

## IT Networking and Security Guideline for Helvar Imagine

### Document Purpose and Scope

This document defines high-level security and network installation practices for Helvar Imagine lighting control systems. It is intended for building IT/network administrators, systems integrators, and commissioning engineers responsible for deploying, operating, and supporting Imagine. It covers network architecture, access control, remote maintenance, and firewall requirements.

### Helvar Imagine Lighting Control System Overview

Helvar Imagine application controllers (routers) communicate over IP, discovering peers primarily via UDP broadcast (recommended) and optionally multicast; unicast is used during normal operations. Designer 5 on the head-end PC must be able to see broadcast/multicast discovery traffic for commissioning and management.

Helvar Imagine solution has been designed to work on its own separate network without access to internet. However, there are three use cases for connectivity:

- 1) Monitoring and analytics
- 2) Integration to other technical building systems or building management systems
- 3) Remote connection for maintenance

### Monitoring and Analytics

Cloud-based Helvar Insights offers an authenticated and authorised access to the Helvar Imagine solution. A separate document describes security of the Helvar Insights solution and is available from Helvar representative.

### Integrations

Local on-premise integration is achieved through an on-premise gateway. For example, Helvar 436 Gateway supports BACnet and Modbus connectivity to the other technical building systems. In this case, there is no authentication or authorisation at the gateway level. Consequently, the connected other building system must prevent unauthorised access to the Helvar Imagine system via the gateway connection.

### Remote Connections

After commissioning, there must be no computer left on site connected to the Helvar Imagine system. After commissioning, remote connectivity is achieved using a forced tunnelling VPN connection. In this case, the third-party solution offers a secure connectivity from a remote location and all the connected computer's traffic is forwarded through the secure VPN connection. The remote computer must not have any other internet connectivity while being connected to the Helvar Imagine system via the secure VPN connection. For example, Tosibox can be used for the secure connectivity.

### Network Design

There are two options to build the ethernet network connecting Helvar Imagine Application Controllers together as described below. Furthermore, it is possible to use Helvar Imagine

Application Controllers as stand-alone systems without connecting them with ethernet to anything.

#### Closed Network with Unmanaged Switches

This setup expects the Helvar Imagine solution to be totally separated from the other systems. It is impossible to access the network without a physical connection.

#### Managed Network with Managed Switches

In this case, a dedicated VLAN is created for the Helvar Imagine solution. The firewalls on managed switches provide protection. The security and its maintenance are managed by the building's IT / network administrator. A separate document regarding network communications is available from Helvar representative.

#### Required ports

The following ports should be open for Helvar Imagine application controllers to communicate with one another over the IP network. Helvarnet is used between application controllers and gateways as well as ST7 touch screens.

Function	Protocol	Port
Broadcast Discovery	UDP	<b>60000</b>
TCP listener	TCP	<b>60002</b>
UDP messaging	UDP	<b>60004–60008</b>
Multicast discovery	UDP	<b>60009</b>
Helvarnet TCP	TCP	<b>50000</b>
Helvarnet UDP	UDP	<b>50001–50005</b>

#### Contact Us

We have our headquarters in Finland, have offices also in Poland, Sweden and United Kingdom, and we work with Partners all over the world.

<https://helvar.com/contact-our-team/>