

PROXY PRO HOST ADVANCED USAGE GUIDE: STEALTH MODE

A strength of the Proxy Networks remote desktop software product lineup is the flexibility around how the client experience can range when a remote control connection can be established. Specifically, those connections can be made to Host computers without there being any indication or obvious clue to the user in front of it. This is a standard feature available within the on-premise PROXY Pro P2P and PROXY Pro RAS Editions and the hosted PROXY Air Dedicated remote desktop service. This document will describe several ways to achieve a stealth mode configuration state from both the perspective of a new installation as well as from an existing installation where a Stealth Mode configuration is desired but not currently in use.

The primary questions answered in this document are:

- Shadowing my users in stealth sounds interesting, what should I know about this capability?
- How can I test this on one Host computer?
- How do I get all (or some) of my Host machines to behave in Stealth Mode?

Background Information & Defining Stealth Mode

The PROXY Pro Host is the client application installed on each Windows computer that is to be remotely accessed. It runs as a service in the background and starts with Windows, so it's always running in the background and allows for connectivity to the machine regardless as to where it's online from. The Proxy Host Control Panel is the UI for the client and has a number of tabs containing settings that dictate, among other things, how the Host should behave when a connection to it has either been begun or has been closed. When either of these two connection events occur, the Host can emit a series of beeps, a popup notification in the bottom right corner among others that are useful in attended support scenarios but not for stealth. The easiest way to familiarize yourself with the Host settings is to open the Proxy Host Control Panel from the Proxy Networks program group on the start menu. There is not one singular setting that enables Stealth Mode and it is instead achieved through the use of a few settings covered within the next section of this document.

For new Host installations, we recommend using the PROXY Pro Deployment Tool to first create a Host settings template containing what we recommend here, plus your own Host license and Gateway server details, and then turn it into a transform.mst file that contains and applies settings at installation time. The Host is actually installed via msixexec command that would run in an automated fashion in several ways but the most common is via group policy as a startup/login script.

For existing Host installations, we can recommend up to three methods that can be used to configure them to behave in stealth mode. The Deployment Tool has an Update Host Settings capability that pushes out settings to existing machines it can reach and change the Host settings described here, plus your own Host license key and Gateway server connectivity details (if applicable) and you'll have your own install file that applies all of it. In the case where Hosts are already deployed but are not presently configured to behave in stealth mode when they should be, the Host Settings Updater Tool can remotely apply a new string of Host settings real-time. The final approach is to use the Host's command line configuration utility PhSetup which requires building a command and then ensuring it runs via group policy as a startup/login script or similar.

Additionally, note that if you have input control rights to the Hosts, you will get mouse and keyboard control immediately unless you connect in View Only mode. Note that View Only mode will connect you to the Host but will not have the mouse and keyboard functionality enabled until you click the Input Control button on the connection window toolbar.

To connect for View Only in the PROXY Pro Web Console, right-click a Host, click Connection -> Connect in View Only. From the installed PROXY Pro Master, right-click a Host -> Connect Special -> Remote View. Connecting in this manner will ensure that

you do not immediately have the mouse and keyboard control of that Host, which can make it very obvious to the end user that somebody has control of their computer if they notice their mouse moving.

Furthermore, please note that it's possible to revoke the input control right altogether if needed.

Defining each of the PROXY Pro Host Settings making up Stealth Mode

This section will cover the individual settings that make up Stealth Mode on the PROXY Pro Host computers within the Proxy Host Control Panel UI. Several settings make up stealth mode and each can be controlled with the use of PhSetup.exe, the Host's command line configuration utility. For each setting you'll see where to find it within the Host Control Panel UI and at the end we'll provide the exact phsetup syntax necessary to apply all of it in one shot.

- 1) Proxy Host Control Panel -> General tab
 - a. Host Appearance – When there is no connection, set the drop-down to **Hidden**
 - b. Host Appearance – When a connection is active, set the drop-down to **Hidden**
 - c. Beeping – Both beep settings should be **unchecked**
 - d. Popup Notifications – All 3 popup settings should be **unchecked**
 - e. Watermark – Both should be **unchecked**

- 2) Proxy Host Control Panel -> Options tab
 - a. Action on Disconnect should be **None**
 - b. Keyboard and Mouse suppression should either be **None** or **Suppress if the Master requests it** (and if using Suppress if requested, don't use it or your cover may be blown)
 - c. Screen Blanking should be set to **Never** or **Permit** (if Permit, don't use it or your cover may be blown)

- 3) Proxy Host Control Panel -> Access tab
 - a. Access restrictions should be set to **Permit connection**
 - b. Connection Permission should be set to **No permission required**

- 4) Proxy Host Control Panel -> Effects tab
 - a. When to Disable Visual Effects on the Host should be set to **Never disable effects**

The above configuration can be applied to the Host with a PhSetup script, the Host Settings Updater Tool, or the Deployment Tool's "Update Host Settings" capability. One method may work better than another depending on the scenario.

4 Approaches to Achieving Stealth Mode

1) Creating a PROXY Pro Host Install Package with Stealth Mode

The first approach starts with creating a Host installation package that contains and applies the settings necessary to achieve Stealth Mode immediately at install time. When using the PROXY Pro Deployment Tool to create a settings template, the below settings would be adjusted. From the Deployment Tool, expand Product Configurations, right-click Host and choose New. Give the template a name and you'll see a list of all available settings. Below is what to change *in addition to* any other settings you would need such as the Host license and Gateway server connectivity parameters.

- a. Access Restrictions – Set to **Permit**
- b. Connection Permissions – Set to **None**
- c. Manage Visual effects – Set to **Never**
- d. Beep on connect/disconnect – Set to **Off**
- e. Host Console Watermarks – **Uncheck** both
- f. Host Notifications – **Uncheck** all
- g. Show icon while connected? - Set to **Hidden**
- h. Show icon while idle? - Set to **Hidden**
- i. Keyboard and Mouse Suppression – Set to **Never**
- j. Lock Workstation on Disconnect – Set to **No**
- k. Screen Blanking – Set to **Never**

If you can create your transform file with these settings (in addition to your license and any other settings) you will have an install file that configures the Host to behave in stealth mode right from install time. Right-click your template in the left pane, choose New -> Transform File, ensuring your Host-x64.msi is selected as the installation file. If it's blank, back out, right-click Installation files -> New -> Installation file to plug in the Host installer and try again.

2) Using the PROXY Pro Deployment Tool's Update Host Settings Function

This approach requires that the following conditions are met:

- The user running the PROXY Pro Deployment Tool is a member of the local administrator's group on each target Host computer; this applies assuming default Host security has not been modified
- The PROXY Pro Host computers are within the same LAN as that of the computer running the PROXY Pro Deployment Tool and are reachable on the Host's default listening port and protocol (UDP/TCP 1505)
- The Host is configured to accept P2P connections (Host Control Panel -> Security tab ->) with either the Windows Security, OR, Simple Password and the Allow remote administration (peer-to-peer) checkbox enabled

Assuming the above criteria are met:

- a. From the Proxy Deployment Tool's left pane right-click Active Directory Domains and click Refresh.
- b. One or more domains may be found – right-click your domain and click Refresh.
- c. A list of OUs will appear and clicking them will cause the right pane to populate with the computers inside it. Use the right pane to select the machines you want (Control+A to select all) and choose Update Host Settings.
- d. In the case where Hosts are set to Simple Password, provide that password into the field and hit OK. Ignore if the Hosts use default security (Windows auth). Repeat this on other containers.

3) Using the Host's Command Line Configuration Utility to Apply Stealth Mode Settings

For command line use (startup/login script) or similar, this contains all of the previously mentioned settings and will change them to the appropriate values so that the Host behaves in Stealth Mode upon a connection. PhSetup is used to modify the settings of an existing Host – no need to uninstall/reinstall if you can automate the following command.

This approach requires that the following conditions are met:

- Customer has existing mechanism/knowledge of automating commands in a startup or login script (SCCM, GPO)
- The Host computers to be updated can successfully receive login/startup scripts

```
"C:\Program Files (x86)\Proxy Networks\Host\PhSetup.exe" access:permit blankscreen:never  
connappear:hidden connectbeep:off hostnotifications:0 idleappear:hidden  
lockworkstationondisconnect:no managevisualeffects:never permission:none suppresskeys:never  
watermark:0
```

4) Using the PROXY Pro Host Settings Updater Tool to apply Stealth Mode Settings

For use with the Host Settings Updater Tool, below you will find the input it needs in JSON format. The Host Settings Updater Tool user guide can be found at www.proxynetworks.com/documentation. This tool is installed with the current Deployment Tool and can be used to update Host Settings through the existing PROXY Pro RAS server. Note that this option is not available to P2P customers.

This approach requires that the following conditions are met:

- The user running the Host Settings Updater Tool can provide the Gateway service account credentials when prompted or at least a user account that is a member of the local administrators group on each Host
- The computer running the Host Settings Updater Tool must be able to make an outbound connection to the RAS server (on typically WSS 443)
- All of the computers that need to be updated are members of the same managed Host group; the tool sends a Host settings update on a group-by-group basis.
- The Hosts to be updated have an OK status & therefore good relationship with the RAS server

With the above requirements met, please follow the Host Settings Updater Tool Guide and insert the below json string when prompted. Also note that you can find our Host Settings Updater Tool Walk Through video on the Proxy Networks YouTube channel.

```
{  
  "access" : 0,  
  "beepOnConnect" : 0,  
  "connectedAppearance" : 0,  
  "hostNotifications" : 0,  
  "hostconsolewatermark" : 0,  
  "idleAppearance" : 0,  
  "keySuppression" : 2,  
  "lockWorkstationOnDisconnect" : 0,  
  "manageVisualEffects" : 2,  
  "permission" : 0,  
  "screenBlanking" : 2  
}
```

The Proxy Networks Support Team is available by email at support@proxynetworks.com or by phone at 1-877-PROXY-US.