WOLFVISION

Driving Knowledge Creation

Network Integration Guide: Cynap Pure Next Gen

Contents

Contents 2
1. Basics 5
1.1. Before starting 5
1.2. Attention 5
Guide 5
1.3. LAN / Ethernet settings 6
1.4. LAN / WLAN port 6
Hint - WLAN: 6
Optional Feature Pack 6
2. User Interface 7
3. Administration 8
4. Security 9
4.1. Admin password 9
4.2. Login Security 9
4.3. Network Security 9
4.4. LAN Security 9
4.5. WLAN (WiFi) Security 9
Hint 9
Security Settings 9
5. Network Integration Scenario 10
5.1. Network Segmentation and Security 10
5.2. Wired Connectivity 10
LAN 1 - Corporate Network 10
LAN 2 - Isolated Management Network or Visualizer connection 10
5.3. Wireless Connectivity 11
Infrastructure Mode 11
WLAN Access Point / Miracast (Wi-Fi Direct) / Bluetooth discovery (BLE) 11
6. Settings 13
6.1. LAN1 13
6.2. LAN 2 14
6.3. Access Point 15
6.4. Infrastructure (WLAN) 17
6.5. Host Name 19

6.6. Date and Time....20
6.7. FTP Client settings (with Feature Pack enabled)....21
6.8. Cloud Services (with Feature Pack enabled)....22
6.9. Network Drive (with Feature Pack enabled)....23
7. Services....24
7.1. Document and Media Player (with Feature Pack enabled)....24
7.2. Network Stream Input (with Feature Pack enabled)....25
7.3. Peripheral Control....27
8. BYOD....28
8.1. BYOD Screen Sharing....28
1.1. vSolution Cast (with Feature Pack enabled)....30
Firewall Rules....30
8.2. vSolution App....31
Firewall Rules....31
8.3. AirPlay (with Feature Pack enabled)....32
Firewall Rules....32
Steps to establish an AirPlay connection....32
8.4. Miracast (with Feature Pack enabled)....37
Firewall Rules....37
Steps to establish a Miracast connection....38
8.5. Chromecast (with Feature Pack enabled)....43
Firewall Rules....43
Steps to establish a Chromecast connection:....43
8.6. Differences of Open Mode and Protected Mode....48
Open Mode....48
Protected Mode....48
9. System Requirements....49
9.1. Third-Party Client-Device....49
Important....49
vSolution App....49
vSolution Link Pro....49
vSolution Cast....50
AirPlay Mirroring OS X Mountain Lion v10.8 (Release 2012) or later:....50
AirPlay Mirroring iOS 5.0 (Release 2011) or later:....50

Miracast 50
Chromecast 51
9.2. Firewall Rule - Full list 52
AirPlay (with Feature Pack enabled) 52
Miracast (with Feature Pack enabled) 52
Chromecast (with Feature Pack enabled) 53
Wake On LAN 53
FTP 53
SSH 53
HTTP, Cynap Pure (Next Gen) Control 54
HTTPS, Cynap Pure (Next Gen) Control 54
HTTPS, SSL, e.g. Cloud Service, Cynap control 54
Proxy 54
Network Drive (with Feature Pack enabled) 54
NTP, Time Server Client 54
PJLink 55
vSolution Cast (with Feature Pack enabled) 55
vSolution App 56
WebRTC 56
TLS Control 57
WebSocket 57
vSolution Link Pro 57
Zoom (with Feature Pack enabled) 58
1. Changelog 60

1. Basics

Cynap Pure (Next Gen) 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 (Next Gen). 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 (Next Gen) 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 VESA mount is included and a DC power supply is available as optional accessory.

1.1. 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 (Next Gen) can be integrated into the network.
When connecting Cynap Pure (Next Gen) to LAN and WLAN at the same time, please use different IP ranges in order to prevent address conflicts.
The listed IP addresses in this are only examples.
Cynap Pure (Next Gen) can be treated as a standard network device and it is as secure as the supporting network.
Cynap Pure (Next Gen) 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 Pure (Next Gen)´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 Pure (Next Gen) 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.

1.2. 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 Pure (Next Gen) 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 Pure (Next Gen) to an existing company network, some information from the local administrator is required.

1.3. 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 Pure (Next Gen) offers 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).

1.4. LAN / WLAN port

The LAN port enables integration of Cynap Pure (Next Gen) into an internal network. Administrators of a large number of Cynap Pure (Next Gen) 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 (Next Gen) 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 Pure (Next Gen) to standby closes all connections.

Optional Feature Pack
Activate the optional Cynap Pure Feature Pack to unlock the following features:

- File explorer with multimedia and document playback from cloud services, network drives, FTP servers, and USB storage devices
- WebConference services (WebRTC services, Zoom, and Microsoft Teams)
- Input sources (HDMI, USB UVC, and streaming sources)
- Annotation

For more details refer to Feature Pack

2. User Interface

Cynap Pure (Next Gen) 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 (Next Gen). 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 USB mouse&keyboard, or USB touch screen.
Cynap Pure (Next Gen) 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 application allows smartphones / tablets / PCs (iOS, Windows, Android) to control Cynap Pure (Next Gen) over the network, wired or wireless. More information about the vSolution Control App can be found on in the support section of our website www.wolfvision.com

3. Administration

Cynap Pure (Next Gen) can be managed using the vSolution Link Pro software.
With vSolution Link Pro software, administration tasks can be performed for multiple Cynap Pure (Next Gen) systems. With this admin tool, you can perform central firmware upgrades as well as determining the state of Cynap Pure (Next Gen) and Wake-on-LAN (WoL). You can also create, manage, and distribute a settings profile to all Cynap Pure (Next Gen) systems using vSolution Link Pro software.
More information about vSolution Link Pro software can be found in the support section of our website www.wolfvision.com.

4. Security

4.1. 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 Pure (Next Gen) at any time. The default password is “Password”. Remember to make a note of any changed passwords!

4.2. Login Security

Accessing Cynap Pure (Next Gen) 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.

4.3. Network Security

Accessing Cynap Pure (Next Gen) 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.

4.4. LAN Security

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

4.5. WLAN (WiFi) Security

When using wireless network, use encryption to maximize security.
Cynap Pure (Next Gen) complies with following standards:

- WPA2 / WPA 3 mixed
- WPA3

Hint

Miracast MS-MICE only works via a secure connection.
WPA2/WPA3 allows passwords with a length of 8 ~ 63 characters.
Use special characters carefully, not every thirdparty device can handle them.

Security Settings

To limit http/https access, and to disable the support of USB storage devices.

5. Network Integration Scenario

The following diagram illustrates a typical network integration scenario for a Cynap Pure (Next Gen) system. It shows how the device can simultaneously connect to a corporate network, an isolated management network, and wireless BYOD devices while maintaining strict network separation.
By default, all network interfaces are isolated from each other and no routing is performed between network segments. This separation enhances security and simplifies device administration. Optionally, HTTP/HTTPS routing can be enabled to allow connected wireless clients to access external network resources through the designated uplink interface.

5.1. Network Segmentation and Security

The architecture separates the following network domains:

- Corporate Network
- Guest Network
- Isolated Management Network
- Miracast P2P (Wi-Fi Direct) Connections

This segmentation helps maintain security while allowing flexible integration of collaboration devices, management systems, and wireless user devices.

5.2. Wired Connectivity

The Cynap Pure (Next Gen) provides two independent Ethernet interfaces that support flexible network integration while maintaining strict network separation.

LAN 1 - Corporate Network
LAN 1 serves as the primary connection to the corporate infrastructure. Typical use cases include access to:

- Corporate servers
- Enterprise applications
- User resources
- Internet connectivity
- Network time services (NTP) for automatic date and time synchronization

Access to a network time server ensures that the Cynap maintains accurate system time automatically. Correct time synchronization is important for authentication services, and network management, like network certificates.

This port supports Power over Ethernet Plus (PoE+) additionally, allowing the Cynap Pure (Next Gen) to be powered directly from a PoE+ capable network switch.
Corporate users connect through the organization's wired and wireless network infrastructure via the corporate access point.

LAN 2 - Isolated Management Network or Visualizer connection
LAN 2 is configured as a dedicated and fully isolated management network.
Typical use cases include:

- Device management

- Configuration
- Monitoring
- Firmware updates

OR

- Direct connection of a WolfVision Visualizer

5.3. Wireless Connectivity

The integrated wireless module supports two operating modes:

Infrastructure Mode

In Infrastructure mode, the Cynap Pure (Next Gen) connects to an existing wireless network, such as a guest Wi-Fi (WLAN). This allows wireless BYOD devices to access the system through the organization's wireless infrastructure.

Typical characteristics:

- Uses an existing access point
- Supports guest network integration
- Enables wireless collaboration without additional cabling

WLAN Access Point / Miracast (Wi-Fi Direct) / Bluetooth discovery (BLE)

The Cynap Pure (Next Gen) can also provide its own wireless connectivity for BYOD devices.

Supported connection methods:

- WLAN Access Point (AP) mode
- Miracast P2P (Wi-Fi Direct)
- Features device discovery

This enables users to connect directly to the system without requiring access to the corporate or guest wireless network.

Additionally,

Please note

This integrated wireless module not only provides WLAN connectivity but also broadcasts the wireless beacons required for Miracast operation. This includes support for both Miracast connection methods: Wi-Fi Direct (P2P) and Miracast over Infrastructure (MS-MICE).

Optionally, the module can also transmit Bluetooth Low Energy (BLE) beacons to support vSolution App device discovery and Apple AirPlay connectivity. These beacon services simplify device discovery and connection establishment, particularly in network environments where standard discovery protocols are restricted or blocked.

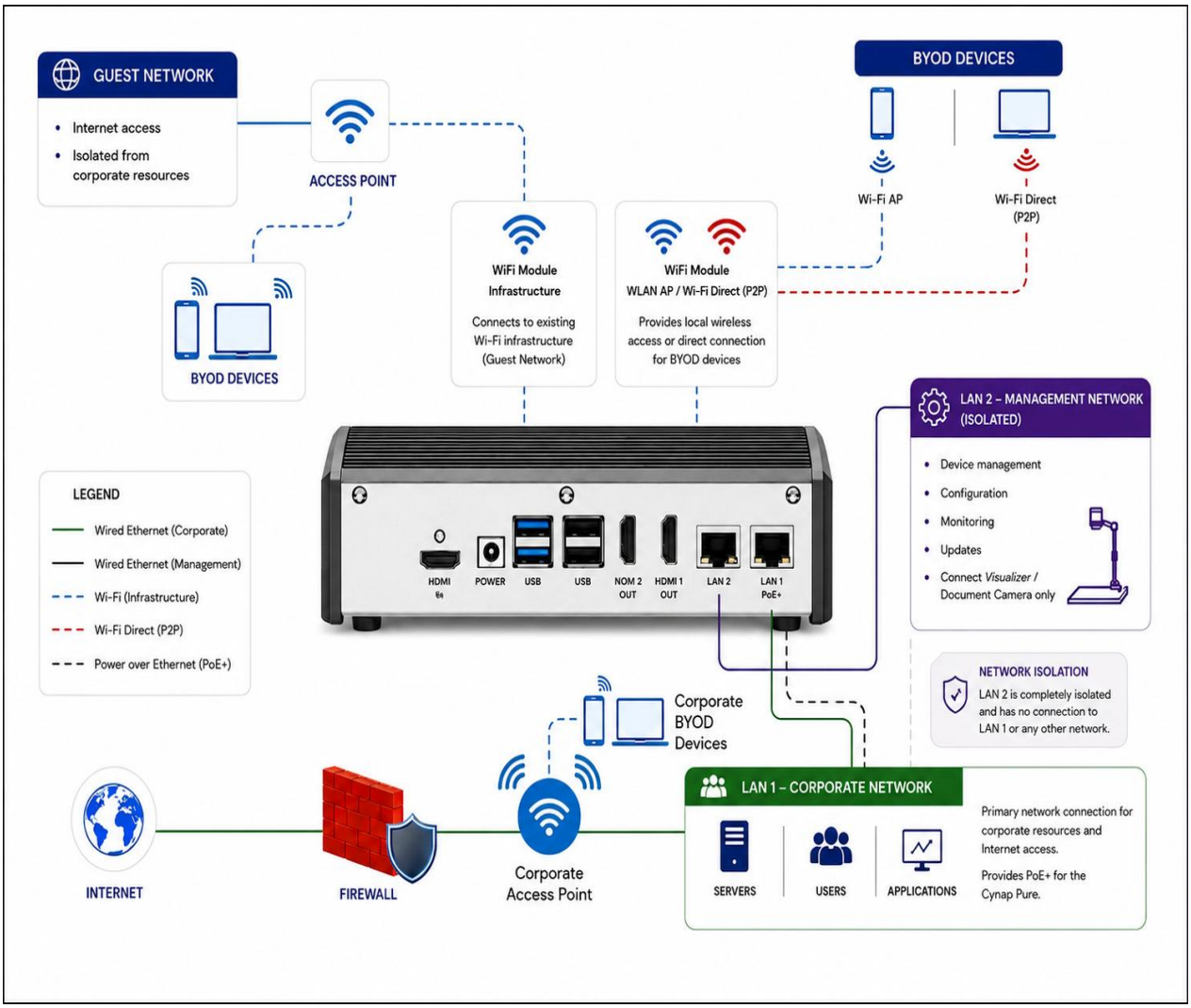
The corresponding settings are available in the General and Mirroring sections of the Cynap Pure (Next Gen)'s settings.

Guest Network Integration

BYOD devices connected to the guest network can communicate with the Cynap Pure (Next Gen) through the wireless infrastructure while remaining separated from the corporate network.

The Cynap Pure (Next Gen) can optionally perform HTTP/HTTPS routing between the wireless network and the network interface designated as the primary uplink (Priority 1). This enables connected wireless clients to access external network resources, including corporate services and Internet-based HTTP/HTTPS applications.

For increased security, Client Isolation can be enabled. With Client Isolation active, communication between wireless clients associated with the access point is blocked, while communication with the Cynap and routed network services remains available. This prevents direct device-to-device communication between connected clients and helps maintain network segmentation.



Please note

To fully integrate a Visualizer, configure LAN 2 for "Visualizer" mode. In this mode, the Cynap Pure (Next Gen) acts as a DHCP server and automatically assigns an IP address to the Visualizer.

Do not power the Cynap Pure (Next Gen) via PoE+ and DC simultaneously.

6. Settings

6.1. LAN1

The following list shows the available settings:

Setting	Notes
Priority Interface Access	The higher prioritized interface (value = 1) will be used for network service first. Ensure that the value is different from the other LAN and from WLAN Infrastructure interface priority.
DHCP	Cynap Pure (Next Gen) 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 (Next Gen) 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 (Next Gen) is directly connected only to a PC, then enter the IP address of the PC.
Name server 1	Input the IP address of the preferred Domain Name System (DNS). This Server translates domain names into corresponding IP addresses.
Name server 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 (Next Gen) 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-----“

6.2. LAN 2

The following list shows the available settings:

Setting	Notes
Priority Interface Access	The higher prioritized interface (value = 1) will be used for network service first. Ensure that the value is different from the other LAN and from WLAN Infrastructure interface priority.
DHCP	Cynap Pure (Next Gen) 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 (Next Gen) 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 (Next Gen) is directly connected only to a PC, then enter the IP address of the PC.
Name server 1	Input the IP address of the preferred Domain Name System (DNS). This Server translates domain names into corresponding IP addresses.
Name server 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 (Next Gen) 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-----“

6.3. Access Point

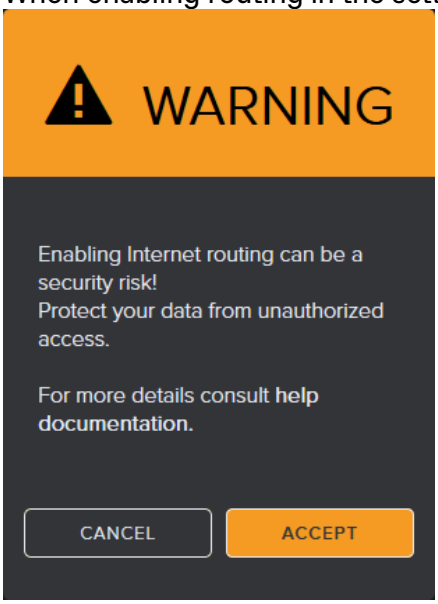
The following list shows the available settings:

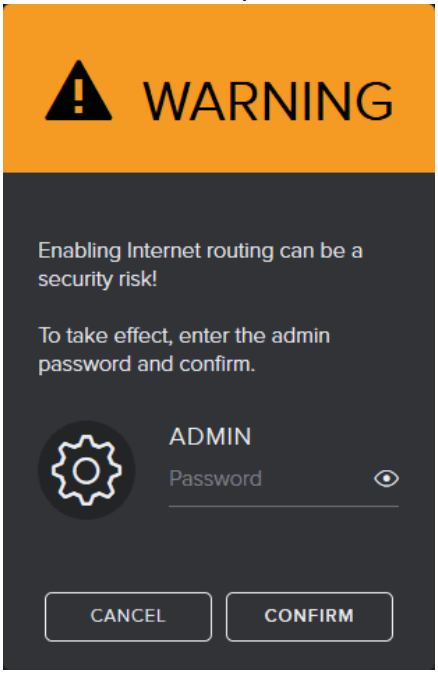
WARNING
By default, Cynap Pure (Next Gen) does not act as router or gateway and only serves up a “Cynap closed” network that will not connect to the internet even if the LAN port is connected to the internet.
Enabling Internet Routing could be a security risk!
Protect your data from unauthorized access.

Setting	Notes
OFF / Access Point	Enable/Disable access point.
MAC Address	Indicates the MAC address of the built-in access point. This field cannot be changed.
Enable Routing	Enable ROUTING to allow HTTP/HTTPS routing through LAN interface. WARNING, this settings could be a security risk. The administrator password needs to be entered again for confirmation.
Country	Select the country where the system is being operated.
Band	The Cynap Pure (Next Gen) uses the 2.4GHz, 5 GHz, or 6GHz frequency band.
Bandwidth	Bandwidth, select the desired bandwidth of the WLAN channel. The used bandwidth can be set to 20 MHz, 40 MHz, or 80 MHz. Higher WLAN bandwidth increases throughput but also increases susceptibility to interference and instability.
Client Isolation	Prevents communication between connected clients.
SSID Auto	Auto-generated SSID exists of "Cynap-Pure-" and the serial number of this particular device.
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 • _-:$& ()
Security	Select the desired security algorithm, None, WPA2, WPA 2/WPA3 mixed, WPA3.
Password	Password, input the WPA2 / WPA 3 password. This password needs the client to connect to this access point.
IP address	Unique address in the network, i.e. 192.168.0.100. The IP address of Cynap Pure

	(Next Gen) 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
Channel	Select the desired channel for wireless traffic (non-overlapping channels are listed only to ensure max. throughput). The available channels are depending on the selected region and band. Selecting a DFS channel may delay AP startup by several minutes and automatically disables Miracast in the backend, since DFS-related radar detection and channel switching can interrupt unstable Wi-Fi Direct/Miracast connections.
Maximum Number of Clients	For security reasons, the number of clients can be reduced (max. 15 ~ 1 clients).

Please note
When enabling routing in the settings, the administrator password needs to be entered again.





6.4. Infrastructure (WLAN)

The following list shows the available settings:

Setting	Notes
OFF / Infrastructure	Enable/Disable Infrastructure Mode.
Access Point list	Scans the WLAN environment for available access point to connect.
MAC Address	Indicates the MAC address of the built-in access point. This field cannot be changed.
Priority Interface Access	The higher prioritized interface (value = 1) will be used for network service first. Ensure that the value is different from the other LAN interfaces priority.
Use BSSID	Toggles between SSID and BSSID mode. With BSSID (Basic Service Set Identification), the used access point will be fixed and Cynap Pure (Next Gen) 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.
Band	By default, Cynap Pure (Next Gen) 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.
Country	Select the country where the system is being operated.
Security	Defines encryption for safe network traffic. All connected units must use the same algorithm (None, WPA2/WPA3 mixed, WPA3).
Signal Level Limit (dBm)	Defines when Cynap Pure (Next Gen) starts 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).
Password	Enter the password for your WLAN infrastructure. Available with enabled Security.
IP address	Unique address in the network, i.e. 192.168.0.100. The IP address of Cynap

	Pure (Next Gen) 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 (Next Gen) is directly connected only to a PC, then enter the IP address of the PC.
Name server 1	Input the IP address of the preferred Domain Name System (DNS). This Server translates domain names into corresponding IP addresses.
Name server 2	Input the IP address of the preferred Domain Name System (DNS). This Server translates domain names into corresponding IP addresses.
Signal Level	Shows the current strength of the WLAN signal in dBm.
Reconnect Counter (Connection Loss)	Counts every lookup then the measured signal falls below the user defined signal level limit.
Reconnect Counter (Low Signal Level)	Counts every lookup then the measured signal falls below the user defined signal level limit.

6.5. Host Name

Define a host name (box name), allowing easy identification of your Cynap Pure (Next Gen) in the local network, e.g. number of the classroom.
It can be changed in the 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.

Important
Keep the name as short as possible and don't use "." to prevent misinterpreting the suffix as domain.
In Miracast MS-MICE environments "." are not allowed at all.

6.6. Date and Time

Adjust time and date.

Important
Accurate time and date settings are mandatory. Wrong setting will result in refused certificates.

Setting	Notes
Time Server	Cynap Pure (Next Gen) 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 (Next Gen) can be synchronized to an external time server. Enable Time server and input a valid URL or IP address of a NTP time server.
Time Format	Select the format you prefer. DDMMYYY/24H MMDDYYYY/12H
Time Zone	Select the time zone from the dropdown list where the system is being operated.

6.7. FTP Client settings (with Feature Pack enabled)

To access your FTP server with the file explorer of your Cynap Pure (Next Gen), enable this feature and enter valid credentials.

Setting	Notes
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 to your FTP server settings.
Password	Input the password according to your FTP server settings.
Test it now	During the test, Cynap Pure (Next Gen), will upload a text file onto the FTP-server (“Cynap Pure.txt” without content)

6.8. Cloud Services (with Feature Pack enabled)

Cynap Pure (Next Gen) 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.

6.9. Network Drive (with Feature Pack enabled)

Cynap Pure (Next Gen) allows direct access to network drives (write-access 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.

7. Services

7.1. Document and Media Player (with Feature Pack enabled)

Cynap Pure (Next Gen) can present almost all commonly used document and video file formats. This functionality is built into Cynap Pure (Next Gen) and no additional applications need to be installed.
Cynap Pure (Next Gen) also supports different storage media for presentation of documents and videos.
The following storage media are available for Cynap Pure (Next Gen).

- Internal storage
- USB flash drive
- Network Drive
- Cloud services
- Online Office documents

The following media formats are supported:

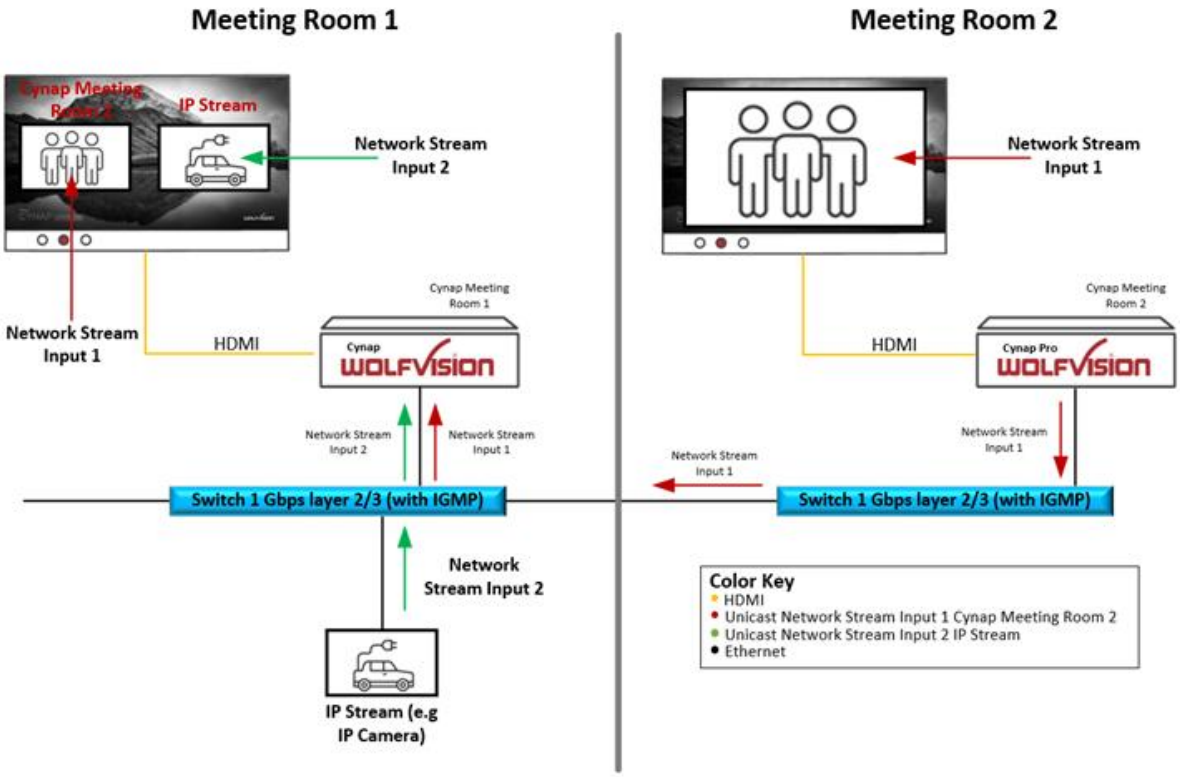
- Supported pictures file formats: GIF, JPEG, BMP, PNG
- Supported video file formats: AVI, WMV, MOV, MP4, DivX, MKV, M4V, OGV
- Supported document file formats: PDF, Word, PowerPoint, Excel
- Supported audio file formats: MP3, MKA, OGA, OGG, WMA

7.2. Network Stream Input (with Feature Pack enabled)

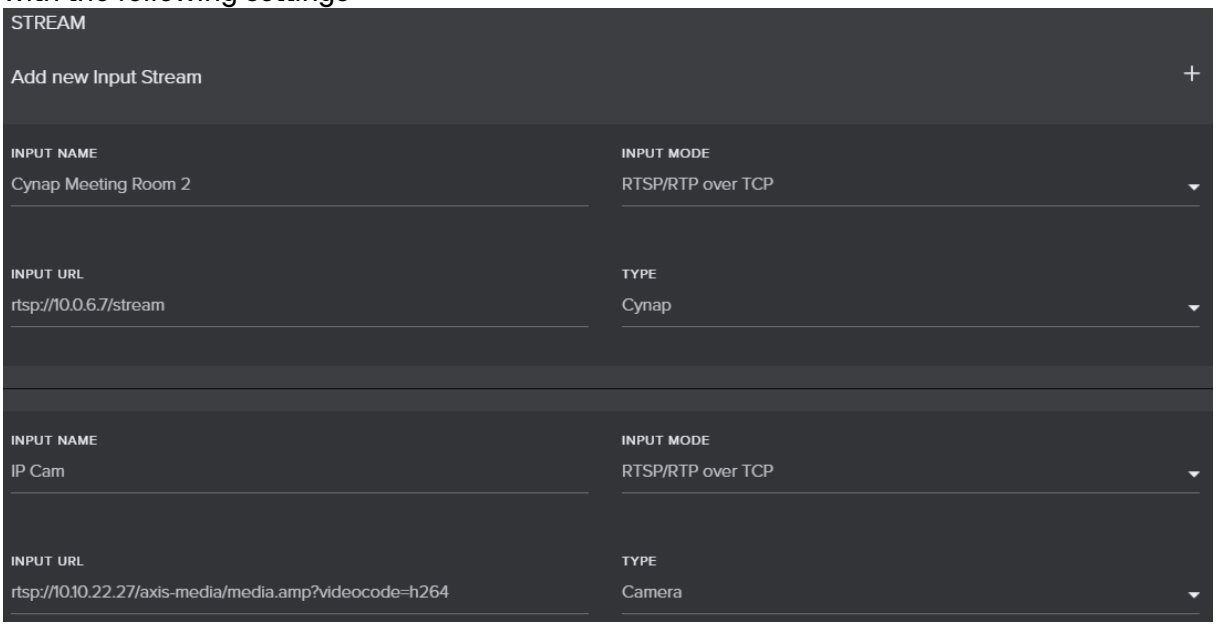
Cynap Pure (Next Gen) has a built-in streaming client which is capable of receiving broadcast video content over the network.
Up to 20 Stream sources can be defined and individually named in the GUI settings (Input).

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 at the Cynap Pure (Next Gen) “Meeting Room1” with two sources, one from a WolfVision Cynap Pro “Meeting Room 2” and one from an IP Camera.



At the Cynap Pure (Next Gen) “Meeting Room 1” two network stream inputs are configured with the following settings:



After saving configuration the two new 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.

7.3. Peripheral Control

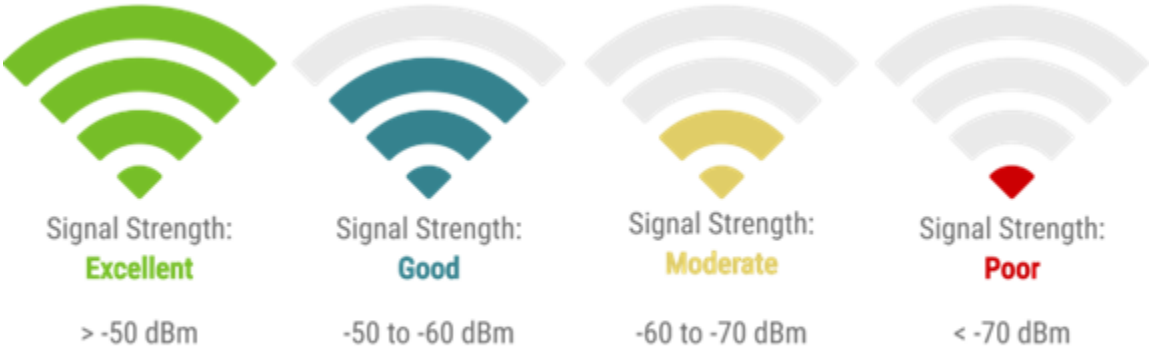
Cynap Pure (Next Gen) is able to send up to 20 commands to connected network devices, e.g. to fully power up the connected projector. This feature will be triggered by power events of Cynap Pure (Next Gen).
The peripheral devices, like projectors, monitor, lighting, windows shades, etc. need to be in the same network as Cynap Pure (Next Gen).

Function	Description
Command enable	Enable / disable certain commands (entered command settings will be not deleted
Event	To define at which power state of Cynap Pure (Next Gen) the command will be sent (Power ON or Power OFF). Select event None to delete this entry.
Delay Sensing Command	Allows sending the command delayed.
Name	To give the command an individual name (like “projector”)
Description	To give the command a detailed description (like “power up”)
Protocol	Defines the network protocol used (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.

8. BYOD

8.1. BYOD Screen Sharing

Cynap Pure (Next Gen) is designed to make it as easy as possible for users to connect to it. Cynap Pure (Next Gen) 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 Pure (Next Gen) to share to a big display device.



Please refer to respective manufacturer to get detailed information regarding 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 (minumum 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

Encryption
TLS encryption

1.1. vSolution Cast (with Feature Pack enabled)

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, the IP address of a Cynap system 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 Pure (Next Gen) to standby closes all connections.

Firewall Rules

Function / Application	Port	Type	Inbound / Outbound	Description
Discovery Multicast	50000	UDP	Inbound	This port is used for device discovery all available Cynap 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 and / or Visualizer. If this port is blocked, secure communication to Cynap 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 stream are possible.
Touchback	50922	TCP	Outbound	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 is not possible

8.2. vSolution App

The vSolution App allows controlling your Cynap Pure (Next Gen). 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 Pure (Next Gen) manually when discovering services are blocked in your network (Bonjour, mDNS).

Firewall Rules

Function / Application	Port	Type	Inbound / Outbound	Description
Discovery Multicast	50000	UDP	Inbound	This port is used for device discovery all available Cynap 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 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 web for secure connect to the Cynap 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
For control purposes	50917	TCP	Inbound	This port is for secure communication between WolfVision applications (e.g., vSolution App) to Cynap and / or Visualizer. If this port is blocked, secure communication to Cynap and / or Visualizer, inclusive firmware updates are blocked
For control purposes	50921	TCP	Inbound	Video streams between WolfVision App to Cynap and Visualizer. If this port is blocked, no streams are possible
For control purposes	50922	TCP	Outbound	This port is for touchback between Cynap and WolfVision App vSolution Cast to send mouse events back to the computer. If this port is blocked, bi-directional inputs is not possible. (Windows and macOS only)

8.3. AirPlay (with Feature Pack enabled)

It is recommended to use the latest versions of iOS, iPadOS, and macOS (outdated systems may not be supported).
AirPlay is transmitted via LAN and/or WLAN. It can be used for displaying up to four sources.

Firewall Rules

Using mDNS for Device Discovery

Function / Application	Port	Type	Inbound / Outbound	Description
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.

Using Bluetooth for Device Discovery
Verify that Bluetooth has been enabled on your Apple device.

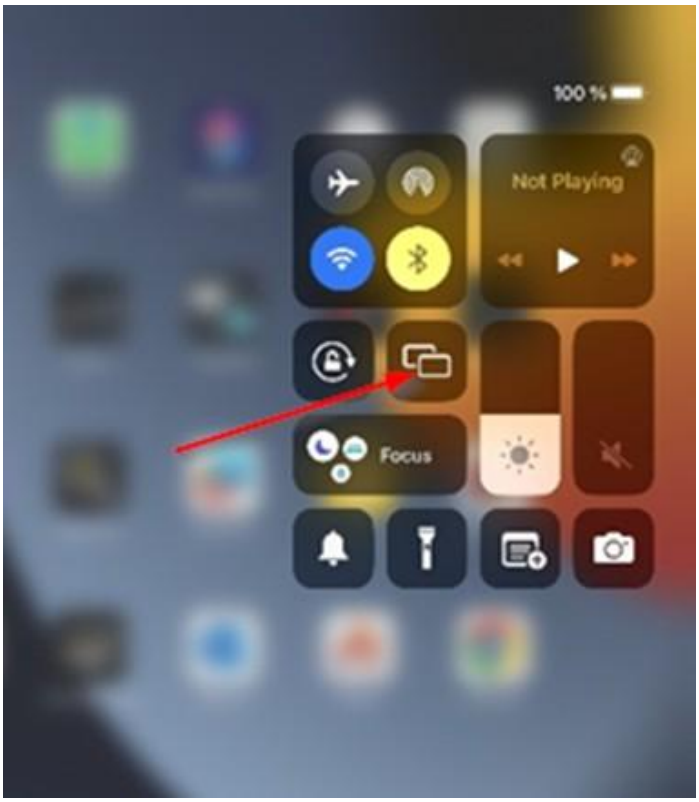
Function / Application	Port	Type	Inbound / Outbound	Description
Audio	4100 ~ 4164	TCP UDP	Inbound	Audio for AirPlay.
AirPlay	5000	TCP	Inbound	AirPlay communication with legacy devices.
AirPlay	7000	TCP	Inbound	Primary AirPlay communication.
Video	7100	TCP	Inbound	AirPlay video communication.
Audio	47000	TCP	Inbound	AirPlay audio communication.

Steps to establish an AirPlay connection

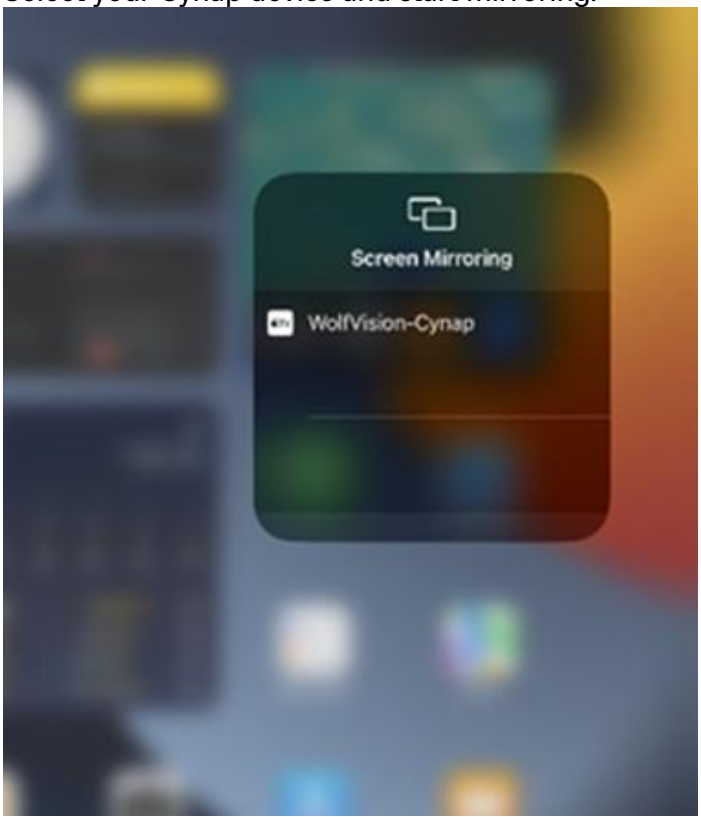
iPhone, iPad
Screenshots taken on iPadOS 17.5, other versions and models may vary.

1. Connect to WLAN (Wi-Fi)
Make sure your Apple device and the Cynap Pure (Next Gen) 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.



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

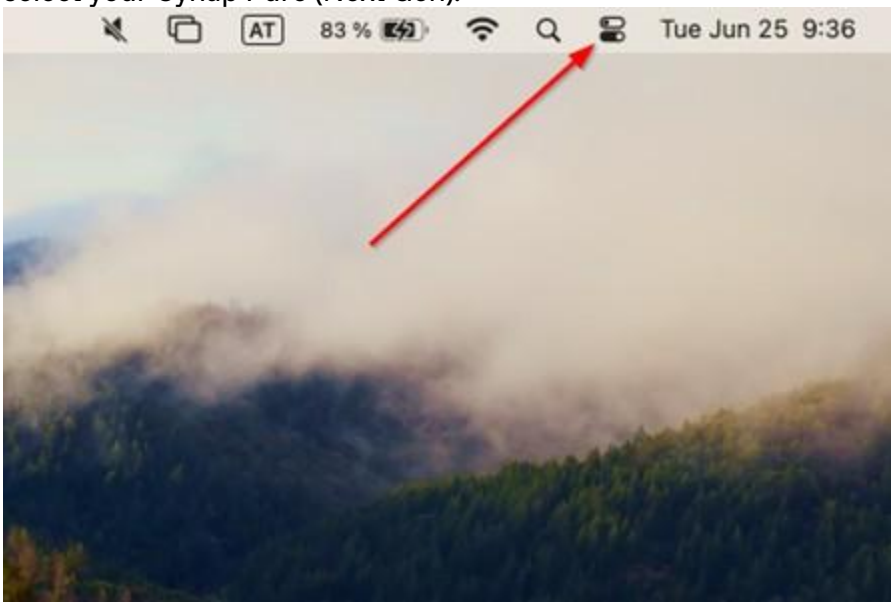


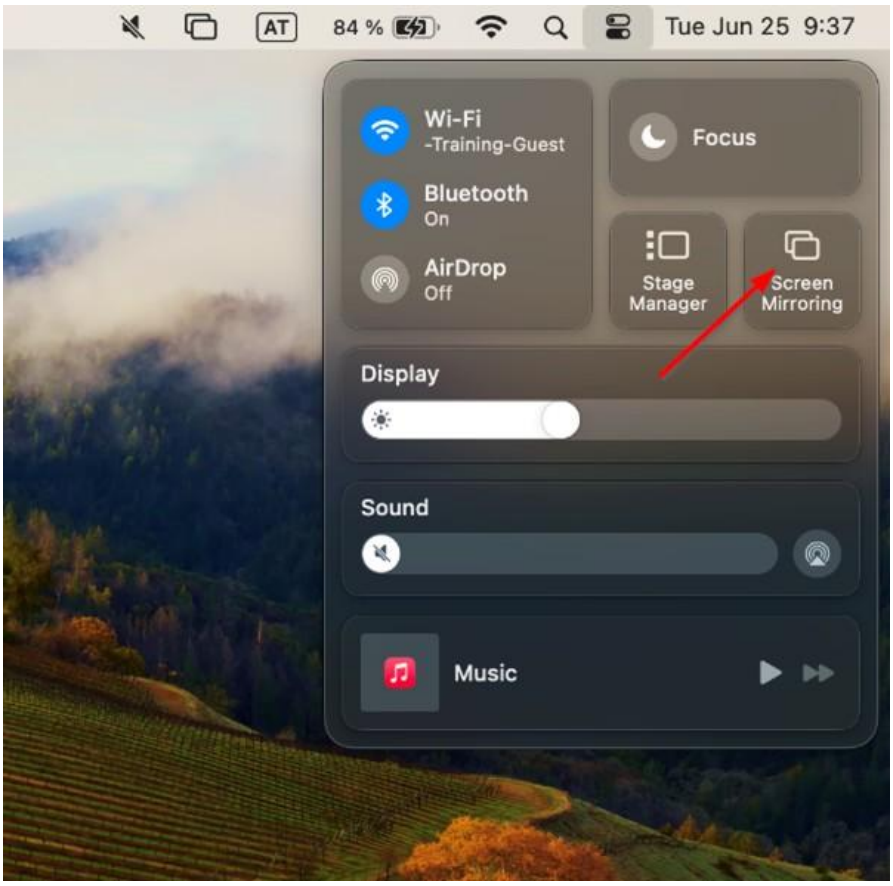
4. Security (Optional)
Enter PIN, if configured.

MacOS
Screenshot taken on MacOS Sonoma 14.5, other versions and models may vary.

1. Connect to WLAN (Wi-Fi)
Ensure both your Mac and the Cynap Pure (Next Gen) system are on the same network (WLAN or LAN)

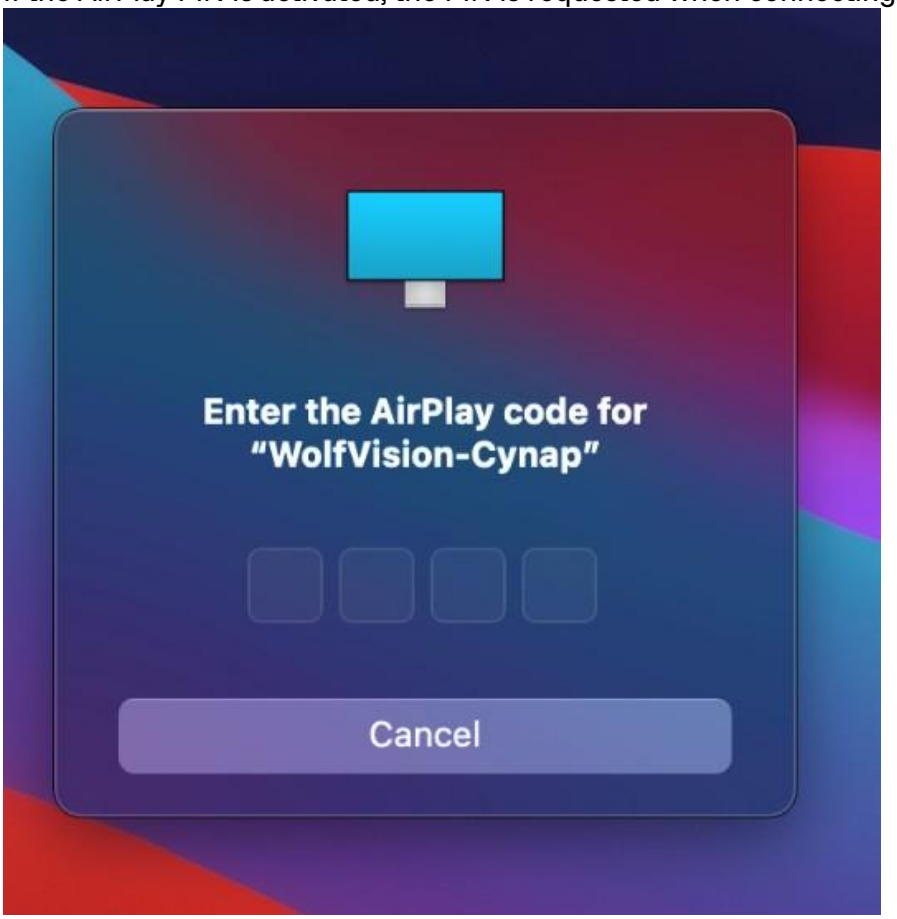
2. Open Control Center
Click on the "Control Center" icon in the menu bar, click on the "Screen Mirroring" icon and select your Cynap Pure (Next Gen).





3. Start mirroring
Your Mac's display will now be mirrored on your Cynap Pure (Next Gen) system.

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



8.4. Miracast (with Feature Pack enabled)

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 Pure (Next Gen) 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 Pure (Next Gen) 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.

Firewall Rules

Function / Application	Port	Type	Inbound / Outbound	Description
Multicast DNS (mDNS)	5353	UDP	Inbound	Multicast DNS (mDNS 224.0.0.251).
DHCP	67 / 68	UDP	Inbound	DHCP communication between device, receiver, and DHCP server.
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	7250	TCP	Inbound	Control port on which Cynap family system listen

Control				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	UCP	Inbound	Hardware cursor to reduce latency when using touchback.

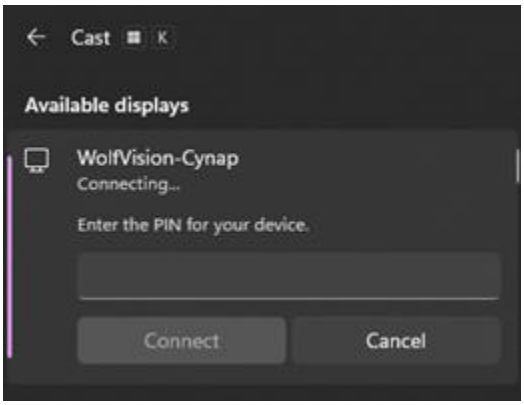
Steps to establish a Miracast connection

Windows 11
Screenshot taken on Windows 11 Version 23H2, other versions and models may vary.

1. Press the Windows Key + K
To bring up a side panel.

2. Select your Cynap system
Check the list and connect to the desired receiver.

3. Security (Optional)
If the Miracast PIN is activated, the PIN is requested when connecting.



Please note:
Windows devices are caching the PIN. To force requirement of a new PIN, start a "New Presentation", the Windows device that has established a connection to the Cynap before, must enter a new PIN.

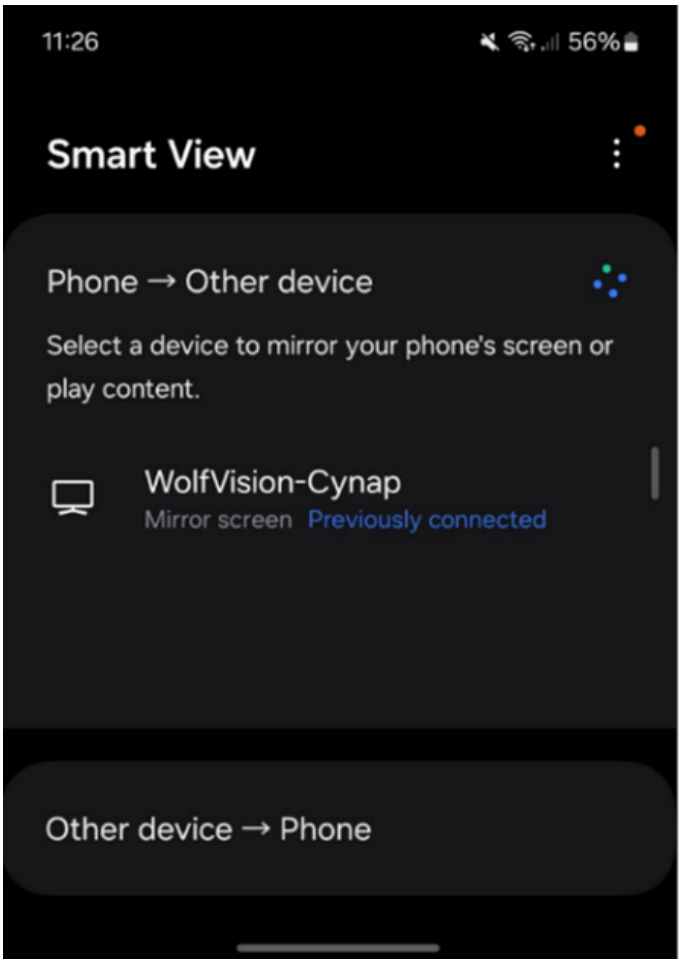
Android (Miracast P2P)
Android devices are not supporting Miracast MS-MICE.
Miracast P2P is not supported by every Android device, consult documentation of your third-party Android device, use Chromecast, or vSolution App alternatively.
Do not connect to the same WiFi when the Android device used is supporting Miracast and you want to use Miracast P2P.
Screenshots taken on Samsung S21 FE, Android 14, other versions and models may vary.

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

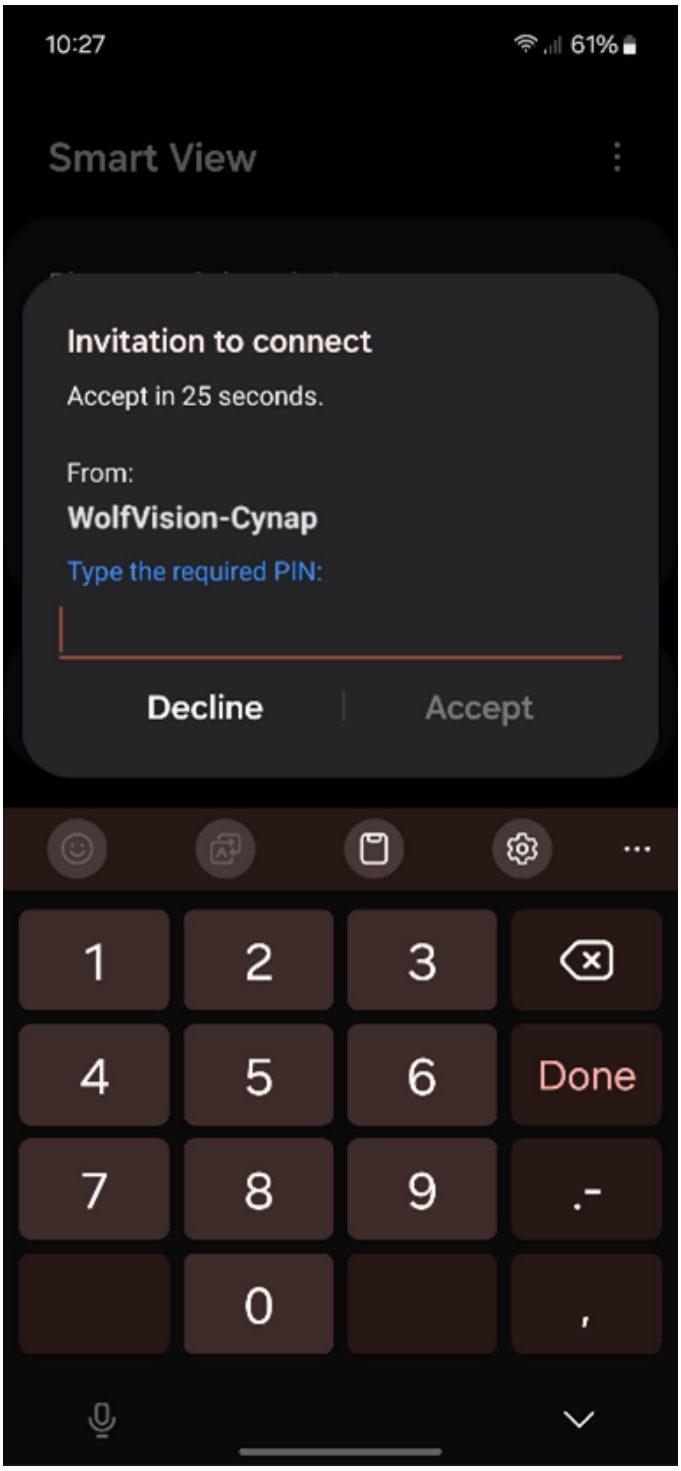
2. Open the control center on your Android Phone
Swipe down from the top of your screen to open the control panel.

3. Find and Tap on Cast:
Some phones and tablets list this feature as “Screen Mirroring”, “Smart View,” “Wireless Display”, etc. - check the documentation of your Android device.
You might need to navigate through additional menus such as Connection preferences or More connection settings to find the mirroring feature.

4. Select your Cynap system
Check the list and connect to the desired receiver.



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


10:27
61%
Smart View
Invitation to connect
Accept in 25 seconds.
From:
WolfVision-Cynap
Type the required PIN:
Decline
Accept
1
2
3
4
5
6
Done
7
8
9
.-
0
,

8.5. Chromecast (with Feature Pack enabled)

Support for Chromecast capable devices. Chromecast is transmitted via LAN and/or WLAN.
It can be used for displaying up to four sources.

Important
Chromecast requires internet access, allow Cynap Pure (Next Gen) accessing the internet.

Firewall Rules

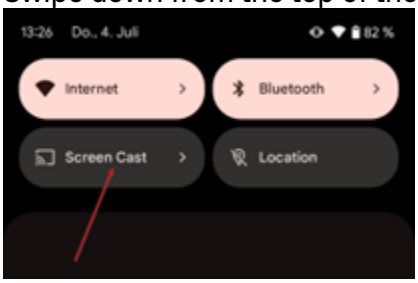
Function / Application	Port	Type	Inbound / Outbound	Description
Multicast DNS (mDNS)	5353	UDP	Inbound Outbound	Multicast DNS (mDNS 224.0.0.251).
Discovery	1900	UDP	Inbound	Chromecast discovery.
Audio	4100 ~ 4164	TCP UDP	Inbound	Audio for Chromecast.
Chromecast	8008	TCP	Inbound	Primary Chromecast communication.
Chromecast	8009	TCP	Inbound	Communication Chromecast.
Video data stream	1 ~ 65535	UDP	Inbound Outbound	Chromecast (video data stream).

Steps to establish a Chromecast connection:

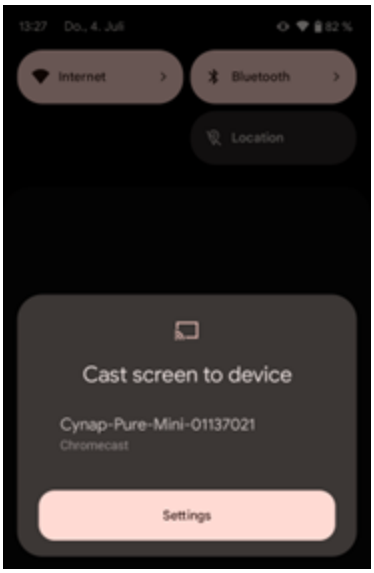
Google Pixel:
Screenshot taken on Google Pixel 6a, Android 15, other versions and models may vary.

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.



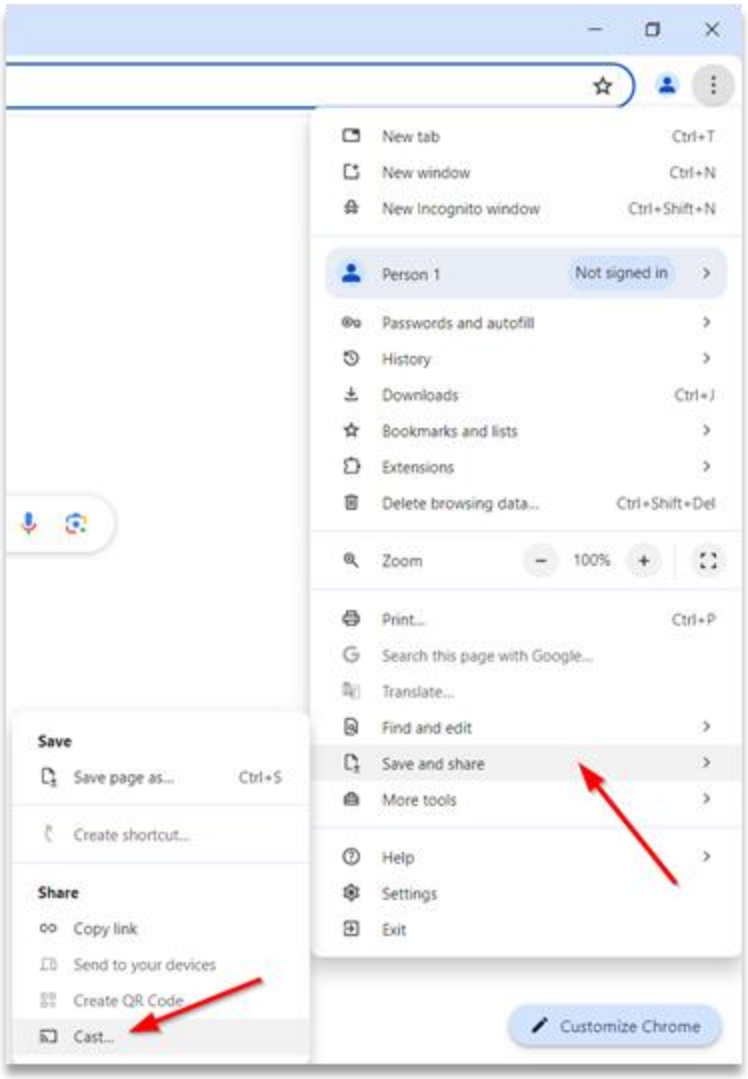
3. Tap Screen Cast:
Select your Cynap system and start mirroring. Choose between mirroring a single app or the entire screen.



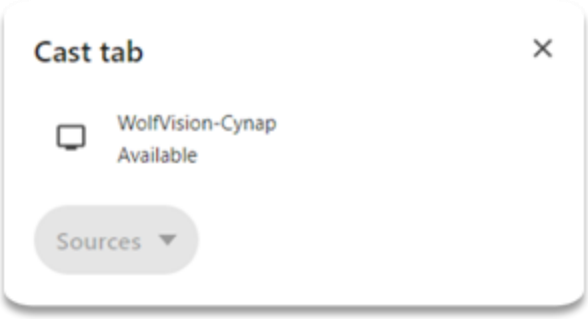
Google Chrome:
Screenshot taken on Chrome Version 126.0.6478.127, other versions and models may vary.

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…”



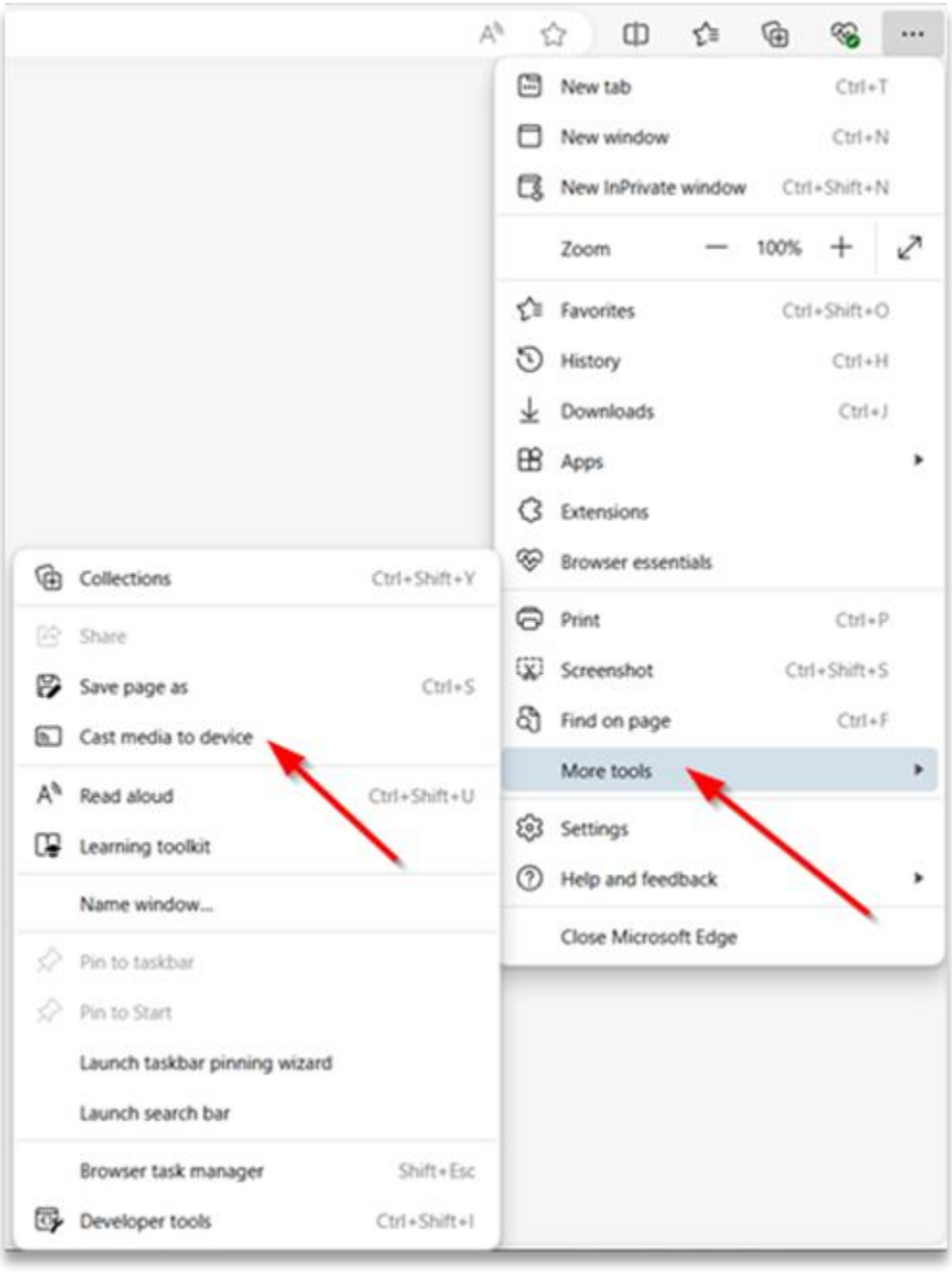
3. Select your Cynap system:
In the Cast menu, select the Cynap system you want to cast to.



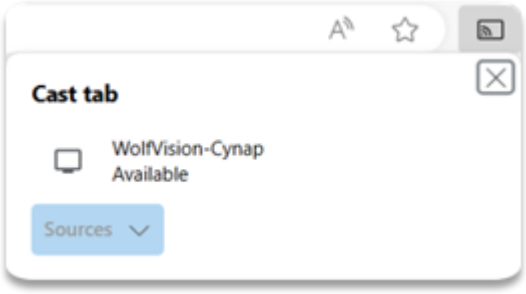
Microsoft Edge:
Screenshot taken on Edge Version 126.0.2592.87, other versions and models may vary.

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”.



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



8.6. Differences of Open Mode and Protected Mode

When using Cynap Pure (Next Gen), it is possible to choose between either open mode or protected mode.
This different mode can be selected in the settings.

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 the Cynap Pure (Next Gen).
In Open Mode, PIN can be enabled for Airplay, Miracast, and vSolution App vSolution Cast to prevent disturbance of extern devices. The PIN will be shown on the connected HDMI display only.

Protected Mode
Protected Mode prevents unauthorized or unintended mirroring connections.
When Protected Mode is enabled, connection approval must be initiated manually on the Cynap Pure (Next Gen) before a third-party device can connect. Once approval has been granted, a connection window is opened for the configured period of time.
During this connection window, only one third-party device is permitted to establish a mirroring connection. After a device has connected or the time window has expired, no further devices can connect until connection approval is initiated again.
Protected Mode does not support PIN-based authentication.

9. System Requirements

9.1. Third-Party Client-Device

Important
These requirements represent the absolute minimum supported configuration from a technical perspective.
Support, functionality, and performance on outdated systems cannot be guaranteed.
Outdated devices, operating systems, drivers, firmware (including BIOS), or network infrastructure may cause performance degradation, instability, feature limitations, or compatibility issues.
To ensure optimal performance, maximum compatibility, and compliance with current security standards, all devices, software components, drivers, firmware (including BIOS), and infrastructure must be kept up to date.
Customers are responsible for verifying compatibility, supported software versions, service requirements, and End-of-Life (EoL) status of all third-party products and services by consulting the respective vendor documentation.

Systems containing unsupported or End-of-Life components may expose the entire environment to unacceptable security risks and are therefore strongly discouraged.
Issues resulting from the use of outdated, unsupported, or End-of-Life devices, operating systems, drivers, firmware, or infrastructure components do not constitute a product defect and do not qualify as a valid basis for complaints, warranty claims, or support escalation requests.
Please note
The achievable system performance and user experience are dependent on the capabilities of the connected third-party devices and infrastructure. Devices with limited processing power, memory, network bandwidth, or hardware acceleration capabilities may not be able to deliver the same level of performance as current, adequately sized hardware platforms.

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

Please Note
The BYOD feature is not available on iOS/iPadOS-based devices.

vSolution Link Pro
For 24/7 use, installation on IIS server is strongly recommended.

Product	Version
Windows	Windows 11 x64 (running on officially supported hardware) 4GB RAM 10GB minimum free disk space for firmware files.
macOS	macOS 10.15 4GB RAM 10GB minimum free disk space for firmware files.

vSolution Cast

Product	Version
Windows	Windows 7 Old hardware may not offer sufficient performance.

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	Mid 2011 or later
Mac Pro	Late 2013 or later

AirPlay Mirroring iOS 5.0 (Release 2011) or later:

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

Miracast

Product	Version
Android	4.4.2 or later Hardware with Miracast support required.
Windows PC	8.1 or later Hardware with Miracast support required.
Windows Phone	8.1 or later
Blackberry	10.2.1 or later

Chromecast

Product	Version
Android	4.0.3 or later Hardware with Chromecast support required.
Windows and other OSs	Chromecast capable browser Plugin may required

9.2. Firewall Rule - Full list

Ensure that all necessary ports, services and IP addresses are available and not blocked by your firewall (external and personal). Acknowledgements (''ACKs'') of TCP packets are not considered in the following table in order to be able to illustrate the direction of the data packets. Since acknowledgements are usually sent back via the same TCP port, the other direction shall not be blocked to ensure smooth functioning.
Additional firewall rules maybe necessary due to your specific local network infrastructure. Consult the relevant documentation on your network infrastructure.

AirPlay (with Feature Pack enabled)

Using mDNS for Device Discovery

Function / Application	Port	Type	Inbound / Outbound	Description
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.

Using Bluetooth for Device Discovery
Verify that Bluetooth has been enabled on your Apple device.

Function / Application	Port	Type	Inbound / Outbound	Description
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.

Miracast (with Feature Pack enabled)

Function / Application	Port	Type	Inbound / Outbound	Description
Multicast DNS (mDNS)	5353	UDP	Inbound	Multicast DNS (mDNS 224.0.0.251).
DHCP	67 / 68	UDP	Inbound	DHCP communication between device, receiver, and DHCP server.
RTP Stream	19000 ~ 19007	UDP	Inbound	RTP media traffic port for delivering audio and video.

	19010 ~ 19017			
RTSP Control	7236	TCP	Outbound	RTSP control port is used to establish and manage session.
MS-MICE Control	7250	TCP	Inbound	Control port on which the Cynap Pure (Next Gen) 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 Pure (Next Gen) and Windows computer. If this port is blocked, bi-directional inputs is not possible.
Hardware Cursor extension	19020 ~ 19027 19030 ~19037	UCP	Inbound	Hardware cursor to reduce latency when using touchback.

Chromecast (with Feature Pack enabled)

Function / Application	Port	Type	Inbound / Outbound	Description
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).

Wake On LAN

Function / Application	Port	Type	Inbound / Outbound	Description
Powering the unit on	7 / 9	UDP	Inbound Outbound	Usually port 7 is used for sending the magic packet.

FTP

Function / Application	Port	Type	Inbound / Outbound	Description
FTP connection	21	TCP	Outbound	Connection to FTP server

SSH

Function /	Port	Type	Inbound /	Description

Application			Outbound	
SSH Connection	22	UDP	Inbound Outbound	Access for Wolfvision support

HTTP, Cynap Pure (Next Gen) Control

Function / Application	Port	Type	Inbound / Outbound	Description
http, control	80	TCP	Inbound	This port used to connect to the Cynap Pure (Next Gen) web interface (httpd). If this port is blocked, no connection can be made.

HTTPS, Cynap Pure (Next Gen) Control

Function / Application	Port	Type	Inbound / Outbound	Description
https, TLS control	443	TCP	Inbound	This port used to connect to Cynap Pure (Next Gen) web interface (https). If this port is blocked, no connection can be made.

HTTPS, SSL, e.g. Cloud Service, Cynap control

Function / Application	Port	Type	Inbound / Outbound	Description
https, SSL, e.g. Cloud Service, Cynap control	443	TCP / UDP	Inbound Outbound	This port is used for cloud services and for secure connection to Cynap Pure (Next Gen) web interface. If this port is blocked, no connection can be made.

Proxy

Function / Application	Port	Type	Inbound / Outbound	Description
Proxy	8080	TCP	Inbound	Default port proxy function (This port can be changed in the Proxy settings).

Network Drive (with Feature Pack enabled)

Function / Application	Port	Type	Inbound / Outbound	Description
NFS	111 / 2049	TCP / UDP	Outbound	Connection to network drives
CIFS	137 / 139	TCP / UDP	Outbound	Connection to network drives.

NTP, Time Server Client

Function /	Port	Type	Inbound /	Description

Application			Outbound	
NTP	123	UDP	Outbound	For automated time synchronization by a time server (Network Time Protocol, NTP)

PJLink

Function / Application	Port	Type	Inbound / Outbound	Description
PJLink	4352	TCP	Outbound	This is the default port for PJLink and cab be changed in the settings (Peripheral Control).

vSolution Cast (with Feature Pack enabled)

Function / Application	Port	Type	Inbound / Outbound	Description
Discovery Multicast	50000	UDP	Inbound	This port is used for device discovery all available Cynap and Visualizer systems 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 and / or Visualizer systems. If this port is blocked, secure communication to Cynap and / or Visualizer systems, inclusive firmware updates is blocked.
Video Streams	50921	TCP	Inbound	Video streams between Wolfvision App and Cynap system. If this port is blocked, streams are not possible.
Touchback	50922	UDP	Outbound	This port is for touchback between Cynap Pure (Next Gen) and Wolfvision App vSolution Cast to send mouse events back to the Windows computer. If this port is blocked, bi-directional inputs are not possible.

vSolution App

Function / Application	Port	Type	Inbound / Outbound	Description
Discovery Multicast	50000	UDP	Inbound	This port is used for device discovery all available Cynap and Visualizer systems 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.
http, Cynap control	80	TCP	Inbound	This port is used to connect to the Cynap Pure (Next Gen) 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 Pure (Next Gen) web for secure connect to the Cynap Pure (Next Gen) web interface. If this port is blocked, no connection can be made.
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 and / or Visualizer systems, inclusive firmware updates is blocked.
Video Streams	50921	TCP	Inbound	Video streams between WolfVision App and Cynap system. If this port is blocked, streams are not possible.
Touchback	50922	UDP	Outbound	This port is for touchback between Cynap Pure (Next Gen) and Wolfvision App vSolution Cast to send mouse events back to the Windows computer. If this port is blocked, bi-directional inputs are not possible.

WebRTC

Function /	Port	Type	Inbound /	Description

Application			Outbound	
WebRTC	10000 – 16000 50000 - 65000	TCP / UDP	Outbound	Communication Port.
WebRTC Pexip	1720	TCP	Outbound	This port is used WebRTC services like Pexip.

TLS Control

Function / Application	Port	Type	Inbound / Outbound	Description
TLS Control	50917	TCP	Inbound	This port is for secure communication between Wolfvision application (e.g. vSoltuion Link Pro) and Cynap and / or Visualizer systems. If this port is blocked, secure communication to Cynap and / or Visualizer system, inclusive firmware updates is blocked.

WebSocket

Function / Application	Port	Type	Inbound / Outbound	Description
Websocket	7681	TCP	Inbound	User interface communication with Cynap Pure (Next Gen) (via browser)
Websocket	7682	TCP	Inbound	User interface communication with Cynap Pure (Next Gen) (via fully integrated Visualizer)

vSolution Link Pro

Function / Application	Port	Type	Inbound / Outbound	Description
Multicast DNS (mDNS)	7 / 9	UDP	Inbound Outbound	Multicast DNS (mDNS 224.0.0.251).
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 control	80	TCP UDP	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 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. This port is also used for the WolfVision Management .Hub (vSolution Link Pro

				hosted in the cloud)
SMTP	587	SMTP	Inbound	Mail Server – default Port for communication with SMTP server.
Discovery Multicast	50000	UDP	Outbound	This port is used for device discovery all available Cynap and Visualizer systems 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.
For control purposes	50917	TCP	Inbound	This port is used for control purposes. If this port is blocked, no control is possible.

Zoom (with Feature Pack enabled)

Function / Application	Port	Type	Inbound / Outbound	Description
http	80	TCP	Outbound	For Zoom clients and meeting connector
https over TLS / SSL	443	TCP	Outbound	For Zoom clients and meeting connector
	8801	TCP	Outbound	For Zoom clients
	8002	TCP	Outbound	For Zoom clients
	3478	UDP	Outbound	For Zoom clients
	3479	UDP	Outbound	For Zoom clients
	8801 ~ 8810	UDP	Outbound	For Zoom clients
Function / Application	Port	Type	Inbound / Outbound	Description
Discovery Multicast	50000	UDP	Inbound	Discovery Multicast – This port is used for device discovery all available Cynap Pure (Next Gen) 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 / Outbound	For master control mode

https, Cynap 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 Pure (Next Gen) and / or Visualizer. If this port is blocked, secure communication to Cynap Pure (Next Gen) 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

Optional Feature Pack

Activate the optional Cynap Pure Feature Pack to unlock the following features:

- File explorer with multimedia and document playback from cloud services, network drives, FTP servers, and USB storage devices
- WebConference services (WebRTC services, Zoom, and Microsoft Teams)
- Input sources (HDMI, USB UVC, and streaming sources)
- Annotation

For more details refer to Feature Pack

1. Changelog

Changelog of the Network Integration Guide for Cynap Pure (Next Gen):

Version	***Date***	***Changes***
1.0	2026-06-03	Initial document