PROXY Pro Deployment Tool Guide

Release 8.0.2
July 2012

Proxy Networks, Inc.
320 Congress Street
Boston, MA 02210
617-453-2700
http://www.proxynetworks.com

© Copyright 2006-2012 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. 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/).

Table of Contents

PROXY Pro overview 5
What's New in PROXY Pro 8.0 6
What's New in PROXY Pro 7.0 6
What's New in PROXY Pro 6.10 7
What's New in PROXY Pro 6.0 7
PROXY Pro solutions 9
PROXY Pro Workstation Edition 9
PROXY Pro Gateway Edition 9
PROXY Pro Enterprise Edition 9
PROXY Pro applications 11
PROXY Pro Host 12
PROXY Pro Terminal Services Host 13
PROXY Pro VDI Host 14
PROXY Pro Master 15
PROXY Pro Gateway 16
PROXY Pro Web Console 17
PROXY Pro Web Desktop 18
PROXY Pro Deployment Tool 19
PROXY Pro technologies 20
PROXY Pro services 21
PROXY Pro connection types 22
RDP session sharing: Follow the active session 22
Peer-to-peer connections 22
Gateway-managed connections 23
Firewall-friendly connections 25
Terminal Services connections 25
VDI connections 26
VNC connections 27
PROXY Pro security features 28
Authentication 28
Authorization 31
Auditing 31
Encryption 31

PROXY Pro networking features 33
Network protocols 33
Network addressing schemas 33
Wake-on-LAN support 33
PROXY Pro documentation and technical support 35
Typographical conventions in documentation 35
Technical support options 36
Deployment Tool Installation 37
System requirements 38
Operating System Requirements 38
Hardware Requirements 38
Installation Requirements 38
Operating Requirements 39
Microsoft Management Console requirements 40
Adding the Deployment Tool to the MMC 40
Target computer requirements 41
Sharing and security requirements for Windows XP 41
WMI Windows Installer Provider installation 41
Installation notes 42
Licensing 42
Deployment Tool Operation 43
Installation files 45
Loading Proxy Installer Files (.msi) 45
Product Configurations 47
Creating a new Product Configuration file 47
Changing Configuration Settings in the Product Configuration file 49
Creating Windows Installer Transform file 49
Create new configurations 50
Create custom configurations 51
Network Places 58
Add computer 58
Specify target computers for install or uninstall 59
Refresh Details 60
Install Software 61
Update Host Settings 62
Restart Computer 63
Remove Software 64

Upgrade Software 64
Install/uninstall Host, Master or Gateway 64
Active Directory Domains 67
Specify target computers for install or uninstall 67
Refresh Details 68
Install Software 69
Update Host Settings 70
Restart Computer 71
Remove Software 72
Upgrade Software 72
Reports 72
Troubleshooting 75
Authentication failure 75
Trouble installing software or refreshing details on Windows XP 76
Trouble installing/removing software to/from a computer 77
Generate unique HostIDs 78
Prepare the Host and operating system for imaging 78
HostPrep command line syntax 79
Remove duplicate HostIDs 80
RmHostID command line syntax 80
Requirements for RmHostID 81

PROXY Pro overview

Thank you for selecting PROXY™ Pro remote desktop solutions.

PROXY Pro remote desktop solutions provide professional features that enable helpdesk technicians, network administrators, IT managers, and software trainers to deliver professional remote support for a fraction of the cost of hosted solutions.

Some selected features include:

- **Remote Access**: Reach anyone, anywhere, anytime using firewall- and NAT-friendly remote control connections.
- **Remote Control**: Diagnose and resolve support issues without having to physically visit remote computer.
- **Remote Management**: Repair remote computers and make configuration changes in real-time and without disturbing currently logged-on user.
- **Collaboration**: Enable two or more technicians to work on the same remote computer at the same time using chat, screen-sharing and easy-to-pass remote support.

NOTE: *Before you use PROXY Pro remote desktop solutions, you should be familiar with basic network concepts, such as protocols, encryption, IP addresses, ports, and subnets.*

To learn more about PROXY Pro remote desktop solutions, see:

- "What's New"
- "PROXY Pro solutions"
- "PROXY Pro applications"
- "PROXY Pro technologies"
- "PROXY Pro services"
- "PROXY Pro connection types"
- "PROXY Pro security features"
- "PROXY Pro networking features"
- "PROXY Pro documentation and technical support"

What's New in PROXY Pro 8.0

PROXY Pro 8.0 introduces the following new features and capabilities:

- **Web Console**: A new server-side application that enables browser-based access to the Gateway Server for configuration and administration. If Enterprise Edition key is present, Web Console will also be enabled for Web Desktop feature (see *PROXY Pro Web Console Operating Guide*)

- **"Click Once" Web Desktop**: Ability to generate a window to a remote desktop directly from the Web Console (Master not required). No administrative rights needed and no reboot required. Enterprise Edition key required for activation (see *PROXY Pro Web Console Operating 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 Master 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*)

- **Concurrent User License Mode**: In this mode, the Gateway will monitor the number of simultaneous Gateway users according to account type (Administrative, Master, Personal) (see *PROXY Pro Web Console Operating Guide*)

- **Inactivity Timeouts**: To free up concurrent user licenses when users are connected to the Gateway but not active, Web Console, Master and Gateway Administrator will be automatically disconnected from the Gateway, and input control will be automatically released from Web Desktop or Connection Window (see *PROXY Pro Gateway Administrator Guide*)

- **Automatic Grouping of Hosts**: Ability to configure Hosts to automatically report to custom Gateway group(s) according to custom or generic rules (see *PROXY Pro Gateway Administrator Guide*)

- **Virtual Desktop support**: Enables virtual desktop images generated in environments such as Citrix XenDesktop to include Hosts, and to have the Hosts report to Gateway until the desktop image is discarded (see *PROXY Pro Host Guide)*

What's New in PROXY Pro 7.0

- **Windows 7 support**: PROXY Pro 7.0 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 provides full support (remote access, remote control, remote management) for Windows Server 2008 R2 computers (64-bit platforms only).

- **Mac, Linux support**: PROXY Pro 7.0 provides support (remote access, remote control) for Macintosh and Linux computers running VNC server software (standard on Macs).

- **Wake-on-LAN support**: PROXY Pro 7.0 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 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 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 Host will capture and provide input control to the RDP session.
- **Active Directory integration:** PROXY Pro 7.0 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.

What’s New in PROXY Pro 6.10

- **Remote Management service**: PROXY Pro 6.10 features a new service that allows Master user to generate inventory of hardware and software assets on a remote Host. Also allows Master user to query and change certain system settings.
- **Terminal Services support**: PROXY Pro 6.10 supports server-side Hosts for thin client, terminal services sessions for Citrix XenApp (formerly Citrix Presentation Server) and Windows Terminal Server.
- **User-Mode Screen Capture optimization**: PROXY Pro 6.10 includes significant performance and reliability enhancements for user-mode screen capture technology introduced in PROXY Pro 6.0.

What's New in PROXY Pro 6.0

PROXY Pro 6.0 introduced the following new features and capabilities:

- **Windows Vista and Server 2008 support**: PROXY Pro 6.0 applications (Host, Master, Gateway, Deployment Tool) now run on Windows Vista and Windows Server 2008 operating systems.

NOTE: *PROXY Pro 6.0 introduces a new screen capture technology (user-mode) for Windows Vista and Windows Server 2008 platforms.*

- **Bandwidth throttling**: PROXY Pro 6.0 allows screen capture settings to be modified in order to reduce the amount of bandwidth used. Usually, this will reduce screen capture quality but improve responsiveness and overall performance (see *PROXY Pro Host Guide* for more information).
- **Popup notifications**: PROXY Pro 6.0 supports popup "toast" notifications when connections are established to remote computers (see *PROXY Pro Host Guide* for more information).
- **Send keystroke button**: PROXY Pro 6.0 now provides a new toolbar button on the Master Remote Desktop Window, which can be configured to send Ctrl+Alt+Del or one of the other available keyboard combinations to remote computer (see *PROXY Pro Master Guide* for more information).
- **Host-based chat**: PROXY Pro 6.0 introduces support for Host-based chat. This new service automatically creates a private chat room including Host user and any technicians

connected to the Host. Technicians can see and participate in multiple chat rooms simultaneously (see *PROXY Pro Master Guide* for more information).

- **File transfer resume**: Occasionally, a file transfer operation is interrupted when a connection is lost. PROXY Pro 6.0 introduces the ability to resume interrupted file transfers exactly from the point of interruption (see *PROXY Pro Master Guide* for more information).

- **Windows Media format support**: PROXY Pro screen recording files are produced in a streamlined, proprietary format and play back in a viewer provided with PROXY Pro Master. PROXY Pro 6.0 introduces a new utility to enable technicians to convert PROXY Pro screen recording files into Windows Media format for play back in WM-compatible players and editing in off-the-shelf media tools (see *PROXY Pro Master Guide* for more information).

PROXY Pro solutions

Proxy Networks provides three solutions for remote desktop support:

PROXY Pro Workstation Edition

PROXY Pro Workstation Edition is an easy-to-use remote desktop solution that uses simple peer-to-peer connections between helpdesk technicians and end-user remote computers. It is ideally suited for smaller companies and workgroups in which the number of remote computers being supported is small and manageable.

PROXY Pro Gateway Edition

PROXY Pro Gateway Edition is an enterprise-class remote desktop solution that uses a robust, scalable server to establish and maintain a secure network of connections to end-user machines. It leverages centralized administration, security and network access to simplify and automate the creation, management, and monitoring of this “network within a network”. PROXY Pro Gateway Edition is ideally suited for enterprises and corporate workgroups with large numbers of remote computers, multiple domains and/or employees with remote computers outside the network.

PROXY Pro Enterprise Edition

PROXY Pro Enterprise Edition is a web-enabled version of the Gateway Edition, and includes Web Desktop for on-demand access to remote desktops in place of the installed Master application.

PROXY Pro Features	PROXY Pro Workstation Edition	PROXY Pro Gateway Edition	PROXY Pro Enterprise Edition
Components			
PROXY Pro Host	Yes	Yes	Yes
PROXY Pro Terminal Services Host	No	Yes	Yes
PROXY Pro VDI Host	No	Yes	Yes
PROXY Pro Master	Yes	Yes	No
PROXY Pro Gateway	No	Yes	Yes
PROXY Pro Web Console	No	Yes	Yes
PROXY Pro Web Desktop	No	No	Yes
PROXY Pro Deployment Tool	Yes	Yes	Yes
Connection Types			
Peer-to-peer connections	Yes	Yes	Yes

Gateway-managed connections	No	Yes	Yes
Firewall-friendly connections	No	Yes	Yes
Terminal services connections	No	Yes	Yes
VDI connections	No	Yes	Yes
VNC connections	Yes	Yes	No

PROXY Pro applications

The PROXY Pro remote desktop solutions include some or all of the following applications:

PROXY Pro Components	PROXY Pro Workstation Edition	PROXY Pro Gateway Edition	PROXY Pro Enterprise Edition
PROXY Pro Host	Yes	Yes	Yes
PROXY Pro Terminal Services Host	No	Yes	Yes
PROXY Pro VDI Host	No	Yes	Yes
PROXY Pro Master	Yes	Yes	No
PROXY Pro Gateway	No	Yes	Yes
PROXY Pro Web Console	No	Yes	Yes
PROXY Pro Web Desktop	No	No	Yes
PROXY Pro Deployment Tool	Yes	Yes	Yes

PROXY Pro Host

PROXY Pro Host runs as a Windows service on the machine on which it is installed, and supports both peer-to-peer connections as well as Gateway-managed connections. By installing PROXY Pro Host on a computer in your network, you can:

- Allow technicians to make peer-to-peer remote control connections to the machine, whether someone is there or not. Each Host manages its own security settings and access rights.
- Allow or force technicians to make Gateway-managed remote support connections to the machine through a central server (PROXY Pro Gateway), which will automatically enforce security settings and access rights according to policies set at the server.

The PROXY Pro Host requires a Host license key.

For more information about configuring and operating PROXY Pro Host, please see the *PROXY Pro Host Guide*.

PROXY Pro Terminal Services Host

PROXY Pro Terminal Services Host is a server-side version of the PROXY Pro Host designed to support Terminal Services sessions.

The Terminal Services Host, also known as the root Host, runs on the Terminal Server (such as those from Citrix or Microsoft), and is configured to support one or more concurrent Terminal Services sessions. Each time the Terminal Server generates a new Terminal Services session, the Terminal Services Host injects a copy of the Host into the session. The session Host will include instructions for reporting to one or more Gateways. When the TS session is discarded, the TS Host session will also be discarded and will be automatically removed from the Gateway(s).

The PROXY Pro Terminal Services Host requires a special Host license key that will specify the maximum number of concurrent Terminal Services sessions that can be supported on that Terminal Server.

For more information about configuring and operating PROXY Pro Terminal Services Host, please see the *PROXY Pro Host Guide*.

PROXY Pro VDI Host

PROXY Pro Virtual Desktop Image Host is a special version of the PROXY Pro Host designed to support the transient nature of virtual desktops.

The VDI Host can be included as part of a virtual desktop template; when one or more virtual desktop sessions are generated using this template (often to create a pool of virtual desktop images), the sessions will include a Host with all the features of the installed Host but not the permanent nature. When the virtual desktop session is discarded, the Host will also be discarded and will be removed automatically from the Gateway(s).

The PROXY Pro VDI Host requires a special Host license key that will specify the maximum number of concurrent VDI sessions that can be supported in the virtual desktop environment.

For more information about configuring and operating PROXY Pro VDI Host, please see the *PROXY Pro Host Guide*.

PROXY Pro Master

PROXY Pro Master is a console application that technicians can use to establish remote support connections to one or more Host computers. With PROXY Pro Master, you can:

- Make one or more peer-to-peer remote support connections to Host computers in your network.
- Connect to PROXY Pro Gateway and make one or more Gateway-managed remote support connections to Host computers from a directory of available Hosts.
- View the entire screen of the remote computer.
- Take complete control of a Host computer using the local keyboard and mouse.
- Share control of the Host computer with its end-user.
- Passively monitor the Host computer without exercising control.
- Use the clipboard transfer feature to transfer portions of text, bitmaps, and other objects between your Host and Master computers.
- Use the PROXY Pro file transfer feature to copy files between your Host and Master computers.
- Use the PROXY Pro remote printing feature to print locally from applications running on a remote computer.
- Record screen activity on the Host and play back the recording on the Master.
- Chat with end-user and any other technicians connected to the same Host.

For more information about configuring and operating PROXY Pro Master, please see the *PROXY Pro Master Guide*.

PROXY Pro Gateway

PROXY Pro Gateway is an enterprise class server, which provides centralized administration, security and management for a network of remote support connections to Host computers in your environment.

With PROXY Pro Gateway configured as the hub of your remote support network, you can:

- Organize large numbers of Host computers into logical groups for easier access and management.
- Reach remote computers outside the network, behind firewalls or NAT-devices.
- Utilize SSL for certificate-based authentication.
- Create custom access rights policies and apply them to groups to make configuration changes more quickly and efficiently.
- Monitor and manage remote support activity in real-time.
- Keep detailed records of all remote support activity in your network with comprehensive audit logs.
- Record screen activity on one or more remote computers simultaneously using PROXY Pro Gateway's screen recording feature.

PROXY Pro Gateway includes the PROXY Pro Gateway Administrator, a tool for configuring the Gateway and for monitoring, managing and auditing remote support activity in your network.

For more information about configuring and operating PROXY Pro Gateway, please see the *PROXY Pro Gateway Server Guide*.

PROXY Pro Web Console

PROXY Pro Web Console is a web application that provides browser-based access to the PROXY Pro Gateway Server for administration and configuration. It is effectively a web-based version of the Gateway Administrator.

The Web Console also includes an optional feature called the Web Desktop, which allows on-demand access to remote desktops directly from the Web Console. It is effectively a web-based version of the Master application.

With PROXY Pro Web Console:

- Administrators can access and edit all the configuration information on the Gateway Server, including Groups, Security, Permissions, etc. The Administrative web account can be used in conjunction with or instead of the standalone Gateway Administrator application.
- If the Web Desktop is enabled, Helpdesk technicians can view and access remote desktops connected to the Gateway.

For more information about configuring and operating PROXY Pro Web Console, please see the *PROXY Pro Web Console Operating Guide*.

For more information about installing PROXY Pro Web Console, please see the *PROXY Pro Web Console Installation Guide*.

PROXY Pro Web Desktop

The Web Desktop is an optional feature of the Web Console, which allows on-demand access to remote desktops directly from the Web Console. It is effectively a web-based version of the Master application.

With PROXY Pro Web Destkop:

- Helpdesk technicians can view and access remote desktops connected to the Gateway.
- Employees can view and access their computers at work, even if they are on the road or at home. The Personal web account offers convenient, secure, reliable alternative to VPN.

To enable the Web Desktop, a special key must be entered into the Gateway Server.

For more information about configuring and operating PROXY Pro Web Desktop, please see the *PROXY Pro Web Console Operating Guide*.

PROXY Pro Deployment Tool

PROXY Pro Deployment Tool is an easy-to-use software distribution utility that automates the deployment and installation of PROXY Pro applications to remote computers in your network.

With PROXY Pro Deployment Tool, you can:

- Automatically deploy an image of PROXY Pro Host, Master or Gateway to one or more computers or groups of computers in your network and avoid manual effort of going to each machine.
- Create an image of PROXY Pro Host, Master or Gateway with custom configuration options that can be mass deployed on large numbers of computers in your environment.
- Create and push custom configuration options for PROXY Pro Host, Master or Gateway, without having to reinstall underlying software.
- Use Active Directory to find remote computers and push software and configuration settings to them.

For more information about configuring and operating PROXY Pro Deployment Tool, please see the *PROXY Pro Deployment Tool Guide*.

PROXY Pro technologies

PROXY Pro remote desktop solutions utilize highly optimized technologies to deliver speed, performance and reliability, including:

- **Highly efficient screen capture algorithms**. PROXY Pro utilizes two kinds of screen capture technology:
  - Kernel-mode screen capture. This technology utilizes the PROXY Pro mirror driver, which reproduces graphics drawing commands from the remote Host on the PROXY Pro Master user's screen quickly and efficiently.
  - User-mode screen capture. This technology works without a mirror driver and is designed to adjust automatically to the amount of CPU and bandwidth available on the remote Host machine.
- **Streamlined communication protocol**. The PROXY Pro protocol has been honed over 15 years for efficiency and reliability when sending screen capture data to another computer in real-time and receiving keyboard/mouse input.

Using these technologies, PROXY Pro remote support solutions enable technicians to find and fix problems on remote computers faster and easier than ever before.

PROXY Pro services

PROXY Pro remote desktop solutions offer technicians a number of professional-quality services for investigating and solving problems on Host remote computers, including:

- **Remote Control:** ability to view screen activity on an end-user's remote machine, and with proper authorization, take control of and send keyboard/mouse inputs to the remote machine in real-time
- **Remote Clipboard**: ability to copy selected items on the screen of a remote machine into the clipboard on the remote machine and transfer the contents to the clipboard on the technician's machine, and vice versa
- **File Transfer**: ability to drag-and-drop files or directories on the remote machine to the technician's machine, and vice versa
- **Host-based Chat**: ability to chat with the end-user on a remote machine, and any other technicians connected to that machine
- **Remote Printing**: ability to print selected items from the remote machine to a printer attached to the technician's machine
- **Host Administration**: ability to view and edit configuration settings of the PROXY Pro Host installed on the remote machine
- **Remote Management**: ability to generate inventory of hardware and software assets on remote machine, and to query and change certain system settings. See "Remote Management features" for more information about tools available through this service.

PROXY Pro connection types

PROXY Pro services are performed over service connections between a PROXY Pro Master (with appropriate access rights) and a PROXY Pro Host. Service connections are established on demand, when a PROXY Pro Master requests a service from a PROXY Pro Host.

PROXY Pro supports several different types of remote access connections:

PROXY Pro Connection Types	PROXY Pro Workstation Edition	PROXY Pro Gateway Edition	PROXY Pro Enterprise Edition
RDP session sharing	Yes	Yes	Yes
Peer-to-peer connections	Yes	Yes	Yes
Gateway-managed connections	No	Yes	Yes
Firewall-friendly connections	No	Yes	Yes
Terminal Services connections	No	Yes	Yes
VDI connections	No	Yes	Yes
VNC connections	Yes	Yes	No

RDP session sharing: Follow the active session

PROXY Pro connections can be used to share an active RDP session in real-time.

If PROXY Pro Host is running on a desktop-class operating system (e.g. Windows 7), and there is an active/connected RDP session being hosted on that computer, then the Host will automatically capture and provide input control to that RDP session. In essence, the Host will capture what the remote RDP session user is seeing, not what the local physical console on that machine is showing (probably the Windows login screen).

When there is no active/connected RDP session being hosted on that computer, or if an active/connected RDP session is stopped, the Host will automatically capture and provide input control to the session running on the computer and being displayed on the local console. The Host will follow the active session as it moves from RDP user back to the local console.

***Note**: This feature only applies to desktop-class operating systems, which support only one active session at a time. Server-class operating systems (e.g. Windows Server 2003 or Server 2008) can support multiple sessions simultaneously via Terminal Services; use the Terminal Services support in the Host to capture and/or provide input control to one or more sessions on server-class OS.*

Peer-to-peer connections

When a computer with PROXY Pro Master establishes a direct connection to a computer with PROXY Pro Host, the connection that is established is a **peer-to-peer connection**.

By default, PROXY Pro Master searches the network for Host computers when it starts up. Any Host computers it finds are listed on the **Peer-to-Peer Hosts** tab of the PROXY Pro Master window.

Peer-to-peer connections from Master (M) to Host (H)

The dotted and solid lines, shown in above depict two different sets of peer-to-peer connections between PROXY Pro Masters to PROXY Pro Hosts. PROXY Pro's peer-to-peer connections enable the following:

- PROXY Pro Master users with proper credentials can securely access Host computers within the network.
- When you permit full access to a Host computer, the PROXY Pro Master user can monitor all activity on the Host computer. In addition, PROXY Pro Master users with full access rights can exercise complete control over that computer.
- When the Host and Masters are in the same domain, PROXY Pro Host can be configured to use the Microsoft Windows authentication service to check credentials of any PROXY Pro Master users. An access control policy can allow (or deny) full or partial access for authenticated PROXY Pro Master users to access services on a Host computer.

Although PROXY Pro's peer-to-peer connections provide a secure solution for remote support, this solution is not recommended for large and/or highly distributed networks; instead, consider using PROXY Pro Gateway for centrally managed remote support connections.

Gateway-managed connections

When a computer with PROXY Pro Master establishes a connection to a computer with PROXY Pro Host through a central server (i.e. PROXY Pro Gateway), the connection that is established is a **Gateway-managed connection**. In this way, the Gateway serves as a central location for managing and monitoring connections, configuration, security and reporting. Any Host computers found by the Gateway are listed on the **Gateway Hosts** tab of the PROXY Pro Master window.

In large networks, the PROXY Pro Gateway can be configured to manage connections with hundreds or thousands of Hosts simultaneously, enabling Masters to find and take control of Hosts instantly.

Gateway-managed connections utilize the same strong authentication and authorization that is available with PROXY Pro's peer-to-peer connections. In addition, PROXY Pro Gateway provides the following capabilities:

- Seamless connections from Master computers to Host computers through a PROXY Pro Gateway. To the PROXY Pro Master user, the connection appears as if it were a peer-to-peer connection to the Host computer, even if the Host is outside the domain and/or behind a firewall or NAT device.

- Centralized management of access rights to remote computers in your network. Once you configure your Host computers to report to the PROXY Pro Gateway, you can achieve global management through a single security policy that you configure using PROXY Pro Gateway Administrator.

- User-based access policies. Customize and apply access policies to individual PROXY Pro Master users or groups in your network. Allow full remote access to one or more Host computers for some PROXY Pro Master users, while restricting access rights for others.

- Comprehensive logging and auditing of all remote control activity within your network. With this feature, you can keep records of all remote support connections.

- Continuous screen recording. PROXY Pro Gateway allows you to record screen activity on any remote Host. Efficient file compression makes 24x7 recording economical and manageable.

Gateway (G)-managed connections from Master (M) to Host (H)

Firewall-friendly connections

When PROXY Pro Master users need access to Hosts that are outside the domain, and/or behind a firewall or NAT-device, normal peer-to-peer or Gateway-managed connections will not work. In these cases, it is difficult to find and maintain a secure remote support connection because of dynamic port assignments and other network challenges.

For these situations, PROXY Pro Gateway builds special firewall-friendly connections to these Hosts. When Hosts are outside the domain, the Hosts are programmed to automatically initiate contact with the Gateway. The Gateway will use this initial contact to build a firewall-friendly connection to the Host. In this way, the remote Host outside the domain will appear just like any Host inside the domain.

Terminal Services connections

PROXY Pro provides server-side support (screen capture, input control, screen recording) for session-based virtual desktops hosted by Terminal Services on Windows Server 2003 or Window Server 2008 (now called "Remote Desktop Services"). Windows Server creates and hosts the Terminal Services (TS) sessions like virtual machines. A presentation technology using a display protocol such as RDP from Microsoft or ICA from Citrix is typically used to remote the session display, as well as the keyboard and mouse input, to and from an end user device (such as a thin client computer like a Wyse terminal).

PROXY Pro allows technicians to capture (and if desired, record) the session presentation information at the Windows Server before it is remoted to the end user device over the RDP or ICA display protocol. PROXY Pro is able to do this by injecting a Host instance into each server-side TS session, which in turn captures and sends presentation information directly to PROXY Pro Gateway for recording and/or further transmission to a PROXY Pro Master.

***Note**: Because TS sessions are captured at the Windows Server (and not at the end user device), PROXY Pro Host effectively bypasses the technology used to remote the sessions to the end users, and will therefore be compatible with Microsoft Terminal Services clients as well as Citrix Presentation Server (now known as XenApp) clients.*

***Note**: PROXY Pro only supports TS sessions created on server-class Windows operating systems such as Windows Server 2003 and Windows Server 2008.*

See **Terminal Services tab** in PROXY Pro Host Guide for more specific configuration and setup information.

Root Host for TS sessions

The “Terminal Services” feature of Windows Server 2003 and Windows Server 2008 allows multiple virtual desktop sessions to be active simultaneously. PROXY Pro provides remote access and remote control to these sessions on the Windows Server by injecting a separate instance of the Host service into every new TS session. A special version of the Host called the "root" Host must be loaded on the TS server (a "root" Host is a standard Host with a special TS license key - see **About tab** in the *PROXY Pro Host Guide* for more information); it will automatically spawn new Host instances every time a new TS session is created.

Transient Hosts

Each TS instance of the Host will have its own unique workstationID and must be configured to report to a Gateway. When it first reports to the Gateway Server, it will be automatically managed and added to the “All Hosts” group. The TS Hosts are considered transient, since they go away when the TS user logs out of his/her session. In order to keep track of transient TS Hosts, the PROXY Pro Gateway will create a new Group called "Terminal Services on <Servername>", and automatically insert transient Hosts into this Group. They are automatically deleted from the Gateway when the TS session ends. The main purpose of this Group is to allow security to be assigned to the Hosts and TS sessions that belong to this Group, and to provide the correct and appropriate access to the TS-based Host instances.

***Note**: PROXY Pro Host for Terminal Services works on Server 2003 & Server 2008, and requires a Gateway Server v6.10 or later.*

Recording TS Hosts

Recordings are normally deleted from the Gateway database when their associated workstation record is deleted. Transient TS Host workstation records are automatically deleted from the Gateway when the TS user logs out of his/her session. However, to prevent recordings of TS Hosts from being automatically deleted when the TS session ends, the TS session recordings are reassigned to an artificial permanent workstation record called "Recordings on <Servername>". All recordings of all TS Hosts on a given TS server will be associated with this one record. This approach has the following advantages:

- Recordings are not orphaned
- All recordings can be kept in one place,
- TS recordings can be kept separate from console (root Host) recordings
- Security can be configured separately for each recording.

Limitations of TS Hosts

Due to technical limitations and the nature of Terminal Services sessions, the following Host features are not supported.

- Remote printing
- Keyboard and mouse suppression (requires kernel-based input stack intercept)
- Screen blanking (requires kernel-based support and physical display to blank)
- Peer-to-peer connections: all protocols are disabled, and the only connections that can be made are through a configured Gateway Server
- Kernel-mode screen capture (even on Windows Server 2003, requires kernel-mode display support)

VDI connections

PROXY Pro provides a special version of the Host to run inside of virtual desktop images (VDI) created from virtual desktop templates in environments such as Citrix XenDesktop. If the regular Host is specified in the template, then the Host will automatically be installed when the virtual desktops are created using this template.

This works fine with Peer-to-Peer connections to the Host in the VDI, but has some complications when the Host is configured to report to one or more Gateway Servers:

- The GWS must be configured to “automatically manage new Hosts” to have the Host become available without any manual intervention.

- If the virtual desktop is discarded when the user logs out, the Host is effectively destroyed as well, but the Gateway doesn’t know this. The Host remains known to the Gateway (and managed, using a Managed Hosts license) until it is manually cleaned up by an administrator, or until the **Delete Hosts older than** feature kicks in and deletes it. (But note that setting is measured in days, default is set to 120, and setting that to a low value runs the risk of deleting conventional installed Hosts that are simply offline for a while.)

To address both of these problems, the Gateway Server supports a special version of the Host for VDI that is “transient” in nature (similar to a Terminal Services Host session); when the VDI Host is specified in the template, the following will occur:

- A new group, “Transient VDI Hosts”, is automatically created at the Gateway when a Host of this type first reports. All Hosts of this type are automatically managed (independent of the “automatically manage Hosts” setting), and are added to this group.

- If the virtual desktop is discarded when the user logs out, the VDI Host, because of its transient nature, will automatically be disconnected and removed from the Gateway, freeing up a Managed Host license.

- Similar to what happens when recording TS Host sessions, a new pseudo-host, “Recordings of Transient VDI Hosts”, is created when any of these Hosts is recorded. The recording of the VDI Host is associated with this pseudo-Host instead of with the Host workstation, and will remain in there even after the virtual desktop is discarded

- If the Gateway is in Managed Hosts licensing mode, a new license key that limits the maximum number of VDI Hosts that can be connected to the Gateway concurrently is required

VNC connections

PROXY Pro provides remote access and remote control to computers running a standard version of VNC (Virtual Network Computing) server. A VNC server is built into recent versions of the Mac OS X operating system from Apple Computer, and is also available on many versions of the Linux operating system. When properly configured, technicians can use PROXY Pro Master on Windows to connect to and take control of Mac and Linux computers running standard VNC server.

PROXY Pro currently supports peer-to-peer connections to VNC servers. Support for Gateway-managed connections to VNC servers is expected in the next release.

See "VNC Hosts" in the *PROXY Pro Master Guide* for more information on configuring and connecting to VNC servers.

Supported Platforms

PROXY Pro Master can interoperate with standard VNC servers on following platforms:

- Mac OS X v10.5-10.7
- Red Hat Linux Fedora 11-16

PROXY Pro security features

One of the most valuable aspects of PROXY Pro remote desktop solutions is the ability to create and enforce fine-grained access control policies, and to easily modify them to reflect changes in your organization.

PROXY Pro security features include the following:

- "Authentication"
- "Authorization"
- "Auditing"
- "Encryption"

Authentication

In the PROXY Pro model, PROXY Pro applications that request information and services are considered "clients" and those that provide information and services are considered "servers". For example, the PROXY Pro Master is considered a client when it connects to and requests a list of Hosts from a PROXY Pro Gateway. In turn, the PROXY Pro Gateway is considered a client when it connects to and requests information from a PROXY Pro Host in the same domain.

Connection	Client	Server
Peer-to-peer	Master	Host
Gateway-managed (Gateway & Host are in same domain)		
◆ Master-Gateway relationship	Master	Gateway
◆ Gateway-Host relationship	Gateway	Host
Gateway-managed (Gateway & Host are not in same domain)		
◆· Master-Gateway relationship	Master	Gateway
◆ ·Gateway-Host relationship	Host	Gateway

When PROXY Pro Host is not in the same domain as the Gateway, the relationship is automatically reversed: The Host is programmed to be the client and will reach out to the Gateway (see "Firewall-friendly connections" for more information about PROXY Pro firewall-friendly connections).

To guarantee security in the PROXY Pro environment, it is critical that PROXY Pro components acting as servers validate the credentials of users of PROXY Pro components acting as clients before they provide access or data. The burden is placed on the client to authenticate itself to the server. PROXY Pro implements two types of authentication to support this:

- "Identity Authentication"
- "Endpoint Authentication"

Identity Authentication

In general, this operation answers the following security question: How does the server know who the client is? A PROXY Pro application acting as a server will not provide access or information to any PROXY Pro application acting as a client until it can validate that client's identity. PROXY Pro provides the server three different methods of authenticating the identity of the PROXY Pro client:

Connection	Windows authentication	Simple password	Shared-secret password
Peer-to-peer	Yes	Yes	No
Gateway-managed (Gateway & Host are in same domain)			
◆ Master-Gateway relationship	Yes	No	No
◆ · Gateway-Host relationship	Yes	No	Yes
Gateway-managed (Gateway & Host are not in same domain)			
◆ Master-Gateway relationship	Yes	No	No
◆ · Gateway-Host relationship	No	No	Yes

◆ **Windows authentication**: By default, a PROXY Pro application acting as a server uses Windows authentication to check the Windows credentials of the client application:

- ◆··· The Host will check the Windows credentials of the PROXY Pro Master user in the case of a peer-to-peer connection;
- ◆···The Gateway will check the Windows credentials of the PROXY Pro Master users in the Master-Gateway part of a Gateway-managed connection;
- ◆···The Host will check the Windows credentials of the user logged into the Gateway in the Gateway-Host part of a Gateway-managed connection (when Host and Gateway are in the same domain).

NOTE: *If Host and Gateway are not in the same domain, Windows authentication will not usually be available. In that case, Host and Gateway will rely on Shared secret password.*

◆ **Simple password**: Prior to making a connection, a custom password can be created on the **Security** tab of the Host and shared with PROXY Pro Master user. This feature permits the PROXY Pro Master user to connect to a Host without regard to PROXY Pro Master user's Windows credentials.

NOTE: *Simple password applies only to peer-to-peer connections.*

- **Shared secret password**: In the case that the Host does not share a domain relationship with the PROXY Pro Gateway, or if the Host is outside of the network and cannot contact its domain controller, Windows authentication will not usually be available. Behind the scenes, the PROXY Pro Gateway and the Host will exchange a 16-byte secret password that only they will know. As a result, in all subsequent connections, the PROXY Pro Gateway and Host will have some measure of authentication when they are not in the same domain. If the Host belongs to the same domain as the PROXY Pro Gateway, and the Host is able to reach a domain controller, the Host will prefer to do Windows authentication instead of shared secret password.

Endpoint Authentication

In general, this operation answers the following security question: How does the client know it is connected to the right server? Identity authentication doesn't prohibit the client from being fooled into connecting to a different server. In order to guarantee that information and services are coming from the expected server, PROXY Pro supports endpoint authentication using Secure Sockets Layer (SSL).

- **SSL certificate authentication** (PROXY Pro Gateway only): PROXY Pro has implemented server endpoint authentication using SSL, which means the client will request and validate a certificate from the server before providing requested information or services. This ensures the client has connected to the right server. The following list describes where SSL authentication can and cannot be used:

  - **Peer-to-peer connections:** SSL authentication is not available for peer-to-peer connections. This would require each Host (acting as server) to carry its own certificate, which would be unwieldy and costly to manage.

  - **Gateway-managed connections (Host is in same domain as Gateway)**: SSL authentication is available between Master (acting as client) and Gateway (acting as server). Before connecting, the Master will request and validate a certificate from the Gateway. In general, SSL between Master and Gateway would be most useful when the Master is outside the LAN and/or coming in through a corporate firewall to access the Gateway.

  NOTE: *SSL authentication is not available between the Gateway (acting as client) and the Host (acting as server). As in peer-to-peer connections, this would require each Host to carry its own certificate. SSL connections to the Host are generally not required because the Host can be configured to use a reverse connection to the Gateway, which can use SSL.*

  - **Gateway-managed connections (Host is not in same domain as Gateway)**: When the Host is outside the LAN and/or behind a firewall or NAT-device, the Host is the client and has responsibility to contact the Gateway. SSL authentication is supported and would be appropriate to ensure that the Host is connecting to the right Gateway. The Host will validate the Gateway Server certificate before accepting the connection, ensuring that the Host is communicating with the correct Gateway Server.

In summary, SSL can be used by the Master to authenticate a Gateway, and by a Host to authenticate a Gateway when the Host is outside the domain:

Connection	Client	Server	SSL Supported
Peer-to-peer	Master	Host	No

Gateway-managed (Master & Host are in same domain)			
◆ Master-Gateway relationship	Master	Gateway	Yes
◆ Gateway-Host relationship	Gateway	Host	No
Gateway-managed (Master & Host are not in same domain)			
◆ Master-Gateway relationship	Master	Gateway	Yes
◆ Gateway-Host relationship	Host	Gateway	Yes

Authorization

One of the strongest features of PROXY Pro remote support solutions is the fine-grained access control. For example, to perform remote support, you must have the following:

- Proper credentials with which to connect to the Host computer
- Authorization to view the Host computer remotely
- Authorization to control the Host computer remotely

Your credentials are established when you connect to a Host computer (or to a PROXY Pro Gateway), and persist until the connection breaks. You can configure access and other rights directly on the Host computer for peer-to-peer connections. Alternatively, you can use the PROXY Pro Gateway to enforce custom access rights policies on PROXY Pro Master users, roles, or groups for Gateway-managed connections.

Auditing

PROXY Pro Gateway provides a detailed log of connection attempts, actions and other activities that occur in the network. This log is also customizable and exportable to 3rd party reporting products using standard formats.

PROXY Pro Gateway also features screen recording for any Host in contact with a Gateway, whether or not there is an active remote support connection. With this feature, PROXY Pro Master users can keep a visual log of activities going on in the network.

Encryption

To ensure privacy of communications between PROXY Pro applications across the network, PROXY Pro provides advanced encryption using Advanced Encryption Standard (AES) block ciphers and Secure Hashing Algorithm (SHA-1). This protection will be automatic and transparent every time two PROXY Pro 5.20 components or later are communicating with each other.

By default, PROXY Pro Workstation Edition and PROXY Pro Gateway Edition uses AES 256-bit encryption, however other encryption options can be set, including:

- AES encryption (256-bit key) with SHA1 hash
- AES encryption (192-bit key) with SHA1 hash

- AES encryption (128-bit key) with SHA1 hash
- Triple-DES (3DES) encryption (192-bit key) with SHA1 hash
- RC4-compatible encryption (128-bit key) with MD5 hash

NOTE: *PROXY Pro 5.10 applications and older support only RC4 encryption; thus, this would be the encrpytion option negotiated between a PROXY Pro 5.20 or later application (e.g. PROXY Pro Master) and PROXY Pro 5.10 application (e.g. PROXY Pro Host).*

Order of precedence

When two PROXY Pro components have different encryption options set, the first encryption choice in common between the two is used (going down the list in order), with preference set as follows:

- Preference set by the Host, when the Gateway requests connection to the Host
- Preference set by the Gateway, when the Master requests connection to a Host through the Gateway

PROXY Pro networking features

PROXY Pro remote desktop solutions support several standard transport protocols for computer-to-computer communication, and two types of network addressing schemas.

Network protocols

PROXY Pro products support most of the standard networking and transport protocols, including:

- **IP:** IP is a general-purpose protocol supported on a wide variety of networks and servers. PROXY Pro components support communications using either the TCP or UDP transport protocols running over IP. PROXY Pro has established the following standard ports for use with either TCP or UDP:
  - PROXY Pro Host listens on port 1505 by default
  - PROXY Pro Gateway listens on port 2303 by default
- **SSL**: The SSL protocol runs above TCP/IP and below higher-level protocols such as HTTP or IMAP. Using TCP/IP on behalf of the higher-level protocols allows an SSL-enabled server to authenticate itself to an SSL-enabled client, and then establish an encrypted connection between the remote computers.
  - By default, PROXY Pro Gateway listens for incoming SSL connections on port 443, but it might be appropriate to note that this can be easily changed to avoid conflicts with other server software installed on the same machine.
  - The PROXY Pro Gateway now ships with a Gateway Certificate Manager to manage the creation and/or selection of a SSL security certificate for the PROXY Pro Gateway.

Network addressing schemas

The PROXY Pro UDP, TCP and SSL transport protocols support the use of either IPv4 (32-bit) or IPv6 (128-bit) addresses.

Wake-on-LAN support

PROXY Pro can be used to "wake-up" remote computers that have been shut down (sleeping, hibernating, or soft off; i.e., ACPI state G1 or G2), with power reserved for the network card, but not disconnected from its power source. The network card listens for a specific packet containing its MAC address, called the *magic packet,* that is broadcast on the subnet or LAN.

In order to execute this feature, both the MAC address and the last known IP address of the remote computer must be known. Since the PROXY Pro Gateway knows both of these pieces of information, it is in a position to send the Wake-on-LAN signal.

PROXY Pro implements this functionality in Gateway-managed connections in two ways:

- **Implicit Wake-on-LAN**: If Gateway is asked to make a connection to a remote computer and the last status indicates that the remote computer is "Offline", the Gateway will automatically attempt to wake up the remote computer by sending appropriately configured WOL signal. If the remote computer was shut down in a state capable of

receiving WOL signal, it will wake up and report to the Gateway and a connection will be established.

- **Explicit Wake-on-LAN**: A network administrator, using either PROXY Pro Master or PROXY Pro Gateway Administrator, can attempt to wake up a remote computer by explicitly sending the WOL signal to that machine. If the remote computer was shut down in a state capable of receiving WOL signal, it will wake up and report to the Gateway and a connection will be established.

See "Send Wake-on-LAN Signal" in the *Proxy Pro Master Guide* for more information.

PROXY Pro documentation and technical support

Each of the four PROXY Pro components has its own guide:

- *PROXY Pro Master Guide*
- *PROXY Pro Host Guide*
- *PROXY Pro Gateway Server Guide*
- *PROXY Pro Web Console Operating Guide*
- *PROXY Pro Web Console Installation Guide*
- *PROXY Pro Deployment Tool Guide*

For more information about PROXY Pro documentation and technical support, see:

- "Typographical conventions"
- "Technical support options"

Typographical conventions in documentation

PROXY Pro documentation uses typographical conventions to convey different types of information.

Computer text

Filenames, directory names, account names, IP addresses, URLs, commands, and file listings appear in a plain fixed-width font:

> You can use the default domain user account named ‘`RemoteControlGateway`’.

In examples, text that you type literally is shown in a bold font.
To run the installation program, type **`installme`** in the command line.

Screen interaction

Text related to the user interface appears in **bold sans serif type**.

> Enter your username in the **Login** field and click **OK**.

Menu commands are presented as the name of the menu, followed by the **>** sign and the name of the command. If a menu item opens a submenu, the complete menu path is given.

> Choose **Edit > Cut**.
> Choose **Edit > Paste As… > Text**.

Variable text

Variable text that you must replace with your own information appears in a fixed-width font in italics. For example, you would enter your name and password in place of ***`YourName`*** and ***`YourPassword`*** in the following interaction.

```
Enter your name: YourName
Password: YourPassword
```

File names and computer text can also be displayed in italics to indicate that you should replace the values shown with values appropriate for your enterprise.

Key names

Names of keyboard keys appear in SMALL CAPS. When you need to press two or more keys simultaneously, the key names are joined by a + sign:

Press RETURN.

Press CTRL+ALT+DEL.

Technical support options

If you have any problems installing or using the PROXY Pro remote support products, information and support resources are available to help:

This manual and the `Release Notes` may contain the information you need to solve your problem. Please re-read the relevant sections. You may find a solution you overlooked.

Our technical support staff can be contacted by the following means:

- Web: Fill out a support request at `http://www.proxynetworks.com/support` and a case number will be automatically assigned to you
- Phone: (617) 453-2710
- Email: `support@proxynetworks.com`.

We offer a range of support options including support and maintenance contracts, and time and materials projects. Consult our web site for the support plan that best meets your needs. Go to `http://www.proxynetworks.com` and navigate to the **Support** section of the web site for more information.

Deployment Tool Installation

PROXY Pro Deployment Tool can be installed with the following considerations:

- "System requirements"
- "Microsoft Management Console requirements"
- "Target computer requirements"

System requirements

PROXY Pro Deployment Tool can be installed on any computer that runs a supported operating system (OS) and matches the requirements described in this section.

Operating System Requirements

Supported operating systems are:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2

PROXY Pro applications are supported on both 32- and 64-bit editions of these operating systems (except Windows Server 2008 R2, which only comes in 64-bit edition).

Hardware Requirements

The hardware requirements are:

- Minimum requirements – Same as those specified by Microsoft for the respective operating system.
- Recommended requirements – Same as those specified by Microsoft for the respective operating system.

Installation Requirements

The following additional requirements are required or recommended for installation of PROXY Pro Deployment Tool:

- Windows Installer 2.0 or later – Required by the installer. If needed, this upgrade is applied automatically when the `setup.exe` installer image is run.
- Adobe Reader - Required for documentation.
- Microsoft Management Console 3.0 is recommended
- Local Administrator access rights – Required for the user who is installing PROXY Pro Deployment Tool on the machine.
- Microsoft Core XML Services (MSXML) 6.0 – Required. If the Deployment Tool cannot find the redistributable MSXML6 system component, an error message will appear and the navigation tree will be restricted to the single root node. In this case, you must install MSXML6 and restart the Deployment Tool. See http://www.microsoft.com for more information about the redistributable msxml6.msi package.

NOTE: *These prerequisites are met by the supported platforms, and therefore they are not included in the PROXY Pro software distribution packages.*

Operating Requirements

The following requirements are recommended for operation of PROXY Pro Deployment Tool:

◆ Domain Administrator access rights - Because the PROXY Pro Deployment Tool accesses other computers on the network, the tool should be operated with domain administrator credentials. This provides the access rights to manage all of the computers within the domain. If the PROXY Pro Deployment Tool is run from an account that does not have access rights to a computer in your network, a password prompt will appear.

Microsoft Management Console requirements

PROXY Pro Deployment Tool uses the Microsoft Management Console (MMC).

PROXY Pro Deployment Tool stores state information, such as the list of paths to the installation files, product configurations, the network places hierarchy, and the reports, via MMC.

NOTE: *In MMC v2.0, different users of the console file do not share state data. State information is preserved if the PROXY Pro Deployment Tool is uninstalled and later reinstalled.*

Adding the Deployment Tool to the MMC

PROXY Pro Deployment Tool can be added to other console files in MMC by selecting **File > Add/Remove Snap-in** from the MMC menu bar. On the Standalone page of the **Add/Remove Snap-in** dialog that appears, follow these steps:

1. Click **Add** and select PROXY Pro Deployment Tool from the list that appears.
2. Click **Add** and then **Close**.
3. Click **OK** to close the remaining dialog and complete the process.

Target computer requirements

PROXY Pro Deployment Tool can be used to install or uninstall PROXY Pro software (usually PROXY Pro Host) on target computers that meet the following requirements:

◆ Windows Management Instrumentation (WMI) must be installed and the service must be running. This is installed by default for Windows XP and later platforms.

◆ WMI Windows Installer Provider must be installed. For Windows Server 2003, you must explicitly select this optional component. See "WMI Windows Installer Provider installation" below.

◆ Microsoft Windows Networking must be installed and enabled

◆ Remote Procedure Call (RPC) must be enabled on target computers (i.e. standard administrative shares `IPC$` and `ADMIN$` must be accessible).

◆ Your target computers must support authentication of remote users. Under Windows XP Professional on computers that are not members of the domain, there is a local security policy that may prevent this. See “Sharing and security requirements for Windows XP” below for more information. Windows XP Home does not support authentication of remote users and therefore is not supported as a target operating system.

Sharing and security requirements for Windows XP

Follow this procedure to set up a sharing and security policy for local accounts, which is required for Windows XP:

1 Select **Control Panel > Administrative Tools > Local Security Policy**.

2 Under **Security Settings > Local Policies > Security Options > Network access: Sharing and security model for local accounts**, set the value to **Classic - local users authenticate as themselves**.

WMI Windows Installer Provider installation

To install the WMI Windows Installer Provider for Windows Server 2003, follow these steps:

1 Double-click **Add/Remove Programs** in the Control Panel.

2 Select **Add/Remove Windows Components** from the left-hand column.

3 Select **Management & Monitoring Services** in the list.

4 Click **Details**.

5 Check **WMI Windows Installer Provider**.

6 Click **OK**.

7 Click **Next** to complete the installation.

Installation notes

The PROXY Pro Deployment Tool is distributed as part of the *PROXY Pro Workstation Edition or PROXY Pro Gateway Edition* bundles available for download from http://www.proxynetworks.com. Unzip the contents (while preserving the directory tree structure) on your computer.

Click on the *DeploymentTool.msi* file to install the product.

Licensing

PROXY Pro Deployment Tool can be operated without a license key.

Deployment Tool Operation

After installing PROXY Pro Deployment Tool, it can be started by selecting **Start > Programs > Proxy Networks > PROXY Pro Deployment Tool**.

The **PROXY Pro Deployment Tool** window appears:

PROXY Pro Deployment Tool has five main options, which are represented in the left-hand side navigation window:

- "Installation Files", for loading PROXY Pro Host, PROXY Pro Gateway, or PROXY Pro Master installer files to distribute via the Deployment Tool
- "Product Configurations", for creating Windows Installer Transform `.mst` files with custom configuration changes that you wish to push out to remote computers via the Deployment Tool
- "Network Places", for specifying target computers within your network on which to install or uninstall software on (as well as to remotely rebooting any network computer) using NetBIOS commands
- "Active Directory Domains", for discovering remote computers and OUs in your domain, and for installing new PROXY Pro software or upgrading older versions of existing PROXY Pro software
- "Reports", for viewing results of product deployment activities via the Deployment Tool

The general process for loading and distributing software via the Deployment Tool is described in the results pane:

There are five simple steps to deploying PROXY Pro software:

1 Inform the Deployment Tool where the product installation image (i.e. `HOST.MSI`) you wish to use is. Because the Deployment Tool is not tied to a specific release of PROXY Pro, you must have a copy of the version of PROXY Pro you wish to deploy either on the local computer, or on a network share.

2 Create a product configuration, customizing the PROXY Pro Host or PROXY Pro Master settings according to your environment. All of the Host settings are configurable at install time; in addition, installation-time information like User Name, Organization, and License Key can be specified as well.

3a Scan the network for domains and workgroups, then scan a domain or workgroup for computers. This allows the Deployment Tool to remember information about each computer that it gets details on, including what version of PROXY Pro software is installed on that computer, and whether we have access to deploy software to it. Note that unlike the Windows Explorer, the PROXY Pro Deployment Tool does not automatically refresh the "Network Places" collection; you need to manually refresh this list.

- or -

3b Use Active Directory to locate domains, organizational units and computers. This allows the Deployment Tool to remember information about each computer that it gets details on, including what version of PROXY Pro software is installed on that computer, and whether we have access to deploy software to it. As with "Network Places", the PROXY Pro Deployment Tool does not automatically refresh the "Active Directory" collection; you need to manually refresh this list.

4 Having completed step 3a or 3b, you're almost ready to deploy PROXY Pro software. Right-click on a domain or workgroup name under **Network Places**, and pick **Refresh Computer List**, in order to enumerate the computers in the domain or workgroup. Or right-click on a domain under **Active Directory** and pick **Refresh Organizational Units and Computers** to enumerate the domain. Select the domain, workgroup, or org unit, select one or more computers in the list in the result pane, then right-click and pick **Install Software...**. to begin the software deployment process.

5 The results of each Deployment Tool task will be available in a report under the **Reports** node.

NOTE: *If the Deployment Tool cannot find the redistributable MSXML6 system component, an error message will appear and the navigation tree will be restricted to the single root node. In this case, you must install MSXML6 and restart the Deployment Tool. See http://www.microsoft.com for more information about the redistributable msxml6.msi package.*

Installation files

The first step of the software deployment process is to a load either an original PROXY Pro installer file with default configuration settings (e.g. `Host.msi` file for PROXY Pro Host) or a Windows Installer Transform file with custom configuration settings (see "Product Configurations" for more information about creating and loading transform files).

Loading Proxy Installer Files (.msi)

Any of the PROXY Pro .msi files with default configurations can be loaded into PROXY Pro Deployment Tool for distribution to target computers.

To assign one or more installer files for PROXY Pro Host, PROXY Pro Gateway, or PROXY Pro Master, follow these steps:

1 Right-click on **Installation Files** in navigation tree and select **New > Installation File**.

2 Navigate to the directory containing the original product installer (.msi) file for either PROXY Pro Host, PROXY Pro Gateway, or PROXY Pro Master.

3 Select the file(s), and click **Open**. The selected file will be loaded into the Deployment Tool and details will appear in results pane on the right-hand side.

PROXY Pro Deployment Tool
File Action View Window Help
Proxy Deployment Tool
Installation Files
Host.msi
Product Configurations
Network Places
Active Directory Domain
Reports
C:\Documents and Settings\Administrator\Desktop\Proxy-v7-0-0-1506-GatewayEdition\
Create Transform File
Name
Value
File Type
Installation Database
Company
Proxy Networks, Inc.
Product Name
PROXY Pro Host
Upgrade Code
{EA621266-B692-11D4-8526-
Compatible Configuration
Host
Product Version
6.0.0
Comments
PROXY Pro Host v7.0.0.1506
Package Code
{E680DD4F-AEBF-4842-BE7D
Keywords
Installer; MSI; Database
Creating Application
InstallShield® 2008 - Professi
Last Updated By
InstallShield
Code Page
1252
Minimum Installer Version
2.00
Source Image Flags
0x0
Locale
United States (English)
Done

Product Configurations

If you would like to change any configuration settings in the Proxy Installer files before you distribute them, the next step of the software deployment process is to create and load a Windows Installer Transform file with the custom settings you desire.

In order to create a Windows Installer Transform file, you must first create and/or edit a Product Configuration file containing the configuration changes you wish to make for a particular Proxy Installer file. Then you must apply these changes to a Proxy Installer file to create the Transform file.

Creating a new Product Configuration file

Every new Product Configuration file created in PROXY Pro Deployment Tool initially has all configuration options set to default values.

To create a configuration for PROXY Pro Host, Master or Gateway with default configuration options, follow these steps:

1 Right-click on the Product (Host, Master or Gateway) listed under **Product Configurations** for which you intend to create a default configuration.

2 Select **New Configuration**.

3 Enter a name for the configuration and click **OK**.

A new node for this named configuration appears in the left-hand navigation tree under the Product that you selected.

Changing Configuration Settings in the Product Configuration file

Initially, the Product Configuration file starts off with all default values. To modify one or more of these, double click on the setting in the result pane and select the desired setting in the resulting popup window.

1 Select the configuration to modify. All configurations parameters are listed on the right-hand side of the Deployment Tool.

2 Double-click the configuration parameter you want to modify. When a properties dialog appears, select any options you want. If you select **Use current value or installation default,** then the parameter is assigned according to the following:

- If an existing installation with a configured value for this parameter already exists (for upgrades), the existing installation parameter value is retained.
- The default installation configuration options for the selected parameter are used either when an existing installation does not yet have a value for this parameter or for new installations.

3 Click **OK** when you are done.

Once you apply the change, the new setting will be reflected in the result pane of the Product Configuration file.

For more information about specific configuration settings for PROXY Pro Host, Master or Gateway, see:

- “Configuration options for the Host”
- “Configuration options for the Master”
- “Configuration options for the Gateway”

Creating Windows Installer Transform file

You are now ready to create a Windows Installer Transform file:

1 Right-click on a Product Configuration file in the navigation tree and select **New > Transform File**.

2 In the first dropdown box, find the original Proxy Installer (.msi) file corresponding to the type of Product Configuration file you selected in the left-hand navigation box (this should have been loaded in the first step of this process (see "Installation Files").

3 Input a filename for the new Windows Installer Transform file and click **OK** to create new Windows Installer Transform file.

The new Windows Installer Transform file will appear in the left-hand navigation under **Installation File.** Note that configuration settings that have been changed will show new setting in the Value column and Default flag will be set to "No".

You can now proceed to either Network Places or Active Directory Domains to select target computers and deploy either the original Proxy Installer file or the new Windows Installer Transform file.

Create new configurations

Every new configuration created in PROXY Pro Deployment Tool initially has all configuration options set to default values.

To create a configuration for PROXY Pro Host, Master or Gateway with default configuration options, follow these steps:

1 Right-click the application (PROXY Pro Host, Master or Gateway) listed under Product **Configurations** for which you intend to create a default configuration.

2 Select **New > Configuration**.

3 Enter a name for the configuration and click **OK**.

A new node for this named configuration appears in PROXY Pro Deployment Tool. The configuration options currently all have default values. To modify these, follow the instructions in “Create custom configurations”.

For the PROXY Pro Host product, you can also choose **New > Terminal Services Configuration**. This configuration file will be applied to the Terminal Services Template instead of the standard root Host settings.

Note: Some Host settings do not apply to the Terminal Services Template, and will appear disabled on the right-hand side of PROXY Pro Deployment Tool.

Create custom configurations

After creating a named configuration for PROXY Pro Host, Master, or Gateway, any options can be modified.

To modify a configuration in PROXY Pro Deployment Tool, follow these steps: PROXY Pro Deployment Tool Guide

1 Select the configuration to modify. All configurations parameters are listed on the right-hand side of PROXY Pro Deployment Tool.

2 Double-click the configuration parameter you want to modify. When a properties dialog appears, select any options you want. If you select **Use current value or installation default**, then the parameter is assigned according to the following:

◆ If an existing installation with a configured value for this parameter already exists (for upgrades), the existing installation parameter value is retained.

◆ The default installation configuration options for the selected parameter are used either when an existing installation does not yet have a value for this parameter or for new installations.

3 Click **OK** when you are done.

See the following topics:

◆ "Configuration options for the Master"

◆ "Configuration options for the Host"

◆ "Configuration options for the Gateway"

Configuration options for the Master

Modify the following configuration options for PROXY Pro Master:

◆ **Add/Remove in Control Panel**: Set this option to **Disable** to prevent users from modifying the PROXY Pro Master configuration.

◆ **Installation Directory**: Specify an installation directory other than the default.

◆ **License**: Specify your product license here. Note that the Master does not use a "version upgrade" license, so only one license key is required – your full product or subscription upgrade key. Keys from previous versions are not accepted by the Master, and should not be entered.

◆ **Organization**: Change the organization name that is shown when you select **Help > About PROXY Pro Master**.

◆ **Restart after Installation**: After installing with PROXY Pro Deployment Tool, PROXY Pro Master reboots only if necessary. If a reboot is required, it occurs without any prompts. You can suppress the automatic reboot without prompting by selecting **Use this value** and the **Reallysuppress** option.

◆ **User Name**: Change the licensee name from the default (Windows) user name with this option. This is the registered user name that is displayed when you select **Help > About PROXY Pro Master.**

Configuration options for the Host

Most of the configuration options in the PROXY Pro Host Control Panel window can be modified. These options are related to the `PHSetup` commands that you execute from a command line. For more information, see the *PROXY Pro Host Guide*.

Modify the following configuration options for PROXY Pro Host:

Access tab

- **Access Restrictions**: Specify the remote access policy:
  - Select **Permit connection** to permit remote connections from authenticated PROXY Pro Master users to your Host computer.
  - Select **Lock out connection** to prevent any remote connections from PROXY Pro Master users to your Host computer.
  - Select **Lock out or Permit connection based on time zone** to permit or refuse remote connections to your Host computer based on the day of the week and the time of day. You can specify permitted access by time when you click **Time Zone Settings**.
- **Connection Permissions**: You can optionally specify that you require or allow the Host computer operator to grant remote access permission to the Host computer. If you require this feature, you can change the **Grant Permission Time**. If you allow for this feature, you change the **Request Permission Time**.
  - Select **No permission required** (default) to allow remote connection to your Host computer from anyone who satisfies restrictions you specify as authentication security settings.
  - Select **Permission must be granted by Host** if you want to know when a remote user attempts a connection. From the **Host's user must respond within** list, select the time within which you must accept or reject a request. When a remote connection is requested, the Request Permission for Remote Desktop Window appears. You can accept or reject the request. If you do not respond within the specified time, the request is rejected automatically.
  - Select **Permission requested from Host** if you want to know when a remote user attempts a connection. From the **connection continues after** list, select the time after which the connection will be made. When a remote connection is requested, the Request Permission for Remote Desktop Window appears. You can accept or reject the request. If you do not respond within the specified time, the request is accepted automatically.
  - Select **Lock workstation if permission not explicitly granted** if you want the Host to lock the workstation prior to beginning a new remote control connection (if user is bypassing Host permission). This prevents the new user from "hijacking" the logged-in user's session unless he/she knows the credentials to unlock it.
- **Grant Permission Time**: Specify the period before the time-out when you require the Host computer operator to grant remote access permission to the Host computer.
- **Lock Workstation on Default**: If "Yes", the workstation is locked if the "Permission to connect" dialog times out. The workstation is not locked if the console user responds to the dialog. If "No", the workstation is never locked.

- **Request Permission Time**: Specify the period before the time-out when you allow the Host computer operator to grant remote access permission to the Host computer.
- **Time Zone**: Specify the period for remote access.

Effects tab

- **Manage Visual Effects**: Specify the how visual effects features are remotely controlled.
- **Effects**: Sets the flags for the management of visual effects. Checking a box for a category causes that category of effects to be disabled during a connection.

Gateways tab

- **Gateways**: List the Gateways to which this Host computer reports. These PROXY Pro Gateways must already be deployed in your network.
- **Require Gateway**: Require that all remote connections through this Host computer be conducted through the listed PROXY Pro Gateway or servers.

General tab

- **Beep on Connect/Disconnect:** Request to hear a quick series of three tones rising in pitch whenever a remote connection succeeds. With this option, you also hear a series of tones falling in pitch when the remote connection is terminated.
- **Beep While Connected?** Request to hear a short tone periodically, throughout the duration of any remote connection. You can set the interval between beeps from 0 to 9999 seconds. If you set this field to 0, then it turns the beeping off completely.
- **Extension Tags:** Displays any name/value pairs specifying custom information for this Host.
- **Host Notifications**: Sets the flags for enabling/disabling host notification popups. Checking a box enables that class of notifications. Unchecking a box disables that class of notifications.
- **Show icon while connected?**: Display (or hide) the PROXY Pro Host tray icon when the service is running and there is an active remote connection.
- **Show icon while idle?**: Display (or hide) the PROXY Pro Host tray icon when the service is running but there is no active remote connection.
- **Station Name**: Modify the name by which your Host computer identifies itself to PROXY Pro Gateways or PROXY Pro Master users.

Host station name macros are now supported. The Host station name can include strings in the form %MACRO%, and these macros are substituted at runtime for the correct values. This complements the $MACRO$ feature in PHSETUP, which provides a one-time substitution at PHSETUP runtime.

This feature may be useful when creating a Host image for deployment, either using the Deployment Tool or via imaging of the entire disk. The macro names supported are:

Macro	Description
%NAME%	Host computer machine name
%USER%	Logged in user at the Host machine console
%USERNAME%	Logged in user at the Host machine console in “<username>” only format

%VER%	Host software version number (e.g. “v5.10.2.1003”)
%INTVER%	Internal Host software version number
%PID%	Process ID of the Host service
%PLATFORM%	Host operating system platform (e.g. “Win2000”)
%PROT%	Network protocol (e.g. “IP” or “TCP”)
%ADDR%	Network address (e.g. “192.168.0.15”)
%PORT%	Network port (e.g. “1505”)

Installation group

- **"Add or Remove Programs" list in Control Panel**: Setting this value to "disable" will disable the ability to Add/Remove/Modify the product via the system control panel. Do not set this value to have the product appear in the Add/Remove Programs listing.
- **Installation Directory**: Specify an alternate to the default installation directory.
- **License**: Specify your product license here. Note that the Host does not use a “version upgrade” license, so only one license key is required – your full product or subscription upgrade key. Keys from previous versions are not accepted by the Host, and should not be entered.
- **Organization**: Allows you to override the default organization with a new value.
- **Restart after Installation**: After installing with PROXY Pro Deployment Tool, PROXY Pro Host reboots only if necessary. Suppress the automatic reboot without prompting by selecting **Use this value** and the **Reallysuppress** option.
- **User Name**: Allows you to override the default username with a new value.

Options tab

- **Lock Workstation on Disconnect**: Lock the Host computer when the remote user connection is terminated (it can be unlocked or restarted using Windows commands).
- **Reboot on Disconnect:** Reboot the Host computer when the remote user connection is terminated.
- **Suppress Keys: C**ontrol how the keyboard and mouse of your Host computer behave during remote connection:
  - Select **Never suppress the local keyboard and mouse** to retain control of the Host computer’s keyboard and mouse when a remote user connects to the Host.
  - Select **Suppress local input, if the Master requests it** to give a remote user control of the Host computer’s keyboard and mouse when the remote user requests it. The default settings for PROXY Pro Host and PROXY Pro Master allow the mouse and keyboard to be shared during a connection, with each side able to use both.
  - Select **Suppress the local keyboard and mouse at system startup** to give full control of the Host computer’s keyboard and mouse to the remote user who connects to the Host. This option does not permit mouse or keyboard input on the Host computer.

Protocols tab

- **Access Restriction Addresses**: Sets the TCP/IP restricted addresses
- **Access Restriction Mode**: Sets "Grant" or "Deny" access to the Host based on TCP/IP addresses specified by "tcprestrictions"
- **Enable IPX Protocol**: Allow access to Host through IPX configuration
- **Enable TCP Protocol**: Allow access to Host through TCP configuration
- **Enable UPD/IP Protocol**: Allow access to Host through UDP configuration
- **Encrypt Connection**: Turn on encryption, as defined in Preferred Ciphers, for connections to this Host
- **Port Number for IP**: Allow access through IP protocol using this port number
- **Port Number for IPX**: Allow access through IPX protocol using this port number
- **Port Number for TCP**: Allow access through TCP protocol using this port number
- **Preferred Ciphers**: Use ciphers in order of specification in this list for encrypting connections to this Host

Screen tab

- **Allow Kernel Mode screen capture**: Allow Gateway connections to use kernel-mode screen capture driver, even if user-mode driver is preferred.
- **Attach Kernel Mode mirror display driver at Startup**: Attach kernel-mode driver to the desktop when Host service starts up to avoid screen flashing (applies when Allow Kernel Mode screen capture option is enabled)
- **Prefer User Mode screen capture**: Uses user-mode driver to capture screen data. This is the default option on all platforms.
- **Select User Mode Profile**: Create your own user mode profile with the following bandwidth throttling options:
  - **Description string**: Enter a name for this custom profile
  - **Image type**: Current default value is “JPEG”
  - **Image compression quality**: Specify a numeric value between 1-100, with 100 being best quality
  - **Polling frequencies** (three values -- Capture Rate, Foreground, and Background, in milliseconds): Specify three values on a scale of 1 to 10, with 1 being the least aggressive (longest time), and 10 being the most aggressive (shortest time).
  - **Bandwidth limit**: Specify a numeric value between 5-200 kilobytes/sec, or -1 for unlimited.

Security tab

- **Administration Password**: Sets simple password required for administration, if Windows Authentication isn't used.
- **Administration Password Required**: If "same", then the connection password is used for administration access and any Administration Password setting is ignored. If "different", then the Administration Password is used for administration access.
- **Administration Security**: Specify PROXY Pro Host administrative security settings when you use Windows security for remote connections.

- **Allow Remote Administration**: Specify whether to allow the settings to be changed by a remote administrator.
- **Host Settings Security**: Specify PROXY Pro Host security settings when you use Windows security for remote connections.
- **Service Security**: Specify PROXY Pro Host service security settings when you use Windows security for remote connections.
- **Use Windows Authentication**: Use Windows security for remote connection administration.

Terminal Services tab

- **Provide Host services for Citrix XenApp 'desktop' sessions only**: Inject Host instances into virtual desktop sessions only (otherwise inject Host instances into all terminal services sessions).
- **Terminal Services Template**: Apply the settings in this Configuration file to the Terminal Services Template (otherwise, the settings defined will apply to the root Host).
- **Terminal Services Users**: Specify which Terminal Services session users get a Host instance when they log in.

Configuration options for the Gateway

Modify the following options for PROXY Pro Gateway:

- **Components to install**: Install one or both (default) of the following:
  - The server, PROXY Pro Gateway (Select **Use this value > Server**)
  - The administration tool, PROXY Pro Gateway Administrator (Select **Use this value > Administration**)
- **Gateway server account name**: The Gateway server account name is required for new installations and ignored for upgrades of PROXY Pro Gateway. Type an alternate to the default domain account used by the PROXY Pro Gateway, by selecting **Use this value**. Configure full security rights for this domain account in any PROXY Pro Host configuration that uses this PROXY Pro Gateway to administer all remote connections.
- **Gateway server account password**: Specify the password for the domain account used for the PROXY Pro Gateway. This password is required for new installations and ignored for upgrades of PROXY Pro Gateway.
- **Add/Remove Programs list in Control Panel**: Set this option to **Disable** to prevent users from modifying the PROXY Pro Gateway configuration.
- **Installation Directory**: Specify a non-default installation directory.
- **License**: Specify your product license here. Note that the upgrade process preserves any previously installed licenses to deployments of PROXY Pro Gateway, and none of these licenses should be deleted on the product.
- **Organization**: Change the organization name that is displayed when you right-click **Remote Control Gateway Servers > About**.
- **Restart after installation**: After installing with PROXY Pro Deployment Tool, PROXY Pro Gateway reboots only if necessary. If a reboot is required, it occurs without any prompts. You can suppress the automatic reboot without prompting by selecting **Use this value** and the **Reallysuppress** option.

- **User Name**: Change the licensee name from the default (Windows) user name with this option. This is the registered user name that is displayed when you right-click **Remote Control Gateway Servers > About**.

Network Places

Once you have loaded your Proxy Installer file(s) and/or your Windows Installer Transform file(s), you can go to **Network Places** to specify the list of target computers for deployment. Network Places uses NetBIOS to discover and provide access to remote computers in your domain or workgroup.

Once you select the target computers, you can use the Deployment Tool to install, uninstall Proxy software or push configuration settings.

Add computer

Network Places uses NetBIOS to discover and provide access to remote computers in your domain or workgroup. If the target computer(s) do not appear, you can explicitly add a computer to the Deployment Tool navigation tree.

Follow these steps add a target computer:

1 Right-click on the domain or workgroup that contains the target computer. Select the **Add Computer...** command:

2 In the dialog box that appears, enter the DNS name of the target computer or the IP address. If the account you are using doesn't have administrator privileges on the target computer, you may need to enter the credentials of an account that does.

The target computer will appear under the domain or workgroup in the left pane navigation tree.

Specify target computers for install or uninstall

To update the list the domains and workgroups, right-click **Network Places** and select **Refresh Domain/Workgroup List**. Information appears in the left and right panes:

- The left pane provides each domain and workgroup name only.
- The right pane provides the name of each domain and workgroup, along with additional columns for the number of times it was found, the date it was found, and the number of computers in it.

To obtain information about the computers in a domain or workgroup, right-click the domain or workgroup and select **Refresh Computer List**. Then expand the domain or workgroup to see the computers in it.

Select one or more computers in the results pane, right-click on one of the highlighted computers to bring up the context menu. It is recommended that you click on Refresh Details first, to ensure that necessary requirements are in place for other tasks.

Refresh Details

Click **Refresh Details** to refresh the deployment details for the selected computer(s). Check to see if a version of the software you are interested in deploying is already on the target computer(s). Also, check to see if the prerequisites for deployment are met (click on **show details** to see the state of specific requirements, including access to WMI and RPC (IPC$). If prerequisites for deployment are met, the **Can Deploy?** field will indicate

"Yes". If these are not met, you must enable them in order for the Deployment Tool to access the remote computer (see "Target computer requirements").

A prompt for credentials may appear, if you are not logged in with the proper credentials to view or modify one or more of your network computers. It is recommended that you use domain administrator credentials with the Deployment Tool (see "Operating requirements").

Install Software

If the **Can Deploy?** field value is "Yes", then you can proceed to install software on that target computer. Click **Install Software** to install one of your configurations on the selected computer. The **Install Software** window appears**.**

◆ To install a default .msi configuration file for either PROXY Pro Host, Master, or Gateway on the selected computer, select the preloaded Proxy Installer file under **Installation File Name**, and select **No additional modifications**.

◆ To install a customized `.msi` configuration file for PROXY Pro Host, Master, or Gateway on the selected computer, select the preloaded Proxy Installer file under **Installation File Name**, and select a preloaded Product Configuration file under **Configuration Name**.

◆ To install an `.mst` configuration file for PROXY Pro Host, Master, or Gateway on the selected computer, create an `.mst` file from your custom Product Configuration file. Then select the Proxy Installer file under **Installation File Name**, and select the Windows Installer Transform file under **Transform File Name**.

Select one of the **Computer Restart Options** before clicking **OK**.

The Deployment Tool will proceed to deploy the specified Proxy Installer file with any additional modifications, and will generate a deployment report that will appear under Reports.

Update Host Settings

If PROXY Pro Host is installed on the target computer(s), the Deployment Tool can be used to change Host settings without having to reinstall the Host software itself (e.g. add a Gateway entry to Gateway tab on one or more target computers).

Follow these steps to update Host settings:

1 Create a new Product Configuration file and include the new Host settings you wish to push to the target computer(s) (see "Product Configurations")

2 Click **Update Host Settings** and in the popup dialog box, select the Product Configuration file you created above in the dropdown box next to **Configuration Name**.

3 By default, PROXY Pro Host is set to listen on port 1505 over TCP/IP; if the Host on the remote computer you are trying to reach has been configured to listen on a different protocol/port combination, enter the new values.

4 You should be using a domain account that has administrative rights on the remote computer you are trying to reach (such as Domain Administrator credentials). If the Host on the target computer is configured for simple password authentication, you can enter the password here.

5 Click **OK** to push the Host settings specified in the Product Configuration file to the target computer.

Restart Computer

Click **Restart** to restart the target computer.

Remove Software

Click **Remove Software** to remove PROXY Pro Host, Master, or Gateway on the selected computer. The Remove Software window appears. Select the product to remove and click **OK**. The Deployment Tool will attempt to uninstall and delete any Proxy Installer files or Windows Installer Transform files corresponding to the type of software you have selected.

Upgrade Software

If older version of Proxy software is installed on target computer(s), and a newer version is loaded into the Deployment Tool, the Deployment Tool will attempt to execute a product upgrade when **Install Software** is selected.

If **No additional modifications** is selected, existing configuration settings will be retained, while new product configuration values are specified for new features. If either a Transform file or Product Configuration file is specified, new settings will replace existing settings during the upgrade.

Install/uninstall Host, Master or Gateway

PROXY Pro Host, Master, or Gateway can be deployed to any selected computer by viewing its details.

Rather than deploying a configuration one-at-a-time, multiple workstations can be selected in the right-hand results view when you select a domain or workgroup name in the tree. After multi-selecting the desired workstations (by pressing Shift+Click and Ctrl+Click), right-click and select any of the options available on a single computer, for example, **Refresh Details**, **Install Software**, **Restart Computer**, or **Remove Software**.
To view the details of a selected computer in your domain or workgroup, right-click the computer and select **Refresh Details**.

Use the window to perform the following tasks:

- "Refresh details"
- "Install software"
- "Remove software"
- "Restart"

Refresh details

Click **Refresh Details** to refresh the deployment details for the selected computer.

Install software

Click **Install Software** to install one of your configurations on the selected computer. The **Install Software window** appears.

◆ To install a default .msi configuration file for either PROXY Pro Host, Master, or Gateway on the selected computer, select the installation file under Installation File Name, and do not change any Select modifications to install settings.
◆ To install a customized .msi configuration file for PROXY Pro Host, Master, or Gateway on the selected computer, select the installation file under Installation File Name, and select a customized named configuration under Configuration Name.
◆ To install an .mst configuration file for PROXY Pro Host, Master, or Gateway on the selected computer, create an .mst file from your customized configuration. Then select the installation file under Installation File Name, and select a file name under Transform File Name.
◆ Select one of the Computer Restart Options before clicking OK.

Remove software

Click **Remove Software** to remove PROXY Pro Host, Master, or Gateway on the selected computer. The Remove Software window appears. Select the product to remove and click **OK.**

Restart

Click **Restart** to restart the selected computer.

Active Directory Domains

Once you have loaded your Proxy Installer file(s) and/or your Windows Installer Transform file(s), you can go to **Active Directory Domains** to specify the list of target computers for deployment. Once you select the target computers, you can use the Deployment Tool to install, uninstall Proxy software or push configuration settings.

Specify target computers for install or uninstall

Active Directory Domains uses Active Directory to discover and provide access to remote computers in your domain or in a foreign domain that you specify.

To list the domains in your domain, right-click **Active Directory Domains** and select **Refresh Local Domains**. To list the domains in a foreign domain, right-click **Active Directory Domains** and select **Add Foreign Domains...** Enter domain credentials to get access to the foreign domain.

Any domains discovered will appear in the lefthand navigation window:

- The left pane provides each domain
- The right pane provides the name of each domain, along with additional columns for the number of times it was found, the date it was found, and the number of computers in it.

To obtain information about the computers in a domain, right-click the domain and select **Refresh Organizational Units and Computers**. Then expand the domain to see the computers in it.

Select one or more computers in the results pane, right-click on one of the highlighted computers to bring up the context menu. It is recommended that you click on Refresh Details first, to ensure that necessary requirements are in place for other tasks.

Refresh Details

Click **Refresh Details** to refresh the deployment details for the selected computer(s). Check to see if a version of the software you are interested in deploying is already on the target computer(s). Also, check to see if the prerequisites for deployment are met (click on **show details** to see the state of specific requirements, including access to WMI and RPC (IPC$). If prerequisites for deployment are met, the **Can Deploy?** field will indicate "Yes". If these are not met, you must enable them in order for the Deployment Tool to access the remote computer (see "Target computer requirements").

A prompt for credentials may appear, if you are not logged in with the proper credentials to view or modify one or more of your network computers. It is recommended that you use domain administrator credentials with the Deployment Tool (see "Operating requirements").

Install Software

If the **Can Deploy?** field value is "Yes", then you can proceed to install software on that target computer. Click **Install Software** to install one of your configurations on the selected computer. The **Install Software** window appears**.**

◆ To install a default .msi configuration file for either PROXY Pro Host, Master, or Gateway on the selected computer, select the preloaded Proxy Installer file under **Installation File Name**, and select **No additional modifications**.

◆ To install a customized `.msi` configuration file for PROXY Pro Host, Master, or Gateway on the selected computer, select the preloaded Proxy Installer file under **Installation File Name**, and select a preloaded Product Configuration file under **Configuration Name**.

◆ To install an `.mst` configuration file for PROXY Pro Host, Master, or Gateway on the selected computer, create an `.mst` file from your custom Product Configuration file. Then select the Proxy Installer file under **Installation File Name**, and select the Windows Installer Transform file under **Transform File Name**.

Select one of the **Computer Restart Options** before clicking **OK**.

The Deployment Tool will proceed to deploy the specified Proxy Installer file with any additional modifications, and will generate a deployment report that will appear under Reports.

Update Host Settings

If PROXY Pro Host is installed on the target computer(s), the Deployment Tool can be used to change Host settings without having to reinstall the Host software itself (e.g. add a Gateway entry to Gateway tab on one or more target computers).

Follow these steps to update Host settings:

1 Create a new Product Configuration file and include the new Host settings you wish to push to the target computer(s) (see "Product Configurations")

2 Click **Update Host Settings** and in the popup dialog box, select the Product Configuration file you created above in the dropdown box next to **Configuration Name**.

3 By default, PROXY Pro Host is set to listen on port 1505 over TCP/IP; if the Host on the remote computer you are trying to reach has been configured to listen on a different protocol/port combination, enter the new values.

4 You should be using a domain account that has administrative rights on the remote computer you are trying to reach (such as Domain Administrator credentials). If the Host on the target computer is configured for simple password authentication, you can enter the password here.

5 Click **OK** to push the Host settings specified in the Product Configuration file to the target computer.

Restart Computer

Click **Restart** to restart the target computer.

Remove Software

Click **Remove Software** to remove PROXY Pro Host, Master, or Gateway on the selected computer. The Remove Software window appears. Select the product to remove and click **OK**. The Deployment Tool will attempt to uninstall and delete any Proxy Installer files or Windows Installer Transform files corresponding to the type of software you have selected.

Upgrade Software

If older version of Proxy software is installed on target computer(s), and a newer version is loaded into the Deployment Tool, the Deployment Tool will attempt to execute a product upgrade when **Install Software** is selected.

If **No additional modifications** is selected, existing configuration settings will be retained, while new product configuration values are specified for new features. If either a Transform file or Product Configuration file is specified, new settings will replace existing settings during the upgrade.

Reports

The Deployment Tool generates a brief summary for each action taken in either **Network Places** or Active Directory Domains, and stores the summary in a time-stamped folder under **Reports.**

The **Reports** folder can contain summaries for each of the five different types of action available, including:

- **Computer Details** folder which shows results of **Refresh Details** action.
- **Software Installations** folder which shows results of **Install Software** action.
- **Remove Software** folder which shows results of **Remove Software** action.
- **Restart Computer** folder which shows results of **Restart Computer** action.
- **Update Host Settings** folder which shows results of **Update Host Settings** action.

In the example, below, a summary of a successful **Refresh Details** action for computer VM1 in the TestDomain domain is shown:

Troubleshooting

Troubleshooting tips are provided for the following issues:

- "Authentication failure"
- "Trouble installing software or refreshing details on Windows XP"
- "Trouble installing/removing software to/from a computer"
- "Generate unique HostIDs"
- "Remove duplicate HostIDs"

Authentication failure

If you experience authentication failure, carefully check your authentication credentials. You must have administration rights on the target computer to install software.

Trouble installing software or refreshing details on Windows XP

The local security policy Network access: Sharing and security model for local accounts can prevent remote access to the administrative shares and WMI.

It is possible that you cannot refresh details or install the software on a target networked Windows XP computer that is a workgroup member.

See “Target computer requirements” for the correct configuration details.

Trouble installing/removing software to/from a computer

If you address all requirements in "Target computer requirements", you should not have any problems installing or removing software.

If you are unable to install or remove software from a target computer, confirm that the following are installed and active on the target computer:

◆ Microsoft Networking `IPC$` share: Check that this share is displayed on the target computer.

◆ Microsoft Networking `ADMIN$` share: Check that this share is displayed on the target computer. To do this, open Windows Explorer and type *<target_machine>**admin$* and check to see that you don't get any type of access error.

◆ Windows Management Instrumentation (WMI): Check that the WMI service is started. You can test that the target machine has WMI available and installed properly by using Microsoft's built-in tool WMIC. In a command prompt, type "WMIC". From the resulting prompt, type the following command to confirm WMI access:

```
wmic /node:<target machine> /user:<username> /password:<password>
```

◆ WMI Windows Installer Provider: This is an option for Windows Server 2003. See "WMI Windows Installer Provider installation" for information on how to install this option.

Note: "*Error: WMI: Provider load failure (0x80041013)" and "Error: WMI: Invalid class (0x80041010)" are indicative of the optional "WMI Windows Installer Provider" not being installed on Windows Server 2003. Go to Add or Remove Programs, Add/Remove Windows Components, Management and Monitoring Tools, Details and check WMI Windows Installer Provider.*

Generate unique HostIDs

Each PROXY Pro Host installation is identified by a unique identifier, called the HostID. This identifier is used by the PROXY Pro Gateway to identify a Host, even as other information about the Host, such as the machine name, may change. This identifier contains no additional information and has no use other than to allow the PROXY Pro Gateway to identify individual Hosts on the network. The HostID is a *GUID*, a 16-byte number with a text representation like "{C8E645A4-AF10-46f7-838B-A75105C8AA13}".

Issues arise with operating system imaging, the process by which an operating system is installed on one machine and then replicated to other remote computers. Typically, a third-party utility program, such as Symantec Norton Ghost ™ or PowerQuest Drive Image, is used for operating system imaging.

If PROXY Pro Host is installed on an operating system that is then imaged, all of the remote computers will end up with the same HostID. PROXY Pro Gateway will recognize the first Host it sees with this HostID, but ignore any others with the same HostID. The result is that many Hosts will not show up in the PROXY Pro Gateway directory.

There are two strategies for dealing with this issue:

◆ The preferred solution is to prepare the Host installation for imaging before creating the operating system snapshot to be duplicated. Just as you use the Microsoft-provided "SysPrep" utility to prepare the operating system, you can use the PROXY Pro Host "HostPrep" utility to prepare the Host before imaging. This is described in the next section.

◆ If a deployment has been completed and duplicate HostIDs exist on the network, the PROXY Pro Host "RmHostID" utility can be used to remove the duplicate HostIDs and cause the affected remote computers to be assigned a new (and unique) ID. This is described later in this document.

Prepare the Host and operating system for imaging

PROXY Pro Host includes a utility program named `hostprep.exe` to address issues with operating system imaging. The Hostprep utility is available in the *PROXY Pro Utilities* file.

To avoid the problem of having duplicate HostIDs, you must run the `hostprep` utility to delete the ID before the operating system image is captured.

NOTE: *You must prepare the Host software for imaging just before you use the Microsoft-provided SysPrep utility to prepare the operating system.*

After the machine is set up and all Host settings are configured, and immediately before running the Microsoft-provided SysPrep utility, run the `hostprep.exe` utility from a command prompt. The optional command line argument "`-y`" can be used to avoid a prompt to continue. When HostPrep runs, it stops the Host service and prepares the Host for imaging. It is critical that the Host service not restart before the operating system image is captured because when the Host starts, it undoes the actions completed by the HostPrep utility.

For more information about operating system imaging, please see the Microsoft TechNet Desktop Deployment Center at

`http://www.microsoft.com/technet/desktopdeployment/`

HostPrep command line syntax

HostPrep accepts a command line flags that control its behavior:

- -y do not ask for confirmation; default is to prompt before continuing
- -yes same as '-y'
- -guid deletes the HostID only, but does not prepare the settings
- -restart restarts the Host Service when compute; should only be used with '-guid'

To prepare an installation for imaging, run `hostprep.exe` with no arguments, and press the "y" key when prompted.

To delete the HostID on the local computer and cause a new one to be assigned immediately, run the command line "`hostprep.exe –guid –restart`".

HostPrep runs on all of the operating systems supported by the PROXY Pro Host.

Remove duplicate HostIDs

The RmHostID utility is available in the *PROXY Pro Utilities* file.

The RmHostID utility runs on one computer and searches one or more computers for Host installations that have a specified HostID. If a matching HostID is found, the HostID is deleted and the Host Service restarted so that a new ID will be assigned. This utility can be used to “clean up” Host installations with duplicate IDs on a LAN.

RmHostID command line syntax

RmHostID accepts command line flags that control its behavior:

- -p prompt for confirmation before deleting HostID
- -prompt same as ‘-p’
- -? displays help text describing how to use RmHostID

RmHostID expects two arguments (in addition to any flags) on its command line. The first argument specifies which HostIDs should be considered duplicates, and therefore should be deleted. The second argument specifies which machine or remote computers should be examined.

The HostID specification (first argument) can be one of:

- A specific GUID, in the form “{C8E645A4-AF10-46f7-838B-A75105C8AA13}”
- A star (“*”), signifying that all HostIDs found should be deleted
- An at sign (“@”) followed immediately by a filename. This causes the specified file to be read, and each line should contain a single GUID.

The machine’s specification (second argument) can be one of:

- If the machine specification is missing, the local machine is checked
- A specific machine name, as either a NetBIOS machine name or a DNS name
- A star (“*”), which instructs RmHostID to enumerate all remote computers on the network
- An at sign (“@”) followed immediately by a filename. This causes the specified file to be read, and each line should contain a single machine name (as either a NetBIOS machine name or a DNS name).

Examples:

- RmHostId {078A9A01-6931-42A3-9371-EA00F1DC7D99} *

This example enumerates the remote computers on the network, and deletes the HostID of any installations that match the specified ID.

- RmHostId {078A9A01-6931-42A3-9371-EA00F1DC7D99} MACHINE04

This example connects to the one machine named “Machine04”, and deletes the HostID on that machine if and only if it matches the specified ID.

- RmHostId * MACHINE04

This example connects to the one machine “Machine04”, and deletes the HostID unconditionally, because “*” was specified as the HostID pattern.

- RmHostId GUIDS.TXT *

This example enumerates the remote computers on the network, and deletes the HostID of any installations that match any of the IDs specified in the GUIDS.TXT file.

- Example `GUIDS.TXT` file:
    - {078A9A01-6931-42A3-9371-EA00F1DC7D99}
    - {078A9A02-6931-42A3-9371-EA00F1DC7D99}

Requirements for RmHostID

The user must be logged in as Administrator, or otherwise have access permissions to the ADMIN$ share on the Host remote computers.

The Host remote computers must allow remote access to the Service Control Manager and to the Registry. Typically, this means that Microsoft File & Printer Sharing is enabled and that these services are not blocked by a firewall.

Enumerating remote computers on the network with "*" can take some time; this utility uses the same algorithm and APIs to enumerate the network as the PROXY Pro Deployment Tool.

Host GUIDs can be obtained by copying from:

- the Host Control Panel **Gateways** tab
- the Gateway Administrator Host Properties **General** tab
- the registry on an affected machine in HKCR\Proxy.Host\HostID\GUID