



PC-Duo Host Guide

Release 11.6
June 2010

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

© Copyright 2010 Vector Networks Technologies and Proxy Networks, Inc. Certain portions under copyright by Funk Software, a division of Juniper 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. 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 (eay@cryptsoft.com), and compression software from the ZLIB project (<http://www.zlib.net/>).

Table of Contents

PC-Duo overview	7
What's New with PC-Duo 11.6	8
PC-Duo solutions.....	10
PC-Duo Express	10
PC-Duo Enterprise.....	10
PC-Duo applications.....	11
PC-Duo Host.....	11
PC-Duo Master	11
PC-Duo Gateway	12
PC-Duo Deployment Tool.....	13
PC-Duo technologies.....	14
PC-Duo services.....	15
PC-Duo connection types.....	16
Peer-to-peer connections.....	18
Gateway-managed connections	19
Firewall-friendly connections	20
Terminal services connections	20
VNC connections	22
PC-Duo security features	23
Authentication	24
Authorization	27
Auditing	27
Encryption	27
PC-Duo networking features	29
Network protocols	29
Network addressing schemas.....	29
PC-Duo documentation and technical support.....	30
Typographical conventions in documentation	30
Technical support options.....	31
Host Installation.....	33
Requirements	34
Operating system requirements.....	34
Terminal Services requirements.....	34
Hardware requirements	34

PC-Duo Host Guide

Installation requirements.....	35
Network requirements.....	35
Installation notes.....	36
Install via <code>msiexec</code> command line utility.....	36
Install via internet download.....	36
Install via Deployment Tool.....	36
Install via 3rd-party imaging tools.....	36
Configure security settings.....	40
Configure network settings for IPX.....	41
<i>Licensing</i>	42
Add a license key before your trial period expires.....	42
Add a license key after your trial period expires.....	42
Upgrade a license key.....	43
Host Operation.....	45
Start the Host Control Panel.....	46
Status tab.....	48
General tab.....	49
Security tab.....	51
Simple password configuration.....	51
Windows authentication configuration.....	52
Shared secret password authentication.....	65
Options tab.....	66
Keyboard and mouse suppression.....	66
Action on disconnect or termination.....	67
Confirm Host Options Settings.....	67
Access tab.....	68
Access restrictions.....	68
Connection permission.....	69
Effects tab.....	71
Protocols tab.....	73
Select ciphers.....	74
TCP/IP address restrictions.....	75
Gateways tab.....	77
Manage Gateway order.....	78
Add Gateway.....	78
Edit Gateway.....	80
Remove Gateway.....	81

Move Up.....	81
Move Down	81
Details	81
Resend Status	81
View Error	82
Screen tab	83
Bandwidth throttling	85
About tab	88
Add a license key.....	89
Generate a System Information report	89
Terminal Services tab.....	91
Configuring the TS Host.....	91
Setting Users for TS Hosts	94
Open chat window	106
Set up remote printing	107
Configure remote printer settings	107
Command Line Configuration	109
Configure Host from the command line.....	110
PHSETUP command line syntax	111
Syntax that waits for command completion	111
PHSETUP syntax examples	112
PHSETUP access parameters	114
PHSETUP control parameters.....	117
PHSETUP effects parameters	121
PHSETUP error handling.....	123
PHSETUP Gateways parameters.....	124
PHSETUP general parameters.....	126
PHSETUP license parameter	128
PHSETUP options parameters	129
PHSETUP protocol parameters.....	130
PHSETUP security parameters	133
PHSETUP Windows security parameters.....	135
Install Host with the MSIEXEC command line	139
MSIEXEC options	139
SETUP.EXE options	140
MSIEXEC variables	141
Examples	143

PC-Duo Host Guide

Lock-down settings.....	145
Lock Host settings.....	145
Unlock Host settings	145

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.
- ◆ **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 with PC-Duo 11.6

PC-Duo 11.6 introduces the following new features and capabilities:

◆ **Terminal Services Host configuration:** The Root Host can be configured to restrict the injection of a Host image to Terminal Services sessions that meet predetermined criteria (previously, the Root Host injected a Host image into every TS session). The criteria for determining which TS sessions should receive a Host image are available on the Terminal Services tab in the Root Host control panel.

What's New with 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.

◆ **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.

What's New with PC-Duo 11.3

◆ **Terminal Services support:** PC-Duo 11.3 supports server-side Hosts for thin client, terminal services sessions for Citrix XenApp (formerly Citrix Presentation Server) and Windows Terminal Server.

◆ **User-Mode Screen Capture optimization:** PC-Duo 11.3 includes significant performance and reliability enhancements for user-mode screen capture technology introduced in PC-Duo 11.2.

What's New with PC-Duo 11.2

PC-Duo 11.2 introduced the following new features and capabilities:

◆ **Windows Vista and Server 2008 support:** PC-Duo 11.2 applications (Host, Master, Gateway, Deployment Tool) now run on Windows Vista and Windows Server 2008 operating systems.

NOTE: *PC-Duo 11.2 introduces a new screen capture technology (user-mode) for Windows Vista and Windows Server 2008 platforms.*

- ◆ **Bandwidth throttling:** PC-Duo 11.2 allows screen capture settings to be modified in order to reduce the amount of bandwidth used. Usually, this will reduce screen capture quality but improve responsiveness and overall performance (see *PC-Duo Host Guide* for more information).
- ◆ **Popup notifications:** PC-Duo 11.2 supports popup "toast" notifications when connections are established to remote computers (see *PC-Duo Host Guide* for more information).
- ◆ **Send keystroke button:** PC-Duo 11.2 now provides a new toolbar button on the Master Connection Window, which can be configured to send Ctrl+Alt+Del or one of the other available keyboard combinations to remote computer (see *PC-Duo Master Guide* for more information).
- ◆ **Host-based chat:** PC-Duo 11.2 introduces support for Host-based chat. This new service automatically creates a private chat room including Host user and any technicians connected to the Host. Technicians can see and participate in multiple chat rooms simultaneously (see *PC-Duo Master Guide* for more information).
- ◆ **File transfer resume:** Occasionally, a file transfer operation is interrupted when a connection is lost. PC-Duo 11.2 introduces the ability to resume interrupted file transfers exactly from the point of interruption (see *PC-Duo Master Guide* for more information).
- ◆ **Windows Media format support:** PC-Duo screen recording files are produced in a streamlined, proprietary format and play back in a viewer provided with PC-Duo Master. PC-Duo 11.2 introduces a new utility to enable technicians to convert PC-Duo screen recording files into Windows Media format for play back in WM-compatible players and editing in off-the-shelf media tools (see *PC-Duo Master Guide* for more information).

PC-Duo solutions

Vector Networks provides two solutions for remote desktop support:

PC-Duo Express

PC-Duo Express 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

PC-Duo Enterprise 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 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 Features	PC-Duo Express	PC-Duo Enterprise
Components		
PC-Duo Host	Yes	Yes
PC-Duo Master	Yes	Yes
PC-Duo Gateway	No	Yes
PC-Duo Deployment Tool	Yes	Yes
Connection Types		
Peer-to-peer connections	Yes	Yes
Gateway-managed connections	No	Yes
Firewall-friendly connections	No	Yes
Terminal services connections	No	Yes
VNC connections	Yes	No

PC-Duo applications

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

PC-Duo Applications	PC-Duo Express	PC-Duo Enterprise
PC-Duo Host	Yes	Yes
PC-Duo Master	Yes	Yes
PC-Duo Gateway	No	Yes
PC-Duo Deployment Tool	Yes	Yes

PC-Duo Host



PC-Duo Host is an agent application that enables remote support connections to be established to the machine on which it runs. 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.

PC-Duo Host can now be installed in server-side terminal sessions for application virtualization solutions such as Citrix XenApp and Microsoft Terminal Server.

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.
- ◆ 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.
- ◆ 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 Administrator 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 for Windows XP, Windows Server 2003 and older platforms. 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 for Windows Vista and Windows Server 2008 remote computers. 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
- ◆ **Host Administration:** ability to view and edit configuration settings of the PC-Duo Host installed on the remote machine

For more information, see *PC-Duo Master Guide*.

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	PC-Duo Enterprise
Peer-to-peer connections	Yes	Yes
Gateway-managed connections	No	Yes
Firewall-friendly connections	No	Yes
Terminal services connections	No	Yes
VNC connections	Yes	No

RDP compatibility: 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 XP or Vista), 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: *This 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 2003 or Server 2008) can support multiple sessions simultaneously via Terminal Services; use the Terminal Services support in the Host to capture and/or provide input control to one or more sessions on server-class OS.*

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.

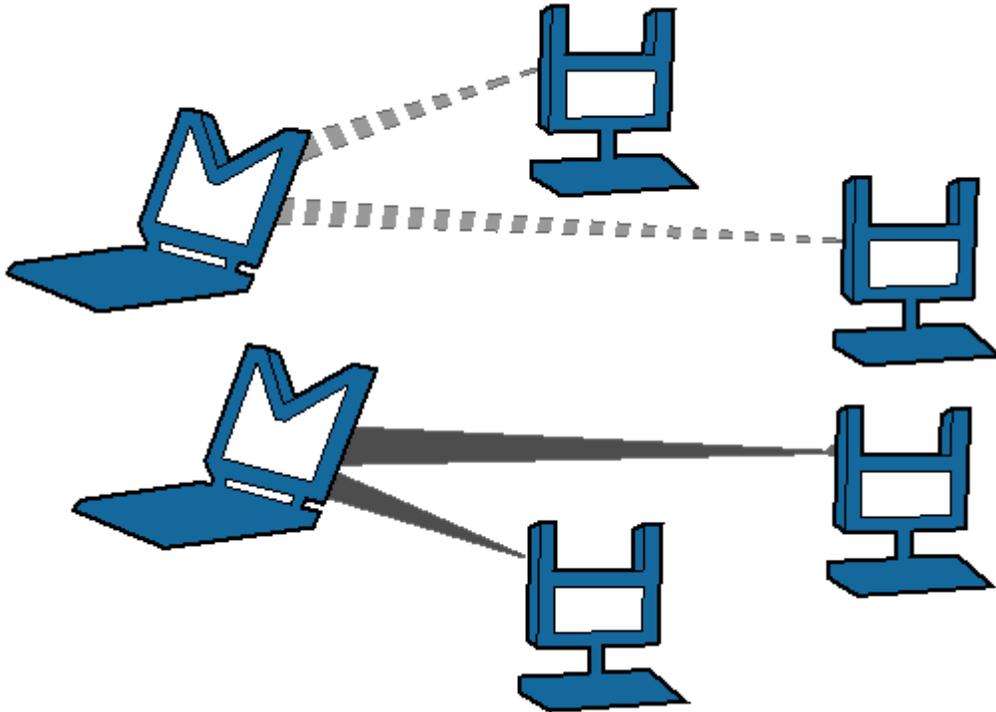
- ◆ **Explicit Wake-on-LAN:** A network administrator, using either PC-Duo Master or PC-Duo Gateway Administrator, can attempt to wake up a remote computer by explicitly sending the WOL signal to that machine. If the remote computer was shut down in a state capable of receiving WOL signal, it will wake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

See "Send Wake-on-LAN Signal" for more information.

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.

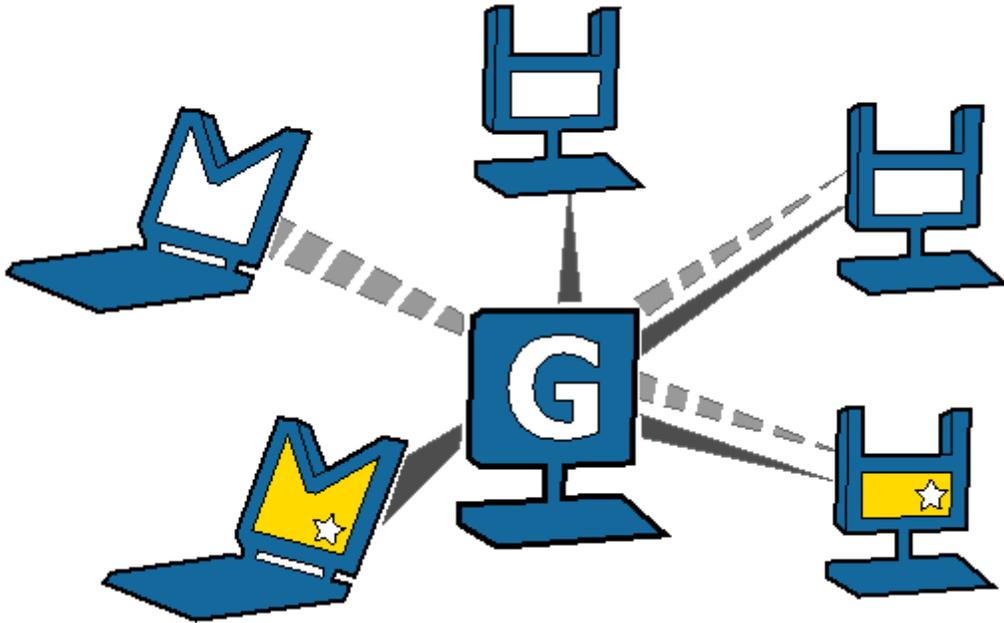
Gateway-managed connections

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.

Terminal services connections

PC-Duo provides server-side support (screen capture, input control, screen recording) for session-based virtual desktops hosted by Terminal Services on Windows Server 2003 or Windows Server 2008 (now called "Remote Desktop Services"). Windows Server creates and hosts the Terminal Services (TS) 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 remotied 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 TS 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 TS 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 Terminal Services clients as well as Citrix Presentation Server (now known as XenApp) clients.*

Note: *PC-Duo only supports TS sessions created on server-class Windows operating systems such as Windows Server 2003 and Windows Server 2008.*

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

Root Host for TS sessions

The "Terminal Services" feature of Windows Server 2003 and Windows Server 2008 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 TS session. A special version of the Host called the "root" Host must be loaded on the TS server (a "root" Host is a standard Host with a special TS 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 TS session is created.

Transient Hosts

Each TS 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 TS Hosts are considered transient, since they go away when the TS user logs out of his/her session. In order to keep track of transient TS Hosts, the PC-Duo Gateway will create a new Group called "Terminal Services on <Servername>", and automatically insert transient Hosts into this Group. They are automatically deleted from the Gateway when the TS session ends. The main purpose of this Group is to allow security to be assigned to the Hosts and TS sessions that belong to this Group, and to provide the correct and appropriate access to the TS-based Host instances.

Note: *PC-Duo Host for Terminal Services works on Server 2003 & Server 2008, and requires a Gateway Server v11.3 or later.*

Recording TS Hosts

Recordings are normally deleted from the Gateway database when their associated workstation record is deleted. Transient TS Host workstation records are automatically deleted from the Gateway when the TS user logs out of his/her session. However, to prevent recordings of TS Hosts from being automatically deleted when the TS session ends, the TS session recordings are reassigned to an artificial permanent workstation record called "Recordings on <Servername>". All recordings of all TS Hosts on a given TS 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,
- ◆ TS recordings can be kept separate from console (root Host) recordings
- ◆ Security can be configured separately for each recording.

Limitations of TS Hosts

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

- ◆ Remote printing
- ◆ 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 (even on Windows Server 2003, requires kernel-mode display support)

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. Support for Gateway-managed connections to VNC servers is expected in the next release.

See "VNC Hosts" 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 v10.5 "Leopard"
- ◆ Mac OS X v10.6 "Snow Leopard"
- ◆ Red Hat Linux Fedora 11

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	Master	Gateway	Yes

relationship			
◆ 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 and Secure Hashing Algorithm (SHA-1). 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 Express and PC-Duo Enterprise uses AES 256-bit encryption, however other encryption options can be set, including:

- ◆ AES encryption (256-bit key) with SHA1 hash
- ◆ AES encryption (192-bit key) with SHA1 hash

- ◆ AES encryption (128-bit key) with SHA1 hash
- ◆ Triple-DES (3DES) encryption (192-bit key) with SHA1 hash
- ◆ RC4-compatible encryption (128-bit key) with MD5 hash

NOTE: *PC-Duo 10.0 applications and older support only RC4 encryption; thus, this would be the encryption option negotiated between a PC-Duo 11.0 or later application (e.g. PC-Duo Master) and PC-Duo 10.0 application (e.g. PC-Duo Host).*

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

◆ **IPX:** IPX provides access to Novell NetWare servers. PC-Duo components support communications using this protocol.

◆ **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.

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.

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 Administrator 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

The 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

The 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 the Host, note the following:

- ◆ If you plan to use the Host with the Gateway, then install the Host after you install the Gateway. See the *Gateway Administrator Guide* before installing the Host.
- ◆ If you plan to deploy the Host using a 3rd party imaging tool, you must first prepare the Host software with the 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 XP
- ◆ Windows Server 2003
- ◆ Windows Vista
- ◆ Windows Server 2008
- ◆ Windows 7
- ◆ Windows Server 2008 R2

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

NOTE: *The Host 11.x does not support Windows 9X (98, 98SE, ME), Windows NT4, Windows 2000 and all operating systems on the IA64 (Itanium) processor architecture. Use the Host 10.x on these platforms.*

Terminal Services requirements

The Host can be configured to allow remote viewing & remote control of Terminal Services sessions in addition to the server console (see ["Terminal Services 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 2003
- ◆ Windows Server 2008
- ◆ Citrix Presentation Server 4.x
- ◆ Citrix XenApp

This feature works with Terminal 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 the Host:

- ◆ Windows Installer 2.0 or later – Required by the installer. If needed, this upgrade is applied automatically when the `setup.exe` installer image is run.
- ◆ Internet Explorer 4.0 or later – Required for online help.
- ◆ Local Administrator access rights – the Host runs as a Windows service on the local machine. Therefore, Local Administrator access rights are required for the user who is installing the Host on the machine.

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

Network requirements

The 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).
- ◆ IPX provides access to Novell NetWare servers. To enable communication using IPX, it is not necessary for any computer to be logged into a NetWare server, nor is it necessary to run a NetWare client. To enable communication using IPX, you must have the Microsoft NWLink IPX/SPX Compatible Transport (included with the operating system).
- ◆ 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 the UDP, TCP and SSL transports fully support IPv4 and IPv6 addressing.

Installation notes

The the 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

The Host can be installed manually by using the `msiexec` command line utility. For more information on using the `msiexec` utility, see [Install the Host with the MSIEXEC command line](#).

Install via internet download

The Host is distributed as part of 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 Deployment Tool

The Deployment Tool can be used to automatically deploy and install a standard or customized configuration of the Host on one or more computers in your network. See *Deployment Tool Guide* for information on configuring and operating the 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 the Host as part of an operating system image:

Generate unique HostIDs

Each the Host installation is identified by a unique identifier, called the HostID. This identifier is used by the 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 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 the Host is installed on an operating system that is then imaged, all of the machines will end up with the same HostID. the 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 Gateway directory.

NOTE: *This problem occurs independently of how the imaging or replication is done, and affects the 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 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 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

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

Remove duplicate Host IDs

If the 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, there is a utility called RmHostID; it appears in the *the 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 the 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 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

%VER%	Host software version number (e.g. "v10.0.2.1003")
%PLATFORM%	Host operating system platform (e.g. "Win2000")
%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 Terminal Services session Hosts

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

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

Configure security settings

If you run the 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 “the Host” and “the 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 the.

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

Configure network settings for IPX

All the components can be installed on one computer, as long as the individual system requirements for each component are met. If you install the Host and the Gateway on the same computer, they may both use the IPX protocol. However, the two products cannot share the same IPX socket. Consequently, if you install the Host and the Gateway on a computer that uses IPX, then you must either disable the IPX protocol for one of the applications, or assign a different IPX port to each application.

For information on how to enable or disable IPX for the Host computer (or for assigning ports), see "[Protocols tab](#)". For instructions on how to enable or disable the protocol for the Gateway, see the *Gateway Administrator Guide*.

Licensing

If you download this software 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 us directly. Your purchase provides an appropriate license key to use with the 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

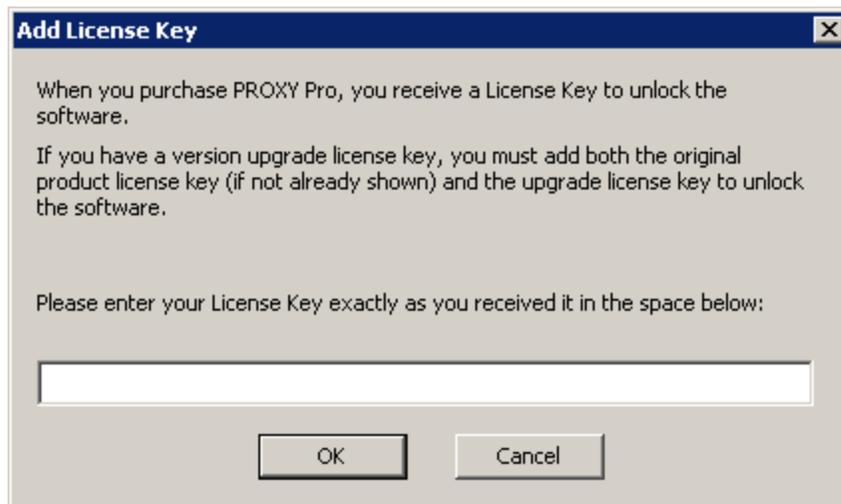
If you attempt to run the Host after your trial period has expired, the message **Thank you for trying** appears. Within the message, click **Add License and enter your new license key**.

Your license is activated immediately. You do not need to restart the 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 Start the Host Control Panel from the Windows Start menu.
- 2 Select the **About** tab from the 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 the Host.

NOTE: A Host that is meant to be used as the root for Hosts running in Terminal Services sessions will require a special license key that will specify the number of simultaneous TS sessions that can be supported (see [About tab](#) for more information).

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 Operation

The Host runs as a Windows service whenever you start up your computer. It can be configured to accept connections from a 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 Host.
- ◆ [“Gateway-managed connections”](#) between a Master computer and a Host computer through a Gateway. With these connections, authentication and authorization are enforced by the Gateway.

NOTE: By default, the Host allows the 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 Host Control Panel window for the Host computer. In addition, the default Gateway user account `RemoteControlGateway` also has full access. Other Master users must be added (see the [“Security tab”](#)) in order to have access to the Host.

The Host includes many configuration options, including:

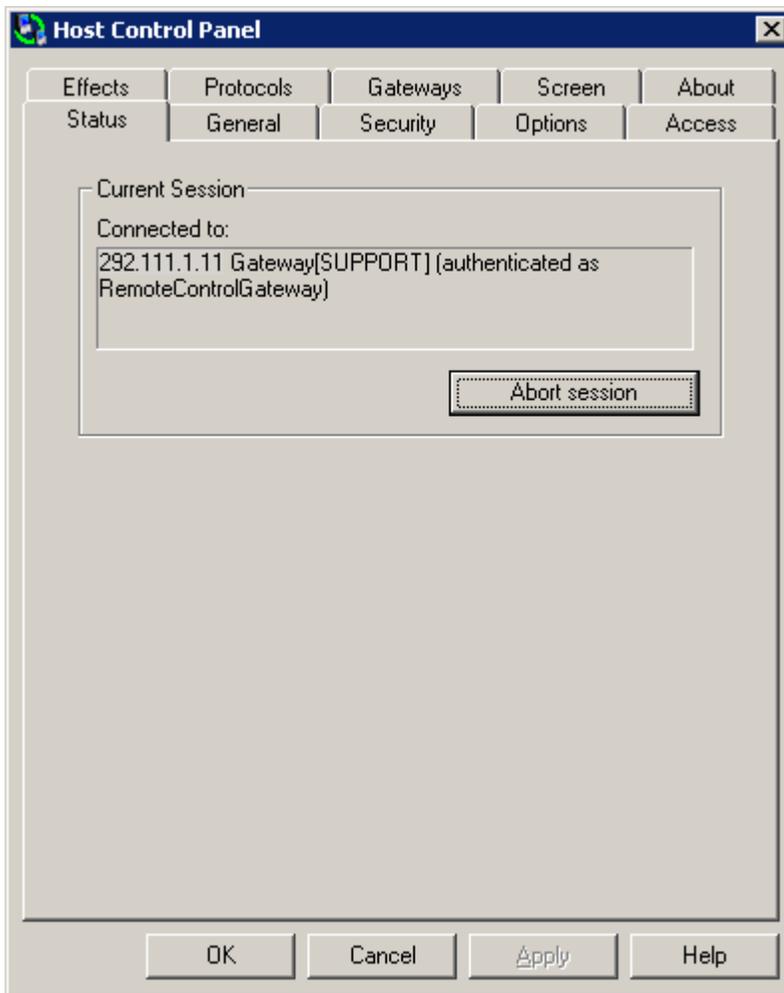
- ◆ [“About tab”](#): The ability to manage license keys and see system information about the Host.
- ◆ [“Access tab”](#): The ability to block remote access entirely.
- ◆ [“Effects tab”](#): The ability to control graphical effects transmitted from the Host.
- ◆ [“Gateways tab”](#): The ability of the Host computer to report to one or more the Gateways in your network. Access to the Host can then be centrally managed and monitored by the Gateways.
- ◆ [“General tab”](#): The ability to provide audible and/or visible notification on the Host computer when a 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 the features, to the Master users or groups.
- ◆ [“Status tab”](#): The ability to view current connection status and/or end active connection.
- ◆ [“Terminal Services tab”](#): The ability to view and manage configuration settings for Hosts operating in terminal services sessions.
- ◆ [“Open chat window”](#): The ability to enter private chat room with one or Master users connected to the Host.
- ◆ [“Set up remote printing”](#): The ability to set up remote printing.

Start the Host Control Panel

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

- ◆ Start the Host Control Panel from the Windows Start menu.
- ◆ Double-click the Host icon in your system tray (lower right corner of your monitor).
- ◆ Run the executable `phost.exe` located in the `the Host` program directory.

The Host Control Panel window appears.



NOTE: The default behavior of starting the Host Control Panel is to connect to the local Host instance; if Host is enabled for Terminal Services, the Host Control Panel will connect to the Host instance if run inside of a Terminal Services session, or the root Host if run from the physical console. This behavior can be overridden with switches – the “`phost.exe /root`” switch connects to the root Host. The “`phost.exe /tts`” switch connects

to the terminal services template settings for the Host instance. These command line switches are mutually exclusive, and cannot be used in conjunction with any other (undocumented) switches. See the [Terminal Services tab](#) for more information about root Hosts and Host instances for terminal services sessions.

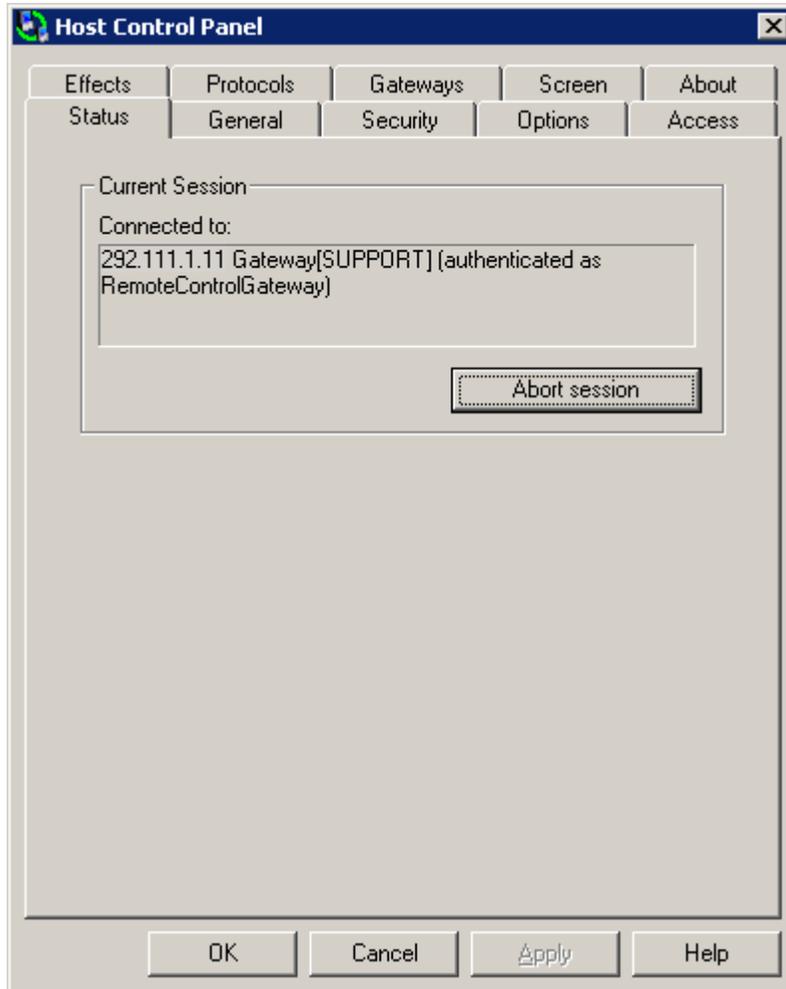
Use the Host Control Panel to configure the Host features through the following tabs

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 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.
About	To review information about the product.

NOTE: Some or all of the Host features may not be accessible, depending on how the Host is configured. Some features, such as Protocols 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.

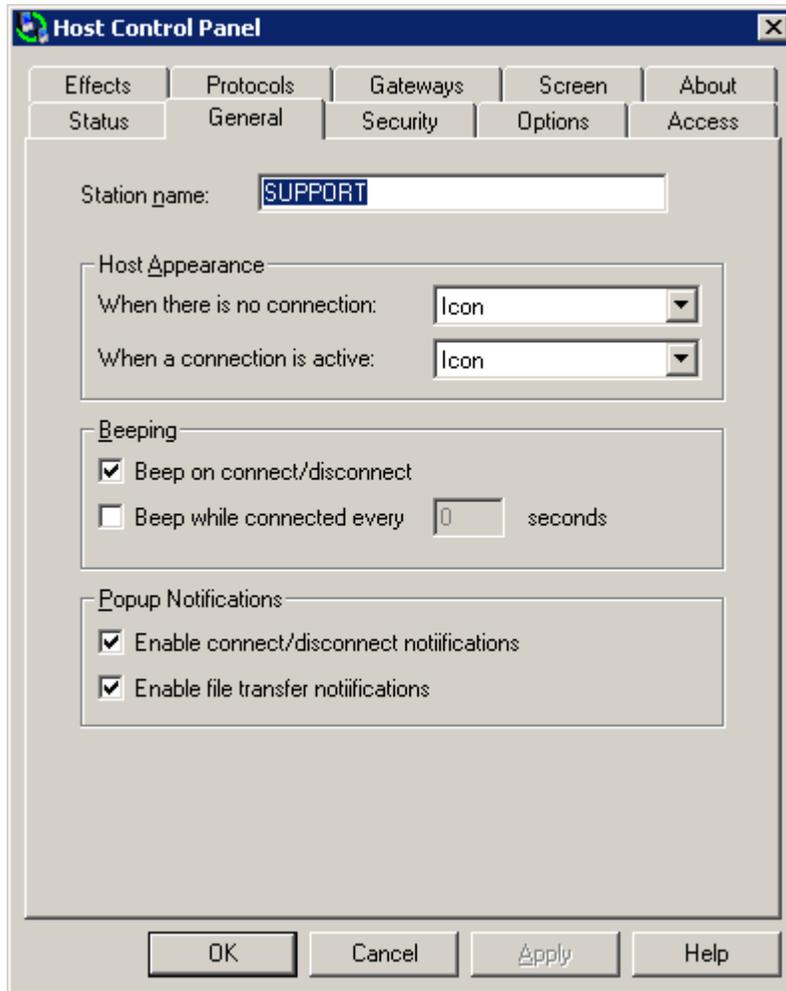


View the status of a remote connection to your Host computer as follows:

- ◆ Whenever there is a remote connection to your Host computer, the network address and username will appear in the **Connected to** field.
 - ◆ When a Master user makes a direct peer-to-peer connection to your computer, the Master user's account name and the network address will appear.
 - ◆ When a Master user makes a connection through a Gateway, the Gateway's network address and the 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 the Gateways and/or the Masters. To use macros to change the Station name automatically, see "[Change Station name](#)".
- ◆ **Host Appearance:** Configure the 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 the Host icon appears (or is hidden) when there is no active remote connection.
 - ◆ **When a connection is active:** The the Host icon appears (or is hidden) when a remote connection is active.
- ◆ **Beeping:** Set auditory cues to indicate when a 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** to see popup notifications when a Master user connects or disconnects from the Host.



- ◆ Select **Enable file transfer notifications** to see popup notifications when a Master initiates file transfer operations to/from the Host.

Security tab

To authenticate the identity of the 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”

Simple password configuration

For authentication that does not require network-based credentials, use a simple password to check the identity of the 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 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 Host settings on your Host computer (for any person to view or modify these settings locally) with the 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 the Host settings remotely; otherwise, only the local logged-in user can access and modify the 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 the Master users who request access to your Host computer. Select **Require Windows authentication** from the Security tab. The Host will check the credentials (username/password) of the 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 the Host Security Settings window appears.



One of the strongest features of the is the availability of fine-grained permissions. the 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 **Host Control Panel window**.
- ◆ “Settings Security tab”, defines permissions for modifying configuration settings for the **Host Control Panel window**.

An **access control policy**, comprised of a specific set of permissions, can be assigned to one or more the 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 Gateway domain user account with full access and administrative rights be configured on the Host computer.

NOTE: As long as the Gateway is on the known list of the 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 the Host security settings are set by default for Windows authentication:

- ◆ **Service Security:** The local machine's Administrators group and the default the Gateway domain user account (`RemoteControlGateway`) have full access to all the 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 the Gateway domain user account have full access to all administrative rights for this the 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 the Gateway domain user account have full access rights to all administrative settings for this the Host.

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

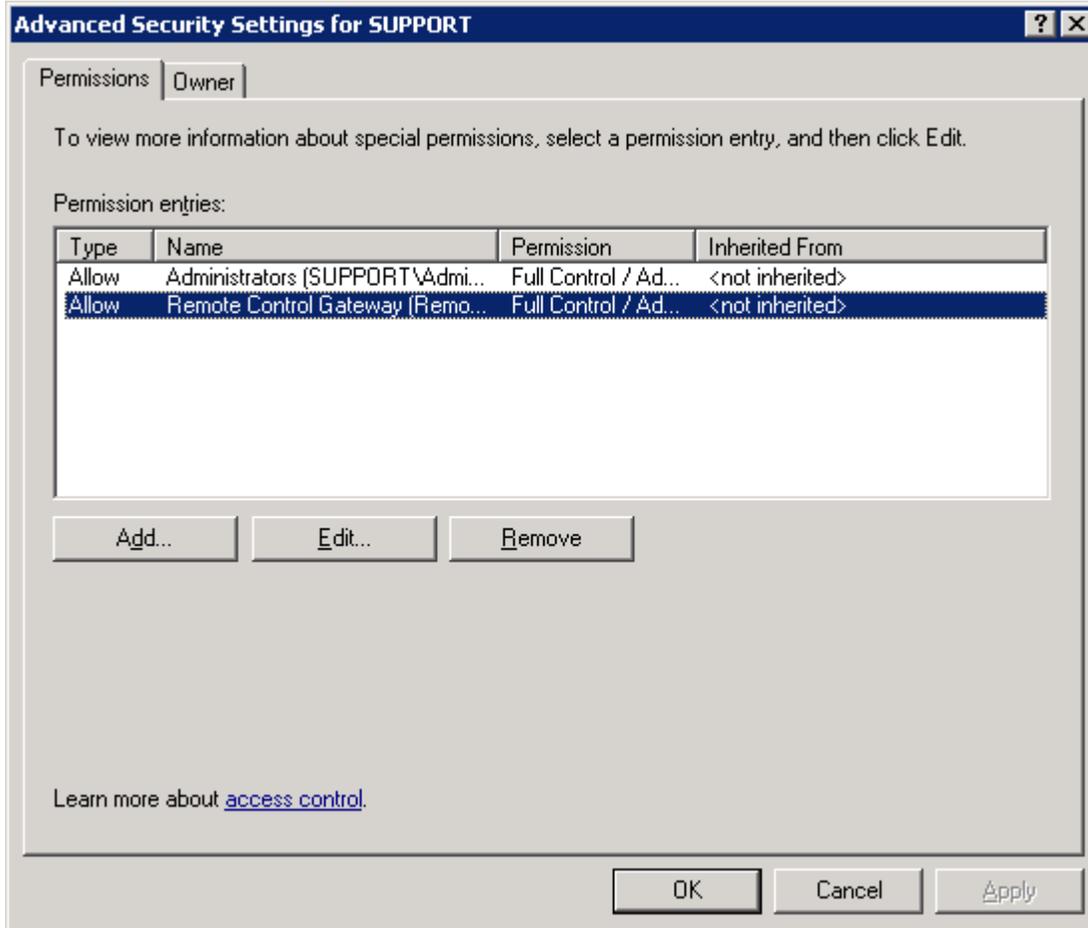
For any the Master user or group of users, set permissions for remote control services to the Host through the **Service Security** tab.



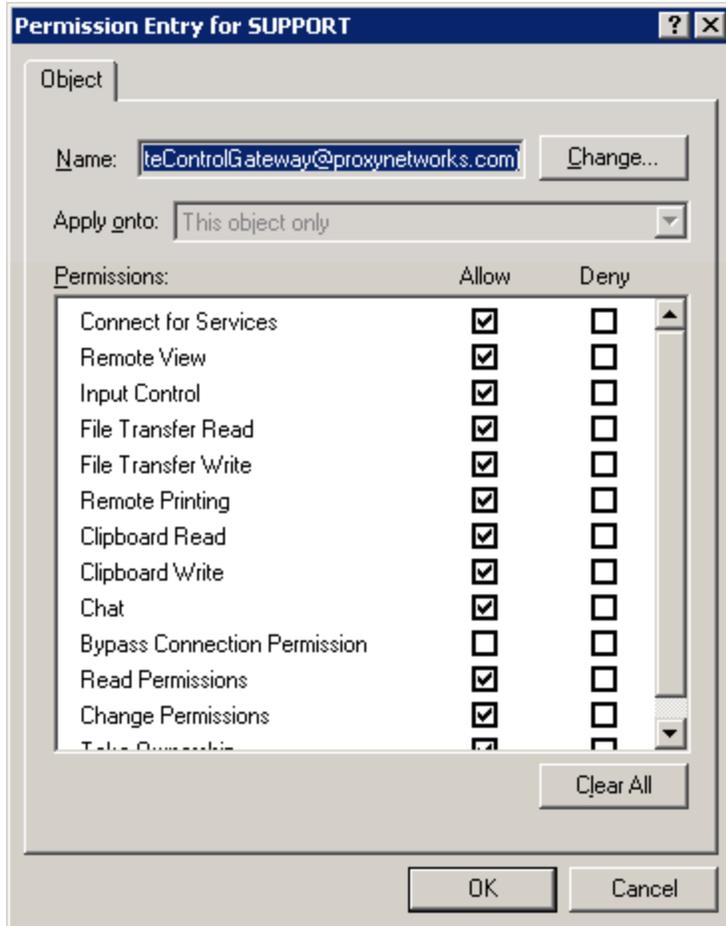
In the **Service Security** tab, you can perform the following tasks:

- ◆ Click **Add** to add a new the Master user or group for which you want to specify permissions.
- ◆ Select an existing the Master user or group that has permissions and click **Remove** to remove it.
- ◆ Select a 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.



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:

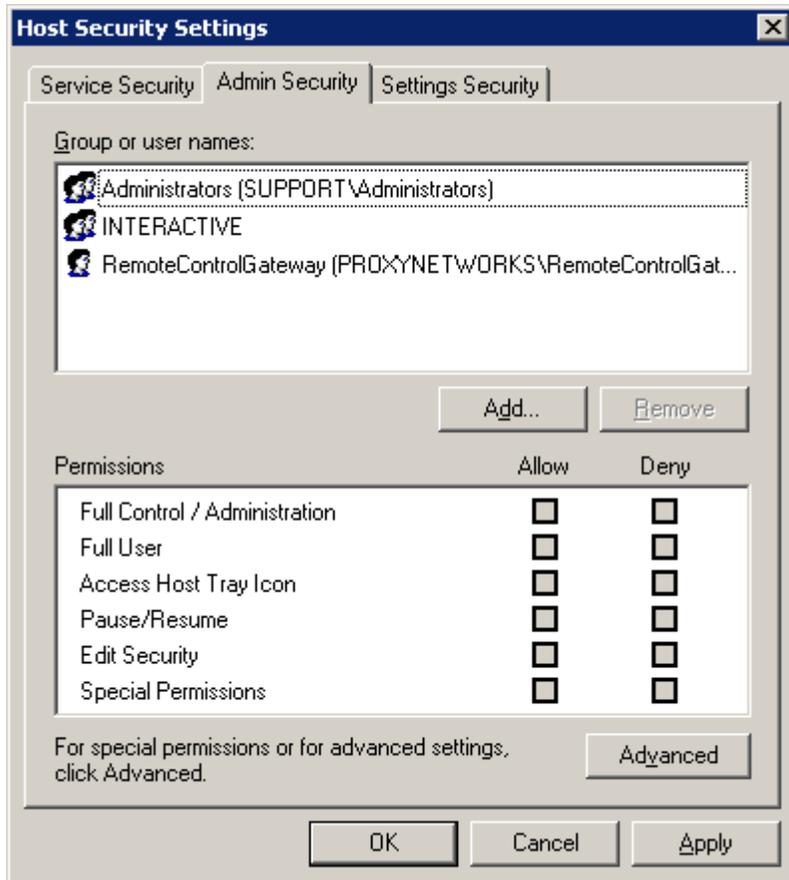
- ◆ **Connect for Services** determines whether a domain account or machine-local account has permission to connect to this the Host computer. It does not determine what a Master user can do once connected to this the Host computer, but you must (through this setting) allow the connection permission for a Master the Master user or the Gateway for the remote connection to occur.
- ◆ **Remote View** determines whether a a Master user or a group can view the screen of the Host computer once connected. Without this permission, the 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 Master user or a group as the ability to control the Host computer mouse and keyboard once connected. Without this permission, the Master users can only view the screen of the Host computer.
- ◆ **File Transfer Read** determines whether a Master user or a group has the ability to navigate to and read files that are located on the Host computer. Without this permission, the 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 Master user or a group has the ability to write files to the Host computer. Without this permission, the 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 Master user or a group can connect to the Host computer and use the remote printing feature. This feature allows the Master users to print from applications running on the Host computer to a printer connected to the Master computer. You must enable both the **Connect for Services** and **Remote Printing** permissions for the Master the Master users to print locally from remote applications.
- ◆ **Clipboard Read** determines whether a Master user or a group can copy information from the Host computer Windows clipboard to another application on the Master user's local computer.
- ◆ **Clipboard Write** determines whether a 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 Master user can be added to a private chat room including the Host user, and any other the Master users connected to the same Host.
- ◆ **Bypass Connection Permission** determines whether a Master user or group can connect to a 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 Master user or group can view the Service Security tab of the Host Security Settings window.
- ◆ **Change Permissions** determines whether a Master user or group can modify the permissions on the Service Security tab.
- ◆ **Take Ownership** determines whether a Master user or group can take ownership.

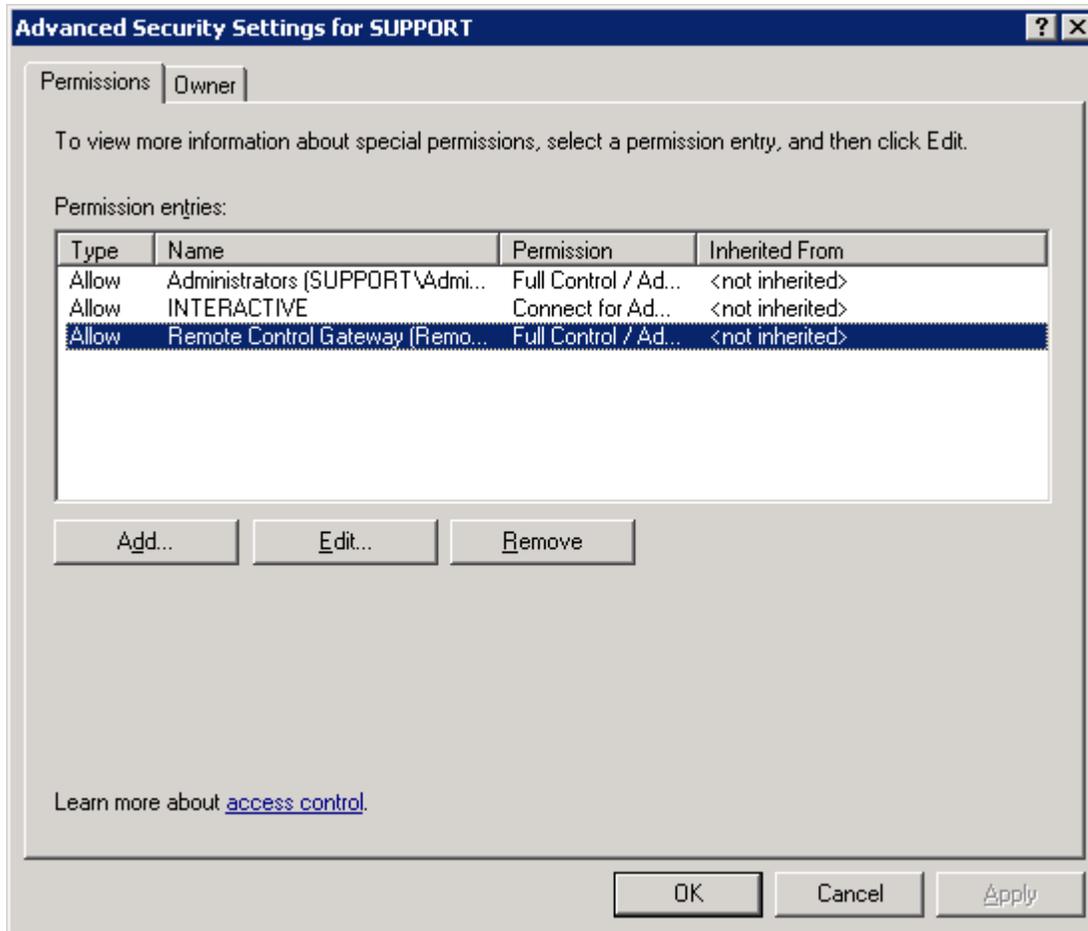
Admin Security tab

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

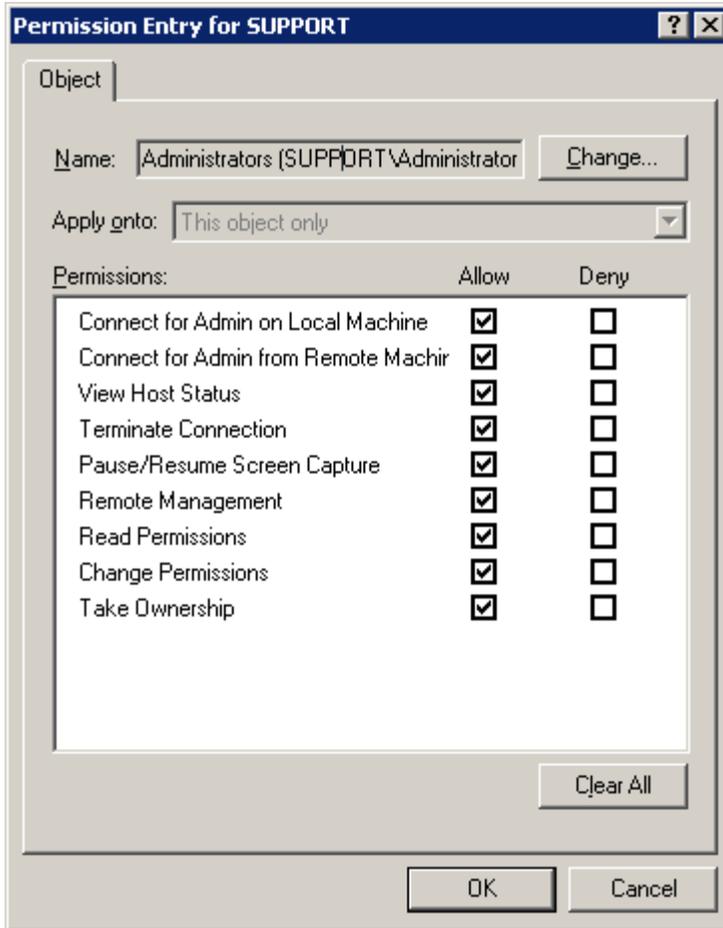


In the **Admin Security** tab, you can perform the following tasks:

- ◆ Click **Add** to add a Master user or group for which you will specify permissions.
- ◆ Select an existing the Master user or group that has permissions and click **Remove** to remove it.
- ◆ Select a 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 the 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.



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:



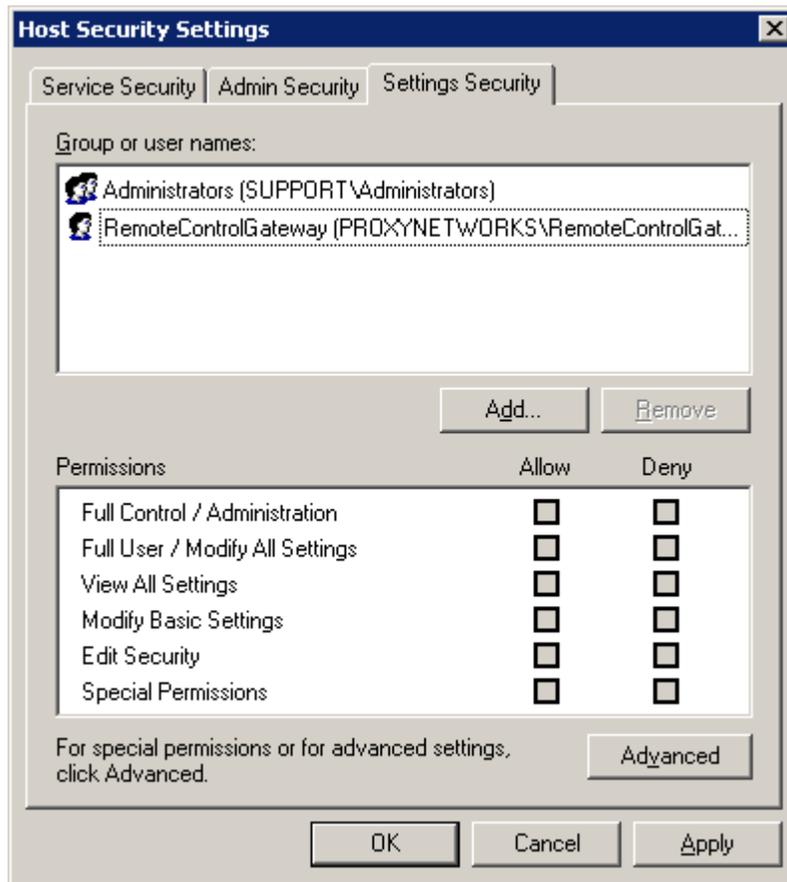
Each advanced permission is treated individually; click **Allow** or **Deny** for any of them. The following permissions exist:

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

- ◆ **Read Permissions** determines whether a Master user or a group can view the **Admin Security** tab of the Host **Security Settings** window.
- ◆ **Change Permissions** determines whether a Master user or a group can modify the **Admin Security** tab permissions.
- ◆ **Take Ownership** determines whether a Master user or a group can take ownership.

Settings Security tab

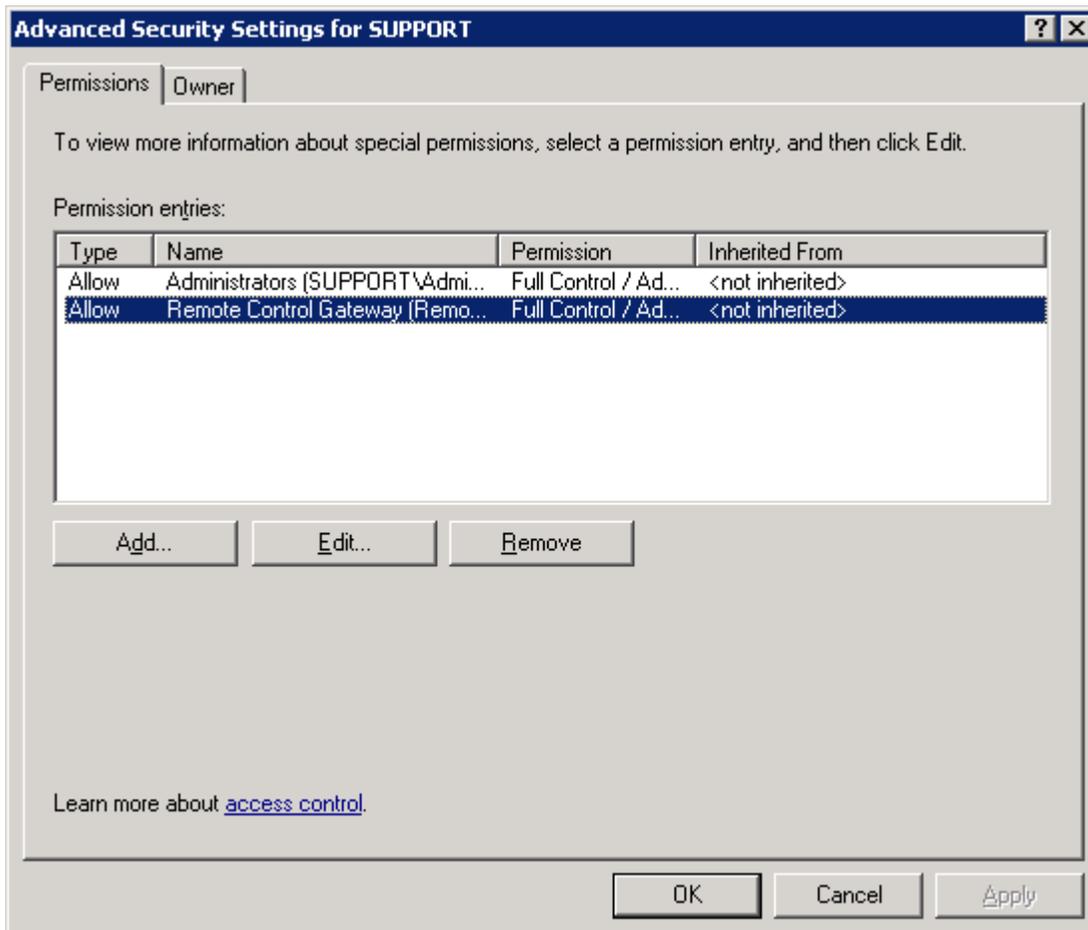
Administrative settings for the Host Control Panel window can be modified in the **Settings Security** tab.



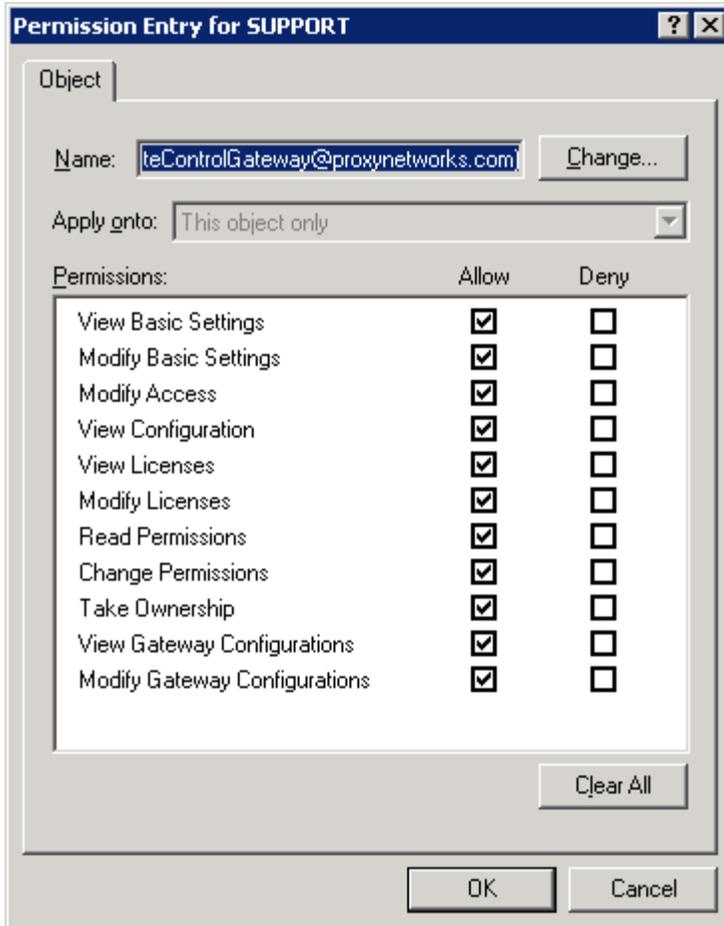
In the **Settings Security** tab, you can perform the following tasks:

- ◆ Click **Add** to add a Master user or group for which you will specify permissions.
- ◆ Select an existing the Master user or group that has permissions and click **Remove** to remove it.
- ◆ Select a 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 Master user or a group can modify basic the Host settings. This feature does not allow the 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 Master user or group can view the basic the Host settings.
- ◆ **Modify Basic Settings** determines whether a Master user or group can modify basic the Host settings. This feature does not allow the 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 Master user or group can modify the items on the **Security** and **Access** tabs.
- ◆ **View Configuration** determines whether a Master user or group can read the names and version numbers of the Host components for diagnostic purposes.
- ◆ **View Licenses** determines whether a Master user or group can read the list of installed license keys on the **About** tab.

- ◆ **Modify Licenses** determines whether a Master user or group can add license keys via **Add License** button on the **About** tab.
- ◆ **Read Permissions** determines whether a Master user or group can view the **Settings Security** tab of the Host **Security Settings** window.
- ◆ **Change Permissions** determines whether a Master user or group can modify permissions on the **Settings Security** tab.
- ◆ **Take Ownership** determines whether a Master user or group can take ownership.
- ◆ **View Gateway Configurations** determines whether a Master user or group can read the settings on the **Gateways** tab.
- ◆ **Modify Gateway Configurations** determines whether a 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 the Gateway (i.e. a Gateway listed on the **Gateways** tab), Windows Authentication will fail (the Host cannot authenticate the 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 Host and the 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 Gateway first communicate with each other, and is unique to each the Gateway - Host pair.

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

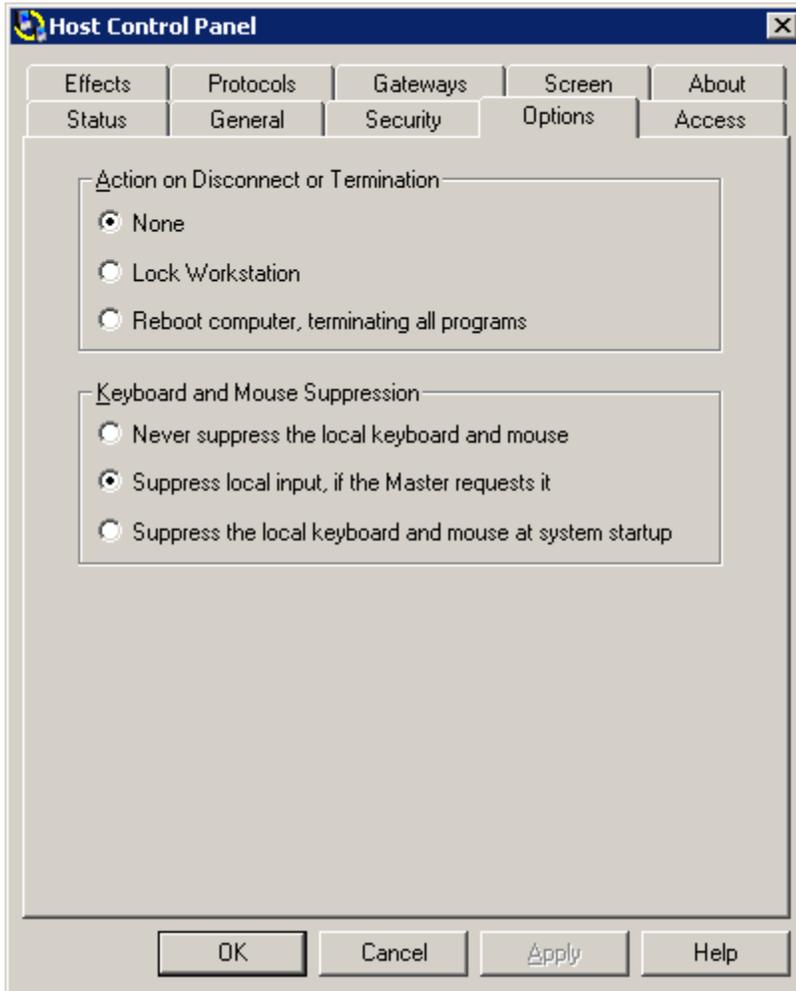
On all subsequent connection attempts when the Host and the Gateway are not in the same domain, the shared secret password will be presented and accepted for authentication (because it is known only to the Host and the Gateway). No configuration change is required and the Host security remains set at 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 Gateway is on the known list of the 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. 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.
- ◆ **the Gateway requests a connection and Host security is set to Simple Password:** Previously, the Host did not ask for a password from the Gateway. Now, the 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.

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.



The following 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 the Master users, but you can override them. For more information, see “[Confirm Host Options Settings](#)”.

Keyboard and mouse suppression

The keyboard and mouse of your Host computer behavior can be configured with the following options:

- ◆ 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.
- ◆ 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 Master user requests it. The default settings for the Host and the 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 the Host Options Settings](#)".

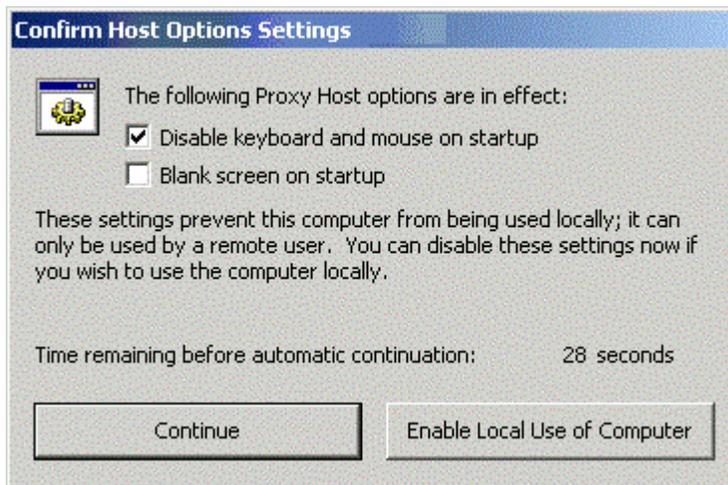
Action on disconnect or termination

The the Master user can arrange for certain events to occur after a remote control connection is terminated:

- ◆ Select **None** for the termination of a Master user connection to have no effect on the Host computer.
- ◆ 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.

Confirm Host Options Settings

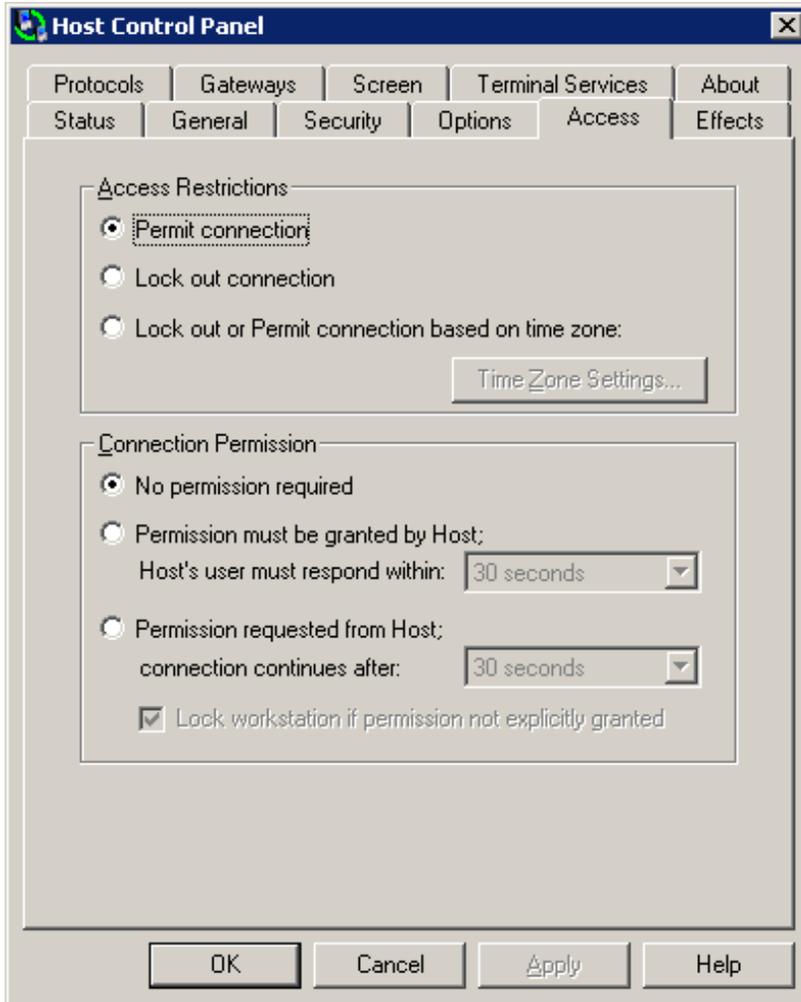
Even if the Host is configured to give the Master user control over the keyboard, mouse and display during a remote control connection, the Host user is given the opportunity to override such settings on startup of your Host computer.



From the time the **Confirm Host Options Settings** window appears, you have 30 seconds to click **Enable Local Use of Computer**. If you click **Continue**, the preemptive settings remain in effect and you 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.

Access restrictions

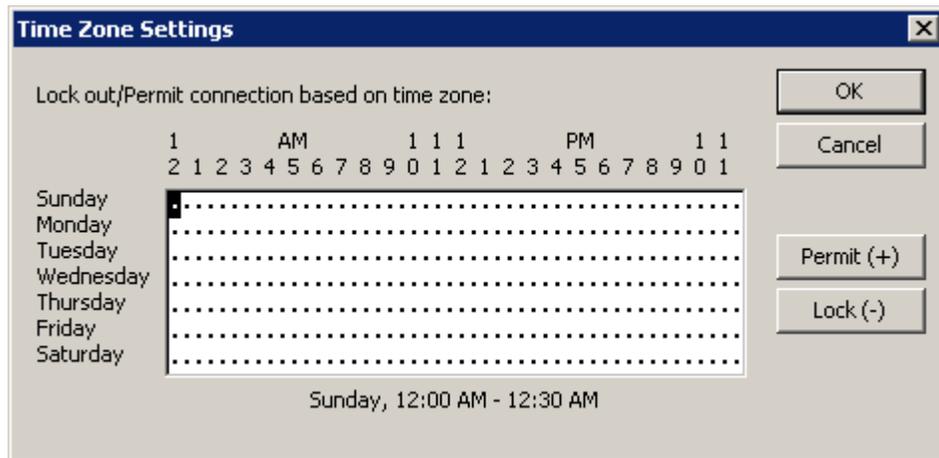
Lock out access to this Host computer:

- ◆ Select **Permit connection** (default) to permit remote connections from any authenticated the Master users to your Host computer.
- ◆ Select **Lock out connection** to prevent remote connections from any the 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 the Master user at any time.
- ◆ Select **Permission must be granted by Host** if you want to grant an authenticated the 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

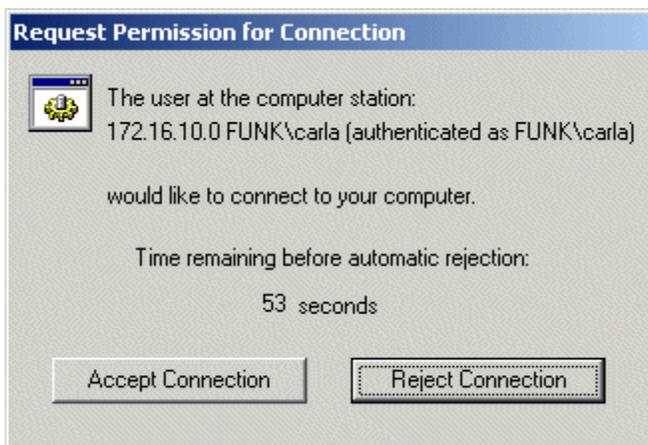
2 minutes) within which you want to make a decision. If you do not respond within the specified time, the request is rejected automatically.

◆ Select **Permission requested from Host** if you want to grant an authenticated the 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.*

Permission for connection

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



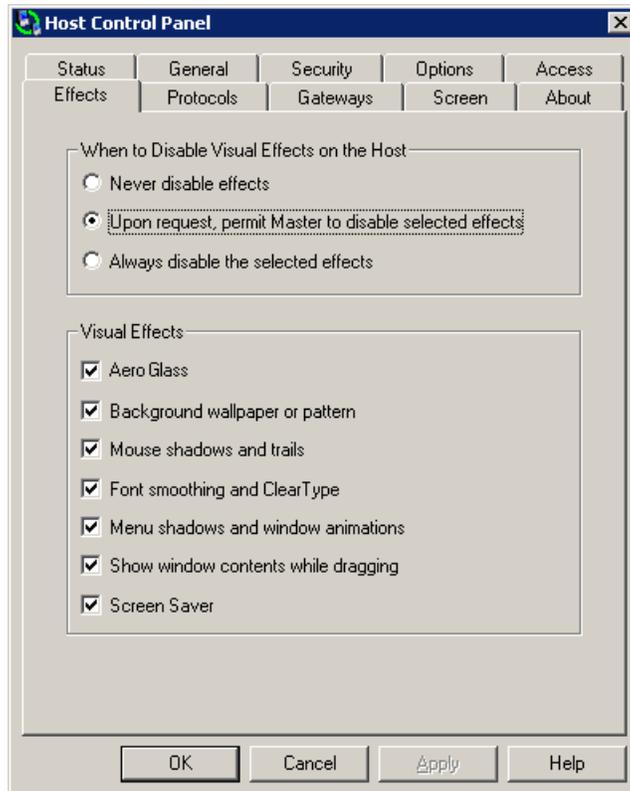
If Connection Permission is set to **Permission must be granted by Host**, then the Host user must respond within the time period or the connection request will be rejected.

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.

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 the 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 the 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 the Master user to have control over.

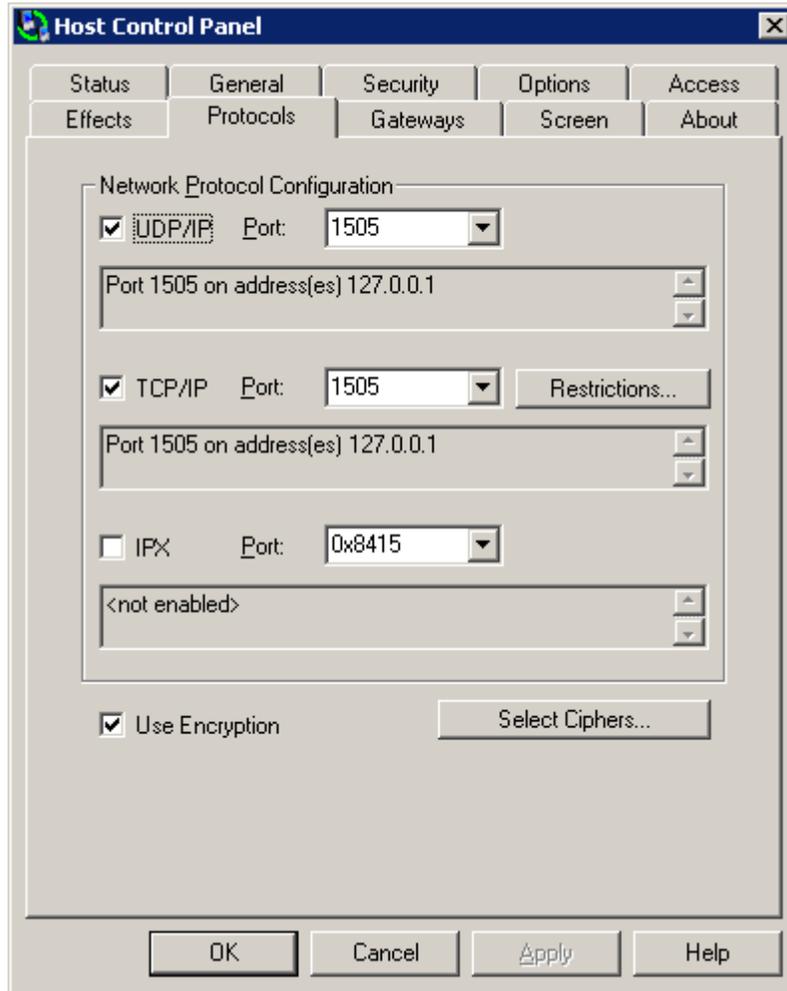
The particular visual effects that are enabled or disabled are controlled by the settings you check under **Visual Effects**:

PC-Duo Host Guide

- ◆ Aero Glass (desktop composition)
- ◆ Background wallpaper or pattern
- ◆ Mouse shadows and trails
- ◆ Font smoothing and ClearType
- ◆ Menu shadows and Windows animations
- ◆ Show window contents while dragging
- ◆ Screen Saver

Protocols tab

Configure the network protocols and ports for communication with the 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: the 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: *the Host can be installed on a computer that is also running the 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 the Host, or choose an alternate port (other than **Standard**) for IPX in either the Host or the Gateway.*

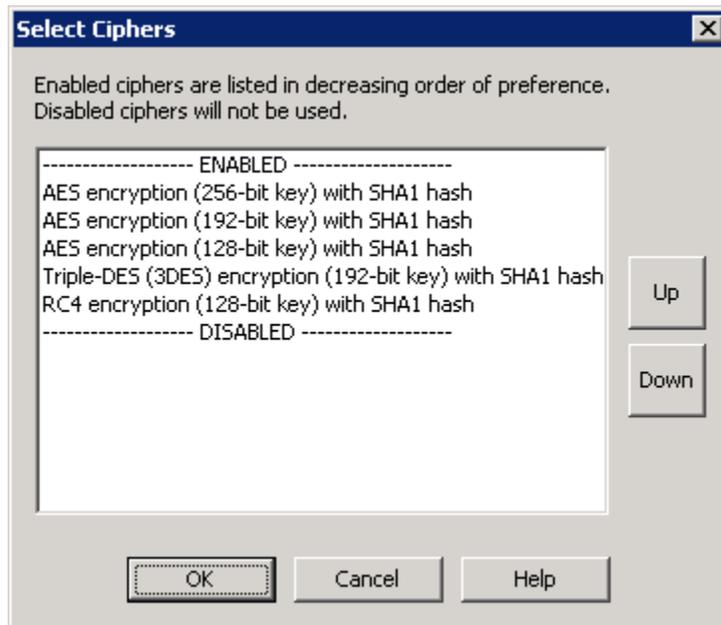
Select ciphers

When the Master or the Gateway requests a connection to the Host, the two applications negotiate to determine the highest level of encryption that is supported by both. For example, the Master 11.2 will try to use AES 256-bit encryption by default but a Host 11.0 might be configured to use Triple-DES; in that case, the two applications will agree to use Triple DES).

NOTE: *Older the 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.

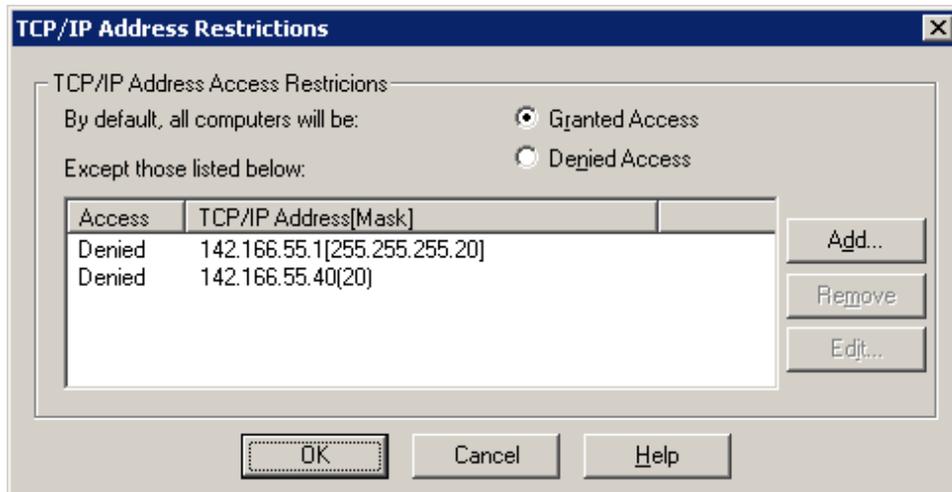
Specific configurations can be disabled by moving them below the “DISABLED” line; in that case, they will never be considered by the Host:



- ◆ 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 Host over TCP can be restricted according to the IP address of the Gateway or the 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.

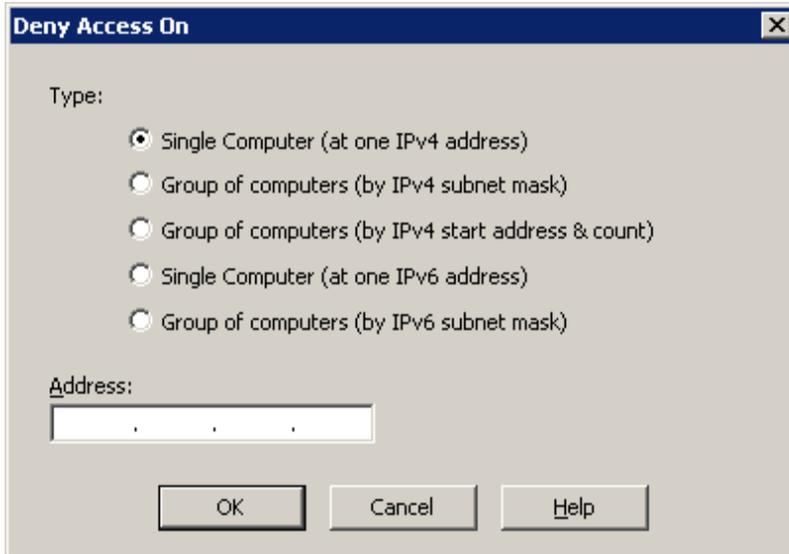
Configure the policy as follows:

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

Adding, editing, or removing a TCP/IP address exception

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.

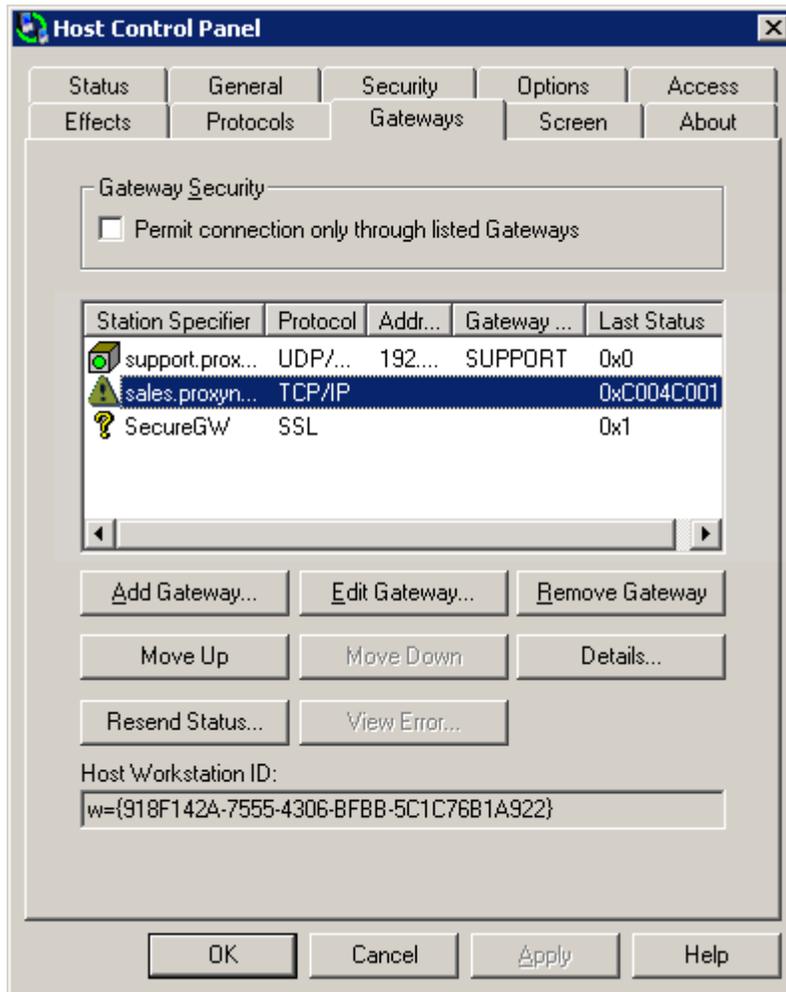


There are five options available:

- ◆ 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

Hosts can be configured to report to one or more Gateways.



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.

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 the Gateway uses for reporting and reference purposes.

Manage Gateway order

The ability to control the order of the Gateway list allows the 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 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 the Gateway and will proceed to the next the Gateway entry.

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

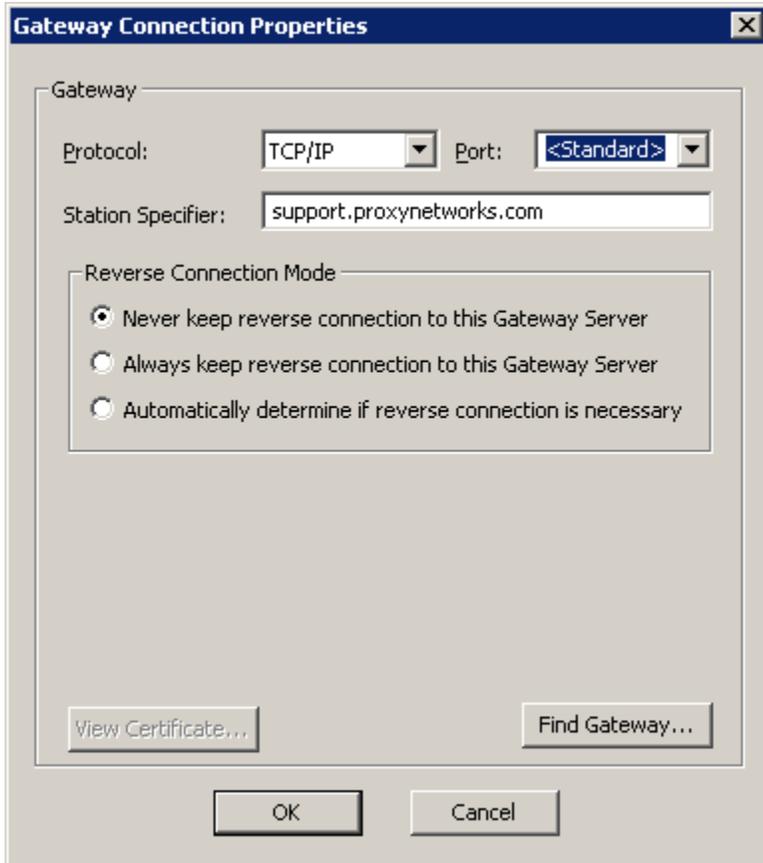
For example, a typical the Gateway may have two entries in the **Gateway** tab: One with the internal IP address or DNS name when the Host is in the same domain (regular connection), and another with the external IP address or DNS name when the Host is outside the domain (reverse connection).

If a Host computer (for example, a laptop) is routinely moved in and out of the domain with the 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

Hosts report status information to each Gateway listed on the **Gateways** tab. To add a 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 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 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, the 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 Gateway outside the 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 the Gateway are on the same LAN and the 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 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 Gateway. By having the Host establish a reverse connection to the Gateway, the 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 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.

Gateway configuration status

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

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 the Gateway, follow these steps:

- 1 Select any the 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 the Gateway, follow these steps:

- 1 Select any the 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 the 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 listed Gateways. Gateways that are available will show either  or . Gateways that are 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

the includes two different types of screen capture technology:

◆ **Kernel-mode screen capture:** Uses kernel-mode drivers to capture screen data. This is the default option on Windows XP, Windows 2003 Server and older platforms.

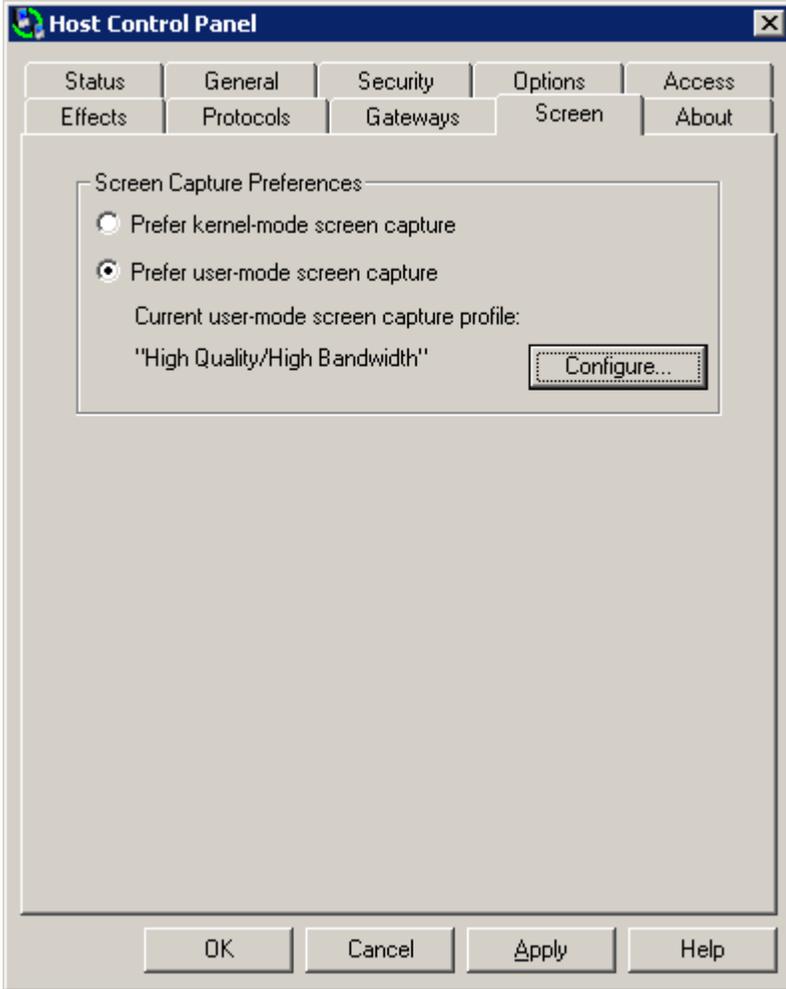
- ◆ Display Filter Driver (DFD): kernel-mode code supported on Windows XP, x86 only. Requires kernel-mode driver to process data. Installed by default, but activated only if the Mirror Display Driver is not loaded.
- ◆ Mirror Display Driver (DSP): kernel-mode code supported on Windows XP, and Windows Server 2003, in both x86 and x64. Requires kernel-mode driver to process data. Installed and activated by default. Can be disabled in Device Manager.

◆ **User-mode screen capture:** Uses user-mode code to capture screen data. This is the default option on Windows Vista and Window Server 2008 platforms but can also be used on Windows XP, Windows 2003 and older platforms.

- ◆ User Mode Screen Capture (UMSC): user-mode code supported on Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008. Runs as 32-bit x86 user mode code, but can capture either x86 or x64 systems. Only supported screen capture technology for Windows Vista and Windows Server 2008, and in Terminal Services sessions (any OS).

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 algorithm is currently preferred. If the preferred algorithm is user-mode, then the preferred user-mode screen capture profile is also indicated.



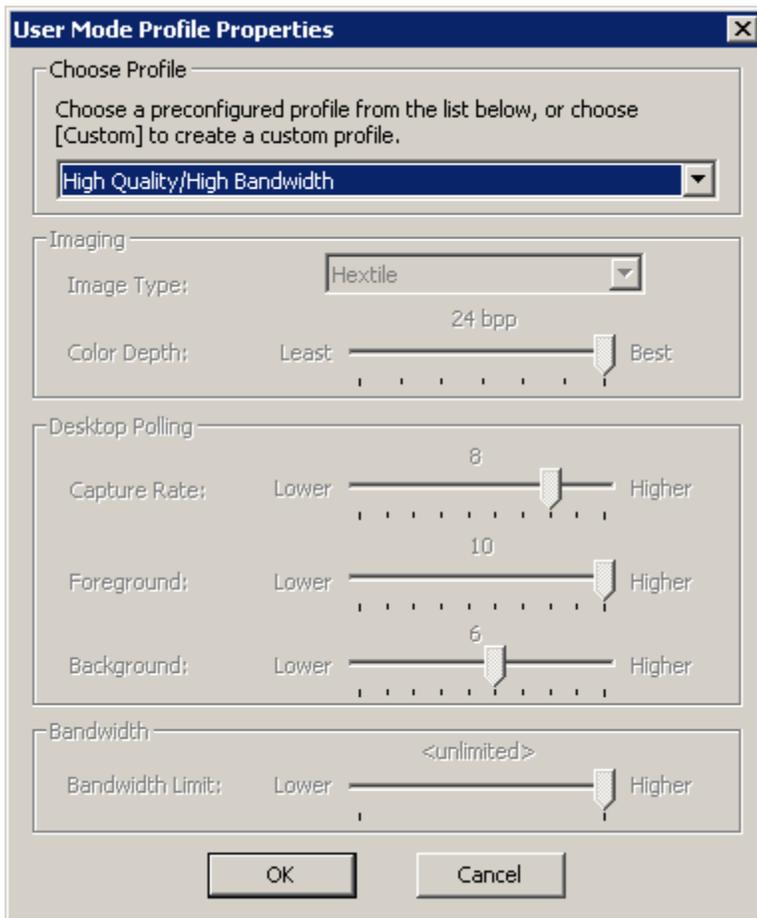
By default, the Host will try to use kernel-mode screen capture first. If the kernel mode drivers are not present or not working, the Host will automatically switch to user-mode, and will apply the currently selected screen capture profile (the default profile is "High Quality/High Bandwidth".)

In general, on XP and older platforms where the user has a choice of screen capture algorithms, kernel-mode will have better performance characteristics than user-mode, unless the screen being captured has one or more active elements (e.g. flash or video). In this case, user-mode will probably deliver better results and should be selected as preferred algorithm.

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.



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.
- ◆ Color depth (Hextile)/Image quality (JPEG). When the image type is Hextile, then the quality value (in the range of 20-100) controls the color depth reduction feature, with the rule that 24bpp = 100%, 21bpp = 88%, 18bpp = 75%, 15bpp = 63%, 12bpp = 50%, 9bpp = 38%, 6bpp = 25%. When the image type is JPEG, there is no color depth reduction, and the quality value (in the range of 20-100) controls the JPEG compression level.

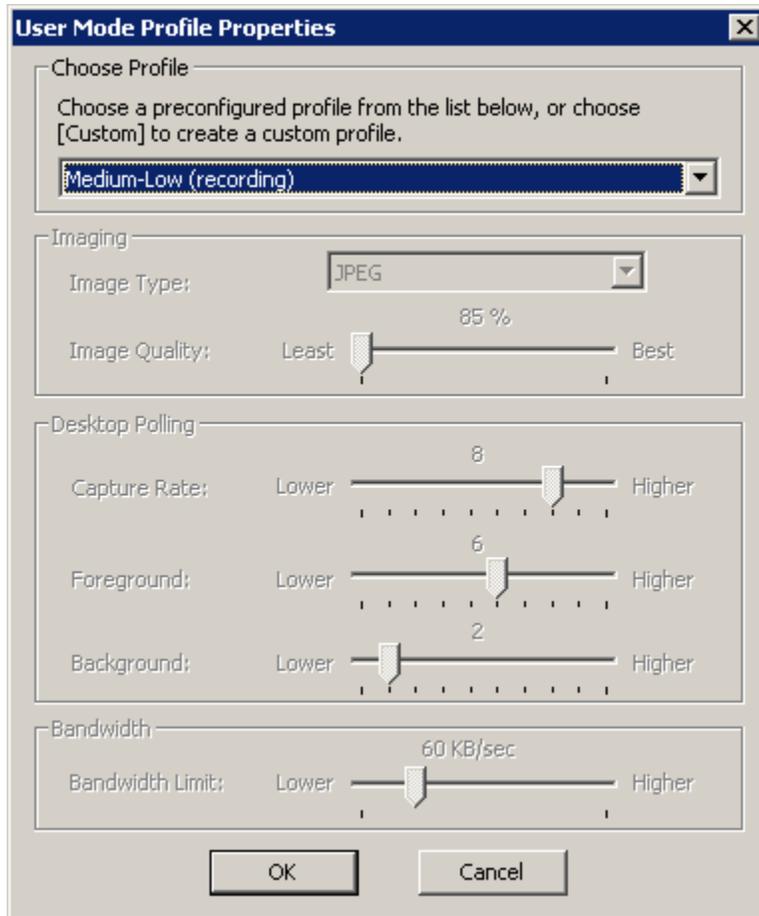
◆ Polling frequencies (three values -- Capture Rate, Foreground, and Background, in milliseconds). Note however that the UI will display these values on a scale of 1 to 10, with 1 being the least aggressive (longest time), and 10 being the most aggressive (shortest time). The underlying API and settings storage will have the raw millisecond values.

◆ Bandwidth limit (numeric value 5-200 kilobytes/sec, for -1 for unlimited)

There are four preconfigured user mode profiles:

Profile Settings	High	Medium	Medium Low	Low
Description	High Quality	Medium	Medium-Low (recording)	Low (recording)
Image Type	Hextile	Hextile	JPEG	JPEG
Image Quality (JPEG only)	N/A	N/A	85	75
Color Depth (Hextile only)	24 bpp	15 bpp	N/A	N/A
Polling Frequency	8/10/6	8/8/4	8/6/2	8/4/1
Bandwidth Limit	Unlimited	100 Kbyte/sec	60 Kbyte/sec	30 Kbyte/sec

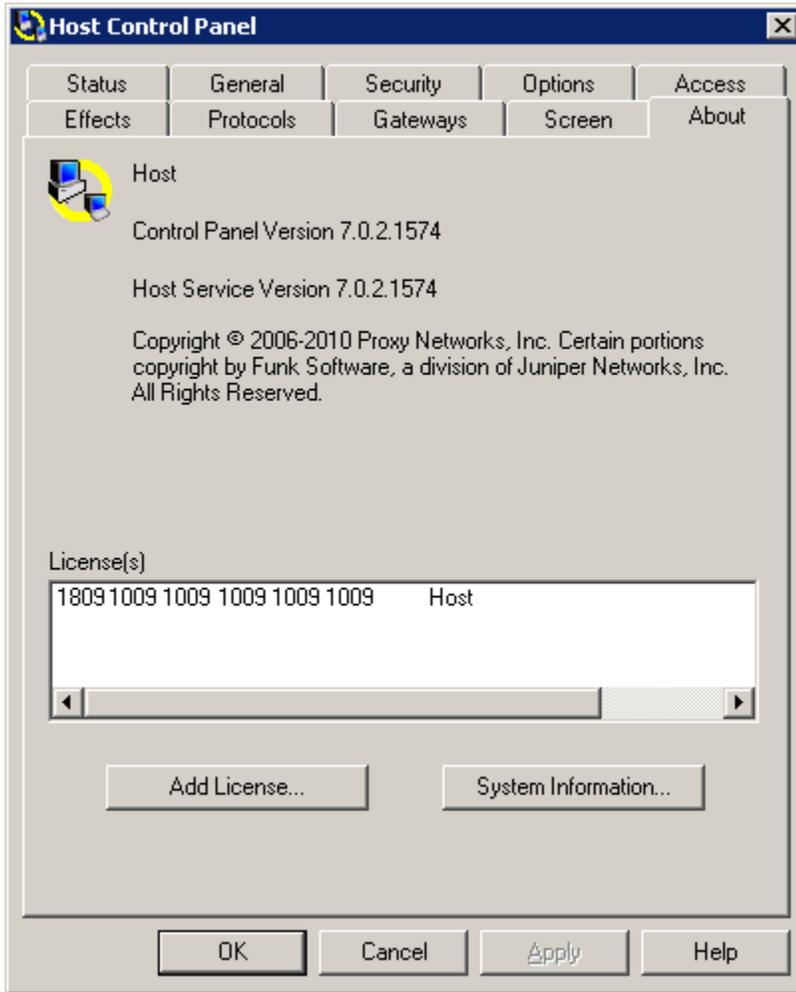
The Medium-Low and Low profiles are appropriate for high volume screen recording environments, when screen quality can be traded off for lower screen capture rates, smaller screen recording file sizes and restricted bandwidth usage.



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

About tab

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



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

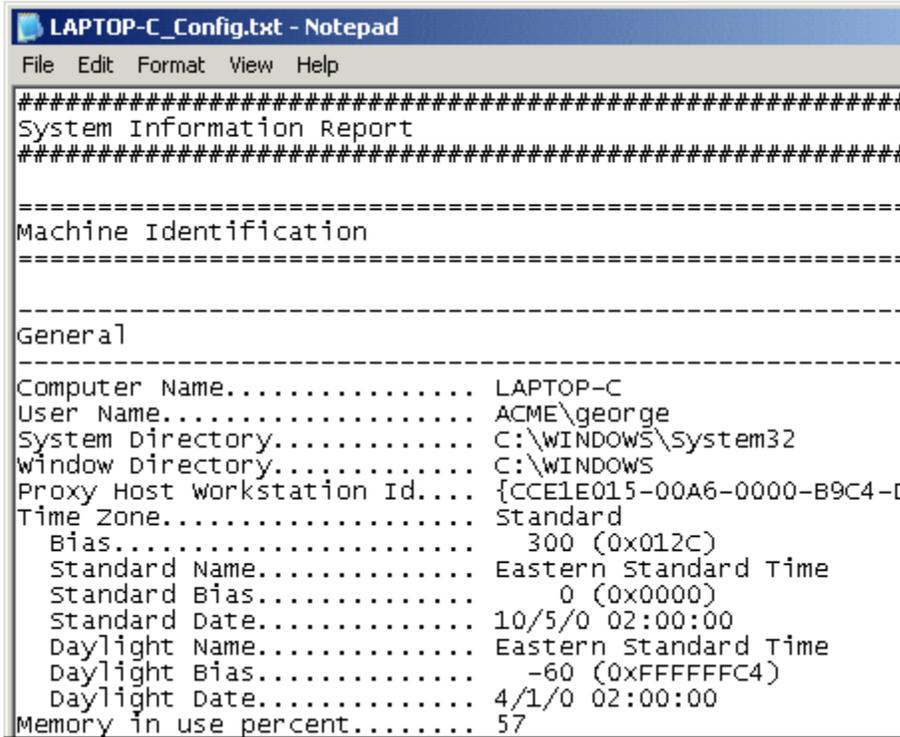
- 1 Click **Add License**. The **Add License Key** window appears.



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

Generate a System Information report

For auditing and technical support purposes, the 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.



```
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
Time Zone..... Standard
  Bias..... 300 (0x012C)
  Standard Name..... Eastern Standard Time
  Standard Bias..... 0 (0x0000)
  Standard Date..... 10/5/0 02:00:00
  Daylight Name..... Eastern Standard Time
  Daylight Bias..... -60 (0xFFFFFC4)
  Daylight Date..... 4/1/0 02:00:00
Memory in use percent..... 57
```

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`.

Terminal Services tab

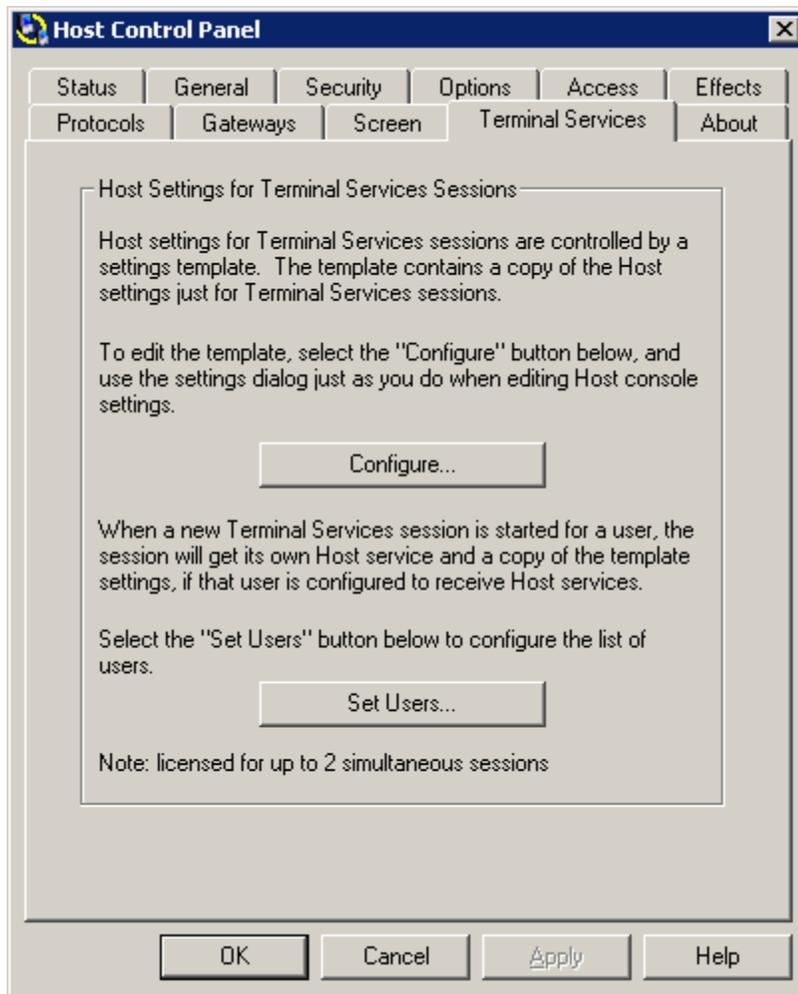
Hosts can be configured to allow remote viewing and remote control of one or more simultaneous Terminal Services sessions, as well as the Terminal Services server console.

A standard Host with a special TS license key must be installed and configured on the server console to serve as the "root". When a new Terminal Services session is started, the root Host will execute the Startup procedure inherited from the server console, which includes a task to inject a Host instance into the terminal session and start it. The Host will distinguish the session from the server console and start up a Host service specifically for the session.

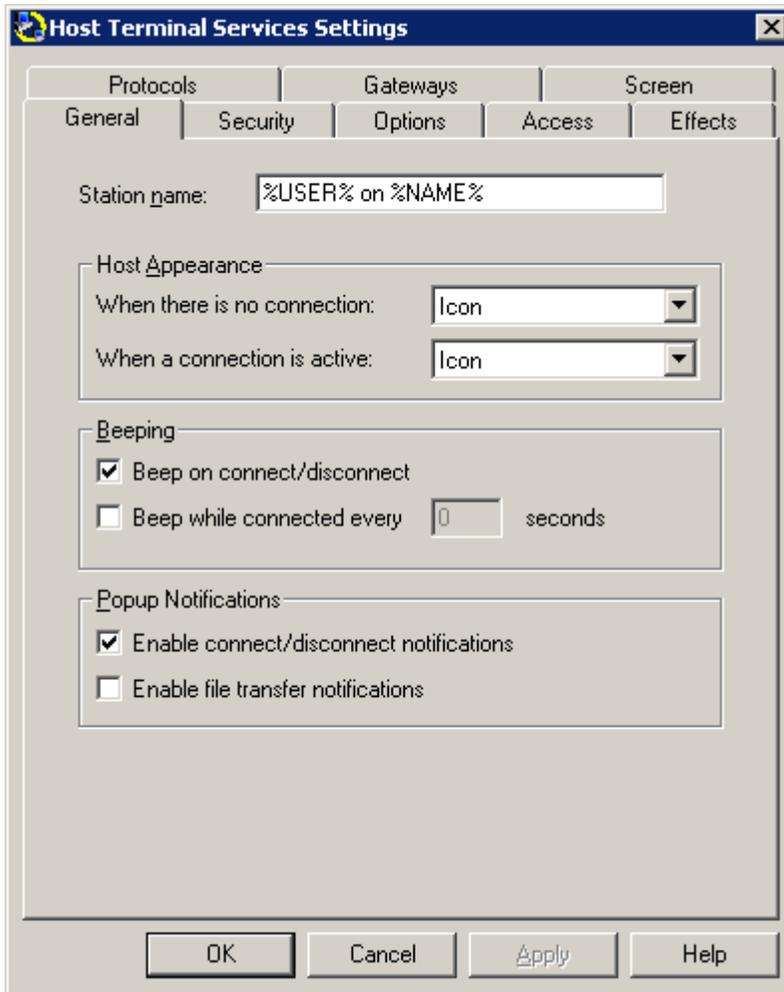
NOTE: *You must first configure a standard Host to be the root. This is done by entering a special license key that will enable the Host to support a specified number of simultaneous Terminal Services sessions - see [About tab](#) for more information).*

Configuring the TS Host

The root Host maintains a Terminal Services template to hold the Host configuration settings for these Host instances (in this way, the Host settings for the root Host running on the terminal server may be different than those specified in the TS template for each Host instance injected into a terminal session). To view or edit this template, go to the Terminal Services tab in the root Host Control Panel and click on **Configure**.



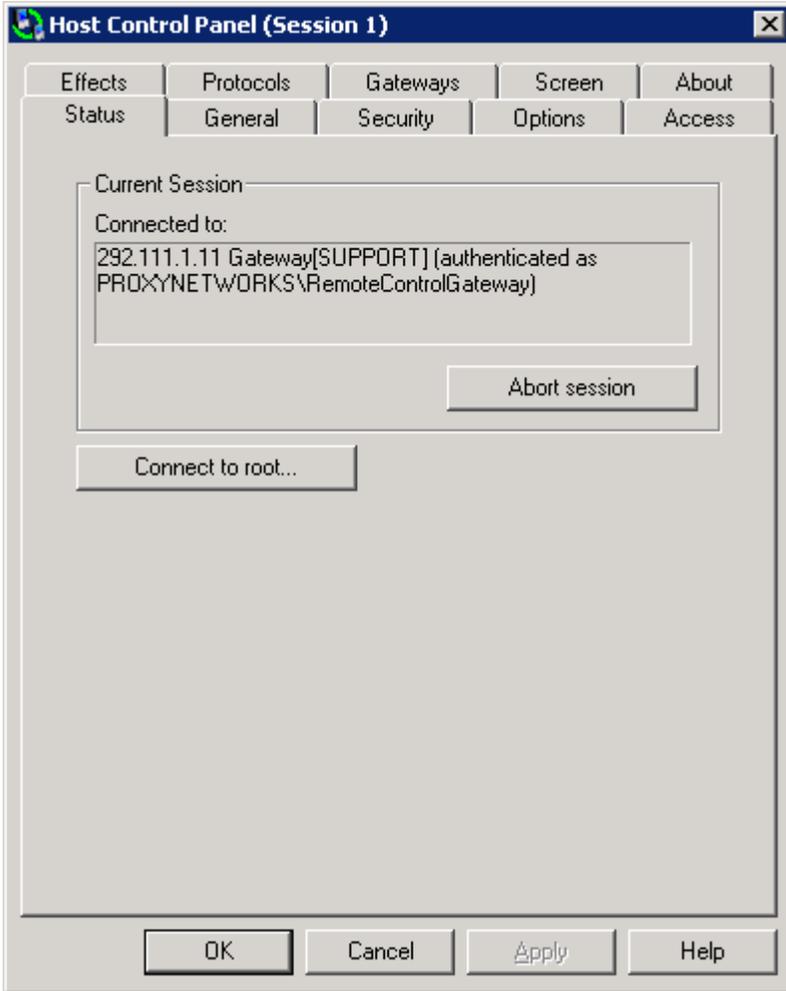
Most of the configuration options are the same as those available on the standard Host Control Panel, although the **About** and **Status** tabs are not present because the settings on these tabs are not directly applicable to TS Hosts. Note that the macro %USER%o%NAME% is used to distinguish each terminal session Host instance, where NAME is the name of the terminal server.



For more information about specific configuration settings available for the Terminal Services template, see below:

- ◆ [“General tab”](#)
- ◆ [“Security tab”](#)
- ◆ [“Options tab”](#)
- ◆ [“Access tab”](#)
- ◆ [“Effects tab”](#)
- ◆ [“Protocols tab”](#)
- ◆ [“Gateways tab”](#)
- ◆ [“Screen tab”](#)

Once the Host instance for a specific Terminal Services session is started, you can view the effective settings for this Host instance by clicking on the Host Control Panel icon  in the TS session:



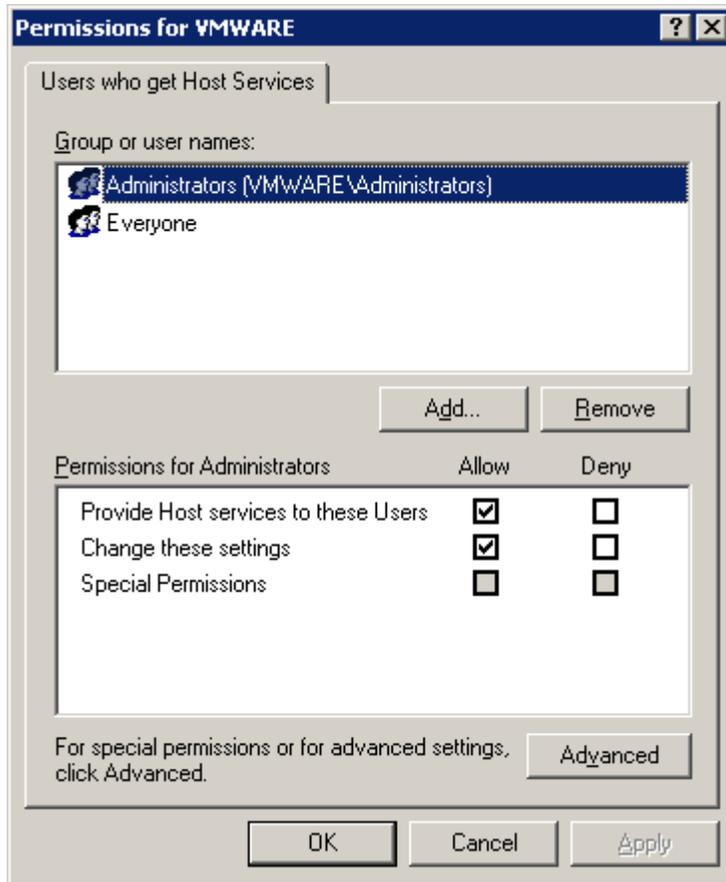
Note that the title bar shows the session number (in this case, "Session 1"). Each root Host is capable of supporting as many simultaneous sessions as the license key allows.

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 terminal session Hosts is view only mode because the settings are based on the settings in the root Host Control Panel.

Setting Users for TS Hosts

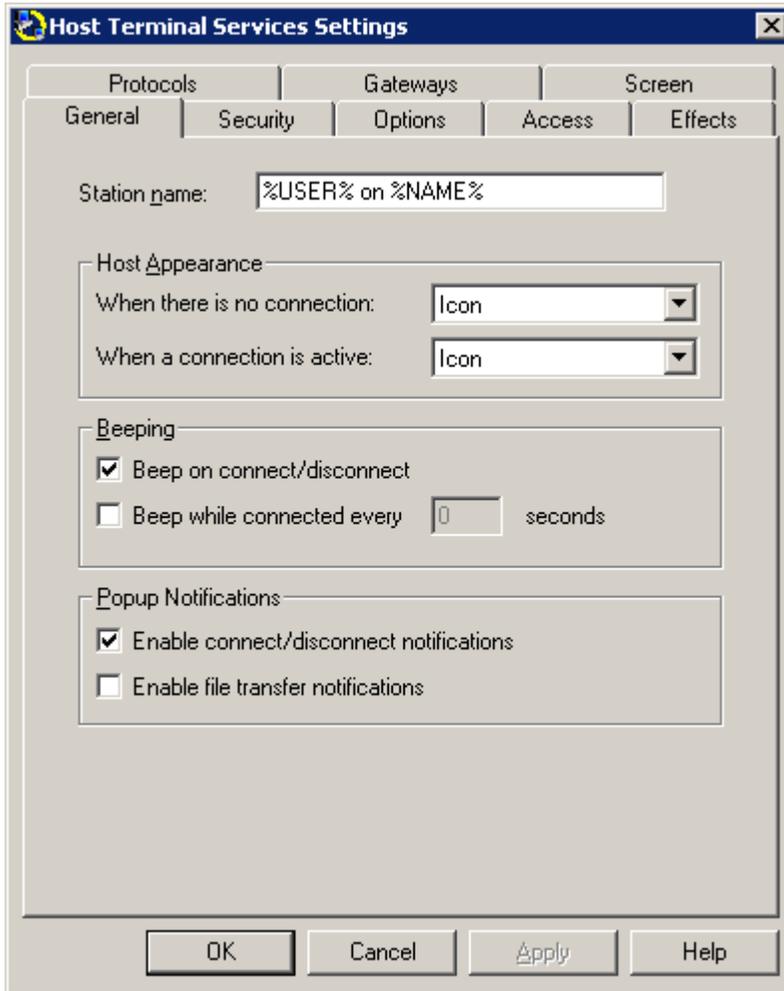
You can configure the root Host to inject a Host instance into certain terminal sessions and not into others. Click on **Set Users** in the root Host Control Panel to select which users should get a Host instance:



In this example, whenever a user with administrator credentials for the VMWARE domain gets a terminal session, the root Host on the terminal server will inject a Host instance.

General tab

The **General** tab allows you to set some preferences about appearance and notifications for terminal session Hosts.



You can change the following from the **General** tab:

- ◆ **Station name:** Modify the name by which your Host computer identifies itself to the Gateways and/or the Masters. To use macros to change the Station name automatically, see "[Change Station name](#)".
- ◆ **Host Appearance:** Configure the 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 the Host icon appears (or is hidden) when there is no active remote connection.
 - ◆ **When a connection is active:** The the Host icon appears (or is hidden) when a remote connection is active.

◆ **Beeping:** Set auditory cues to indicate when a 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).

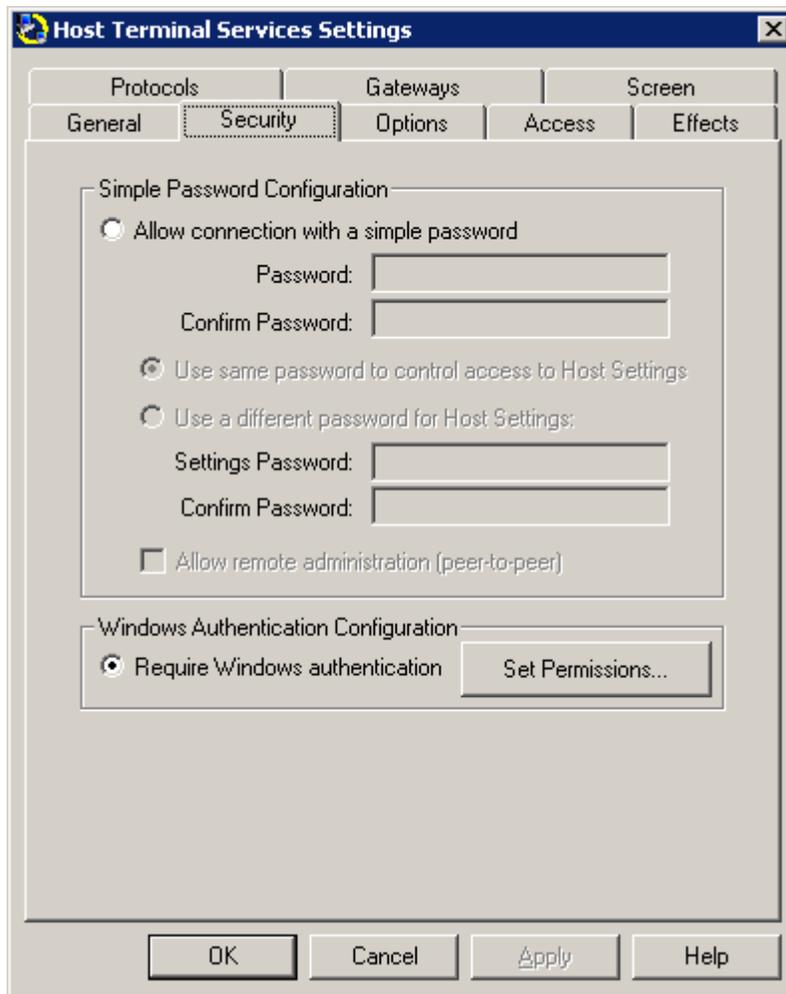
- ◆ Select **Enable connect/disconnect notifications** to see popup notifications when a Master user connects or disconnects from the Host.



- ◆ Select **Enable file transfer notifications** to see popup notifications when a Master initiates file transfer operations to/from the Host.

Security tab

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

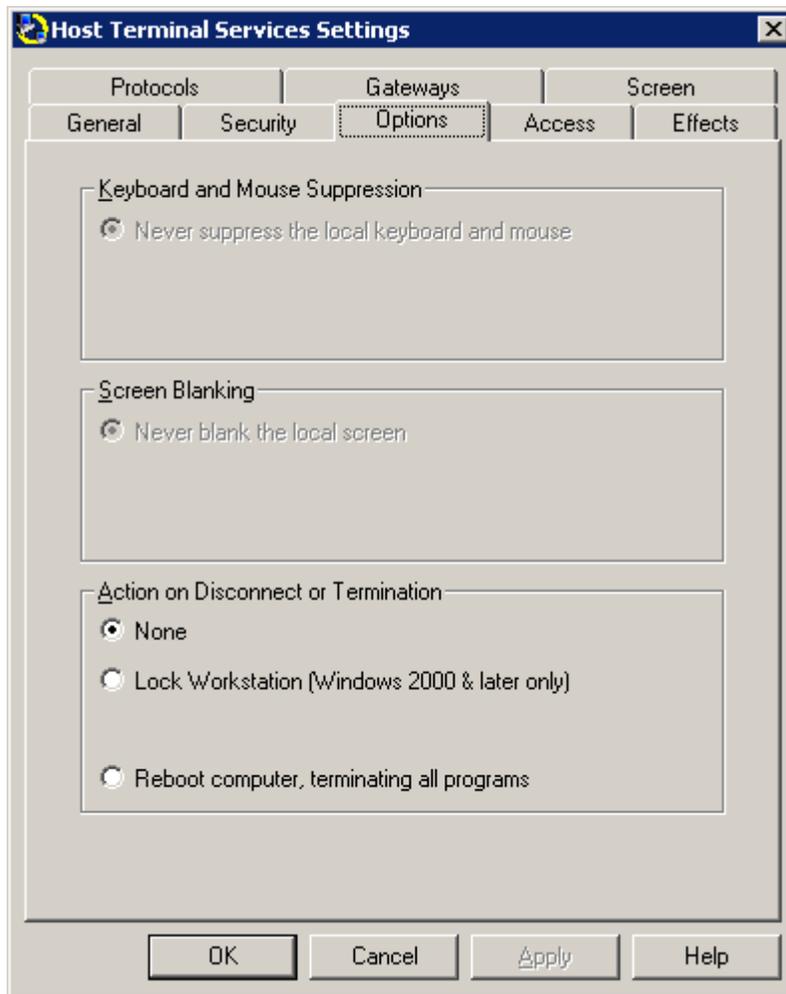


The following authentication methods are available:

- ◆ “Simple password configuration”
- ◆ “Windows authentication configuration”
- ◆ “Shared secret password authentication”

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.



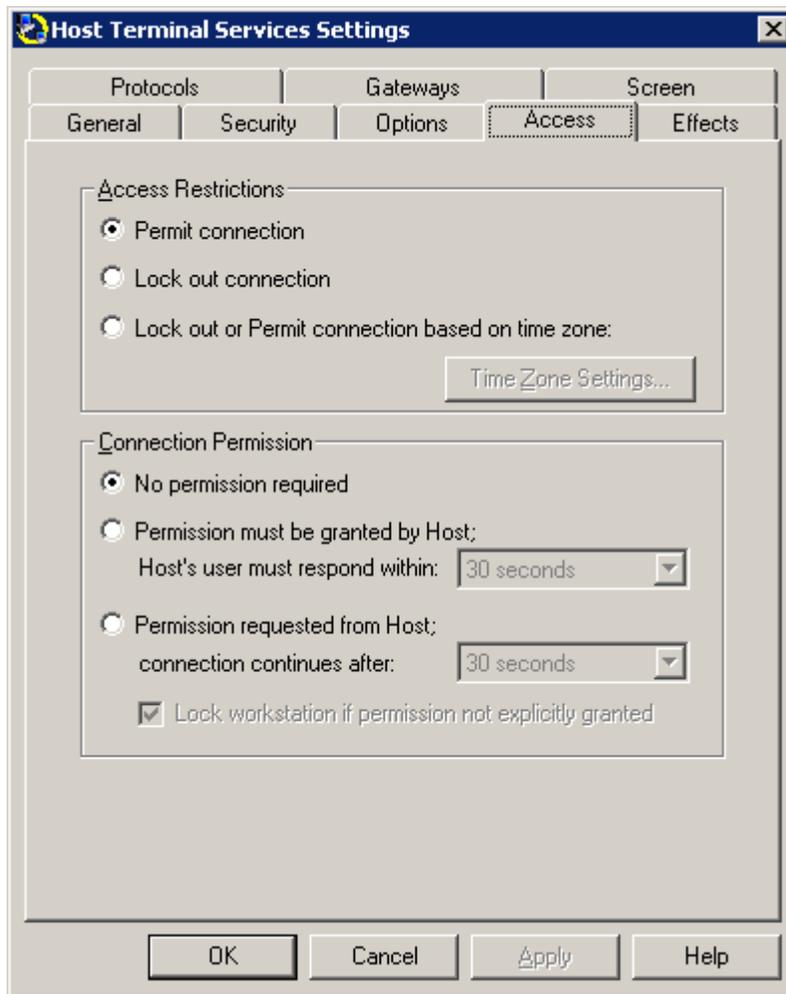
The following options can be configured from the **Options** tab:

- ◆ “Keyboard and mouse suppression” (disabled for terminal session Hosts)
- ◆ “Action on disconnect or termination”

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

Access tab

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

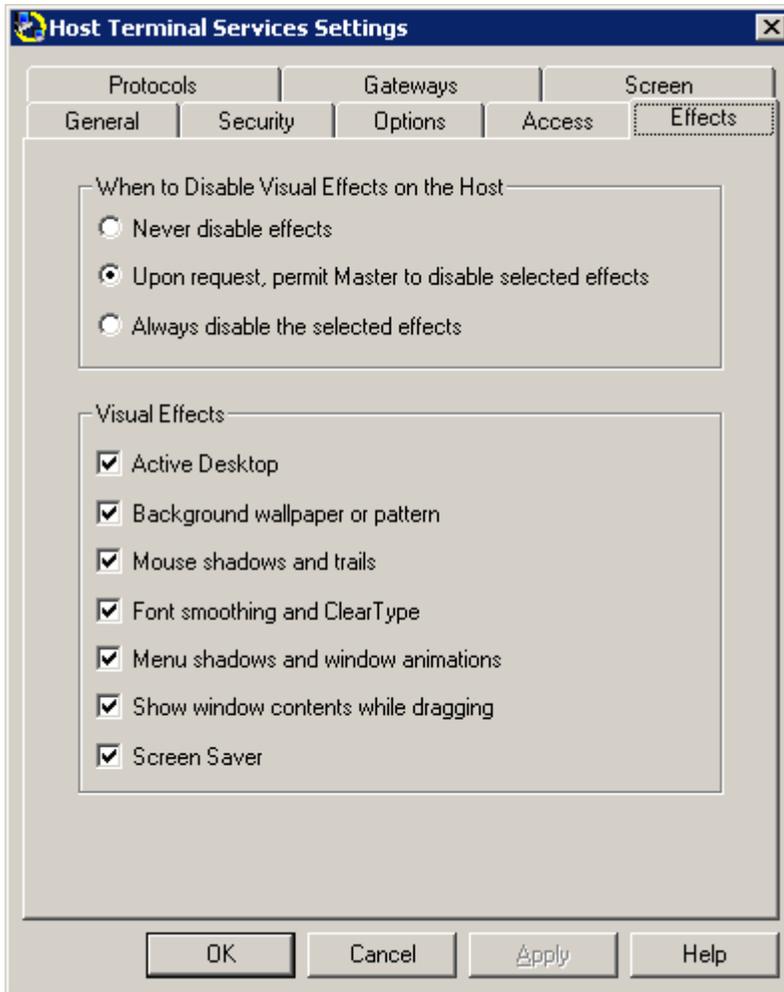


Restrict access with the following options:

- ◆ “Access restrictions”: lock out connections to this Host.
- ◆ “Connection permission”: require explicit permission to connect to this Host.
- ◆ “Access to Host settings” (disabled for terminal session Hosts)

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 the 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 the 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 the Master user to have control over.

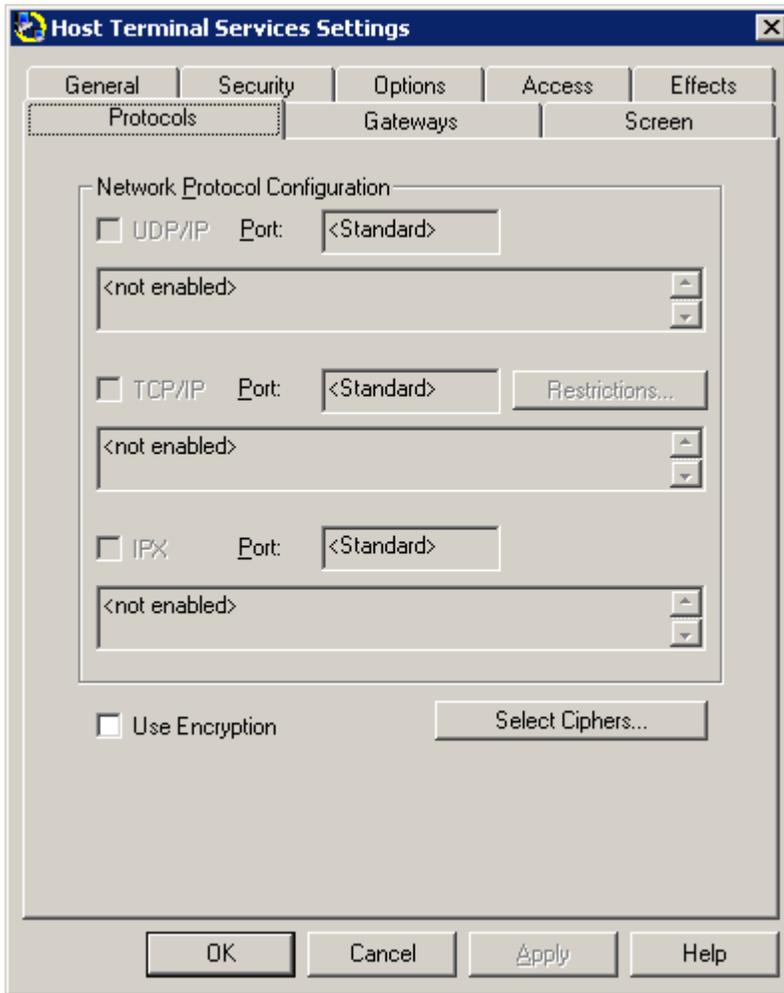
The particular visual effects that are enabled or disabled are controlled by the settings you check under **Visual Effects**:

- ◆ Active Desktop
- ◆ Background wallpaper or pattern
- ◆ Mouse shadows and trails

- ◆ Font smoothing and ClearType
- ◆ Menu shadows and Windows animations
- ◆ Show window contents while dragging
- ◆ Screen Saver

Protocols tab

Configure the network protocols and ports for communication with the Host in the **Protocols** tab. These settings are disabled for terminal 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..

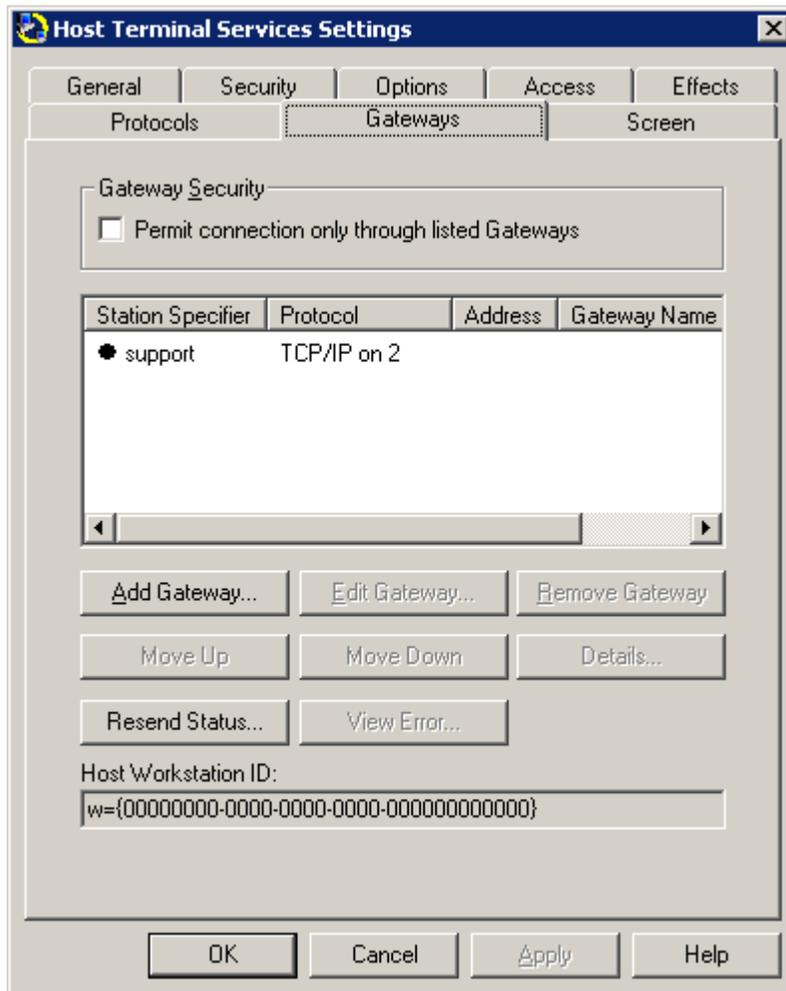


For more information about these settings, see [Protocols tab](#).

Gateways tab

The root Host for must be configured to report to one or more the Gateways; it is through these connections that terminal services session Hosts will be reached.

Note that connection status icon next to Gateway entries and the Host Workstation ID are generic in the root Host template. These will be replaced by actual icons and values when the Host service is started in the terminal session (see [Terminal Services 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.

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 the Gateway uses for reporting and reference purposes.

Manage Gateway order

The ability to control the order of the Gateway list allows the 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 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 the Gateway and will proceed to the next the Gateway entry.

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

For example, a typical the 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 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.

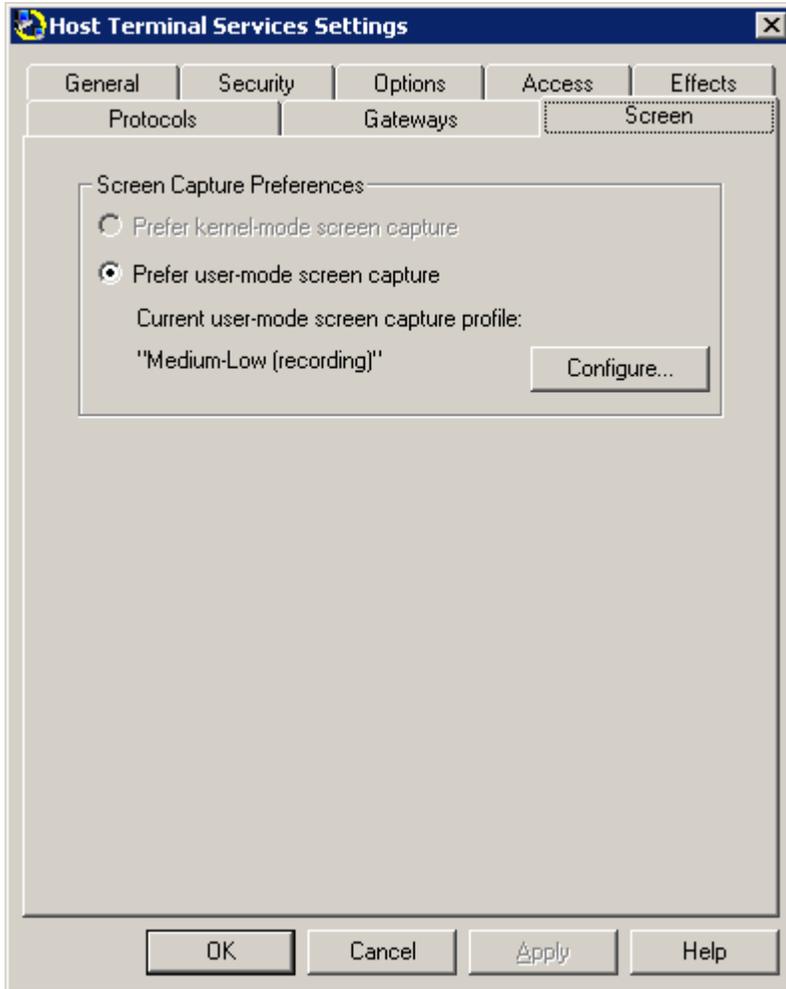
Screen tab

For Terminal Services Hosts, only user-mode screen capture is available.

- ◆ **Kernel-mode screen capture:** For more information about kernel-mode screen capture, see [Screen tab](#) for regular the Hosts.
- ◆ **User-mode screen capture:** Uses user-mode code to capture screen data. This is the only option for Terminal Services Hosts.
 - ◆ User Mode Screen Capture (UMSC): user-mode code supported on Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008. Runs as 32-bit x86 user mode code, but can capture either x86 or x64 systems. Only supported screen capture technology for Windows Vista and Windows Server 2008, and in Terminal Services sessions (any OS).

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 for Terminal Services Hosts indicates that user-mode screen capture algorithm is the only option, and also indicated the preferred user-mode screen capture profile.



Open 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 **Open 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 11.2 or later.

Set up remote printing

One of the key services provided by the remote support solutions is remote printing. The 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, in order to enable this service, the Host computer must be configured for remote printing.

To configure your Host computer for remote printing, a printer driver must be added to the Host computer, and assigned to a local port on the Host computer with the name "the". The printer driver that is added must correspond to the local printer to be used by the Master user.

The procedure for configuring the Host for remote printing depends on your operating system:

Configure remote printer settings

To configure a Host computer running Windows XP for remote printing, follow these steps:

- 1 Select **Start > Settings > Printers and Faxes**.
- 2 In the **Printer Tasks** list on the left, click **Add a Printer**. The Add Printer Wizard appears. Click **Next**.
- 3 Select **Local Printer attached to this computer**.
- 4 Select **Use the following port**, and select the from the list. Click **Next**.
- 5 Select the manufacturer and printer model of the local printer to which the Master users wants to print. Click **Next**.
- 6 Optionally, change printer name in the box provided. Select **No** under the question **Do you want to use this printer as the default printer?** Click **Next**.
- 7 Select **Do not share this printer**. Click **Next**.
- 8 Respond **No** to the question **Do you want to print a test page?**
- 9 Click **Finish** to complete the wizard

NOTE: Depending upon which version of Windows you 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: Remote printing service is not supported on x64 Hosts, or on Hosts running on Windows Server 2003 or Windows Server 2008.

Command Line Configuration

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

- ◆ Use the command line utility `PHSETUP` to set the Host configuration options from a command line. See "[Configure Host from the command line.](#)"
- ◆ In addition to specifying options in the Host Control Panel window, use `PHSETUP` to lock down other the Host features. See "[Lock-down settings](#)".
- ◆ Use the Windows `MSIEXEC` installation command line utility to install a customized the Host configuration. This feature is useful if you want to push the 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 Deployment Tool can also be used to mass deploy the Host configurations. For more information, see the Deployment Tool Administration Guide.*

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

In addition, with the proper access rights, the 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](#)"
- ◆ "[PHSETUP Gateways parameters](#)"
- ◆ "[PHSETUP general parameters](#)"
- ◆ "[PHSETUP license parameter](#)"
- ◆ "[PHSETUP options parameters](#)"
- ◆ "[PHSETUP protocol parameters](#)"
- ◆ "[PHSETUP security parameters](#)"
- ◆ "[PHSETUP screen 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 the Host:

- ◆ Set the Host computer station name to *HowdyDoody*

```
phsetup name:HowdyDoody
```

- ◆ Set the Host computer station name to *Julia's Game Machine*

```
phsetup name:"Julia's Game Machine"
```

- ◆ Set the Host computer station name to *Julia's "little" Machine.*

```
phsetup name:"Julia's ""little"" machine"
```

- ◆ Set access restrictions, so that the Host computer is locked from 9am to 5pm Monday to Friday

```
phsetup access:time
timezone:0000000000000000FCFF03000000FCFF03000000FCFF03000000FCFF
03000000FCFF03
```

- ◆ Add a Gateway to which the Host computer reports using UDP/IP

```
phsetup addgateway:"IP,@198.186.160.77"
```

- ◆ Remove all the Gateways from the Host reporting list

```
phsetup removegateway:all
```

- ◆ Assign full access control to a domain account (mydomain\YourRemoteControlGateway). You can use this command to assign full access control rights to your the Gateway domain account, or any other domain account.

```
phsetup addservicesecurityace:"mydomain\YourRemoteControlGateway,
0xE00FF"
addadminsecurityace:"mydomain\YourRemoteControlGateway,0xE00F"
addsettingssecurityace:"mydomain\YourRemoteControlGateway,0xE00FF"
"
```

- ◆ Reset settings to their the Host default values (for systems using simple password)

```
name:$NAME$ connectbeep:on beeevery:0 idleappear:icon
connappear:icon hostnotifications:1
usewindowssecurity:no adminpasswordrequired:different
allowremoteadmin:no password:randomstring adminpassword:""
lockworkstationndisconnect:no rebootndisconnect:no
suppresskeys:permit
access:permit permission:none granttime:30 requesttime:30
lockworkstationndefault:yes
managevisualeffects:permit visualeffects:0x7F
tcp:on ip:on ipx:on encryption:on preferredciphers:A4A3A233R2"
requiregateway:no removegateway:all
preferusermode:no selectusermodeprofile:"High Quality/High
Bandwidth"
```

In addition, you can reset the following default security settings:

```
usewindowssecurity:yes removeservicesecurityace:*
addservicesecurityace:Administrators,0xE01FF
```

```
setsecurityowner:Administrators removeadminsecurityace:*  
addadminsecurityace:Administrators,0xE003F  
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 the 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 999.</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 the 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</p>

permitted.
 If you set
request or
grant, you
 must also
 specify the
requesttime
 or *granttime*.

lockworkstationondefault:
yes|no

By default, this
 setting is set to
 yes to
 automatically
 lock workstation
 if access
 permission is not
 granted. Set this
 to no to prevent
 workstation from
 being locked.

requesttime: number

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
 999.

timezone: hexnum

Set the time
 zone settings.
 These settings
 lock or permit
 access if you
 also specify
access: time.
 You must specify
 a sequence of
 hexadecimal
 digits for
hexnum.
 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>
/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>

`/s` (peer-to-peer)

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.

The following are some protocol-specific examples:

```
/pUDP /S192.168.160.138
/pTCP /Sjackson
/pTCP /Sjackson.acme.com
/pIPX /S@20:1B13DAE9
/pIPX /S"Dell P200"
/pIPX /S"2:Dell
```

`/g` `/s` (connections through a Gateway)

Specify the Gateway and Host computer when connecting to a Host computer through a Gateway for the purpose of Host computer configuration. Specify these values in double quotes. Note that when you specify the Gateway and protocol (using `/p`), the protocol applies to the connection between your local computer and the 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 Gateway.

The Gateway syntax for `/s` values depends on your host specification. Use `u` for a logged-in user and `w` (with curly braces) for a workstation:

- `"u=host_key"`
- `"w={host_key}"`

NOTE: The `u` that you use for the Gateway syntax of `/s` is independent of the `/U` command.

To find the workstation Host key, navigate to the "[About tab](#)" of the Host. Click **System Information**, and select the text listed next to **Host Workstation Id**.

The following rows have host format-specific examples.

```
/g"Gateway 1"
/s"w={6F93DF16-8352-46EB-
ADDF-7FD752EA72FA}"
/g"Gateway 1"
/s"u=ACME\george"
```

`/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 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 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 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 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 three `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 the 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.

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).

`mode:reset`

This command can be used in the following ways:

- `mode:reset`, to reset standard settings to program defaults.
- `mode:lockdown mode:reset`, to lift the lockdown of settings.
- `mode:terminalservices mode:reset`, to reset the terminal services template settings to program defaults.

NOTE: When you use the `mode:lockdown` parameter to lock down the 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 the Host.

Parameter	Definition
<pre>managevisualeffects: always managevisualeffects: permit managevisualeffects: off managevisualeffects: never</pre>	<p>Set to <code>always</code> to disable visual effects whenever a remote connection is established.</p> <p>Set <code>visualeffects</code> flags when you use this setting.</p> <p>Set to <code>never</code> or <code>off</code> to deny remote users from controlling visual effects.</p> <p>Set to <code>permit</code> to allow remote users to control visual effects when they configure this feature.</p> <p>The default is <code>permit</code>.</p>
<pre>visualeffects: number</pre>	<p>Set the flags for visual effects.</p> <p>0x0001 – Aero Glass</p> <p>0x0002 - Desktop wallpaper and patterns</p> <p>0x0004 - Mouse effects: cursor shadow, mouse trails</p> <p>0x0008 - Font effects: font smoothing, ClearType</p> <p>0x0010 - Windows effects: menu</p>

and window
animation
0x0020 - Show
Window
contents while
dragging
0x0040 -
Screen saver
The default is
0x7F (all
effects).

PHSETUP error handling

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:

```
addServiceSecurityACE
removeServiceSecurityACE
setServiceSecurityOwner
addAdminSecurityACE

removeAdminSecurityACE
setAdminSecurityOwner
addSettingsSecurityACE
removeSettingsSecurityACE
setSettingsSecurityOwner
addLicense
```

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 the Host.

Parameter	Definition
<pre>requiregateway: yes</pre>	<p>Set to <code>yes</code> to require that all remote control connections to this Host computer pass through a 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 Gateway.</p>
<pre>addgateway: "protocol port", "station_specifier" [, " control_connection_mode "]</pre>	<p>Add a specified Gateway to which the Host can report. You can use the following values:</p> <p><code>protocol</code> = TCP, UDP, SSL or IPX</p> <p><code>port</code> (optional) = a valid port number if you do not use the standard port</p> <p><code>station_specifier</code> = a protocol-dependent specification for the station:</p> <p>UDP/IP or TCP/IP</p> <ul style="list-style-type: none"> • <code>network_address</code> • <code>station_name</code> • <code>dns_name</code> <p>IPX</p> <ul style="list-style-type: none"> • <code>@node</code> • <code>@network:node</code> • <code>station_name</code> • <code>network:station_name</code> • <code>control_connection_mode</code> (optional) = <code>auto</code>, <code>never</code>, <code>always</code> <p>NOTE: Specify the <code>protocol port</code> pair in quotes when you specify the port, and specify the <code>station_specifier</code> in quotes. Separate the <code>protocol port</code> and the <code>station_specifier</code> with a comma.</p>

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

`protocol = TCP, UDP, SSL 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
"
```

<pre>removegateway: all</pre>	<p>Eliminate all the Gateways from the list of the Gateways to which the Host is configured to report.</p>
<pre>resetgateway: " protocol port ", " station_specifier "</pre>	<p>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.</p> <p>See <code>removegateway</code> for information on value options.</p>
<pre>resetgateway: all</pre>	<p>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").</p>

PHSETUP general parameters

The following PHSETUP parameters correspond to the "[General tab](#)" settings in the Host.

Parameter	Definition
beepevery: <i>number</i>	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.
connappear:hidden connappear:icon	Set to <i>hidden</i> to hide the Host icon when a connection is active. Set to <i>icon</i> to render the Host icon visible when a connection is active.
connectbeep:on connectbeep:off	Set to <i>on</i> in order to have the system beep when a remote connection connects or disconnects. Set to <i>off</i> in order to have no sound when remote connect or disconnect occurs.
idleappear:hidden idleappear:icon	Set to <i>hidden</i> to hide the Host icon when there is no active connection. Set to <i>icon</i> to render the Host icon visible when there is no active connection.
hostnotifications:number	Turn on popup notifications on the Host when <i>number</i> is set to (or sum of): 0x1 - Connect/Disconnect

0x2 - File Transfer

<code>name: <i>string</i></code>	Use this parameter to provide a string that specifies a new station name.
----------------------------------	---

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\$	Host software version number (e.g. "v10.0.2.1003")
\$PLATFORM\$	Host operating system platform (e.g. "Win2003")

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 the 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 the Host.

PHSETUP options parameters

The following PHSETUP parameters correspond to the "[Options tab](#)" settings in the Host.

Parameter	Definition
<code>lockworkstationondisconnect:yes</code>	Set to <code>yes</code> to lock the Host computer when a remote user's session is over.
<code>rebootondisconnect:on</code>	Set to <code>on</code> to restart the Host computer when a remote session is over. Otherwise set to <code>off</code> (default the Host behavior).
<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 the Host behavior) or <code>off</code> to disable both options.

PHSETUP protocol parameters

The following PHSETUP parameters correspond to the "[Protocols tab](#)" settings in the Host.

Parameter	Definition
encryption: <i>on</i> encryption: <i>off</i>	Set to <i>on</i> to encrypt all remote data exchanges. Otherwise set to <i>off</i> .
ip: <i>on</i> ip: <i>off</i>	Specify whether (<i>on</i>) or not (<i>off</i>) this Host computer 'listens' on the UDP/IP protocol, or accepts connections on that protocol. Specify <i>ipport</i> when you set this <i>on</i> .
ipport: <i>number</i>	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.
ipx: <i>on</i> ipx: <i>off</i>	Specify whether (<i>on</i>) or not (<i>off</i>) this Host computer supports the IPX protocol. Specify <i>ipxport</i> when you set this <i>on</i> .
ipxport: <i>number</i>	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.

<p>tcp: <i>on</i> tcp: <i>off</i></p>	<p>Specify whether (<i>on</i>) or not (<i>off</i>) this Host computer supports the TCP/IP protocol. Specify <i>tcpport</i> when you set this <i>on</i>.</p>
<p>tcpport: <i>number</i></p>	<p>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.</p>
<p>tcpaccessmode: <i>grant</i> tcpaccessmode: <i>deny</i></p>	<p>Determine whether (<i>grant</i>) or not (<i>deny</i>) to grant or deny most TCP/IP traffic. Set <i>tcprestrictions</i> to define exceptions to this policy. The default is <i>grant</i>.</p>
<p>tcprestrictions: <i>addresses</i></p>	<p>Set exceptions to your <i>tcpaccessmode</i> policy. Specify the <i>addresses</i> parameter as a single entry, or a set of entries separated by commas. Use one of the following formats for the variable: <i>IPAddress</i>, <i>IPAddress (count)</i>, or <i>IPAddress [IPAddressmask]</i> For example: <i>tcprestrictions = "111.111.111.111, 222.222.222.222 (5), 111.112.113.0 [255.255.255.0]"</i></p>
<p>tcprestrictions: <i>addresses</i></p>	<p>Add the following IPv6 formats to the list of possible formats: <i>x:x:x:x:x:x, x:x:x:x:x:x/n</i></p>

```
preferredciphers:ciphers
```

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. the Host v11.0 and later support the following ciphers:

- "A4" - AES encryption (256-bit key) with SHA1 hash
- "A3" - AES encryption (192-bit key) with SHA1 hash
- "A2" - AES encryption (128-bit key) with SHA1 hash
- "33" - Triple-DES (3DES) encryption (192-bit key) with SHA1 hash
- "R2" - RC4-compatible encryption (128-bit key) with MD5 hash

The cipher list is a single string of concatenated cipher strings, in order of preference from first to last, e.g. "A4A3A233R2".

PHSETUP security parameters

The PHSETUP parameters in this section correspond to "[Security tab](#)" settings in the Host.

usewindowsecurity:yes

The `usewindowsecurity:yes` command lets you use Windows security mechanisms for the 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 Host authentication. When set to `no`, the parameters in "[PHSETUP access parameters](#)" are required.

Parameter	Definition
<code>adminpassword:string</code>	Sets the password for the Host administration to <i>string</i> .
<code>adminpasswordrequired:same</code> <code>adminpasswordrequired:different</code>	Uses the Windows password for the Host administration. Uses the <code>adminpassword</code> setting for the Host administration.
<code>allowremoteadmin:yes</code> <code>allowremoteadmin: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 Host password to <i>string</i> .

PHSETUP screen parameters

The following PHSETUP parameter corresponds to the "[Screen tab](#)" settings in the Host.

Parameter	Definition
<pre>preferusermode:yes no</pre>	<p>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 host platforms. By default, this setting is set to yes on Windows Vista, Windows Server 2008 and later platforms.</p>
<pre>selectusermodeprofile : "profilename"</pre>	<p>Select default user mode profile for user mode screen capture preferences. Current options are:</p> <ul style="list-style-type: none"> ▪ <i>High Quality/High Bandwidth</i> ▪ <i>Medium</i> ▪ <i>Medium-Low (recording)</i> ▪ <i>Low (recording)</i> ▪ <i>[Custom]</i>
<pre>setusermodeprofile: "profilename", imagetype, imagequality, fgfrequency, bgfrequency, capturefrequency, bandwidthlimit"</pre>	<p>Specify bandwidth throttling options when creating a [Custom] user mode profile:</p> <ul style="list-style-type: none"> ▪ <i>profilename</i> = custom profile name ▪ <i>imagetype</i> = Hextile (default), JPEG ▪ <i>imagequality</i> = integer between 20 and 100 ▪ <i>fgfrequency</i> = integer between 1 and 10 ▪ <i>bgfrequency</i> = integer between 1 and 10 ▪ <i>capturefrequency</i> = integer between 1 and 10 ▪ <i>bandwidthlimit</i> = -1 (unlimited) or integer between 5 and 200 (KB/sec) <p>The imagequality value is always an integer between 20 and 100. When imagetype = Hextile, it controls color depth reduction, with 24bpp = 100%, 21bpp = 88%, 18bpp = 75%, 15bpp = 63%, 12bpp = 50%, 9bpp = 38%, 6bpp = 25%. When imagetype = JPEG, it controls the JPEG compression level.</p>

PHSETUP Windows security parameters

The following PHSETUP parameters correspond to Windows security settings on the "[Security tab](#)" in the 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> <ul style="list-style-type: none"> 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
<code>setservicesecurityowner:user</code>	<p>Specify the service security rights owner to a particular user (provide domain\username).</p>

`removeservicesecurityace:user`

Set flags to remove service security rights for a given *user* (use the `domain\username` syntax).

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

`addadminsecurityace:user,flags`

Set flags to specify the administration security rights (in hexadecimal format) for a given user account. See [“Admin Security tab”](#).

- 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
- 0xE003F - All Rights

`setadminsecurityowner:user`

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

`removeadminssecurityace:user`

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

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

`addsettingssecurityace:user,flags`

Set flags to specify settings security (in hexadecimal format) for a given user account. See ["Settings Security tab"](#).

- 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

`setsettingssecurityowner:user`

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

`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 the 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"](#)
- ◆ ["SETUP EXE 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	<p>Specify a user interface level:</p> <p>/qn No user interface</p> <p>/qb Basic user interface</p> <p>/qr Reduced user interface, modal dialog displayed at the end of installation</p> <p>/qf Full user interface with modal dialog displayed at the end of installation</p>
----	---------	--

/l	e v * <i>logfile</i>	<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: msiexec /i example.msi /le logfile.txt</p>
----	-------------------------	---

SETUP.EXE options

The following table contains a partial list of `MSIEXEC` setup options:

Option	Command Line	Description
/s	setup.exe /s	Run the setup.exe portion of the MSI in silent mode.
/a	setup.exe /a	Run MSI installation in administrative mode
/x	setup.exe /x	Uninstall the application
/w	setup.exe /w	Force setup.exe to wait until the installation is complete before exiting.
/v	setup.exe /v "parameters"	Pass the parameters to msiexec.exe. NOTE: The /v option requires the complete set of parameter:value pairs to be enclosed in double quotes.

MSIEXEC variables

Any of the following `MSIEXEC` parameters can be included when you implement command line installation of the 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 the Host license key that is distributed with the purchase of the software.

HOSTSETTINGS	<p>The required the Host configuration properties that are passed to the PHSETUP utility.</p> <p>See "Configure Host from the command line".</p>
ARPSYSTEMCOMPONENT	<p>Setting this value to "1" disables the ability to Add/Remove/Modify the product via Control Panel.</p> <p>NOTE: <i>Default value "0" allows users to modify the program through Add/Remove Programs.</i></p>
TRANSFORMS	<p>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.</p>
INSTALLDIR	<p>Specify the directory in which to install the software.</p>
<pre>REBOOT { Force Suppress ReallySuppress }</pre>	<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: <i>The Host</i></p>

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.

NOFIREWALLCONFIG

Turn off automatic registration of the 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.

NOTE: By default, when the Host Installer runs in silent mode (no user interface), it restarts the target computer after the Host is installed. Override this behavior by using the REBOOT argument with *setup.exe*:

```
setup /s /v"/qn REBOOT=Suppress INSTALLDIR=path"
```

During a non-silent install (that is, an installation process that includes an installer wizard), the Host user can control whether or not the computer reboots after the Host is installed.

Examples

The following examples use command lines to install the Host:

- ◆ MSIEXEC
- ◆ SETUP
- ◆ Start/Wait

MSIEXEC

The following two examples use command lines to install the Host using `msiexec`.

- ◆ The first example silently runs the Host installer file located in the `C:\Program Files\...\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\...\Host"
```

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

NOTE: If there are embedded quotes, `MSIEXE` requires that they be quote-quoted; i.e., " becomes `""`. For example, the `PHSETUP` command line:

```
PHSETUP name:"hello there" ip:on ipx:off
```

becomes:

```
MSIEXEC /I Host.msi HOSTSETTINGS="name:""hello there"" ip:on ipx:off"
```

- ◆ The second example silently runs the the Host installer file `Host.msi` and applies the transform file `STANDARDHOST.MST`. Transform files can be created using the 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"
```

SETUP

The following example silently installs the Host from the `SETUP.exe` file located in the `C:\Program Files\...\Host` directory and suppresses the `REBOOT` at the end of the installation, and then, through `PHSETUP` commands, configures the Host computer name to “apple,” sets the password to “core.”

```
setup.exe /s /v"/qn LICENSE=1234567890 REBOOT=Suppress  
HOSTSETTINGS=\name:""apple password:core\""  
INSTALLDIR="c:\Program Files\...\Host"
```

NOTE: Make sure that `INSTALLDIR` is the last argument in the sequence when using long file names.

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\...\Host"
```

Lock-down settings

Use the 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 the Host settings, so that any the 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 the 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 the 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 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 the 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 Host settings, execute the following command line string:

```
phsetup mode:lockdown mode:reset
```

NOTE: *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 group that executed the original lockdown.*

