WOLFVISION
Driving Knowledge Creation

Network Integration Guide: CYNAP PRO

WolfVision GmbH
Oberes Ried 14
A-6833 Klaus / AUSTRIA
Tel. +43-5523-52250
Fax +43-5523-52249
E-Mail: wolfvision@wolfvision.com
www.wolfvision.com

vSolution Cynap Pro
Network Integration

Basics 4
Guide 4
LAN / Ethernet settings 4
LAN / WLAN port 5
LAN / Ethernet settings 5
WLAN settings – access point 6
WLAN settings – infrastructure (Cynap Pro acts as client) 7
Date and time 8
Host name 8
FTP Client settings 9
Proxy settings 9
Security 10
Network integration examples 12
Cynap Pro LAN only mode 12
Cynap Pro wireless network access point mode 13
Cynap Pro network infrastructure mode 14
Cynap Pro connection to a Visualizer 15
BYOM 17
Differences in Open Mode / Protected Mode 18
BYOD / BYOM 19
AirPlay 19
Miracast 23
Chromecast 27
vSolution App 31
vSolution Cast (Windows) 32
Document and media player 34
Streaming RTP / RTSP 34
Unicast Streaming 36
Multicast Streaming 37
Streaming with enable Webcasting Feature Pack 38
YouTube Live 38
Custom (e.g. to share content to Facebook) 38
Network Stream (input) 39

Control of Peripheral Devices 41
Recording 42
Recording with enabled Capture Feature Pack (optional) 43
Capture Feature Pack: Panopto 43
Capture Feature Pack: Opencast 45
vSolution Matrix Feature Pack (optional) 47
Cloud services 49
Network Drive 49
User interface 49
Hardware and OS 50
Administration 50
Client System Requirements 51
Firewall rules (full list) 53
Changelog 58

Basics

Before starting, check the existing infrastructure and define the required equipment and settings.
Various examples in this document show the different ways in which Cynap Pro can be integrated into the network.
When connecting Cynap Pro to LAN and WLAN at the same time, please use different IP ranges in order to prevent address conflicts.
The listed IP addresses are only examples.
Cynap Pro can be treated as a standard network device and it is as secure as the supporting network. Cynap Pro cannot be considered as a router, switch or firewall. Communication to other networks and access must to be controlled using your existing equipment (firewall, router, switch and so on).
By default, Cynap Pro´s second LAN port (LAN 2) is dedicated to fully integrate a WolfVision Visualizer. The behaviour of this LAN port (LAN 2) can be changed to connect Cynap Pro to da dedicated RMS network (Room Management System) and mirroring purposes. This way, the built-in DHCP server is de-activated and a Visualizer cannot be fully integrated.

Attention:
When the second LAN port (LAN 2) is set to Visualizer Mode, never connect this LAN port for the Visualizer to your existing network infrastructure!
If this port is set to Visualizer mode, Cynap Pro acts as DHCP-server on this port and this could cause conflicts with the existing infrastructure.
When using vSolution Matrix, LAN 1 has to be used to connect all stations together.

Guide

This guide will assist you in setting up the network correctly. Please note that to connect a Cynap Pro to an existing company network, some information from the local administrator is required.

LAN / Ethernet settings

To achieve optimum network performance, all network devices such as switches, wireless controllers (WLC), access points (AP), etc. have to be powerful and suitable for your customised Cynap setup requirements.
Energy Efficient Ethernet (EEE) or ‘Green ethernet’ (IEEE 802.3az) should be disabled for full performance.

On-premise managed devices benefit from lower lag for real-time applications. WLAN repeaters may have a negative impact on network speed and bandwidth.
Please always consult the documentation of the network devices used in your infrastructure.

All network interface controllers (NICs) in Cynap systems are strictly separated to ensure maximum security. The Cynap Core Pro and Cynap Pro offer two LAN ports and two wireless modules (one dedicated to Miracast).

The Cynap Pure series offers one LAN port and one wireless module. The (by default) strictly separated NICs can optionally be routed to allow for HTTP (port 80) and HTTPS (port 443) traffic, including DNS (port 53).

LAN / WLAN port

The LAN port enables integration of Cynap Pro into an internal network. Administrators of a large number of Cynap Pro systems can use the LAN port to control, support and update all of their units from their local desktop PC.

The list of applications for the Cynap Pro LAN port is constantly increasing. It can be used for controlling, capturing still images, viewing live video streams, firmware updates, adjustments, menu settings and for maintenance purposes. Some features are only supported when using vSolution Link software.

The following protocols are supported: TCP/IP, IGMP, RTP, RTSP, UDP and ARP.
Supported (tested) internet browsers are: Microsoft Edge, Firefox, Chrome, and Safari.
By default, DHCP is activated to receive all network settings automatically from the server.

Please note that only WIFI-5 is supported for wireless connectivity.

Hint - WLAN:
To ensure optimal performance of supplied remote control, prevent channel 13 in the band of 2.4 GHz. Switch Cynap Pro to standby closes all connections.

LAN / Ethernet settings

Priority Interface Access	The higher prioritized interface (value = 1) will be used for network service first. Ensure that the value is different from the WLAN interface priority.
DHCP	Cynap Pro will get all network settings automatically from the DHCP server in the existing network. Switch it to OFF to set the static addresses manually.
IP address	Unique address in the network, i.e. 192.168.0.100. The IP address of Cynap Pro can for example be set to 192.168.0.1.
Subnet mask	Available IP addresses can be limited. A commonly used subnet mask would be 255.255.255.0
Gateway	Defines the IP address of the server / connection to other networks (such as the internet). When Cynap Pro is directly connected only to a PC, then enter the IP address of the PC.
Name server 1 / 2	Input the IP address of the preferred Domain Name System (DNS). This Server translates domain names into corresponding IP addresses.
Identity	Login credentials to connect Cynap Pro in a protected network. (802.1x).
Anonymous Identity	The identity to be used on an unencrypted session before Identity is being validated on an encrypted session.
Authentication Method	Supported are PEAP with MSCHAPv2 and TTLS-PAP
Root Certificate	Only root certificates are supported, load the certificate by using the Web Interface through the WLAN interface. Allowed certificates: • root certificate (CA) with common file extension .crt Base-64-coded X.509 encoded DER certificate • Privacy Enhanced Mail with common file extension .perm Base-64-coded X.509 encoded DER certificate

	certificate stored between 2 tags: “---Begin Certificate---“and” ---- ---End Certificate-----“

WLAN settings – access point

Mode OFF	Disable access point.
Mode Access Point	Enable access point.
Channel	Defines the channel used for wireless communication. For optimum performance, select a currently unused channel.
SSID Auto	If activated, an automatic SSID is generated using the Cynap Pro serial number (e.g. “Cynap Pro-01074809”)
SSID Manual	Defines the network name in plain text for easy identification of the WLAN network. Following characters are supported: - AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuV vWwXxYyZz - 0123456789 - _-:$& ()
IP address	Defines the IP address of the access point. Cynap Pro acts as a DHCP server and provides the necessary network settings to the connected devices.
Subnet mask	Available IP addresses can be limited. A commonly used subnet mask would be 255.255.255.0
Encryption	Defines encryption for safe network traffic. All connected devices must use the same algorithm (WPA2).
Transmit Power	Select the desired transmission power to optimize the range. The maximum power depends on selected channel and region.

Hint:
Cynap Pro does not act as router or gateway and only serves up a “Cynap Pro closed” network that will not connect to the internet even if the LAN port is connected to the internet.

WLAN settings – infrastructure (Cynap Pro acts as client)

Use the access point list to check the currently available access point and its signal strength.

Mode OFF	Disable Infrastructure
Mode Infrastructure	Enable Infrastructure, Cynap Pro can be connected as client to an existing access point.
Band	By default, Cynap Pro uses the 2.4GHz and 5 GHz frequency band. The used frequency band can be limited to either 2.4GHz or 5 GHz. This setting is available in SSID mode only.
Priority Interface Access	The higher prioritized interface (value = 1) will be used for network service first. Ensure that the value is different from the LAN interface priority.
BSSID On / Off	Toggles between SSID and BSSID mode. With BSSID (Basic Service Set Identification), the used access point will be fixed and Cynap Pro will connect to the defined access point only. Access point hopping, which is available in SSID mode (Service Set Identification), will be prevented.
SSID	Defines the network name in plain text for easy identification of the WLAN network. Check existing WLAN infrastructure to get SSID. Following characters are supported: - AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz - ÄäÖöÜü - 0123456789 - _-:$& ()
BSSID	Defines the network name in plain text for easy identification of the WLAN network. Check existing WLAN infrastructure to get SSID. This setting is available in SSID mode only.
Subnet mask	Available IP addresses can be limited. A commonly used subnet mask would be 255.255.255.0
Gateway IP	Defines the IP address of the server / connection to other networks (such as the internet). When Cynap Pro is directly connected only to a PC, then enter the IP address of the PC.
Name server 1 / 2	Input the IP address of the preferred Domain Name System (DNS). This Server translates domain names into corresponding IP addresses.
Encryption	Defines encryption for safe network traffic. All connected units must use the same algorithm (None, WEP, WPA2, WPA2 Enterprise).
Identity	Login credentials to connect Cynap Pro in a WPA Enterprise protected network.
Anonymous Identity	The identity to be used on an unencrypted session before Identity is being validated on an encrypted session.
Authentication Method	Supported are PEAP with MSCHAPv2 and TTLS-PAP
Root Certificate	Only root certificates are supported, load the certificate by using the Web Interface through the LAN interface. Allowed certificates: • root certificate (CA) with common file extension .crt Base-64-coded X.509 encoded DER certificate • Privacy Enhanced Mail with common file

	extension .perm Base-64-coded X.509 encoded DER certificate certificate stored between 2 tags: “---Begin Certificate---“and” --- ---End Certificate-----“
Signal Level Limit (dBm)	Defines when Cynap Pro start to search for another access point with the same SSID in your infrastructure (WLAN roaming). Monitoring the current signal level to prevent too low values. Lookups could interrupt the network connection shortly and every lookup will be counted (Reconnect Counter (Low Signal Level).
Signal Level	Shows the current strength of the WLAN signal in dBm.
Reconnect Counter (Connection Loss)	Counts every connection loss, e.g. when the selected access point would be powered down.
Reconnect Counter (Low Signal Level)	Counts every lookup then the measured signal falls below the user defined signal level limit.

Date and time

Time source	Cynap Pro has a built-in battery-buffered RTC clock (Real Time Clock). Settings will only be lost if the battery is empty. To eliminate the risk of incorrect time stamps, Cynap Pro can be synchronized to an external time server. Select external and input a valid URL or IP address of a NTP time server.

Host name

Host name	The Host name can be changed in the settings under general settings. The host name can be useful for network administrators to see the device name in plain text in the list of clients. Please note, this host name is not automatically listed in the DNS list, and therefore cannot be used in a browser without DNS registration.

FTP Client settings

FTP enable	Enable or disable FTP client functionality to backup and share recorded videos and snapshots. Additional features such as active/passive mode or secure layers (eg. Kerberos etc.) are not supported.
URL	Address of your FTP server in your network, like 192.168.0.100. (up to 256 characters, no space between the characters)
Username	Input the username according your FTP server settings.
Password	Input the password according your FTP server settings.
Test it now	During the test, Cynap Pro will upload a text file onto the FTP-server (“Cynap Pro.txt” without content)

Proxy settings

To increase security level, use a proxy server to control HTTP and HTTPS traffic from Cynap Pro. Built-in access point and other local services are not controlled. To take effect the new settings, Cynap Pro will reboot automatically.

Proxy enable	Enable / disable proxy service When enable, all HTTP and HTTPS traffic will be routed to the your proxy server. Please note, using a Proxy server may block Skype for Business (optional) functionality.
URL	URL of the proxy server in your network, like 104.236.10.17 (or DNS name up to 256 characters, no space between the characters). DNS server not required, when using IP addresses.
Host Port	Port, set the used network port to connect to your proxy server.
Authentication	Disable / enable Authentication When enabled, valid user name and password has to be entered.
Username	Username, given by your server.
Password	Password, given by your server.

Security

Admin password
Defines the necessary password for administrator access. This login data is needed to change settings. Using the login data, an administrator can connect to Cynap Pro at any time. The default password is “Password”. Remember to make a note of any changed passwords!

Login Security
Accessing Cynap Pro can be protected by authentication (admin, moderator or PIN).
To prevent unauthorized access of the settings, the admin password needs to be entered once per session.

Network Security
Accessing Cynap Pro can be limited to secure connections only (https). Please note, the accessing application needs to support SSL / TLS (e.g. the most modern browsers are supporting HTML5 and SSL /TLS).
Wolfvision support access can be prohibited by disabling SSH.

LAN Security
When using wired network, use authentication (according 802.1x) to maximize security.
When using certificates, load it busy using the Web Interface.

WLAN (WiFi) Security
When using wireless network, use encryption to maximize security.
Cynap Pro complies with following standards:

- WEP
- WPA2
- WPA2 Enterprise (according 802.1x)

Hint
Miracast MS-MICE only works via a secure connection (e.g., WPA2-PSK or WPA2-Enterprise Security).
WEP allows passwords with a length of 13 characters (128 bit).
WPA2 allows passwords with a length of 8 ~ 63 characters.
Use special characters carefully, not every thirdparty device can handle them.
When using WPA2 Enterprise, load the certificate by using the Web Interface.
When using the built-in access point, the security settings will be handled automatically.
When starting a new presentation, the SSID and the password will be changed to maximize security.

Security Settings
To prevent unauthorized changes of the settings through the front display. Additionally the support of USB storage devices can be disabled.

BYOD Screen Sharing
Please refer to manufacturers on detailed protocol information about their screen sharing protocol encryption.

Miracast

Protocol	Type of encryption	Key	PIN
Wi-Fi Direct	Transport encryption	WPA2 – Windows client dependent	No PIN required
MS-MICE	Transport encryption	Based on network configuration (and mandatory WPA2 encryption)	Key or certificate required
MS-MICE	Video encryption	DTLS (ECDHE-RSA-AES256-SHA384)	PIN pairing required

AirPlay

Encryption	Key
Copyright DRM	Apple FairPlay
Transport	Based on network configuration
Media content	DTLS (ECDHE-RSA-AES256-SHA384)

Please note: AirPlay uses SSL and a multitude of ciphers throughout a connection life cycle such as Curve25519-Donna, ED25519, ChaChaPoly1305, AES, SHA-512 / SHA-256

Chromecast

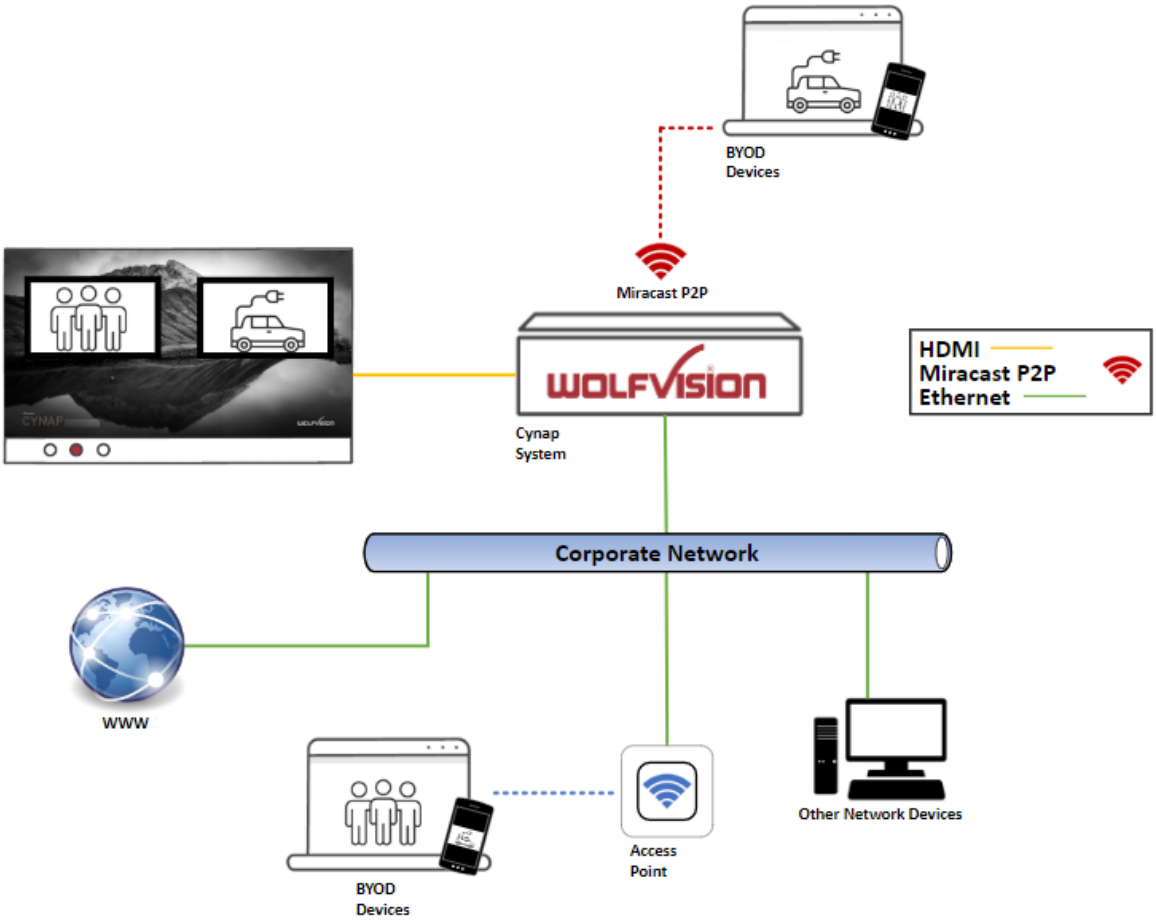
TLS encryption

Network integration examples

The following examples are showing different ways to integrate Cynap Pro into your network infrastructure, wired and wireless.
BYOD (Bring Your Own Device) allows sharing the screen content of different devices with various operating systems to Cynap Pro to share to a big display device.
BYOM (Bring Your Own Meeting) allows using audio and video of the Cynap Pro at your personal computer.

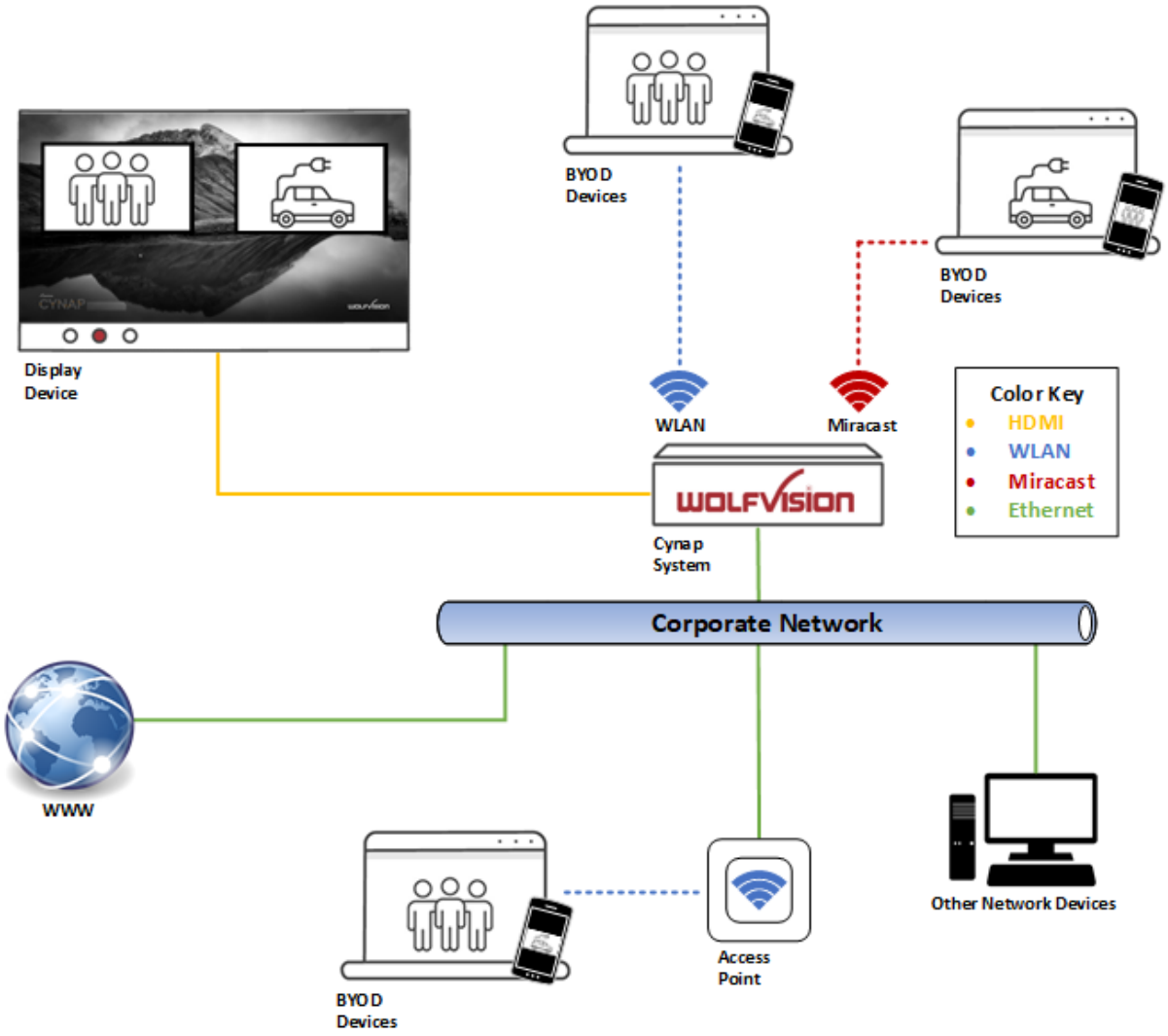
Cynap Pro LAN only mode

Cynap Pro integrated via a cable connection into an existing network. LAN settings for Cynap Pro can be obtained from an existing DHCP server. Cynap Pro remains available for Miracast P2P connections.



Cynap Pro wireless network access point mode

Cynap Pro is integrated via a cable connection into an existing network, and is operated in wireless network access point mode. LAN settings for Cynap Pro can be provided by the DHCP server. Cynap Pro generates an independent WLAN, and WLAN enabled devices (BYOD) can connect to Cynap Pro.



Advantages:

- All devices can communicate with each other
- Cynap Pro has access to the Internet and cloud services can be activated
- Cynap Pro can access the internet to check for firmware updates without using additional devices

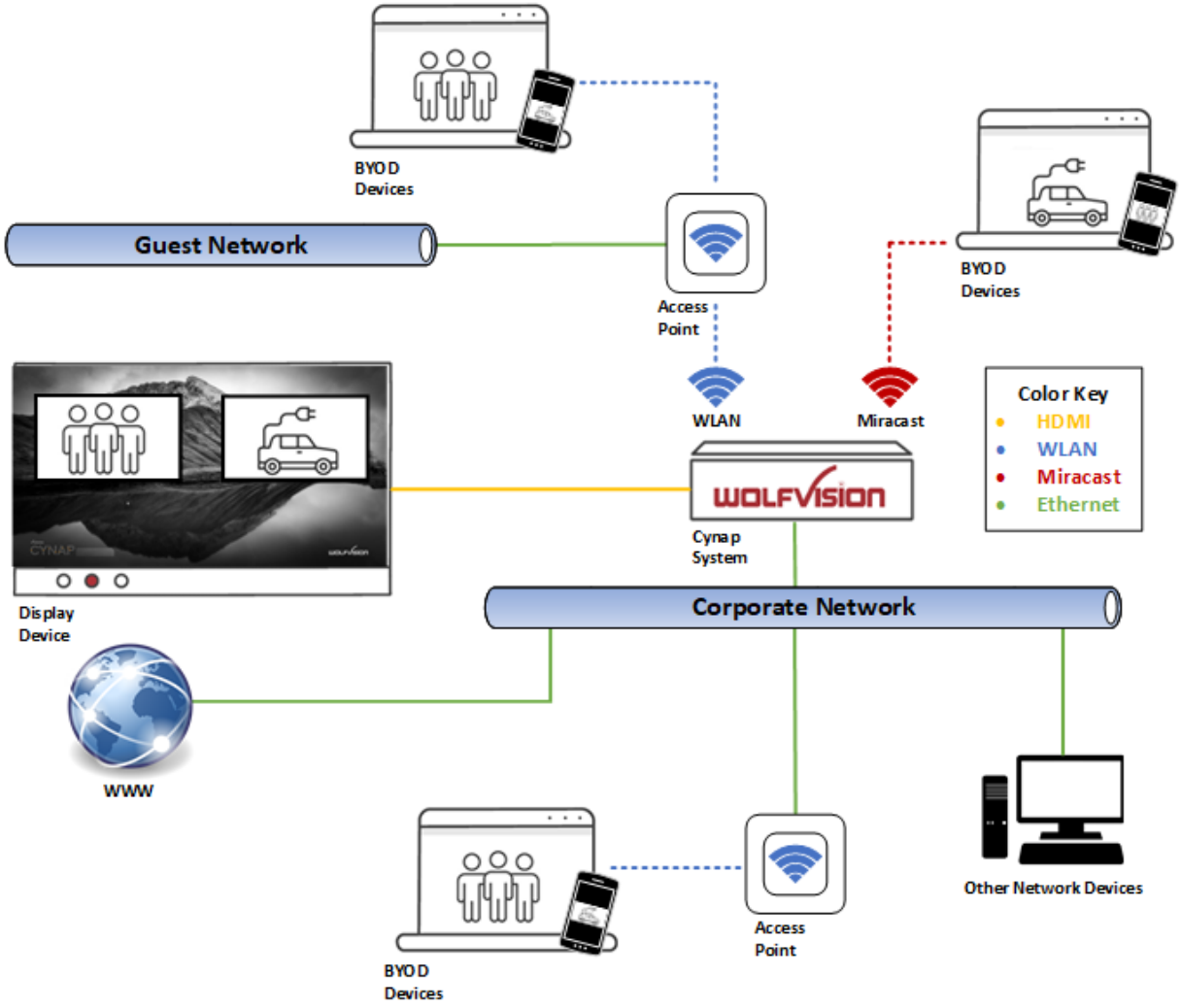
Disadvantages:

- Performance issues (all traffic is on the same network)

Hint:
If the units are in different subnets, Cynap Pro might not be able to be discovered automatically by vSolution applications.

Cynap Pro network infrastructure mode

Cynap Pro is integrated via a cable connection into an existing network (e.g. Corporate network), and is operated in network infrastructure mode. LAN settings for Cynap Pro can be provided by the DHCP server. In infrastructure mode, Cynap Pro is connected to an existing wireless access point in the existing network (e.g. Guest network). BYOD devices in the Corporate network and in the Guest network can connect to Cynap Pro.



Advantages:

- All devices can communicate with each other
- Cynap Pro has access to the internet and cloud services can be activated
- Cynap Pro can be moved within the range of the access point
- Cynap Pro can access the internet to check for firmware updates without using additional devices

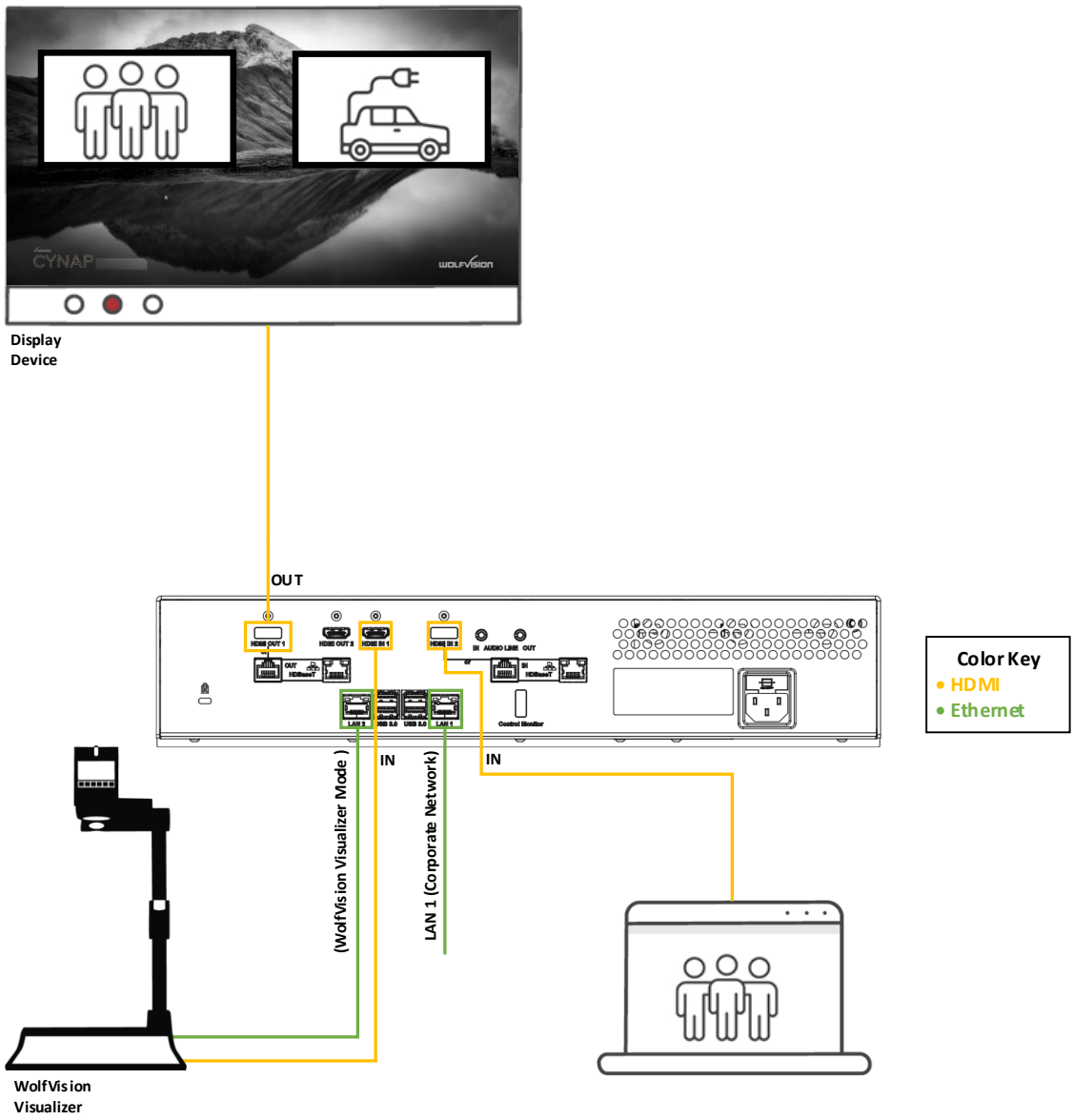
Disadvantage:

- Performance issues (all traffic is on the same network)

Hint:
If the units are in different subnets, Cynap Pro might not be able to be discovered automatically by vSolution applications.
Cynap Pro can also be installed in a VLAN.

Cynap Pro connection to a Visualizer

Cynap Pro has a dedicated LAN port for connecting to a Visualizer with built-in DHCP server functionality. Activate on the Visualizer to obtain all necessary network settings from Cynap Pro automatically. Communication between Visualizer and Cynap Pro is over the Wolfprot protocol. The connection between Cynap Pro and the Visualizer is a direct connection (point to point) and shouldn't be made through a switch or similar device.
More information on this protocol can be found on our website in the support section www.wolfvision.com.



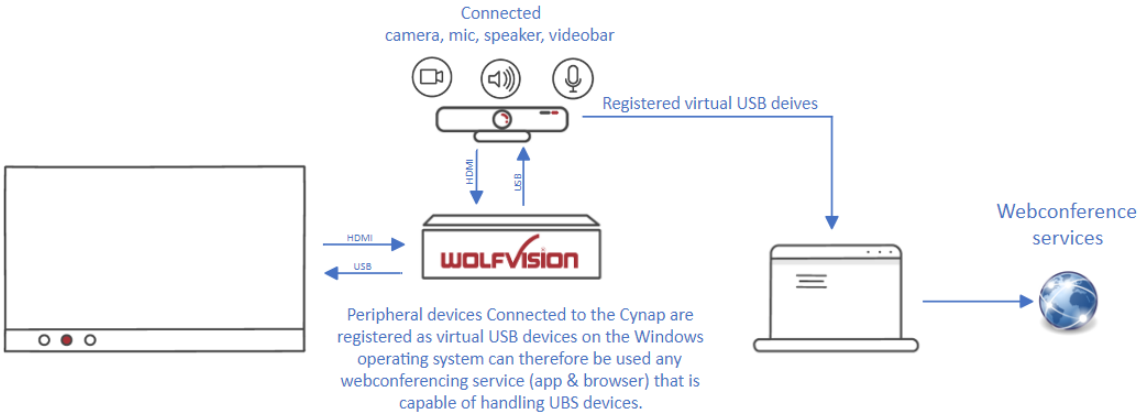
Attention:
When the second LAN port is set to Visualizer Mode, never connect this LAN port for the Visualizer to your existing network infrastructure!
If this port is set to Visualizer mode, Cynap Pro acts as DHCP-server on this port and this could cause conflicts with the existing infrastructure.

Hint:

- Connect the Visualizer straight to the dedicated port. Do not add switchers, hubs, routers or similar between Cynap Pro and the Visualizer to prevent error sources.
- Cynap Pro can be controlled with the keys of the Visualizer. The functions of keys from the camera head are dedicated to control Cynap Pro. These keys are note have no effect to the Visualizer anymore. The IR-remote control of the Visualizer is not effective in this setup.
- Visualizer can be controlled with Cynap Pro.
- Cynap Pro and Wolfvision Visualizer are supporting cable runs up to 100m according Ethernet specification.
- The behavior of this LAN port can be changed to connect Cynap Pro to a dedicated RMS network (Room Management System). This way the built-in DHCP-server is de-activated and a Visualizer cannot be fully integrated.
- Be sure USB input type is not defined as “Visualizer”

BYOM

BYOM (Bring Your Own Meeting) allows using audio and video of the Cynap Pro at your personal computer.



Differences in Open Mode / Protected Mode

When using Cynap Pro, it is possible to choose between either open mode or protected mode.
This different mode can be selected using Cynap Pro settings.

Modes:

Open Mode
The open is intended for quick and easy connections and BYOD without the need of high security and big effort for administration.
When Open Mode is active, all available devices can connect to Cynap Pro.
In the Open Mode, Airplay PIN can be used to prevent disturbance of extern Apple devices.
The PIN will be shown on the connected display only (HDMI or HDBaseT).

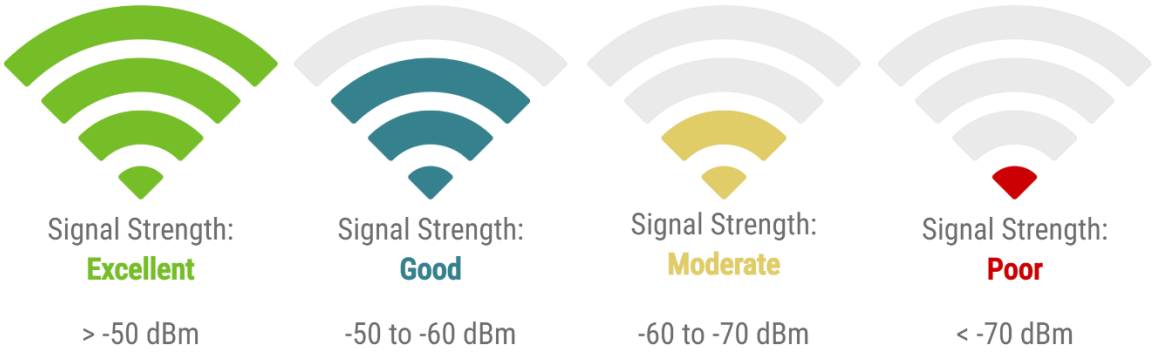
Protected Mode
Is a password protected mode to prevent misuse and disturbances

- Users with knowledge of the password can connect to Cynap Pro
- Users who knowing the security PIN, the PIN will be displayed on the selected interface(s)
- Users can connect when Cynap Pro is awaiting a mirror connection

For more information, please refer to the manual.

BYOD / BYOM

Cynap Pro is designed to make it as easy as possible for users to connect to it. Cynap Pro supports multiple mirroring protocols: AirPlay, Chromecast, Miracast, and vSolution Cast. BYOD (Bring Your Own Device) allows sharing the screen content of different devices with various operating systems to Cynap Pro to share to a big display device.
BYOM (Bring Your Own Meeting) allows using audio and video of the Cynap Pro at your personal computer.



AirPlay

It is recommended to use the latest versions of iOS, iPadOS, and macOS. AirPlay is transmitted via Ethernet / WLAN. It can be used for displaying up to four sources.

Function / Application	Port	Type	Inbound / Outbound	Description
Airplay				
Multicast DNS (mDNS)	5353	UDP	Inbound / Outbound	Multicast DNS (mDNS 224.0.0.251) Bonjour
Audio	4100 – 4164	TCP / UDP	Inbound	Audio for Airplay
Airplay	7000	TCP	Inbound	Airplay pairing
Video	7100	TCP	Inbound	Airplay video
Audio	47000	TCP	Inbound	Airplay audio
Airplay Bluetooth				
Audio	4100 – 4164	TCP / UDP	Inbound	Audio for Airplay
Airplay	5000	TCP	Inbound	AirPlay communication with legacy devices
Airplay	7000	TCP	Inbound	Airplay pairing
Video	7100	TCP	Inbound	Airplay video
Audio	47000	TCP	Inbound	Airplay audio

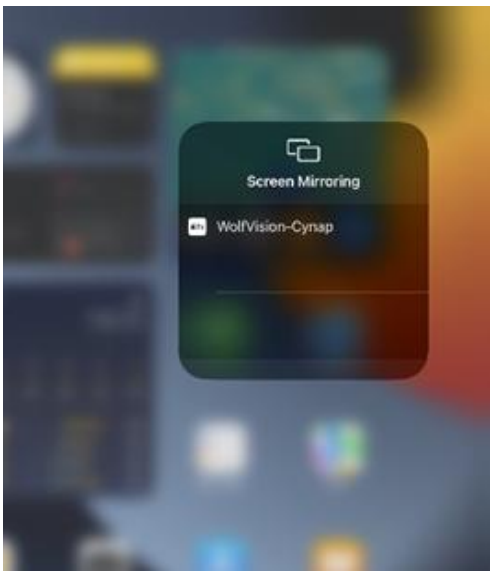
Steps to establish an AirPlay connection:
iPhone, iPad:

1. **Connect to Wi-Fi:** Make sure your Apple device and the Cynap system are connected to the same network (WLAN).

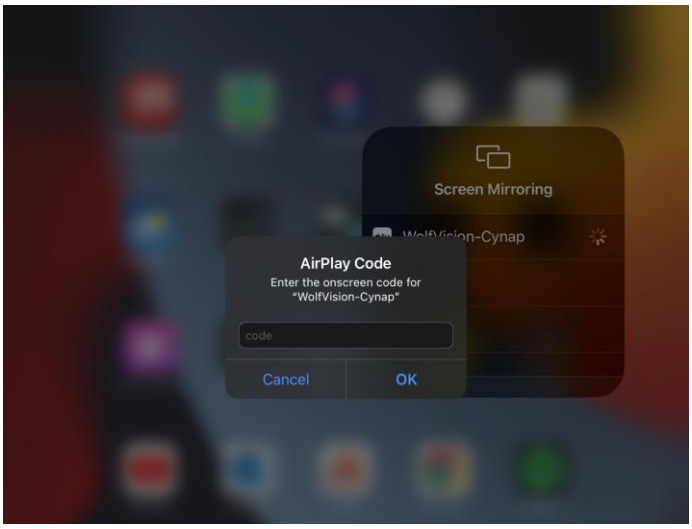
2. **Open Control Center:**

- On iPhone, iPad: Swipe down from the upper-right corner of the screen.
  Screenshot taken on iPadOS 17.5, other versions and models may vary.

3. **Tap Screen Mirroring:** Select your Cynap device and start mirroring.



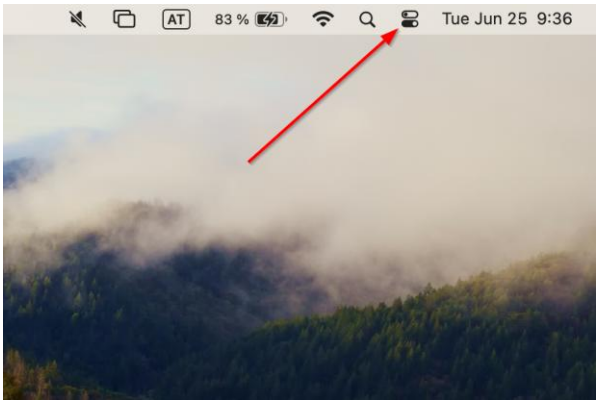
4. (Optional): Enter PIN, if configured.

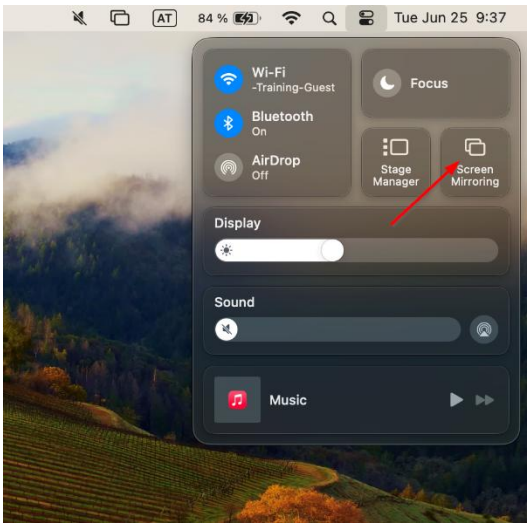


MacOS:

1. **Connect to Wi-Fi:** Ensure both your Mac and the Cynap system are on the same Wi-Fi network.

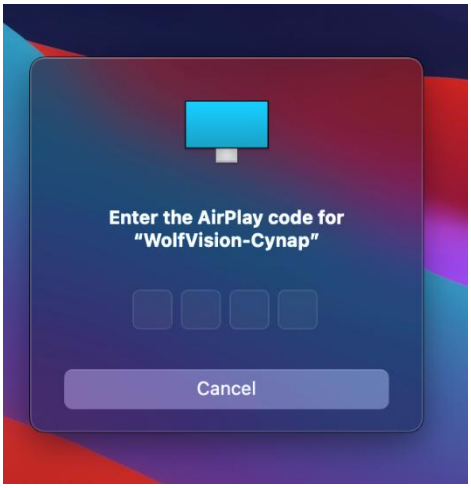
2. **Click** on the "Control Center" icon in the menu bar, click on the "Screen Mirroring" icon and select your Cynap system.
Screenshot taken on MacOS Sonoma 14.5, other versions and models may vary.





3. **Start mirroring**: Your Mac's display will now be mirrored on your Cynap system.

4**. (Optional):** If the AirPlay PIN is activated, the PIN is requested when connecting.



Miracast

Miracast is based on a Wi-Fi Direct connection, which allows devices to connect directly to each other without needing a Wi-Fi network. Miracast can only be used in close proximity to the Cynap system. Any physical barriers, such as cabinets, can reduce the transmission radius. With Miracast, the screen and audio is transmitted. Additionally, inputs can be sent back to the device using touchback functionality.

Discovery beacons will always be sent by the Cynap dedicated built-in WLAN module and requires a device with a WLAN component.

Dense WLAN traffic in your environment may reduce the transmission radius due to radio interference, increase the delay of video transmission, or result in reduced audio/video quality. MS-MICE (Miracast over Infrastructure Connection) support can help to increase the transmission radius.

Miracast P2P switches constantly between the current WLAN connection and the additional P2P connection, leading to bandwidth splitting. This could cause issues like stability, quality etc. To solve these problems, **Miracast over infrastructure (MS-MICE)** was created.

Multicast DNS (mDNS) and DNS queries are used to pair (host resolve) Miracast receivers.

The Task Manager indicates if a P2P or MS-MICE connection is being used.
(Task-Manager -> Performance -> WiFi-Adapter/s).

How it Works

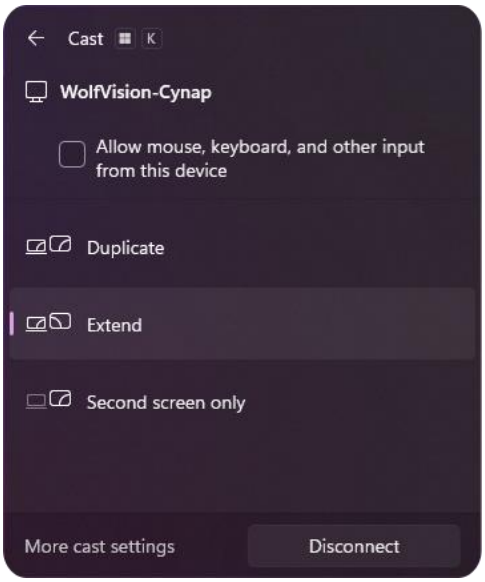
Users attempt to connect to a Miracast receiver via their Wi-Fi adapter. When the list of Miracast receivers is populated, Windows recognizes that the receiver can support a connection via the infrastructure. When the user selects a Miracast receiver, Windows attempts to resolve the device's hostname using standard DNS and Multicast DNS (mDNS). If the name cannot be resolved using either DNS method, Windows falls back to setting up the Miracast session by using the standard-based Wi-Fi direct connection.

Miracast MS-MICE				
Multicast DNS (mDNS)	5353	UDP	Inbound / Outbound	Multicast DNS (mDNS 224.0.0.251)
DHCP	67 / 68	UDP	Inbound	DHCP communication between device and receiver
RTP Stream	19000 – 19007 19010 – 19017	UDP	Inbound	RTP media traffic port for delivering audio and video
RTSP Control	7236	TCP	Outbound	RTSP control port is used to establish and manage session
MS-MICE Control	7250	TCP	Inbound / Outbound	Control port on which Cynap family system listen for Miracast packets when over existing network mode is enabled
Touchback	50000	TCP	Outbound	This port is for touchback to send mouse events back between Cynap to the Windows computer. If this port is blocked, bi-directional inputs is not possible.
Hardware cursor extension	19020 – 19027 19030 – 19037	UDP	Inbound	Hardware cursor to reduce latency when using touchback.

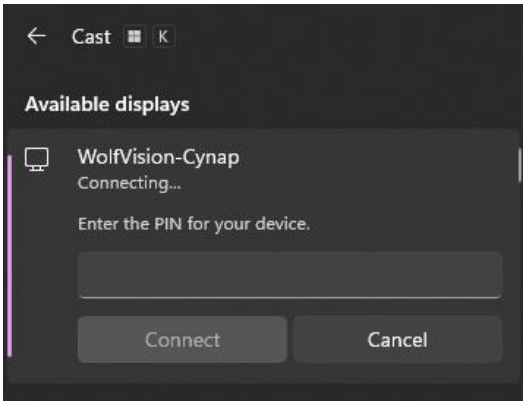
Steps to establish a Miracast connection:
Windows 11:

1. Press the Windows Key + K: To bring up a side panel.
Screenshot taken on Windows 11 Version 23H2, other versions and models may vary.

2. Select your Cynap system from the list and connect.



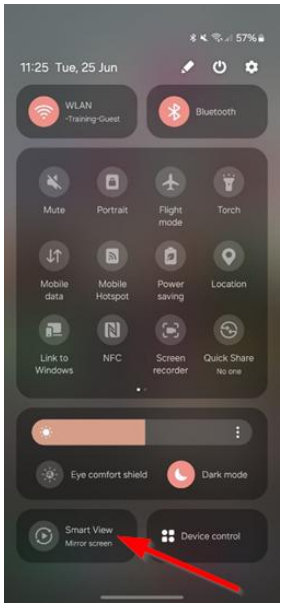
3. **(Optional):** If the Miracast PIN is activated, the PIN is requested when connecting.
Please note: Windows devices save the PIN in the cache. As soon as a "New Presentation" is executed, the Windows device that has established a connection to the Cynap must enter a new PIN.



Android (Miracast P2P)
Android devices are not supporting Miracast MS-MICE.
Miracast P2P is not supported by every Android device, consult documentation of your third-party Android device, use Chromecast, or vSolution App alternatively.

Do not connect to the same WiFi when the Android device used is supporting Miracast and you want to use Miracast P2P.

1. **Connect to Wi-Fi:** Ensure both your Android phone and your Cynap system are connected to the same Wi-Fi network.

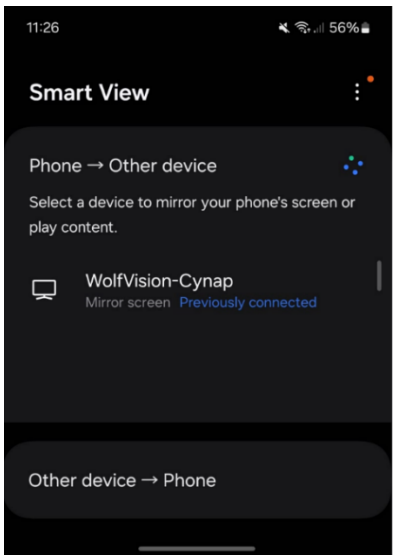


2. **Open the control center on your Android Phone:** Swipe down from the top of your screen to open the control panel.
Screenshot taken on Samsung S21 FE, Android 14, other versions and models may vary.

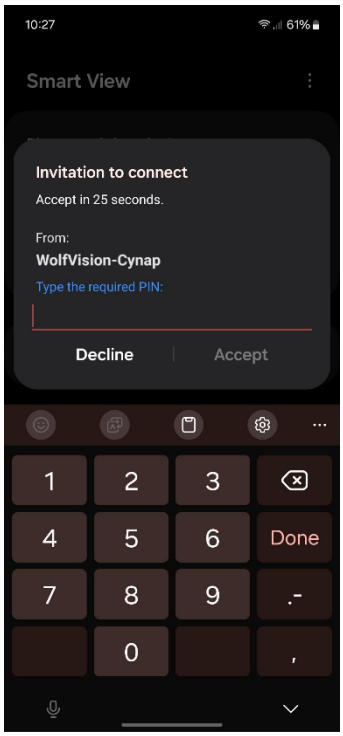
3. **Find and Tap on Cast:**

- Some phones and tablets list this feature as Screen Mirroring, Smart View, or Wireless Display.
- You might need to navigate through additional menus such as Connection preferences or More connection settings to find the mirroring feature.

4. **Choose your Cynap system and connect.**



5. **(Optional):** If the Miracast PIN is activated, the PIN is requested when connecting.



Chromecast

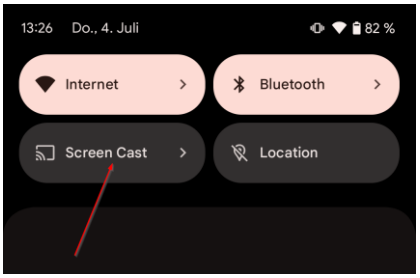
Support for Chromecast capable devices. Chromecast is transmitted via Ethernet / WLAN. It can be used for displaying up to four sources. (Chromecast requires internet access)

Chromecast				
Multicast DNS (mDNS)	5353	UDP	Inbound / Outbound	Multicast DNS (mDNS 224.0.0.251)
Discovery	1900	UDP	Inbound	Chromecast discovery
Audio	4100 – 4164	TCP / UDP	Inbound	Audio for Chromecast
Chromecast	8008	TCP	Inbound	Primary Chromecast communication
Chromecast	8009	TCP	Inbound	Communication Chromecast
Video data stream	1 – 65535	UDP	Inbound /Outbound	Chromecast (video data stream)

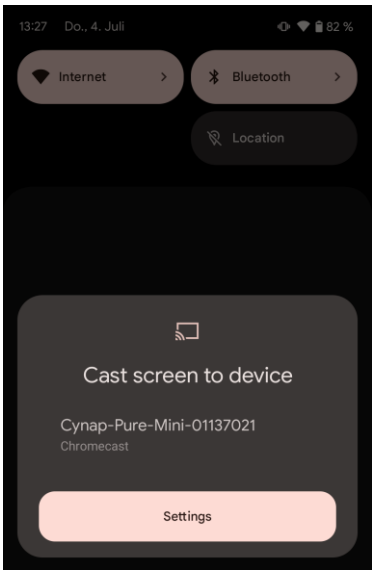
Steps to establish a Chromecast connection:
Google Pixel:

1. **Connect to Wi-Fi:** Make sure your Chromecast device and the Cynap system are connected to the same Wi-Fi network and have an Internet connection.

2. **Open Control Center:** Swipe down from the top of the screen.
Screenshot taken on Google Pixel 6a, Android 15, other versions and models may vary.



3. Tap Screen Cast: Select your Cynap system and start mirroring. Choose between mirroring a single app or the entire screen.

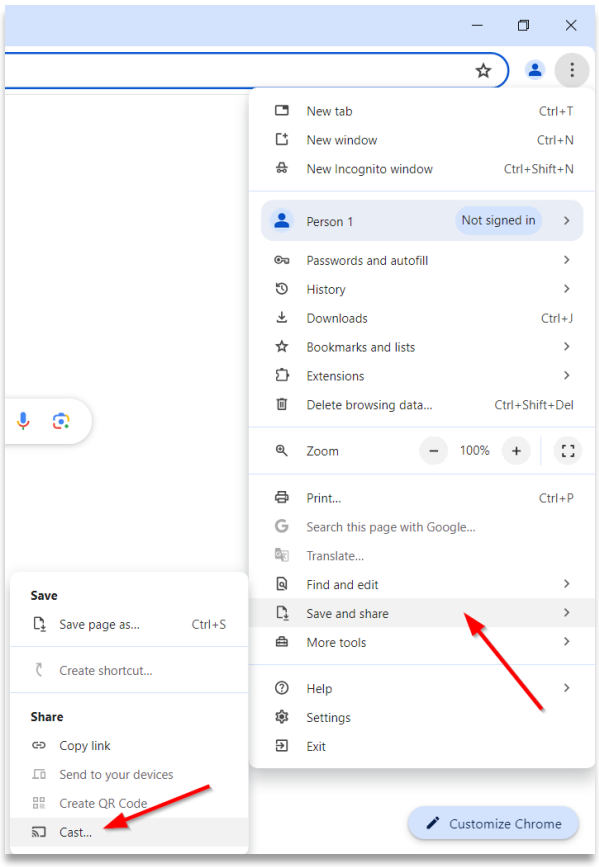


Google Chrome:

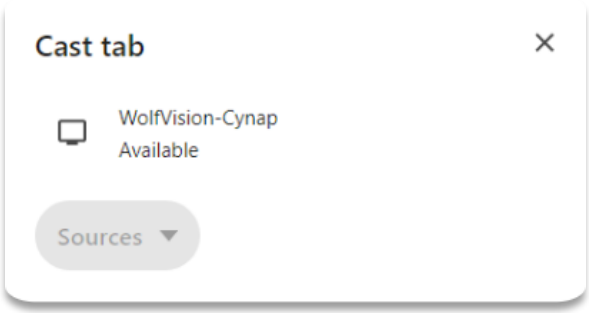
1. **Connect to Wi-Fi:** Make sure your Notebook device and the Cynap system are connected to the same Wi-Fi network and have an Internet connection.

2. **Access the Cast Feature:**

- From the Menu: Click on the three-dot menu in the upper-right corner of Chrome, then select "Save and share" then press “Cast…”
- Screenshot taken on Chrome Version 126.0.6478.127, other versions and models may vary.



3. **Select your Cynap system:** In the Cast menu, select the Cynap system you want to cast to.

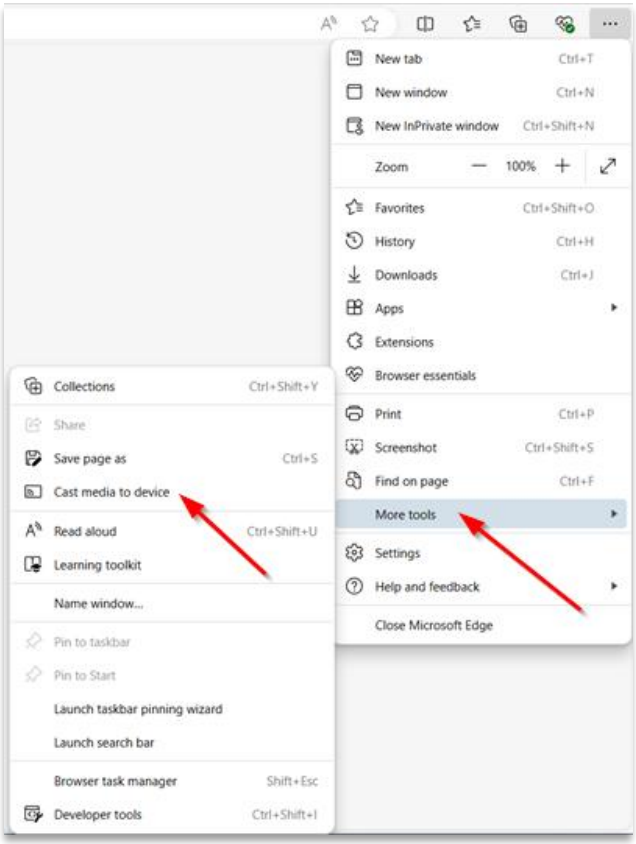


Microsoft Edge:

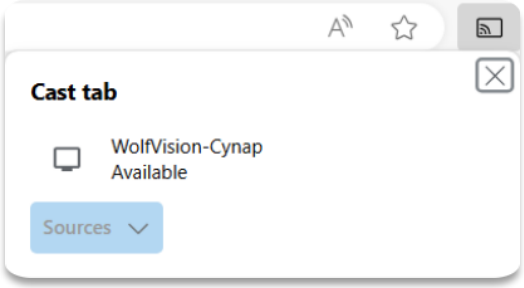
1. **Connect to Wi-Fi:** Make sure your Notebook device and the Cynap system are connected to the same Wi-Fi network and have an Internet connection.

2. **Access the Cast Feature:**

- From the Menu: Click on the three-dot menu in the upper-right corner of Edge, then select "More tools" then press “Cast media to device”.
- Screenshot taken on Edge Version 126.0.2592.87, other versions and models may vary.



3. **Select your Cynap system:** In the Cast menu, select the Cynap system you want to cast to.



vSolution App

The vSolution App allows controlling your Cynap Pro. Using our vSolution App for Android, iOS, macOS, or Windows, with a Cynap system, enables students or work colleagues to receive shared content and to control the unit. The vSolution App supports all functions of the vSolution Cast. On Android, iOS and macOS, you can register your Cynap Pro manually when discovering services are blocked in your network (Bonjour, mDNS).

vSolution App iOS / Android / Windows				
Discovery Multicast	50000	UDP	Inbound	This port is used for device discovery all available Cynap system and Visualizer in the network by vSolution applications (uses Multicast IP address 239.255.255.250). If this port is blocked, vSolution applications may not be able to find devices automatically.
http, Cynap control	80	TCP	Inbound	This port is used to connect to the Cynap system web interface (httpd). If this port is blocked, no connection can be made.
https, SSL, e.g. Cloud Service, Cynap control	443	TCP	Inbound	This port is used to cloud services and for secure connect to the Cynap system web for secure connect to the Cynap system web interface. If this port is blocked, no connection can be made.
Device Discovery	50913	UDP	Inbound	This port is used for device discovery.
For control purposes	50915	TCP	Inbound	This port is used for control purposes e.g. room control system, and others). If this port is blocked, no control is possible
TLS Control	50917	TCP	Inbound	This port is for secure communication between WolfVision applications (e.g. vSolution App) to Cynap system and / or Visualizer. If this port is blocked, secure communication to Cynap system and / or Visualizer, inclusive firmware updates are blocked
Video streams	50921	TCP	Inbound	Video streams between WolfVision App to Cynap and Visualizer. If this port is blocked, no streams are possible.
Touchback (Windows, macOS)	50922	TCP	Outbound	This port is for touchback between Cynap and WolfVision App vSolution Cast to send mouse events back to the

				Windows computer or MacBook. If this port is blocked, bi-directional inputs are not possible.
Video data stream	32768 - 61000	UDP	Inbound /Outbound	Video data stream (e.g., BYOM, Chromecast)

vSolution Cast (Windows)

In applications where a Miracast connection is not possible due to the installation, multiple Windows devices can be connected at the same time using the alternative vSolution Cast.

AirPlay, Chromecast, Miracast and vSolution Cast are based on device discovery technologies for maximum ease of use. Therefore, it is necessary that the appropriate services (see Firewall rules) are available. Alternatively, when using vSolution Cast, a Cynap Pro IP address can be entered manually. On Windows systems, vSolution Cast can either be run temporarily by users, or permanently installed (copied). The application can also be used from a USB stick without needing administrator permission, however with the restriction that no sound is transmitted.
Switching Cynap Pro to standby closes all connections.

vSolution Cast				
Discovery Multicast	50000	UDP	Inbound	This port is used for device discovery all available Cynap system and Visualizer in the network by vSolution applications (uses Multicast IP address 239.255.255.250). If this port is blocked, vSolution applications may not be able to find devices automatically.
Device Discovery	50913	UDP	Inbound	This port is used for device discovery
For control purposes	50915	TCP	Inbound	This port is used for control purposes e.g. room control system, and others). If this port is blocked, no control is possible
TLS Control	50917	TCP	Inbound	This port is for secure communication between WolfVision applications (e.g. vSolution App) to Cynap system and / or Visualizer. If this port is blocked, secure communication to Cynap system and / or Visualizer, inclusive firmware updates are blocked.
Video streams	50921	TCP	Inbound	Video streams between Wolfvision App to Cynap system and Visualizer. If this port is blocked, no stream are possible.
Touchback	50922	TCP	Outbound	This port is for touchback

				between Cynap system and Wolfvision App vSolution Cast to send mouse events back to the Windows computer. If this port is blocked, bi-directional inputs is not possible

Document and media player

Cynap Pro can present almost all commonly used document and video file formats. This functionality is built into Cynap Pro and no additional applications need to be installed.

Cynap Pro also supports different storage media for presentation of documents and video.

The following storage media are available for Cynap Pro.

- Internal storage
- USB flash drive
- Network Drive
- Cloud services
- Online Office documents with optional Office 365 Feature Pack

The following media formats are supported:

- Supported pictures file formats: GIF, JPEG, BMP, PNG
- Supported video file formats: AVI, WMV, MOV, MP4, DivX, MKV, M4V, OGV
- Supported document file formats: PDF, Word, PowerPoint, Excel
- Supported audio file formats: MP3, MKA, OGA, OGG, WMA

Streaming RTP / RTSP

Cynap Pro has a built-in streaming server which is capable of broadcasting audio and video content over the network for RTP or RTSP Streaming.
Prepare Ethernet connection (wired or wireless) and select the setting on Cynap Pro. In the settings, you can assign the IP address of the destination (for RTP multicast select: 225.0.0.0 to 238.255.255.255, with all other addresses the RTP Unicast stream can be received at the entered destination only, 224.x.x.x and 239.x.x.x are reserved), port, resolution, frame rate and format of the stream (up to RTP H.264). Select the settings for resolution, frame rate and format. Cynap Pro broadcasts the currently shown content of video and audio files to the network. For RTP, all necessary settings will be provided to the player / browser in a file.
RTSP Streaming is a Unicast stream, an end-to-end connection between server and clients and all settings be handled automatically.
The respective link will be shown below the QR-code by using “Link To Stream” in the toolbox.

- RTP stream: e.g.: http://192.168.0.100/stream/stream.sdp (exchange the example address with the IP address of your Cynap Pro).
- RTSP stream: e.g.: rtsp://192.168.0.100/stream (exchange the example address with the IP address of your Cynap Pro).

Streaming settings

Enable / Disable Streaming	When disabled, the Streaming button will be not displayed in the toolbox and will be not available with Media Cast key).
Resolution	Resolution of the network stream, up to 1080p (note resulting network traffic)
Frame Rate	Frame rate, ,higher frame rate results in more network traffic (LOW=10, MEDIUM=20, HIGH=30).
Bandwidth Mode	With setting constant, the used bandwidth will never exceed the set limit. With setting variable, the used average bandwidth will not exceed set limit (for a short period of time, the used bandwidth could be higher than the limit).

Bandwidth	Limits the maximum used bandwidth for streaming (constant or average). Certain services or the used network infrastructure may be not able to handle streams of e.g. 40 Mbit, check the contract agreements of the used service and / or your network infrastructure to limit the bandwidth accordingly.
Dynamic QR-Code	Enable / Disable Dynamic QR-Code to allow random URLs to receive the stream (QR-Code and URL changes with every new presentation).
RTP Stream enable	Enable / Disable RTP Stream (RTSP cannot be simultaneously)
Time to Live	To specify how many hops (routers) the packet can elapse before the data will be discarded. This setting is available for RTP only.
IP Address	IP address for UDP stream, 225.x.x.x to 238.255.255.255 are valid multicast addresses. To use unicast, enter the destination IP address (IP address of the receiving device). This setting is available for RTP only.
Port	Where the stream will be sent over the network (range 8800 – 9002, even numbers allowed only). The used audio port will be displayed for information, it cannot be changed separately (it is always 2 ports higher). This setting is available for RTP only.
RTSP Stream enable	Enable / Disable RTSP Streaming (RTP cannot be used simultaneously). Cynap Pro is sending several UDP streams (Unicast streams) according the number of connected clients. This way, also several clients connected to built-in access point and at the same time over the LAN interface, can receive the stream. All settings will be handled automatically between Cynap Pro and the client. The used protocol can be UDP and / or TCP.
Display QR-Code Interface	Select the desired interface and the respective link will be shown, wired (LAN) or wireless (WLAN). Use “Link To Stream” form the Toolbox to show the link to your partners. The stream itself will be sent to both interfaces. This setting is available for RTSP only and can be set in the general settings.

How to get the Stream
Open the Toolbox, select Start Streaming and use the button “Link to Stream” to show the QR code to easily access the stream e.g. when using vSolution Capture.

When using RTSP, the stream will be sent to both interfaces, but the QR code will show just the selected interface (LAN or WLAN).

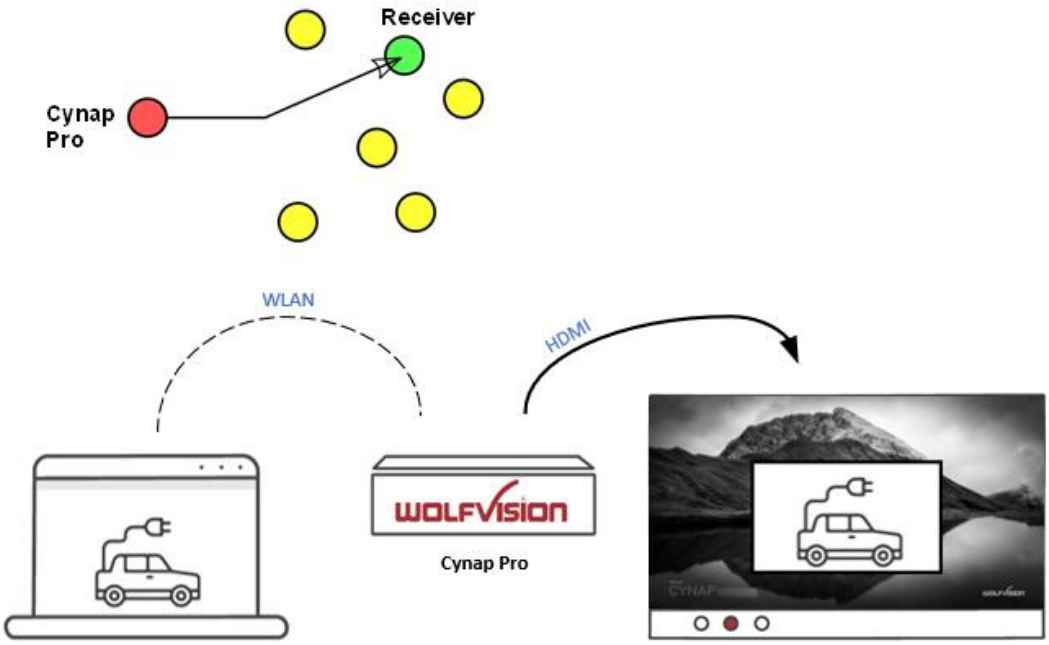
Please note:
If RTSP streaming is enabled, the maximum 50 connections to Cynap Pro are possible to receive the stream.

Please note:
When the vSolution Matrix Master Mode is enabled, the streaming settings are handled automatically and cannot be changed manually (a respective note will inform you).

Unicast Streaming

Cynap Pro`s sending stream to a single receiver. That`s a one to one connection. The IP address the unique listening receiver can be adjusted in the streaming settings.

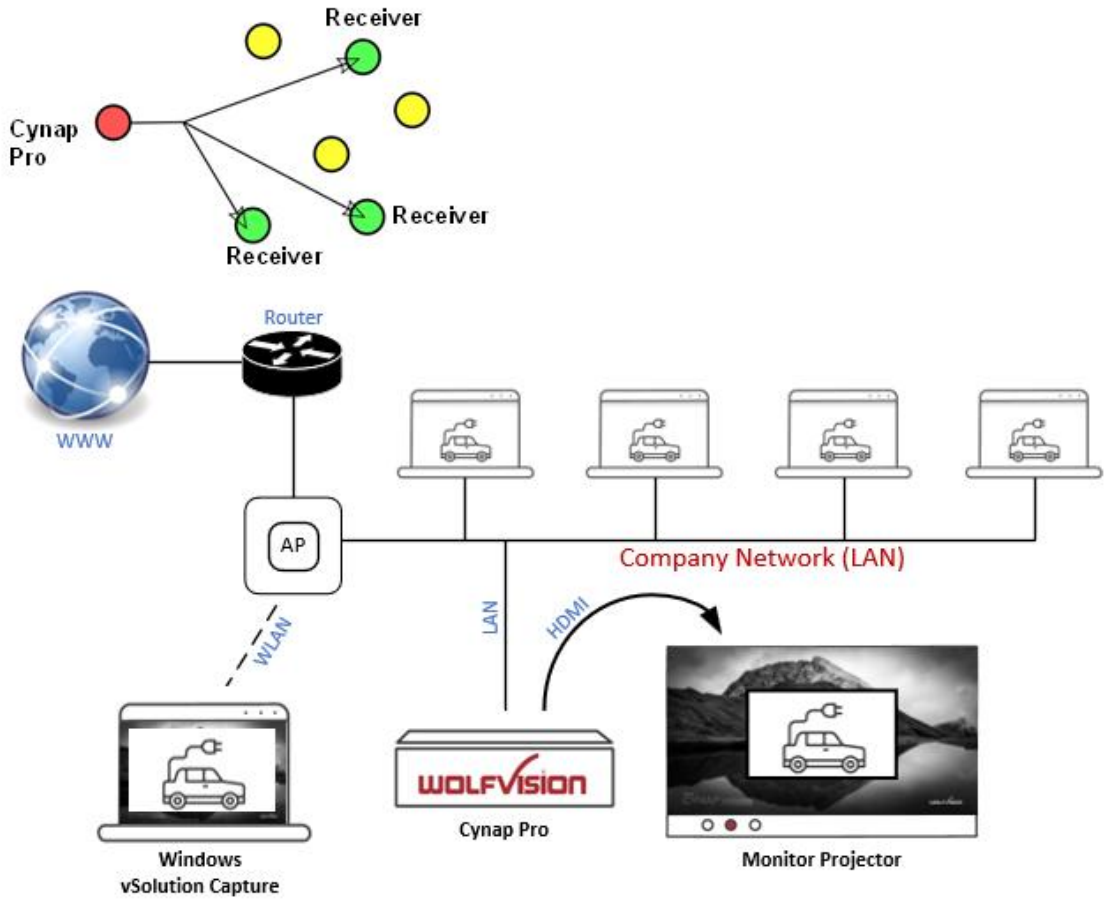
When using RTSP, more than one client would be able to watch the stream over LAN and WLAN simultaneously. Cynap Pro will start a separate unicast stream to each client according of connected clients. The settings will be handled automatically between server and client.



Hint:
Cynap Pro in Access point mode, UDP-streams over WLAN are limited to Unicast. Multicast not supported on Cynap Pro Access point.

Multicast Streaming

Cynap Pro`s sending stream to a Multicast group. That`s a one to many connection. The IP address of the Multicast group can be adjusted in the streaming settings.
Multicast stream is being sent over LAN 1 interface only.
Note: 224.x.x.x and 239.x.x.x are reserved IP areas and should not be used.



Important:
Activate IGMP snooping.
Normally (without IGMP snooping) a switch will forward a multicast frame to all switch port (except incoming port). IGMP snooping allows the switch to send multicast frames only to those receivers that join a particular group by listening leave messages from the hosts.

Please note:
The more clients are connected the more the network could be stressed. The maximum number of connected clients mainly depends on the local infrastructure.
Not every device (client) is supporting Multicast, use RTSP instead.
Switching Cynap Pro to standby or ending the presentation closes all connections and stops streaming.

Streaming with enable Webcasting Feature Pack

The Webcasting function allows uploading live streams onto live view and on-demand service providers. Audiences of any size can watch the recorded video anytime, from any location. This way, your local network will be less stressed.

Available services / mode are:

- YouTube Live
- Custom (e.g. to share content on Facebook)

YouTube Live

Webcast enable	Enable / Disable Webcast functionality
Mode	Choose the YouTube Live
Login	Login to the Google Account

Custom (e.g. to share content to Facebook)

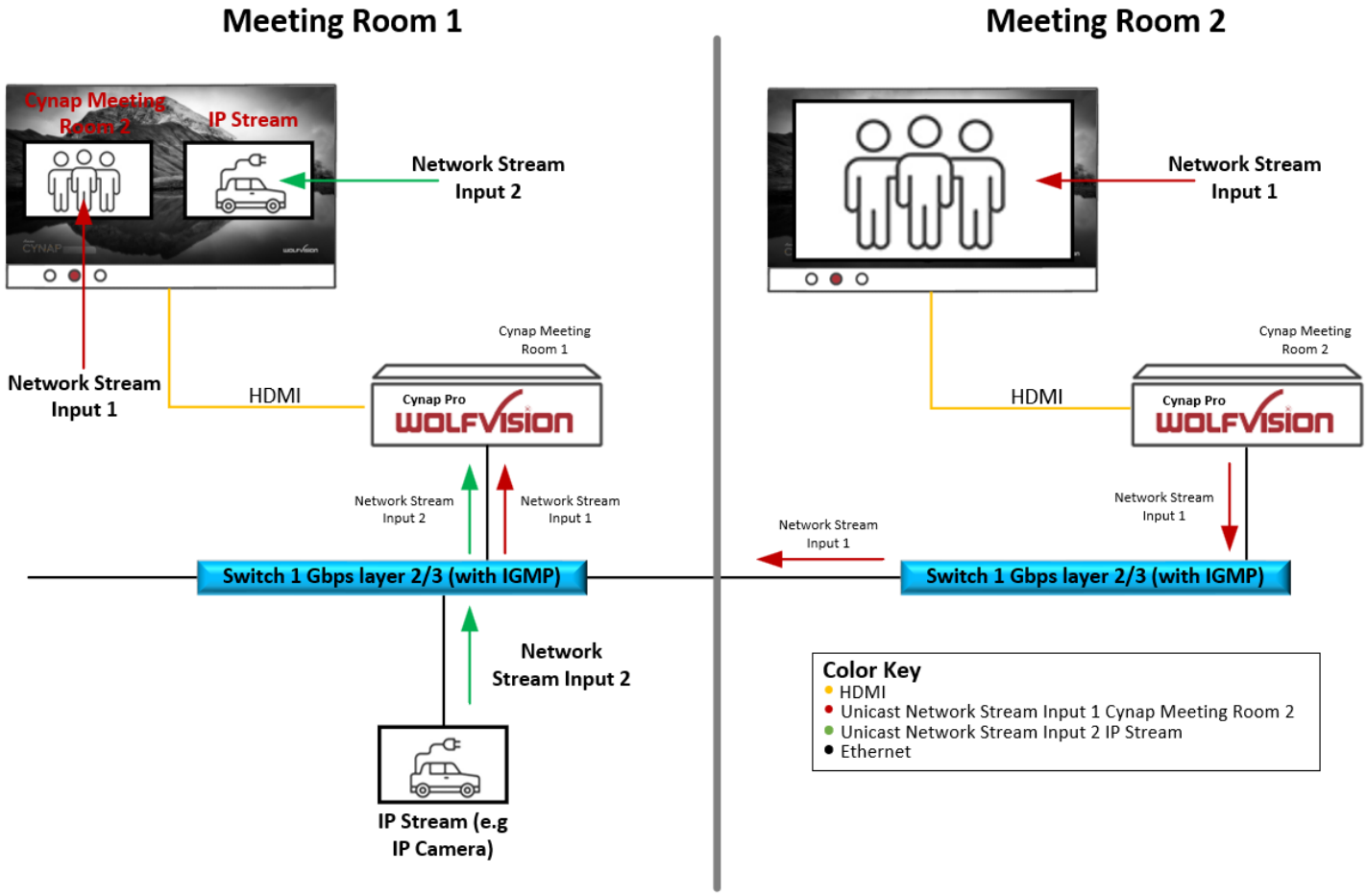
Webcast enable	Enable / Disable Webcast functionality
Mode	Choose the Custom
URL	Input the URL according recommendations of your RTMP capable provider, e.g. Facebook

Network Stream (input)

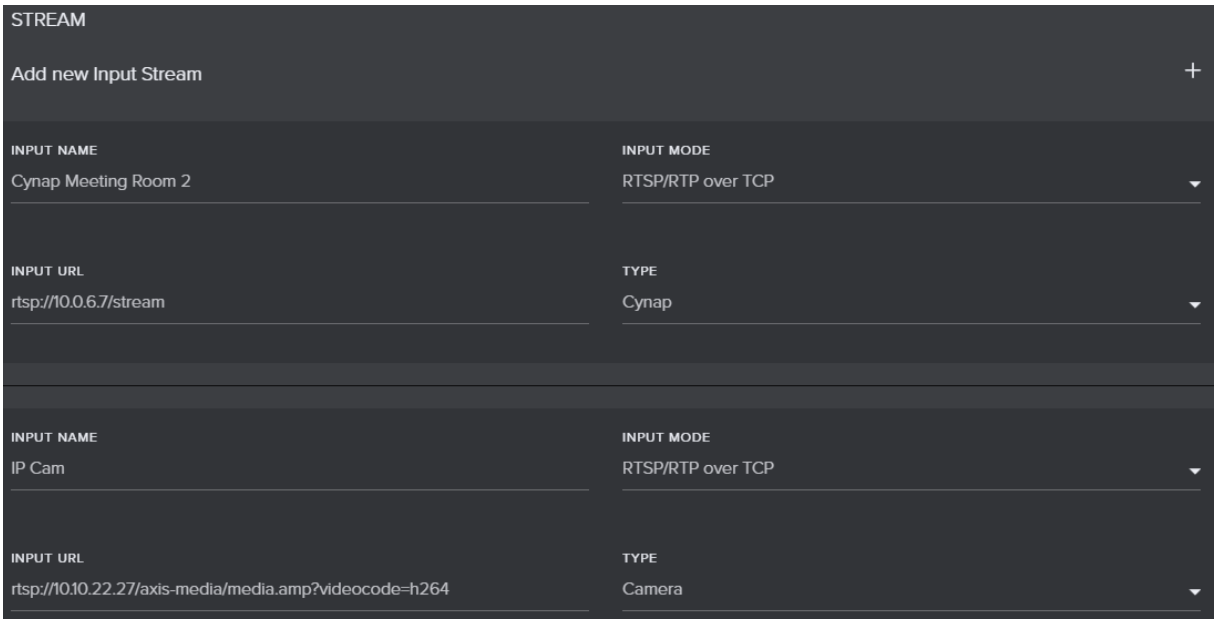
Cynap Pro has a built-in streaming client which is capable of receiving broadcast video content over the network.
Up to four Stream sources can be defined and individually named in the GUI settings (Input).

Add new Input Stream	Allows adding up to four network streams selectable as source (click the + symbol).
Input name	Gives the source an individual name for easy identification
Input mode	Defines the kind of stream. • None, disables receiving this stream • Generic allows streams using UDP and TCP protocol • RTSP / RTP over TCP allows TCP protocol only
Input URL	Record Stream Input URL defines the source of the stream
Type	Defines the icon for easier identification

Example:
Network stream input with two devices, one from Cynap Pro Meeting Room 2 and one from IP Camera.



At the Cynap Pro Meeting Room 1 are two network stream input configured with the following settings.



After saving configuration the new two sources (IP Camera, Cynap Pro Meeting Room 2) are available.
At the Cynap Pro Meeting Room 2 the RTSP Stream is enabled, and Streaming must be started.
Then choose the sources IP Camera and Meeting Room 1 (Cynap Pro) and then contents will be displayed on Cynap Pro in Meeting Room 2.

Control of Peripheral Devices

Cynap Pro is able to send up to 10 commands to connected network devices, e.g. to fully power up the connected projector. This feature will be triggered by power events of Cynap Pro.
The peripheral devices, like projectors, monitor, lightings, windows shades, etc. need to be in the same network as Cynap Pro.

Command enable	Enable / disable certain commands (entered command settings will be not deleted
Name	To give the command an individual name (like “projector”)
Description	To give the command a detailed description (like “power up”)
Event	To define at which power state of Cynap Pro the command will be sent (Power ON or Power OFF). Select event None to delete this entry.
Protocol	Defines the used network protocol (TCP, UDP or PJLink)
IP address	Defines the destination, enter the address of the third-party device
Port	Defines at which network port the command will be sent (note documentation of the third-party device and firewall settings)
Hex Command	Enter the command according to documentation of the third-party device.
Password	Available when protocol PJLink is selected.

Recording

Cynap Pro has a recording function to record presentations. All types of content can be stored internally. The resolution of recordings can be adjusted in the settings.
Supported video file format is MP4-container with codec H.264 (video file extension is *.mp4).

Recording settings

Recording Enable / Disable	When disabled, the Recording button will be not displayed in the toolbox and not available with Media Cast key).
Resolution	Defines the resolution of the system - 360p (640x360 pixels) - 540p (960x540 pixels) - 720p (1280x720 pixels) - 1080p (1920x1080 pixels)
Frame rate	Defines the max frame rate (refresh rate) of the stream - LOW=10fps - MEDIUM=20fps - HIGH=30fps
Custom Recording Name Enable / Disable	To allow personal naming of the files. The displayed box, when starting recording, allows changing the prefix of the file name (the time stamp cannot be changed).

Example:

Video	**Power Point**
Source: Big Buck Bunny 1080p (file size 885 MB)	**Source:** Presentation with text and a few graphics, 60 pages (file size 863 KB)
Settings: Resolution 720p30	**Settings:** Resolution 720p30
Recording: For one hour	**Recording:** For one hour
Result: File size recording 1,43 GB	**Result:** File size recording 596 MB

Please note:
Recording will stop automatically when recording time has reached 16 hours.
Switching Cynap Pro to standby stops recording and deletes file from system folder.

Please note:
Local recording will be disabled when the optional capture agent has initiated remote recording.

Recording with enabled Capture Feature Pack (optional)

With enabled Capture Feature Pack, the services for Panopto and Opencast are available. The current state will be indicated, available states are:

- For Panopto „logged in“ or „not logged”
- For Opencast “disabled”, “idle”, “recording” “fail”

Additional settings are:

Capture Agent	Enable / Disable Capture Agent - Standby function of Cynap Pro is blocked when the Capture Agent is enabled - When a server controlled task is running, local recording through the Toolbox is blocked
Capture Agent Type	Allows selecting Panopto or Opencast

Capture Feature Pack: Panopto

With enabled Capture Feature Pack, Cynap Pro’s recordings can be automatically uploaded to a Panopto server. Additionally Cynap Pro is able to record the network stream of an external camera as a second file in the background. A symbol at the right top corner of the main screen indicates the state of the external stream.
To record a huge amount of sessions, a USB storage device can be used instead of the internal SSD.

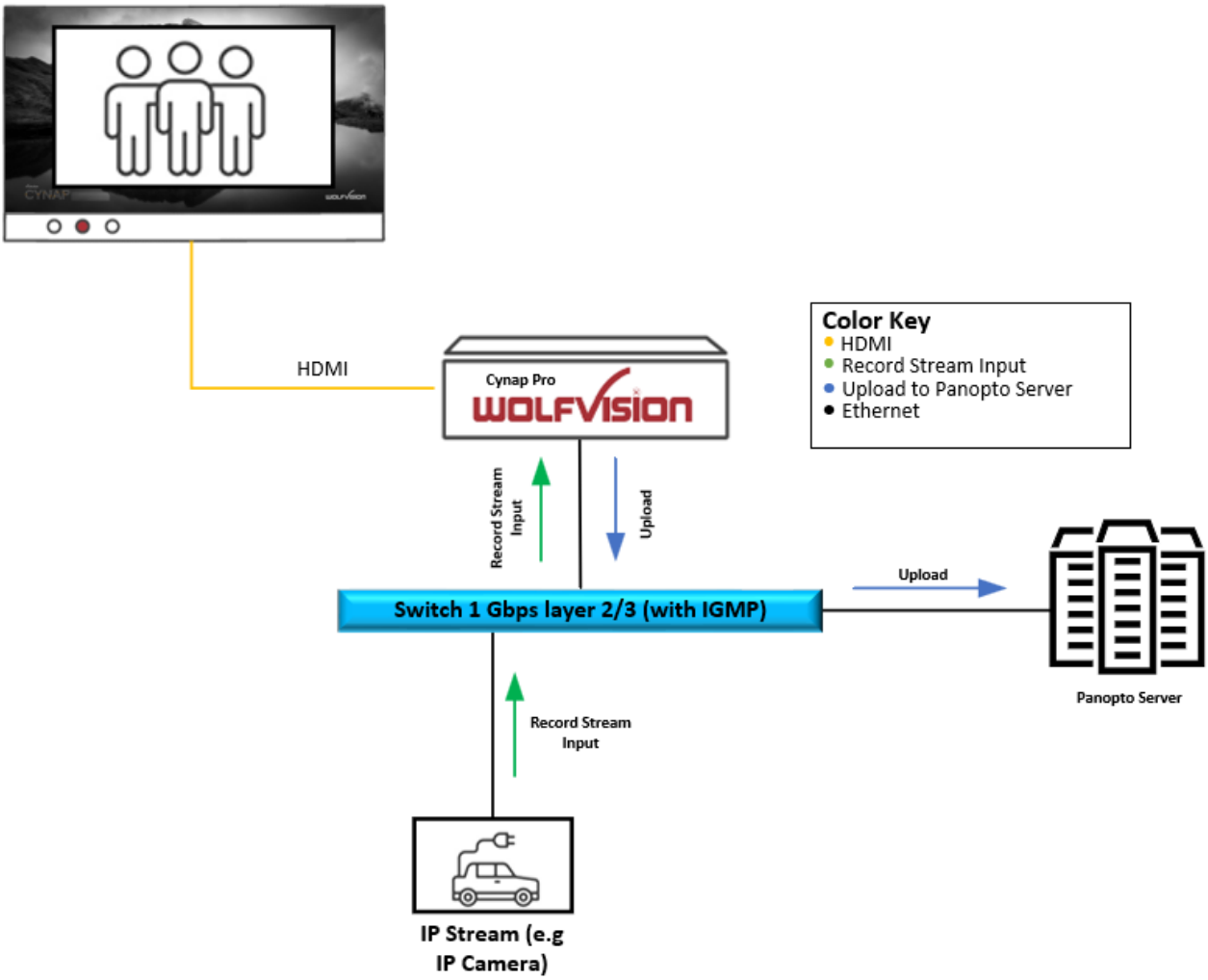
Available settings are:

IP Camera Mode	Allows recording of the additional streaming input (Record Stream Input).
Ingest Time Mode	Select AUTO and the recorded files will be uploaded to the server as soon as recording is finished. Select MANUAL and set the desired starting time, e.g. to upload the files in the night to prevent additional network traffic during the day.
Start Time	Allows starting the upload at the desired time. This field is available in manual ingest mode only.
File Prefix	File Prefix adds a prefix to the file name for easier identification on the server.
Hostname	Input the hostname of the used server, given by your Panopto administrator.
Username / Password	Username and Password are required by the Panopto server (credentials required at the server).
Root Certificate	This allows connecting to a Root Certificate (CA) protected server. To load the certificate, click the Browser button and select the respective file in the explorer window (Base-64-coded X.509). The certificates cannot be loaded when using the local GUI (on HDMI).
Recorded Stream Input	Allows adding external network stream which will be saved as separate video file. - None, disable receiving any stream. - Generic allows streams using UDP and TCP protocol. - RTSP / RTP over TCP allows TCP protocol only.
Recorded Stream Input URL	Defines the source of the stream.
Recorded Stream Input	Allows adding the audio content from the stream to the

audio	recording.
Test stream input	By using the test button, Cynap Pro will open a new window to show the stream local.

Time and date of Cynap Pro and also the server have to be in sync for proper function (see settings General)!

Example Panopto:
Cynap Pro has a connection to Panopto Server. Ingest time Mode is AUTO and the recorded files will be uploaded to the Panopto Server as soon as recording is finished. The IP Camera (Record Stream Input), will be also initiated when you start recording (Start Panopto) automatically. The Record Stream Input will not be displayed at the HDMI Out. Recording files will not deleted after uploading to the Panopto Server in the Cynap Pro but remain as a backup in the internal or external storage. The successfully completed events (recordings & upload) are stored in a ring memory, which is deleted in succession starting with the oldest recording, if the storage space is too low.



Capture Feature Pack: Opencast

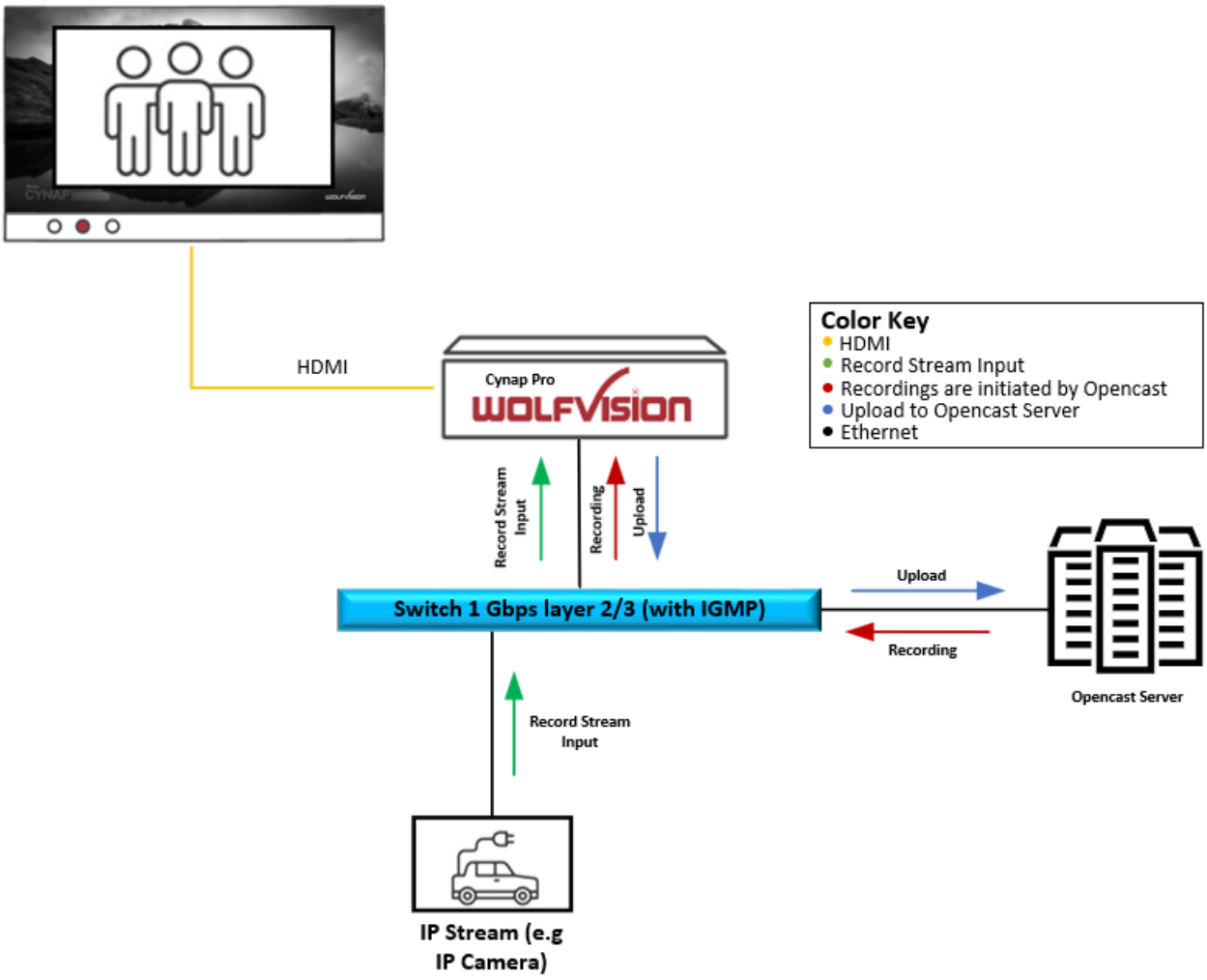
With enabled Capture Feature Pack, Cynap Pro's recording functionality can be managed remotely by an Opencast server. The Opencast server can fully control the recording functionality of Cynap Pro and local recording will be disabled when the optional capture agent has initiated remote recording.
Additionally Cynap Pro is able to record the network stream of an external camera as a second file in the background. A symbol at the right top corner of the main screen indicated the state of the external stream. To record a huge amount of sessions, a USB storage device can be used instead of the internal SSD.

Available settings are:

Capture Agent Name	Allows identification at the Opencast server.
Recording Path	Allows recording onto a connected USB storage device. The external USB storage device has be to formatted in EXT4. When the external USB storage device should be unavailable, Cynap Pro will record onto internal storage.
URL	Defines the address of the Opencast server (depending on network environment, add the port number).
Username / Password	Are required by the Opencast server (credentials required at the server)
Ingest Time Mode	Select AUTO and the recorded files will be uploaded to the server as soon as recording is finished. Select MANUAL and set the desired starting time, e.g. to upload the files in the night to prevent additional network traffic during the day.
Time	Allows starting recording at the desired time. This field is available in manual ingest mode only.
Root Certificate	This allows connecting to a Root Certificate (CA) protected server. To load the certificate, click the Browse button and select the respective file in the explorer windows (Base-64-coded X.509). The certificates cannot be loaded when using the local GUI (on HDMI).
Record Stream Input	Allows adding external network stream which will be saved as separate video file. - None, disables receiving any stream - Generic allows streams using UDP and TCP protocol - RTSP / RTP over TCP allows TCP protocol only
Record Stream Input URL	Defines the source of the stream.
Record Stream Input Audio	Allows adding the audio content from the stream to the recording.
Test Stream Input	Cynap Pro will open a new window to show the stream local.
External Storage	Indicates the state.
Storage Action	Allows mounting and formatting the external drive. The drive has to be mounted before it can be used. Formatting will delete all content from the USB storage device! Use file format is EXT4.
Execute Action (Button)	Changes for the external drive will take effect. During initialization, the state is changing to busy.

Time and date of Cynap Pro and also the server have to be in sync for proper function (see settings General)!

Example:
Cynap Pro has a connection to Opencast Server. Ingest time Mode is AUTO and all recordings are initiated by the Opencast Server. The IP Camera (Record Stream Input), will be also initiated by the Opencast Server. The Record Stream Input will not be displayed at the HDMI Out. After recordings from the Capture Agent, they are automatically uploaded to Opencast Server. Recording files will not deleted after uploading to the Opencast Server on the Cynap Pro but remain as a backup on the internal or external storage. The successfully completed events (recordings & upload) are stored in a ring memory, which is deleted in succession, starting with the oldest recording, if the storage space is too low.



vSolution Matrix Feature Pack (optional)

The vSolution Matrix Feature Pack enables networked AV functionality and it is optimized for touch screens. Network AV allows cost-effective installation by using an existing IP network for transmission of AV signals. This means that there is no longer a need to maintain separate AV infrastructure. Cynap Pro systems do not need additional encoding / decoding hardware. Configuration of vSolution Matrix for Cynap Pro also means that cabling requipments are reduced. Selecting Cynap Pro and Cynap Pro Core systems for your e.g. active learning classroom means less hardware, more straightforward installation plus reduced ongoing maintenance. You also have the flexibility to scale up or down easily in the future, as required to keep your huddle rooms effective. A Cynap Pro system at every workstation ensures an intuitive and easy-to-use collaborative working environment for all users. The simple drag and drop interface enables content to be moved effortlessly between different screens in the room. vSolution Matrix uses intelligent and optimized stream processing to ensure high quality video and audio with low latency, and a moderate bandwidth requirement.

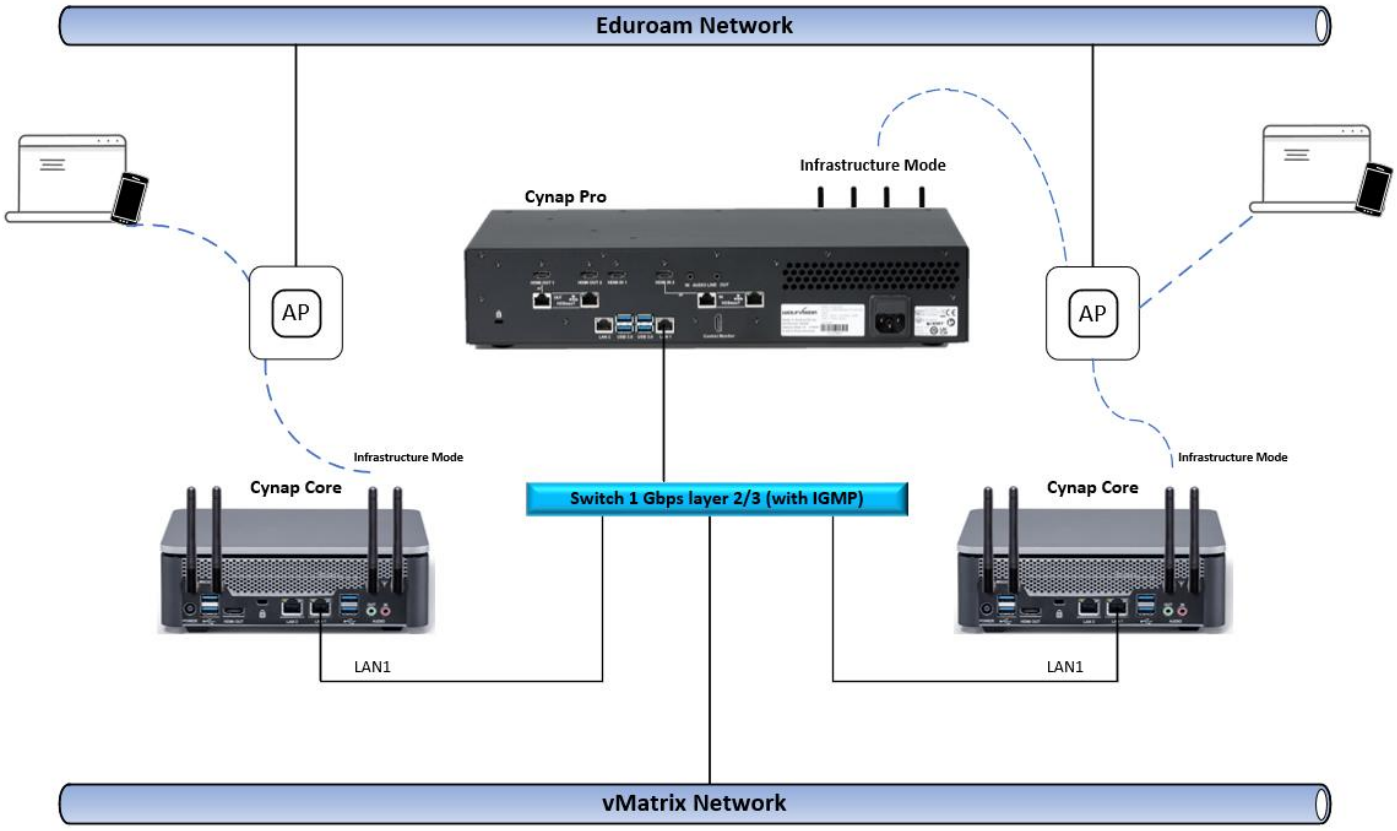
Active collaboration using Cynap Pro and Cynap Pro Core systems, connected using existing IP infrastructure. Collaboration made easy using simple drag and drop control functionality.

For more information, please refer to the manual.

Specifications:

Maximum stations	40 Cynap Pro Core or Cynap Pro
Bandwidth Stream	40 Mbit/s
Latency	Approximately 50 milliseconds for 1080p30
Communications	Wired, LAN 1 only
Switch	Layer 2 or Layer 3 with enabled IGMP Snooping (IGMP snooping v2 or v3)

Example:
Network overview vSolution Matrix with Master Cynap Pro and two Cynap Pro Core station connected over the LAN 1 interface to the switch. In infrastructure mode, Master Cynap Pro and Cynap Pro Core station is connected to an existing wireless access point in the existing network (e.g. Eduroam network). BYOD devices in the vMatrix network and in the Eduroam network can connect to Cynap Pro.



Cloud services

Cynap Pro supports Dropbox, Jianguoyun, OneDrive and WebDAV cloud services. These services can be enabled or disabled in the settings. For specific firewall settings, check the individual service provider.

Network Drive

Cynap Pro allows direct access to network drives (writeable or read-only). A default drive can be specified to simplify the upload functionality of a recording or snapshot.

Up to 10 network drives can be configured in the network drive settings.

CIFS 2.x and NFSv4 file systems are supported.

User interface

You can adjust Cynap Pro basic settings using the function keys on the front of the device. Cynap Pro can be controlled using any current standard browser. The user interface has been developed using the latest web programming standards, and this means that there is no need for additional add-ons or plugins such the Java Platform, in order to have full control of Cynap Pro. HTML5 technology only requires a browser that can handle JavaScript and Websockets, and this has been state-of-the-art for the last few years. You can also adjust the settings using the remote control. The remote control uses the 2.4 GHz band. The remote control has a built-in gyro sensor and can be used as a digital laser pointer.
Cynap Pro can also be used in combination with room management systems. Communication is possible via the Wolfprot protocol. More information about this protocol can be found in the support section of our website www.wolfvision.com .
The vSolution Control app allows smartphones / tablets (iOS, Windows, Android) to control Cynap Pro directly via WLAN. More information about the vSolution Control App can be found on in the support section of our website www.wolfvision.com .

Hardware and OS

Cynap Pro uses a Linux operating system. The distribution is a WolfVision specific variant, which in addition to the Linux kernel contains only the individual libraries and packages required for the functionality of Cynap Pro. This operating system is efficient, secure and lean. The operating system is installed after the installation process, and every update is installed to a read-only partition that cannot be changed after the installation process. This feature and the strict separation of system and user data, such as pictures, videos etc. ensures a very high level of system security. The system structure is protected against any external access, and it does not require additional security programs (antivirus, firewall, etc.). The Cynap Pro system includes all viewer and software packages, and no additional licenses are required.

The current hardware specifications, connectors, delivery, and technical specifications can be found on our website www.wolfvision.com.

A 19” rack mount is available as an optional accessory if required for installing Cynap Pro (2HE).

Administration

Cynap Pro can be managed using the vSolution Link software.
With vSolution Link software, administration tasks can be performed for multiple Cynap Pro systems. With this admin tool, you can perform central firmware upgrades as well as determining the state of Cynap Pro and Wake-on-LAN (WoL). You can also create, manage, and distribute a settings profile to all Cynap Pro systems using vSolution Link software.

More information about vSolution Link software can be found in the support section of our website www.wolfvision.com.

Client System Requirements

Please note, these are absolute minimum requirements.
Outdated devices, outdates OSs, outdated drivers, and/or outdated infrastructure can lead to performance problems and incompatibility issues. Support for outdated systems can no longer be provided.
Keep your devices and your infrastructure up to date to ensure highest compatibility.
Consult documentation of the third-party devices used to check compatibility of services used and to check EoL status.

Requirement vSolution App

Product	Version
Windows	Windows 11 x64 for full support (running on officially supported hardware) Minimum CPU Intel i5 or AMD Ryzen 5 (higher is recommended) Minimum 8GB RAM
macOS	macOS 13 or higher
iOS / iPadOS	iOS / iPadOS 14 or higher
Android	Android 11 or higher

Note: The BYOM feature is not available on iOS/iPadOS or Android-based devices

Requirement vSolution Link Pro

Product	Version
Windows	64 bit Windows operating system 4GB RAM 10GB minimum free disk space for firmware files. Installation on IIS strongly recommended.
macOS	Version 10.15 4GB RAM 10GB minimum free disk space for firmware files. Installation on IIS strongly recommended.

Requirement vSolution Cast

• Minimum Windows 7 (running on officially supported hardware)
• Old hardware may not offer sufficient performance
• It is recommended to use an up-to-date version of your Windows operating system

Requirement AirPlay Mirroring OS X Mountain Lion v10.8 (Release 2012) or later:

Product	Version
iMac	Mid 2011 or later
Mac mini	Mid 2011 or later
MacBook Air	Mid 2011 or later
MacBook Pro	Early 2011 or later
Mac Pro	Late 2013 or later

Requirement AirPlay Mirroring iOS 5.0 (Release 2011) or later:

Product	Version
iPhone	4 or later
iPad	2 or later
iPad	mini or later
iPod touch	5th generation or later

Requirement Miracast:

Product	Version
Android	4.4.2 or later Hardware with Miracast support required
Microsoft Windows	8.1, 10, 11 Hardware with Miracast support required
Windows Phone	8.1, 10
Blackberry	10.2.1 or later

Requirement Chromecast:

Product	Version
Android	4.0.3 or later Hardware with Miracast support required
Microsoft Windows	7, 8.1, 10, 11 (Chromecast Browser Plugin may required)

Firewall rules (full list)

Cynap Pro has firewall rules that must be adhered to in order to allow successful network communications, and the corresponding services to be used.

Function / Application	Port	Type	Inbound / Outbound	Description
Airplay				
Multicast DNS (mDNS)	5353	UDP	Inbound / Outbound	Multicast DNS (mDNS 224.0.0.251) Bonjour
Audio	4100 – 4164	TCP / UDP	Inbound	Audio for Airplay
Airplay	7000	TCP	Inbound	Primary Airplay communication
Video	7100	TCP	Inbound	Airplay video communication
Audio	47000	TCP	Inbound	Airplay audio communication
Airplay Bluetooth				
Audio	4100 – 4164	TCP / UDP	Inbound	Audio for Airplay
AirPlay	5000	TCP	Inbound	AirPlay communication with legacy devices
AirPlay	7000	TCP	Inbound	Primary Airplay communication
Video	7100	TCP	Inbound	Airplay video communication
Audio	47000	TCP	Inbound	Airplay audio communication
Chromecast				
Multicast DNS (mDNS)	5353	UDP	Inbound / Outbound	Multicast DNS (mDNS 224.0.0.251)
Discovery	1900	UDP	Inbound	Chromecast discovery
Audio	4100 – 4164	TCP / UDP	Inbound	Audio for Chromecast
Chromecast	8008	TCP	Inbound	Primary Chromecast communication
Chromecast	8009	TCP	Inbound	Communication Chromecast
Video data stream	1 – 65535	UDP	Inbound /Outbound	Chromecast (video data stream)
Miracast MS-MICE				
Multicast DNS (mDNS)	5353	UDP	Inbound / Outbound	Multicast DNS (mDNS 224.0.0.251)
DHCP	67 / 68	UDP	Inbound	DHCP communication between device and receiver
RTP Stream	19000 – 19007 19010 – 19017	UDP	Inbound	RTP media traffic port for delivering audio and video
RTSP Control	7236	TCP	Outbound	RTSP control port is used to establish and manage session
MS-MICE Control	7250	TCP	Inbound / Outbound	Control port on which Cynap Pro family system listen for Miracast packets when over existing network mode is enabled
Touchback	50000	TCP	Outbound	This port is for touchback to send mouse events back between Cynap Pro to the Windows computer. If this port is blocked, bi-directional inputs is not possible.
Hardware cursor extension	19020 – 19027 19030 – 19037	UDP	Inbound	Hardware cursor to reduce latency when using touchback.
vMatrix				

Discovery Multicast	50000	UDP	Inbound	Discovery Multicast – This port is used for device discovery all available Cynap Pro and Visualizer in the network by vSolution applications (uses Multicast IP address 239.255.255.250). If this port is blocked, vSolution applications may not be able to find devices automatically
http, Cynap Pro control	80	TCP	Inbound / Outbound	For master control mode
https, Cynap Pro control	443	TCP / UDP	Inbound / Outbound	For master control mode
NFS	111 / 2049	TCP / UDP	Outbound	NFS – Connection to networks drives
CIFS	137 / 139	TCP / UDP	Outbound	CIFS – Connection to networks drives
SSHFS	50930	TCP	Inbound	SSHFS – vSolution Matrix File Sharing Key Exchange
TLS Control	50917	TCP	Inbound	TLS Control – This port is for secure communication between Wolfvision applications (e.g. vSolution Link) to Cynap Pro and / or Visualizer. If this port is blocked, secure communication to Cynap Pro and / or Visualizer, inclusive firmware updates are blocked
RTSP	554	TCP	Inbound	RTSP – This the communication port for the RTSP stream.
RTSP	555	TCP	Inbound	Required for RTSP negotiations of dual screen stream in Composer mode
RTMP	1935	TCP	Outbound	This port is used for streaming to panopto server. If this port is blocked, no stream to panopto server is possible.
Webcasting	1935	TCP	Outbound	This port is used for streaming to Webcasting Server. If this port is blocked, no stream to Webcasting server is possible.
Wake On LAN	7 / 9	UDP	Inbound / Outbound	Usually port 7 is used for sending the magic packet
FTP	21	TCP	Outbound	Connection to FTP server
SSH	22	TCP	Inbound	Access for Wolfvision support
http, Cynap Pro control	80	TCP	Inbound	This port used to connect to Cynap Pro web interface (httpd). If this port is blocked, no connection can be made.
https, SSL, e.g. Cloud Service, Cynap Pro control	443	TCP / UDP	Inbound	This port is used to cloud service and for secure connect to Cynap Pro web for secure connect to Cynap Pro web interface. If this port is blocked, no connection can be made.
Proxy	8080	TCP / UDP	Outbound	Default port proxy function (This port can be changed in the Proxy settings).
NTFS	111 / 2049	TCP / UDP	Outbound	Connection to network drives
CIFS	137 / 139	TCP / UDP	Outbound	Connection to network drives

NTP	123	UDP	Outbound	For optional clock synchronization by a time server (Network Time Protocol, NTP)
LDAP	389	TCP / UDP	Outbound	Connection to LDAP server
LDAPS	636	TCP / UDP	Outbound	Connection to LDAPS server (TLS)
Streaming Multicast / Unicast	8800 – 9002	UDP	Inbound	Used for Multicast / Unicast / Audio / Video Streaming
Streaming RTSP	554	TCP	Inbound	This is the communication port for the RTSP stream. This used UDP port will be handled automatically
PJLink	4352	TCP	Outbound	This is the default port for PJLink and cab be changed in the settings (Peripheral Control)
vSolution Cast				
Discovery Multicast	50000	UDP	Inbound	This port is used for device discovery all available Cynap Pro and Visualizer in the network by vSolution applications (uses Multicast IP address 239.255.255.250). If this port is blocked, vSolution applications may not be able to find devices automatically.
Device Discovery	50913	UDP	Inbound	This port is used for device discovery
For control purposes	50915	TCP	Inbound	This port is used for control purposes e.g. room control system, and others). If this port is blocked, no control is possible
TLS Control	50917	TCP	Inbound	This port is for secure communication between WolfVision applications (e.g. vSolution App) to Cynap Pro and / or Visualizer. If this port is blocked, secure communication to Cynap Pro and / or Visualizer, inclusive firmware updates are blocked.
Video streams	50921	TCP	Inbound	Video streams between Wolfvision App to Cynap Pro and Visualizer. If this port is blocked, no stream are possible.
Touchback	50922	TCP	Outbound	This port is for touchback between Cynap Pro and Wolfvision App vSolution Cast to send mouse events back to the Windows computer. If this port is blocked, bi-directional inputs is not possible
vSolution App iOS / Android / Windows				
Discovery Multicast	50000	UDP	Inbound	This port is used for device discovery all available Cynap Pro and Visualizer in the network by vSolution applications (uses Multicast IP address 239.255.255.250). If this port is blocked, vSolution applications may not be able to find devices automatically.
http, Cynap control	80	TCP	Inbound	This port is used to connect to the Cynap Pro web interface (httpd). If

				this port is blocked, no connection can be made.
https, SSL, e.g. Cloud Service, Cynap control	443	TCP	Inbound	This port is used to cloud services and for secure connect to the Cynap Pro web for secure connect to the Cynap Pro web interface. If this port is blocked, no connection can be made.
Device Discovery	50913	UDP	Inbound	This port is used for device discovery.
For control purposes	50915	TCP	Inbound	This port is used for control purposes e.g. room control system, and others). If this port is blocked, no control is possible
TLS Control	50917	TCP	Inbound	This port is for secure communication between WolfVision applications (e.g. vSolution App) to Cynap Pro and / or Visualizer. If this port is blocked, secure communication to Cynap Pro and / or Visualizer, inclusive firmware updates are blocked
Video streams	50921	TCP	Inbound	Video streams between WolfVision App to Cynap and Visualizer. If this port is blocked, no streams are possible.
Touchback (Windows, macOS)	50922	TCP	Outbound	This port is for touchback between Cynap and WolfVision App vSolution Cast to send mouse events back to the Windows computer or MacBook. If this port is blocked, bi-directional inputs are not possible.
Video data stream	32768 - 61000	UDP	Inbound /Outbound	Video data stream (e.g., BYOM, Chromecast)
WebRTC	10000 – 16000 50000 - 65000	TCP / UDP	Outbound	Communication Port
WebRTC (Pexip)	1720	TCP	Outbound	This port used WebRTC services like Pexip
TLS Control	50917	TCP	Inbound	This port is for secure communication between Wolfvision application (e.g. vSoltuion Link) t Cynap Pro and / or Visualizer. If this port is blocked, secure communication to Cynap Pro and / or Visualizer, inclusive firmware updates are blocked.
WebSocket	7681	TCP	Inbound	User interface communication with Cynap Pro (via browser)
WebSocket	7682	TCP	Inbound	User interface communication with Cynap Pro (via fully integrated Visualizer)
vSolution Link Pro				
Wake On LAN	7 / 9	UDP	Inbound / Outbound	Wake On LAN – Usually port 7 is used for sending the magic packet
DNS	53	TCP / UDP	Inbound / Outbound	DNS – This port will be used for Domain Name System. If this port

				is blocked, DNS service are not available
http, Cynap Pro control	80	TCP	Inbound	This is the default port to connect to the web interface (httpd) of vSolution Link Pro. Of this port is blocked, connection cannot be established
https, SSL, e.g. Cloud Service, Cynap Pro control	443	TCP	Inbound	This is the default port to connect to web interface (https) of vSolution Link Pro. If this port is blocked, connection cannot be established.
SMTP	587	SMTP	Outbound	Mail Server – Port for communication with SMTP server.
Discovery Multicast	50000	UDP	Inbound	This port is used for device discovery all available Cynap Pro and Visualizer in the network by vSolution applications (uses Multicast IP address 239.255.255.250). If this port is blocked, device discovery is not possible
Device Discovery	50913	UDP	Inbound	This port is used for device discovery. If this port is blocked, device discovery is not possible.
For control purposes	50915	TCP	Inbound	This port is used for control purposes. If this port is blocked, no control is possible
Zoom				
http	80	TCP	Outbound	For Zoom clients and meeting connector
http over TLS / SSL	443	TCP	Outbound	For Zoom clients and meeting connector
	8801	TCP	Outbound	For Zoom clients
	8802	TCP	Outbound	For Zoom clients
	3478	UDP	Outbound	For Zoom clients
	3479	UDP	Outbound	For Zoom clients
	8801 - 8810	UDP	Outbound	For Zoom clients
Panopto				
Communication to Panopto server	80	TCP	Inbound / Outbound	This port is used for http communication to the Panopto server.
Communication to Panopto server	443	TCP	Inbound / Outbound	This port is used for http communication to the Panopto server.
Streaming to Panopto server	1935	TCP	Outbound	This port is sending a stream to Panopto server.

Changelog

Version	Date	Changes
1.9	2026-03-19	Google Drive support has been removed as of firmware v1.76a
1.8	2025-10-14	Added note about Energy Efficient Ethernet (EEE) Adapted Miracast MS-MICE firewall rules. Client System Requirements updated. Version number corrected
1.7	2025-05-09	Adapted port range for Chromecast firewall rules (firmware v1.68c) Added details to Miracast on Android
1.6	2024-07-11	Guide revised
1.5	2024-03-01	Addition Firewall rules
1.4	2023-10-18	Addition Firewall rules
1.3	2023-10-02	Services updated
1.2	2023-07-31	Minor text edits Addition Firewall rules Illustrations updated
1.1	2020-11-30	Minor text edits Addition Firewall rules (Panopto)
1.0	2020-02-21	Created