EOTSS Defined Services
Commonwealth VPN

Product Description

What is Commonwealth VPN?

A Virtual Private Network (VPN) enables remote users to communicate securely and confidentially over a public network (i.e. internet) to protected resources within the Commonwealth of Massachusetts and its Wide-Area-Network (MAGNET).

EOTSS provides 2 methods for Commonwealth employees, contractors, vendors and business partners to connect to the Commonwealth network:

> **Standard Remote Access**
> The VPN Client is desktop software that secures traffic between a remote computer and Commonwealth IT resources—all data traffic is encrypted leveraging SSL and ESP using AES256 bit encryption for maximum security. This VPN client leverages the Commonwealth Active Directory services and Idaptive Multi-Factor Authentication to securely authenticate and identify users.
>
> **CJIS Approved Remote Access**
> For Criminal Justice, Law Enforcement and Public Safety Agencies that are required to meet FBI CJIS Security standards, EOTSS offers a Windows-based and Apple iOS-based client for connectivity to access CJIS data and systems. Both clients require the use of a PKI (public key infrastructure) certificate to ensure unique identity of the user. All data traffic is encrypted leveraging SSL and ESP using AES256 bit encryption for maximum security.

VPN Features

Included Features

Secure Connection
Remote Access VPN establishes an encrypted tunnel for all data to be securely transmitted so that remote users can communicate confidentially over a public network—i.e., the Internet.

Data Encryption
User credentials and all data traffic are encrypted in compliance with IPSEC standards, leveraging SSL (Secure Sockets Layer) and ESP (Encapsulating Security Payload) with AES 256-bit encryption for maximum security.

User Authentication

Users are allowed access to restricted state IT resources only if they can verify identification at login. *Unauthorized users are not permitted access.*

Authentication Directory
Each user is authenticated to the Commonwealth Active Directory and/or Idaptive MFA.

Limitation
When using VPN remote access, any local network devices available to the computer prior to the VPN connection (e.g., networked home printers and other computer resources) may not be available when the VPN client is connected. If this occurs, to use or access local network home printers and other local computer resources, the VPN session must be disconnected.

Features Not Included

Remote Access Connection
All users must have an internet connection—e.g., commercial or residential DSL, cable, fios, public kiosk service, public wifi internet, or other internet service.

System Requirements

- ✓ Must be a currently supported version of Microsoft Windows or Apple MacOs.
- ✓ EOTSS-supported Web browser such as MS Internet Explorer11, Google Chrome and Firefox.

EOTSS and Agency Responsibilities

EOTSS Responsibilities:

- ✓ EOTSS will deliver the product described in this product description.
- ✓ EOTSS will provide instructions for product use.
- ✓ EOTSS will operate and maintain the Pulse Secure VPN Appliances and all supporting infrastructure.
- ✓ To ensure the security of Commonwealth information technology resources, EOTSS may block telecommuters' access to the State Network when troubleshooting security intrusions.
- ✓ EOTSS will enforce the Teleworking Policy, Commonwealth Enterprise Security Policy and Standards, and Acceptable Use policies.
- ✓ EOTSS will provide instructions for installing and configuring the VPN Client software.
- ✓ In cases where EOTSS provides End User Services for the Agency, EOTSS End User Services will be responsible for deployment and support of the client.

Agency Responsibilities:

- ✓ Follow established process to submit online orders that have been properly approved for requesting the addition, modification, or deletion of VPN groups, VPN users or access type.
- ✓ The user will obtain a remote access internet connection—e.g., commercial or residential DSL, cable, fios or other internet service.
- ✓ Non-employee users must be sponsored by a Commonwealth of Massachusetts agency and must be able to install and support their own devices.

VPN Client:

- ✓ The agency IT support organization will be responsible for setting up the user's computer with the software required to access the agency LAN and other business software required by the VPN user.

- ✓ The agency IT support organization will assist the user with installing and configuring the VPN Client software as requested.
- ✓ The agency IT organization will be responsible for assisting user’s with connecting to local agency resources, including Remote Desktop Connections.
- ✓ VPN users will comply with the Commonwealth’s Acceptable Use Policy, the Commonwealth Enterprise Security Policy and Standards and the Commonwealth’s Telework Policy.