Remote Access Guidelines

Application Note

Introduction

This application note covers the basics of connecting a Pharos installation to the Internet so that it can be controlled and managed remotely. Networks and connections to the Internet can be set up in many ways. Setup may require the advice, assistance or cooperation of IT professionals and network administrators. Please feel free to pass on these guidelines.

Remote Access using Pharos Cloud

Getting access beyond the local network doesn't have to involve additional skills or hardware, or the potential security risks of a misconfigured network.

Our award-winning remote management solution, Pharos Cloud, provides simple, secure remote lighting installation control and management, from any Internet-connected device, at anytime, anywhere in the world.

Benefits of Pharos Cloud

- Devices connecting with Pharos Cloud will only tunnel out securely over HTTPS via port 443
- All data is encrypted during transit and at rest
- No inbound connection is required, no ports need to be opened
- Granular individual user permissions
- Support for two factor authentication

More information about Pharos Cloud is available at pharoscontrols.com/cloud

Other Approaches to Remote Access

While we recommend the use of Pharos Cloud for simple and secure remote access, other options are available. These methods may require the advice, assistance or cooperation of IT professionals and network administrators.

The Pharos support team are happy to provide basic assistance with the setup of our products for these applications. However, setup of networking systems can get complex, and we are unable to provide advice or assistance on configuration of third-party systems such as VPNs or routers.

Terms

Pharos Designer: Commissioning software used for programming a Designer installation as well as uploading programming to the Designer controllers connected to a network.

Pharos Express Software: Commissioning software used for programming an Express installation as well as uploading programming to Express Control.

Local Area Network (LAN): The Ethernet network that connects all of the Pharos hardware, computers and lighting fixtures. It does not connect directly to the Internet or another network.

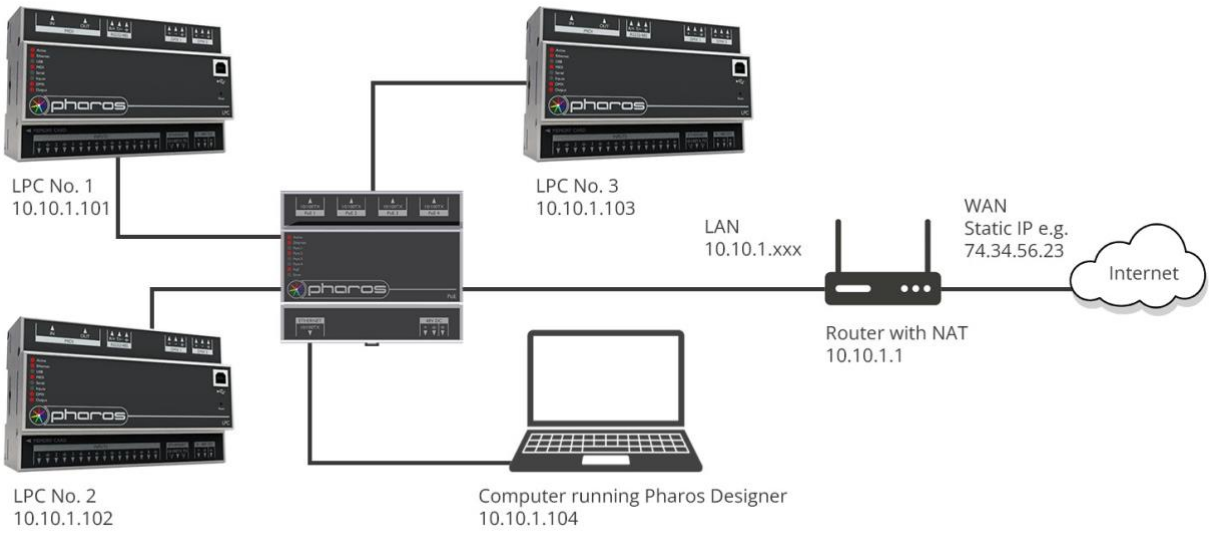
IP Address: The numerical address that a computer uses to communicate on a Network.

Router: A device that allows two networks to connect to each other. A router can be used to connect two local networks or connect a local network to the Internet.

VPN: Virtual Private Network. An arrangement whereby a secure, apparently private network is achieved using encryption over a public network, typically the Internet.

VLAN: Virtual Local Area Network. A virtualized connection that connects multiple devices and network nodes from different LANs into one logical network

Here is an example of a Pharos system comprised of three LPCs, a computer and a PoE Ethernet switch. The switch is connected to the Internet via a router. See the diagram below:



Pharos Designer and Express Software

Pharos Designer or Express desktop applications are able to discover controllers on the same LAN as the computer, and this provides the simplest user experience for controller configuration.

If using Pharos Cloud, the applications provide a seamless experience whether uploading to the local network or to remote controllers over the cloud.

Controller Web Interface

Pharos controllers provide built-in web interfaces. Navigating to the controller's IP address in a web browser will present pages showing the status of the controller including timeline, scene and input status, output values, etc. The Control and Configuration pages allow you to trigger events, change settings and upload new shows. These pages can be password protected.

This web interface requires web sockets (RFC 6455) between the Controller and the client web browser. If web sockets are blocked on the network (or proxy server) the web interface will not populate with data. Additionally, port **80** is required for web interface access (HTTP) or **443** (HTTPS).

In a network which is accessible to other clients, such as a network with publicly accessible connections or wireless connectivity, we strongly recommend that controllers should be secured with a username/password and that connections should be secured with an HTTPS certificate.

For more information on creating and uploading HTTPS certificates, see our guide here.

Networking Methods for other Remote Access Approaches

Port Forwarding – Web Interface

Using a router with Port Forwarding configured, it is possible, although not recommended, to expose the controller web page to the Internet directly.

For example, in the system above if the secured web server is running on port 443, the router can be configured to forward incoming requests to the controller, thus "exposing" the web interface to the internet.

Importantly, the provided Internet connection uses a static IP. Internet service providers who offer dynamic connections often rotate through IP addresses. Without knowing the public facing IP of the system on the Internet you will not be able to gain access to the web interface.

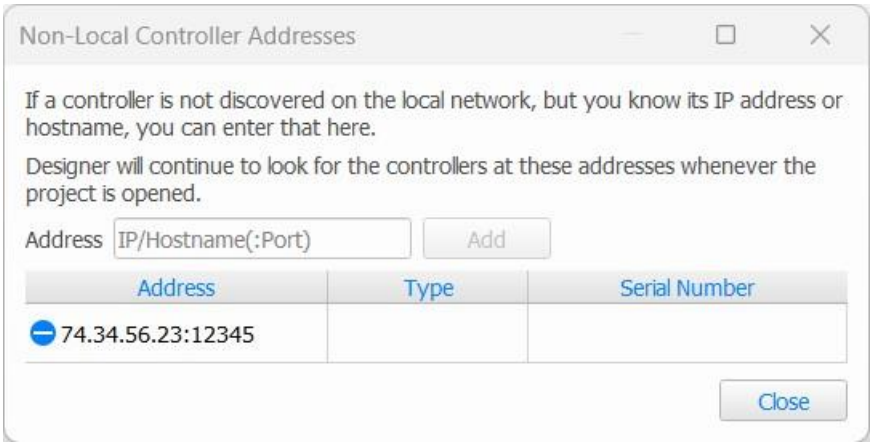
If you plan to use this mechanism you MUST enable security, and we would very strongly recommend using HTTPS. Any server open to the internet will inevitably be subject to probes and attacks. Even with these controls turned on, we do not recommend this option as these scans and attacks may have a negative effect on the controller.

Port Forwarding – Controller Connection

Similarly to the web interface setup described above, the port that Pharos software needs to communicate with can be port-forwarded through the router to be available for the internet.

This method has the same major concerns as the method described above – the exposed ports of the controllers are likely to be probed and attached, with unknown consequences for the stability of the controllers.

The port required for a software connection is port **38008**. If this port is forwarded through the router, the connection can be established from an instance of Designer or Express software using the "Find" option in Designer, or the "Find Express Control using IP address or hostname" option in Express. For example, in the system above if port 38008 was forwarded to port 12345 by the router, in Designer you would enter:



If you have a multi-controller system, as above, you can forward a different public-facing port on the internet side of the router to each controller's 38008 port, to allow for access to all controllers from the internet.

© 2004-2024 Pharos Architectural Controls Limited pharoscontrols.com All rights reserved. Subject to change without notice.

VPN (Virtual Private Network)

Commonly used for creating a connection to an office network, a VPN is set up using standard network settings on a computer. A VPN typically requires an IP address, username and password to be provided by a network administrator. Controllers' web interfaces can be accessed by navigating to their IP address in a web browser. Port 80 is required for access to a controller's web interface over HTTP, or 443 over HTTPS. Pharos software cannot discover Pharos controllers using a VPN connection, but you can directly connect to a controller over a VPN using the "Find" feature in Designer, or the "Find Express Control using IP Address or Hostname" option in Express.

VLAN (Virtual Local Area Network)

A VLAN allows computers and Pharos controllers to communicate as if they're connected to the same wire, regardless of their geographical locations. If an installation site can't allow Pharos Software or controllers to be exposed on their network, or if the existing network configuration blocks multicast packets which Designer uses to find controllers, then a VLAN may provide a solution.

A VLAN can be configured to forward multicast packets for Pharos products. For multicast access, the following addresses need to be routed throughout the VLAN:

239.192.38.7 – Discovery

239.192.38.8 – Controller to Desktop Software communication

Summary of Remote Access Methods

As a summary of the available methods, the table below can be used as a guide to choosing your method.

	Method			
	Pharos Cloud	**Port Forwarding**	**VLAN**	**VPN**
Ease of Configuration	Easy	Difficult	Difficult	Difficult
Security	Fully Secure	Major Security Concerns	Secure	Secure
Requires Additional 3rd Party Hardware/Software	No	No	Yes	Yes
Recommended by Pharos	Yes	No	Yes	Yes

Further Information

Information on Local Network Setup can be found in the application note: Local Network Guidelines. If you need further help, please email support@pharoscontrols.com

© 2004-2024 Pharos Architectural Controls Limited pharoscontrols.com All rights reserved. Subject to change without notice.