



PROXY Pro 8.0.3 (Hotfix #7)

Release Notes

August 2016

Overview of PROXY Pro 8.0.3

PROXY Pro 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 PROXY Pro 8.0.3 documentation (in Adobe Acrobat .PDF format) is included in the download packages available at <http://www.proxynetworks.com> and at <ftp://ftp.proxynetworks.com>.

PROXY Pro Supported Platforms

PROXY Pro 8.0.3 is supported on the following platforms:

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

PROXY Pro Components

PROXY Pro 8.0.3 consists of the following components:

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

PROXY Pro Services

PROXY Pro 8.0.3 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 PROXY Pro 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 8.0.3

PROXY Pro 8.0.3 introduces the following new features and capabilities:

- **Supported Operating Systems:** PROXY Pro is now supported on Windows 8.1 and Windows Server 2012 R2

New Features in 8.0.2

PROXY Pro 8.0.2 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 *PROXY Pro 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 Web Desktop or Connection Window (see *PROXY Pro 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 *PROXY Pro 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 *PROXY Pro Host Guide*)

New Features in 8.0.1

PROXY Pro 8.0.1 was an internal maintenance release.

New Features in 8.0.0

PROXY Pro 8.0.0 introduced the following new features and capabilities:

- **Web Console:** A new server-side application that enables browser-based access to the Gateway Server (see *PROXY Pro 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 *PROXY Pro 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 *PROXY Pro 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 *PROXY Pro 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 *PROXY Pro Host Guide*)
- **Assignment of Hosts:** Ability to automate the assignment of Hosts to custom Gateway Groups using Windows Powershell scripting (see *PROXY Pro 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 *PROXY Pro Gateway Administrator Guide*)

New Features in 7.0.5

PROXY Pro 7.0.5 was performance enhancement release.

New Features in 7.0.4

PROXY Pro 7.0.4 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 PROXY Pro 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 PROXY Pro 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.

New Features in 7.0.3

PROXY Pro 7.0.3 was an internal maintenance release.

New Features in 7.0.2

PROXY Pro 7.0.2 introduced the following new features and capabilities:

- **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.

New Features in 7.0.1

PROXY Pro 7.0.1 introduced the following new features and capabilities:

- **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.

New Features in 7.0.0

PROXY Pro 7.0.0 introduced the following new features and capabilities:

- **Windows 7 support:** PROXY Pro 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:** PROXY Pro 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:** PROXY Pro 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:** PROXY Pro 7.0.0 includes ability to turn on remote computers that are configured to listen for Wake-on-LAN signal.
- **Remote Power Scheme management:** PROXY Pro 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:** PROXY Pro 7.0.0 includes ability for Master to playback a PROXY Pro screen recording from a standard web server over HTTP or HTTPS.
- **RDP compatibility:** If a remote computer is hosting an active RDP session, PROXY Pro 7.0.0 Host will capture and provide input control to the RDP session.
- **Active Directory integration:** PROXY Pro 7.0.0 Deployment Tool can now be used to discover computers and OUs in Active Directory domains, install new PROXY Pro software, upgrade existing software, and/or push configuration changes to existing software.

Defect Fixes & Performance Enhancements

Following is a list of major defects fixes and performance enhancements in recent releases:

PROXY Pro 8.0.3 (Hotfix #7)

PROXY Pro 8.0.3 (Hotfix #7) includes the following defect fixes and performance enhancements:

- **Host reliability fix:** long-running Host could crash due to address space leak in Host status reporting. Other status reporting improvements, especially around failed status reports to overloaded Gateway Server.
- **Gateway Server reliability improvements,** including fixing memory leaks that degrade Gateway Server performance over time.
- **Gateway Certificate Manager** now checks for “write encryption” access right to attempt change to Gateway encryption settings (including selected SSL certificate).
- Master ability to playback recorded session from URL now works reliably.

PROXY Pro 8.0.3 (Hotfix #6)

PROXY Pro 8.0.3 (Hotfix #6) includes the following defect fixes and performance enhancements:

- **Gateway Server now verifies SPNs:** When the Gateway server service starts, it now does a check to verify the registered SPNs for the Gateway service and audit logs any issues or errors. Also, the CheckSPNs utility program now has improved messaging.
- **Improved Host status reporting logic for multiple Gateway entries:** Host logic to correctly report to a Gateway where multiple configurations refer to the same Gateway has been improved. Specifically the number of connections made by the Host to that Gateway have been reduced.
- Replaced OpenSSL library with version 1.0.2h, which is a security release of OpenSSL. Customers with internet-facing Gateway Servers listening for SSL connections are encouraged to upgrade to this release.
- The Gateway Certificate Manager now handles wildcard SSL certificates, and creates/requests certificates with an SHA256 signature.
- A grey screen no longer appears when trying to control a device with text scale >100%. (UMSC only)
- Host no longer reports EventID=0 on connection with bad license.
- Host trial expiration notification made less intrusive.
- Host station name was not being updated at the Gateway Server if Host maintained a reverse connection with the Gateway.

PROXY Pro 8.0.3 (Hotfix #5)

PROXY Pro 8.0.3 (Hotfix #5) includes the following defect fixes and performance enhancements:

- Replaced OpenSSL library with version 1.0.1o, which includes fixes for some newly found security vulnerabilities.

PROXY Pro 8.0.3 (Hotfix #4)

PROXY Pro 8.0.3 (Hotfix #4) includes the following defect fixes and performance enhancements:

- Replaced OpenSSL library with version 1.0.1k, which includes fixes for newly found security vulnerabilities.
- Gateway Server SSL connections now support TLS v1.0, TLS v1.1, and TLS v1.2 protocols for improved compatibility with future releases.
- This release accepts new time-limited trial keys that allow trials to extend further in the future than previous releases. This software version is required for use with time-limited trials (other than the standard 30-day trial) after June 30, 2015.

PROXY Pro 8.0.3 (Hotfix #3)

PROXY Pro 8.0.3 (Hotfix #3) includes the following defect fixes and performance enhancements:

- Replaced OpenSSL library with version 1.0.1j, which includes fixes for newly found security vulnerabilities post the “Heartbleed” fix. Anyone with Gateway Server version 7.0.x through 8.0.3 should upgrade to PROXY Pro Gateway 8.0.3 (Hotfix #3), especially if Gateway Server is configured to listen for connections directly from the Internet.
- When running Host on a touch-based device that does not have an attached mouse, and does not show a mouse pointer, the Master may not see a mouse pointer when it connects, making it difficult to remotely operate the system. This hotfix enables a workaround for this issue that requires specific configuration; contact technical support for additional guidance if you have this scenario.
- Host has compatibility fix to ensure the PROXY Pro Remote Desktop application for iOS can join other Masters and share a Host session.

PROXY Pro 8.0.3 (Hotfix #2)

PROXY Pro 8.0.3 (Hotfix #2) includes the following defect fixes and performance enhancements:

- Replaced OpenSSL library with version 1.0.1h, which includes fixes for newly found security vulnerabilities. These vulnerabilities allow a denial-of-service attack against the Gateway Server, if it’s configured to listen for incoming SSL connections. Anyone with Gateway Server version 7.0.x through 8.0.3 should upgrade to PROXY Pro Gateway 8.0.3 (Hotfix #2).

PROXY Pro 8.0.3 (Hotfix #1)

PROXY Pro 8.0.3 (Hotfix #1) includes the following defect fixes and performance enhancements:

- Replaced OpenSSL library with version 1.0.1g, which includes fix for the “Heartbleed” vulnerability. Anyone with Gateway Server version 7.0.x through 8.0.3 should upgrade to PROXY Pro Gateway 8.0.3 (Hotfix #1), especially if Gateway Server is configured to listen for connections directly from the Internet.

PROXY Pro 8.0.3

PROXY Pro 8.0.3 includes the following defect fixes and performance enhancements:

- Reliability fixes for Gateway Server, including:
 - Duplicate GUID prevention
 - More robust Host status reporting
 - Length of Gateway “Local Network Address” increased from 255 to 1024 bits
 - More robust communications at transport layer, making network connections more reliable
- Reliability fixes for the Host, including:
 - More robust user-mode screen capture in the event of start and/or stop commands

PROXY Pro 8.0.2 (Hotfix #4)

PROXY Pro 8.0.2 (Hotfix #4) includes the following defect fixes and performance enhancements:

- 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

PROXY Pro 8.0.2 (Hotfix #3)

PROXY Pro 8.0.2 (Hotfix #3) included the following defect fixes and performance enhancements:

- 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

PROXY Pro 8.0.2 (Hotfix #2)

PROXY Pro 8.0.2 (Hotfix #2) included the following defect fixes and performance enhancements:

- 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 Pro 8.0.2 (Hotfix #1)

PROXY Pro 8.0.2 (Hotfix #1) included the following defect fixes and performance enhancements:

- 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 7.0.4

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 PROXY Pro versions 5.20.0 through 7.0.2.

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 7.0.4.** This maintenance release contains a fix for the root cause of the defect. The fix will enforce encryption when a 7.0.4 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 7.0.2 or older component. Customers should upgrade all Proxy components to 7.0.4 in order to ensure persistent enforcement of encryption on their connections. At a minimum, customers should upgrade Masters (and Gateways if present) to 7.0.4 to ensure encryption is enforced. Hosts can be a client in reverse connections but those are not affected by this defect. If a 7.0.2 or older Proxy client application tries to connect to a 7.0.4 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 6.0.2 through 7.0.2, a simple registry patch can be used to work around this defect. (Note: Customers with Proxy components from version 5.20.0 to 6.0.1 must either upgrade (at least the clients) to 7.0.4 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 7.0.4 (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 7.0.4	Upgrade Proxy clients only (Masters, Gateways)	Upgrade Proxy servers (Hosts) only	Patch Proxy clients & servers to 7.0.4	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 (5.20.0 to 7.0.2)	Yes	Yes	Yes	Yes	Does not apply to 5.20.0 - 6.0.1	Does not apply to 5.20.0 - 6.0.1

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 © 2006-2016 Proxy Networks, Inc. All rights reserved. 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 (ey@cryptsoft.com), and compression software from the ZLIB project (<http://www.zlib.net/>).