White Paper

Important Ports for DMP Product Compatibility

Below are the ports you will need for compatibility with DMP products and features. As an overview, author Edward Tetz ("Network Basics: Networking Port Overview") explains:

In TCP/IP and UDP networks, a port is an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic. If you use a command such as netstat -n on Microsoft Windows or Linux, you see a listing of the local addresses (and ports) and the foreign addresses (and ports) to which they are connected.

The three categories of TCP and UDP ports are:

- **Well-known ports:** When Internet Protocol was being implemented, there was a slow start of assigning services that needed to use specific ports. The ports were initially assigned from the lowest port number and worked their way up.

  Ports 0–1,023 are considered well-known ports because they were used by many of the core services on the Unix servers, and most required privilege permissions on the server to implement. Telnet (23) and Simple Mail Transport Protocol (SMTP) (25) are two examples of these services.

- **Registered ports:** The Internet Assigned Numbers Authority (IANA) keeps the list of all services that run on the well-known ports and all registered ports. The registration process puts a permanent association in place with the port number and the service.

  These services are all long-running and assigned to ports between 1,024 and 49,151. The Microsoft Remote Desktop Protocol (RDP) (3389) and Network File System (NFS) (2049) are two examples of registered ports.

- **Dynamic and/or private ports:** All other ports, from 49,152 to 65,535, are referred to as dynamic or private ports. These are not permanently associated to any service.

If you write your own service, you can configure it to use any dynamic port you want, but others may write their own service and use the same port. This will not cause any issue until you install both services on the same IP host because they are both going to want to use the same port.

Let's say you have a warehouse, and its address is 192.168.1.100 (much like a street address) with hundreds (or thousands) of docks (ports). In general, each dock can be allocated only once to a specific function or process. So long as the port is open (the dock workers or application is present), then outside sources can connect to the bay and exchange data.

DMP Panel Common Ports and Uses:

- **Inbound TCP Port 2001:** For accepting connections from Remote Link™/System Link™ or the Virtual Keypad™ servers when the connection strategy is set to "Network." May require a NAT, public IP address and/or firewall rules to work correctly.
- **Inbound TCP Port 2011:** For accepting connections from the Entré™ application server. May require a NAT, public IP address and/or firewall rules to work correctly.
- **Inbound TCP Port 2002:** For accepting connections from 734N Network Access Control Modules that are remote to the control panel. While these are typically on the same local area network (LAN), some may require a NAT, public IP address and/or firewall rules to work correctly.
- **Outbound TCP Port 2001:** The panel transmits to the monitoring center on port 2001 TCP by default for network and on 2001 UDP on cellular. This value is programmable and may change from the default of 2001 if the panel is programmed as such, requiring the port to also be changed on the firewall. If the panel is using cellular, firewall changes are not necessary as the panel will be using the cellular network to communicate.
- **Outbound TCP Port 4001:** For initiating connections to the remote SecureCom™ EASYconnect™ servers. This strategy is used on DMP network control panels only. It may require an outbound port exception on the firewall in some cases. Panels using SecureCom cellular devices do not require any additional configuration. Destination: *Please refer to the chart on Page 3 for clarification of URLs by panel update versions.*

  Note: The panel transmits to the SecureCom Wireless server environments on port 4001 TCP for network/EASYconnect.
- **Outbound TCP Port 6001:** For requesting weather updates. Weather requests and sunset/sunrise requests on network occur hourly, and on cellular they occur four times daily (5 a.m., 10 a.m., 5 p.m. and 10 p.m.) based on the time zone for which the panel is programmed. Weather is then displayed on the keypad of the DMP system. In addition, this port is necessary to get sunrise and sunset times for schedules that rely on them. May require an outbound port exception on the firewall in some cases. Panels using SecureCom cellular devices don't require any additional configuration. Destination: *Please refer to the chart on the next page for clarification of URLs by panel update versions.*

  Note: The panel transmits to the SecureCom Wireless server environments on port 6001 TCP for network and on 6001 UDP on cellular.
- **Outbound TCP Port 7001:** For sending panel events (opening, closing, etc.), real-time status and other updates to the SecureCom servers. Events are then displayed in the Virtual Keypad app and on the Dealer Admin™ site. This port is also used to send the daily analytic message to the SecureCom servers. This diagnostic message contains cell signal strength highs and lows, voltages, communication retries over the last 24 hours, etc. May require an outbound port exception on the firewall in some cases. Panels using SecureCom cellular devices don't require any additional configuration. Destination: *Please refer to the chart on the next page for clarification of URLs by panel update versions.*

  Note: The panel transmits to the SecureCom Wireless server environments on port 7001 TCP for network/EASYconnect and on 7001 UDP on cellular. (x1checkin.securecomwireless) For determining online or off-line status of the X1 Series™. This is used on the X1s only, and they are sent every 10 minutes over network and every hour over cell. X1s using SecureCom cellular devices don't require additional configuration.

- **Outbound TCP Port 8463** (x1tm.securecomwireless.com): For keeping the time up to date. The X1 Series will request time from SecureCom servers using this port. This is used on the X1s only, and time is only requested once every day, as well as on power up and on a reset. May require an outbound port exception on the firewall in some cases. X1s using SecureCom cellular devices don't require additional configuration.

DMP PANEL URLs **Version 211 or later** **XR SERIES**	**XT SERIES**	**X1 SERIES**
XRtunnel.securecomwireless.com	XTtunnel.securecomwireless.com	X1tunnel.securecomwireless.com
XRweather.securecomwireless.com	XTweather.securecomwireless.com	X1weather.securecomwireless.com
XRactivity.securecomwireless.com	XTactivity.securecomwireless.com	X1activity.securecomwireless.com
Version 202 or earlier		
ALL PANELS: tunnel.securecomwireless.com		
ALL PANELS: weather.securecomwireless.com		
ALL PANELS: activity.securecomwireless.com		

Remote Link/System Link:

- **Outbound TCP Port 2001:** For connecting to SecureCom servers to facilitate a connection to DMP cellular control panels. This port is configurable in the panel settings. If changed in the panel it will need to be adjusted here as well. In some cases, it may require an outbound port exception on the firewall.
- **Direct Cell Connection Port 3001:** For connecting to the alarm panel via direct cell connections on a private VPN. (Requires data center level network engineering support and agreements). Requires Entré or Remote Link software. This port is not configurable in the panel settings.
- **Outbound TCP Port 443 (TLS):** For connecting to the SecureCom Wireless provisioning servers. This allows for the activation, disconnect and status of SecureCom Wireless provisioned devices. May require an outbound port exception on the firewall in some cases.

Note: SSL has been disallowed for security reasons, only TLS 1.1 and higher are supported.

Dealer Admin, VirtualKeypad.com, Virtual Keypad iOS and Android Apps:

- **Outbound TCP Port 443 (TLS):** Allows users to connect to all available management and app services. Users must use a browser that supports TLS 1.1, at minimum.
  Note: SSL has been disallowed for security reasons, only TLS is accepted.

Video Ports:

- **SecureCom Cameras / Analog Converter:**

  123/UDP: time.windows.com: Update camera time.

  1194/UDP: camtun.securecomwireless.com: EASYconnect VPN.

  80/TCP: camcheck.securecomwireless.com: Camera check-ins.

  22 and 8080/TCP: hclips.securecomwireless.com: Send video clips.

- **SecureCom NVR:**

  123/UDP: time.windows.com: Update camera time.

  1194/UDP: camtun.securecomwireless.com: EASYconnect VPN.

  443/TCP: camcheck.securecomwireless.com: Camera check-ins.

- **Digital Watchdog Cameras:**

  123/UDP: time.nist.gov: Update camera time.

  1194/UDP: dwcamtun.securecomwireless.com: EASYconnect VPN.

  443/TCP: dwcamcheck.securecomwireless.com: Camera check-ins.

  80/TCP: dwvidclp.securecomwireless.com: Send video clips.

- **SecureCom Video Doorbell:**

  8000: Data transfer, ONVIF.

  554: RTSP.

  80: HTTP port.

  443: HTTPS port.

  31006: DAS server.

  8666: LBS server.

  6000: P2P server.

  7760

Entré Ports:

- **2001:** Allows the panel to receive programming from Entré.
- **2011:** Used to send programming to the DMP control panel.
- **1433:** The Microsoft SQL database port.
- **443:** The Web Server port for SSL configuration.
- **8080:** The Web Server port when using Apache Tomcat for incoming and outgoing information.
- **1236 & 1237:** The client ports.
- **9090 & 9091:** The debugging ports for the app server and can only be accessed locally.

SCS-VR Ports:

- **1433:** The outbound Microsoft SQL default port.
- **2001:** The default inbound TCP/UDP panel communication port for the first group created. If a second group is created, it will default to 2002. Users may define any listening port they like. As such, any additional ports defined may need to be excepted by the user.
- **3001:** The primary TCP inbound automation server port. This port listens for automation to connect if inbound automation has been enabled.
- **4001:** The secondary TCP inbound automation server port. This port listens for automation to connect if inbound automation has been enabled.
- **2002:** The primary and secondary TCP outbound automation server port. Individual IPs may be entered to designate specific destinations.

XV Gateways Ports:

Note: The XV Gateway will auto update to the latest software once it is connected to the internet. Please allow up to 30 minutes to update before arming your system with AlarmVision. If the XV Gateway is being installed on a restricted network, please ensure the floowing URLs and ports are unblocked.

New critical services on additional ports may be added in future. (If not monitoring and acting on announcements of updates to this document, please allow the "STRONGLY RECOMMENDED" list of ports rather than the "minimal" one.)

- **Outbound to Internet**

WHITELIST ENTRIES	PORTS	DESCRIPTION
camect.securecomwireless.com	10443/TCP	DMP XV Gateways cloud services & configuration
video1.whitelist.camect.com video2.whitelist.camect.com video3.whitelist.camect.com video4.whitelist.camect.com	STRONGLY RECOMMENDED (to avoid maintenance issues): TCP: all ports UDP: all ports minimal list: TCP: 3478, 19302 UDP: 3478, 19302	WebRTC traffic and associated infrastructure for video streaming. Currently this is limited to TURN and STUN services on ports 3478 and 19302. Allowing all ports allows flexibility for changes to be made to this in future.
cloud1.whitelist.camect.com cloud2.whitelist.camect.com cloud3.whitelist.camect.com cloud4.whitelist.camect.com	STRONGLY RECOMMENDED (to avoid maintenance issues): TCP: All ports UDP: 53 minimal list: TCP: 9998, 8888, 3443, 443, 80 UDP: 53	Camect's main cloud service, used to support operation, management, and licensing of gateways, coordination to set up WebRTC connections, monitoring of gateway health, and a ddns-like service for gateways.
connectivity1.whitelist.camect.com connectivity2.whitelist.camect.com connectivity3.whitelist.camect.com connectivity4.whitelist.camect.com	ICMP ping and ping response	Used to ensure gateway network hardware is working and able to connect to the internet properly. Destinations are tested using ICMP ping.
ntp1.whitelist.camect.com ntp2.whitelist.camect.com ntp3.whitelist.camect.com ntp4.whitelist.camect.com	UDP: 123	Network time protocol servers that are used to keep the time accurate.
swupdate1.whitelist.camect.com swupdate2.whitelist.camect.com swupdate3.whitelist.camect.com swupdate4.whitelist.camect.com	TCP: 443, 80	AI Model updates. A gateway can operate without model updates, but users will be unable to receive improved AI detections.
aimodel1.whitelist.camect.com aimodel2.whitelist.camect.com aimodel3.whitelist.camect.com aimodel4.whitelist.camect.com aimodel5.whitelist.camect.com	TCP: 443, 80	AI model updates and feedback sharing. A gateway can operate without model updates, but users will be unable to report AI problems or to receive the results of model updates from their feedback and feedback of others.
dns1.whitelist.camect.com dns2.whitelist.camect.com dns3.whitelist.camect.com dns4.whitelist.camect.com	UDP: 53	DNS servers that are known to work reliably with the software update system. Software update validation has stringent requirements on DNS – we have seen many cases where software updates fail even though local DNS servers appear to be usable for other purposes.
DNS	Port 53	Ensure the XV Gateways can send and receive DNS traffic.

- **Outbound to Local Network**

9011/TCP: XV Gateway to DMP panel communication.

554/TCP: XV Gateway to camera video streaming.

554/UDP: XV Gateway to camera video streaming.

3702/UDP: WS-Discovery for XV Gateways to the DMP panel, camera (ONVIF discovery) and future support. WS-Discovery is a multicast protocol.

7946/TCP and 7946/UDP: for future support when clustering AlarmVision devices.

1025/UDP: for future support when clustering AlarmVision devices.

- **Inbound from Local Network**

  9001/TCP: DMP panel to XV Gateway communication.

  7946/TCP and 7946/UDP: for future support when clustering AlarmVision devices.

  1024/UDP: for WS-Discovery responses from the DMP Panel. WS-Discovery is a multicast protocol.

  1025/UDP: for future support when clustering AlarmVision devices.

- **Video Verification at Central Station**

WHITELIST ENTRIES	PORTS	DESCRIPTION
h.home.camect.com	443/TCP	for Camect web services
video1.whitelist.camect.com video2.whitelist.camect.com video3.whitelist.camect.com video4.whitelist.camect.com	STRONGLY RECOMMENDED (to avoid maintenance issues): TCP: all ports UDP: all ports minimal list: TCP: 3478, 19302 UDP: 3478, 19302	WebRTC traffic and associated infrastructure for video streaming. Currently this is limited to TURN and STUN services on ports 3478 and 19302. Allowing all ports allows flexibility for changes to be made to this in future.
cloud1.whitelist.camect.com cloud2.whitelist.camect.com cloud3.whitelist.camect.com cloud4.whitelist.camect.com	STRONGLY RECOMMENDED (to avoid maintenance issues): TCP: All ports UDP: 53 minimal list: TCP: 9998, 8888, 3443, 443, 80 UDP: 53	Camect's main cloud service, used to support operation, management, and licensing of gateways, coordination to set up WebRTC connections, monitoring of gateway health, and a ddns-like service for gateways.

<u>IMMIX Integration:</u>

- **Inbound (Must be forwarded from the IMMIX IP Address to the XV Gateway)**

  HTTPS: TCP/443

  - Used by IMMIX to gather camera and alert information from the XV Gateway

  RTSP: TCP/554 and UDP/554

  - Video streaming from XV Gateway to IMMIX

  Source: Hostname provided by your IMMIX provider

- **Outbound**

  SMTP: TCP/25

  - Alerts from XV Gateway to IMMIX
  - If your ISP blocks port 25, try port 1025.
  - If port 1025 is also blocked, contact your ISP

  Destination: Same address used in the SMTP Server field in **Dealer Admin Final Setup**

<u>Other Standard Ports:</u>

- **UDP Port 53 (DNS):** A common port that allows host name to IP resolution, and is an IP standard.
- **TCP Port 443 (SSL/TLS):** A common port that secures HTTP communications to web servers.
- **TCP Port 80 (HTTP):** The standard port for unencrypted HTTP communication. TLS is a preferred communication method as all communication is encrypted.

866-266-2826
DMP.com
INTRUSION • FIRE • ACCESS • NETWORKS
2500 North Partnership Boulevard
Springfield, Missouri 65803-8877