Persistent Data Network (PDN) is an application on ProSoft Connect, ProSoft Technology's secure, cloud-native service optimized for high reliability and availability. PDN is a **simple**, **secure**, and **managed** infrastructure network designed to enable remote communications between automation devices that are geographically dispersed. PDN is intuitive and easy to set up, without the need to configure complicated communication settings or manage security certificates. An activity log provides detailed account activity information.

PDN users can establish safe and secure remote communications with their machines anywhere in the world. Using Connect's unique EasyBridge™ technology, automation programming tools (such as Studio 5000, Unity® Pro, TIA Portal, and many more) can talk directly to the automation devices.
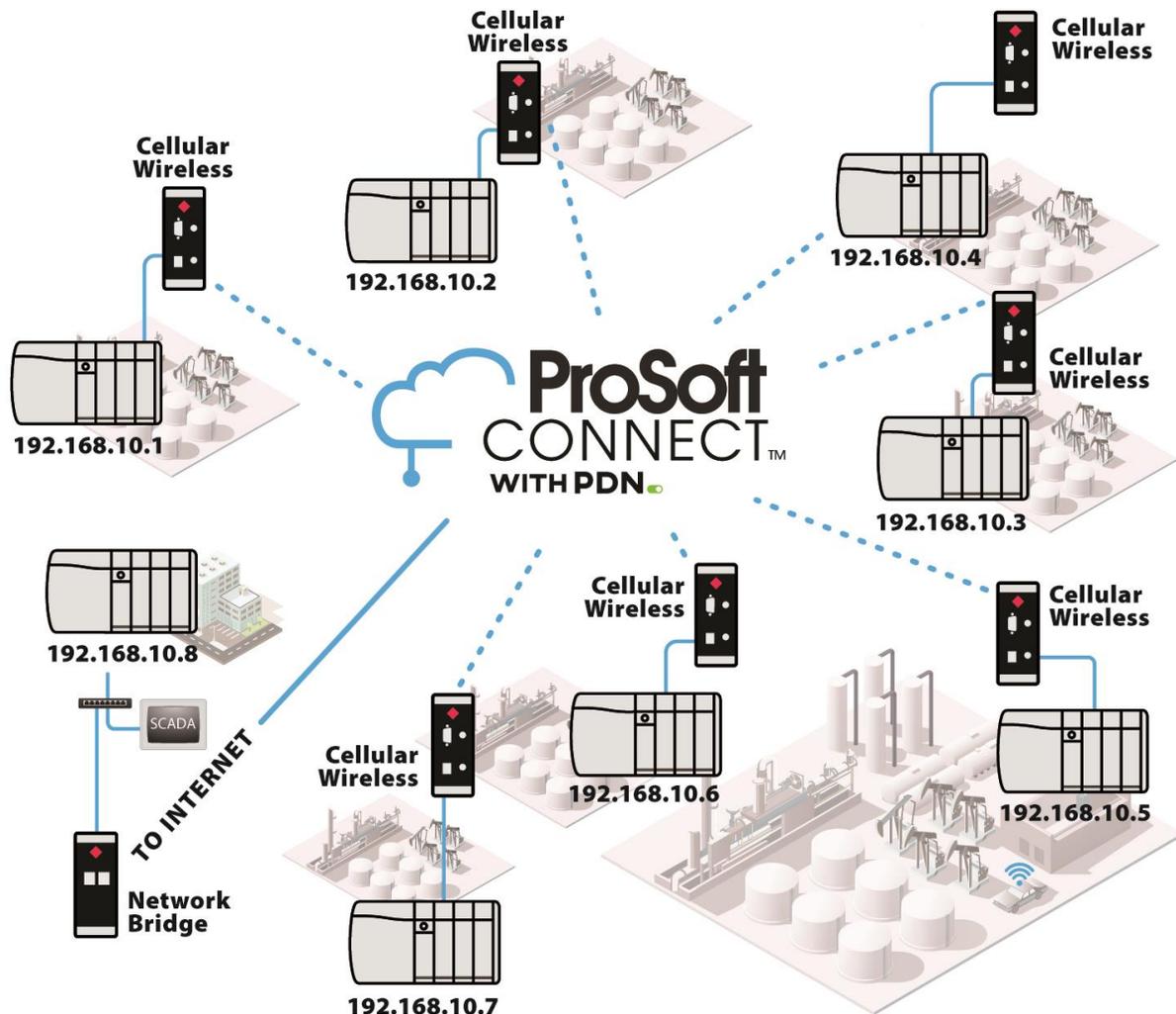
Simple

PDN is the simplest way to create a secure remote communications infrastructure network. To create a PDN network, users need:

❖ An account in ProSoft Connect (Sign up at https://www.prosoft.io)
❖ A paid Subscription plan (see below)
❖ ICX35-HWC-A/E or PLX35 gateways

The user must create the PDN project and add the gateways to the project. This creates the Layer 2 VPN connection between the remote sites.

Security

All communications with ProSoft Connect is secured using a multilayered approach.

❖ Gateways are activated using two-factor authentication
❖ Each gateway uses a unique one-time key to establish a tunnel to a local tunnel service
❖ Tunnels are encrypted using 256-bit AES encryption
❖ A separate and secure Web Sockets control path maintains communication with gateways

Remote access to sites is achieved using ProSoft Connect Secure Remote Access. If Virtual Lockout Tagout (vLOTO™) is enabled, the user must obtain permission for remote access. If Single Sign On (SSO) is enabled, then IT can manage user access.

Projects

Gateways and users are organized into Projects within the organization in ProSoft Connect. All gateways added to a PDN Project are connected to form one Layer 2 network (single subnet). Automation devices connect to this network through the gateways, and communicate with each other just as they would if connected to the same Ethernet switch. Each organization requires a PDN subscription.

Subscription Plans

A PDN subscription is required. Plans are based on the number of sites in a network. Each site needs a cellular (ICX35-HWC-A/E) or wired gateway (PLX35-NB2).

What is included with a PDN Subscription?
❖ 3GB of VPN data per month per site
❖ Single Sign On (SSO)
❖ Advanced Two-Factor Authentication (2FA)
❖ virtual Lockout-Tagout (vLOTO™)
❖ Concurrent tunneling (for Secure Remote Access)
❖ Activity log for 30 days
❖ Alarm Notification

Managed Layer 2 VPN Network

A Persistent Data Network (PDN) is intended to enable quick and easy SCADA style applications. A PDN is a collection of ProSoft gateway endpoints that participate in a Layer 2 network between the regional tunnel server and the gateways. ProSoft Connect manages the tunnel connections between the gateway and the tunnel server.

Advanced Two-Factor Authentication (2FA)

With Advanced Two-Factor Authentication, customers can be confident that only registered users can access the account. When advanced 2FA is enabled, users must enter a username, password, and a unique time-based one-time password. The time-based, one-time password is auto-generated via an authenticator app on the user's phone.

Single Sign On (SSO)

Single Sign On allows users to access multiple applications with one set of credentials. With SSO, IT can manage user access which improves security, productivity. SSO uses SAML 2.0. SSO works by sending the login request to a known federated identity provider (IDP) and the credentials are checked against the organization's active directory server. If the credentials are correct, then the user will be allowed to access the application.

Virtual Lockout-Tagout (vLOTO™)

vLOTO allows authorized plant personnel to control when and how their machines are remotely accessed. The Connect user requests access for a specific period of time, which the authorizer(s) must approve. The authorizer does not need to be a ProSoft Connect user – the person can be an IT manager, plant engineer, shift supervisor, or other authorized person. The authorizer(s) can deny or revoke access at any time. Companies can also access activity logs of permissions, acceptances, and denials.

IP Whitelisting

Access specific IP addresses when connected remotely to the gateway.

VPN Tunneling

The cloud to gateway connections in the PDN network are IPSec over HTTPS. ProSoft Connect provides an AES256 encrypted Layer2 VPN connection between the sites in a PDN network.

User Accounts and Access Control

The ProSoft Connect Organization owner and project administrators can invite team members to join projects in the organization. Access control for users is managed by the account administrator. Users are assigned rights to administer, connect, and configure gateways, or to connect only. An Organization Owner can transfer ownership of remote access devices (for example, a machine builder granting ownership to an end user once the OEM no longer needs control of the equipment).

Ethernet/Cellular Connections

Connections from gateways use HTTPS only, and can only be initiated outbound from the gateway. Client VPN connections use SSTP via TCP port 443 or L2TP via ports 500, 4500, and 1701.

No PC Client Software

User-installed software is not required for Connect. Connect is compatible with current versions of Chrome, Firefox, and Internet Explorer 10 or later. EasyBridge uses the OS-native SSTP or L2TP client software. Windows 7 or later is recommended.

ProSoft Connect works with the ICX35-HWC Industrial Cellular Gateway and the PLX35-NB2 Network Bridge. ProSoft offers data plans (U.S. Only) for the Industrial Cellular Gateway with AT&T or Verizon activated at the factory.