



iPassConnect Client User Privileges



Introduction

The iPassConnect Client is an intelligent and dynamic client that has many features that enable the iPass service to provide high levels of resilience, advanced reporting (via IOQ) and dynamic access directory (phonebook) management. This all adds to provide the user with a simple but effective user interface that strives to deliver a first time connection every time.

This document outlines the user privileges to install and support the use of the iPassConnect Client.

Background

To provide these features the client obviously has to have some enhanced user privilege rights over the local desktop. The client must be able to add and remove PoPs or broadband access points from the phonebook. Local in-country dialing rules need to be regularly updated as local telecom authorities enact changes. As our network of Wireless ISPs (WISP) modifies their gateways (SSID and WEP keys) our client must adapt to provide continuous connectivity. Furthermore, we allow each customer to make dynamic changes to the client configuration (ranging from simple dial timers to enhanced VPN, Personal Firewall and AV integration). Lastly, we also allow our client to be remotely upgraded, to allow new features and enhancements to be exploited as soon as they become available. This all adds up to iPassConnect being the most advanced, flexible and feature-rich global roaming solution available on the market today.

iPassConnect - Installation

The very nature of such a client means that it requires to be run with Power user rights (or at least full access rights of (read/modify and create) over certain key files and directories). In general, iPassConnect v2.4 does not make changes to the registry so the user does not need to have any administrative privileges to install the software, however v3.x does require at least Power rights.

- You only need Power User Rights in order to install the client but Admin rights if the client is to use pre-login. Admin rights are required to install the Cisco VPN Client.

iPassConnect - Operation

By default, iPass recommend that a user must be a member of the Power Users Group in order to run iPassConnect successfully. Since this may not always be permissible or practical we have found that is often possible for the following permissions to be set manually to allow iPassConnect to run:

- Full Control of iPassConnect folder and contents (including create & modify)
 - Lack of this can cause anything from passwords or bookmarks not saving, to tabs not displaying, PB update problems etc.)
- iPassConnect must be able to create a DUN connectoid in the system phonebook. iPassConnect needs write access to the following folder:

`%ALLUSERSPROFILE%\Application Data\Microsoft\Network\Connections\Pbk`

- Full Control of "rasphone.pbk" Without this, users will get an error saying "Could not create phonebook entry".

This is usually located in:

`C:\Documents and Settings\All Users\Application Data\Microsoft\Network\Connections\Pbk`

This file contains the Windows DUN entries.

Third Party Application Integration

It should however be noted that iPassConnect does require registry access for customization options when iPass controls third party applications for security policy enforcement, such as VPN (such as Auto-teardown on the Cisco VPN) and personal firewall integration settings.

Lastly any independent scripts that are to be launched by iPC may also need enhanced privileges.

- The following permissions are required for VPN integration:
- Full access to : `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\VPN Client`
- For AV and PFW integration for Access to appropriate Registry setting is also required.

For example for we read the OS. For 98 and ME, we read the registry

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\McAfeeVirusScanService.`

If it is present, we start that process. For NT, 2K and XP, we try to launch the service AvSynMgr. If that doesn't launch, we try to launch the enterprise version, McShield. For polling we check the OS. For 98 and ME, we check if AvSynMgr.exe is running. For NT, 2K and XP, we check if the service (AvSynMgr or McShield) is running.

Lastly any independent scripts that are to be launched by iPC may also need enhanced privileges.

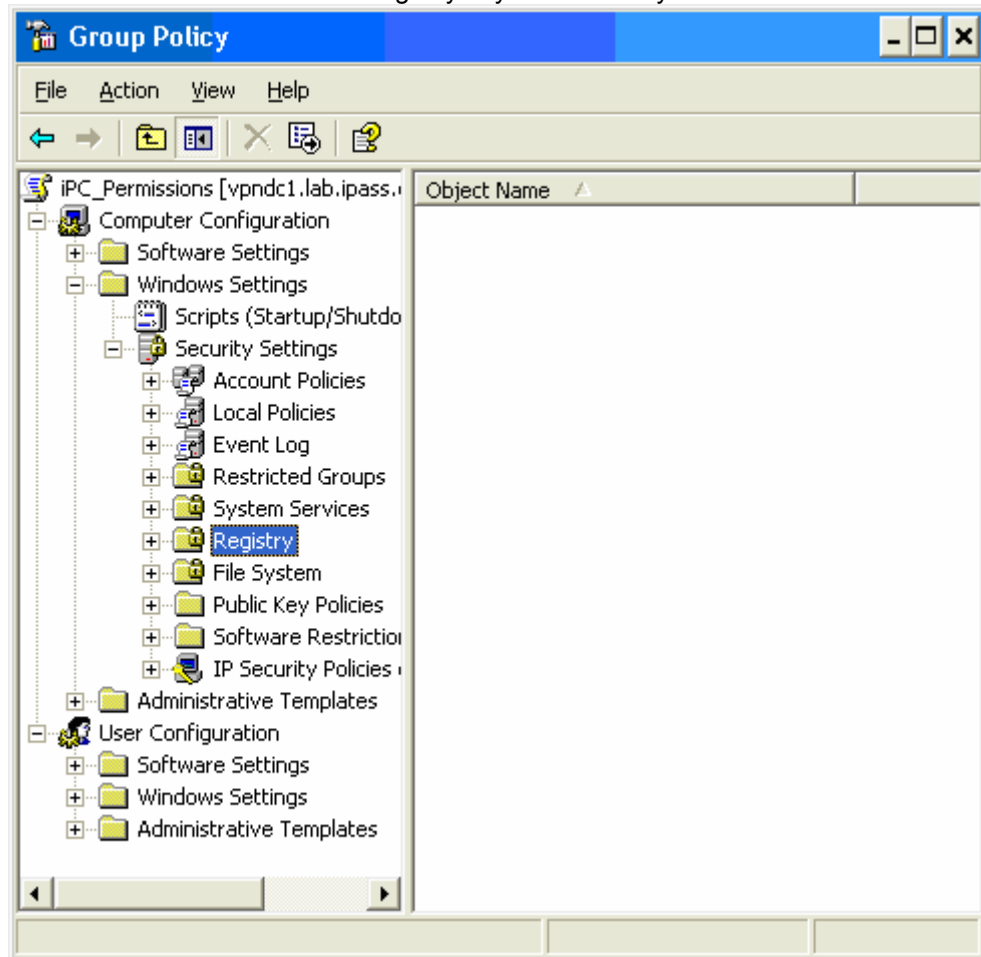
Note: These problems will only occur on Windows NT/2000/XP and only when using an NTFS Partition.

Using Active Directory to modify iPC registry/directory permissions

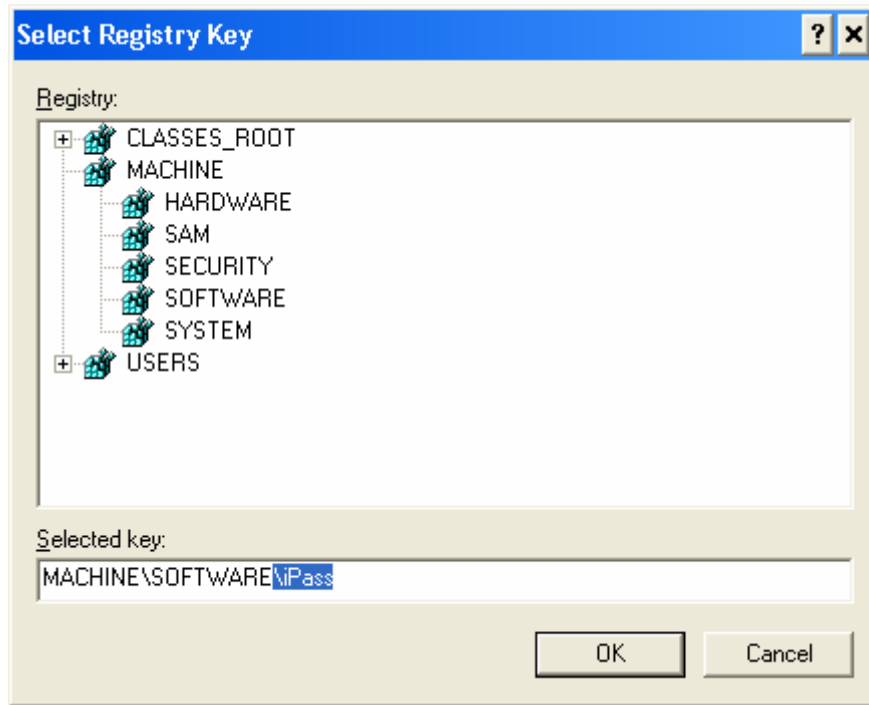
If a customer is using Microsoft Active directory, it is possible to push the necessary registry and directory setting for iPassConnect to all users.

Start by creating a new Group Policy Object (GPO) or edit an existing one. It is preferred to edit an existing GPO as added more GPO's to the directory can have adverse affects on system boot/logon performance.

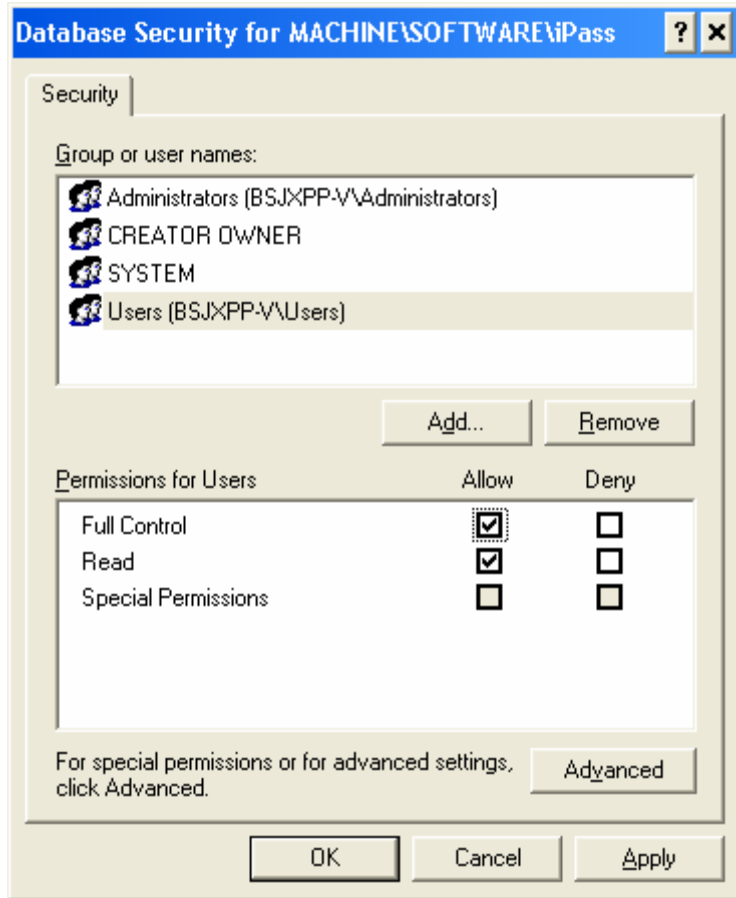
Under the GPO, navigate to the following containers to add access control lists (ACL's) to modify the permissions on the iPassConnect registry key and directory.



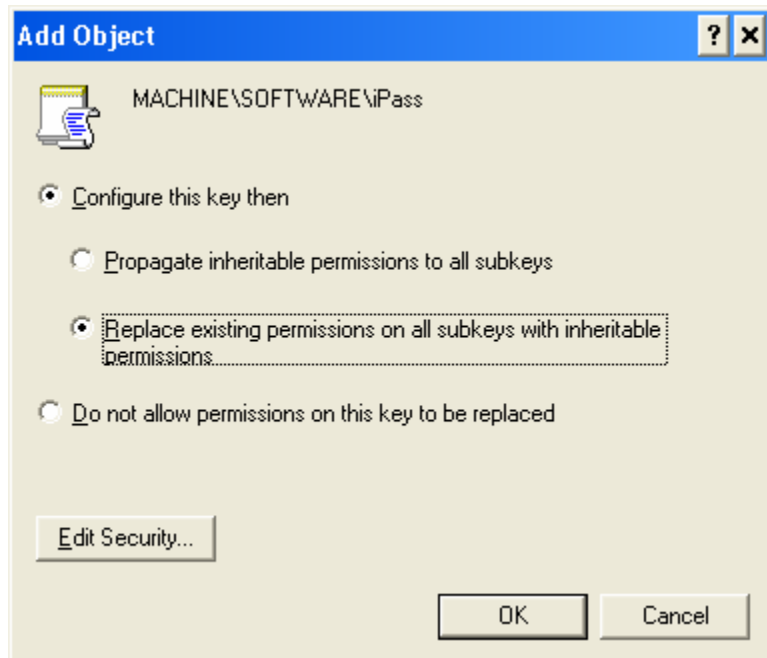
To modify the registry permissions, right click the container and select "Add key". Browse to "MACHINE\SOFTWARE" and manually type in the `\iPass` path as shown below:



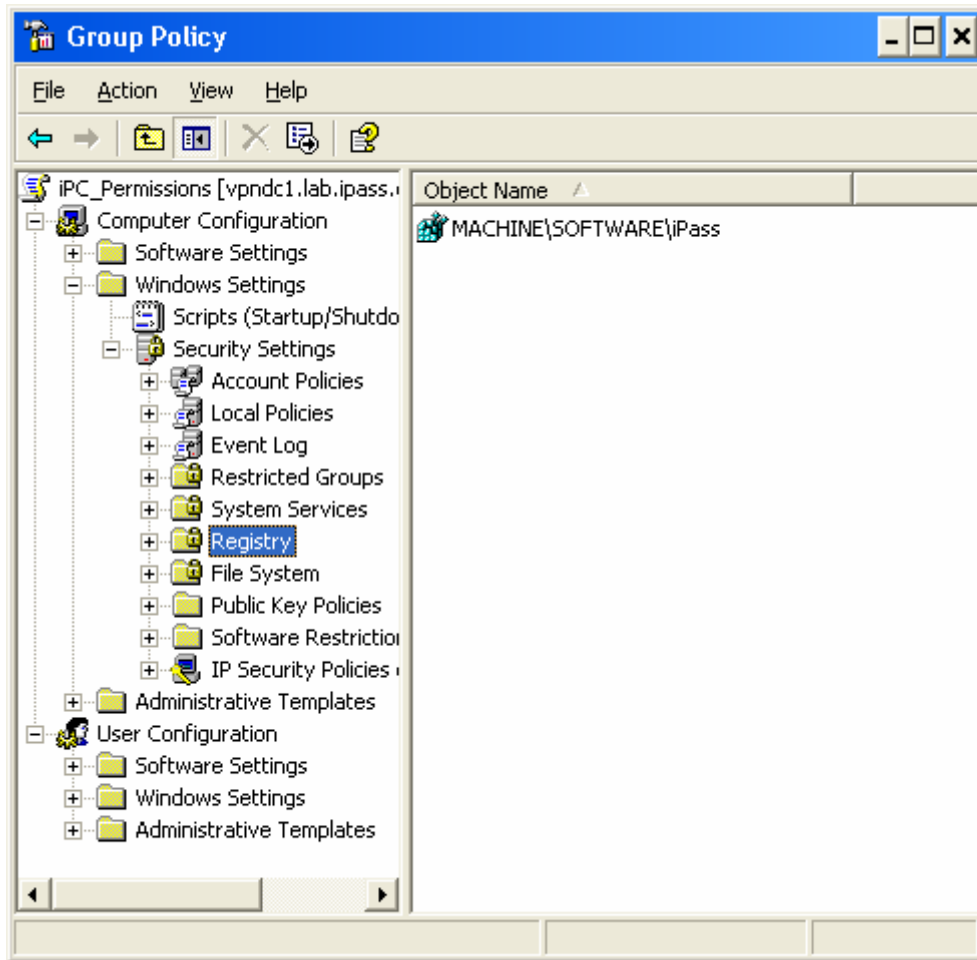
Click OK. You will then be presented with the permissions dialog screen. Select the "Users" local group and then check the "Full Control" check box as shown below:



Click OK. You will then be presented with the “Add object” dialog screen. Make sure the setting for “Replace existing permissions on all subkeys with inheritable permissions” is checked as shown below:

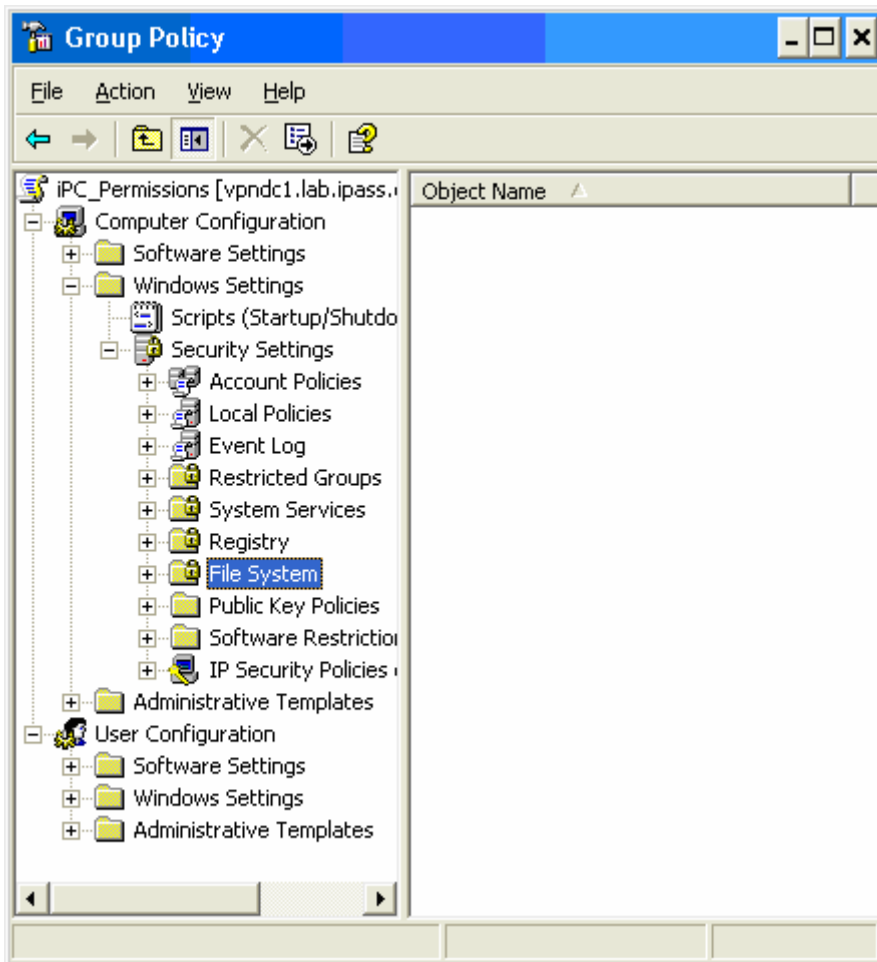


Click OK. You should see the following:

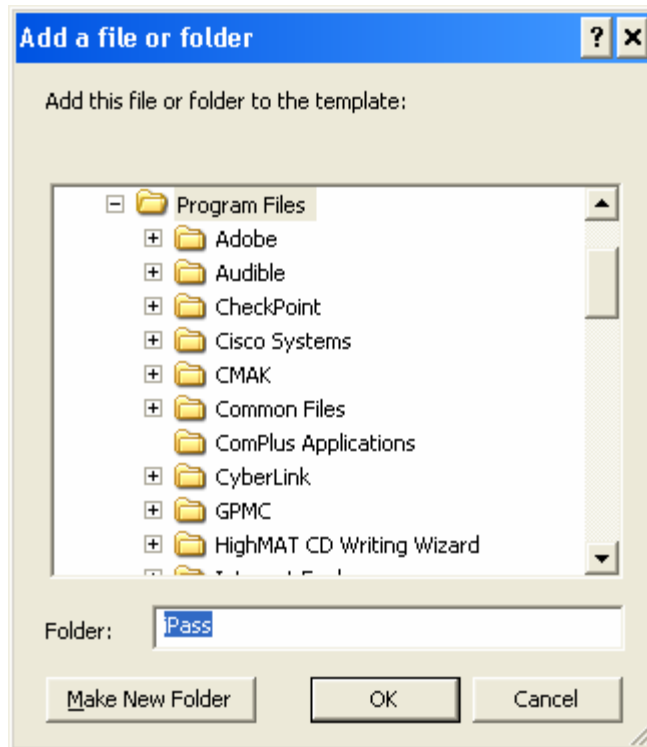


This concludes the section on modifying the iPassConnect registry permissions.

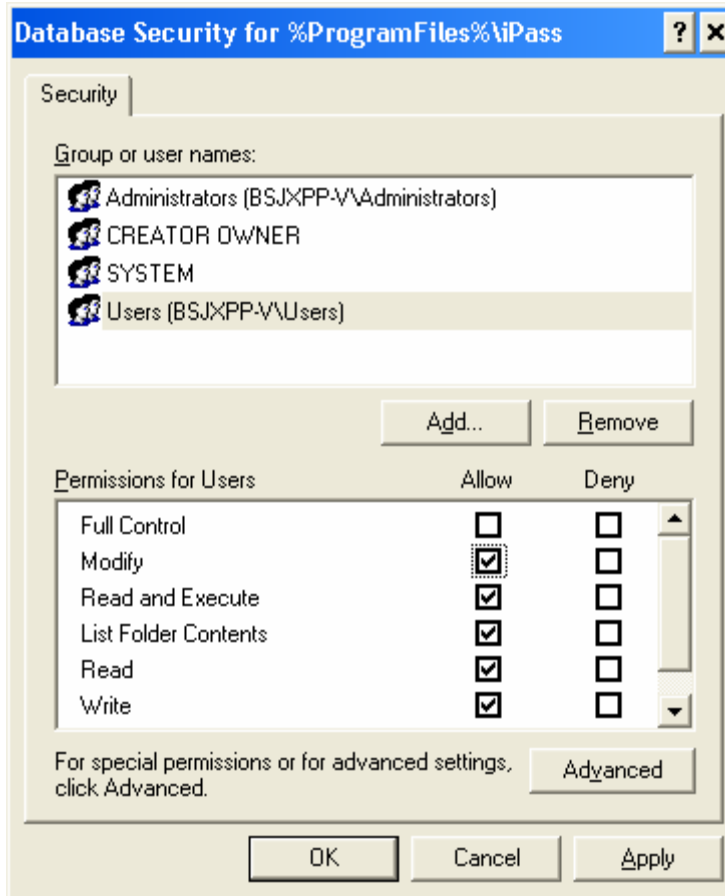
To modify the iPassConnect installation directory permissions via GPO, right click the “File System” container and select “Add file”.



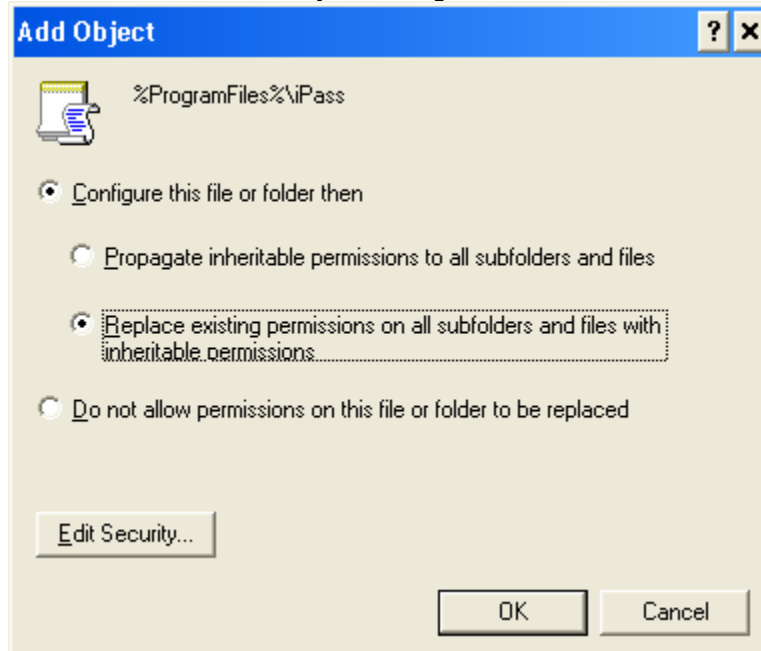
You will be presented with a “Add a file or folder” dialog screen as shown below:



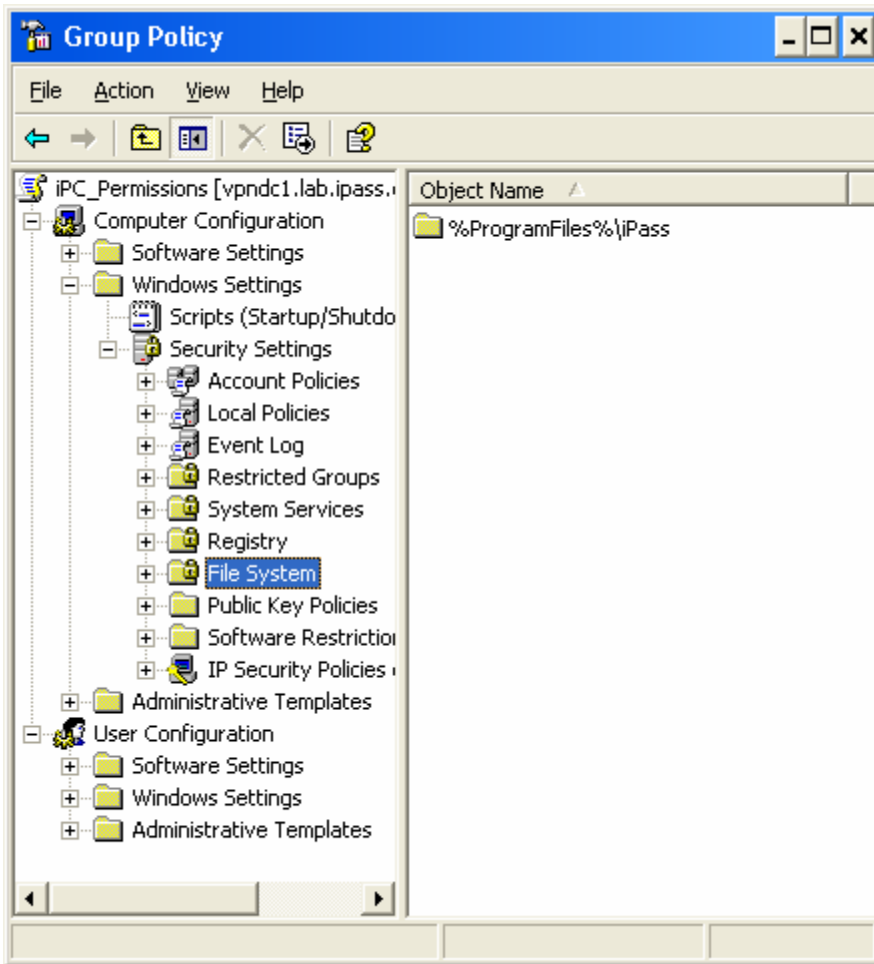
Since the iPass directory doesn't exist on the server you are authoring/editing the GPO on, you'll need to create it. Do this by first browsing to the "\Program Files\" directory and then OVERWRITE the word "Program Files" in the "Folder:" field and insert "iPass" (without the quotes) as shown in the above image. Click OK to be presented with the security permissions dialog box for the iPass directory. Select the local "Users" group and check the "Allow" check box in the "Modify" row. You may optionally enable the "Allow" check box for the "Full Control" row, but "Modify" permissions is sufficient.



Click OK to be presented with the “Add Object” dialog box and ensure the following settings:



Click OK and confirm the following entry in the GPO “File System” container:



Close the Group Policy window to commit the GPO.

The registry key and install directory must already exist on the target PC. If they do not exist, no permissions are applied (i.e. the registry key and directory are not “created” if not present). Users who do not have the iPassConnect client installed must do so first (manually or have it pushed to their PCs) and then either reboot their PC on the LAN or type GPUPDATE.EXE at any command line (or the Windows “Start → Run” dialog box) in order to refresh the group policy objects on the local PC.

Corporate Headquarters
iPass Inc.
3800 Bridge Parkway
Redwood Shores, CA 94065
United States
Tel: +1 650.232.4100
Fax: +1 650.232.4111
www.ipass.com

United Kingdom
iPass (U.K.) Limited
139 Piccadilly
London W1J 7NU
United Kingdom
Tel: +44 20.7317.4400
Fax: +44 20.7317.4450

Germany
iPass (U.K.) Limited
Stiglmaierplatz/Dachauer
Straße 37 (5.OG)
80335 Munich
Germany
Tel: +49 (0) 89.54.55.8.120
Fax: +49 (0) 89.54.55.8.333

Australia
iPass Holdings Pty Ltd.
Level 1, 80 Waterloo Road
Macquarie Park, NSW 2113
Australia
Tel: +612 8876.8700
Fax: +612 8876 8777

Hong Kong
iPass Asia Pte Ltd.
3802A, Lippo Centre Tower
Two
89 Queensway, Admiralty
Hong Kong
Tel: +852.2918.8268
Fax: +852.2918.8278

Japan
iPass Inc.
Ginko Kyokai Building
15th Floor
1-3-1 Marunouchi
Chiyoda-ku, Tokyo 100-0005
Japan
Tel: +81 3.3216.7266
Fax: +81 3.3216.7281

Singapore
iPass Asia Pte Ltd.
7 Temasek Boulevard
#23-02 Suntec Tower One
Singapore 038987
Tel: +65 6334.8783
Fax: +65 6337.0331