



PROXY Pro Version 10.3

What's New

Release 10.3 Hotfix #3
October 2020

Proxy Networks, Inc.
1234 Chestnut Street Suite 102
Newton, MA 02464
617-453-2700
<https://www.proxynetworks.com>

© Copyright 2006-2020 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 (eay@cryptsoft.com), and compression software from the ZLIB project (<http://www.zlib.net/>).

Overview

Version 10.0 marked the beginning of the 3rd generation of PROXY Pro technology. The new architecture helps to lay the foundation for many enhancements down the road including things like scale up and scale out as well as multi-factor authentication, native x64 versions etc.

Version 10.3 builds on the v10.0 architecture and v10.1 and v10.2 releases to deliver improved capabilities and added value.

Major New Features in v10.3

PROXY Pro Host for Mobile (Android and Apple iOS Devices)

Version 10.3 introduces support for screen viewing of Android devices (v8 “Oreo” or later) and Apple iOS devices (iOS v11.2 or later). These phones and tablets will run a native application that will provide an On-Demand Host (HOD) that can be configured to report to a standard v10.3 PROXY Pro Server.

New and Easier Identification of All Hosts – Installed and HOD

A new mechanism to help identify a specific Host, installed or on Demand (HOD), in the Web Console or installed Master has been implemented. The Host instance will be assigned a unique 6-digit personal identification number (PIN) that the end user can provide to the Master user for quick identification. This will be the case for all Host implementations, both installed and On Demand and for all platforms (Windows, Macintosh and the new Android and iOS sessions). This is especially helpful for non-enterprise managed machines where station names may not contain information that is meaningful to the Master user.

Quick Connect ability directly from the Web Console Landing Page

A Host can now be connected to by simply entering the 6-digit PIN, as discussed in the item above, directly into the landing page of the Web Console. The security model remains intact as credentials will still be required, but upon entering credentials, the Master user will be brought directly to the associated desktop.

Gateway Server Component as a Native 64-bit (x64) Application

Improved capacity for the PROXY Pro Gateway server component for Hosts reporting from the internet. Along with Windows 64-bit Operating Systems, increased addressable memory relaxes capacity restrictions, allowing up to 2500 reverse connections from Hosts – (a 25% increase).

Macintosh File and Folder Transfer via Clipboard

The Host and Master for Macintosh now support file transfer using the clipboard. This includes single file, group of files, and folders with recursive transfer. This functionality works both from Macintosh to Macintosh as well as between Macintosh and Windows operating systems.

Remote Management Service Improvements

Performance and reliability improvements have been made in the Remote Management feature of the connection window with special attention to, and a drastic improvement in, the speed of the “Software Manager -> Installed Products” node.

In-Browser Connection Window Allows Easy Launch of the Full Client

A new button on the In-Browser (HTML5) connection window allows an easy switch to the full client, ClickOnce or installed Master, when available.

Improved and Streamlined Experience for Launching Master and Host on Mac and iOS

Both Mac machines and iOS devices now make the process of launching Master and Host simpler. Previously, PROXY prompted to ensure required helper apps were installed before trying to launch them. In v10.3, a

newly designed web page automatically launches the apps if they're already installed and provides instructions on how to get them (by download or AppStore) they're not yet installed.

Ability to Hide Unused Window Tabs in Installed Master

We have reintroduced the ability to configure the installed Master UI to hide the window tabs that are not in use by that installation.

Integration of the latest OpenSSL Library Series (v1.1.1)

To keep up with the latest security trends, the OpenSSL Library integrated with PROXY Pro is now the v1.1.1 series as of this release (v10.3)

Dynamic Station Name Resolution

Hosts that are configured to use Dynamic Station Name Macros will now display the evaluated name in their Host Control Panel or settings, depending upon the Host. This is helpful in order to know what the Master user should expect to see for the reported Host Station Name.

Easy Scroll to Navigate Viewing Larger Desktops

Easily scroll across desktops larger than the Master connection window by simply holding either of the SHIFT keys and moving the pointer to any edge of the screen. This is available in both the Installed and ClickOnce Master for Windows as well as the Master for Mac.

Send Clipboard as Keystrokes to Login Screen

Master for Windows, ClickOnce Master, and Master for Mac now support “Send Clipboard as Keystrokes” function. This takes plain text on the clipboard and types the corresponding characters, which is useful for entering credentials in places where the clipboard functionality is not available, e.g. the Windows logon screen.

Responsive Web Console Landing Page

The landing page of the Web Console will now display cleanly on various screen sizes for phone, desktop and iPad.

PROXY Air will now Support Mobile Host Devices

The new Hosts for iOS and Android, as discussed above, will be supported in our PROXY Air service.

Major New Features in v10.2

Host Console Watermark and Border Options to Show Connection

This version of the Host now supports additional options for alerting a console user when a remote control session starts or is active. These settings are configured in the Host Control Panel and include the ability to show a border around the screen being captured (all monitors) and/or a translucent watermark that displays the connected user, also on all monitors. Note that this is in addition to the previous alert features including Popup Notifications, Beep, etc.

Ability to Launch the Installed Master from the Web Console

The installed Master connection window can now be launched when clicking on a Host name in the Web Console. This is in addition to the “Connect in Browser” and ClickOnce options and is available on the Windows platform. This capability is available for both live remote control sessions as well as playback of recorded sessions.

New Utility to Allow Host Settings Updates Through a Gateway

The new PROXY Pro Host Updater Utility is a long-running desktop application that connects to a Gateway and allows an administrator to automatically apply a set of Host settings updates in JSON format to all Hosts that are in communication with that Gateway, regardless of whether they are on the LAN or in the same

domain. (This is in contrast to the Deployment Tool, which only works peer-to-peer with Hosts that are on the LAN). This new utility is installed alongside the Deployment Tool via the DeploymentTool.msi installation package.

New Gateway Host Grouping Rule (by Active Directory Computer Membership in Security Groups)

PROXY v10 supports automatically organizing Hosts in the Gateway Server by Active Directory "organizational unit" hierarchy. Version 10.2 extends this functionality to include a new type of Host Grouping Rule "AD Security Membership". This new rule is similar to the existing "Active Directory" rule (which is now renamed to "AD Organizational Unit"). However, instead of placing the Host in a group named for the one OU which contains the Host computer, the Host is placed in one group for each of the possibly many AD security Groups of which the Host computer is a member.

Ability to Have HOD Report to Multiple Gateway Servers

To meet certain availability and redundancy requirements, PROXY will allow a downloaded HOD to report to multiple PROXY Pro Server installations. The first set will always be the Server installation the HOD was downloaded from while alternate/additional Servers can be configured by an administrator.

Host Settings JSON Representation Improvements

The PhSetup command has supported exporting and importing Host Settings from and to a Host for several releases. This release introduces new functionality to make this easier. First, the Deployment Tool now lets you Export a Host Configuration to JSON, either by saving to a file or copying to the Clipboard. Second, PhAdmin now has a hidden button that lets you import a JSON file, which can be made visible either by holding down the Shift key when you start it up, or by using a new "/all" option on the command line. This is a good option meant for administrators of the Hosts.

New Package Names for Easier Identification

The downloadable packages have now been renamed to align with current terminology and naming. The base name for the downloads is now "PROXYPro" and the editions are now named "RAS-Edition" (formerly Private Cloud Edition, or PCE) and "P2P-Edition" (formerly Workstation Edition).

Major New Features in v10.1

Improved High DPI and Scaling Support

Host v10.1 will automatically "scale down" a high DPI screen to reduce the amount of data sent to the Master, and to let the Master have a reasonable "Fit 1-to-1" view. Master has performance improvements in rendering the Host screen, especially in the case of "Fit-to-Window".

Host on Demand for Windows as EXE Deployment

The Host on Demand can now be deployed as an executable download in all browsers, and no longer requires ClickOnce Deployment support. In browsers that support ClickOnce deployment, the Host on Demand is still deployed that way for an improved user experience.

Clipboard Transfer Improvements

Master v10.1 on Windows connected to Host v10.1 on Windows has enhanced Clipboard Transfer support, including the ability to transfer files and folders (e.g. via Windows Explorer), and to drag-and-drop files from the Master desktop onto the Master Connection Window to initiate a clipboard transfer operation to the remote Host.

Recording Retention Guard

Recordings can be created on demand or by policy (Auto-Recording feature), and may need to be preserved indefinitely by some customers in order to meet certain compliance requirements. The Gateway can now be configured to prevent the deletion of recording either by automatic controls, such as age settings, or by manual attempts. This includes archiving recordings of Hosts that are deleted from the Gateway to a new item, "Recordings of Deleted Hosts" in the "System" Gateway group.

Macintosh and iOS Master Enhancements

The Master for Macintosh and Master for iOS now have full PROXY v10 authentication support, and can handle all authentication scenarios both on initial connection and when connecting to items from the “Recent Hosts” or “Recent Recordings” lists. (Previously, configurations that required a web-based login, like Azure Active Directory, did not work from the “Recent” lists.)

Macintosh software is supported on OS X 10.9 (Mavericks) and later, including the recently released 10.14 (Mojave). iOS software is supported on iOS v9 and later, including the recently released iOS v12.

Web Console Improvements

Improvements across many pages of the Web Console. Session state now remembers group selection when navigating back to the Hosts page or upon Refresh. Easier access to key information across pages, with more reliable and flexible sorting of data.

Gateway Server “HTTPSYS” Transport Support

When Web Console and Gateway Server are installed on the same machine, Gateway Server can now register with the Windows operating system “HTTP.SYS” driver and share the listening ports with Web Console. This allows WSS-protocol connections (only) to be made to the Gateway Server on the port normally used to access Web Console (e.g. port 443), and in many configurations facilitates only having to open one port to the internet to allow access to all of Identity Manager, Web Console, and Gateway Server.

Reverse Web Proxy Support

PROXY Pro Server now supports being placed behind a “reverse web proxy”. This is an appliance or other software product that terminates incoming HTTPS connections, and forwards them to the back-end service (PROXY Pro Server).

New Setting: Allow access to Find a Desktop from External Addresses

This new setting, which is “on” by default, can be turned “off” to disallow any attempt to connect as an authenticated client to the Identity Manager, Web Console, or Gateway Server. In this configuration, the system can be exposed to the internet and the only functionality available to external users is “Share my Desktop” (i.e., Host on Demand).

Major New Features in v10.0

Two-Factor Authentication

Until now, authentication had been limited to Windows Authentication. Version 10 allows us to break from that in order to use alternate identity providers and provide multi-factor authentication. The initial release will include support for talking directly to the Microsoft Azure Active Directory (AAD) tenant service.

Hierarchical Grouping

The Gateway now supports hierarchical groups. These groups will possess security inheritance, and Active Directory synchronization via Host Grouping rules (i.e. organizing Hosts workstations according to their location in AD).

Active Directory Synchronization

This feature allows for Hosts to be organized in the same way that they are organized in Active Directory. This is driven by enhancements to the Host Grouping rules feature and the addition of hierarchical groups.

Decoupling of components

The Gateway Server, Web Console, and supporting SQL Server instance can now be installed on different machines. This specifically includes running against a SQL instance managed separately (perhaps a SQL Server high-availability cluster)

Streamlined installation experience

Highly improved installation experience for Web Console and Gateway Server. This will facilitate the services running on multiple boxes, setting up of SQL Express if needed, and automatic handling of prerequisites.

HTML5 Remote Control and Recording Playback

As an alternative to the ClickOnce or installed connection windows, version 10 introduces the ability to use an HTML5 browser with no plugin. The Web Console will offer HTML5 as an option when ClickOnce is available, and use it by default when there is no native helper application available.

Migration to SQL database

All data is now kept and managed by Microsoft SQL Server. Use of the "Jet" database engine (MDB files) has been retired.

Tighter integration between Gateway Server and Web Console

The Gateway companion service will no longer be necessary as Web Console and Gateway Server now communicate directly with each other.

Refreshed UI

Both installed components and Web UI will have an updated look and feel

More functionality available in the Web Interface

This includes full administrative functionality, so that the MMC-based Gateway Administrator is no longer required to perform certain administrative tasks.

Remote PrxSysInfo generation

Ability to generate PROXY System Information reports (prxsinfo) remotely. An administrator can now remotely request their respective servers, Host and Gateway, to initiate PrxSysInfo reports, and the results of those reports will be transmitted to the client for viewing and storage.

Optimized Scrolling

Version 10 Masters connecting to version 10 Hosts have an optimization that greatly improves vertical scrolling.

Operating System Requirements

PROXY Pro v10.3 works on all the same Windows operating systems as v10.2 but is only officially supported on operating systems within Microsoft extended support. Specifically, Host, Master, and other client components are supported on all Windows operating systems currently in support by Microsoft:

- Windows 8.1, Windows 10
- Server 2012, Server 2012r2, Server 2016, Server 2019

Note that Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008r2 are no longer supported by Microsoft at the time of this release but were supported by PROXY v10.0. No changes have been made to PROXY v10.3 to prevent the software from working on these operating systems, but PROXY is not officially supported on them.

The PROXY Pro Server (Identity Manager, Web Console, and Gateway Server) require Windows Server 2012, Server 2012r2, Server 2016, or Server 2019.

PROXY Pro for Macintosh now requires Macintosh OS X v10.9 (Mavericks) or later. Earlier versions of OS X do not support TLS v1.2 and therefore cannot communicate with PROXY Pro v10.0 or later.

Compatibility

The PROXY Pro Server can manage a variety of Host software versions in your environment. Due to restrictions to ensure reliable, secure encryption is always used, not all previous Host software versions are compatible with version 10. The minimum supported Host version is v7.0.4, although the latest release/hotfix version of the major version you're running is recommended.

In addition, because SSL support has been restricted to TLSv1.2 or later only in version 10, the following Host versions are required in order to connect to the Gateway Server v10 with the SSL or WSS protocols:

- v8.0.3.2060 hotfix#4 or later (released February 2015)
- v8.10.1 original release or later (released May 2014)
- v9.0.0 original release or later (released June 2015)
- v10.0.0 original release or any later major or minor version

Furthermore, due to a bug in earlier versions of PROXY WSS protocol support, not all Host versions that support TLSv1.2 and WSS can be managed successfully when they report via WSS to the HTTPS port(s) introduced in v10.1. Incompatible Hosts will perform status reporting correctly, but cannot be connected to for services. The following Host versions are fully compatible with Gateway Server v10.1 HTTPS support:

- Host v10.1 original release or later (released November 2018)
- Host v10.0 hotfix#3 or later (released August 2018)
- Host v9.0.1 hotfix#8 or later (released August 2018)
- At the time of this writing, no Host v8.10.2 is compatible (through hotfix#6), and there are no plans to provide this support in the v8.10 series.

Enhancements and Fixes in v10.3 Hotfix #3

Major changes in this release:

- Several important reliability fixes are included in the Web Console and Gateway Server components. Although the issues rarely occur, and may not occur in all environments, it's recommended that all PROXY Pro Server installations be upgraded to this release to avoid these issues.
 - A Gateway Server crash due to an error in Host status processing was fixed. This could happen only in a small window if the connection failed after it was established but before the Gateway read the Host status.
 - A transport-level crash due to improper error handling was fixed. This could impact either Host or Gateway, and occurred if an inbound connection was established, and the initial protocol negotiation occurs, but then client fails to send expected data within a timeout period.
 - A memory leak in the Web Console, resulting in error code 0xC004C056, could occur if the HTML5 Remote Control feature was used and the Gateway Server internal access was using the TCP, WS, or SSL protocols (and not WSS).
- Gateway Server system host "Performance Monitor" now reports on Identity Manager and Web Console process statistics, if those processes are on the same machine as the Gateway Server.
- ServerConfigCheck utility now reports on Identity Manager discovery document problems with much more accurate and useful information; previously, most problems would be (possibly incorrectly) reported as HTTP 503 (service not available).
- Web Console Analytics > Services page showed station name plus machine name (if these are different) in this view, but only allowed search on station name. Elsewhere in the product, the station name (only) is shown. The machine name was removed from the Services view for consistency and to avoid confusion with searching.
- Web Console's Host context menu options "Connect via [Client] for View Only" was not properly handling the "view only" request and the helper application would take input control on connection.

This impacted “Connect via ClickOnce for View Only” and “Connect via Installed Master for View Only” on Windows, and “Connect via Helper for View Only” on Macintosh.

- Web Console > Gateway > Gateway Settings > Grouping Rules > IPv4 Grouping Rule was previously limited to a range of 4096 addresses per rule. This has been relaxed and ranges up to 16777215 are now permitted.
- Installed Master did not dismiss the automatic reconnect dialog if remote control was reconnected, but one of the other services could not be connected-to. This specifically happened with Gateway-based connections where the Master user did not have the right to access the Chat service.
- The HostPrep utility (used to prepare a Host installation on a system that is being “sysprep”ed for duplication or imaging) did not work correctly in any v10.x release, and the result was that Host settings could not be established in the base image and preserved across the Windows “sysprep” operation.
- Host for Transient VDI-type Hosts were not generating new or unique Host PIN values, so all VDI instances from the same image had the same Host PIN.
- An issue with remote controlling a Host machine that in turn runs the Hyper-V Manager Virtual Machine Connection (VMC) window to remote control a Hyper-V virtual machine has been fixed. The behavior is that shifted characters, e.g. symbols type by using SHIFT and a number key, were not reliably being injected into the virtual machine. PROXY Pro Host now works around this issue with the VMC application to ensure these characters are entered correctly. If you experience this issue, you must upgrade the PROXY Pro Host on the machine running VMC to get the fixed behavior.

Enhancements and Fixes in v10.3 Hotfix #2

Major changes in this release:

- Master for Macintosh now has full support for Hosts with multiple monitors, with features comparable to the Master for Windows. Specifically, the “Select Host Monitor” menu and the “Next Host Monitor” button are on the toolbar and in the menus. Master for Macintosh also now supports autoscroll of the Host view when in Fit 1-to-1 mode by holding the SHIFT key while moving or dragging the mouse.
- Remote Control clients now have “Next Host Monitor” button on toolbar. When remote controlling a Host with multiple monitors, in addition to the previous features to select single monitors to view, a new toolbar button “Next Host Monitor” is available to cycle through the monitors more conveniently. This is available in Master for Windows, Master for Macintosh, and in the HTML5 Remote Control page in Web Console. Additionally, the keyboard accelerator Ctrl+] activates the “Next Host Monitor” feature, and keyboard accelerator Ctrl+[toggles Fit-to-Window mode. These accelerators work in Master for Windows and Master for Macintosh.
- The Host for Android is now supported on ChromeOS Chromebooks that support running Android applications. This allows a Web Console user to view the screen of the Chromebook when it is shared.
- The Host handling of SSL certificate errors when configured to report to a Gateway Server has been updated. Previously, the option to accept an untrusted certificate was conditional on the specific error that was reported. Because the error could change, this was not a completely predictable configuration option. In this release, the option to accept a particular certificate ties that acceptance to the specific certificate, independent of what the error is. This makes this functionality more predictable, and has been implemented consistently on all PROXY Pro Host platforms – Windows, Macintosh, iOS, and Android.
- Identity Manager setting “Require Azure AD for interactive web-based logins”. This configuration option is designed to accommodate a specific configuration, where Windows Accounts are to be used by PROXY SDK clients (including custom applications written against the SDK, as well as the Master), but all web-based logins should require Azure AD and not provide the choice of entering a Windows account. This streamlines single sign-on using Azure AD for browser-based client activity, without disabling Windows Accounts for other usages.

- The Server Configuration Check utility (in the PROXY Pro Server installation) now performs additional checks and warns on configuration issues that were not previously detected. Specifically, the IIS Application Pools for Web Console and Identity Manager are started if they're not running, and a warning is issued if they cannot be started. The utility also checks that the Application Pools and Gateway Server are configured to run as the account specified at installation time.
- The PROXY System Information reporting tool now reports on some additional data to help diagnose problems. More information about the machine's relationship to its Windows domain, including whether that relationship seems to be working, is reported. The total size and free disk space of each drive is also reported, to help identify low disk space issues.
- The "text mode" screen used by the PROXY Pro Server "System" Hosts (Gateway At-a-Glance and Gateway Server Performance) were not drawn with the correct colors by the HTML5 Remote Control client or the Master for Macintosh. This is now fixed.

Enhancements and Fixes in v10.3 Hotfix #1

Major changes in this release:

- New feature: HTML5 Remote Control clipboard support now supports placing a selected file (uploaded from the client browser) onto the Host clipboard; this file can then be Pasted on the Host into the file system. This feature provides a basic file transfer capability (from Master to Host only) within the HTML5 Remote Control experience. This works with all Hosts that support file objects on the clipboard (both Windows and Macintosh), up to a file size of 28 megabytes.
- Web Console now correctly detects the "ClickOnce Deployment" ready state of all browsers on Windows to correctly choose when to use ClickOnce Deployment of the helper applications. Previously, some scenarios in Web Console, and some browser configurations, were not properly detected.
- A resource leak in Web Console in the HTML5 Remote Control component could cause the process to run out of address space and stop accepting new logins with error 0xC004C056; this has been fixed.
- A regression bug in installed Master on Windows prevented the Gateway Hosts tab, Hosts listview, from preserving user customizations (changes in column order, changes in column width, which column to sort by, etc.) when a new Gateway Server was connected to, or when the existing connection was refreshed.
- A transport-layer issue could cause TCP connections to take up to 30 seconds to close; this most commonly impacted the Master Connection Window closing a Peer-to-Peer connection to a Host via TCP.
- The Web Console "Host Settings" feature now reliably prompts for end-to-end credentials; previously, an incorrect error code may have prevented the prompt from appearing.
- Deployment Tool "Export Settings to JSON File" was not exporting the Installation Files list; this meant that exporting the settings and importing them for another user, or on another machine, did not restore this state. This is now fixed and these settings are exported (and later imported) correctly.
- Several Host station name macros (including USERUPN, USERDISPLAY, and USEREMAIL) depend on lookups from Active Directory. If the user logs in when a domain controller is inaccessible, these values cannot be retrieved, however, when a DC becomes available later (e.g. if user gets on a VPN to the corporate network), the Host did not update them. The Host now attempts to refresh this information when there is a network address list change (e.g. changing networks or joining/leaving a VPN).
- Host for Macintosh and Master for Macintosh are now "sleep aware" and respond promptly when the Macintosh sleeps or wakes up, restoring connections much quicker than previous releases.

Enhancements and Fixes in v10.3

In addition to the major new features in v10.3, several issues were resolved in this release:

- Server installation default protocol for external access to the Gateway Server is now set to WSS port 443; previously this was TCP port 2303, and that's not commonly exposed to the internet. This is an installation default change only; no settings are changed on upgrade.
- The Host back-off policy has been modified to distribute reconnection attempts after a Gateway Server restart better. This results in faster recovery of Host control connections to provide connectivity to all Hosts. Note that upgrading Hosts is required to gain this improvement.
- The product names PROXY Pro Master and PROXY Pro Host have been standardized and unified across all platforms; previously, some clients were referred to with different names.
- Web Console Group Security Editor had a regression error introduced in v10.2 HF#2 that is now fixed; the ability to change security to apply to "This group only" or "This group and subgroups" was impacted.
- Proxy System Information report (prxsinfo) has several improvements in information collected, including information about SSL certificates selected in IIS and available in the local machine store.
- The PROXY Server Products installer (aka Bundle installer) upgrades the ODBC Driver 17 from the originally redistributed version v17.1.0.1 to v17.5.2.1. A bug in the original package from Microsoft requires that the component be repaired after upgrade; this is handled automatically by the PROXY installer.
- If the Master requests the Host suppress the local keyboard and mouse, or manage visual effects, whether those things happen or not are controlled by whether the Host supports those features, and the Host settings. If the requested function is not done, the button or menu item in the Master should change to reflect that state. Previously, not all Master platforms handled this correctly; specifically, Master for Mac and Master for iOS now correctly show the proper state, and Host for Mac correctly reports that it cannot perform these functions.
- Host and Master for Macintosh are now notarized by Apple; this provides an assurance when installing in newer versions of macOS. Host for Macintosh now preflights screen capture and input control access, which guides the user to provide the necessary access in system Preferences.

Enhancements and Fixes in v10.2 Hotfix #3

Major changes in this release:

- The PROXY Identity Manager has been updated to be compatible with Google Chrome version 80, which changes the handling of some cookies. This update is **required** in order to ensure that PROXY integration with Azure Active Directory works correctly; it's **strongly recommended** in all cases. See the blog post <https://web.dev/samesite-cookies-explained/> for more information about this change in Chrome.
- Host and Master installers no longer default to installing the optional "Remote Printing Support" component. If Remote Printing support is desired, this optional component should be selected during an interactive installation of Host or Master or enabled via the MSIEXEC command line option "INSTALLLEVEL=100" (this works the same for both Host and Master installers). Note well this only

changes the default for new installations; upgrades will update the Remote Printing component if it was previously installed, or leave it uninstalled if it was not installed.

- Gateway Server issue that could cause the Web Console “Activity” views to be inaccurate is resolved. The issue only occurred if, while the Gateway Server is operating, the SQL Server database becomes unavailable, and then becomes available again. In this case, updates to the “active” objects (connections, host activity, recording activity, etc.) could have been lost, resulting in “stuck” activity items. Note that these were always cleaned up when Gateway Server restarts, so there’s no persistent errors, but the Activity views were not perfectly reliable when this issue occurred.

Enhancements and Fixes in v10.2 Hotfix #2

Major changes in this release:

- OpenSSL has been updated from the v1.0.2 series to the v1.1.1 series. This release includes OpenSSL v1.1.1c, and restricts the default ciphers used to be higher quality/more secure than previous PROXY versions, while maintaining backward compatibility with all PROXY versions that supported TLS v1.2. Additionally, TLSv1.3 is now supported in the Host and Master for Windows, Gateway Server, and ClickOnce Connection Window for Windows. Further support for TLSv1.3 will depend on operating system support in Windows (for Web Console, via IIS) and on Macintosh and iOS. Elliptic Curve Cryptography (ECC) certificates are also now supported by the Gateway Server and Gateway Server Certificate Manager.
- Deployment Tool “Export Settings to JSON File” functionality has not been working since v10.0 HF#1, and is fixed in this release. Additionally, the Deployment Tool was not registered as an MMC snapin correctly, so that it did not appear in the “Add/Remove SnapIn...” list.
- Several installed Master issues are addressed in this release, including:
 - Installed Master v10 connecting to GWS v9 as a master-category user now works correctly
 - Master inactivity prompt no longer appears if Master Control Panel window does not have focus; this keeps that popup from interrupting ongoing work in a Connection Window.
 - Master Gateway Groups dropdown list now sorts items correctly even if user does not have access to top-level group(s).
- Gateway Server has a number of reliability and “edge case” processing fixes, primarily around Host status update processing. While the issues addressed generally only occur in unusual or uncommon situations, customers with installations involving either a large number of Hosts, or relatively large numbers of Host reverse connections, or that use Host for Macintosh, are advised to upgrade to this release to ensure the most reliable operations.

Enhancements and Fixes in v10.2 Hotfix #1

Major changes in this release:

- Deployment Tool allowed the new “Watermark” settings to be configured, but did not include this setting when creating a Windows Installer Transform (MST) file.
- The new Web Console feature to launch the installed Master as the default connection experience was not remembering and using that setting if the browser was not Click-Once Deployment enabled.

- Additional information is included in the System Information report to facilitate diagnosing certain kinds of problems.

Enhancements and Fixes in v10.2

In addition to the major new features in v10.2, several issues were resolved in this release:

- The “Suppress Input” feature of the Host was not working in v10.1 and its hotfix releases. This feature is disallowed by default (in Host Control Panel, Options tab, Keyboard and Mouse Suppression), but when allowed, input suppression was not happening. This is fixed in v10.2.
- The ability of the Gateway Server to restrict a Master user to only File Transfer Read or File Transfer Write access to a Host was not working correctly in Host v10.0 or later; the Master user was incorrectly given both File Transfer Read and File Transfer Write access. This only is an issue if users are in the Gateway Server security model as having only one of the two File Transfer rights, and this issue does not affect any other Host services or access rights.
- The Gateway Server incorrectly created two Audit log events with ID=209 for each closed reverse connection. This problem was introduced in v9.0.1 hotfix#6 and exists in all v10.x releases until now. This simply resulted in a redundant entry in the AuditLogs*.CSV files, and had no material impact on anything.
- A few regression issues in the installed Master v10.x (versus installed Master v9 and earlier) were found and fixed. Specifically:
 - Having a pipe character (|) in the Host station name caused peer-to-peer connection attempts to fail with error 0xC004C001 (Host not found).
 - Connection Window window automatic resizing logic was not working for text-mode Hosts (like the Gateway Server “System” group Hosts).
 - The “Send Keystroke” menu on the full screen toolbar, when connected to a Host for Macintosh, did not reflect the Macintosh shortcuts, whereas the Send Keystroke menu on the main toolbar did.

Enhancements and Fixes in v10.1 Hotfix #2

Major changes in this release:

- Fixed Gateway Server reliability problems. Problems could occur if SQL database connection is lost and then restored just as the Gateway Server is being stopped; if a single user opened 9 or more connection windows to different Hosts; or if SQL database connection is not available when the Gateway Server is stopped.
- Host “Active Users” window may have appeared off-screen on a High-DPI monitor.
- Host support for importing and exporting settings in JSON format has been improved. All settings can be expressed in this format for import, and export generates all settings except licenses and simple passwords (these are omitted for security reasons). Deployment Tool supports saving a Host settings configuration to a JSON document.
- Master application could crash on certain Windows OS versions if a defective version of a system DLL (ATLTHUNK.DLL) is installed. This version of Master no longer uses that DLL.
- The latest OpenSSL, v1.0.2r, has been incorporated into the product.

Enhancements and Fixes in v10.1 Hotfix #1

Major changes in this release:

- An issue in certain account management operations in v10.1 original release has been found and fixed. When changing an imported account from Administrative to Master category, or when changing which groups an imported Master-category account has access to, the security associated with existing Hosts was not updated properly. As a result, users who previously had access to Hosts and who no longer should have that access due to the change, could continue to access those Hosts. On upgrade from v10.1 to v10.1 hotfix#1, any incorrect entries in the database are fixed, and all account management operations are processed properly in Hotfix#1.
- The database used by PROXY Pro Server (normally named RemoteControlGatewayDb, although this name may have been changed/configured at original install time) is now automatically backed up before performing a database upgrade. The backup is performed with the T-SQL "BACKUP DATABASE" command to the default location for backups configured in SQL Server. The file name for the backup is the database name, the text "_beforeupgrade_schema_", and the internal schema number of the database being backed up. In a default installation, upgrading from v10.1 to hotfix#1 results in a backup file "RemoteControlGatewayDb_beforeupgrade_schema_1003580.bak". Note that once the database is backed up and upgraded, other install/uninstall operations will not create additional backups.
- The Gateway Server runs several cleanup tasks according to the "periodic tasks" schedule configured via Web Console. These tasks normally run at Gateway Server startup, and then periodically according to the schedule. A bug in v10.0 hotfix#3 and later commonly prevented these tasks from being scheduled and run. This generally did not cause any problems in the installation, although Audit log CSV files, recording files, and other items that get cleaned up by age policy were not cleaned up. This issue is fixed in Hotfix#1, and all items that should have previously been cleaned up will be cleaned up after upgrade to Hotfix#1.
- PROXY Pro Sever v10.1 reintroduced support for reverse web proxies (web proxies configured to be immediately in front of the Server system); this was supported in v9 but not v10.0. Minor issues around the handling of the X-Forwarded-For header were fixed in Hotfix#1, and this release is recommended if a reverse web proxy is in use.
- Improved forward web proxy support for clients and Host, when using the WS and WSS protocols, is implemented in Hotfix#1. Forward web proxy support now looks for:
 - PROXY-specific registry overrides to control and configure the behavior, including the ability to turn auto-discovery of proxy configuration off and omitting all web proxy support. For more information about this configuration, please contact technical support.
 - For client software running as a logged-in user in Windows (e.g., Master), use the system per-user proxy configuration (in Internet Explorer > Internet Options, or system Control Panel > Internet Options, or Windows 10 Settings > Network > Proxy). If the auto detection flag is set, the operating system's WPAD support is used to automatically detect the proxy configuration.
 - For both client software, and the Host service, the system-wide proxy configuration set via the "netsh winhttp set proxy" command is read, and used if set. Note that these settings do not provide auto-configuration, but can provide an explicit proxy configuration.
 - If no instructions regarding web proxy have been found, auto-detection using the WPAD support is tried. Note that because auto-detection can be a time-consuming process, a direct connection (without proxy) is attempted while the web proxy configuration is detected. If

the direct connection fails, and a web proxy configuration is discovered, the connection is automatically retried through the web proxy.

- The software free trial period in this release is 14 days, and does not require any license key. If a longer trial period is required, a time-limited license key can be issued; please contact Sales for help with this.
- The latest OpenSSL, v1.0.2q, has been incorporated into the product.

Enhancements and Fixes in v10.1

In addition to the major new features in v10.1, several issues were resolved in this release:

- Installers now fully support TLSv1.2-only environments. Previously, the software could run in this environment, but TLSv1.0 and TLSv1.1 had to be enabled to install or update the software.
- Installed Host reliably allows the Master to have input control of the Host machine. Previously, plug-and-play operations (e.g. unplugging a mouse or keyboard, or starting up without an attached mouse or keyboard) could cause the Host to lose the ability to inject input into the system.
- Host on high DPI or non-100%-scale displays did not display the “toast” popup messages (if they are configured to display on connect, disconnect, and file transfer). These messages now reliably appear on the display.

Enhancements and Fixes in v10.0.0 Hotfix #3

Major changes in this release:

- Gateway Server has a number of reliability and performance improvements. All customers using PROXY Pro Server v10 are encouraged to upgrade to Hotfix#3 for the best experience.
- 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.
- PROXY Pro Server logins of users that had a large number of security group memberships (more than approximately 80 groups) may not have been evaluated correctly; excessive groups were ignored, so user may not have been given all rights they were eligible for.
- Installed Master fixed a bug with credentials prompting in peer-to-peer (Workstation Edition) connections.
- 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 “HTTPS support”, and is planned for PROXY v10.1 release.)
- OpenSSL library has been updated to v1.0.2p release.

Enhancements and Fixes in v10.0.0 Hotfix #2

New for this release:

PROXY Pro Server

The v10.0.0 release has performance limitations that made installations managing large numbers of Hosts (say, greater than 5000) not work reliably. The performance “hot spots” have been addressed in the Hotfix#2 release, and installations managing over 10,000 Hosts are now supported and perform reasonably.

Major defect fixes in this release:

- Gateway Server now has more robust computation of SPN name for Kerberos authentication to Hosts; this specifically helps in environments with multiple trusted domains.
- Gateway Server has many improvements in reliability, supportability, and performance of Host status processing.
- Gateway Server may fail to stop in a timely fashion when the Server Control Manager requests it to stop, and a crash-at-exit behavior has been fixed.
- If SQL authentication (SQL account and password) are used to set up the SQL database in the ServerProducts installer, these credentials are now correctly stored and used on subsequent upgrades. Previously, they were stored encrypted correctly, but not restored and decrypted properly.
- Master cannot save connection information on machines with a non-English locale (specifically, one where the numeric decimal symbol is not a period “.”).
- Master menu bar and toolbars can now only be moved by clicking the grabber control; this prevents accidental moving or undocking of these bars.
- PhSetup and Deployment Tool (deploying Host with settings) no longer fail when “removesecurityace” is followed by an “addsecurityace”.

Enhancements and Fixes in v10.0.0 Hotfix #1

Note on upgrading to this release:

This release supports upgrading of all server-side components directly from the v10.0.0 initial release. No uninstalls are required. The server-side components cannot be upgraded from v9 or earlier releases. All other product components, including Host and Master, support upgrading from previous releases.

New for this release:

Server Installation

In version 10.0.0, installation of the server software was greatly simplified by providing a bundle installer. This allowed all of the server-side components to be installed by running a single installation file. With hotfix #1, we took this further and now guide the user step by step to ensure these components are configured correctly. Additionally, we now actively guard against many potential misconfigurations. Various scenarios which some customers ran into with the initial release have been collected, analyzed and now guarded against.

Server Configuration Check utility

This is a new standalone utility added to help diagnose and modify a server installation. It will examine the server system’s configuration and identify possible configuration errors. It also allows for easy changing of the DNS name, networking ports, and SSL certificate selections for the installation. This utility is conveniently accessible from the Windows Start menu.

Deployment Tool

In the initial release of v10.0.0, the PROXY pro Deployment Tool had not been updated. This release contains an updated release of the Deployment Tool (v10). Installation of this tool will upgrade v9 and earlier versions while preserving the relevant/supported state. This resolves the issues around creating and applying configurations for the Master component.

Major defect fixes in this release:

- Better handling of transparent/invisible cursor shapes has been implemented. Master now treats invisible pointer as equivalent to “null” pointer, so “show local cursor if Host cursor is missing or hidden” option works.
- Cursor calibration now correct when scaling. Host user mode mouse input injection was wrong in multiple monitor configuration with different display scale factors.
- Print spooler is now stopped as appropriate after installation of Remote Printing.
- Various user interface glitches fixed throughout Web Console – popup display, column sorting, etc.
- Master v10 was not sorting by IP address correctly.
- Host Manage Visual Effects (MVE) feature more reliable, should restore wallpaper correctly, and manages ClearType setting explicitly.
- Gateway Server v10 TCP polling was broken. The Gateway server tried to simultaneously connect to entire poll range, which caused severe problems for large polling ranges. This now polls as before, one address at a time.
- Security and Reliability “X-Forwarded-For” in HTTP header on WSS protocol caused Gateway crash.
- A Master crash in specific circumstances fixed.
- A Host crash in specific circumstances fixed.
- Using PhSetup to repeatedly add security to Host configuration no longer creates duplicate entries.
- Other reliability improvements that enhance the stability of Host, Master and Gateway components.
- Account validation on non-domain joined machines evaluates the authority.
- Master cycling monitor window is now always view-only and cannot take input control.
- The Gateway server may not automatically remove transient Hosts that have gone away and may blank out most fields of a Host record if there was an error during Host status processing.
- The latest OpenSSL, v1.0.2o, has been incorporated into the product.
- The End User License Agreement for all components (EULA) has been updated.

Documentation

Documentation is available at:

- The “**PROXY Pro Server Installation Guide**” is a PDF included in the Private Cloud Edition download (zip file)
- [PROXY Pro Web Console Operations Guide](https://products.proxynetworks.com/docs/proxy/v100/wc/)
(https://products.proxynetworks.com/docs/proxy/v100/wc/)
- [PROXY Pro Host Guide](https://products.proxynetworks.com/docs/proxy/v100/host/)
(https://products.proxynetworks.com/docs/proxy/v100/host/)
- [PROXY Pro Master Guide](https://products.proxynetworks.com/docs/proxy/v100/master/)
(https://products.proxynetworks.com/docs/proxy/v100/master/)
- [PROXY Pro Deployment Tool Guide](https://products.proxynetworks.com/docs/proxy/v100/pdt/)
(https://products.proxynetworks.com/docs/proxy/v100/pdt/)