

## [SECURE SETUP OF PCANYWHERE]

This document provides recommended configuration settings to enhance the level of security provided by Symantec's PCAnywhere® remote control software

## Purpose

This document provides details on various configuration settings within Symantec's PCAnywhere remote control software product that can be used to enhance the level of security provided by the product.

MICROS recommends that PCAnywhere be used as a remote control method only in conjunction with standard dial-up modem or a secure internet connection. It is recommended that PCAnywhere not be configured for use on direct internet based network connections or in situations where the PCAnywhere Host is placed in a "listening" or "Waiting for Connection" mode for any period other than when remote support access is needed. MICROS further recommends that customers take full advantage of all security options available within the PCAnywhere product.

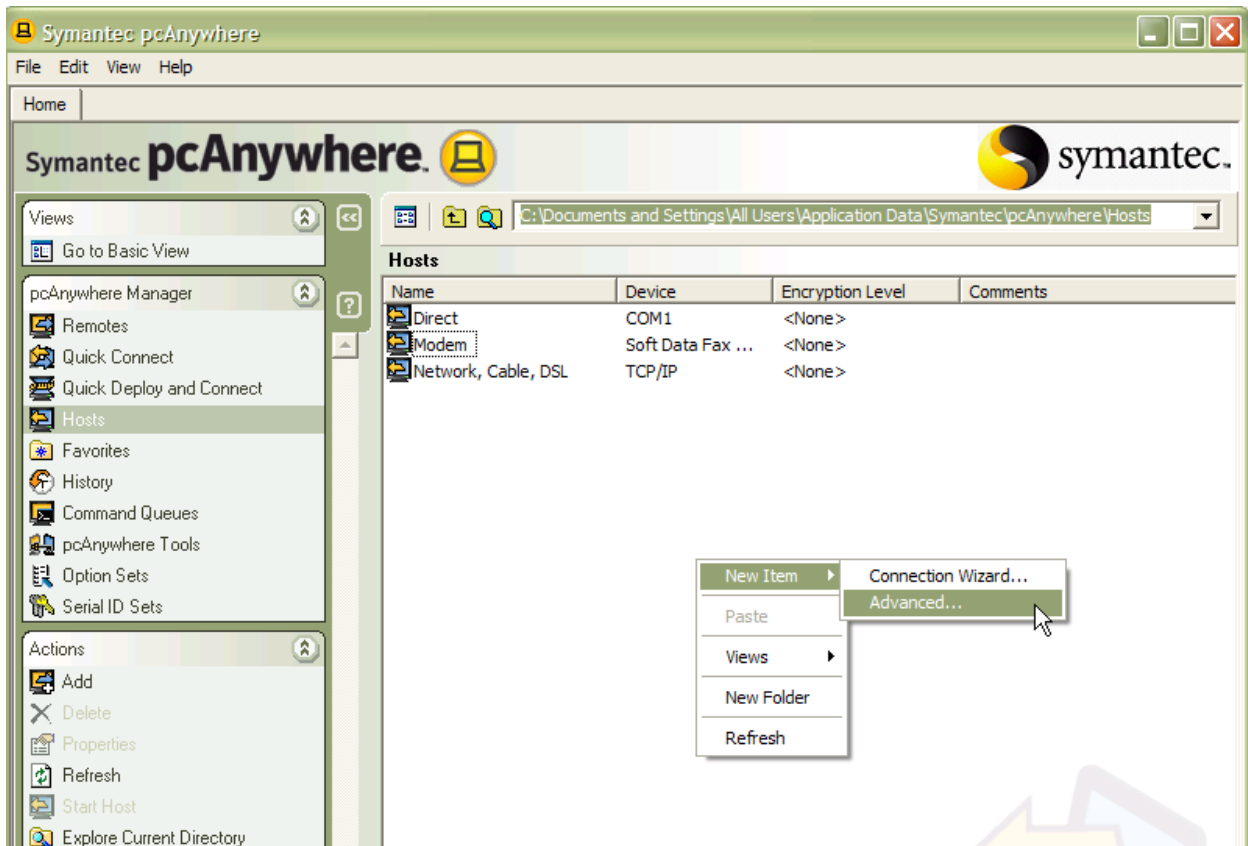
This information included in this document is based upon configuration options and settings available in Symantec PCAnywhere version 12.5 and later.

## Secure PCAnywhere Host Configuration

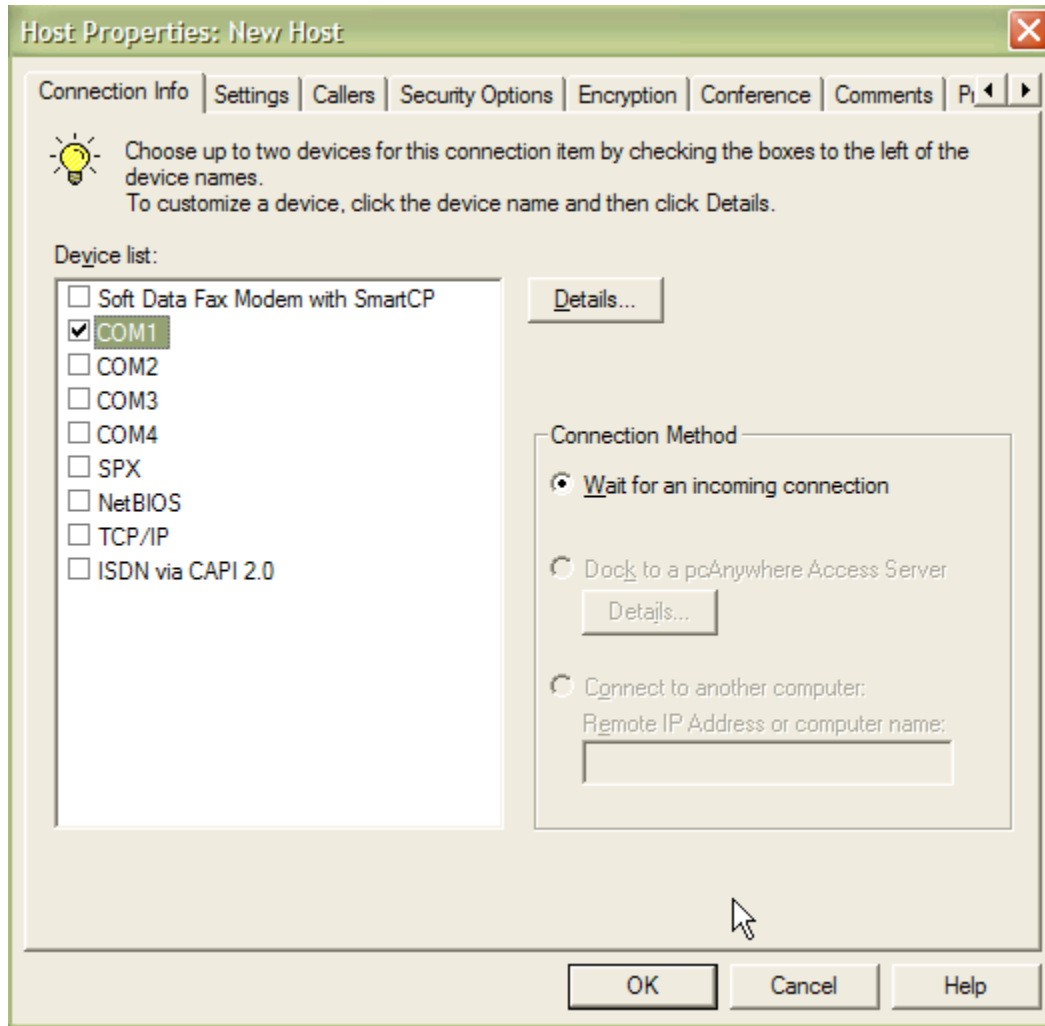
The following steps will help you configure a secure PCAnywhere Host for use by MICROS Customer Support as a remote control and support method.

### 1. Create a new Host

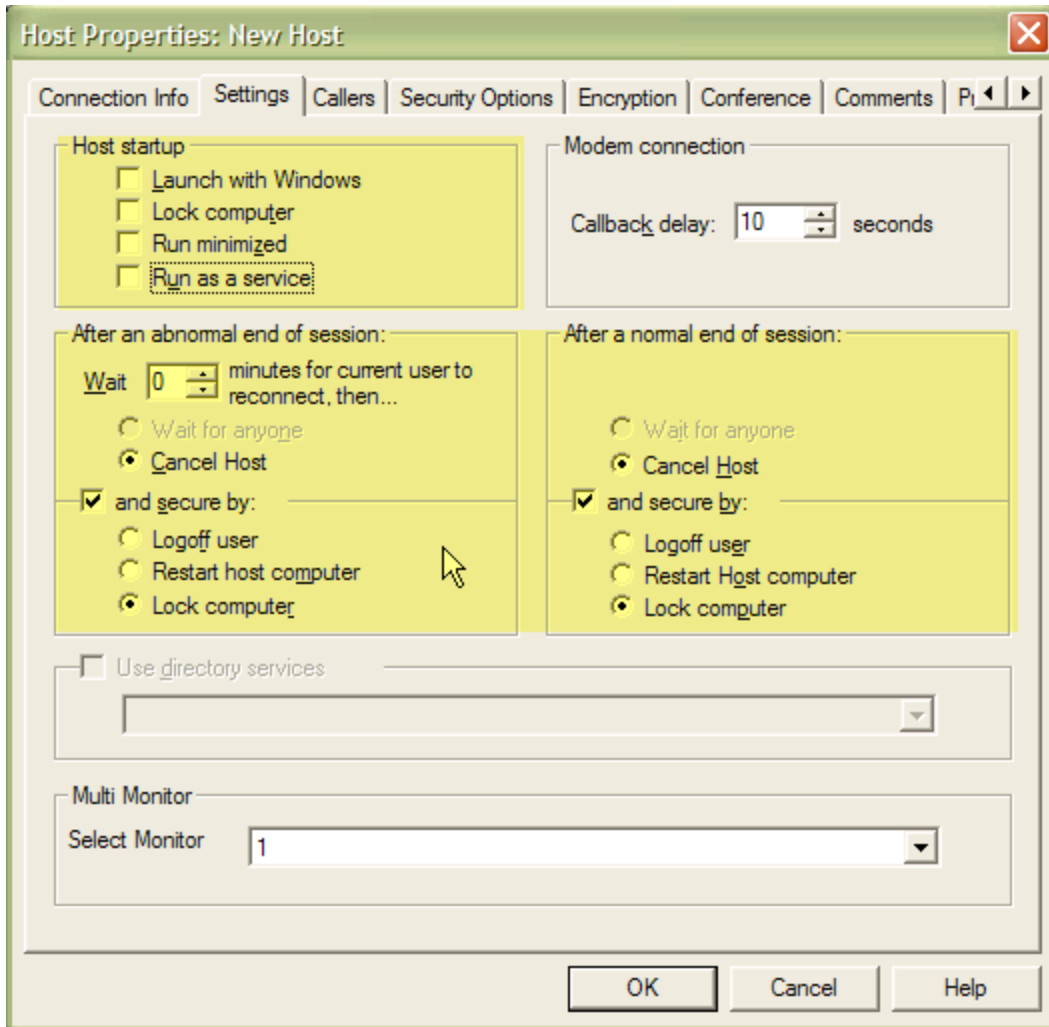
Open PCAnywhere and navigate to the "Hosts" tab or section. A list of existing Hosts will be displayed. In the menu bar at the top of the application window select "File" → "New Item" → "Advanced" or right-click in the Hosts area and select the same options:



The Host Properties window will now be displayed. On the Connection Info tab, in the Device List window, select the device which MICROS Customer Support will use to remotely access your system (be sure to NOT select your Credit Card modem if one is in use). Make certain that the desired device is the only device selected. If you are using a secure internet connection select "TCP/IP"; if using a dial up modem select the appropriate COM port on which the modem is connected and configured. Uncheck any other devices that are not in use.

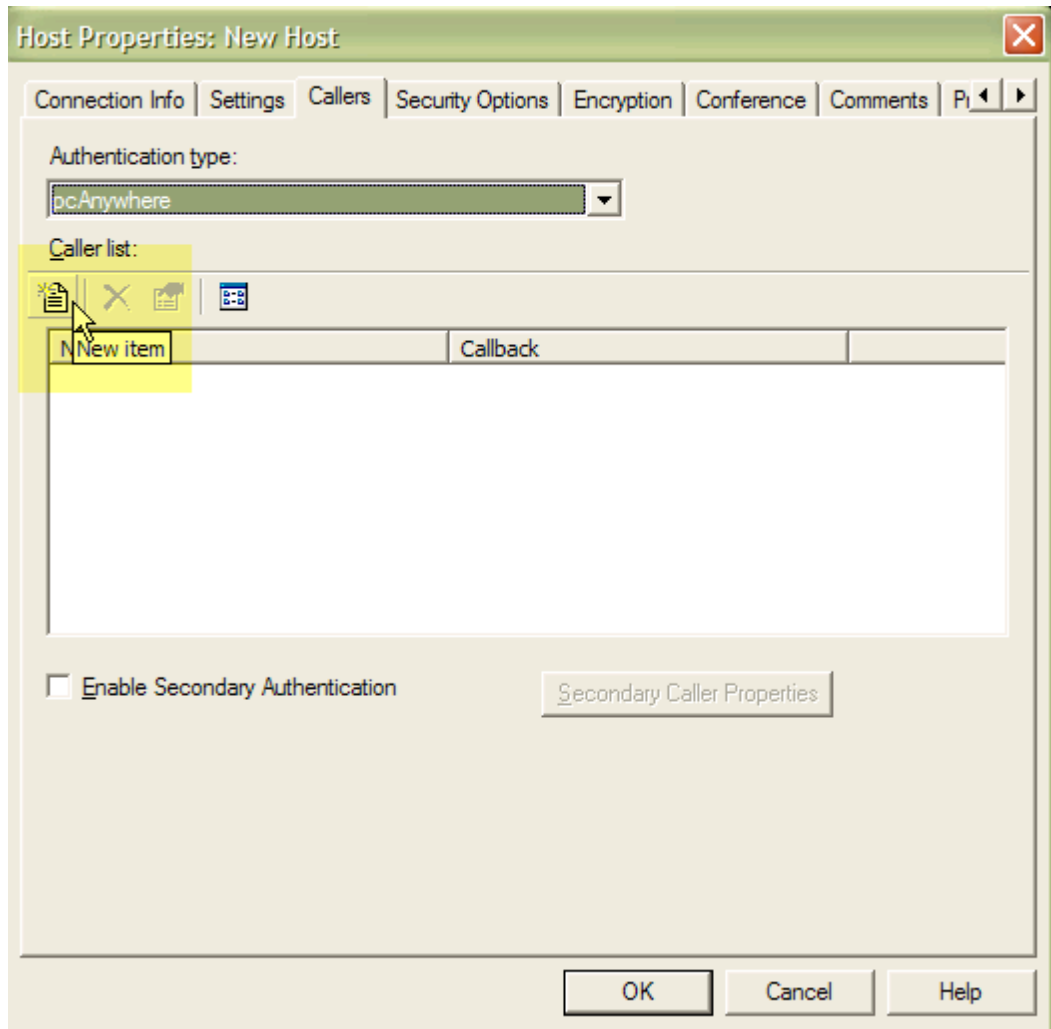


Click on the "Settings" tab and select the following options:

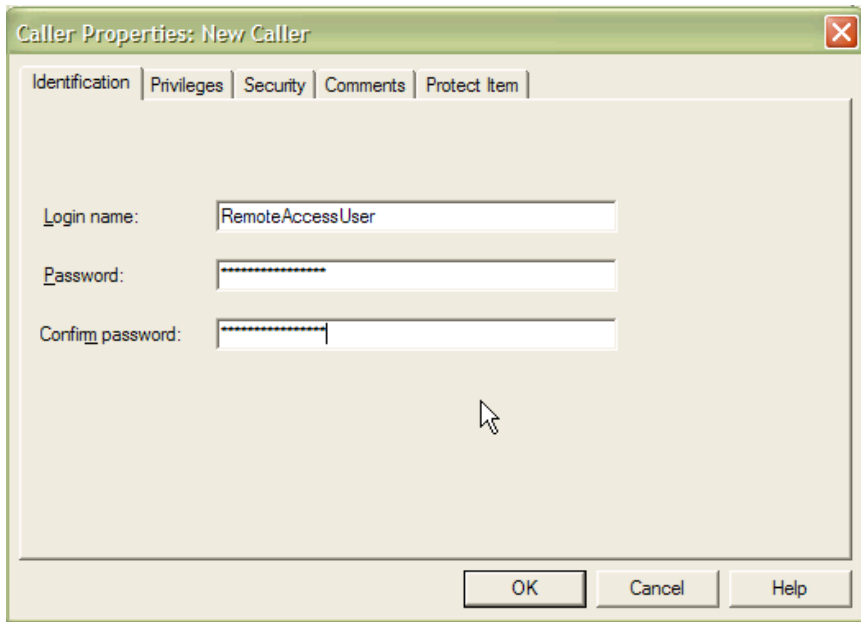


- In the Host Startup area the following options should be unselected:
  - o Launch with Windows
  - o Lock Computer
  - o Run minimized
  - o Run as a service
- In the “After abnormal end of session” area select:
  - o “Cancel Host”
  - o Select “and secure by:”
  - o Select “Lock computer”
- In the “After a normal end of session” area select:
  - o “Cancel Host”
  - o Select “and secure by”
  - o Select “Lock computer”

On the “Callers” tab click on the “New Item” icon:

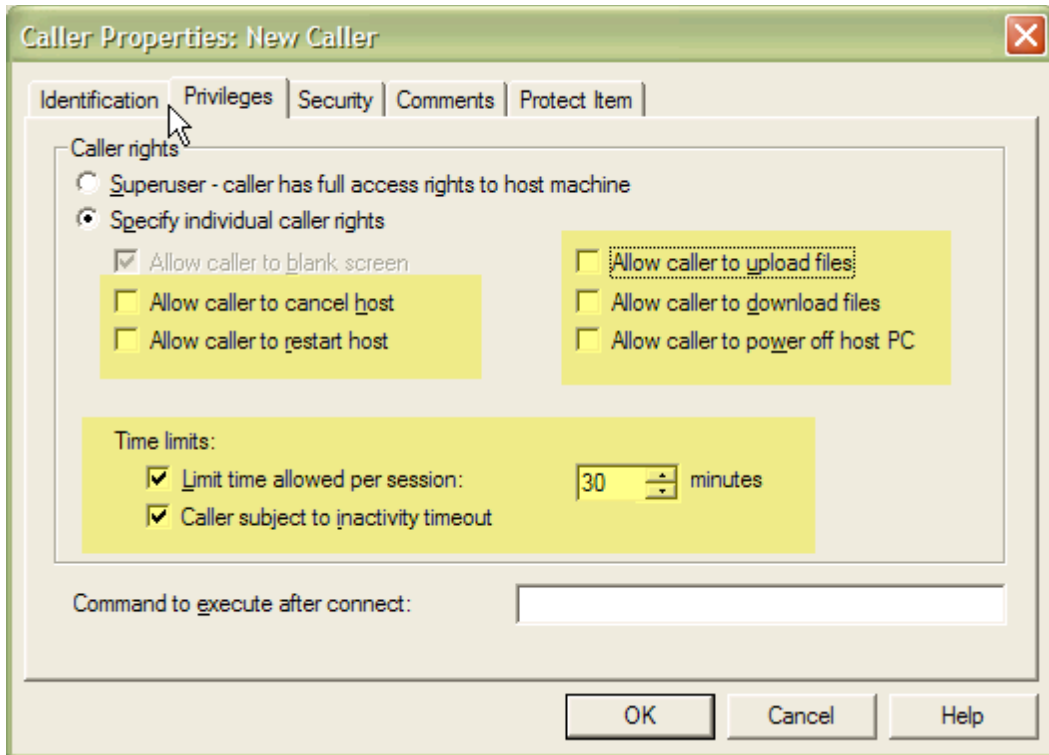


This will display the Caller Properties window. This is where the username and password will be created for MICROS Customer Support to use when remotely accessing your system. Create a unique username avoiding the use of common names such as “micros”, “support”, “administrator” or other easily guessed usernames. Create a unique and complex password for this username using a combination of at least eight upper and lower case letters, numbers and special characters (i.e. @\$%^&\*()\_+). Do not store this password in an unsafe location where it can be accessed by unauthorized individuals.



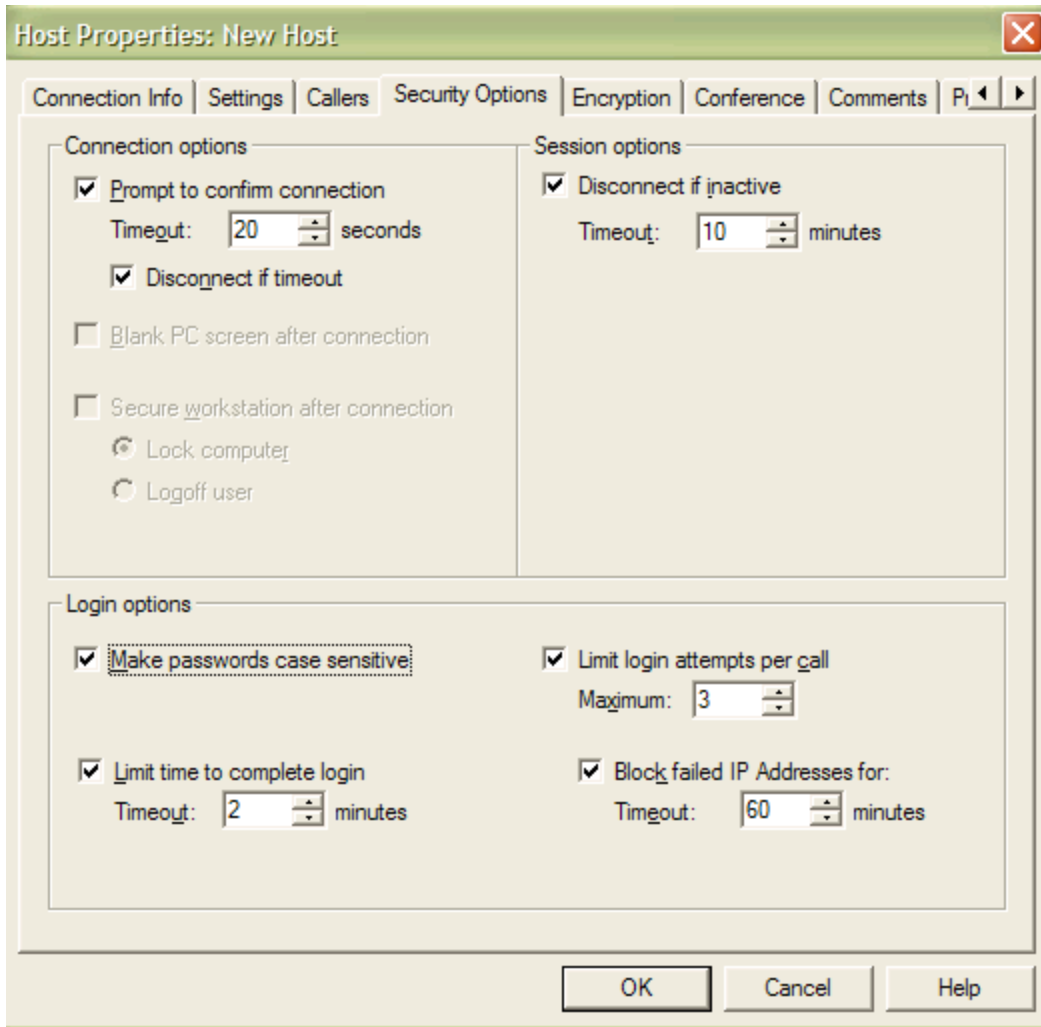
Click on the "Privileges" tab and verify the following settings:

- "Allow caller to blank screen" should be unselected
- "Allow caller to cancel host" should be unselected
- "Allow caller to restart host" should be unselected
- "Allow caller to upload files" should be unselected
- "Allow caller to download files" should be unselected
- "Allow caller to power off host PC" should be unselected
- "Limit time allowed per session" should be selected and the "minutes" value should be set to a desired time limit
- "Caller subject to inactivity timeout" should be selected



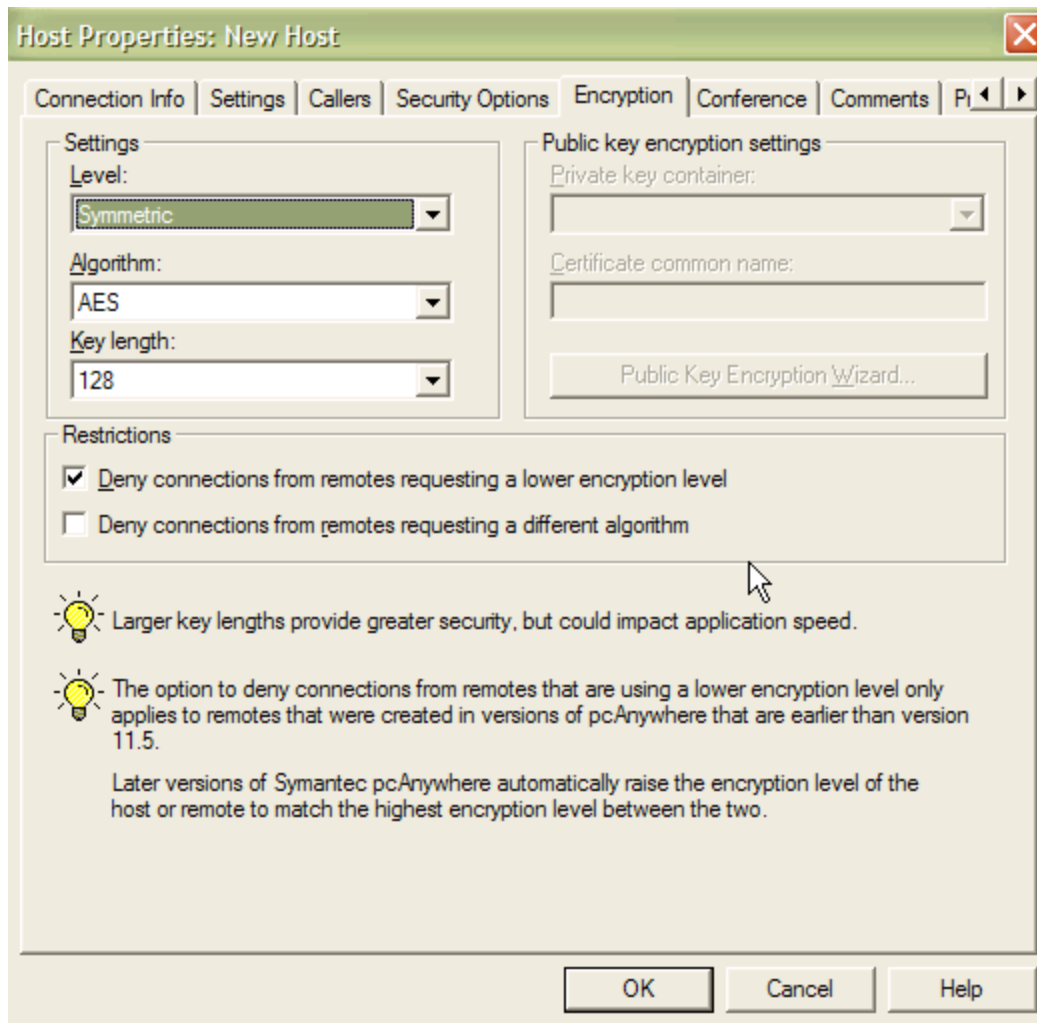
Click "OK" to save these settings and return to the Host Properties window.

Select the "Security Options" in the Host Properties window and verify the following settings:



- "Prompt to confirm connection" is selected
- "Timeout:" is set to an appropriate value
- "Disconnect if timeout" is selected or checked
- "Disconnect if inactive" is selected or checked
- "Timeout:" is set to an appropriate value
- "Make passwords case sensitive" is selected
- "Limit time to complete login" is selected and "Timeout" is set to an appropriate value
- "Limit login attempts per call" is selected and "Maximum" is set to an appropriate value
- "Block failed IP Address for" is selected and "Timeout" is set to an appropriate value

Select the "Encryption" tab and verify the following settings:



- "Level" is set to "Symmetric"
- Algorithm is set to "AES"
- "Key Length is set to at least "128"
- "Deny connections from remotes requesting a lower encryption level" is selected
- "Deny connections from remotes requesting a different algorithm" is selected

Other settings not covered in the document such as the "Protect Item" tab can be set as needed or desired.

Click "OK" to finish the configuration of your new Host. In the Hosts window, name the connection with something that can be readily identified as the connection to be used by MICROS Support (i.e. MICROS Remote Support Host").