# Door Station - Exterior: Security Best Practices

## Introduction

The Control4® Door Station – Exterior is the first smart Control4 device designed to be installed on the outside of a dwelling. The Door Station has connections for relays (to open doors, gates, etc.) and contacts. If installed without the proper security precautions, unauthorized access to the Door Station could provide access to Ethernet signals, Control4 signaling, and gate or door relays. Control4 advises Control4 Dealers to be aware of these risks and take all necessary precautions depending on each specific installation you will be doing.

It is each Dealer's sole responsibility to advise their customer at each installation of any security risks specific to such installation. Control4 makes no claims, representations or warranties regarding the security of this product and accepts no liability for any security risk attendant to a specific installation.

## Best Practices

1. The Door Station - Exterior ships standard with security screws. Dealers are encouraged to use these screws, or even substitute alternate security screws per the Dealer's or customer's preference. Screw size is metric M3.5x.6-30L.
2. Security gates or automatic doors should not be connected to the relay in the Door Station if mounted in an unsecured area; such relays could be accessed in the event of a breach of the device. Secure relay-driven devices should be connected to a more secure relay controller mounted behind a secure wall.
3. Security devices, for example numeric keypads, should not be connected to the contact sensors in the Door Station if mounted in an unsecured area; such devices could be accessed in the event of a breach of the device. Security-sensitive devices should be connected to more secure contacts mounted behind a secure wall.
4. Although the best video performance will be enabled by Ethernet connectivity, unauthorized access to the Door Station could provide access to the dwelling's Ethernet network and corresponding personal data.

   There are alternatives to mitigate this risk. The Dealer should consider the following options:

   - Running Control4 on an isolated LAN from PCs on the network would limit exposure to personal data.
   - Running MAC address filtering on the router or switch to force a hacker to spoof the Door Station's MAC address to gain access to the LAN.
   - Configuring the Door Station as WiFi instead of Ethernet would allow the Dealer to use robust WiFi security protocols, for example, WPA.

   Note: WiFi signals must be very strong and stable to support Video Intercom.

- Routing the Ethernet cable to the Door Station through a secure managed switch to limit data access from the Door Station.

## Summary

Dealers should take time to assure they are not creating an unforeseen security risk for the customer, and any such risks should be discussed with the customer prior to the installation.

Carefully consider with your customer any contacts or relays before connecting them to the Door Station, and what implications could arise if someone gained access to the rear of the Door Station.

Also, think about what could happen if someone gained access to the Ethernet cable, and take necessary precautions to protect private customer information unless your customer is willing to assume these risks. Making available the proper security protections to a customer for their residence is the responsibility of the Control4 Installer.

## About this Document

Part number: DOC-00054, Rev. A  05/16/2012