



Systech Corporation

OnDemand Version 2.0 – Release Notes

September 16, 2010

This document contains Systech concepts and basics regarding OnDemand Remote Port Access client and Remote Port Access Host. Throughout this document, RPA refers to OnDemand and Remote Port Access.

For an overview of the OnDemand product, see our web site, www.systech.com under OnDemand. A Concepts section at the end of this document is also provided.

All documentation remains on the installation disk. You must manually save them to your PC or read them from the installation disk. Documentation is in PDF and requires an Adobe Reader to view or print them.

For Demos, Beta testing, and limited Systech Device access, the OnDemand administrator is Systech Support. The RPA username and password provides access at the user level. A user can have access to multiple Systech devices. An OnDemand administrator authorizes access to multiple Systech devices. For this reason, Systech manages access and devices. When a company owns an OnDemand RPA host, they can allocate their own administrator. For more details, please examine the OnDemand RPA User guide located on your installation disk.

All devices that connect to the OnDemand RPA host receive an initial 60 day license for remote access. To extend remote access service, contact your Systech sales representative.

It is important to review all installation instructions on the installation disk before installing this product. A user guide is also included to understand the operation of the OnDemand client tunnel and host.

Known Issues:

OnDemand RPA Client issues:

1. Occasionally, you may see a message stating “RPA Tunnel Service does not appear to be running” when first booting up your PC. This is only temporary until the connection of the RPA Tunnel Service establishes a network connection to the OnDemand RPA Host.
2. In the new RPA Tunnel Client Manager on login interface, the description area can be edited. This information is not saved. It will remain however, until you quit and restart the application.
3. If the Port Assignment tab area on the RPA Tunnel Client Manager does not display any Systech devices (empty or blank), do not use the Assign button. This causes an exception error and closes the application. Your OnDemand Administrator must add your Username as an Authorized User for a device for you to continue.
4. The RPA Client Tunnel installer repair has problems. Use un-install and install only.
5. Quit the RPA Client Tunnel Manager before un-installing the software.
6. Firefox cannot open and run the installer. Firefox must save the file to your Download folder then open and run it.
7. If your installation fails due to an MSI error, copy the contents of the CD on your PC. From the “Software” folder, run setup.exe.

RPA Host issues:

1. When you Save Changes in Device Management, first query page always displays.
2. You currently cannot add more than 9 ports to one Systech device.
3. RPA host server can retain an inaccurate device connection status. Use the RPA client tunnel manager to connect devices

Concepts:

This section is provided for your reference.

The Problem

As it operates today, NativeCOM connects to a port on a device server by making a TCP connection to the IP address of the device server and a TCP port number associated with the physical port. Similarly other applications may make direct TCP connections to a port. However, when connecting to devices over the Internet it can be both impractical and undesirable to open a hole in the end user network firewall to allow incoming connections.

It is impractical because:

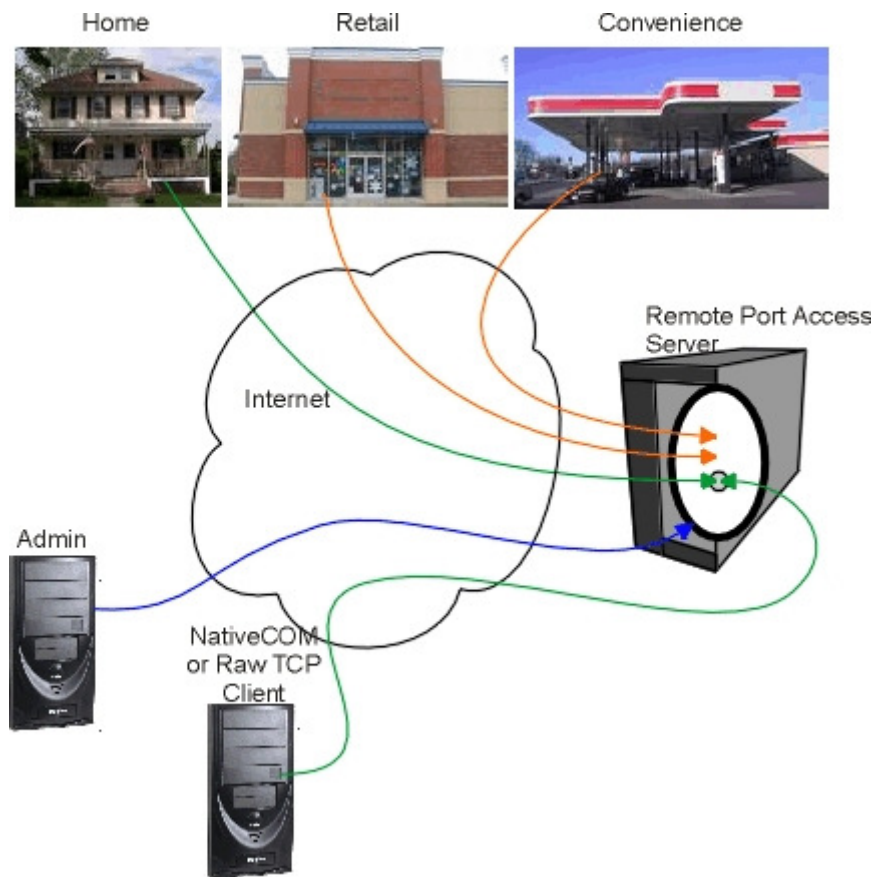
- it requires modifications to the target network (firewall, etc)
- it is likely something the owner of the network doesn't know how to do
- it requires a static private IP address on the local network - at best, frequently difficult to obtain
- it also requires a static public Internet address for the site - this is not typical for a home environment. It is more likely in a business environment, but by no means common
- it requires site-specific configuration; therefore installation is not "plug-n-play"

It is undesirable because, in addition to the work above,

- it opens an incoming hole to the network, providing a potential security breach
- Standard NativeCOM doesn't use encryption, potentially making sensitive information publically available

The Solution

To overcome these problems Systech has developed a "Remote Port Access" service (RPA) that runs on a host accessible on the Internet from both the remote site and from the NativeCOM or Raw TCP client (referred to from here on as simply the client). For each configured device, the server listens on two ports... for a connection from the device in the field and a connection from the client. The device automatically connects to the RPA server and waits for communication. To access a given device, the client connects to the RPA server which then links the two, allowing data to pass from client to device and back again.



In the illustration above, the **green** lines indicate a complete connection from the device to the server and from the client to the server. The host application and the device can now communicate. The **orange** lines indicate devices that have connected to the server and are ready to accept communication from a client. The **blue** line indicates an administrative connection to the server to check status (for instance: which devices can accept connections or which are connected) or to select which device to connect to.

- This solution requires no modifications to the target network
- No static IP address is required on the local network - the device server will obtain a DHCP address on the local network
- No static Internet address is required for the site. Any address will work. NAT and firewall are unaffected.
- The installation is "plug-n-play" on the target network. The device server will be pre-configured to contact the RPA server. The end-user only has to connect the device server to their local network and attach the device to the serial port.

- With an appropriate model NDS/IPG, the device server can connect to the RPA server using SSL.

Applications

In one application for this service, there are many devices at remote sites, but a relatively small number of clients that want to connect to them, and these clients only connect periodically and one-at-a-time to the devices. An administrative interface on the server allows the users to select which of many devices to connect to "this time". So a single NativeCOM or raw TCP port can be used to access multiple devices.

In another application for this service, there are many devices that are simultaneously connected. NativeCOM allows up to 255 virtual COM ports to be defined, per client machine, which may all be attached to devices through the server. Raw TCP may connect to any number of ports. The server itself supports 1000's of simultaneous connections.

The browser-based, secure HTTPS administrative interface allows you to create sub-users, giving each user access to only their devices.

Server Operation

The RPA service runs on a Windows machine using the standard Windows web server (IIS) for the administrative interface. For smaller numbers of connections, the server may be run on XP (Professional) or Vista (Business). To support a large number of connections or many simultaneously active connections we strongly advise using Windows Server 2003. IIS is free and included with the Windows OS. If using SSL for device-to-server connections or for the administrative interface, you may need to purchase an SSL certificate for the server.