pennsylvania
DEPARTMENT OF TRANSPORTATION

494-16-02

DATE: February 12, 2016

SUBJECT: Traffic Signal Remote Communication Policy and Guidance Document

TO: District Executives

FROM: Richard N. Roman, P.E., Director *Richard Roman /s/*
Bureau of Maintenance and Operations

This Strike-off Letter identifies the guidelines to follow when remotely connecting to a traffic signal in the Commonwealth network. This guidance is considered "cost-neutral" and "time-neutral."

The purposes of this document is to:

- Establish a Commonwealth policy on remote traffic signal communication
- Describe the operations of remote traffic signal communications
- Establish a formal process to request access to the Commonwealth network
- Identify the roles and responsibilities in establishing the remote communication
- Provide guidelines to develop requirements for the remote communication
- Provide guidelines to design remote communication
- Establish a formal process/procedure for establishing the remote communication using the Commonwealth network
- Establish a formal process to access the Commonwealth network, which in turn will allow anyone with proper access rights to access traffic signals remotely

Should you have any questions, please contact Daniel Farley, Chief,Traffic Operations Deployment and Maintenance Section, at 717.783.0333.

Attachments

4940/MLD/hmq

cc: Renee Sigel, Division Administrator, FHWA Pennsylvania Division Office
Assistant District Executives – Maintenance
Assistant District Executives – Construction
Assistant District Executives – Design
Maintenance Service Executives
District Traffic Engineers
Distrct Bridge Engineers
District Permit Managers
Richard Roman, P.E., Director, BOMO
Brian Thompson, P.E., Director, BOPD
Division Chiefs, Bureau of Project Delivery
Division Chiefs, Bureau of Maintenance and Operations
Daniel Farley, Chief, Traffic Operations Deployment and Maintenance Section, BOMO
Matthew DePaoli, Senior Civil Engineer, BOMO

pennsylvania
DEPARTMENT OF TRANSPORTATION

PENNDOT TRAFFIC SIGNAL REMOTE COMMUNICATION

POLICY AND GUIDANCE DOCUMENT

February 2016

PennDOT Traffic Signal Remote Communication: Policy and Guidance Document

CONTENTS

EXHIBITS

APPENDICES

1 - INTRODUCTION

Advancements in technology have made it possible to communicate with traffic signal systems remotely from a central location. A central location could be a municipal office, PennDOT Engineering District office, PennDOT Central Office, or any workstation/laptop with access to an internet connection. Advantages of remote communication include but are not limited to, the ability to remotely:

- Monitor the working status of traffic signal systems
- Monitor the operations of traffic signal systems
- Evaluate the performance of traffic signal systems
- Troubleshoot traffic signal systems
- View live video of traffic signal systems to identify operational issues or aid in incident management
- Upgrade firmware
- Upload/download data to traffic signal systems without the need for a field visit

Typically, remote communication is established using a third party public communication network for exchanging information between the field and the central location. This form of communication has several security challenges. PennDOT has created a private Commonwealth communication network (Commonwealth Network) with high security standards to allow for secure remote communication between field traffic signal systems and the central location. Any traffic signal owner who either currently communicates remotely with field traffic signal systems or would like to remotely communicate with a field traffic signal system can use PennDOT's Commonwealth Network to establish the remote communication.

The purpose of this document is to:

- Section 2 - Establish a policy on traffic signal remote communication
- Section 3 - Describe the operations of traffic signal remote communication
- Section 4 - Identify the roles and responsibilities in establishing remote communication
- Section 5 - Provide guidelines to develop requirements for remote communication
- Section 6 - Provide guidelines to design remote communication
- Section 7, 8, 9 - Establish a formal process/procedure for establishing remote communication using the Commonwealth Network
- Section 10 - Establish a formal process to access the Commonwealth network, which in turn will allow anyone with proper access rights to access traffic signals remotely

Use of the Commonwealth's Network by signal owners will ensure that established remote communication is compatible with the Next Generation Advanced Traffic Management System (ATMS) Software.

2 - TRAFFIC SIGNAL REMOTE COMMUNICATION POLICY

PennDOT has established the following policy for establishing remote communication between traffic signal systems and a central location.

"PennDOT requires that the remote communication connection between the traffic signal system(s) and any central location established with State or Federal funds use the Commonwealth communication network." Any traffic signal owner in Pennsylvania could leverage the Commonwealth's communication network for remote communication.

Using the Commonwealth's communication network has the following advantages:

- The Commonwealth's communication network is secure
- The Commonwealth will provide IT support and expertise for remote communication
- The Commonwealth network will allow third parties (vendors/manufacturers) to have secure access to traffic signal systems from any remote location

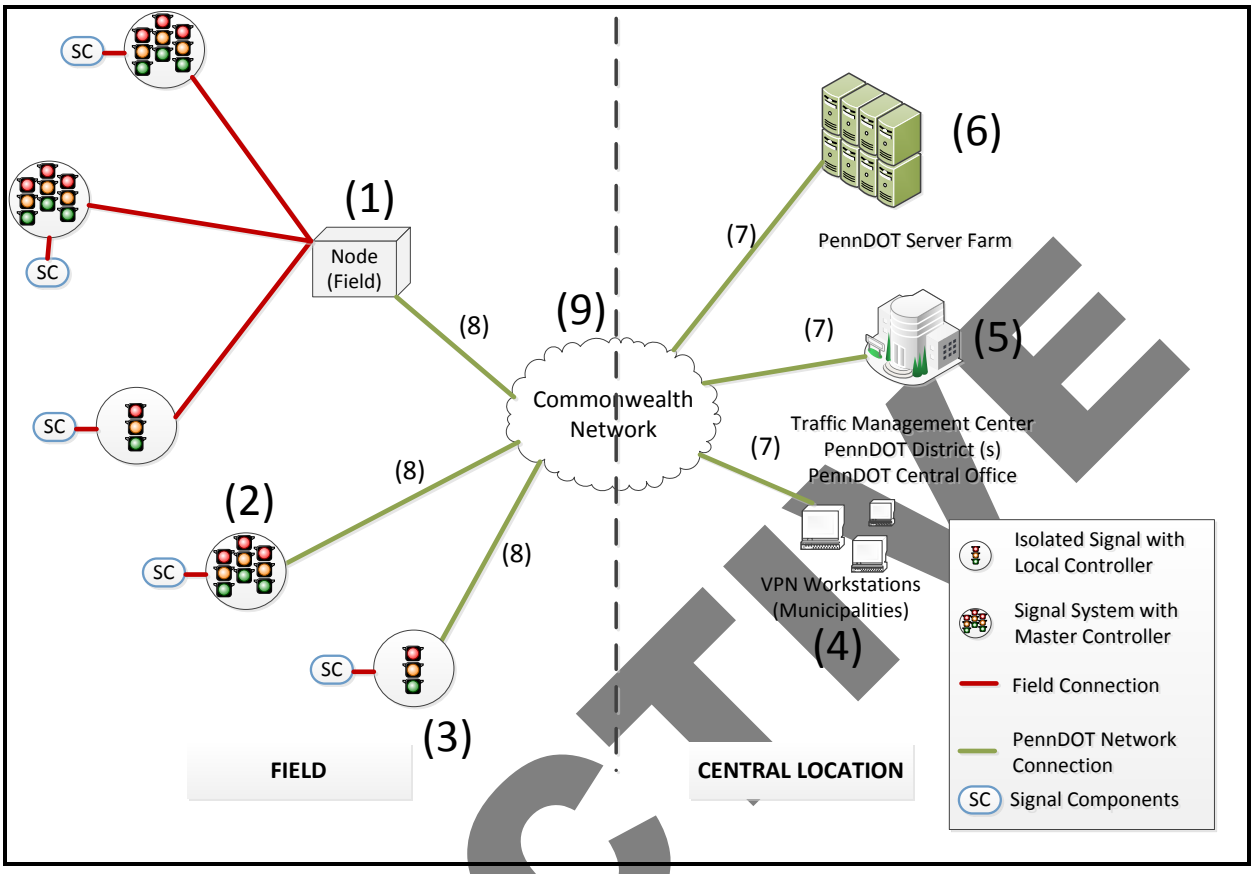
3 - CONCEPT OF OPERATIONS

Most traffic signals and signal systems in Pennsylvania operate independently in the field without any active participation from the traffic signal system owners/operators. Operations of the traffic signal systems are not actively monitored. Any issues with the signal system operations go unnoticed until the public complains about it or maintenance personnel happen to notice in the field. Remote monitoring and controlling functions will provide additional capabilities to the owners/operators of the signal systems to proactively operate and maintain the traffic signal systems in a good state of repair.

PennDOT has setup a statewide, secure, internet protocol (IP) based digital private communication network. Accessibility to the network is provided only to those with accessibility clearances (typically signal owners and their designees, PennDOT District traffic personnel, consultants, and manufacturers). Traffic signal owners can leverage the secure Commonwealth Network to establish remote communication between the field traffic signals' communication system and the central location. Once both the traffic signal systems in the field and the central location are connected to the Commonwealth Network, the field traffic signal systems' operations and performance can be monitored and controlled remotely from any central location.

Exhibit 1 depicts the concept of operations of communication between the traffic signal systems in the field and the remote central locations via the secure Commonwealth Network. To describe the communication system in terms more familiar to signal/traffic professionals, think of the Commonwealth Network as a roadway network. Think of the traffic signal systems in the field as the origin of the trip and the remote central locations (which could be work stations in municipal buildings, PennDOT Districts, PennDOT Servers, and Traffic Management Centers) as the destination of the trip. As vehicles with proper registration can use the roadway network to go between the origin and destination, stakeholders with proper credentials can use the Commonwealth Network to access the traffic signal systems from the central location.

Exhibit 1: Concept of Operations



To more thoroughly explain the concept of operations, each component of the Commonwealth Network is numbered in **Exhibit 1** and described as follows:

(1), (2), and (3) represent the traffic signals (isolated or a signal system) and related internal communication (red lines) system in the field. The signal system field communication (communication along a corridor or within a closed loop system) and associated hardware is not considered part of the remote communication. The 'field' side of the signal system can include things such as an isolated traffic signal system with a local controller, a coordinated traffic signal system with a master controller or processor, and an aggregated (in the field) system of traffic signals. Signal components (SC) including video [multiple users accessing the video may degrade quality - refer to manufacturer specifications]/other detections, conflict monitoring unit, power relay, and any other equipment connected to the signal systems may also be considered as part of the signal as designated by numbers (1), (2) and (3). If desired, all these components can be 'communicated with' via the Commonwealth Network as long as they are IP based;

(4) and (5) represent the work stations in the remote central location (which may be a municipal building, Traffic Management Center (TMC), PennDOT District(s) buildings, PennDOT Central office, etc.,) that the stakeholders with proper credentials can use to access the traffic signal systems through the Commonwealth Network. The remote work stations should have access to internet and have Virtual Private Network (VPN) installed. Any other external stakeholders including law enforcement who may want to access the field devices at the intersection from a remote location will need access to the Commonwealth Network through the VPN.

(6) represents the PennDOT Server Farm, which is maintained by PennDOT. The server farm may host the traffic signal system firmware. Currently, the information from the traffic signal systems cannot be stored in the

Commonwealth Network. The signal owners can use the Commonwealth Network to access the information from the traffic signal systems. However, the signal owners are responsible for storing the information in their own workstations/internal network location.

(7) represents the communication of the central location to the Commonwealth Network. For faster access to the traffic signal system information, PennDOT requires an internet connection with a minimum guaranteed upload/ download speed of 3 Mbps at any central location.

(8) represents a backhaul connection (in the field) to the Commonwealth Network (for faster access to the traffic signal system information, PennDOT requires an internet connection with a minimum bandwidth of 3 Mbps at field).

(9) represents the Commonwealth Network.

4 - ROLES AND RESPONSIBILITIES

REMOTE COMMUNICATION CONNECTION

Exhibit 2 identifies the roles and responsibilities for establishing traffic signal remote communication connections for either signal owner or PennDOT lead projects. Signal owner refers to the municipality who owns, maintains, and operates the signals. Please note that every project is unique and responsibilities of different stakeholders may vary. The below roles and responsibilities are for a typical remote connection project.

Exhibit 2: Remote Communication Connections, Roles and Responsibilities

Task	Signal Owner	PennDOT District	PennDOT Central Office	PennDOT IT
Preliminary Assessment				
Determine remote communication needs	P	S (1)		
Design and Review				
Develop requirements for remote traffic signal system communication	P	(1)		
Develop field communication design	P	S (1)	S	S
Design backhaul communication between the traffic signal system and the remote location (coordinate with PennDOT)	P	(1)	S	S
Approve, deny, or request additional information (field communication)		P		
Approve, deny, or request additional information (remote communication)			P	S
Installation/Testing				
Installation of communication devices	P	(1)		
Inspection of communication devices	P	(1)		
As-built drawings	P	(1)		
Testing of field communication	P	S (1)		
Testing of backhaul communication	P	(1)	S	S
Department acceptance		P	S	S
Operation				
Traffic signal system	P			
Field communication system	P			
Backhaul communication system				P
Maintenance				
Traffic signal system	P			
Field communication system	P			
Backhaul communication system				P

P – Primary responsible party
S – Secondary responsible party
(1) – PennDOT is the primary responsible party for PennDOT construction projects on state highways but local authorities may be responsible for a share of the costs

Signal owners are responsible for assessing the needs for remote traffic signal system communication with inputs from the PennDOT Districts during the scoping meeting. Factors including traffic volume and congestion at the intersection/corridor and the importance of the corridor to the region should be considered during the needs assessment. These roles would be reversed on PennDOT construction projects. Once it is determined that a

particular traffic signal system requires remote access, the PennDOT District will inform PennDOT Central Office of the need for remote communication, which in turn will communicate the need to PennDOT IT.

Once, the need for remote communication is determined, signal owners (or PennDOT in the case of PennDOT construction projects) either work with a consultant or work internally to develop the requirements and design for the remote communication. The field communication design will be approved by the PennDOT District and the backhaul communication will be reviewed by both PennDOT Central Office and PennDOT IT and finally approved by PennDOT Central Office.

Signal owners (or PennDOT in the case of PennDOT construction projects) are responsible for the installation and testing of the field devices. The signal owners are responsible to coordinate with PennDOT Central Office and IT to test the remote communication. Final remote communication will be approved by PennDOT IT.

Once the remote communication is established, the signal owners are responsible for the operations and maintenance of the traffic signal systems. The remote communication system will be operated and maintained by PennDOT IT.

Should any issue arise with the field/backhaul communication system, the signal owner will be responsible for initial troubleshooting with assistance from PennDOT IT.

GENERAL TRAFFIC SIGNAL PROJECTS

Please note that the roles and responsibilities for the plan development and construction of traffic signal systems remains as outlined in **Exhibit 3** which is an excerpt from PennDOT Publication 46, Chapter 4, Exhibit 4-1.

Exhibit 3: General Traffic Signal Projects, Roles and Responsibilities

Task	Local Authorities	PennDOT
Preliminary Assessment		
Process review	X	(1)
Site investigation	X	(1)
Data collection	X	(1)
Study development	X	(1)
Municipal concurrence	X	
Application Submission		
TE-952 form, certifying that the local officials have approved a municipal resolution committing resources to install and maintain signals if approved	X	
Study by P.E., complete with intersection plan view and warrant analysis	X	(1)
Maintenance agreement	X	
Department Application Review		
Approve, deny, or request additional information		X
Authorize plan development		X
Explain required detail based on type of project, e.g., if modifying an existing permit simplifies the level of detail		X
Design and Review		
Develop permit plan sheets with signal heads, supports, detectors, controller, phasing diagram, signs, pavement markings, etc.	X	(1)
Develop construction plans and specifications	X	(1)
Authorization to construct	X	X
Construction		
Inspection	X	(1)
As-built drawings	X	(1)
Operational Validation		
30-day testing	X	(1)
Department acceptance		X
Maintenance		
Budgeting	X	
Response and preventative maintenance	X	
Operational maintenance	X	
Design modifications	X	
(1) – PennDOT would generally perform this function for PennDOT construction projects on state highways but local authorities may be responsible for a share of the costs		

5 - REQUIREMENTS GUIDELINE

This section provides guidelines for identifying requirements for accessing traffic signal systems through the Commonwealth Network.

FUNCTIONAL REQUIREMENTS

Functional requirements identify what the system should do. Consider the following functional requirements for accessing traffic signals through the Commonwealth Network. The communication system may:

- Allow remote time synchronization among controllers to establish a common time reference to provide a common cycle length and to establish appropriate offsets
- Allow remote upload and download of timing plans and other parameters to the field controller
- Allow remote monitoring of field equipment status and reporting of equipment malfunctions
- Allow remote selection and implementation of timing plans
- Support adaptive control algorithms
- Allow remote monitoring and control of video information from the central location
- Allow remote monitoring and control of other system detectors
- Allow remote upload of logs developed by emergency vehicle signal preemption equipment
- Support signals required for transit priority
- Allow remote monitoring and control of traffic signal controller conflict monitor

OPERATIONAL REQUIREMENTS

Operational requirements identify who or what performs the functions. Consider the following operational requirements for accessing traffic signals through the Commonwealth Network. The communication system may:

- Allow the functions to be performed by signal owners, PennDOT, and/or their representatives with proper authority
- Allow the functions to be performed from any work station with access to the Commonwealth Network
- Allow the functions to be performed only by authorized personnel with proper credentials

PERFORMANCE REQUIREMENTS

Performance requirements identify how well the system should perform for successful functioning of the communication through the Commonwealth Network. Consider the following performance requirements for accessing traffic signals through the Commonwealth Network. The communication system may:

- Allow the functions to be performed in near real time (or any periodic interval)
- Allow the video images to be seen at the workstations at least at a rate of 30 frames per second

SECURITY REQUIREMENTS

Accessing traffic signals through the Commonwealth Network requires following the Commonwealth's security protocol. All the communication equipment used for communication between the traffic signal and the central location shall be approved and configured by PennDOT.

6 - DESIGN GUIDELINES

During the design stage, the signal owner will: design for the field and backhaul communication based on the system requirements; submit a request for a Commonwealth of Pennsylvania (CWOPA) account; submit a request for approval of proprietary communication devices; and submit a request for IP addresses.

DESIGN

Traffic signal communication systems actually refer to two distinct communication functions; the field communication of the system, to enable interconnection of and communication among signalized intersections; and the networking communication system, to enable remote access to signal data and information. These are typically referred to as field communication and backhaul communication. The design of both the field and backhaul communication of the signal system will be accomplished by the signal owner per roles and responsibilities table. However, for the backhaul design, the signal owner (or the PennDOT in the case of PennDOT construction projects) will coordinate the design and plans with both PennDOT Central Office and the PennDOT IT Department.

The design of the communication system to satisfy the requirements (identified in the previous section) will consider the following design factors and the signal owner should be prepared to address the needs of the system as it relates to these factors to coordinate the design with PennDOT IT:

- Throughput
- Communication interval (real time vs non real-time)
- Communication technology including wireless and wireline and their respective limitations
- Existing cable and conduit infrastructure
- Performance
- Redundancy and reliability
- Security
- Cost

Signal owners (or the PennDOT in the case of PennDOT construction projects) will develop alternative high-level designs and compare them with respect to the defined selection criteria to identify the superior design. They will also conduct cost-benefit analysis for alternatives over the life span of the communication system prior to finalizing the communication system design.

During the design, the signal owner (or PennDOT in the case of PennDOT construction projects) will determine the need for internet connection in the field to communicate with the Commonwealth network. Based on the quantity of field equipment, number of intersections, types of devices, and the bandwidth requirements of the field devices, the signal owner will determine the bandwidth needed for the internet connection.

Refer to Chapter 9, PennDOT Publication 646, Intelligent Transportation Systems Design Guide, for additional guidelines on designing the communication between the field and the central location.

REQUEST FOR IP ADDRESSES

The Commonwealth Network is a private network owned by the Commonwealth. Any traffic signal system devices using the Commonwealth Network should have the IP addresses provided by PennDOT. Complete the form in **Appendix A** to request a block of Commonwealth specific IP addresses during the design phase. Request for Commonwealth specific IP addresses need the following information:

- Number of corridors (consider traffic signal systems interconnected to each other as one corridor)
- Number of intersections within a corridor
- Number of traffic signal devices within an intersection which would require an IP address

Exhibit 4 on the next page identifies a sample IP address request form for a corridor with five (5) intersections and various field IP devices. PennDOT Central Office recommends requesting a minimum of 10 IP addresses per intersection even if there are fewer IP devices at an intersection to account for future expansion. If additional intersections within a corridor are expected to be connected to the Commonwealth network within the next three (3) to five (5) year timeframe, request additional spare IP addresses for future expansions. If there are multiple corridors (which are not interconnected) in a project, submit one (1) IP address request form for each of the corridors. PennDOT IT will review the request for IP addresses and provide a block of IP addresses, which can be assigned to individual communication devices.

Exhibit 4: Sample IP Address Request Form

Project Information (Use one for each corridor)				
Project Name:	Township Name Remote Traffic Signal Communications			
District:	District X-0			
County:	County Name			
Township:	Township Name			
Corridor Name:	Corridor B			
Requesting Entity				
Entity Name	**Role (Underline one)**	**Phone**		
Consultant C	Contractor/Vendor/ Municipality/Consultant	**(717) XXX-YYYY**		
Person Name	**Others**	**Email**		
		ConsultantC@ConsultantC.com		
IP Address Request				
ID	**Intersection Name**	**No. of IP Devices**	**No. of IP's Requested (use a min of 10 per intersection)**	**Total IP per Intersection**
1	Street A1 and Street B1	5	10	10
2	Street A2 and Street B2	6	10	10
3	Street A3 and Street B3	4	10	10
4	Street A4 and Street B4	14	20	20
5	Street A5 and Street B5	10	10	10
	Spare for future Expansion:			
	5 intersections	5	10	50
			Total	**110**
PennDOT IP Address Block Allocation (Provided by PennDOT)				
Subnet Mask	Gateway	DNS		
IP address Range: From	TO	VLAN		

REQUEST FOR CWOPA ACCOUNT

A CWOPA account (user name/password) is required to access the Commonwealth's network as an authorized user. The traffic signal owner will need to complete the form in **Appendix C** and submit to the PennDOT District Traffic Unit for requesting a CWOPA account from PennDOT Central Office.

REQUEST FOR PROPRIETARY COMMUNICATION DEVICES

For security reasons, certain proprietary communication devices with security protocols have to be installed in the field to access the Commonwealth Network. If communication is planned for the backhaul, the signal owner will use the Cisco 866 VAE-K9 router. The signal owner (or PennDOT in the case of PennDOT construction projects) will coordinate with PennDOT Central Office and IT to determine the right proprietary communication device(s) for any other method of backhaul communication. The traffic signal owner will need to complete the letter in **Appendix D** for proprietary item approval requests.

7 - PRE-INSTALLATION/PRE-CONSTRUCTION

During the pre-installation/pre-construction stage, the signal owner (or PennDOT in the case of PennDOT construction projects) will procure and configure all the communication devices, and develop and get approval for the test plans.

The signal owner (or PennDOT in the case of PennDOT construction projects) will submit the cutsheet(s) for communication equipment for approval by PennDOT along with the IP address assignments for each of the communication devices at all the intersections. Refer to **Appendix B** for traffic signal IP address assignment guidelines. The cutsheet(s) for the backhaul communication device(s) will be the same as the pre-approved proprietary communication equipment.

All the field related communication device(s) will be approved by the PennDOT District Traffic Unit and all the backhaul related communication devices will be approved by PennDOT Central Office. IP address assignments will be approved by PennDOT Central Office. PennDOT Districts will be responsible for maintaining a list of all the assigned IP addresses. PennDOT is currently developing a Traffic Signal Asset Management System (TSAMS). In the future, PennDOT Districts will be able to maintain the IP address in TSAMS.

Following the approval of the cutsheets and IP address assignment, the signal owner or their contractor will procure the approved communication devices. Following the procurement, the signal owner will be responsible for sending the backhaul communication device(s) to the PennDOT IT for security related configurations. Once configured, PennDOT IT will return the configured backhaul communication equipment to the traffic signal owner. The signal owner or their contractor will be responsible for configuring all the field communication devices and also configuring the non-security related part of the backhaul communication devices. .

The signal owner (or PennDOT in the case of PennDOT construction projects) will also procure the internet connection in the field with sufficient bandwidth as required for connecting to the Commonwealth's network. PennDOT requires a minimum of 3 Mbps of bandwidth for remote communication.

In addition to procuring and configuring the communication devices, the signal owner (or PennDOT in the case of PennDOT construction projects) will develop test plans for both the field and backhaul communication and submit

to PennDOT for approval. The PennDOT District Traffic Unit will approve the field communication test plan and PennDOT IT will approve the backhaul communication test plan.

8 - INSTALLATION/TESTING

During the installation/testing phase, the signal owner (or PennDOT in the case of PennDOT construction projects) will install and test the field and backhaul communication system. Refer to **Appendix E** for the backhaul communication device deployment guide. Following the installation of the communication devices, the signal owner will test the field communication system following the approved test plan. Following the successful testing, the PennDOT District Traffic Unit will approve the field communication system through an email to the signal owner.

Following the testing of the field communication system, the signal owner will schedule the backhaul communication system testing with PennDOT IT and conduct the backhaul communication system testing following the approved test plans. Following the successful testing, PennDOT IT will approve the backhaul communication system testing through an email to the signal owner.

9 - POST INSTALLATION

During the post installation phase, the signal owner will operate the traffic signal systems using remote communication from any central location (e.g., municipal building) through the Commonwealth Network. Access to the traffic signal systems through the Commonwealth Network will require an internet connection, a CWOPA account (obtained during the design phase), and a VPN installed in the workstation. Note: The VPN procedure for signal access only pertains for access from OUTSIDE the Commonwealth Network. Internal devices have direct connectivity.

The signal owner will install the VPN in the workstation from which the signal owner will operate the traffic signal systems. Refer to **Appendix F** for PennDOT's external VPN installation and configuration process. Once PennDOT provides the user with a CWOPA account the user will be provided a one-time password that they will need to update.

The signal owner will be responsible for maintaining the traffic signal systems including the field communication system. PennDOT IT will maintain the backhaul communication system. In cases where the signal owner can not remotely communicate with the traffic signal systems, the signal owner will coordinate with PennDOT IT to troubleshoot the issue, if any, with the backhaul communication system. The signal owner will be responsible for fixing the communication system in the field to make it operational.

10 - IMPLEMENTATION CHECKLIST

Exhibit 5 below is a checklist of action items for signal owners (or PennDOT in the case of PennDOT construction projects) to utilize when establishing remote communication. **The PennDOT District Traffic Unit will act as the interface between the signal owner and PennDOT Central Office/PennDOT IT**.

Exhibit 5: Implementation Checklist

A - DESIGN
☐ Assess remote communication needs
☐ Develop requirements for communication system
☐ Design traffic signal field communication system
☐ Design traffic signal backhaul communication system
☐ Complete IP Address Request Form (See Appendix A)
☐ Complete CWOPA Account Request Form (See Appendix C)
☐ Complete Proprietary Item Approval Request Letter (See Appendix D)
☐ Submit a design package to PennDOT District Traffic Unit. The design package will include: - Designs of the communication systems (field and backhaul) - Traffic Signal IP Address Request Form - CWOPA Account Request Form - Proprietary Item Approval Request Letter
☐ Obtain design approval for field communication system (from PennDOT District Traffic Unit)
☐ Obtain design approval for backhaul communication system (from PennDOT IT)
☐ Obtain CWOPA Account (from PennDOT Central Office)
☐ Obtain a block of IP addresses (from PennDOT IT)
☐ Obtain approval for using proprietary communication device (from PennDOT Central Office)

B - PRE-INSTALLATION/ PRE-CONSTRUCTION

- ☐ Submit cutsheet(s) for communication devices for approval (prior to procuring) (to PennDOT District Traffic Unit)
- ☐ Assign IP addresses to all field devices (Refer to Appendix B) based on the assigned block of IP addresses and submit for approval (to PennDOT District Traffic Unit)
- ☐ Obtain approval for field communication devices (from PennDOT District Traffic Unit)
- ☐ Obtain approval for backhaul communication devices (from PennDOT Central Office)
- ☐ Obtain approval for assigned IP addresses (from PennDOT Central Office)
- ☐ Procure field and backhaul communication devices
- ☐ Send backhaul communication device(s) directly to PennDOT IT for security configuration
- ☐ Obtain configured backhaul communication device(s) (from PennDOT IT)
- ☐ Configure communication devices
- ☐ Develop and submit test plan for field communication (to PennDOT District Traffic Unit)
- ☐ Obtain approval for field communication test plan (from PennDOT District Traffic Unit)
- ☐ Develop and submit test plan for backhaul communication (to PennDOT IT)
- ☐ Obtain approval for backhaul communication test plan (from PennDOT IT)
- ☐ Install and Configure VPN for communication with Commonwealth network (see Appendix F for PennDOT External VPN Installation and Configuration)
- ☐ Request one-time VPN installation password (directly from PennDOT IT)

C - INSTALLATION/TESTING

- ☐ Install field communication device(s)
- ☐ Install backhaul communication devices(s) (see Appendix E for Backhaul Communication Device Deployment Guide)
- ☐ Field test all field communication devices based on approved test plan.
- ☐ Obtain approval for field communication testing (from PennDOT District Traffic Unit)
- ☐ Schedule backhaul testing date with PennDOT IT Department
- ☐ Conduct backhaul testing based on approved backhaul test plan
- ☐ Obtain approval for backhaul communication testing (from PennDOT IT)
- ☐ Obtain PennDOT acceptance for successful installation (from PennDOT District Traffic Unit)

D - POST INSTALLATION

- ☐ Use CWOPA Account to VPN into the Commonwealth Network
- ☐ Operate and maintain traffic signal communication system

11 - PENNDOT CONTACTS

For coordination with PennDOT Central Office, use the following contact information:

PennDOT Policy and Procedure Questions:

RA-PDSignals@pa.gov

PennDOT IT Requests or Coordination:

PennDOT Help Desk: (717) 783-8330

Appendix A
PennDOT Department of Transportation
Traffic Signal Unit
IP Address Request Form

Project Information (Use one for each corridor)				
Project Name:				
District:				
County:				
Township:				
Corridor Name:				
Requesting Entity				
Entity Name	**Role (Underline one)**	**Phone**		
	Contractor/Vendor/ Municipality/Consultant			
Person Name	**Others**	**Email**		
IP Address Request				
ID	**Intersection Name**	**No. of IP Devices**	**No. of IP's Requested (use a min of 10 per intersection)**	**Total IP per Intersection**
	Spare for future Expansion:			
	Total			
PennDOT IP Address Block Allocation (Provide by PennDOT)				
Subnet Mask	Gateway	DNS		
IP address Range: From	TO	VLAN		

Appendix B
Pennsylvania Department of Transportation
Traffic Signal Unit
IP Address Assignment Guidelines

As part of the design, the municipalities/designers must request IP addresses to allow accessing the traffic signal devices through the PennDOT network. PennDOT will allocate a block of the IP addresses for use based on the request. Municipalities must follow the guidelines below to allocate IP addresses to the traffic signal devices.

- Use a block of ten (10) IP addresses for each intersection.
  - Don't use IP addresses within the block of ten (10) for any other intersection.
- Use a new block of ten (10) IP addresses for every intersection
- Within the block, assign the last digit as specified below to correlate the type of device so that it may assist with the management and troubleshooting of the various IP devices.
  - .x0 – Primary Controller/Processor
  - .x1 – Ethernet switch/radio
  - .x2 – NB Camera/detector
  - .x3 – SB Camera/detector
  - .x4 – EB Camera/detector
  - .x5 – WB Camera/detector
  - .x6 – DIN Relay
  - .x7 – Conflict Monitor
  - .x8 – Secondary Controller
  - .x9 – Other

Once IP addresses are assigned, municipalities must submit the IP address assignment table to PennDOT for review and approval prior to configuring the devices with IP addresses.

A sample assignment table for an intersection with one (1) primary controller/processor, one (1) wireless radio, four (4) cameras, and (1) conflict monitor is provided for your reference below. Assume PennDOT provided the following:

Subnet: 10.240.49.3 through 10.240.49.126; Subnet Mask: 255.255.255.128; Gateway: 10.240.49.1

If there are additional devices at the intersections and some unused IP addresses, use unused IP addresses first before using another block of ten (10) IP addresses. For example, if there are two (2) additional detectors at this sample intersection, use 0.19 (first) and 0.18 for the two (2) additional detectors.

	I.P.	Device
Carlisle Pike at PA 144	10.240.49.10	Processor
	10.240.49.11	Wireless Radio
	10.240.49.12	NB Camera
	10.240.49.13	SB Camera
	10.240.49.14	EB Camera
	10.240.49.15	WB Camera
	10.240.49.16	Not Used
	10.240.49.17	Conflict Monitor
	10.240.49.18	Not Used
	10.240.49.19	Other

Appendix B
Pennsylvania Department of Transportation
Traffic Signal Unit
IP Address Assignment Guidelines

Site Identification Name (SIN) District: _____ County: _____ Intersection ID: _____	**Street Address**: _____ City: _____ Corridor: _____	**Latitude/Longitude (N/W) or State Plane Coordinate (N/E)** _____ = _____ _____ = _____
Requesting Entity:		
Entity Name: _____ **Person Name**: _____	**Role (Circle one)**: Contractor/Vendor/Municipality/ Municipality Consultants/ Others:_____	**Contact Information**: **Phone**: _____ **Email**: _____
Master Intersection: Yes/No	**Total IP Addresses Needed:** _____	
General IP Information (Provided by PennDOT)		
Subnet Mask: _____	Gateway: _____	DNS: _____
IP address Range: _____ thru _____		VLAN: _____

Device	IP Address Needed? (Yes/No)	Assigned IP Address
Primary Controller/Processor		
Secondary Controller/Processor		
Ethernet switch/Wireless Radio		
NB Sensor/Detector 1		
SB Sensor/Detector 2		
EB Sensor/Detector 3		
WB Sensor/Detector 4		
____ Sensor/Detector 5		
____ Sensor/Detector 6		
____ Sensor/Detector 7		
____ Sensor/Detector 8		
____ Sensor/Detector 9		
____ Sensor/Detector 10		
____ Sensor/Detector 11		
____ Sensor/Detector 12		
____ Sensor/Detector 13		
____ Sensor/Detector 14		
____ Sensor/Detector 15		
____ Sensor/Detector 16		
Remote Relay		
VPN Router		
Cellular Modem		
Adaptive System		
Preemption System		
Transit Priority System		
MMU/Conflict Monitor		
Uninterrupted Power Supply (UPS)		
Bluetooth/wi-fi travel time reader		
Other: _____		

Appendix C
Pennsylvania Department of Transportation
Traffic Signal Unit
CWOPA Account Request Form

Provide the following information for the agency/contractor requesting access to traffic signals using PennDOT network:

Name:	
Address:	
Email:	
Phone:	
Project Name:	
Purpose:	

Appendix D

Pennsylvania Department of Transportation
Traffic Signal Unit
Sample Proprietary Item Approval Request

OS-600C (1-13)

pennsylvania
DEPARTMENT OF TRANSPORTATION

MEMO

DATE: April XX, 2015

SUBJECT: Project Name
Project SR & Section (ECMS #)
Municipality(ies), County(ies)
Proprietary Item Approval Request

TO: Richard N. Roman, P.E., Director
Bureau of Maintenance and Operations

FROM: District Executive Name
District Executive
PennDOT Engineering District XX-0

We are providing the following information for Proprietary Item Approval. Attached is a request to use proprietary items on Project SR & Section (ECMS #) in the Municipality(ies), County(ies).

The project will involve implementation of an Adaptive Signal System on 20 existing intersections along US 22 in two Districts (11 and 12) and two Counties (Allegheny and Westmoreland). Other minor signal upgrades will be incorporated in to the project. This approval request is to use the following proprietary items:

Equipment	Manufacturer/Model
1. Cisco 866 VAE-K9 Secure Router	Cisco Systems

This request is in compliance with the Code of Federal Regulations Title 23 - Highways, Part 635 -Construction and Maintenance, Subsection 411 - Material or product selection. This request is essential for operation of the Adaptive Signal Control System.

This project is not a Federal oversight project, therefore it should not be forwarded to FHWA for approval.

The District concurs with the justification and requests your approval for the subject proprietary item(s).

Should you have any questions, please contact District Contact.

Attachment

TE-152

Reviewed and Approved by: _____ Date: _____
Chief, Traffic Signals and Arterial Management Section

Concurrence by: _____ Date: _____
Director, Bureau of Maintenance and Operations

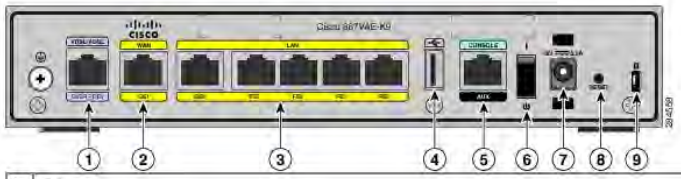
Cisco 866VAE-K9 – Traffic Signal EZVPN Install/Deployment Guide

Router Installation Procedures

(see attached picture below)

1. Place Cisco 866 router in centralized SECURE location within the site and connect power to device and power source. (7) Preferably into a surge protector power strip if available. Toggle the power switch to ON. (6)
2. Connect Ethernet cable from Vendor provided DSL/Cable Modem to interface: **WAN GE 1 –** (2).
3. Connect Ethernet cables from such as Vendor Hub and other network attached devices in the central location into the **LAN ports-** (3) ports numbered FE0 – FE3. **All these ports are configured the same(VLAN 1) so it does not matter what port they terminate in.**

Figure 1-15 Back Panel of the Cisco 867VAE-K9 ISR



1	xDSL port	6	On/Off switch
2	GE WAN interface	7	Power connector
3	Ethernet LAN GE and FE interfaces (GE0 interface and FE0 through FE3 interfaces)	8	Reset button
4	USB port	9	Kensington security slot
5	Serial port—console or auxiliary		

Deployment Procedures

PennDOT Network Verification:

1. Once router is powered up and DSL/Cable connection is plugged in the IPsec tunnel connectivity back to PennDOT will build dynamically.
2. Please call the PennDOT Developers Hotline at 717 346 5576. Inform them you are at a Traffic Signal Corridor and need to speak with a staff member from Core Networks to verify connectivity. You will then be transferred to a Core Network Engineer.
3. Please have the following information ready for the Core Networks Engineer:
    a. Traffic Signal Corridor Location.
    b. PennDOT Project Manager Name
    c. Subnet/Router Name Information from the top labels of the Cisco 866 Router.
    d. RFID Asset Tag # and Serial # of the router
    e. Broadband provider (if known)
    f. Special Comments – Router location, connections, anything out of the ordinary.

Penndot External VPN

Installation and Configuration

Appendix F

Revision History

Date	Version	Description	Author
Original		Created	Matt Mehl
4/15/2015	*1.2*	Added VDI info, revision block, TOC	Paul Joseph
6/01/2015	*1.3*	Added note to connect to VPN before proceeding with setup/use of VDI.	Paul Joseph
08/31/2015	*1.4*	Added Add PennDOT's Web URL to Java 7 and above section	Vinh Ly

Table of Contents

Important!

Before starting this installation, you must have a one-time16 character password sent to you in the last 24 hours by the PennDOT Service Desk. If your password is over 24 hours old it will not work and you must request a new one. Please call the PennDOT Service Desk at (717-783-8330)

Introduction

This document contains two sections for accessing PennDOT computer system and network resources remotely.

Part 1 – VPN setup: covers the steps required to setup a VPN connection to PennDOT. Cisco's AnyConnect client is required to be installed on your PC.

Part 2 – Virtual Desktop Infrastructure (VDI): for instances where in addition to a VPN connection, a Windows Desktop is required to be accessed. This solution is the PennDOT Terminal Server replacement solution effective May 13th, 2015. The VMWare client is required to be installed on your PC.

These directions were developed based on a Windows 7 installation using Internet Explorer (32-bit). The AnyConnect client also supports the following OS:

- Microsoft Windows 7 (32-bit and 64-bit),
- Microsoft Windows Vista (32-bit and 64-bit) – SP2 or Vista Service Pack 1 with KB952876,
- Microsoft Windows XP SP2 and SP3,
- Mac OS X 10.6, 10.6.1, and 10.6.2 (each of these versions on 32-bit and 64-bit)

To install AnyConnect, you will need one of the following browsers:

- Internet Explorer 6.0 + or Firefox 2.0+, with ActiveX or Sun JRE 1.4+ enabled.
- Safari

Installations other than Windows 7/Internet Explorer may have differing screen shots.
The PennDOT Service Desk only supports PennDOT hardware and software. Please do not contact them for support for other hardware or software.

Setting up VPN AnyConnect

Add the required certificate to the PC's certificate store

Follow the steps below to add the required CoPA Root Certificate

In Internet Explorer, go to https://www.copapki.state.pa.us/pkicdp/CoPAEnterpriseRootAIA.crt to download the Commonwealth of Pennsylvania's Root certificate to a personally owned machine.

1. As shown in Figure 1, click "open"

Figure 1 - Click Open

2. As shown in Figure 2, click "Install Certificate"

Figure 2 - Install Certificate

3. As shown in Figure 3, click “Next >” on Certificate Import Wizard

Figure 3 - Certificate Import Wizard

4. As shown in Figure 4, choose “Place all certificates in the following store” and click “Browse…”

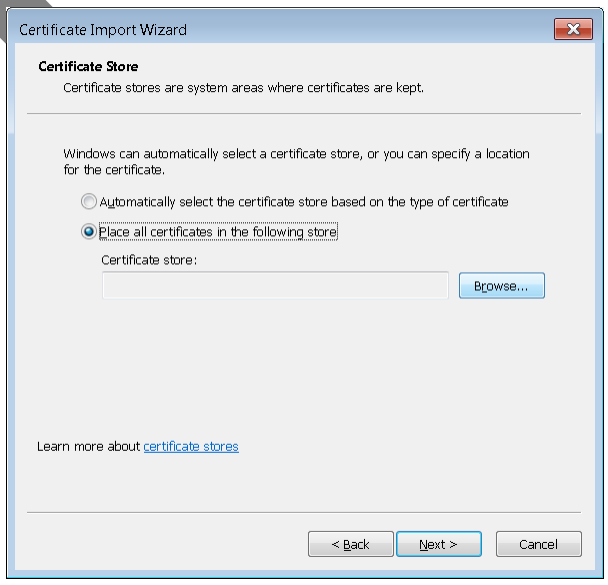


Figure 4 – Place all certificates in the following store

5. As shown in Figure 5, choose “Trusted Root Certification Authorities”

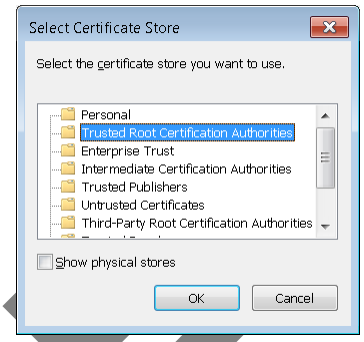


Figure 5 - Trusted Root Certification Authorities

6. As shown in Figure 6, click “Next >”

Figure 6

7. As shown in Figure 7, click “Finish”

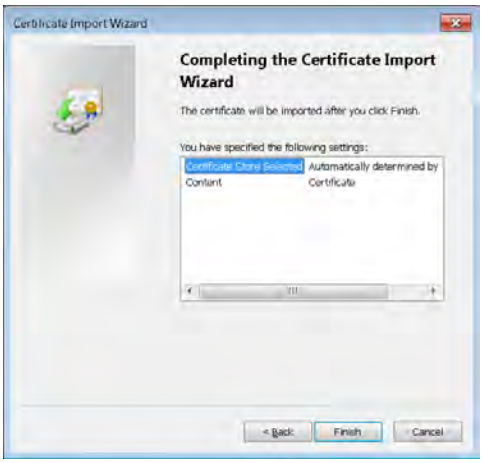


Figure 7 - Click Finish

8. As shown in Figure 8, click “Yes” to the Security Warning. Thumbprint value should match.

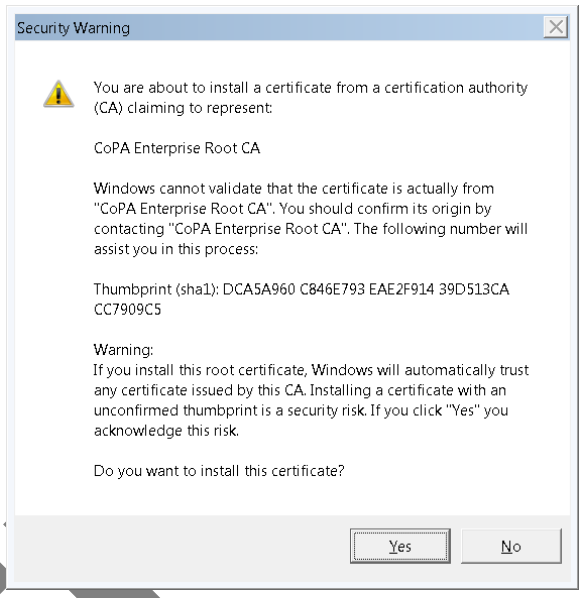


Figure 8 – Check Thumbprint value, click yes

9. As shown in Figure 9, click “OK”

Figure 9

Add PennDOT's Web URL to IE Trusted Sites

Add the "https://pdotvpn1.pa.gov" to the trusted sites list in Internet Explorer. This will enable the Cisco Any Connect client to install via ActiveX control as described further in this document.

1. As shown in Figure 10, go to the "gear" icon, or Tools – choose "Internet Options" in drop down.

Figure 10 - Internet options

2. As shown in Figure 11, choose the "Security" tab and select "Trusted sites", and click the "Sites" button.

Figure 11 - Security Tab

3. As shown in Figure 12, enter "https://pdotvpn1.pa.gov" and click Add.

Figure 12 - Add https://pdvpn1.pa.gov

Now click "Close", and then "OK" on the Internet Options window.

Add PennDOT's Web URL to Java 7 and above

If you have Java 7 and above, please continue with this section. If you have Java 6 and below, please continue to the next section.

1. As shown in Figure 13, open up your Control Panel. Click on Programs and then click on the Java applet.

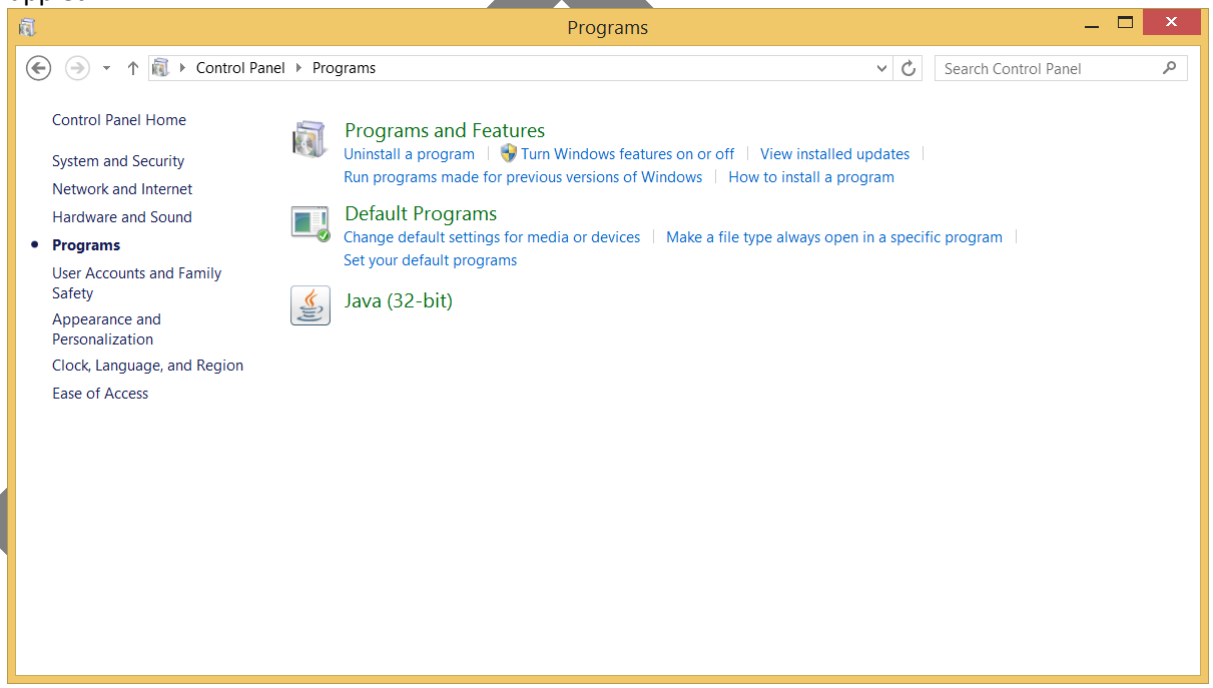


Figure 13 – Java applet

2. As shown in Figure 14, click on the "Security" tab and click on "Edit Site List"

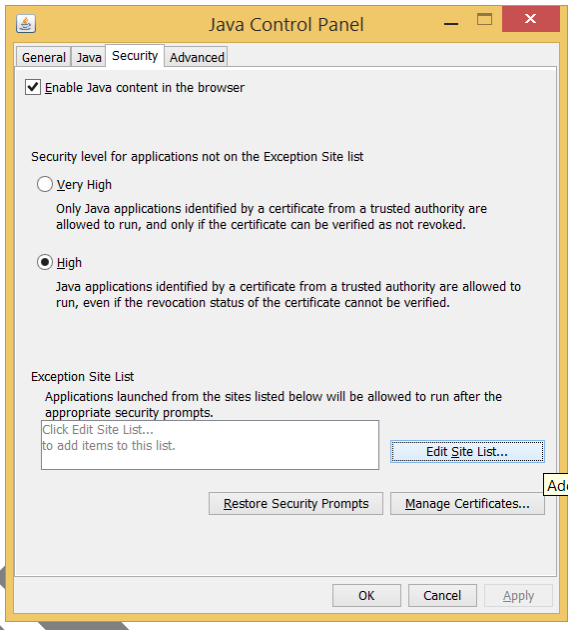


Figure 14 – Edit Site List

3. As shown in Figure 15, click on "Add". Enter in "https://pdotvpn1.pa.gov" and click "OK".

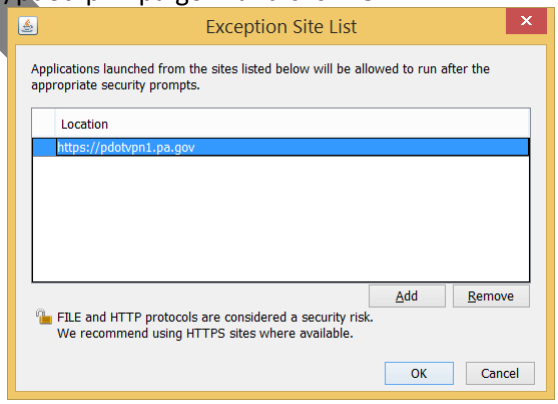


Figure 15 - Add https://pdvpn1.pa.gov

4. As shown in Figure 16, click "OK".

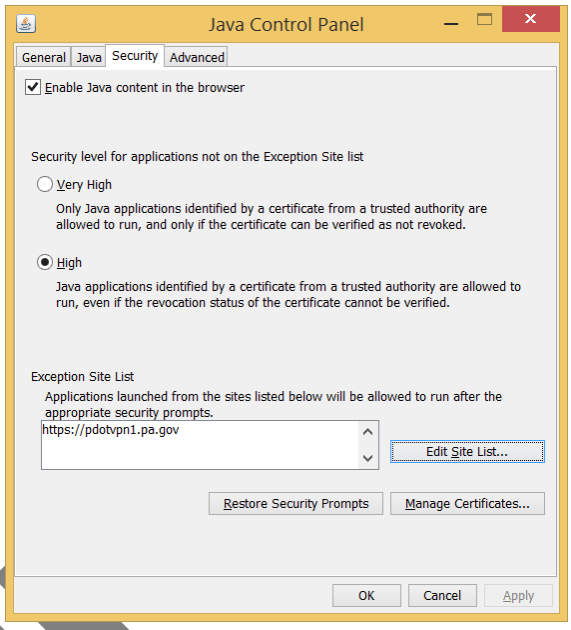


Figure 16 – Click "OK"

Install and Configure Cisco AnyConnect VPN Client

5. Using Internet Explorer, go to http://pdotvpn1.pa.gov. Installation will begin. If other users are logged into the machine log them off before proceeding. Only one user can be logged in during installation.

Figure 17

6. As shown in Figure 18, Choose “PDOT_VPN_PC_Enroll” in the Group drop down box then enter your CWOPA Username and Password. Select “Logon”

Figure 18 - Choose PDOT_VPN_PC_Enroll

7. As shown in Figure 19, installation will begin.

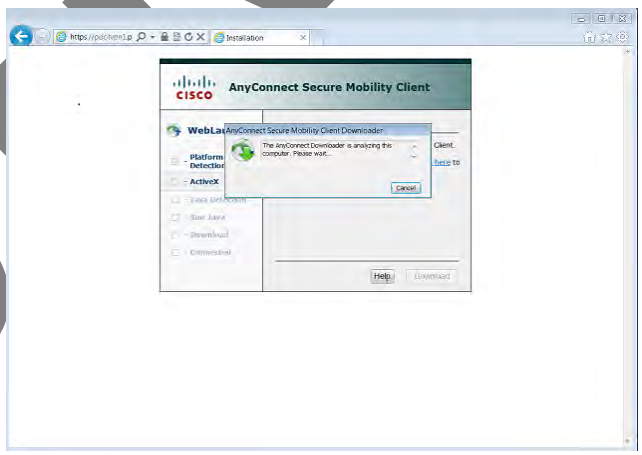


Figure 19 – Installation Begins

8. AnyConnect Client will then start to download and install automatically.

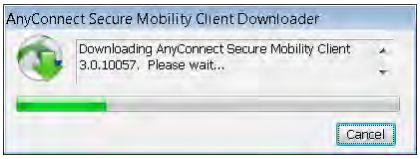


Figure 20– Download status

9. User Certificate enrollment required notification. Select "OK"

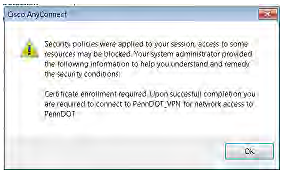


Figure 21- Certificate enrollment banner

10. As shown in Figure 22, enter the one-time password supplied to you by the PennDOT Service Desk. This password is valid for one use only, and for 24 hour duration. If you're your password was sent over 24 hours ago, please call the PennDOT Service Desk at (717-783-8330). The one-time password is 16 characters consisting of numbers and capital letters. Please take care in entering it correctly in the CA Password box. Cutting and pasting the password is encouraged. Select "Enroll"

An Example of a One-Time Password: 0DC88A2F23FEED28

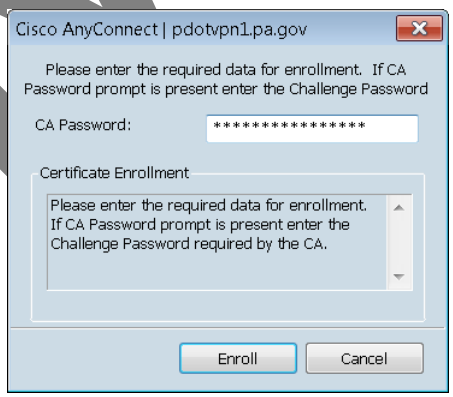


Figure 22 - Certificate Enrollment Password Entry

11. If enrollment is successful the message in Figure 23 will display. Click "OK"

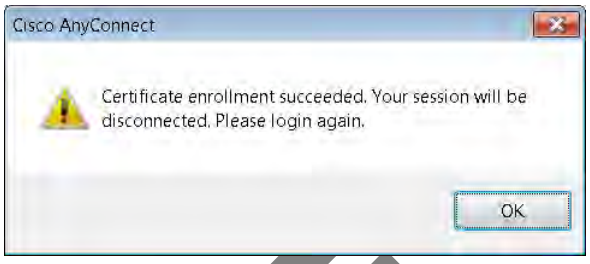


Figure 23– Successful Enrollment

If enrollment is NOT successful "Certificate enrollment failed" displays go to the end of this document for troubleshooting tips.

12. The Enrollment VPN will now disconnect, and a full VPN will attempt to reconnect. After a few moments a Username/Password prompt will appear, as shown in Figure 24.

IMPORTANT: Be sure to choose "PennDOT_VPN" from the Group drop down box. Enter your CWOPA username and password. Select "Logon".

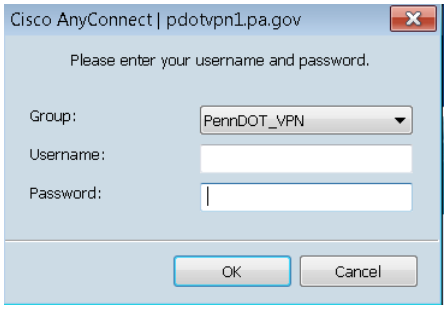


Figure 24 - CWOPA username and password

13. Click “Accept” to the message, as shown in Figure 25.

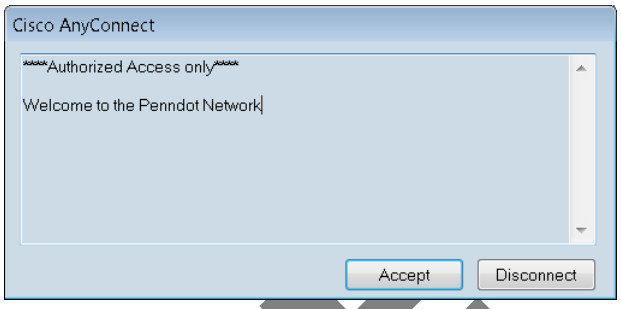


Figure 25 – Click Accept

14. AnyConnect will advise what security policies apply to your connection. Non-PennDOT machines or home users will be allowed Terminal Services (RDP) access. Click “OK”

Figure 26 – Security Policy

Congratulations! Your VPN is now connected. You will see a gold lock icon in the system tray. If you click on the tray icon, you will see a green check and “Connected to pdotvpn1.pa.gov” as shown in Figure 27. Utilize this utility to Disconnect when finished. Please follow the below steps to access a terminal server to access your applications and network drives.

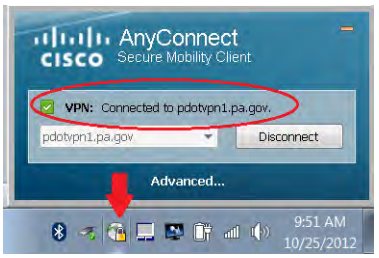


Figure 27 – Connected

Install and Configure VDI – External Users

The following steps detail how to configure a VDI client connection for a Windows desktop.

1. Go to www.vmware.com/go/viewclients and download the client install for your Operating System.
2. Once downloaded run the installer by double-clicking on the file.
3. Accept the default settings until you get to this page (***Figure 3***). Set the Default Horizon Connection Server to pdvdi.penndot.lcl

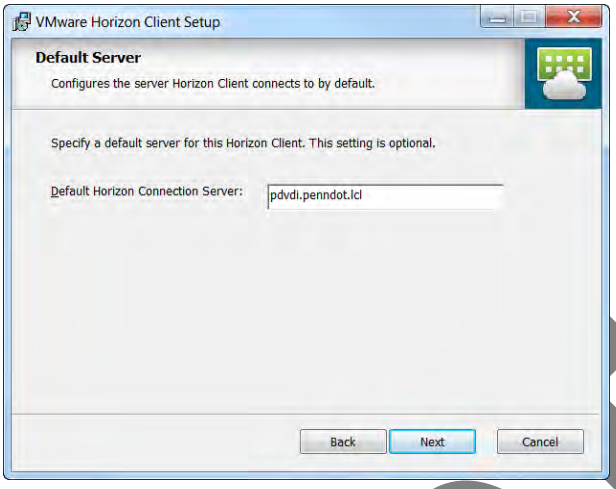


Figure 3

From this point forward, using and configuring the VDI client, you must first connect to the PennDOT VPN.

4. Once the software is installed properly click on *Start…All Programs…VMware…VMware Horizon View Client* to open the application (***Figure 4a***). The app should appear as seen in the figure below (***Figure 4b***).

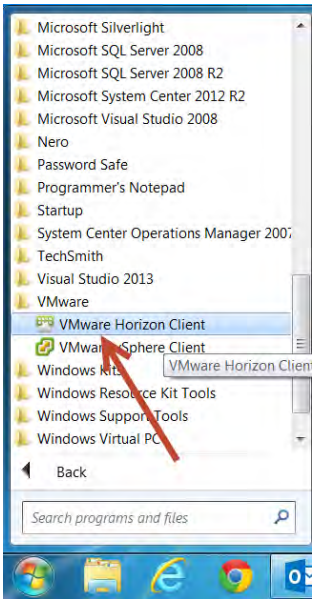


Figure 4a

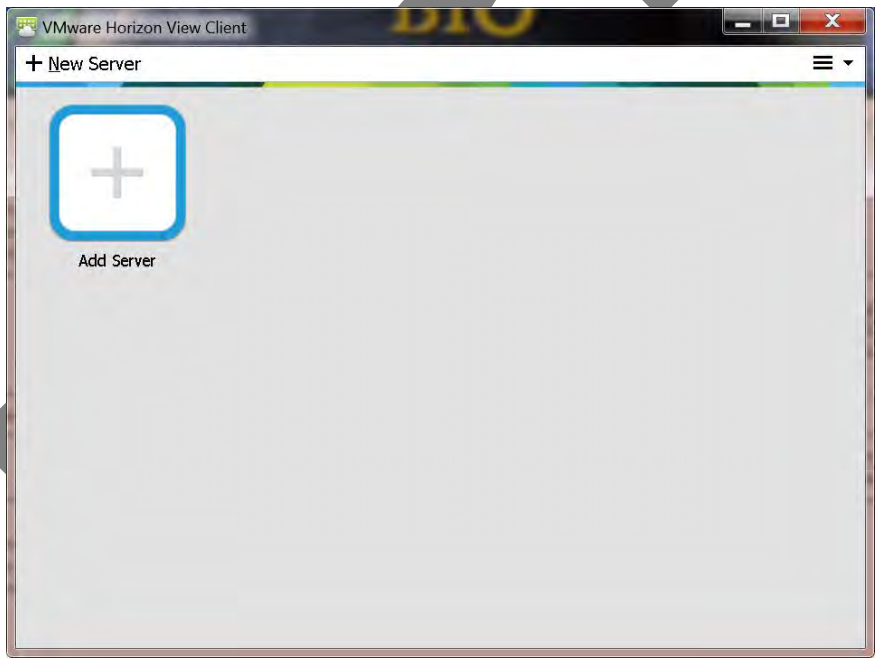


Figure 4b

5. A server must be setup to let the client know where to try and connect. Type **pdvdi.penndot.lcl** as the name of the Connection Server (***Figure 5***). Click *Connect* after the required information has been entered.

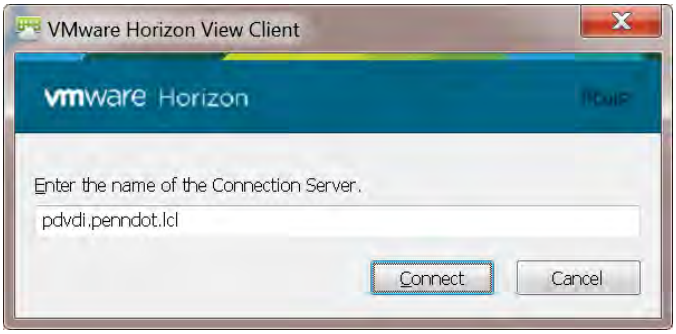


Figure 5

6. The next screen requires authentication credentials to log into the VDI connection. The first thing to do on this screen is change the *Domain* designation to CWOPA.
Once CWOPA has been selected as the appropriate Domain, enter your PennDOT *User name* and Password and click *Login* (***Figure 6***).

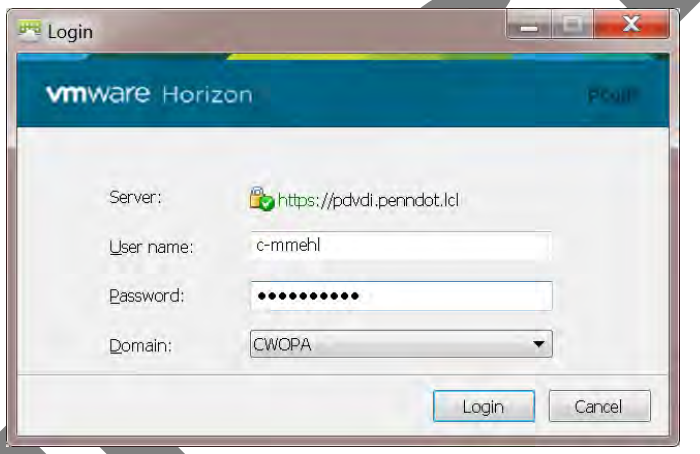


Figure 6

7. The client app will then display the *PennDOT Remote Access* icon as seen in the figure below (***Figure 7***).

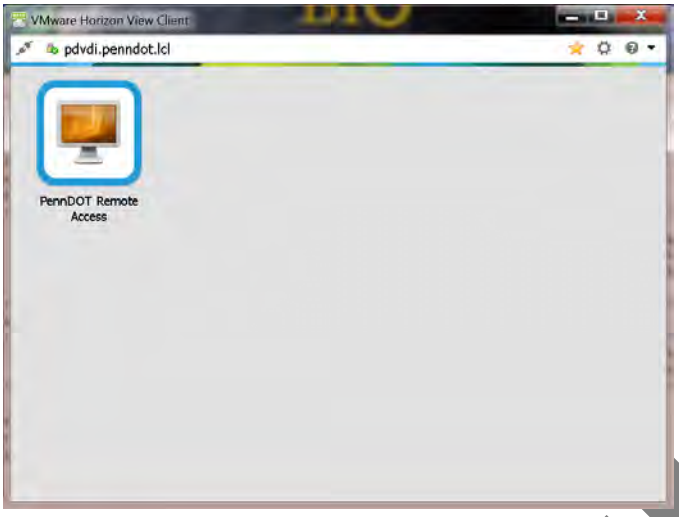


Figure 7

STOP! and follow these next steps *a* through *c*:

a. If you use more than one monitor at your desk than Right-click the icon labeled *PennDOT Remote Access* then click *Display…Full Screen* as seen in the figure below (***Figure 7a***). You may also choose *Window – Large, Window – Small* or *Custom* if you prefer.
Note: the default setting is *Display…All Monitors*; therefore, if you don't change this setting the client will fill all your monitors; then if you try to re-size the window you could lose your mouse pointer.

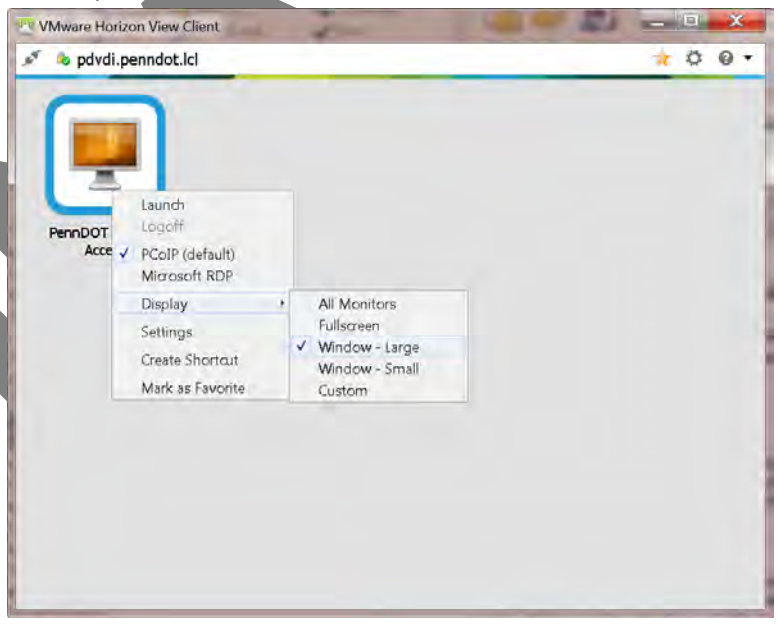


Figure 7a

b. Right-click again on the icon labeled *PennDOT Remote Access* then click *Microsoft RDP* as seen in the figure below (***Figure 7b***).
Note: if you don't make this setting change than you could lose your mouse pointer.

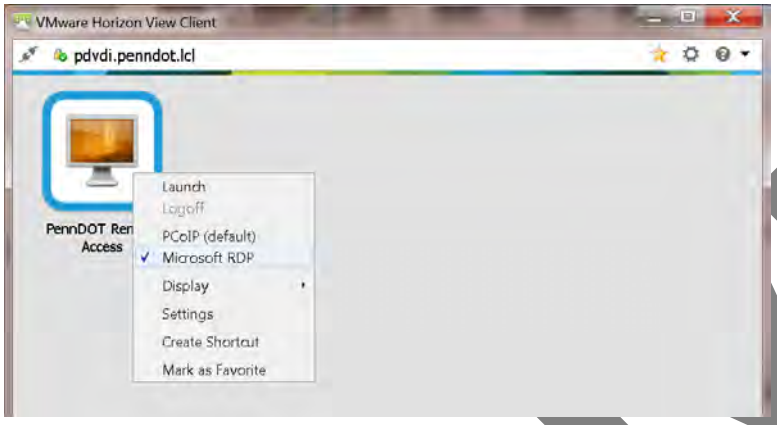


Figure 7b

c. Once all settings are complete, double click the icon *PennDOT Remote Access*.

8. A Windows 7 Enterprise desktop is then displayed as shown in ***Figure 8***. Click *OK*.

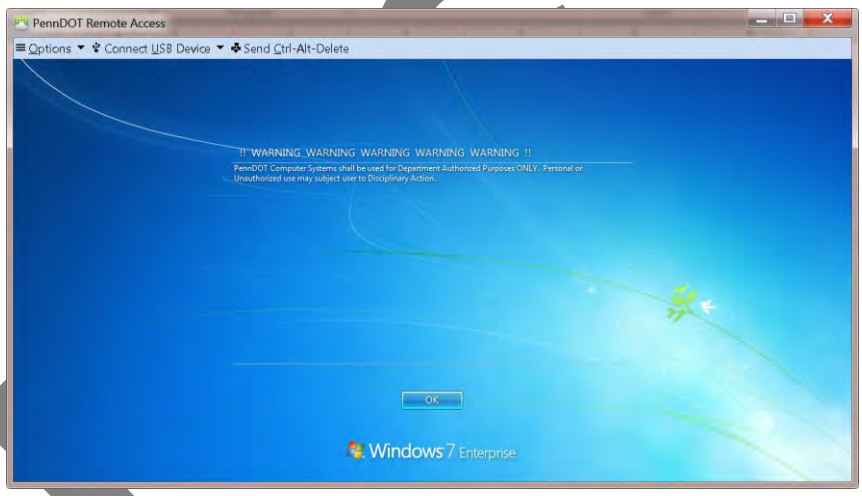


Figure 8

9. The Windows7 Enterprise desktop will appear as shown in ***Figure 9***.
Note: the virtual desktop may take some time to load because it is updating the desktop; please be patient☺.
You are now ready to use this remote desktop.

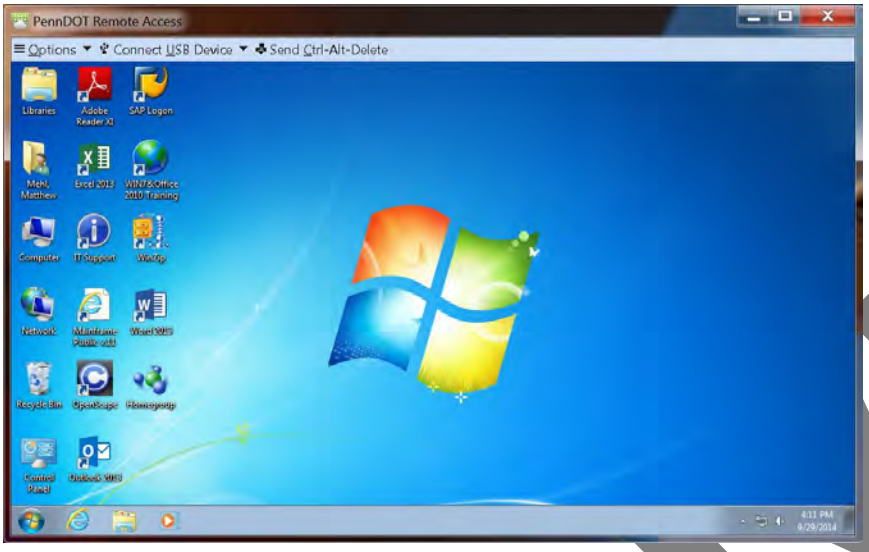


Figure 9

Microsoft Office Pop-up Windows upon first use

In the event that you use Microsoft Office in the VDI, upon first use you will be presented with several pop-up windows. Click *Next* on each pop-up window until you get to the last window when you click *All done!* **You are now ready to use the Microsoft Office application.**

If you have any issues please refer to the next page "troubleshooting" or contact the PennDOT Service Desk at 717-783-8330 for further assistance.

Troubleshooting

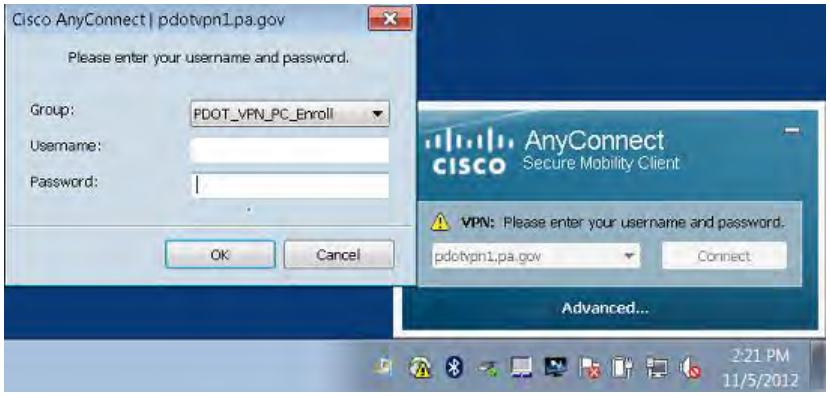
If you receive a Certificate enrollment failed message box like the one below follow the below steps

1. click “OK”

2. In the system tray left click on the AnyConnect globe. The second icon from the left in our example.

3. Select “Connect”

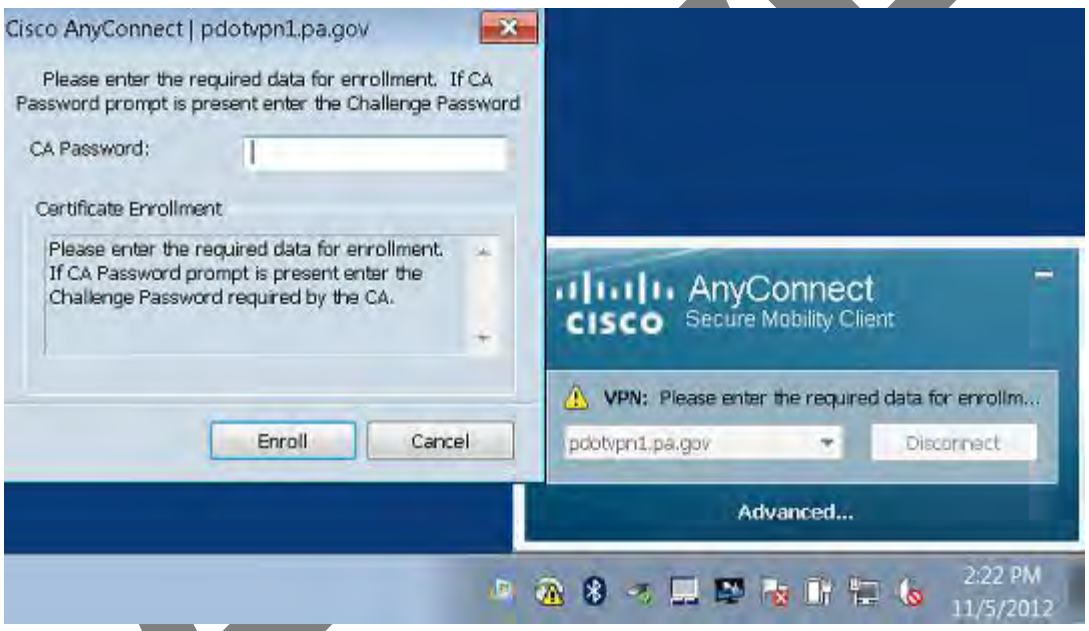
4. Enter CWOPA Username and password under “PDOT_VPN_PC_Enroll” and select “OK”



5. re-enter your one-time password in the CA Password box and select “Enroll”

If you receive a Certificate enrollment succeeded box select “OK” and go back to **Step 20** to connect to the PennDOT_VPN.

If Certificate enrollment failed again start with **Step 1** under troubleshooting and ensure you are pasting in or typing in the correct one-time password. TIP Make sure there are no spaces when cutting and pasting at the end.

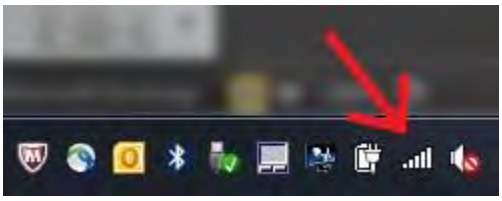


If AnyConnect shows that you are connected successfully to pdotvpn1.pa.gov but you are unable to access any network locations or run the "Reconnect Drives and Favorites" batch file, follow the below steps.

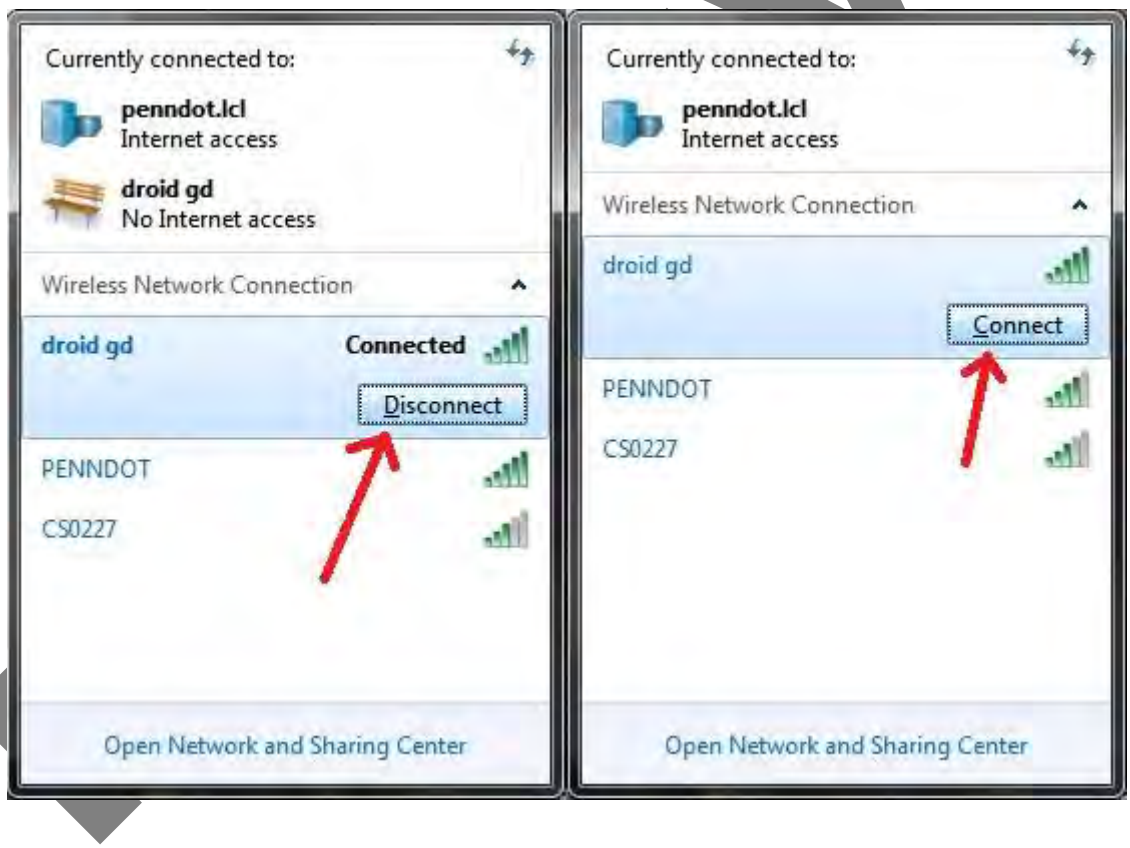
1. Open AnyConnect and click "Advanced…"

2. Ensure you are on the 'Statistics' tab and check if you have a '0' value for both "Bytes Received" and "Frames Received".

3. If you have ‘0’ for “Bytes Received” and “Frames Received”, you will want to drop your Internet connection and re-connect it immediately. If you are connected via an Ethernet cable, just un-plug and re-plug the cable, if you are connected via Wi-Fi, click the Wi-Fi manager icon in your taskbar.



4. Click the Wi-Fi connection you are connected to, and click ‘Disconnect’, then ‘Connect’ once it’s disconnected itself.



5. Go back and check AnyConnect>Advanced>Statistics and you should now see the numbers rising for both “Bytes Received” and “Frames Received”.

6. Re-run the “Reconnect Drives and Favorites” shortcut after you’ve ensured you are receiving network traffic.