

XPe Thin Client Provision Networks Connection Broker SmartCard Integration with Smooth Roaming

Written by:

Huy Nguyen
Sr. Technical Support Engineer
Provision Networks, A Division of Quest Software
huy.nguyen@quest.com

Date:

April 2008

Purpose

The purpose of this document is to show how to configure Smooth Roaming with Smart Cards and the Provision Networks Virtual Access Suite Connection Broker.

End Result

An End-user walks up to XPe Thin Client, slides Smart Card into card reader. The End-user enters his/her PIN, gets authenticated against AD and logs in to the thin client. Provision Networks Virtual Access client will automatically launch, authenticate the user against the Connection Broker and based on what the ACL is set to automatically launch the end-user's Virtual Desktop. If the End-user's Virtual Desktop was in a Disconnection State, the End-user will reconnect to that Virtual Desktop. Once the End-user is done with his/her Virtual Desktop session, all he or she needs to do is unplug the Smart Card from the card reader.

Based on Microsoft GPOs set on the Thin Client OU and VDI OU, the Virtual Desktop will enter into a Disconnected State and the thin client will Log Off.

The End-user can then walk up to a new Thin client, slide in their card and the session will be reconnected and the end-user can continue their session.

Thin Client Setup

While logged in as Administrator, plug card reader into Thin Client and make sure reader installs properly.

- i. Install ActivIdentity Software on Thin Client
- ii. Install Provision Networks Virtual Access Client on Thin Client
- iii. Join Thin Client to Domain
- iv. Login as Local Administrator account
- v. Open regedit, go to:
 - a. HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
 - b. Modify Shell from Explorer.exe to "C:\Program Files\Provision Networks\Virtual Access Client\pnap32.exe" /di (Desktop Integrated Mode)

****Note, once you replace the shell on the thin client, no one will have access to the desktop anymore. By default, only the Administrator will be able to launch Task Manager to do administrative tasks.****

VDI Setup

- i. Install PNTools
- ii. Install ActivIdentity Software

Active Directory GPO Setup

Create 2 OUs, One for Thin Clients and one for VDIs. Create a new GPO for each OU.

GPO for Thin Client OU

Set:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Interactive logon: Smart card removal behavior

Force Logoff

GPO for VDI OU

Set the following policies:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Interactive logon: Smart card removal behavior

Disconnect if a remote Terminal Services session

Computer Configuration\Administrative Templates\Terminal Services

Keep-Alive Connections

Automatic reconnection

Computer Configuration\Administrative Templates\Terminal Services\Sessions

Set time limit for disconnected sessions

Never

Set a time limit for active but idle Terminal Services sessions

15-30 minutes depending on customer requirements

Configuring the AppPortal Client

The "Download Automatically" option is the ideal way to propagate the configuration to your users, and there are a couple of ways to do it.

- Assuming your users' computers are joined to an internal AD domain, simply customize config.xml per the VAS admin guide and place it on ANY web server. The trick is to add a DNS host entry named provision.domainname (i.e., provision.xyz.com). By doing so, AppPortal will auto-seek config.xml from http://provision.xyz.com or https://provision.xyz.com.
- Alternatively, instead of hosting config.xml on http://provision.xyz.com or https://provision.xyz.com, you can put it on any web server by any name. You can even put it on a file server. However, for AppPortal to know where the config.xml resides, you must specify the URL or file share in the computer's registry.
 - This means that you would need to push the reg value AutoConnectURL to HKLM or HKCU using a logon script, group policy, or something like SMS.

AutoConnectURL is a registry value of type String (REG_SZ) and can reside under either "HKLM\Software\Provision Networks\Provision-IT Client"

Or

"HKCU\Software\Provision Networks\Provision-IT Client"

Examples of valid AutoConnectURL values include:

- ✓ http://provision.xyz.com
- ✓ https://provision.xyz.com
- ✓ <file://fileserver/share>

CONFIG.XML

Config.xml file can be found on your Connection Broker (C:\Program Files\Provision Networks\Provision-IT) or on your Web-IT server (C:\Inetpub\wwwroot\Provision\web-it)

<ServerFarms>

- NOTE: All element names are case sensitive.

<Farm FarmName = "XYZ Farm Connection"

HideSettings = "1"
DefaultLocation = "1"
PromptForLocation = "0"
EnableSSO = "0"
EnableKerberos = "1"
KerberosMode = "0"
DisallowSaveCredentials = "0"
DesktopWidth = "1024"
DesktopHeight = "768"
FullScreen = "1"
SpanMonitors = "1"
ColorDepth = "24"
SeamlessMode = "1"
EnableSmartSizing = "1"
DisplayConnectionBar = "0"
PinConnectionBar = "0"
AudioMode = "0"
KeyboardHook = "0"
RedirectDrives = "0"
RedirectPrinters = "0"
RedirectUniversalPrinters = "1"
RedirectComPorts = "0"
RedirectSmartCards = "1"
RedirectHandhelds = "0"
RedirectClipboard = "0"
RedirectMicrophone = "0"
EnableWallpaper = "0"
EnableFullWindowDrag = "0"
EnableAnimation = "0"
EnableThemes = "0"
EnableBitmapCaching = "1"
AutoReconnect = "1"
AllowPasswordManagement = "0"
PasswordManagementServer = ""
PasswordManagementPort = "443"
DShortcutLocations = "7"
AutoLaunchApp1 = "Desktop1"
AutoLaunchApp2 = ""
AutoLaunchApp3 = "" >

<Location Number = "1"
Name = "Inside Office"
Protocol = "0"
TCPPort = "8080"
UseProxy = "1"
ProxyServer = ""
ProxyBypassList = ""
ServerList = "10.0.0.X,10.0.0.Y"
RDPonSSL = "0"
EnableNAT = "0" />

<Location Number = "2"
Name = "Outside Office (SSL)"
Protocol = "1"
TCPPort = "443"

```
UseProxy = "0"  
ProxyServer = ""  
ProxyBypassList = ""  
ServerList = "ssl.mycompany.com"  
RDPonSSL = "1"  
SSLGateway = "ssl.mycompany.com"  
EnableNAT = "1" />  
</Farm>  
</ServerFarms>
```

Sections in the Config.xml of interest

- i. EnableKerberos = "1"
 - a. In order to use Kerberos passthrough, PNTools must already be installed on VDI Workstation and pngina.dll is the gina set on VDI workstation
- ii. KerberosMode = "0"
 - a. Set KerberosMode to "1" if you are using the Softgrid client within the VDI Workstation. This will initiate a second PIN re-authentication for the user after the Virtual Desktop has launched
- iii. AutoLaunchApp1 = "Desktop1"
 - a. Enter the name of the Published Desktop as it is shown in the Managed Applications section of the PNConsole
- iv. RedirectSmartCards = "1"
 - a. Required for Smart Cards to passthrough from thin client to Virtual Desktop

Final Testing

To verify that the solution meets all customer Smart Card criteria, set the policy on the AD user account to require Smart Card to login.