Vector PCDUO

PC-Duo 12.5

Release Notes

Overview of PC-Duo 12.5

PC-Duo remote desktop software has been an essential tool for helpdesk organizations for nearly 20 years — providing 24x7 access to desktops and critical network devices, and speeding problem diagnosis and resolution.

General Information

The PC-Duo 12.5 documentation (in Adobe Acrobat .PDF format) is included in the download packages available at http://www.vector-networks.com.

PC-Duo Supported Platforms

PC-Duo 12.5 is supported on the following platforms:

- Windows 8.1
- Windows Server 2012 R2
- Windows 8
- Windows Server 2012
- Windows 7
- Windows Server 2008 R2
- Windows Vista
- Windows Server 2008
- Windows XP
- Windows Server 2003

PC-Duo Components

PC-Duo 12.5 consists of the following components:

- **PC-Duo Host** enables the desktop of a Windows PC or server to be viewed and controlled remotely.
- **PC-Duo Terminal Server Host** injects a Host instance into one or more concurrent terminal sessions.
- **PC-Duo VDI Host** is a special version of the Host that can be included as part of a virtual desktop template and will run as a transient service in a virtual desktop image. Allows for much easier management of Gateway connections.
- **PC-Duo Host on Demand (HOD)** is a streamlined version of the Host that that can be launched from the Share My Desktop button on the Web Console landing page. It enables the desktop of any internet-accessible machine to be shared instantly. No local or network administrative privileges are required, and no reboot is necessary to run the HOD.
- **PC-Duo Master** allows user 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 web-based 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 user to easily configure and automatically deploy PC-Duo applications to large numbers of computers enterprise-wide.

PC-Duo Services

PC-Duo 12.5 supports the following services over 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 12.5

PC-Duo 12.5 introduces the following new features and capabilities:

- **UAC Elevation:** Master user can elevate Host on Demand process to high privilege level by allowing the remote user to enter administrative credentials on the HOD desktop (see *PC-Duo Web Console Operating Guide*)
- **Host on Demand:** New type of Host that can be launched from the Share My Desktop button on the Web Console landing page. Enables the desktop of any internet-accessible machine to be shared instantly. No local or network administrative privileges are required, and no reboot is necessary to run this new Host type (see *PC-Duo Web Console Operating Guide*)
- **View/Edit Host Settings from Web Console:** Host settings for any Host connected to the Gateway can be viewed and/or edited by Account Users with appropriate credentials through the Web Console. No connection window to Host desktop required (see PC-Duo Web Console Operating Guide)
- **WebSocket Transport (WS, WSS):** In addition to the UDP, TCP and SSL transports already available, the Gateway Server now supports WebSocket (binary WebSocket over HTTP) and Secure WebSocket (binary WebSocket over HTTPS) transports to facilitate connections through corporate firewalls (see PC-Duo Gateway Guide)
- **Support for LDAPS**: Encryption of connections between the PC-Duo Gateway and the domain controller(s) when doing Active Directory lookups
- **Web Console support for Safari, Chrome and Firefox**: Web Console now supports Safari, Chrome and Firefox web browsers, in addition to Internet Explorer; helper apps may be required to enable Remote Desktop and other features (see *PC-Duo Web Console Installation Guide*)

New Features in 12.1

PC-Duo 12.1 introduced the following new features and capabilities:

- **Concurrent User License Mode**: In this mode, the Gateway will monitor the number of simultaneous Gateway users according to account type (Administrative, Master, Personal) (see *PC-Duo Web Console Operating Guide*)
- **Inactivity Timeouts:** To free up concurrent user licenses when users are connected to the Gateway but not active, Web Console, Master and Gateway Administrator will be automatically disconnected from the Gateway, and input control will be automatically released from Remote Desktop or Master Connection Window (see *PC-Duo Gateway Administrator Guide*)
- **Automatic Grouping of Hosts**: Ability to configure Hosts to automatically report to custom Gateway group(s) according to custom or generic rules (see *PC-Duo Gateway Administrator Guide*)

- **Virtual Desktop support:** Enables virtual desktop images generated in environments such as Citrix XenDesktop to include Hosts, and to have the Hosts report to Gateway until the desktop image is discarded (see *PC-Duo Host Guide*)
- **Web Console**: A new server-side application that enables browser-based access to the Gateway Server (see *PC-Duo Web Console Operating Guide*)
- **Remote Desktop Window**: Ability to launch a Remote Desktop window through the Web Console, bypassing need to have an installed 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 introduced 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 Proxy 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 7.0.0 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 7.0.0 provides full support (remote access, remote control, remote management) for Windows Server 2008 R2 computers (64-bit platforms only).
- **Mac, Linux support**: PC-Duo 7.0.0 provides support (remote access, remote control) for Macintosh and Linux computers running VNC server software (standard on Macs).
- **Wake-on-LAN support**: PC-Duo 7.0.0 includes ability to turn on remote computers that are configured to listen for Wake-on-LAN signal.
- **Remote Power Scheme management**: PC-Duo 7.0.0 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 7.0.0 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 7.0.0 Host will capture and provide input control to the RDP session.
- **Active Directory integration:** PC-Duo 7.0.0 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 and Fixes

New Enhancements and Fixes in 12.5

Following is a list of major enhancements in PC-Duo 12.5:

- Explicit web proxy support: If a customer uses a web proxy server to manage internet traffic coming into or going out of its network, PC-Duo applications that are outside the network (such as Host or Master) will be able to negotiate automatically with the web proxy to reach a Gateway server inside the network.
- Json file delivery mode: If Web Console is behind a firewall, the location of the Json file for Host on Demand can be pre-configured, eliminating the need to make an additional HTTP request.
- Host services enabled by default configuration option is now applicable only to Host on Demand. Default settings are available in the Web Console Settings > Host on Demand section of the Gateway tab in the Web Console.
- Local network address exceptions: The Gateway server allows for one or more addresses or address ranges to be reclassified as external, even if they appear in the range of local network addresses.
- Trusted Device list: If the Windows account user has any trusted devices, they can be added to list of machines that will be granted access to the Gateway server.
- View/edit Host services enabled at connection time: Host user will be able to specify which Host services to enable by default when Remote Desktop connections are established; if Permission to Connect is enabled, then Host user will be able to view/edit the list of Host services to enable for each Remote Desktop connection request.
- Permission to Connect suppression option: If Permission to Connect is enabled, this new option will suppress the Permission to Connect requirement if the Host desktop is locked or waiting for logon
- Toast notification for any active connections: When the Host user logs in, he/she will be presented with a list of any Account Users with active Remote Desktop connections to the Host in a toast popup notification window
- Import/export Host settings in JSON format: Host settings can be exported to a text file in JavaScript Object Notation (JSON) format; Host settings can also be imported from a text file in JSON format.
- Connect to Host settings options: New security options for accessing Host settings from the Host tray icon and the Host Control Panel itself allow for connection to the Host settings as different user.
- Web Console database overflow protection: Unneeded data is now regularly purged from the SQL database.
- More Host Grouping Rules: Additional grouping rules have been added to allow for more flexibility in creating custom collections of Hosts (see PC-Duo Gateway Guide)
- Peer-to-Peer Host Administration: Allows access to Host settings when Host is configured to accept connections through listed Gateways only. Particularly useful for certain operations involving the Deployment Tool.

Following is a list of major defect fixes in PC-Duo 12.5:

- Replaced OpenSSL library with version 1.0.1g, which includes fix for the "Heartbleed" vulnerability. Anyone with Gateway Server version 11.6 through 12.1 should upgrade to PC-Duo Gateway 12.5, especially if Gateway Server is configured to listen for connections directly from the Internet.
- Duplicate GUID protection. Duplicate Host GUIDs can occur when the HostPrep utility is not run on a Windows OS image containing PC-Duo Host software prior to deployment. This condition resulted in unexpected behavior.
- Host for Terminal Services Session Host process injection issue resolved. This was a regression from version 7 to version 8.0 and was seen only on Windows Server 2003. (Back-ported to 8.0.2 Hotfix #4). This allows for more robust compatibility with software like Citrix XenApp.

New Enhancements and Fixes in 12.1

Following is a list of major defect fixes in PC-Duo 12.1:

- Remote Management fixed in ClickOnce connection window (Defect #3993)
- Web Console database overflow protection
- More robust handling of Host for Terminal Services on slow systems, especially in Server 2003
- Support for users belonging to more than 85 AD groups (large token)
- Transport updated to support WS and WSS protocols for use with future releases
- Web Console now redistributes MVC3, thus removing the prerequisite
- Windows Server 2012 and Windows 8 platform correctly identified (Defect #3514)
- Deployment Tool now shows all available choices across supported platforms (Defect #3595)
- VNC connection to OS X v10.8.2 now supports virtual sessions and mouse wheel (Defect #3676, 3677)
- Host for Terminal Services now showing correct Client address and name at the Gateway (Defect #3700)
- Remote Printing support added to connection window
- Connection Window now supports “Prompt to Reconnect”
- OpenSSL updated to v1.0.1e
- SDK samples updated
- Registry override to restore upper-left justification of remote Host display in Master
- Restore better handling of multiple monitors with negative coordinates
- Improved File Transfer error reporting (Defect #2388)
- Web Console support for Windows Server 2012 (Defect #3498)
- Clicking on “Reconnect” will use saved credentials (Defect #3542)
- Clipboard service connection/termination messages fixed (Defect #3745, 3870)
- Improved diagnostic logging

- Support for 64-bit SDK encoder module
- More robust handling of special characters in Web Console
- Proxy SDK Runtime x64 now includes the PrxEnc SDK control for media conversion. Previously, this control was unavailable in x64.
- German messages that got broken in 8.0.0 are now fixed (Defect #3475)
- Mirror driver correctly processes screen resolution changes made in-between Remote Control sessions in all cases (Defect #3481)
- Resolved lack of input at console problem when specific Symantec LiveState driver was installed (Defect #3482)

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 Proxy 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 Proxy 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 Proxy 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.
    - Proxy 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 Proxy components.
    - The initial connection between Proxy 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 Proxy “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 Proxy 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 Proxy 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 Proxy components.** For customers with Proxy components from version 10.0 through 11.6, a simple registry patch can be used to work around this defect. (Note: Customers with Proxy components from version 10.0 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 Proxy 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 Proxy clients & servers to 11.6	Upgrade Proxy clients only (Masters, Gateways)	Upgrade Proxy servers (Hosts) only	Patch Proxy clients & servers to 11.6	Patch Proxy 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)	Yes	Yes	Yes	Yes	Does not apply to 10.0	Does not apply to 10.0

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

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/).