



PC-Duo Host Guide

***Release 12.7 Hotfix #1
April 2016***

Vector Networks, Inc.
541 Tenth Street, Unit 123
Atlanta, GA 30318
(800) 330-5035
<http://www.vector-networks.com>

© Copyright 2016 Vector Networks Technologies and Proxy Networks, Inc. All rights reserved.

PC-Duo is a trademark of Vector Networks Technologies, and PROXY is a trademark of Proxy Networks, Inc. Microsoft, Windows, Windows NT, Windows Server, and other Microsoft products referenced herein are either trademarks or registered trademarks of the Microsoft Corporation in the United States and other countries. Apple, AirPlay, Finder, iPad, iPhone, iPod, iPod touch, iTunes, Keychain, Mac, Macintosh, Mac OS, OS X, Retina, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc. IOS is a trademark or registered trademark of Cisco in the U.S. and other countries. Novell and NetWare are registered trademarks of Novell, Inc. All other trademarks are the property of their respective owners.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>), cryptographic software written by Eric Young (eyay@cryptsoft.com), and compression software from the ZLIB project (<http://www.zlib.net/>)

Table of Contents

PC-Duo overview	6
What's New in PC-Duo 12.7	7
What's New in PC-Duo 12.6	11
What's New in Earlier Versions of PC-Duo 12	12
What's New in PC-Duo 11.5	12
PC-Duo solutions.....	14
PC-Duo Express Edition	14
PC-Duo Enterprise Edition.....	14
PC-Duo On-Demand Edition	14
PC-Duo applications.....	15
PC-Duo Host.....	16
PC-Duo Host for Remote Desktop Services (RDS).....	17
PC-Duo Host for VDI.....	18
PC-Duo Host on Demand	19
PC-Duo Master	20
PC-Duo Gateway	21
PC-Duo Web Console.....	22
PC-Duo Master on Demand	23
PC-Duo Deployment Tool.....	23
<i>PC-Duo technologies.....</i>	<i>24</i>
<i>PC-Duo services.....</i>	<i>25</i>
<i>PC-Duo connection types.....</i>	<i>26</i>
RDP session sharing: Follow the active session	26
Peer-to-peer connections	26
Gateway-managed connections	28
Firewall-friendly connections	29
Remote Desktop Services connections	29
Root Host for RDS sessions	30
Recording RDS Hosts	30
Limitations of Hosts for RDS	31
VDI connections.....	31
VNC connections	32
Host on Demand connections.....	32
<i>PC-Duo security features</i>	<i>33</i>
Authentication	33

Authorization	36
Auditing	36
Encryption	36
<i>PC-Duo networking features</i>	38
Network protocols	38
Network addressing schemas.....	38
Wake-on-LAN support	38
<i>PC-Duo documentation and technical support</i>	40
Typographical conventions in documentation	40
Technical support options	41
Requirements	43
Operating system requirements.....	43
Hardware requirements	44
Installation requirements.....	44
Network requirements.....	44
Installation notes.....	45
Licensing.....	51
Host Operation	53
Host Tray Icon	54
Host Context Menu	55
Chat Window.....	55
Active Users List	56
Popup Toast Notification	58
Host Control Panel	59
Status tab.....	60
General tab.....	61
Security tab.....	63
Simple password configuration	64
Windows authentication configuration	64
Shared secret password authentication.....	78
End-to-end authentication.....	78
Options tab	80
Action on Disconnect or Termination.....	80
Keyboard and Mouse suppression	81
Confirm Host Options Settings	81
Access tab	83
Access restrictions	84

Connection permission	85
Services Enabled by Default.....	86
Effects tab.....	86
Select ciphers	90
TCP/IP address restrictions	91
Gateways tab.....	93
Manage Gateway order	94
Add Gateway	94
Edit Gateway.....	96
Remove Gateway	96
Move Up.....	97
Move Down	97
Details	97
Resend Status	97
View Error	97
Screen tab	98
Kernel-mode Screen Capture	98
User-mode Screen Capture	99
Bandwidth throttling	99
Tags tab.....	102
Tag Security Considerations.....	103
About tab	104
Add a license key.....	105
Generate a System Information report	105
Host License Key types	106
RDS tab	107
Configure Host Instances	108
Set Users	108
Citrix XenApp support.....	109
Remote Desktop Services Session Host Control Panel	109
Remote Printing.....	113
Restart in Safe Mode.....	114
Host Audit Log	115
Command Line Configuration	117
Configure Host from the command line.....	118
PHSETUP Command line syntax	119
PHSETUP Syntax examples	120

PHSETUP Access parameters	121
PHSETUP Control parameters	123
PHSETUP Effects parameters.....	126
PHSETUP Error Handling parameters	128
PHSETUP Gateways parameters.....	129
PHSETUP General parameters.....	132
PHSETUP License parameter	134
PHSETUP Options parameters	135
PHSETUP Protocol parameters	136
PHSETUP Screen parameters	138
PHSETUP Security parameters.....	139
PHSETUP Tag parameters	140
PHSETUP Terminal Services (Remote Desktop Services) parameters	141
PHSETUP Windows Security parameters	142
Install Host with the MSIEXEC command line.....	145
MSIEXEC options	145
MSIEXEC variables	146
Examples	147
Lock-down settings.....	149
Lock Host settings.....	149
Unlock Host settings	149

PC-Duo overview

Thank you for selecting PC-Duo remote desktop solutions.

PC-Duo remote desktop solutions provide professional features that enable helpdesk technicians, network administrators, IT managers, and software trainers to deliver professional remote support for a fraction of the cost of hosted solutions.

Some selected features include:

- ◆ **Remote Access:** Reach anyone, anywhere, anytime using firewall- and NAT-friendly remote control connections.
- ◆ **Remote Control:** Diagnose and resolve support issues without having to physically visit remote computer.
- ◆ **Remote Management:** Repair remote computers and make configuration changes in real-time and without disturbing currently logged-on user.
- ◆ **Collaboration:** Enable two or more technicians to work on the same remote computer at the same time using chat, screen-sharing and easy-to-pass remote support.

NOTE: Before you use PC-Duo remote desktop solutions, you should be familiar with basic network concepts, such as protocols, encryption, IP addresses, ports, and subnets.

To learn more about PC-Duo remote desktop solutions, see:

- ◆ "What's New"
- ◆ "PC-Duo solutions"
- ◆ "PC-Duo applications"
- ◆ "PC-Duo technologies"
- ◆ "PC-Duo services"
- ◆ "PC-Duo connection types"
- ◆ "PC-Duo security features"
- ◆ "PC-Duo networking features"
- ◆ "PC-Duo documentation and technical support"

What's New in PC-Duo 12.7

Note: Some terminology was changed in PC-Duo v12.7 in order to keep current and to be more accurate. This included changing “Terminal Services” to “Remote Desktop Services (RDS)”. This Host is now referred to as, “Host for RDS”. “PC-Duo Remote Desktop” is now simply “PC-Duo Master” or “PC-Duo Master on Demand” if launched from the Web Console.

PC-Duo 12.7 introduces the following new features and capabilities:

- **Official support for Windows 10:** This release fully supports Microsoft's Windows version 10 and the new Edge browser.
- **All new Remote Printing:** The Remote Printing feature has been completely redesigned and re-written to remove all previous restrictions. Remote Printing no longer requires matching print drivers on Host and Master; can print both from Host to Master and from Master to Host; works on all Windows operating systems (desktop and server) and editions (x86 and x64) supported by PC-Duo v12.7.
- **Master on Demand for Macintosh:** Native Macintosh application that provides Connection Window and Recording Playback functionality on the Macintosh. This application is downloaded and installed from the Web Console, and is launched when a “connect” link is selected in the Web Console.
- **Ability to export data from the Web Console:** You can now export tables directly from the Web Console to a CSV or XLSX file.
- **Asynchronous notifications in Web Console:** The Web Console introduces a way for asynchronous notifications to be delivered to the user. When a notification is available, a new “Notification” icon appears in the top-level toolbar. Clicking on it provides details.
- **Security hardened Web Console:** The Web Console has undergone a major security review and overhaul. Issues addressed include enhanced protection against Cross Site Request Forgery (CSRF), Cross-Site Scripting (XSS) attack, and SQL injection attacks. (*Thanks to Ezenta A/S, ezenta.com, for working with us to improve security.*)
- **Password guessing lockout:** The PC-Duo Networking component now automatically locks out connection requests from any IP address that fails to authenticate after a certain number of attempts in a certain amount of time. This prevents scripted attempts to guess passwords.
- **Deploy and update pre-installed Master Gateway Configurations:** The Deployment Tool now allows you to define one or more Gateway configurations to deploy along with the installation of the Master. Also, there is now the ability to define a new or updated set of Gateway configurations and push them out to

existing installations of Master. Up until now, the installed Master was not ready for Gateway based connections until someone manually added a Gateway configuration.

- **Export / Import of Deployment Tool settings:** You now have the ability to export and re-import important settings for the Deployment Tool via a JSON-formatted text file. This makes copying state from one machine to another much more straightforward.
- **Remote Printing module now available for download from the Web Console:** The Remote Printing Support installation file can now be downloaded directly from the Web Console. This is extremely useful if you want to enable Remote Printing for the Host on Demand or on any machine that the Remote Printing support has not previously been installed.
- **Forms Authentication:** In addition to Windows Authentication, the Web Console now supports Forms authentication. Basic authentication is no longer supported. This makes logout and “Login As” more robust and reliable. It also enables Apple products to work more reliably with the Web Console. From an end-user’s perspective, Forms and Basic authentication methods are functionally equivalent.
- **Master auto-connect for Remote Printing is now optional:** The installed Master now has an option to not auto-connect the Remote Printing service. This appears in the Options > Master Settings dialog, in a new tab “Remote Printing”. This feature is added primarily to ensure that administrators/supervisors can continue to connect to a user/agent in a “stealth” manner, without them being alerted.
- **Selectively install Remote Printing:** The Host and Master installers now make the Remote Printing feature optional. The installer dialog provides the option, with the default to install all components. The MSIEXEC command line also allows for this option.
- **Analytics default period now covers past 24 hours:** Instead of displaying a 24-hour period covering 12:00 AM of the current day to 12:00 AM of the following day, “Analytics” reports will now default to showing the past 24-hours based on your local time zone.
- **Improved and more intuitive searching in Web Console:** The global Find Host search box now behaves more like the extremely well received installed Master “filter” functionality. In addition, search boxes throughout the WC no longer require wildcard characters (“A/*G/*N”) to search for a partial name.
- **Host installation default settings improvement:** In an effort to improve the user experience just out of the box, a clean installation of the PC-Duo Host will now have a default Station Name configured with the macro %NAME% instead of the machine name at time of installation. This

change will allow the Host's Station Name to automatically be updated if the machine name changes. Also, the IPX protocol will now be disabled by default.

- **Web Console's "Host Details" popup includes more information:** For convenience, and completeness, the "Host Details" dialog popup will now include the "Machine Name" and "User" information.
- **Gateway Server now verifies SPNs:** When the Gateway server service starts, it now does a check to verify the registered SPNs for the Gateway service and audit logs any issues or errors. Also, the CheckSPNs utility program now has improved messaging.
- **Re-enabled Firefox ClickOnce support:** Upon request to Vector Networks support team, a Web Console administrator can enable the Host on Demand and ClickOnce connection window to be available in the Firefox browser. Support for this browser had been halted when Microsoft withdrew their ClickOnce "addin". We can now enable use of this browser with certain caveats.
- **Improved Host status reporting logic for multiple Gateway entries:** Host logic to correctly report to a Gateway where multiple configurations refer to the same Gateway has been improved. Specifically the number of connections made by the Host to that Gateway have been reduced.
- **iOS app published to the Apple app store:** The "PROXY Remote" app for iOS has been published to the Apple app store. It includes support for Web Console Forms authentication mode, including credentials autofill. Minor defects have also been fixed around navigation and cancellation of Web Console validation while adding or editing a Web Console entry.
- **Web Console now has the option to display more rows per page:** The Web Console had previously been restricted to showing a maximum of 50 rows per page. This has been expanded to now allow for 100, 150 and 250 rows per page. The setting for this is in the Web Console "Settings" page.
- **Updated SSL/TLS support:** The latest OpenSSL libraries have been incorporated - (v1.0.2g). Customers with internet-facing Gateway Servers listening are encouraged to upgrade to this release.
- **Automatic reconnect to Hosts:** Upon an unexpected dropped connection to a Host, both the installed and Windows ClickOnce Master will automatically attempt to reconnect to the Host.
- **Host on Demand for Macintosh:** Host for Macintosh has many improvements, including improved Permission to Connect user experience and support for recording the Host.

- **Significantly smaller Host on Demand download package:** The download package for the Windows Host on Demand ClickOnce application has been reduced to almost a 3rd of its former size, allowing for much faster downloads.
- **iOS Master for iOS application:** The Master for iOS application is called, PROXY Pro Master and is compatible with iOS 9. Both 32-bit and 64-bit binaries are now built. Included are various bug-fixes and enhancements to improve stability.

Note: Version 9.0.1106 (released October 26, 2015), or later, is required in order to connect to v12.7 of the Web Console and Gateway. Earlier versions of this application will fail trying to make Host or Playback connections.

- **Expanded Host-side “toast” notifications:** The “toast”, or popup, notifications seen on the Host will now contain more information including timestamps. The “pin” behavior has also been improved to be more intuitive.
- **Smarter installation defaults:** Installation defaults have been rethought and are now optimized to provide the best experience out of the box. This includes setting clipboard to auto-share, better Host settings for the Gateway’s recording override feature, locking the workstation on disconnect for Hosts running server class operating systems. Note that upgrades will NOT have any settings changed as this pertains to fresh installs only.
- **Enhanced SSL/TLS support:** The latest OpenSSL libraries have been incorporated and stronger cipher support is enabled by default. This enables support for Perfect Forward Secrecy, but PFS may require additional configuration steps (contact support for details).
- **Enhanced encryption:** non-SSL connections use stronger key agreement parameters.
- **Local cursor option:** This is an option to show a locally drawn cursor. This feature is intended to address performance problems on network connections with very high latency.
- **Host tray icon Tooltip:** Hovering over the PC-Duo Host icon in the Windows system tray now shows the station name of the Host.

What's New in PC-Duo 12.6

PC-Duo 12.6 introduces the following new features and capabilities:

- ◆ **Host on Demand:** New type of Host that can be launched from the Share My Desktop button on the Web Console landing page. Enables the desktop of any internet-accessible machine to be shared instantly. No local or network administrative privileges are required, and no reboot is necessary to run this new Host type. (see *PC-Duo Web Console Operating Guide*)
- ◆ **UAC Elevation (HOD Pin):** Master user can elevate Host on Demand process to high privilege level by providing administrator credentials to HOD remote desktop. This is now known as “Pinning” the HOD and will allow the HOD to survive logouts/reboots until explicitly exited. A Windows HOD instance will now launch as Pinned if the user has the necessary rights. (see *PC-Duo Web Console Operating Guide*)
- ◆ **View/Edit Host Settings from Web Console:** Host settings for any Host connected to the Gateway can be viewed and/or edited by Account Users with appropriate credentials through the Web Console. No connection window to Host desktop required (see *PC-Duo Web Console Operating Guide*)
- ◆ **WebSocket Transport (WS, WSS):** In addition to the UDP, TCP and SSL transports already available, the Gateway Server now supports WebSocket (binary WebSocket over HTTP) and Secure WebSocket (binary WebSocket over HTTPS) transports to facilitate connections through corporate firewalls (see *PC-Duo Gateway Guide*)
- ◆ **More Host Grouping Rules:** Additional grouping rules have been added to allow for more flexibility in creating custom collections of Hosts, especially when considering your AD (see *PC-Duo Gateway Guide*)
- ◆ **Support for LDAPS:** Encryption of connections between the PC-Duo Gateway and the domain controller(s) when doing Active Directory lookups.
- ◆ **Web Console support for Safari, Chrome and Firefox:** Web Console now supports Safari, Chrome and Firefox web browsers, in addition to Internet Explorer; helper apps may be required to enable Remote Desktop and other features (see *PC-Duo Web Console Installation Guide*)
- ◆ **Expanded Search for Recordings:** Web Console now provides a more robust search mechanism for identifying records on a particular Gateway.
- ◆ **Master Support for Selecting a Specific Monitor for View:** Both the installed Master and ClickOnce connection windows now have the ability to view either the entire remote desktop or to “zoom in” on just a single monitor of that remote desktop.
- ◆ **ClickOnce Connection Window can Suppress Host Mouse and Keyboard:** This mirrors the functionality previously available only with the installed Master.
- ◆ **Built-in Utility to Clear the Windows ClickOnce Cache:** The Windows operating system does not provide a convenient way to do this. We have now built this functionality into the Web Console itself.
- ◆ **Most Recent OpenSSL Library:** In order to provide the most secure SSL experience possible, the most recent (as of this release) OpenSSL library has been integrated. Hotfix releases will be made available as needed to provide even newer libraries as they become available.
- ◆ **Automatic Recording:** When this feature is enabled, all specified live Master connections to Hosts for remote control will be recorded. This is configurable in the Web Console.

◆ **Official Method and Support for Web Console Graphics Customization:**

Customization of the Web Console landing page and colors are now easier to put in place and will be maintained when the software is upgraded.

What's New in Earlier Versions of PC-Duo 12

◆ **Web Console:** A new server-side application that enables browser-based access to the Gateway Server for configuration and administration. If On-Demand Edition key is present, Web Console will also be enabled for Remote Desktop feature (see *PC-Duo Web Console Operating Guide*)

◆ **“Click Once” Web Desktop:** Ability to generate a window to a remote desktop directly from the Web Console (Master not required). No administrative rights needed and no reboot required. On-Demand Edition key required for activation (see *PC-Duo Web Console Operating Guide*)

◆ **Kernel-mode Screen Capture driver:** The kernel-mode screen capture driver is now available for Windows 7, Vista and Windows 2008 Server. In many situations, the kernel-mode screen capture driver will outperform the default user-mode screen capture driver (see *PC-Duo Host Guide*)

◆ **Input Suppression:** Ability to turn off keyboard and mouse input on the remote desktop machine for Windows 7, Vista and Windows 2008 Server (see *PC-Duo Master Guide*)

◆ **Address Bindings:** Ability to bind the SSL and TCP network protocols to all addresses or to select specific addresses on the Gateway Server (see *PC-Duo Gateway Administrator Guide*)

◆ **Concurrent User License Mode:** In this mode, the Gateway will monitor the number of simultaneous Gateway users according to account type (Administrative, Master, Personal) (see *PC-Duo Web Console Operating Guide*)

◆ **Inactivity Timeouts:** To free up concurrent user licenses when users are connected to the Gateway but not active, Web Console, Master and Gateway Administrator will be automatically disconnected from the Gateway, and input control will be automatically released from Remote Desktop or Connection Window (see *PC-Duo Gateway Administrator Guide*)

◆ **Automatic Grouping of Hosts:** Ability to configure Hosts to automatically report to custom Gateway group(s) according to custom or generic rules (see *PC-Duo Gateway Administrator Guide*)

◆ **Virtual Desktop support:** Enables virtual desktop images generated in environments such as Citrix XenDesktop to include Hosts, and to have the Hosts report to Gateway until the desktop image is discarded (see *PC-Duo Host Guide*)

What's New in PC-Duo 11.5

◆ **Windows 7 support:** PC-Duo 11.5 provides full support (remote access, remote control, remote management) for Windows 7 computers, including 32- and 64-bit platforms.

◆ **Windows Server 2008 R2 support:** PC-Duo 11.5 provides full support (remote access, remote control, remote management) for Windows Server 2008 R2 computers (64-bit platforms only).

◆ **Mac, Linux support:** PC-Duo 11.5 provides support (remote access, remote control) for Macintosh and Linux computers running VNC server software (standard on Macs).

- ◆ **Wake-on-LAN support:** PC-Duo 11.5 includes ability to turn on remote computers that are configured to listen for Wake-on-LAN signal.
- ◆ **Remote Power Scheme management:** PC-Duo 11.5 includes new remote management tools that allows Master user to view and change power scheme settings on remote computers.
- ◆ **Screen Recording Playback via URL:** PC-Duo 11.5 includes ability for Master to playback a PC-Duo screen recording from a standard web server over HTTP or HTTPS.
- ◆ **RDP compatibility:** If a remote computer is hosting an active RDP session, PC-Duo 11.5 Host will capture and provide input control to the RDP session.
- ◆ **Active Directory integration:** PC-Duo 11.5 Deployment Tool can now be used to discover computers and OUs in Active Directory domains, install new PC-Duo software, upgrade existing software, and/or push configuration changes to existing software.

PC-Duo solutions

Vector Networks provides three solutions for remote desktop support:

PC-Duo Express Edition

PC-Duo Express Edition is an easy-to-use remote desktop solution that uses simple peer-to-peer connections between helpdesk technicians and end-user remote computers. It is ideally suited for smaller companies and workgroups in which the number of remote computers being supported is small and manageable.

PC-Duo Enterprise Edition

PC-Duo Enterprise Edition is an enterprise-class remote desktop solution that uses a robust, scalable server to establish and maintain a secure network of connections to end-user machines. It leverages centralized administration, security and network access to simplify and automate the creation, management, and monitoring of this “network within a network”. PC-Duo Enterprise Edition is ideally suited for enterprises and corporate workgroups with large numbers of remote computers, multiple domains and/or employees with remote computers outside the network.

PC-Duo On-Demand Edition

PC-Duo On-Demand Edition is a web-enabled version of the Enterprise Edition, and includes Master on Demand for on-demand access to remote desktops in place of the installed Master application.

PC-Duo applications

The PC-Duo remote desktop solutions include some or all of the following applications:

PC-Duo Components	PC-Duo Express Edition	PC-Duo Enterprise Edition	PC-Duo On-Demand Edition
PC-Duo Host	Yes	Yes	Yes
PC-Duo Host for RDS	No	Yes	Yes
PC-Duo Host for VDI	No	Yes	Yes
PC-Duo Host on Demand	No	Yes	Yes
PC-Duo Master	Yes	Yes	No
PC-Duo Gateway	No	Yes	Yes
PC-Duo Web Console	No	Yes	Yes
PC-Duo Master on Demand	No	No	Yes
PC-Duo Deployment Tool	Yes	Yes	Yes

PC-Duo Host



PC-Duo Host runs as a Windows service on the machine on which it is installed, and supports both peer-to-peer connections as well as Gateway-managed connections. By installing PC-Duo Host on a computer in your network, you can:

- ◆ Allow technicians to make peer-to-peer remote control connections to the machine, whether someone is there or not. Each Host manages its own security settings and access rights.
- ◆ Allow or force technicians to make Gateway-managed remote support connections to the machine through a central server (PC-Duo Gateway), which will automatically enforce security settings and access rights according to policies set at the server.

The PC-Duo Host requires a Host license key.

For more information about configuring and operating PC-Duo Host, please see the *PC-Duo Host Guide*.

PC-Duo Host for Remote Desktop Services (RDS)



PC-Duo Host for Remote Desktop Services, formerly called “Terminal Services”, is a server-side version of the PC-Duo Host designed to support Remote Desktop sessions.

The PC-Duo Host runs on the Windows Server with the Remote Desktop role, which may also include software support from Citrix. It is configured to support one or more concurrent Remote Desktop sessions. Each time a new Remote Desktop session is started, the Host injects a copy of itself into the session. This session Host will include instructions for reporting to one or more Gateways. When the Remote Desktop session is discarded, the session Host instance will also be discarded and will be automatically removed from the Gateway(s).

The PC-Duo Host for RDS requires a special Host license key that will specify the maximum number of concurrent RD sessions that can be supported on that Server.

For more information about configuring and operating PC-Duo Host, please see the *PC-Duo Host Guide*.

PC-Duo Host for VDI



PC-Duo Virtual Desktop Image Host is a special version of the PC-Duo Host designed to support the transient nature of virtual desktops.

The PC-Duo Host for VDI can be included as part of a virtual desktop template; when one or more virtual desktop sessions are generated using this template (often to create a pool of virtual desktop images), the sessions will include a Host with all the features of the installed Host but not the permanent nature. When the virtual desktop session is discarded, the Host will also be discarded and will be removed automatically from the Gateway(s).

The PC-Duo Host for VDI requires a special Host license key that will specify the maximum number of concurrent VDI sessions that can be supported in the virtual desktop environment.

For more information about configuring and operating PC-Duo Host, please see the *PC-Duo Host Guide*.

PC-Duo Host on Demand

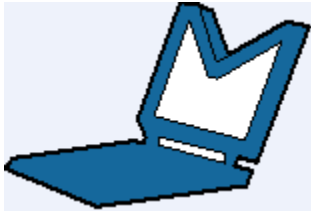


PC-Duo Host on Demand (HOD) is a streamlined version of the Host that can be launched from the Share My Desktop button on the Web Console landing page. It enables the desktop of any internet-accessible machine to be shared instantly. No local or network administrative privileges are required, and no reboot is necessary to run this special Host type.

The PC-Duo Host on Demand is hosted by the Gateway Server and is enabled by a special license key installed in the Gateway Server. When enabled, the Share My Desktop button on the Web Console landing page will light up, and end users will be able to install as many instances of HOD as they like. Each instance will report back to and be accessible through the Gateway Server from which it was served.

For more information about configuring and operating PC-Duo Host on Demand, please see the *PC-Duo Web Console Operating Guide*.

PC-Duo Master



PC-Duo Master is a console application that technicians can use to establish remote support connections to one or more Host computers. With PC-Duo Master, you can:

- ◆ Make one or more peer-to-peer remote support connections to Host computers in your network.
- ◆ Connect to PC-Duo Gateway and make one or more Gateway-managed remote support connections to Host computers from a directory of available Hosts.
- ◆ View the entire screen of the remote computer or just a single monitor.
- ◆ Take complete control of a Host computer using the local keyboard and mouse.
- ◆ Share control of the Host computer with its end-user.
- ◆ Passively monitor the Host computer without exercising control.
- ◆ Use the clipboard transfer feature to transfer portions of text, bitmaps, and other objects between your Host and Master computers.
- ◆ Use the PC-Duo file transfer feature to copy files between your Host and Master computers.
- ◆ Use the PC-Duo remote printing feature to print locally from applications running on a remote computer or vice-versa.
- ◆ Record screen activity on the Host and play back the recording on the Master.
- ◆ Chat with end-user and any other technicians connected to the same Host.

For more information about configuring and operating PC-Duo Master, please see the *PC-Duo Master Guide*.

PC-Duo Gateway



PC-Duo Gateway is an enterprise class server, which provides centralized administration, security and management for a network of remote support connections to Host computers in your environment.

With PC-Duo Gateway configured as the hub of your remote support network, you can:

- ◆ Organize large numbers of Host computers into logical groups for easier access and management.
- ◆ Reach remote computers outside the network, behind firewalls or NAT-devices.
- ◆ Utilize SSL for certificate-based authentication.
- ◆ Create custom access rights policies and apply them to groups to make configuration changes more quickly and efficiently.
- ◆ Monitor and manage remote support activity in real-time.
- ◆ Keep detailed records of all remote support activity in your network with comprehensive audit logs.
- ◆ Record screen activity on one or more remote computers simultaneously using PC-Duo Gateway's screen recording feature.

PC-Duo Gateway includes the PC-Duo Gateway Administrator, a tool for configuring the Gateway and for monitoring, managing and auditing remote support activity in your network.

For more information about configuring and operating PC-Duo Gateway, please see the *PC-Duo Gateway Server Guide*.

PC-Duo Web Console

PC-Duo Web Console is a web application that provides browser-based access to the PC-Duo Gateway Server for administration and configuration. It is effectively a web-based version of the Gateway Administrator.

The Web Console also includes an optional feature called the Master on Demand, which allows on-demand access to remote desktops directly from the Web Console. It is effectively a web-based version of the Master application.

With PC-Duo Web Console:

- ◆ Administrators can access and edit all the configuration information on the Gateway Server, including Groups, Security, Permissions, etc. The Administrative web account can be used in conjunction with or instead of the standalone Gateway Administrator application.
- ◆ If the Master on Demand is enabled, Helpdesk technicians can view and access remote desktops connected to the Gateway.

For more information about configuring and operating PC-Duo Web Console, please see the *PC-Duo Web Console Operating Guide*.

For more information about installing PC-Duo Web Console, please see the *PC-Duo Web Console Installation Guide*.

PC-Duo Master on Demand

The Master on Demand is a feature of the Web Console, which allows on-demand access to remote desktops directly from the Web Console. It is effectively a web-based version of the Master application.

With PC-Duo Master on Demand:

- ◆ Helpdesk technicians can view and access remote desktops connected to the Gateway.
- ◆ Employees can view and access their computers at work, even if they are on the road or at home. The Personal web account offers convenient, secure, reliable alternative to VPN.

To enable the Master on Demand, a special key must be entered into the Gateway Server.

For more information about configuring and operating PC-Duo Master on Demand, please see the *PC-Duo Web Console Operating Guide*.

PC-Duo Deployment Tool

PC-Duo Deployment Tool is an easy-to-use software distribution utility that automates the deployment and installation of PC-Duo applications to remote computers in your network.

With PC-Duo Deployment Tool, you can:

- ◆ Automatically deploy an image of PC-Duo Host, Master or Gateway to one or more computers or groups of computers in your network and avoid manual effort of going to each machine.
- ◆ Create an image of PC-Duo Host, Master or Gateway with custom configuration options that can be mass deployed on large numbers of computers in your environment.
- ◆ Create and push custom configuration options for PC-Duo Host, Master or Gateway, without having to reinstall underlying software.
- ◆ Use Active Directory to find remote computers and push software and configuration settings to them.

For more information about configuring and operating PC-Duo Deployment Tool, please see the *PC-Duo Deployment Tool Guide*.

PC-Duo technologies

PC-Duo remote desktop solutions utilize highly optimized technologies to deliver speed, performance and reliability, including:

◆ **Highly efficient screen capture algorithms.** PC-Duo utilizes two kinds of screen capture technology:

- ◆ Kernel-mode screen capture. This technology utilizes the PC-Duo mirror driver, which reproduces graphics drawing commands from the remote Host on the PC-Duo Master user's screen quickly and efficiently.
- ◆ User-mode screen capture. This technology works without a mirror driver and is designed to adjust automatically to the amount of CPU and bandwidth available on the remote Host machine.

◆ **Streamlined communication protocol.** The PC-Duo protocol has been honed over 15 years for efficiency and reliability when sending screen capture data to another computer in real-time and receiving keyboard/mouse input.

Using these technologies, PC-Duo remote support solutions enable technicians to find and fix problems on remote computers faster and easier than ever before.

PC-Duo services

PC-Duo remote desktop solutions offer technicians a number of professional-quality services for investigating and solving problems on Host remote computers, including:

- ◆ **Remote Control:** ability to view screen activity on an end-user's remote machine, and with proper authorization, take control of and send keyboard/mouse inputs to the remote machine in real-time
- ◆ **Remote Clipboard:** ability to copy selected items on the screen of a remote machine into the clipboard on the remote machine and transfer the contents to the clipboard on the technician's machine, and vice versa
- ◆ **File Transfer:** ability to drag-and-drop files or directories on the remote machine to the technician's machine, and vice versa
- ◆ **Host-based Chat:** ability to chat with the end-user on a remote machine, and any other technicians connected to that machine
- ◆ **Remote Printing:** ability to print selected items from the remote machine to a printer attached to the technician's machine, and vice versa
- ◆ **Host Administration:** ability to view and edit configuration settings of the PC-Duo Host installed on the remote machine
- ◆ **Remote Management:** ability to generate inventory of hardware and software assets on remote machine, and to query and change certain system settings. See "Remote Management features" for more information about tools available through this service.

PC-Duo connection types

PC-Duo services are performed over service connections between a PC-Duo Master (with appropriate access rights) and a PC-Duo Host. Service connections are established on demand, when a PC-Duo Master requests a service from a PC-Duo Host.

PC-Duo supports several different types of remote access connections:

PC-Duo Connection Types	PC-Duo Express Edition	PC-Duo Enterprise Edition	PC-Duo On-Demand Edition
RDP session sharing	Yes	Yes	Yes
Peer-to-peer connections	Yes	Yes	Yes
Gateway-managed connections	No	Yes	Yes
Firewall-friendly connections	No	Yes	Yes
RDS connections	No	Yes	Yes
VDI connections	No	Yes	Yes
VNC connections	Yes	Yes	No
Host on Demand connections	No	Yes	Yes

RDP session sharing: Follow the active session

PC-Duo connections can be used to share an active RDP session in real-time.

If PC-Duo Host is running on a desktop-class operating system (e.g. Windows 7), and there is an active/connected RDP session being hosted on that computer, then the Host will automatically capture and provide input control to that RDP session. In essence, the Host will capture what the remote RDP session user is seeing, not what the local physical console on that machine is showing (probably the Windows login screen).

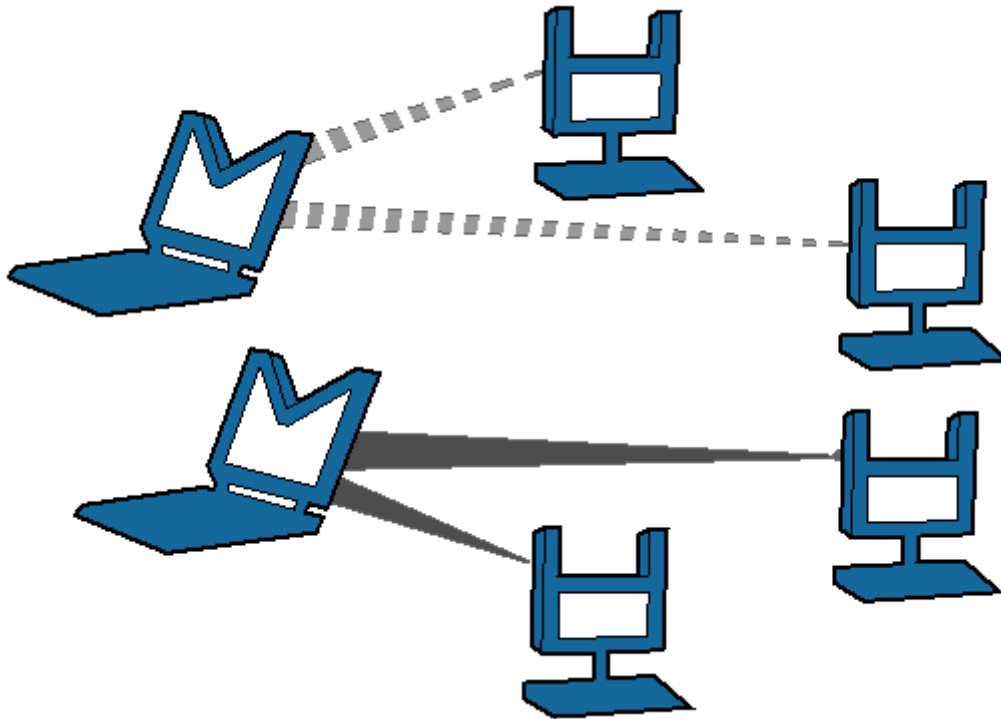
When there is no active/connected RDP session being hosted on that computer, or if an active/connected RDP session is stopped, the Host will automatically capture and provide input control to the session running on the computer and being displayed on the local console. The Host will follow the active session as it moves from RDP user back to the local console.

Note: feature only applies to desktop-class operating systems, which support only one active session at a time. Server-class operating systems (e.g. Windows Server 2008, 2012 or 2016) can support multiple sessions simultaneously via Remote Desktop Services; use the Host for RDS to capture and/or provide input control to one or more sessions on server-class OS.

Peer-to-peer connections

When a computer with PC-Duo Master establishes a direct connection to a computer with PC-Duo Host, the connection that is established is a **peer-to-peer connection**.

By default, PC-Duo Master searches the network for Host computers when it starts up. Any Host computers it finds are listed on the **Peer-to-Peer Hosts** tab of the PC-Duo Master window.



Peer-to-peer connections from Master (M) to Host (H)

The dotted and solid lines, shown in above depict two different sets of peer-to-peer connections between PC-Duo Masters to PC-Duo Hosts. PC-Duo's peer-to-peer connections enable the following:

- ◆ PC-Duo Master users with proper credentials can securely access Host computers within the network.
- ◆ When you permit full access to a Host computer, the PC-Duo Master user can monitor all activity on the Host computer. In addition, PC-Duo Master users with full access rights can exercise complete control over that computer.
- ◆ When the Host and Masters are in the same domain, PC-Duo Host can be configured to use the Microsoft Windows authentication service to check credentials of any PC-Duo Master users. An access control policy can allow (or deny) full or partial access for authenticated PC-Duo Master users to access services on a Host computer.

Although PC-Duo's peer-to-peer connections provide a secure solution for remote support, this solution is not recommended for large and/or highly distributed networks; instead, consider using PC-Duo Gateway for centrally managed remote support connections.

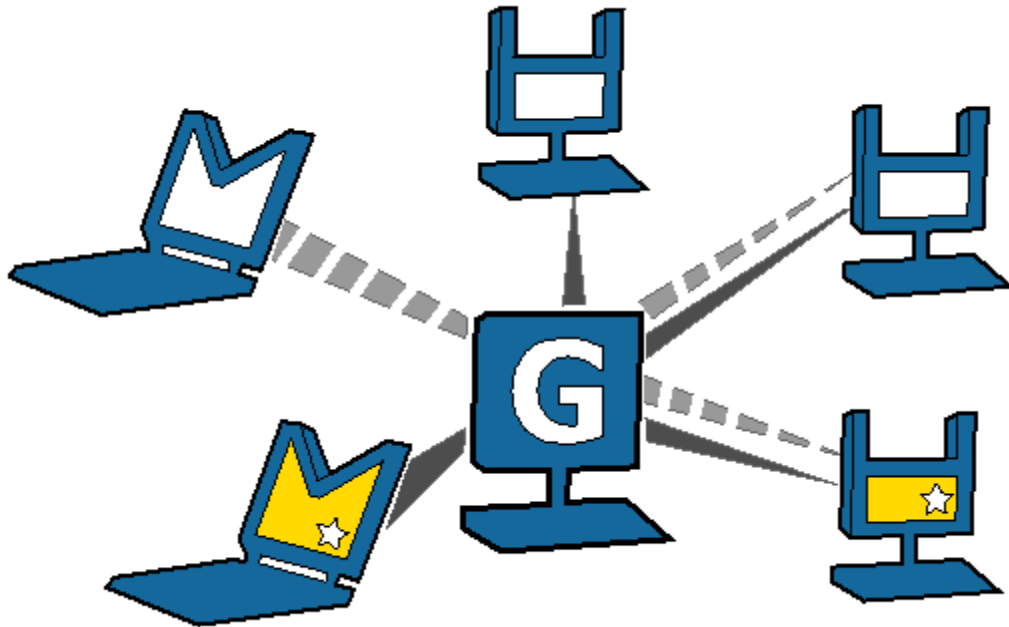
Gateway-managed connections

When a computer with PC-Duo Master establishes a connection to a computer with PC-Duo Host through a central server (i.e. PC-Duo Gateway), the connection that is established is a **Gateway-managed connection**. In this way, the Gateway serves as a central location for managing and monitoring connections, configuration, security and reporting. Any Host computers found by the Gateway are listed on the **Gateway Hosts** tab of the PC-Duo Master window.

In large networks, the PC-Duo Gateway can be configured to manage connections with hundreds or thousands of Hosts simultaneously, enabling Masters to find and take control of Hosts instantly.

Gateway-managed connections utilize the same strong authentication and authorization that is available with PC-Duo's peer-to-peer connections. In addition, PC-Duo Gateway provides the following capabilities:

- ◆ Seamless connections from Master computers to Host computers through a PC-Duo Gateway. To the PC-Duo Master user, the connection appears as if it were a peer-to-peer connection to the Host computer, even if the Host is outside the domain and/or behind a firewall or NAT device.
- ◆ Centralized management of access rights to remote computers in your network. Once you configure your Host computers to report to the PC-Duo Gateway, you can achieve global management through a single security policy that you configure using PC-Duo Gateway Administrator.
- ◆ User-based access policies. Customize and apply access policies to individual PC-Duo Master users or groups in your network. Allow full remote access to one or more Host computers for some PC-Duo Master users, while restricting access rights for others.
- ◆ Comprehensive logging and auditing of all remote control activity within your network. With this feature, you can keep records of all remote support connections.
- ◆ Continuous screen recording. PC-Duo Gateway allows you to record screen activity on any remote Host. Efficient file compression makes 24x7 recording economical and manageable.



Gateway (G)-managed connections from Master (M) to Host (H)

Firewall-friendly connections

When PC-Duo Master users need access to Hosts that are outside the domain, and/or behind a firewall or NAT-device, normal peer-to-peer or Gateway-managed connections will not work. In these cases, it is difficult to find and maintain a secure remote support connection because of dynamic port assignments and other network challenges.

For these situations, PC-Duo Gateway builds special firewall-friendly connections to these Hosts. When Hosts are outside the domain, the Hosts are programmed to automatically initiate contact with the Gateway. The Gateway will use this initial contact to build a firewall-friendly connection to the Host. In this way, the remote Host outside the domain will appear just like any Host inside the domain.

Remote Desktop Services connections

PC-Duo provides server-side support (screen capture, input control, screen recording) for session-based virtual desktops hosted by Remote Desktop Services, formerly called "Terminal Services", on Windows Server 2008, Windows Server 2012 and Windows Server 2016. Windows Server creates and hosts the Remote Desktop Services (RDS) sessions like virtual machines. A presentation technology using a display protocol such as RDP from Microsoft or ICA from Citrix is typically used to remote the session display, as well as the keyboard and mouse input, to and from an end user device (such as a thin client computer like a Wyse terminal).

PC-Duo allows technicians to capture (and if desired, record) the session presentation information at the Windows Server before it is remoted to the end user device over the RDP or ICA display protocol. PC-Duo is able to do this by injecting a Host instance into each server-side RDS session, which in turn captures and sends presentation information directly to PC-Duo Gateway for recording and/or further transmission to a PC-Duo Master.

Note: Because RDS sessions are captured at the Windows Server (and not at the end user device), PC-Duo Host effectively bypasses the technology used to remote the sessions to the end users, and will therefore be compatible with Microsoft Remote Desktop Services clients as well as Citrix Presentation Server (now known as XenApp) clients.

Note: PC-Duo only supports RDS sessions created on server-class Windows operating systems such as Windows Server 2008, Windows Server 2012 and Windows Server 2016.

See the **RDS tab** in PC-Duo Host Guide for more specific configuration and setup information.

Root Host for RDS sessions

The “Remote Desktop Services” feature of Windows Server editions allows multiple virtual desktop sessions to be active simultaneously. PC-Duo provides remote access and remote control to these sessions on the Windows Server by injecting a separate instance of the Host service into every new RDS session. A special version of the Host called the “root” Host must be loaded on the RDS server (a “root” Host is a standard Host with a special PC-Duo Host for RDS license key - see **About tab** in the *PC-Duo Host Guide* for more information); it will automatically spawn new Host instances every time a new RDS session is created.

Transient Hosts

Each RDS session’s instance of the Host will have its own unique workstationID and must be configured to report to a Gateway. When it first reports to the Gateway Server, it will be automatically managed and added to the “All Hosts” group. The Hosts for RDS are considered transient, since they go away when the RDS user logs out of his/her session. In order to keep track of transient RDS Hosts, the PC-Duo Gateway will create a new Group called “Host for RDS on <Servername>”, and automatically insert transient Hosts into this Group. They are automatically deleted from the Gateway when the RDS session ends. The main purpose of this Group is to allow security to be assigned to the Hosts and RDS sessions that belong to this Group, and to provide the correct and appropriate access to the RDS-based Host instances.

Note: PC-Duo Host for RDS works on Windows Server editions, and requires a Gateway Server v6.10 or later.

Recording RDS Hosts

Recordings are normally deleted from the Gateway database when their associated workstation record is deleted. Transient Host for RDS workstation records are automatically deleted from the Gateway when the RDS user logs out of his/her session. However, to prevent recordings of Host for RDS from being automatically deleted when the RDS session ends, the RDS session recordings are reassigned to an artificial permanent workstation record called “Recordings of Host for RDS”. All recordings of all RDS Hosts on a given RDS server will be associated with this one record. This approach has the following advantages:

- ◆ Recordings are not orphaned
- ◆ All recordings can be kept in one place,
- ◆ RDS recordings can be kept separate from console (root Host) recordings

- ◆ Security can be configured separately for each recording.

Limitations of Hosts for RDS

Due to technical limitations and the nature of Remote Desktop Services sessions, the following Host features are not supported.

- ◆ Keyboard and mouse suppression (requires kernel-based input stack intercept)
- ◆ Screen blanking (requires kernel-based support and physical display to blank)
- ◆ Peer-to-peer connections: all protocols are disabled, and the only connections that can be made are through a configured Gateway Server
- ◆ Kernel-mode screen capture (requires kernel-mode display support)

VDI connections

PC-Duo provides a special version of the Host to run inside of virtual desktop images (VDI) created from virtual desktop templates in environments such as Citrix XenDesktop. If the regular Host is specified in the template, then the Host will automatically be installed when the virtual desktops are created using this template.

This works fine with Peer-to-Peer connections to the Host in the VDI, but has some complications when the Host is configured to report to one or more Gateway Servers:

- ◆ The GWS must be configured to “automatically manage new Hosts” to have the Host become available without any manual intervention.
- ◆ If the virtual desktop is discarded when the user logs out, the Host is effectively destroyed as well, but the Gateway doesn’t know this. The Host remains known to the Gateway (and managed, using a Managed Hosts license) until it is manually cleaned up by an administrator, or until the **Delete Hosts older than** feature kicks in and deletes it. (But note that setting is measured in days, default is set to 120, and setting that to a low value runs the risk of deleting conventional installed Hosts that are simply offline for a while.)

To address both of these problems, the Gateway Server supports a special version of the Host for VDI that is “transient” in nature (similar to a Host for RDS session); when the VDI Host is specified in the template, the following will occur:

- ◆ A new group, “Host for VDI”, is automatically created at the Gateway when a Host of this type first reports. All Hosts of this type are automatically managed (independent of the “automatically manage Hosts” setting), and are added to this group.
- ◆ If the virtual desktop is discarded when the user logs out, the VDI Host, because of its transient nature, will automatically be disconnected and removed from the Gateway, freeing up a Managed Host license.
- ◆ Similar to what happens when recording Host for RDS sessions, a new pseudo-host, “Recordings of Host for VDI”, is created when any of these Hosts is recorded. The recording of the VDI Host is associated with this pseudo-Host instead of with the Host workstation, and will remain in there even after the virtual desktop is discarded
- ◆ If the Gateway is in Managed Hosts licensing mode, a new license key that limits the maximum number of VDI Hosts that can be connected to the Gateway concurrently is required

VNC connections

PC-Duo provides remote access and remote control to computers running a standard version of VNC (Virtual Network Computing) server. A VNC server is built into recent versions of the Mac OS X operating system from Apple Computer, and is also available on many versions of the Linux operating system. When properly configured, technicians can use PC-Duo Master on Windows to connect to and take control of Mac and Linux computers running standard VNC server.

PC-Duo currently supports peer-to-peer connections to VNC servers.

See "VNC Hosts" in the *PC-Duo Master Guide* for more information on configuring and connecting to VNC servers.

Supported Platforms

PC-Duo Master can interoperate with standard VNC servers on following platforms:

- ◆ Mac OS X
- ◆ Red Hat Linux Fedora

Host on Demand connections

PC-Duo provides remote access and remote control to computers running a streamlined version of the Host called "Host on Demand" (HOD). The Host on Demand can be accessed from the Web Console landing page by any internet-accessible machine and will enable end user to share his/her desktop instantly through the Gateway Server.

Supported Web Browsers

PC-Duo Host on Demand is supported on following web browsers:

- ◆ Internet Explorer
- ◆ Edge
- ◆ Firefox
- ◆ Chrome
- ◆ Safari

Note that helper apps may be required to run certain features of the Web Console for browsers other than Internet Explorer or Edge.

See the *PC-Duo Web Console Operating Guide* for more information on enabling and configuring Host on Demand.

PC-Duo security features

One of the most valuable aspects of PC-Duo remote desktop solutions is the ability to create and enforce fine-grained access control policies, and to easily modify them to reflect changes in your organization.

PC-Duo security features include the following:

- ◆ “Authentication”
- ◆ “Authorization”
- ◆ “Auditing”
- ◆ “Encryption”

Authentication

In the PC-Duo model, PC-Duo applications that request information and services are considered “clients” and those that provide information and services are considered “servers”. For example, the PC-Duo Master is considered a client when it connects to and requests a list of Hosts from a PC-Duo Gateway. In turn, the PC-Duo Gateway is considered a client when it connects to and requests information from a PC-Duo Host in the same domain.

Connection	Client	Server
Peer-to-peer	Master	Host
Gateway-managed (Gateway & Host are in same domain)		
◆ Master-Gateway relationship	Master	Gateway
◆ Gateway-Host relationship	Gateway	Host
Gateway-managed (Gateway & Host are not in same domain)		
◆ Master-Gateway relationship	Master	Gateway
◆ Gateway-Host relationship	Host	Gateway

When PC-Duo Host is not in the same domain as the Gateway, the relationship is automatically reversed: The Host is programmed to be the client and will reach out to the Gateway (see [“Firewall-friendly connections”](#) for more information about PC-Duo firewall-friendly connections).

To guarantee security in the PC-Duo environment, it is critical that PC-Duo components acting as servers validate the credentials of users of PC-Duo components acting as clients before they provide access or data. The burden is placed on the client to authenticate itself to the server. PC-Duo implements two types of authentication to support this:

- ◆ “Identity Authentication”
- ◆ “Endpoint Authentication”

Identity Authentication

In general, this operation answers the following security question: How does the server know who the client is? A PC-Duo application acting as a server will not provide access or information to any PC-Duo application acting as a client until it can validate that client's identity. PC-Duo provides the server three different methods of authenticating the identity of the PC-Duo client:

Connection	Windows authentication	Simple password	Shared-secret password
Peer-to-peer	Yes	Yes	No
Gateway-managed (Gateway & Host are in same domain)			
◆ Master-Gateway relationship	Yes	No	No
◆ Gateway-Host relationship	Yes	No	Yes
Gateway-managed (Gateway & Host are not in same domain)			
◆ Master-Gateway relationship	Yes	No	No
◆ Gateway-Host relationship	No	No	Yes

◆ **Windows authentication:** By default, a PC-Duo application acting as a server uses Windows authentication to check the Windows credentials of the client application:

- ◆ The Host will check the Windows credentials of the PC-Duo Master user in the case of a peer-to-peer connection;
- ◆ The Gateway will check the Windows credentials of the PC-Duo Master users in the Master-Gateway part of a Gateway-managed connection;
- ◆ The Host will check the Windows credentials of the user logged into the Gateway in the Gateway-Host part of a Gateway-managed connection (when Host and Gateway are in the same domain).

NOTE: *If Host and Gateway are not in the same domain, Windows authentication will not usually be available. In that case, Host and Gateway will rely on Shared secret password.*

◆ **Simple password:** Prior to making a connection, a custom password can be created on the **Security** tab of the Host and shared with PC-Duo Master user. This feature permits the PC-Duo Master user to connect to a Host without regard to PC-Duo Master user's Windows credentials.

NOTE: *Simple password applies only to peer-to-peer connections.*

◆ **Shared secret password:** In the case that the Host does not share a domain relationship with the PC-Duo Gateway, or if the Host is outside of the network and cannot contact its domain controller, Windows authentication will not usually be available. Behind the scenes, the PC-Duo Gateway and the Host will exchange a 16-byte secret password that only they will know. As a result, in all subsequent connections, the PC-Duo Gateway and Host will have some measure of authentication when they are not in the same domain. If the Host belongs to the same domain as the PC-Duo Gateway, and the Host is able to reach a domain controller, the Host will prefer to do Windows authentication instead of shared secret password.

Endpoint Authentication

In general, this operation answers the following security question: How does the client know it is connected to the right server? Identity authentication doesn't prohibit the client from being fooled into connecting to a different server. In order to guarantee that information and services are coming from the expected server, PC-Duo supports endpoint authentication using Secure Sockets Layer (SSL).

◆ **SSL certificate authentication (PC-Duo Gateway only):** PC-Duo has implemented server endpoint authentication using SSL, which means the client will request and validate a certificate from the server before providing requested information or services. This ensures the client has connected to the right server. The following list describes where SSL authentication can and cannot be used:

- ◆ **Peer-to-peer connections:** SSL authentication is not available for peer-to-peer connections. This would require each Host (acting as server) to carry its own certificate, which would be unwieldy and costly to manage.
- ◆ **Gateway-managed connections (Host is in same domain as Gateway):** SSL authentication is available between Master (acting as client) and Gateway (acting as server). Before connecting, the Master will request and validate a certificate from the Gateway. In general, SSL between Master and Gateway would be most useful when the Master is outside the LAN and/or coming in through a corporate firewall to access the Gateway.

***NOTE:** SSL authentication is not available between the Gateway (acting as client) and the Host (acting as server). As in peer-to-peer connections, this would require each Host to carry its own certificate. SSL connections to the Host are generally not required because the Host can be configured to use a reverse connection to the Gateway, which can use SSL.*

- ◆ **Gateway-managed connections (Host is not in same domain as Gateway):** When the Host is outside the LAN and/or behind a firewall or NAT-device, the Host is the client and has responsibility to contact the Gateway. SSL authentication is supported and would be appropriate to ensure that the Host is connecting to the right Gateway. The Host will validate the Gateway Server certificate before accepting the connection, ensuring that the Host is communicating with the correct Gateway Server.

In summary, SSL can be used by the Master to authenticate a Gateway, and by a Host to authenticate a Gateway when the Host is outside the domain:

Connection	Client	Server	SSL Supported
Peer-to-peer	Master	Host	No

Gateway-managed (Master & Host are in same domain)

◆ Master-Gateway relationship	Master	Gateway	Yes
◆ Gateway-Host relationship	Gateway	Host	No

Gateway-managed (Master & Host are not in same domain)

◆ Master-Gateway relationship	Master	Gateway	Yes
◆ Gateway-Host relationship	Host	Gateway	Yes

Authorization

One of the strongest features of PC-Duo remote support solutions is the fine-grained access control. For example, to perform remote support, you must have the following:

- ◆ Proper credentials with which to connect to the Host computer
- ◆ Authorization to view the Host computer remotely
- ◆ Authorization to control the Host computer remotely

Your credentials are established when you connect to a Host computer (or to a PC-Duo Gateway), and persist until the connection breaks. You can configure access and other rights directly on the Host computer for peer-to-peer connections. Alternatively, you can use the PC-Duo Gateway to enforce custom access rights policies on PC-Duo Master users, roles, or groups for Gateway-managed connections.

Auditing

PC-Duo Gateway provides a detailed log of connection attempts, actions and other activities that occur in the network. This log is also customizable and exportable to 3rd party reporting products using standard formats.

PC-Duo Gateway also features screen recording for any Host in contact with a Gateway, whether or not there is an active remote support connection. With this feature, PC-Duo Master users can keep a visual log of activities going on in the network.

Encryption

To ensure privacy of communications between PC-Duo applications across the network, PC-Duo provides advanced encryption using Advanced Encryption Standard (AES) block ciphers. This protection will be automatic and transparent every time two PC-Duo 11.0 components or later are communicating with each other.

By default, PC-Duo uses AES 256-bit encryption, however other encryption options can be set, including:

- ◆ AES encryption (256-bit key)
- ◆ AES encryption (192-bit key)

- ◆ AES encryption (128-bit key)
- ◆ Triple-DES (3DES) encryption (192-bit key)

NOTE: PC-Duo 11.0 and later also support RC4 encryption for the sole purpose of being able to connect to older Hosts (v10.0 and earlier), which only allows RC4.

Order of precedence

When two PC-Duo components have different encryption options set, the first encryption choice in common between the two is used (going down the list in order), with preference set as follows:

- ◆ Preference set by the Host, when the Gateway requests connection to the Host
- ◆ Preference set by the Gateway, when the Master requests connection to a Host through the Gateway

PC-Duo networking features

PC-Duo remote desktop solutions support several standard transport protocols for computer-to-computer communication, and two types of network addressing schemas.

Network protocols

PC-Duo products support most of the standard networking and transport protocols, including:

- ◆ **IP:** IP is a general-purpose protocol supported on a wide variety of networks and servers. PC-Duo components support communications using either the TCP or UDP transport protocols running over IP. PC-Duo has established the following standard ports for use with either TCP or UDP:
 - ◆ PC-Duo Host listens on port 1505 by default
 - ◆ PC-Duo Gateway listens on port 2303 by default
- ◆ **SSL:** The SSL protocol runs above TCP/IP and below higher-level protocols such as HTTP or IMAP. Using TCP/IP on behalf of the higher-level protocols allows an SSL-enabled server to authenticate itself to an SSL-enabled client, and then establish an encrypted connection between the remote computers.
 - ◆ By default, PC-Duo Gateway listens for incoming SSL connections on port 443, but it might be appropriate to note that this can be easily changed to avoid conflicts with other server software installed on the same machine.
 - ◆ The PC-Duo Gateway now ships with a Gateway Certificate Manager to manage the creation and/or selection of a SSL security certificate for the PC-Duo Gateway.
- ◆ **WebSocket:** The WebSocket protocol runs above HTTP or HTTPS. This provides a web-proxy friendly and firewall-friendly transport. Only the Gateway Server accepts WebSocket connections; the Host can report to the Gateway this way, and the Master and other client software can connect to the Gateway this way.
 - ◆ The PC-Duo Gateway listens for incoming Secure WebSocket connections (WSS) when SSL is enabled, and uses the same port. It listens for WebSocket connections (WS) when TCP is enabled, and uses the same port.

Network addressing schemas

The PC-Duo UDP, TCP and SSL transport protocols support the use of either IPv4 (32-bit) or IPv6 (128-bit) addresses.

Wake-on-LAN support

PC-Duo can be used to "wake-up" remote computers that have been shut down (sleeping, hibernating, or soft off; i.e., ACPI state G1 or G2), with power reserved for the network card, but not disconnected from its power source. The network card listens for a specific packet containing its MAC address, called the *magic packet*, that is broadcast on the subnet or LAN.

In order to execute this feature, both the MAC address and the last known IP address of the remote computer must be known. Since the PC-Duo Gateway knows both of these pieces of information, it is in a position to send the Wake-on-LAN signal.

PC-Duo implements this functionality in Gateway-managed connections in two ways:

- ◆ **Implicit Wake-on-LAN:** If Gateway is asked to make a connection to a remote computer and the last status indicates that the remote computer is "Offline", the Gateway will automatically attempt to wake up the remote computer by sending appropriately configured WOL signal. If the remote computer was shut down in a state capable of receiving WOL signal, it will wake up and report to the Gateway and a connection will be established.
- ◆ **Explicit Wake-on-LAN:** A network administrator, using either PC-Duo Master or PC-Duo Gateway Administrator, can attempt to wake up a remote computer by explicitly sending the WOL signal to that machine. If the remote computer was shut down in a state capable of receiving WOL signal, it will wake up and report to the Gateway and a connection will be established.

See "Send Wake-on-LAN Signal" in the *PC-Duo Master Guide* for more information.

PC-Duo documentation and technical support

Each of the four PC-Duo components has its own guide:

- ◆ *PC-Duo Master Guide*
- ◆ *PC-Duo Host Guide*
- ◆ *PC-Duo Gateway Server Guide*
- ◆ *PC-Duo Web Console Operating Guide*
- ◆ *PC-Duo Web Console Installation Guide*
- ◆ *PC-Duo Deployment Tool Guide*

For more information about PC-Duo documentation and technical support, see:

- ◆ "Typographical conventions"
- ◆ "Technical support options"

Typographical conventions in documentation

PC-Duo documentation uses typographical conventions to convey different types of information.

Computer text

Filenames, directory names, account names, IP addresses, URLs, commands, and file listings appear in a plain fixed-width font:

You can use the default domain user account named `'RemoteControlGateway'`.

In examples, text that you type literally is shown in a bold font.

To run the installation program, type **`installme`** in the command line.

Screen interaction

Text related to the user interface appears in **bold sans serif type**.

Enter your username in the **Login** field and click **OK**.

Menu commands are presented as the name of the menu, followed by the > sign and the name of the command. If a menu item opens a submenu, the complete menu path is given.

Choose **Edit > Cut**.

Choose **Edit > Paste As... > Text**.

Variable text

Variable text that you must replace with your own information appears in a fixed-width font in italics. For example, you would enter your name and password in place of ***YourName*** and ***YourPassword*** in the following interaction.

Enter your name: *YourName*
Password: *YourPassword*

File names and computer text can also be displayed in italics to indicate that you should replace the values shown with values appropriate for your enterprise.

Key names

Names of keyboard keys appear in SMALL CAPS. When you need to press two or more keys simultaneously, the key names are joined by a + sign:

Press RETURN.

Press CTRL+ALT+DEL.

Technical support options

If you have any problems installing or using the PC-Duo remote support products, information and support resources are available to help:

This manual and the *Release Notes* may contain the information you need to solve your problem. Please re-read the relevant sections. You may find a solution you overlooked.

Our technical support staff can be contacted by the following means:

- ◆ For Americas and Asia/Pacific:
email: support@vector-networks.com
phone: (800) 330-5035
- ◆ For Europe, Middle East and Africa:
email: support@virtualnetworkpartners.eu
phone: +44 2030040750

We offer a range of support options including support and maintenance contracts, and time and materials projects. Consult our web site for the support plan that best meets your needs. Go to <http://www.vector-networks.com> and navigate to the Support section of the web site for more information.

Host Installation

PC-Duo Host can be installed on any computer that runs a supported operating system (OS) and meets the minimum requirements described in this section.

- ◆ ["Requirements"](#)
- ◆ ["Installation notes"](#)
- ◆ ["Licensing"](#)

Requirements

PC-Duo Host can be installed and operated on any computer that runs a supported operating system (OS) and meets the minimum requirements described in this section.

Before installing PC-Duo Host, note the following:

- ◆ If you plan to use PC-Duo Host with PC-Duo Gateway, then install PC-Duo Host after you install PC-Duo Gateway. See the *PC-Duo Gateway Server Guide* before installing PC-Duo Host.
- ◆ If you plan to deploy PC-Duo Host using a 3rd party imaging tool, you must first prepare the Host software with the PC-Duo-provided HostPrep utility and the Microsoft-provided SysPrep utility (see [“Install via 3rd-party imaging tools”](#) for more information).

Operating system requirements

Supported operating systems are:

- ◆ Windows Vista
- ◆ Windows Server 2008
- ◆ Windows 7
- ◆ Windows Server 2008 R2
- ◆ Windows 8
- ◆ Windows Server 2012
- ◆ Windows 8.1
- ◆ Windows Server 2012 R2
- ◆ Windows 10
- ◆ Windows Server 2016

PC-Duo Host runs on x86 natively and as a 32-bit application (with x64 kernel components) on x64.

Remote Desktop Services requirements

PC-Duo Host can be configured to allow remote viewing & remote control of Remote Desktop Services sessions in addition to the server console (see ["RDS tab"](#) for more information). This feature is available when a special license key enabling this support is installed on the Host (see ["About tab"](#) for more information).

This feature is supported on the following operating systems:

- ◆ Windows Server 2008 and 2008 R2
- ◆ Windows Server 2012 and 2012 R2
- ◆ Windows Server 2016

This feature works with Remote Desktop Services in “administrative” mode, but is designed primarily to support “application” mode, with a larger number of different users logged into the server.

It is compatible with Microsoft RDP clients, as well as with Citrix ICA clients.

Hardware requirements

The hardware requirements are:

- ◆ Minimum requirements – Same as those specified by Microsoft for the respective operating system.
- ◆ Recommended requirements – Same as those specified by Microsoft for the respective operating system.

Installation requirements

The following additional requirements are required or recommended for installation of PC-Duo Host:

- ◆ Windows Installer 3.1 or later – Required by the installer. If needed, this upgrade is applied automatically when the `setup.exe` installer image is run.
- ◆ Acrobat Reader – Required for documentation.
- ◆ Local Administrator access rights – PC-Duo Host runs as a Windows service on the local machine. Therefore, Local Administrator access rights are required for the user who is installing PC-Duo Host on the machine.

NOTE: *These prerequisites are met by the supported platforms, and therefore they are not included in the PC-Duo software distribution packages.*

Network requirements

PC-Duo Host operates over any type of network, including dial-up, Ethernet, token ring, and FDDI, provided that the network supports the TCP/IP, UDP/IP, IPX or SSL protocols.

The following conditions apply:

- ◆ IP is a general-purpose protocol supported on a wide variety of networks and servers. To enable communication using TCP or UDP over IP, you must enable the Microsoft TCP/IP Protocol (or you can use another WinSock 2 compliant IP stack).
- ◆ The SSL protocol runs above TCP/IP and below higher-level protocols such as HTTP or IMAP. Using TCP/IP on behalf of the higher-level protocols allows an SSL-enabled server to authenticate itself to an SSL-enabled client, and both machines to establish an encrypted connection.
- ◆ The WebSocket protocol runs above HTTP or HTTPS. PC-Duo uses the binary WebSocket protocol over HTTP (which in turn is over TCP) as well as over HTTPS (which in turn runs over SSL). For plain WebSocket (WS) connections over HTTP, PC-Duo uses the same encryption used for TCP connections. For Secure WebSocket (WSS) connections, the connection is encrypted and secured by the underlying HTTPS/SSL connection.
- ◆ The PC-Duo UDP, TCP and SSL transports fully support IPv4 and IPv6 addressing.

Installation notes

The PC-Duo Host can be installed using any of the following methods:

- ◆ “Install via command line utility”
- ◆ “Install via internet download”
- ◆ “Install via Deployment Tool”
- ◆ “Install via 3rd-party imaging tools”
- ◆ “Change station name with macros”
- ◆ “Configure security settings”
- ◆ “Configure Windows Firewall exceptions”
- ◆ “Configure network settings for IPX”

Install via `msiexec` command line utility

PC-Duo Host can be installed manually by using the `msiexec` command line utility. For more information on using the `msiexec` utility, see [“Install PC-Duo Host with the MSISEXEC command line”](#).

Install via internet download

PC-Duo applications are distributed as ZIP files available for download from <http://www.vector-networks.com>. Unzip the contents (while preserving the directory tree structure) on your computer and simply run the appropriate `Host.msi` file (based on the type of Windows operating system you are using) to install the product.

Executable File	Description
Host.msi	Host for x86 systems
Host-x64.msi	Host for x64 systems

Install via the Deployment Tool

PC-Duo Deployment Tool can be used to automatically deploy and install a standard or customized configuration of PC-Duo Host on one or more computers in your network. See *PC-Duo Deployment Tool* for information on configuring and operating PC-Duo Deployment Tool.

Install via 3rd-party imaging tools

When a third-party utility program, such as Symantec Norton Ghost [™] or PowerQuest Drive Image, is used for operating system imaging, the following considerations must be taken into account when including PC-Duo Host as part of an operating system image:

Generate unique HostIDs

Each PC-Duo Host installation is identified by a unique identifier, called the HostID. This identifier is used by the PC-Duo Gateway to identify a Host, even as other information about the Host, such as the machine name, may change. This identifier contains no additional information and has no use other than to allow the PC-Duo Gateway to identify individual Hosts on the network. The HostID is a *GUID*, a 16-byte number with a text representation like "{C8E645A4-AF10-46f7-838B-A75105C8AA13}".

If PC-Duo Host is installed on an operating system that is then imaged, all of the machines will end up with the same HostID. PC-Duo Gateway will recognize the first Host it sees with this HostID, but ignore any others with the same HostID. The result is that many Hosts will not show up in the PC-Duo Gateway directory.

NOTE: *This problem occurs independently of how the imaging or replication is done, and affects PC-Duo Host v4.0 and later installations.*

There are two strategies for dealing with this issue:

- ◆ The preferred solution is to prepare the Host installation for imaging before creating the operating system snapshot to be duplicated. Just as you use the Microsoft-provided "SysPrep" utility to prepare the operating system, you can use the PC-Duo Host "HostPrep" utility to prepare the Host before imaging. This is described in the next section.

- ◆ If a deployment has been completed and duplicate HostIDs exist on the network, the PC-Duo Host "RmHostID" utility can be used to remove the duplicate HostIDs and cause the affected machines to be assigned a new (and unique) ID. This is described later in this document.

Prepare the Host and operating system for imaging

PC-Duo Host includes a utility program named `hostprep.exe` to address issues with operating system imaging. The Hostprep utility appears in the *PC-Duo Utilities* file.

To avoid the problem of having duplicate HostIDs, the `hostprep` utility must be run to delete the ID before the operating system image is captured.

NOTE: *You must prepare the Host software for imaging just before you use the Microsoft-provided SysPrep utility to prepare the operating system.*

After the machine is set up and all Host settings are configured, and immediately before running the Microsoft-provided SysPrep utility, run the `hostprep.exe` utility from a command prompt. The optional command line argument `"-y"` can be used to avoid a prompt to continue. When HostPrep runs, it stops the Host service and prepares the Host for imaging. It is critical that the Host service not restart before the operating system image is captured because when the Host starts, it undoes the actions completed by the HostPrep utility.

For more information about operating system imaging, please see the Microsoft TechNet Desktop Deployment Center at

<http://www.microsoft.com/technet/desktopdeployment/>

HostPrep command line syntax

HostPrep accepts a command line flags that control its behavior:

- ◆ `-y` do not ask for confirmation; default is to prompt before continuing
- ◆ `-yes` same as `'-y'`

- ◆ -guid deletes the HostID only, but does not prepare the settings
- ◆ -restart restarts the Host Service when compute; should only be used with '-guid'

To prepare an installation for imaging, run `hostprep.exe` with no arguments, and press the "y" key when prompted.

To delete the HostID on the local computer and cause a new one to be assigned immediately, run the command line "`hostprep.exe -guid -restart`".

HostPrep runs on all of the operating systems supported by the PC-Duo Host.

Remove duplicate Host IDs

If PC-Duo Host has been deployed using an imaging tool, and one or more Hosts are not found by the Gateway, you may have a duplicate HostID problem. In this case, the Gateway recognizes the first Host machine with the HostID but ignores any other machines with the same HostID. To resolve this situation, PC-Duo provides a utility called `RmHostID`; it appears in the *PC-Duo Utilities* file.

The `RmHostID` utility runs on one computer and searches one or more computers for Host installations that have a specified HostID. If a matching HostID is found, the HostID is deleted and the Host Service restarted so that a new ID will be assigned. This utility can be used to "clean up" Host installations with duplicate IDs on a LAN.

RmHostID command line syntax

`RmHostID` accepts command line flags that control its behavior:

- ◆ -p prompt for confirmation before deleting HostID
- ◆ -prompt same as '-p'
- ◆ -? displays help text describing how to use `RmHostID`

`RmHostID` expects two arguments (in addition to any flags) on its command line. The first argument specifies which HostIDs should be considered duplicates, and therefore should be deleted. The second argument specifies which machine or machines should be examined.

The HostID specification (first argument) can be one of:

- ◆ A specific GUID, in the form "{C8E645A4-AF10-46f7-838B-A75105C8AA13}"
- ◆ A star ("*"), signifying that all HostIDs found should be deleted
- ◆ An at sign "@" followed immediately by a filename. This causes the specified file to be read, and each line should contain a single GUID.

The machine's specification (second argument) can be one of:

- ◆ If the machine specification is missing, the local machine is checked
- ◆ A specific machine name, as either a NetBIOS machine name or a DNS name
- ◆ A star ("*"), which instructs `RmHostID` to enumerate all machines on the network
- ◆ An at sign "@" followed immediately by a filename. This causes the specified file to be read, and each line should contain a single machine name (as either a NetBIOS machine name or a DNS name).

Examples:

- ◆ `RmHostId {078A9A01-6931-42A3-9371-EA00F1DC7D99} *`

This example enumerates the machines on the network, and deletes the HostID of any installations that match the specified ID.

◆ RmHostId {078A9A01-6931-42A3-9371-EA00F1DC7D99} MACHINE04

This example connects to the one machine named “Machine04”, and deletes the HostID on that machine if and only if it matches the specified ID.

◆ RmHostId * MACHINE04

This example connects to the one machine “Machine04”, and deletes the HostID unconditionally, because “*” was specified as the HostID pattern.

◆ RmHostId GUIDS.TXT *

This example enumerates the machines on the network, and deletes the HostID of any installations that match any of the IDs specified in the GUIDS.TXT file.

◆ Example GUIDS.TXT file:

- ◆ {078A9A01-6931-42A3-9371-EA00F1DC7D99}
- ◆ {078A9A02-6931-42A3-9371-EA00F1DC7D99}

Requirements for RmHostID

The PC-Duo Master user must be logged in as Administrator, or otherwise have access permissions to the ADMIN\$ share on the Host machines.

The Host machines must allow remote access to the Service Control Manager and to the Registry. Typically, this means that Microsoft File & Printer Sharing is enabled and that these services are not blocked by a firewall.

Enumerating machines on the network with “*” can take some time; this utility uses the same algorithm and APIs to enumerate the network as the PC-Duo Deployment Tool.

Host GUIDs can be obtained by copying from:

- ◆ the Host Control Panel **Gateways** tab
- ◆ the Gateway Administrator Host Properties **General** tab
- ◆ the registry on an affected machine in HKCR\Proxy.Host\HostID\GUID

Change station name with macros

Host station name macros are now supported. The Host station name can include strings in the form %MACRO%, and these macros are substituted at runtime for the correct values. This complements the \$MACRO\$ feature in PHSETUP, which provides a one-time substitution at PHSETUP runtime.

This feature may be useful when creating a Host image for deployment, either using the Deployment Tool or via imaging of the entire disk. The macro names supported are:

Macro	Description
%NAME%	Host computer machine name
%USER%	Logged in user at the Host machine console in Windows “<domain>\<username>” format
%USERNAME%	Logged in user at the Host machine console in “<username>” only

	format
%USERUPN%	Logged in user at the Host machine console in UPN (universal principal name) format, or blank if not a domain account
%USERUPN+%	Same as %USERUPN%, except provides %USER% value for local account
%USERDISPLAY%	Logged in user at the Host machine console account display name
%USERDISPLAY+%	Same as %USERDISPLAY%, except provides %USER% value if account display name is blank
%USEREMAIL%	Logged in user at the Host machine console account email address, or blank if not a domain account or not configured in Active Directory
%USEREMAIL+%	Same as %USEREMAIL%, except provides %USER% value if account email address is blank
%VER%	External Host software version number (e.g. "v8.0.0.1800")
%INTVER%	Internal Host software version number
%PLATFORM%	Host operating system platform (e.g. "Win7")
%PID%	Process ID of the Host service
%PROT%	Network protocol (e.g. "IP" or "TCP")
%ADDR%	Network address (e.g. "192.168.0.15")
%PORT%	Network port (e.g. "1505")

Macros for Remote Desktop Services session Hosts

The following macros are available for customizing station name for Hosts running in Remote Desktop Services sessions. They should be applied in the RDS Host Control Panel template but can also be specified in the root Host Control Panel (see [RDS tab](#) for more information).

Macro	Description
%CLIENTNAME%	Machine name that the client of the RDS session has connected from, or the name of the server machine (same as %NAME%) if the session is not a RDS instance
%CLIENTADDR%	IP address that the client of the RDS session has connected from, or the IP address of the server machine (same as %ADDR%) if the session is not a RDS instance
%SESSION%	RDS session number. This will be 0 (zero) for the root Host instance, and non-zero for RDS instances.

Configure security settings

If you run PC-Duo Host on Windows XP, you may need to modify security settings according to the following procedure:

- 1 Select **Start > Settings > Control Panel > Administrative Tools**.
- 2 Double-click **Local Security Policy**.
- 3 Set the following in **Security Settings > Local Policies > Security Options**:
 - ◆ Set the **Network Access: Sharing and Security** model for local accounts policy to **Classic**. You can set the value for this item by double-clicking it, and selecting **Classic** from the list.
 - ◆ Optionally, set the **Accounts: limit local account** use of blank passwords to console logon only policy to **disabled** if you want to be able to use blank passwords to connect to this Host computer.

NOTE: *This is a significant security risk and is NOT recommended.*

- ◆ Optionally, set the **Accounts: Guest account** status policy to **disabled** to prevent problems with guest authentication to the Host computer.

NOTE: *Depending upon which version of Windows you are using, and your Windows UI settings, the procedure above may vary. Items may be named differently and navigating to them may be slightly different as well. Note that in XP Home Edition, these security settings cannot be set and you must use simple password authentication. On Vista Home, the setting must be set to Classic. If the machine is joined to a domain, it should automatically be set to this.*

Configure Windows Firewall exceptions

At installation time, the Host installer and Gateway installer create program-based exceptions in the Windows Firewall. The exceptions are named “PC-Duo Host” and “PC-Duo Gateway”, and allow network traffic to the Host service and Gateway service programs, respectively, over their standard default ports.

If you do not want the exceptions (e.g. because the Host is set for reverse connections only, and should not be “exposed”), disable the exceptions by unchecking the box in the configuration dialog for Windows Firewall itself. It is not recommended that the exceptions be deleted, because they will be recreated and enabled automatically if you upgrade to a later version of PC-Duo.

The exceptions are removed automatically when the products (Host, Gateway) are uninstalled.

Licensing

If you download this software from the Vector Networks web site on a 30-day trial basis and want to continue using the product, you may purchase it by contacting a preferred reseller, or by contacting Vector Networks directly. Your purchase provides an appropriate license key to use with PC-Duo Host.

The software does not need to be reinstalled after you purchase it. The product package contains a license key that you can add to your existing installation. This key converts your 30-day trial software directly to an unlimited version.

Add a license key before your trial period expires

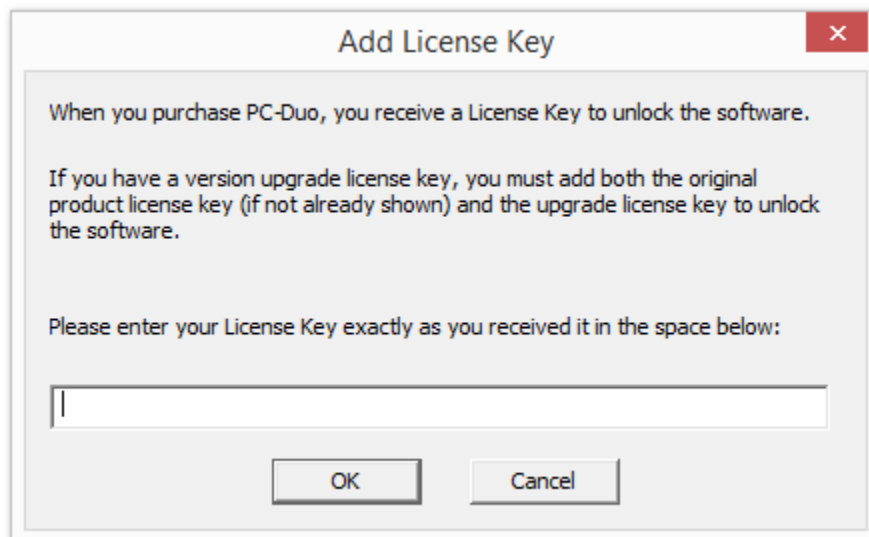
If you attempt to run PC-Duo Host after your trial period has expired, the message **Thank you for trying PC-Duo** appears. Within the message, click **Add License and enter your new license key**.

Your license is activated immediately. You do not need to restart PC-Duo Host.

Add a license key after your trial period expires

To add a license key before your 30-day trial expires, follow these steps:

- 1 Select **Start > All Programs > Vector Networks > PC-Duo Host Control Panel**.
- 2 Select the **About** tab from the PC-Duo Host Control Panel window.
- 3 Click **Add License**. The **Add License Key** window appears.



- 4 Enter the license key, and click **OK**.

Your license is activated immediately. You do not need to restart PC-Duo Host.

NOTE: A PC-Duo Host that is meant to be used as the root for Hosts running in Remote Desktop Services sessions will require a special license key that will specify the number of simultaneous RDS sessions that can be supported (see [About tab](#) for more information). Note that the PC-Duo Host must be restarted in order for the Remote Desktop Services support to be activated.

Upgrade a license key

If you are upgrading your license, you will receive an Upgrade license key, which you should add using the instructions above. Both the original product license and the upgrade license will be listed on the **About** tab.

Host license key types

Below is a list of Host license key types:

Host License Key Types	Description
Host (Prefix: 411, 412, 413)	<ul style="list-style-type: none">• Permanently installed Host• Accessible by Peer-to-peer and Gateway-managed connections• Hosts that are automatically or manually moved to All Hosts group on Gateway will be counted under the Managed Host license mode
Remote Desktop Services Host (Prefix: 414)	<ul style="list-style-type: none">• Transforms a regular Host into a special version that can be installed/run on a Remote Desktop Services server, where it will generate Host images to be injected into new RDS sessions created• These RDS Host images will appear as transient Hosts• Accessible only by Gateway-managed connections• RDS Hosts are automatically added to All Hosts and the RDS groups, and will be counted as concurrent RDS sessions under the Managed Hosts license mode <p>Note: When this key is added to the regular Host, the Host service must be restarted; the Remote Desktop Services tab to configure settings for the RDS Host sessions, including which Gateway to report to, will then be enabled in the Host Control Panel.</p>
VDI Host (Prefix: 416)	<ul style="list-style-type: none">• Transforms a regular Host into a special version that can be configured as part of a virtual desktop template and will inject transient VDI Hosts into any virtual desktop images created• Accessible by Peer-to-peer and Gateway-managed connections• The VDI Host will only exist while the virtual desktop is running, and will automatically be deleted from the Gateway when the desktop is discarded• VDI Hosts are automatically added to All Hosts and the Host for VDI groups, and will be counted as concurrent VDI session under the Managed Hosts license mode

Host Operation

PC-Duo Host runs as a Windows service whenever you start up your computer. It can be configured to accept connections from a PC-Duo Master user in two different ways:

- ◆ “[Peer-to-peer connections](#)” between a Master computer and a Host computer. With these connections, authentication and authorization are enforced by the PC-Duo Host.
- ◆ “[Gateway-managed connections](#)” between a Master computer and a Host computer through a PC-Duo Gateway. With these connections, authentication and authorization are enforced by the PC-Duo Gateway.



NOTE: By default, PC-Duo Host allows PC-Duo Master users who belong to the Host computer’s Administrators group (a Windows group) full access to control the Host computer and to configure the PC-Duo Host Control Panel window for the Host computer. In addition, the default Gateway user account `RemoteControlGateway` also has full access. Other PC-Duo Master users must be added (see the “[Security tab](#)”) in order to have access to the Host.

PC-Duo Host includes many configuration options, including:

- ◆ “[About tab](#)”: The ability to manage license keys and see information about the Host.
- ◆ “[Access tab](#)”: The ability to block remote access entirely.
- ◆ “[Effects tab](#)”: The ability to control graphical effects transmitted from the Host.
- ◆ “[Gateways tab](#)”: The ability of the Host computer to report to one or more PC-Duo Gateways in your network. Access to the Host can then be centrally managed and monitored by the PC-Duo Gateways.
- ◆ “[General tab](#)”: The ability to provide audible and/or visible notification on the Host computer when a PC-Duo Master user requests a connection.
- ◆ “[Options tab](#)”: The ability to view and change default Host settings.
- ◆ “[Protocols tab](#)”: The ability to select network protocol and/or port for communication with the Host.
- ◆ “[Screen tab](#)”: The ability to select desired screen capture technology and in the case of user-mode screen capture, limit the amount of bandwidth used.
- ◆ “[Security tab](#)”: The ability to create and apply custom access rights policies, including permissions and restrictions for specific PC-Duo features, to PC-Duo Master users or groups.
- ◆ “[Status tab](#)”: The ability to view current connection status and/or end connection.
- ◆ “[Tags tab](#)”: The ability to view custom information specified by the administrator for this Host.
- ◆ “[RDS tab](#)”: The ability to view and manage configuration settings for Hosts operating in Remote Desktop Services sessions.
- ◆ “[Chat window](#)”: The ability to enter private chat room with one or Master users connected to the Host.
- ◆ “[Remote Printing](#)”: The ability to set up remote printing.
- ◆ “[Host Audit Log](#)”: The ability to review a log of all connections to Host.

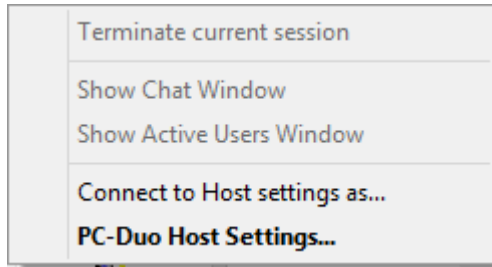
Host Tray Icon

When the PC-Duo Host service is successfully started, a tray icon will appear in the bottom right hand corner of the Windows screen:

Tray Icon	Description
	Service is started; active connection
	Service is started; no connection

Host Context Menu

Right-clicking on the Host tray icon will cause a context menu to appear.




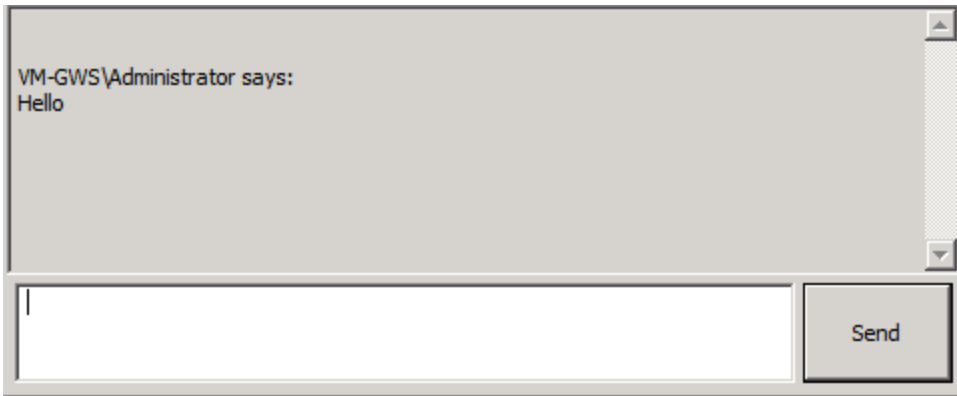
Below is a table of menu options available:

Option	Description
Terminate current session	Will disconnect remote user immediately
Show Chat Window	Will open a chat window that can be used by Host user to communicate with an remote users connected to this Host (see <i>Chat Window</i> for more information)
Show Active Users	Will display a list of all remote users with active connections to this Host (see <i>Active Users list</i> for more information)
Connect to Host Settings as...	Display the PC-Duo Host Control Panel (see <i>Host Control Panel</i> for more information), after a credentials prompt allowing you to connect as a user different than the console user.
PC-Duo Host Properties	Display the PC-Duo Host Control Panel (see <i>Host Control Panel</i> for more information)

Chat Window

When there is an active connection to your Host, a chat room is automatically created that will include the Master user connected to the Host, and if it is a Gateway-managed connection, any other Master users connected to the same Host. To send and receive

text messages with other members of the chat room, right-click on the  tray icon on the Windows task bar and select **Show chat window** from the context menu. A chat window will appear.



When you type a text message and click **Send**, the message will appear in a similar chat window on the Master display of any Masters connected to your Host. If the chat window is not already up on Master display, it will automatically be started to display the message.

NOTE: Chat support requires that all components (Host, Master, Gateway) be version 11.1 or later.

Active Users List





The Host will display a list of all remote users (Master, Administrators) actively connected to this Host by choosing the menu option called **Show Active Users** in the Host context menu:

Client's Identity			Address	Gateway
PROXYNETWORKS\aaaa			192.168.1.1	GWS (authenticated: PROXYNETWO...
PROXYNETWORKS\administrator (...)			192.168.1.7	GWS (authenticated: PROXYNETWO...

A resizable modeless dialog window will appear, featuring a list view with following columns:

- The identity of each Master-based client (“display name” and “authenticated identity”, unless they are the same, in which case only one identity will be listed).
- A column with an icon indicating that the user has input control or is viewing the screen.
- A column with an icon indicating that the user has Chat connected.
- A column(s) with an indication of other services that may be connected (e.g. File Transfer, Remote Printing, Remote Management and Clipboard).
- A column with network address of the Client.
- In the case of a Gateway based connection, a column with the Gateway’s name and Gateway identity (tooltip if not displayed). This is like the information displayed in the toast message.

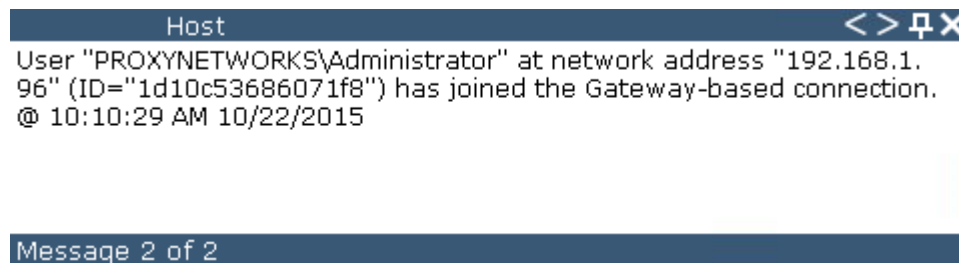
Note that in this example, there are 2 users (Masters) joined to the connection to this Host through the Gateway. Also note that the first client has input control, as indicated by

the  icon, and the second client is view only . Both clients have access to chat  and the shared clipboard  for this Host.

Popup Toast Notification

If **Popup Notifications > Enable connect/disconnect notifications** option is enabled in the Host Control Panel (default = enabled), the Host will display a “popup toast” message when a new connection is made. This popup toast notification will display the following information:

- When a new connection is made by a Master, the display name of the computer running the Master, authenticated identity of the Master user, the network address, and the viewer ID (for tracking purposes) of the Master will be displayed:



Note: If display name and authenticated ID are the same, only one entry will be listed.

- When a new connection is made by a Gateway to start a Recording, the session ID and authenticated identity of the user requesting the Recording will be displayed in the popup toast.
- If the initial connection is Gateway-managed, subsequent connections through the same Gateway will cause the Host toast notification to reappear. Previously, only the first connection to a Host resulted in the toast popup notification.
- When an active connection is ended, the viewer ID (if the connection is from a Master) or the session ID (if the connection is from a Recording) will be displayed in the popup toast.

Host Control Panel

Configuration options are managed through the PC-Duo Host Control Panel. It can be accessed in any of the following ways:

- ◆ Select **Start > All Programs > Vector Networks > PC-Duo Host Control Panel**.
- ◆ Double-click the PC-Duo Host icon in your system tray (lower right corner of your monitor) and choose **PC-Duo Host Properties**.
- ◆ Run the executable `phost.exe` located in the `PC-Duo Host` program directory.

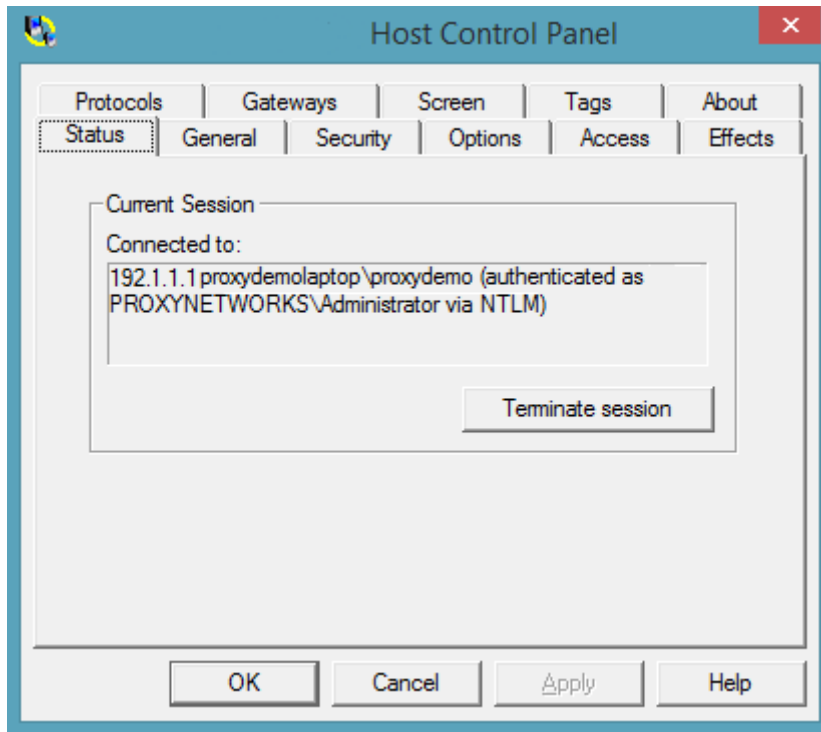
The PC-Duo Host Control Panel window appears. Use the PC-Duo Host Control Panel to configure the PC-Duo Host features through the following tabs

Tab	Function
Status	To view connection status and/or disconnect a session.
General	To set basic screen preferences
Security	To set a password or Windows credentials based access and control policy.
Options	To set keyboard and screen options.
Access	To define global (credentials-independent) connection options.
Effects	To enable or disable visual effects.
Protocols	To specify the allowed Host computer protocols and enable encryption.
Gateways	To specify the PC-Duo Gateways in your network to which your Host computer reports, and to require Gateway-managed connections.
Screen	To choose desired screen capture technology to use, and in the case of user-mode screen capture, to select bandwidth throttling options.
Remote Desktop Services	To specify configuration information for Host instances to be injected into RDS sessions
Tags	To display custom information specified by the administrator for this Host
About	To review information about the product.

NOTE: Some or all of PC-Duo Host features may not be accessible, depending on how PC-Duo Host is configured. Some features, such as Protocol or Gateways, may be locked and hidden from view by your administrator.

Status tab

The Status tab indicates the current status of any remote control connections to your computer.

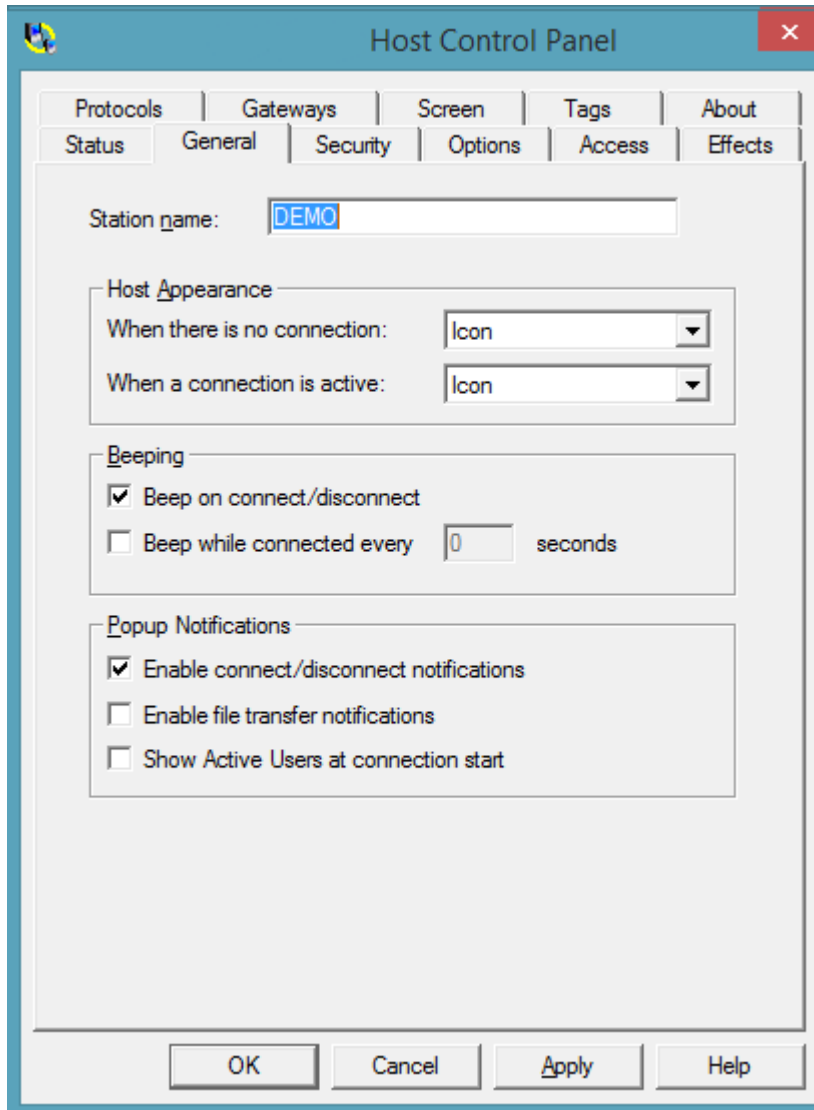


View the status of a remote connection to your Host computer as follows:

- ◆ Whenever there is a remote connection to your Host computer, the network address and username will appear in the **Connected to** field.
 - ◆ When a PC-Duo Master user makes a direct peer-to-peer connection to your computer, the PC-Duo Master user's account name and the network address will appear.
 - ◆ When a PC-Duo Master user makes a connection through a PC-Duo Gateway, the PC-Duo Gateway's network address and PC-Duo Master user account name at the Gateway will appear
 - ◆ When there is no remote connection to your computer, the field displays **<none>**.
- ◆ Disconnect any remote session by clicking **Abort session**.

General tab

Use the General tab to change preferences.



Change the following from the **General** tab:

- ◆ **Station name:** Modify the name by which your Host computer identifies itself to PC-Duo Gateways and/or PC-Duo Masters. To use macros to change the Station name automatically, see ["Change Station name"](#).
- ◆ **Host Appearance:** Configure the PC-Duo Host icon to appear (**Icon**) or not (**Hidden**) in your system tray (lower right corner of your monitor) by selecting either **Icon** (default) or **Hidden** for each of the following:
 - ◆ **When there is no connection:** The PC-Duo Host icon appears (or is hidden) when there is no active remote connection.

- ♦ **When a connection is active:** The PC-Duo Host icon appears (or is hidden) when a remote connection is active.
- ♦ **Beeping:** Set auditory cues to indicate when a PC-Duo Master user requests to connect to your Host computer.
 - ♦ Select **Beep on connect/disconnect** to hear a quick series of three tones rising in pitch whenever a remote connection succeeds. With this option, a series of tones falling in pitch will be made when the remote connection is terminated.
 - ♦ Select **Beep while connected every...seconds** to hear a short tone, periodically throughout the duration of any remote connection. The interval between beeps can be set from 0 to 9999 seconds. To turn the feature off completely, set this to 0.
- ♦ **Popup Notifications:** Set visual cues that "popup" on Host screen to indicate when certain events occur (also called "toast" notifications).
 - ♦ Select **Enable connect/disconnect notifications** (default = selected) to see popup notifications when a PC-Duo Master user connects or disconnects from the Host.



- ♦ Select **Enable file transfer notifications** (default = not selected) to see popup notifications when a PC-Duo Master initiates file transfer operations to/from the Host.
- ♦ Select **Show Active Users at connection start** (default = not selected) to have the Active Users dialog automatically pop up when a connection is established. The dialog can be closed during a connection, and it will not display automatically again until a new network connection begins (that is, all current users disconnect, and a completely new connection is started). If hidden (or lost behind some windows), the tray icon context menu **Show Active Users** can be used to show the dialog and bring it to the front.

Note that in general most users will probably prefer that either **Show Active Users at connection start** or **Enable connect/disconnect notifications** is on, but both can be enabled.

Security tab

To authenticate the identity of PC-Duo Master users who request a connection to the Host, choose your preferred authentication method in the **Security** tab.

The following authentication methods are available:

- ◆ “Simple password configuration”
- ◆ “Windows authentication configuration”
- ◆ “Shared secret password authentication”
- ◆ “End-to-end authentication”

Simple password configuration

For authentication that does not require network-based credentials, use a simple password to check the identity of PC-Duo Master users who request access to your Host computer. Select **Allow connection with a simple password** and enter the password you would like to use to authenticate an incoming connection request.

To configure simple password authentication, consider the following options:

- ◆ Select **Allow connection with a simple password** from the Security tab to require simple password (or no password) for any remote connections to your Host computer. If you want to establish a password, type the same password in the **Password** and **Confirm Password** fields.
- ◆ Select **Use same password to control access to Host Settings** to control access to the PC-Duo Host settings on your Host computer (for any person to view or modify these settings locally) with the same simple password that you provide for any remote connections to your Host computer.
- ◆ Select **Use a different password for Host Settings** to control access to the PC-Duo Host settings on your Host computer (for any person to view or modify these settings locally) with a different simple password (or no password) that you provide for any remote connections to your Host computer. If you want to supply a password, type in the same password in the **Settings Password** and **Confirm Password** fields.

If **Allow Remote Administration** is selected, anyone with administrative privileges on your Host computer can configure PC-Duo Host settings remotely; otherwise, only the local logged-in user can access and modify the PC-Duo Host settings.

NOTE: Where possible, it is recommended that Windows authentication be used. Simple password authentication remains available for those cases where Windows authentication is not appropriate or is unavailable (for example, Windows XP Home Edition does not support “classic” authentication security policy, and must use simple password).

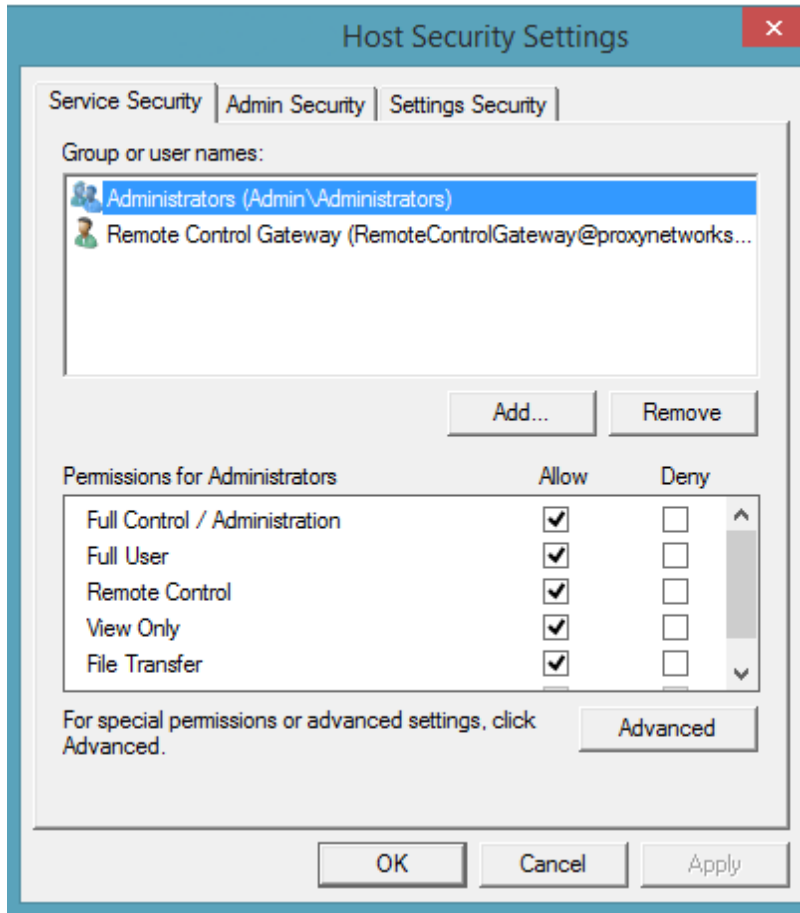
Windows authentication configuration

For authentication based on network credentials, use Windows authentication to check the identity of PC-Duo Master users who request access to your Host computer. Select **Require Windows authentication** from the Security tab. PC-Duo Host will check the credentials (username/password) of the PC-Duo Master user requesting access against those kept at the domain controller (usually in Active Directory). If the credentials match, the connection will be established; if not, connection request will be refused.

- ◆ "Permissions"
- ◆ "Default Host security settings"
- ◆ "Service Security tab"
- ◆ "Admin Security tab"
- ◆ "Settings Security tab"

Permissions

Windows authentication configuration options can be set/modified by clicking on **Set Permissions**. The PC-Duo Host Security Settings window appears.



One of the strongest features of PC-Duo is the availability of fine-grained permissions. PC-Duo Master users or groups can be added or deleted from three different sets of permissions:

- ◆ “[Service Security tab](#)”, defines permissions for services on this Host for the user or group selected.
- ◆ “[Admin Security tab](#)”, defines permissions for access to the **PC-Duo Host Control Panel window**.
- ◆ “[Settings Security tab](#)”, defines permissions for modifying configuration settings for the **PC-Duo Host Control Panel window**.

An **access control policy**, comprised of a specific set of permissions, can be assigned to one or more PC-Duo Master users or groups in the network. A common configuration approach is to create role-based access control policies and assign them to specific groups of users in the network (e.g. Senior Administrators may be granted more permissions than Junior Administrators).

NOTE: If Windows authentication is selected, all Gateway-managed connections require that a PC-Duo Gateway domain user account with full access and administrative rights be configured on the Host computer.

NOTE: As long as the PC-Duo Gateway is on the known list of PC-Duo Gateways on the Host’s Gateways tab, the Host will automatically add that Gateway’s user account to its security settings list with full access rights.

Default Host security settings

The following PC-Duo Host security settings are set by default for Windows authentication:

- ◆ **Service Security:** The local machine's Administrators group and the default PC-Duo Gateway domain user account (`RemoteControlGateway`) have full access to all the PC-Duo services. Also, any new accounts created on Gateways known to the Host will have full access.
- ◆ **Admin Security:**
 - ◆ The local machine's Administrators group and the default PC-Duo Gateway domain user account have full access to all administrative rights for this PC-Duo Host.
 - ◆ The Interactive group only has rights to **Connect for Admin on Local Machine** and **View Host Status**.
- ◆ **Settings Security:** The local machine's Administrators group and the default PC-Duo Gateway domain user account have full access rights to all administrative settings for this PC-Duo Host.

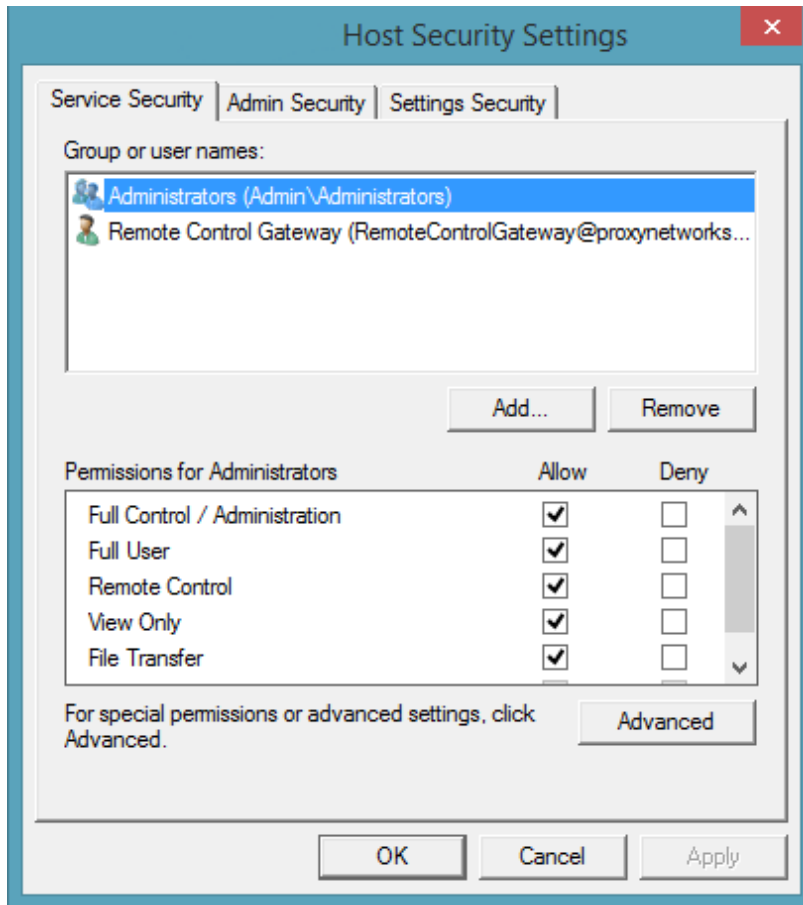
With these default settings, any other PC-Duo Master user that connects to this Host will be limited to just the **Status** tab of the PC-Duo Host Control Panel (the other tabs will be hidden). These PC-Duo Master users have no other rights with respect to viewing or modifying other PC-Duo Host settings.

The default settings allow for easy configuration of Gateway-managed connections. Use the default user account `RemoteControlGateway` or any new account created on the Gateway to access configuration options on the Host.

If neither of these options is used, a new user account name must be created and configured for full access rights in PC-Duo Host. It is recommended that the user account name not be a member of any group. This strategy keeps the account isolated in case it ever becomes compromised.

Service Security tab

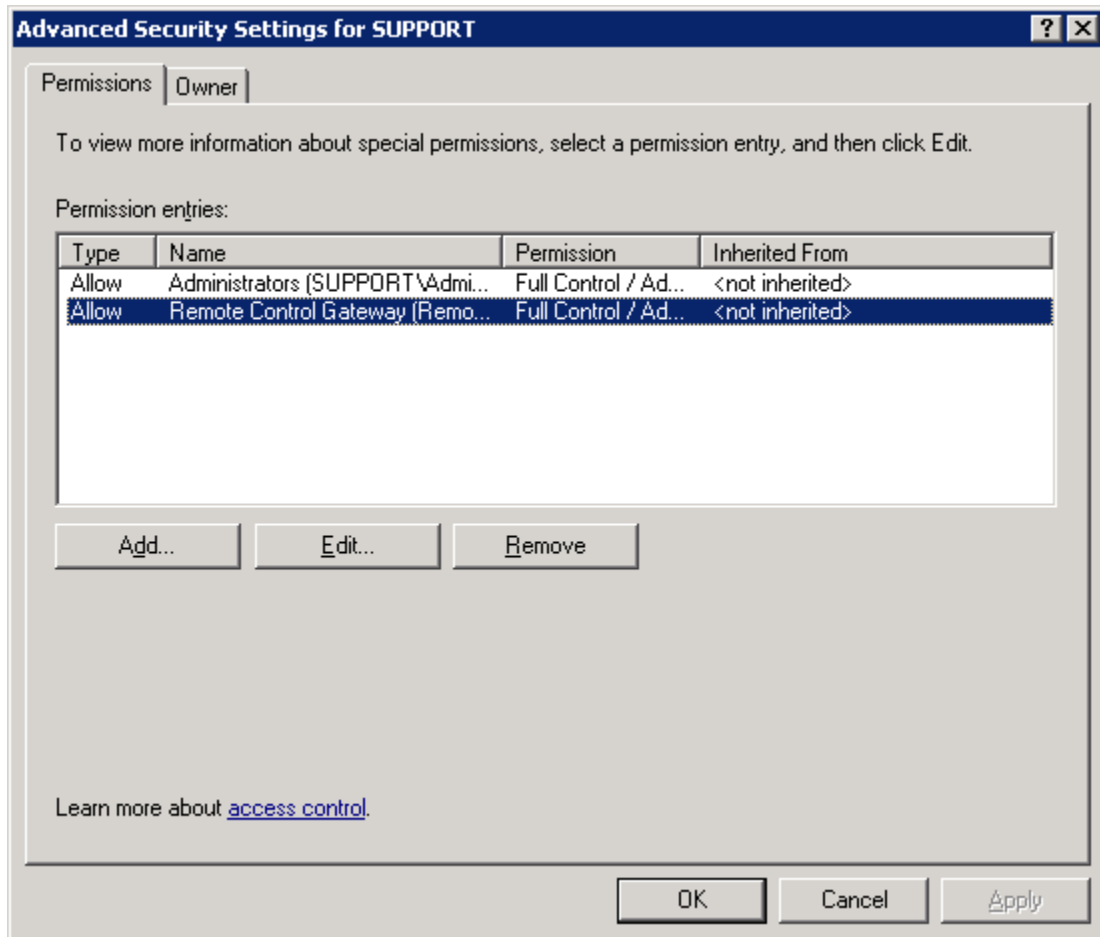
For any PC-Duo Master user or group of users, set permissions for remote control services to the Host through the **Service Security** tab.



In the **Service Security** tab, you can perform the following tasks:

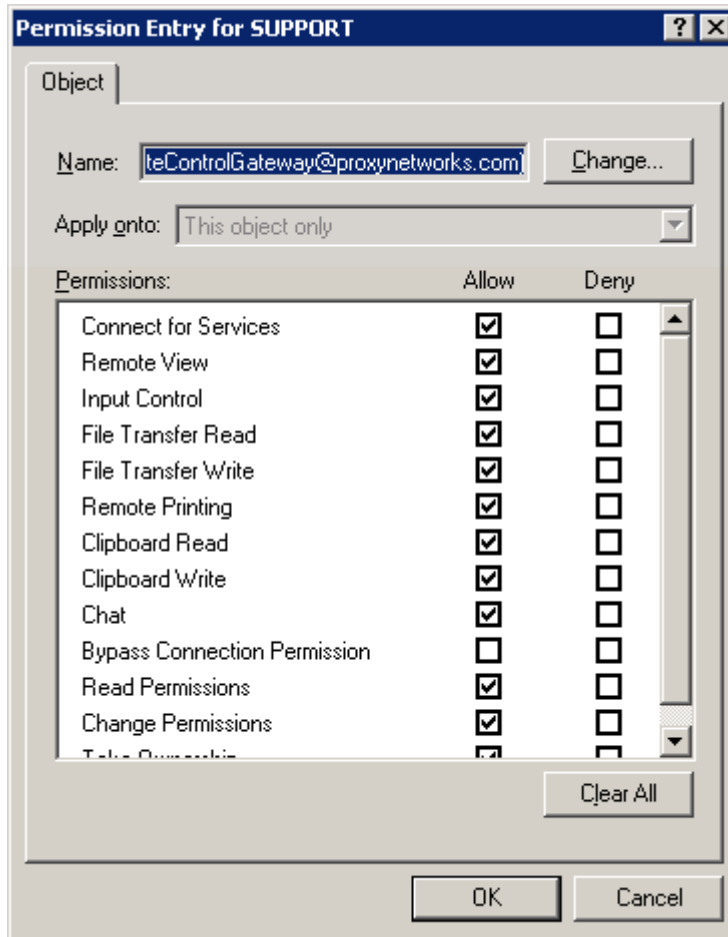
- ◆ Click **Add** to add a new PC-Duo Master user or group for which you want to specify permissions.
- ◆ Select an existing PC-Duo Master user or group that has permissions and click **Remove** to remove it.
- ◆ Select a PC-Duo Master user or group and click **Allow** or **Deny** in the list of **Permissions**. The individual permissions can be seen on the **Advanced** page. The following common groupings exist:
 - ◆ **Full Control/Administration**: Includes every permission in the Advanced list (see below).
 - ◆ **Full User**: Includes all permissions in the Advanced list (see below) except the **Edit Security** permission.
 - ◆ **Remote Control**: Includes permission to connect for services, remote view Host screen, and input control of the Host.
 - ◆ **View Only**: Includes permission to connect for services and remote view Host screen, but not to take input control of the Host.
 - ◆ **File Transfer**: Includes permission to connect for services and file transfer read-write, but not to view the Host screen.
 - ◆ **Edit Security**: Includes permission to change these security rights: read permissions, change permissions, and take ownership.

- ♦ **Special Permissions:** Indicates a non-standard grouping of permissions not exactly matching one or more of the previously described groups. [See "Permission Entry window - Service Security"](#).
- ♦ Click **Advanced** to specify permissions and open the **Advanced Security Settings** window.



Advanced Security Settings window - Service Security

In the **Permissions** tab of the **Advanced Security Settings** window, select an entry for which you want to assign advanced permissions and click **Edit**. The **Permission Entry** window opens:



Permission Entry window - Service Security

Each advanced permission is treated individually; click **Allow** or **Deny** for any of them. The following permissions exist:

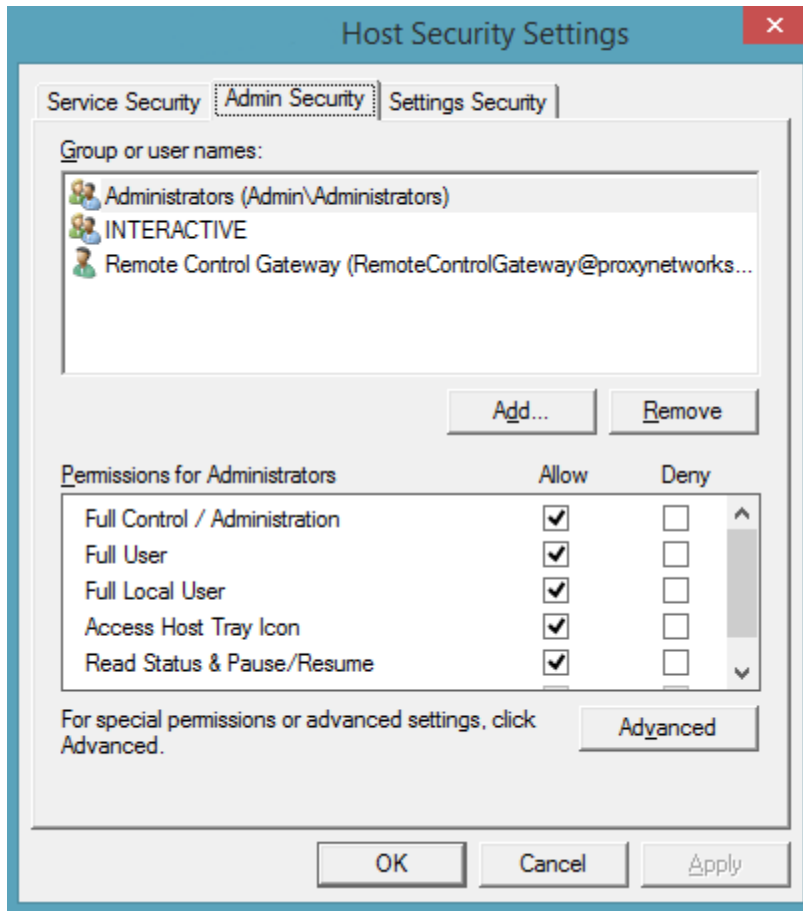
- ◆ **Connect for Services** determines whether a domain account or machine-local account has permission to connect to this PC-Duo Host computer. It does not determine what a PC-Duo Master user can do once connected to this PC-Duo Host computer, but you must (through this setting) allow the connection permission for a PC-Duo Master PC-Duo Master user or PC-Duo Gateway for the remote connection to occur.
- ◆ **Remote View** determines whether a PC-Duo Master user or a group can view the screen of the Host computer once connected. Without this permission, the PC-Duo Master user may connect for other services, such as file transfer, but sees a message in the Remote Control window that remote view access is denied.
- ◆ **Input Control** determines whether a PC-Duo Master user or a group has the ability to control the Host computer mouse and keyboard once connected. Without this permission, PC-Duo Master users can only view the screen of the Host computer.
- ◆ **File Transfer Read** determines whether a PC-Duo Master user or a group has the ability to navigate to and read files that are located on the Host computer. Without this permission, PC-Duo Master users can navigate to drives or subdirectories on the Host computer, but cannot see the contents of those directories. This permission gives you the right to use the File Transfer feature to read files. Additionally, file system access is still

controlled by the Windows Security settings for files and directories, so you must have read permission on the files and directories you want to access.

- ◆ **File Transfer Write** determines whether a PC-Duo Master user or a group has the ability to write files to the Host computer. Without this permission, PC-Duo Master users cannot make any changes to files or directories on the Host computer. This permission gives you the right to use the File Transfer feature to write files. Additionally, file system access is still controlled by the Windows Security settings for files and directories, so you must have write permission on the files and directories you want to access.
- ◆ **Remote Printing** determines whether a PC-Duo Master user or a group can connect to the Host computer and use the remote printing feature. This feature allows PC-Duo Master users to print from applications running on the Host computer to a printer connected to the Master computer and vice versa. You must enable both the **Connect for Services** and **Remote Printing** permissions to enable this functionality.
- ◆ **Clipboard Read** determines whether a PC-Duo Master user or a group can copy information from the Host computer Windows clipboard to another application on the PC-Duo Master user's local computer.
- ◆ **Clipboard Write** determines whether a PC-Duo Master user or a group can copy information from the Windows clipboard on their local computer to an open application running on the Host computer.
- ◆ **Chat**: Determines whether a PC-Duo Master user can be added to a private chat room including the PC-Duo Host user, and any other PC-Duo Master users connected to the same Host.
- ◆ **Bypass Connection Permission** determines whether a PC-Duo Master user or group can connect to a PC-Duo Host without causing the Permission to Connect window to pop-up on the Host even if it is set to do so.
- ◆ **Read Permissions** determines whether a PC-Duo Master user or group can view the Service Security tab of the PC-Duo Host Security Settings window.
- ◆ **Change Permissions** determines whether a PC-Duo Master user or group can modify the permissions on the Service Security tab.
- ◆ **Take Ownership** determines whether a PC-Duo Master user or group can take ownership.

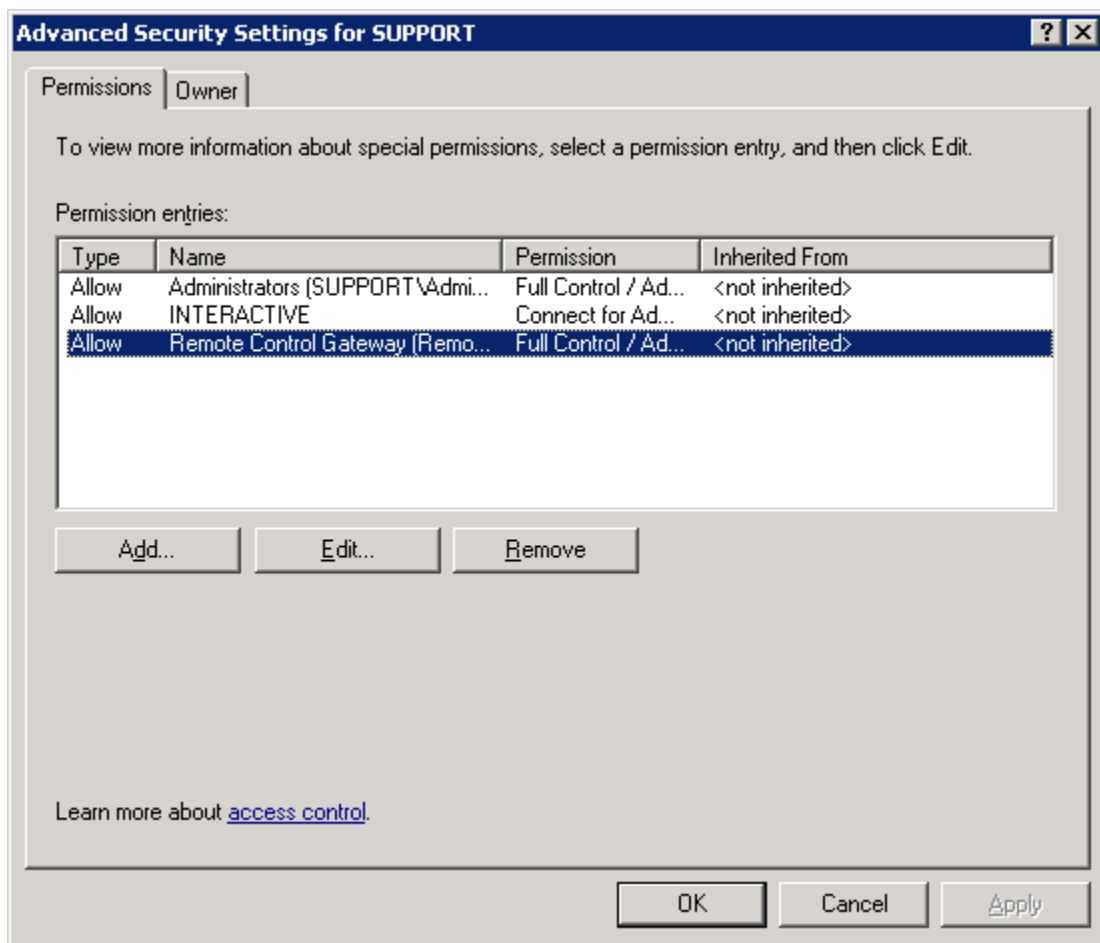
Admin Security tab

Access rights to the PC-Duo Host Control Panel window can be modified through the **Admin Security** tab.



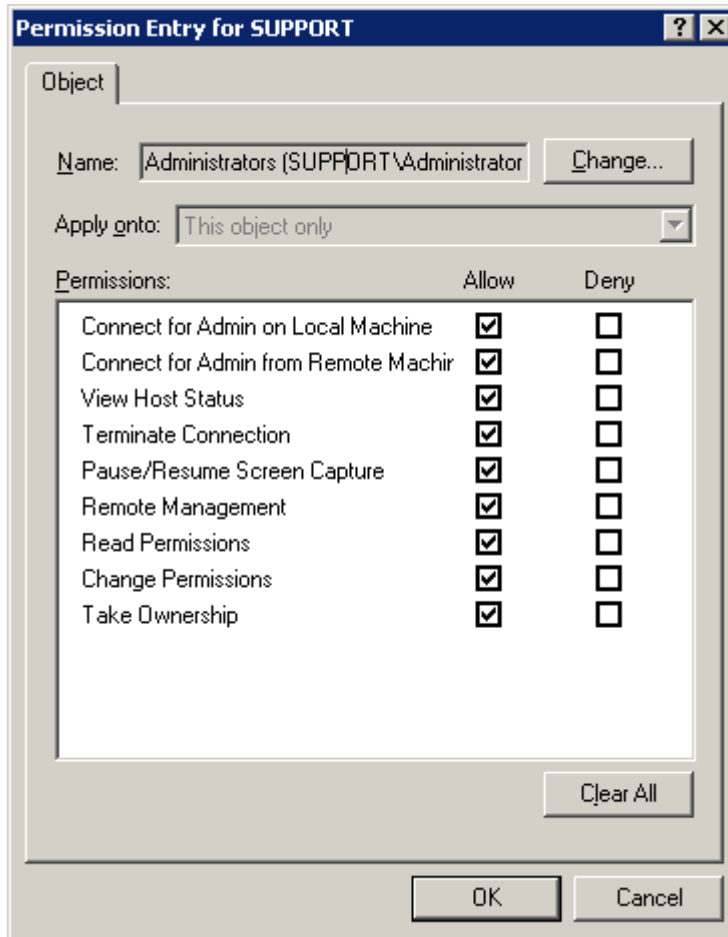
In the **Admin Security** tab, you can perform the following tasks:

- ◆ Click **Add** to add a PC-Duo Master user or group for which you will specify permissions.
- ◆ Select an existing PC-Duo Master user or group that has permissions and click **Remove** to remove it.
- ◆ Select a PC-Duo Master user or group and click **Allow** or **Deny** for the list of **Permissions**, each of is a common grouping of individual permissions. The individual permissions can be seen on the **Advanced** page. The following common groupings exist:
 - ◆ **Full Control/Administration**: Includes every permission in the list.
 - ◆ **Full PC-Duo Master user**: Includes all permissions except the Edit Security permission.
 - ◆ **Access Host Tray Icon**: Includes permission to connect for Administration on the local machine and view Host status. This set of permissions is required for the Host icon to appear in the system tray area.
 - ◆ **Edit Security**: Includes permission to change these security rights: read permissions, change permissions, and take ownership.
 - ◆ **Special Permissions**: Indicates a non-standard grouping of permissions not exactly matching one or more of the previously described groups.
- ◆ Click **Advanced** to specify permissions and open the **Advanced Security Settings** window.



Advanced Security Settings window - Admin Security

In the **Permissions** tab of the **Advanced Security Settings** window, select an entry for which you want to assign advanced permissions and click **Edit**. The **Permission Entry** window opens:



Permission Entry window - Admin Security

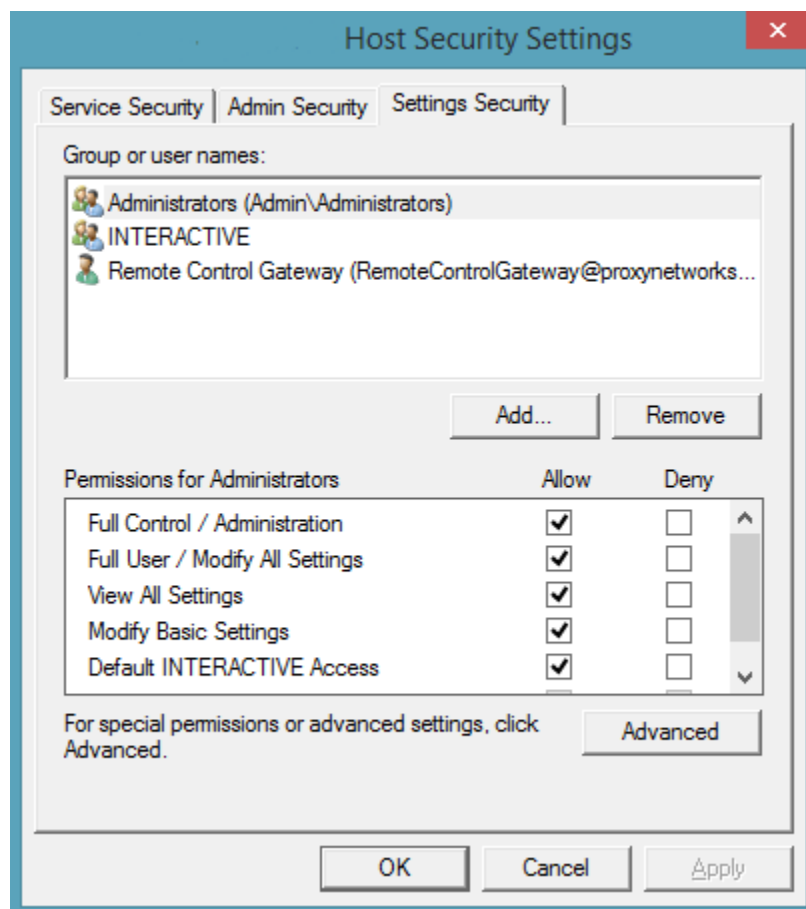
Each advanced permission is treated individually; click **Allow** or **Deny** for any of them. The following permissions exist:

- ◆ **Connect for Admin on Local Machine** determines whether a PC-Duo Master user or a group has permission to connect to PC-Duo Host settings. This setting does not determine what a PC-Duo Master user can do once connected to PC-Duo Host for administration.
- ◆ **Connect for Admin from Remote Machine** determines whether a PC-Duo Master user or a group has permission to view (and potentially access) PC-Duo Host settings through a remote connection. This setting does not determine what a PC-Duo Master user can do once connected to PC-Duo Host for administration.
- ◆ **View Host Status** determines whether a PC-Duo Master user or a group can view the current status panel of PC-Duo Host. You should allow current PC-Duo Master users of the Host computer **View Host Status** to be able to interact with the PC-Duo Host system tray icon.
- ◆ **Terminate Connection** determines whether a PC-Duo Master user or a group can terminate an existing remote control connection.
- ◆ **Pause/Resume Screen Capture** determines whether a PC-Duo Master user or a group can pause and resume screen capture in the Master Remote Desktop Window.

- ◆ **Remote Management** determines whether a PC-Duo Master user or a group can access the information and features on the Remote Management tab in the Master Remote Desktop Window.
- ◆ **Read Permissions** determines whether a PC-Duo Master user or a group can view the **Admin Security** tab of the PC-Duo Host **Security Settings** window.
- ◆ **Change Permissions** determines whether a PC-Duo Master user or a group can modify the **Admin Security** tab permissions.
- ◆ **Take Ownership** determines whether a PC-Duo Master user or a group can take ownership.

Settings Security tab

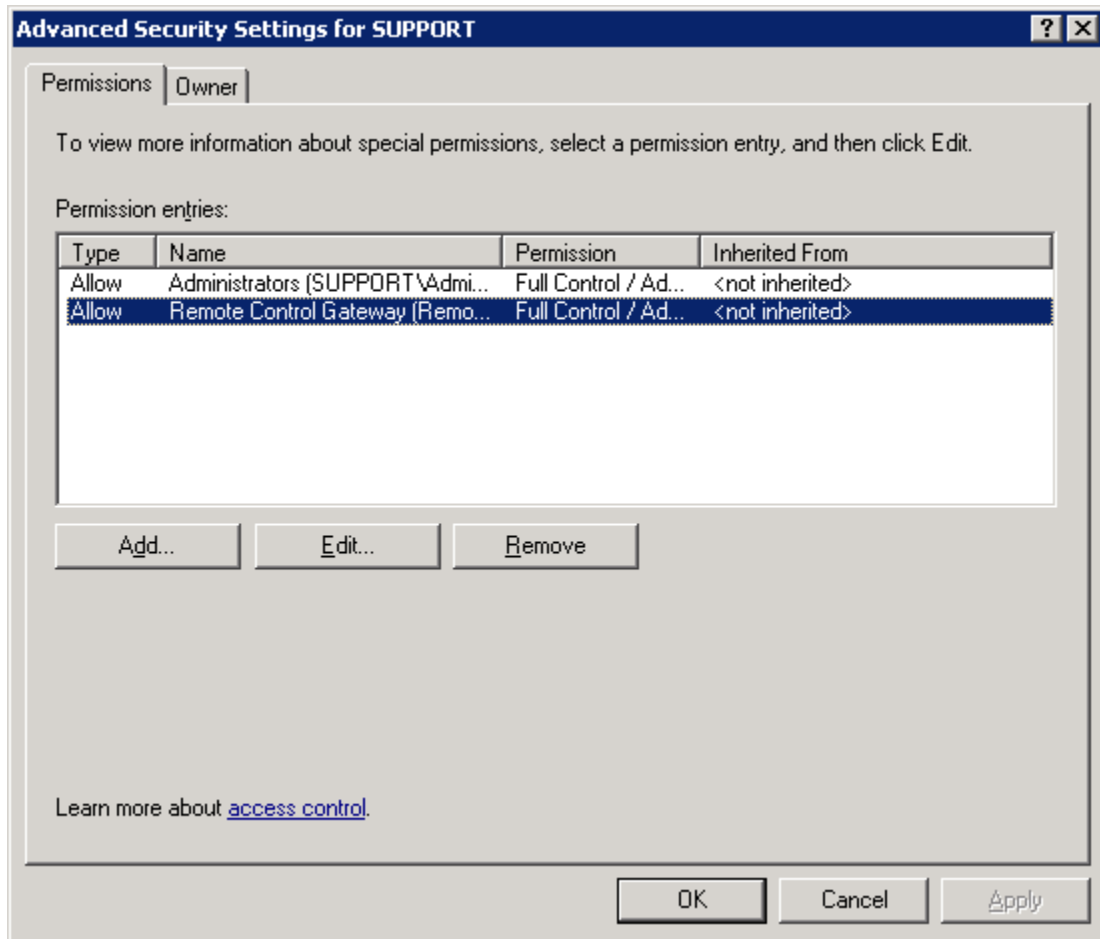
Administrative settings for the PC-Duo Host Control Panel window can be modified in the **Settings Security** tab.



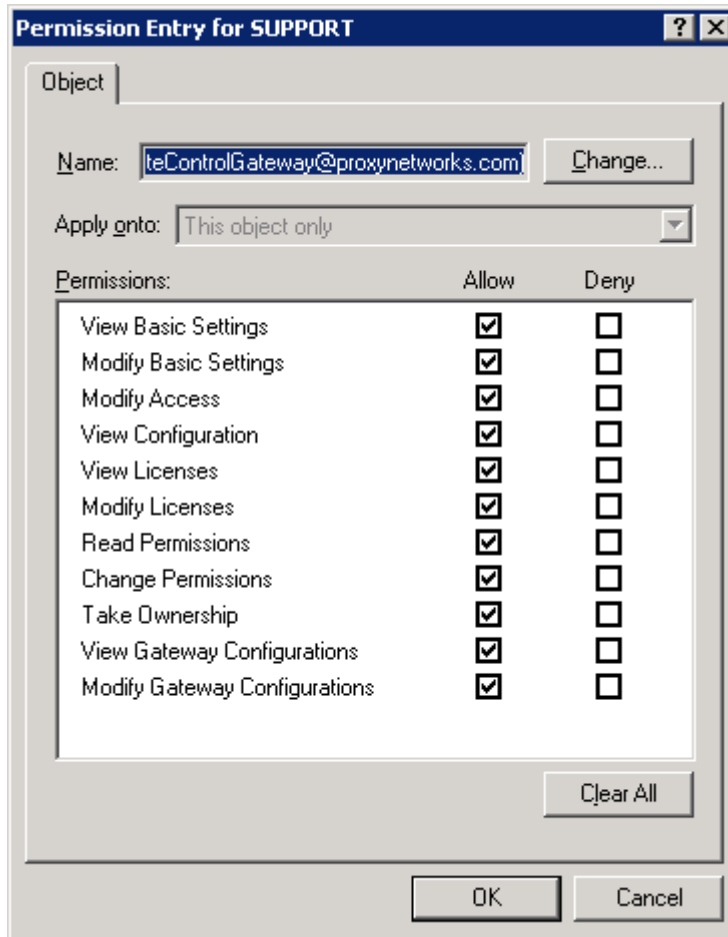
In the **Settings Security** tab, you can perform the following tasks:

- ◆ Click **Add** to add a PC-Duo Master user or group for which you will specify permissions.

- ◆ Select an existing PC-Duo Master user or group that has permissions and click **Remove** to remove it.
- ◆ Select a PC-Duo Master user or group and click **Allow** or **Deny** for the list of **Permissions**, each of is a common grouping of individual permissions. The individual permissions can be seen on the **Advanced** page. The following common groupings exist:
 - ◆ **Full Control/Administration**: Includes every permission in the list.
 - ◆ **Full User/Modify All Settings**: Includes permissions to view and modify all Host-specific settings, but does not include the **Edit Security** permission to change the security configuration.
 - ◆ **View All Settings**: Includes **View Basic Settings**, **View Configuration**, **View Licenses**, **View Gateway Configurations**, and **Read Permissions**; allows all Host settings to be viewed (but not changed).
 - ◆ **Modify Basic Settings**: Grants the **Modify Basic Settings** permission. Determines whether a PC-Duo Master user or a group can modify basic PC-Duo Host settings. This feature does not allow PC-Duo Master users to modify the information displayed on the **Security** tab, the **Access** tab, or the license keys displayed on the **About** tab.
 - ◆ **Edit Security**: Includes permission to change these security rights: read permissions, change permissions, and take ownership.
 - ◆ **Special Permissions**: Indicates a non-standard grouping of permissions not exactly matching one or more of the previously described groups. [See "Permission Entry window - Settings Security"](#).
- ◆ Click **Advanced** to specify permissions and open the **Advanced Security Settings** window.



In the **Permissions** tab of the **Advanced Security Settings** window, select an entry for which you want to assign advanced permissions and click **Edit**. The **Permission Entry** window opens:



Each advanced permission is treated individually; click **Allow** or **Deny** for any of them. The following permissions exist:

- ◆ **View Basic Settings** determines whether a PC-Duo Master user or group can view the basic PC-Duo Host settings.
- ◆ **Modify Basic Settings** determines whether a PC-Duo Master user or group can modify basic PC-Duo Host settings. This feature does not allow PC-Duo Master users to modify the information displayed on the **Security** tab, the **Access** tab, or the license keys displayed on the **About** tab.
- ◆ **Modify Access** determines whether a PC-Duo Master user or group can modify the items on the **Security** and **Access** tabs.
- ◆ **View Configuration** determines whether a PC-Duo Master user or group can read the names and version numbers of the Host components for diagnostic purposes.
- ◆ **View Licenses** determines whether a PC-Duo Master user or group can read the list of installed license keys on the **About** tab.
- ◆ **Modify Licenses** determines whether a PC-Duo Master user or group can add license keys via the **Add License** button on the **About** tab.
- ◆ **Read Permissions** determines whether a PC-Duo Master user or group can view the **Settings Security** tab of the PC-Duo Host **Security Settings** window.

- ◆ **Change Permissions** determines whether a PC-Duo Master user or group can modify permissions on the **Settings Security** tab.
- ◆ **Take Ownership** determines whether a PC-Duo Master user or group can take ownership.
- ◆ **View Gateway Configurations** determines whether a PC-Duo Master user or group can read the settings on the **Gateways** tab.
- ◆ **Modify Gateway Configurations** determines whether a PC-Duo Master user or group can modify the settings on the **Gateways** tab.

Shared secret password authentication

If the Host security is set to Windows Authentication but the Host is not in the same domain as a known PC-Duo Gateway (i.e. a Gateway listed on the **Gateways** tab), Windows Authentication will fail (the Host cannot authenticate PC-Duo Gateway account credentials if domain controller with Active Directory is not accessible).

To get around this problem without requiring any manual configuration management on the Host machine, the PC-Duo Host and PC-Duo Gateway are programmed to automatically establish a 16-byte secret password between each other called a 'shared secret password'. This secret is established behind the scenes when the Host and the known PC-Duo Gateway first communicate with each other, and is unique to each PC-Duo Gateway/Host pair.

NOTE: During this initial connection, the Host implicitly trusts the PC-Duo Gateway because it is on the known Gateways list. For stronger authentication, use SSL to confirm the identity of the PC-Duo Gateway.

On all subsequent connection attempts when the Host and PC-Duo Gateway are not in the same domain, the shared secret password will be presented and accepted for authentication (because it is known only to the Host and PC-Duo Gateway). No configuration change is required and the Host security remains set at Windows Authentication for all other requests.

This authentication method is ideal for the following situations:

- ◆ Host not installed before domain 'RemoteControlGateway' account was created: Previously, this account had to be added manually to the Host security settings (or some other Gateway account had to be created and added to the Host security settings). As long as the PC-Duo Gateway is on the known list of PC-Duo Gateways on the Host's **Gateways** tab, the Host will automatically add that Gateway's PC-Duo Master user account to its security settings list with full access rights. With this autoconfiguration feature, there is no longer any need to manually add the default Gateway user account or to create and configure a new Gateway user account on the Host.
- ◆ PC-Duo Gateway requests a connection and Host security is set to Simple Password: Previously, the Host did not ask for a password from the PC-Duo Gateway. Now, the PC-Duo Gateway will be asked to share a secret password with the Host, and will be required to present it to the Host for a connection request, even with Host security set to Simple Password.

End-to-end authentication

When a Master connects to a Gateway and requests services from a Host, the Gateway connects to (and authenticates to) the Host on the Master's behalf (using the Gateway account). However, for maximum security, there are certain services (such as file

transfer, remote Host administration, and remote management), that require the Master end-user to authenticate directly to the Host.

We refer to this as end-to-end authentication: If the current credentials (i.e. the credentials the Master used to authenticate to the Gateway) do not suffice at the Host, the user will now be prompted to enter another set of credentials (previously these services were not accessible).

The following describes in more detail typical connection scenarios in which end-to-end authentication may be required from the Master:

- If Master connects either peer-to-peer or through a Gateway to a Host configured for simple password authentication, the logged-in console user identity at the Host is the identity used for services that require end-to-end authentication (i.e. the process of simple password authentication is essentially equivalent to end-to-end authentication in this case).

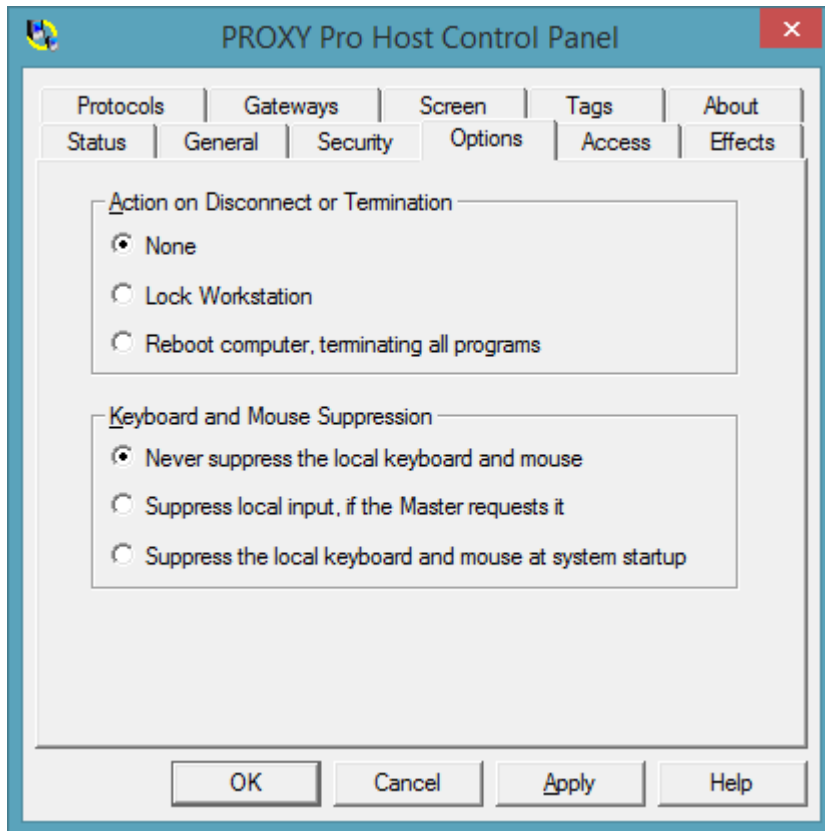
*Note: Remote management and remote Host administration require the user logged into the Host to have local administration rights. Also note that these connections are disallowed if the option **Allow remote administration (peer-to-peer)** is not checked on the **Security** tab in the Host control panel.*

- If Master connects peer-to-peer to a Host configured for Windows Authentication, the Master must authenticate with username and password to the Host, and this identity is used for services that require end-to-end authentication (i.e. peer-to-peer connection requires the Master to authenticate directly to the Host, which is essentially the same as end-to-end authentication).
- If Master connects through a Gateway to a Host configured for Windows Authentication, the Master may be required to present two sets of credentials: First, the credentials that the Master used to authenticate to the Gateway will be presented to the Host. If these credentials are accepted by the Host (which would be the case if the Gateway and the Host are in the same domain), no additional credentials are needed, and end-to-end services will be enabled. If the credentials do not work (perhaps because the Host is not in the same domain as the Gateway), the Master end-user will be prompted to present an alternate set of credentials directly to the Host.

Note: The alternate credentials will be applicable during the lifetime of the Remote Desktop Window to the Host but will not be saved when the Remote Desktop Window is closed.

Options tab

Use the **Options** tab to specify what happens to the keyboard, mouse, and display on your Host computer during a remote control connection.



Three types of options can be configured from the **Options** tab:

- ◆ “Action on Disconnect or Termination”

- ◆ “Keyboard and Mouse suppression”

NOTE: Some of these options render your Host computer unusable by local PC-Duo Master users, but you can override them. For more information, see [“Confirm Host Options Settings”](#).

Action on Disconnect or Termination

A Master user can arrange for certain events to occur after a remote control connection is terminated with this Host:

- ◆ Select **None** for the termination of a Master user connection to have no effect on the Host computer (this is the default setting).
- ◆ Select **Lock Workstation** to lock the Host computer when a Master user connection is terminated. (It can be unlocked or restarted using Windows commands).

- ◆ Select **Reboot computer, terminating all programs** to reboot the Host computer upon the termination of a Master user connection.

NOTE: Starting in PC-Duo v12.7, the default setting will be the more secure: “Lock Workstation” for Hosts running server class operating systems. This pertains to fresh/clean installs only and will not affect upgrades.

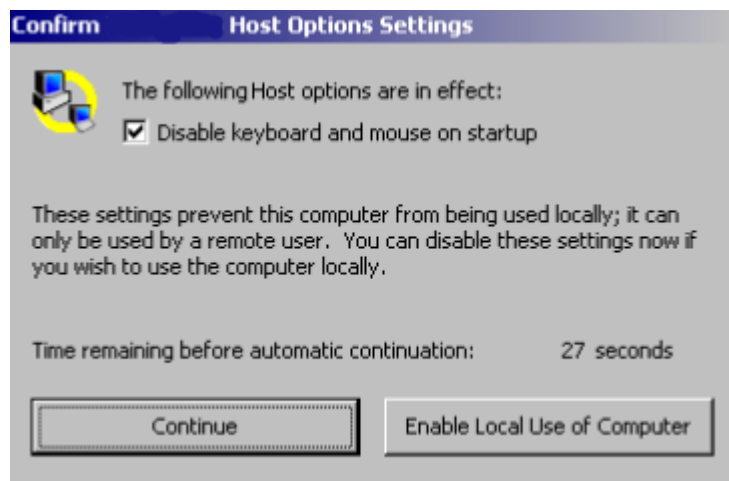
Keyboard and Mouse suppression

The Master user can suppress the keyboard and mouse of your Host computer while he/she is connected to your remote desktop. Following are options that can be set by the Host user to manage local keyboard and mouse suppression during a remote control session:

- ◆ Select **Never suppress the local keyboard and mouse** to retain control of the Host computer's keyboard and mouse when a Master user connects to the Host (this is the default setting).
- ◆ Select **Suppress local input, if the Master requests it** to give a Master user control of the Host computer's keyboard and mouse when the user requests it. The default settings for Host and Master allow the mouse and keyboard to be shared during a connection, with each side able to use both.
- ◆ Select **Suppress the local keyboard and mouse at system startup** to give full control of the Host computer's keyboard and mouse to the Master user who connects to the Host. This option does not permit mouse or keyboard input on the Host computer. If you select this option, you can override it at startup time. For more information, see [“Confirm Host Options Settings”](#).

Confirm Host Options Settings

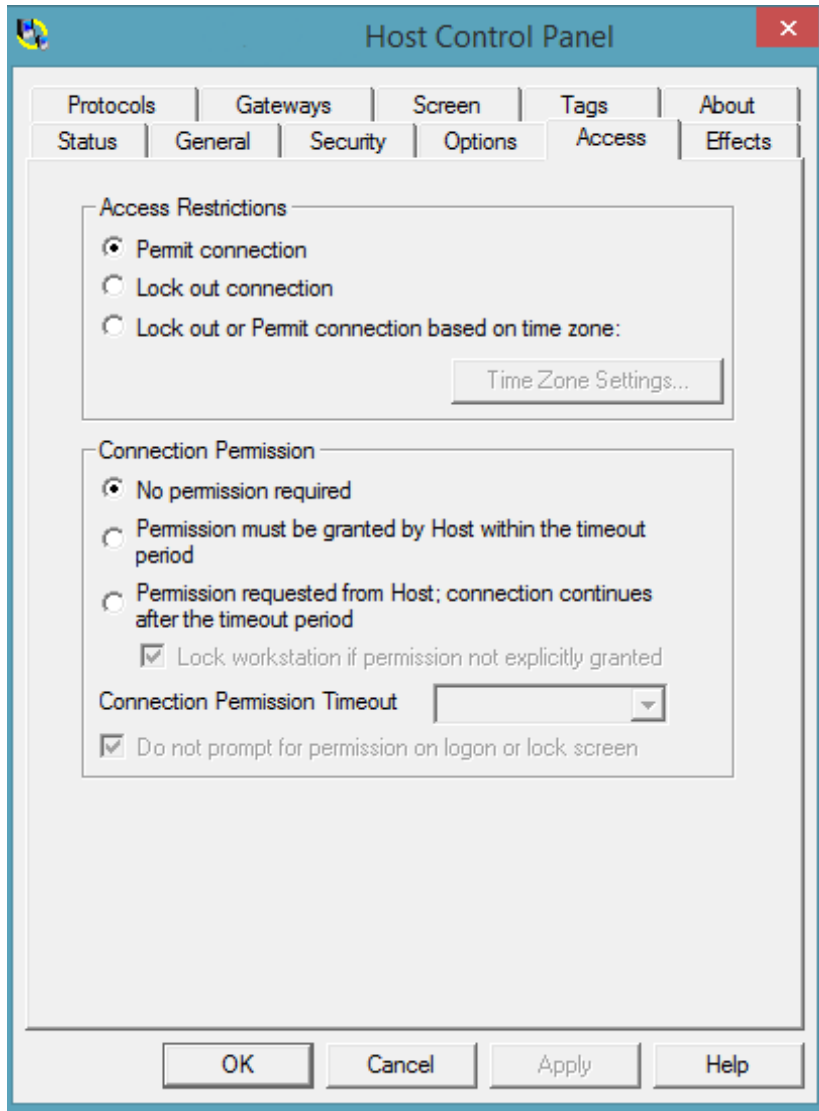
Even if Host is configured to give the Master user control over the keyboard, mouse and display during a remote control connection, the Host user is given the opportunity to override such settings when Master requests access to the desktop:



From the time the **Confirm PC-Duo Host Options Settings** window appears, you have 30 seconds to click **Enable Local Use of Computer**. If you click **Continue**, any preemptive settings configured at Host startup time (see checkbox options) will apply and you may lose local use of the Host computer when the Master user connects.

Access tab

Restrict access and require explicit permission to connect through settings on the **Access** tab.



Restrict access with the following options:

- ◆ **“Access restrictions”**: lock out connections to this Host.
- ◆ **“Connection permission”**: require explicit permission to connect to this Host.
- ◆ **“Services Enabled by Default”**: configure which services this Host offers

NOTE: “Services Enabled by Default” now available for Host on Demand only.

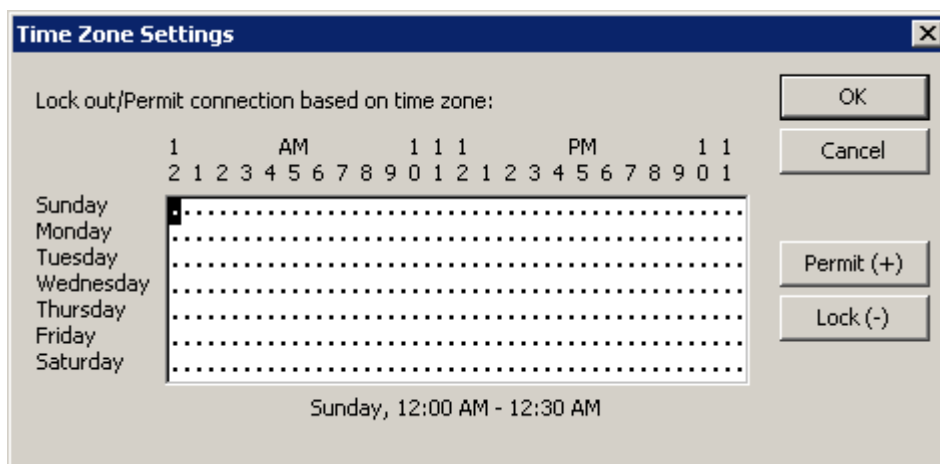
Access restrictions

Lock out access to this Host computer:

- ◆ Select **Permit connection** (default) to permit remote connections from any authenticated PC-Duo Master users to your Host computer.
- ◆ Select **Lock out connection** to prevent remote connections from any PC-Duo Master users to your Host computer.
- ◆ Select **Lock out or Permit connection based on time zone** to permit or prevent remote connections to your Host computer based on the day of the week and the time of day. You can specify permitted access by time when you click **Time Zone Settings**.

Time zone settings

Use the **Time Zone Settings** window to specify the times at which the Host computer is available for remote connections.



The time map is divided into half-hour time slots for each day of the week. Each half-hour time slot is marked with a dot or a blank, as follows:

- ◆ A dot indicates a connection is permitted during a specified half-hour period.
- ◆ A blank indicates a connection is not permitted during that half-hour period.

In this example, remote connections are permitted only from 9:00 AM to 5:00 PM on Monday through Friday.

To edit the time map, follow these steps:

- 1 Select a time period (rectangle) in the time zone map.
- 2 Click **Permit** or **Lock** to specify whether remote connections are permitted during the selected time period. You can also use the arrow keys to navigate to the desired time, and press the **[+]** or **[-]** keys on your keyboard to enable or disable connections for a selected time interval.
- 3 Click **OK** when you are finished

Connection permission

Specify certain conditions that must be met for remote control connections to your Host computer:

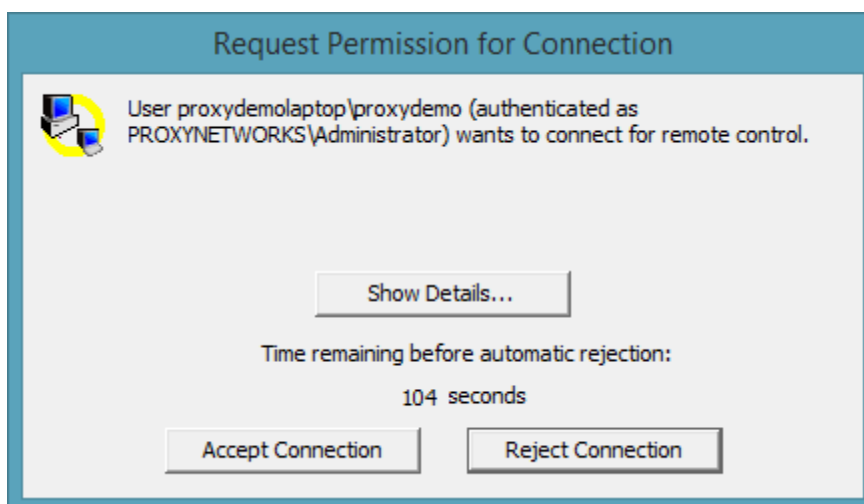
- ◆ Select **No permission required** (default) to allow remote control connections to your Host computer from any authenticated PC-Duo Master user at any time.
- ◆ Select **Permission must be granted by Host** if you want to grant an authenticated PC-Duo Master user explicit permission to connect to your Host computer. From the **Host's user must respond within** drop-down list, select the time (10 seconds, 30 seconds, 1 minute, or 2 minutes) within which you want to make a decision. If you do not respond within the specified time, the request is rejected automatically.
- ◆ Select **Permission requested from Host** if you want to grant an authenticated PC-Duo Master user explicit permission to connect to your Host computer but you don't want it to be mandatory. If you do not respond within the specified time, the request is accepted automatically.

NOTE: These conditions apply to both peer-to-peer and Gateway-managed connections.

- ◆ Select **Do not prompt for permission on logon or lock screen** to automatically accept the connection without user interaction if the Host console is at the Windows logon screen or lock screen. In this case, it is likely that there is no user at the console to accept the connection, and Windows will require the remote control user to login or unlock the console.

Permission for connection

If **Permission must be granted by Host** or **Permission requested from Host** is selected in the **Access** tab, the Request Permission Connection window appears when a PC-Duo Master user attempts to connect to your Host computer.



If Connection Permission is set to **Permission must be granted by Host**, then the PC-Duo Host user must respond within the time period or the connection request will be rejected.

Even if one of these two options is selected in the **Access** tab, the Request Permission for Connection window can be suppressed on the Host if the **Bypass Connection Permission** option is selected in the Permission Entry window under Advanced Security Settings (see [“Service Security tab”](#)).

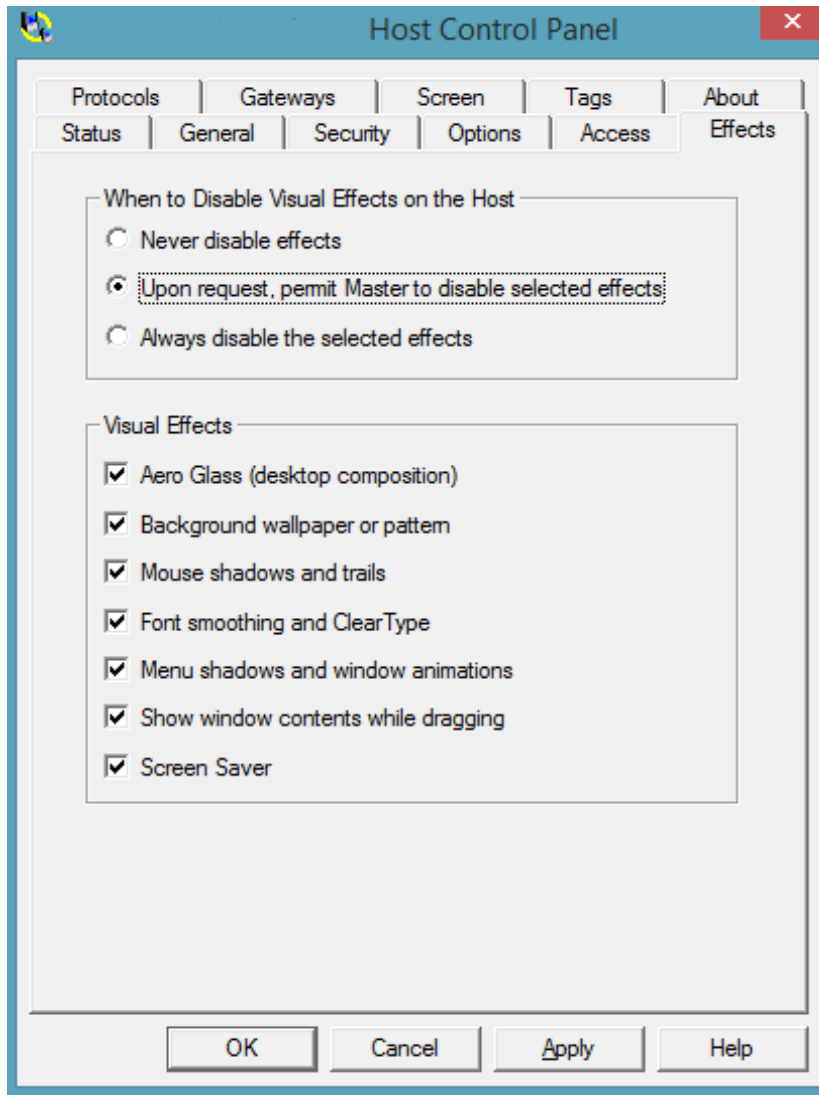
If **Lock workstation if permission not explicitly granted** is selected (default = enabled), the Host will lock the workstation prior to beginning the new remote control connection. This prevents the new user from "hijacking" the logged-in user's session unless he/she knows the credentials to unlock it.

Services Enabled by Default

Specify which services the Host enables for use by remote control users. Services that are not enabled cannot be accessed. These defaults apply for connections that do not request connection permission; the defaults can be changed by the console user in the permission for connection dialog.

Effects tab

Graphical effects on the Host screen during remote control connections can be configured through settings on the **Effects** tab. By disabling visual effects, for example, the amount of screen data that is captured and transmitted over the network can be greatly reduced, improving speed and performance.



Choose one of three options to determine whether or not visual effects should be disabled:

- ◆ Enable visual effects on the Host computer: Select **Never disable effects** to keep current visual effects settings on the Host in place.
- ◆ Allow PC-Duo Master user to disable some or all visual effects on the Host computer: Select **Upon request, permit Master to disable selected effects** (this is default option). Check any options under **Visual Effects** which you want PC-Duo Master user to have control over.
- ◆ Disable some or all visual effects on the Host computer whenever a remote control connection is made: Select **Always disable the selected effects**. Check any options under **Visual Effects** which you want PC-Duo Master user to have control over.

The particular visual effects that are enabled or disabled are controlled by the settings checked under **Visual Effects**:

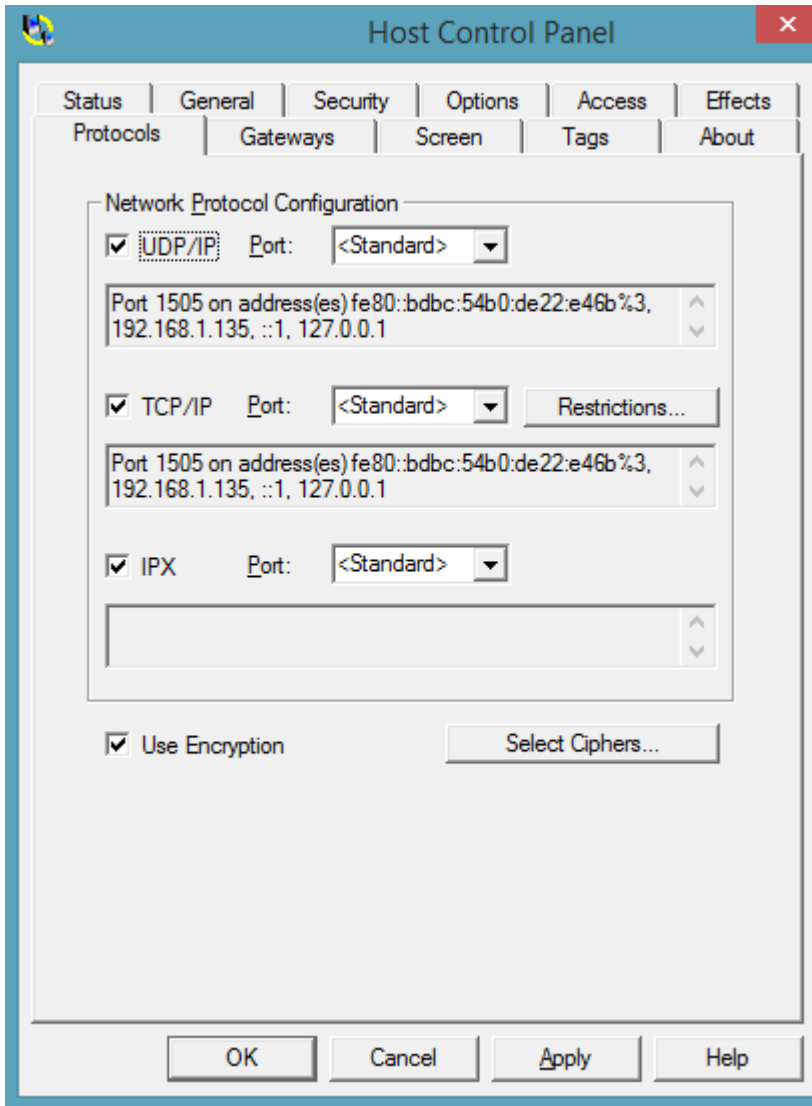
- ◆ Aero Glass (desktop composition)

- ◆ Background wallpaper or pattern
- ◆ Mouse shadows and trails
- ◆ Font smoothing and ClearType
- ◆ Menu shadows and window animations
- ◆ Show window contents while dragging
- ◆ Screen Saver

NOTE: *Aero Glass will be activated on Windows Vista and later platforms*

Protocols tab

Configure the network protocols and ports for communication with PC-Duo Host in the **Protocols** tab.



The **UDP/IP**, **TCP/IP**, and **IPX** check boxes enable/disable the network protocols that can be used for peer-to-peer or Gateway-managed connections to the Host.

To the right of each check box is a **Port** list. Use the **Port** list to select **<Standard>** or enter the specific port number on which the Host computer should listen for each enabled protocol. By default, the standard port for UDP and TCP is 1505.

NOTE: PC-Duo Host listens on all addresses. Even addresses that do not appear on the **Protocols** tab are monitored and can be used for communication.

Access from specific IP addresses or from a range of IP addresses can be explicitly blocked (see "[TCP/IP address restrictions](#)").

If you check **Use Encryption**, data exchanged over remote control connections are protected with an encryption algorithm negotiated with the client (see the [“Selecting ciphers”](#) for more information about encryption).

NOTE: *PC-Duo Host can be installed on a computer that is also running PC-Duo Gateway. Both programs can have the IP protocol enabled, because they use different UDP ports (Host uses 1505, Gateway uses 2303). However, the two programs must compete for a single IPX port. Either disable (uncheck) IPX on the Protocols tab of PC-Duo Host, or choose an alternate port (other than **Standard**) for IPX in either the PC-Duo Host or PC-Duo Gateway.*

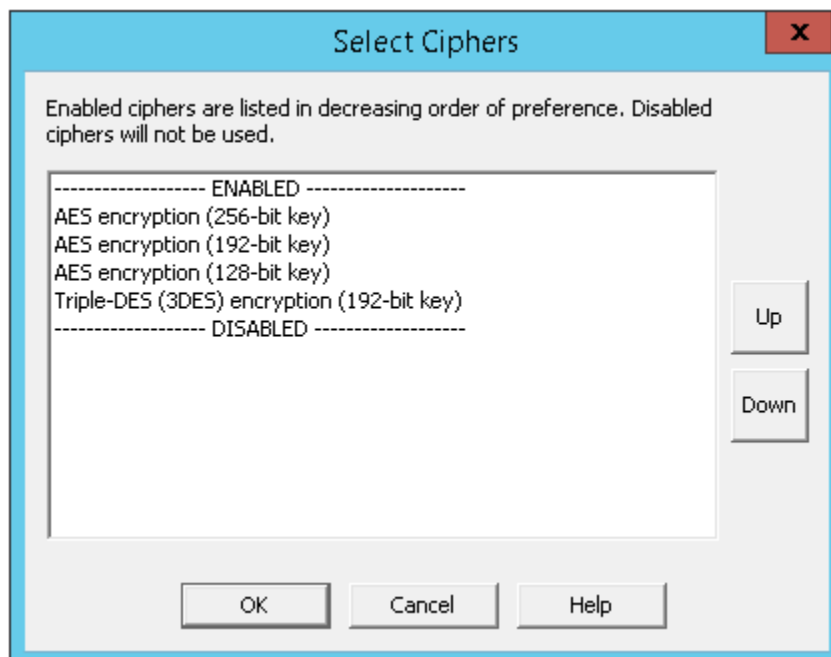
Select ciphers

When PC-Duo Master or PC-Duo Gateway requests a connection to PC-Duo Host, the two applications negotiate to determine the highest level of encryption that is supported by both. For example, PC-Duo Master 11.1 will try to use AES 256-bit encryption by default but a PC-Duo Host 11.0 might be configured to use Triple-DES; in that case, the two applications will agree to use Triple DES).

NOTE: *Older PC-Duo Host versions up to 10.0 support only RC4. Newer versions starting with 11.0 support Triple-DES and AES.*

The **Select Ciphers** window lists the encryption ciphers that are supported by the Host in decreasing order of preference. In the default configuration, this order always begins with AES encryption with 256-bit keys.

Specific configurations can be disabled by moving them below the “DISABLED” line; in that case, they will never be considered by the Host:

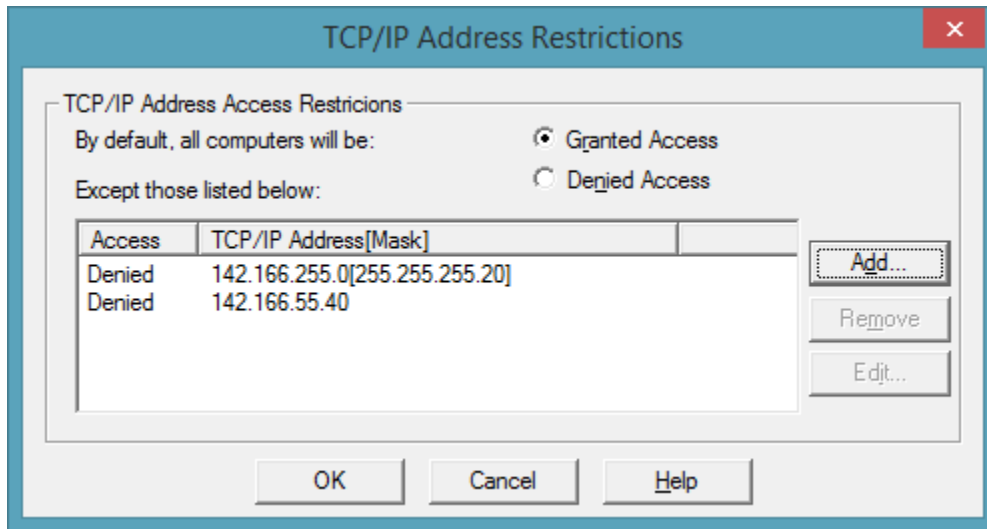


◆ To enable a cipher option, select it from the **DISABLED** list and move it to the **ENABLED** list by clicking **Up**.

- ◆ To disable a cipher option, select it from the **ENABLED** list and move it to the **DISABLED** list by clicking **Down**.
- ◆ Click **OK**.

TCP/IP address restrictions

Access to the PC-Duo Host over TCP can be restricted according to the IP address of the Gateway or PC-Duo Master trying to connect with it. Press **Restrictions** to specify a policy for granting Host computer access according to IP address:



Grant or deny access by default and then specify a list of exceptions according to specific IP address. This policy, along with the exceptions, is applied before any authentication security rules you configure in the Security tab.

Configure the policy as follows:

- ◆ Select **Granted Access** to grant remote access to your Host computer via the TCP/IP protocol to all except the IP addresses in the list.
- ◆ Select **Denied Access** to deny remote access to your Host computer via the TCP/IP protocol to all except the IP addresses in the list.

Add, edit, or remove addresses from the exception list as follows:

- ◆ To add an exception to your TCP/IP restriction policy, click **Add** in the **TCP/IP Address Restrictions** window. Enter an IP address, subnet address, or range of IP addresses in the list.

Deny Access On

Type:

- ☒ Single Computer (at one IPv4 address)
- ☐ Group of computers (by IPv4 subnet mask)
- ☐ Group of computers (by IPv4 start address & count)
- ☐ Single Computer (at one IPv6 address)
- ☐ Group of computers (by IPv6 subnet mask)

Address:

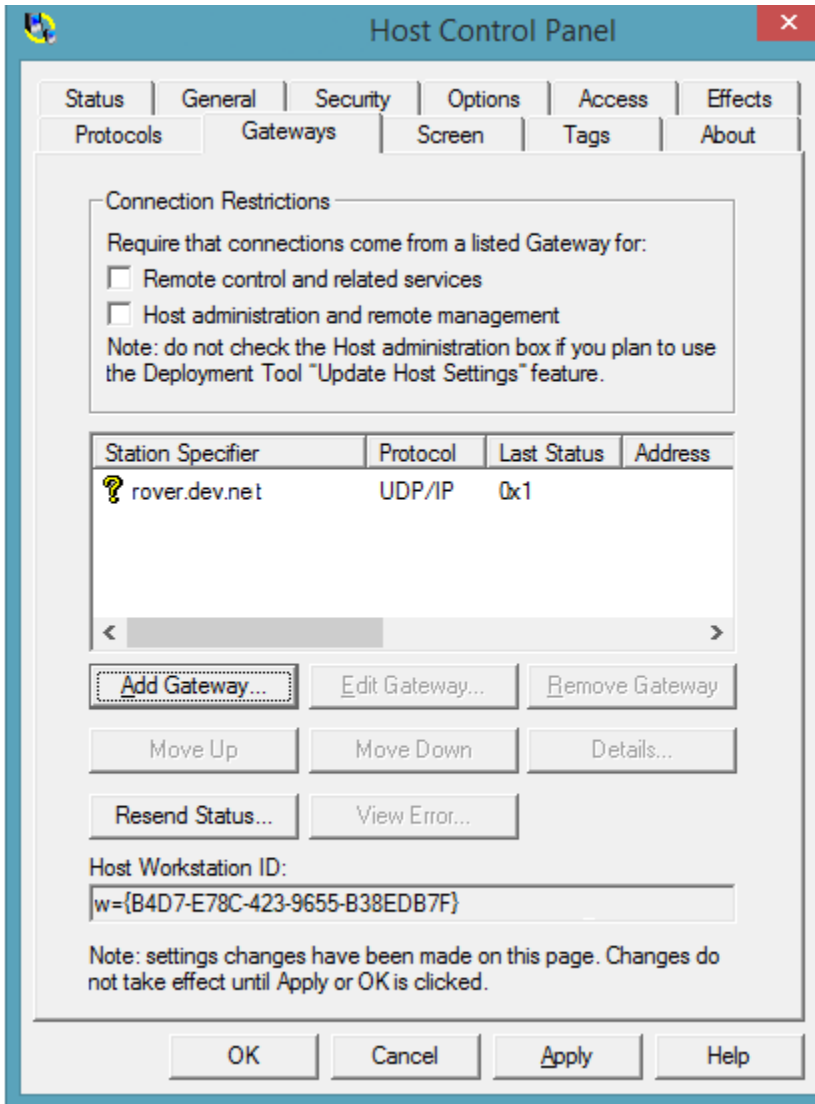
OK Cancel Help

There are five options available:

- ◆ Select **Single Computer (at one IPv4 address)** and enter an IP address in the **Address** field.
- ◆ Select **Group of computers (by IPv4 subnet mask)** and enter the appropriate values into **Address** and **Mask**.
- ◆ Select **Group of computers (by IPv4 start address & count)**, enter the first address in a range in the **Address** field, and enter the number of addresses in the range in the **Number of addresses** field.
- ◆ Select **Single Computer (at one IPv6 address)** and enter an IP address in the **Address** field.
- ◆ Select **Group of computers (by IPv6 subnet mask)** and enter the appropriate values into **Address** and **Mask**.
- ◆ To edit a listed exception to your TCP/IP restriction policy, select an entry from the list of exceptions, and click **Edit** in **TCP/IP Address Restrictions**. Modify any items for that entry and click **OK**.
- ◆ To remove a listed exception to your TCP/IP restriction policy, select an entry from the list of exceptions, and click **Remove** in **TCP/IP Address Restrictions**.

Gateways tab

PC-Duo Hosts can be configured to report to one or more PC-Duo Gateways.



For security purposes, all connection attempts can be forced to go through the specified Gateways by selecting the appropriate Connection Restrictions. Select Remote control and related services to require remote control (including viewing the screen and input control), file transfer, remote printing, clipboard transfer, and chat connections to come through a Gateway listed on the Gateways tab. Select Host administration and remote management to require remote Host administration and remote management connections to come through a Gateway listed on the Gateways tab. With these option, administrators can take advantage of Gateway-based security policies and prevent unauthorized connections via peer-to-peer or unlisted Gateways.

Note that the Deployment Tool “Update Host Settings” feature makes a peer-to-peer (non-Gateway based) connection to the Host, so checking the Host administration checkbox prevents that feature from being used.

The list of valid Gateways to which the Host should report can be managed with the following options:

- ◆ “Add Gateway”
- ◆ “Edit Gateway”
- ◆ “Remove Gateway”
- ◆ “Move Up”
- ◆ “Move Down”
- ◆ “Details”
- ◆ “Resend Status”
- ◆ “View Error”

The **Host Workstation ID** is a unique identifier generated at installation time, which PC-Duo Gateway uses for reporting and reference purposes.

Manage Gateway order

The ability to control the order of the Gateway list allows the PC-Duo Master user to control the order in which connections are attempted. The Host will automatically go down the list in order to establish a connection and report to a PC-Duo Gateway. If a connection attempt fails, the Host will automatically move to the next entry in the list; if a connection attempt succeeds, the Host will ignore all other entries in the list to that same PC-Duo Gateway and will proceed to the next PC-Duo Gateway entry.

Since connection attempts occur automatically (and without notice to the PC-Duo Master user) and failures can take up to 30 seconds, it may be preferable to list the PC-Duo Gateway connections most likely to be available at the top of the list.

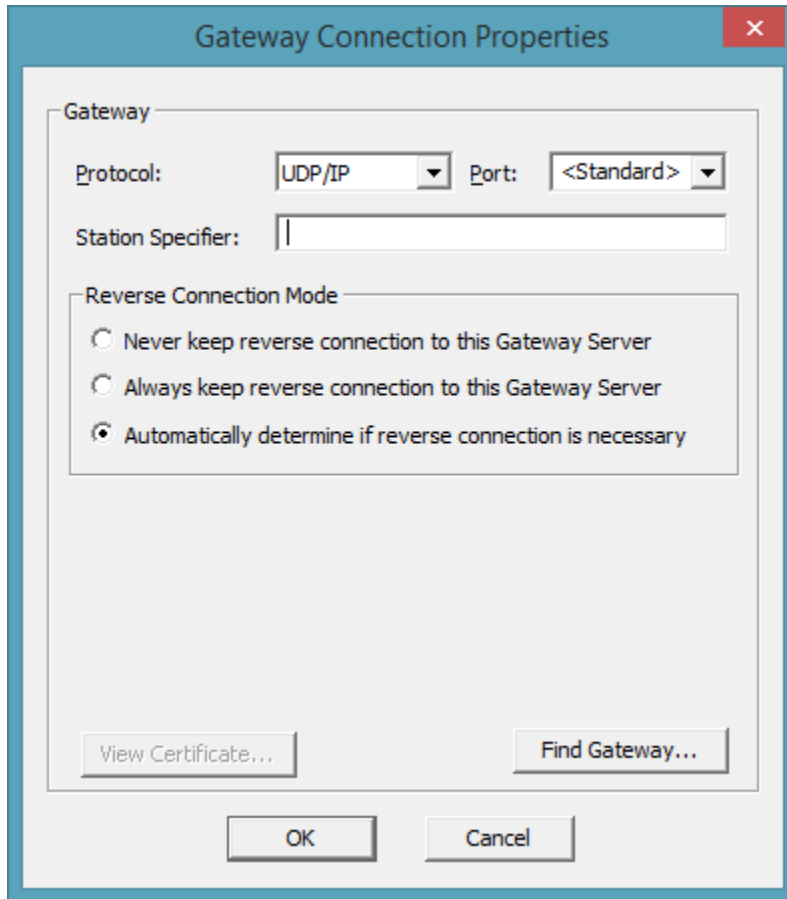
For example, a typical PC-Duo Gateway may have two entries in the **Gateway** tab: One with the internal IP address or DNS name when the Host is in the same domain (regular connection), and another with the external IP address or DNS name when the Host is outside the domain (reverse connection).

If a Host computer (for example, a laptop) is routinely moved in and out of the domain with the PC-Duo Gateway (for example, from office to home and back), you may want to list the address which is used more often ahead of the one that is used less often.

Add Gateway

PC-Duo Host reports status information to each PC-Duo Gateway listed on the **Gateways** tab. To add a PC-Duo Gateway to the list, follow these steps:

- 1 Click **Add Gateway**. The **Gateway Connection Properties** window appears.



◆ If you do not know the station name and/or address of the PC-Duo Gateway to which you want to connect, click **Find Gateway**. The **Find Gateway Wizard** appears. Follow the instructions on the wizard and click **Finish** when you are done.

◆ If you know the station name and/or address of the PC-Duo Gateway to which you want to connect, follow these steps:

- i Select the protocol to use from this list.
- ii Specify the port number if it is not standard (default standard port is 2303).
- iii Type the DNS name, PC-Duo Gateway name or network IP address in the Station Specifier field. See [“PHSETUP Gateways parameters”](#) for more information on the protocol-specific syntax for station specifiers.
- iv If you are trying to reach a PC-Duo Gateway outside the PC-Duo Gateway network, make sure that either option (2) or (3) below is selected so that a firewall-friendly reverse connection with the Host can be established:

- (1) **Never keep reverse connection to this Gateway server.** Select this option when the Host and PC-Duo Gateway are on the same LAN and the PC-Duo Gateway can easily establish a remote control connection to the Host when necessary.
- (2) **Always keep an reverse connection to this Gateway server.** Select this option when the Host is not easily accessible to the PC-Duo Gateway, e.g. is behind a firewall and/or router with a Net Address Translation (NAT) table. The Host will use a reverse connection to maintain communication with the PC-Duo Gateway. By

having the Host establish a reverse connection to the PC-Duo Gateway, the PC-Duo Gateway can always talk back over that connection to the Host and use it to deliver other services such as remote control, file transfer, etc. The potential downside of always maintaining the reverse connection is the overhead necessary to maintain these persistent connections. When multiple hosts are involved this overhead can add up to an unacceptable level for some LANs.

(3) **Automatically determine if reverse connection is necessary.** Select this option (default) to cause the Host to figure out if it needs a reverse connection to communicate with the PC-Duo Gateway based upon its IP address.






NOTE: Option (3) is the default when adding a new Gateway, and is the recommended option.

- 2 Click **OK** when you are done.

PC-Duo Gateway configuration status

In the **Gateways** tab, next to the Station Specifier of each PC-Duo Gateway you attempt to add, a status symbol will appear. Following is a list of possible status symbols and their meaning:

PC-Duo Gateway configuration status symbols

Status Symbol	Gateway Configuration Status
	Status OK, relationship to Gateway is OK, reverse connection established
	Status OK, relationship to Gateway is OK
	Status unknown, possibly waiting for 'Resend'
	SSL certificate error; select entry and click 'View Error' for more information
	Error condition; see error code for more information

Edit Gateway

To edit the connection settings (protocol, port, or address) for any PC-Duo Gateway, follow these steps:

- 1 Select any PC-Duo Gateway listed on the **Gateways** tab.
- 2 Click **Edit Gateway**. The **Gateway Connection Properties** window appears.
- 3 Modify the information as you require, and click **OK**.

Remove Gateway

To remove any listed PC-Duo Gateway, follow these steps:

- 1 Select any PC-Duo Gateway listed on the **Gateways** tab.
- 2 Click **Remove Gateway** on the **Gateways** tab.

Move Up

To move a specific Gateway up on list of Gateways, follow these steps:

- 1 Select any Gateway listed on the **Gateways tab**.
- 2 Click **Move Up** on the **Gateways tab**.

For more information about the significance of the order of listed Gateways, see [Manage Gateway order](#).

Move Down

To move a specific Gateway down on list of Gateways, follow these steps:

- 1 Select any PC-Duo Gateway listed on the **Gateways tab**.
- 2 Click **Move Down** on the **Gateways tab**.




For more information about the significance of the order of listed Gateways, see [Manage Gateway order](#).

Details

To obtain the details of any listed Gateway, follow these steps:

- 1 Select the Gateway from the list on the **Gateways tab**.
- 2 Click **Details** on the **Gateways tab**.

Resend Status

Resend Status causes the Host to recheck the connection status for all the Gateways. Gateways that are available will show either  or ; those not available will show .

To resend status for the list of Gateways, follow this step:

- 1 Click **Resend Status** on the **Gateways tab**.

View Error

View Errors causes the Host to display a report showing SSL certificate errors.

To view the error details of an unsuccessful SSL connection attempt, follow this step:

- 1 Click **View Errors** on the **Gateways tab**

The following response options will be available:

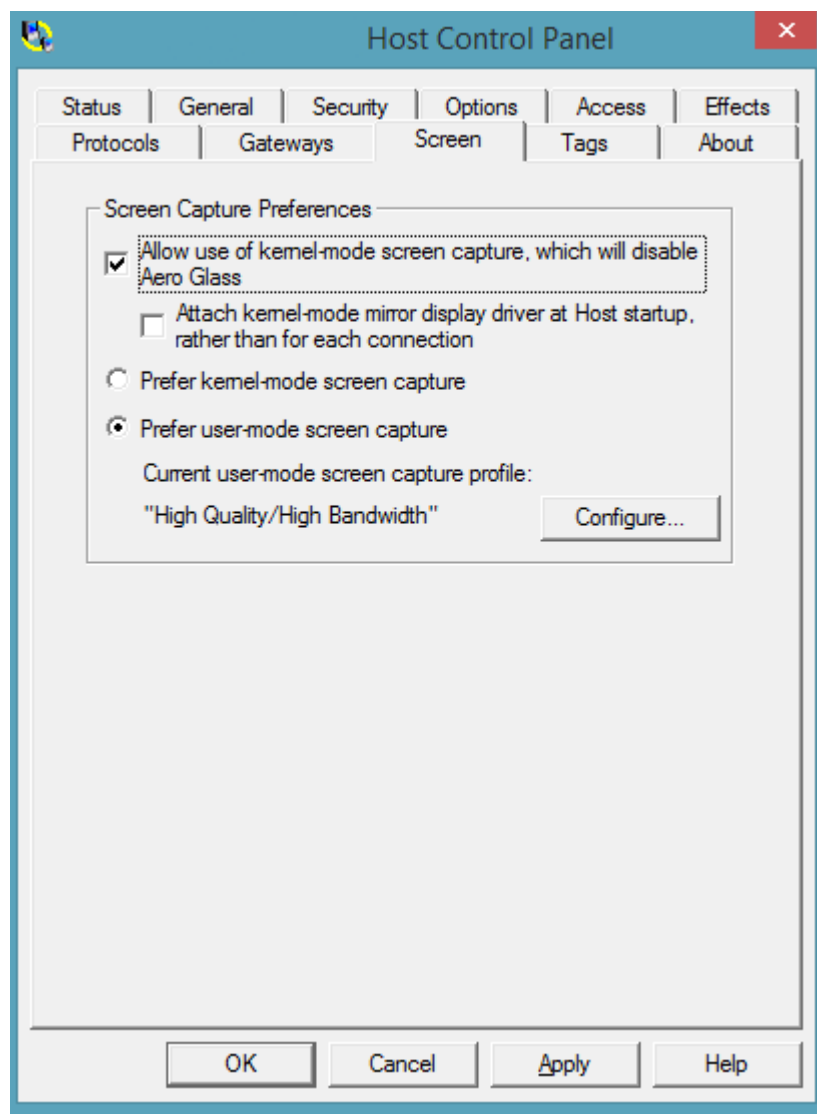
- ◆ **Reject:** Cause Host to reject connection attempt because of SSL errors
- ◆ **Accept with Errors:** Cause Host to ignore errors related to this SSL certificate and accept connection
- ◆ **Accept Any:** Cause Host to always accept all connection attempts, regardless of SSL errors

Screen tab

PC-Duo includes two different types of screen capture technology: Kernel-mode and user-mode.

Kernel-mode Screen Capture

The kernel-mode screen capture driver is a mirror driver that can be used to capture the remote desktop for Windows 7, Vista, Windows 2008 Server and older platforms. By default, the Host will be configured to use user-mode screen capture driver, so the user will have to explicitly choose the kernel-mode screen capture driver on the **Screen** tab in the Host Control Panel by clicking the radio button next to **Prefer kernel-mode screen capture**.



The checkbox for **Allow use of kernel-mode screen capture, which will disable Aero Glass** will also be checked, indicating that the kernel-mode screen capture driver will always be used on this Host. Note also that the use of the kernel-mode screen capture driver will result in Aero Glass effects being disabled on Hosts running Windows 7.

The user can further specify that the kernel-mode screen capture driver be preloaded at Host startup time by clicking on the checkbox next to **Attach kernel-mode mirror display driver at Host startup**; otherwise, the mirror driver will be attached and unattached with each connection to the Host, which may be disruptive for the user.

User-mode Screen Capture

The user-mode screen capture driver is the default option to capture the remote desktop for all supported platforms. It runs as 32-bit x86 user mode code, but can capture either x86 or x64 systems, and is the only supported screen capture technology for Remote Desktop Services sessions.

*Note: The user can check the **Allow use of kernel-mode screen capture, which will disable Aero Glass** option with the user-mode screen capture driver. By checking this option, the user allows Gateway connections to use kernel-mode screen capture. This might be useful for making screen recordings while a different user has remote access to the desktop.*

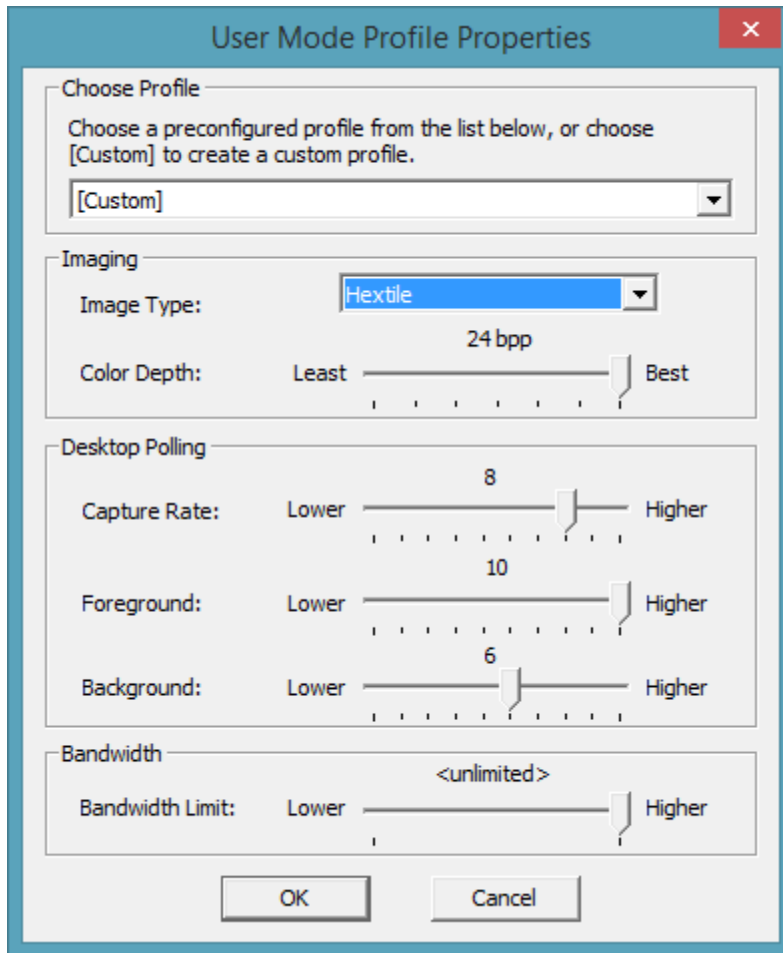
When user-mode screen capture is selected, the amount of bandwidth used to capture and transmit remote desktop screen can be restricted or "throttled" by reconfiguring a user-mode screen capture profile. The default profile is "High Quality/High Bandwidth" but other profiles corresponding to smaller bandwidth limits are available. See "[Bandwidth throttling](#)" for more information.

The Screen tab indicates which user-mode screen capture profile is applicable.

Bandwidth throttling

The user-mode screen capture technology has the ability to "throttle" itself to a restricted amount of bandwidth. This may be preferable when responsiveness and throughput are more important than screen quality, particularly over low-bandwidth connections.

The amount of throttling is controlled by parameters set in a "user-mode screen capture profile". The "**Configure...**" button on the Screen tab brings up a dialog that allows the end-user to select a hard-coded, predefined configuration, or to specify a custom configuration.



The dialog box is titled "User Mode Profile Properties" and contains the following sections:

- Choose Profile:** A text box with the instruction "Choose a preconfigured profile from the list below, or choose [Custom] to create a custom profile." Below it is a dropdown menu currently showing "[Custom]".
- Imaging:**
 - Image Type:** A dropdown menu currently showing "Hextile".
 - Color Depth:** A slider between "Least" and "Best" with a value of "24 bpp" displayed above it.
- Desktop Polling:**
 - Capture Rate:** A slider between "Lower" and "Higher" with a value of "8" displayed above it.
 - Foreground:** A slider between "Lower" and "Higher" with a value of "10" displayed above it.
 - Background:** A slider between "Lower" and "Higher" with a value of "6" displayed above it.
- Bandwidth:**
 - Bandwidth Limit:** A slider between "Lower" and "Higher" with a value of "<unlimited>" displayed above it.

At the bottom are "OK" and "Cancel" buttons.

Each profile consists of the following information:

- ◆ Description string
- ◆ Image type (two choices -- Hextile (default), or JPEG). The Host will automatically use JPEG compression if the connected Master doesn't support Hextile. For Hextile encoding, the 'image compression quality' value is not used because Hextile is a lossless compression.
- ◆ Image compression quality (numeric value 1-100, with 100 being best quality)
- ◆ Polling frequencies (three values -- Capture Rate, Foreground, and Background, in milliseconds). Note however that the UI will display these values on a scale of 1 to 10, with 1 being the least aggressive (longest time), and 10 being the most aggressive (shortest time). The underlying API and settings storage will have the raw millisecond values.
- ◆ Bandwidth limit (numeric value 5-200 kilobytes/sec, for -1 for unlimited)

The Host settings are preconfigured with the following four profiles:

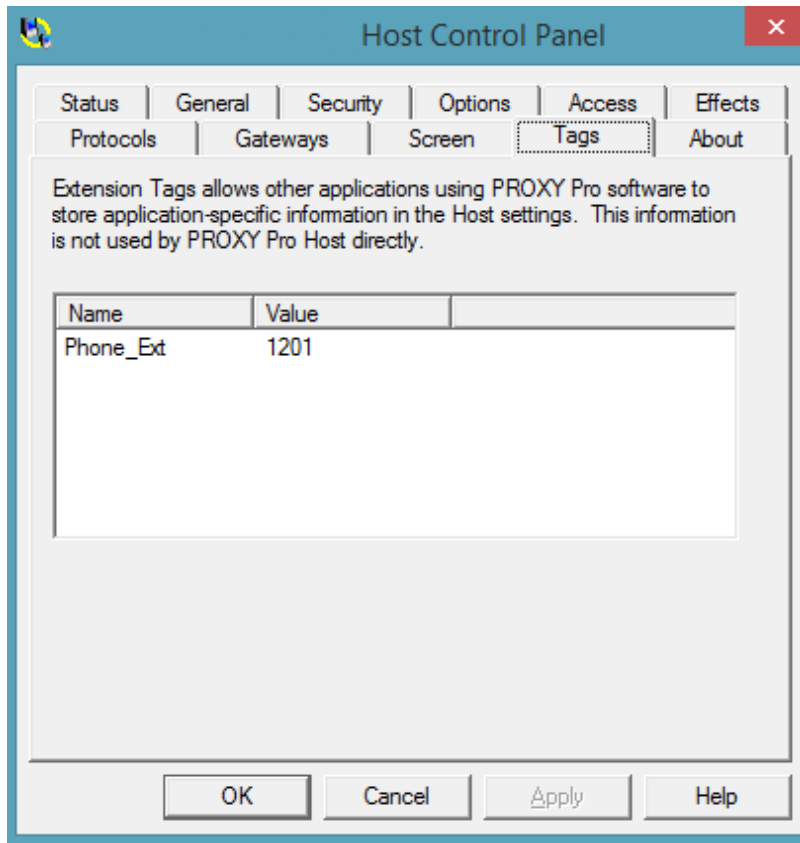
Profile Settings	High	Medium	Medium Low	Low
Description	High Quality	Medium	Medium-Low (recording)	Low (recording)
Image Type	Hextile	Hextile	Hextile	Hextile
Compression Quality	100	100	100	100
Polling Frequency	9/8/6	7/6/4	4/5/4	2/2/2
Bandwidth Limit	Unlimited	100 Kbyte/sec	60 Kbyte/sec	30 Kbyte/sec

The Medium-Low and Low profiles are appropriate for high volume screen recording environments, when screen quality can be traded off for lower screen capture rates, smaller screen recording file sizes and restricted bandwidth usage.

You can create your own custom profile by selecting **[Custom]** from the drop-down list and specifying your desired parameters.

Tags tab

Administrators and/or 3rd party application providers can define one or more name/value pairs to specify custom information for one or more Hosts. When applied, this information will appear in the **Tags** tab of the Host Control Panel. Each name is limited to 128 characters, and each corresponding value is limited to 1024 characters.

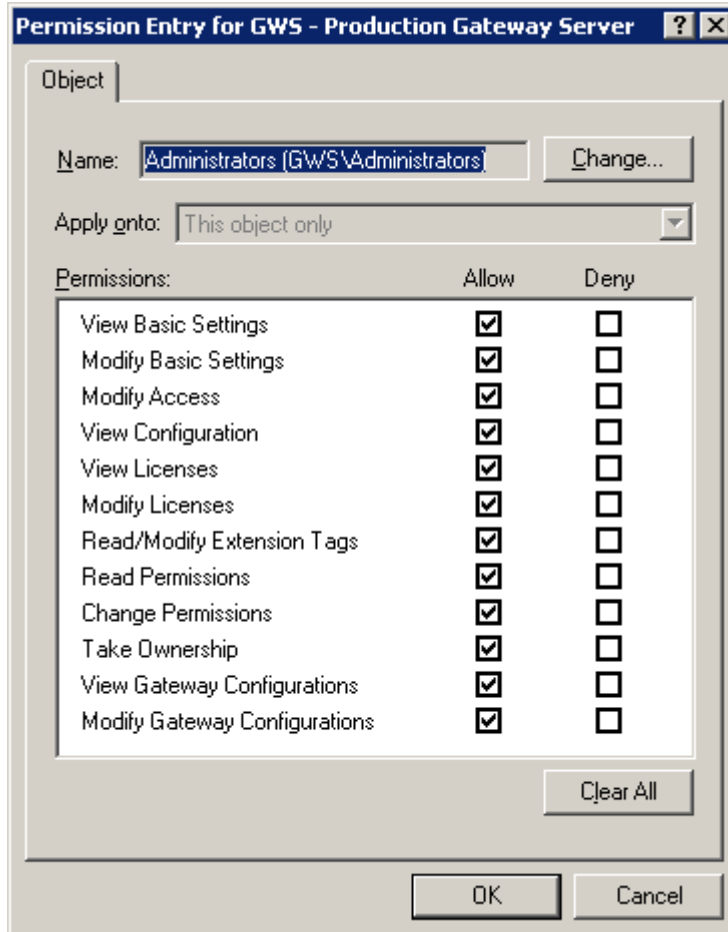


Extension tags can be managed in one of two ways: 1) PC-Duo Deployment Tool or 2) PhSetup command

- The PC-Duo Deployment Tool includes a setting to the Host configuration that allows a list of name/value pairs to be set and configured at the Host. Note that the "Extension Tags" entry in the Host configuration is under the "General" class. Also note that the Deployment Tool does not support having a double-quote character (") appear in the value of a tag, although PhSetup and the Host itself do not have this limitation.
- The PhSetup command line program includes the following keywords to manage the tags:
 - "addtag:name,value" adds a tag with "name" and "value"
 - "removetag:name" removes a tag with the name matching "name"
 - "removetag:*" removes all tags

Tag Security Considerations

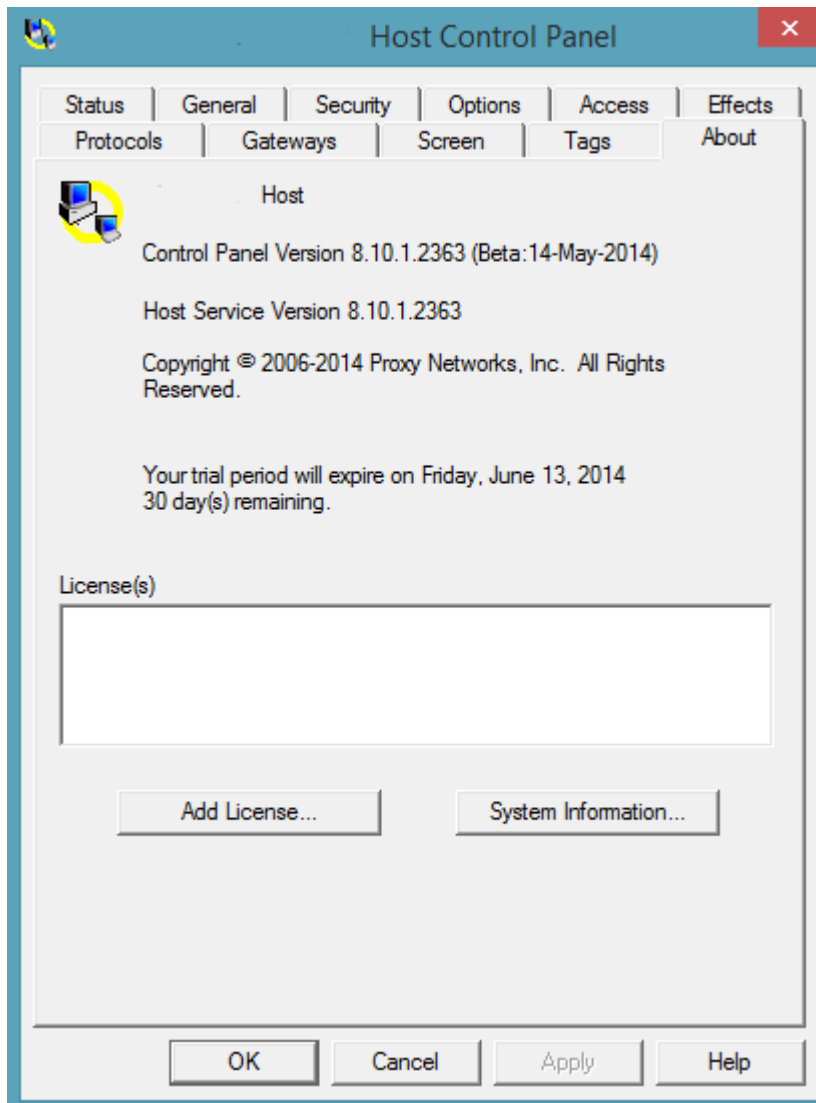
The **Host Settings** security tab includes a new item for managing access to the extension tags: Read/Modify Extension Tags.



This permission will be granted to any users with “full user” (or “full control”), and also to the default Interactive user profile. This will allow an interactive program to access this information.

About tab

View product and license key information in the **About** tab



NOTE: To configure a Host to support one or more Remote Desktop Services sessions, the Host must have a special Remote Desktop Services license key. This key will enable the RDS tab in the Host Control Panel and will enable the Host to support a specified number of RDS sessions simultaneously.

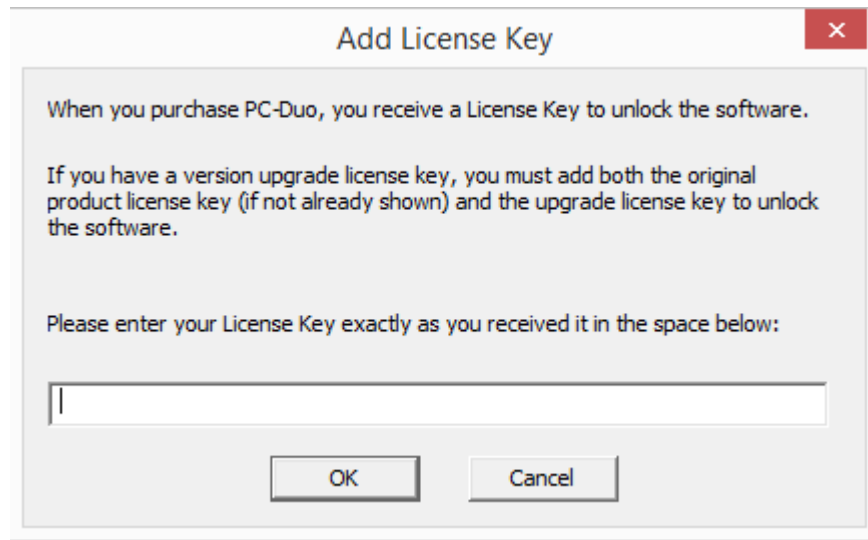
The following administrative actions are supported here:

- ◆ “Add a license key”
- ◆ “Generate a System Information report”

Add a license key

To add a license key to the **License(s)** list, follow these steps:

- 1 Click **Add License**. The **Add License Key** window appears.



- 2 Enter a license key in the field provided.
- 3 Click **OK**.

Generate a System Information report

For auditing and technical support purposes, PC-Duo Host includes a utility to generate a dump file of configuration information about the Host computer. Click **System Information** on the About tab create this detailed report.

The system information report is automatically generated and saved as a plain text file on your desktop. The name of the text file is derived from your computer name and ends with `_Config.txt`.

```

LAPTOP-C_Config.txt - Notepad
File Edit Format View Help
#####
System Information Report
#####

=====
Machine Identification
=====

-----
General
-----

Computer Name..... LAPTOP-C
User Name..... ACME\george
System Directory..... C:\WINDOWS\System32
Window Directory..... C:\WINDOWS
Proxy Host workstation Id.... {CCE1E015-00A6-0000-B9C4-D

```

Host License Key types

Below is a list of valid Host license key types and their prefixes:

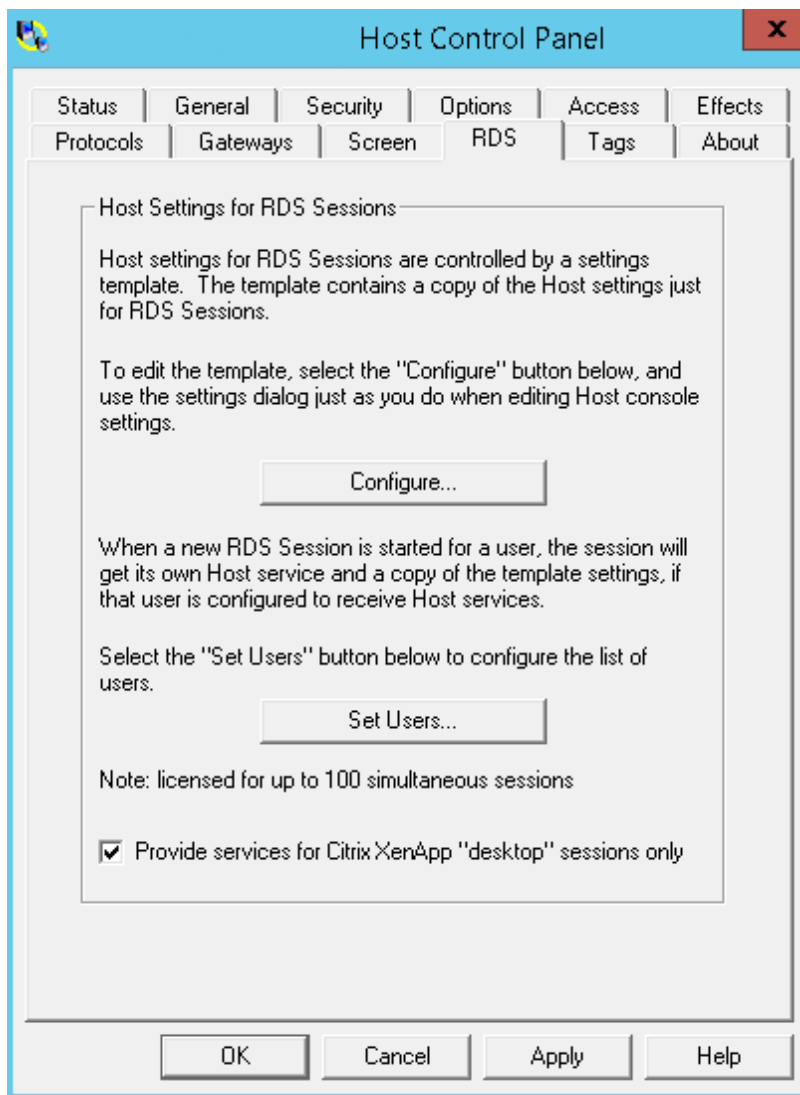
Host License Key Types	Description
Host (Prefix: 411, 412, 413)	<ul style="list-style-type: none"> • Permanently installed Host • Accessible by Peer-to-peer and Gateway-managed connections • Hosts that are automatically or manually moved to All Hosts group on Gateway will be counted under the Managed Host license mode
Host for RDS (Prefix: 414)	<ul style="list-style-type: none"> • Transforms a regular Host into a special version that can be installed/run on a Remote Desktop Services server, where it will generate Host images to be injected into new RDS sessions created • These RDS Host images will appear as transient Hosts • Accessible only by Gateway-managed connections • RDS Hosts are automatically added to All Hosts and the Remote Desktop Services groups, and will be counted as concurrent RDS sessions under the Managed Hosts license mode <p>Note: When this key is added to the regular Host, the Host service must be restarted; the RDS tab to configure settings for the RDS Host sessions, including which Gateway to report to, will then be enabled in the Host Control Panel.</p>
VDI Host (Prefix: 416)	<ul style="list-style-type: none"> • Transforms a regular Host into a special version that can be configured as part of a virtual desktop template and will inject transient VDI Hosts into any virtual desktop images created • Accessible by Peer-to-peer and Gateway-managed connections • The VDI Host will only exist while the virtual desktop is running, and will automatically be deleted from the Gateway when the desktop is discarded • VDI Hosts are automatically added to All Hosts and the Host for VDI groups, and will be counted as concurrent VDI session under the Managed Hosts license mode

RDS tab

PC-Duo Host can be configured to allow remote viewing and remote control of one or more simultaneous Remote Desktop Services sessions, as well as the Remote Desktop Services server console.

A standard PC-Duo Host with a special RDS license key must be installed and configured on the server console to serve as the "root". When a new RDS session is started, it will execute the Startup procedure inherited from the server console, which includes a task to start a Host service. PC-Duo Host will distinguish the session from the server console and start up a Host service specifically for the session.

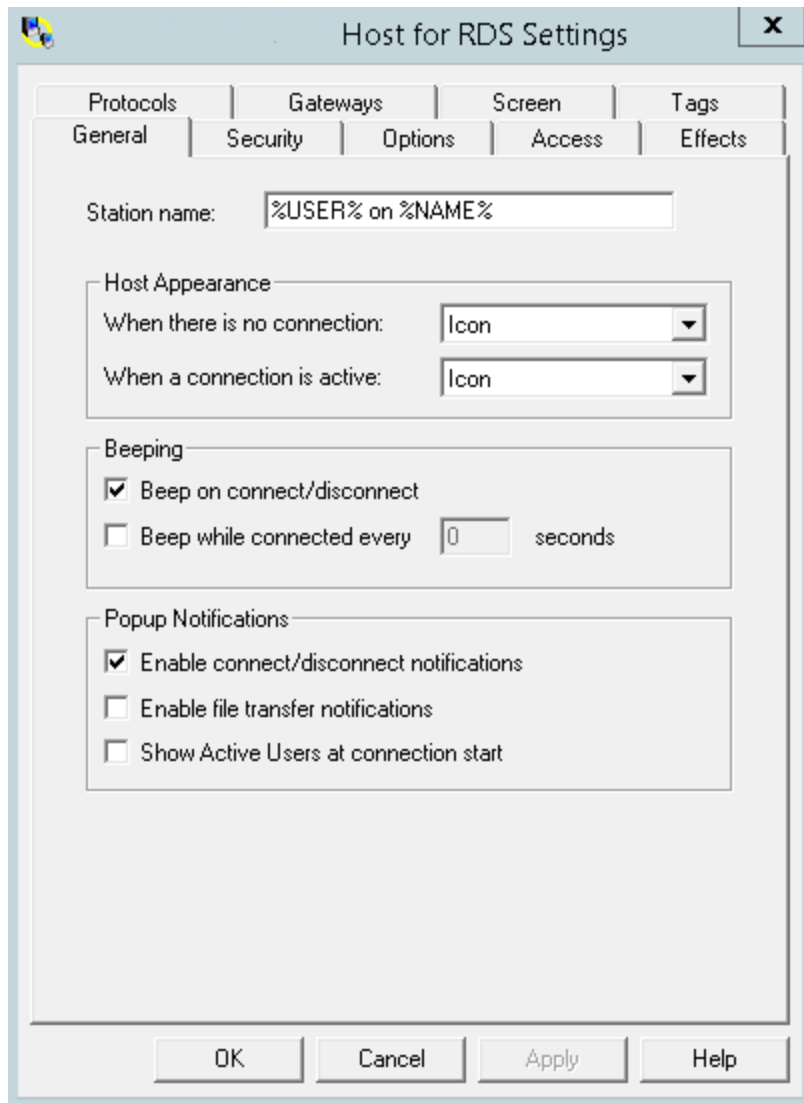
Note: If the Host is running with a time-limited trial or with a non-RDS Host license key, and a Host for RDS key is added while the Host is running, the Host Service must be restarted before the RDS functionality will be effective.



Configure Host Instances

The root Host maintains a Remote Desktop Services template to hold the Host configuration settings for these Host service instances (in this way, the Host settings for the root may be different than those specified in the RDS template). To view or edit this template, go to the RDS tab in the root Host Control Panel and click on **Configure**.

Most of the configuration options are the same as those available on the standard Host Control Panel, although the **About** and **Status** tabs are not present because the settings on these tabs are not directly applicable to RDS session Hosts.

The image shows a Windows-style dialog box titled "Host for RDS Settings". It has a standard Windows icon in the top-left corner and a close button (X) in the top-right corner. The dialog box contains several tabs: "Protocols", "Gateways", "Screen", "Tags", "General", "Security", "Options", "Access", and "Effects". The "General" tab is currently selected. Inside the "General" tab, there is a "Station name:" label followed by a text input field containing "%USER% on %NAME%". Below this is a "Host Appearance" section with two dropdown menus: "When there is no connection:" and "When a connection is active:", both set to "Icon". Underneath is a "Beeping" section with a checked checkbox "Beep on connect/disconnect" and an unchecked checkbox "Beep while connected every" followed by a numeric input field set to "0" and the word "seconds". At the bottom of the dialog box are four buttons: "OK", "Cancel", "Apply", and "Help".

Set Users


The administrator can restrict Host instances generated by the root Host to specific users or groups of users. To do this, click on the **Set Users** button, select a user or group of users and assign permissions.

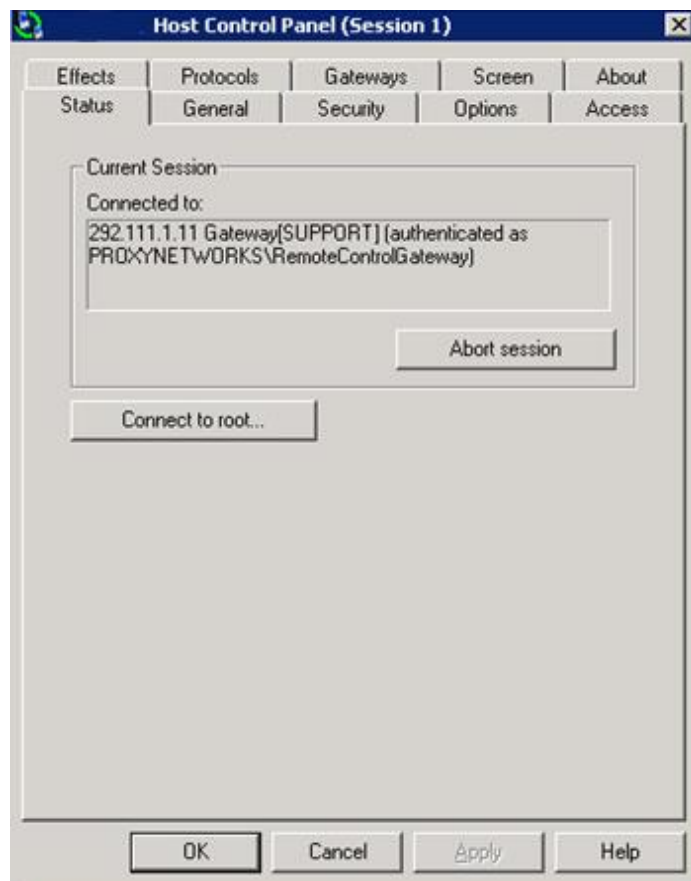
Citrix XenApp support

If the checkbox, Provide services for Citrix XenApp “desktop” sessions only is selected in the Host Control Panel (default = unchecked), Host instances will only be injected into virtualized “desktop” sessions, and not into virtualized “application” sessions. This will allow administrators to conserve the number of licensed Host instances available on a RDS Server machine.

Note: The Host for RDS “Provide services for Citrix XenApp ‘desktop’ sessions only” feature requires the Citrix XenApp WMI provider that is only in Enterprise and Platinum editions of the product; it’s not available in the “Advanced” edition. The WMI provider is required for the Host feature to work, therefore, only the Enterprise and Platinum editions are supported.

Remote Desktop Services Session Host Control Panel

Once the Host service for a specific Remote Desktop Services session is started, you can view the effective settings for this Host service by clicking on the Host Control Panel icon  in the RDS session:



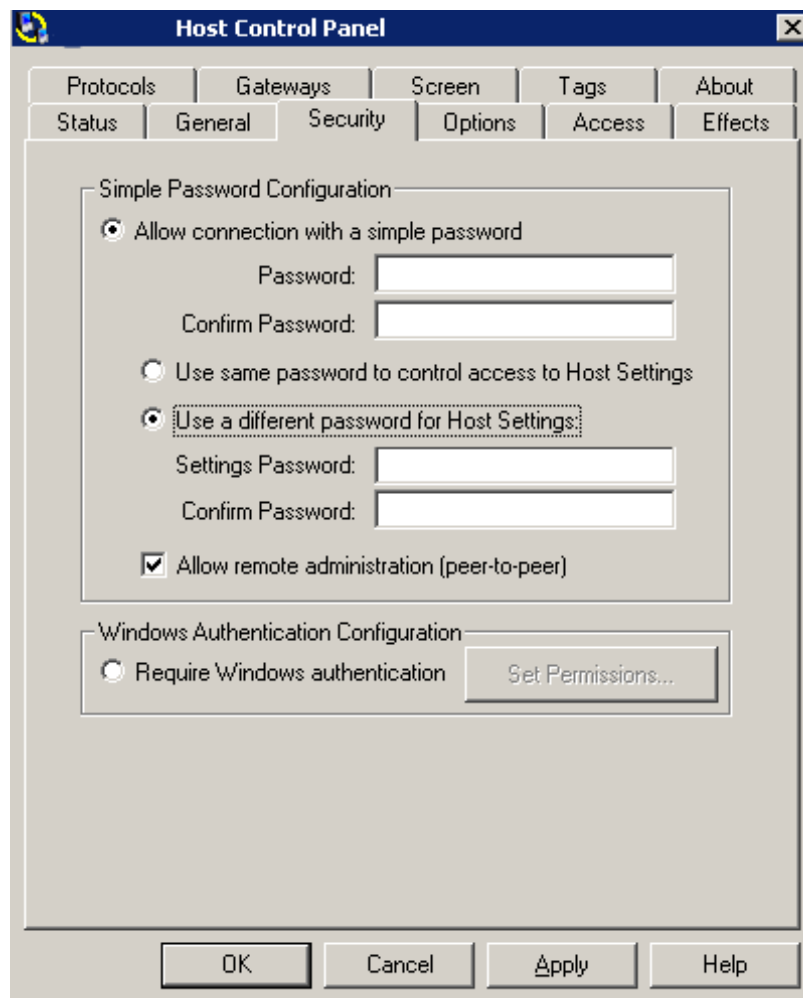
Note that the title bar shows the session number. Each root Host is capable of supporting as many simultaneous sessions as the license key allows.

You can view information about the root Host by selecting **Connect to root**. The Control Panel for the root Host will appear.

The configuration information in the Control Panel for Remote Desktop Services session Hosts is view only because the settings are based on the settings in the root Host Control Panel.

Host Control Panel Authentication for Remote Desktop Services Sessions

If the Host Control Panel is launched from a Remote Desktop Services server console session, it will attempt to connect to the Root Host service running in the console session. Because the Root Host is capable of listening for connections, the Host Control Panel can use a peer-to-peer connection to communicate with the Root Host. By default, the Host Control Panel will attempt to use the credentials that were used to log into the console session; if this is disabled (either by deselecting this option under Simple Password Configuration on the **Security** tab or disabling the Access Host Tray Icon permission on the **Admin Security** tab for Windows Authentication Configuration), the Host Control Panel user will be asked to authenticate directly to the Root Host for access.



If the Host Control Panel is launched inside a Remote Desktop Services session with a Host instance running, two different sets of credentials may be required: First, the Host Control Panel user will need to present credentials to authenticate to the Gateway; if accepted, the user will then need to present credentials to authenticate to the Host instance (similar to Master connecting through the Gateway to a Host configured for Windows Authentication). If the credentials used to authenticate to the Gateway are also acceptable by the Host instance (which would be the case if the Gateway and the RDS server are in the same domain), then only one set of credentials will be needed. However, if they are not acceptable (i.e. the Gateway and RDS server are in different domains), then Host Control Panel user will be asked to present a second set of credentials specifically for authenticating to the Host instance.

In general, the configuration options for Host instance are similar to those available for installed Host application. Please refer to specific tabs below to see any differences.

General tab

Same as the General tab for installed Host except the station name refers to the RDS Host instance and Remote Desktop Services server it is running on.

Security tab

Same as the Security tab for installed Host.

Options tab

Same as Options tab for installed Host except that keyboard and mouse suppression option is not available.

Access tab

Same as the Access tab for installed Host

Effects tab

Same as the Effects tab for installed Host

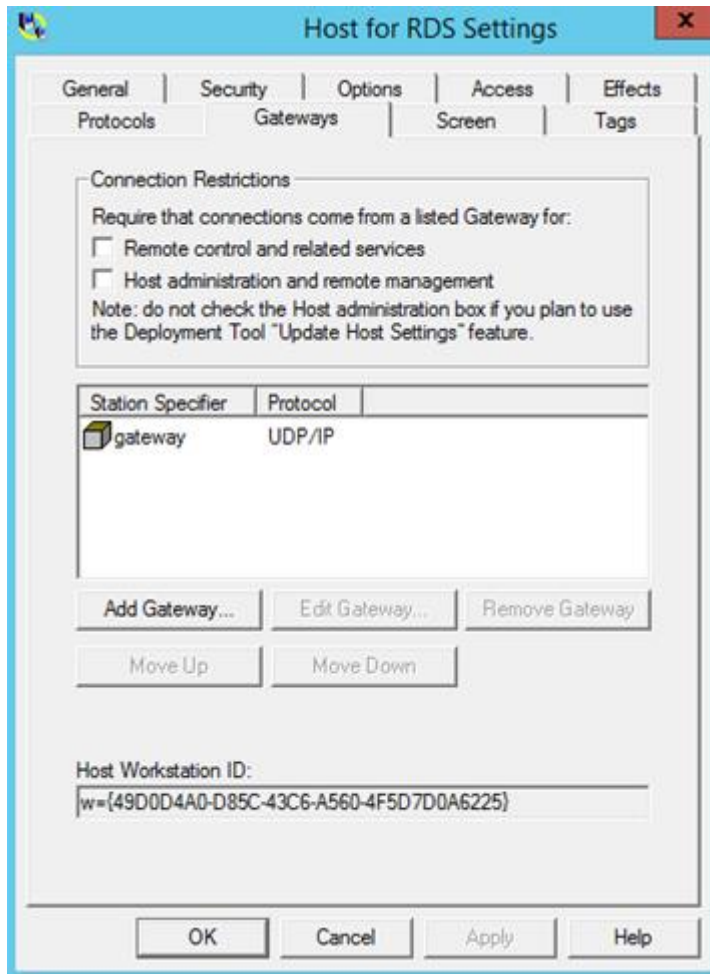
Protocols tab

Configure the network protocols and ports for communication with PC-Duo Host in the **Protocols** tab. These settings are disabled for RDS session Host instances because they do not listen for connections; the root Host, however, will specify protocol(s) to be used for its connection to the Gateway..

Gateways tab

The RDS Host must be configured to report to one or more PC-Duo Gateways; it is through these connections that RDS session Host instances will be reached.

Note that connection status icon next to Gateway entries and the Host Workstation ID are generic in the RDS Server Host template. These will be replaced by actual icons and values when the Host service is started in the RDS session (see [RDS tab](#) for an example).



For security purposes, all connection attempts can be forced to go through the specified Gateways by selecting **Permit connection only through listed Gateways** on the Gateways tab. With this option, administrators can take advantage of Gateway-based security policies and prevent unauthorized connections via peer-to-peer or unlisted Gateways.

Screen tab

Same as the Screen tab for installed Host except user-mode screen capture algorithm is the only option.

Tags tab

Same as the Tags tab for installed Host.

Remote Printing

One of the key services provided by PC-Duo remote support solutions is remote printing. PC-Duo Master users will usually use this service to redirect a print command on the Host to a printer that is connected locally to the Master. However, this feature now offers much more flexibility:

Remote printing has been completely re-written for PC-Duo 12.7. You now have the ability to print in both directions, from Host to Master or from Master to Host. You no longer have to install matching printer drivers on Host and Master. You can send the same print job to multiple destinations at once. You can send saved print job files to a remote printer without going through the print process all over again. And remote printing works Peer-to-Peer as well as via Gateway, and on all PC-Duo 12.7 supported Windows platforms, (desktop and server operating systems, both 32-bit and 64-bit editions). All of this is made possible by two key components of PC-Duo remote printing - the PC-Duo XPS Printer driver, and the PC-Duo Remote Print Manager.

For detailed information regarding the configuration and usage of this feature, please see the "Remote Printing tab" section of the PC-Duo Master Guide.

Restart in Safe Mode

For diagnostic and troubleshooting purposes, it may be necessary to operate a computer in Safe mode. In Safe mode, typically the operating system will load and run the minimum set of executable functions necessary for the computer to run. This allows a technician to quickly isolate the root cause of problems observed in Normal mode, remove dangerous and/or unnecessary software, and fix/maintain other parts of the system.

In order to do this on a remote computer, a Master user can execute a new Start menu item in the **Vector Networks > Utilities** start menu group on the Host called **Restart system in 'Safe Mode with Networking'**. This menu option will execute a program installed along with the Host that will configure the system to start in safe mode (with networking enabled) on next reboot. The user will then be prompted to continue with the reboot.

Note: Once rebooted, the Host service will automatically be restarted; however, Master will need to re-establish connection to the Host.

This program has following features:

- On Windows Vista/7/Server 2008, an elevation prompt for account credentials with administrator privileges will appear, if necessary.
- On Windows XP/Server 2003, the Safe mode program will check that it has sufficient access privileges to run; if not, it will prompt the Master user for alternate credentials which have sufficient rights (typically, administrator level). In the case that the logged-in user on the Host does not have administrator privileges, this will allow the Master user to enter appropriate credentials and restart without having to logout and log back in to the Host as an administrator.
- A confirmation prompt is displayed to the end user to confirm the operation; if accepted, the system is configured for safe mode boot, and restarted programmatically.

Once the system is restarted in Safe mode, it will automatically be reset to start in Normal mode on the next reboot.

Note: In Safe Mode, the Host will run with user-mode screen capture capabilities only.

Host Audit Log

The connection message generated when the first user connects to a Host will be recorded in the Application Event Log section of the Windows system event log. In addition, corresponding messages for any subsequent users who either join or leave the connection will be recorded. Finally, the disconnection message generated when the last user disconnects from a Host will be recorded.

Below is an excerpt from the Application Event Log for the Host example above, and individual log entries for the 2 users that were joined to the Host:

```
=====
Event Logs
=====
```

```
-----
Application Event Log
-----
```

```
EVENTLOG_INFORMATION_TYPE .. 02/24/2011 04:14:13 PM ProxyHostService 120 N/A
..... User "PROXYNETWORKS\Administrator" at network address "192.168.1.71" (
..... ID="1cbd2d25631a42c") has joined the Gateway-based connection.

EVENTLOG_INFORMATION_TYPE .. 02/24/2011 04:11:16 PM ProxyHostService 120 N/A
..... User "PROXYNETWORKS\akim" at network address "192.168.1.105" (ID="1cbd
..... 2d25631a423") has joined the Gateway-based connection.

EVENTLOG_INFORMATION_TYPE .. 02/24/2011 04:11:16 PM ProxyHostService 100 N/A
..... Connection opened by Gateway[GWS] (authenticated as PROXYNETWORKS\Remo
..... teControlGateway via NTLM) at network address 192.168.1.116.
```


Command Line Configuration

The following combination of PC-Duo Host and Windows tools can be used to customize and automatically deploy PC-Duo Host to one or more target machines in your network:

- ◆ Use the command line utility `PHSETUP` to set PC-Duo Host configuration options from a command line. See ["Configure Host from the command line."](#)
- ◆ In addition to specifying options in the PC-Duo Host Control Panel window, use `PHSETUP` to lock down other PC-Duo Host features. See ["Lock-down settings"](#).
- ◆ Use the Windows `MSIEXEC` installation command line utility to install a customized PC-Duo Host configuration. This feature is useful if you want to push PC-Duo Host with the same set of configuration options to a large number of target machines automatically. See ["Install Host with the MSIEXEC command line"](#).
- ◆ Use a login script to run commands at login time and then use this script to configure an installed Host with `PHSETUP`, or install the Host using `MSIEXEC`.

NOTE: *The PC-Duo Deployment Tool can also be used to mass deploy PC-Duo Host configurations. For more information, see the PC-Duo Deployment Tool Administration Guide.*

No matter which method you choose to install PC-Duo Host, the configuration settings can be modified later using either `PHSETUP` from the command line, or directly from the PC-Duo Host Control Panel window.

NOTE: *For the Host to be available and the installation to be completed, you must reboot the computer after initial installation.*

NOTE: *To configure a copy of PC-Duo Host that is already installed on a Host computer, you must have the administrative rights to configure the product on the Host computer. On Windows Vista and Server 2008 platforms, you may have to run `PHSETUP` in an already-elevated command prompt (which you may not be able to do from a login script). See ["Security tab"](#).*

Configure Host from the command line

After installation, PC-Duo Host can be configured using the `PHSETUP` command line utility. Settings that do not explicitly change in the command line retain their current values. `PHSETUP` updates the settings in the registry, and updates any copy of the PC-Duo Host that is currently running on the computer on which you execute `PHSETUP`.

Use this command line utility, along with the Windows utility `MSIEXEC` (see [“Install Host with the MSIEXEC command line”](#)), to create a preconfigured installer for PC-Duo Host.

In addition, with the proper access rights, PC-Duo Host settings can be changed remotely. See [“PHSETUP Control parameters”](#).

Following is the full list of parameters that can be configured using the `PHSETUP` command line utility:

- ◆ "PHSETUP Command line syntax"
- ◆ "PHSETUP Access parameters"
- ◆ "PHSETUP Control parameters"
- ◆ "PHSETUP Effects parameters"
- ◆ "PHSETUP Error Handling parameters"
- ◆ "PHSETUP Gateways parameters"
- ◆ "PHSETUP General parameters"
- ◆ "PHSETUP License parameter"
- ◆ "PHSETUP Options parameters"
- ◆ "PHSETUP Protocol parameters"
- ◆ "PHSETUP Security parameters"
- ◆ "PHSETUP Screen parameters"
- ◆ "PHSETUP Tag parameters"
- ◆ "PHSETUP Remote Desktop Services parameters"
- ◆ "PHSETUP Windows Security parameters"

PHSETUP Command line syntax

Set `PHSETUP` parameters directly from the command line, separating each parameter name and its value with a colon, as in the following:

```
phsetup param1:value1 param2:value2 ... paramn:valuen
```

The following is a specific example:

```
phsetup name:"JOE's PC" connectbeep:yes
```

Different parameters require different formats, as shown below.

Parameter	Format Description
string	An alphanumeric string, in quotes, if spaces or punctuation are required
number	A numeric value, given in decimal format
hexnum	A numeric value, given in hexadecimal format
user	A user name, specified in the format domain\username
ace	A username, specified in the format domain\username , followed by a comma and a hexadecimal numeric value

NOTE: Enclose parameter values that contain spaces in quotation marks. If a value with spaces contains embedded quotation marks, you must additionally enclose the marks in quotes. For example, use "" in place of "within a string, in addition to enclosing the entire string in quotes. See ["PHSETUP syntax examples"](#).

Syntax that waits for command completion

Although `PHSETUP` is executed from the command line, it is a Windows application. Consequently, it does not necessarily finish executing before the prompt returns unless you use the `start/wait` syntax:

```
start/wait PHSETUP.EXE params
```

NOTE: If you call `PHSETUP` from a batch file or network login script and you want to have the entire script completed before returning the prompt, you must include the `start/wait` command in each line. If you use the `@` control parameter so that `PHSETUP` executes the commands in a specified text file, each command in the file is executed in sequence. See ["PHSETUP control parameters"](#).

PHSETUP Syntax examples

The following examples illustrate how you can use PHSETUP to configure PC-Duo Host:

- ◆ `phsetup name:HowdyDoody` sets the Host computer station name to *HowdyDoody*.
- ◆ `phsetup name:"Julia's Game Machine"` sets the Host computer station name to *Julia's Game Machine*.
- ◆ `phsetup name:"Julia's ""little"" machine"` sets the Host computer station name to *Julia's "little" Machine*.
- ◆ `phsetup access:time`
`timezone:0000000000000000FCFF03000000FCFF03000000FCFF03000000FCFF`
`03000000FCFF03` sets access restrictions, so that the Host computer is locked from 9am to 5pm Monday to Friday.
- ◆ `phsetup addgateway:"IP,@198.186.160.77"` adds a PC-Duo Gateway to which the Host computer reports using UDP/IP.
- ◆ `phsetup removegateway:all` removes all PC-Duo Gateways from the PC-Duo Host reporting list.
- ◆ `phsetup addservicessecurityace:"mydomain\YourRemoteControlGateway,0xE00FF"` `addadminsecurityace:"mydomain\YourRemoteControlGateway,0xE00F"` `addsettingssecurityace:"mydomain\YourRemoteControlGateway,0xE00FF"` assigns full access control to a domain account (mydomain\YourRemoteControlGateway). You can use this command to assign full access control rights to your PC-Duo Gateway domain account, or any other domain account.
- ◆ `phsetup name:$NAME$ connectbeep:on beepervery:0 idleappear:icon connappear:icon controlpanel:on usewindowssecurity:no`
`adminpasswordrequired:different allowremoteadmin:no`
`password:randomstring adminpassword:"" access:permit`
`permission:none granttime:30 requesttime:30`
`lockworkstationondisconnect:no logoutondisconnect:no`
`rebootondisconnect:no suppresskeys:permit blankscreen:permit`
`ip:on ipx:on encryption:on` resets settings to their PC-Duo Host default values (for systems using simple password).

In addition, you can refer to the following settings that are in effect under Windows XP, and Windows Server 2003:

```
usewindowssecurity:yes removeservicessecurityace:*
addservicessecurityace:Administrators,0xE00FF
setservicessecurityowner:Administrators
removeadminsecurityace:*
addadminsecurityace:Administrators,0xE00F
addadminsecurityace:Interactive,0x03
setadminsecurityowner:Administrators
removesettingssecurityace:*
addsettingssecurityace:Administrators,0xE00FF
setsettingssecurityowner:Administrators
```

NOTE: Enter all commands and parameters on one line. Due to limited page width, some of the following examples present commands on multiple lines.

PHSETUP Access parameters

The following PHSETUP parameters correspond to the "Access tab" settings in PC-Duo Host.

Parameter	Definition
<code>access:permit</code> <code>access:locked</code> <code>access:time</code>	<p>Set access restrictions.</p> <p>Set to <code>permit</code> to allow access to the Host computer after security is checked.</p> <p>Set to <code>locked</code> to deny all remote control access to the Host computer.</p> <p>Set to <code>time</code> to require a timezone setting (that you must also specify).</p>
<code>granttime:number</code>	<p>Set the number of seconds allowed for the Host computer to grant or deny access. Set this number between 1 and 86400.</p>
<code>permission:none</code> <code>permission:request</code> <code>permission:grant</code>	<p>Set connection permissions.</p> <p>Set to <code>none</code> (default PC-Duo Host behavior) if you do not require permission for remote access.</p> <p>Set to <code>request</code> to request a Host computer user for access within a specified time.</p> <p>Set to <code>grant</code> to request the Host computer to deny user for access within a specified time, or access is permitted.</p> <p>If you set <code>request</code> or <code>grant</code>, you must also specify the <code>requesttime</code> or <code>granttime</code>.</p>
<code>lockworkstationondefault:</code> <code>yes no</code>	<p>By default, this setting is set to <code>yes</code> to automatically lock workstation if access permission is not granted. Set this to <code>no</code> to prevent workstation from being locked.</p>

<code>requesttime: <i>number</i></code>	Set the number of seconds during before time-out for the consideration of a remote control request to the Host computer. Set this number between 1 and 86400.
<code>sensitivetolockscreen: <i>yes no</i></code>	Configures whether permission to connect prompt appears if Host console is at the Windows login screen or lock screen. Set this to <i>yes</i> to be sensitive to lock screen, that is, do not display prompt when console is locked.
<code>servicesenabled: <i>hexnum</i></code>	Set the services that are enabled by default. 0x0008 – Input Control 0x0040 – File Transfer 0x0080 – Remote Printing 0x0100 – Clipboard Transfer 0x0800 – Chat 0x1000 – Remote Management 0x19C8 – all services Default is all services enabled, consistent with the Host license.
<code>timezone: <i>hexnum</i></code>	Set the time zone settings. These settings lock or permit access if you also specify <i>access:time</i> . You must specify a sequence of hexadecimal digits for <i>hexnum</i> . In the string, bits set to 0 permit access and bits set to 1 lock access. The low-order bit of the first byte represents Sunday at 12AM and the bits continue in sequence through Sunday and the subsequent days of the week. See “Time zone settings” .

PHSETUP Control parameters

The table below lists and defines PHSETUP control parameters.

Parameter	Definition
@path&filename	<p>Create a text file the includes a series of PHSETUP commands. Use this parameter with a call to PHSETUP to run the text file (command line script) (referred to here as <i>filename</i>), and process the PHSETUP commands listed in the text file exactly as if you were to call them directly from PHSETUP .</p> <p>If you include lines in the text file that begin with a semicolon (;), they are treated as comment lines and are ignored.</p>
importjson:path&filename	<p>Import a JSON-formatted file of Host settings, such as one created with the <code>mode:exportjson</code> option. This option can be combined on the command line with other options to fully configure the Host.</p>
/p	<p>Specify the <i>protocol</i> or a "<i>protocol/port</i>" pair to use when connecting to a Host computer for the purpose of configuring it. For peer-to-peer connections to a Host computer for the purpose of configuration, the protocol you specify connects your local computer to the Host computer. The entire phrase is in double quotes. You can use this command to specify the protocol and port (other than defaults).</p> <p>The following examples assign the standard port in each case:</p> <p>/pTCP For TCP/IP protocol. No quotes required.</p> <p>/pUDP For UDP/IP protocol. No quotes required.</p> <p>/pIPX For IPX protocol. No quotes required.</p> <p>Use the following syntax to specify the port:</p> <p>/p "<i>Protocol_name Port_number</i>"</p> <p>Example:</p> <p>/p "TCP 5001"</p> <p>Notice that the vertical bar is required as a separator for the protocol/port number pair.</p>

<p>/s (peer-to-peer)</p>	<p>Specify the station when connecting directly to a Host computer for the purpose of configuring it. This value is in quotes, and is the string value for the station name, DNS name, or network address specifier for peer-to-peer connections. The peer-to-peer syntax depends on your protocol specification.</p> <p>The following are some protocol-specific examples:</p> <pre> /pUDP /S192.168.160.138 /pTCP /Sjackson /pTCP /Sjackson.acme.com /pIPX /S@20:1B13DAE9 /pIPX /S"Dell P200" /pIPX /S"2:Dell </pre>
<p>/g /s (connections through a PC-Duo Gateway)</p>	<p>Specify the PC-Duo Gateway and Host computer when connecting to a Host computer through a PC-Duo Gateway for the purpose of Host computer configuration. Specify these values in double quotes. Note that when you specify the PC-Duo Gateway and protocol (using /p), the protocol applies to the connection between your local computer and the PC-Duo Gateway. The /g value is the string value for the Gateway name, and the /s value is the string value for the type of host (logged-in user or workstation) and the Host key for remote connections through a PC-Duo Gateway.</p> <p>The Gateway syntax for /s values depends on your host specification. Use <i>u</i> for a logged-in user and <i>w</i> (with curly braces) for a workstation:</p> <ul style="list-style-type: none"> • "u=host_key" • "w={host_key}" <p>NOTE: The <i>u</i> that you use for the Gateway syntax of /s is independent of the /U command.</p> <p>To find the workstation Host key, navigate to the "About tab" of PC-Duo Host. Click System Information, and select the text listed next to PC-Duo Host Workstation Id.</p> <p>The following rows have host format-specific examples.</p> <pre> /g"Gateway 1" /s"w={6F93DF16-8352-46EB-ADDF-7FD752EA72FA}" /g"Gateway 1" /s"u=ACME\george" </pre>

`/u"domain\username"`

When configuring a Host computer, specify a user account name to use when connecting to the Host computer (either peer-to-peer, or through a PC-Duo Gateway). You need only specify the user account name when your logged in credentials are not sufficient for configuring the Host computer (either directly, or through a PC-Duo Gateway).

Example:

`/U"ACME\george"`

`/x`

When configuring a Host computer, specify a password for the user account you use when connecting to the Host computer (either peer-to-peer, or through a PC-Duo Gateway). You need only specify the password when your logged in credentials are not sufficient for configuring the Host computer (either directly, or through a PC-Duo Gateway).

The value to specify is a string value for the password in quotes. The syntax is as follows:

`/X"password"`

Example:

`/X"foo"`

`mode`

There are several `mode` commands you can issue at the beginning of a `PHSETUP` command:

- `mode:interactive`, to allow for error messages to appear during the command executions.
- `mode:lockdown`, to lock one or more PC-Duo Host features.
- `mode:terminalservices`, to cause the command line to affect the Terminal Services template copy of the settings, not the root Host settings. Note that this is mutually exclusive with `mode:lockdown`, which is not applicable to TS template.
- `mode:exportjson`, to export the settings into JSON format at the end of execution; this allows settings changes to be made using other keywords on the command line. The exported settings are placed in a file name `<machinename>_HostSettings.json` on the desktop.
- `mode:reset`, to reset all settings associated with the current mode (e.g. `mode:lockdown`, or `mode:terminalservices`, or default mode) to their installation defaults

If none of these options is specified, then the default mode is `non-interactive`.
PHSETUP does not display error messages even if an error occurs (this avoids interrupting a batch file or login script processing).

NOTE: When you use the `mode:lockdown` parameter to lock down PC-Duo Host, you cannot use the `/p`, `/g`, `/s`, `/x`, or `/u` parameters. See [“Lock Host settings”](#) for more information on this control.

PHSETUP Effects parameters

The following PHSETUP parameters correspond to the [“Effects tab”](#) settings in PC-Duo Host.

Parameter	Definition
<code>managevisualeffects: always</code>	Set to <code>always</code> to disable visual effects whenever a remote connection is established. Set <code>visualeffects</code> flags when you use this setting. Set to <code>never</code> or <code>off</code> to deny remote users from controlling visual effects. Set to <code>permit</code> to allow remote users to control visual effects when they configure this feature. The default is <code>permit</code> .
<code>managevisualeffects: permit</code>	
<code>managevisualeffects: off</code>	
<code>managevisualeffects: never</code>	

`visualeffects: hexnum`

Set the flags for visual effects.

0x0001 - Active Desktop

0x0002 - Desktop wallpaper and patterns

0x0004 - Mouse effects: cursor shadow, mouse trails

0x0008 - Font effects: font smoothing, ClearType

0x0010 - Windows effects: menu and window animation

0x0020 - Show Window contents while dragging

0x0040 - Screen saver

0x0080 - Aero Glass

The default is 0xFF (all effects).

PHSETUP Error Handling parameters

One or more of the following error messages may be returned if you supply `mode:interactive` at the beginning of the command line call to PHSETUP.

- ◆ If you pass bad credentials to the `/u` or `/x` parameters, PHSETUP detects the failure to connect to the settings, displays an error message, and then exits. Note that if you use a bad user account name in adding an ACE (access control entry) to a security descriptor, PHSETUP does not detect any problem. However, no change is made to the settings, and PHSETUP silently exits.
- ◆ PHSETUP returns an error if you attempt to pass it an invalid keyword or if you pass an invalid parameter to a keyword that accepts a limited set of values (such as `on` and `off`).
- ◆ No error information is reported if you pass an invalid parameter to any of the following keywords:

<code>addServiceSecurityACE</code>	<code>removeAdminSecurityACE</code>
<code>removeServiceSecurityACE</code>	<code>setAdminSecurityOwner</code>
<code>setServiceSecurityOwner</code>	<code>addSettingsSecurityACE</code>
<code>addAdminSecurityACE</code>	<code>removeSettingsSecurityACE</code>
	<code>setSettingsSecurityOwner</code>
	<code>addLicense</code>

NOTE: Use `mode:interactive` at the beginning of the command line call to display any error messages at all.

PHSETUP Gateways parameters

The following PHSETUP parameters correspond to the "Gateways tab" settings in PC-Duo Host.

Parameter	Definition
<code>requiregateway: yes no</code>	<p>Set to <code>yes</code> to require that all remote control connections to this Host computer pass through a PC-Duo Gateway.</p> <p>Set <code>addgateway</code> when you use this setting.</p> <p>Set to <code>no</code> (default behavior) to allow peer-to-peer remote control connections that do not pass through a PC-Duo Gateway.</p>
<code>requiregatewayforadmin: yes no</code>	<p>Set to <code>yes</code> to require that all administration and remote management connections to this Host computer pass through a PC-Duo Gateway.</p> <p>Set <code>addgateway</code> when you use this setting.</p> <p>Set to <code>no</code> (default behavior) to allow peer-to-peer administration and remote management connections that do not pass through a PC-Duo Gateway.</p>

Add a specified Gateway to which PC-Duo Host can report. You can use the following values:

protocol = TCP, UDP, SSL, WS, WSS, or IPX

port (optional) = a valid port number if you do not use the standard port

station_specifier = a protocol-dependent specification for the station:

UDP/IP or TCP/IP

- *network_address*
- *station_name*
- *dns_name*

IPX

- *@node*
- *@network:node*
- *station_name*
- *network:station_name*

controlmode = optional control mode, one of "auto", "never", or "always"

NOTE: Specify the *protocol|port* pair in quotes when you specify the port, and specify the *station_specifier* in quotes. Separate the *protocol|port* and the *station_specifier* with a comma.

```
addgateway: "protocol|port",  
            "station_specifier"  
[ , controlmode ]
```

Remove a specified Gateway to which PC-Duo Host is configured to report. You can use the following values:

`protocol` = TCP, UDP, SSL, WS, WSS
or IPX

NOTE: You can also specify the port, as in "addgateway:
"protocol|port",
"station_specifier".

`station_specifier` = a
protocol-dependent
specification for the
station:

UDP/IP or TCP/IP

- network_address
- station_name
- dns_name

IPX

- @node
- @network:node
- station_name
- network:station_name

NOTE: Specify the
`station_specifier` in quotes.
Separate the `protocol` and the
`station specifier` with a
comma.

```
removegateway:
" protocol|port ",
" station_specifier "
```

<code>removegateway: all</code>	Eliminate all PC-Duo Gateways from the list of PC-Duo Gateways to which PC-Duo Host is configured to report.
<code>resetgateway: " protocol port ", " station_specifier "</code>	Reset the security model for the specified Gateway to zero ("original model, or will negotiate with Gateway"). This keyword can be used to script the resetting of the security model to clear the "0xC004C009" error. See <code>removegateway</code> for information on value options.
<code>resetgateway: all</code>	Reset the security model for all Gateways to which PC-Duo Host is configured to report to zero ("original model, or will negotiate with Gateway").

PHSETUP General parameters

The following PHSETUP parameters correspond to the "General tab" settings in PC-Duo Host.

Parameter	Definition
<code>beepevery: <i>number</i></code>	Use this parameter to set a beeper to sound every <i>number</i> seconds. No beeper sounds if you set <i>number</i> to 0. Supply a number in the range 0 to 9999.
<code>connappear: hidden</code> <code>connappear: icon</code>	Set to <code>hidden</code> to hide the PC-Duo Host icon when a connection is active. Set to <code>icon</code> to render the PC-Duo Host icon visible when a connection is active.
<code>connectbeep: on</code> <code>connectbeep: off</code>	Set to <code>on</code> in order to have the system beep when a remote connection connects or disconnects. Set to <code>off</code> in order to have no sound when remote connect or disconnect occurs.
<code>idleappear: hidden</code> <code>idleappear: icon</code>	Set to <code>hidden</code> to hide the PC-Duo Host icon when there is no active connection. Set to <code>icon</code> to render the PC-Duo Host icon visible when there is no active connection.
<code>hostnotifications: <i>number</i></code>	Turn on popup notifications on the PC-Duo Host when <i>number</i> is set to (or sum of): 0x1 - Connect/Disconnect 0x2 - File Transfer 0x10000 – Show Active Users at Connect (not a popup notification but controls whether the Active Users UI is automatically shown)
<code>name: <i>string</i></code>	Use this parameter to provide a string that specifies a new station name.
<code>showbugpanel: yes</code> <code>showbugpanel: no</code>	Host-on-Demand Only: Use this parameter to show or hide the HOD Host Mini Control Panel

NAME parameter macros

The NAME parameter provides support for static substitution of station name. For example, the following command resets the station name to the name of the computer:

```
name: $NAME$
```

Enclose all macros between dollar signs (\$)

Macro	Description
\$NAME\$	Host computer machine name
\$USER\$	Logged in user at the Host machine console
\$VER\$	External Host software version number (e.g. "v8.0.0.1800")
\$INTVER\$	Internal Host software version number
\$PLATFORM\$	Host operating system platform (e.g. "Win7")

Macros are evaluated and inserted statically at the time that you run `PHSETUP`. To change station name dynamically at runtime, use the % macros as described in ["Change station name with macros"](#).

NOTE: Macro names are not case sensitive.

PHSETUP License parameter

The following PHSETUP parameter corresponds to the "About tab" settings in PC-Duo Host.

Parameter	Definition
<code>addlicense:string</code>	Add a license string (that you specify with the value <i>string</i>) to the current copy of PC-Duo Host.

PHSETUP Options parameters

The following PHSETUP parameters correspond to the "Options tab" settings in PC-Duo Host.

Parameter	Definition
<code>lockworkstationondisconnect:</code> <code>yes no</code>	Set to <code>yes</code> to lock the Host computer when a remote user's session is over.
<code>logoutondisconnect:yes no</code>	Set to <code>on</code> to restart the Host computer when a remote session is over. Otherwise set to <code>off</code> (default PC-Duo Host behavior).
<code>rebootondisconnect:yes no</code>	Set to <code>on</code> to restart the Host computer when a remote session is over. Otherwise set to <code>off</code> (default PC-Duo Host behavior).
<code>blankscreen:always</code> <code>blankscreen:permit</code> <code>blankscreen:never</code> <code>blankscreen:off</code>	Sets "permit screen blanking" and "blank screen on startup" options. Set to <code>always</code> to enable both of these options. Set to <code>permit</code> to enable "permit screen blanking" but disable "blank on startup." Set to <code>never</code> (default PC-Duo Host behavior) or <code>off</code> to disable both options.
<code>suppresskeys:always</code> <code>suppresskeys:permit</code> <code>suppresskeys:never</code> <code>suppresskeys:off</code>	Sets "permit suppression of keyboard/mouse" and "disable keyboard and mouse on startup" options. Set to <code>always</code> to enable both of these options. Set to <code>permit</code> to enable "permit suppression" but disable "disable on startup." Set to <code>never</code> (default PC-Duo Host behavior) or <code>off</code> to disable both options.

PHSETUP Protocol parameters

The following PHSETUP parameters correspond to the "Protocols tab" settings in PC-Duo Host.

Parameter	Definition
<code>encryption: on off</code>	Set to <code>on</code> to encrypt all remote data exchanges. Otherwise set to <code>off</code> .
<code>ip: on off</code>	Specify whether (<code>on</code>) or not (<code>off</code>) this Host computer 'listens' on the UDP/IP protocol, or accepts connections on that protocol. Specify <code>ipport</code> when you set this <code>on</code> .
<code>ipport: number</code>	Set the port number for IP usage. The value <i>number</i> is an unsigned hexadecimal, octal, or decimal short integer. For example: <ul style="list-style-type: none">• The number 10 = "10" (decimal), "012" (octal), or "0xA" (hexadecimal).• The number seventy-two = "72" (decimal), "0110" (octal), or "0x48" (hexadecimal).• The number one hundred ten = "110" (decimal), "0156" (octal), or "0x6E" (hexadecimal). Set to 0 to use the default port.
<code>ipx: on off</code>	Specify whether (<code>on</code>) or not (<code>off</code>) this Host computer supports the IPX protocol. Specify <code>ipxport</code> when you set this <code>on</code> .
<code>ipxport: number</code>	Set the port number for IPX usage. The value <i>number</i> is an unsigned hexadecimal, octal or decimal short integer. For example: <ul style="list-style-type: none">• The number 10 = "10" (decimal), "012" (octal), or "0xA" (hexadecimal).• The number seventy-two = "72" (decimal), "0110" (octal), or "0x48" (hexadecimal).• The number one hundred ten = "110" (decimal), "0156" (octal), or "0x6E" (hexadecimal). Set to 0 to use the default port.
<code>tcp: on off</code>	Specify whether (<code>on</code>) or not (<code>off</code>) this Host computer supports the TCP/IP protocol. Specify <code>tcpport</code> when you set this <code>on</code> .
<code>tcpport: number</code>	Set the port number for TCP/IP usage. The value <i>number</i> is an unsigned hexadecimal, octal or decimal short integer. Set to 0 to use the default port.
<code>tcpaccessmode: grant deny</code>	Determine whether (<code>grant</code>) or not (<code>deny</code>) to grant or deny most TCP/IP traffic. Set <code>tcprestrictions</code> to define exceptions to this policy. The default is <code>grant</code> .

<pre>tcprestrictions: addresses</pre>	<p>Set exceptions to your <code>tcpaccessmode</code> policy. Specify the <code>addresses</code> parameter as a single entry, or a set of entries separated by commas. Use one of the following formats for the variable:</p> <p><i>IPAddress</i>, <i>IPAddress (count)</i>, or <i>IPAddress[IPAddressmask]</i></p> <p>For example:</p> <pre>tcprestrictions = "111.111.111.111, 222.222.222.222(5), 111.112.113.0[255.255.255.0]"</pre>
<pre>tcprestrictions: addresses</pre>	<p>Add the following IPv6 formats to the list of possible formats:</p> <p><code>x:x:x:x:x:x,x</code>, <code>x:x:x:x:x:x:x/n</code></p>
<pre>preferredciphers: ciphers</pre>	<p>Set the list of encryption ciphers in order of preference from first to last. Ciphers are encoded as a two-character string, where the first character indicates the cipher algorithm, and the second character indicates the number of bits used. PC-Duo Host v11.0 and later support the following ciphers:</p> <ul style="list-style-type: none"> • "A4" - AES encryption (256-bit key) • "A3" - AES encryption (192-bit key) • "A2" - AES encryption (128-bit key) • "33" - Triple-DES (3DES) encryption (192-bit key) • "R2" - RC4-compatible encryption (128-bit key) with MD5 hash <p>The cipher list is a single string of concatenated cipher strings, in order of preference from first to last, e.g. "A4A3A233R2".</p>

PHSETUP Screen parameters

The following PHSETUP parameter corresponds to the "Screen tab" settings in PC-Duo Host.

Parameter	Definition
<code>preferusermode: yes no</code>	By default, this setting is set to no on Windows XP, Windows 2003 Server and older platforms so that kernel-mode screen capture is used. Set this setting to yes to use user-mode screen capture on those platforms. By default, this setting is set to yes on Windows Vista, Windows Server 2008 and later platforms.
<code>allowkernelmode: yes no</code>	Set this setting to yes to ensure that the kernel-mode screen capture driver is always used on this Host. Note: <i>The use of the kernel-mode screen capture driver will result in Aero Glass effects being disabled on Hosts running Windows 7.</i>
<code>attachatstartup: yes no</code>	Set this setting to specify that the kernel-mode screen capture driver be preloaded at Host startup time
<code>selectusermodeprofile: "profilename"</code>	Select default user mode profile for user mode screen capture preferences. Current options are: <ul style="list-style-type: none">• High Quality/High Bandwidth▪ Medium▪ Medium-Low (recording)▪ Low (recording)▪ [Custom]
<code>setusermodeprofile: "profilename, imagetype, imagequality, fgfrequency, bgfrequency, capturefrequency, bandwidthlimit"</code>	Specify bandwidth throttling options when creating a [Custom] user mode profile: <ul style="list-style-type: none">▪ <code>profilename</code> = custom profile name▪ <code>imagetype</code> = Hextile (default), JPEG▪ <code>imagequality</code> = integer between 20 and 100▪ <code>fgfrequency</code> = integer between 1 and 10▪ <code>bgfrequency</code> = integer between 1 and 10▪ <code>capturefrequency</code> = integer between 1 and 10▪ <code>bandwidthlimit</code> = -1 (unlimited) or integer between 5 and 200 (KB/sec)

PHSETUP Security parameters

The PHSETUP parameters in this section correspond to "Security tab" settings in PC-Duo Host.

usewindowsecurity:yes

The `usewindowsecurity:yes` command lets you use Windows security mechanisms for PC-Duo Host authentication. When set to `yes`, the `adminpassword`, `password` and `adminpasswordrequired` settings that are described in the next section are ignored.

usewindowsecurity:no

The `usewindowsecurity:no` command lets you use a simple password or not require a password for PC-Duo Host authentication. When set to `no`, the parameters in following table are applied:

Parameter	Definition
<code>adminpassword:string</code>	Sets the password for PC-Duo Host administration to <i>string</i> .
<code>adminpasswordrequired :same different</code>	Uses the Windows password for PC-Duo Host administration. Uses the <code>adminpassword</code> setting for PC-Duo Host administration.
<code>allowremoteadmin: yes no</code>	Allows the settings to be changed by a remote administrator. Any administration of the Host must be done at that computer's console (through PHSETUP or the Host Control Panel).
<code>password:string</code>	Sets the PC-Duo Host password to <i>string</i> .

PHSETUP Tag parameters

The PHSETUP parameters in this section correspond to "Tags tab" settings in PC-Duo Host.

Parameter	Definition
addtag:name,value	Add a tag with "name" and "value".
removetag:name	Remove a tag with the name matching "name"
removetag:*	Remove all tags

PHSETUP Terminal Services (Remote Desktop Services) parameters

The following PHSETUP parameters correspond to Windows security settings on the "Set Users..." dialog on the **RDS** tab in the Host Control Panel.

NOTE: These settings apply to the Root Host settings, not the Terminal Services Template, and so cannot be used in conjunction with the "mode:terminalservices" keyword.

Parameter	Definition
addTSUserACE: user, flags	Set the "Provide Host Services" flag for a given user account name to specify which users receive Host services when they log in. Flag values: 0x01 - Provide Host Services
removeTSUserAC: user	Remove the given user from the list of those who receive Host services. Use the * wildcard to remove all users.
setTSUserOwner: user	Specify the owner of the Terminal Services User settings.

The following PHSETUP parameter corresponds to the "Citrix XenApp" setting on the **RDS** tab in the Host Control Panel.

NOTE: This setting applies to the Root Host settings, not the Remote Desktop Services Template, and so cannot be used in conjunction with the "mode:terminalservices" keyword.

Parameter	Definition
citrixdesktoponly: yes no	Provide Host services for Citrix XenApp "desktop" sessions only. If "No", the Host will provide services to all Citrix XenApp sessions. (For XenApp Platinum and Enterprise editions only.)

PHSETUP Windows Security parameters

The following PHSETUP parameters correspond to Windows security settings on the "Security tab" in PC-Duo Host.

Parameter	Definition
<code>addservicesecurityace:user,flags</code>	<p>Set flags to specify service security options (in hexadecimal format) for a given user account name. See "Service Security tab".</p> <p>0x01 - Connect 0x02 - Remote View 0x04 - Remote Control 0x08 - FileTransfer Read 0x10 - FileTransfer Write 0x20 - Remote Printing 0x40 - Clipboard Read 0x80 - Clipboard Write 0x100 - Chat 0x8000 - Bypass Connection Permission 0x20000 - Read Permissions 0x40000 - Write Permissions 0x80000 - Take ownership 0xE01FF - All Rights, except Bypass Connection Permission 0xE81FF - All Rights, including Bypass Connection Permission</p>
<code>setservicesecurityowner:user</code>	<p>Specify the service security rights owner to a particular user (provide domain\username).</p>
<code>removeservicesecurityace:user</code>	<p>Set flags to remove service security rights for a given <i>user</i> (use the domain\username syntax).</p> <p>Use the * wildcard to remove service security rights for all users, or *\<i>user</i> for the user in all domains, or <i>domain</i>* for all users in the specified domain.</p>

<code>addadminsecurityace:user,flags</code>	<p>Set flags to specify the administration security rights (in hexadecimal format) for a given user account. See "Admin Security tab".</p> <p>0x01 - Connect Locally 0x02 - View Host Status 0x04 - Terminate Connection 0x08 - Connect Remotely 0x10 - Pause/Resume Screen Capture 0x20 - Remote Management 0x20000 - Read Permissions 0x40000 - Write Permissions 0x80000 - Take ownership 0xE000F - All Rights</p>
<code>setadminsecurityowner:user</code>	<p>Use this to set the admin security rights owner for a given <i>user</i> (use the <code>domain\username</code> syntax).</p>
<code>removeadminssecurityace:user</code>	<p>Use this to remove admin security rights for a given <i>user</i> (use the <code>domain\username</code> syntax).</p> <p>Use the <code>*</code> wildcard to remove admin security rights for all users, or <code>*\user</code> for the user in all domains, or <code>domain*</code> for all users in the named domain.</p>
<code>addsettingssecurityace:user,flags</code>	<p>Set flags to specify settings security (in hexadecimal format) for a given user account. See "Settings Security tab".</p> <p>0x01 - View Basic Settings 0x02 - Modify Basic Settings 0x04 - Modify Access 0x08 - View Licenses 0x10 - Modify Licenses 0x20 - View Gateway Configurations 0x40 - Modify Gateway Configurations 0x80 - View Configuration 0x20000 - Read Permissions 0x40000 - Write Permissions 0x80000 - Take Ownership 0xE00FF - All Rights</p>
<code>setsettingssecurityowner:user</code>	<p>Use this to set the settings security rights owner for a given <i>user</i> (use the <code>domain\username</code> syntax).</p>

`removesettingssecurityace:user`

Use this to remove settings security rights for a given *user* (use the `domain\username` syntax).

Use the `*` wildcard to remove settings security rights for all users, or `*\user` for the user in all domains, or `domain*` for all users in the named domain.

Install Host with the MSIEXEC command line

MSIEXEC is an executable Microsoft program that interprets packages and installs products. You can install or uninstall PC-Duo Host from the command line using standard MSIEXEC commands.

This section describes a partial list of the MSIEXEC commands. For a detailed list of commands, check the Microsoft web site (<http://www.microsoft.com>), and enter "msiexec command line" as a Search item.

- ◆ "MSIEXEC options"
- ◆ "MSIEXEC variables"
- ◆ "Examples"

MSIEXEC options

The following table contains a partial list of MSIEXEC options and parameters:

Option	Parameters	Description
/I	<i>package</i>	Install a software package using the command line
/a	<i>package</i>	Install a software package on the network. NOTE: This option requires Active Directory and Windows 2003 or XP, at minimum. Specify the shared directory in which to install the software package.
/x	<i>package</i>	Uninstall a software package using the command line.
/q	n b r f	Specify a user interface level: /qn No user interface /qb Basic user interface /qr Reduced user interface, modal dialog displayed at the end of installation /qf Full user interface with modal dialog displayed at the end of installation

<pre>/l</pre>	<pre>e v * logfile</pre>	<p>Specify path to log file. Flags indicate which information to log.</p> <p>/le Log all error messages to a file</p> <p>/lv Verbose output</p> <p>/l* Wildcard; Log all information, except verbose mode</p> <p>/l*v Wildcard; Log all information including verbose mode. This is the recommended logging level to use when you are troubleshooting installation issues.</p> <p>Example:</p> <pre>msiexec /i example.msi /le logfile.txt</pre>
---------------	--------------------------	--

MSIEXEC variables

Any of the following `MSIEXEC` parameters can be included when you implement command line installation of PC-Duo Host. Modify these directly in the `.MSI` file or apply them to a `.MST` transform file.

NOTE: These property values are case sensitive. Do not change other values in the `.MSI` file.

Property	Description
LICENSE	The required PC-Duo Host license key that is distributed with the purchase of the software.
HOSTSETTINGS	The required PC-Duo Host configuration properties that are passed to the PHSETUP utility. See "Configure Host from the command line" .
ARPSYSTEMCOMPONENT	Setting this value to "1" disables the ability to Add/Remove/Modify the product via the Control Panel. NOTE: Default value "0" allows users to modify the program through Add/Remove Programs.

TRANSFORMS	Use the TRANSFORMS property to specify any transforms (*.MST files) to be applied to the installation package. You can separate multiple transforms with a semicolon. Do not use the semicolon character in the name of your transform because it will be interpreted as a separator.
INSTALLDIR	Specify the directory in which to install the software.
REBOOT { Force Suppress ReallySuppress }	<p>Force: Always prompt for a reboot at the end of the installation</p> <p>Suppress: Suppress prompts for a reboot at the end of the installation</p> <p>ReallySuppress: Suppress all prompts for reboots during the installation.</p> <p>NOTE: The PC-Duo installer is configured to reboot at the end of a silent installation, unless otherwise overridden by the REBOOT parameter. This is true for both the MSI and the Setup.exe.</p>
NOFIREWALLCONFIG	Turn off automatic registration of PC-Duo Host as an exception to Windows Firewall. If this is set to a non-blank value, no firewall configuration is done by the installer. The default is that this property is not set, and the installer does the firewall configuration.
ADDLOCAL	Used to skip installation of the "Remote Printing Support" component. If not specified, ALL components are installed. To not install Remote Printing, specify: "ADDLOCAL=Host,Common"

Examples

The following examples use command lines to install PC-Duo Host:

- ◆ MSIEXEC
- ◆ Start/Wait

MSIEXEC

The following two examples use command lines to install PC-Duo Host using `msiexec`.

- ◆ The first example silently runs the PC-Duo Host installer file located in the `C:\Program Files\Vector Networks\Host` directory and suppresses the REBOOT at the end of the installation, and then, through PHSETUP commands, assigns the Host computer name to "apple," sets the password to "core."

```
msiexec /qn /I Host.msi LICENSE=1234567890 REBOOT=Suppress  
HOSTSETTINGS="name:apple password:core" INSTALLDIR="c:\Program  
Files\Vector Networks\Host"
```

NOTE: For the MSI install, follow the `/I` immediately by its parameter, the package name.

- ◆ The second example silently runs the PC-Duo Host installer file `Host.msi` and applies the transform file `STANDARDHOST.MST`. Transform files can be created using the PC-Duo Deployment Tool. This example assumes all files are in the current working directory with the appropriate paths specified as needed.

```
msiexec /qn /I Host.msi TRANSFORMS="StandardHost.mst"
```

Start/Wait

The following example is identical to the `msiexec` example, except that it uses the `start/wait` syntax to wait for the installation to be complete before continuing in a batch file.

```
start/wait msiexec /qn /I Host.msi LICENSE=1234567890  
REBOOT=Suppress HOSTSETTINGS="name:apple password:core"  
INSTALLDIR="c:\Program Files\Vector Networks\Host"
```

Lock-down settings

Use the PC-Duo Host lock-down feature to set individual settings to permanent values.

◆ "Lock Host settings"

◆ "Unlock Host settings"

The lock-down feature differs from setting permissions in several ways:

- ◆ Settings lock-down is granular. Individual settings can be locked down. The security features work on groups of settings, not individual ones.
- ◆ Settings lock-down is permanent. Once a setting is locked down, it cannot be changed again (without resetting the entire lock-down). The security features control who can change different groups of settings, but do not restrict the specific changes that are allowed.
- ◆ Settings lock-down is extremely secure. Because of the security applied to the registry key, only members of the authorized administrative group can remove the lock-down. If the group is a domain-level group, local administrators of a computer cannot change the lock-down policy.

Lock Host settings

Lock down one or more PC-Duo Host settings, so that any PC-Duo Host users (even users who have administrative privileges) cannot modify them. You must first create and then be a member of a group named `Remote Control Host Admins` to lock down any PC-Duo Host settings. This group can either be a local (computer-specific) group or a domain group. For NT compatibility (which doesn't support a group name of this length), use the name `RC Host Admins`. If this is the case, then you must either be a member of `RC Host Admins` or `Remote Control Host Admins`.

To lock down any PC-Duo Host settings, run the `PHSETUP` program with the special name/value pair `mode:lockdown` as the first entry on the command line. Follow this with a list of settings that you want to lock down, along with their values. For information on using `PHSETUP`, see ["Configure Host from the command line"](#). When you are finished, stop the PC-Duo Host service from **Control Panel > Administrative Tools > Services**, and then restart it to activate the lock-down.

The affected settings are visible but disabled in PC-Duo Host. Once settings are locked down, you can lock down other settings by running `PHSETUP` with the `mode:lockdown` keywords, and include additional feature/value pairs.

NOTE: Some settings must be locked down together. In particular, locking down one network protocol locks down all network protocols. For example, if you run `PHSETUP mode:lockdown ipx:off` from the command line, `IPX` is never enabled, but additionally the `IP` setting is completely locked.

Unlock Host settings

Locked down settings must be unlocked all at once. Settings cannot be unlocked individually.

To unlock PC-Duo Host features, you must be a member of the group used to create the lockdown originally (either `RC Host Admins` or `Remote Control Host Admins`).

That group must be have the same authority (local machine or domain) as the original lockdown. Before you do so, stop the PC-Duo Host service, from **Control Panel > Administrative Tools > Services**.

To unlock PC-Duo Host settings, follow these steps:

- 1 Run **regedit**, and navigate to HKLM\Software\Funk Software, Inc.\Proxy v5\Proxy Host Restrictions.
- 2 Remove this registry key which stores the settings lock-down.
- 3 Restart the PC-Duo Host service.

NOTE: *This registry key is protected. Consequently, only members of the Remote Control Host Admins group can do this.*