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 Pure
Network Integration

1. 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 Pure can be integrated into the network.
When connecting Cynap Pure 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 Pure can be treated as a standard network device and it is as secure as the supporting network. Cynap Pure 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, the built-in access point is enabled, SSID and password are the serial number of the unit (inclusive leading zero, e.g. 0106406).

2. Glossary

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

2.1. LAN / Ethernet settings

Priority Interface Access	The higher prioritized interface (value = 1) will be used for network services first. Ensure that the value is different from the WLAN interface priority.
DHCP	Cynap Pure 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 Pure 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 Pure 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 Pure 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-----“

2.2. WLAN settings – access point

Mode OFF	Disable access point.
Mode Access Point	Enable access point.
Region	Select the region where Cynap will be operated (US-region or others).
Channel	Defines the channel used for wireless communication. For optimum performance, select a currently unused channel.
IP address	Defines the IP address of the access point. Cynap Pure 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

2.3. WLAN settings – infrastructure (Cynap Pure acts as client)

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

Mode Infrastructure	Enable Infrastructure, Cynap Pure can be connected as client to an existing access point.
Band	By default, Cynap Pure 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 services first. Ensure that the value is different from the LAN interface priority.
BSSID On / Off	Use the button to toggle between SSID and BSSID mode. With BSSID (Basic Service Set Identification), the used access point will be fixed and Cynap Pure 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 Pure 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 Pure 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 Pure 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.

2.4. Date and time (General Settings)

Time source	Cynap Pure 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 Pure can be synchronized to an external time server. Select external and input a valid IP address or URL of a NTP time server.

2.5. Host name (General Settings)

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.

2.6. LAN / WLAN port

The LAN port enables integration of Cynap Pure into an internal network. Administrators of a large number of Cynap Pure 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 Pure 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 Internet Explorer, Microsoft Edge, Firefox, Chrome, and Safari.
By default, DHCP is activated to receive all network settings automatically from the server.

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

2.7. Proxy settings

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

Proxy enable	Enable / disable proxy service When enable, all HTTP and HTTPS traffic will be routed to your proxy server.
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.

2.8. Security

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

Login Security
Accessing Cynap Pure 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 Pure 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 Pure complies with following standards:

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

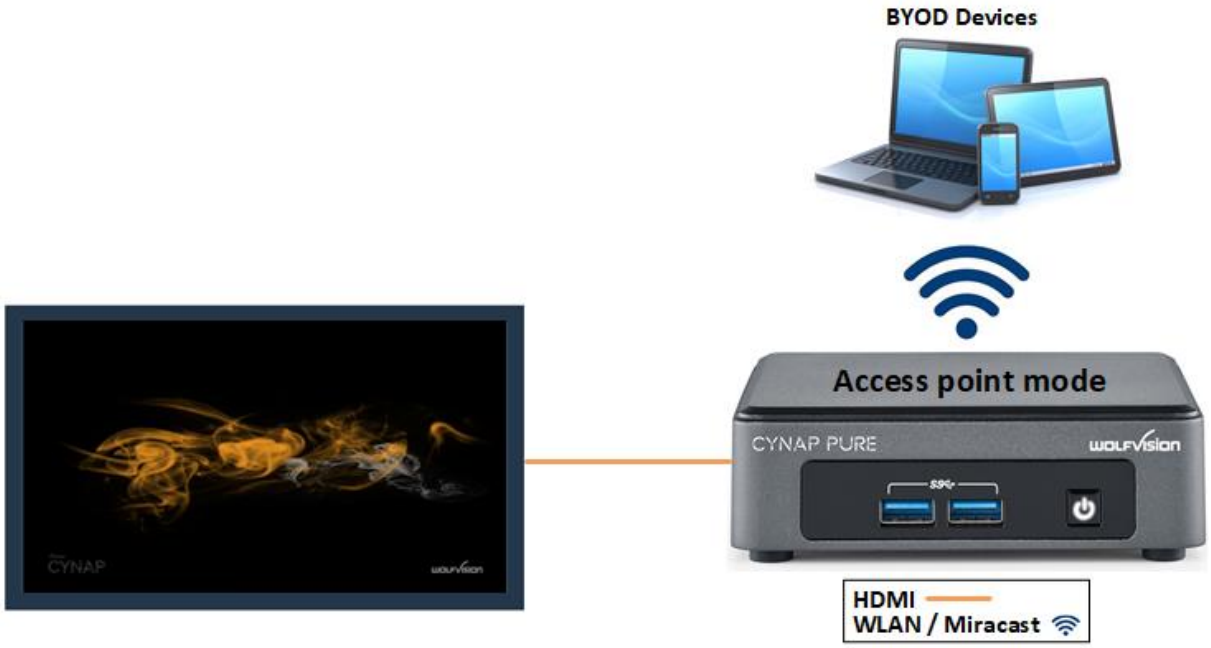
Hint
WEP allows password with a length of 13 characters.
WPA2 allows password with a length of 8 ~ 63 characters.
Use special characters carefully, not every third party device can handle it.
When using WPA2 Enterprise, load the certificate by using the Web Interface.

3. Network integration (examples)

The following examples are showing different ways to integrate Cynap Pure into your network infrastructure, one network and one wireless network.
BYOD (bring your own device) allows sharing the screen content of different devices with various operating systems to Cynap Pure to share to a big display device.

3.1. Stand-alone access point mode (without wired network integration)

Cynap Pure is operated in stand-alone access point mode.
Cynap Pure is acting as DHCP server to provide the addresses to your WLAN devices.
Cynap generates an independent WLAN, and WLAN enabled devices (BYOD) can connect to Cynap Pure.



Advantages:

- No complex network infrastructure necessary
- Cynap Pure generates its own stand-alone access point
- No connection to internal IT infrastructure
- Security issues - no other unit from the internal IT infrastructure can access Cynap Pure

Disadvantages:

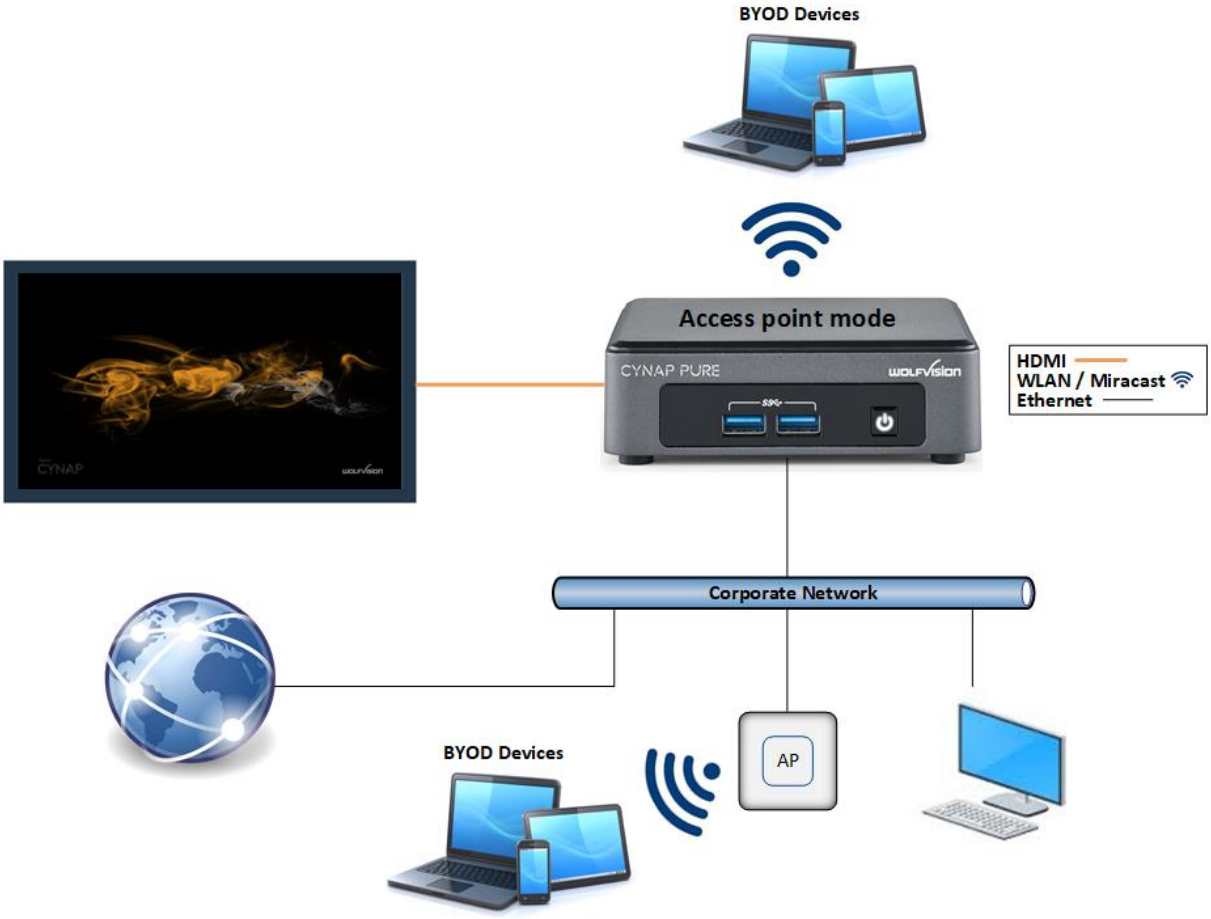
- No devices have internet access

Required settings:

DHCP	Switch to OFF to enable manual setting of addresses
IP Address	Unique address in the network, like 192.168.0.100. The IP address of a connected PC could be set to 192.168.0.1 for maintenance purposes
Subnet Mask	Available IP addresses can be limited. A commonly used subnet mask would be 255.255.255.0
Gateway	Enter the IP address of a directly connected PC for maintenance purposes
Name server	Not needed

3.2. Cynap Pure wireless network access point mode

Cynap Pure integrated via a cable connection into an existing network, and operates in wireless network access point mode additionally. LAN settings for Cynap Pure can be obtained from an existing DHCP server. Cynap Pure generates an independent WLAN, and WLAN enabled (BYOD) can connect to Cynap Pure.



Advantages:

- All devices can communicate with each other
- Cynap Pure has access to the internet.
- Cynap Pure can access the internet to check for firmware updates without using additional devices
- Security issues – BYOD devices over the access point have no access to the existing network and internet.

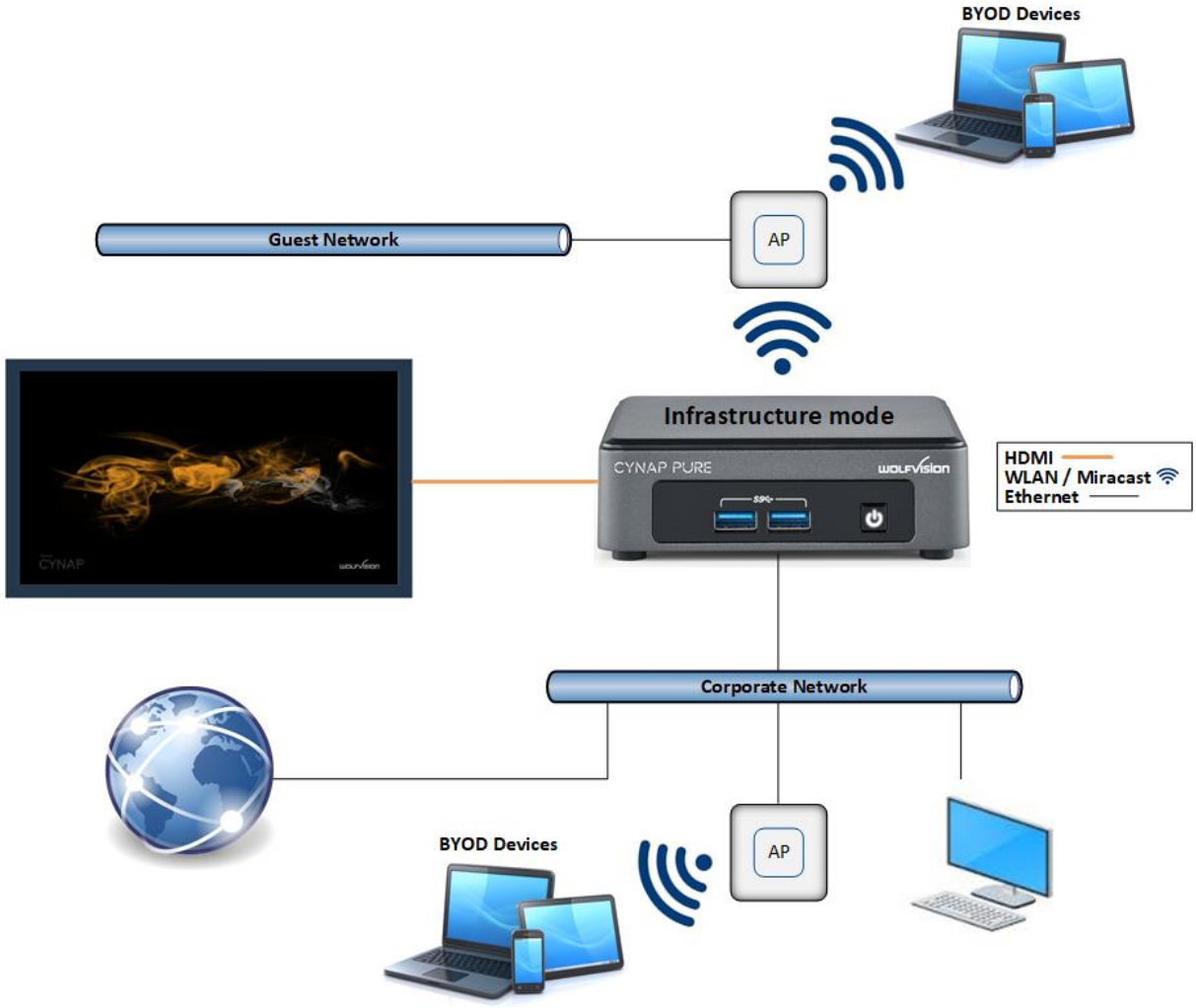
Disadvantages:

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

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

3.3. Cynap Pure network infrastructure mode

Cynap Pure is integrated to an existing wired network (e.g. Corporate network) wired, and additionally connected to a wireless network (e.g. Guest network as separate VLAN).
LAN and WLAN settings for Cynap Pure can be obtained from an existing DHCP server. All devices of the Corporate and also the Guest network can be connected to Cynap Pure.



Advantages:

- All devices can communicate with each other
- Cynap Pure has access to the internet.
- Cynap Pure can be moved within the range of the access point
- Cynap Pure 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 Pure might not be able to be discovered automatically by vSolution applications.
Cynap Pure can also be installed in a VLAN.

4. Firewall rules

Cynap Pure has firewall rules that must be adhered to in order to allow successful network communications, and the corresponding services to be used. To use services with user defined addresses and ports, be sure these are not blocked by your firewall.

Port	Type	Function	Description
7 / 9	UDP	Wake On LAN	Usually port 7 is used for sending the magic packet.
22	TCP	SSH	Access for WolfVision support.
80	TCP	http, Cynap Pure control	This port is used to connect to the Cynap Pure web interface (httpd). If this port is blocked, no connection can be made.
8080	TCP / UDP	Proxy	Default port for proxy function (This port can be changed in the Proxy settings).
123	UDP	NTP	For optional clock synchronization by a time server (Network Time Protocol, NTP)
443	TCP/UDP	https, SSL, e.g., Cynap Pure control	This port is used to connect to the Cynap Pure web interface (httpd). If this port is blocked, no connection can be made.
4100	TCP/UDP	Chromecast / Airplay	Audio for Chromecast and Airplay
4100 – 4164	TCP/UDP	Chromecast	Audio for Chromecast
5353	UDP	Multicast DNS	This port is used to connect Airplay devices to Cynap Pure. If this port is blocked, no connection can be made. (Bonjour)
32768 – 61000	UDP	Chromecast	Chromecast (video data stream)
7236	TCP	Miracast MICE	Miracast MICE connection establishment
7250	TCP	WebSocket	User interface communication with Cynap (via browser).
50000	UDP	Discovery Multicast	This port is used for device discovery all available Cynap Pure 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.
50913	UDP	Device Discovery	This port is used for device discovery. If this port is blocked, device discovery is not possible.
50915	TCP	For control purposes	This port is used for control purposes (e.g. room control system, and others). If this port is blocked, no control is possible.
50916	TCP/UDP	Communication Wolfvision App Cynap Pure	This port is for communication between Wolfvision applications (e.g. vSolution App) to Cynap Pure. If this port is blocked, communication to Cynap Pure, inclusive firmware update are blocked.
50917	TCP	TLS Control	This port is for secure communication between WolfVision applications (e.g. vSolution Connect) to Cynap Pure. If

			this port is blocked, secure communication to Cynap Pure and, inclusive firmware updates are blocked.
50921	TCP	Video streams	Video streams between WolfVision App to Cynap Pure. If this port is blocked, no streams are possible.
50922	TCP	Touchback	This port is for touchback between Cynap and Wolfvision App vSolution Cast to send mouse events back to the Windows computer. If this port is blocked, bi-directional inputs not possible.
7681	TCP	WebSocket	User interface communication with Cynap Pure (via browser).
7000 7100 8008 8009 47000	TCP	Chromecast / Airplay	Communication Chromecast / Airplay

5. Differences in Open Mode / Protected Mode

When using Cynap Pure, it is possible to choose between either Open or Protected Mode in Cynap 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 Pure. Additionally, a user password cab be set.
In the Open Mode, Airplay, Miracast and / or vSolution Cast PIN can be used to prevent disturbance of external devices. The PIN will be shown on the connected display only (HDMI).

Protected Mode
This mode allows desired mirroring sessions only, to prevent misuse and disturbances.
The moderator has to enable a coming session in front by using the room management system. (The room management system needs be correctly implemented)

Mirror Settings
To change the security behaviour to grant or deny connection requests.
To select which kind of mirroring systems could be connected. Disabled systems couldn't share their content.
Possible settings are:

- Mode:
  Open Mode, everybody can connect.
  Protected Mode, every connection or mirroring has to be enabled by using the room management system.
- Miracast for Android devices
- AirPlay for iOS devices
- Chromecast for Google Chrome
- vSolution Cast

6. BYOD

Cynap Pure is designed to make it as easy as possible for users to connect to it. Cynap Pure supports integrated mirroring protocols in its operating system. Users can connect to Cynap Pure without needing any additional software. The mobile platforms are AirPlay for iOS devices and Miracast for Android and Windows devices. Regarding laptop and computer operating systems, AirPlay is also supported for Mac OS X. Windows Intel Wireless Display is also supported, and this integrates natively with Windows 8.1.

AirPlay	Support for iOS 5.0 (released 2011) and above, or OS X 10.8 Mountain Lion (released 2012) and above. AirPlay is transmitted via Ethernet / WLAN. It can be used for displaying up to four sources.
Miracast	Miracast is based on a Wi-Fi direct connection. This means that Miracast can only be used in close proximity to Cynap Pure. Any used cabinet will reduce the possible transmission radius. High WLAN traffic in your environment may reduce the possible radius, increase the delay of picture transfer or results in reduced image quality (MICE support could help to increase the radius, the discovery beacon will be always sent by the dedicated built-in WLAN module. For more information, please refer to the manual.
vSolution App	The vSolution App allows controlling your Cynap Pure. 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. On Android, iOS and macOS, you can register your Cynap Pure manually when discovering services are blocked in your network (Bonjour, mDNS).
vSolution Cast (Windows)	In applications where a Wi-Fi direct connection is not possible due to the installation, multiple Windows devices can be connected at the same time using the alternative vSolution Cast.
Chromecast Screen Mirroring	Support for Chromecast capable devices. Chromecast is transmitted via Ethernet / WLAN. It can be used for displaying up to four sources.

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 Pure 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 rights, however with the restriction that no sound is transmitted.
Switching Cynap Pure to standby closes all connections.

7. User interface

Cynap Pure 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 Pure. 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 (optional). 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 Pure 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 App allows smartphones / tablets (iOS, Windows, Android) to control Cynap Pure directly via WLAN. More information about the vSolution App can be found on in the support section of our website www.wolfvision.com .

8. Hardware and OS

Cynap Pure 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 Pure. 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 Pure 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.

9. Administration

Cynap Pure can be managed using the vSolution Link software.
With vSolution Link software, administration tasks, like firmware updates, can be performed for multiple Cynap systems simultaneously. With this tool, you can also determine the state of you Cynap Pure system and sending a Wake-on-LAN (WoL) command. You can create, manage and distribute a settings profile to all Cynap systems using vSolution Link software, and you can change the background wallpaper easily.

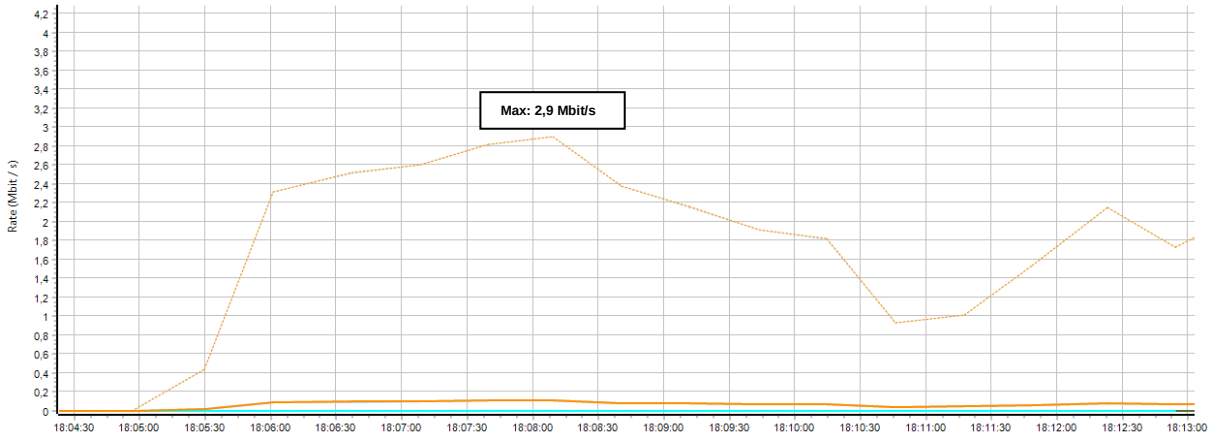
More information about vSolution Link software can be found in the support section of our website www.wolfvision.com.

10. Bandwidth Measurement Data

This bandwidth measurement data has been taken using a notebook PC with a Windows operating system. The computer was connected to Cynap Pure via WLAN, and was operating in network infrastructure mode.

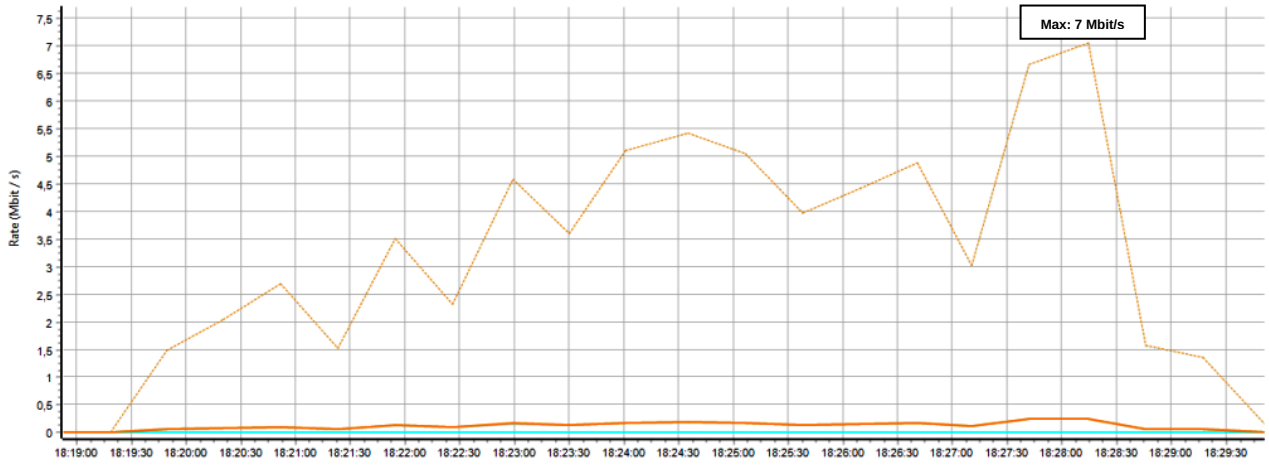
10.1. PowerPoint Presentation

Presentation with text and a few graphics are displayed from the notebook and are mirrored to Cynap Pure using vSolution Cast Software to a single connected client. (Traffic Out)



10.2. Multimedia from Notebook to Cynap Pure using vCast Software

1080p video (Big Buck Bunny) is displayed on the notebook and is mirrored using the vSolution Cast Software to a single connected client. (Traffic Out)



11. Client System Requirements

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
Microsoft Windows	8.1, 10 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 (Chromecast required)
Microsoft Windows	7, 8.1, 10 (Chromecast Browser Plugin required)

12. Index

Version	Date	Changes
1.0	13.03.2019	Created