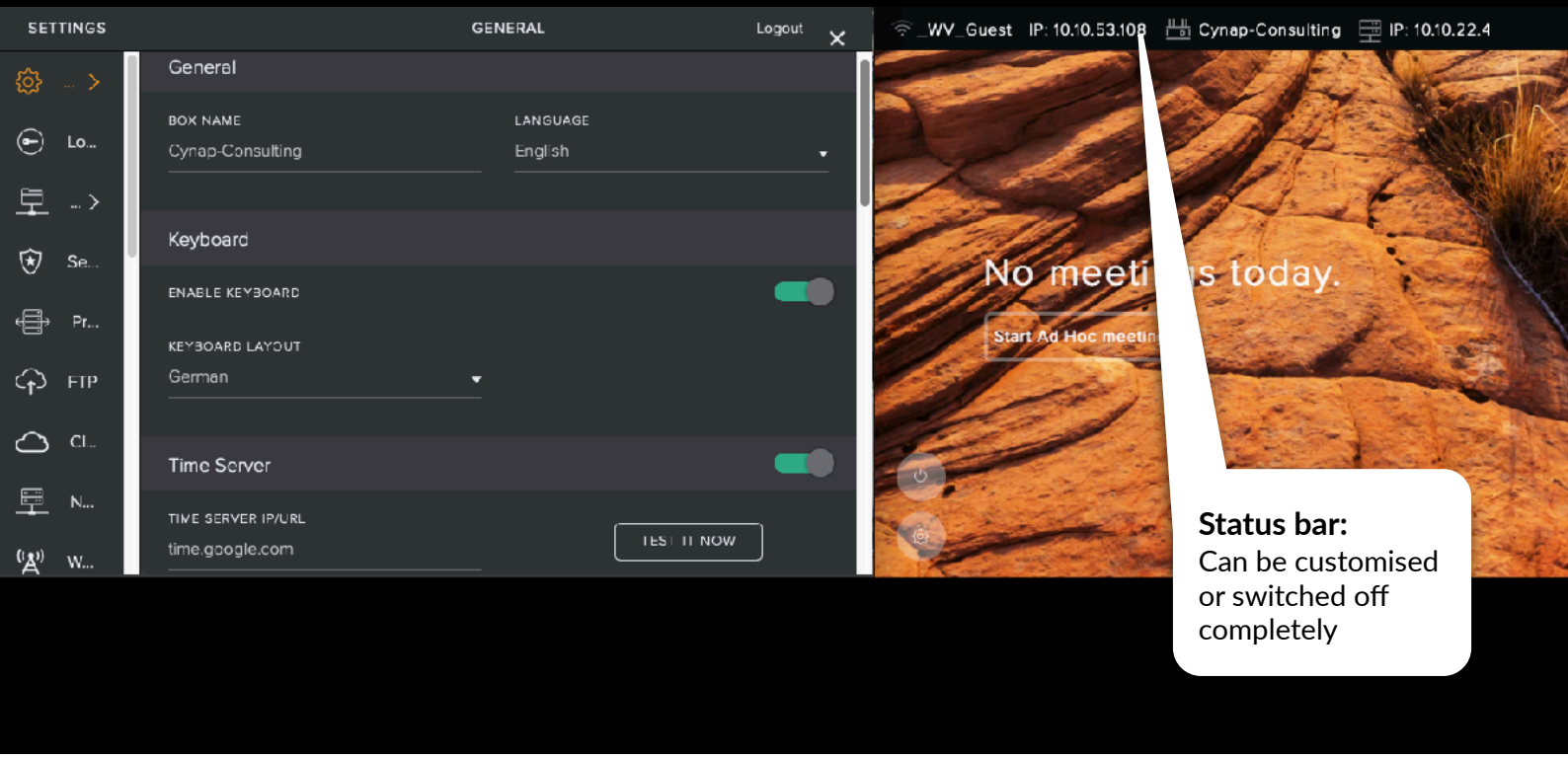
Again, press Down-Arrow-Key until you see the **IP address**

4

Once again, press **Down**-Arrow-Key until you can read the **MAC address**.

Note: The same information can also be fetched from the Browser when you're connected to Cynap's Settings (***Settings -> LAN1, LAN2 and WLAN***)





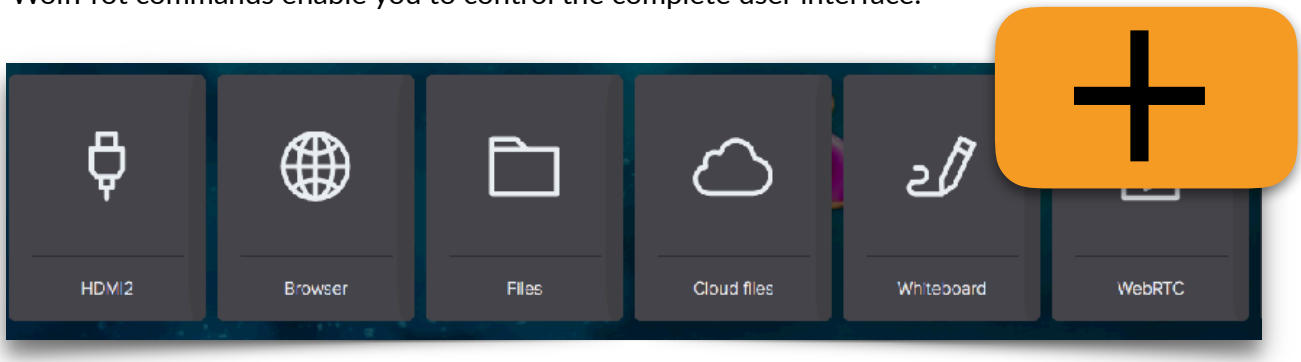
7 User interface

7.1 input sources

Cynap offers various applications, these applications are called sources. Each source, when pressed on the yellow circle (source button) opens up in a new window.

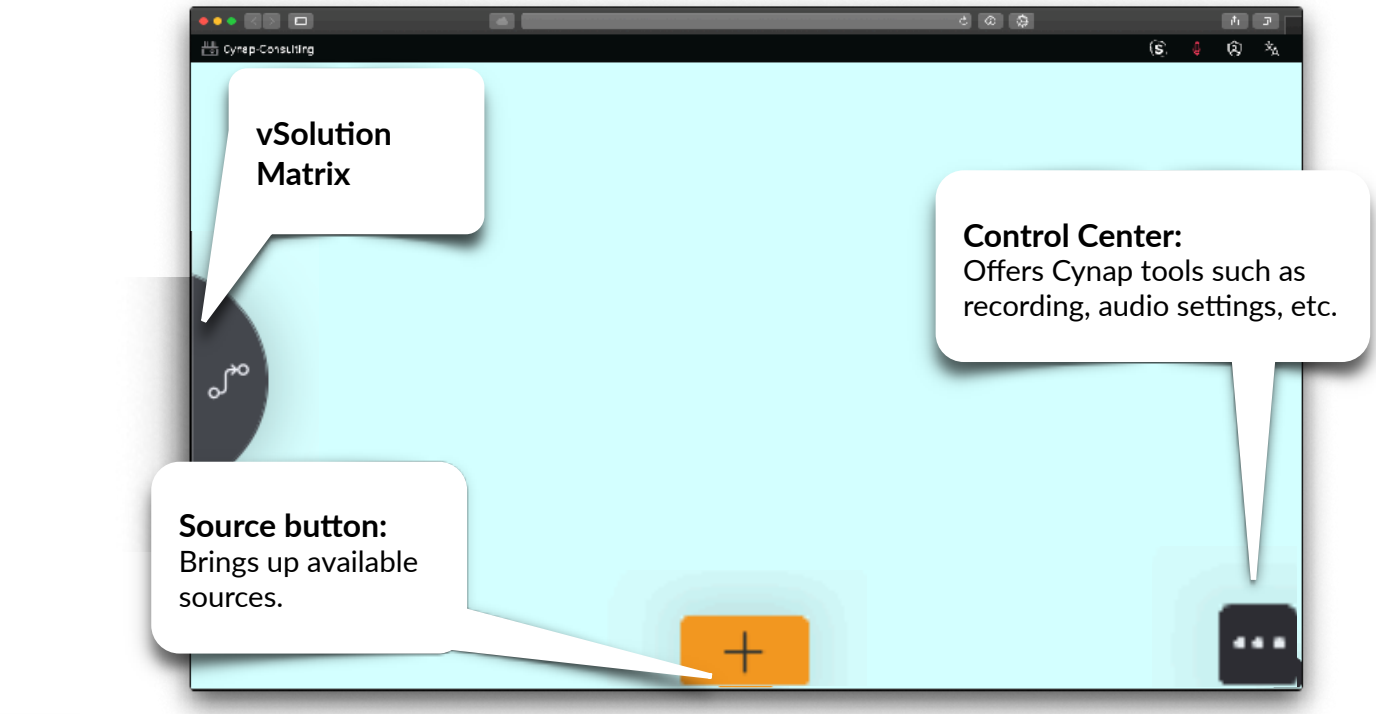
The windows are fixed on a total number of 4. Trying to opening up a fifth one will result in a pop-up message about 4 windows already in use.

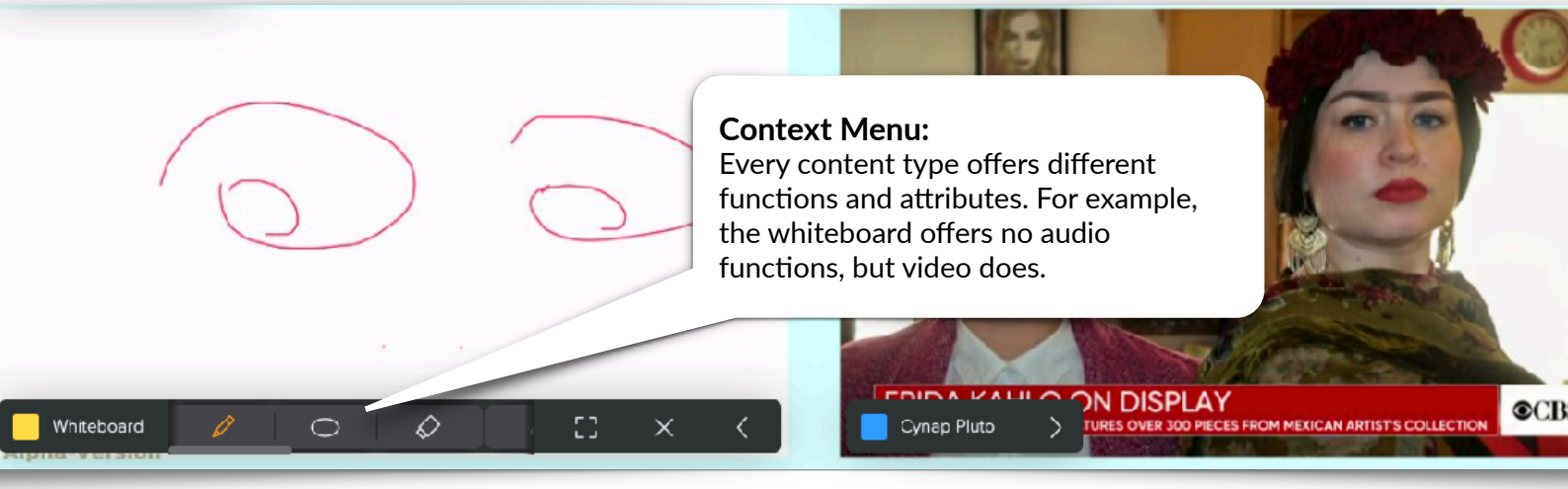
WolfProt commands enable you to control the complete user interface.



Icon/label	Description
Web browser	Opens a web browser
Files	Opens the file dialog menus
Cloud files	Opens the Cloud file list or the login screens if not logged in

Whiteboard	Opens an empty whiteboard
WebRTC	Opens a configured WebRTC session - Cynap works best in host mode.
WebCam	UVC attached USB Camera
Input Stream	Video input streams from various sources (IP cameras, Streaming servers, etc.)
Office Documents	Microsoft Office 365 components
HDMI1, HDMI2 input	Attached HDMI input devices
Allow mirroring	Initiate a timed window where a user will be allowed to initiate a screen mirroring connection (times out after 30 sec unless you repeat cycle using the appropriate WolfProt command).





Input Sources on Cynap's user interface do consist of a number of icons sending individual Window Start commands (0D CB 2C).

Window Start (0D CB 2C)

Window Start	0D CB2C ab cd wn wt lp0..lp1 p0..pn		
		wn: Window number (Control)	0x00..0x03 = Window number (0..3) 0xFF = Auto arrange
		wt: Window type (Window Start)	0x01 = Visualizer 0x02 = HDMI 0x03 = Browser 0x06 = Video 0x08 = Image 0x09 = PDF 0x0A = Office PPT/PPTX 0x0B = Office DOC/DOCX/TXT 0x0C = Office XLS/XLSX 0x0D = Whiteboard 0x0E = Audio 0x0F = Webconference 0x10 = Webcam 0x11 = Stream Input 0x13 = Office 365 Outlook 0x14 = Office 365 Word 0x15 = Office 365 Excel 0x16 = Office 365 PowerPoint 0x17 = Office 365 OneNote 0x18 = vMatrix Pull Stream (from station) 0x19 = vMatrix Push Stream (to station) 0x1A = vMatrix Station Browser
		lp0..lp1: Parameter length	Max. 65531 bytes
		p0..pn: Parameter	

From the official WolfProt Command List available on wolfvision.com

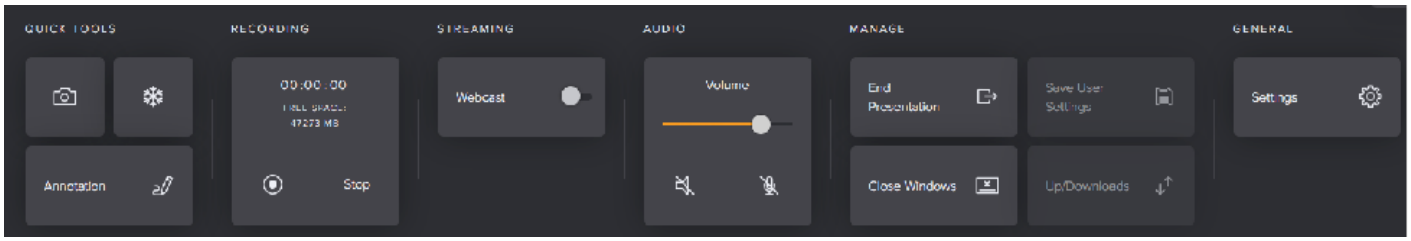
Sending a Window Start of type browser with parameter, Cynap will open up the browser on the specified location (web site). If no parameters have been passed, then a browser window containing the default or starting page (configured at *SETTINGS—>GENERAL—>BROWSER—>START PAGE)* will be opened.

7.2 Control Center

Controlling the Cynap and Cynap Core in general is hidden behind the menu Control Center, Indicated by three dots on the right hand side.

It contains action buttons which initiate a direct action such as “Mute”, Create Snapshot etc.

All toolbar functions can be executed using the WolfProt commands.



Label	Description
Annotation	Freezes the screen and displays drawing tools to annotate and save the annotation as a JPG file.
Recording	Starts recording the content on HDMI1 out - if moderator mode in *Settings->Output* is set on HDMI2, then HDMI2 out is being recorded
Snapshot	Creates a JPG image in 1920x1080 resolution (72dpi).
Start/Stop Streaming	Start or stop streaming function - optionally there’s a function to have recording on capturing device disabled
Apps	From Cynap local download of vSolutionCast in cases where guests are not allowed access to internet.
Mute Mic	Mutes the Mic
Volume	Volume up or down
Freeze	Freezes the screen.
Settings	Cynap Configuration settings - admin login required
Help	Onboard help file.
Close Windows	Closes all 4 windows.
End Presentation	End the running presentation - start a new one, enter standby or activate screensaver.

7.3 vSolutionMatrix

vSolution Matrix allows manipulation of video signal and document traffic between master and clients.

The video signal is being pushed from the master or pulled from the master, the attached client devices do not offer any Matrix functions, all is done on the Matrix master unit (Cynap Core is limited to the client role, and a Cynap can act as master or client).

Therefore integrating the vSolution Matrix by using WolfProt commands is possible on the Matrix master Cynap. All video push and pulls are going through the master, there is no sending signal from client A to client B without going through the master first (pull signal from client A and push signal to client B).

Sharing files from the master unit to the client units is supported on WolfProt. On the vSolution client device you simply mount the Matrix mount to get access to the shared files - it*s as simple as accessing a file on any mounted disk.

Addressing devices is done using the clients serial numbers instead of IP or MAC addresses.

WolfProt commands for this feature is available as a separately sold Feature Pack - The WolfProt commands for this and all other additional Feature Packs (Capture Agent, Office 365 etc.) are always included.

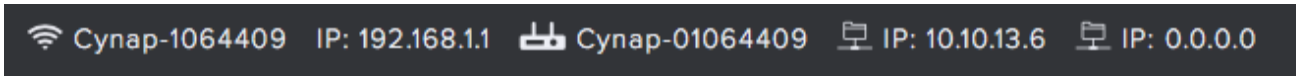
Commands without installed Feature Packs will be ignored by the system.

Using WolfProt commands in your implementation allows for extended functions not available for normal use (e.g. Matrix client pushing to master by pressing a 3rd party controller button).

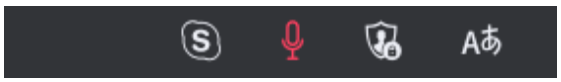
7.4 Status bar

Cynap's top status bar is divided into 2 sections. Section 1 shows the networking configuration settings for user to connect and the right hand side displays indicators on everything else.

Left hand side
Wi-Fi SSID, Wi-Fi IP address, hostname, IP LAN 1, IP LAN 2,



Right hand side
Skype On/Off, Mic On/Off, admin indicator, Language settings



The status bar displays the status of various vital functions such as the actual network state and, if allowed, its IP address or if *audio out-mute* has been activated.

The status bar can also be completely switched off if needed. If switched off (for reason of security, etc) you will also gain 20 pixels more screen estate for your presentation.

Cynap, Cynap Core,, and Cynap Pure are using the same commands to poll for a change.

8 Dual Screen management

Cynap offers 2 separate HDMI outs which can be controlled to display different single window content on each of the screen or HDMI1 using an overview to display a specific windows on HDMI2 out.

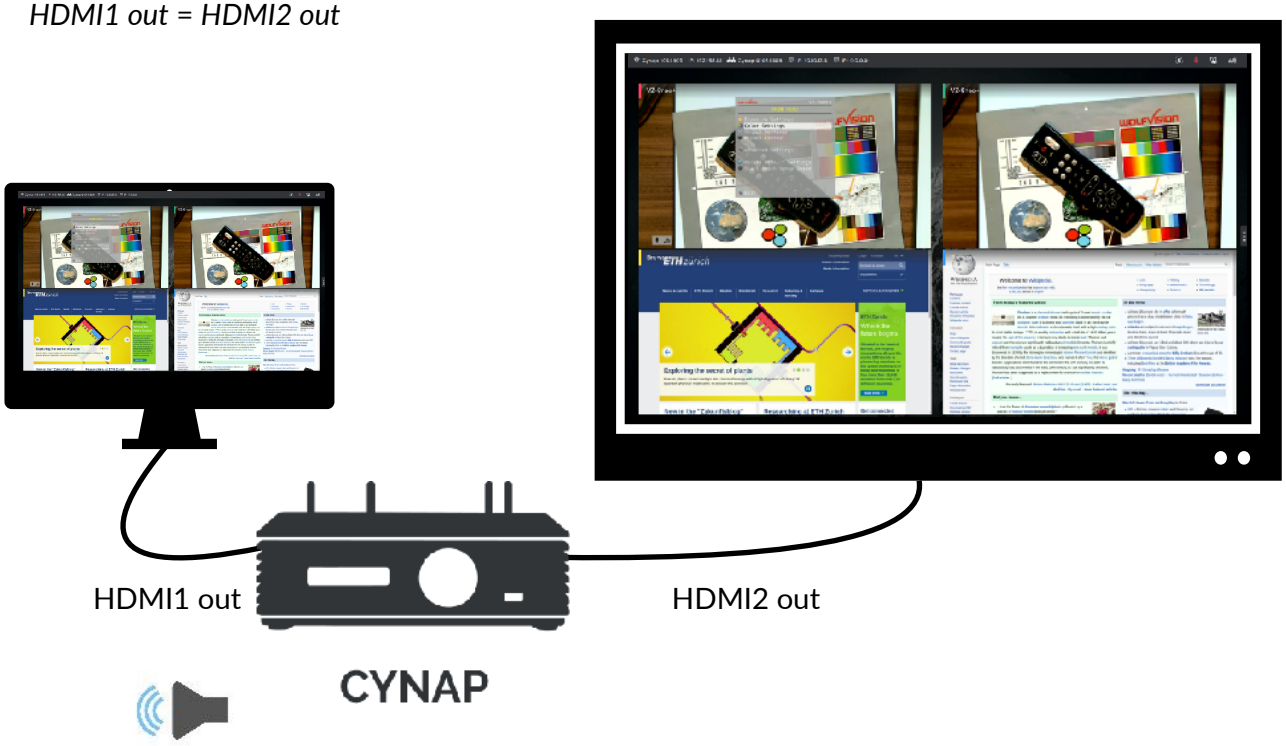
In Content or Moderator Mode, HDMI2 out's output resolution shifts to *1080p60* or *720p60* based on your configured setting.

To manipulate windows settings, shifting contents or restoring previous changed priorities there are a number of commands.

	Video signal	Audio Signal	Override to Mirroring
MIrroring	1:1	1:1	n/a
Content	1 dedicated window	Content from HDMI1 out	Yes
Content WebConference	1 dedicated window	Content from HDMI1 out	Yes
Moderator	1 dedicated window, visible highlight on active window	Content from HDMI2 out	Yes

Mirroring Mode

HDMI1 out = HDMI2 out



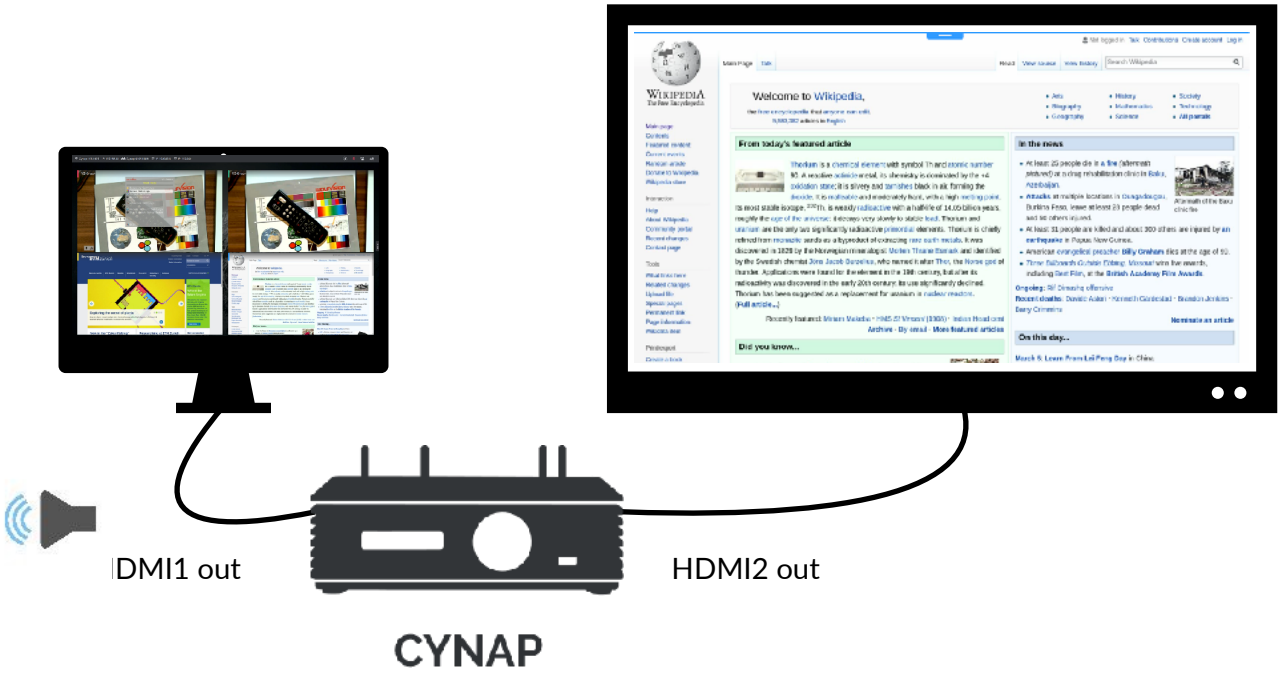
Video:
Same signal of HDMI1 out will be sent to HDMI2 out.

Audio:
Audio of HDMI1 is also sent to HDMI2 out

Content Mode standard

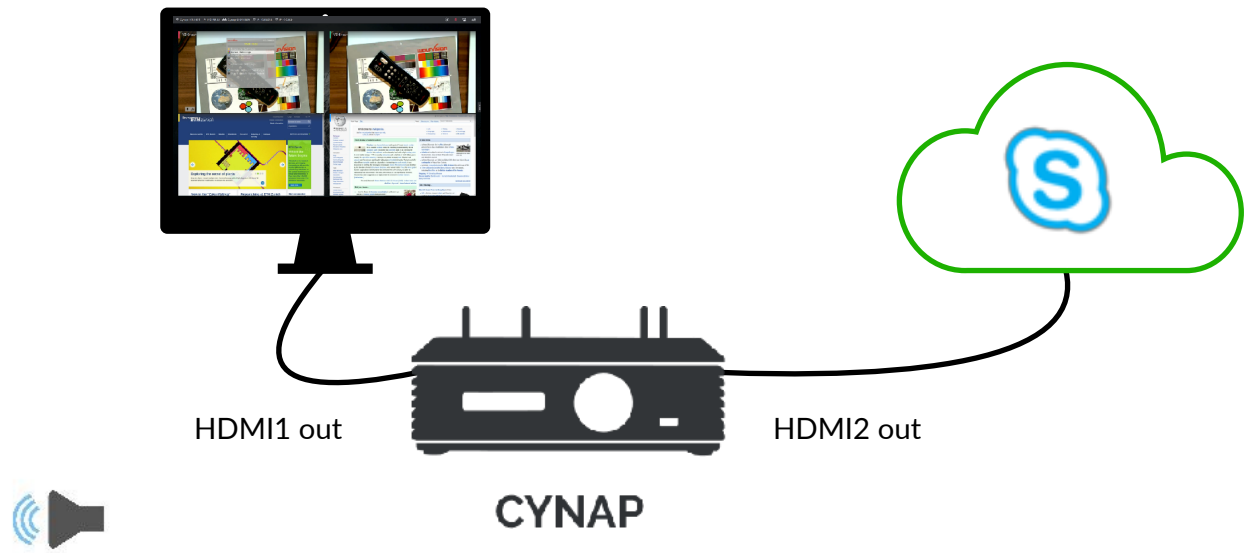
In content mode, *HDMI1 out* will be recorded/streamed. No status bar or user interface on *HDMI2 out*.

Mainly used to highlight one of the 4 available windows.



Content Mode using Skype for business

Streaming, Recording and Skype/WebRTC per default are using the content of HDMI1 out as output. If the optional parameter has been set, the content of HDMI2 out will be recorded, streamed and used in Skype/WebRTC. Audio being sent to HDMI2-out/WebRTC/Skype still is the same as the one on HDMI1 out.



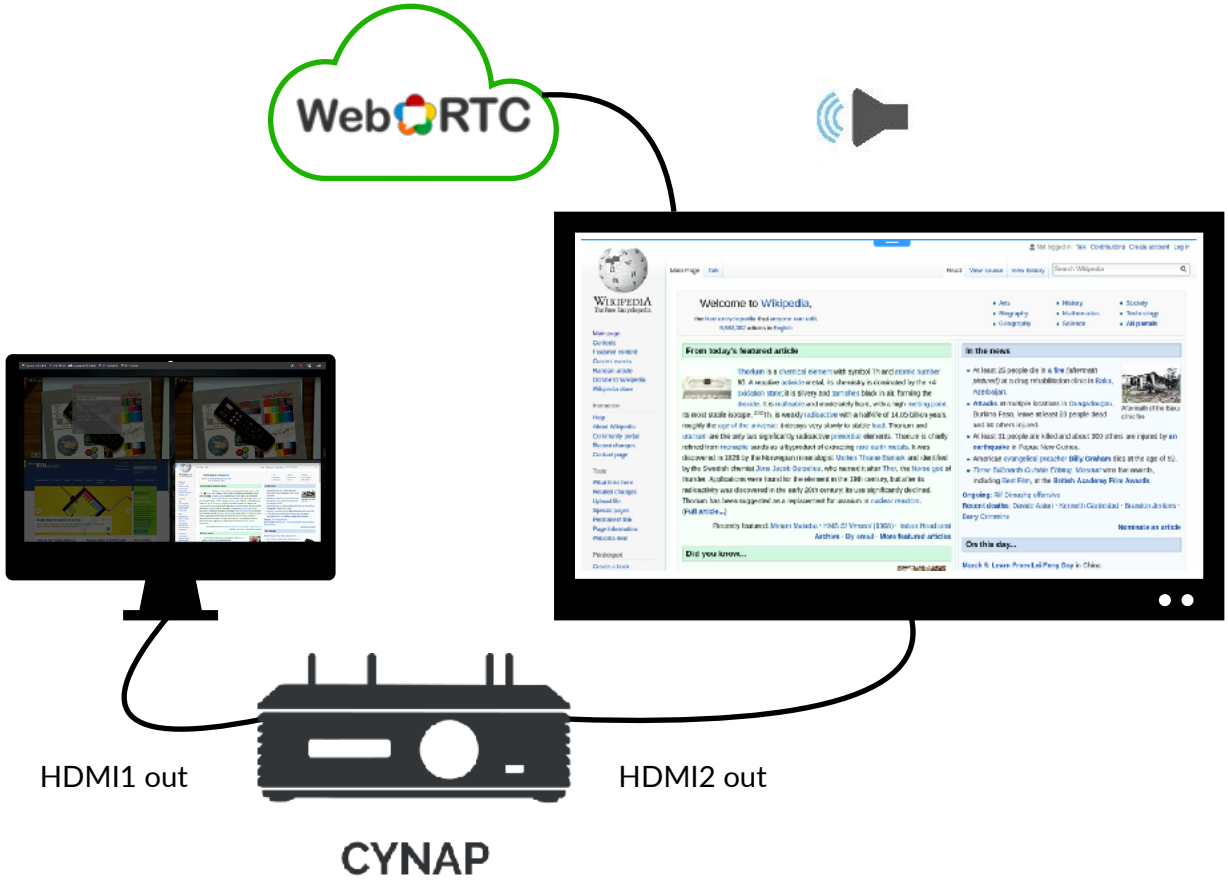
René Grämer

Moderator Mode

In Moderator mode, *HDM1 out* becomes an orchestrating window interface - recording and streaming will be done over *HDMI2 out*.

WebRTC works best in this mode, as the audio being shared is just the one of the dedicated window on HDMI2 out.

The inactive windows are darkened down to highlight the active displayed window on *HDMI2 out*.



There are specific Window Control commands on WolfProt to manipulate single windows to output specific content on HDMI2 only.

Check command Window Control CB28
09 CB 28 02 00 06 to send the first window to ***HDMI2 out***.

HDMI1 and HDMI2 are independent HDMI output ports, means, combining 2 HDMI outs to create a **single stretched 8K** content **window** or getting **8 independent content windows is not possible**.

9 Use of Cynap APIs

The Cynap API extends Cynap functions. as Cynap and Cynap Core in general provide a larger number of functions with higher levels of sophistication.

9.1 Command categories

Cynap APIs are structured into 8 different categories:

Category	Description	Example
Hardware	System commands	Send Standby command
Administration	Basically all the configurable settings (SET commands)	Enable and set GoogleDrive Session
Communications	LAN/WI-FI commands	Stop LAN connection
Services	Cynap services	Start/Stop Recording
Windows	Windows commands	Open new window with content type HDMI 1 in
Storage	File commands	Write to USB
Security	Security related commands	Show Login PIN on HDMI1 out
Matrix	vSolution Matrix commands	Send File to all Matrix clients

Table 6: Command structure

9.2 Cynap specifics

Cynap is slightly different than your usual document cameras - the command syntax not only persists of mainly single commands such as turn on or turn off auto focus.

Most commands also offer an extend data exchange over various kinds of data structures such as JSON strings (**J**ava**S**cript **O**bject **N**otation) - https://en.wikipedia.org/wiki/JSON or self-structured strings based on the command - please check each commands for its respective out

There are different user levels and additional ways to reach Cynap. And the four content windows need to be addressed to change their outputs.

9.3 Cynap User Authentication

There are 5 Users (or 4 User Types) to control Cynap via WolfProt Commands – if you want to just control Cynap (no changing of configuration settings) then we recommend using the Room Management System user which offers a dedicated login for your 3rd party controller on your AV network (switch LAN2 setting from Visualizer to Ethernet to switch off DHCP on LAN2).

The same WolfProt commands are also being used for our range of software (e.g. vSolution Link etc.).

If you need to change certain settings then the user with access level 2, administrator, is the one you need to use to modify Cynap settings.

Passwords have no minimum length; maximum length is 63 bytes (<=63).

API´s which don't require a login will be processed without a required prior login, such a user session will get a user access level of 0 (none).

The difference between Moderator_User and Room Management System_User is, that the Moderator uses a protective layer, forcing web browser visitors/users to log in before they can operate or see content on Cynap.

Note:
you always need to log in (at least on *Access Level 1* – User) to be able to operate with the same commands as a Cynap moderator/user.

Additionally, the password for the Moderator User can be set to a randomised PIN, making it almost impossible to catch up with a proper login to process your own commands and implementation.

If you want to just control Cynap (no changing of configuration settings) then we advise to use the Room Management System User.

The **Room Management System User**, having the same rights as the Moderator, on the other hand, is having its own password and offers no obstructing Cynap created PIN and therefore a simpler access integration for your implementation.

The **Annotation** is the level used for Cynap's annotation functions.

The **Admin user** requires the Password set on Cynap.

The **User None** in general is useful for a quick testing, when you lack the password, and only need to see if you can get a response from Cynap.

Note: It is possible to develop a Cynap controller without a login function. But it requires switching off the login features (user/password combination) and enables everybody with a browser connection to Cynap to possibly interfering with a Cynap presentation.

9.4 Setup Cynap's Room Management System User

There are 5 Users (or 4 User Types) to control Cynap via WolfProt Commands –
If your functions involve dynamic change of settings then you need to log in as Admin user.

Passwords have no minimum length; maximum length is 63 bytes (<=63).

To avoid confusion between the Cynap moderator and your Room Management System solution and offer the same level of access, we provide an extra user for your 3rd party controller implementation.

The user Room Management System offers the same moderator-user rights; but without a randomised PIN.

However, if you don't configure the Room Management System user to protect your access to Cynap, your opened web socket connection will automatically be granted the level USER instead of just UserLevel NONE.

This convenient login feature only works as long as the Moderator USER has no password set.

As soon as the Moderator password has been activated, your setup won't work anymore and a login procedure or the setup of the Room Management System user will be required.

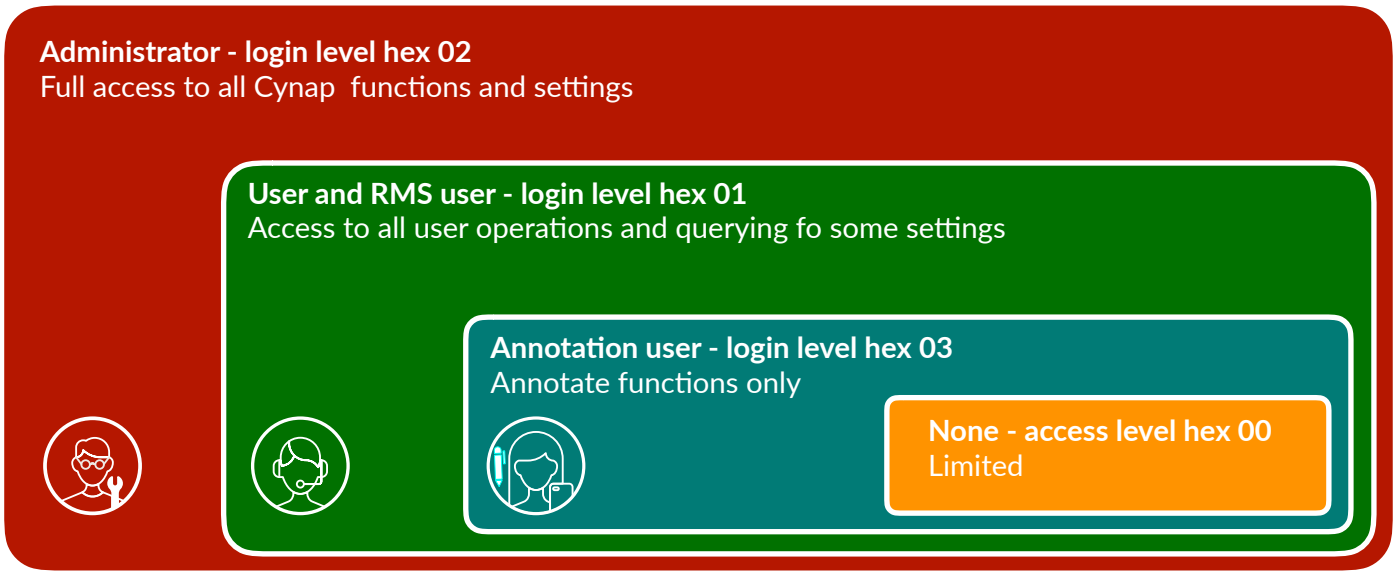
Your anonymous access will be automatically downgraded to user None and most functions will cease to work.

To see which login level for a certain function is needed please **check the WolfProt command list** PDF on our website

Passwords: we strongly advise to change the initial default user password, also make sure that the user password differs from the RMS user password.

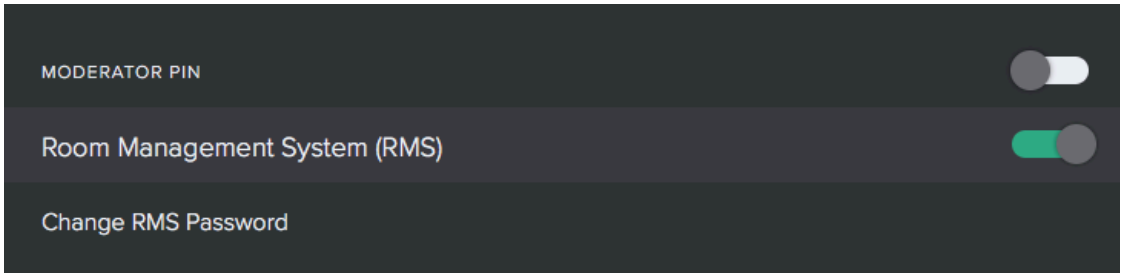
The API´s which require User Level None will be processed without a required prior login.

Example of Login to execute User-Level or Admin -Level commands
Example Login command using 12345678 as password and level user
hex: 09 CB 42 0A 01 08 01 02 03 04 05 06 07 08
Please check the official command list for a description of each byte.



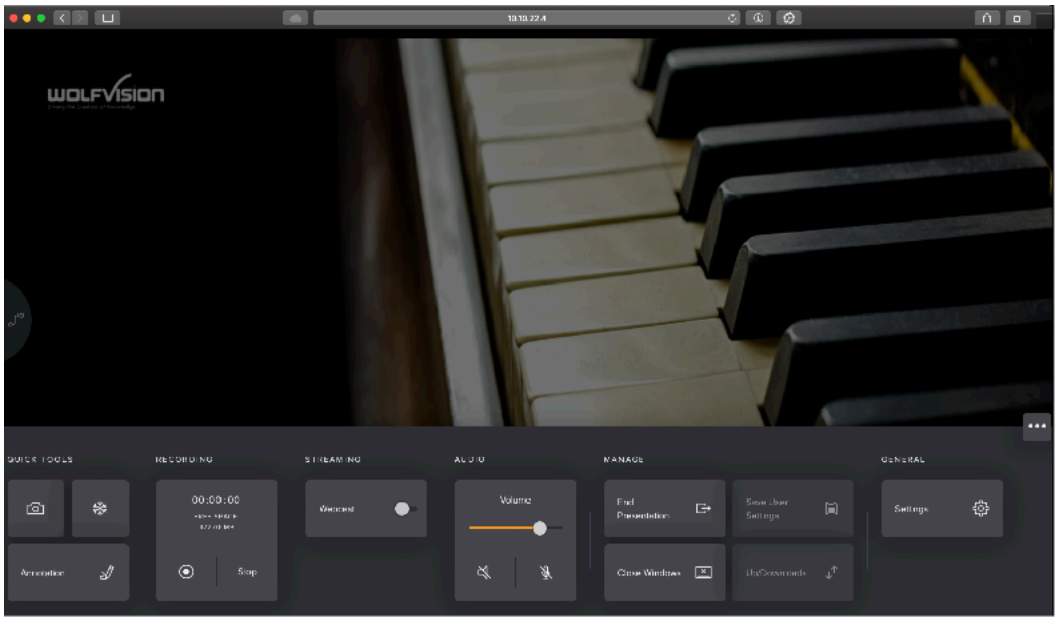
9.5 Three steps to activate the RMS user for your 3rd party controller

1. Enter the LOGIN settings on Cynaps Settings page.
2. Scroll to the bottom.
3. Activate the RMS user (switch enable button) and then add a password for your RMS user.



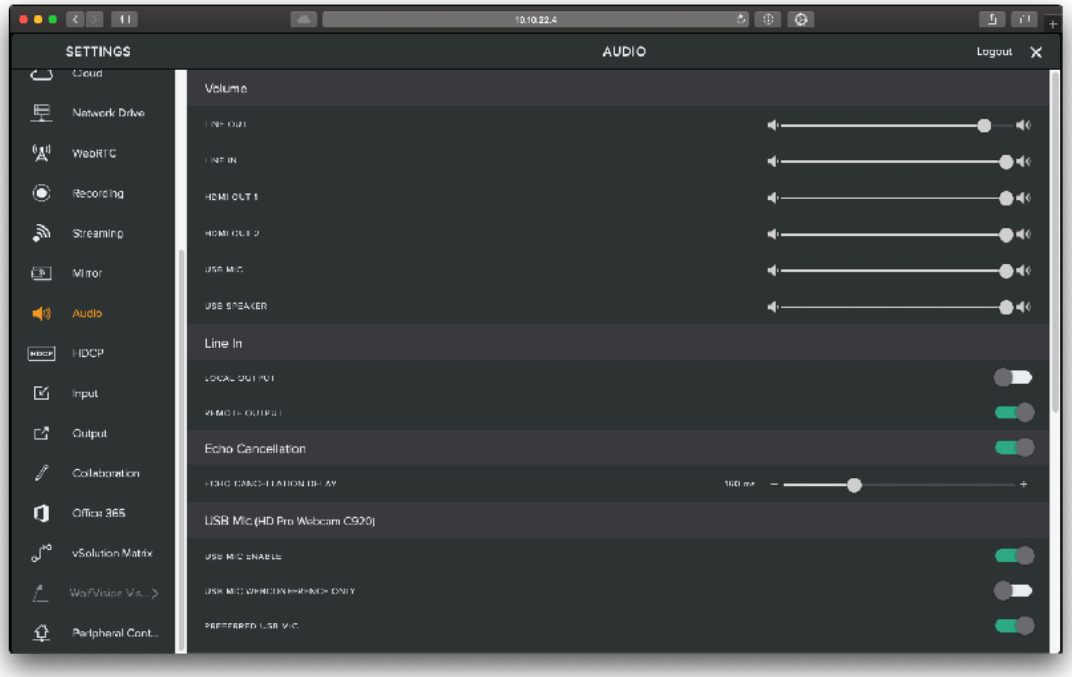
In a nutshell: which API requires which access level

User Access Level
Everything that can be clicked on the user interface has a WolfProt API and required a login on user access level.

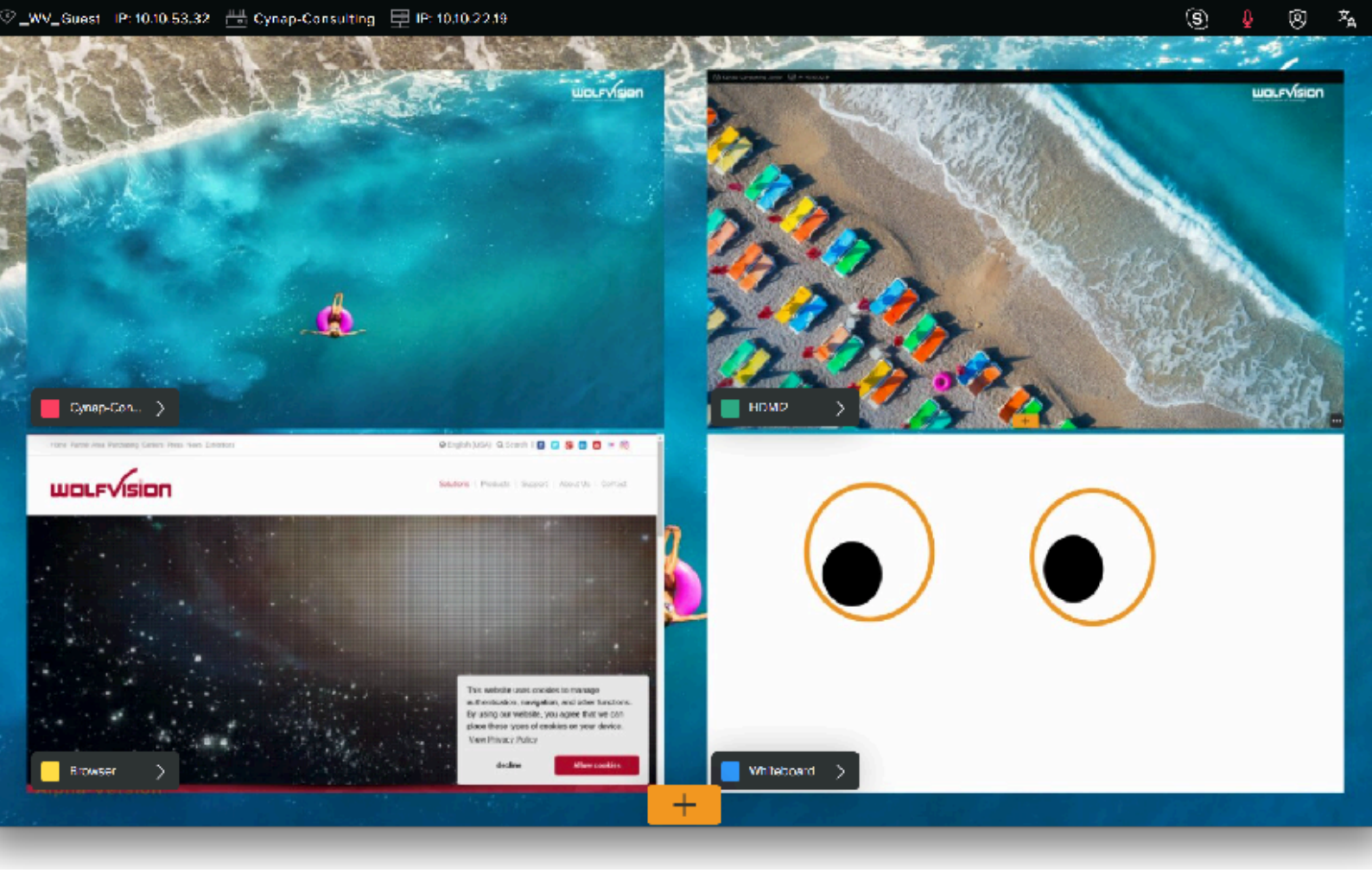


(for example: taking a snapshot picture)

Administrator Access Level
Every setting option that can be changed requires an Administrator access level.



(example: dynamically change audio settings)



10 Cynap Windows

There are four independent windows on Cynap. They are differentiated by IDs which represents always the same color. Opening, closing and manipulating windows can be enriched with parameters to achieve a different outcome (*open browser vs open browser using URL xyz*).

After a total of 4 windows got opened the user won't be able to use a fifth one without closing one of the existing 4. File operations and their windows are not affected. .

10.1 Windows Control

In general windows can be opened/closed, muted, put in full screen or set, if configured, on a second screen (HDMI2 out) called **Dual screen** feature.

WindowControl gives you control to manipulate the 4 Cynap windows. In the API, the set command to open a window uses following structure:

Color and corresponding WindowID:

Priority (same on remote)	Color	WindowID (d0)
1st	red	0
2nd	green	1
3rd	yellow	2
4th	blue	3
SourceButton	autoarrange	-1 (hex ff)

Table 9: Remote Window Color ID

remote

10.2 Window Control (CB 28)

Common control Commands (Window Control) when selecting a specific window.

Set	Command	Window ID (d0)	Action	Function
09	CB 28 02	D0	0	Close window
09	CB 28 02	D0	1	Size: Full screen
09	CB 28 02	D0	2	Size: Window
09	CB 28 02	D0	5	Toggle Full screen/Window
09	CB 28 02	D0	6	HDMI2 Copy: On
09	CB 28 02	D0	7	HDMI2 Copy: Off
09	CB 28 02	D0	8	HDMI2 Copy: Toggle

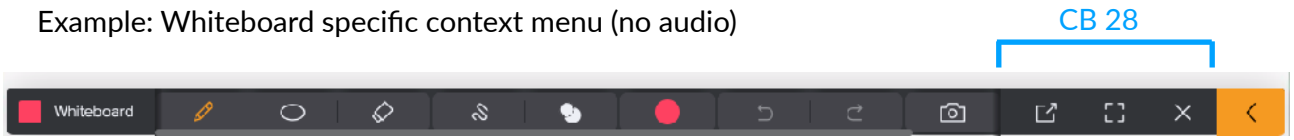
Table 10: Window Commands

Command for specific audio control commands.

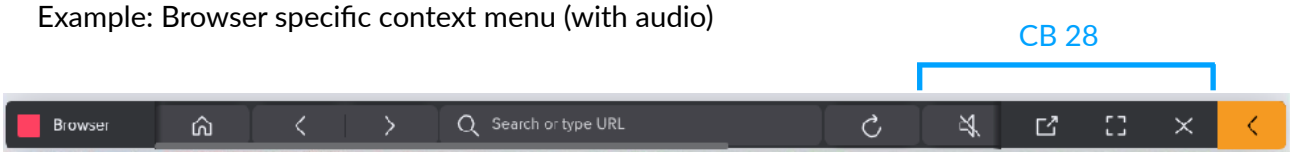
Set	Command	Window ID (d0)	Action	Function
09	CB 28 02	D0	3	0x00 mute off 0x01 mute on
09	CB 28 03	D0	0x04	0x00 to 0x64 (volume in %)

Content-Aware commands such as to pause a video or adding a different URL on a browser content are being executed by processing WindowTypes (see the following chapter) and its specific commands.

Example: Whiteboard specific context menu (no audio)



Example: Browser specific context menu (with audio)



10.3 Window Start (Window Types) CB 2C

Based on a window content the window type changes and offers a different context menu. For example, a video content behaves differently than a PDF in that manner that the video player can be paused and a PDF page can be flipped to the next one.

Some window types offer a parameter when starting to allow opening the window with the corresponding document. The parameter of a web browser consists of the URL and the parameter of an image of the file source location.

Window Types are used for the Window Start (0D CB2C) command. Based on the WindowType its parameters also change.

WindowTypes are:

hex	Name	Functionality	Parameter
0	None	Number of available windows Note: all 4 windows are always active but hidden. If you run out of Window type 0x00 then this means that all 4 windows are being in use.	none
1	Visualizer	Wolfvision Visualizer support	None
2	HDMI Input	Select HDMI1 or HDMI2 input	**0x00** for HDMI1 or **0x01** for HDMI2
3	Web Browser	Start web browser If no URL is specified it will take the default page (either 4 icons or the start page from (Settings -> General).	URL
4	Miracast	Microsoft´s Wi-Fi direct connection	none
5	AirPlay/ GoogleCast	AirPlay and GoogleCast	none
6	Video	.mp4, .mkv, .avi	File location and name
7	vSolutionCast	BYOD for Windows 7	none
8	Image	gif, jpg, png, bmp	File location and name
9	PDF	PDF files	File location and name
0a	Office presentation	PowerPoint files	File location and name
0b	Office text	Word files	File location and name
0c	Office calculation	Excel files	File location and name
0d	Whiteboard	Drawing board	None
0e	Audio	.mp3, .oga	Fil

0f	Webconference	WebRTC client	None
10	Webcam	USB Camera support	None
11	Stream Input	RTSP Input stream	0x00 to 0x03 Index # of predefined URL
12	Skype for Business	Skype for Business window	None
13	Office 365: Outlook	Outlook window	None
14	Office 365: Word	Word window	None
15	Office 365: Excel	Excel window	None
16	Office 365: PowerPoint	PowerPoint window	None
17	Office 365: OneNote	OneNote window	None

Table 11: Cynap Window Types

Example of Browser Opening
Example Window Start command of type browser with no URL attached (starts default or configured Start Page)

hex: 0D CB 2D 00 04 FF 03 00 00

Please check the official command list for a description of each byte.

For further examples please Window Start diagram at end of this manual!

11 File Operations

Cynap supports various file types and file services. If a Cynap user did log into a cloud service will grant you access to upload a snapshot or a recording without the need of mounting the cloud service yourself (no cloud login procedure necessary - just fetch the list of mounted drives and check if a preferred cloud has already been mounted).

Supported are FAT16 and NTFS on a USB memory stick - when storing files on a FAT16 stick, make sure that you remind the user of the 4 GB file limit before copying fails.

API	Command	Description
Get Mounts List	08 CB 3D 00	Information on available mounted file system and their status (JSON array)
Get File List	0C CB 3E	Provide the root path and you will get a list of files (JSON array)
Get File Download List	08 CB 7B 01	If you send a length of 0 you will get a merged list of all downloads otherwise (length == 1) you´re able to filter 0: DropBox 1: Google Drive 2: Box
Get File Upload List	08 CB C1 01	JSON array of all file uploads in progress
Get Cloud Mode	08 CB 8F 00	Disabled/enabled returns per cloud service
Get Cloud Status	08 CB 4C 00	Status on all cloud services returned
Get FTP Mode	08 CB 62 01	FTP server configured – no status on availability

Table 12: File commands

The array of the mounted drive not only tells you the name but also if the drive is writeable or available in the cloud.

name | name of mount	Id | unique ID	type | local, net	status | mounted or not	perms | read/write
Internal	Internal	Local	mounted/notMounted	ro: read only
System	System	system	notMounted	
USB	USB	usb	mounted/notMounted	rw: read, write

Dropbox	dropbox	cloud	mounted/notMounted	rw: read, write
Google Drive	gdrive	cloud	mounted/notMounted	rw: read, write
Box	box	cloud	mounted/notMounted	rw: read, write
Jianguoyun	jianguoyun	cloud	mounted/notMounted	rw: read, write
OneDrive	Onedrive	cloud	mounted/notMounted	rw: read, write
WebDAV	webdav	cloud	mounted/notMounted	rw: read, write
Network Drive 0	netdrive0	netdrive	mounted/disabled	ro/rw
Network Drive 1	Netdrive1	netdrive	mounted/disabled	ro/rw
Network Drive 2	Netdrive2	netdrive	mounted/disabled	ro/rw
Network Drive 3	Netdrive3	netdrive	mounted/disabled	ro/rw
Network Drive 4	Netdrive4	netdrive	mounted/disabled	ro/rw
Network Drive 5	Netdrive5	netdrive	mounted/disabled	ro/rw
Network Drive 6	Netdrive6	netdrive	mounted/disabled	ro/rw
Network Drive 7	Netdrive7	netdrive	mounted/disabled	ro/rw
Network Drive 8	Netdrive8	netdrive	mounted/disabled	ro/rw
Network Drive 9	Netdrive9	netdrive	mounted/disabled	ro/rw
FTP	FTP	ftp	mounted/disabled	wo
cdrive	*cdrive*	*cdrive*	*mounted/notMounted*	*For future use*
Matrix Master	matrixMaster	matrix_master	mounted/notMounted	ro
Matrix Station	matrixStation	matrix_station	mounted/notMounted	ro

The ftp session won't be checked every 10 secs unlike the network drives – the status mounted therefore doesn't tell you if the ftp-connection is working; the status mounted informs you that an ftp connection has been configured.

Cynap's operating system does not allow file manipulations - for security reasons: the file systems are being purged as soon as a new presentation starts or Cynap got rebooted. Temporarily sharing media files content from local and remote resources are allowed (e.g. download from cloud and present on Cynap in image viewer).

- Downloading video images office documents from the cloud services
- Displaying video images office documents from internal/external/remote locations
- Uploading recordings and snapshots only from internal location

The file list array consists of two fields. Field one requires the file name and field two contains the file type.

The file types supported by Cynap have a specific identifier and file types not supported by Cynap are specified as unknown.

To open a file, you have to prepare its fully qualified name. The fully qualified name is generated from the mounted storage device, 3 leading slashes, the path and the filename itself.

e.g. USB:///Folder1/video1.mp4

File Type	Description
Audio	Audiofile (e.g. .mp3, oga, ...)
calc	Spreadsheet files (.xls, xlsx)
dir	Directory
html	Locally saved webpage
image	Pictures in gif, png or other supported formats
pdf	PDF file
presentation	Powerpoint
text	Word or text files
unknown	Unknown file format - please hide or mark as unknown
video	Supported video format

11.1 File Transfer (FTP)

When uploading a file from Cynap to an FTP server please make sure, that your FTP server is already set up with a user and password combination and owns the proper rights to create/replace files – FTP file transfer offers a user/password combination but no further settings such as ACTIVE/PASSIVE or specific parameters such as Kerberos login or other sFTP options.

Cynap's FTP client connection is not polled and uploading a file to the FTP server requires your implementation to handle connection continuity.

11.2 Cloud support

The cloud as read-write device, once logged in by the user, behaves like a common network file share (CIFS).

Mount names of type Cloud

Mount	Id	URL
Box:///	Box	https://www.box.com
Dropbox:///	Dropbox	https://www.dropbox.com/

Google Drive:///	Gdrive	https://www.google.com/drive/
Jianguoyun:///	Jinanguoyun	https://www.jianguoyun.com
OneDrive:///	OneDrive	https://www.onedrive.com
WebDAV:///	WebDAV	Custom WebDAV link

Cloud status: WPC_Cloud_Status (0xCB4C)

0x00	Disconnected	Connect if required
0x01	Oauth Open Authorization 2.0	wait
0x02	Connected	file list access pending: wait before fetching the cloud file list
0x03	Connection failed	Network/authorization problem
0x04	Synced	Cloud directory read: Ready to
0x05	Disabled (not configured)	

Cloud API´s

	WPC_CLOUD_CONNECT	0xCB 0x45
	WPC_CLOUD_PRELOAD	0xCB 0x46
	WPC_CLOUD_STATUS	0xCB 0x4C
Enable/Disable cloud services	WPC_CLOUD_MODE	0xCB 0x8F
	WPC_CLOUD_UPLOAD	0xCB 0xA1
	WPC_BOX_CLOUD_DATA	0xCB 0xCC

11.3 Network file share (CIFS)

Cynap´s network file share is based on CIFS (Common Internet File Share). Once configured (up to 10 drives) it allows you to up/download files from Microsoft servers. A CIFS share can also be configured as a default destination for snapshots and recordings.

Please bear in mind that a CIFS name (e.g. MYSERVER1) needs to be configured on your local DNS server otherwise you have to use the IP address to access the CIFS share otherwise, your CIFS server simply won't be found.

11.4 USB external HDD or memory stick

A single FAT32 or NTFS formatted drive can be attached and accessed via Cynap. Feature Pack **Capture Agent** allows for an ***ext4*** attached drive connection in combination with an Opencast LMS.

11.5 Internal storage

There are two types of files:
1. Cynap created content such as *snapshots* and *recordings* and
2. Temporary files such as downloaded content from attached remote locations

Only Cynap created files can be deleted, uploaded or copied to a USB storage device.


```
[
{"id":"Internal","name":"Internal","type":"local","status":"mounted","perms":"ro"},
{"id":"System","name":"System","type":"system","status":"notMounted"},
{"id":"USB","name":"USB","type":"usb","status":"notMounted"},
{"id":"dropbox","name":"Dropbox","type":"cloud","status":"disabled"},
{"id":"gdrive","name":"Google Drive","type":"cloud","status":"disabled"},
{"id":"box","name":"Box","type":"cloud","status":"disabled"},
{"id":"jianguoyun","name":"Jianguoyun","type":"cloud","status":"disabled"},
{"id":"onedrive","name":"OneDrive","type":"cloud","status":"disabled"},
{"id":"webdav","name":"WebDAV","type":"cloud","status":"disabled"},
{"id":"netdrive0","name":"Network Drive 1","type":"netdrive","status":"disabled"},
{"id":"netdrive1","name":"Network Drive 2","type":"netdrive","status":"disabled"},
{"id":"netdrive2","name":"Network Drive 3","type":"netdrive","status":"disabled"},
{"id":"netdrive3","name":"Network Drive 4","type":"netdrive","status":"disabled"},
{"id":"netdrive4","name":"Network Drive 5","type":"netdrive","status":"disabled"},
{"id":"netdrive5","name":"Network Drive 6","type":"netdrive","status":"disabled"},
{"id":"netdrive6","name":"Network Drive 7","type":"netdrive","status":"disabled"},
{"id":"netdrive7","name":"Network Drive 8","type":"netdrive","status":"disabled"},
{"id":"netdrive8","name":"Network Drive 9","type":"netdrive","status":"disabled"},
{"id":"netdrive9","name":"Network Drive 10","type":"netdrive","status":"disabled"},
{"id":"cdrive","name":"cdrive","type":"cdrive","status":"disabled"},
{"id":"FTP","name":"FTP","type":"ftp","status":"disabled"},
{"id":"matrixMaster","name":"Matrix
Master","type":"matrix_master","status":"mounted","perms":"ro"},
{"id":"matrixStation","name":"Matrix
Station","type":"matrix_station","status":"notMounted"}
]
```


Example: JSON Array of list of mounted storage

```
[
{ "name": "wolfvision", "type": "dir" },
{ "name": "bigbunny.avi", "type": "video" },
{ "name": "compressed.rar", "type": "unknown" },
{ "name": "cynap.log", "type": "unknown" },
{ "name": "music.mp3", "type": "audio" },
{ "name": "test.txt", "type": "text" },
{ "name": "user.data, "type": "unknown" },
{ "name": "video1.mp4", "type": "video" }
{ "name": "video2-h265.mkv", "type": "video" },
]
```

Remember:
Cynap will not support file-types listed as *unknown*.

Example: JSON Array of file listing (root USB:///)

12 Networking

Cynap and Cynap Core offer 4 independent networking interfaces - one Wi-Fi solely dedicated to Wireless-HDMI, Miracast.

Cynap Pure offers only 2; an Ethernet and Wi-Fi interface (no dedicated P2P-Miracast and Wi-Fi at the same time).

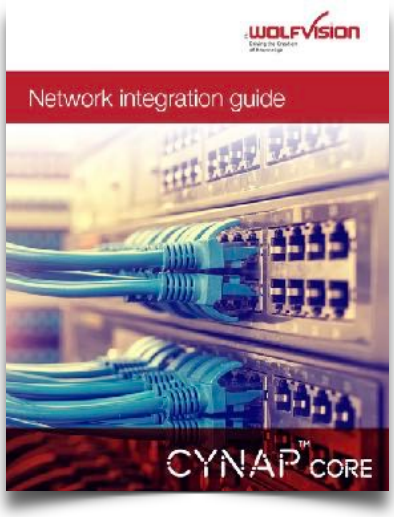
Cynap family

Please check out the **Networking Integration Guides** for the Cynap family to learn more about necessary open ports and further integration using the available networking interfaces.

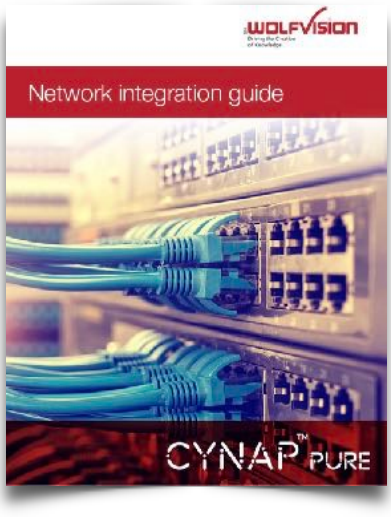
CynapAPI allow to dynamically change the networking settings. Please keep in mind that a wrong setting may render your setup unusable and might need to be fixed manually.

Changing networking settings require a prior login as an administrator (administrator login level hex 02) before a command will be accepted.

http://www.wolfvision.com/wolf/Cynap_Network_Integration_en.pdf



http://www.wolfvision.com/wolf/Cynap_Core_Network_Integration_en.pdf



http://www.wolfvision.com/wolf/Cynap_Pure_Network_Integration_en.pdf

Example Cynap to Cynap dialog using Cynap streaming input/output

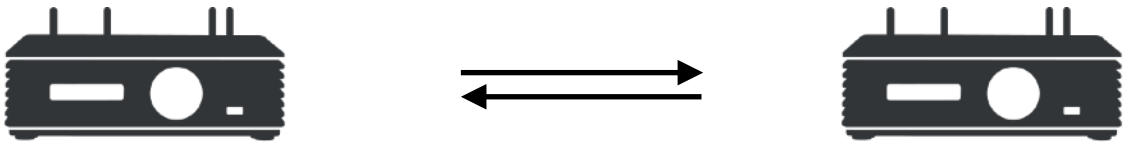
Sending out selective RTSP Unicast streams to different streamer receivers on demand.

Sending out stream from Cynap to Cynap in Output mode MIRRORING would result in a tunnel effect. Using CONTENT mode allows to stream a dedicated window content.

Additionally recording could be started on one or both Cynaps.

The same URL being used to receive the stream on Cynap could be used to receive the stream on a operating systems where VLC player is supported.

Commands		
On Cynap A	Start RTSP streaming	09 CB 93 01 01
On Cynap B	Start RTSP streaming	09 CB 93 01 01
On Cynap A and B	Start stream input (index of configured input stream)	
On Cynap A	Start recording	09 CB 25
O	Open a window of type camera	



Stream and receive single window content.

Cynap A

Cynap B

RTP H.264 unicast stream

13 Cynap in standby

Figure 5: Standby process

Once the user presses the standby button, Cynap will enter the standby mode by checking if vital background processes are needed to be completed (such as an initiated upload on a recording) and adds a grace period of 30 seconds before entering standby (in case a restart command got received).

The networking stack and all other monitoring activities are shut down. The only way to start a Cynap from standby is to use the remote, the power button on the front panel or cable based network* to send a Wake-On-LAN command.

Since your Room Management System is connected to Cynap via Ethernet, you will need to issue a Wake on LAN command.

Polling to keep a connection on Cynap via ping or echo command does not work - you will have to issue a GET command to get the proper status (esp. if Cynap is entering standby)

To wake Cynap from standby a user needs to press the power button on the remote or on Cynap.

Your Room Management System implementation needs to send a broadcast to the MAC address of Cynap issued in a magic packet to initiate the start-up process.

Figure 6: Wake on LAN (WoL) process

***Wake on WI-FI is not supported as antennas are not powered**

For an example please head to the WakeOnLAN source code section in Hands On part

Part 3: Hands On

Only Chuck Norris writes perfect code that optimises itself.

Getting some fast earned experiences by following these examples.

14 Tutorials

14.1 Hello World: Audio Toggle

As a basic fist and simple setup we won't start with a complicated setup; instead we are using the existing Cynap in front of you, which allows us to send a command that will be processed by the device itself.

A simple Audio-Toggle command allows us to see and hear a difference in Cynap behaviour.

To process the command we are using the Peripheral Command feature of Cynap.

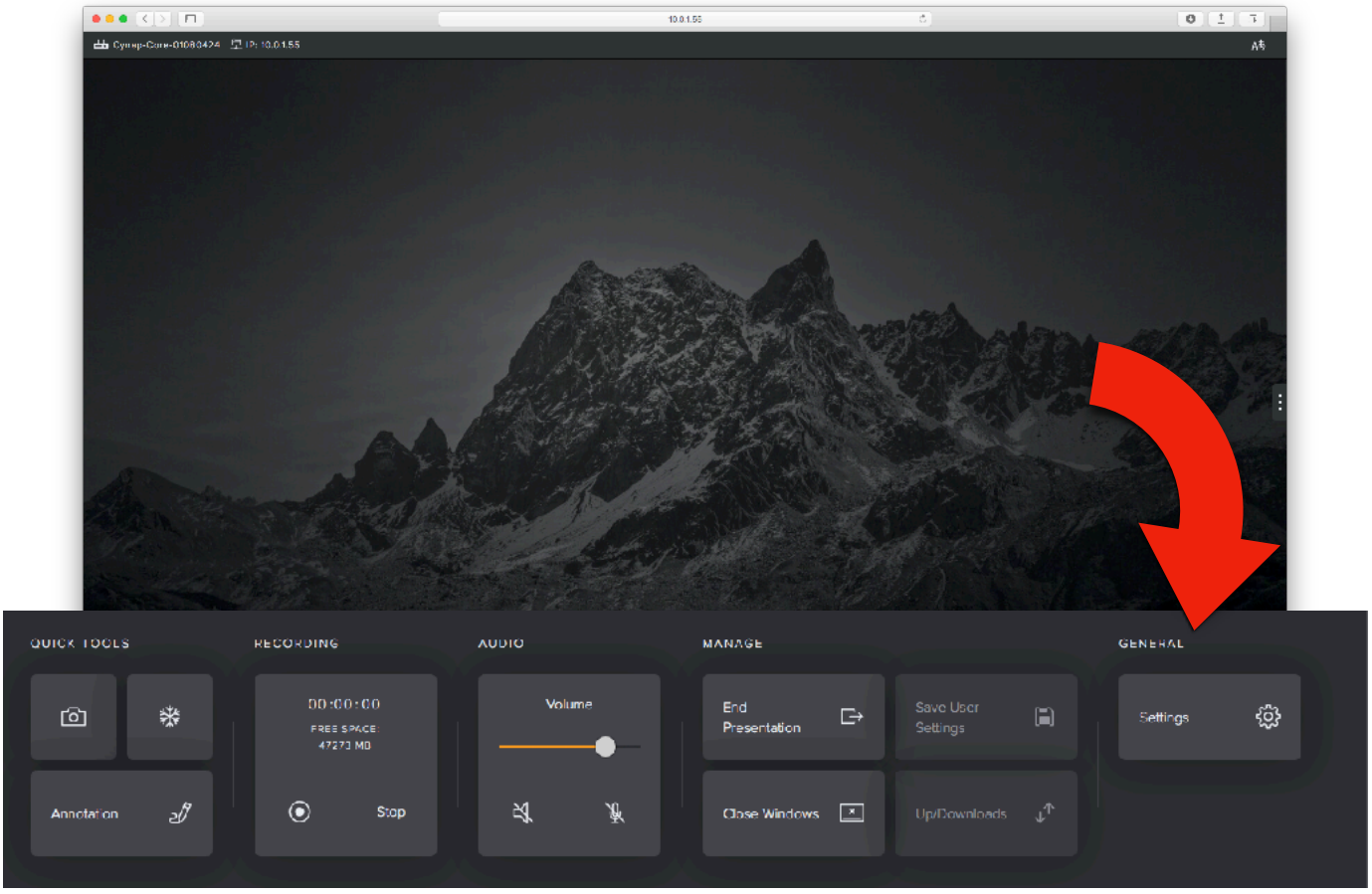
Things to consider:
IP of controlled Cynap (in that case, localhost), Command and the typical WolfProt command port.

IP	Port	Command
127.0.0.1	50915	09CB580102

CB58: Master mute - with parameter "Toggle"

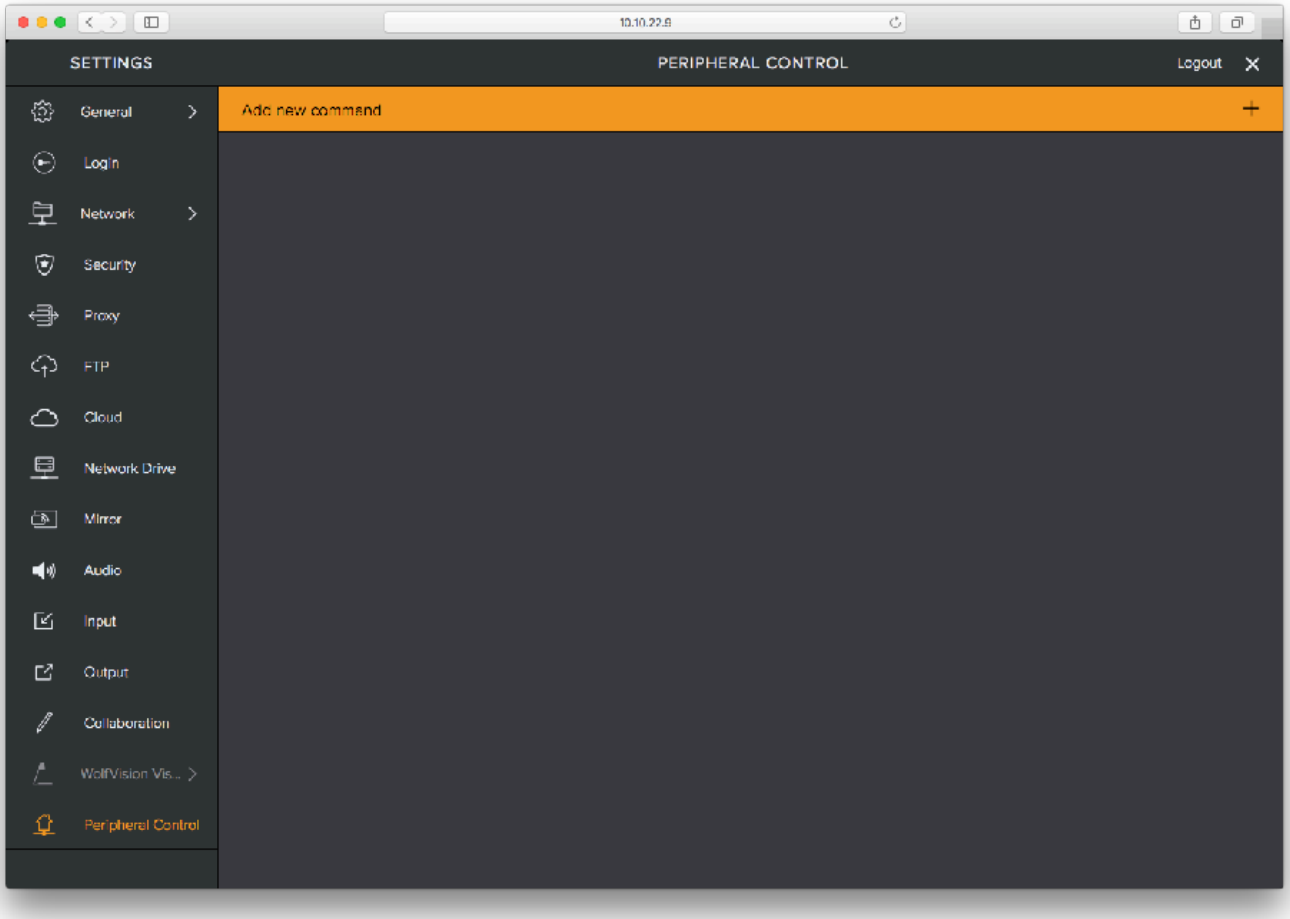
First step

Open Cynap's Toolbar menu and click on Settings to log into the settings menu.



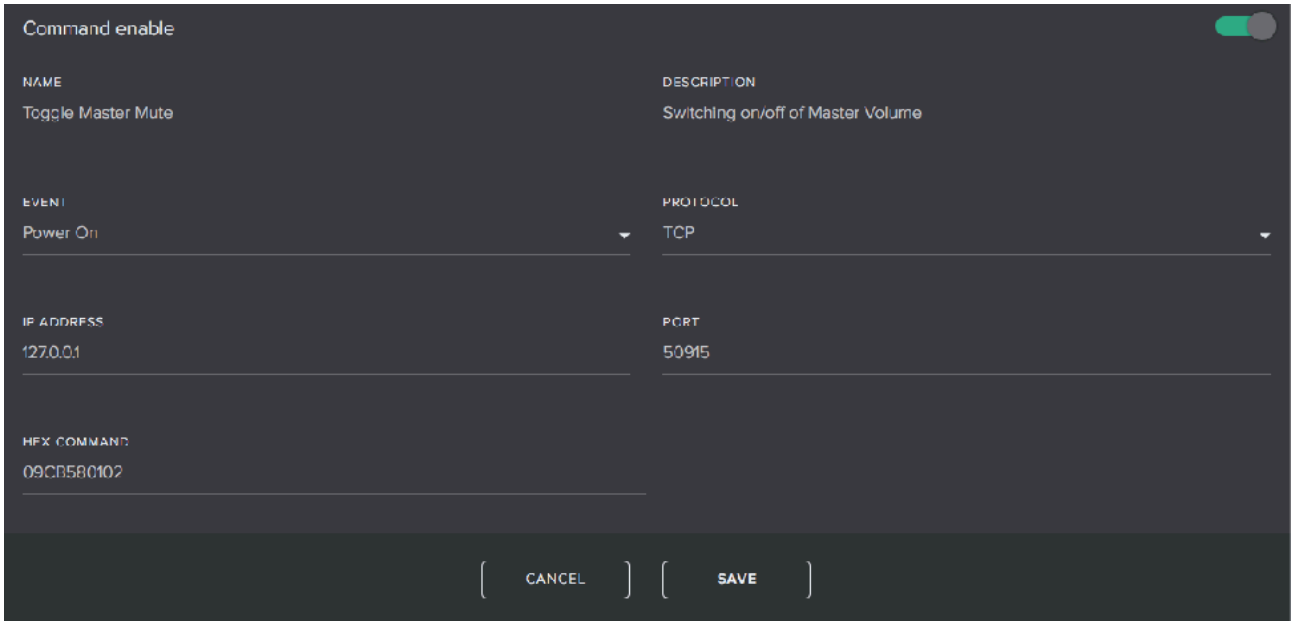
Step 2 and 3

Click on Peripheral Commands and add a new command by clicking the + sign



Step 4

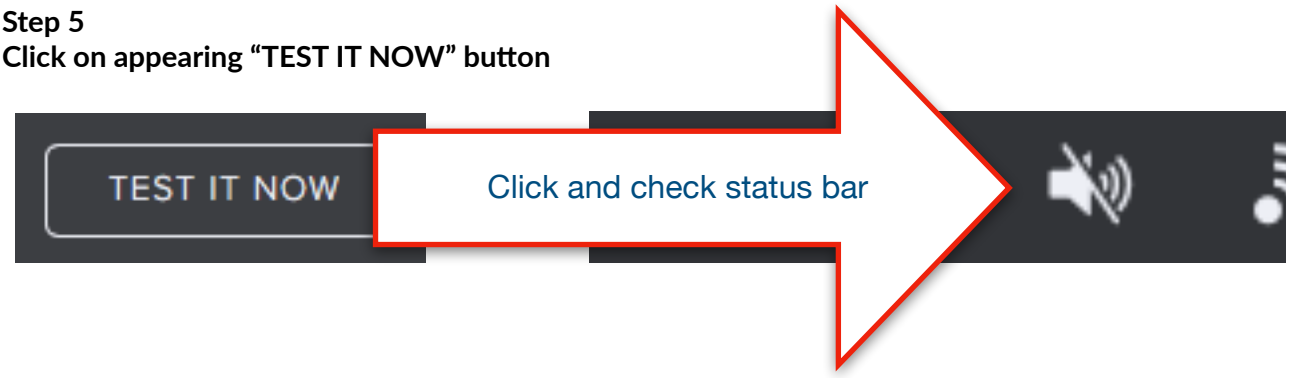
Enter necessary details from table below and press SAVE, right after save a new test button will show up.



Necessary details:

Name: customised Name, eg. **Toggle Mute**	Desc.: maybe a bit more, **esp. if you are executing more than one command at once**
Event: **Power On**	Protocol: **TCP**
IP Add: Localhost, **127.0.0.1**	Port: **50915**
Hex Command: **09CB580102**	

Step 5
Click on appearing "TEST IT NOW" button



More commands to quickly try out:

Start streaming: **09CB200101**	Open window using HDMI1 input: **0DCB2C0005FF02000100**
Log in as admin, using Password as password and switching Mirroring mode from *open mode* to *protected mode*: **09CB420A020850617373776f726409CBD30130**	Enable mirroring in protected mode: **09CB3B0101**

Please remove entries afterwards unless you want to keep them to be triggered on startup or standby.

Note:
If your command won't work it could be that a login password has been set and a prior login command is required.

14.2 Digital Signage

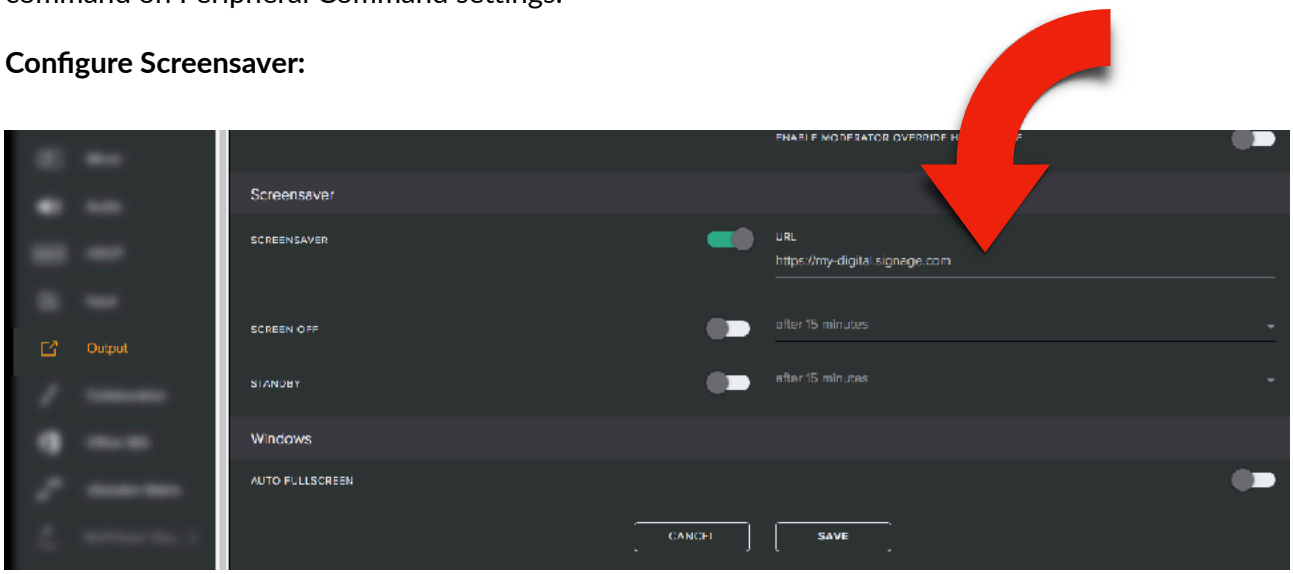
Scenario:
Startup of a Cynap system which shows content from a local website on startup. As soon as a user starts an interaction, the content will disappear and a new presentation is started.

Useful implementations are splash screens, campus information, event/venue informations.

User behaviour:
Cynap Power-UP

Administrator first configures Screensaver function and then needs to add EndPresentation command on Peripheral Command settings.

Configure Screensaver:



Set Startup Command in Peripheral Control:

Name: customised Name, **Digital Signage**	Description: **Specific EndPresentation (keep recordings, keep snapshots, enter Screensaver) command triggers full screen browser**
Event: **Power On**	Protocol: **TCP**
IP Add: Localhost, **127.0.0.1**	Port: **50915**
Hex Command: **09CB4903000003**	

14.3 Open WebSocket in JavaScript

Unlike the BSD socket which uses port 50915, the WebSocket port can be accessed using the standard ports (unencrypted: 80, SSL encrypted. 443).

It's a HTML5 feature and allows you to operate Cynap from standard WebTechnologies such as JavaScript or PHP to send commands and receive messages.

It is supported by most major browsers such as Chrome, Edge, IE, Firefox, Safari and Opera.

URL (wsURL): ws://<IP-of-Cynap>/xxx **e.g. ws://192.168.0.1/xxx**

```
function init_websocket(wsURL) {

        myWebSocket = new WebSocket(wsURL /*,'dumb-increment-protocol'*/ /*'binary'*/ );
        myWebSocket.binaryType = "arraybuffer";

        myWebSocket.onopen = function (evt) {
            console.log("Websocket connection '" + wsURL + "' is now open.");

            // cyclical check of websocket connection and send keepalive command
            setInterval(function () {
                switch (myWebSocket.readyState) {
                case WebSocket.CONNECTING:
                    return -1;
                case WebSocket.OPEN:
                    // no action needed
                    break;
                case WebSocket.CLOSING:
                    return -1;
                case WebSocket.CLOSED:
                    // try to reopen the connection
                    myWebSocket.open();
                    return -1;
                default:
                    // this never happens
                    break;
                }

            }, 60000);
        };
    }
```

14.4 Login command CB42

The login command is a set command which requires the access level you want to get combined with the necessary password.

// open connection, using *BSD* or *web socket* and then send following command:
// 09 CB 42 {*password_length + 2*} {*access_level*} {*password_length* <=63} {*password*}

Send hex command: 09 CB 42 0A 01 08 t e s t I n g 8

0x09	The command starts with a 09 as a set command, the size of the parameters won't exceed 256 therefore the initial hex set command starts with a 09 instead of a 0D.
0xCB 0x42	the call for the Cynap Login command
0A	the size of all parameters in total is 10
0x01	0x01: User level 0x02: Admin level 0x03: Annotation level
0x08	Length of CHARS of password
testing8	Password value Does not need to be converted into hex (ASCII c equals to 0x63)

Troubles?:
You are able to use the Peripheral Command feature of Cynap to experiment with any command even with the login command.

My advise:
Use the admin login command concatenated with a command requiring admin level rights to see if it works.

14.5 Window Start (open browser with URL) Example

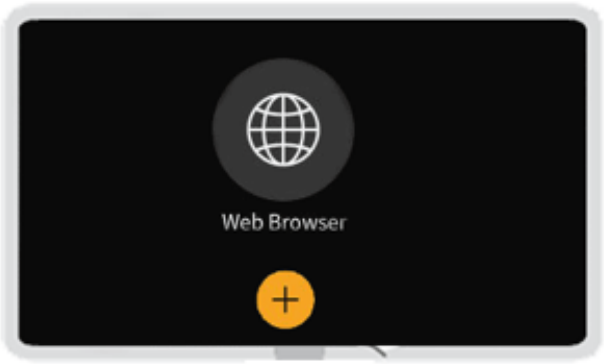
Scenario:
Provide a simple Web Browser function on your Room Management System where the user is able to use the keyboard to enter a URL and then visit the URL on Cynap's web browser.

Should you not provide a URL as a parameter, then Window Start (CB2C) will open the browser with its starting page (either the one you configured in the settings or the default one with the four icons for WolfVision, Wikipedia, YouTube and Google).

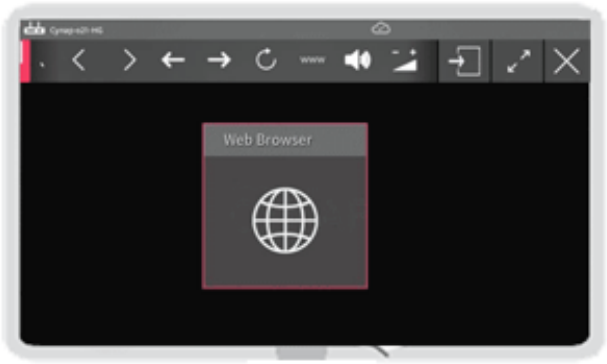
On Cynap we are able to see the newly opened web browser window with a destination URL already loaded.

For simplicity we use the parameter autoarrange (-1 or 0xff) where Cynap opens up the next possible window; if you want to try out the windows ID you're welcome to use one of the four ID´s - *0x00, red, to 0x03, blue,* - to open one of the four specific content windows.

Start with defining your layout



1. Implement your Menu
Simple layout with your own colours and symbols



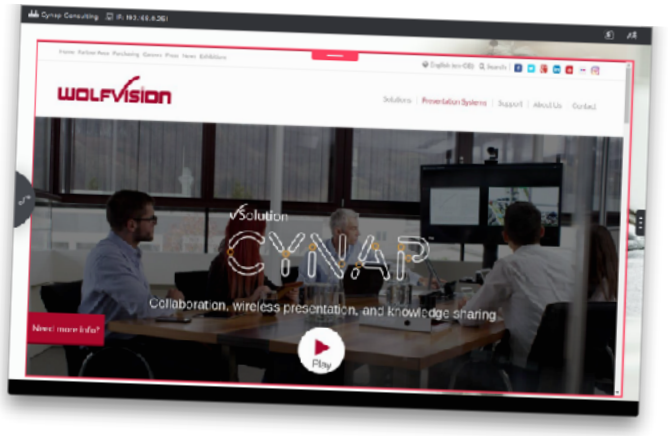
2. Create context
Add context sensitive toolbar (e.g. button for URL)

3. Enable keyboard
Show up keyboard to have URL entered

4. After you store the URL you are able to issue the WolfProt Command :
set the *WindowType* to *Browser* with a specific web address (cynap.net).

The URL will not be parsed by the WolfProt Command Agent – a malformed URL will be displayed as not found – the developer of the controller implementation needs to take care of validating the entered URL which a user typed in.

As soon as you execute the command, a browser window of cynap.net should show up.



WolfProt Command:

```
// Your RMS layout/implementation done
// Loop: Open socket and poll public GET command
//                          (e.g. polling a get command to receive a PIN,
//                          see PIN Status Room, 08 CB 54 00)
// Loop: Check if AuthorizationLevel is set to RMS_User
//                          (Set Login, 09 CB 42 01, see Login)
// All OK? Then send "Window Start, WindowID=auto arranged,
WindowType=browser"

While (socketOpen)
  While (RMS_User_logged_in)
    Send 0D CB 2C 00 0D FF 03 00 09 c y n a p . n e t
```

Command explained

0x0D	This command doesn´t start with the usual 09 visible in the set command, as the length of the parameter could exceed 256 (e.g. URL > 256 chars).
0xCB 0x2C	the call for Window Start
0x00 0x0D	the size of the parameter is 13 or in hex 0D. Since we have to follow protocol, the first 00 must be set to 0 since we are not exceeding 0xFF on the first length parameter.
0xFF	-1 for auto arranging the window (the next free one will be taken until all are used up. Before issuing a window start please make sure that not all Windows already show user content.
0x03	type of window in this example opens browser content
0x00 0x09	size of parameter, in this case, size of the following web address
c y n a p . n e t	Does not need to be converted into hex (ASCII c equals to 0x63)

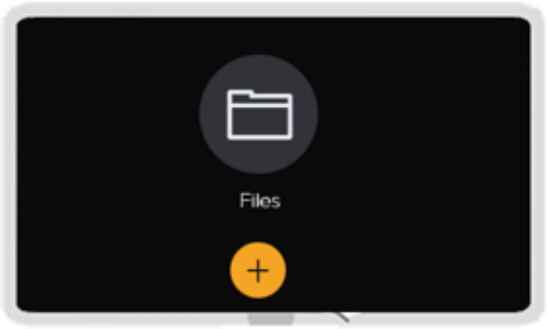
14.6 Tutorial: File Operations

Scenario:
To fetch the file list of an inserted USB thumb drive and open/use a specific file on it.
Before a file list can be requested, it is necessary to get information on the mounted drives (polling

Some files aren't supported by Cynap and we recommend hiding them or at least mark them as unsupported.

User behaviour:
The Cynap user presses the orange Plus-Icon (Source-Button) and selects the files icon. All available sources, including the file source (indicated by “Files” and an icon of a folder), are displayed.

Layout
- Create File list button
- When pressed, show the mounted drives
- Open drive and request the list of files
- Open selected file with the appropriate window type

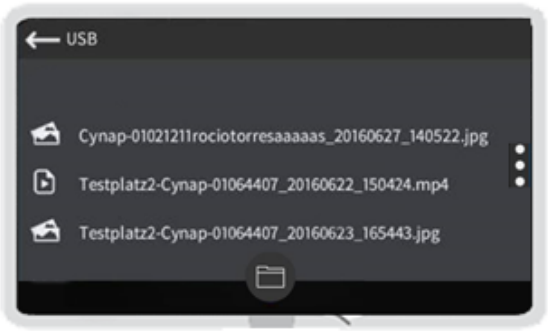


1. Implement File dialogue

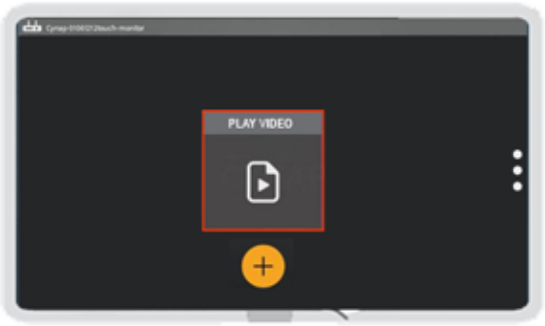
Execute command **GET Windows, 08 CB BA 00**

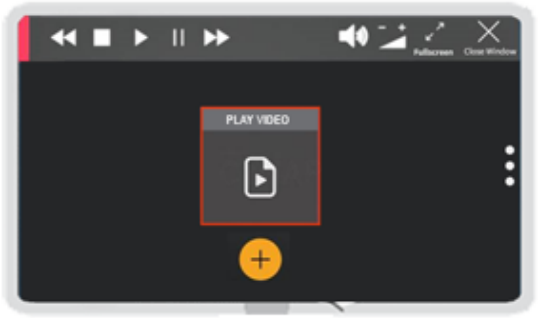
2. Get the list of mounted drives

Execute command
GET Mounts List, 08 CB 3D 00



3. Show file list – filter out files of type unknown which can not be displayed on Cynap
Execute command ***GET File List, 0C CB 3E xx***





4. Play the selected file

Execute command
SET Open File,
0D CB 3C xx
Use fully qualified name:
e.g. **USB:///video.mp4**

5. Set controls based on context of content
Execute command
Get Windows, 08 CB BA 00

WolfProt Commands:

```
// Your layout/implementation done
// Loop: Open socket and poll public GET command
//                            (e.g. polling a get command to receive a PIN,
//                            see PIN Status Room, 08 CB 54 00)
// Loop: Check if AuthorizationLevel is set to RMS_User
//                            (Set Login, 09 CB 42 01)
// All OK? Then send "Window Start, WindowID=auto arranged, WindowType=browser"

While (socketOpen)
  While (RMS_User_logged_in)

    //get and use list of mounted drives
    Send 08 CB 3D 00   //get mounted storage devices
    // process returned JSON array   (e.g. USB:///)

    //fetch event and get list of selected storage device
    // user clicks on USB storage device

    //send mounted device and parent path to show files and directories
    Send 08 CB 3E 00 07 u s b : / / /
    // process returned JSON array  (e.g. video1.mp4)
    // hide files of type unknown or clearly mark them as inaccessible

    //fetch event and open requested file
    // next available window on Cynap will open itself
    Send 0D CB 3C 00 10 u s b : / / / v i d e o . m p 4
```

14.8 Sample C Code for a Wake on LAN (WoL) Broadcast command

Depending on your network configuration a UDP broadcast might be filtered out, making it impossible to wake up/start Cynap.

Please check our *Network Integration Guide* available on our website for more information about required network configurations.

```
// Prepare Broadcasting
// IP = 255.255.255.255  Broadcast IP
// Port = 0xC6E1 Port 50913 decimal to hex
Cynap.connect (
       (0xffffffff), // 255.255.255.255 in hex
       (0xc6e1)      // Port 50913 in hex

// prepare SendBuffer
Init SendBuffer[1024] //address buffer of size of 1024 bytes
int counter=0  // pointer to be used to add required information at correct
buffer pointer location

// first 6 bytes should be 0xff
for (int c=0;c<6;c++)
       SendBuffer[counter++] = "0xff"

// next add 16 times the CYNAP_MAC_ADRESS
CYNAP_MAC_ADDRESS ="086066ff66ff" // (should look like 08:60:66:FF:66:FF or
086066FF66FF)
for  (int c=0; c<16;c++){
       int d=0
       // convert CYNAP_MAC_ADDRESS into hex-format
       for (int e=0;e<6;e++) //6 bytes of CYNAP_MAC_ADDRESS{
              SendBuffer[counter++] = ConvertToHex
(CYNAP_MAC_ADDRESS.substring(d,2),HexValue)
              d+=2}}

// Send Broadcast to activate MAC addressed device
send status=Cynap.send (SendBuffer,1024)
```

Please make sure that you issue a Wake On LAN call when the sending device is **connected and ready to send**.

14.9 Sophisticated commands

Sophisticated commands are commands that go beyond the limitations of the provided template.

For example the number of input streams is limited to 4, but if you need more you are able to change the 4 slots dynamically. If you need to show more than 4 input streams, then you have the possibility to come up with your own UI, using HTML, a web socket connection and a number of javascript instructions.

These combinations usually require a mix between Admin-level and user-level commands. So switching between different user levels requires every session to be authorised before a command will be successfully executed.

The table below is not concluded. Please read the command list from the website to utilised Cynap in your environment.

The listed APIs use only the first 3 bytes for easier finding.

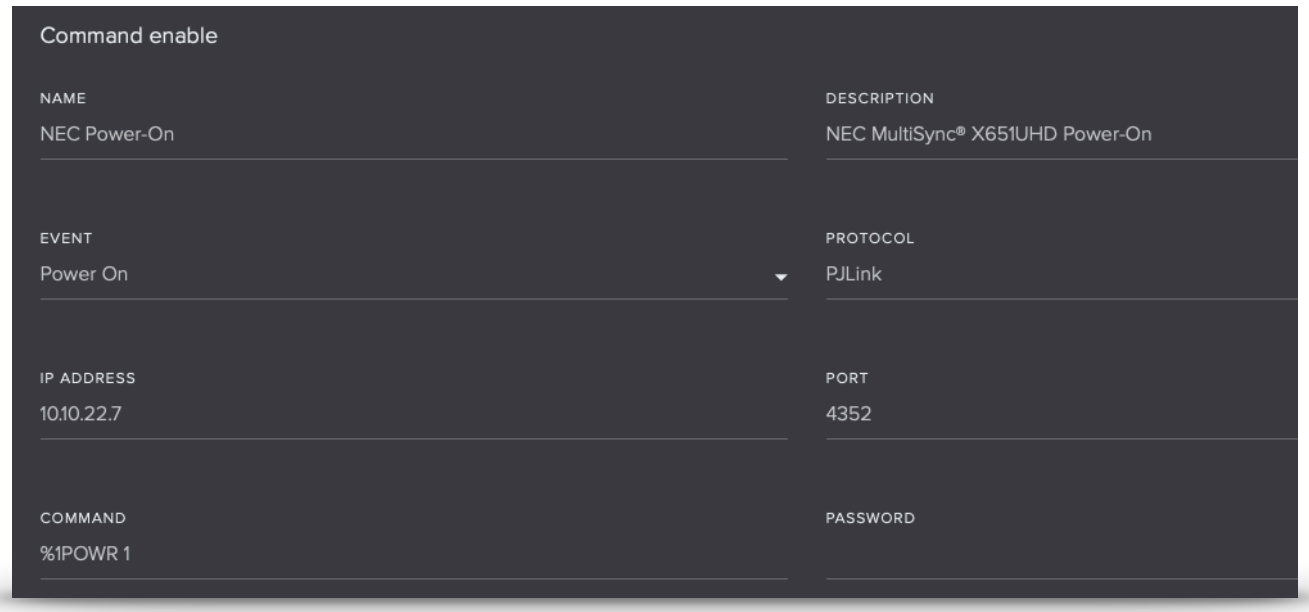
Case	APIs	Description
Change System Language	09 CC41	If you need to support more than one language for Cynap and need to change it dynamically.
Shutdown while recording is still active	09 CB25 0D CBBF 09CB49	Stops the recording, copies the file to a specific location and sends Cynap into Standby mode. You are also able to dynamically log into a cloud and upload/ store files.
Personalise Cynap for each presenter or event	OB01 CC72 09 CB49 OB01 CB80 09 CB45 09 CB46 09 CC5F 09 CB80 00 09 CC5F	Change Screensaver and start of Cynap with a personalised Splash screen of presenter. Change wallpaper to reflect presenter. Offer Cloud access to presenters files (please check each cloud service for specific login command) Change browser starting page to topic or desired page of presenter… …and then roll back to default wallpaper and to remove the starting page after the personalised session is over…
Switch on or off screen (e.g. browser access)	0D CC06 09 CC07	Add a PJLink command and then test/execute it (if already listed, then CC07 to execute it directly)
Force Matrix client to stream its content to all stations	09 CC81 09 CC82	Pull content from Matrix client using its serial number and then push said content to all other connected clients.
Start a recording with a pre-defined name	09 CB25	

15 PJLink

The use of PERIPHERAL COMMANDS in Cynap's settings provide for some interesting setups - you are able to send a Cynap API to a different Cynap in your network, or to the one in use - send a WAKE ON LAN to a specific device and switch on or off a screen when no longer needed by Cynap by using PJLink on supported projectors/screens.

Simply send %POWR 1 to switch on or %POWR 0 to switch off a screen.
All you need to know (usually listed in the device's user manual) is the port number and, if required, userid and password.

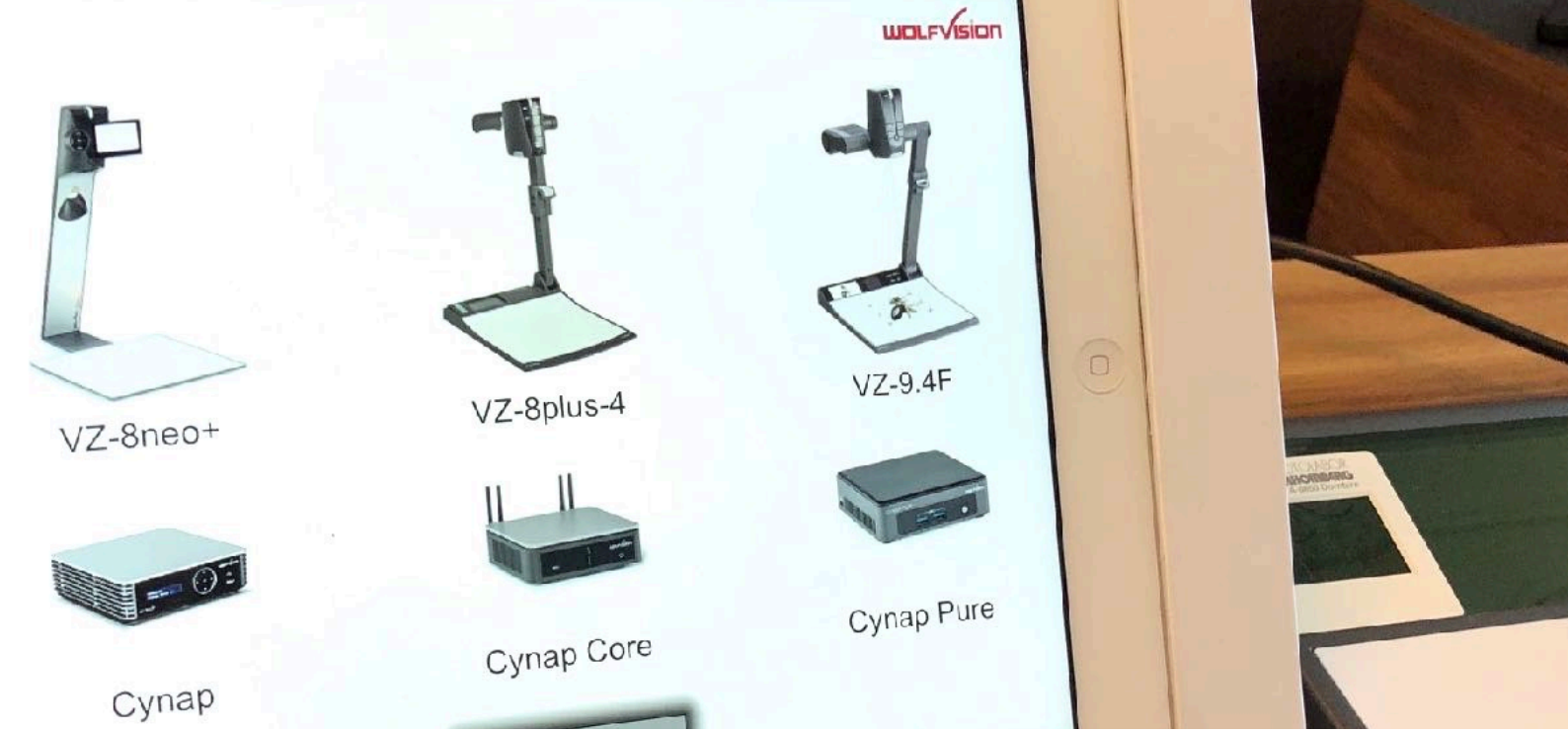
On Cynap's PERIPHERAL CONTROL settings, you need to switch the protocol from TCP/UDP to PJLink and fill in your devices's IP, the port number (usually 4352 - and make sure it's available) and the %POWR 1 to have it switched on on Cynap's startup (EVENT: Power On).



Part 4: 3rd party controllers

If it was hard to write, it should be hard to read!

All about installing and troubleshooting our Cynap module for AMX, CRESTRON and, EXTRON.



16 Room management/control system, 3rd party controller

Cynap products are ready to be controlled by any 3rd party controller on the market.

WolfVision offers ready-made Crestron and AMX modules for a very convenient integration. The included interface allows to fully control and set every aspect of your RMS configuration.

The provided templates should be customised and adapted for your specific integration.

Apart from available AMX and Crestron templates, any control system on the market can be programmed to control Cynap by using our Cynap API protocol via web-socket. A simple and fast way to get access to Cynap on your implementation.

Modules are being refreshed from time to time to add additional Cynap functions.

Caution: the provided templates are for demonstration purposes only. The templates contain ALL functions. We strongly advise to customise the template to improve usability and performance for maximum customer satisfaction!

17 Before we begin

Cynap's streaming services can cause increased network traffic which might interfere with a 3rd party controller.

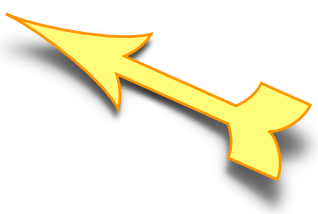
It is highly recommended to follow your 3rd party controller brand's network recommendations in any setup.

Protocol changes do happen, and new commands will be added regularly with every updated release of an updated Cynap OS. We therefore advise to check for obsolete and changed commands in your implementation before applying a new release.

The data sent to Cynap via Cynap API won't be neither parsed nor validated. Please mind this fact before changing vital settings (e.g. network configurations) when using Administrator Access Level commands.

Our Crestron and AMX Demos module are huge, they contain almost all Cynap functionalities.

Please make sure that you adapt your module to the performance of your controller or change the model of your controller to match Cynap's demo module if you copy/paste it for production use.



18 Download and setup

18.1 Basic setup with Wolfvision provided Crestron or AMX templates

IDE:
Make sure that you got your RMS IDE up to date and ready. For example, to seed a Crestron master console with the necessary runtimes and touch-panel-UI you want to use the Crestron MasterInstaller to download the required components with its latest available version.
Crestron Dev Primer: http://www.crestron.com/downloads/pdf/product_misc/sw-simpl_primer.pdf

Or, for AMX, use the AMX WebUpdate to download the necessary IDE (e.g. NetLinx Studio 4) and its components.
AMX Netlinx Programming Language: http://www.amx.com//assets/manuals/NetLinx.LanguageReferenceGuide.pdf

We do provide fully working templates(controller/layout) for AMX and Crestron which can be used as-is or can be altered to suit your needs.

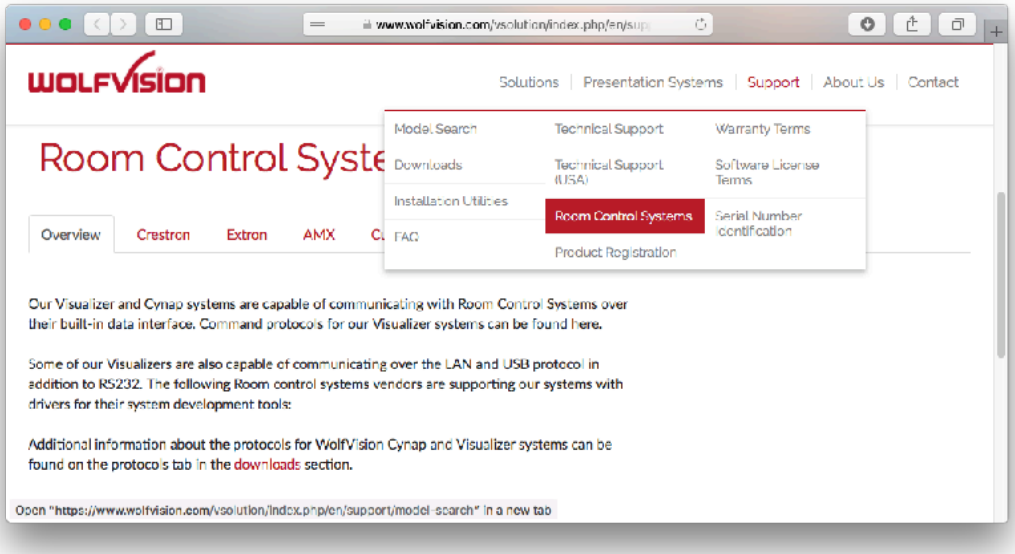
18.2 Download room control templates from wolfvision.com

Templates for AMX and Crestron controllers are available at:
URL: https://www.wolfvision.com/vsolution/index.php/en/support/room-control-systems

Extron controller templates are available on Extron's website, linked also on wolfvision.com.

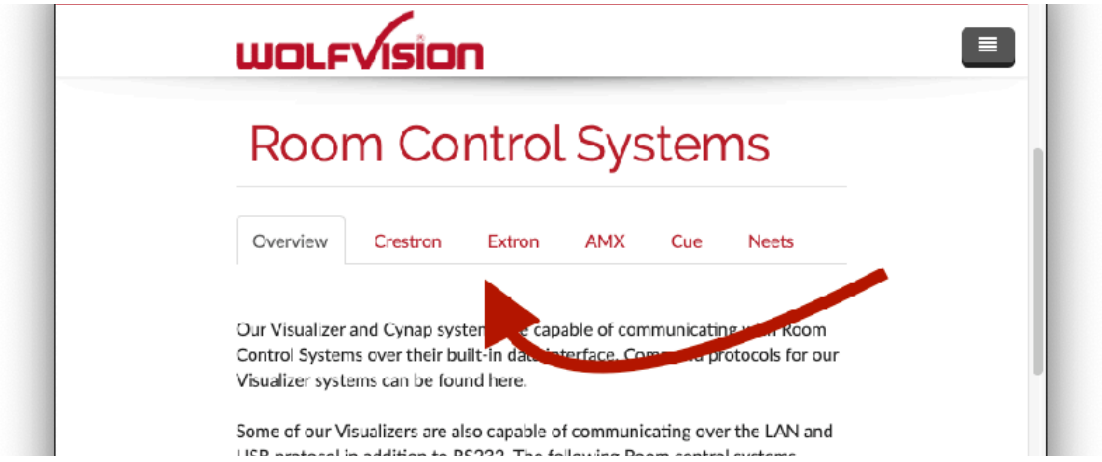
Select the available Crestron or AMX template and download the provided .zip (Crestron) or .axw (AMX) from our server.

Enter www.wolfvision.com and hover on link *Support -> "Room Control Systems"*



On page **Room Control System** click on your 3rd party controller brand (at this time we do provide templates for **Crestron, AMX and, Extron -** the one for Extron is provided by Extron on their website).

Download the .zip for Crestron or the .axw for AMX from our supporting website and please make sure that the template matches your installed Cynap or Cynap Core firmware.



18.3 The setup process

Connectivity
The WolfProt API´s consists of a variety of Get and Set functions to control Cynap or change settings via WolfProt.

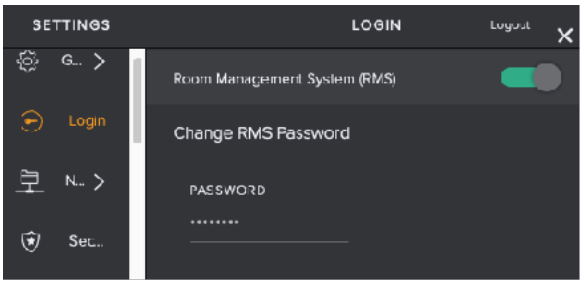
Almost all of the WolfProt commands require an authorised session.

Basic steps to connect your 3rd party controller with Cynap
1.Get the IP and MAC address of your Cynap
2.Set RMS User Password in Cynap's settings
3.Change the template based on Cynap's IP and MAC and RMS User Password
4.Compile and upload the files to your RMS console
5.Make sure that **TCP Port 50915** (reserved for Cynap) is not blocked by a firewall - if you want to have your communication encrypted, then please use the TLS protected web socket address or port TCP 50917

Get the IP and MAC Address of your Cynap/Cynap Core
The MAC address of the corresponding networking interface can be seen using the front panel menu or by visiting the networking configuration in the settings menu. Please see chapter 5.6 for an illustrated example.

Please remember to use a fixed IP or make sure that Cynap always uses the same IP address on DHCP in order to be found by your 3rd party controller.

RMS User
Make sure that an RMS user has been configured to allow access even when no moderator login has been defined.



Integrating the downloaded template
Cynap 3rd party control templates are available for Crestron, AMX and Extron. To transfer the necessary files you need to have the respective development environment (download the latest version via MasterInstaller (Crestron) or WebUpdate (AMX).

There are several templates available, choose the one corresponding to your Cynap firmware or type/model of your management system.

The procedure to prepare the template before it's sent to each controller/terminal is similar on both platforms and consists of replacing the existing default values in the template configuration.

Please do:
1. Replace the existing sample Cynap-IP
2. Replace the existing MAC address of Cynap (for WOL command/magic packet)
3. Replace the password of your defined RMS User

19 Crestron

Module Format
The modules are provided as Simpl+ modules (.usp and .ush) embedded in a Simpl Windows module (.umc).

A file has also been provided in .smw format to allow for an easy integration into your project.

A touch panel file has been provided for X-Panels which can be used without any additional developing.

We do support Model 3 controllers (there is a legacy Model 2 controller module available on our website) – please make sure that you applied the latest updates to your firmware, as Cynap is controlled over WebSockets (model 2 and model 3).

Features
All the features of Cynap, except Feature Pack functions, are included in the template.

Using the modules in your program
The various modules are described in the template PDF file. The module has been optimised for use with a MC3 controller - if you face performance issues, please make sure that you either (recommended) change the demonstration module or switch to a more powerful Crestron processor.

Content of unzipped Crestron Template archive

File	Content	Action
Cynap.smw	SimplWindows demo program file detailing the use of the module	Main file
Cynap_Client.usp	Simpl+ Source Code	Simpl+ source file and can be opened and modified in Simpl+
Cynap_Client.ush	Simpl+ Source Code	generated from the same name .usp file and CAN NOT be opened or modified
Cynap.vtp	TVPro demo Touchpanel project file to use with the SimplWindows program	The .vtp file can be opened in VTPro and modified as desired
Cynap.vtz	VTPro Touchpanel project file	Compilation of .vtp – the vtz file CANNOT be opened in VTPro
Cynap.sig	Crestron Testmanager Signal File	This is the test file for the same name .smw file. The .sig file cannot be opened/modified in SimplWindows
Cynap.lpz	Yoiur built 3 Series SimplWindows compiled code	Uploaded to processor
Cynap.sgd_	Smart Graphics Data file generated by Visiontool Pro-e for Simpl Windows	Cannot be modified or opened in Visiontool
Cynap_Module_Help.pdf	User Guide	To be read
Cynap_documentation.pdf	This Guide	To be read

Unzip the zipped Crestron Template and double-click on file Cynap.smw. Save the UMC, USP and USH files in your project folder. Perform a re-sync. Add the UMC into your program.

Simpl loads the file and all you have to do is heading to the section where you can change the required parameters (IP, Mac and RMS User Password) and save the file.

Crestron Cynap Library (Crestron controller)

Change default values

At the Cynap UI file all you need to change are 3 parameters to have a secured connection and are able to wake Cynap from deep standby.

Following changes need to be applied in order to control your Cynap.

Variable	Example	Description
Server_IP	10.10.50.52	IP of the Cynap you want to integrate into your AMX application
Cynap_RMS_Password	my-secret-pass	Password which got set in Cynap Settings LOGIN section. You are also able to use the admin login password, but please bear in mind that you also need to change the login level.
MAC_Address	$08, $60 $6E $FF $A0 $B1	LAN1 or LAN2 Port MAC address to power up Cynap using a magic packet (WakeOnLAN).

Step 1: Open Cynap.smw

Step 2: in Program View click Folder Logic and pick S-1: Cynap Client

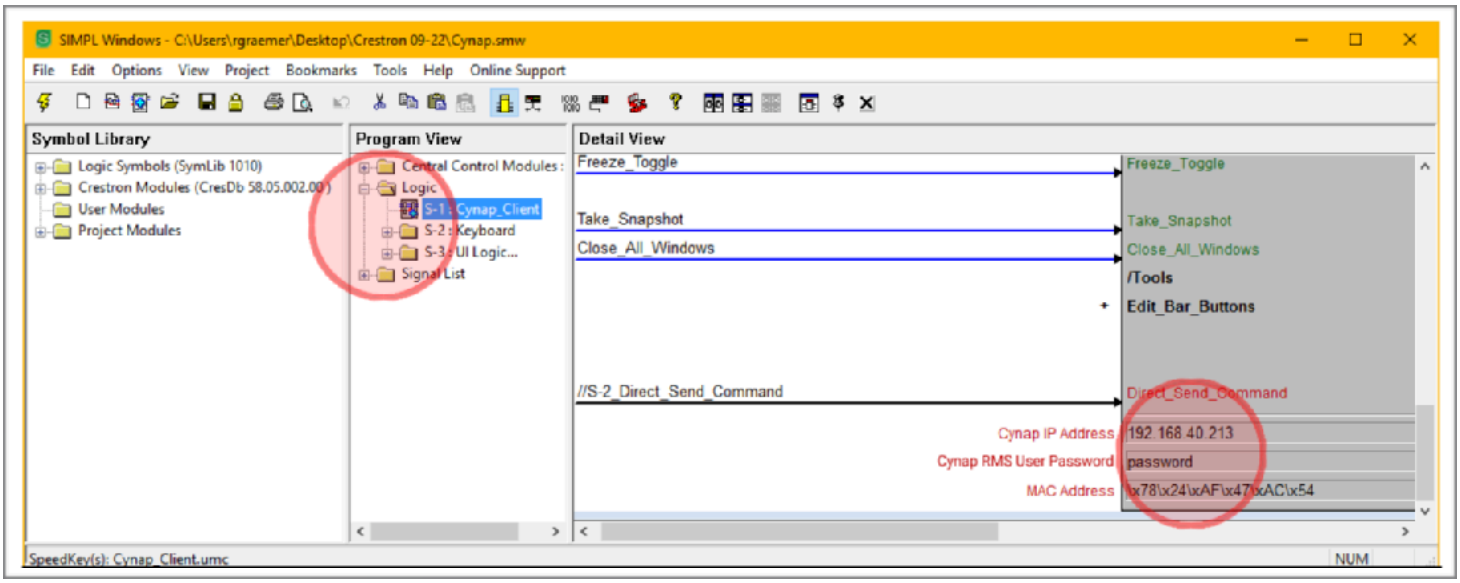
Step 3: In the detail view change following parameters
- Cynap IP address - IP address of LAN1 or LAN2
- Cynap RMS user password (the password which grants you user level access)
- MAC address (for Wake On LAN startup used in Cynap Standby mode - also LAN1 or LAN2)

Hint: please use a fixed IP in order for the AMX system to find your Cynap.
The password should match the one you entered in Cynap's settings at Login->Room Management System User

Build the CynapClient System after changing all 3 parameters.

Step 4: Compile, transfer and run demonstration template

Screenshots



OVERVIEW (STEP 1 - 3)

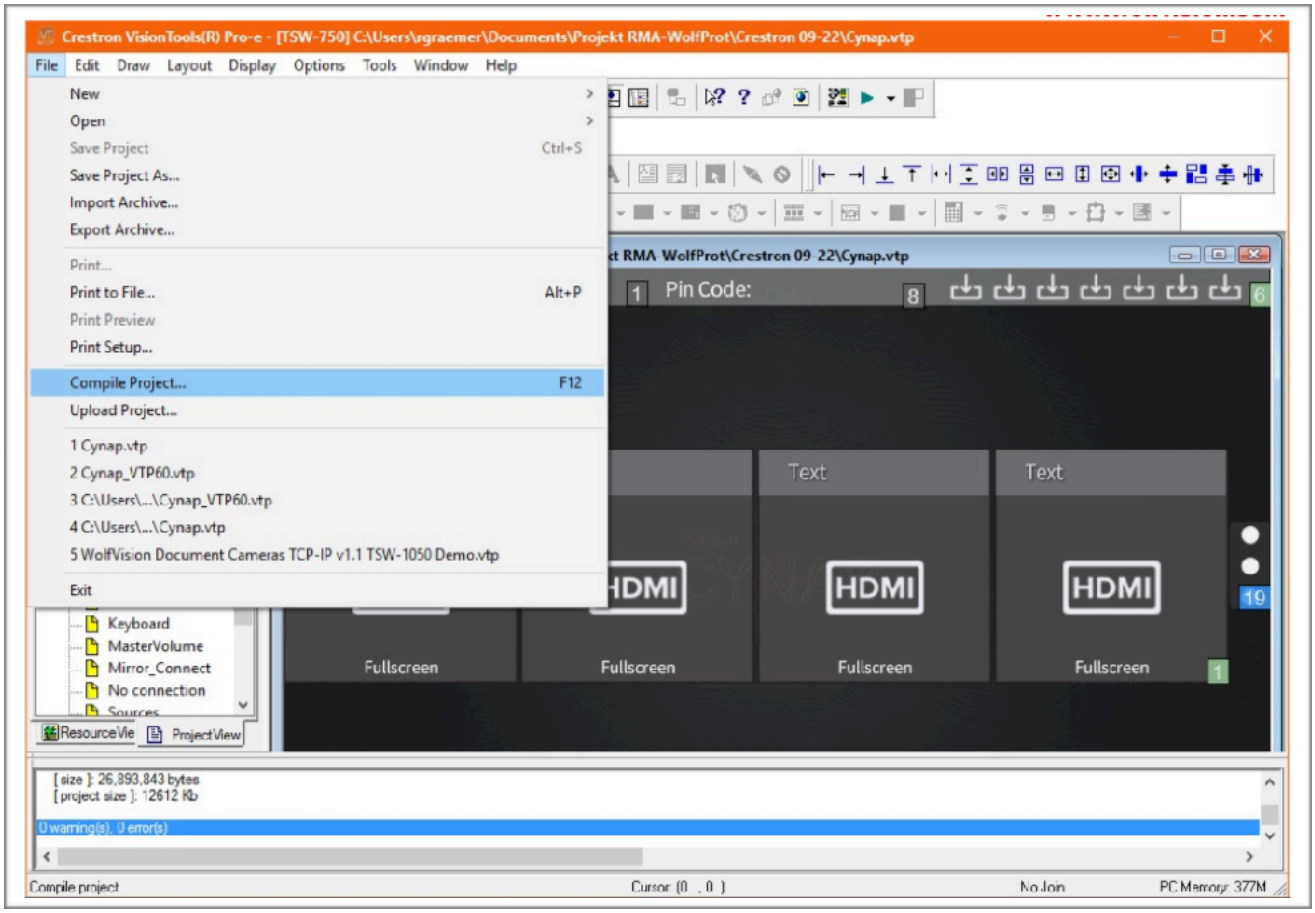
DETAIL VIEW (STEP 3)
Enter values fetched from your Cynap System

Crestron Cynap Touch Layout

The module offers .usp and .ush embedded in a Simpl+Windows module (.umc).

An additional .smw resource file and a touch panel design file (for X-Panels) has been added to allow a quick integration into your project.

Please remove unnecessary buttons as the layout template includes every possible function and has, therefore, not been optimised for an operational environment.



20 AMX

Module Format

The modules are provided as project, source and design file (.apw, .axs and, .tp4) embedded in a *NetLinx Studio* module (.umc).

A file has also been provided in .ax format to allow for an easy integration into your project.

Content of unzipped AMX template archive

File	Content	Action
Cynap_Exported.apw	Project file	Used in NetLinx Studio to build and transfer template
Cynap.TP4	Touch Panel Design	Used in TPDESIGN4 and can be modified
Cynap_Client.axs	Client source file	Used in NetLinx4 Studio/editor and can be modified
Cynap_Test_environment.axs	Test file	Used in NetLinx4 Studio/editor and can be modified
Cynap_UI.axi	UI source file	Used in NetLinx4 Studio/editor and can be modified
CypapUI and COMM modules.pdf	Description of AMX template	Supported commands and details about its development

Setup AMX Template

Please make sure that you've got the latest version of NetLinx Studio installed on your PC.

Download the .awx file from our website and store it on your computer. Double-click on the download file and it will expand itself within NetLinx Studio.

If default behaviour got changed you are able to rename the .awx file into a file with extension.zip to extract its content.

Change default values

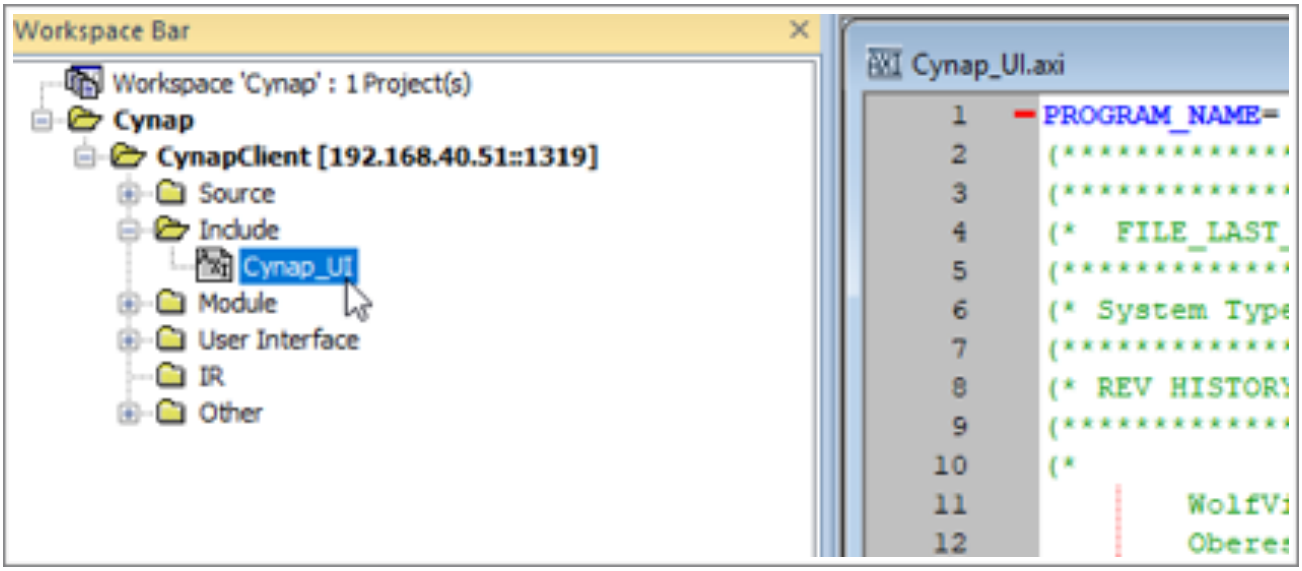
At the Cynap UI file all you need to change are 3 parameters to have a secured connection and are able to wake Cynap from deep standby.

In Cynap_UI: Search (Ctrl-f) for the variable section and change the following variables and its values:

Following changes need to be applied in order to control your Cynap.

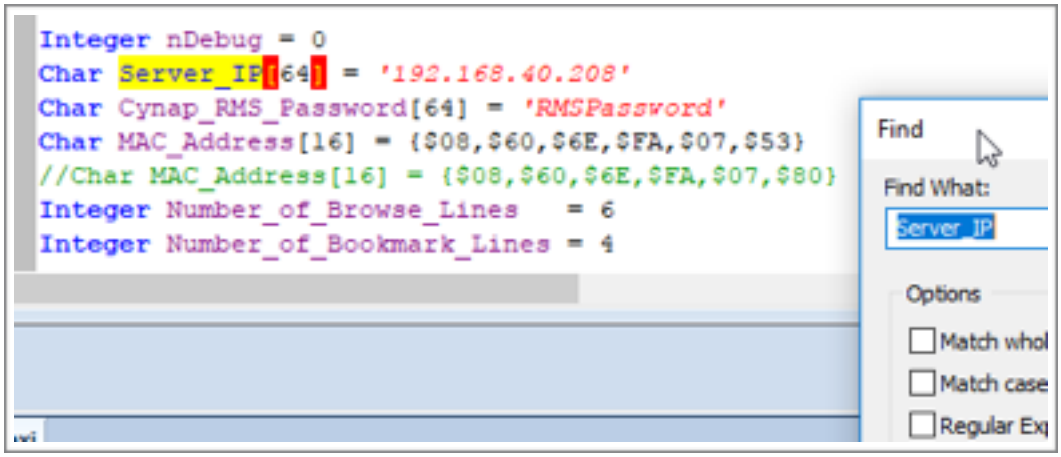
Variable	Example	Description
Server_IP	10.10.50.52	IP of the Cynap you want to integrate into your AMX application
Cynap_RMS_Password	my-secret-pass	Password which got set in Cynap Settings LOGIN section. You are also able to use the admin login password, but please bear in mind that you also need to change the login level.
MAC_Address	$08, $60 $6E $FF $A0 $B1	LAN1 or LAN2 Port MAC address to power up Cynap using a magic packet (WakeOnLAN).

Double-click on Cynap_UI:



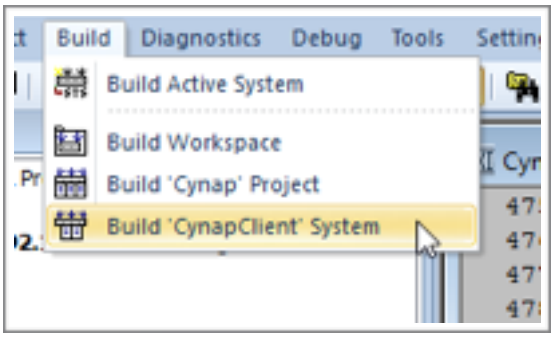
Search for Server_IP

Enter Cynap IP address and MAC address (LAN1 or LAN2 interface).

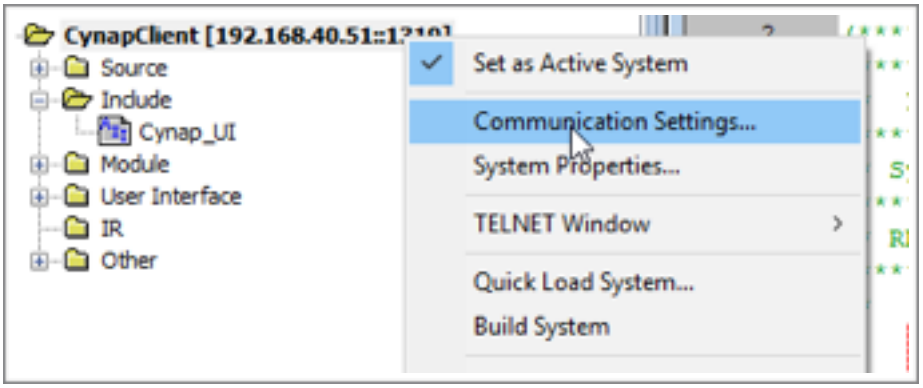


Hint: please use a fixed IP in order for the AMX system to find your Cynap.
The password should match the one you entered in Cynap's settings at Login->Room Management System User

Build the CynapClient System after changing all 3 parameters.



Adjust controller IP address:



21 Extron

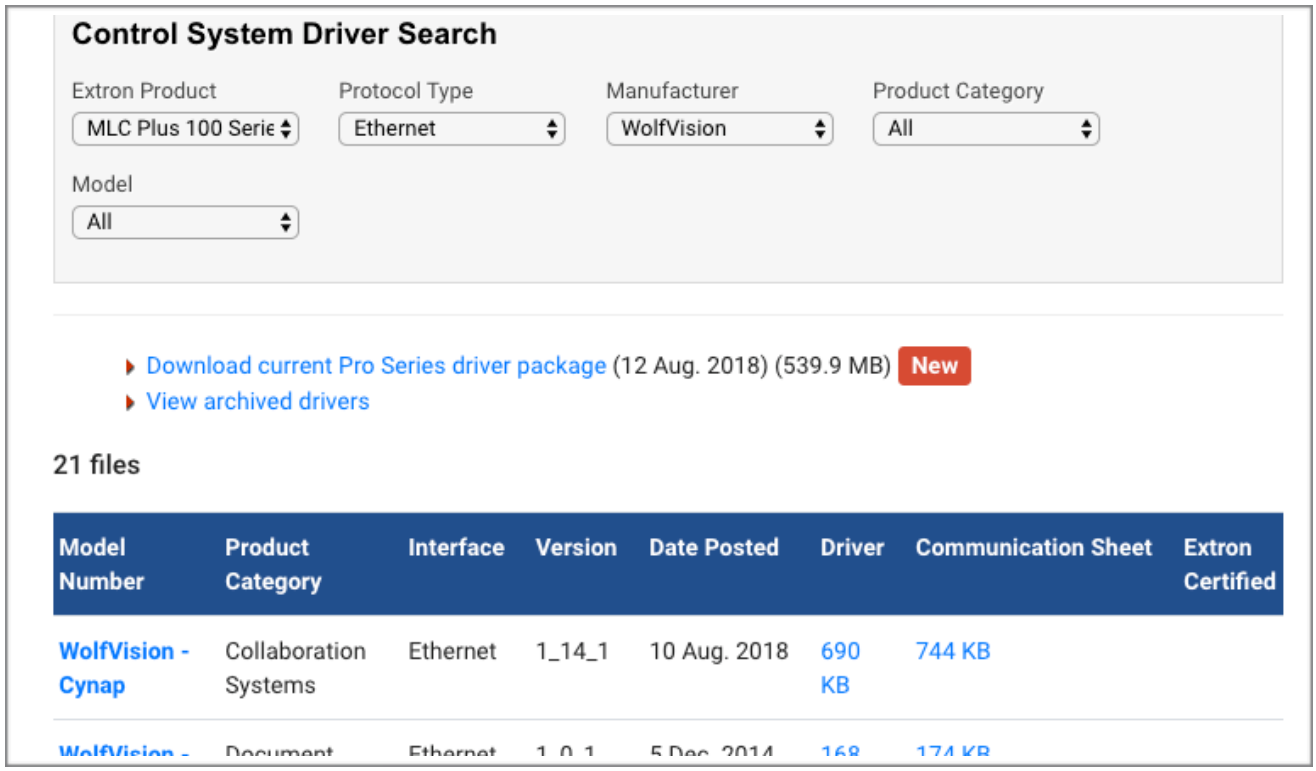
The process to download the Extron template is different. Instead of downloading the template from our web server you need to download the template from Extron itself Extron s

Link: https://www.extron.com/download/driverfilter.aspx?s=db

On the page you need to select your Extron product and filter the results for Protocol Type: Ethernet and Manufacturer WolfVision.

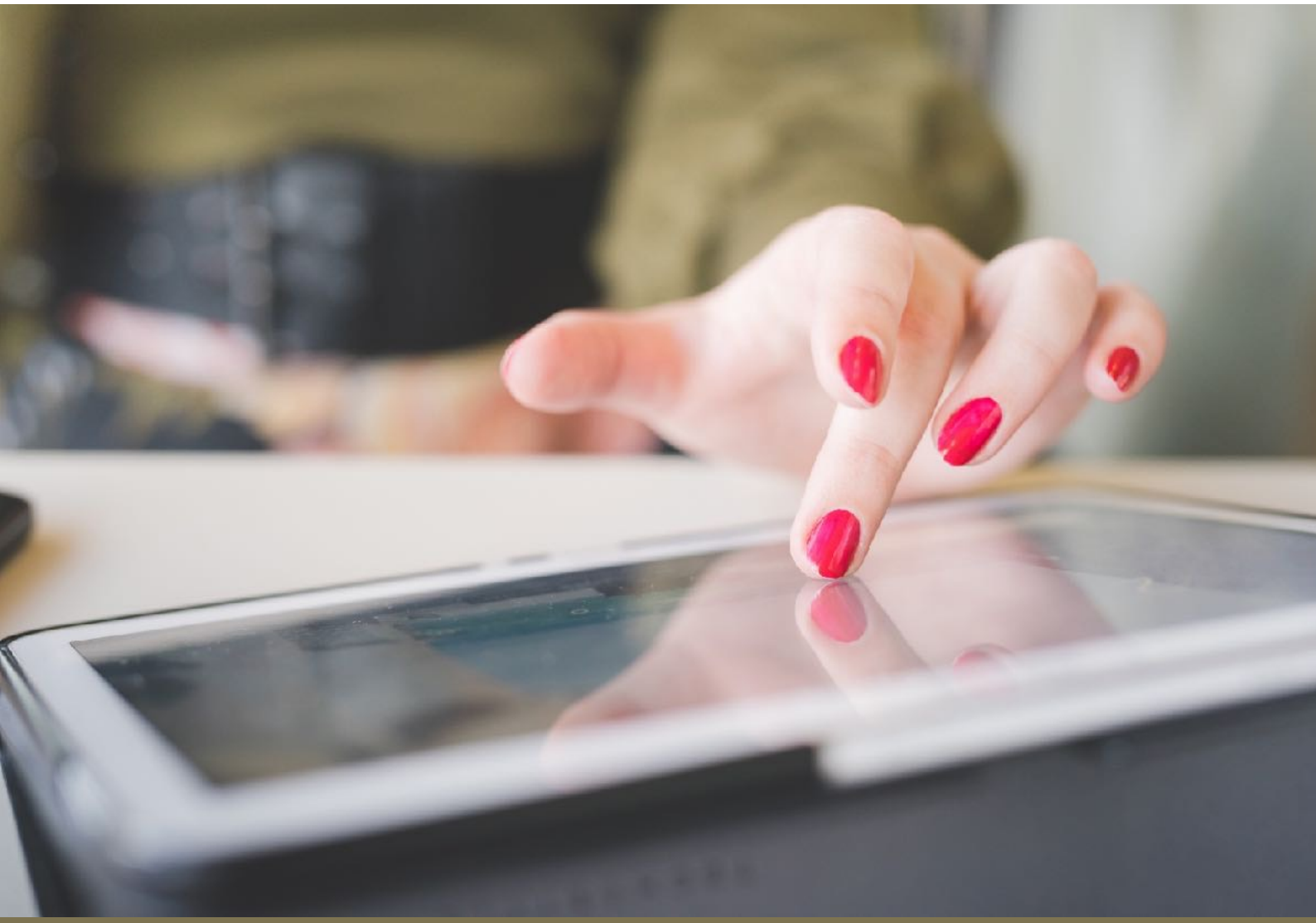
Cynap should pop up on top of the list.

Log-in and download the driver and check the communication sheet for changes of the driver.



Part 5: Troubleshooting

If it was hard to write the source code, it should be hard to read!



Maybe the solution to your problem is already here.

22 Troubleshooting

22.1 Command issues

Check that the MAC and IP address as well as all TCP/UDP ports are configured correctly.

Start Wireshark

Using Wireshark to verify your get and set commands

Start collecting the traffic on the interface used for Cynap communication (e.g. Ethernet) – Important: connect to Cynap after the start of traffic collection, otherwise Wireshark won't be able to initiate properly and won't catch traffic on the WebSocket protocol.

Filter the IP address of your Cynap and your command in hex.
For instance: ***ip.addr == 192.168.10.10 && eth contains 08:cb***
Example of *Get Access Token* command, **08 CB 02** (Screenshot: lines marked in blue).

22.2 Authorisation issues

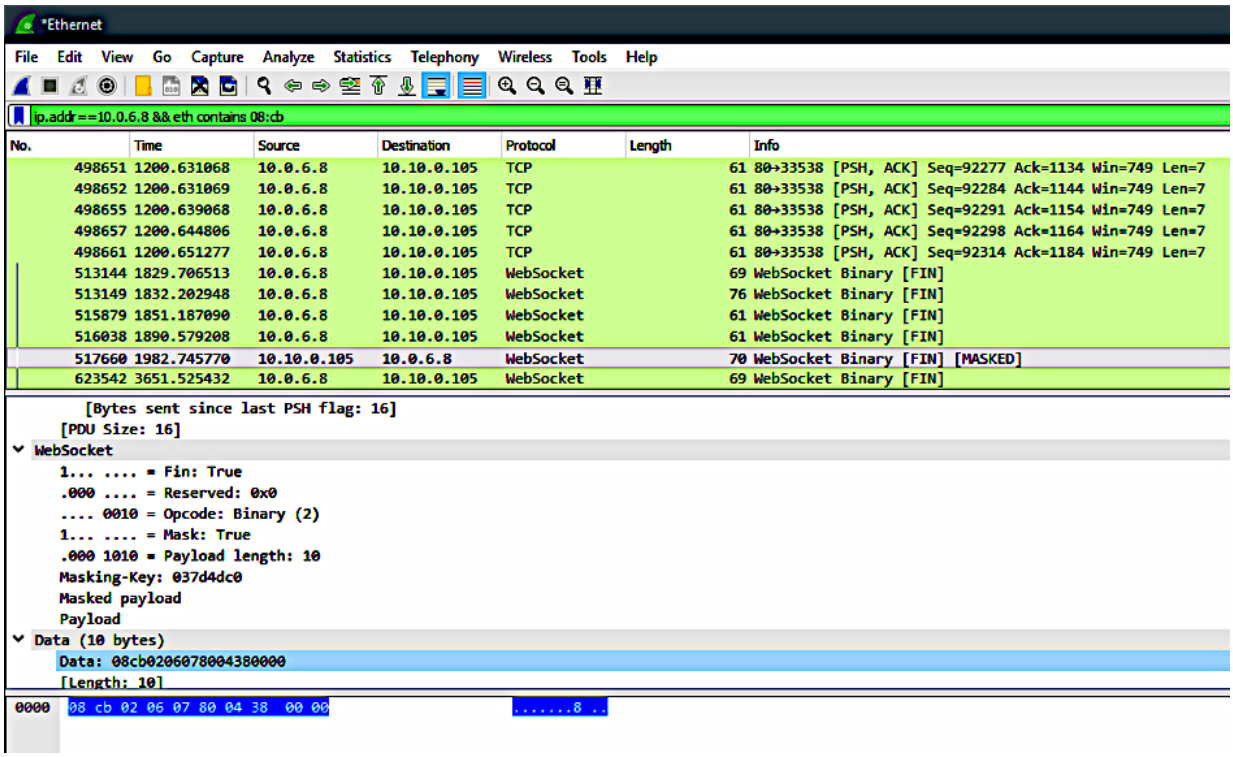
Check that the Room Management System user has been set up with the same corresponding password (on both ends).

Make sure that the command you're sending is being covered by the necessary Access Level of your former login command and is using the same connection.

Try using the *Peripheral Control* in the *settings* of Cynap to issue a simple command.

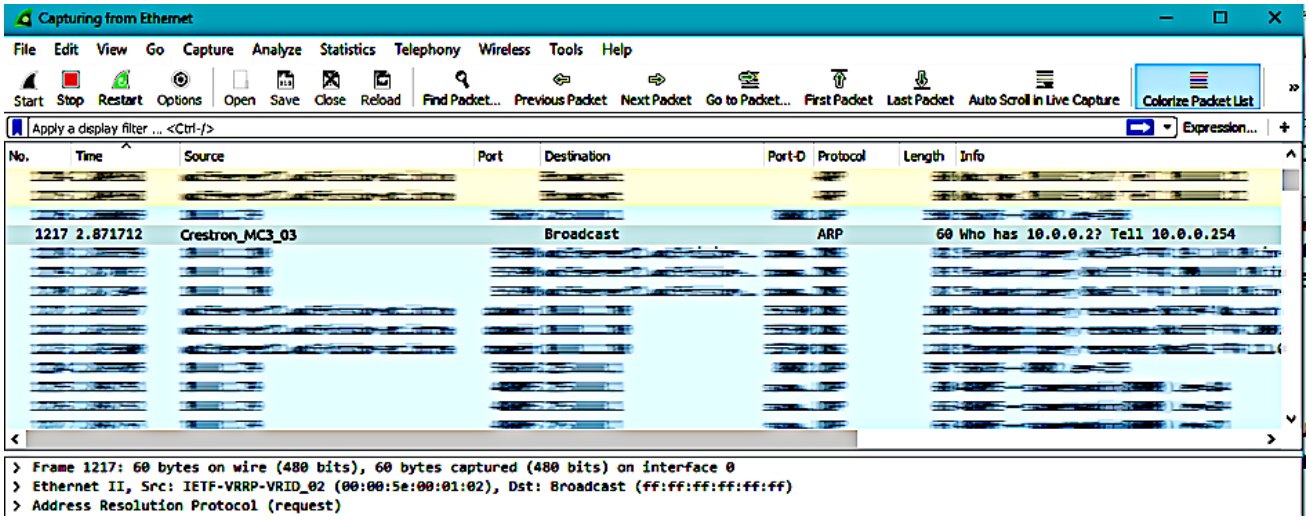
22.3 Networking issues

Command line, terminal or shell: ***ping*** the gateway of your network and issue an ***arp –a to*** get a list of IP and MAC address combinations to check if your Cynap's MAC address is found.



22.4 IP Address of Crestron controller lost?

When you lost your static IP address of your connecting devices then connect your laptop to the same network or hook it up directly attached to your PC/laptop and then start Wireshark. Observe the traffic and check the UDP broadcasts to see, which IP addresses are broadcasting (WHO HAS-ARP messages).



22.5 Every Crestron device got its IP and still nothing is happening on Cynap?

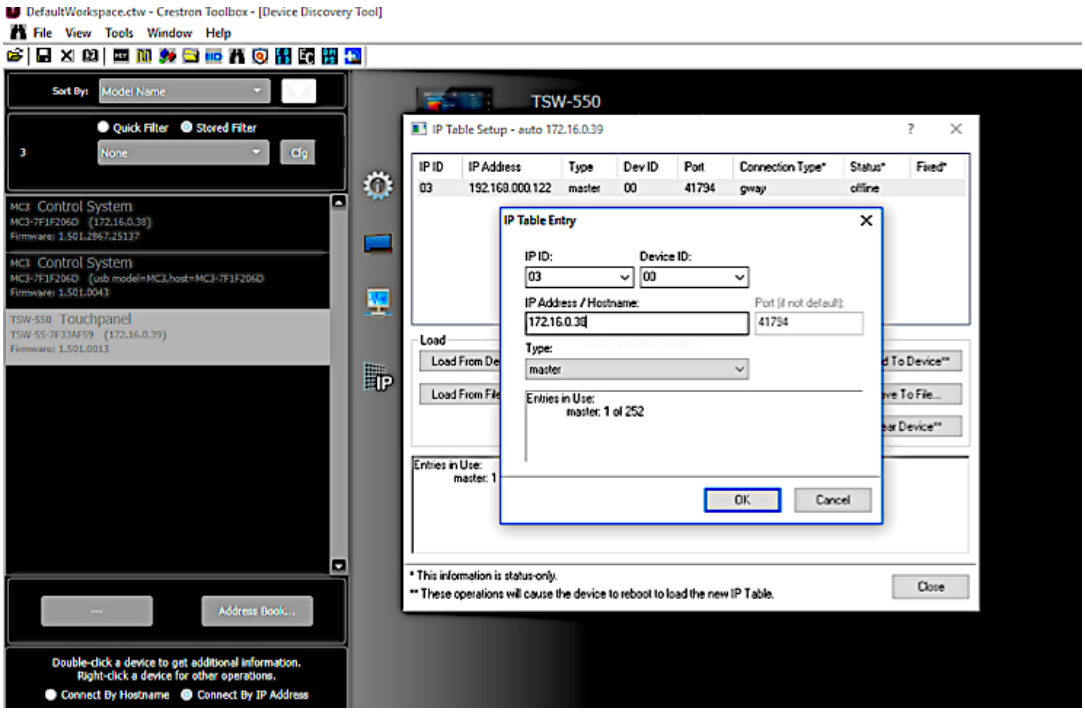
Verify if the IP table on your touch panel lists the master console.

Open op the *Crestron toolbox*, enter the *device discovery* and double-click on your touch panel device. There: click on the *button IP tables* and enter the corresponding control unit.

22.6 Device issues

Check that the Cynap module is being executed on your 3rd party control processor.
Check that the layout file has been transferred and loaded onto your touch terminal.

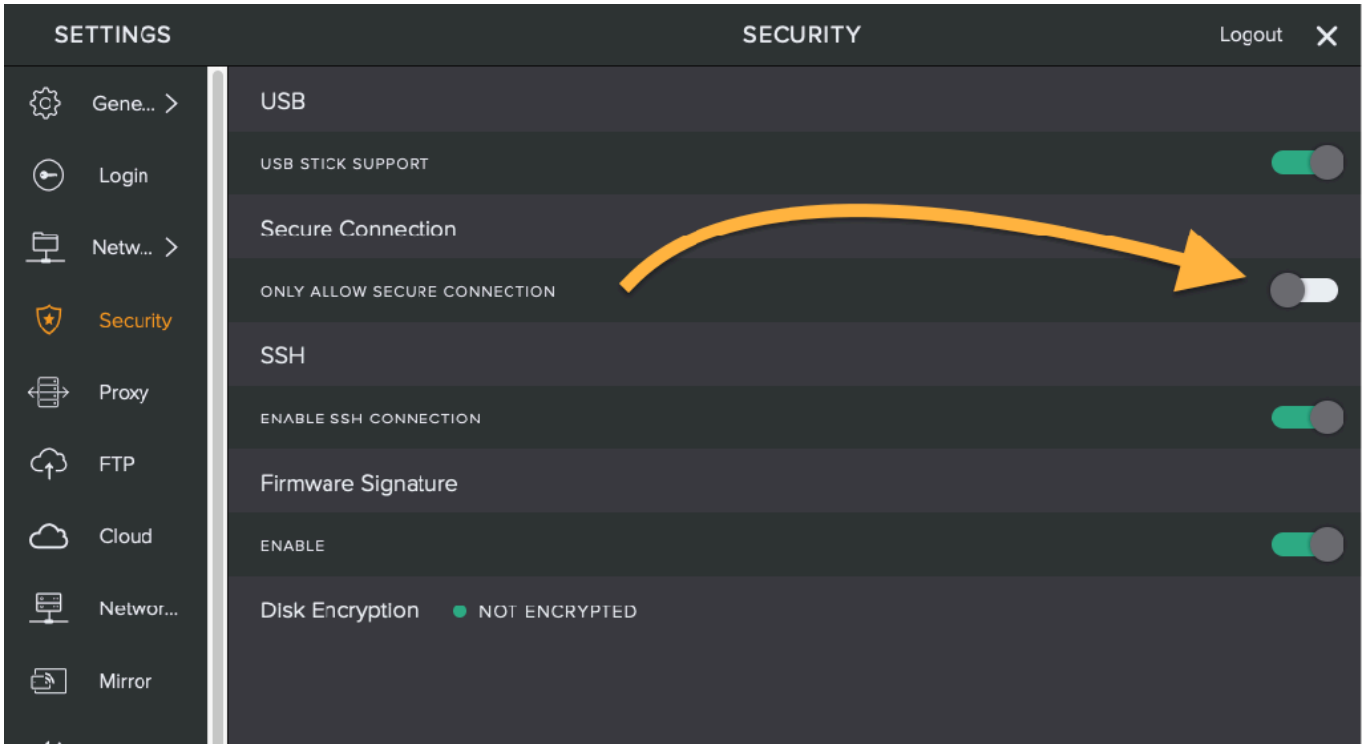
22.7 Crestron: downloaded template installed but no reaction?



Lots of experiences did show that missing connections can be solved by installing the latest controller patches.

22.8 Sending commands on encrypted Cynap port

If anything fails, maybe you did change Cynap Security Settings. If you activate: ONLY ALLOW SECURE CONNECTIONS, then Cynap will stop listening on its unencrypted ports/sockets. Either allow unencrypted ports or build an encryption hand-shake (e.g. use wss:// instead of ws://) to send your commands encrypted.



22.9 Slow performance

If you copy the complete Cynap module from our website and run it without optimisation, then the entry model controller might not be able to give you the performance you need.

Using the provided library along with your personal development might be the fastest way to implement your setup, especially when it comes to only a handful controls

Part 6: Quick Guide

Cynap APIs in a nutshell

Quick guide for a quick start.

23 Quick rundown

23.1 Rules

#1 There are 2 options to choose from.

1. No moderator login has been set => **execute commands without prior login.**
2. Moderator login has been set => **execute each command with a login instruction**.

#2 Send command to port 50915 or to web socket ws://[CYNAP-IP]/xxx

#2 Send SSL encrypted command to port 50917 or to web socket wss://[CYNAP-IP]/xxx

If Cynap security settings have been set to ONLY ALLOW SECURE CONNECTIONS, then you need to use the encrypted ports (and an encryption connection setup) to communicate with your Cynap.

23.2 Example: Open a window with HDMI1 input as source

Start window (hex 0D CB 2C) is explained at page xxx.

Open connected HDMI1 input as an available Cynap window

Without login	0DCB2C0004ff020100
With login (hex CB42) Using 12345678 as password	09CB420A0108010203040506070 8 0DCB2C0004ff020100

netcat command (without login and assuming a Cynap IP of 192.168.0.1)
echo -n -e "\x0D\xCB\x2C\x00\x04\xff\x02\x01\x00" | nc 192.168.0.1 50915

Please consult the rest of the document if you still have pending questions.

23.3 download the list of commands

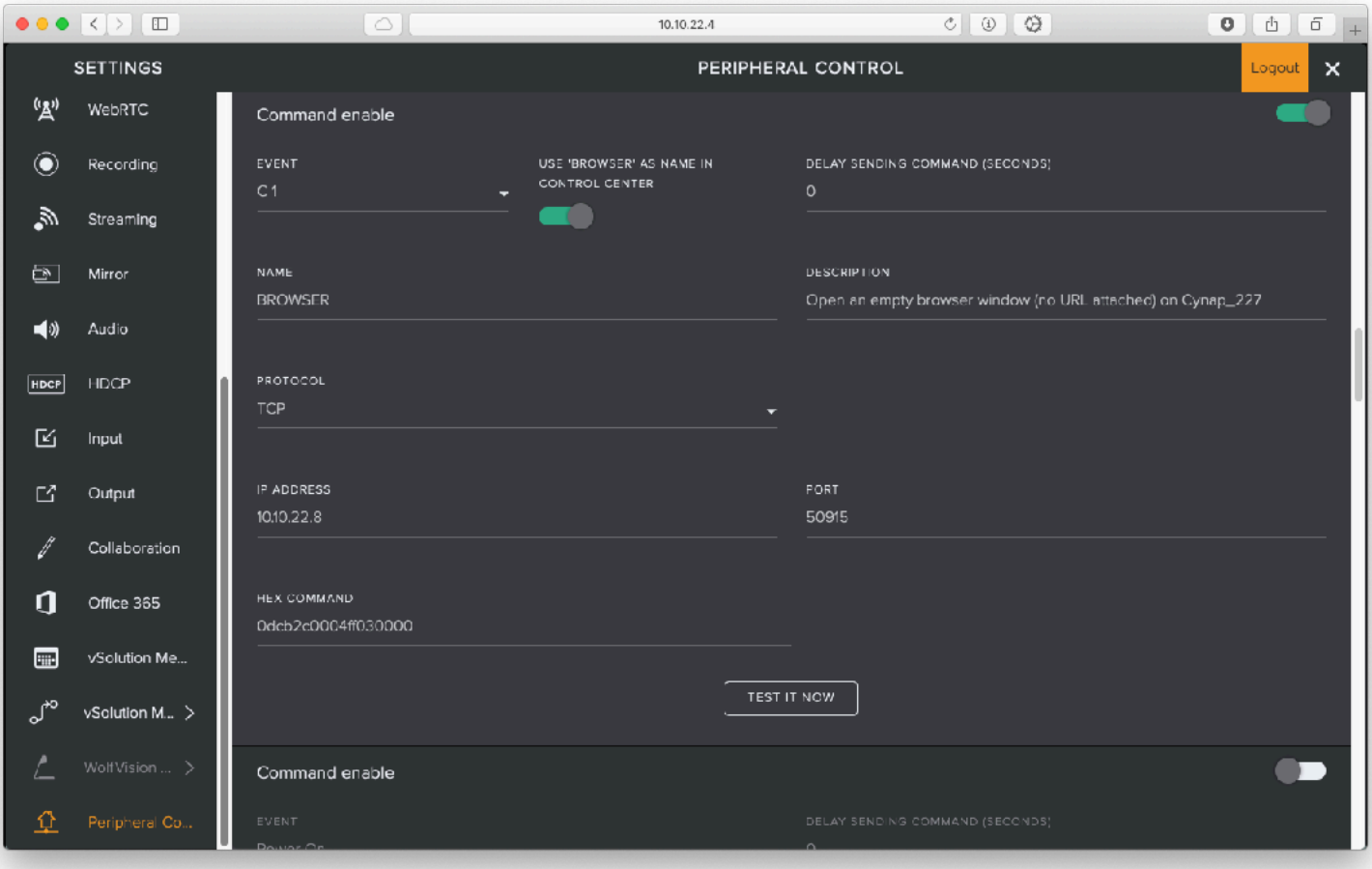
Cynap	https://wolfvision.com/wolf/commands_cynap_wolfvision/protocol/commands_cynap.html
Cynap Core	https://wolfvision.com/wolf/commands_cynap_wolfvision/protocol/commands_cynap_core.html
Changes in APIs	https://wolfvision.com/wolf/commands_cynap_wolfvision/protocol/changes_cynap.htm

23.4 Playground: Peripheral Control

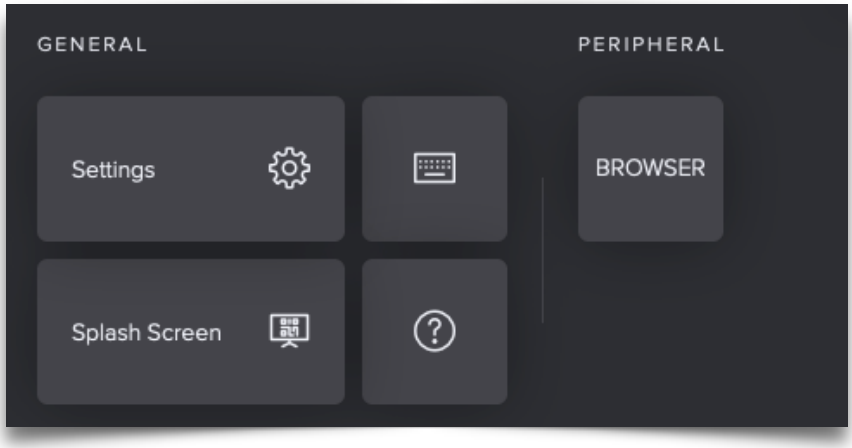
Commands can be entered (for testing or production purposes) in the Peripheral Control Settings of Cynap (available on every Cynap system). It allows for startup control or to add customised functions on buttons visible on the Cynap UI.

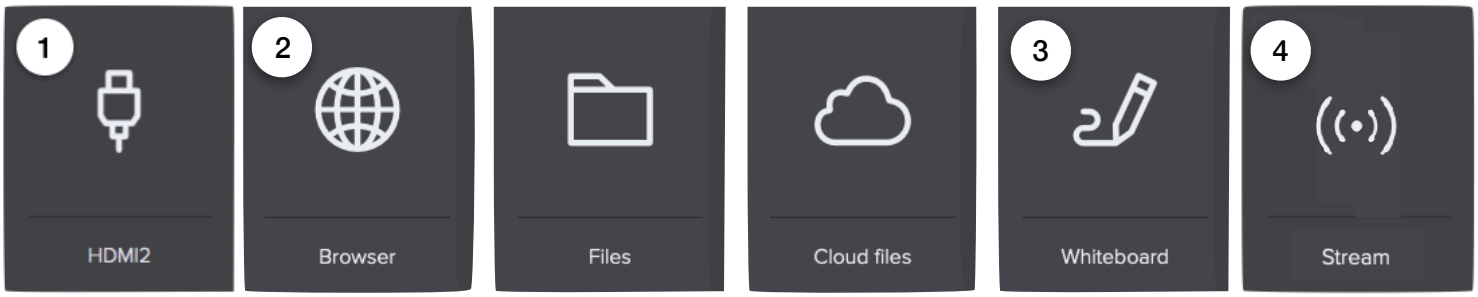
To rule out connection issues you might want to try sending a Cynap API command to 127.0.0.1 (localhost) to try out if a hex command really works.

Cynap Peripheral Command settings



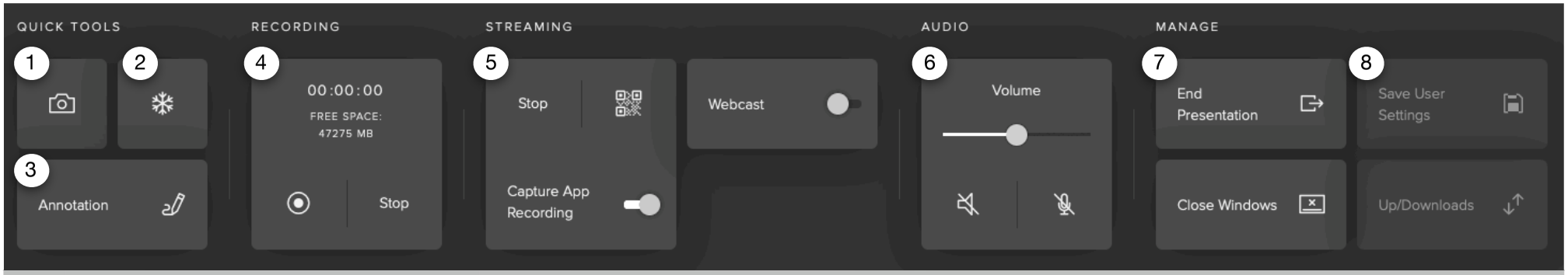
Custom button visible on Cynap UI (Control center)





ID	Function	Hex Command
1	Open HDMI1 input Open HDMI2 input	0D CB 2C 00 04 FF 02 00 01 0D CB 2C 00 04 FF 02 01 01
2	Open browser window (Increase size when adding URL)	0D CB 2C 00 04 FF 03 00 00
3	Open Whiteboard	0D CB 2C 00 04 FF 0D 00 00
4	Open first input stream	0D CB 2C 00 05 FF 11 00 01 00
	Close window 1 (red) Close window 2 (green) Close window 3 (yellow) Close window 4 (blue)	09 CB 28 02 00 00 09 CB 28 02 01 00 09 CB 28 02 02 00 09 CB 28 02 03 00

Please note: **Annotation** and **Matrix UI** have been implemented into our web app and therefore cannot simply be opened and controlled with a single command . They require a complete implementation into your UI environment.

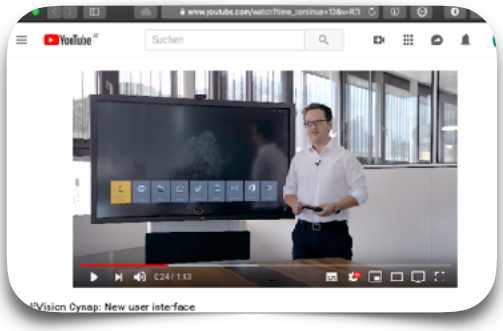


ID	Function	Hex command
1	Create a snapshot	09 CB 32 01 00
2	Freeze Unfreeze Toogle freeze	09 CB 5A 01 01 09 CB 5A 01 00 09 CB 5A 01 02
3	Start annotation	See section annotation/whiteboard
4	Start recording Pause recording Stop recording Start recoding [custom name]	09 CB 25 01 00 09 CB 25 01 01 09 CB 25 01 02 09 CB 25 [total following bytes] 00 [total bytes file name, not exceeding 64] [filename (URL encoded)]
5	Start streaming Stop streaming Show streaming URL/QR Code Hide URL/QR Code Disable recording on stream receivers Enable recording on stream receivers	09 CB 20 01 01 09 CB 20 01 00 09 CB 88 01 01 09 CB 88 01 00 09 CC 25 01 00 09 CC 25 01 01
6	Set volume Audio mute on Audio mute off Audio mute toggle Mic mute on Mic mute off Mic mute toggle	09 CB 56 01 0x64 (0 percent to 100 percent / 0x00 to 0x64) 09 CB 58 01 01 09 CB 58 01 00 09 CB 58 01 02 09 CB 59 01 01 09 CB 59 01 00 09 CB 59 01 02
7	End presentation - Standby New presentation End presentation - Screensaver	09 CB 49 03 00 00 01 09 CB 49 03 00 00 00 09 CB 49 03 00 00 03
8	Save user settings	09 CB 48 00

Latest information on CynapOS updates

Firmware download page
The page where you are able to manually download the latest version also contains the list of changes.
Link: https://wolfvision.com/vsolution/index.php/en/?id=325

Also listed are the former changes of previous firmware versions



How to videos on YouTube channel
Cynap functions demonstrated and explained on YouTube.

Link: https://www.youtube.com/user/WolfVisionVisualizer/f

Certification and Re-Certification

Training and Re-Certification platform
As a WolfVision Cynap partner you get access to our training and certification platform.

Link: https://partner.wolfvision.com

Covers all Cynap products on CynapOS

WOLFVISION

Cynap API Developer's Guide