NoPileups Data Connection Overview

VERSION 2.11, REVISED 09/2023

NoPileups Support
(833) 667-4538 | support@NoPileups.com | www.drb.com/npu

Remote NoPileups Local Server Access Using BeyondTrust (formerly "Bomgar")

NoPileups uses BeyondTrust to access NoPileups local servers. BeyondTrust connects to the internet using TCP port 443.

Before accessing a local server remotely, NoPileups technical support representatives must be connected to DRB Systems' secured network. This requires both an active domain account and successful two-factor authentication. Domain credentials and two-factor authentication must then be re-verified to launch BeyondTrust. After connecting to the local server, a password must be entered as described in "Password Policies". DRB Systems' domain accounts are subject to a password expiration policy and complexity requirements.

The beginning time, end time, representative identity and video of each support session are logged for 6 months. NoPileups customers do not have access to this information but can request it by contacting NoPileups support.

Password Policies

Each NoPileups local server has unique login credentials which can tailored to fit existing customer domain security policies (including length, complexity, and expiratory requirements). All passwords are stored in a 1Password for Business vault and secured using end-to-end AES-256 encryption. For more information about 1Password for Business, see https://support.1password.com/1password-security/.

To access the 1Password vault, each NoPileups technical support representative authenticates using a unique password and two-factor authentication. Password access is restricted to NoPileups technical support representatives.

Windows sessions on NoPileups local servers lock after 15 minutes of inactivity. This does not affect viewing the NoPileups Live view at the location from the Load on Display or configured manager's workstations.

NoPileups Software Passwords

If requested by the customer, NoPileups support can configure NoPileups so that a password is required to access the Live View or stop replays. Multiple user accounts can be created, and each can have unique permissions and passwords.

PCI Compliance

NoPileups does not require any customer data or information from point-of-sale (POS) systems.

When installed following NoPileups best practices, the NoPileups local server is connected to subnets that are separated from existing POS-connected networks by hardware or software firewalls.

Network Access

The NoPileups local server requires access to the listed domains. This allows NoPileups technical support representatives to monitor the performance of NoPileups and push the latest NoPileups software updates to the local server.

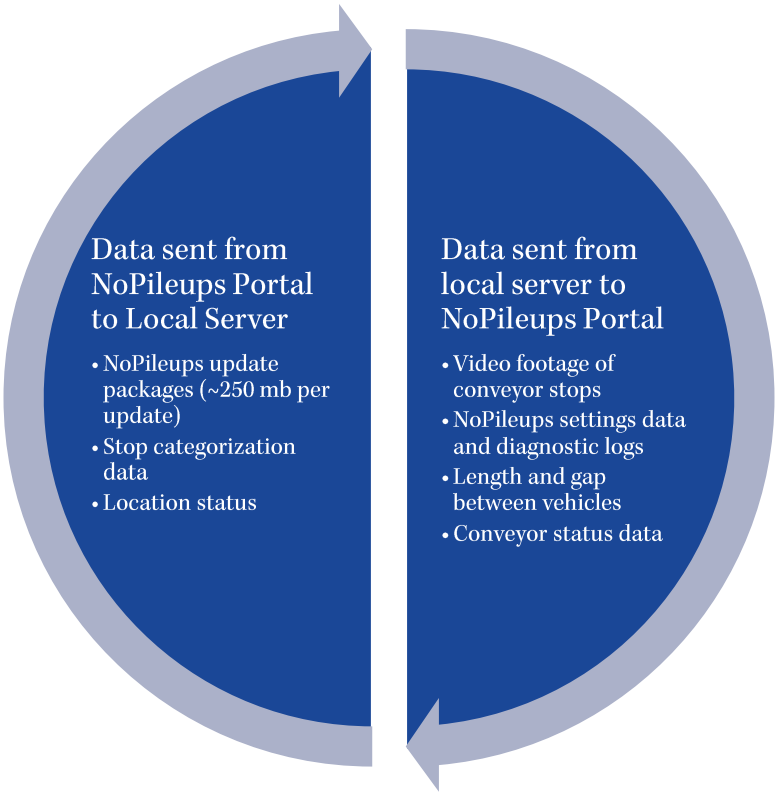
- https://portal.nopileups.com – NoPileups Service Portal
- https://update.nopileups.com – NoPileups Monitoring and Update Server
- https://connect.drbsystems.com – Beyond Trust (Bomgar) Remote Access

Data Storage

Car wash operation data is stored in a database on the NoPileups local server. This data includes conveyor running status, vehicle length and spacing, and tunnel environment information when the conveyor stops. This data is then synced to the NoPileups Portal for long term storage using the process outlined below.

Data Transfer

After initial setup, the NoPileups the local server communicates with the NoPileups Portal at 5-minute intervals, and when a conveyor stop occurs. This data synchronization is required for NoPileups to operate. The local server sends stop videos and software settings to the NoPileups Portal so that they can be viewed by NoPileups Technical Support Representatives to verify proper software operation. The local server then collects stop categorization information, the location's status and NoPileups update files if any are available. If the NoPileups local server is unable to contact the NoPileups Portal for 14 days, a message will be displayed on the Live View and the software will be disabled until it reconnects.



Network Ports

NoPileups requires port 443. This allows connections the NoPileups local server to connect to the NoPileups Portal using SSL and allows the server to be accessed by NoPileups support using BeyondTrust remote access.

Network Connections

NoPileups recommends network connections based on the type of tunnel controller being used at the location.

TunnelWatch4 and Newer

NoPileups connects to DRB's TunnelWatch version 4 and newer using the following API endpoints over a direct TCP-IP connection:

/api/authenticate	**Returns a security token used for all other API calls.**
/api/override/device	Stops the conveyor
/api/graph-data	Returns vehicle dimensions
/api/status	Returns the conveyor running status.

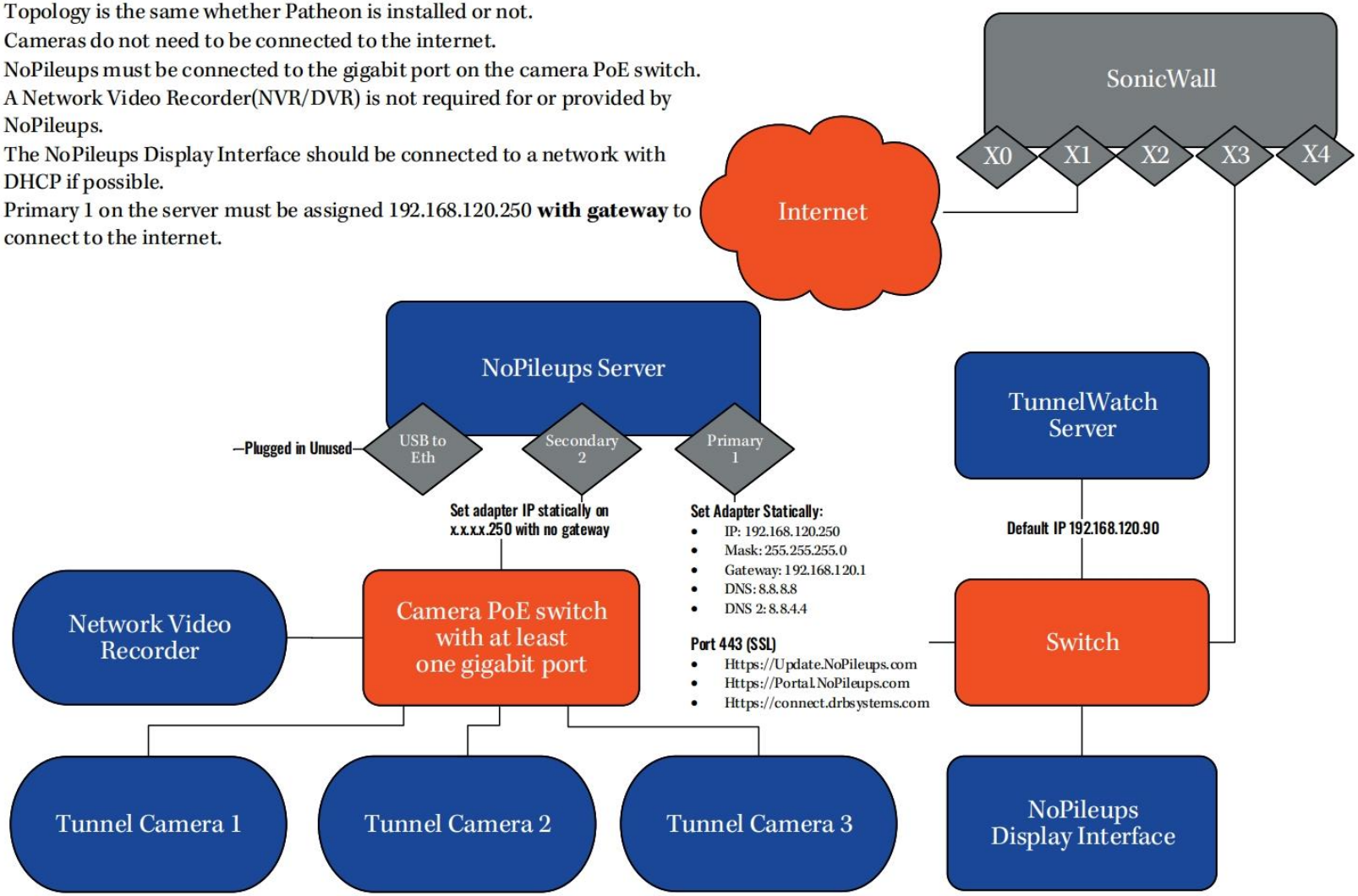
NoPileups uses a TunnelWatch account with a unique password at each location. This information is stored in the 1Password for Business vault as described above in "Password Policies".

NoPileups recommends the following logical network connections when being installed at a location using TunnelWatch 4 or newer: (see next page)

NoPileups Network Topology
TunnelWatch 2021

Version 1.1, Revised 05/2021

- Topology is the same whether Patheon is installed or not.
- Cameras do not need to be connected to the internet.
- NoPileups must be connected to the gigabit port on the camera PoE switch.
- A Network Video Recorder(NVR/DVR) is not required for or provided by NoPileups.
- The NoPileups Display Interface should be connected to a network with DHCP if possible.
- Primary 1 on the server must be assigned 192.168.120.250 **with gateway** to connect to the internet.



Other Tunnel Controllers

When connecting to a tunnel controller that is not DRB's TunnelWatch 4 or newer, NoPileups uses an ADAM 6060 module. The NoPileups local server connects to the ADAM 6060 using a direct TCP-IP connection. The ADAM 6060 then interprets and sends electrical signals to and from the tunnel controller. This allows NoPileups access to the following signals:

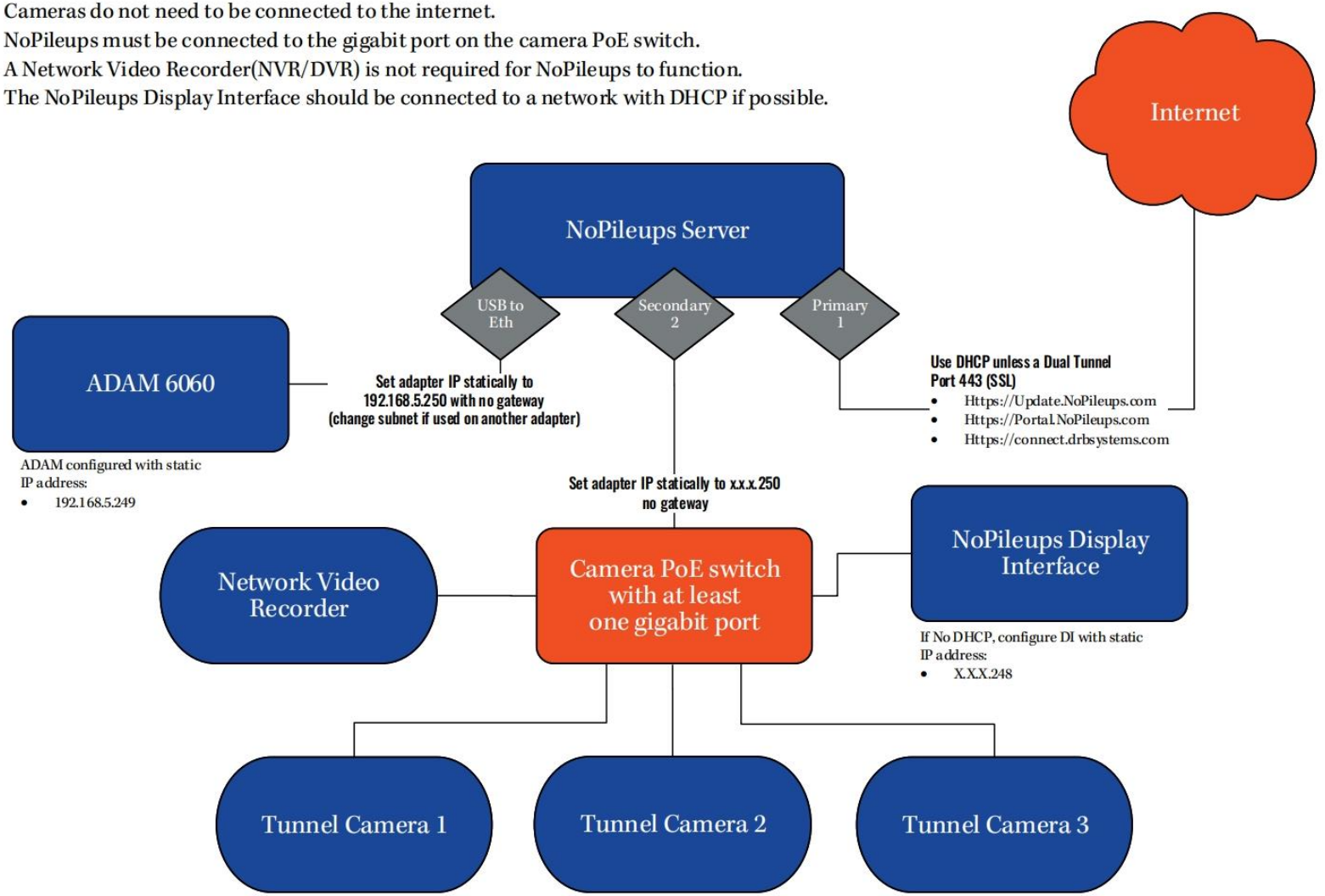
- Conveyor running status
- Photo eye status (used for vehicle detection)
- Pulse signal
- Conveyor e-stop
- Conveyor start (used for NoPileups Smart Exit)
- (Optional) input device (light or horn)

NoPileups recommends the following logical network connections when being installed at a location using a tunnel controller that is not TunnelWatch 4 or newer: (see next page)

NoPileups Network Topology
ADAM 6060

Version 2.4, Revised 05/2021

- Cameras do not need to be connected to the internet.
- NoPileups must be connected to the gigabit port on the camera PoE switch.
- A Network Video Recorder(NVR/DVR) is not required for NoPileups to function.
- The NoPileups Display Interface should be connected to a network with DHCP if possible.



NoPileups Local Server Hardware

- Intel i5-8500T @2.1 GHz
- 16 GB RAM
- 1 TB SATA 3 SSD
- Windows 10 LTSB x64 version 2004
- x2 RJ45 Ports
- x4 USB Ports

NoPileups Email Reports

The NoPileups Portal generates reports based on the location data that is synced from the NoPileups local server to the NoPileups Portal. It then automatically emails a report weekly to users who have been configured to receive them. During installation, NoPileups will ask for contact information for individuals who should receive reports. Required information includes:

- First and Last Name
- Email
- Phone Number
- Job Role

Users can be configured to receive reports for all locations in an organization, or specific locations. They can also choose to have an organization-wide summary page included in their report.

Users can unsubscribe from NoPileups reports by contacting NoPileups support.

More Information

For more information about NoPileups, contact NoPileups support at (833) 667-4538 or support@NoPileups.com.