

Release Notes

PC-Duo 12.0

Overview

PC-Duo remote desktop software has been an essential tool for helpdesk organizations for over 15 years — providing 24x7 access to desktops and critical network devices, and speeding problem diagnosis and resolution.

General Information

The PC-Duo 12.0 documentation (in Adobe Acrobat .PDF format) is available as part of the download packages available at <http://www.vector-networks.com>.

PC-Duo Components

PC-Duo 12.0 runs on Windows 7/Windows Vista/Windows XP/Server 2008 R2/Server 2008/Server 2003 and consists of the following components:

- ▶ **PC-Duo Host** allows a PC or server to be viewed and operated.
- ▶ **PC-Duo Terminal Server Host** injects a Host instance into one or more concurrent terminal sessions.
- ▶ **PC-Duo Master** allows you to view and operate PC-Duo Hosts.
- ▶ **PC-Duo Gateway Server**, the central component of PC-Duo Server Edition, handles configuration and management of security and access to Hosts.
- ▶ **PC-Duo Web Console**, a web application based on Microsoft IIS, enables web-based access to the Gateway Server and to Hosts.
- ▶ **PC-Duo Remote Desktop**, a click-once application available through the PC-Duo Web Console that provides a view of and the ability to control a remote desktop.
- ▶ **PC-Duo Deployment Tool** allows you to easily configure and automatically deploy PC-Duo applications to large numbers of computers enterprise-wide.

PC-Duo Services

PC-Duo 12.0 supports the following services on its secure connections between Hosts and Masters:

- ▶ **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
- ▶ **Remote Management:** ability to generate inventory of hardware and software assets on remote machine, and to query and change certain system settings

New Features

New Features in 12.0

PC-Duo 12.0 introduces the following new features and capabilities:

- ▶ **Web Console:** A new server-side application that enables browser-based access to the Gateway Server (see *PC-Duo Web Console Operating Guide*)
- ▶ **"Click Once" Remote Desktop Window:** Ability to launch a Remote Desktop Window to a remote desktop through the Web Console without a Master. No administrative rights needed and no reboot required (see *PC-Duo Web Console Operating Guide*)
- ▶ **Citrix XenApp support:** Option to restrict injection of Terminal Services Host instances into "desktop" sessions only, and not into "application" sessions (see *PC-Duo Host Guide*)
- ▶ **Kernel-mode Screen Capture driver:** The kernel-mode screen capture driver is now available for Windows 7, Vista and Windows 2008 Server. In many situations, the kernel-mode screen capture driver will outperform the default user-mode screen capture driver (see *PC-Duo Host Guide*)
- ▶ **Input Suppression:** Ability to turn off keyboard and mouse input on the remote desktop machine for Windows 7, Vista and Windows 2008 Server (see *PC-Duo Host Guide*)
- ▶ **Assignment of Hosts:** Ability to automate the assignment of Hosts to custom Gateway Groups using Windows Powershell scripting (see *PC-Duo Host Guide*)
- ▶ **Address Bindings:** Ability to bind the SSL and TCP network protocols to all addresses or to select specific addresses on the Gateway Server (see *PC-Duo Gateway Administrator Guide*)

New Features in 11.6

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

- ▶ **Connection notification enhancements:** Additional connection information is included in "popup toast" notification on the Host, in particular the identity of the Master user requesting connection. If initial connection is Gateway-managed, subsequent connections will cause the toast popup to reappear. Previously, the Host toast notification only appeared on the first connection.
- ▶ **Active users list:** A new option is available when right-clicking the PC-Duo icon in the system tray on the Host which will show all the active users (Masters) connected to it and/or any active recordings.
- ▶ **End-to-end authentication:** For certain services (such as file transfer, remote Host administration, and remote management), the Master end-user may be asked to authenticate directly to the Host, even if the Master has already authenticated successfully to the Gateway. Previously, the Host simply denied these services if proper credentials were not available.

- ▶ **Extension tags:** To support extensibility for 3rd-party applications that want to integrate the PC-Duo solution, extension tags are now available for collecting and persisting metadata attributes of the Host or Host connection (e.g. phone extension for the phone next to the Host computer). Extension tags are name/value pairs that can be used to collect custom information for any Host. A field for an extension tag has also been added to store custom information about a PC-Duo recording.
- ▶ **Restart in Safe Mode:** The Host now includes the ability to reboot in Safe Mode. Note that Host will run with user-mode screen capture capabilities only since the goal is to minimize the number of kernel drivers loaded on a safe-boot.
- ▶ **Display option enhancements:** The Fit-to-Window display option in the Master has been modified to preserve the Host screen aspect ratio, and to center the display in the available space. Also, text mode screen is now centered in available space in all display modes.
- ▶ **Color depth reduction** has been introduced in the Host screen capture algorithm to provide another option for bandwidth throttling.
- ▶ **Manage Visual Effects** has been improved to include support for Aero glass on Windows Vista and Windows 7 desktops.
- ▶ **Clipboard** now supports automatic sharing between Host and Master.
- ▶ **Master toolbar and menu** include several improvements including new option for sending Ctrl-Alt-Del to Host from toolbar.
- ▶ **Queue for Status Update** enables the Gateway to immediately poll any Host for a status update.
- ▶ **Active Host Status and Reverse Connections group** which is located in the Active Status folder on the Gateway, has been split into two separate groups: Pending Host Status Updates and Reverse Connections groups.
- ▶ **PhSETUP** command now has a reset option.
- ▶ **TS 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.
- ▶ **Full Screen mode** now supports auto-scrolling in all directions.
- ▶ **Screen capture** at startup and at subsequent checkpoints are now using higher compression and therefore transmit faster.
- ▶ **Deployment Tool** now includes support for customizing missing Host security settings.
- ▶ **Windows 7 support:** PC-Duo 11.6 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 11.6 provides full support (remote access, remote control, remote management) for Windows Server 2008 R2 computers (64-bit platforms only).

- ▶ **Mac, Linux support:** PC-Duo 11.6 provides support (remote access, remote control) for Macintosh and Linux computers running VNC server software (standard on Macs).
- ▶ **Wake-on-LAN support:** PC-Duo 11.6 includes ability to turn on remote computers that are configured to listen for Wake-on-LAN signal.
- ▶ **Remote Power Scheme management:** PC-Duo 11.6 includes new remote management tools that allows Master user to view and change power scheme settings on remote computers.
- ▶ **Screen Recording Playback via URL:** PC-Duo 11.6 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 11.6 Host will capture and provide input control to the RDP session.
- ▶ **Active Directory integration:** PC-Duo 11.6 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.

Enhancements & Fixes

Enhancements & Fixes in 12.0

PC-Duo 12.0 includes the following defect fixes:

- ▶ **Deployment Tool with large OU**, which failed when a single OU reached 1000 computers, can now scale well beyond that.
- ▶ **Gateway cleanup of old recordings**, which did not always occur, is now run as part of the scheduled periodic tasks.
- ▶ **SSL certificate acceptance dialog**, which sometimes did not allow a user to accept an invalid certificate, even if they elected to do so, has been fixed.
- ▶ **Play back of recordings**, which would fail under some rare conditions, is now more reliable.
- ▶ **Fit-to-Window display mode**, which sometimes looked distorted depending upon the aspect ratio needed for scaling, is now greatly improved with the new "Half-Tone" setting in the Remote Desktop Window.
- ▶ **Export to WMV**, which sometimes did not handle text-mode screens correctly, has been fixed.
- ▶ **Chat with multiple Masters** now consistently shows the correct usernames.
- ▶ **Mouse wheel**, which did not always work correctly in Master, now works as expected.
- ▶ **Unresponsive Host**, which sometimes caused the Gateway to crash, is now handled correctly.
- ▶ **Long Host station names**, which sometime caused the Master to crash, are now handled correctly.
- ▶ **Text mode screen issues**, including centering in Fit 1:1 display mode and preserving of background, have been fixed.
- ▶ **Wake-On-LAN issues**, including asynchronous execution, have been addressed.
- ▶ **Input suppression** now works correctly on Host for XP with user-mode screen capture.
- ▶ **Gateway connection limits** are now monitored to insure that administrative access will always be able to get through, even in the event that the Gateway is overloaded with Host connections.
- ▶ **Reverse connestions**, which were sometimes dropped on certain networks, are now much more resilient and reliable.
- ▶ **Host macros "%USERNAME%" and "%USER%"**, which used to resolve incorrectly on computer restart before any user logs in, has been fixed.

Enhancements & Fixes in 11.6

PC-Duo 11.6 includes the following defect fixes:

- ▶ **Windows + Break key combination**, which was not being injected correctly into remote desktop, has been fixed.
- ▶ **Connection encryption**, which in some circumstances was found to be intermittent, has been fixed. Please see *Note on Encryption Fix* for more information below.
- ▶ **Address restrictions** for accessing Host(s) through Gateway, which were not being enforced, are working now.
- ▶ **Ctrl+Alt+Del sequence** injected into XP/2003 at the logged-in desktop, which did not go to Windows Security screen, goes there now.
- ▶ **User -mode screen capture**, which used to corrupt captured screen data if horizontal screen resolution was not divisible by 8, has been fixed. Note that this only happened in a virtualized environment - no physical display mode has this property/behavior.
- ▶ **Host for Terminal Services**, which didn't work on Server 2003 x64 edition, is now fixed. The fix comes with some limitations, but does allow recording of TS sessions on this operating system. Please see *Note on Host for Terminal Services Fix* for more information below.
- ▶ **Clipboard control**, which was not being enabled for second Master connecting through Gateway to a Host, has been fixed.
- ▶ **Sending WOL signal**, which sometimes takes a long time to process, has been changed to asynchronous operation to reduce response time.
- ▶ **Host macros "%USERNAME%" and "%USER%"**, which used to resolve incorrectly on computer restart before any user logs in, has been fixed.
- ▶ **Keyboard and mouse input control** for Host instances running in terminal server sessions, which in some cases would not run when Microsoft or Citrix virtualization add-ons were installed, is now more compatible with them.
- ▶ **Grey-screen at connect time**, which used to occur in a few reported circumstances, has been fixed.
- ▶ **Permission to Connect**, which used to fail in certain circumstances, has been fixed.
- ▶ **Clipboard control** can now be accessed by subsequent Masters connecting to the same Host.
- ▶ **Host tray icon** no longer disappears when Host service is restarted.

Additional Notes

Note on Encryption Fix in 11.6

Connection encryption, which in some circumstances was found to be intermittent, has been fixed. Below is additional information about the defect, the circumstances in which the defect may affect performance, and mitigation options.

Defect Description

By default, connections between PC-Duo components (for example, Master-to-Host, Gateway-to-Host, Master-to-Gateway) use encryption (the current version is set by default to use the AES 256-bit cypher). We have determined that in certain circumstances, a defect in the encryption code occasionally causes encryption to be dropped, even though one or both PC-Duo components are configured to use encryption.

This defect has been identified in Gateway and Workstation Editions of PC-Duo versions 10.0 through 11.6.

Defect Scenarios

This defect can affect both peer-to-peer and Gateway-managed connections. There is no indication to the user when encryption is dropped (for example, the Lock icon will still show in the status bar of the Master, and Gateway Administrator will indicate encryption method being used in several places), nor is there any error message associated with this defect.

However, the defect does not affect the following circumstances:

- ▶ Does not affect SSL connections. With SSL protocol, encryption is explicitly enforced and is unaffected by this defect.
- ▶ Does not affect reverse connections. Reverse connections are typically utilized when Host is outside the domain of the Gateway. Reverse connections allow Hosts to safely and seamlessly navigate NATs and firewalls and connect to a Gateway. This is arguably the most vulnerable connection type (since it can involve sending information over the public Internet) but it is not affected by this defect, i.e. encryption has been observed to be always in force.
- ▶ The initial connection between PC-Duo components is not affected by this defect, so the very first service activity (e.g. remote viewing, recording playback) will not be affected.

Mitigation Options

Following are mitigation options for this defect:

- ▶ **No action.** For most customers, the intermittent enforcement of encryption may not be a significant issue, and no action may be necessary:

- ▷ Only peer-to-peer or Gateway-managed connections within the same domain are vulnerable to this defect, but most corporate domains are protected and considered safe environments.
 - ▷ PC-Duo data, while not encrypted, is encoded in a proprietary format and compressed, so intercepting and decoding that data would not be a casual challenge. Also note that this defect does not affect the initial connection between PC-Duo components.
 - ▷ The initial connection between PC-Duo components is not affected by this defect, so connections made to accomplish one and only one task will not be affected.
- ▶ **Upgrade to version 11.6.** This maintenance release contains a fix for the root cause of the defect. The fix will enforce encryption when a 11.6 PC-Duo “client” (typically Master in peer-to-peer connections, or the Master connecting to a Gateway in the first half of a Gateway-managed connection, and the Gateway connecting to a Host in the second half) communicates with a 11.6 or older component. Customers should upgrade all PC-Duo components to 11.6 in order to ensure persistent enforcement of encryption on their connections. At a minimum, customers should upgrade Masters (and Gateways if present) to 11.6 to ensure encryption is enforced. Hosts can be a client in reverse connections but those are not affected by this defect. If a 11.6 or older PC-Duo client application tries to connect to a 11.6 Host, and encryption is requested but not enforced, the connection will be terminated and a new error code generated (0xC004DEAD).
 - ▶ **Registry modification to existing PC-Duo components.** For customers with PC-Duo components from version 11.3 through 11.6, a simple registry patch can be used to work around this defect. (Note: Customers with PC-Duo components from version 10.0 to 11.0 must either upgrade (at least the clients) to 11.6 or take no action.) As with the upgrade option, customers should apply the registry patch to all computers running PC-Duo software, but *at a minimum, customers must apply the patch to Masters (and Gateways if present)*. Also note that customers must monitor deployment of new Masters and Gateways, and ensure that registry patch is applied if 11.6 (or later) software is not used. If a new Master or Gateway comes online and the patch is not applied, the defect may be active and will not be noticeable.
 - ▷ The registry setting for Windows x86 systems is:
[HKEY_LOCAL_MACHINE\SOFTWARE\Funk Software, Inc.\Proxy v5\Transport] "ShareSession"=dword:00000000
 - ▷ The registry setting for Windows x64 systems is:
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Funk Software, Inc.\Proxy v5\Transport] "ShareSession"=dword:00000000

Following table summarizes the impact of different mitigation options:

Table 1. Mitigation Options for Encryption Defect

Mitigation Options	No Action	Upgrade PC-Duo clients & servers to 11.6	Upgrade PC-Duo clients only (Masters, Gateways)	Upgrade PC-Duo servers (Hosts) only	Patch PC-Duo clients & servers to 11.6	Patch PC-Duo clients only (Masters, Gateways)
Encryption enforced on SSL connections	Yes	Yes	Yes		Yes	Yes
Encryption enforced on reverse connections	Yes	Yes	Yes		Yes	Yes
Encryption enforced on P2P connections		Yes	Yes		Yes	Yes
Encryption enforced on Gateway-managed connections in same domain		Yes	Yes		Yes	Yes
Connection terminated when encryption not enforced				Yes		
Applies to all affected releases (10.0 to 11.6)	Yes	Yes	Yes	Yes	Does not apply to 10.0 - 11.0	Does not apply to 10.0 - 11.0

Note on Host for Terminal Services on Server 2003 x64 Fix

There is a bug in 64-bit Windows Server 2003 that hinders our ability to get the identity of the user that's logged in to the terminal services session. As a result, the following limitations may be observed:

- ▶ If “%USER%” is in the station name, the name “Not-Logged-In” may be seen instead of the real user name.
- ▶ The “User” column in the Gateway Administrator views should eventually get the correct user name, but this is not guaranteed.
- ▶ We cannot impersonate the logged-in user, so end-to-end services like file transfer and remote management will not work if simple password authentication is used. Note that use of Windows Authentication is strongly recommended over simple password, especially in terminal services environments.
- ▶ File transfer with Windows Authentication cannot evaluate the paths for the “Personal” and “Common” folder collections (which include “Desktop”, “My Documents”, “Shared Documents”, etc.). Users can navigate to these folders using their real paths, but the shortcuts do not appear in the file transfer user interface.

Legal Notices

Copyright © 2012 Vector Networks Technologies and Proxy Networks, Inc. All rights reserved. PC-Duo is a trademark of Vector Networks Technologies and PROXY is a trademark of Proxy Networks, Inc. Microsoft, Windows, Windows NT, Windows Server, and other Microsoft products referenced herein are either trademarks or registered trademarks of the Microsoft Corporation in the United States and other countries.

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/>).

