

## LOCATION NETWORK CONFIGURATION

netPark is a cloud-based software application, so your network will play a vital role in how the netPark system performs. This section details the different network requirements and outbound firewall rules that netPark requires to function properly. If requested/required, a network overview document can be provided.

### OUTBOUND FIREWALL REQUIREMENTS

Outbound TCP 443 to "[np1.netpark.us](https://np1.netpark.us)"

- Continuous use
- Used by PCs, mobile devices, and the NIM to access the netPark system
- Multiple and variable IPs since the service is load balanced for capacity and availability

Outbound TCP 443 to "[tripos.vantive.com](https://tripos.vantive.com)" (Required for all netPark Pay EMV terminals)

- Continuous use
- Used by Verifone and Ingenico EMV devices for credit card processing

Outbound TCP/UDP 9001 to "[device.tripos.vantiv.com](https://device.tripos.vantiv.com)" (Required for all netPark Pay EMV terminals)

- Continuous use
- Used by Verifone and Ingenico EMV devices for credit card processing

Outbound TCP 443 to "[iptran1.dsipscs.com](https://iptran1.dsipscs.com)" (Required for all netPark Pay EMV unattended terminals)

- Continuous use
- Used by Verifone and Ingenico EMV devices for credit card processing

Outbound TCP 443 to "[iptran2.dsipscs.com](https://iptran2.dsipscs.com)" (Required for all netPark Pay EMV unattended terminals)

- Continuous use
- Used by Verifone and Ingenico EMV devices for credit card processing

Outbound TCP 5080 to "[trancloud.dsipscs.com](https://trancloud.dsipscs.com)" (Required for all netPark Pay EMV unattended terminals)

- Continuous use
- Used by Verifone and Ingenico EMV devices for credit card processing

Outbound TCP 443 to "[prod.ssl53.com](https://prod.ssl53.com)" (Required for all netPark Pay EMV unattended terminals)

- Continuous use
- Used by Verifone and Ingenico EMV devices for credit card processing

Outbound UDP 53 to "8.8.8.8/8.8.4.4" (Can utilize client's DNS servers as an alternative)

- DNS Servers for NIM
- Continuous use
- DNS resolution
- Google's public DNS servers

Outbound TCP/UDP 5938 to "\*.teamviewer.com" and "\*.dyngate.com"

- Continuous or may be restricted by the client until needed
- For TeamViewer remote PC support (see below for further information)
- Multiple and variable IPs since the service is load balanced for capacity and availability

Outbound UDP 1194 to "nama.netpark.us" (if self-park equipment is utilized at the client facility)

- Should be restricted by the client until needed
- For remote NIM support (see below for further information)
- Multiple and variable IPs since the service is load balanced for capacity and availability

Outbound TCP 587 to "mail.netpark.us" (if self-park equipment is utilized at the client facility)

- Continuous or may be restricted by the client until needed
- Automatic email of NIM diagnostic logs for technical support
- Multiple and variable IPs since the service is load balanced for capacity and availability

## NETWORK REQUIREMENTS

Our data requirements are small. For regular netPark use (anything excluding Damage Pictures and LPR), a standard **5Mbps Down, 1Mbps Up** should be sufficient. The better the latency, the more responsive the system will feel. If you are planning on taking automated damage images or doing LPR, a larger connection will be needed. In this case we would recommend **25Mbps Down, 10Mbps Up** as a minimum for 2 lanes in, 2 lanes out configuration. Higher bandwidth may be required if there are several self-park devices running.

## TEAMVIEWER (T.V.) REMOTE PC SUPPORT

We do not have full-time access to client networks or devices. When remote assistance is needed, we have the user initialize the support session so they are in full control. This is the standard process:

1. First, the user contacts netPark support to request a support session
2. The user is then asked to activate the customized netPark support client\*
  1. This is typically done through the [Desktop Application](#)
  2. If the Desktop Application is not available, users are typically directed to <http://www.netparkhelp.com> or <https://www.netpark.us/support>
3. Once the client is activated, assuming firewall permissions are enabled, T.V. will prompt the client to allow or deny session
4. If user grants access, the session is initialized
5. At any point during the session the user can terminate the connection by closing the application or restarting the computer
6. Once the session is terminated, the process must be repeated before a new session can be established

\* This client does not get installed on the PC and is only active for the duration of the support session

## SELF-PARK EQUIPMENT REQUIREMENTS

If your location is also having self-park equipment installed, below is a list of network information required for configuration of the netPark supplied self-park equipment. We will need the below information before we can ship out any equipment from netPark.

### NETWORK INFORMATION REQUIREMENTS

- Static IP Addresses (MAC based Static IP addresses are acceptable)
  - 1 Private, internal static IP - NIM
  - 1 Private, internal static IP per - Self-park Device, Damage/LPR Camera & ADAM device
- Subnet
- Gateway

**NOTE: THE NIM DOES NOT NEED AND SHOULD NOT BE GIVEN UNFILTERED INBOUND INTERNET ACCESS.**

**SHIPPING NOTE: THE ABOVE STATIC IP ADDRESSES, SUBNET AND GATEWAY INFORMATION MUST BE SUPPLIED TO NETPARK BEFORE ANY EQUIPMENT WILL BE SHIPPED. FAILURE TO DO SO COULD RESULT IN DELAYS IN THE INSTALLATION AND SETUP OF THE HAMILTON SELF-PARK EQUIPMENT.**