



PROXY Pro 9.0.1

Release Notes

Hotfix #11 – October 2019

Overview of PROXY Pro 9.0.1

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

General Information

The PROXY Pro 9.0 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 9.0 is supported on the following platforms:

- Windows Server 2019
- Windows Server 2016
- Windows 10
- Windows 8.1
- Windows Server 2012 R2
- Windows 8
- Windows Server 2012
- Windows 7
- Windows Server 2008 R2
- Windows Vista
- Windows Server 2008

PROXY Pro Components

PROXY Pro 9.0 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 Host for Remote Desktop Services (RDS)** injects a Host instance into one or more concurrent Remote Desktop Services (RDS) sessions.
- **PROXY Pro Host for VDI** 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 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.
- **PROXY Pro Master** allows users to view and operate PROXY Pro Hosts.
- **PROXY Pro Master on Demand**, a web-based application available through the PROXY Pro Web Console that provides a view of and the ability to control a remote desktop.
- **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 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 9.0 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, and vice-versa
- **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 9.0.1

PROXY Pro 9.0.1 introduces the following new features and capabilities:

- **Security hardened Web Console:** The PROXY Pro Web Console has undergone a major security review and overhaul. Issues addressed include enhanced protection against Cross Site Request Forgery (CSRF), Cross-Site Scripting (XSS) attack, and SQL injection attacks. (*Thanks to Ezenta A/S, ezenta.com, for working with us to improve security.*)
- **Password guessing lockout:** The PROXY Pro Networking component now automatically locks out connection requests from any IP address that fails to authenticate after a certain number of attempts in a certain amount of time. This prevents scripted attempts to guess passwords.
- **Deploy and update pre-installed Master Gateway Configurations:** The PROXY Pro Deployment Tool now allows you to define one or more Gateway configurations to deploy along with the installation of the PROXY Pro Master. Also, there is now the ability to define a new or updated set of Gateway configurations and push them out to existing installations of PROXY Pro Master. Up until now, the installed Master was not ready for Gateway based connections until someone manually added a Gateway configuration.
- **Export / Import of Deployment Tool settings:** You now have the ability to export and re-import important settings for the PROXY Pro Deployment Tool via a JSON-formatted text file. This makes copying state from one machine to another much more straightforward.
- **Remote Printing module now available for download from the Web Console:** The Remote Printing Support installation file can now be downloaded directly from the PROXY Pro Web Console. This is extremely useful if you want to enable Remote Printing for the Host on Demand or on any machine that the Remote Printing support has not previously been installed.

(Please see the section, “New Enhancements and Fixes in 9.0.1”, below for more information about this release.)

New Features in 9.0.0

PROXY Pro 9.0.0 introduces the following new features and capabilities:

Note: Some terminology was changed in PROXY Pro v9.0.0 in order to keep current and to be more accurate. This included changing “Terminal Services” to “Remote Desktop Services (RDS)”. This Host is now referred to as, “Host for RDS”. “PROXY Pro Remote Desktop” is now simply “PROXY Pro Master” or “PROXY Pro Master on Demand” if launched from the Web Console.

- **Official support for Windows 10:** This release fully supports Microsoft’s Windows version 10 and the new Edge browser.
- **All new Remote Printing:** The Remote Printing feature has been completely redesigned and re-written to remove all previous restrictions. Remote Printing no longer requires matching print drivers on Host and Master; can print both from Host to Master and from Master to Host; works on all Windows operating systems (desktop and server) and editions (x86 and x64) supported by PROXY Pro v9.
- **Master on Demand for Macintosh:** Native Macintosh application that provides Connection Window and Recording Playback functionality on the Macintosh. This application is downloaded and installed from the Web Console, and is launched when a “connect” link is selected in the Web Console.
- **Ability to export data from the Web Console:** You can now export tables directly from the Web Console to a CSV or XLSX file.
- **Asynchronous notifications in Web Console:** The Web Console introduces a way for asynchronous notifications to be delivered to the user. When a notification is available, a new “Notification” icon appears in the top-level toolbar. Clicking on it provides details.

(Please see the section, “New Enhancements and Fixes in 9.0.0”, below for more information about this release.)

New Features in 8.10.2

PROXY Pro 8.10.2 introduces the following new features and capabilities:

- **Host on Demand for Macintosh OS X:** The PROXY Pro Web Console now supports launching a Host on Demand on the Macintosh OS X operating systems.
- **Select Single Monitor of Multi-monitor Host:** The installed Master and ClickOnce Connection Window supports a new option to set the view to be only one monitor of a Host that has multiple monitors.
- **Automatic Recording:** When this feature is enabled, all matching live Master connections to Hosts for remote control will be recorded. This will be configurable in the Web Console and includes features like local disk free space monitoring.
- **HOD “Elevate” is now “Pin” and there will be “Session” or “Pinned” HODs:** The type of session will be identifiable in the Web Console with new graphics. An on demand Host will be marked with a “D” and a separate “pin” icon will be highlighted if the HOD session is pinned.
- **ClickOnce connection window can suppress Host mouse and keyboard input:** This now brings functionality available only in the installed Master to the ClickOnce connection window.

- **Utility to clear the Windows ClickOnce cache:** The Windows operating system does not provide a convenient way to do this. We have now built this functionality into the Web Console itself.
- **Improved ability to customize and retain Web Console changes on upgrade:** Customization of the Web Console landing page and colors are now easier to put in place and will be maintained when the software is upgraded.

New Features in 8.10.1

PROXY Pro 8.10.1 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 *PROXY Pro Web Console Operating Guide*)

New Features in 8.10.0

PROXY Pro 8.10.0 introduced the following new features and capabilities:

- **Host on Demand:** New type of Host that can be launched from the Share My Desktop button on the Web Console landing page. Enables the desktop of any internet-accessible machine to be shared instantly. No local or network administrative privileges are required, and no reboot is necessary to run this new Host type (see *PROXY Pro 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 *PROXY Pro 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 *PROXY Pro Gateway Administrator Guide*)
- **Support for LDAPS:** Encryption of connections between the PROXY Pro 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 *PROXY Pro Web Console Installation Guide*)

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 Remote Desktop or Master 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*)
- **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 *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. Requires XenApp Enterprise or Platinum Edition. (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 tool bar 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).
- **Macintosh, Linux support:** PROXY Pro 7.0.0 provides support (remote access, remote control) for Macintosh and Linux computers running VNC server software (standard on Macintosh).
- **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.

Enhancements and Fixes

New Enhancements and Fixes in 9.0.1 Hotfix #11

Following is a list of improvements in PROXY Pro 9.0.1 Hotfix #11:

- **Updated SSL/TLS support:** The OpenSSL libraries used by the client code and Gateway Server have been updated to the newer v1.1.1 series. This release includes OpenSSL v1.1.1c. This upgrade is completely backward compatible with all earlier versions of PROXY that support TLSv1.2. Several new SSL/TLS capabilities are available in this release, including TLSv1.3 support and support for Elliptic Curve (EC) certificates as well as RSA certificates.
- **Gateway Server reliability:** Several reliability issues in the Gateway Server, primarily around unexpected connection problems and behaviors and Hosts that report status more often than expected, have been fixed. These issues are not commonly seen in LAN environments but can occur over the internet.
- **Installer works in TLSv1.2-only environment:** if the Windows operating system is “locked down” to TLSv1.2 only, earlier versions of the PROXY installers reported errors during installation or upgrade and could not proceed. This release resolves these problems, although there is one non-fatal error reported when upgrading from an earlier version to this version; this error can be ignored, and future upgrades will not report any problems in a TLSv1.2-only environment.

New Enhancements and Fixes in 9.0.1 Hotfix #10

Following is a list of improvements in PROXY Pro 9.0.1 Hotfix #10:

- **Gateway Server SSL/WSS connection capacity:** The memory usage for SSL and WSS connections have been reduced, so that it more closely matches the usage of TCP and UDP connections. This allows the Gateway Server to handle more SSL and WSS connections and makes the connection capacity of the system independent of the protocol used. This issue primarily impacts environments where a large number of Hosts maintain reverse connections to the Gateway Server.
- **Master automatic window sizing:** The installed Master has logic to automatically resize the Connection Window based on Host screen size, and to optimize the window size when maximizing the window. Specific cases involving multiple monitor configurations, and Host screen sizes larger than the Master, have been improved to have more natural and expected behavior.
- **Host “Active Users” window on high DPI display:** The Host “Active Users” window now works correctly on high DPI displays (with display scale factor > 100%). Previously, the window could appear off-screen.
- **Host on Demand for Macintosh:** Web Console includes updated version of Host for Macintosh (build 3624) which has additional reliability fixes. Users of Host on Demand for Macintosh will be prompted to upgrade on next use.
- **Updated SSL/TLS support:** The latest OpenSSL libraries have been incorporated (OpenSSL v1.0.2r).

New Enhancements and Fixes in 9.0.1 Hotfix #9

Following is a list of improvements in PROXY Pro 9.0.1 Hotfix #9:

- **Windows Server 2019 support:** All product components are now fully supported on Windows Server 2019, and places where the OS is detected and reported (for informational purposes) now report “Windows Sever 2019” when running on that operating system.
- **WS and WSS protocol support improved:** The network transport support for WebSocket (WS) and Secure WebSocket (WSS) has improvements to ensure clean and efficient closing of connections. Previously, a several second delay could occur, making the Master Connection Window take longer than expected to close.
- **Host notifications on high DPI display:** The Host popup notifications feature now works correctly on high DPI displays (with display scale factor > 100%). Previously, the notification window appeared off-screen and was not visible.
- **Host on Demand for Macintosh:** Web Console includes updated version of Host for Macintosh (build 3620) which has reliability fixes. Users of Host on Demand for Macintosh will be prompted to upgrade on next use.
- **Updated SSL/TLS support:** The latest OpenSSL libraries have been incorporated (OpenSSL v1.0.2q).

New Enhancements and Fixes in 9.0.1 Hotfix #8

Following is a list of improvements in PROXY Pro 9.0.1 Hotfix #8:

- **Gateway Server reliability:** Gateway Server has a number of important fixes resolving issues, both newly discovered, and introduced in the improved Host status processing functionality in Hotfix #6 and Hotfix #7. All customers running Gateway Server v9.0 are encouraged to upgrade to v9.0.1 Hotfix #8 for the highest reliability.
- **Click-Once Deployment support in Chrome:** Web Console now recognizes and supports additional extensions for Chrome that provide Click-Once Deployment support. See <https://products.proxynetworks.com/links/clickonce4chrome/> for the latest information and links to the supported extensions.
- **Host future compatibility:** The Host has a compatibility update to work with a future PROXY Pro Server feature that allows Web Console and Gateway Server to share a single port for SSL/WSS connections. (This feature is known as “HTTPSYS support”, and is planned for PROXY v10.1 release.)
- **Updated SSL/TLS support:** The latest OpenSSL libraries have been incorporated (OpenSSL v1.0.2p).

New Enhancements and Fixes in 9.0.1 Hotfix #7

Following is a list of improvements in PROXY Pro 9.0.1 Hotfix #7:

- **Gateway Server reliability:** Gateway Server has a number of important fixes resolving issues in the improved Host status processing functionality introduced in Hotfix #6. These fixes are especially relevant to polling for Hosts via TCP, and Transient Host (Host for RDS, Host on Demand) support.

- **Gateway Server:** Server did not properly process the “X-Forwarded-For” HTTP header in the WSS protocol.
- **Updated SSL/TLS support:** The latest OpenSSL libraries have been incorporated (OpenSSL v1.0.2o).
- **Cursor Calibration:** Host pointer (cursor) calibration is now correct in all circumstances. Previously, Host and Master did not agree on position when multiple monitors with different scale factors/DPI resolution were used.
- **Host Manage Visual Effects:** The MVE feature has been updated to improve reliability, especially in restoring wallpaper settings, and now explicitly manages the ClearType setting.
- **Host PhSetup Utility:** Using PhSetup to add security to a Host now correctly handles duplicate items, so this can be done in a login script or other repetitive process safely.
- **Master Cursors:** Master now detects blank/invisible cursors on Host correctly, and shows local cursor if there is no pointer shape from Host.
- **Master Cycling Monitor:** Cycling Monitor is now always view-only.
- **End User License Agreement:** The end user license agreement for all product components have been updated, and all components are now covered under one license agreement.

New Enhancements and Fixes in 9.0.1 Hotfix #6

Following is a list of improvements in PROXY Pro 9.0.1 Hotfix #6:

- **Gateway handles multiple Master versions:** Gateway Server has been updated to more intelligently handle allowing different Master versions to connect through to one Host for collaboration. Previously, mismatched versions could easily lead to an error message; now, all Master v6 and later can be mixed-and-matched.
- **Gateway Server SSL improvement:** Gateway Server SSL support now restricts connections to TLS v1.2 only for enhanced security and compliance with industry practices. This limits backwards compatibility with earlier versions of PROXY software (when connecting to Gateway via SSL or WSS only – TCP and UDP are not affected). The following PROXY versions do not support TLS v1.2 for connecting to the Gateway via SSL or WSS:
 - PROXY v5.20 through v7.0, any maintenance release or hotfix
 - PROXY v8.0, any version prior to v8.0.2 hotfix#3
 - PROXY v8.10, any version prior to v8.10.1
- **Gateway Server reliability:** Recording Playback reliability fix: the Gateway Server no longer falsely detects a recording playback paused for a long time (> 10 minutes) as a possible deadlock. Because of this fix, upgrading to this version (or later) is highly recommended in environments that use recording and playback.
- **Gateway Server status reporting improvements:** Gateway Server now handles multiple Host status reports simultaneously, improving throughput.
- **Updated SSL/TLS support:** The latest OpenSSL libraries have been incorporated (OpenSSL v1.0.2l).
- **Various reliability fixes:** a variety of reliability improvements have been made. Specifically, there are fixes to the Master “Gateway Hosts” tab, Clipboard Transfer, Host Remote Management access, Host “Active Users” window, and the Gateway Server.

New Enhancements and Fixes in 9.0.1 Hotfix #5

Following is a list of defects in PROXY Pro 9.0.1 Hotfix #5:

- **Host Safe Mode support:** Host Service now correctly starts in Windows Safe Mode on Windows 10 and Server 2016, and Host support logic for the Restart in Safe Mode utility has improved performance, which improves startup time on some systems.
- **Deployment Tool:** the Deployment Tool now correctly supports machine names longer than 15 characters (the NetBIOS limit) in an Active Directory organization. The full correct DNS name is used to access these machines.
- **Remote Printing:** an installer error was reported installing the Remote Printing component on Windows 10 Creators Edition update. This error occurred in Host and Master installers if installing the Remote Printing component (which is optional, but enabled by default), or if the standalone Remote Printing installer was used. Note that upgrading to Creators Edition after Remote Printing is installed does not cause a problem; the error only occurred on a new install.
- **Gateway Certificate Manager:** the GWSCertMgr now creates certificates that have improved compliance with industry standards. Specifically, the Subject Alternative Name (SAN) entry is populated with the Common Name of the certificate.
- **Host Control Panel “Test Gateway”:** the Host Control Panel, Gateways tab, “test gateway connection” functionality has been fixed to avoid an erroneous error report when configuring a Host to report to a future version of Gateway Server.
- **Updated SSL/TLS support:** The latest OpenSSL libraries have been incorporated (OpenSSL v1.0.2k).

New Enhancements and Fixes in 9.0.1 Hotfix #4

Following is a list of defects in PROXY Pro 9.0.1 Hotfix #4:

- **Improve Host responsiveness:** The User Mode Screen Capture (UMSC) profiles have been updated to provide an improved experience, especially on Windows 10. Upgrade the Host software to this release for the best experience.

New Enhancements and Fixes in 9.0.1 Hotfix #3

Following is a list of defects in PROXY Pro 9.0.1 Hotfix #3:

- **Updated SSL/TLS support:** The latest OpenSSL libraries have been incorporated - (v1.0.2j).
- **Host and Master for Macintosh compatible with macOS Sierra (10.12):** Changes in the latest version of the Macintosh OS, macOS Sierra (10.12) released in Fall 2016, introduced compatibility problems with the PROXY Host on Demand for Macintosh and PROXY Master on Demand for Macintosh. The versions of Host and Master for Macintosh included in v9.0.1 hotfix#3 fix these compatibility problems and are fully supported on Macintosh OS X v10.8 (“Mountain Lion”) and later.

- **Click Once Connection Window:** Error message about font, which occurs under Windows 10, no longer appears.
- **Master:** File > Play Recording via URL functionality is now reliable.
- **Gateway Certificate Manager:** Now checks for “write encryption” access right to attempt change to Gateway encryption settings (including selected SSL certificate).
- **Deployment Tool:** IP address lookup of Active Directory computers is now faster, and refresh can be run on Organizational Units as well as the top-level domain.
- **Host on Demand:** No longer prompts to elevate when run inside of a Remote Desktop session.
- **System Information Report:** Now includes more information, including SQL Server instance information.

New Enhancements and Fixes in 9.0.1 Hotfix #2

Following is a list of defects in PROXY Pro 9.0.1 Hotfix #2:

- **Clipboard Transfer:** The Clipboard Transfer feature could stop working on a Gateway-based connection if the Master loses or releases input control.
- **Gateway Server:** A Gateway Server memory leak in Host Grouping rules processing was fixed.
- **Host Installer:** Host deployment without Remote Printing was introduced in v9.0.1, but this deployment also omitted the Remote Management feature. This is fixed in this release.

New Enhancements and Fixes in 9.0.1 Hotfix #1

Following is a list of enhancements in PROXY Pro 9.0.1 Hotfix #1:

- **Deployment Tool:** Several problems in the Deployment Tool were identified and fixed. Deploying Host settings via “Update Host Settings” no longer reports a spurious error if the configuration includes Remote Printing deployment instructions. Master configuration, Gateways setting “Remove all gateways from settings” checkbox clarified in the user interface. “Copy to Clipboard” option now generates list of installation and product-specific settings with correct delimiter. “Update Master Settings” no longer deletes administrator-defined Gateway configurations when product configuration does not define any and the “remove” checkbox is not checked.
- **Master for Macintosh:** Clipboard Transfer operations were broken against Gateway Server v9.0. About box now shows correct version and copyright information.

- **Web Console:** Forms authentication no longer requires the account authority to be specified. Additional improvements in error handling, detection, and security validation.

New Enhancements and Fixes in 9.0.1

Following is a list of enhancements in PROXY Pro 9.0.1:

- **Forms Authentication:** In addition to Windows Authentication, the Web Console now supports Forms authentication. Basic authentication is no longer supported. This makes logout and “Login As” more robust and reliable. It also enables Apple products to work more reliably with the Web Console. From an end-user’s perspective, Forms and Basic authentication methods are functionally equivalent.
- **Master auto-connect for Remote Printing is now optional:** The installed Master now has an option to not auto-connect the Remote Printing service. This appears in the Options > Master Settings dialog, in a new tab “Remote Printing”. This feature is added primarily to ensure that administrators/supervisors can continue to connect to a user/agent in a “stealth” manner, without them being alerted.
- **Selectively install Remote Printing:** The Host and Master installers now make the Remote Printing feature optional. The installer dialog provides the option, with the default to install all components. The MSIEXEC command line also allows for this option.
- **Analytics default period now covers past 24 hours:** Instead of displaying a 24-hour period covering 12:00 AM of the current day to 12:00 AM of the following day, “Analytics” reports will now default to showing the past 24-hours based on your local time zone.
- **Improved and more intuitive searching in Web Console:** The global Find Host search box now behaves more like the extremely well received installed Master “filter” functionality. In addition, search boxes throughout the WC no longer require wildcard characters (“A*/G*/N”) to search for a partial name.
- **Eliminated “Toast” notification connect/disconnect messages for the Remote Print Manager:** In the v9.0.0 release, the new Remote Printing feature has a popup notification when the Remote Printing service is connected to, disconnected from, and when a print job is processed. In this release, the connect and disconnect popups have been removed because they were distracting. A popup notification still occurs when a print job is processed, as this is valuable information to the user.
- **Host installation default settings improvement:** In an effort to improve the user experience just out of the box, a clean installation of the PROXY Pro Host will now have a default Station Name configured with the macro %NAME% instead of the machine name at time of installation. This change will allow the Host’s Station Name to automatically be updated if the machine name changes. Also, the IPX protocol will now be disabled by default.

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

Following is a list of key defects fixed in PROXY Pro 9.0.1:

- The Gateway Certificate Manager now handles wildcard SSL certificates.
- A grey screen no longer appears when trying to control a device with text scale >100%. (UMSC only)
- Improved error handling and messaging around invalid data and recording paths specified in the Gateway.
- Certain parameters set on the Gateway could not be corrected if entered wrong. Can now correct invalid parameters.
- Corrections to HOD diagnostics logging have been made.
- Host no longer reports EventID=0 on connection with bad license.
- Host and Master installer no longer fail due to inability to install Remote Printing support when system Spooler service is disabled.
- Deployment Tool no longer loses state after upgrade.

- Remote Printing error message enhanced if Spooler process is not running.
- Web Console now sorts Group names alphabetically in drop-down lists.

New Enhancements and Fixes in 9.0.0 (Hotfix #1)

Following is a list of enhancements in PROXY Pro 9.0.0 (hotfix #1):

- **Remote Printing Connection Notification:** In the v9.0.0 release, the new Remote Printing feature has a popup notification when the Remote Printing service is connected to, disconnected from, and when a print job is processed. In hotfix #1, the connect and disconnect popups have been removed because they were distracting. A popup notification still occurs when a print job is processed.
- **Deployment Tool state:** In the v9.0.0 initial release, the Deployment Tool did not load the state created with earlier versions, losing this information. This is fixed in hotfix #1, and the Deployment Tool now correctly loads any previous state.

New Enhancements and Fixes in 9.0.0

Following is a list of enhancements in PROXY Pro 9.0.0:

- **Automatic reconnect to Hosts:** Upon an unexpected dropped connection to a Host, both the installed and Windows ClickOnce Master will automatically attempt to reconnect to the Host.
- **Improved Host on Demand for Macintosh:** Host for Macintosh has many improvements, including improved Permission to Connect user experience and support for recording the Host.
- **Significantly smaller Host on Demand download package:** The download package for the Windows Host on Demand ClickOnce application has been reduced to almost a 3rd of its former size, allowing for much faster downloads.
- **Updated iOS Master for iOS application:** The Master for iOS application has been updated. It is now called, PROXY Pro Master and is compatible with iOS 9. Both 32-bit and 64-bit binaries are now built. Included are various bug-fixes and enhancements to improve stability.

Note: Version 9.0.1106 (released October 26, 2015), or later, is required in order to connect to v9.0 of the Web Console and Gateway. Earlier versions of this application will fail trying to make Host or Playback connections.

- **Expanded Host-side “toast” notifications:** The “toast”, or popup, notifications seen on the Host will now contain more information including timestamps. The “pin” behavior has also been improved to be more intuitive.

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

Following is a list of defect fixes in PROXY Pro 9.0.0:

- Replaced OpenSSL library with version 1.0.2d, which is a security release of OpenSSL. Customers with internet-facing Gateway Servers listening for SSL connections are encouraged to upgrade to this release.
- File Transfer screen now shows expected mapped drive letters regardless of UAC being on or off.
- Master optimized to use local cursor to show Host cursor, which has performance implications when remoting the screen the Master is running on.
- Host trial expiration notification made less intrusive.
- Web Console now monitors for, and reports asynchronously, the final status of a recording after it has been successfully started.
- Web Console robustness improvements around:
 - Saving persistent Host settings
 - Searching for groups containing special characters
 - Starting recordings when there is low disk space
 - Showing Recording Playback activity in "Activity" tab
 - Indicating when system Hosts have an active remote connection
 - Better handling of limited administrator access
- iOS Master robustness improvements around:
 - Better handling of view-only Hosts
 - Handling of specific errors consistent with Windows
 - Display of recording playback meta information
 - Correct cursor display in all situations
- Macintosh Host robustness improvements around:
 - Error state handling
 - Status reporting reliability and feedback
 - Providing connected status information to Web Console
 - Clearing error state after accepting an SSL certificate

- The Gateway's SSL support now delivers the entire certificate chain (up to the trusted root).
- German localization improvements in Gateway Server.

New Enhancements and Fixes in 8.10.2 (Hotfix #1)

Following is a list of major enhancements in PROXY Pro 8.10.2:

- **Master “Search Hosts” feature:** The installed Master now includes a “filter” on both the Peer-to-Peer Hosts tab and the Gateway Hosts tab to filter the results to show only Hosts that match a search string.
- **ClickOnce Connection Window persistent settings:** The ClickOnce Connection Window now allows the fit-to-mode, request manage visual effects, suppress Host console input, and auto-share clipboard settings to be saved for use as the defaults for future Connection Window sessions. The current state of these settings is saved by picking the “Remember current settings for future use...” menu item from the application system menu.

Following is a list of major defect fixes in PROXY Pro 8.10.2 (Hotfix #1):

- Replaced OpenSSL library with version 1.0.1o, which is a security release of OpenSSL. Customers with internet-facing Gateway Servers listening for SSL connections are encouraged to upgrade to this release.
- ClickOnce Connection Window and Recording Player incorrectly prompted for credentials when Web Console Settings, Application Access, was set to “Web Console User”, and the Windows login matched the identity used with the Web Console. That case enables single sign-on, and no credentials prompt should appear.
- Gateway Server SSL support improved to deliver entire SSL certificate chain (up to root), and client processing improved to use intermediate certificates provided this way. Previously, all intermediate certificates as well as the root certificate had to be in the Windows certificate store for a certificate to validate correctly. With this improvement, only the root certificate must be in the “Trusted Root Certificates” store.
- Issue with sorting in Web Console that affected some systems is fixed. When the issue occurred, the correct results were displayed, but they were not sorted on the page correctly.

New Enhancements and Fixes in 8.10.2

Following is a list of major enhancements in PROXY Pro 8.10.2:

- **Updated Web Console graphics:** Better distinction between the various types of Hosts (e.g. Installed, On demand session, On demand pinned, Terminal Services, VDI)
- **Automatic Elevation/Pinning of HOD:** When a Host on Demand is launched, it will automatically start as elevated/pinned if the console user has administrative rights.
- **Expanded search functionality for recordings in Web Console:** The Web Console “Recordings” page will allow the user to search for recordings based on more criteria.
- **WC improved load time and performance with large numbers of Hosts:** The time it takes for the Web Console landing page and

dashboard to show up has been reduced. This is particularly noticeable in environments with thousands of Hosts reporting in.

- **Copy Text and Graphics to Clipboard:** The installed Master and ClickOnce Connection Window now support copying both text-format data and a graphic image when the Host screen is in “plain text” display mode. Note that this primarily occurs with certain error messages, and for the Gateway Server “System” Hosts. This change merges the former “Copy Text to Clipboard” and “Copy Graphics to Clipboard” functions into a single “Copy Host Screen to Clipboard” option.
- **Gateway Server Host Grouping Rule for Active Directory:** The Gateway Server now supports two styles of Active Directory-based Host grouping rules.
- **Various SDK improvements:** Updates to the SDK for better compatibility with newer versions of Visual Studio have been made. Additionally, the SDK support for x64 is now included in the main packaging.
- **Alignment of the installed Master and ClickOnce connection windows:** Changes have been implemented upon both products in order to make them as close as possible despite being different underlying technologies.

Following is a list of major defect fixes in PROXY Pro 8.10.2:

- Improved compatibility for remote controlling devices without a mouse: (e.g. Kiosks and touch-screen tablets)
- Replaced OpenSSL library with version 1.0.11, which is a security release of OpenSSL. Customers with internet-facing Gateway Servers listening for SSL connections are encouraged to upgrade to this release.
- Improved handling of X-Forwarded-For header processing
- Host station name was not being updated at the Gateway Server if Host maintained a reverse connection with the Gateway.
- Gateway Server now ensures the Gateway Companion Service (required by the Web Console) is running when it starts.
- Fixed issues that impacted the PROXY Pro Remote Desktop application for iOS. Note well that the iOS app version 8.10.1051 or later is required for use with PROXY Pro v8.10.2.
- Various improvements to the ClickOnce connection window application launched from the Web Console, including: Host station name is shown instead of Host ID in dialog prompts; error messages and reporting is improved.

New Enhancements and Fixes in 8.10.1 (Hotfix #3)

Following is a list of enhancements in PROXY Pro 8.10.1 hotfix #3:

- An error in the TCP/WS transport resulted in a resource leak if an HTTP request was made to a Gateway Server or Host on the port it was listening for TCP connections. This eventually resulted in 0xC004C055 errors. All customers are encouraged to upgrade their Gateway Servers running v8.10.0 or later to this release, and are encourage to plan to upgrade Hosts as well.
- The Gateway Server could end up with a completely blank workstation record instead of a properly deleted record under very specific circumstances; this no longer occurs.

- Web Console has a performance fix that resolves issues when users have access to large numbers (multiple thousands) of Hosts. Customers with over 5000 managed Hosts are encouraged to upgrade the Web Console to this release.
- Web Console now supports an alternate addin to provide ClickOnce deployment support for the Google Chrome browser. Note that Chrome support for addins is changing this year, and the new addin may not provide a long-term solution. A future maintenance release will provide support for the new Chrome browser.

New Enhancements and Fixes in 8.10.1 (Hotfix #2)

Following is a list of major defect fixes in PROXY Pro 8.10.1 (Hotfix #2):

- Gateway Server and Host have compatibility fixes for the PROXY Pro Remote Desktop application for iOS. Customers using the iOS application in their environment are encouraged to upgrade to this release to avoid any issues.
- New Host station name macros are introduced. These macros get values from Active Directory about the logged-in console user. The properties are:
 - %USERUPN% is the user principal name format of the console user, or blank if the user is not a domain account
 - %USERUPN+% is the same as above, but provides the “authority\username” account name for local accounts.
 - %USERDISPLAY% is the user display name
 - %USERDISPLAY+% is the user account display name, or the account name in “authority\username” format if the account display name is not set
 - %USEREMAIL% is the user account email address, or blank if the user is not a domain account
 - %USEREMAIL+% is the same as above, but provides the “authority\username” account name if the email address is blank.
- Web Console and Gateway Server now respect the X-Forwarded-For header on HTTPS (for Web Console) and WS/WSS (for Gateway Server) connections. In conjunction with the “trusted device list” setting in the Gateway Server, this allows the software to work well with reverse proxy servers like Microsoft Application Request Routing (ARR).
- Master and Connection Window send entered keyboard input to Host promptly; previously, the keystrokes could be cached briefly, introducing delay in typing feedback.
- Host did not send status reports to Gateways with which it had an active status reverse connection in v8.10.0 or later. This primarily affected the updating of the logged-in console user, or Host station name changes, and is fixed in this release.
- Replaced OpenSSL library with version 1.0.1i, which is a security release of OpenSSL. Customers with internet-facing Gateway Servers listening for SSL connections are encouraged to upgrade to this release.
- Web Console now marks cookies as “secure” and “httpOnly” (when possible) for increased security. All Web Console installations are encouraged to upgrade to this release.

New Enhancements and Fixes in 8.10.1 (Hotfix #1)

Following is a list of major defect fixes in PROXY Pro 8.10.1 (Hotfix #1):

- Replaced OpenSSL library with version 1.0.1h, which includes fixes for newly found security vulnerabilities post the “Heartbleed” fix. Anyone with Gateway Server version 7.0.x through 8.10.1 should upgrade to PROXY Pro Gateway 8.10.1 (Hotfix #1), especially if Gateway Server is configured to listen for connections directly from the Internet.

New Enhancements and Fixes in 8.10.1

Following is a list of major enhancements in PROXY Pro 8.10.1:

- Explicit web proxy support: If a customer uses a web proxy server to manage internet traffic coming into or going out of its network, PROXY Pro 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.

New Enhancements and Fixes in 8.10.0 (Hotfix #1)

Following is a list of major defect fixes in PROXY Pro 8.10.0 (Hotfix #1):

- Replaced OpenSSL library with version 1.0.1g, which includes fix for the "Heartbleed" vulnerability. Anyone with Gateway Server version 7.0.x through 8.10.0 should upgrade to PROXY Pro Gateway 8.10.1 (Hotfix #1), especially if Gateway Server is configured to listen for connections directly from the Internet.

New Enhancements and Fixes in 8.10.0

Following is a list of major enhancements in PROXY Pro 8.10.0:

- 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 PROXY Pro 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 PROXY Pro 8.10.0:

- Duplicate GUID protection. Duplicate Host GUIDs can occur when the HostPrep utility is not run on a Windows OS image containing PROXY Pro 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.

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

Legal Notices

Copyright © 2006-2019 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. Apple, AirPlay, Finder, iPad, iPhone, iPod, iPod touch, iTunes, Keychain, Mac, Macintosh, Mac OS, OS X, Retina, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc. IOS is a trademark or registered trademark of Cisco in the U.S. and other countries. Novell and NetWare are registered trademarks of Novell, Inc. All other trademarks are the property of their respective owners.

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