Symantec pcAnywhere™ Administrator’s Guide

Symantec pcAnywhere™

Symantec pcAnywhere™ Administrator's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 10.0

PN: 07-30-00453

Copyright Notice

ALL EXAMPLES WITH NAMES, COMPANY NAMES, OR COMPANIES THAT APPEAR IN THIS GUIDE ARE FICTICIOUS AND DO NOT REFER TO, OR PORTRAY, IN NAME OR SUBSTANCE, ANY ACTUAL NAMES, ORGANIZATIONS, ENTITIES, OR INSTITUTIONS. ANY RESEMBLANCE TO ANY REAL PERSON, ORGANIZATION, ENTITY, OR INSTITUTION IS PURELY COINCIDENTAL.

Every effort has been made to ensure the accuracy of this guide. However, Symantec makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Symantec shall not be liable for any errors or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this document is subject to change without notice.

Trademarks

Symantec pcAnywhere, Symantec, the Symantec logo, ColorScale, and SpeedSend, are U.S. registered trademarks of Symantec Corporation.

Microsoft, MS, Windows, Windows NT, Word, and the Office logo are either registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries.

Other product names mentioned in this guide may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

NOTICE:

Symantec licenses the accompanying software to you only upon the condition that you accept all of the terms contained in this license agreement. Please read the terms carefully before continuing installation, as pressing the "Yes" button will indicate your assent to them. If you do not agree to these terms, please press the "No" button to exit install as Symantec is unwilling to license the software to you, in which event you should return the full product with proof of purchase to the dealer from whom it was acquired within sixty days of purchase, and your money will be refunded.

LICENSE AND WARRANTY:

The software which accompanies this license (the "Software") is the property of Symantec or its licensers and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. Except as may be modified by a license addendum which accompanies this license, your rights and obligations with respect to the use of this Software are as follows:

YOU MAY:

(i) use one copy of the Software on a single computer;

(ii) make one copy of the Software for archival purposes, or copy the software onto the hard disk of your computer and retain the original for archival purposes;

(iii) use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;

(iv) after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this agreement; and

(v) if a single person uses the computer on which the Software is installed at least 80% of the time, then after returning the completed product registration card which accompanies the Software, that person may also use the Software on a single home computer.

YOU MAY NOT:

(i) copy the documentation which accompanies the Software;

(ii) sublicense, rent or lease any portion of the Software;

(iii) reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software; or

(iv) use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version as a replacement of the prior version, unless you donate a previous version of an upgraded version to a charity of your choice, and such charity agrees in writing that it will be the sole end user of the product, and that it will abide by the terms of this agreement. Unless you so donate a previous version of an upgraded version, upon upgrading the Software, all copies of the prior version must be destroyed.

SIXTY DAY MONEY BACK GUARANTEE:

If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or an authorized dealer, postage prepaid, for a full refund at any time during the sixty day period following the delivery to you of the Software.

LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

The above warranty is exclusive and in lieu of all other warranties, whether express or implied, including the implied warranties of merchantability, fitness for a particular purpose and noninfringement. This warranty gives you specific legal rights. You may have other rights, which vary from state to state.

DISCLAIMER OF DAMAGES:

Regardless of whether any remedy set forth herein fails of its essential purpose, in no event will Symantec be liable to you for any special, consequential, indirect or similar damages, including any lost profits or lost data arising out of the use or inability to use the software even if Symantec has been advised of the possibility of such damages.

Some states do not allow the limitation or exclusion of liability for incidental or consequential damages so the above limitation or exclusion may not apply to you.

In no case shall Symantec's liability exceed the purchase price for the software. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

U.S. GOVERNMENT RESTRICTED RIGHTS:

All Symantec products and documentation are commercial in nature. The Software and documentation are "Commercial Items", as that term is defined in 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. §252.227-7014(a)(5) and 48 C.F.R. §252.227-7014(a)(1), and used in 48 C.F.R. §12.212 and 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. §12.212, 48 C.F.R. §252.227-7015, 48 C.F.R. §227.7202 through 227.7202-4, 48 C.F.R. §52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Boulevard, Cupertino, CA 95014.

GENERAL:

This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: Symantec Customer Sales and Service, 20330 Stevens Creek Boulevard, Cupertino, CA 95014.

CONTENTS

Chapter 1 Introducing Symantec pcAnywhere

Chapter 2 Installing Symantec pcAnywhere

Chapter 3 Customizing Symantec pcAnywhere

Chapter 4 Deploying Symantec pcAnywhere

Chapter 5 Performing centralized management

Chapter 6 Integrating pcAnywhere with Directory Services

Chapter 7 Securing Symantec pcAnywhere

Chapter 8 Identifying security risks

CHAPTER 1

Introducing Symantec pcAnywhere

This manual contains advanced procedures for using and configuring Symantec pcAnywhere and is intended for network administrators, information technology professionals (IT), and information security professionals (IS). Some of the features discussed in this manual are available only in the Corporate version of pcAnywhere.

For general information on using pcAnywhere, consult the online documentation or the *Symantec pcAnywhere User's Guide,* provided on the installation CD.

This chapter contains the following:

- What you can do with pcAnywhere
- How pcAnywhere works
- What's changed in this version
- Where to find more information

What you can do with pcAnywhere

Symantec pcAnywhere lets you connect to another computer from a remote location, open any file or program that you have permission to access, and work as though you are sitting at that computer.

Some common uses for pcAnywhere include:

- Troubleshooting computer problems

  Helpdesk operators, network administrators, and other IT professionals use pcAnywhere to remotely connect to another computer and solve computer problems. pcAnywhere lets you view another person's computer screen, check and modify settings, and restart the computer—all from your computer.

- Supporting and maintaining servers

  Network administrators use pcAnywhere to connect to servers within their organization and perform routine maintenance, assess performance, and troubleshoot network issues.

- Retrieving files from home or office

  With pcAnywhere, you can connect to your home or office computer to quickly get the files you need.

- Working from a remote location

  pcAnywhere lets you connect to another computer and perform your work as though you are sitting in front of that computer. You can view and edit files, access network resources, and run programs that you have permission to access. You can also print files located on another computer to your default printer.

How pcAnywhere works

pcAnywhere uses remote control technology to let you connect to another computer or local area network (LAN) and work as though you are sitting in front of the other computer. To make a connection, both computers must be running pcAnywhere. One computer must be configured as a host, and the other computer must be configured as a remote.

Understanding the role of the host

When two computers are connected using pcAnywhere, they function in a client–server relationship. The host computer acts as the server. It waits for connections from a remote computer and provides requested services. During a remote control session, the host computer allows itself to be controlled by the remote.

When you configure a host computer, you control who can connect to the computer and what level of access the remote user should have.

Understanding the role of the remote

The remote computer is the client. It connects to a host computer and specifies what actions should be carried out. Although the actual work is performed on the host computer, anything that happens on the host computer screen is displayed on the remote computer screen as well. This exchange between the remote and host computers is called a remote control session.

What's changed in this version

pcAnywhere includes a number of new features and administrator tools, designed to increase security, optimize performance, and make the software easier to use and to customize.

Security enhancements

pcAnywhere has strengthened its focus on security to help users protect their computers from unauthorized access and to help network administrators and security professionals identify and prevent security holes.

New security features include:

- New authentication methods for Microsoft-based, Novell-based, and Web-based platforms

  The new authentication methods include: Active Directory Service (ADS), FTP, HTTP, HTTPS, Lightweight Directory Access Protocol (LDAP), Novell Bindery Service, and Novell Directory Service (NDS).

- Host now requires passwords for logging on

  The host user must choose an authentication method and set up caller accounts for remote users or user groups.

- The ability to track files and executables opened during a host session, for additional security.

  Users on Windows NT and Windows 2000 can also track pcAnywhere log events in the Event Viewer.

- Remote Access Perimeter Scanner (RAPS)

  This new administrator tool scans for unsecured hosts on the corporate network and detects the presence of many popular remote access products to identify potential security risks. This tool is available only in the Corporate version of pcAnywhere.

  For more information, see the *Symantec pcAnywhere Administrator's Guide.*

- The ability to lock a configuration set to prevent tampering with pcAnywhere configuration files, executables, and registry settings

For more information, see the *Symantec pcAnywhere Administrator's Guide.*

- The ability to protect the security of pcAnywhere configuration, using policy management

  Policy management lets administrators choose which user interface items users can view or modify. This feature is available only for Windows NT and Windows 2000.

Increased customization

pcAnywhere gives administrators more flexibility in customizing pcAnywhere.

New customization features include:

- pcAnywhere Packager

  Using pcAnywhere Packager, administrators can create and deploy custom installation sets to enhance security or performance or reduce the amount of disk space needed to install or run pcAnywhere. This feature is available only for Windows NT and Windows 2000.

- Symantec Web Deployment Tool

  The Symantec Web Deployment Tool lets administrators deploy pcAnywhere on the Internet or on a corporate intranet.

- Pre-configured installation packages

  Administrators can install these packages or use them as templates for building their own custom installation packages.

- Object linking and embedding (OLE) automation

  OLE automation lets administrators write applications to automate certain functions within pcAnywhere and add these functions to the Tools menu.

Improved performance

pcAnywhere's main window has been modified to make it easier to navigate and differentiate between host and remote modes.

Performance enhancements include:

- Optimization Wizard

  The Optimization Wizard walks users through the steps of optimizing a connection, highlighting the options that are available for improving performance and informing users of trade-offs between performance and security.

- pcAnywhere File Manager enhancements make it easier to find and select files and folders for file transfer

  The Go menu lets you quickly navigate to recently visited files and folders. Tagging features let you quickly select files or folders for file transfer or synchronization. You can also use wild card patterns to tag files and folders.

- The ability for ISDN CAPI users to select channel bonding when using the host callback feature

  This version also addresses performance issues involving CAPI channel bonding.

Removed features

To keep pace with the latest technologies, some features are no longer supported in pcAnywhere. If you are upgrading from a previous version of pcAnywhere, consult this table for guidance.

Removed feature	Reason for removal	For more information
pcA Config and AWCustom32	pcAnywhere Packager replaces these administrator tools. Packager provides administrators with more flexibility and stronger security options for building and deploying customized installations.	See the *Symantec pcAnywhere Administrator's Guide.*
Scripting	Extended OLE automation replaces the need for scripting. Existing scripting functions are included in the OLE classes.	See the *Symantec pcAnywhere OLE Automation Guide* on the installation CD.
Virus scanning	To improve performance, pcAnywhere no longer scans for viruses during file transfers.	If you do not have an antivirus program, visit the Symantec Web site (www.symantec.com/downloads) to download a trial version.

Removed feature	Reason for removal	For more information
pcAnywhere+ for Tivoli	Not supported in this version.	If you need to use this feature, install the previous version of pcAnywhere, located on the installation CD.
Gateways	No longer supported.	If you need to use gateways, install the previous version of pcAnywhere, located on the installation CD.
Online services	No longer supported.	If you need to use online services, install the previous version of pcAnywhere, located on the installation CD.
Banyan and IPX protocols	No longer supported.	If you need to use these protocols, install the previous version of pcAnywhere, located on the installation CD.
DOS and Windows 3.X backwards compatibility	No longer supported.	If you need to connect to a computer that uses one of these operating systems, install the previous version of pcAnywhere, located on the installation CD.
Yahoo! Pager	No longer provided.	

Where to find more information

In addition to the technical support options that are described in the back of this manual, pcAnywhere includes features designed to assist you in using the software. You can access some of these features, like the online Help and software wizards, while running pcAnywhere; however, some features are available only on the installation CD.

Information on the Symantec Web site

Check the Symantec Web site (www.symantec.com/pcanywhere) for answers to frequently asked questions, troubleshooting tips, online tutorials, and the latest product information.

Information on the pcAnywhere CD

These documents are available on the installation CD in PDF format.

- *Symantec pcAnywhere Administrator's Guide*
- *Symantec pcAnywhere User's Guide*
- *Symantec pcAnywhere OLE Automation Guide*

CHAPTER 2

Installing Symantec pcAnywhere

Installation procedures might vary, depending on your work environment and which installation option you choose. This chapter focuses on installing the full version of pcAnywhere from the installation CD.

This chapter contains the following:

- Preparing for installation
- Installing pcAnywhere
- Installing Administrator Tools
- Updating pcAnywhere
- Uninstalling pcAnywhere

Preparing for installation

Before you install pcAnywhere, make sure that your computer meets the system requirements. You should also review the Readme file on the installation CD for any last-minute changes that you might need to know about.

System requirements

pcAnywhere runs on Windows 9x, Windows Millennium Edition (ME), Windows NT, and Windows 2000 and requires, at a minimum, these resources to function properly.

Windows 95/98/NT 4

- Pentium or higher microprocessor

- 32 MB RAM
- 30 MB available hard disk space
- VGA or higher resolution monitor
- CD-ROM drive

Windows Millennium Edition

- 150 MHz Pentium or higher microprocessor
- 32 MB RAM
- 30 MB available hard disk space
- VGA or higher resolution monitor
- CD-ROM drive

Windows 2000

- 133 MHz Pentium or higher microprocessor
- 32 MB RAM
- 30 MB available hard disk space
- VGA or higher resolution monitor
- CD-ROM drive

Choosing an installation option

During installation, you can install the full version of pcAnywhere or select an option that contains only the functionality that you need. pcAnywhere provides two full installation options: pcAnywhere for the Professional and pcAnywhere for the Individual. Both options contain full host, remote control, and file transfer functionality. However, the Professional installation option also includes the pcAnywhere Packager and option sets functionality.

If you want to switch between host and remote modes on your computer, install either pcAnywhere for the Professional or pcAnywhere for the

Individual. If you do not need the full product and want to save disk space, choose one of the other options, using this table for guidance.

Installation option	Explanation
pcAnywhere for the Professional	Installs the full version of pcAnywhere, including pcAnywhere Packager and option sets functionality.
pcAnywhere for the Individual	Installs full functionality for host, remote, and file transfer operations, but does not include pcAnywhere Packager or option sets.
Remote Only	Provides remote control and file transfer functionality. Select this option if you do not want to host connections.
Host Only	Provides host server functionality, supporting network and modem connections. Select this option if you do not need remote control or file transfer functionality.
LAN Host	Provides host server functionality, supporting network connections only. Select this option if you do not need remote control or file transfer functionality, and do not want to support modem connections.

If you have a previous version installed

You must uninstall previous versions of pcAnywhere before installing this version. pcAnywhere performs this procedure automatically during the installation process. Before removing the previous version, pcAnywhere confirms whether you want to preserve existing configuration data. This configuration data includes host and remote connection items. However, because of the enhanced security features in pcAnywhere, existing caller properties are no longer valid and must be reconfigured.

Installing pcAnywhere

Follow this procedure when installing pcAnywhere from the installation CD. You can install pcAnywhere on two computers: a host and a remote, depending on your license agreement.

If the installation screen does not appear automatically after you insert the Symantec pcAnywhere CD, run the setup program manually.

For more information, see “To run the pcAnywhere setup program manually” on page 20.

To install Symantec pcAnywhere

1. Insert the Symantec pcAnywhere CD into the CD-ROM drive.
2. On the pcAnywhere installation screen, click **Install pcAnywhere 10.0**.
3. On the installation options screen, select the type of installation that you want to perform.

   For more information, see “Choosing an installation option” on page 18.
4. In the Welcome panel, click **Next**.
5. Accept the terms of the license agreement, then click **Next**.
6. In the Customer Information dialog box, type a user name.
7. Type an organization name.
8. Click **Next**.
9. Do one of the following:
   - Click **Typical** to install pcAnywhere using the program default settings.
   - Click **Custom** to select a different program folder location or choose which components you want to install.
10. Click **Next**.
11. Follow the instructions in the wizard for the type of installation selected.
12. Restart your computer when the installation is complete.

If the installation screen does not appear automatically after you insert the pcAnywhere installation CD, manually run the setup program, then continue with the installation procedures.

To run the pcAnywhere setup program manually

1. Insert the Symantec pcAnywhere CD into the CD-ROM drive.
2. On the Windows taskbar, click **Start** > **Run**.
3. Type **<CD-ROM drive letter>:\setup.exe**.

   For example:

   D:\setup.exe

4 Click **OK**.

5 Install pcAnywhere.

For more information, see "To install Symantec pcAnywhere" on page 20.

Installing Administrator Tools

The Symantec pcAnywhere installation CD contains additional software tools to assist administrators in customizing, managing, and securing pcAnywhere.

Installing RAPS and the Host Administrator

The Remote Access Perimeter Scanner (RAPS) lets you scan your network for unsecure hosts. The Host Administrator lets you remotely manage pcAnywhere hosts.

To install the Administrator Tools

1 Insert the Symantec pcAnywhere Corporate Edition CD into the CD-ROM drive.

2 On the main installation window, click **Administrator Tools**.

3 Click **Administrator Tools** again.

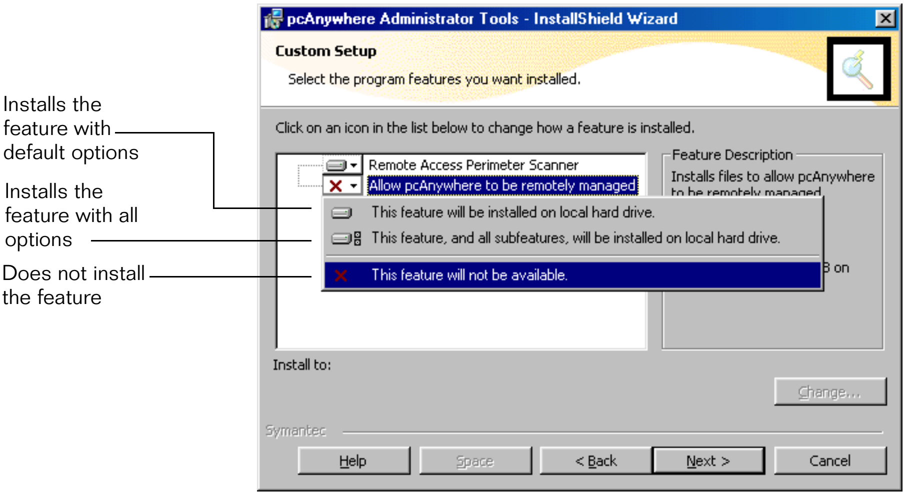
4 Click **Next**.

5 Follow the on-screen instructions until you reach the Custom Setup window.

6 In the Custom Setup window, do one of the following:

- Click **Complete** to install all of the Administrator Tools.

- Click **Custom** to choose which components to install.



pcAnywhere Administrator Tools - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

Remote Access Perimeter Scanner

Allow pcAnywhere to be remotely managed

This feature will be installed on local hard drive.

This feature, and all subfeatures, will be installed on local hard drive.

This feature will not be available.

Feature Description

Installs files to allow pcAnywhere to be remotely managed

Install to:

Installs the feature with default options

Installs the feature with all options

Does not install the feature

7 Click **Next**.

8 Follow the on-screen instructions.

Installing the LiveUpdate Administrator Utility

The LiveUpdate Administrator Utility lets you access the Symantec LiveUpdate server, download the product updates that you want your users to install, and post the updates on your own network so that your users can access them easily.

To install the LiveUpdate Administrator Utility

1 Insert the Symantec pcAnywhere Corporate Edition CD into the CD-ROM drive.

2 Click **Administrator Tools**.

3 Click **LiveUpdate Admin Utility**.

4 When prompted to install the LiveUpdate Administration package, click **Yes**.

5 On the Welcome screen, click **Next**.

6 Choose the destination location.

7 Click **Next**.

8 Click **Next** to start copying files.

9 Follow the on-screen instructions.

Updating pcAnywhere

You can receive software updates associated with your version of pcAnywhere by connecting to the Symantec LiveUpdate server and selecting the updates that you want to install.

To get pcAnywhere updates from Symantec

1. On the Windows taskbar, click **Start** > **Programs** > **Symantec pcAnywhere**.
2. In the pcAnywhere Manager window, click **Help** > **LiveUpdate**.
3. Follow the on-screen instructions.

Uninstalling pcAnywhere

You can uninstall pcAnywhere using the Add/Remove Programs option in Windows. Once the removal process begins, you cannot cancel the action.

To uninstall pcAnywhere

1. On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
2. Double-click **Add/Remove Programs**.
3. In the list of installed programs, click **Symantec pcAnywhere**.
4. Click **Add/Remove**.
5. In the Symantec pcAnywhere Setup window, click **Next**.
6. In the Program Maintenance dialog box, click **Remove**.
7. Click **Next**.
8. In the Remove the Program dialog box, click **Remove**.
9. Click **Finish** to exit the wizard.
10. Restart your computer.

CHAPTER 3

Customizing Symantec pcAnywhere

Symantec pcAnywhere Packager lets you create, modify, and build customized installation sets or packages that you can distribute to users on your network. Using pcAnywhere Packager, you can tailor pcAnywhere to fit your corporate environment, building packages that contain only the features and settings that your users need.

pcAnywhere packages are protected by copyright law and the Symantec license agreement. Distribution of pcAnywhere packages requires a license for each user who installs the package.

Note: pcAnywhere Packager is available for Windows NT and Windows 2000 platforms only. However custom installation files created with pcAnywhere Packager can be installed on any Microsoft 32-bit platform.

This chapter contains the following:

- Getting started
- Configuring a pcAnywhere package
- Building a package
- Changing configuration settings globally

Getting started

pcAnywhere packages are containers that contain the configuration settings needed to create a customized pcAnywhere installation file. The process for creating a custom installation file involves the following steps.

1 Create a package container.

For more information, see "Creating packages" on page 27.

Optionally, you can use one of the pre-configured packages provided in pcAnywhere or copy an existing package.

For more information, see "Using pre-configured packages" on page 26.

2 Configure the package.

pcAnywhere also provides a set of packages that are already configured for you.

For more information, see "Modifying a package" on page 28 or "Configuring a pcAnywhere package" on page 28.

3 Build the package.

During this step, pcAnywhere creates an installation file that contains the settings that you specified in the package. You can create either a Microsoft Software Installer (.msi) file or a self-extracting executable file (.exe).

For more information, see "Building a package" on page 41.

4 Deploy the package.

For more information, see "Deploying Symantec pcAnywhere" on page 45.

Using pre-configured packages

pcAnywhere includes a set of custom installation packages that are pre-configured to support the most common pcAnywhere usage scenarios. Using these packages, you can create an installation file for deployment to licensed users. You can also use them as templates for creating your own custom packages.

To use a pre-configured package

1. In the pcAnywhere Manager window, click **Packages**.
2. Right-click the package that you want to use, then click **Properties**.
3. Review the settings in the package to verify that the configuration meets your needs.

   For more information, see "Configuring a pcAnywhere package" on page 28.
4. In the pcAnywhere Package Properties dialog box, click **Build**.

   For more information, see "Building a package" on page 41.

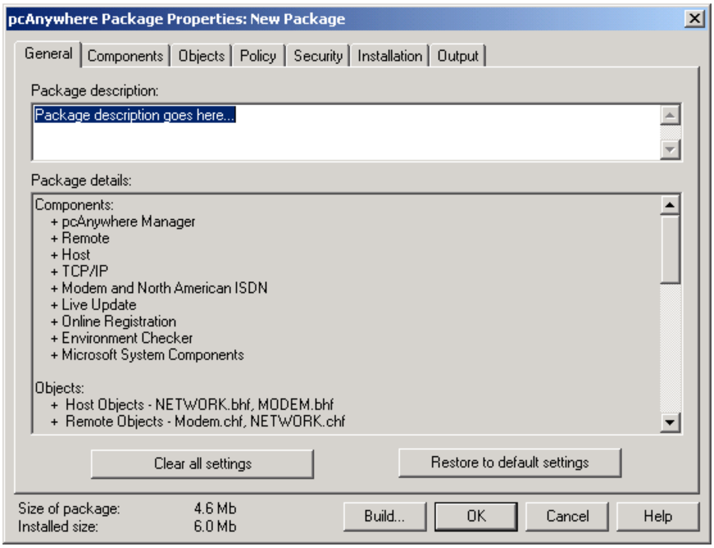
Creating packages

You create custom installation packages by adding a new package and configuring it or by copying an existing package and modifying it. Each package is assigned a default template. You can use this template or clear the settings to start with an empty package.

You can view details about the package in the pcAnywhere Package Properties dialog box and include a package description. Package details are updated dynamically as you modify the package configuration. This information, including the package description, is included in the custom installation file. This information appears during the installation. After installation, the information is included in the About window under Help.

To create a package

1. In the pcAnywhere Manager window, click **Packages**.
2. Double-click **Add Package**.
3. On the General tab, enter a package description.



Package description:
Package description goes here...

Package details:

Components:
+ pcAnywhere Manager
+ Remote
+ Host
+ TCP/IP
+ Modem and North American ISDN
+ Live Update
+ Online Registration
+ Environment Checker
+ Microsoft System Components

Objects:
+ Host Objects - NETWORK.bhf, MODEM.bhf
+ Remote Objects - Modem.chf, NETWORK.chf

Size of package: 4.6 Mb
Installed size: 6.0 Mb

4. Click **Clear all settings** to clear the settings in the default template and start with an empty package.

To create an installation file, you must configure the package, then build it.

For more information, see "Configuring a pcAnywhere package" on page 28 and "Building a package" on page 41.

Modifying a package

Another way to create a new package is to copy an existing package and modify the settings. You can modify the configuration settings in a package before or after you build it. However, if you modify settings after building a package, you must rebuild it.

For more information, see "Configuring a pcAnywhere package" on page 28 and "Building a package" on page 41.

To modify a package

1. In the pcAnywhere Manager window, click **Packages**.
2. Right-click the package that you want to modify, then click **Properties**.
3. On the General tab, do one of the following:
    - Enter a new package description, if applicable.
    - Click **Clear all settings** to clear the settings in the default template and start with an empty package.
    - Click **Restore to default settings** to use the settings in the default template.

You can change other configuration settings in the package.

For more information, see "Configuring a pcAnywhere package" on page 28.

Configuring a pcAnywhere package

pcAnywhere Packager lets you create customized versions of pcAnywhere that users can install on their computers. You can specify which features to include, control whether a user can view or modify a setting, and specify the installation options for the package.

This table explains where to find the settings that you need.

Tab	Explanation	For more information
General	Provides a description of the package, and lets you clear or restore settings.	See "Creating packages" on page 27.
Components	Lets you select the pcAnywhere functionality that you want to include in the package.	See "Selecting pcAnywhere components" on page 29.
Objects	Lets you select the connection items that you want to include in the package, specify startup options, and choose the default option set.	See "Specifying configuration settings" on page 31.
Policy	Lets you manage resource policies and control whether a user can view or modify a specific user interface setting.	See "Managing user interface policies" on page 33.
Security	Lets you lock the package so that it cannot be modified, and assign a serial number to the package.	See "Securing pcAnywhere packages" on page 34.
Installation	Lets you control pcAnywhere installation and start options.	See "Customizing installations" on page 36.
Output	Lets you choose the output options for the installation file.	See "Building a package" on page 41.

Selecting pcAnywhere components

The components you select when creating a package have a direct impact on the size of the installation file. To reduce the size of the footprint, select only the components that your users need. The pcAnywhere Package Properties dialog box displays the size of the package and the size of the installation file. This information is updated as you add or remove components.

Some components are dependent on others. If you select pcAnywhere Manager, the main pcAnywhere window, you must select a Host or Remote component. Selection of a Host or Remote component also requires selection of a communications protocol.

These dependencies apply not only to the items in the Components tab, but to other areas as well, such as user interface policies and security settings. For example, if you plan to lock the configuration settings of the package to prevent users from modifying the configuration of pcAnywhere after installation, do not select the pcAnywhere Manager component. You must include a desktop or menu shortcut, so users can launch a session.

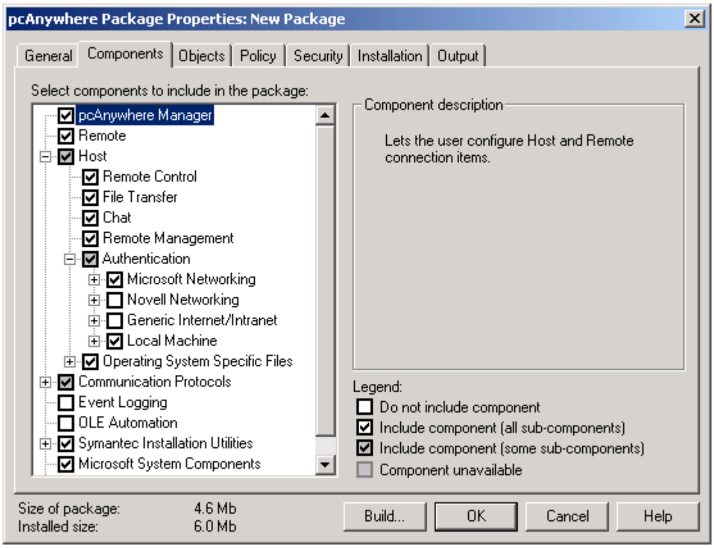
For more information, see "Managing user interface policies" on page 33, "Securing pcAnywhere packages" on page 34, and "Creating Start menu and desktop shortcuts" on page 39.

Checking a component label, for example Remote, automatically selects all of its subcomponents. However, you have the option to choose only the subcomponents that you need.

To select components

1. In the pcAnywhere Manager window, click **Packages**.
2. Right-click the package that you want to configure, then click **Properties**.
3. Do one of the following:
   - Check a component to include it and its subcomponents in the package.
   - Uncheck a component to exclude it and its subcomponents from the package.
   - Uncheck a subcomponent, if you want to exclude specific functionality under a component.

     For example, you can build a package that supports network communications only, by unchecking the other subcomponents under Communications Protocols. The main component label appears shaded and checked.



Select components to include in the package:

- ☑ pcAnywhere Manager
- ☑ Remote
- ☑ Host
  - ☑ Remote Control
  - ☑ File Transfer
  - ☑ Chat
  - ☑ Remote Management
  - ☑ Authentication
    - ☑ Microsoft Networking
    - ☐ Novell Networking
    - ☐ Generic Internet/Intranet
    - ☑ Local Machine
  - ☑ Operating System Specific Files
- ☑ Communication Protocols
- ☐ Event Logging
- ☐ OLE Automation
- ☑ Symantec Installation Utilities
- ☑ Microsoft System Components

Component description

Lets the user configure Host and Remote connection items.

Legend:

- ☐ Do not include component
- ☑ Include component (all sub-components)
- ☑ Include component (some sub-components)
- ▨ Component unavailable

Size of package: 4.6 Mb
Installed size: 6.0 Mb

4 Click **OK**.

Specifying configuration settings

The Objects tab displays the host (.bhf) and remote (.chf) objects that are contained in the pcAnywhere folder on the computer on which you are building the package. Host and remote objects contain the configuration settings for the host and remote connection items.

When creating a package, you can choose which connection items to include, as well as the default settings. However, you can only include objects that are associated with the components that are included in the package. For example, if you are creating a remote only package, the host objects are unavailable.

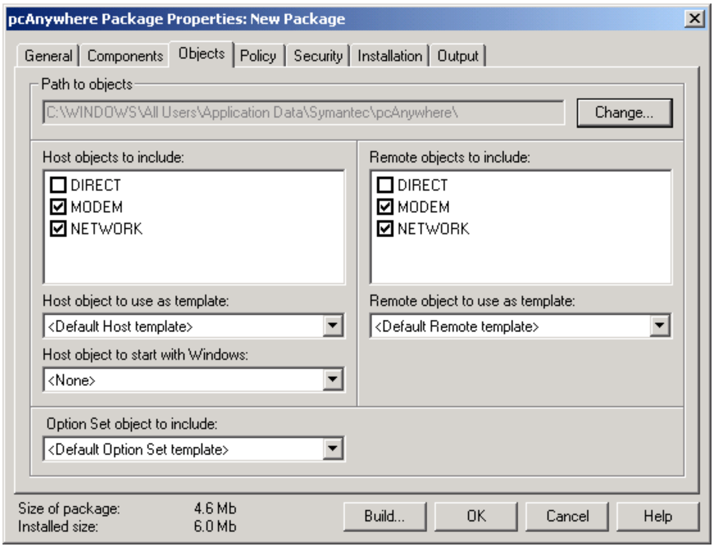
For more information, see “Selecting pcAnywhere components” on page 29.

If your package includes host functionality, you can also control whether a host connection item should launch automatically. You can also control global settings for the package, by selecting an option set.

For more information, see “Changing configuration settings globally” on page 42.

To specify configuration settings

1. In the pcAnywhere Manager window, click **Packages**.
2. Right-click the package that you want to configure, then click **Properties**.
3. On the Objects tab, do one of the following:
   - In the Host objects to include list, select the host connection items that you want to include.
   - In the Remote objects to include list, select the remote connection items that you want to include.



pcAnywhere Package Properties: New Package

Path to objects: C:\WINDOWS\All Users\Application Data\Symantec\pcAnywhere\

Host objects to include:
☐ DIRECT
☑ MODEM
☑ NETWORK

Remote objects to include:
☐ DIRECT
☑ MODEM
☑ NETWORK

Host object to use as template: <Default Host template>

Remote object to use as template: <Default Remote template>

Host object to start with Windows: <None>

Option Set object to include: <Default Option Set template>

Size of package: 4.6 Mb
Installed size: 6.0 Mb

4. Do one of the following to use the settings in a host or remote connection item as a template:
   - Under Host object to use as template, select an item in the list.
   - Under Remote object to use as template, select an item in the list.
5. If you want the host to launch automatically after the user starts Windows, under Host object to start with Windows, select a host connection item.

   The default setting is none.
6. Select the option set that you want to use as the default template.
7. Click **OK**.

Managing user interface policies

pcAnywhere Packager includes a policy manager, which lets you control which user interface resources can be viewed or modified by a user. The list of user interface elements is created dynamically, based on the pcAnywhere resources that are installed on the computer on which you are creating the package.

Resources include dialog boxes, options, check boxes, and group boxes. You can specify whether a user interface is visible or hidden. The Policy tab includes a preview area that lets you identify which user interface element is controlled by the selected resource.

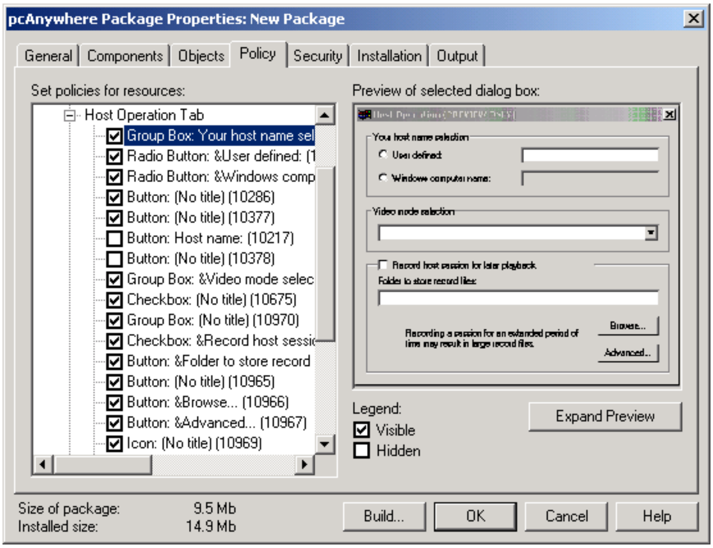
Some resources are dependent on the components that are included in the package, as well as on the operation system on which the custom installation file is installed. If you are building a package that will run on multiple platforms, for example, Windows 98 and Windows NT, remember that some resources are handled differently. For example, the Lock NT Workstation option equates to Windows screen saver on Windows 9x and Windows NT.

If you plan to lock the configuration settings of the package to prevent users from modifying the configuration of pcAnywhere after installation, you cannot set policies for pcAnywhere Manager user interface resources.

To set user interface policies

1. In the pcAnywhere Manager window, click **Packages**.
2. Right-click the package that you want to configure, then click **Properties**.
3. On the Policy tab, select the resource that you want to customize.
4. Do one of the following:
   - Check a resource to let users view or modify the user interface setting that is associated with it.
   - Uncheck a resource to hide the user interface element.

The check box appears shaded and checked. Users can view the setting, but cannot modify it.



pcAnywhere Package Properties: New Package

General | Components | Objects | Policy | Security | Installation | Output

Set policies for resources:

⊟ Host Operation Tab
- ☑ Group Box: Your host name sel
- ☑ Radio Button: &User defined: (1
- ☑ Radio Button: &Windows comp
- ☑ Button: (No title) (10286)
- ☑ Button: (No title) (10377)
- □ Button: Host name: (10217)
- □ Button: (No title) (10378)
- ☑ Group Box: &Video mode selec
- ☑ Checkbox: (No title) (10675)
- ☑ Group Box: (No title) (10970)
- ☑ Checkbox: &Record host sessic
- ☑ Button: &Folder to store record
- ☑ Button: (No title) (10965)
- ☑ Button: &Browse... (10966)
- ☑ Button: &Advanced... (10967)
- ☑ Icon: (No title) (10969)

Preview of selected dialog box:

Your host name selection
○ User defined:
○ Windows computer name:

Video mode selection

□ Record host session for later playback
Folder to store record files:

Recording a session for an extended period of time may result in large record files.

Browse... | Advanced...

Legend:
☑ Visible
□ Hidden

Expand Preview

Size of package: 9.5 Mb
Installed size: 14.9 Mb

Build... | OK | Cancel | Help

5 Click **OK**.

The Policy tab includes a preview area that lets you identify which dialog box is affected by the selected resource. You can also enlarge the preview area.

To preview a dialog box

1 On the Policy tab, select the resource that you want to customize.

A small version of the dialog box appears on the right side of the Policy tab dialog box.

2 Click **Expand Preview** to enlarge the preview area.

3 Close the preview window.

4 Click **OK**.

Securing pcAnywhere packages

pcAnywhere Packager provides two lines of defense in protecting the security of your packages once they are installed: securing the configuration and securing connections.

To protect the security of the configuration, lock the configuration set. When you lock, or integrity stamp, a package, no one can modify the configuration settings of the installed file. If you need to modify the customized version of pcAnywhere after installation, you must create a new installation file and redistribute it.

If a user circumvents the security measures and changes a setting in a locked version of pcAnywhere, pcAnywhere will automatically detect the change and restrict the user from using the software. To regain functionality, the user must reinstall pcAnywhere.

For more information, see "Securing pcAnywhere configuration" on page 103.

To secure the configuration of a package

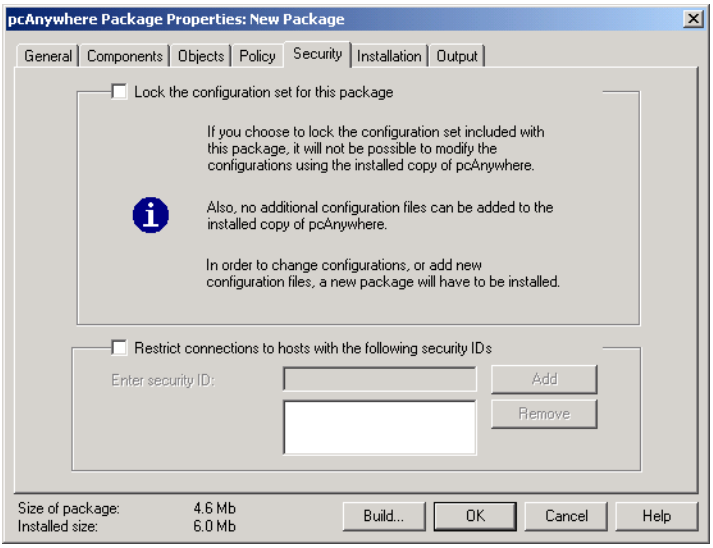
1. In the pcAnywhere Manager window, click **Packages**.
2. Right-click the package that you want to configure, then click **Properties**.
3. On the Security tab, check **Lock the configuration set for this package**.
4. Click **OK**.

Access control is an important step in ensuring security. When creating a package, you can add a security ID or serial number. pcAnywhere sessions are restricted to host computers with matching security ID numbers.

To control access

1. In the pcAnywhere Manager window, click **Packages**.
2. Right-click the package that you want to configure, then click **Properties**.

3 On the Security tab, check **Restrict connections to the following security IDs**.



□ Lock the configuration set for this package

If you choose to lock the configuration set included with this package, it will not be possible to modify the configurations using the installed copy of pcAnywhere.

Also, no additional configuration files can be added to the installed copy of pcAnywhere.

In order to change configurations, or add new configuration files, a new package will have to be installed.

□ Restrict connections to hosts with the following security IDs

Enter security ID:

Size of package: 4.6 Mb
Installed size: 6.0 Mb

4 Do one of the following:

- Type a security ID, then click **Add** to add a serial number.

  The security ID must be numerical and can be no longer than 10 characters.
- Select a security ID, then click **Remove** to remove a serial number.

5 Click **OK**.

Customizing installations

You can control each step of the installation process for your custom installation package, including which panels should appear in the Symantec pcAnywhere Setup program and how interactive you want the installation to be. For example, you can let users specify their license information, or you can provide the information for them.

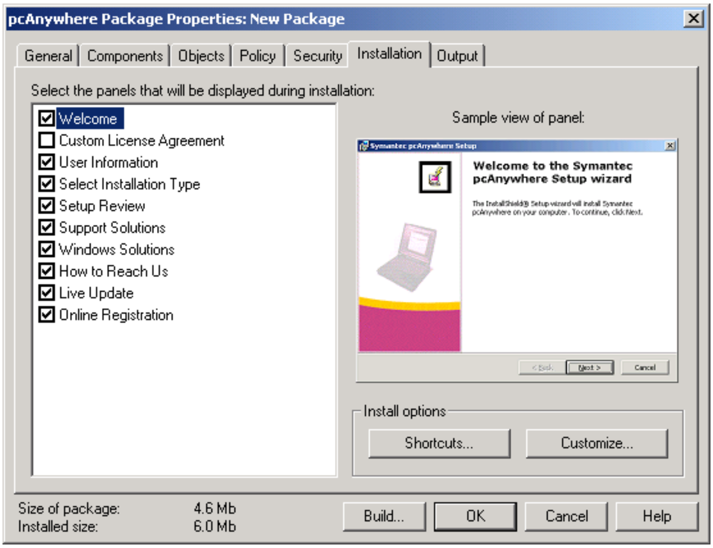
To control which panels appear during installation

1 In the pcAnywhere Manager window, click **Packages**.

2 Right-click the package that you want to configure, then click **Properties**.

3 On the Installation tab, select the panels that you want users to see when they run the setup program.

When you check a panel name, the Installation tab shows a preview of the installation panel.


pcAnywhere Package Properties: New Package
General
Components
Objects
Policy
Security
Installation
Output
Sample view of panel:
Symantec pcAnywhere Setup
Welcome to the Symantec pcAnywhere Setup wizard
The InstallShield® Setup wizard will install Symantec pcAnywhere on your computer. To continue, click Next.
< Back
Next >
Cancel
Install options
Shortcuts...
Customize...
Build...
OK
Cancel
Help

Select the panels that will be displayed during installation:

- ☑ Welcome
- □ Custom License Agreement
- ☑ User Information
- ☑ Select Installation Type
- ☑ Setup Review
- ☑ Support Solutions
- ☑ Windows Solutions
- ☑ How to Reach Us
- ☑ Live Update
- ☑ Online Registration

Size of package: 4.6 Mb
Installed size: 6.0 Mb

4 Click **OK**.

Pre-configuring installation information

pcAnywhere requires specific information to install properly, including the destination directory and licensing information. You can pre-configure this information in your package to minimize the amount of information for which users are prompted. To prevent users from changing this information during the installation, you can make the settings read-only.

To pre-configure installation information

1 In the pcAnywhere Manager window, click **Packages**.

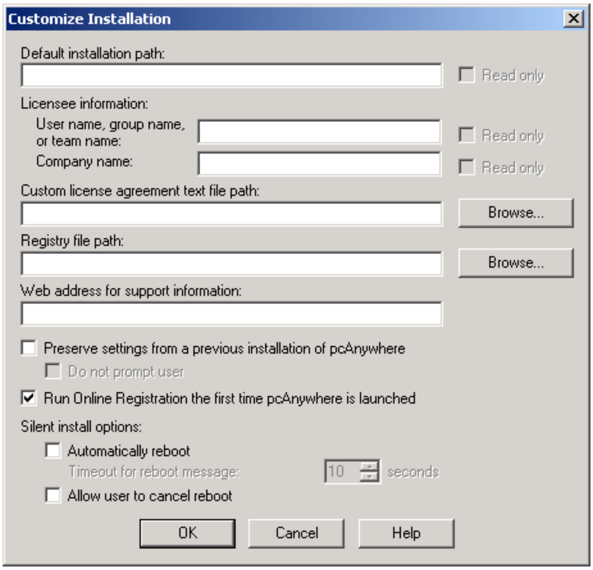
2 Right-click the package that you want to configure, then click **Properties**.

3 On the Installation tab, click **Customize**.

4 Do any of the following:

- Type the path to the directory in which the pcAnywhere package should be installed on the user's computer.
- Type the name of the license holder.

- Type the name of the organization.



Customize Installation

Default installation path: □ Read only

Licensee information:

User name, group name, or team name: □ Read only

Company name: □ Read only

Custom license agreement text file path:

Registry file path:

Web address for support information:

□ Preserve settings from a previous installation of pcAnywhere

□ Do not prompt user

☑ Run Online Registration the first time pcAnywhere is launched

Silent install options:

□ Automatically reboot

Timeout for reboot message: 10 seconds

□ Allow user to cancel reboot

5 Check Read-only to prevent users from changing the installation directory and license information.

6 If you have a custom license agreement or custom support agreement, do one of the following:

- Type the path and file name of the custom license agreement.

  The file must be in rich text format (rtf).

- Type the URL of the custom support agreement.

7 To include registry keys in the package, type the file name, including the path, of the registry (.reg) file.

8 Click **OK**.

Preserving existing configuration settings

If you are creating a package to replace an existing version of pcAnywhere (from version 8.0 or above), you can automatically preserve configuration settings for host and remote objects, the registry file, and the .bin file. However, because of the enhanced security features in pcAnywhere, existing caller properties are no longer valid and must be reconfigured.

For more information, see the *Symantec pcAnywhere User's Guide.*

To preserve existing configuration settings

1. In the pcAnywhere Manager window, click **Packages**.
2. Right-click the package that you want to configure, then click **Properties**.
3. On the Installation tab, click **Customize**.
4. In the Customize Installation dialog box, check **Preserve settings from a previous installation of pcAnywhere**.
5. Check **Do not prompt user**, if you do not want the user to receive a confirmation dialog box.
6. Click **OK**.

Configuring restart options for silent installations

pcAnywhere requires the user to restart the computer after the installation is complete. If you plan to perform a silent installation of the custom installation package, you must configure the restart options to ensure proper functionality.

To configure restart options

1. In the pcAnywhere Manager window, click **Packages**.
2. Right-click the package that you want to configure, then click **Properties**.
3. On the Installation tab, click **Customize**.
4. Do any of the following:
   - Under Silent Install options, check **Automatically reboot**, then specify how long the message box should appear, to restart the computer automatically after the installation is complete.
   - Under Silent Install options, check **Allow user to cancel reboot** to let the user restart the computer later.
5. Click **OK**.

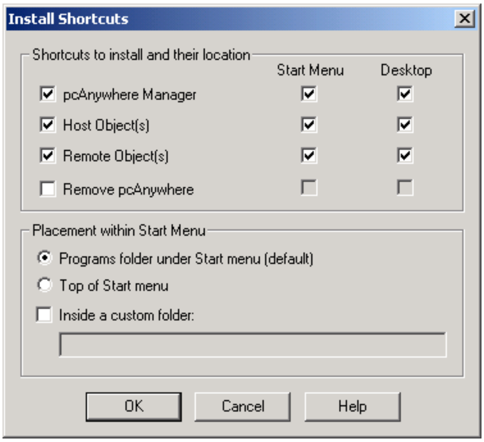
Creating Start menu and desktop shortcuts

By default, the Symantec pcAnywhere executable file is placed in the Windows programs folder when the package is installed. This file launches the pcAnywhere Manager window. In addition to the main executable file, you can add shortcuts to commonly used features, such as the host and remote connection items, to the Windows Start menu or desktop. You can also control the placement of these items in the Start menu.

If you plan to lock the configuration settings of the package to prevent users from modifying the configuration of pcAnywhere after installation, you must include a Start menu or desktop shortcut to the pcAnywhere functionality that is included in your package. You cannot include the pcAnywhere Manager window, which is the main user interface, in a locked package.

To configure Start menu and desktop shortcuts

1. In the pcAnywhere Manager window, click **Packages**.
2. Right-click the connection item that you want to configure, then click **Properties**.
3. On the Installation tab, click **Shortcuts**.
4. Select the items for which you want to create a shortcut.



Install Shortcuts

Shortcuts to install and their location

	Start Menu	Desktop
☑ pcAnywhere Manager	☑	☑
☑ Host Object(s)	☑	☑
☑ Remote Object(s)	☑	☑
□ Remove pcAnywhere	□	□

Placement within Start Menu

● Programs folder under Start menu (default)

○ Top of Start menu

□ Inside a custom folder:

5. Do any of the following:
   - Check **Start Menu** to add the shortcut to the Windows Start menu.
   - Check **Desktop** to add the shortcut to the Windows desktop.
6. When adding items to the Windows Start menu, do one of the following:
   - Click **Programs folder under Start menu** to add the menu items to the Start > Programs > Symantec pcAnywhere menu.
   - Click **Top of Start menu** to add the menu items to the top portion of the Start menu.
   - Check **Inside a custom folder**, then type the directory and path name, to place the menu items in a custom directory.
7. Click **OK**.

Building a package

Once you configure the installation package, you must specify an output option and then build the package. The Windows Installer program is required to install pcAnywhere. If your users do not have Windows Installer, you can create an installation file that includes it.

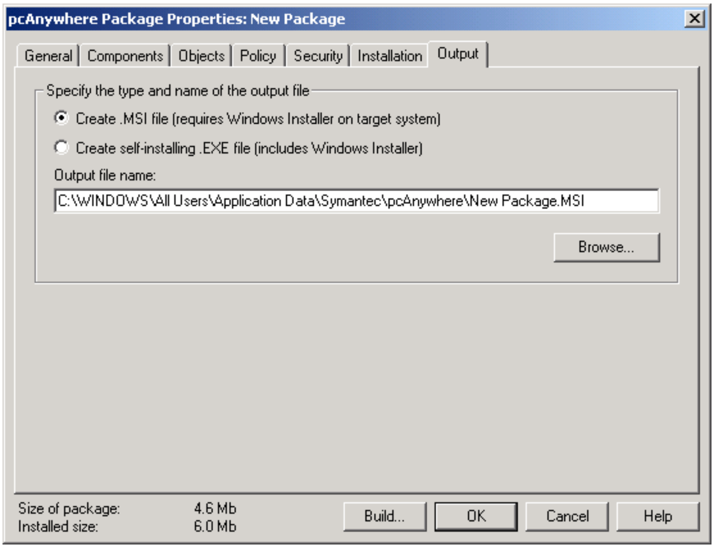
After building the package, it is highly recommended that you test the installation file before deploying it. If you need to change a setting, you can modify the package, then rebuild it.

For more information, see “Modifying a package” on page 28.

You have the option to produce an installation file that includes Windows Installer, if your users do not have already have it.

To build a package

1. In the pcAnywhere Manager window, right-click the package that you want to build, then click **Properties**.
2. On the Output tab, do one of the following:
   - Click **Create .MSI file** to create a Microsoft installation file.
   - Click **Create self-extracting .EXE file**, if the user does not have Windows Installer.
3. Specify a path and file name for the installation (.exe or .msi) file.



pcAnywhere Package Properties: New Package

Specify the type and name of the output file

● Create .MSI file (requires Windows Installer on target system)

○ Create self-installing .EXE file (includes Windows Installer)

Output file name: C:\WINDOWS\All Users\Application Data\Symantec\pcAnywhere\New Package.MSI

Size of package: 4.6 Mb

Installed size: 6.0 Mb

4 Click **Build**.

If this is the first time you are building a package, read the license agreement.

5 Click **Continue**.

A summary window appears, which lets you review the features that you selected for your package.

6 Click **Continue**.

As the package is built, status information, including any warnings or errors, is displayed in the summary window.

You can deploy the installation package to users who have a valid license agreement.

For more information, see "Deploying Symantec pcAnywhere" on page 45.

Changing configuration settings globally

Option sets let you manage global settings for host and remote connections, file transfer, logging, and other functions. When creating a package, you must select the option set that you want to use as a template. The option set controls the settings that appear in the pcAnywhere Options dialog box after a user installs the package.

For more information, see "Specifying configuration settings" on page 31.

You can create multiple option sets to satisfy unique configuration requirements. For example, users on one node might require different network configurations. Other users might require different remote operation settings to address performance issues. When you create a package for these nodes, apply the option set that contains the settings they need.

To add or modify an option set

1 In the pcAnywhere Manager window, click **Option Sets**.

2 Do one of the following:

- Double-click **Add Option Set**.
- Right-click the option set that you want to configure, then click **Properties**.

The pcAnywhere Option Set Properties dialog box works just like the pcAnywhere Options dialog box, which is accessed from the Tools > Options menu.

For more information, see the *Symantec pcAnywhere User's Guide.*

You can also apply an option set to a local computer, overriding the settings in the pcAnywhere Options dialog box. This feature is helpful if you work in different locations that have unique configuration requirements. You can maintain separate option sets for each location, then apply the appropriate option set to the local computer.

To apply a different option set

1. In the pcAnywhere Manager window, click **Option Sets**.
2. Right-click the option set that you want to use, then click **Apply to local system**.

CHAPTER 4

Deploying Symantec pcAnywhere

With pcAnywhere Packager, administrators can create and deploy customized pcAnywhere installations. pcAnywhere Packager builds a custom Windows Installer file (.msi) or Setup file (.exe). Any of the many tools that currently exist for distributing .msi and .exe files can be used to deploy pcAnywhere. In addition, the pcAnywhere CD contains several pre-configured distribution packages that are designed for the most common uses of pcAnywhere.

This chapter provides procedures on deploying pcAnywhere packages, whether custom or pre-configured, by the following methods:

- Using SMS 2.0
- Using Symantec's Web-based deployment
- Using NT login scripts
- Using Netware login scripts

Note: To create a pcAnywhere Package, see "Customizing Symantec pcAnywhere" on page 25.

Using SMS 2.0

Three components are required to deploy pcAnywhere with SMS 2.0 (Microsoft Systems Management Server):

- **pcAnywhere package:** An installation package created by the pcAnywhere Packager that contains only the pcAnywhere files necessary for the installation. It can be created as an .msi file or as an .exe file.

- **SMS Package**: A collection of installation sources and packages that is used to inventory and install software on SMS client computers. SMS packages can be any type of software program that supports installation via SMS.
- **Package Definition File (PDF):** An SMS-specific information file used by SMS to create and deploy SMS packages. The default PDF supplied with pcAnywhere is called Setup.sms.

Minimum requirements for SMS deployment

- Windows NT 4.0 Server with Service Pack 5 or higher
- SQL Server 6.5 or higher
- SMS 2.0 with Service Pack 1 or Service Pack 2 (recommended)
- All deployment clients must either be members of the same domain as the SMS distribution server or have a trust relationship set up between the domains with appropriate permissions allowing the SMS server administrative rights on all clients.
- pcAnywhere 10.0 installed with customized packages created for deployment.

SMS 2.0 must be installed on Windows NT 4.0 with Service Pack 5 or higher. It is recommended that you obtain the SMS Service Pack 2 or higher from Microsoft. Please visit http://www.microsoft.com/sms for the latest information regarding SMS updates and the specific steps that need to be followed to apply the service packs.

Deploying with SMS

An SMS deployment requires four steps:

- Preparing the Package Definition File
- Creating the SMS deployment package
- Assigning distribution points
- Advertising the package

Preparing the Package Definition File

A default Package Definition File (Setup.sms) is provided with pcAnywhere. This file can be modified to accommodate any package created with the pcAnywhere Packager.

To use the supplied Package Definition File without modification, do one of the following:

- For .exe-based packages, rename the pcAnywhere package that you want to use to Package.exe.
- For .msi-based packages, rename the pcAnywhere package that you want to use to Package.msi.

For information on customizing the Package Definition File, see your SMS documentation.

The following values must not be removed or changed in the supplied Package Definition File:

- AfterRunning=ProgramRestart
- CanRunWhen=UserLoggedOn
- AdminRightsRequired=TRUE

Creating the SMS deployment package

An SMS Package must be created and a distribution must be configured for each type of pcAnywhere installation that you want to perform on the client computers.

To create an SMS deployment package

1. Use the pcAnywhere Packager to create an MSI or EXE pcAnywhere package, as appropriate, or use one of the supplied, pre-configured pcAnywhere packages.
2. In the SMS Administrator console, right-click **Packages**, then click **New > Package from definition**.

   The Create Package from Definition Wizard is displayed.
3. When prompted for the name of a package file, click **Browse** to locate the pcAnywhere Setup.sms file.

   The default location is C:\Program Files\Symantec\pcAnywhere\CMS.
4. Click **Open**.

   The Create Package from Definition Wizard displays the pcAnywhere Package definition.
5. Click **Next**.

6 Select Always obtain files from a source directory.

Caution: Do not select This package does not contain any files.

---

7 Click **Browse** to locate the folder that contains the pcAnywhere package you created with by the pcAnywhere Packager (or a supplied, pre-configured package).

The Create Package from Definition Wizard uses this folder to point to the pcAnywhere package.

8 After you complete the Create Package from Definition Wizard, a package for pcAnywhere 10.0 appears in the SMS Administrator Console.

Assigning distribution points

After an SMS package is created, a distribution point must be specified for the package.

To assign distribution points

1 Right-click **Distribution Points**, then click **New** > **Distribution point**.

2 Check the Distribution points to which you want to distribute the package.

3 Click **Finish** to complete the Distribution Point Wizard.

Advertising the package

To send the pcAnywhere installation to the clients, an advertisement of one or more of the packaged installs must be created.

To advertise the package

1 Right-click **Advertisements**, then click **New** > **Advertisement.**

2 Select the package that you want to advertise.

3 Give the advertisement a descriptive name.

4 From the drop-down menu, select one of the following installs:

- Windows ME/Windows 2000 to distribute to Windows ME and Windows 2000 clients that support MSI based installations.
- Windows 9x/Windows NT to distribute the pcAnywhere package to Windows 9x or Windows NT clients.

5 Click **Browse** and pick the collection to which you want to advertise the installation.

6 Set the schedule, requirements, and appropriate security rights of the package.

After the advertisement is created, pcAnywhere should deploy to all of the selected clients.

Note: Advertisements created using the EXE-based installer require user intervention. Users are prompted to choose a temporary directory on the local client computer to extract the installation files. After the files are extracted, users are prompted to click Yes to begin Setup to install pcAnywhere. Users should delete the temporary setup files when installation is complete.

Using Web-based deployment

pcAnywhere 10.0 can be deployed to client workstations using a Web-based install over the corporate Intranet or the Internet. All of the source files necessary to implement Web-based deployment are included on the pcAnywhere CD.

Web-based deployment requires three steps:

- Creating the installation Web site
- Customizing the deployment files: Files.ini, Launch.bat, and Start.htm
- Testing the installation

Creating the installation Web site

For a Web-based deployment, copy the source files to a virtual directory on your Web server. You also need to create a subdirectory in the virtual directory. The deployment source files are located in the Admin Tools\Web Based Deployment Tool folder on the CD.

Note: For the following examples, the virtual directory is called Webinstall and the subdirectory is called Webinst; however, any names can be used.

To create the installation Web site

1 Create a virtual directory on the Web server called Webinstall.

2 Copy the following files into the root of the Webinstall virtual directory:

- Brnotsup.htm
- Default.htm
- Intro.htm
- Oscheck.htm
- Plnotsup.htm
- Start.htm
- Logo.jpg
- Webinst.cab

3 Create a subdirectory in the virtual directory called Webinst.

4 Copy the following files to the Webinst subdirectory:

- Files.ini
- Launch.bat
- The pcAnywhere distribution Package (for example, pcAnywhere.MSI or pcAnywhere.EXE)

5 Ensure that the default document for the virtual directory is set to Default.htm.

Customizing the deployment files

Three files must be modified for the deployment. Start.htm resides in the root of the Webinstall virtual directory. Files.ini and Launch.bat reside in the Webinst subdirectory.

Files.ini

Modify Files.ini to contain the name of the pcAnywhere distribution package. Files.ini is located in the Webinst subdirectory of the Webinstall virtual directory. Only the File1= setting needs to be changed.

Parameter	Value
File1=	The name of the package that was created using the pcAnywhere Packager (for example, File1=pcAnywhere.msi). Long file names can be used.

Launch.bat

Launch.bat, which starts the pcAnywhere package installation, contains the command line used to execute the package installation. Modify this command line to contain the name of the package that is being installed.

Choose the command line for either an MSI or an EXE package. Replace PackageName with the actual name of the pcAnywhere package.

Package Type	Command Line
For an EXE-based package	@PackageName.exe
For an MSI-based package	@msiexec –i PackageName.msi

Start.htm

The parameters in the Start.htm file contain information about the Web server and the locations of the files that need to be installed. The configuration parameters are located toward the bottom of the Start.htm file, inside the <object> tags.

Open the Start.htm file, search for the <object> tags, and enter the correct values.

Parameter	Value
ServerName	The name of the server that contains the installation source files. You can use Hostname, IP address, or NetBIOS name. The source files must reside on an HTTP Web server.
VirtualHomeDirectory	The virtual directory of the HTTP server that contains the installation source files (for example, webinstall).
ConfigFile	The file name of the Files.ini file. The default value for this parameter does not need to be changed unless you've renamed Files.ini.
ProductFolderName	The subdirectory that contains the source files to be downloaded locally. This subdirectory contains the pcAnywhere package, Files.ini, and Launch.bat (for example, Webinst).

Parameter	Value
MinDiskSpaceInMB	The minimum hard disk space requirement. The default value is appropriate.
ProductAbbreviation	The abbreviation for the product. The default value is appropriate.

Testing the installation

To test the roll out, go to the Web site (<your web site>/webinstall, for example) and click the Install button. After the source files are downloaded locally, Launch.bat executes to begin the package installation.

If the install fails, note any error messages displayed:

- If there is a problem with the parameters in Start.htm, an error message showing the path of the files the Web-based install is trying to access is displayed. Verify that the path shown in the error message is the correct path.
- If there is a problem in Files.ini (for example, a File not found error), compare the File1= value with the actual name of the pcAnywhere package file.
- Confirm that no other entries were changed during modification.

Using Windows NT/Windows 2000 login scripts

In a Windows domain, pcAnywhere packages can be deployed to Windows clients using login scripts. Three steps are required:

- Set up the server
- Write the login script
- Test the login script

Windows NT and Windows 2000 users must have local administrative rights on their computers to install the pcAnywhere package.

Setting up the server

The server must be configured to allow for the storage of pcAnywhere Packages and the implementation of login scripts. You must have Administrator rights on the domain to perform these tasks.

To set up the server

1. On the server, create a folder called PCAHOME.
2. Share the folder and use the default share name of PCAHOME.
3. Set the permissions of this share so that all users have Read access.
4. Copy the pcAnywhere Package to the PCAHOME share.

Writing the login script

Use the following sample login script. The script is a simple batch file that copies the pcAnywhere Package to the workstation, launches the pcAnywhere Package installation, and cleans up the installation files when complete.

The following examples assume default installation folders. Modify them, as necessary, to work in your particular environment.

```
@echo off
setlocal

REM ***** Package Variable -- Change to name of pcA Package *****
Set Package=Package.MSI

REM ***** EXE or MSI Variable -- Change to package type (MSI or EXE) *****
Set PkgType=MSI

Rem ***** File Server Name Variable *****
Rem ***** Change to server containing the pcA Package *****
Set FSName=\\2KServer

REM ***** Maps a drive to the network share *****
net use z: %FSName%\PCAHOME

REM ***** Checks for pcA in default folder
If exist c:\progra~1\Symant~1\pcanyw~1\anywhere.bin GOTO End

REM ***** Creates a folder in the Temp dir, and copies the package *****
C:
CD %TEMP%
MD pcapkg
CD pcapkg
Z:
COPY %Package% C:
```

```
REM ***** Launch Package Installation *****
C:
IF %PkgType% == MSI msiexec -i %Package%
IF %PkgType% == EXE %Package%

REM ***** Cleanup *****
del %Package%
CD ..
rd pcapkg
Net Use Z: /DELETE

:End
endlocal
```

Testing the login script

Test the completed script on one or two workstations before setting the script up for all users. Windows NT and Windows 2000 users must have local administrative rights on their computers to install the pcAnywhere package.

Using NetWare login scripts

On a Novell NetWare network, pcAnywhere packages can be deployed to Windows clients using login scripts. Three steps are required:

- Set up the server
- Write the login script
- Test the login script

Windows NT and Windows 2000 users must have local administrative rights on their computers to install the pcAnywhere package.

Setting up the server

To set up the Novell NetWare server

1. Map drive Z: to the SYS: volume.

   If you use another drive letter, substitute the appropriate drive letter in the following steps.
2. In the Z:\LOGIN folder, create a folder called PCA.
3. Create a group called PCA_Users.

The PCA_Users group should exist in the default context for servers that host both NDS and Bindery logins. If the server only hosts NDS logins, this group should exist in a context that exists in the NDS partition stored on the server.

4. Grant the PCA_Users group Read rights to the PCA folder.
5. Copy the pcAnywhere package into the PCA folder.

Writing the login script

Use the following sample login script and deployment batch file to roll out pcAnywhere. The script creates the appropriate drive mappings to the local workstation and launches the deployment batch file. The batch file installs the pcAnywhere package and removes the installation files when complete.

The following examples assume default installation folders. Modify them, as necessary, to work in your particular environment.

Netware login script

```
REM ***** Default mappings *****
MAP *1:=SYS:

REM ***** Maps a drive to the network share *****
MAP Z:=SYS:LOGIN\PCA

REM ***** Launches the deployment batch file *****
#Cmd /c z:\deploy.bat

Exit
```

Deployment batch file

```
@echo off
setlocal

REM ***** Package Variable -- Change to name of pcA Package *****
Set Package=Package.MSI

REM ***** EXE or MSI Variable -- Change to package type (MSI or EXE) *****
Set PkgType=MSI

REM ***** Checks for pcA in default folder *****
If exist c:\progra~1\Symant~1\pcanyw~1\anywhere.bin GOTO End
```

```
REM ***** Creates a folder in the Temp dir, and copies the package *****
C:
CD %TEMP%
MD pcapkg
CD pcapkg
Z:
COPY %Package% c:

REM ***** Launches package installation *****
C:
IF %PkgType% == MSI msiexec -i %Package%
IF %PkgType% == EXE %Package%

REM ***** Cleanup *****
del %Package%
CD ..
rd pcapkg

:End
endlocal
```

Testing the login script

Test the completed script on one or two workstations before setting the script up for all users. Windows NT and Windows 2000 users must have local administrative rights on their computers to install the pcAnywhere package.

CHAPTER 5

Performing centralized management

Symantec pcAnywhere includes a host administrator utility, which lets network administrators remotely control and configure multiple pcAnywhere hosts on a network. One of its more powerful features is the ability to group systems together to quickly distribute pcAnywhere connection items and option sets.

The pcAnywhere Host Administrator utility is a Microsoft Management Console (MMC) snap-in and requires Microsoft Management Console (MMC) to run. MMC is included on the Symantec pcAnywhere CD under Administrator Tools.

For more information, see "Installing Administrator Tools" on page 21.

pcAnywhere also supports integration with a number of industry leaders in network management applications.

This chapter contains the following:

- Integrating with centralized management tools
- Managing pcAnywhere remotely
- Understanding SNMP and central logging
- Using the Microsoft Distributed Component Object Model (DCOM)

Integrating with centralized management tools

Centralized network management applications provide administrators with a single interface for monitoring and managing every node on the network. pcAnywhere is integrated with the following network management applications:

- IBM Tivoli NetView
- Computer Associates Unicenter TNG
- Microsoft SMS

Integration at this level places all administrator tools in one central location, providing a more efficient method of network administration.

Integrating with Tivoli NetView

Tivoli NetView integration is performed by placing a pcAnywhere Application Registration File (pcaconn.arf) in the NetView registration directory. This file adds the pcAnywhere Start, Stop, and Connect menu items. This file is located in the following directory:

\Program Files\Symantec\pcAnywhere\CMS

The contents of the pcaconn.arf file are as follows:

```
Application "pcANYWHERE"
{
        Version "10.0";
   Description {
       "pcAnywhere Remote Control"
   }
Copyright {
       "(C) 2001 Symantec Corporation."
        }
   MenuBar "Tools" {
       "pcAnywhere" _S f.menu PCAItem;
   }
   Menu PCAItem {
       <100> "Start PCA Host" _S f.action PcaStart;
       <90>  "Stop PCA Host" _T f.action PcaStop;
       <80>  "Connect to PCA Host" _C f.action PcaConnect;
   }
   Action "PcaStart"
   {
       SelectionRule isNode && isComputer;
       MinSelected 1;
       Command “awshim.exe -a STARTHOST -b NetView.bhf -h \
“$OVwSelection1””;
   }
   Action "PcaStop"
   {
       SelectionRule isNode && isComputer;
       MinSelected 1;
       Command “awshim.exe -a STOPHOST -h\
“$OVwSelection1””;
   }
   Action "PcaConnect"
   {
       SelectionRule isNode && isComputer;
       MinSelected 1;
            MaxSelected 1;
       Command "awshim.exe -a STARTREMOTE -c NetView.chf -r\
“$OVwSelection1””;
   }}
```

Also in the CMS directory are the netview.bhf and netview.chf files. These files contain the connection objects that are used when NetView starts, stops, or connects with pcAnywhere. If the site requires specific configurations to the connection objects, update these two files before deploying the install images to the managed nodes.

To update the connection objects

1 In Windows Explorer, open the install image.

2 Right-click the file, then click **Properties**.

Unicenter TNG integration

The Unicenter TNG integration, including the 2D and 3D map user interfaces, is accessible whenever the TNG shortcut menu is available. This integration uses TRIX, the TNG Repository Import-Export program to add items to the shortcut menus. Upon integration, the pcAnywhere Start, Stop, and Connect menu items are added.

These items are contained in the pca.tng file. Use the Unicenter TNG Repository Import/Export program (TRIX) to import the pca.tng file.

The file is located in the following directory:

\Program files\Symantec\pcAnywhere\CMS

To use the Unicenter TNG Repository to import:

1 Run TRIX.

2. In the CMS folder, open pca.tng.
3. Make any necessary modifications to the script.
4. Click **Import Repository**.

To edit the menu integration, either alter the TRIX script directly or use the Unicenter TNG Class Wizard to edit the menu interactively.

For more information, see the Unicenter TNG Books Online.

The contents of the PCA.TNG TRIX script are as follows:

```
ADDOBJECT="PCA_ConnectToHost" Method
BEGIN
type TNGWV_OT_INT 0 0
exe_name TNGWV_OT_STRING "awshim.exe" 0
parameter TNGWV_OT_STRING "-a startremote -c tng.chf -r
\"&address&\"" 0
END
ADDOBJECT="PCA_StartHost" Method
BEGIN
type TNGWV_OT_INT 0 0
exe_name TNGWV_OT_STRING "awshim.exe" 0
parameter TNGWV_OT_STRING "-a starthost -b tng.bhf -h
\"&address&\"" 0
END
ADDOBJECT="PCA_StopHost" Method
BEGIN
type TNGWV_OT_INT 0 0
exe_name TNGWV_OT_STRING "awshim.exe" 0
parameter TNGWV_OT_STRING "-a stophost -h  \"&address&\"" 0
END
ADDOBJECT="ManagedObject" Popup_Menu
BEGIN
sequence_no TNGWV_OT_INT 500 0
label TNGWV_OT_STRING "0" 0
method_name TNGWV_OT_STRING "0" 0
flag TNGWV_OT_INT 1 0
END
ADDOBJECT="ManagedObject" Popup_Menu
BEGIN
sequence_no TNGWV_OT_INT 501 0
label TNGWV_OT_STRING "Start PCA Host" 0
```

```
method_name TNGWV_OT_STRING "PCA_StartHost" 0
flag TNGWV_OT_INT 0 0
END
ADDOBJECT="ManagedObject" Popup_Menu
BEGIN
sequence_no TNGWV_OT_INT 502 0
label TNGWV_OT_STRING "Stop PCA Host" 0
method_name TNGWV_OT_STRING "PCA_StopHost" 0
flag TNGWV_OT_INT 0 0
END
ADDOBJECT="ManagedObject" Popup_Menu
BEGIN
sequence_no TNGWV_OT_INT 503 0
label TNGWV_OT_STRING "Connect to PCA Host" 0
method_name TNGWV_OT_STRING "PCA_ConnectToHost" 0
flag TNGWV_OT_INT 0 0
END
```

Once imported, these items can be modified to meet the site's requirements, using the Unicenter TNG Class Wizard.

The CMS folder also contains a tng.bhf file and a tng.chf file, which represent the pcAnywhere remote control connection items. These items are used whenever TNG starts, stops, or connects with pcAnywhere. If the site has specific configuration requirements, modify these connection files before distributing the install images to the managed nodes.

Integrating with Microsoft System Management Server

This integration is performed using the SMSAddin tool. The SMSAddin tool uses pcAnywhere registry keys to add pcAnywhere functionality to SMS. Upon integration, the pcAnywhere Start, Stop, and Connect options are added to the Tools menu in SMS.

The registry keys are added as follows:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Applications
\Symantec]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Applications\Syma
ntec\ SymantecConnectToPCAHost]
"ApplicationName"="Connect To PCA Host"
"Order"=dword:0000000b
```

```
"Command"="awshim.exe"
"Description"="Connect To PCA Host"
"WorkingDir"=hex(2):63,3a,5c,00
"RunWindow"="Normal"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Applications\Syma
ntec\ SymantecConnectToPCAHost\SMSMachine]
"EnableRule"=hex(7):00,00,00
"PresentRule"=hex(7):00,00,00
"Arguments"=hex(7):2d,61,00,73,74,61,72,74,72,65,6d,6f,74,65
,00,2d,63,00,73,6d,\73,2e,63,68,66,00,2d,72,00,24,28,41,74,7
4,72,28,4d,49,43,52,4f,53,4f,46,54,\7c,49,44,45,4e,54,49,46,
49,43,41,54,49,4f,4e,7c,31,2e,30,3a,4e,61,6d,65,29,\29,00,00
,00,00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Applications\Syma
ntec\ SymantecStartPCAHost]
"ApplicationName"="Start PCA Host"
"Order"=dword:00000009
"Command"="awshim.exe"
"Description"="Start PCA Host"
"WorkingDir"=hex(2):63,3a,5c,00
"RunWindow"="Normal"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Applications\Syma
ntec\ SymantecStartPCAHost\SMSMachine]
"EnableRule"=hex(7):00,00,00
"PresentRule"=hex(7):00,00,00
"Arguments"=hex(7):2d,61,00,73,74,61,72,74,68,6f,73,74,00,2d
,62,00,73,6d,73,2e,\62,68,66,00,2d,68,00,24,28,41,74,74,72,2
8,4d,49,43,52,4f,53,4f,46,54,7c,49,\44,45,4e,54,49,46,49,43,
41,54,49,4f,4e,7c,31,2e,30,3a,4e,61,6d,65,29,29,00,\00,00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Applications\Syma
ntec\ SymantecStopPCAHost]
"ApplicationName"="Stop PCA Host"
"Order"=dword:0000000a
"Command"="awshim.exe"
"Description"="Stop PCA Host"
"WorkingDir"=hex(2):63,3a,5c,00
"RunWindow"="Normal"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Applications\Syma
ntec\ SymantecStopPCAHost\SMSMachine]
"EnableRule"=hex(7):00,00,00
"PresentRule"=hex(7):00,00,00
"Arguments"=hex(7):2d,61,00,73,74,6f,70,68,6f,73,74,00,2d,68
,00,24,28,41,74,74,72,28,4d,49,43,52,4f,53,4f,46,54,7c,49,44
,45,4e,54,49,46,49,43,41,54,49,4f,4e,7c,31,2e,30,3a,4e,61,6d
,65,29,29,00,00,00
```

These registry keys add three new menu items to the Tools menu on the SMS console. The sms12.reg file that creates these entries is located in the CMS subfolder under the pcAnywhere installation directory at:

\Program Files\Symantec\pcAnywhere\CMS

In addition to this file, SMSAddin creates three ATD files. These files can be used to modify or adjust the SMS1.2 integration. The SMS.[B|C]HF files used whenever SMS starts, stops, or connects with pcAnywhere are located in the CMS subfolder. If the site requires specific configurations to the caller items, modify these two files before distributing the install images to the managed hosts.

To update the host connection objects

1. In Windows Explorer, open the install image.
2. Right-click the file, then click **Properties**.

Using Microsoft BackOffice with SMS

The Package Distribution File (.pdf) required for SMS software distribution is located in the \installs\utility\sms directory on the Symantec pcAnywhere CD.

To install BackOffice

1. In the SMS Administrator, use the Import utility to import the pcaw90.pdf file.
2. Copy the contents of all seven disks located in the \installs\pcanywhere\pca32full\cd\disk1 directory into a directory on the BackOffice server.

For more information on setting up and distributing applications using the BackOffice server, see the SMS documentation.

Managing pcAnywhere remotely

The pcAnywhere Host Administrator tool lets you do the following:

- Remotely start, stop, and connect to pcAnywhere hosts anywhere on the network.
- Create configuration groups to remotely manage and configure multiple workstations on the network.

- Simultaneously distribute pcAnywhere configuration files, including option sets and host, remote, and caller files, to multiple workstations on the network.

The Symantec pcAnywhere CD includes an admin.bhf file in the CMS subfolder of the pcAnywhere program directory. You can customize the settings in the admin.bhf file before installing the Host Administrator tool.

Upon installation of the Host Administrator utility, you can add it as a snap-in to MMC.

To add the Host Administrator snap-in to MMC

1. On the Windows taskbar, click **Start** > **Programs** > **pcAnywhere Administrator**.
2. Start the Microsoft Management Console (MMC).
3. On the Console menu, click **Add/Remove Snap-In**.
4. On the Standalone tab, click **Add**.
5. In the Add Snap-In dialog box, click **pcAnywhere Administrator**.
6. Click **Add**.

Creating configuration groups

To remotely manage and configure computers using MMC, you must create a configuration group, then add computers to the group. These procedures are performed in the MMC window.

For more information on using MMC, see the Microsoft Management Console documentation.

To create a configuration group

1. In the MMC left window pane, right-click **Configuration Groups**, then click **New** > **Configuration Group**.
2. Type a name for this group.
3. Click **OK**.

Once you create a configuration group, you must add the computers that you want to manage remotely. The MMC window lists the domains and workgroups that are on your network.

To add a computer to a configuration group

1. In the MMC left window pane, select the computer or computers that you want to add.
2. Drag and drop the listing of computers onto the name of the configuration group.

Configuring host computers in the group

pcAnywhere requires host users to specify an authentication method and configure a logon account for remote users who connect to the host. Before you can manage a host in your configuration group, you must set up a caller account.

You can also configure option sets to specify global settings.

For more information, see "Changing configuration settings globally" on page 42.

To create host files

1. In the MMC left window pane, right-click **Connection Items**, then click **New** > **Be A Host**.
2. Type a name for this connection item.
3. Click **OK**.

Configure the host connection item, specifying caller information and other needed information.

For more information, see the *Symantec pcAnywhere User's Guide*.

After you set up an administrator caller account, you can distribute the host template to the computers in the configuration group, using MMC.

To distribute host files

1. In the MMC left window pane, right-click a Configuration Group, then click **Distribute Host Files**.
2. Select the computers to which you want to distribute the file.
3. Select the file that you want to distribute.
4. Click **OK**.

Managing a host

Once you have configured the computers in your configuration group, use the Host Administrator to start, stop, or connect to any managed host in the group.

To manage a host using MMC

1. In the MMC left window pane, in the Configuration Group list, right-click the computer that you want to manage, then click **All Tasks**.
2. Do one of the following:
   - Click **Start Specific Host** to start a host session on the selected host computer, using the settings that are configured in the admin.bhf host file.
   - Click **Start Admin Host** to start a host session on the Host Administrator computer, using the settings that are configured in the admin1n.bhf host file.
   - Click **Start Last Host** to start a host session on the computer on which you most recently started a host session.
   - Click **Stop Host** to cancel the host session and disconnect any active sessions on the host.
   - Click **Connect to Admin Host** to connect to the Host Administrator computer, using the settings that are configured in the admin.chf remote file.
   - Click **Configure Admin Host** to reconfigure the settings on the Host Administrator computer.
   - Click **Get Activity Log** to retrieve the activity log from the remote computer.

Understanding SNMP and central logging

Security, accountability, and logging are important concerns in a distributed computing environment. pcAnywhere provides an extended logging utility, which supports event logging on centralized servers. An administrator can collect logging information from every pcAnywhere host on the network and store this information on a single computer.

The pcAnywhere Host Administrator MMC tool can retrieve log files from a remote computer on the network and let the administrators view and process them locally.

pcAnywhere also supports logging on a Simple Network Management Protocol (SNMP) monitor. SNMP is used to send SNMPv1 events to a compatible console, which records the information. pcAnywhere provides a Management Information Base (MIB) containing over 40 SNMP generated events. pcAnywhere also lets an administrator direct the SNMP logging to multiple consoles.

Using SNMP event consoles

pcAnywhere 10.0 supports any SNMP event console that handles SNMP traps, such as Unicenter TNG, SMS, and Tivoli NetView. The event console usually has a way to automate actions, depending on the incoming SNMP trap and the variable that it contains. The capabilities of the automated action, typically referred to as a rule or action, vary for each network management platform. Most include the facility to start any program that can be run from the command line.

Using Awshim.exe

AwShim is the pcAnywhere management shim between pcAnywhere and the network management integration. The Host Administrator uses AwShim to start and stop host and remote sessions. For each action, you can specify specific host or remote configuration files.

AwShim uses the following parameters:

- -A Action
- -B Bhf File Name
- -C Chf File Name
- -H HostName on which to perform action
- -R Remote machine to which to connect

Supported actions with -A parameter:

- STARTHOST
- STARTREMOTE
- STOPHOST

The -B and -C parameters specify the Be Host and Call Host items that are contained in the CMS folder in the pcAnywhere directory.

The -H parameter identifies the name or address of the host computer on which the action is performed.

The -R parameter is only used with STARTREMOTE to specify the name of the host computer to which the remote connects. Whenever a remote is started, all connection parameters specified in the CHF file are used, with the exception of the host computer address. This address must be specified with the -R parameter.

When a password protected connection item is run on a managed computer, the password prompt appears only on the managed computer. The password prompt is not displayed on the computer from which the administrator initiated the action.

Using the pcAnywhere v10.0 MIB

The pcAnywhere MIB outlines over 40 different SNMP traps, which pcAnywhere can generate. Use the pcAnywhere MIB as a tool to help build automated responses to pcAnywhere events that occur on the network.

The MIB file is located in the following directory:

\Program Files\Symantec\pcAnywhere\CMS

```
--
--  pcANYWHERE MIB Definitions
--  Copyright 2001, Symantec Corporation.
--
PCA-Alert-MIB DEFINITIONS ::= BEGIN
IMPORTS
enterprises
FROM RFC1155-SMI
OBJECT-TYPE
FROM RFC-1212
TRAP-TYPE
FROM RFC-1215
DisplayString
                FROM RFC1213-MIB;
symantec        OBJECT IDENTIFIER ::= { enterprises 393 }
pcanywhere      OBJECT IDENTIFIER ::= { symantec 100 }
pcaversionnine  OBJECT IDENTIFIER ::= { pcanywhere 9 }
PcaHost         OBJECT IDENTIFIER ::= { pcaversionnine 1 }
PcaRemote       OBJECT IDENTIFIER ::= { pcaversionnine 2 }
PcaFileXfer     OBJECT IDENTIFIER ::= { pcaversionnine 3 }
PcaGateway      OBJECT IDENTIFIER ::= { pcaversionnine 4 }
PcaMonitor      OBJECT IDENTIFIER ::= { pcaversionnine 5 }
```

```
PcaInstall       OBJECT IDENTIFIER ::= { pcaversionnine 6 }
PcaReset         OBJECT IDENTIFIER ::= { pcaversionnine 7 }
PcaLDAP          OBJECT IDENTIFIER ::= { pcaversionnine 8 }
PcaObject        OBJECT IDENTIFIER ::= { pcaversionnine 9 }
-- Pca Alert Objects - These are not able to be queried,
-- however they are used for the trap variables we will bind
-- to specific traps.
HostComputerName  OBJECT-TYPE
              SYNTAX    DisplayString (SIZE (0..128))
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION "The computer that is running the
PCA Host"
              ::= { PcaObject 1 }
RemoteComputerName  OBJECT-TYPE
              SYNTAX    DisplayString (SIZE (0..128))
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
"The computer that is running the PCA Remote"
              ::= { PcaObject 2 }
CallerName    OBJECT-TYPE
              SYNTAX    DisplayString (SIZE (0..128))
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
"The name of the remote caller."
              ::= { PcaObject 3 }
HostConnectionObject    OBJECT-TYPE
              SYNTAX    DisplayString (SIZE (0..255))
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
"The name of the connection object used to start the PCA
Host"
              ::= { PcaObject 4 }
RemoteConnectionObject    OBJECT-TYPE
              SYNTAX    DisplayString (SIZE (0..255))
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
```

```
"The name of the connection object used to start the PCA
Remote"
              ::= { PcaObject 5 }
XferFiles OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS  read-only
              STATUS  optional
              DESCRIPTION
"Number of files transferred by file transfer"
              ::= { PcaObject 6 }
XferBytes OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS  read-only
              STATUS  optional
              DESCRIPTION
"Number of bytes transferred by this file transfer
operation"
              ::= { PcaObject 7 }
XferOperation OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS  read-only
              STATUS  optional
              DESCRIPTION
"The operation last performed by file transfer"
              ::= { PcaObject 8 }
XferVirusFlag OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS  read-only
              STATUS  optional
              DESCRIPTION
"This is the file transfer virus flag."
              ::= { PcaObject 9 }
XferSourceFile    OBJECT-TYPE
              SYNTAX    DisplayString (SIZE (0..255))
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
"The name of the source file in a file transfer operation"
              ::= { PcaObject 10 }
XferDestFile    OBJECT-TYPE
              SYNTAX    DisplayString (SIZE (0..255))
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
"The name of the destination file in a file transfer
operation"
              ::= { PcaObject 11 }
HostEncryptionLevel  OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS  read-only
              STATUS  optional
              DESCRIPTION
"The desired encryption level of the PCA Host"
              ::= { PcaObject 12 }
RemoteEncryptionLevel OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS  read-only
              STATUS  optional
              DESCRIPTION
"The desired encryption level of the PCA Remote"
              ::= { PcaObject 13 }
HostEndedReason OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS  read-only
              STATUS  optional
              DESCRIPTION
"The reason a PCA Host was terminated"
              ::= { PcaObject 14 }
DeviceType OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS  read-only
              STATUS  optional
              DESCRIPTION
"This represents the type of device in which a connection was
made."
              ::= { PcaObject 15 }
XferFailedFlag OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS  read-only
              STATUS  optional
              DESCRIPTION
"Flag is set if a file transfer operation had failed."
```

```
              ::= { PcaObject 16 }
Encryption Error Message OBJECT-TYPE
              SYNTAX  Displaystring (size )0...255))
              ACCESS  send-only
              STATUS  optional
              DESCRIPTION "encryption message."
              ::= { PcaObject 17}
-- Pca Host Alert Traps
PcaHostStarted   TRAP-TYPE
ENTERPRISE  PcaHost

VARIABLES   { DeviceType, HostConnectionObject}
DESCRIPTION "PCA Host was started"
                 ::= 1
PcaHostEndSession TRAP-TYPE
ENTERPRISE  PcaHost
VARIABLES   {HostEndedReason}
DESCRIPTION "PCA Host has shut down"
                 ::= 2
PcaHostAbnormalEnd   TRAP-TYPE
ENTERPRISE  PcaHost
DESCRIPTION "PCA Host has shut down abnormally"
                 ::= 3
PcaHostConnFailDeviceError   TRAP-TYPE
ENTERPRISE  PcaHost
VARIABLES   {DeviceType}
DESCRIPTION "PCA Host connection failed - device error"
                 ::= 4
PcaHostStopped   TRAP-TYPE
ENTERPRISE  PcaHost
VARIABLES   {HostEndedReason}
DESCRIPTION "PCA Host was stopped"
                 ::= 5
PcaHostInSession   TRAP-TYPE
ENTERPRISE  PcaHost
VARIABLES   {RemoteComputerName, CallerName}
DESCRIPTION "PCA Host is in session"
                 ::= 6
PcaHostConnFailAccessDenied   TRAP-TYPE
ENTERPRISE  PcaHost
```

```
VARIABLES   {RemoteComputerName, CallerName}
DESCRIPTION "PCA Host connection failed - access denied"
                 ::= 7
PcaHostConnFailEncrypt   TRAP-TYPE
ENTERPRISE  PcaHost
VARIABLES   {HostEncryptionLevel, RemoteEncryptionLevel}
DESCRIPTION "PCA Host connection failed - encryption error"
                 ::= 8
PcaHostUnsecuredHostStarted   TRAP-TYPE
ENTERPRISE  PcaHost
VARIABLES   {HostConnectionObject}
DESCRIPTION "PCA Host was launched insecurely"
                 ::= 9
PcaHostRebooting   TRAP-TYPE
ENTERPRISE  PcaHost
DESCRIPTION "PCA Host rebooting the system"
                 ::= 10
PcaHostLockingWorkstation TRAP-TYPE
ENTERPRISE  PcaHost
DESCRIPTION "PCA Host locking workstation"
        ::= 11
PcaHostLoggingOffUser TRAP-TYPE
ENTERPRISE  PcaHost
DESCRIPTION "PCA Host is logging off the current user"
        ::= 12
-- PCA Remote Generated Traps
PcaRemoteStarted   TRAP-TYPE
ENTERPRISE  PcaRemote
VARIABLES   {DeviceType, RemoteConnectionObject}
DESCRIPTION "PCA Remote was started"
                 ::= 1
PcaRemoteInSession   TRAP-TYPE
ENTERPRISE  PcaRemote
VARIABLES   {HostComputerName}
DESCRIPTION "PCA Remote is in session"
                 ::= 2
PcaRemoteEndSession   TRAP-TYPE
ENTERPRISE  PcaRemote
DESCRIPTION "PCA Remote has ended the session"
                 ::= 3
```

```
PcaRemoteAbnormalEndSession   TRAP-TYPE
ENTERPRISE  PcaRemote
DESCRIPTION "PCA Remote has ended the session abnormally"
                 ::= 4
PcaRemoteConnFailDeviceError   TRAP-TYPE
ENTERPRISE  PcaRemote
VARIABLES   {DeviceType}
DESCRIPTION "PCA Remote connection failure - device error"
                 ::= 5
PcaRemoteConnFailHostBusy   TRAP-TYPE
ENTERPRISE  PcaRemote
DESCRIPTION "PCA Remote connection failure - host busy"
                 ::= 6
PcaRemoteConnFailHostNotFound   TRAP-TYPE
ENTERPRISE  PcaRemote
DESCRIPTION "PCA Remote connection failure - host not found"
                 ::= 7
PcaRemoteConnFailBadPassword   TRAP-TYPE
ENTERPRISE  PcaRemote
DESCRIPTION "PCA Remote connection failure - bad password"
                 ::= 8
PcaRemoteConnFailEncryption   TRAP-TYPE
ENTERPRISE  PcaRemote
VARIABLES   {RemoteEncryptionLevel, HostEncryptionLevel}
DESCRIPTION "PCA Remote connection failure - encryption
error"
                 ::= 9
-- PCA File Transfer Generated Traps
PcaFileXferStarted   TRAP-TYPE
ENTERPRISE  PcaFileXfer
VARIABLES   {HostComputerName, RemoteComputerName,
HostConnectionObject, RemoteConnectionObject, DeviceType}
DESCRIPTION "PCA File Transfer started"
                 ::= 1
PcaFileXferEnded   TRAP-TYPE
ENTERPRISE  PcaFileXfer
VARIABLES   {XferFiles, XferBytes}
DESCRIPTION "PCA File Transfer ended"
                 ::= 2
PcaFileXferAbnormalEnd   TRAP-TYPE
ENTERPRISE  PcaFileXfer
```

```
VARIABLES   {ComputerName}
DESCRIPTION "PCA File Transfer ended abnormally"
                 ::= 3
PcaFileXferOperationCancelled   TRAP-TYPE
ENTERPRISE  PcaFileXfer
DESCRIPTION "PCA File Transfer operation cancelled"
                 ::= 4
PcaFileXferOperation   TRAP-TYPE
ENTERPRISE  PcaFileXfer
VARIABLES   { XferOperation, XferSourceFile, XferDestFile,
XferBytes, XferVirusFlag, XferFailedFlag}
DESCRIPTION "PCA File Transfer received file"
                 ::= 5
-- PCA Monitor Traps
PcaMonitorFullProductNotInstalled   TRAP-TYPE
ENTERPRISE  PcaMonitor
DESCRIPTION "PCA Monitor - The PCA Full product is not
installed"
                 ::= 1
PcaMonitorHostNotInstalled   TRAP-TYPE
ENTERPRISE  PcaMonitor
DESCRIPTION "PCA Monitor - The PCA Host is not installed"
                 ::= 2
PcaMonitorRemoteNotInstalled   TRAP-TYPE
ENTERPRISE  PcaMonitor
DESCRIPTION "PCA Monitor - The PCA Remote is not installed"
                 ::= 3
PcaMonitorHostNotWaiting   TRAP-TYPE
ENTERPRISE  PcaMonitor
DESCRIPTION "PCA Monitor - The PCA Host is not waiting for a
connection"
                 ::= 4
```

```
PcaMonitorHostNotAutoStart   TRAP-TYPE
ENTERPRISE  PcaMonitor
DESCRIPTION "PCA Monitor - The PCA Host is not set to auto
start"
                 ::= 5
PcaMonitorHostNotWaitingOnDialup   TRAP-TYPE
ENTERPRISE  PcaMonitor
DESCRIPTION "PCA Monitor - The PCA Host is not waiting on a
dialup"
                 ::= 6
PcaMonitorHostLanOnlyNotInstalled   TRAP-TYPE
ENTERPRISE  PcaMonitor
DESCRIPTION "PCA Monitor - The PCA Host LAN only is not
installed"
                 ::= 7
PcaMonitorLiveUpdateNotRun   TRAP-TYPE
ENTERPRISE  PcaMonitor
DESCRIPTION "PCA Monitor - Live Update was not run on this
host"
                 ::= 8
-- Reset Events
-- These events are defined so that when generated by
-- the monitor they can be used to clear the status of
-- previously generated events.
PcaResetNotInstalledReset   TRAP-TYPE
ENTERPRISE  PcaReset
DESCRIPTION "PCA Monitor - Reset install traps"
                 ::= 1
PcaResetHostNotWaitingReset   TRAP-TYPE
ENTERPRISE  PcaReset
DESCRIPTION "PCA Monitor - Reset Host not waiting traps"
                 ::= 2
PcaResetHostNotAutoStartReset   TRAP-TYPE
ENTERPRISE  PcaReset
DESCRIPTION "PCA Monitor - Reset Host not auto start traps"
                 ::= 3
PcaResetHostWaitingOnDialupReset   TRAP-TYPE
ENTERPRISE  PcaReset
DESCRIPTION "PCA Monitor - Reset Host waiting on dialup
traps"
                 ::= 4
PcaResetLiveUpdateNotRunReset   TRAP-TYPE
```

```
ENTERPRISE  PcaReset
DESCRIPTION "PCA Monitor - Reset Live Update not run traps"
                 ::= 5
-- pcA Install Traps
PcaInstallRebootRequired  TRAP-TYPE
ENTERPRISE  PcaInstall
DESCRIPTION "PCA Install - A reboot is required"
                 ::= 1
        END
```

Monitoring network performance

Network administrators can identify and troubleshoot problems on the network by setting SNMP traps. This information can then be sent to multiple computers, so, for example, all members of your IT department have access to the same information. To use this feature, you must have Microsoft Management Console, Microsoft Systems Management System, or UniCenter TNG installed on the host server.

To monitor performance using SNMP traps

1. In the pcAnywhere Manager window, click **Tools > Options**.
2. On the Event Logging tab, check **Enable SNMP traps**.
3. Click **Add** to specify which computers should receive the logging information.
4. In the SNMP Trap Destination dialog box, type an IP address.
5. Repeat steps 3 and 4 to add more destinations.
6. Click **OK**.

Using the Microsoft Distributed Component Object Model (DCOM)

pcAnywhere uses Microsoft DCOM technology for all point-to-point communications during remote management tasks. DCOM is used in the Host Administrator as well as in every pcAnywhere integration into network management applications.

DCOM runs on a variety of network protocols and, by default, attempts to make connections on all installed protocols. After connecting to the network, it uses Windows NT Authentication to verify the necessary access privileges. For example, an administrator with access privileges can perform management tasks on a locked pcAnywhere host from any location.

To ensure that NT Authentication is used for pcAnywhere DCOM management tasks, pcAnywhere connection items should be configured to use the same Windows NT domain or a trusted domain.

Implementing DCOM on Windows platforms

pcAnywhere configures DCOM during the installation process. The default settings should be sufficient for pcAnywhere management applications to function normally and maintain a sufficient amount of security. However, modifications can be made to DCOM to alter default security and let an administrator explicitly allow or deny DCOM access to a system.

Configuring Windows NT for DCOM

To remotely configure and control pcAnywhere on Windows NT from a network management system, the network administrator must comply with the following requirements:

- The administrator must be logged on as a domain administrator.
- The administrator's computer and the client's computer must be in the same domain.

The Windows NT default configuration requires all manager activity to be authenticated on the Windows NT domain.

Configuring Windows 9x for DCOM

To remotely configure and control pcAnywhere on Windows 9x from a network management system, the network administrator must comply with the following requirements:

- The Windows 9x client must be logged on to the same Windows NT domain as the network administrator.
- The domain name and the workgroup name on the Windows 9x computer must be the same.
- The Windows 9x computer must be configured with user level access. This access is required to adjust the DCOM security settings when running dcomcnfg.exe.

- File and print sharing for Microsoft Windows Networks should be installed and enabled on the Windows 9x computer.

Note: If Allow pcAnywhere to be remotely managed is checked during the pcAnywhere installation, the DCOM settings are automatically modified to the required defaults.

Meeting these configuration requirements should resolve any connectivity problems encountered when using the pcAnywhere Host Administrator or one of the pcAnywhere Network Management integration components.

The most common failure experienced is an Access Denied error. Typically, this error occurs because of incorrect DCOM settings. Use the dcomcnfg.exe utility to modify security settings for the client to resolve the error. Edit the default security and add only the domain users or administrators who are allowed to access the host.

Modifying DCOM settings

pcAnywhere configures DCOM during the installation process. The default settings should be sufficient to allow pcAnywhere management applications to function normally.

To modify DCOM settings on Windows NT

- From the \WinNT\System32 folder, run dcomcnfg.exe.

To modify DCOM settings on Windows 9x

- From the \Windows\System folder, run dcomcnfg.exe.

Modifying DCOM security settings on a managed computer might require adjustments to the DCOM settings on the administrator computer. Be sure that all managed computers are authenticating on the same Windows NT domain or on trusted domains.

When an administrator connection is made to a remote computer, the management software attempts to impersonate the user who is making the connection. If the user is not logged on to a Windows NT system with administrator privileges, this impersonation fails.

To further ensure security, a caller without Windows NT administrator privileges cannot perform administrator functions or have access beyond what they would normally have when logged on to the computer directly.

To avoid connection problems because of access denied errors, make sure the computer that is running the management shim and host administrator can access the shared drives on the remote system without having to enter a password.

For more information, consult the dcomcnfg.exe online documentation.

CHAPTER 6

Integrating pcAnywhere with Directory Services

The Directory Services feature in pcAnywhere is an example of a Lightweight Directory Access Protocol (LDAP) client application, which stores and retrieves information about users. It facilitates looking up host computers that are waiting for a connection on the Internet or Intranet.

Directory servers enable communication using the LDAP protocol. pcAnywhere supports any client developed with the LDAP SDK.

The benefit of using directory services with pcAnywhere is increased speed. Normally, when you launch a remote connection, it scans the network for waiting pcAnywhere hosts. This can be time consuming and the results can vary depending on the size of the network and whether the host is on a different subnet. LDAP-registered hosts provide instant results to remote queries.

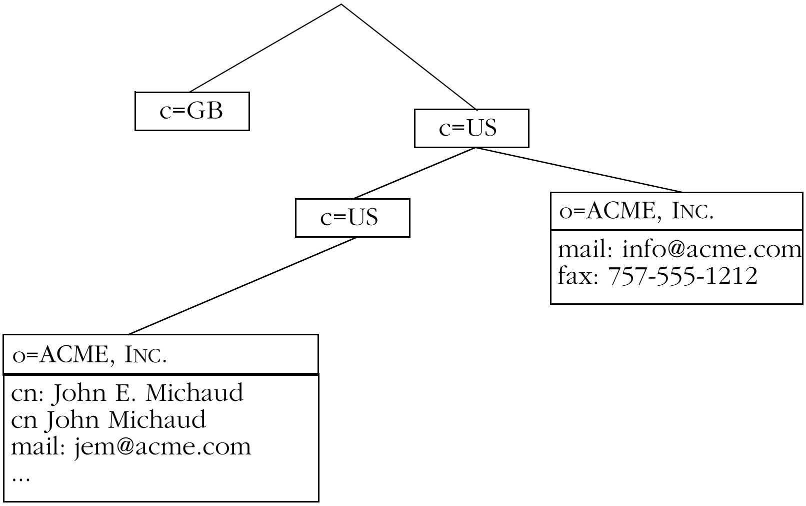
This chapter contains the following:

Overview of LDAP informational model

The LDAP directory stores information in a hierarchical tree structure that is similar to a file system with subdirectories and files. Each object in the directory is called an entry. Entries can be either containers or leaf entries.

Containers are entries that can hold other entries while leaf entries are the endpoints of the tree. These types of entries are used to show an organizational structure by creating entries that represent countries, organizational units, and people that fit into the various areas of the organization.

The following example has entries representing countries at the top of the tree. Below them are entries representing states or national organizations. Below them might be entries representing people, organizational units, printers, or any other type of information.



LDAP lets attributes be stored with each entry to provide further information about the entry such as a person's name, email address, phone number, or title. Each entry may contain many values for the same attribute.

The attributes that can be stored with an entry are determined by the objectclass they belong to. An LDAP server has a list of all known objectclasses. Administrators can add new and edit existing objectclasses to let client applications store specific types of attributes. The objectclass is stored as an entry attribute and controls which attributes are required and permitted in an entry. Some common objectclass values are person, organizationalUnit, and organizationalPerson. Combinations of objectclasses can be used to represent complex entries such as employees in a company.

Using Directory Services with pcAnywhere

In Directory Services, the host starts and waits for incoming connections as usual. At the same time, the host connects to an LDAP server and updates the user's entry by adding an attribute that stores the current IP address, the computer name, and the current status of the host.

When the remote starts, a new application, the Directory Services browser, launches and connects to an LDAP server. The Directory Services browser queries all entries that satisfy its filter criteria and displays the entries in a list view. When one of the entries is double-clicked, the remote connects to the selected host.

Configuring the directory servers

Before you can use directory services in pcAnywhere, you need to configure a directory server so that it works with pcAnywhere. Follow the instructions for the type of directory server that you use.

Configuring the LDAP server

To use directory services, add a custom objectclass description to the LDAP server's configuration. This custom objectclass describes the information the LDAP server needs to store for each host that a user starts. Once the custom objectclass is available, modify all existing entries to store values that belong to the new objectclass.

The custom pcAnywhere objectclass must be called pcaHost and must contain a single binary attribute called pcaHostEntry:

objectclass: pcaHost

pcaHostEntry: binary

Configuring Netscape Directory Server 3.1

Administrator rights are needed to perform this task.

To configure Directory Services

1 Connect to the Server Administration page with Netscape Communicator 4.5.

2 Click the button for the configured directory server.

3 On the top selection bar, click **Schema**.

4 On the left selection bar, click **Edit or View Attributes**.

5 In the Attribute Name field, type **pcaHostEntry**.

6 In the Syntax box, click **Binary**.

7 Under Manage Attributes, click **Add New Attribute**.

8 Type the password for the Directory Manager, then click **Submit**.

9 On the left selection bar, click **Create Objectclass**.

10 In the ObjectClass Name field, type **pcaHost**.

11 In the Available Attributes list, locate the objectclass attribute and click **Add** to include it in the Required Attributes list.

12 In the Available Attributes list, locate the pcaHostEntry attribute and add it to the Allowed Attributes list.

13 Click **Create New ObjectClass**.

14 Type the password for Directory Manager.

15 Click **Submit**.

16 Restart the server for the new settings to take effect.

Configuring Netscape Directory Server 4.0

Administrator rights are needed to perform this task.

To configure Directory Services

1 Start the Netscape Console 4.0 application.

2 In the left-hand tree view, open the item that represents this server.

3 Open the Server Group.

4 Double-click the **Directory Server** item.

5 On the Configuration tab, in the left-hand tree view, open the **Database** item.

6 Click the **Schema** sub-item.

7 On the Attributes tab, click **Create**.

8 In the Attribute Name field, type **pcaHostEntry**.

9 For Syntax, click **Binary**.

10 Click **Multi-Valued**, then click **OK**.

11 On the Object Classes tab, click **Create**.

12 In the Name field, type **pcaHost**.

13 In the Available Attributes box, click **objectclass**.

14 Click **Add** to include the Required Attributes box.

15 In the Available Attributes box, click **pcaHostEntry**.

16 Click **Add** to include the Allowed Attributes box.

17 Click **OK** to add the object class.

18 On the Tasks tab, click **Restart the Directory Server**.

19 At the prompt, click **Yes**.

Configuring Novell v5.0 server

The following steps only apply if LDAP is installed, configured, and functioning on the Novell server with NDS 8.0.

Administrator rights to the server are needed to perform these steps.

To create the pcaHostEntry in ConsoleOne

1 Log onto the LDAP server that contains the LDAP group object.

2 Open ConsoleOne from:

sys:public\mgmt\ConsoleOne\1.2\bin\ConsoleOne.exe

3 On the Tools menu, click **Schema Manager**.

4 On the Attribute tab, click **Create**.

5 Click **Next**.

6 In the Attribute Name field, type **pcaHostEntry**, leaving the ASNI ID field blank.

All entries are case sensitive.

7 Click **Next**.

8 For the Attribute Syntax, click **Octet String**.

9 For the Attribute Flag, click **Public Read**.

10 Click **Next**.

11 Click **Finish**.

To create the pcaHost object in ConsoleOne

1 Open ConsoleOne from sys:public\mgmt\ConsoleOne\1.2\bin\ConsoleOne.exe.

2 On the Tools menu, click **Schema Manager**.

3 On the Class tab, click **Create**.

4 Click **Next**.

5 In the Name field, type **pcaHost**, leaving the ASNI ID blank.

This entry is case sensitive.

6 Click **Next**.

7 Click **Auxiliary Class**.

8 Click **Next**.

9 Double-click **Top** and add it to the Inherit From box.

10 Click **Next**.

Objectclass appears in the Add These Attributes window.

11 Click **Next**.

12 Double-click the pcaHostEntry and add it to the Add These Attributes window.

13 Click **Next**.

Review the summary for the new class to be created.

14 Click **Finish**.

To map the LDAP attribute to the NDS attribute

1 Double-click the **LDAP Group** icon.

2 On the Attribute Map tab, click **Add**.

3 In the LDAP attribute field, type **pcaHostEntry;binary**.

4 In the NDS Attribute box, click **pcaHostEntry**.

5 Click **OK**.

6 Click **Add**.

7 In the LDAP attribute field, type **pcaHostEntry**.

This entry is case sensitive and must be entered exactly as it appears above.

8 In the NDS Attribute box, click **pcaHostEntry**.

9 Click **OK**.

10 Do one of the following:

- Click **Apply** to map other attributes.
- Click **OK** to finish.

11 To modify the attributes for this map, highlight the attribute and click **Modify**.

To map the NDS class to the LDAP class

1. Double-click the **LDAP Group** icon.
2. On the Class Map tab, click **Add**.
3. In the LDAP class field, type **pcaHost**.

   This entry is case sensitive and must be entered exactly as it appears above.
4. In the NDS Attribute box, click **pcaHost**.
5. Click **OK**.
6. Do one of the following:
   - Click **Apply** to map other attributes.
   - Click **OK** to finish.

Note: To perform the following steps, you need access to a word processing utility such as Notepad, as well as access to the server or remote control through Rconag6.nlm and Rconj.exe.

To create an LDIF file

1. In Notepad, type the following four lines for each user:

   DN:cn=user,ou=organization_unit,o=organization

   Changetype:modify

   Add:objectclass

   Objectclass:pcaHost
2. Save this file locally and copy it to sys:system\schema\.
3. At the server prompt, type **Load Bulkload.nlm**.
4. Click **Apply LDIF file**.
5. At the prompt, type the log path:

   sys:system\schema\

To assign rights to an individual user

1. Select the LDAP server.
2. Right-click a user, then click **Trustees of the object**.
3. Click the user.
4. Click **Assigned Rights**.
5. Click **Add a Property**.

6. Uncheck **Show Only Properties Of This Object Class**.
7. Click **pcaHostEntry**.
8. Click **OK**.
9. Click the write access rights to apply to this property.
10. Click **OK**.

To assign rights to multiple users

1. Click the container in which to place the group.
2. Right-click the container, then click **New** > **Group**.
3. Type a name for the group.
4. Right-click the group name, then click **Properties**.
5. On the Members tab, click **Add** to include other users.
6. On the File menu, click **Properties Of Multiple Objects** to establish access rights.
7. On the NDS Rights tab, click **Add Trustee**.
8. Click the pcAnywhere group, then click **OK**.
9. Click **Add Property**.
10. Uncheck **Show Only Properties Of This Object Class**.
11. Click **pcaHostEntry**.
12. Click **OK**.
13. Click the write access rights to apply to this user group.
14. Click **OK**.

Configuring Windows Active Directory

The Windows 2000 server with Active Directory must be installed and configured before configuring pcAnywhere for Windows 2000 active directory.

Administrator rights to the server are needed to perform these steps.

Extending the Schema

To extend the schema, you add the snap-in, create the pcaHostEntry attribute, create the pcaHost object, associate the pcaHost object with the user class object, then set the rights for the pcAnywhere user.

To add the snap-in

1. On the Windows taskbar, click **Start** > **Run**.
2. Type **MMC**.
3. Click **OK**.
4. On the Console1 toolbar, click **Console** > **Add/Remove Snap-in**.
5. In the Add/Remove Snap-in dialog box, click **Add**.
6. Click **Active Directory Schema**, then click **Add**.
7. Close the Add standalone snap-in dialog box.
8. In the Add/Remove Snap-in dialog box, click **OK**.
9. In the left pane, right-click **Active Directory Schema**, then click **Operations Master**.
10. Check **The schema may be modified on this Domain Controller**.
11. Click **OK**.

To create the pcaHostEntry attribute

1. In the left pane, expand the **Active Directory** schema item in the left pane.

   The Classes and Attribute subfolders should now be available.
2. Right-click the **Attributes** folder, then click **Create Attribute**.

   Continue through the resulting warning message.
3. In the Common Name entry field, type **pcaHostEntry**.

   This is case sensitive, and must be typed exactly as it appears.
4. In the LDAP Display Name field, type **pcaHostEntry** exactly as it appears.
5. In the Unique X500 Object ID field, type:

   1.3.6.1.4.1.393.100.9.8.1
6. In the syntax list, click **Octet string**.
7. Check **Multi-Valued**.
8. Click **OK**.
9. In the left pane, right-click the **Classes** folder, then click **Create Class**.

   Continue through the warning message.

To create the pcaHost object

1. In the Common Name entry field, type **pcaHost**.

This is case sensitive, and must be typed exactly as it appears.

2 In the LDAP Display Name field, type **pcaHost** exactly as it appears.

3 In the Unique X500 Object ID field, type:

1.3.6.1.4.1.393.100.9.8.2

4 In the Parent class field, type **Top**.

5 In the Class list, click **Auxilary**.

6 Click **Next**.

7 In the Create New Schema Class dialog box, click the **Add** button for the Optional attribute field.

8 Select the pcaHostEntry attribute.

9 Click **OK**.

The pcaHostEntry should appear as an optional attribute.

10 Click **Finish**.

To associate the pcaHost object with the user object class

1 In the left pane of Console1, expand the Class folder.

2 Right-click the user object class, then click **Properties**.

3 Select the Relationship tab, and click **Add** for the Auxiliary Classes field.

4 Select the pcaHost object class.

5 Click **OK**.

6 Click **Apply**.

7 Click **OK**.

8 In the left pane, right-click **Active Directory Schema**.

9 Click **Reload the Schema**.

Setting the rights for the pcAnywhere user

To set up the rights for the pcAnywhere user, you must first set up view rights, and then set up modify rights.

To set up view rights for the user

1 On the Windows taskbar, click **Start** > **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.

2 On the View menu, make sure Advanced Features is checked.

This enables the Security tab in the property pages.

You can set the following rights at any organizational unit. Ideally, you set these rights at the level containing the pcAnywhere users.

3 Right-click the organizational unit, then click **Properties**.

4 On the Security tab, click **Add**.

5 Click the **Everyone** group.

6 Click **Add**.

7 Click **OK**.

8 In the Allow column, check **Read Only**.

9 On the organizational unit's property page, click **Advanced**.

10 Select the Everyone group that you just added.

11 Click **View/Edit**.

12 On the Object tab, in the Apply onto list, click **This object and all child objects**.

13 Click **OK** until you close the Security property page.

To set up modify rights for the user

1 On the organizational unit's Security tab, click **Add**.

2 Click the **Self** group.

3 Click **Add**.

4 Click **OK**.

5 In the Allow column, check **Write**.

6 Click **Advanced**.

7 Select the Self group that you just added, then click **View/Edit**.

8 On the Object tab, in the Apply onto list, click **Child objects only**.

9 Click **OK** until you close the Security property page.

Configuring pcAnywhere to use directory services

You can set up pcAnywhere to use directory services in three different ways:

- Set up directory services in pcAnywhere Options so that all connection items use the same settings.

- Set up directory services for a host connection item.
- Set up directory services for a remote connection item.

Setting up directory services in pcAnywhere options

Configure the directory server entries before beginning.

To set up directory services in pcAnywhere options

1. On the Tools menu, click **Options**.
2. On the Directory Services tab, click **Add**.
3. In the Display Name field, type a name that clearly describes the directory server.
4. In the Directory Server field, type the host name or IP address of the directory server.
5. In the Name field, type the account name specified on the directory server.
6. In the Password field, type the password that authenticates the account.

   The password is case sensitive.
7. Click **Advanced** to configure the port number and the search base of the directory tree.

   The Port number controls the port that the directory server uses to accept queries from the client. The default port is 389. Search Base is the root of the directory structure that begins the query search.
8. Click **OK**.

   pcAnywhere attempts to connect to the directory server and search for the entry specified in the Name field. If multiple entries are found, users must select the one that represents them. Once the entry is identified, pcAnywhere stores its Distinguished Name in the registry for easy identification and labels the entry as Verified.

   Note: Common reasons for failed verification include being disconnected from the network, having incorrect TCP/IP configuration settings, using an incorrect user name or password, or not having user information configured on the server.

Setting up the host computer

When you set up a host connection to use directory services, pcAnywhere searches the directory server for the specified common name when you launch the host connection. If it finds a corresponding entry, it updates it with the connection information and current status of the host.

As the status changes, the host updates its entry in the directory server so that remote computers can see the current status. When the host is cancelled, it resets the host user's entry.

To set up the host computer to use directory services

1. In the pcAnywhere Manager window, click **Hosts**.
2. Right-click a host connection item that uses a network connection, then click **Properties**.
3. On the Settings tab, click **Use directory services**.
4. Select the appropriate directory server in the list.
5. Click **OK**.

   The directory server entry selected in the Directory Servers box is used to register this host when it starts.

Setting up the remote computer

When you set up a remote connection to use directory services, the remote looks on the directory server for waiting host connections.

To configure a remote object

1. In the pcAnywhere Manager window, click **Remotes**.
2. Right-click a remote connection item that uses a network connection, then click **Properties**.
3. On the Settings tab, click **Use directory services**.
4. Select a directory server in the list.

   The list contains only the directory servers that have been pre-configured and verified.
5. Click **Filter** to set the initial filter settings.

   The Filter Page narrows the results. Fill out some or all of the fields. Only the entries matching those criteria are returned. You can use wildcards in these fields. For example, A* returns entries that have a name beginning with the letter A.

CHAPTER 7

Securing Symantec pcAnywhere

Network security is a paramount concern because of the growing number of mobile professionals who need external access to their corporate computer networks, the increasing complexity of maintaining these networks, and the rising value of intellectual property that is stored inside the computer infrastructure. Network administrators must balance the need for remote access with the need to protect their systems from unauthorized access and system overload.

Symantec pcAnywhere has a number of built-in security features designed to ensure a secure computing environment. Many of these security features are integrated with the inherent security features of the network operating system.

For more information on using and configuring these features, see the *Symantec pcAnywhere User's Guide.*

This chapter contains the following:

- How pcAnywhere works with Windows security
- Securing connections to the host
- Securing pcAnywhere sessions
- Securing pcAnywhere configuration
- Auditing sessions

How pcAnywhere works with Windows security

pcAnywhere runs on all Microsoft Windows 32-bit operating systems; however, if maintaining the highest level of security is a priority, Windows NT and Windows 2000 are the recommended operating systems. Although pcAnywhere runs on Windows 9x and Windows ME, these operating systems are not designed for security.

pcAnywhere is integrated into several portions of the Windows NT and Windows 2000 platforms to leverage their inherent security features, such as user authentication, event logging, and data encryption. pcAnywhere has its own built-in security features, which provide basic protection, but for the highest level of security, you should use the security measures provided by the operating system.

Although Windows NT and Windows 2000 are among the most secure, publicly available operating systems, public interest groups and hobbyists, as well as malicious users and hackers, constantly test the security of these operating systems. Network administrators should monitor newsgroups, the Symantec Web site, and other reputable Web sites offering information about security. Many sites, including symantec.com, offer patches to address newly discovered security risks.

Securing connections to the host

The first step in securing a computer environment is controlling remote access to the network. Administrators who are concerned about unauthorized access to their networks should limit the number of external entry points into their networking infrastructure. This objective can be achieved by limiting the number of network hosts that are available for remote access, implementing an authentication method, and using centralized remote access servers in place of individual dial-up devices.

Restricting TCP/IP remote connections

Restrict access to pcAnywhere hosts by listing only the TCP/IP addresses that you consider safe. Limiting the number of available hosts reduces exposure of the network and protects the system from unauthorized connections.

Creating remote access accounts

pcAnywhere requires you to create a logon account for each remote user or user group who connects to the host server and to select an authentication method for verifying the user's identity. This information is required for all host sessions to prevent unauthorized access.

Depending on your network configuration, you can configure pcAnywhere to verify a user's credentials by checking a directory server, such as Active Directory Server (ADS) or Novell Directory Server (NDS), a Lightweight Directory Access Protocol (LDAP) compliant database, a Web-based server, a shared directory, or a domain list.

User authentication is required for all pcAnywhere host sessions, regardless of whether a host is waiting for network connections, dial-up connections, or direct connections. If no other method of user authentication is available, use pcAnywhere Authentication.

pcAnywhere Authentication can be used on any operating system. This method of authentication validates users by checking a list of users and passwords that are maintained on the local computer. Because a local computer can be vulnerable to outside attack, this method of authentication is the least secure.

Using Windows-based authentication methods

The following table provides information on the authentication methods available for Microsoft-based platforms.

Microsoft-based authentication methods	Explanation	Implementation in pcAnywhere
ADS (Active Directory Server) (For Windows 2000 only)	Validates a user or group by checking a list stored in an Active Directory Service.	Users can browse an ADS tree for user or group names.
Microsoft LDAP	Validates a user or group by checking a user list stored in a Lightweight Directory Access Protocol (LDAP) 3.0 compliant directory service.	Users must log on to the LDAP server, then can browse for user names.

Microsoft-based authentication methods	Explanation	Implementation in pcAnywhere
NT (For Windows NT and Windows 2000 only)	Validates a user or group by checking a workstation or user domain list.	Users on Windows NT can browse a domain list for user or group names.
Windows	Validates a user or group by checking a Microsoft Networking Shared Directory.	Users on Windows 9x or Windows ME can browse a shared directory for user or group names.

Using Novell-based authentication methods

The following table provides information on the authentication methods for Novell-based platforms.

Novell-based authentication methods	Explanation	Implementation in pcAnywhere
Novell Bindery	Validates a user by checking a list stored in a Novell NetWare Bindery. This method requires Novell NetWare 32.	Users must specify the name of the server and a valid user name.
NDS	Validates a user or group by using a list stored in a Novell Directory Service.	Users can browse an NDS tree for user or group names.
Novell LDAP	Validates a user or group by checking a user list stored in an LDAP 3.0 compliant directory service.	Users must log on to the LDAP server, then can browse for user names.

Using Web-based authentication methods

The following table explains the Web-based authentication methods that are available.

Web-based authentication methods	Explanation	Implementation in pcAnywhere
FTP	Lets a host that is running on an FTP server validate a user by checking a user list associated with the FTP service. User name and password are sent over the network in clear text.	Users must specify a server name and a valid user name.
HTTP Caller Authentication	Lets a host that is running on an HTTP Web server validate a user by checking a user list associated with the HTTP service. User name and password are sent over the network in clear text.	Users must specify a server name and a valid user name.
HTTPS Caller Authentication	Lets a host that is running on an HTTPS Web server validate a user by checking a list associated with an HTTPS service. This method is more secure than FTP and HTTP authentication because the user name and password are encrypted before they are sent over the network.	Users must specify a server name and a valid user name.
Netscape LDAP Caller Authentication	Validates a user by checking a list stored in an LDAP 3.0 compliant directory service.	Users must log on to the LDAP server, then can browse for user names.

Controlling logon attempts

Protect the host server from hacker and denial of service attacks by restricting the number of logon attempts and setting a time limit for logons.

The following table explains where to find settings to control logon security on the host.

Option	Explanation	Location
Prompt to confirm connection	Notifies host user of a connection attempt, and lets the host user choose to accept or deny the connection.	Security Options properties tab for the host connection item.
Make passwords case sensitive	Lets the host user use upper and lower case letters in a password to decrease chances of discovery by unauthorized users.	Security Options properties tab for the host connection item.
Limit login attempts per call	Limits the number of consecutive times that a remote user can attempt to log on to the host computer before being locked out.	Security Options properties tab for the host connection item.
Limit time to complete login	Limits the amount of time that a remote user has to establish a connection on the host computer.	Security Options properties tab for the host connection item.
Callback the remote user (for modem connections only)	Confirms the identity of remote users who connect over a modem. The host computer terminates the connection and calls the remote computer at the specified number. The remote computer must be waiting for a connection.	Callback properties tab for the caller item.

Ending connections securely

It is important to securely end a pcAnywhere session to prevent potential security breaches. pcAnywhere also provides security options for handling an abnormal end of session. These options are available on the Settings property tab for the host connection item. The following table explains the options that are available.

Option	Explanation
Logoff user	Automatically logs off the host user after the session ends.
Restart host computer	Restarts the host computer after the session ends.
Lock NT Workstation (for Windows NT and Windows 2000)	Prevents unauthorized users from cancelling the waiting host by locking the NT workstation with a password.
Use Windows screen saver (for Windows 9x and Windows ME)	Starts the Windows screen saver after the session ends. This option can be used to lock the host computer, if the host user sets a password for the screen saver.

Securing pcAnywhere sessions

pcAnywhere provides a number of options that protect the privacy of a remote control or file transfer session, as well as the security of the host computer during a session. When configuring logon accounts, you can set access privileges to provide full access to the host or restrict the remote user from performing certain tasks. You can use encryption to protect the privacy and integrity of sessions and logon information.

By setting time limits for a session, you can protect the host from malicious users intent on disrupting service, as well as from innocent users who unintentionally forget to end a session. You can also configure the host to automatically disconnect after a long period of inactivity.

Specifying caller privileges

Caller privileges let you limit the level of access that a remote user has to the host computer. pcAnywhere lets you restrict users from performing certain functions on the host, such as blanking the host screen, restarting the host computer, transferring files to or from the host computer, or cancelling the host.

On Windows 9x and Windows ME, you can limit a user's access computer drives on the host. This option is not available for Windows NT or Windows 2000 because those operating systems provide their own drive security measures.

Using data encryption

When deciding whether to use encryption and which method to use, you must balance performance with the need for security. Using strong encryption can protect the privacy and integrity of your data. However, it can also slow performance because stronger encryption requires more resources to process and transfer the data.

Sometimes protecting the security of the data is more important than sacrificing performance. Use strong encryption if the data you are sending is highly confidential or sensitive, and you want to ensure that it came from the right sender and that it has not been viewed by unauthorized users or been otherwise tampered with.

If the security of the data is not as important to you as knowing that it came from the right source, consider encrypting only the user name and password to enhance performance.

If you are using a secure network to transfer data to another user on the same network, you might not need to use encryption at all.

When using encryption, both the host and remote users should choose the same level of encryption. Either user can deny a connection if the other is using a lower level of encryption.

Using public-key encryption

If you choose public-key encryption, pcAnywhere uses a public-key certificate file or store to verify the identity of the person attempting to connect and send data, then uses the faster symmetric encryption to secure the session.

Some configuration is required to ensure that both the host and remote users have access to the appropriate key pairs. Host and remote users must provide each other with their certificates and set up a certificate store, containing the certificates of those users who will connect their computers. The host and remote users should be configured with the common name from their certificates. When a connection is attempted, the common name for the host and the remote are verified for authenticity.

Using symmetric encryption

If you choose symmetric encryption, pcAnywhere generates a unique public key and uses this key to encrypt and safely distribute the symmetric key used to encrypt the session. Because the public key is not obtained from a certificate authority, it does not provide the level of user authentication that public-key encryption does. However, you can offset this factor by using pcAnywhere's caller authentication features.

The Symmetric encryption level is available on any operating system that supports CryptoAPI, such as Windows NT 4.0. For the Windows 95 operating system, CryptoAPI 1.0 is available with OSR2 or with Microsoft Internet Explorer 3.0 and higher.

Using pcAnywhere encryption

pcAnywhere encryption applies a simple transformation to data so that the data stream cannot be easily interpreted by a third party. This encryption level is compatible with earlier versions of pcAnywhere that do not support public-key encryption.

Protecting the privacy of host sessions

pcAnywhere provides a number of options to prevent unauthorized users from viewing or tampering with a host session. You can specify which user (host, remote, or both) has control of the keyboard or mouse, blank the host screen upon connection, and specify whether the remote user can cancel the host session.

Securing pcAnywhere configuration

Configuration is an important issue for network administrators to consider. Even if all security precautions are taken and the network is properly configured, any user who has access privileges to the configuration presents a security risk.

Protecting pcAnywhere connection items

pcAnywhere connection items, which appear as icons in pcAnywhere Manager, contain the settings needed to establish and manage a connection, including what type of hardware device to use, logon information, access privileges, and security settings. You can prevent unauthorized users from viewing, modifying, or launching a host or remote connection item by setting a password.

Protecting caller accounts

Even if you have protected your connection items, you should also set a password for your caller accounts to prevent users who might be authorized to view your other settings from changing user passwords and access privileges.

Choosing a password

A common mistake people make is selecting a password that is easy to remember. Once the user's logon name is known, a simple program can be written that runs through every possible combination of values for the password.

Using numbers, special characters, and mixing upper and lower case letters in the password decreases the chances of discovery. A tip for creating a password that is easy to remember, but difficult for others to decode is to choose a line or title from a book, movie, poem, or song. Then, take the first letter of each word to string together a password, keeping the punctuation or capitalization.

Securing the configuration of pcAnywhere installation packages

pcAnywhere custom installation packages can be integrity stamped, which locks the configuration set. Integrity stamping ensures that users do not bypass the security measures that are configured in the package or otherwise tamper with the configuration.

How integrity checking works

You can significantly reduce the risk of a user inadvertently changing your custom configuration by locking the configuration set before you build and deploy the installation package.

For more information, see "Customizing Symantec pcAnywhere" on page 25.

After a user installs a locked installation package, pcAnywhere automatically checks the integrity of the configuration each time the user launches pcAnywhere, starts a remote session, or starts a host session to ensure that the configuration has not changed.

If pcAnywhere detects that a pcAnywhere executable or configuration file has been changed, the user receives a warning message, indicating that integrity has been compromised, and the user is prevented from using pcAnywhere.

Handling software updates

Any change to a locked configuration set, including the installation of a software patch or update, is considered a compromise to the integrity of the configuration. To install and distribute software updates, you must build and deploy a new package. Although this approach may seem time consuming, it ensures that everyone on the network receives the update and is using the same version of the software.

What if a computer fails an integrity check

If a computer fails an integrity check, pcAnywhere alerts the user that integrity has been compromised, and the user is prevented from using pcAnywhere. The only way to restore functionality is to reinstall pcAnywhere.

Auditing sessions

To address growing concerns about network security, many corporations use auditing tools that create journals and record the activities of the remote user during a remote control session.

Logging events

Event logging in pcAnywhere lets you monitor session activities and track performance issues behind the scenes. For security purposes, you can log information about failed logon attempts, how many host sessions are running, or whether sensitive files have been accessed.

Although logging can be a useful tool, be aware that tracking some types of events, such as logging every file that is opened on the host, can degrade performance. If you select an event that could affect performance, you will be prompted to confirm the action.

Depending on your operating environment, you can choose to send information events that occurred during a session to a pcAnywhere generated log file, NT or Windows 2000 event log, or a system network management protocol (SNMP) monitor.

Recording sessions

In addition to the logging tools described above, pcAnywhere can record sessions. The network administrator can playback this visual recording and view every activity that has occurred on the host computer. You can store the recording on the local computer or on a central network.

CHAPTER 8

Identifying security risks

As a pcAnywhere user, you already know the value of a remote access product. However, an improperly configured remote access product can leave your network vulnerable. The Remote Access Perimeter Scanner helps you identify where you are at risk.

RAPS is available only in the Corporate Edition.

This chapter contains the following:

Remote Access Perimeter Scanner overview

An improperly configured remote access product can pose a serious security risk to a corporate network, allowing unauthorized users to connect to the network and access sensitive information. The Remote Access Perimeter Scanner (RAPS) scans your network for remote access products and identifies potential security risks.

RAPS lets you do the following:

- Scan the corporate network and/or telephone numbers for the presence of pcAnywhere and other remote control or remote access products.
- Automatically shut down unprotected pcAnywhere hosts.
- View a log of scan information.

For installation instructions, see "Installing Administrator Tools" on page 21.

Disclaimer

The Remote Access Perimeter Scanner is intended to help you identify security risks in your own organization. Using RAPS for malicious purposes is a violation of the Remote Access Perimeter Scanner license agreement.

You are prompted to read the license agreement each time you open RAPS.

When you use RAPS to scan TCP/IP connections, RAPS sends a packet to the computer that you connect to saying, "The Remote Access Perimeter Scanner is scanning your system from" and identifies your TCP/IP address, user name, and computer name.

What RAPS scans for

RAPS scans for these remote access and remote control products.

- pcAnywhere version 2.0 and versions 7.5 through 10.0

  pcAnywhere for DOS, version 5.0

  RAPS can automatically shut down pcAnywhere hosts that do not require a logon.

  For more information, see "Setting global options" on page 110.
- LapLink 2000, version 3.01
- Carbon Copy, version 5.5
- Timbuktu Pro 32, version 3.0
- ReachOut, version 8.3
- NetSupport/PcDuo, version 5.03
- NetMeeting, version 3.01
- VNC, version 3.3.3
- NetBus Pro, version 2.0

- PPP Ras Server
- Windows Dial-Up Server
- Terminal Server for NT4
- Citrix Server
- X Server, version 11

Opening RAPS

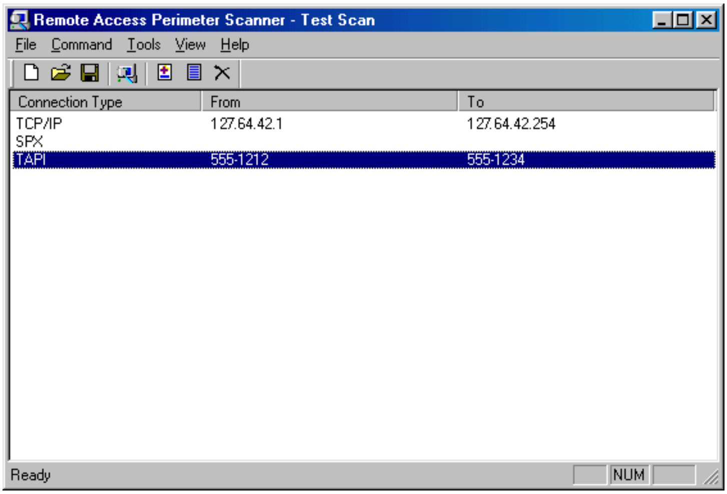
The instructions in the remainder of this chapter assume that you know how to open the Remote Access Perimeter Scanner.

Every time you open RAPS, you are prompted to read the RAPS license agreement.

To open RAPS

- On the Windows taskbar, click **Start** > **Programs** > **Remote Access Perimeter Scanner**.

  This RAPS window shows the contents of a scan file.



Connection Type	From	To
TCP/IP	127.64.42.1	127.64.42.254
SPX		
TAPI	555-1212	555-1234

Command list

You can use the RAPS command line to run a RAPS scan from a program scheduler or batch file.

To use RAPS from the command line

- Type the following:

  raps /s filename.ras

where /s starts the scan and filename.ras is the name of your scan file.

The /s and filename.ras arguments are optional. If you don’t specify a file name, RAPS uses the last scan file you opened. If you don’t include /s, RAPS opens the scan file, but doesn’t start the scan.

It might be necessary to include the fully qualified path to the RAPS executable and scan file name.

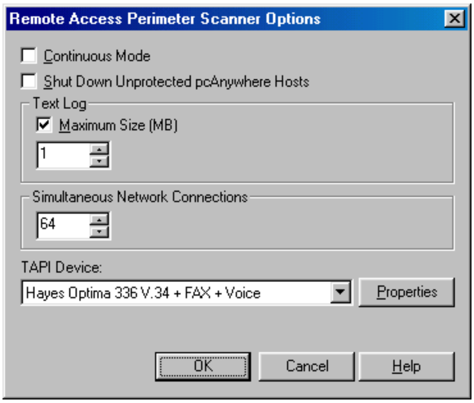
Setting global options

You can configure RAPS to run once or to run in continuous mode. You can automatically shut down unsecured pcAnywhere hosts and place limits on the maximum size of the text log file it generates.

You can also control the amount of network traffic by increasing or decreasing the number of simultaneous connections, as well as select and configure properties for a TAPI device.

To set global options

1 On the RAPS Tools menu, click **Options**.



Remote Access Perimeter Scanner Options

□ Continuous Mode

□ Shut Down Unprotected pcAnywhere Hosts

Text Log

☑ Maximum Size (MB)

1

Simultaneous Network Connections

64

TAPI Device:

Hayes Optima 336 V.34 + FAX + Voice

2 Check **Continuous Mode** to run the scan repeatedly.

The default is to run the scan once. This occurs when Continuous Mode is unchecked.

3 If you want to shut down unprotected pcAnywhere hosts, check **Shut down Unprotected pcAnywhere Hosts**.

4 Check **Maximum Size (MB)** and enter a number in MB to restrict how large the text log grows.

5 Set the network usage.

The number of Simultaneous Network Connections ranges from 1 to 64. Use a lower number to decrease network traffic. Use a higher number to increase scan speed.

This setting applies only to TCP/IP and SPX commands.

6. In the TAPI Device list, select the modem you want to use to make TAPI connections.
7. Click **OK**.

Logging RAPS events

RAPS logs events separately from pcAnywhere, but RAPS uses the same methods. This section covers the procedures for setting up SNMP traps, NT Event Logging, and local text file logging.

SNMP traps and NT Event Logging are more robust than simple text file logging. Text logging on the local computer is always enabled during RAPS scanning.

What events RAPS logs

RAPS classifies events in two ways: Potential Vulnerability and Product Found.

When RAPS is able to connect to a host or server and determine that the host or server is running an unsecured remote access product, it logs the event as a Potential Vulnerability event.

Other Potential Vulnerability events include:

- RAPS detects a known product that does not require a user to log on.
- RAPS finds a known product, but cannot detect whether the user is required to log on.
- RAPS finds a known product that is not running on its default port.

When RAPS is able to connect to a host or server, but is unable to determine the product, it logs the event as a Product Found event.

Other Product Found events include:

- RAPS finds an unknown product. (Unknown means that the product is not detected by RAPS.)

- RAPS looks for one product and finds another. For example, if RAPS is looking for pcAnywhere and finds LapLink, then LapLink is “unknown” for that scan.

Setting SNMP traps

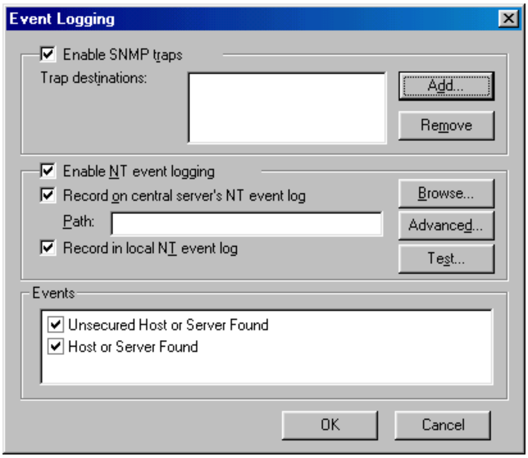
Follow this procedure to set up SNMP traps to log RAPS events.

For more information, see “Understanding SNMP and central logging” on page 66.

To set SNMP traps

1 On the RAPS Tools menu, click **SNMP and NT Event Logging**.

2 Check **Enable SNMP traps**.



Event Logging

☑ Enable SNMP traps

Trap destinations:

☑ Enable NT event logging

☑ Record on central server's NT event log

Path:

☑ Record in local NT event log

Events

☑ Unsecured Host or Server Found

☑ Host or Server Found

3 Do one of the following:

- Click **Add** to enter trap destinations.

  New trap destinations appear in the Trap destination window.

- Click **Remove** to remove selected trap destination from the list.

4 Check the events that you want to include in the log.

5 Click **OK**.

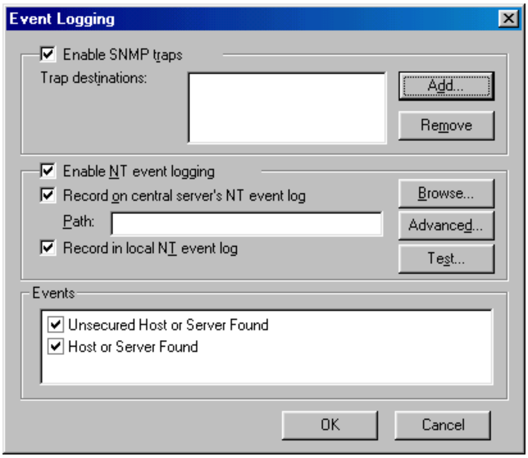
Setting up NT Event Logging

Follow this procedure to log RAPS events in the NT Event Log on your local computer or on a central server.

To record NT events

1 On the RAPS Tools menu, click **SNMP and NT Event Logging**.

2 Check **Enable NT event logging**.



☑ Enable SNMP traps

☑ Enable NT event logging

☑ Record on central server's NT event log

☑ Record in local NT event log

☑ Unsecured Host or Server Found

☑ Host or Server Found

3 Check **Record on central server's NT event log** to save the events in a central location.

4 Enter the path or click **Browse** to navigate to it.

5 Click **Advanced** to enter any authentication information needed to access the server.

6 Check **Record in local NT event log** if you want to save the events locally.

7 Check the events that you want to include in the log.

8 Click **OK**.

Creating a custom scan file

The first step in determining the security of your network is to identify the remote access products that are being used. You can use RAPS to determine if anyone on the network is using an unauthorized remote access product and to identify any unsecured hosts.

Before you can create and run a RAPS scan, you need to gather all of the information needed to add a command to the scan, such as the telephone numbers and IP addresses that you want to scan. This lets you create, customize, and save a scan file.

Creating and saving a scan file

RAPS lets you create multiple scan files so you can customize what you're scanning. Or, you can add multiple commands to one scan file. For example, you can create one scan file to scan your entire network and phone system on the weekend, and another scan file to scan only crucial network connections during the week.

After you create the scan, you customize it by adding commands to it.

To create a scan file

1. On the RAPS File menu, click **New**.
2. Select whether to include a command that scans for pcAnywhere hosts on the default TCP/IP subnet.
3. On the RAPS File menu, click **Save**. You can also press **Ctrl+S**.

Adding commands to a scan file

Before running a scan, you need to determine the connection types that you want to scan, then configure the settings for each connection type. Possible connection types are TCP/IP, SPX, TAPI, and CAPI. Each connection type requires its own command in the scan file. You can also have multiple commands for one connection type. For example, create multiple TCP/IP commands that scan different subnets.

To add commands to a scan file

1. Open the scan file that you want to customize or create a new scan file.
2. On the RAPS Command menu, click **New**.
3. On the General tab, click a Connection Type: TCP/IP, SPX, TAPI, or CAPI.

   SPX detects only pcAnywhere hosts.
4. In the Detect Products list, click the remote access products that you want to detect.

5 Click the tab associated with the Connection Type that you selected and follow the associated procedure.

Tab	Lets you	For more information, see
General	Select the connection type and the remote access products that you want to detect. You also use this tab to set up an SPX command.	"Scanning SPX connections" on page 117.
TCP/IP	Specify the IP addresses that you want to scan. You can specify the IP address by the full subnet or partial subnet address. You can also include additional ports in the scan.	"Scanning TCP/IP connections" on page 115.
TAPI	Specify the numbers that you want to dial, including the country code.	"Scanning TAPI connections" on page 118.
CAPI	Specify the numbers that you want to dial.	"Scanning CAPI connections" on page 120.

Scanning TCP/IP connections

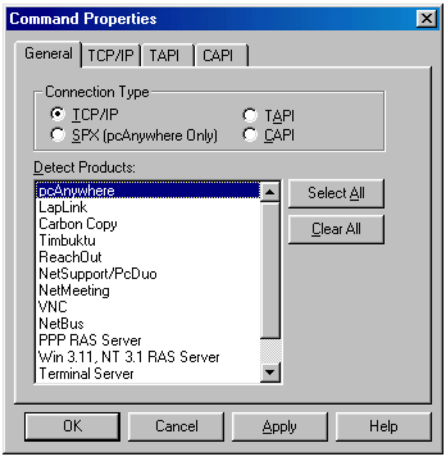
To scan for remote access products using a TCP/IP connections, add a TCP/IP command to your scan file.

To add a TCP/IP command to a scan file

1 Open the scan file that you want to customize or create a new scan file.

2 On the RAPS Command menu, click **New.**

3 Under Connection Type, click **TCP/IP**.



Connection Type

● TCP/IP ○ TAPI
○ SPX (pcAnywhere Only) ○ CAPI

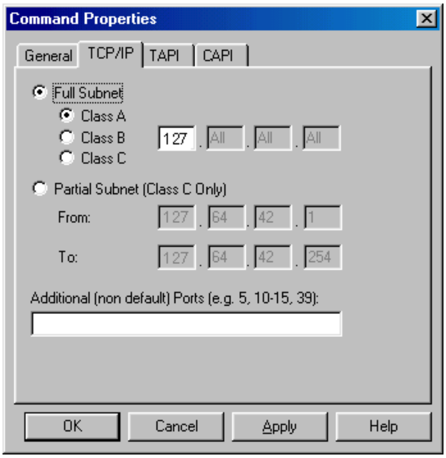
Detect Products:

pcAnywhere
LapLink
Carbon Copy
Timbuktu
ReachOut
NetSupport/PcDuo
NetMeeting
VNC
NetBus
PPP RAS Server
Win 3.11, NT 3.1 RAS Server
Terminal Server

4 Under Detect Products, select the products that you want to detect.

5 On the TCP/IP tab, do one of the following:

- Click **Full Subnet** to scan a full subnet. Type the Class A, Class B, and Class C addresses.



● Full Subnet
● Class A
○ Class B 127 . All . All . All
○ Class C

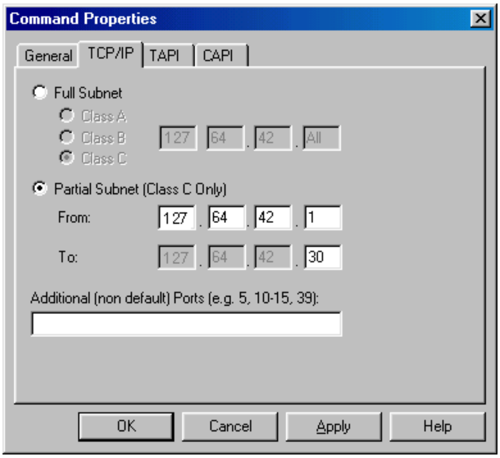
○ Partial Subnet (Class C Only)

From: 127 . 64 . 42 . 1

To: 127 . 64 . 42 . 254

Additional (non default) Ports (e.g. 5, 10-15, 39):

- Click **Partial Subnet** to scan a specific range of Class C addresses. Type the start and end subnet addresses.



○ Full Subnet

○ Class A

○ Class B

● Class C

127 . 64 . 42 . All

● Partial Subnet (Class C Only)

From: 127 . 64 . 42 . 1

To: 127 . 64 . 42 . 30

Additional (non default) Ports (e.g. 5, 10-15, 39):

6 Type any additional ports that you want to scan.

7 Click **OK** to add the command to the scan file.

Scanning SPX connections

To scan for remote access products using an SPX connection, add an SPX command to your scan file.

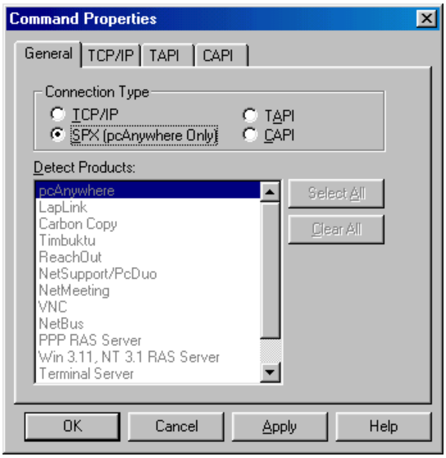
On SPX connections, RAPS only scans for pcAnywhere.

To add an SPX command to a scan file

1 On the RAPS Command menu, click **New**.

2 Under Connection Type, click **SPX**.

When you click SPX, RAPS automatically selects pcAnywhere and disables the remainder of the Detect Products list.



Connection Type
○ TCP/IP
● SPX (pcAnywhere Only)
○ TAPI
○ CAPI

Detect Products:
pcAnywhere
LapLink
Carbon Copy
Timbuktu
ReachOut
NetSupport/PcDuo
NetMeeting
VNC
NetBus
PPP RAS Server
Win 3.11, NT 3.1 RAS Server
Terminal Server

3 Click **OK** to add the command to the scan file.

Scanning TAPI connections

To scan for remote access products using a TAPI connection, add a TAPI command to your scan file.

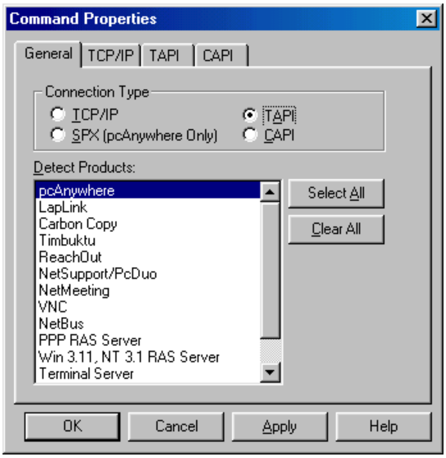
Symantec is not responsible for telephone charges incurred during a RAPS scan.

To add a TAPI command to a scan file

1 Open a scan file that you want to customize or create a new scan file.

2 On the RAPS Command menu, click **New**.

3 Under Connection Type, click **TAPI**.



Connection Type

○ TCP/IP
○ SPX (pcAnywhere Only)
● TAPI
○ CAPI

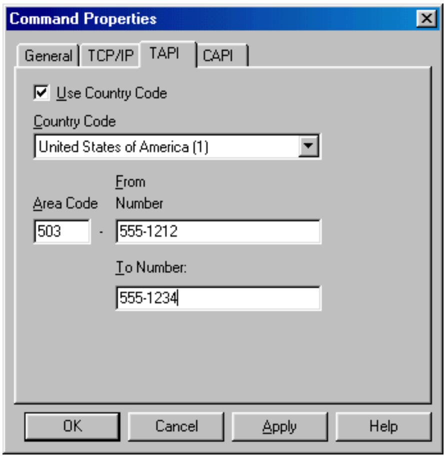
Detect Products:

- pcAnywhere
- LapLink
- Carbon Copy
- Timbuktu
- ReachOut
- NetSupport/PcDuo
- NetMeeting
- VNC
- NetBus
- PPP RAS Server
- Win 3.11, NT 3.1 RAS Server
- Terminal Server

4 Select the remote access products that you want to detect.

5 On the TAPI tab, enter the phone number range you want to scan.

- If the Country Code will be used in dialing, check Use Country Code and type the Country Code to be used.
- If the Country Code option is not checked, this box will be grayed out. Type the Area Code for the range of numbers to be dialed. In the From Number box, type the starting number to be dialed. Enter the ending number in the To Number box.



☑ Use Country Code

Country Code: United States of America (1)

Area Code: 503 - From Number: 555-1212

To Number: 555-1234

6 Click **OK** to add the command to the scan file.

Scanning CAPI connections

To scan for remote access products using a CAPI connection, add a CAPI command to your scan file.

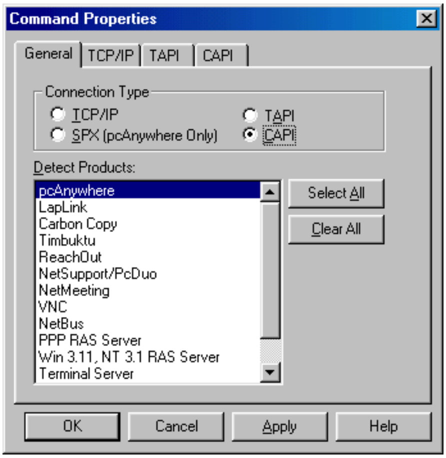
Symantec is not responsible for telephone charges incurred during a RAPS scan.

To add a CAPI command to a scan file

1 Open the scan file you want to customize or create a new scan file.

2 On the RAPS Command menu, click **New**.

3 Under Connection Type, click **CAPI**.



Command Properties

Connection Type

○ TCP/IP ○ TAPI

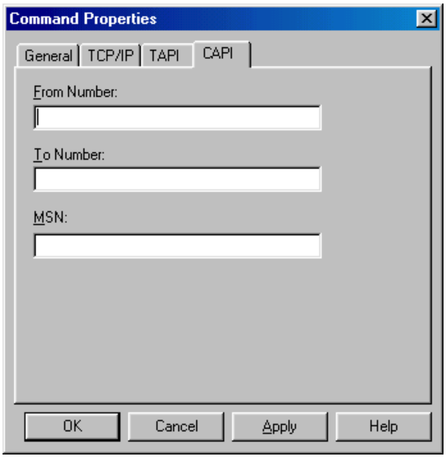
○ SPX (pcAnywhere Only) ● CAPI

Detect Products:

pcAnywhere
LapLink
Carbon Copy
Timbuktu
ReachOut
NetSupport/PcDuo
NetMeeting
VNC
NetBus
PPP RAS Server
Win 3.11, NT 3.1 RAS Server
Terminal Server

4 Select the products that you want to detect.

5 On the CAPI tab, type the starting number and ending numbers in the From Number and To Number fields, respectively.



6 In the MSN field, type your local telephone number.

7 Click **OK** to add the command to the scan file.

Modifying a command

Once you add a command to a scan file, you can modify it at any time.

To modify a command

1 Open the scan file that contains the command that you want to modify.

2 Double-click the command.

3 Make the necessary changes.

4 Click **OK**.

Deleting a command from a scan file

You can remove a command from a scan file at any time.

To delete a command from a scan file

1 Open the scan file that contains the command that you want to delete.

2 Highlight the command, then press **Delete**.

Running a RAPS scan

When you run a RAPS scan, the Scan Results dialog box displays scan data as it occurs. Results are stored in the local text log file.

The status information that displays in the Scan Results window shows when RAPS starts a connection. It takes time to make the connection, detect the remote access products, and return that information to RAPS. The status might not change for a few moments while RAPS processes the information.

To run a RAPS scan

- On the RAPS File menu, click **Start Scan**. You can also press **F5**.

  The Scan Results window displays status information.

Viewing scan results

Upon the completion of the scan, the Scan Results dialog box is displayed. This information is also stored in the local text file log. The most recent data appears at the end of the log file. When the log file exceeds its maximum size, old events are deleted first.

To review scan results

- On the RAPS View menu, click **Text Log**.

Service and support solutions

Service and support information is available from the Help system of your Symantec product. Click the Service and Support topic in the Help index.

Technical support

Symantec offers several technical support options:

- StandardCare support

  Connect to the Symantec Service & Support Web site at http://service.symantec.com, then select your product and version. This gives you access to product knowledge bases, interactive troubleshooter, Frequently Asked Questions (FAQ), and more.

- PriorityCare, GoldCare, and PlatinumCare support

  Fee-based telephone support services are available to all registered customers. For complete information, please call our automated fax retrieval service at (800) 554-4403 and request document 933000.

  For telephone support information, connect to http://service.symantec.com, select your product and version, and click Contact Customer Support.

- Automated fax retrieval

  Use your fax machine to receive general product information, fact sheets, and product upgrade order forms by calling (800) 554-4403. For technical application notes, call (541) 984-2490.

Support for old and discontinued versions

When a new version of this software is released, registered users will receive upgrade information in the mail. Telephone support will be provided for the old version for six months after the release of the new version. Technical information may still be available through the Service & Support Web site (http://service.symantec.com).

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will be available for discontinued products from the Service & Support Web site only.

Customer service

Visit Symantec Customer Service online at http://service.symantec.com for assistance with non-technical questions and for information on how to do the following:

- Subscribe to the Symantec Support Solution of your choice.
- Obtain product literature or trialware.
- Locate resellers and consultants in your area.
- Replace missing or defective CD-ROMS, disks, manuals, and so on.
- Update your product registration with address or name changes.
- Get order, return, or rebate status information.
- Access customer service FAQs.
- Post a question to a Customer Service representative.

For upgrade orders, visit the online upgrade center at: http://www.symantec.com/upgrades/ or call the Customer Service Order Desk at (800) 568-9501.

Worldwide service and support

Technical support and customer service solutions vary by country. For information on Symantec and International Partner locations outside of the United States, please contact one of the service and support offices listed below, or connect to http://www.symantec.com, select the country you want information about, and click Go!

Service and support offices

North America

Symantec Corporation
175 W. Broadway
Eugene, OR 97401
U.S.A.

http://www.symantec.com/
Fax: (541) 984-8020

Automated Fax Retrieval

(800) 554-4403
(541) 984-2490

Argentina and Uruguay

Symantec Region Sur
Cerritos 1054 - Piso 9
1010 Buenos Aires
Argentina

http://www.symantec.com/region/mx
+54 (11) 4315-0889
Fax: +54 (11) 4314-3434

Asia/Pacific Rim

Symantec Australia Pty. Ltd.
408 Victoria Road
Gladesville, NSW 2111
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 9850 1000
Fax: +61 (2) 9817 4550

Brazil

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12° andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

http://www.symantec.com/region/br/
+55 (11) 5189-6200
Fax: +55 (11) 5189-6210

Other Latin America

Symantec Corporation
175 W. Broadway
Eugene, OR 97401
U.S.A.

http://www.symantec.com/region/mx/
+1 (541) 334-6054 (U.S.A.)
Fax: (541) 984-8020 (U.S.A.)

Europe, Middle East, and Africa

Symantec Customer Service Center P.O. Box 5689 Dublin 15 Ireland	http://www.symantec.com/region/reg_eu/ +353 (1) 811 8032 Fax: +353 (1) 811 8033
Automated Fax Retrieval	+31 (71) 408-3782

Mexico

Symantec Mexico Blvd Adolfo Ruiz Cortines, No. 3642 Piso 14 Col. Jardines del Pedregal Ciudad de México, D.F. C.P. 01900 México	http://www.symantec.com/region/mx +52 (5) 481-2600 Fax: + 52 (5) 481-2626

Virus protection subscription policy

If your Symantec product includes virus protection, you might be entitled to receive free virus protection updates via LiveUpdate. The length of the free subscription could vary by Symantec product.

When you near the end of your virus protection subscription, you will be prompted to subscribe when you start LiveUpdate. Simply follow the instructions on the screen. After your free subscription ends, you must renew your subscription before you can update your virus protection. Renewal subscriptions are available for a nominal charge.

To order a subscription, do one of the following:

- Visit our Web site at: http://www.shop.symantec.com.
- Outside the United States, contact your local Symantec office or representative.

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

February 2001

pcAnywhere v10.0
CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive CD replacements.

FOR CD REPLACEMENT

Please send me: ___ CD Replacement

Name ____

Company Name ____

Street Address (No P.O. Boxes, Please)____

City ______________________________ State _______ Zip/Postal Code ________________

Country* ______________________________Daytime Phone ______________________________

Software Purchase Date ____

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributer.

Briefly describe the problem:____

____

CD Replacement Price	$ 10.00
Sales Tax (See Table)	______
Shipping & Handling	$ 9.95
TOTAL DUE	______

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (CHECK ONE):

___ Check (Payable to Symantec) Amount Enclosed $ _________ __ Visa __ Mastercard __ American Express

Credit Card Number ____Expires _________

Name on Card (please print) ______________________________ Signature ______________________________

****U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.**

MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
175 West Broadway
Eugene, OR 97401-3003 (800) 441-7234

Please allow 2-3 weeks for delivery within the U.S.

I N D E X