Creo Inc.
3700 Gilmore Way
Burnaby, B.C., Canada
V5G 4M1
Tel: 1.604.451.2700
Fax: 1.604.437.9891

Request support:
ecentral.creo.com

www.creo.com

Internal: 731-00203A-EN Rev A
Release date: 08 March 2004

Technical bulletin

PPTP-based VPN Connectivity Setup for ServiceWire

This bulletin outlines how to configure a PPTP VPN to allow authorized Creo personnel to connect to a remote customer site and support the on site Creo equipment.

What is VPN?

Virtual Private Network is a secure way of remotely accessing a network using the shared infrastructure of the Internet. It makes use of tunneling protocols to maintain data privacy by encrypting the data as it travels over the public infrastructure and is then decrypted at the opposite end of the tunnel.

What is PPTP based VPN?

Point-to-point tunneling protocol (PPTP) was developed by a consortium including Microsoft® and is used for establishing a virtual private network (VPN). This allows remote users to securely and inexpensively access other corporate networks from anywhere on the Internet. PPTP has several advantages as a connection technology. Most Microsoft operating systems ship with a PPTP client, so there is no need to purchase third-party client software. PPTP has the additional advantage over other VPN technologies of being easy to set up.

Process overview

To set up the broadband connectivity with Creo Service, your site will need a broadband connection to the Internet and a firewall and/or IT infrastructure that supports PPTP-based VPN. Once the Creo support VPN account is created and tested at your site, call the Creo Solutions Center. A service representative will test the connectivity and add your account to ServiceWire™.

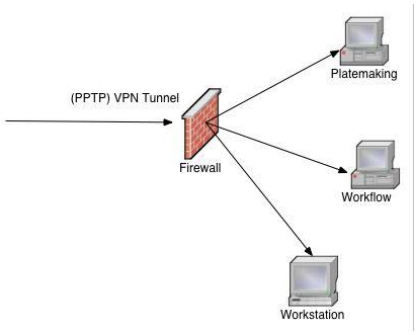
Infrastructure Requirements, Setup, and Testing

Requirements

For your site to be set up and activated in ServiceWire, you need a VPN infrastructure that supports PPTP-based VPN with MPPE 128-bit encryption. No protocol filtering can take place at your end of the connection—Creo service tools need full access for all ICMP, TCP, and UDP traffic.

This configuration can be initiated either directly at your firewall, if it supports PPTP-based VPN, or at some other end point on your network. In the later case, your firewall needs to support pass-through of inbound PPTP-based VPN to the end point.

Firewall Supports VPN Directly

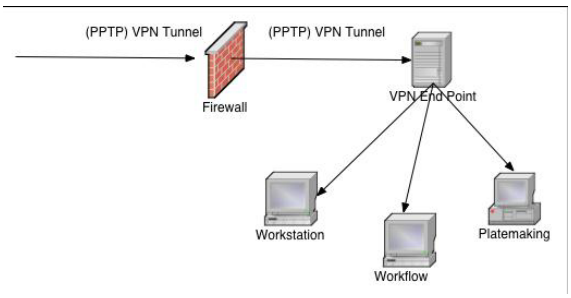


If your firewall has built in support for PPTP-based VPN, consult the firewall user manual for setup details.

If the firewall supports filtering incoming traffic based on the source IP, consider adding the following source addresses/networks to the list:

- 204.174.12.0/24
- 194.7.172.0/24
- 221.186.82.84

The Pass-Through Option



If you use a pass-through option to configure the connection, there are a few things to consider before configuring the services. Creo strongly recommends that when choosing the server for the VPN end point, you do not choose a production workstation. If that workstation is down and needs servicing, we will not be able to connect and help you with it or any other device at your site. Configure the firewall to forward the following two protocols: TCP port 1723 and IP 47.

The workstation that will serve as an end point could be any Windows® (Windows 2000 Server, Windows 2000 Pro, Windows XP, Windows Server 2003) or Linux/UNIX® workstation that has the necessary protocol support or a VPN hardware solution. To learn more, or to access specific information on how to configure the VPN end point workstation, see the system administration documentation for your operating system or the following Web sites:

- For Windows products: http://www.microsoft.com/windows2000/technologies/communications/vpn/default.asp#section2
- For Linux and a variety of UNIX flavors: http://www.poptop.org

To learn how to configure the firewall, see the firewall vendor documentation.

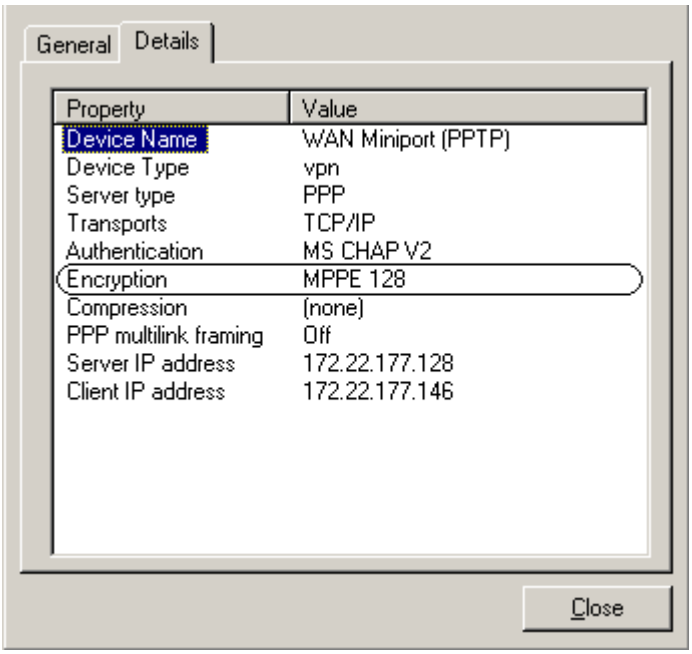
Creating the Creo Support Account

When creating the Creo Support account on your VPN infrastructure, we strongly recommend you use a "strong" user name and password (at least 8 characters long, combination of uppercase, lowercase, and special characters).

Note: If your security policy so requires, you can disable the support account when Creo does not need to access the equipment on your site. If this is the case, please make sure that there is always someone at your site who can activate the account should there be a need.

Testing

After setting up the account, we recommend that you test it from a point outside your network. Confirm that the MPPE 128-bit encryption is forced on the connection and that lesser encryption options are non-negotiable. If lesser encryption is negotiable, Remote Support Server will not be able to connect. See the following example from the Microsoft VPN client software connection details confirming the MPPE 128-bit encryption:



Registering with ServiceWire and Checking Connectivity

After you have successfully tested the connection, call a Creo Solutions Center in your region to register. An engineer will connect to your site according to the information you provide. We will test the connection and register all Creo-supported equipment with ServiceWire. Afterwards, your site will be on our system and we will be able to connect with and support you more quickly and reliably.

To register with ServiceWire and to establish a successful VPN connection to your site, you must provide the following:

- User name, password, and domain information of the Creo support account you created
- The address of your VPN gateway server or your registered host/domain name (for example, `vpn_gateway.printshop.com`)
- IP addresses of Creo-supportable devices

Note: Never send this information by e-mail or fax—telephone the Solutions Center in your region.

If any of the connection information changes, inform the Solutions Center of the change so we can update the system and test the connectivity with the new settings. For example, if your public Internet address changes, you need to advise Creo of the change, as some Internet service providers (ISPs) are known to change this address often.

ServiceWire System Overview

The ServiceWire system consists of two main components: Remote Support Servers (RSS), located inside the Creo corporate network, and Creo ServicePorts (CSPs), installed on supported equipment.

Creo ServicePort is a remote service agent that is a part of the ServiceWire system. It is developed specifically to support Creo service tools network traffic. It is normally dormant and listens at the IP port 6503. To communicate with it, it requires a 1024 PKI authentication. Once authenticated, it carries out an encrypted conversation with the ServiceWire server within the Creo network.

Note: ServiceWire only registers the workstations that have Creo ServicePort software installed on them.

We recommend that you configure your production floor network so that all the production workstations supported by Creo are on one subnet, and that subnet is different from your other corporate subnets. This way, you are assured that Creo service can access all the supported equipment.

About Creo

Creo is a world leader in solutions for the graphic arts industry. Core product lines include image capture systems; inkjet proofers; thermal imaging devices for films, plates, and proofs; professional color and copydot scanning systems; workflow management software; and proofing and printing consumables. Creo is also an original equipment manufacture supplier of on-press imaging technology, components for digital presses, and color servers for high-speed, print-on-demand digital printers. Creo trades under the symbols CREO on NASDAQ and CRE on the Toronto Stock Exchange. www.creo.com

© 2004 Creo Inc. The Creo product names mentioned in this document are trademarks or service marks of Creo Inc. and may be registered in certain jurisdictions. Other company and brand, product, and service names are for identification purposes only and may be trademarks or registered trademarks of their respective holders. Data is subject to change without notice.