

Continental Access

A Napco Security Group Company

CA4K™

TCP/IP PORTS

Revision: Rev D

Date: 1/13/2022



DISCLAIMER

Continental Instruments LLC makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. Further, Continental Instruments LLC reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Continental Instruments LLC to notify any person of such revision or changes.

Copyright © 2016 by Continental Instruments LLC. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, or stored in a retrieval system, without the prior written permission of Continental Instruments LLC, 355 Bayview Avenue, Amityville, NY 11701. Telephone: 631-842-9400 • FAX: 631-842-9135

This document contains proprietary information of NAPCO Security Technologies. Unauthorized reproduction of any portion of this manual without the written authorization of NAPCO Security Technologies is prohibited. The information in this manual is for informational purposes only. It is subject to change without notice. Companies, names and data used in examples herein are fictitious unless otherwise noted. NAPCO Security Technologies assumes no responsibility for incorrect information this manual may contain.

A NAPCO SECURITY TECHNOLOGIES COMPANY
Publicly traded on NASDAQ Symbol: NSSC

Visit our websites:

<http://www.cicaccess.com/>

<http://www.napcosecurity.com/>

<http://www.alarmlock.com/>

CA4K™ TCP/UDP ports to be open on Firewall:

CA4K™ software uses the following TCP/UDP ports for various applications. The following ports should have exceptions on firewall as described below.

CA4K™ installer will automatically create required inbound and outbound rules, as long as installed user has **ADMINISTRATOR** permissions.

Rules created during install:

Rule Name	Direction	Protocol	Ports
CA4K TCP in ports	inbound	TCP	local port=1433, 1434, 5001, 5003, 5501-5507, 5601-5607, 8003, 9000, 9001, 9002, 9003, 9005, 10050, 10081, 8080, 8731, 38880, 22609, 10019,8010, 18772, 443, 4040, 4021
CA4K TCP out ports	outbound	TCP	remote port=3001, 5001, 5003, 5501-5502, 5601-5602, 8003, 9000, 9001, 9002,9003, 9005, 10001, 10081, 38880, 22609, 10019,8010, 18772, 443, 4040, 4021
CA4K UDP out ports	inbound	UDP	local port=30717, 30718, 48307, 47307, 45308, 45303, 46303, 46308
CA4K UDP in ports	outbound	UDP	local port=1434, 30717, 30718, 48307, 47307, 45308, 45303, 46303, 46308

Applications and Ports:

Application Name	Protocol	Ports	Purpose	
Main Business Layer (MBL)	TCP	9001	Application remoting (TCP Listener)	required
	TCP	9005	Application remoting (HTTP Listener)	required
	UDP	8888	CardAccess MBL Discovery	optional
Main Messaging Service (MMS)	TCP	9000	Application remoting	required
	UDP	8899	CardAccess CMS Discovery	optional
Host Communication Service (HCS)	TCP	5501	1 st HCS Application remoting – status update	required
	TCP	5502	2 nd HCS Application remoting – status update	optional
	TCP	5503	3 rd HCS Application remoting – status update	optional
	TCP	5504	4 th HCS Application remoting – status update	optional
	TCP	5505	5 th HCS Application remoting – status update	optional
	TCP	5506	6 th HCS Application remoting – status update	optional
	TCP	5507	7 th HCS Application remoting – status update	optional
	TCP	3001	Default port for panel polling (for all HCS PCs)	required
	TCP	9002	Callback Listener- Data transfer with MBL	required

Wireless Lock	TCP	10050	Application to receive events from Wireless Gateway (only if use wireless lock devices)	optional
	TCP	10001	WL application to wireless gateway (requires only if use wireless lock devices)	optional
	UDP	30718	Discover Gateways (requires only if use wireless lock devices)	optional
	TCP	5601	1 st Application remoting – wireless lock status update (requires only if use wireless lock devices)	optional
	TCP	5602	2 nd Application remoting - wireless lock status update (requires only if use wireless lock devices)	optional
	TCP	5603	3 rd Application remoting - wireless lock status update (requires only if use wireless lock devices)	optional
	TCP	5604	4 th Application remoting - wireless lock status update (requires only if use wireless lock devices)	optional
	TCP	5605	5 th Application remoting - wireless lock status update (requires only if use wireless lock devices)	optional
	TCP	5606	6 th Application remoting - wireless lock status update (requires only if use wireless lock devices)	optional
	TCP	5607	7 th Application remoting - wireless lock status update (requires only if use wireless lock devices)	optional
	TCP	9003	Callback Listener- Data transfer with MBL (requires only if use wireless lock devices)	optional
Napco Integration	TCP	8003, 10081	Connect to RCM devices (requires only if use NAPCO Panels)	optional
	TCP	5003	Connect to NL-Mod (requires only if use NAPCO Panels)	optional
	UDP	30717	Discover RCM devices (requires only if use NAPCO Panels)	optional
Central Station Reporting	TCP	5001	Application remoting (requires only if Central Station Reporting is used)	optional
SQL Server Engine	TCP	1433	To connect SQL Server database	required
SQL Server Browser	UDP	1434	To browse SQL Server instances	required
DVR	UDP	9002	Pelco DVR default port. (and more...should be opened by user) *	optional
	TCP	5100	Aventura server configuration	optional
	TCP	8731	Aventura Playback	optional
	TCP	38880	Avigilon server configuration	optional
	TCP	22609	ExacqVision server configuration	optional
	TCP	10019	VideoView (Hitron) Search	optional

	TCP	8010	VideoView (Hitron) Audio	optional
	TCP	8080	Luxriot server configuration	optional
	TCP	8080	Milestone Video	optional
	TCP	18772	PelcoDS server configuration	optional
	TCP	443	PelcoVideoXpert server configuration	optional
	TCP	4020	VideoInsight Data	optional
	TCP	4021	VideoInsight Command	optional
CA4K Mobile Web App	TCP	8080	Default port for the CA4K Mobile App	required
CA4K Web Client	TCP	80	Default port for the CA4K Web Client (Normally open by default)	required
OTIS Elevator Integration	UDP	48307	Multicast health check end point send port	optional
	UDP	47307	Multicast health check end point receive port	optional
	UDP	45308	Unicast DEC send port	optional
	UDP	45303	Unicast DEC receive port	optional
	UDP	46303	Unicast DES send port	optional
	UDP	46308	Unicast DES receive port	optional
Email Notification	TCP	443	Send email (requires only if Email Notification feature is used)	optional

***NOTES:**

- 1) There are other ports that might have to be manually opened as specific features are enabled by user. *For example: If DVR integration is enabled and Milestone DVR server is running at port 8083, this port has to be opened manually by user and the port depends on server configuration.*
- 2) Ports for the CA4K Mobile Web App and the CA4K Web Client can be changed in IIS under Bindings and port must be opened at firewall accordingly.
- 3) Majority of the optional ports should be open only if the feature is used. *For example: If the wireless lock devices are not used no need to open up ports related to wireless lock configuration.*