Network Integration Guide: CYNAP PURE RECEIVER

WOLFVISION vSolution Cynap Pure Receiver Network Integration Installation Guide

Contents

WOLFVISION vSolution Cynap Pure Receiver Network Integration Installation Guide

Product Information

The vSolution Cynap Pure Receiver is a network integration device manufactured by WolfVision GmbH. It is designed to connect to an existing company network and provide network services. The device is equipped with LAN/Ethernet settings, allowing for easy integration into the network infrastructure. It supports various authentication methods, encryption protocols, and network configurations to ensure secure and reliable connectivity.

Product Usage Instructions

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 Receiver can be integrated into the network.

When connecting Cynap Pure Receiver 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 Receiver can be treated as a standard network device and it is as secure as the supporting network. Cynap Pure Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver in a protected network. (IEEE 802.1x).
Anonymous Identity	The identity to be used on an unencrypted session before Identity is being validated on an encrypted session.
Authentication	Allow authentication according to IEEE 802.1X. Enter valid login data to connect.

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: 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 – infrastructure (Cynap Pure Receiver acts as client)
Use the access point list to check the currently available access point and its signal strength.

Mode OFF	Disable Infrastructure
Mode Infrastructure	Enable Infrastructure, Cynap Pure Receiver can be connected as client to an existing access point.
Band	By default, Cynap Pure Receiver uses the 2.4GHz and 5 GHz frequency band. The frequency band used can be limited to either 2.4GHz or 5 GHz. This setting is not available in BSSID mode.
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 Receiver 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: – AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuV vWwXxYyZz – 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 Receiver 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). WEP allows passwords with length of 13 characters (128 bit WEP). WPA2 allows passwords with a length of 8 ~ 63 characters. Use special characters carefully, not every third party can handle it. When using WPA2 Enterprise, load the certificate by using the Web Interface through the LAN interface.
Identity	Login credentials to connect Cynap Pure Receiver 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: 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 Receiver 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.

- root certificate (CA) with common file extension .crt Base-64-coded X.509 encoded DER certificate

- Privacy Enhanced Mail with common file extension .perm

2.3 Date and time (General Settings)

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

2.4 Host name (General Settings)

Hos t na me	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

2.5 LAN / WLAN port

The LAN port enables integration of Cynap Pure Receiver into an internal network. Administrators of a large number of Cynap Pure Receiver 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 Receiver 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 DHCP 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 Receiver to standby closes all connections.

2.6 Proxy settings

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

Proxy enable	Enable or disable proxy functionality to control HTTP and HTTPS traffic (other services and built-in access point are not controlled). Please note, using a Proxy server may block

vSolution Link Pro functionality. |
| URL | URL of the proxy server in your network, like 104.236.10.17 (or DNS name up to 256 characters, no space between the

characters). DNS server not required, when using IP addresses. |
Host Port	Port, set the used network port to connect to your proxy server.
Authentication	Allows authentication with username and password.
Username	Input the username according to your proxy server settings.
Password	Input the password according to your proxy server settings.

2.7 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 Receiver at any time. The default password is "Password". Remember to make a note of any changed passwords!

Login Security

Accessing Cynap Pure Receiver can be protected by authentication (admin, moderator, PIN or LDAP user).

To prevent unauthorized access to the settings, the credentials needs to be entered whenever you start a new session or when logged out previously.

Network Security

Accessing Cynap Pure Receiver 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 (IEEE 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 Receiver complies with following standards:

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

Hint

- WEP allows passwords with a length of 13 characters (128 bit). WPA2 allows passwords with a length of 8 ~ 63 characters.
- Use special characters carefully, not every third party device can handle them. When using WPA2 Enterprise, load the certificate by using the Web Interface.
- When using the built-in access point, the security settings will be handled automatically. When starting a new presentation, the SSID and also the password will be changed.

3. Network integration

The following example is showing a way to integrate Cynap Pure Receiver into your network infrastructure. The Cynap Pure Receiver can only be integrated into an existing vSolution Matrix. (Cynap Pro as main station is required)
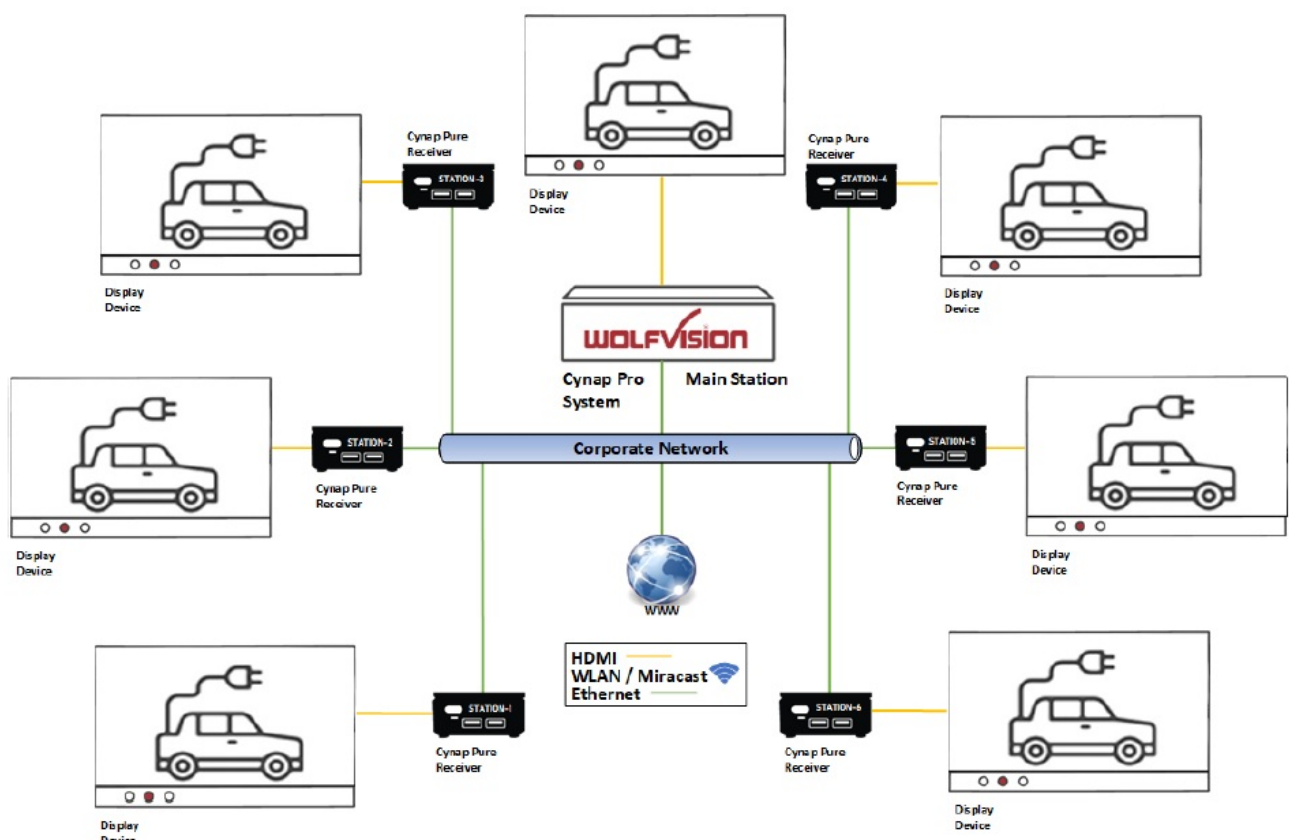
4. vSolution Matrix (optional Feature Pack, Cynap Pro required)

The vSolution Matrix Feature Pack enables Network AV functionality with an optimized interface for touch screens. Network AV allows cost-effective installations by using the existing IP network infrastructure to transmit AV signals. Means there is no longer a need to maintain separate AV infrastructure for your e.g. huddle room (active learning classroom). This results in a straightforward installation with less hardware and reduced ongoing maintenance. You also have the flexibility to scale your setup up or down easily, as required to keep the huddle rooms effective. Every workstation, equipped with a vSolution Cynap, ensures intuitive and easy-to-use collaboration participative users. Contents can be simply forwarded between different screens by drag & drop. Please note that the multicast address must be unique in each network to prevent problems with streaming.

Specifications:

Maximum station	1 main station 40 client stations
Bandwidth Stream	40 Mbit/s
Latency	Approximately 50 milliseconds for 1080p30
IP Multicast Group Address Range	adjustable
Streaming PortMulticast / Unicast Audio / Video	adjustable
Communications	Wired, LAN 1 only
Switch	Layer 2 or Layer 3 with enabled IGMP Snooping
File Sharing	TCP 50930 SSHFS

5. Firewall rules

Cynap Pure Receiver has firewall rules that must be adhered to in order to allow successful network communication with vSolution Matrix main station 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.

Function / Application	Port	Type	Inbound / Outbound	Description
vSolution Matrix				
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 used to connect to Cynap web interface (httpd). If this port is blocked, no connection can be made.
https, SSL, e.g. Cynap control	443	TCP / UDP	Inbound	This port is used to cloud service and for secure connect to Cynap web for secure connect to Cynap web interface. If this port is blocked, no connection can be made.
NFS	111 / 2049	TCP UDP	Outbound	NFS – Connection to network drives
CIFS	137 / 139	TCP UDP	Outbound	CIFS – Connection to network drives
SSHFS	50930	TCP	Inbound	SSHFS – vSolution Matrix File Sharing Key Exchange
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
Streaming RTSP	554	TCP	Outbound	This is the communication port for the RTSP stream. This used UDP port will be handled automatically
Wake On LAN	7 / 9	UDP	Inbound / Outbound	Usually port 7 is used for sending the magic packet
FTP	21	TCP	Outbound	Connection to FTP server
SSH	22	TCP	Inbound	Access for Wolfvision support
http, Cynap control	80	TCP	Inbound	This port used to connect to Cynap web interface (httpd). If this port is blocked, no connection can be made.
Proxy	8080	TCP / UDP	Outbound	Default port proxy function (This port can be changed in the Proxy settings).

NTP	123	UDP	Outbound	For optional clock synchronization by a time server (Network Time Protocol, NTP)
Streaming Multicast / Unicast	8800 – 9000	UDP	Inbound	Used for Multicast / Unicast / Audio / Video Streaming
Streaming RTSP	554	TCP	Outbound	This is the communication port for the RTSP stream. This used UDP port will be handled automatically
PJLink control	4352	TCP	Outbound	This is the default port for PJLink and cab be changed in the settings (Peripheral Control)
vSolution App iOS / Android / Windows				
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. 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	UDP	Inbound	This port is used for device discovery.
For control purposes	50917	TCP	Inbound	This port is for secure communication between Wolfvision application (e.g. vSoltuion Link) t 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	Inbound	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)
For control purposes	32768 - 61000	UDP	Outbound	Video data stream (e.g., BYOM, Chromecast)

WebSocket	7681	TCP	Inbound	User interface communication with Cynap (via browser)
WebSocket	7682	TCP	Inbound	User interface communication with Cynap (via fully integrated Visualizer)
vSolution Link Pro				
Wake On LAN	7 / 9	UDP	Inbound / Outbound	Wake On LAN – Usually port 7 is used for sending the magic packet
DNS	53	TCP / UDP	Inbound / Outbound	DNS – This port will be used for Domain Name System. If this port is blocked, DNS service are not available
http, Cynap control	80	TCP	Inbound	This is the default port to connect to the web interface (httpd) of vSolution Link Pro. Of this port is blocked, connection cannot be established
https, SSL, e.g. Cloud Service, Cynap control	443	TCP	Inbound	This is the default port to connect to web interface (https) of vSolution Link Pro. If this port is blocked, connection cannot be established.
SMTP	587	SMTP	Outbound	Mail Server – Port for communication with SMTP server.
Discovery Multicast	50000	UDP	Inbound	This port is used for device discovery all available Cynap and Visualizer in the network by vSolution applications (uses Multicast IP address 239.255.255.250). If this port is blocked, device discovery is not possible
Device Discovery	50913	UDP	Inbound	This port is used for device discovery. If this port is blocked, device discovery is not possible.
For control purposes	50915	TCP	Inbound	This port is used for control purposes. If this port is blocked, no control is possible

6. User interface

Cynap Pure Receiver 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 Receiver. 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 Receiver 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 Receiver via network. More information about the vSolution App can be found on in the support section of our website **www.wolfvision.com** .

7. Hardware & OS

Cynap Pure Receiver 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 Receiver. 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 Receiver 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.

8. Administration

Cynap Pure Receiver can be managed using the vSolution Link Pro software.

With vSolution Link Pro 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 Receiver 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 Pro software, and you can change the background wallpaper easily.

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

9. Index

Version	Date	Changes
1.0	1.08.2023	Created
1.1	19.09.2023	Adaptations for Cynap Pure Receiver Ports adjusted, matrix section added, general changes etc.
1.2	18.10.2023	– Addition Firewall rules

—

Specifications

- Manufacturer: WolfVision GmbH
- Model: vSolution Cynap Pure Receiver
- Address: Oberes Ried 14, A-6833 Klaus, Austria
- Contact: Tel. +43-5523-52250, Fax +43-5523-52249, E-Mail:
  wolfvision@wolfvision.com

- Website: **www.wolfvision.com**

FAQ

Q: How do I connect the Cynap Pure Receiver to my company network?

A: To connect the Cynap Pure Receiver to your company network, you need to obtain the necessary LAN/Ethernet settings from your local administrator. Follow the instructions in section 2.1 of the user manual to configure the network settings correctly.

Q: What authentication methods are supported by the Cynap Pure Receiver?

A: The Cynap Pure Receiver supports authentication methods according to IEEE 802.1X, including PEAP with MSCHAPv2 and TTLS-PAP. Refer to section 2.1 of the user manual for more information on setting up authentication.

Q: Can I use self-signed certificates for authentication?

A: No, the Cynap Pure Receiver only supports root certificates (CA) with common file extension .crt or base-64-coded X.509 encoded DER certificates. Refer to section 2.1 of the user manual for more information on certificate requirements.

Documents / Resources

WOLFVISION vSolution Cynap Pure Receiver Network Integration [pdf] Installation Guide vSolution Cynap Pure Receiver Network Integration, vSolution Cynap, Pure Receiver Network Integration, Receiver Network Integration, Network Integration, Integration

References

- ☑ **Presentation, Collaboration & Visualizer Systems - WolfVision GmbH**
- ☑ **Presentation, Collaboration & Visualizer Systems - WolfVision GmbH**
- **User Manual**