

Symantec pcAnywhere™ Administrator's Guide



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 11.0

PN: 10079000

Copyright Notice

Copyright © 2003 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

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

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, and select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone at 800-927-4017 (U.S. and Canada only) or online at www.symantec.com/techsupp. Telephone support is charged on a per-incident basis.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
 - Error messages/log files
 - Troubleshooting performed prior to contacting Symantec
 - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Technical support

Chapter 1 Planning for Symantec pcAnywhere installation

Preparing for installation	10
System requirements	10
User rights requirements	11
Choosing an installation option	12
If you have a previous version installed	13
Planning a migration and upgrade strategy	13
Migrating from pcAnywhere 10.x in Windows NT/2000/XP	14
Migrating from pcAnywhere 10.x in Windows 98/Me	15
Converting AutoTransfer files	15
Upgrading from pcAnywhere 9.2x in Windows NT/2000/XP	16
Upgrading from pcAnywhere 9.2x in Windows 98/Me	16
Using Symantec Packager to streamline migrations and upgrades	17

Chapter 2 Creating custom installation packages

About Symantec Packager	20
What you can do with Symantec Packager	20
How Symantec Packager works	21
Importing a product module	22
Customizing product settings	23
Selecting product features	24
Including configuration files	26
Integrity stamping a product configuration	28
Serializing a pcAnywhere installation	30
Managing configuration settings globally	32
Setting product installation options	34
Creating a custom command	40
Creating installation packages	41
Adding products and commands to a package definition	42
Building product installations and packages	43
Building a product configuration file	43
Building a package	44
Testing packages	45

Chapter 3 Deploying Symantec pcAnywhere custom installations

About deployment	48
About installation file locations	49
Deploying installation packages using Web-based deployment	49
About Web-based deployment requirements	50
Setting up the installation Web server	50
Customizing the deployment files	53
Testing the installation	57
Notifying users of the download location	58
Deploying pcAnywhere using SMS 2.0	59
Minimum requirements for SMS deployment	59
Deploying with SMS	60
Using Windows NT/2000/XP logon scripts	62
Setting up the server	63
Writing the logon script	63
Testing the logon script	64
Using NetWare logon scripts	64
Setting up the server	64
Writing the logon script	65
Testing the logon script	66

Chapter 4 Performing centralized management

About centralized management	68
Managing pcAnywhere hosts remotely	68
Installing the pcAnywhere Host Administrator tool	68
Adding the Host Administrator snap-in to MMC	69
Creating configuration groups	70
Adding computers to a configuration group	70
Configuring administrator host and remote connection items	71
Configuring a host item in pcAnywhere Host Administrator	73
Distributing pcAnywhere configuration files	74
Managing hosts in a configuration group	74
Integrating with Microsoft Systems Management Server	75
Importing the package definition file into SMS	75
About the Microsoft Distributed Component Object Model (DCOM)	76
Implementing DCOM in Windows NT/2000/XP	77
Implementing DCOM in Windows 98/Me	77
Modifying DCOM settings	77
About AwShim	78
About centralized logging	79
Monitoring performance using SNMP traps	79
About the pcAnywhere MIB file	80

Chapter 5 Integrating pcAnywhere with Directory Services

About directory services	112
Overview of the LDAP informational model	112
Using Directory Services with pcAnywhere	113
Configuring the directory servers	114
Configuring the LDAP server	114
Configuring Netscape Directory Server 3.1	114
Configuring Netscape Directory Server 4.0	115
Configuring Novell v5.0 server	116
Configuring Windows Active Directory	120
Configuring pcAnywhere to use directory services	124
Setting up directory services in pcAnywhere	124
Setting up the host computer to use directory services	125
Setting up the remote computer to use directory services	126

Chapter 6 Managing security in Symantec pcAnywhere

Ways to secure pcAnywhere	128
How pcAnywhere works with Windows security	128
Controlling access to pcAnywhere hosts	128
Limiting connections to specific computer names or IP addresses	130
Leveraging centralized authentication in pcAnywhere	130
Protecting session security	134
Maintaining audit trails	135
Implementing policy-based administration	136
Implementing Group Policy in Windows 2000/XP	136
Implementing system policy in Windows 98/Me/NT4	136
Importing the pcAnywhere administrative template	137
Managing user policies	138

Chapter 7 Identifying security risks

About the Remote Access Perimeter Scanner	144
Disclaimer	144
Products included in a scan	144
Installing the Remote Access Perimeter Scanner	145
Opening the Remote Access Perimeter Scanner	146
Running the Remote Access Perimeter Scanner from a command line	147
Setting global options	147
Logging Remote Access Perimeter Scanner events	148
About event log classifications	149
Setting SNMP traps	149
Setting up Windows Event Logging	150

- Creating a custom scan file152
 - Creating and saving a scan file152
 - Adding commands to a scan file152
 - Modifying a command160
 - Deleting a command from a scan file160
- Running a Remote Access Perimeter Scanner scan160
- Viewing scan results161

Index

CD Replacement Form

Planning for Symantec pcAnywhere installation

This chapter includes the following topics:

- [Preparing for installation](#)
- [Planning a migration and upgrade strategy](#)
- [Using Symantec Packager to streamline migrations and upgrades](#)

Preparing for installation

Before installing pcAnywhere, ensure that your computer meets the system requirements. Review the Readme file on the installation CD for any known issues.

For installation procedures, see the *Symantec pcAnywhere User’s Guide*.

Note: Installation of Symantec pcAnywhere is not supported on encrypted file systems.

System requirements

Symantec pcAnywhere runs on Windows 98/Me/NT/2000/XP and requires, at a minimum, the resources that are listed in [Table 1-1](#) to function properly.

Table 1-1 System requirements

Operating system	Requirements
Windows XP Home Edition/Professional	■ Service Pack 1 (SP1) or later ■ Intel Pentium (or compatible) processor at 233 MHz or higher ■ 64 MB of RAM (128 MB recommended) ■ 32 MB of hard disk space ■ VGA or higher resolution monitor ■ CD-ROM or DVD-ROM drive
Windows 2000 Professional/Server	■ Service Pack 3 (SP3) or later ■ Intel Pentium (or compatible) processor at 150 MHz or higher ■ 64 MB of RAM ■ 32 MB of hard disk space ■ VGA or higher resolution monitor ■ CD-ROM or DVD-ROM drive
Windows NT Workstation 4/NT Server 4	■ Service Pack 6 (SP6) or later ■ Intel Pentium (or compatible) processor at 150 MHz or higher ■ 64 MB of RAM ■ 32 MB of hard disk space ■ VGA or higher resolution monitor ■ CD-ROM or DVD-ROM drive

Table 1-1 System requirements

Operating system	Requirements
Windows 98/Me	■ Intel Pentium (or compatible) processor at 150 MHz or higher ■ 64 MB of RAM ■ 32 MB of hard disk space ■ VGA or higher resolution monitor ■ CD-ROM or DVD-ROM drive

To ensure proper functionality of some features, the following third-party programs are also required. These programs are located on the pcAnywhere installation CD in the Tools folder.

- Adobe Acrobat Reader 5.1 or later
- Internet Explorer 5.5 SP2 or later

User rights requirements

Users on Windows NT/2000/XP must have administrator rights to install pcAnywhere.

Windows XP restricts users who are assigned to the limited user or guest accounts from installing or uninstalling software, changing system-wide settings, or adding, editing, or deleting user accounts. For optimal performance, log on as a user with administrator rights when running pcAnywhere on Windows XP.

Choosing an installation option

Symantec pcAnywhere lets you install the full version of the product or select a custom installation package that contains only the functionality that you need. [Table 1-2](#) lists the installation options that are available.

Table 1-2 Installation options

Installation option	Description
Symantec pcAnywhere	Installs the full version of pcAnywhere, including host, remote control, remote management, and file transfer features. On the Corporate CD, this installation also includes the Host Administrator tool and Remote Access Perimeter Scanner. On the retail CD, this installation also includes the Host Administrator tool.
pcAnywhere for the individual	Installs the full version of pcAnywhere without the Host Administrator tool or Remote Access Perimeter Scanner.
Host Only Version	Installs host server features, supporting network and modem connections. Select this option if you only want to receive connections or if you want to install pcAnywhere on two computers, where one computer is a host and the other is a remote.
LAN Host Version	Installs host server features, supporting network connections only. Select this option if you only want to receive connections or if you want to install pcAnywhere on two computers, where one computer is a host and the other is a remote.
Remote Only Version	Installs the features needed to connect to a host computer for remote control, remote management, and file transfer. Does not include host server features. Select this option if you only want to initiate connections or if you want to install pcAnywhere on two computers, where one computer is a host and the other is a remote.
pcAnywhere Express	Lets you connect to another computer using any Internet browser that supports ActiveX controls. This installation option is unsupported.

Table 1-2 Installation options

Installation option	Description
pcAnywhere with DynIP	Installs a custom package that bundles the full version of pcAnywhere with a 6-month trial version of DynIP. This installation option is unsupported.

If you have a previous version installed

During the installation process, pcAnywhere automatically scans for a previous version. If you are installing pcAnywhere on a computer that has pcAnywhere 10.0x or later, pcAnywhere confirms whether you want to preserve existing data before installing over the previous version. How pcAnywhere handles the data conversion process depends on your operating system and the version of pcAnywhere that is installed.

See [“Planning a migration and upgrade strategy”](#) on page 13.

If you are installing pcAnywhere on a computer that has a version of pcAnywhere earlier than 9.2.1, pcAnywhere prompts you to uninstall it. This removes all preexisting configuration data. Configuration data from these versions cannot be converted or preserved. If you need to install the new version on multiple computers that have an unsupported version of pcAnywhere installed, you can use Symantec Packager to simplify the roll-out process.

See [“Using Symantec Packager to streamline migrations and upgrades”](#) on page 17.

Planning a migration and upgrade strategy

Symantec pcAnywhere supports migration from versions 10.x to version 11.0 on Windows 98/Me/NT/2000/XP. During a migration, pcAnywhere lets you install over the previous version of the product and preserve user-defined settings.

Symantec pcAnywhere supports upgrades from version 9.2x to version 11.0 on Windows 98/Me/NT/2000/XP. An upgrade lets you install over the previous version of the product; however, user-defined settings are not automatically preserved.

A system restart for migrations and upgrades is required only if system files need to be updated. Symantec pcAnywhere requires a system restart if you are migrating or upgrading to the new version in Windows 98/Me.

Symantec Packager helps you simplify the process of uninstalling previous versions or distributing preconfigured settings to multiple users.

See [“Using Symantec Packager to streamline migrations and upgrades”](#) on page 17.

Use [Table 1-3](#) as a reference in planning your migration and upgrade strategy.

Table 1-3 Symantec pcAnywhere migration and upgrade strategy matrix

Symantec pcAnywhere version	Operating system	Restart required	Data preserved automatically
10.x	Windows NT/2000/XP	No	Host items Caller items Remote items Option sets Registry settings AutoTransfer files (must be converted)
10.x	Windows 98/Me	Yes	Host items Caller items Remote items Option sets Registry settings AutoTransfer files (must be converted)
9.2x	Windows NT/2000/XP	No	None
9.2x	Windows 98/Me	Yes, previous version must be uninstalled	None

Migrating from pcAnywhere 10.x in Windows NT/2000/XP

Symantec pcAnywhere supports full migration without requiring a system restart when installing pcAnywhere 11.0 on a Windows NT/2000/XP computer that has the following versions of pcAnywhere 10.x installed.

- Full product version
- Host only version

During the installation, you are prompted to preserve existing configuration settings. This data includes settings for host, remote, and caller items as well as option sets.

AutoTransfer files (.atf) that were created in earlier versions of pcAnywhere are preserved. However, to use the .atf files in this version of pcAnywhere, you must convert the .atf files to command queue files.

See [“Converting AutoTransfer files”](#) on page 15.

Migration of remote-only packages and integrity-checked packages is not supported.

Migrating from pcAnywhere 10.x in Windows 98/Me

Symantec pcAnywhere supports full migration when installing pcAnywhere 11.0 on a Windows 98/Me computer that has the following versions of pcAnywhere 10.x installed:

- Full product version
- Host only version

During the installation, you are prompted to preserve existing configuration settings. This data includes settings for host, remote, and caller items as well as option sets.

AutoTransfer files (.atf) that were created in earlier versions of pcAnywhere are preserved. However, to use the .atf files in this version of pcAnywhere, you must convert the .atf files to command queue files.

See [“Converting AutoTransfer files”](#) on page 15.

This migration requires a system restart to remove older pcAnywhere system files. You can use Symantec Packager to streamline the migration process.

See [“Using Symantec Packager to streamline migrations and upgrades”](#) on page 17.

Migration of remote-only packages and integrity-checked packages is not supported.

Converting AutoTransfer files

The Command Queue replaces the AutoTransfer feature that was provided in earlier versions of pcAnywhere. If you are migrating from pcAnywhere 10.x to pcAnywhere 11.0, pcAnywhere preserves the AutoTransfer files (.atf) that are stored in the pcAnywhere default program directory. However, to use these files in pcAnywhere 11.0, you must convert them to command queue files.

Symantec pcAnywhere provides an ATF Converter tool, which lets you convert .atf files that were created in pcAnywhere 10.0 or later to command queue files. The ATF Converter tool is located in the Unsupported folder on the Symantec pcAnywhere CD.

Upgrading from pcAnywhere 9.2x in Windows NT/2000/XP

Symantec pcAnywhere supports upgrades of the full product and host-only versions of pcAnywhere 9.2x to version 11.0 in Windows NT/2000/XP. A system restart is not required.

The upgrade process does not automatically preserve user-defined data. If you need to upgrade pcAnywhere on multiple computers, you can use Symantec Packager to create a custom installation package that contains preconfigured data files.

See [“Using Symantec Packager to streamline migrations and upgrades”](#) on page 17.

Upgrading from pcAnywhere 9.2x in Windows 98/Me

If you are installing pcAnywhere version 11.0 on a Windows 98/Me computer that has version 9.2x installed, pcAnywhere prompts you to uninstall the program. This is required to ensure proper functionality.

To automate this process, you can use Symantec Packager to create a custom installation package to handle the uninstall and installation process. You can also include preconfigured data files in the package and deploy it to other users.

See [“Using Symantec Packager to streamline migrations and upgrades”](#) on page 17.

Using Symantec Packager to streamline migrations and upgrades

Symantec Packager is an administrator tool that lets you create, modify, and build custom installation packages that you distribute to target systems. Symantec Packager is available as an installation option on the pcAnywhere CD.

Symantec Packager helps you streamline the process of migrating or upgrading from earlier versions of pcAnywhere in the following ways:

The product installation requires you to manually uninstall a previous version of the product.	Create a custom installation package that includes a custom command to silently uninstall the previous version before installing the product.
The product installation requires you to restart the computer to complete the installation process.	Create a custom installation package for the product installation and configure the package to install in passive or silent mode.
The product installation does not support preservation of preconfigured product settings.	Create a custom installation package that includes preconfigured data files that contain the settings you need.

See [“Creating custom installation packages”](#) on page 19.

Creating custom installation packages

This chapter includes the following topics:

- [About Symantec Packager](#)
- [What you can do with Symantec Packager](#)
- [How Symantec Packager works](#)
- [Importing a product module](#)
- [Customizing product settings](#)
- [Creating a custom command](#)
- [Creating installation packages](#)
- [Building product installations and packages](#)
- [Testing packages](#)

About Symantec Packager

Symantec Packager lets you create, modify, and build custom installation packages that you distribute to target systems. Using Symantec Packager, you can tailor installations to fit your corporate environment, building packages that contain only the features and settings that your users need.

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

Note: Symantec Packager runs on Windows NT/2000/ XP Professional platforms only. However, installation packages that are created with Symantec Packager can be installed on all Microsoft 32-bit platforms except for Windows 95/NT 3.51.

What you can do with Symantec Packager

Symantec Packager lets you do the following:

- Tailor products to adhere to your security policy, giving users full access to all features, or limiting access where appropriate.
- Reduce deployment bandwidth and application footprint by creating a custom installation package that contains only the features that your users need.
- Reduce installation complexity by including preconfigured data files.
- Minimize deployment costs and complexity by installing multiple products at once.
- Simplify application deployment and migration by including custom commands with product installations.

How Symantec Packager works

Symantec Packager uses a phased approach for creating custom installation packages. Each phase depends on the output of the previous phase.

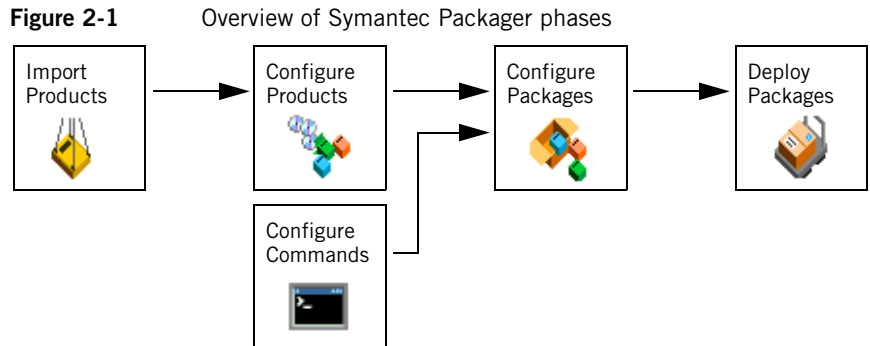


Figure 2-1 illustrates the process for creating custom installation packages with Symantec Packager. This process involves the following steps:

- Import product modules into Symantec Packager.
Product modules contain the installation binary and product template files that are needed to create a custom installation of the product.
See [“Importing a product module”](#) on page 22.
- Configure products.
You can select the features that you want your users to have, add preconfigured data and configuration files, and set default installation options for each product.
See [“Customizing product settings”](#) on page 23.
- Configure commands that you want to include in a package.
Custom commands let you add additional functionality that is not supported in the product templates, such as including a third-party program or batch file.
See [“Creating a custom command”](#) on page 40.
- Configure packages.
You can bundle one or more product configurations and custom commands in a package. You can further customize the package by setting package installation options, product installation order, and other settings.
See [“Creating installation packages”](#) on page 41.

- Build custom products or packages.

When you build a package, Symantec Packager creates an installation file that incorporates the product, command, and package options that you specified.

Alternatively, Symantec Packager lets you build a product configuration file, which creates a Microsoft Installer (.msi) file for a single product installation. See [“Building product installations and packages”](#) on page 43.

- Test the package.

You should test packages before deploying them to end users to ensure proper functionality.

See [“Testing packages”](#) on page 45.

- Deploy the package.

The Deploy Packages tab holds the packages that you create, which you can deploy to your users. Symantec provides a Package Deployment tool in Symantec Packager and a Web-based deployment tool on the pcAnywhere CD. You can also use your current deployment tools.

See [“Deploying Symantec pcAnywhere custom installations”](#) on page 47.

Importing a product module

Product modules are the building blocks for creating packages. Symantec Packager extracts the product installation binary files and the product template from the product module. The product template details the feature requirements and conflicts, making it possible to create custom installations of the product. During installation, Symantec Packager automatically checks the Packager/Products folder for product module files and imports them automatically.

Symantec pcAnywhere provides a product module file (Symantec pcAnywhere <version>.PMI) on the installation CD. If you install Symantec Packager from the pcAnywhere installation CD, Symantec Packager automatically imports this product module file.

If no products appear on the Import Products tab when you open Symantec Packager, you must import the product module manually.

To import a product module

- 1 Open Symantec Packager.
- 2 In the Symantec Packager window, on the Import Products tab, on the File menu, click **Import New Product**.
- 3 In the Open dialog box, navigate to the folder that contains the product module that you want to import.
- 4 Select the product module, then click **Open**.
Symantec Packager imports the product module and returns you to the Import Products tab. Depending on the size and complexity of the product module, the registration process might be lengthy.

Customizing product settings

Symantec Packager creates a default product configuration file (.pcg) for each product module that you import into Symantec Packager. Each product configuration file contains the features, installation options, and preconfigured settings that you want to include for that product. Symantec Packager uses this information to construct installation packages.

You can edit the default product configuration file or create a new one. [Table 2-1](#) provides an overview of the configuration options that are available in the default pcAnywhere product configuration file.

Table 2-1 Symantec pcAnywhere product configuration options

Tab	Settings
Features	You can customize the following features in pcAnywhere: ■ User interface (pcAnywhere Manager) ■ Remote components ■ Host components ■ Communications protocols ■ OLE Automation ■ Event logging ■ pcAnywhere administrator tools (Host Administrator and Remote Access Perimeter Scanner) ■ Documentation (online manuals and Help) ■ Symantec installation utilities ■ Microsoft system components

Table 2-1 Symantec pcAnywhere product configuration options

Tab	Settings
Configuration Files	The pcAnywhere product template includes default remote and host configuration items that you can configure after the package or custom product installation. You can add configuration files that you create in pcAnywhere to the package or custom product installation for further customization.
Installation Options	You can customize the following product installation options for pcAnywhere: ■ Product description ■ Target location ■ Start online registration at startup ■ Host object to use as a template ■ Host object to start with Windows ■ Remote object to use as a template ■ Run LiveUpdate after installation ■ Preserve existing configuration settings

After you select the product features, installation options, and optional configuration files to include in your custom product, you can build it for testing purposes. Building the product configuration file creates a Microsoft Installer (.msi) file. Symantec Packager supports installation of pcAnywhere .msi files only.

See [“Building a product configuration file”](#) on page 43.

Selecting product features

Symantec Packager lets you customize product installations by including the features that you want and removing the features that you do not need. The product size and installed size change depending on the features that you choose.

Some features in pcAnywhere have dependencies on other components. Although Symantec Packager has a level of built-in dependency checking, it is possible to build a pcAnywhere installation package that does not include all required files.

As you select product features to include or exclude from a package, you should read the feature descriptions that are provided in the Product Editor window on the Features tab. The feature descriptions provide information about feature

dependencies. [Table 2-2](#) provides a reference for product dependencies. This list is not all-inclusive.

Table 2-2 Symantec pcAnywhere product dependencies

Feature	Dependency
pcAnywhere Manager	Required if you want to let users modify configuration settings Exclude pcAnywhere Manager if you want to include integrity management
Remote	Requires at least one communications protocol
Host	Requires a caller configuration file (.cif) if you configure the product to start a host automatically at startup Requires at least one authentication type Requires at least one communications protocol
Remote Control	Required for all custom product installations
File Transfer	Requires at least one communications protocol
Remote Management	Requires at least one communications protocol
Chat	Requires at least one communications protocol
Authentication	Required for all custom product installations
Communication protocols	Required for all custom product installations

To select product features

- 1 In the Symantec Packager window, on the Configure Products tab, do one of the following:
 - Create a new product configuration.
 - Double-click an existing product to edit it.
- 2 In the Product Editor dialog box, on the Features tab, do any of the following:
 - Check the product features that you want to include in the custom product.
 - Uncheck the features that you do not want to include.
 - Click the plus sign next to a feature to select or remove its subfeatures.

- 3 Select one of the following:
 - OK: Saves your changes and closes the Product Editor dialog box.
 - Apply: Saves your changes and lets you continue the product configuration.
- 4 If prompted, type a file name, then click **Save**.

Including configuration files

Symantec Packager lets you include preconfigured data or configuration files so that your users do not have to make configuration changes during or after installation. For product-specific configurations, you must configure these files in the product first, then add them to the Configuration Files tab in Symantec Packager. Configuration files cannot be edited in Symantec Packager.

For more information, see the Symantec Packager online Help.

The pcAnywhere product template provides the following default configuration files, depending on the features that you selected on the Features tab:

Symantec Live Update file (LIVEUPDT.HIST)	Provides the information needed to support connections to the Symantec LiveUpdate server to receive automatic product updates associated with your version of pcAnywhere.
Remote connection item files (.chf)	Provide default settings to support connections to a host computer over a modem, network, or direct connection. Also provide default settings to start a connection in file transfer or remote management mode.
Host connection item files (.bhf)	Provide default settings to allow remote users to connect to the computer over a modem, network, or direct connection.

Depending on the features that you selected on the Features tab, you can configure the following files in pcAnywhere and add them to the custom product installation:

Option sets	Let you configure global options for pcAnywhere to accommodate unique configuration requirements.
Host Security IDs	Let you serialize the pcAnywhere installation.
Remote connection item files (.chf)	Let you preconfigure the connection and security settings needed to connect to another computer remotely. For more information, see the <i>Symantec pcAnywhere User's Guide</i> .
Command queue files	Let you automate file transfer, command-line, and end-of-session tasks. For more information, see the <i>Symantec pcAnywhere User's Guide</i> .
Host connection item files (.bhf)	Let you preconfigure the connection and security settings needed to allow a connection from another computer. For more information, see the <i>Symantec pcAnywhere User's Guide</i> .
Caller files (.cif)	Let you preconfigure a logon account for users who connect to the host computer and select an authentication method to verify their identities. This information is required to launch a host. For more information, see the <i>Symantec pcAnywhere User's Guide</i> .

Symantec pcAnywhere configuration files are located in the following folders:

Windows 2000/XP	\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere
Windows NT 4.0	\Winnt\Profiles\All Users\Application Data\Symantec\pcAnywhere
Windows 98/Me	\Windows\All Users\Application Data\Symantec\pcAnywhere

These folders are hidden by default in the operating system. To browse for the pcAnywhere configuration files, you must edit the folder options on your operating system to show hidden files.

You can also add registry key files to control certain pcAnywhere settings. The registry keys that are contained in the file are added to the system registry on the target computer when the package or custom product is installed.

Warning: Use caution when configuring a registry key file. An incorrect setting could make the operating system or product inoperable.

To include a configuration file

- 1 In the Symantec Packager window, on the Configure Products tab, do one of the following:
 - Create a new product configuration.
 - Double-click an existing product to edit it.
- 2 In the Product Editor dialog box, on the Configuration Files tab, do one of the following:
 - Select the type of preconfigured file that you want to add, then click **Add**.
Browse to the configuration file that you want to include, then click **Open**. Symantec pcAnywhere configuration files are added to the list. For other types of configuration files, this replaces the default file with your preconfigured file.
 - Select the file that you want to remove, then click **Remove**.
This removes your preconfigured file and replaces it with the default file provided by Symantec, if one is available.
- 3 In the Product Editor dialog box, do one of the following:
 - Click **OK** to save your changes and close the Product Editor dialog box.
 - Click **Apply** to save your changes and continue the product configuration.
- 4 If prompted, type a file name, then click **Save**.

Integrity stamping a product configuration

You can prevent unauthorized changes to the installed product by selecting the Integrity Management feature on the Features tab in the Product Editor. If pcAnywhere detects that a pcAnywhere executable, registry, or configuration file

has been changed in an installed, integrity-stamped package, pcAnywhere will not run.

If you select the Integrity Management feature, you must exclude the pcAnywhere Manager and LiveUpdate features. Once an integrity-stamped package is installed, users are restricted from changing or updating pcAnywhere in any way, including installation of software upgrades via LiveUpdate. When updates are needed, you must create and deploy a new package.

Breaches to integrity, including changes to the registry or adding or deleting files, can result in denial of service. Use integrity checking in conjunction with policy management and overall strong security practices, such as hardening the operating system.

See [“Implementing policy-based administration”](#) on page 136.

To integrity stamp a product configuration

- 1 In the Symantec Packager window, on the Configure Products tab, do one of the following:
 - Create a new product configuration.
 - Double-click an existing product to edit it.
- 2 In the Product Editor window, on the Feature tab, click the plus sign next to Symantec installation utilities to expand the listing.
- 3 Check **Integrity management**.
- 4 Select the other features that you want to include or exclude from the product.
- 5 On the Installation Options tab, select the product installation options that you want to use.

See [“Setting product installation options”](#) on page 34.

- 6 Select one of the following:
 - OK: Saves your changes and closes the Product Editor dialog box.
 - Apply: Saves your changes and lets you continue the product configuration.
- 7 If prompted, type a file name, then click **Save**.
- 8 Build a product installation or package.

Building a product configuration file creates an .msi file that contains the single product.

You can add the product configuration file to a package to further customize the installation. Building a package creates a self-extracting .exe file.

Serializing a pcAnywhere installation

Symantec pcAnywhere lets you create a custom installation that contains an embedded security code, or serial ID. This serial ID number must be present on both the host and remote computers to make a connection.

Serialization involves the following process:

- In pcAnywhere, generate a serial ID file (.SID).
- In Symantec Packager, in the Product Configuration Editor, select the feature components that you want to include, then add the serial ID configuration file.
- Build the package.
- Deploy and install the package.

Generating a serial ID file

Symantec pcAnywhere lets you generate a security code, or serial ID, which can be embedded into a custom installation. The serial ID must be numerical and can be no longer than 10 numbers. To let a remote user connect to a host computer that uses a different serial ID, you must include the serial IDs for each host computer in the serial ID file.

To generate a serial ID file

- 1 In the pcAnywhere Manager window, on the left navigation bar, click **Serial ID Sets**.
- 2 On the File menu, click **New > Item > Advanced**.
- 3 In the Serial ID Set Properties window, under Limit host connections by using the following serial IDs, type the serial ID number that you want to use.
- 4 Click **Add**.
- 5 Click **OK**.

The Serial ID file is added to the right pane under Serial ID Sets.

Creating a serialized installation file

To create a serialized version of pcAnywhere, you must add the serial ID file that you generate in pcAnywhere to a product definition file. The serial ID is embedded in the product when you build the product or build a package that contains the product definition.

The custom product installation or package must be installed on the host and remote computers. To allow a connection between a host and remote computer, the host and remote computers must have matching serial IDs.

To create a serialized installation file

- 1 In the Symantec Packager window, on the Configure Products tab, do one of the following:
 - Create a new product configuration.
 - Double-click an existing product to edit it.
- 2 In the Product Editor dialog box, on the Features tab, do any of the following:
 - Check the product features that you want to include in the custom product.
 - Uncheck the features that you do not want to include.
 - Click the plus sign next to a feature to select or remove its subfeatures.

To configure a custom product installation or package that includes host and remote features, select Host and Remote. To create separate installations, select only Host or Remote.
- 3 On the Configuration Files tab, click **Host Security IDs File (*.SID)**, then click **Add**.
- 4 Browse to the folder that contains the serial ID file (*.SID) that you generated in pcAnywhere, select the file, then click **Open**.

The serial ID file is added to the list of data and configuration files.
- 5 On the Installation Options tab, select the product installation options that you want to use.

See [“Setting product installation options”](#) on page 34.
- 6 Select one of the following:
 - **OK**: Saves your changes and closes the Product Editor dialog box.
 - **Apply**: Saves your changes and lets you continue the product configuration.
- 7 If prompted, type a file name, then click **Save**.
- 8 Build a product installation or package.

Building a product configuration file creates an .msi file that contains a single product.

You can add the product configuration file to a package to further customize the installation. Building a package creates a self-extracting .exe file.

Managing configuration settings globally

Symantec pcAnywhere option sets let you manage global settings for host and remote connections, file transfer, logging, and other functions to improve performance, enhance security, or manage connections. Symantec pcAnywhere lets you create multiple option sets to accommodate unique configuration requirements.

Preconfigured option sets can be used for custom installation packages created with Symantec Packager. They can also be used as the default preferences for the local computer.

Configuring an option set in pcAnywhere

Symantec pcAnywhere groups the option set properties by tabs. [Table 2-3](#) explains where to find the settings that you need.

Table 2-3 Symantec pcAnywhere option set properties

Tab	Description
Host Operation	Controls basic host operations, such as host name and record settings
Remote Operation	Controls performance and display settings for remote sessions
Host Communications	Contains customization options for modem and network connections on the host
Remote Communications	Contains customization options for modem and network connections on the remote
Session Manager	Controls basic session options, such as the background color for the unusable part of the remote desktop, and lets you view or edit the command prompt exclusion list
File Transfer	Controls file transfer settings
Event Logging	Enables logging of events that occur during pcAnywhere sessions
Directory Services	Controls settings for using a directory service to find hosts
Remote Printing	Contains settings for configuring remote printing
Encryption	Specifies certificate information required for public-key encryption

To configure an option set in pcAnywhere

- 1** In the pcAnywhere Manager window, on the left navigation bar, click **Option Sets**.
- 2** Do one of the following:
 - To create a new option set, on the File menu, click **New > Item > Advanced**.
 - To modify an existing option set, in the right pane, right-click the option set, then click **Properties**.
- 3** In the Option Set Properties window, click the left and right arrows to scroll through the list of tabs.
See [Table 2-3, “Symantec pcAnywhere option set properties,”](#) on page 32.
- 4** Configure the settings that you want to use.
- 5** When you are finished, click **OK**.
For more information about a feature, see the *Symantec pcAnywhere User’s Guide*.

Adding an option set to a custom installation file

You can add the option sets that you create in pcAnywhere to a custom installation file. After the package or custom product is installed on the target computer, the option set can be applied on the local computer.

To add an option set to a custom installation file

- 1** In the Symantec Packager window, on the Configure Products tab, do one of the following:
 - Create a new product configuration.
 - Double-click an existing product to edit it.
- 2** In the Product Editor window, on the Configuration Files tab, click **Option Set File (*.OPT)**, then click **Add**.
- 3** Browse to the folder that contains the option set files (*.opt) that you created in pcAnywhere, select the one you want to use, then click **Open**.
The option set file is added to the list of data and configuration files.

- 4 In the Product Editor window, do one of the following:
 - Click **OK** to save your changes and close the Product Editor dialog box.
 - Click **Apply** to save your changes and continue the product configuration.
- 5 If prompted, type a file name, then click **Save**.

Applying an option set on the local computer

Symantec pcAnywhere lets you maintain multiple option set files to accommodate unique configuration requirements. For example, if you work in different locations, you can avoid changing the default settings each time you change locations. Create an option set for each location, then apply it when you arrive. When you apply an option set on the local computer, you override the default preferences in pcAnywhere.

To apply an option set on the local computer

- 1 In the pcAnywhere Manager window, on the left navigation bar, click **Option Sets**.
- 2 In the right pane, right-click the option set file that you want to use, then click **Apply to Local System**.

Setting product installation options

Symantec Packager lets you specify product installation options, which vary by product and by the features that you have included in the product configuration.

There are other installation options that you can control at the package level. These include installation mode, restart, logging, and rollback options.

For more information, see the Symantec Package online Help.

Symantec pcAnywhere lets you customize the following installation options:

Description	Lets you specify a unique description for the product.
Target location	Lets you select the directory in which you want to install the product on the target computer. See “Changing the target installation directory” on page 36.

Start online registration at startup	Prompts users to register the product when they start the program for the first time. See “Prompting users to register upon startup” on page 36.
Host object to use as template	Lets you select the host configuration file that you want to use as a template for new host connection items that the user creates after installation. See “Selecting the default template for host connections” on page 37.
Host object to start with Windows	Lets you select a host connection item to start automatically when the user on the target computer starts Windows. See “Selecting the default template for host connections” on page 37.
Remote object to use as template	Lets you select the remote configuration file that you want to use as a template for new remote connection items that the user creates after installation. See “Selecting the default template for remote connections” on page 38.
Run LiveUpdate after installation	Lets you configure the custom installation to automatically connect to the Symantec LiveUpdate server to download product updates. See “Updating products” on page 39.
Preserve existing configuration settings	Lets you configure the product to preserve existing configuration settings if you are installing over a previous version of pcAnywhere.

Changing the target installation directory

Symantec pcAnywhere custom installations that you create with Symantec Packager are installed in the Program Files directory under Symantec\pcAnywhere by default. You can specify a different directory.

To change the target installation directory

- 1 In the Symantec Packager window, on the Configure Products tab, do one of the following:
 - Create a new product configuration.
 - Double-click an existing product to edit it.
- 2 In the Product Editor window, on the Installation Options tab, double-click **Target location**.
- 3 In the Target Location window, select one of the following:
 - Program Files directory
 - Root of system drive
 - Custom path
Under Folder specification, type the full path to the location in which you want to install the product.
- 4 Click **OK**.
- 5 In the Product Editor window, do one of the following:
 - Click **OK** to save your changes and close the Product Editor dialog box.
 - Click **Apply** to save your changes and continue the product configuration.
- 6 If prompted, type a file name, then click **Save**.

Prompting users to register upon startup

Symantec Packager lets you configure the product to prompt users to complete the online registration process the first time they start the product. To use this installation option, you must include the pcAnywhere Manager feature in the product configuration.

To prompt users to register upon startup

- 1 In the Symantec Packager window, on the Configure Products tab, do one of the following:
 - Create a new product configuration.
 - Double-click an existing product to edit it.
- 2 In the Product Editor window, on the Installation Options tab, double-click **Start online registration at startup**.
- 3 In the Start online registration at startup window, check **Start online registration at startup**.
- 4 Click **OK**.
- 5 In the Product Editor window, do one of the following:
 - Click **OK** to save your changes and close the Product Editor dialog box.
 - Click **Apply** to save your changes and continue the product configuration.
- 6 If prompted, type a file name, then click **Save**.

Selecting the default template for host connections

Symantec Packager lets you select the host configuration file that you want to use as a template for new host connection items that the user creates after installation. Host connection items contain the configuration settings needed to let remote users connect to the host computer.

You can select the pcAnywhere program default settings, select a preconfigured host connection item provided by pcAnywhere, or select a user-provided host connection item.

To select the default template for host connections

- 1 In the Symantec Packager window, on the Configure Products tab, do one of the following:
 - Create a new product configuration.
 - Double-click an existing product to edit it.
- 2 In the Product Editor window, on the Installation Options tab, double-click **Host object to use as template**.
- 3 In the Host object to use as template window, under value, select the host connection item file (.bhf) that you want to use as a template.
- 4 Click **OK**.

- 5 To configure the product to automatically start a host when the user starts Windows, in the Product Editor window, on the Installation Options tab, double-click **Host object to start with Windows**.
- 6 In the Host object to start with Windows window, under Value, select the .bhf file that you want to use.
- 7 In the Product Editor window, do one of the following:
 - Click **OK** to save your changes and close the Product Editor dialog box.
 - Click **Apply** to save your changes and continue the product configuration.
- 8 If prompted, type a file name, then click **Save**.

Selecting the default template for remote connections

Symantec Packager lets you select the remote configuration file that you want to use as a template for new remote connection items that the user creates after installation. Remote connection items contain the configuration settings needed to connect to another computer remotely.

You can select the pcAnywhere program default settings, select a preconfigured remote connection item provided by pcAnywhere, or select a user-provided remote connection item.

To select the default template for remote connections

- 1 In the Symantec Packager window, on the Configure Products tab, do one of the following:
 - Create a new product configuration.
 - Double-click an existing product to edit it.
- 2 In the Product Editor window, on the Installation Options tab, double-click **Remote object to use as template**.
- 3 In the Remote object to use as template window, under Value, select the remote connection item file (.chf) that you want to use as a template.
- 4 Click **OK**.
- 5 In the Product Editor window, do one of the following:
 - Click **OK** to save your changes and close the Product Editor dialog box.
 - Click **Apply** to save your changes and continue the product configuration.
- 6 If prompted, type a file name, then click **Save**.

Updating products

If you include the LiveUpdate feature in the product configuration, Symantec Packager lets you configure the product to automatically connect to the Symantec LiveUpdate server after installation to download product updates.

If you have installed the Symantec LiveUpdate Administration Utility to manage LiveUpdate operations for your network, you can configure the product to connect to the LiveUpdate server on your network. You must customize the LiveUpdate configuration file (LIVEUPDT.HST) to include the location of the LiveUpdate Server.

For more information, see the LiveUpdate documentation.

To update products

- 1 In the Symantec Packager window, on the Configure Products tab, do one of the following:
 - Create a new product configuration.
 - Double-click an existing product to edit it.
- 2 In the Product Editor window, on the Installation Options tab, double-click **Run LiveUpdate after installation**.
- 3 In the Run LiveUpdate after installation window, check **Run LiveUpdate after installation**.
- 4 Click **OK**.
- 5 In the Product Editor window, do one of the following:
 - Click **OK** to save your changes and close the Product Editor dialog box.
 - Click **Apply** to save your changes and continue the product configuration.
- 6 If prompted, type a file name, then click **Save**.

Preserving existing configuration settings

If you are installing a package over an existing version of pcAnywhere (from version 10.0 and later), Symantec Packager lets you preserve existing registry, host, remote, and caller configuration settings.

See [“If you have a previous version installed”](#) on page 13.

This option is available for silent and passive mode installations only. You must configure installation mode settings at the package level.

See [“Creating installation packages”](#) on page 41.

To preserve existing configuration settings

- 1 In the Symantec Packager window, on the Configure Products tab, do one of the following:
 - Create a new product configuration.
 - Double-click an existing product to edit it.
- 2 In the Product Editor window, on the Installation Options tab, double-click **Preserve existing configuration settings**.
- 3 In the Preserve existing configuration settings window, check **Preserve existing configuration settings**.
- 4 Click **OK**.
- 5 In the Product Editor window, do one of the following:
 - Click **OK** to save your changes and close the Product Editor dialog box.
 - Click **Apply** to save your changes and continue the product configuration.
- 6 If prompted, type a file name, then click **Save**.

Creating a custom command

In addition to creating custom products, you can create custom commands to include in your packages. Examples of custom commands include batch files, third-party executables, command-line arguments, or simple file copies. Custom commands let you simplify application deployment by including multiple tasks in one package. Once defined, you can reuse custom commands in different packages.

When you create a custom command, Symantec Packager creates a command configuration file. A command configuration file is a generic product configuration file that does not reference a product template file. Therefore, custom commands do not require you to import a product module. The build process for custom commands creates a self-extracting executable (.exe) file, which can be tested prior to inclusion in a package.

Symantec pcAnywhere packages do not require custom commands. For more information about custom commands, see the Symantec Packager online Help.

To create a custom command

- 1 In the Symantec Packager window, on the Configure Products tab, on the File menu, click **New Custom Command**.
- 2 In the Command Editor window, on the Parameters tab, double-click **Description**.
- 3 In the Command Description window, type a descriptive name for the command so that you can easily identify it later.
 For example:
 Uninstall pcAnywhere 9.0 without user intervention
- 4 Click **OK**.
- 5 In the Command Editor window, on the Parameters tab, double-click **Command line**.
- 6 In the Command Line Specification window, under Command line and switches, type the command-line arguments and switches that are required to run the command.
 For example, to run the uninstall program for pcAnywhere 9.0 without requiring user interaction, type the fully qualified path to the remove.exe file that is located in the pcAnywhere 9.0 program directory followed by the /s switch.
`"C:\Program Files\Symantec\pcAnywhere\remove.exe" /s`
 You must type a double quotation mark before and after the fully qualified path to ensure that the operating system handles spaces in the file name and long file names properly.
- 7 Under Optional switches, type the command-line switches that you want to use to control the installation behavior.
- 8 Under Run options, select how the installation should appear to the user.
- 9 Click **OK**.

For more information about configuring custom commands, see the Symantec Packager online Help.

Creating installation packages

Symantec Packager lets you bundle one or more product configuration files and custom commands in a package definition file. The package definition file contains the configuration information and installation instructions that Symantec Packager requires to build the package.

Package creation is optional for pcAnywhere custom installations. Symantec Packager lets you build the Symantec pcAnywhere product configuration file, which creates an .msi file that can be installed locally. You can deploy the Symantec pcAnywhere .msi file using a third-party deployment tool. The Symantec Packager Deployment Tool does not support MSI deployment.

Creating a package definition lets you do the following:

- Bundle one or more products and custom commands in one installation package.
- Configure the installation to run in interactive, passive, or silent mode.
- Add custom graphics to the installation panels for interactive installations.
- Configure restart options, including whether to prompt users to save work.
- Select rollback options for handling an installation that fails.
- Generate a log file to determine whether the package installed successfully.
- Include technical support contact information.

For more information about configuring package settings, see the Symantec Packager online Help.

Adding products and commands to a package definition

Symantec Packager lets you create a custom installation package that includes one or more products or custom commands. As you add an item to a package definition file, its properties, as defined in the product configuration file, are displayed in the Package Editor dialog box, as well as any product requirements or conflicts.

To add products and command to a package definition

- 1 In the Symantec Packager window, on the Configure Packages tab, do one of the following:
 - Create a new package definition.
 - Double-click a package definition to edit an existing one.
- 2 In the Package Editor dialog box, on the Product Selection tab, click **Add**.
- 3 In the Open window, select the product or custom command (.pcg) file that you want to add.
- 4 Click **Open**.

The Estimated package size changes to reflect the product or command that you include.

- 5 Repeat steps 2 through step 4 to add more products or custom commands.
- 6 In the Package Editor window, do one of the following:
 - Click **OK** to save your changes and close the Package Editor dialog box.
 - Click **Apply** to save your changes and continue the package definition.
- 7 If prompted, type a file name, then click **Save**.

Building product installations and packages

After you define the contents and installation options for the package definition file, you must build the package definition to create the installation file. When you build a package, Symantec Packager creates a self-extracting .exe file that incorporates the product, command, and package options that you specified.

Alternatively, Symantec Packager lets you build a product configuration file, which creates a Microsoft Installer (.msi) file for a single product installation.

Building a product configuration file

Building a product configuration file lets you create an .msi file that you can use for testing or installation. Symantec Packager supports MSI installation for pcAnywhere product modules only. You do not need to build a product configuration file to include it in a package.

Symantec Packager stores the .msi files in the Symantec Packager data directory. You can view these files on the Deploy Packages tab if you edit the Symantec Packager preferences to list supported .msi files.

You can use an industry-standard, third-party deployment tool to deploy the pcAnywhere .msi file. The Symantec Packager Deployment Tool does not support deployment of .msi files.

To build a product configuration file

- 1 In the Symantec Packager window, on the Configure Products tab, select the product configuration file that you want to build.
- 2 On the File menu, click **Build**.
 The Product Build Status window appears, which provides information about the progress of the build and logs any problems that have occurred. If the product build is successful, the last line in the Product Build Status window reads Product was built successfully.
- 3 In the Product Build Status window, click **Close**.

Building a package

During the build process, Symantec Packager retrieves information from the package definition file and product configuration files to determine what products to include in the installation file as well as the product features, installation instructions, and custom settings. Symantec Packager then checks the contents of the package for product conflicts. If Symantec Packager encounters a product conflict, the build process stops. You must resolve the conflict, and then repeat the build process.

After checking for product conflicts, Symantec Packager verifies that product requirements are met. This includes verification that all required products are included in the package definition file. If Symantec Packager encounters an error, the user receives an error message; however, the build process continues.

After completing the validation phases, Symantec Packager creates a self-extracting executable file and places it on the Deploy Packages tab for testing and distribution to licensed users.

To build a package

- 1 In the Symantec Packager window, on the Configure Packages tab, select the package definition file that you want to build.
- 2 On the File menu, click **Build**.
The Package Build Status window appears, which provides information about the progress of the build and logs any problems that have occurred. If the package build is successful, the last line in the Build Status window reads Package was built successfully.
- 3 In the Build Status dialog box, click **Close**.

Testing packages

It is important to test packages before deploying them to end users to ensure proper functionality. You should test package installation and deployment in an isolated, controlled environment. One to two test computers should be sufficient to conduct testing.

Although some error checking occurs during the build process, some errors cannot be detected until installation. This is especially true if the package includes a product that requires a third-party product or if the package includes a custom command.

During installation, Symantec Packager checks for product conflicts and verifies that required products are present on the target computer. The installation fails if Symantec Packager encounters a conflict that it cannot resolve. You should test packages to verify that product requirements are met and that the installation sequence is correct.

You should also open each installed program to ensure that it functions correctly. Ensure that the features that you want are present. This step is especially important if you customized a product to reduce the installation footprint. Product testing ensures that you have not overlooked an important feature. Once you thoroughly test the package, you can deploy it to end users.

Deploying Symantec pcAnywhere custom installations

This chapter includes the following topics:

- [About deployment](#)
- [About installation file locations](#)
- [Deploying installation packages using Web-based deployment](#)
- [Deploying pcAnywhere using SMS 2.0](#)
- [Using Windows NT/2000/XP logon scripts](#)
- [Using NetWare logon scripts](#)

About deployment

You can deploy the custom pcAnywhere installations that you create with Symantec Packager and the preconfigured installations that are included on the Symantec pcAnywhere CD using any of the following methods:

- **Local computer installation**

Opening an .exe file or supported .msi file on the Deploy Packages tab in Symantec Packager starts the installation process. Ensure that the target computer meets the system requirements for pcAnywhere installation.

For more information about using the Deploy Packages tab, see the *Symantec Packager Implementation Guide* on the pcAnywhere CD.

For more information about installing pcAnywhere, see the *Symantec pcAnywhere User's Guide*.
- **Symantec Packager deployment tool**

This tool lets you deploy packages to one or more computers on your network. The Symantec Packager deployment tool supports deployment to Microsoft 32-bit computers only (for example, Windows NT/2000/XP).

For more information, see the *Symantec Packager Implementation Guide* on the pcAnywhere CD.
- **Symantec Web Deploy tool**

This tool lets you deploy package or product installations to one or more computers using a Web server.

See [“Deploying installation packages using Web-based deployment”](#) on page 49.
- **Third-party tools**

Package and product installations created with Symantec Packager can be distributed using a third-party deployment product, such as Microsoft Systems Management Server (SMS).

See [“Deploying pcAnywhere using SMS 2.0”](#) on page 59.
- **Ligon scripts**

Package and product installations created with Symantec Packager can be distributed to Windows NT/2000/XP and Novell NetWare target computers using a logon script.

See [“Using Windows NT/2000/XP logon scripts”](#) on page 62.

See [“Using NetWare logon scripts”](#) on page 64.

About installation file locations

Preconfigured package and product installation files are stored in the Packages directory on the Symantec pcAnywhere CD. Packages and product installation files that you create with Symantec Packager are listed on the Deploy Packages tab in Symantec Packager.

To view .msi files, you must edit the Symantec Packager preferences to list supported product .msi files. Symantec Packager supports MSI deployment only for pcAnywhere .msi files.

For more information, see the online Help in Symantec Packager or the *Symantec Packager Implementation Guide* on the pcAnywhere installation CD.

Deploying installation packages using Web-based deployment

Packages that are created with Symantec Packager can be deployed over your corporate intranet using a Web-based deployment tool that is provided by Symantec. All of the source files that are necessary to implement Web-based deployment are included on the Symantec pcAnywhere CD in the Tools/Web Deploy folder.

Deploying packages using Web-based deployment requires the following steps:

- Review the Web-based deployment requirements.
- Set up the installation Web server, which includes copying the package files to the deployment directory on the Web server.
- Customize the deployment files.
- Test the installation.
- Notify users of the download location.

The Web-based deployment tool supports the deployment of Symantec Packager packages and Microsoft Installer (.msi) files. Symantec Packager lets you create a package installation file as self-extracting executable (.exe) file or create a custom product installation for a single product as an .msi file.

About Web-based deployment requirements

Before you implement Web-based deployment on a Web server or target computer, review the requirements in [Table 3-1](#).

Table 3-1 Web server and target computer requirements

Deployment on	Requirements
Web server	■ HTTP Web server. ■ Microsoft Internet Information Server (IIS) version 4.0/5.0. ■ Apache HTTP Server version 1.3 or later. UNIX and Linux platforms are also supported.
Target computer	■ Internet Explorer 4.0 or later. Symantec pcAnywhere requires Internet Explorer 5.5 SP2 or later for installation. ■ Windows Installer 2.0 or later (required only for MSI installations). ■ Browser security must allow ActiveX controls to be downloaded to the target computer. When the installation is complete, the security level can be restored to its original setting. ■ Must meet system requirements for the package to be installed. ■ Must be logged on to the computer with the rights that are required for the package to be installed. You must have administrator rights to install pcAnywhere.

Setting up the installation Web server

To set up the Web server, complete the following tasks in the order in which they are listed:

- Copy the installation files to the Web server.
- Configure the Web server.

Copying the installation files to the Web server

You must copy the installation files required to support Web-based deployment to a directory on the Web server. You should create a separate directory on the Web server for these files. You must also copy the installation files (.exe or .msi) that you want to make available.

After you complete this process, you must edit the start.htm and files.ini files to specify the location and names of the installation files.

See [“Customizing the deployment files”](#) on page 53.

To copy the installation files to the Web server

- 1 On the Web server, create a directory in which you want to place the deployment files.
For example:
Deploy
- 2 From the Packages folder on the Symantec pcAnywhere CD, copy the installation files that you want to make available for deployment to the Webinst subfolder on the Web server.
For example:
Deploy\Webinst\Webinst
- 3 Ensure that the default document for the virtual directory is Default.htm.
See [“Setting up the installation Web server”](#) on page 50.

The following is an example of the folder structure on the Web server. All files are case sensitive.

- Deploy\Webinst
 - brnotsup.htm
 - default.htm
 - intro.htm
 - logo.jpg
 - oscheck.htm
 - plnotsup.htm
 - readme.htm
 - start.htm
 - webinst.cab
- Deploy\Webinst\Webinst
 - files.ini
 - Launch.bat (required only for MSI installations)
 - Installation packages
For example:
Symantec pcAnywhere - Full Product.exe
Symantec pcAnywhere - Host Only (Network).msi

Creating a virtual directory on the Web server

You must configure the Web server to create a virtual directory.

Create a virtual directory on a Microsoft Internet Information Server or Apache Web Server

The Web-based deployment tool supports Microsoft Internet Information Server (IIS) or Apache HTTP Web Server. The procedures for creating a virtual directory on these servers vary.

To create a virtual directory on a Microsoft Internet Information Server

- 1 Do one of the following to launch the Internet Services Manager:
 - In IIS version 4.0: On the Windows taskbar, click **Start > Programs > Windows NT 4.0 Option Pack > Microsoft Internet Information Server > Internet Service Manager**.
 - In IIS version 5.0: On the Windows taskbar, click **Start > Programs > Administrative Tools > Internet Services Manager**.
- 2 Double-click the Web server icon to open it.
- 3 Right-click **Default Web Site**, then click **New > Virtual Directory**.
- 4 Click **Next** to begin the Virtual Directory Creation Wizard.
- 5 In the **Alias** text box, type a name for the virtual directory (for example, **ClientInstall**), then click **Next**.
- 6 Type the location of the installation folder (for example, **C:\Client\Webinst**), then click **Next**.
- 7 For access permissions, check **Read only**, then click **Next**.
- 8 Do one of the following to complete the virtual directory creation:
 - In IIS 4.0: Click **Finish**.
 - In IIS 5.0: Click **Next**, then click **Finish**.

To create a virtual directory on an Apache Web Server

- 1 In a text editor, open Srm.conf.
 The Srm.conf file is installed by default in C:\Program Files\
 Apache Group\Apache\conf.
- 2 Type the following five lines at the end of the Srm.conf file:
DirectoryIndex default.htm
<VirtualHost 111.111.111.111>
#ServerName machinename
DocumentRoot "C:\Client\Webinst"
</VirtualHost>

For the VirtualHost	Replace 111.111.111.111 with the IP address of the computer on which Apache HTTP Server is installed.
For ServerName	Replace machinename with the name of the server.
For the DocumentRoot	Specify the folder in which you copied the Web install files (for example, "C:\Client\Webinst"). Double quotation marks are required to specify the DocumentRoot. If the quotation marks are omitted, Apache services might not start.

Customizing the deployment files

You must edit the following files to deploy and install packages using the Web-based deployment tool:

- **Start.htm:** Contains the parameters for the Web server and the location of the files that need to be installed
 This file resides in the root of the Webinstall directory.
- **Files.ini:** Contains the file name parameters for the packages and files that you want to deploy and install
 This file resides in the Webinst subdirectory.
- **Launch.bat:** Contains the command line used to execute the package installation
 This file resides in the Webinst subdirectory. Launch.bat is required only for MSI installations.

Customizing Start.htm

The parameters in the Start.htm file contain information about the Web server and the location of the files that need to be installed. The configuration parameters in [Table 3-2](#) are located near the bottom of the Start.htm file, inside the <object> tags.

Table 3-2 Start.htm configuration parameters and 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, Deploy\Webinst).
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 package and Files.ini (for example, Webinst).
MinDiskSpaceInMB	The minimum hard disk space requirement. The default value is appropriate.
ProductAbbreviation	The abbreviation for the product. The default value is appropriate.

To customize Start.htm

- 1 In a text editor, open Start.htm.
- 2 Search for the <object> tags and type the correct values.
See [Table 3-2, “Start.htm configuration parameters and values,”](#) on page 54.
- 3 Save Start.htm.

Customizing Files.ini for package deployment

Modify Files.ini to contain the name of the package executable file that you want to deploy. Additional information is required to support MSI deployment.

See [“Customizing Files.ini for MSI deployment”](#) on page 55.

You can also include additional files to support the deployment of third-party applications.

To customize Files.ini for package deployment

- 1 In a text editor, open Files.ini.
- 2 In the [General] section, edit the line LaunchApplication= so that it references the package executable file that you want to start after the download completes.
For example, LaunchApplication=Symantec pcAnywhere - Full Product.exe
- 3 If you are deploying multiple files, edit the FileCount= line to reflect the number of files that you want to deploy.
The default setting is FileCount=1.
- 4 In the [Files] section, edit the line File1= so that it references the name of the package that you want to deploy.
For example, File1=Symantec pcAnywhere - Full Product.exe
Long file names are supported.
- 5 For each additional file, add a new File*n*= *filename* line, where *n* is a unique number and filename is the name of the file.
- 6 Save Files.ini.

Customizing Files.ini for MSI deployment

Modify Files.ini to contain the names of the .msi files that you want to deploy. MSI deployment requires Launch.bat, which is used to start the installation program. You must also modify Files.ini to reference the Launch.bat file.

See “[Customizing Launch.bat](#)” on page 57.

You can also include additional files to support the deployment of third-party applications.

To customize Files.ini for MSI deployment

- 1 In a text editor, open Files.ini.
- 2 In the [General] section, edit the line LaunchApplication= so that it references Launch.bat.
For example, LaunchApplication=Launch.bat
This launches the MSI installation after the download is complete. You must also edit the Launch.bat file to include the name of the .msi file that you want to deploy.
- 3 Edit the FileCount= line to reflect the number of files that you want to deploy.
MSI deployment requires two files, so the FileCount= line must be set at least to two.
For example, FileCount=2
- 4 In the [Files] section, edit the line File1= so that it references the Launch.bat file.
For example, File1=Launch.bat
- 5 Delete the semicolon next to the line File2= to uncomment the entry.
- 6 Edit the line File2= so that it references the name of the .msi file that you want to deploy.
For example, File2=Symantec pcAnywhere - Host Only.msi
Long file names are supported.
- 7 For each additional file, add a new File n = *filename* line, where n is a unique number and filename is the name of the file.
- 8 Save Files.ini.

Customizing Launch.bat

Launch.bat contains the command-line argument used to execute an MSI installation. This file is required only for MSI installations.

Modify Launch.bat to specify the .msi file that you want to deploy. The default Launch.bat file sets the path to the Windows system directory. This command line is required for MSI deployment in Windows 98/Me/NT to ensure that the system finds the msixec.exe file, which is required to install the .msi file.

You must also modify the Files.ini file to run Launch.bat.

See [“Customizing Files.ini for MSI deployment”](#) on page 55.

Note: Installation of .msi files requires Windows Installer 2.0 or later. You should ensure that the target computer meets the system requirements before you deploy the product installation.

To customize Launch.bat

- 1 In a text editor, open Launch.bat.
- 2 Ensure that the following command line is included in the file:
`@SET PATH=%path%;%windir%\system`
- 3 Edit the line `@msiexec -i Package.msi` so that it reflects the name of the .msi file that you want to deploy.
For example, `@msiexec -i Symantec Packager - Host Only.msi`

Testing the installation

To test the installation, go to the Web site (for example, <your web site>/webinstall), then click Install.

If the installation fails, note any error messages that are displayed:

- If there is a problem with the parameters in Start.htm, an error message shows the path of the files that the Web-based installation is trying to access. Verify that the path is correct.
- 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 package file.
- Confirm that no other entries were changed during modification.

Notifying users of the download location

You can email instructions to your users to download the package that you want to deploy.

To install a pcAnywhere installation program, users must have Internet Explorer 4.0 or later on their computers. The Internet Explorer security level for the local intranet must be set to Medium so that Symantec ActiveX controls can be downloaded to the client. When the installation is complete, the security level can be restored to its original setting.

Make sure that users understand the system requirements and have the administrative rights that are required for the products that they are installing. For example, to install pcAnywhere, users who are installing on Windows NT/2000/XP must have administrator rights on their own computers and must be logged on with administrator rights. Symantec pcAnywhere also requires Internet Explorer 5.5 SP2 or later for installation.

If your package restarts the client computer at the end of the installation, notify your users that they should save their work and close their applications before they begin the installation. For example, a silent installation on Windows 98 computers restarts the computer at the end of Setup.

Include a URL in your email message that points to the client installation as follows:

- For Internet Information Server:
http://Server_name/Virtual_home_directory/Webinst/
where Server_name is the name of the Web-based server,
Virtual_home_directory is the name of the alias that you created, and
Webinst is the folder that you created on the Web server. (For example,
http://Server_name/ClientInstall/Webinst/)
- For Apache Web Server:
http://Server_name/Webinst/
where Server_name is the name of the computer on which Apache Web
Server is installed. The IP address of the server computer can be used in place
of the Server_name.

Deploying pcAnywhere using SMS 2.0

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

- pcAnywhere installation file: An installation package or custom product installation created by Symantec Packager. It can be created as a self-extracting .exe file or an .msi 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 that is supplied with pcAnywhere is named pcAnywhere.pdf.

Minimum requirements for SMS deployment

The following resources are required to deploy pcAnywhere using SMS:

- 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)
- Symantec Packager 1.0 or later with customized packages created for deployment

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.

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 an SMS deployment package
- Assigning distribution points
- Advertising the package

Preparing the Package Definition File

A default Package Definition File (pcAnywhere.pdf) is provided with pcAnywhere. This file can be modified to accommodate any package created with Symantec 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=UserLoggedIn
- AdminRightsRequired=TRUE

Creating an 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 Symantec Packager to create a product installation .msi file or package installation .exe file, as appropriate, or use one of the supplied, preconfigured pcAnywhere packages.
- 2 In the SMS Administrator console, right-click Packages, then click **New > Package from definition**.
- 3 In the Create Package from Definition Wizard, when prompted for the name of a package file, click **Browse** to locate the pcAnywhere.pdf 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 Click **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 Symantec Packager (or a supplied, preconfigured 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 pcAnywhere package 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 In 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 and 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 Windows NT/2000/XP logon scripts

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

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

Windows NT/2000/XP 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 logon 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 logon script

You can use the following sample logon script to deploy pcAnywhere packages to Windows NT/2000/XP clients. 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 msixec -i %Package%  
IF %PkgType% == EXE %Package%  
  
REM ***** Cleanup *****  
del %Package%  
CD ..  
rd pcapkg  
Net Use Z: /DELETE  
  
:End  
endlocal
```

Testing the logon script

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

Using NetWare logon scripts

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

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

Windows NT/2000/XP 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 logon scripts. You must have administrator rights to perform these tasks.

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 logons. If the server only hosts NDS logons, 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 logon script

Use the following sample logon 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 logon 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 msixec -i %Package%
IF %PkgType% == EXE %Package%

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

:End
endlocal
```

Testing the logon script

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

Performing centralized management

This chapter includes the following topics:

- [About centralized management](#)
- [Managing pcAnywhere hosts remotely](#)
- [Integrating with Microsoft Systems Management Server](#)
- [About the Microsoft Distributed Component Object Model \(DCOM\)](#)
- [About centralized logging](#)

About centralized management

Symantec pcAnywhere includes the pcAnywhere Host Administrator tool, which lets you remotely manage multiple pcAnywhere hosts on a network. The pcAnywhere Host Administrator tool is a Microsoft Management Console (MMC) snap-in and requires MMC to run. MMC is included on the Symantec pcAnywhere CD in the Tools folder.

Symantec pcAnywhere also supports integration with Microsoft Systems Management Server.

See [“Integrating with Microsoft Systems Management Server”](#) on page 75.

Symantec pcAnywhere supports centralized event logging using the pcAnywhere Host Administrator or an SNMP monitor.

See [“About centralized logging”](#) on page 79.

Managing pcAnywhere hosts remotely

The pcAnywhere Host Administrator is an administrator tool that lets you remotely manage the hosts on your network. The pcAnywhere Host Administrator lets you do the following:

- Remotely start, stop, and connect to pcAnywhere hosts 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.

Installing the pcAnywhere Host Administrator tool

The pcAnywhere Host Administrator tool is available as a custom setup option in the full product installation. The pcAnywhere Host Administrator tool requires Windows NT/2000/XP.

Follow this procedure to install the Host Administrator tool after pcAnywhere installation.

To install the Host Administrator Tool

- 1** On the Windows taskbar, click **Start > Settings > Control Panel**.
- 2** In the Control Panel window, double-click **Add/Remove Programs**.
- 3** In the Add/Remove Programs window, click **Symantec pcAnywhere**.
- 4** Click **Change**.
- 5** In the Modify or Remove Symantec pcAnywhere window, click **Next**.
- 6** In the Program Maintenance window, click **Modify**.
- 7** Click **Next**.
- 8** In the Custom Setup window, under pcAnywhere Tools, click the down arrow next to Host Administrator, then click **This feature will be installed on local hard drive**.
- 9** Click the down arrow next to Host Administrator Agent, then click **This feature will be installed on local hard drive**.
The Host Administrator Agent is required to allow pcAnywhere to be remotely managed using Distributed Component Object Management (DCOM) technology.
- 10** Click **Next**.
- 11** To include the program icon on the Windows desktop, check **pcAnywhere Host Administrator**.
- 12** Click **Install**.
- 13** Follow the on-screen instructions to continue the installation process. When the installation is complete, click **Finish**.
- 14** If your computer requires updates to system files, you will be prompted to restart your computer. This step is necessary to ensure proper functionality.

Adding the Host Administrator snap-in to MMC

The Microsoft Management Console (MMC) lets you run and manage administrator tools from a central location. Upon installation of the pcAnywhere Host Administrator tool, you can add it as a snap-in to MMC.

MMC is included with the operating system in Windows 2000/XP. If you need to install MMC, you can install it from the Symantec pcAnywhere CD.

To add the Host Administrator snap-in to MMC

- 1 On the Windows taskbar, click **Start > Programs > pcAnywhere Host Administrator**.
- 2 To start MMC, on the Windows taskbar, click **Start > Run**, then type **mmc**
- 3 On the Console menu, click **Add/Remove Snap-in**.
- 4 In the Add/Remove Snap-in window, on the Standalone tab, click **Add**.
- 5 In the Add Standalone Snap-in window, click **pcAnywhere Host Administrator**.
- 6 Click **Add**.
- 7 Click **Close**.
- 8 In the Add/Remove Snap-in window, click **OK**.

Creating configuration groups

To remotely manage and configure computers using the pcAnywhere Host Administrator console, you must create a configuration group, then add computers to the group.

See [“Adding computers to a configuration group”](#) on page 70.

If you are using MMC, the pcAnywhere Host Administrator console is listed under Console Root.

For more information, see the documentation for MMC.

To create a configuration group

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

Adding computers to a configuration group

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

To add computers to a configuration group

- 1 In the console window, on the left pane, browse to the location of the computers that you want to add, for example Microsoft Windows Network.
- 2 In the left pane, right-click the system that contains the computers that you want to add, then click **Add Systems to Configuration Groups**.
- 3 In the Add Systems to Configuration Groups window, select the computers that you want to add.
- 4 Under Select Destination Group(s), select the configuration group to which you want to add the computers.
- 5 Click OK.

Configuring administrator host and remote connection items

Before you can use the pcAnywhere Host Administrator to remotely manage the hosts on your network, you must first configure the administrator host and remote connection items. These files contain the connection and security settings needed to support connections between the pcAnywhere Host Administrator console and the host computers that you want to manage.

Symantec pcAnywhere provides the following preconfigured host and remote connection items that you can use as templates:

- **Admin.bhf:** Host template for the host computers that you want to remotely manage
To use this template to start a host session, you must configure the caller information. Symantec pcAnywhere requires a user name and password for all host sessions.
For more information, see the *Symantec pcAnywhere User's Guide*.
- **Admin11.chf:** Host Administrator template for the computer from which you want to remotely manage hosts

You can modify these templates in pcAnywhere or you can create new administrator items. Template files are located in the following directory:

\Program Files\Symantec\pcAnywhere\CMS

Creating a new administrator remote item

The administrator remote connection item contains the connection and security information needed to connect to a host computer from the pcAnywhere Host Administrator console. This file has a .chf extension.

You can add this file to the CMS folder to use it with the pcAnywhere Host Administrator or include it in a packaged installation.

To create a new administrator remote item

- 1** In the pcAnywhere Manager window, on the left navigation bar, click **Remotes**.
- 2** On the File menu, click **New > Item > Advanced**.
- 3** In the Remote Properties window, on the Connection Info tab, select one of the following network protocols:
 - TCP/IP
 - SPX
 - NetBIOS
- 4** In the Remote Properties window, configure the other settings that you want to use.
- 5** When you are finished, click **OK**.
For more information, see the *Symantec pcAnywhere User's Guide*.
- 6** In the pcAnywhere Manager window, in the right pane, under Remotes, right-click the remote connection item that you just created, then click **Rename**.
- 7** Type a name.
For example:
Admin11

Creating a new administrator host item

The administrator host connection contains the connection and security information needed to allow a remote administrator to connect from the pcAnywhere Host Administrator console. You must include a caller item.

This file has a .bhf extension. Caller files have a .cif extension. You can add these files to the CMS folder to use them with the pcAnywhere Host Administrator or you can include them in a packaged installation.

To create a new administrator host item

- 1 In the pcAnywhere Manager window, on the left navigation bar, click **Hosts**.
- 2 On the File menu, click **New > Item > Advanced**.
- 3 In the Host Properties window, on the Connection Info tab, select one of the following network protocols:
 - TCP/IP
 - SPX
 - NetBIOS
- 4 On the Callers tab, select the authentication type that you want to use.
- 5 Under Caller list, click the New Item icon.
- 6 In the Caller Properties window, type the logon information for the users who can connect to the host computer, then click **OK**.

A user name and password is required for all host sessions. You can configure other settings, for example, access privileges.

For more information, see the *Symantec pcAnywhere User's Guide*.
- 7 In the Host Properties window, configure the other settings that you want to use, then click **OK**.

For more information, see the *Symantec pcAnywhere User's Guide*.
- 8 In the pcAnywhere Manager window, in the right pane, under Hosts, right-click the host connection item that you just created, then click **Rename**.
- 9 Type a name.

For example:

Admin

Configuring a host item in pcAnywhere Host Administrator

The pcAnywhere Host Administrator tools lets you create a host item that you can distribute to the host computers in your configuration group. Symantec pcAnywhere requires that you set up a logon account for users who connect to your computer and select an authentication method to verify their identities.

To configure a host item in pcAnywhere Host Administrator

- 1 In the console window, in the left pane, under pcAnywhere Host Administrator, click the plus sign next to Configuration Groups to expand it.
- 2 Under the name of the configuration group to which you want to add a host item, right-click **Connection Items**, then click **New > Be A Host**.
- 3 Type a name for this connection item.
- 4 Click **OK**.
- 5 Configure the host connection item, specifying the caller information and other settings that you want to use.

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

Distributing pcAnywhere configuration files

The pcAnywhere Host Administrator tool lets you distribute pcAnywhere configuration files, such as host connection items, to the host computers in your configuration group from the pcAnywhere Host Administrator console.

The host computer must be waiting for a connection.

To distribute pcAnywhere configuration files

- 1 In the pcAnywhere Host Administrator console, in the left pane, under pcAnywhere Host Administrator, click the plus sign next Configuration Groups to expand it.
- 2 Under Configuration Groups, right-click the configuration group to which you want to send the files, then click **Distribute pcAnywhere Files**.
- 3 In the Distribute pcAnywhere Files window, select the computers to which you want to distribute the file.
- 4 Select the file that you want to distribute.
- 5 Click **OK**.

Managing hosts in a configuration group

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

To manage hosts in a configuration group

- 1 In the pcAnywhere Host Administrator console, on the left pane, under pcAnywhere Host Administrator, click the plus sign next to Configuration Groups to expand it.
- 2 Under Configuration Groups, click the plus sign next to the name of your configuration group to expand it.
- 3 Under Systems, right-click the computer that you want to manage, then click **All Tasks**.
- 4 Select one of the following:
 - **Start Specific Host:** Starts a host session on the selected host computer
 - **Start Admin Host:** Starts a host session on the Host Administrator computer
 - **Start Last Host:** Starts a host session on the computer on which you most recently started a host session
 - **Stop Host:** Cancels the host session and disconnects any active sessions on the host
 - **Connect to Admin Host:** Connects to the Host Administrator computer, using the settings that are configured in the admin11.chf remote file
 - **Configure Admin Host:** Reconfigures the settings on the Host Administrator computer
 - **Get Activity Log:** Retrieves the activity log from the remote computer

Integrating with Microsoft Systems Management Server

Symantec pcAnywhere supports integration with the Microsoft Systems Management Server (SMS). SMS is a scalable change and configuration management system for Microsoft Windows-based computers and servers.

Symantec pcAnywhere provides the support files needed to integrate with SMS. These files are offered only on the Symantec pcAnywhere Corporate CD.

Importing the package definition file into SMS

Symantec pcAnywhere provides a package definition file (pcAnywhere.pdf), which contains program settings and other product-specific information that is required for integration with SMS. You must import this file into SMS.

This file is available in the Tools folder on the installation CD.

To import the package definition file into SMS

- 1** Insert the Symantec pcAnywhere CD into the CD-ROM drive.
- 2** In the pcAnywhere installation window, click **Tools**.
This opens an HTML page.
- 3** In the Web browser window, under Third-party tools, click **Microsoft System Management Server (SMS)**.
- 4** Under Microsoft System Management Server (SMS), click **Save pcAnywhere.pdf file**.
- 5** In the Explorer window, select the location in which you want to save the file.
- 6** On the BackOffice server, start SMS.
- 7** In the SMS Administrator, use the Import utility to import the pcAnywhere.pdf file.
- 8** Copy the contents of all seven disks, which are located in the \installs\pcanywhere\pca32full\cd\disk1 directory, into a directory on the server.

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

About the Microsoft Distributed Component Object Model (DCOM)

Symantec pcAnywhere uses Microsoft DCOM technology for all point-to-point communications during remote management tasks. DCOM is used in the pcAnywhere Host Administrator tool and in the SMS integration.

DCOM runs on a variety of network protocols and, by default, attempts to make connections on all installed protocols. After connecting to the network, DCOM uses Windows NT authentication to verify the necessary access rights. For example, an administrator with the appropriate access rights 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 domain or a trusted domain.

Implementing DCOM in Windows NT/2000/XP

To remotely configure and control pcAnywhere on Windows NT/2000/XP using a centralized management tool, you must meet the following system 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.

Implementing DCOM in Windows 98/Me

To remotely configure and control pcAnywhere on Windows 98/Me using a centralized management tool, you must meet the following system requirements:

- The Windows 98/Me client must be logged on to the same Windows NT domain as the administrator.
- The domain name and the workgroup name on the Windows 98/Me computer must be the same.
- The Windows 98/Me computer must be configured with user-level access. This access is required to adjust the DCOM security settings when running the dcomcnfg.exe utility.
- File and print sharing for Microsoft Windows Networks should be installed and enabled on the Windows 98/Me computer.

Modifying DCOM settings

Symantec pcAnywhere configures DCOM during the installation process. The default settings should be sufficient for pcAnywhere management applications to function normally and maintain a sufficient level of security. However, administrators can modify the default security settings in DCOM to allow or deny access to a system.

Modifying DCOM security settings on a managed computer might require adjustments to the DCOM settings on the administrator computer. Ensure 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 centralized management software attempts to impersonate the user who is

making the connection. If the user is not logged on with administrator privileges, this impersonation fails.

To further ensure security, a caller without 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, run the dcomcnfg.exe utility to check the security settings for the client. Edit the default security and add only the domain users or administrators who are allowed to access the host.

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

To modify DCOM settings on Windows NT

- ◆ Do one of the following:
 - In Windows NT/2000/XP, open the \WinNT\System32 folder, then run dcomcnfg.exe.
 - In Windows 98/Me, open the \Windows\System folder, then run dcomcnfg.exe.

About AwShim

AwShim is the management shim between pcAnywhere and the centralized management integration. The pcAnywhere Host Administrator tool uses AwShim to start and stop host and remote sessions. For each action, you can assign 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 the -A parameter are:

- STARTHOST
- STARTREMOTE
- STOPHOST

The -B and -C parameters specify the Be a Host and Call a 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.

About centralized logging

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

The pcAnywhere Host Administrator tool lets you retrieve log files from a host computer on the network and view and process them locally.

Symantec pcAnywhere also supports logging to a Simple Network Management Protocol (SNMP) console. SNMP is used to send SNMPv1 traps to a compatible console, which records the information. Symantec pcAnywhere provides a Management Information Base (MIB) that contains the SNMP events that pcAnywhere generates.

Monitoring performance using SNMP traps

SNMP is a network-monitoring protocol that monitors and logs activities on network devices and equipment, such as adapters, routers, and hubs.

This information can then be sent to any management console that supports SNMP traps, for example MMC or SMS. 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 centralized management tool. Most include the facility to start any program that can be run from the command line.

See [“About the pcAnywhere MIB file”](#) on page 80.

To monitor performance using SNMP traps

- 1 In the pcAnywhere Manager window, on the Edit menu, click **Preferences**.
- 2 In the pcAnywhere Options window, on the Event Logging tab, check **Enable SNMP traps**.
 To find this tab, click the left and right arrows to scroll through the list of tabs.
- 3 Click **Add** to specify which computer should receive the logging information.
- 4 In the SNMP Trap Destination window, type an IP address.
 Repeat this process for each computer that you want to add.
- 5 Click **OK**.
- 6 Select the events that you want to log.
 For more information, see the *Symantec pcAnywhere User's Guide*.
- 7 Click **OK**.

About the pcAnywhere MIB file

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

The pcAnywhere MIB file is located in the following directory:

\Program Files\Symantec\pcAnywhere\CMS\pca_trap.mib

```
--
--  pcAnywhere MIB Definitions (pcAnywhere 11.0)
--  Copyright 1999, 2000, 2003 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 }

-- pcAnywhere version 9x information --
pcversionnneOBJECT 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 declares variable definitions
PcaObject  OBJECT IDENTIFIER ::= { pcaversionnine 9 }

-- pcA version 10 specific information:
pcaversiontenOBJECT IDENTIFIER ::= { pcanywhere 10 }
PcaHostV10 OBJECT IDENTIFIER ::= { pcaversionten 1 }
PcaObjectV10OBJECT IDENTIFIER ::= { pcaversionten 2 }

-- pcA version 11 specific information:
pcaversionelevenOBJECT IDENTIFIER ::= { pcanywhere 11 }
PcaRemoteManagementOBJECT IDENTIFIER ::= { pcaversioneleven 1 }
```

```
-- 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 }

```

```
-- Possible values for XferOperation are:
```

```
-- 0. Sent
-- 1. Recieved
-- 2. Folder Created
-- 3. Delete
-- 4. Copy
-- 5. Move
-- 6. Rename
```

```
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 }

-- Possible reasons for HostEndedReason, these would occur on a
session end.
```

```
-- 0. Remote Logged Off
-- 1. Host Ended Session
-- 2. Connection Lost
-- 3. Remote canceled
-- 4. Inactivity timeout
-- 5. Usage timeout
-- 6. Host reboot
-- 7. Remote reboot
-- 8. Login failed
-- 9. Invalid password
-- 10. Encryption failure
-- 11. Device Failure

-- If the Host Stopped for any reason, HostEndedReason will contain
-- one of the following negative results
-- -1. Device type is unavailable
-- -2. Couldn't Sync State
-- -3. cm_open failed
-- -4. cm_attach failed
-- -5. cm_stat failed
-- -6. Generic failure to get a connection
-- -7. The host was busy
-- -8. The user cancelled the operation
-- -9. Network host name not found
-- -10. Unable to load a modem configuration
-- -11. Asked to change an invalid parameter
-- -12. Unable to process a modem script
-- -13. Modem responded with unknown response
-- -14. Modem could not answer
-- -15. Couldn't sync to modem speed
-- -16. No answer from the modem
-- -17. Gateway error
-- -18. ISDN call rejected
-- -19. ISDN no phone line
-- -20. ISDN line out of order
```

```
-- -21. ISDN invalid destination address
-- -22. ISDN destination number changed
-- -23. ISDN outgoing calls unauthorized
-- -24. ISDN dest not authorized to accept calls
-- -25. Could not update LDAP with status
```

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 }

-- Available Device Types

```
-- 0. Null Device
-- 1. TTY
-- 2. Printer
-- 3. 8250
-- 4. NCSI
-- 5. IPX
-- 6. NetBios
-- 7. INT 14
-- 8. AppleTalk
-- 9. IPX Driver for MACs with NAS
-- 10. Telebit ACS device
-- 11. Banyan
-- 12. SPX
-- 13. TCP/IP
-- 14. TAPI
-- 15. CAPI
```

```

XferFailedFlag OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  optional
    DESCRIPTION
        "This flag will be set if a file transfer event had
        failed."

    ::= { PcaObject 16 }

EncryptionErrorMessage  OBJECT-TYPE
    SYNTAX  DisplayString (SIZE (0..255))
    ACCESS  read-only
    STATUS  optional
    DESCRIPTION
        "Encryption error message"

    ::= { PcaObject 17 }

P3SerialNumber OBJECT-TYPE
    SYNTAX  DisplayString (SIZE (0..255))
    ACCESS  read-only
    STATUS  optional
    DESCRIPTION
        "Processor serial number"

    ::= { PcaObject 18 }

SystemName OBJECT-TYPE
    SYNTAX  DisplayString (SIZE (0..255))
    ACCESS  read-only
    STATUS  optional
    DESCRIPTION
        "Name of the system generating the event."

    ::= { PcaObject 19 }

-- pca Version 10 - Newly added Host events --

```

```
FileAccessReason OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS   read-only
    STATUS   optional
    DESCRIPTION
        "How a file was accessed"
    ::= { PcaObjectV10 1 }

-- Possible values for FileAccessReason are:
-- 0. File Create
-- 1. File Read
-- 2. File Delete
-- 3. File Edit

SourceFile      OBJECT-TYPE
    SYNTAX      DisplayString (SIZE (0..255))
    ACCESS       read-only
    STATUS       optional
    DESCRIPTION
        "The file that was accessed"
    ::= { PcaObjectV10 2 }

IPAddressOBJECT-TYPE
    SYNTAXDisplayString (SIZE (0..255))
    ACCESS   read-only
    STATUS   optional
    DESCRIPTION
        "IP Address generating event"
    ::= { PcaObjectV10 3 }

CommandLineOBJECT-TYPE
    SYNTAXDisplayString (SIZE (0..255))
    ACCESS   read-only
    STATUS   optional
```

```
DESCRIPTION
"A Command Line was executed from the command prompt"
::= { PcaRemoteManagement 1 }

SystemFileNameOBJECT-TYPE
SYNTAXDisplayString (SIZE (0..255))
ACCESS read-only
STATUS optional
DESCRIPTION
"The name of the system file that was changed"
::= { PcaRemoteManagement 2 }

SystemStateOBJECT-TYPE
SYNTAXDisplayString (SIZE (0..255))
ACCESS read-only
STATUS optional
DESCRIPTION
"System State generating event"
::= { PcaRemoteManagement 3 }

ApplicationNameOBJECT-TYPE
SYNTAXDisplayString (SIZE (0..255))
ACCESS read-only
STATUS optional
DESCRIPTION
"The name of the application removed"
::= { PcaRemoteManagement 4 }

ProcessEventOBJECT-TYPE
SYNTAXDisplayString (SIZE (0..255))
ACCESS read-only
STATUS optional
DESCRIPTION
"ProcessEvent generating event"
::= { PcaRemoteManagement 5 }

ProcessNameOBJECT-TYPE
SYNTAXDisplayString (SIZE (0..255))
ACCESS read-only
STATUS optional
```

```
DESCRIPTION
"The name of the process which handles the event"
::= { PcaRemoteManagement 6 }

ServiceStateOBJECT-TYPE
SYNTAXDisplayString (SIZE (0..255))
ACCESS read-only
STATUS optional
DESCRIPTION
"Service State generating event"
::= { PcaRemoteManagement 7 }

ServiceNameOBJECT-TYPE
SYNTAXDisplayString (SIZE (0..255))
ACCESS read-only
STATUS optional
DESCRIPTION
"The name of the service that handles the event"
::= { PcaRemoteManagement 8 }

ServiceDisplayNameOBJECT-TYPE
SYNTAXDisplayString (SIZE (0..255))
ACCESS read-only
STATUS optional
DESCRIPTION
"The service display name"
::= { PcaRemoteManagement 9 }

ServiceDescriptionOBJECT-TYPE
SYNTAXDisplayString (SIZE (0..255))
ACCESS read-only
STATUS optional
DESCRIPTION
"The service description"
::= { PcaRemoteManagement 10 }

LogOnTypeOBJECT-TYPE
SYNTAXDisplayString (SIZE (0..255))
ACCESS read-only
STATUS optional
```

```

        DESCRIPTION
        "Service log on type"
        ::= { PcaRemoteManagement 11 }

ServiceInteractWithDesktopOBJECT-TYPE
    SYNTAXDisplayString (SIZE (0..255))
    ACCESS read-only
    STATUS optional
    DESCRIPTION
    "Service Interact With Desktop generating event"
    ::= { PcaRemoteManagement 12 }

RegistryChangeOBJECT-TYPE
    SYNTAXDisplayString (SIZE (0..255))
    ACCESS read-only
    STATUS optional
    DESCRIPTION
    "Registry Change generating event"
    ::= { PcaRemoteManagement 13 }

RegKeyNameOBJECT-TYPE
    SYNTAXDisplayString (SIZE (0..255))
    ACCESS read-only
    STATUS optional
    DESCRIPTION
    "The registry key name"
    ::= { PcaRemoteManagement 14 }

RegValueNameOBJECT-TYPE
    SYNTAXDisplayString (SIZE (0..255))
    ACCESS read-only
    STATUS optional
    DESCRIPTION
    "The registry value name"
    ::= { PcaRemoteManagement 15 }

RegValueDataOBJECT-TYPE
    SYNTAXDisplayString (SIZE (0..255))
    ACCESS read-only
    STATUS optional

```

```
DESCRIPTION
"The registry value data"
::= { PcaRemoteManagement 16 }

RegFileNameOBJECT-TYPE
SYNTAXDisplayString (SIZE (0..255))
ACCESS read-only
STATUS optional
DESCRIPTION
"The registry file name"
::= { PcaRemoteManagement 17 }

RegNewKeyNameOBJECT-TYPE
SYNTAXDisplayString (SIZE (0..255))
ACCESS read-only
STATUS optional
DESCRIPTION
"The new registry key name"
::= { PcaRemoteManagement 18 }

RegNewValueNameOBJECT-TYPE
SYNTAXDisplayString (SIZE (0..255))
ACCESS read-only
STATUS optional
DESCRIPTION
"The new registry value name"
::= { PcaRemoteManagement 19 }
```

```
-----
-- Version 9 Trap Definitions
-----
```

```
-- Pca Host Alert Traps
```

```
PcaHostStarted TRAP-TYPE
ENTERPRISE PcaHost
VARIABLES {
    DeviceType,
    HostConnectionObject,
    P3SerialNumber,
```

```

        SystemName
    }
    DESCRIPTION "PCA Host was started"
    ::= 1

PcaHostEndSession TRAP-TYPE
    ENTERPRISE PcaHost
    VARIABLES {
        HostEndedReason,
        SystemName
    }
    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,
        SystemName
    }
    DESCRIPTION "PCA Host connection failed - device
error"
    ::= 4

PcaHostStopped TRAP-TYPE
    ENTERPRISE PcaHost
    VARIABLES {
        HostEndedReason,
        SystemName
    }

```

```
DESCRIPTION "PCA Host was stopped"  
::= 5
```

```
PcaHostInSession    TRAP-TYPE  
ENTERPRISE PcaHost  
VARIABLES {  
    RemoteComputerName,  
    CallerName,  
    SystemName  
}  
DESCRIPTION "PCA Host is in session"  
::= 6
```

```
PcaHostConnFailAccessDenied    TRAP-TYPE  
ENTERPRISE PcaHost  
VARIABLES {  
    SystemName  
}  
DESCRIPTION "PCA Host connection failed - access  
denied"  
::= 7
```

```
PcaHostConnFailEncrypt    TRAP-TYPE  
ENTERPRISE PcaHost  
VARIABLES {  
    EncryptionErrorMessage,  
    SystemName  
}  
DESCRIPTION "PCA Host connection failed - encryption  
error"  
::= 8
```

```
PcaHostUnsecuredHostStarted    TRAP-TYPE  
ENTERPRISE PcaHost  
VARIABLES {
```

```

        HostConnectionObject,
        SystemName
    }

    DESCRIPTION "Unsecure launch of PCA Host"
    ::= 9

PcaHostRebooting    TRAP-TYPE
    ENTERPRISE PcaHost
    VARIABLES {
        SystemName
    }

    DESCRIPTION "PCA Host rebooting the system"
    ::= 10

PcaHostLockingWorkstation TRAP-TYPE
    ENTERPRISE PcaHost
    VARIABLES {
        SystemName
    }

    DESCRIPTION "PCA Host locking workstation"
    ::= 11

PcaHostLoggingOffUser TRAP-TYPE
    ENTERPRISE PcaHost
    VARIABLES {
        SystemName
    }

    DESCRIPTION "PCA Host is logging off the current
user"

    ::= 12

-----
-- pcA Version 10.0 New host traps --
-----

```

```

PcaHostFileAccess TRAP-TYPE
    ENTERPRISE PcaHostV10
    VARIABLES {
        HostComputerName,
        RemoteComputerName,
        SourceFile,
        FileAccessReason
    }
    DESCRIPTION "Host file access"
    ::= 1

PcaHostExeLaunch TRAP-TYPE
    ENTERPRISE PcaHostV10
    VARIABLES {
        HostComputerName,
        RemoteComputerName,
        SourceFile
    }
    DESCRIPTION "Host executable launch"
    ::= 2

PcaConnPortScanned TRAP-TYPE
    ENTERPRISE PcaHostV10
    VARIABLES {
        IPAddress
    }
    DESCRIPTION "Port Scanned"
    ::= 3

PcaConnRapsScanned TRAP-TYPE
    ENTERPRISE PcaHostV10
    VARIABLES {
        IPAddress
    }
    DESCRIPTION "Raps Scanned"

```

```

::= 4

PcaConnFailedRestrictedIP TRAP-TYPE
    ENTERPRISE PcaHostV10
    VARIABLES {
        IPAddress
    }
    DESCRIPTION "Restricted IP"
::= 5

PcaConnFailedSerialMismatch TRAP-TYPE
    ENTERPRISE PcaHostV10
    VARIABLES {
        IPAddress,
        RemoteComputerName
    }
    DESCRIPTION "Serial Mismatch"
::= 6

PcaAuthWarning TRAP-TYPE
    ENTERPRISE PcaHostV10
    VARIABLES {
        CallerName
    }
    DESCRIPTION "Authentication Warning - Weak
Password"
::= 7

-----

PCA Remote Generated Traps

-----

PcaRemoteStarted TRAP-TYPE
    ENTERPRISE PcaRemote
    VARIABLES {
        DeviceType,

```

```

        RemoteConnectionObject,
        P3SerialNumber,
        SystemName
    }
    DESCRIPTION "PCA Remote was started"
    ::= 1

```

```

PcaRemoteInSession    TRAP-TYPE
    ENTERPRISE  PcaRemote
    VARIABLES   {
        HostComputerName,
        SystemName
    }
    DESCRIPTION "PCA Remote is in session"
    ::= 2

```

```

PcaRemoteEndSession    TRAP-TYPE
    ENTERPRISE  PcaRemote
    VARIABLES   {
        SystemName
    }
    DESCRIPTION "PCA Remote has ended the session"
    ::= 3

```

```

PcaRemoteAbnormalEndSession    TRAP-TYPE
    ENTERPRISE  PcaRemote
    VARIABLES   {
        SystemName
    }
    DESCRIPTION "PCA Remote has ended the session
abnormally"
    ::= 4

```

```

PcaRemoteConnFailDeviceError    TRAP-TYPE
    ENTERPRISE  PcaRemote

```

```

                                VARIABLES    {
                                    DeviceType,
                                    SystemName
                                }
error"
                                DESCRIPTION "PCA Remote connection failure - device

                                ::= 5

PcaRemoteConnFailHostBusy    TRAP-TYPE
                                ENTERPRISE   PcaRemote
                                VARIABLES    {
                                    SystemName
                                }
busy"
                                DESCRIPTION "PCA Remote connection failure - host

                                ::= 6

PcaRemoteConnFailHostNotFound    TRAP-TYPE
                                ENTERPRISE   PcaRemote
                                VARIABLES    {
                                    SystemName
                                }
not found"
                                DESCRIPTION "PCA Remote connection failure - host

                                ::= 7

PcaRemoteConnFailBadPassword    TRAP-TYPE
                                ENTERPRISE   PcaRemote
                                VARIABLES    {
                                    SystemName
                                }
password"
                                DESCRIPTION "PCA Remote connection failure - bad

                                ::= 8

PcaRemoteConnFailEncryption    TRAP-TYPE

```

```

ENTERPRISE  PcaRemote
VARIABLES   {
              EncryptionErrorMessage,
              SystemName
            }
DESCRIPTION "PCA Remote connection failure -
encryption error"
::= 9

```

```

-----
-- PCA File Transfer Generated Traps
-----

```

```

PcaFileXferStarted  TRAP-TYPE
ENTERPRISE  PcaFileXfer
VARIABLES   {
              HostComputerName,
              RemoteComputerName,
              SystemName
            }
DESCRIPTION "PCA File Transfer started"
::= 1

```

```

PcaFileXferEnded  TRAP-TYPE
ENTERPRISE  PcaFileXfer
VARIABLES   {
              SystemName
            }
DESCRIPTION "PCA File Transfer ended"
::= 2

```

```

PcaFileXferAbnormalEnd  TRAP-TYPE
ENTERPRISE  PcaFileXfer
VARIABLES   {
              HostComputerName,

```

```

        RemoteComputerName,
        SystemName
    }

    DESCRIPTION "PCA File Transfer ended abnormally"
    ::= 3

PcaFileXferOperationCancelled    TRAP-TYPE

    ENTERPRISE PcaFileXfer
    VARIABLES {
        SystemName
    }

    DESCRIPTION "PCA File Transfer operation cancelled"
    ::= 4

PcaFileXferOperation    TRAP-TYPE

    ENTERPRISE PcaFileXfer
    VARIABLES {
        XferOperation,
        XferSourceFile,
        XferDestFile,
        XferBytes,
        XferVirusFlag,
        XferFailedFlag,
        SystemName
    }

    DESCRIPTION "PCA File Transfer detailed operation
notice"

    ::= 5

PcaFileXferVirusFound    TRAP-TYPE

    ENTERPRISE PcaFileXfer
    VARIABLES {
        XferSourceFile,
        SystemName
    }

```

```

virus."
        DESCRIPTION "PCA File Transfer has detected a
        ::= 6

```

```

-----
-- PCA Version 11 - Remote Management Events
-----

```

```

RMCmdPrmptCmdLine  TRAP-TYPE
        ENTERPRISE  PcaRemoteManagement
        VARIABLES {
                CommandLine
        }
        DESCRIPTION "Command Prompt - Command Line"
        ::= 1

```

```

RMSysFileChanges  TRAP-TYPE
        ENTERPRISE  PcaRemoteManagement
        VARIABLES {
                SystemFileName
        }
        DESCRIPTION "System File Changes"
        ::= 2

```

```

RMSysStateChanges  TRAP-TYPE
        ENTERPRISE  PcaRemoteManagement
        VARIABLES {
                SystemState
        }
        DESCRIPTION "System State Changes"
        ::= 3

```

```

RMUninstallApp  TRAP-TYPE
        ENTERPRISE  PcaRemoteManagement
        VARIABLES {

```

```

        ApplicationName
    }
    DESCRIPTION "Uninstall Application"
    ::= 4

RMProcessChanges TRAP-TYPE
    ENTERPRISE PcaRemoteManagement
    VARIABLES {
        ProcessEvent,
        ProcessName
    }
    DESCRIPTION "Process Changes"
    ::= 5

RMServiceStateChanges TRAP-TYPE
    ENTERPRISE PcaRemoteManagement
    VARIABLES {
        ServiceState,
        ServiceName
    }
    DESCRIPTION "Service State Changes"
    ::= 6

RMServiceCfgChanges TRAP-TYPE
    ENTERPRISE PcaRemoteManagement
    VARIABLES {
        ServiceName,
        ServiceDisplayName,
        ServiceDescription,
        LogOnType,
        ServiceInteractWithDesktop
    }
    DESCRIPTION "Service Configuration Changes"
    ::= 7
```

```

RMRegistryChanges TRAP-TYPE
    ENTERPRISE PcaRemoteManagement
    VARIABLES {
        RegistryChange,
        RegKeyName,
        RegValueName,
        RegValueData,
        RegFileName,
        RegNewKeyName,
        RegNewValueName
    }
    DESCRIPTION "Registry Changes"
    ::= 8

-----

-- The remaining pcAnywhere SNMP Traps are not yet implemented
-- PCA Monitor Traps
-----

PcaMonitorFullProductNotInstalled TRAP-TYPE
    ENTERPRISE PcaMonitor
    VARIABLES {
        SystemName
    }
    DESCRIPTION "PCA Monitor - The PCA Full product is
not installed"
    ::= 1

PcaMonitorHostNotInstalled TRAP-TYPE
    ENTERPRISE PcaMonitor
    VARIABLES {
        SystemName
    }
    DESCRIPTION "PCA Monitor - The PCA Host is not
installed"

```

```
::= 2
```

```
PcaMonitorRemoteNotInstalled    TRAP-TYPE
                                ENTERPRISE PcaMonitor
                                VARIABLES {
                                    SystemName
                                }
                                DESCRIPTION "PCA Monitor - The PCA Remote is not
installed"
                                ::= 3
```

```
PcaMonitorHostNotWaiting    TRAP-TYPE
                                ENTERPRISE PcaMonitor
                                VARIABLES {
                                    SystemName
                                }
                                DESCRIPTION "PCA Monitor - The PCA Host is not
waiting for a connection"
                                ::= 4
```

```
PcaMonitorHostNotAutoStart    TRAP-TYPE
                                ENTERPRISE PcaMonitor
                                VARIABLES {
                                    SystemName
                                }
                                DESCRIPTION "PCA Monitor - The PCA Host is not set
to auto start"
                                ::= 5
```

```
PcaMonitorHostNotWaitingOnDialup    TRAP-TYPE
                                ENTERPRISE PcaMonitor
                                VARIABLES {
                                    SystemName
                                }
                                DESCRIPTION "PCA Monitor - The PCA Host is not
waiting on a dialup"
```

```
::= 6
```

```
PcaMonitorHostLanOnlyNotInstalled    TRAP-TYPE
    ENTERPRISE    PcaMonitor
    VARIABLES {
        SystemName
    }
    DESCRIPTION "PCA Monitor - The PCA Host LAN only is
not installed"
    ::= 7
```

```
PcaMonitorLiveUpdateNotRun    TRAP-TYPE
    ENTERPRISE    PcaMonitor
    VARIABLES {
        SystemName
    }
    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
    VARIABLES {
        SystemName
    }
    DESCRIPTION "PCA Monitor - Reset install traps"
    ::= 1
```

```
PcaResetHostNotWaitingReset    TRAP-TYPE
    ENTERPRISE    PcaReset
```

```

                                VARIABLES {
                                    SystemName
                                }
                                DESCRIPTION "PCA Monitor - Reset Host not waiting
traps"
                                ::= 2

PcaResetHostNotAutoStartReset    TRAP-TYPE
                                ENTERPRISE PcaReset
                                VARIABLES {
                                    SystemName
                                }
                                DESCRIPTION "PCA Monitor - Reset Host not auto start
traps"
                                ::= 3

PcaResetHostWaitingOnDialupReset  TRAP-TYPE
                                ENTERPRISE PcaReset
                                VARIABLES {
                                    SystemName
                                }
                                DESCRIPTION "PCA Monitor - Reset Host waiting on
dialup traps"
                                ::= 4

PcaResetLiveUpdateNotRunReset    TRAP-TYPE
                                ENTERPRISE PcaReset
                                VARIABLES {
                                    SystemName
                                }
                                DESCRIPTION "PCA Monitor - Reset Live Update not run
traps"
                                ::= 5

```

```
-----  

-- PCA Install Traps  

-----
```

```
PcaInstallRebootRequired TRAP-TYPE  

    ENTERPRISE PcaInstall  

    VARIABLES {  

        SystemName  

    }  

    DESCRIPTION "PCA Install - A reboot is required"  

    ::= 1  

END
```


Integrating pcAnywhere with Directory Services

This chapter includes the following topics:

- [About directory services](#)
- [Overview of the LDAP informational model](#)
- [Using Directory Services with pcAnywhere](#)
- [Configuring the directory servers](#)
- [Configuring pcAnywhere to use directory services](#)

About 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.

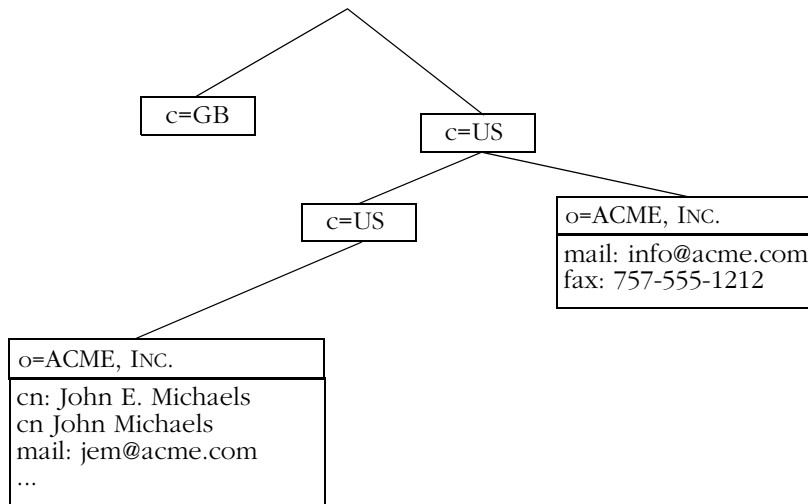
The benefit of using directory services with pcAnywhere is increased speed. Normally, when you launch a remote connection, it scans the network for waiting pcAnywhere hosts. This can be time consuming and the results can vary depending on the size of the network and whether the host is on a different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

Overview of the 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. Containers and leaf entries are used to show an organizational structure by creating entries that represent the countries, organizational units, and people that fit into the various areas of the organization.

The example in [Figure 5-1](#) 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.

Figure 5-1 Example of an LDAP hierarchical tree

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 object class to which they belong. An LDAP server has a list of all known object classes. Administrators can add new and edit existing object classes to let client applications store specific types of attributes. The object class is stored as an entry attribute called `objectclass` and controls which attributes are required and permitted in an entry. Some common object class values are `person`, `organizationalUnit`, and `organizationalPerson`. Combinations of object classes 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 you double-click one of the entries, 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 object class description to the LDAP server's configuration. This custom object class describes the information the LDAP server needs to store for each host that a user starts. Once the custom object class is available, modify all existing entries to store values that belong to the new object class.

The custom pcAnywhere object class 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 Netscape Directory Server 3.1

- 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 the 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 Netscape Directory Server 4.0

- 1 Start the Netscape Console 4.0 application.
- 2 In the left 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 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 procedures only apply if LDAP is installed, configured, and functioning on the Novell server with Novell Directory Services (NDS) 8.0.

Administrator rights to the server are needed to perform these procedures, which include:

- Configuring the `pcaHostEntry`
- Configuring the `pcaHost` object
- Mapping the LDAP attribute
- Mapping the NDS class
- Creating an LDIF file
- Assigning rights

Creating the `pcaHostEntry` in ConsoleOne

Follow this procedure to create the `pcaHostEntry`.

To create the `pcaHostEntry` in ConsoleOne

- 1 Log on to 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 ASN1 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**.

Creating the **pcaHost** object in ConsoleOne

Follow this procedure to create the **pcaHost** object.

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**.

Mapping the **LDAP** attribute to the **NDS** attribute

Follow this procedure to map the LDAP attribute to the NDS attribute.

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**.

Mapping the NDS class to the LDAP class

Follow this procedure to map the NDS class to the LDAP class.

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.

Creating an LDIF file

Follow this procedure to create an LDIF file.

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\

Assigning rights to an individual user

Follow this procedure to assign rights to an individual user.

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**.

Assigning rights to multiple users

Follow this procedure to assign rights to multiple users.

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.

To implement Windows Active Directory in pcAnywhere, you must extend the schema on the server. This process involves the tasks:

- Adding the snap-in
- Creating the pcaHostEntry attribute
- Creating the pcaHost object
- Associating the pcaHost object
- Setting user rights

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

Adding the snap-in

Follow this procedure to add the snap-in to the Microsoft Management Console (MMC).

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**.

Creating the `pcaHostEntry` attribute

Follow this procedure to create the `pcaHostEntry` attribute.

To create the `pcaHostEntry` attribute

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

Creating the **pcaHost** object

Follow this procedure to create the **pcaHost** object.

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 **Auxiliary**.
- 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**.

Associating the **pcaHost** object with the user object class

Follow this procedure to associate the **pcaHost** object with the user object class.

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.

Setting up edit rights for the user

Follow this procedure to set up edit rights for the user.

To set up edit 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

Configuring pcAnywhere to use directory services involves the following process:

- Set up directory services in pcAnywhere preferences 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

Configure the directory server entries before beginning the following procedure.

To set up directory services in pcAnywhere

- 1 In the pcAnywhere Manager window, on the Edit menu, click **Preferences**.
- 2 In the pcAnywhere Options window, 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.
You should always configure this information. 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**.
Symantec 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 to use directory services

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 to use directory services

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

To set up the remote computer to use directory services

- 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 preconfigured 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.

Managing security in Symantec pcAnywhere

This chapter includes the following topics:

- [Ways to secure pcAnywhere](#)
- [How pcAnywhere works with Windows security](#)
- [Controlling access to pcAnywhere hosts](#)
- [Protecting session security](#)
- [Maintaining audit trails](#)
- [Implementing policy-based administration](#)

Ways to secure 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. 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*.

How pcAnywhere works with Windows security

Symantec pcAnywhere runs on all Microsoft Windows 32-bit operating systems. However, if maintaining the highest level of security is a priority, Windows NT/2000/XP are the recommended operating systems. These operating systems were designed for security.

Symantec pcAnywhere leverages many of the inherent security features in Windows NT/2000/XP such as user authentication, event logging, and data encryption. For the highest level of security, you should use the security measures provided by the operating system.

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

Controlling access to pcAnywhere hosts

The first step in securing a computer environment is controlling remote access to the network. Administrators 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 and implementing secure, remote access server (RAS) and Virtual Private Network (VPN) solutions in place of individual dial-up devices.

These are some of the methods that pcAnywhere provides to control access to pcAnywhere hosts:

- Limiting connections to specific computer names or IP addresses
See [“Limiting connections to specific computer names or IP addresses”](#) on page 130.
- Serializing pcAnywhere installations
Symantec pcAnywhere lets you create custom installation package with an embedded security code, or serial number. This serial number must be present on both the host and remote computers to make a connection.
See [“Serializing a pcAnywhere installation”](#) on page 30.
- Implementing an authentication method
Symantec pcAnywhere supports a number of centralized authentication types, including Active Directory, Novell Directory Services, Novell Bindery, NT, and RSA SecurID, giving you the flexibility of using the authentication measures already in place on your network.
See [“Leveraging centralized authentication in pcAnywhere”](#) on page 130.
- Scanning for unsecured hosts
The Remote Access Perimeter Scanner lets you scan your network and telephone lines to identify unprotected remote access hosts and plug security holes. This separately installed administrator tool is available on the Symantec pcAnywhere Corporate CD.
See [“Identifying security risks”](#) on page 143.
- Limiting logon attempts per call
Limiting the number of consecutive times that a remote user can attempt to log on to the host computer helps protect against hacker and denial of service attacks. Symantec pcAnywhere ends the connection if a remote user is not able to log on successfully before reaching the limit.
For more information, see the *Symantec pcAnywhere User’s Guide*.
- Limiting time to complete logon
Limiting the amount of time that a remote user has to successfully log on to the host computer helps protect against hacker and denial of service attacks.
For more information, see the *Symantec pcAnywhere User’s Guide*.
- Prompting to confirm connections
If you enable this option, pcAnywhere notifies the host user that someone is attempting to connect. The host user has the option to allow or deny the connection.
For more information, see the *Symantec pcAnywhere User’s Guide*.

Limiting connections to specific computer names or IP addresses

Block outside connections to a pcAnywhere host by configuring the host to accept only the connections that fall within a specific subnet or range of TCP/IP addresses that you specify. Remote users outside the firewall must connect through a secure tunnel or VPN that is included in the range of addresses that you specify.

An experienced hacker might be able to circumvent this measure by spoofing or stealing a valid IP address. For maximum security, use this feature in combination with serialization.

To limit connections to specific computer names or IP addresses

- 1 In the pcAnywhere Manager window, on the Edit menu, click **Preferences**.
- 2 In the pcAnywhere Options window, on the Host Communications tab, under Limit connections to the following names or IP addresses, type the computer name or IP address of the remote users from which you want to allow connections.
- 3 Click **Add Restriction**.
- 4 Repeat steps 2 and 3 for each computer name or IP address from which you want to allow connections.
- 5 Click **OK**.

Leveraging centralized authentication in pcAnywhere

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

Symantec pcAnywhere supports a number of centralized authentication types, including Active Directory, Novell Directory Services, Novell Bindery, NT, and RSA SecurID, giving you the flexibility of using the authentication measures already in place on your network.

Using two-factor authentication

Symantec pcAnywhere supports RSA SecurID two-factor authentication. SecurID validates users against a security code, which is generated by an authenticator, and a user-provided PIN.

You must have the RSA ACE/Server and Agents properly installed and configured on your network.

For more information, visit the RSA Web site at:

www.rsa.com

To implement SecurID in pcAnywhere, you must do the following:

- Install and configure the RSA ACE/Agent on the host computer.
For more information, see the documentation provided by RSA.
- On the host computer, open pcAnywhere and configure a host connection item to use SecurID authentication.
For more information, see the *Symantec pcAnywhere User's Guide*.

When a remote user attempts to connect to a host computer that uses SecurID authentication, the user is prompted for authentication credentials, which include a PIN number, logon name, and passcode.

The host computer handles the data requests between the remote computer and the RSA ACE/Agent, which is installed on the host computer. The RSA ACE/Agent handles the data requests between the host computer and the RSA ACE/Server.

If the tokencode that is provided by the remote user is out of sync with the server clock or appears to be compromised, the user is prompted for another tokencode. This Next Tokencode is generated by the SecurID authenticator. The remote user must wait for this tokencode before continuing.

Note: To use RSA SecurID authentication, the host and remote computers must be running Symantec pcAnywhere 11.0.

Using Microsoft Windows-based authentication types

Table 6-1 provides information on the authentication types available for Microsoft Windows-based platforms.

Table 6-1 Microsoft Windows-based authentication types

Microsoft Windows-based authentication types	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.

Table 6-1 Microsoft Windows-based authentication types

Microsoft Windows-based authentication types	Explanation	Implementation in pcAnywhere
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.
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.

Setting up Windows NT authentication for global users

Symantec pcAnywhere lets you configure a server using NT authentication to support callers from the local administrator user group and any global groups that are included in the local group.

Using this feature, you can set up a caller account on a server for all administrators in your company by adding a domain account to the local administrator group. This configuration option is less time-consuming than adding an individual account for each administrator to the local administrator group.

This feature is supported only for Windows NT authentication.

To set up Windows NT authentication for global users

- 1 In the pcAnywhere Manager window, on the left navigation bar, click **Hosts**.
- 2 Do one of the following:
 - To add a new connection item, on the File menu, click **New > Item > Advanced**.
 - To modify an existing connection item, in the right pane, under Host, right-click a connection item, then click **Properties**.
- 3 In the Host Properties window, on the Callers tab, under Authentication type, click **NT**.

- 4 Do one of the following:
 - To add a new caller, under Caller list, double-click the New Item icon.
 - To modify an existing caller, in the Caller list, double-click a name.
- 5 In the Caller Properties window, on the Identification tab, check **Support global NT users and groups defined in Local NT groups**.
- 6 Click OK.

Using Novell-based authentication types

Table 6-2 provides information on the authentication types for Novell-based platforms.

Note: Novell-based authentication requires Novell NetWare Client 32.

Table 6-2 Novell-based authentication types

Novell-based authentication types	Explanation	Implementation in pcAnywhere
Novell Bindery	Validates a user by checking a list stored in a Novell NetWare Bindery.	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 types

Table 6-3 explains the Web-based authentication methods that are available.

Table 6-3 Web-based authentication types

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. The 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. The 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.

Protecting session security

Symantec pcAnywhere provides a number of options to protect the privacy of a session and prevent users from performing specific tasks that might interfere with the host session. These security measures provide an additional layer of security, but are most effective when used in combination with stronger security features in pcAnywhere. These measures include authentication and encryption, which are designed to protect the host from unauthorized access and intentional disruption of service.

These are some of the methods that pcAnywhere provides to protect session security:

- **Strong encryption**
Protect the data stream, including the authorization process, from eavesdropping and hacker attacks by using strong encryption. Symantec pcAnywhere supports public-key and symmetric types of strong encryption. For further security, pcAnywhere lets you deny connections to or from a computer that uses a lower level of encryption.
- **Inactivity time limits for sessions**
Protect the host from users who might inadvertently forget to end a session by configuring the host to disconnect if there has been no keyboard or mouse input within a specified time limit.
- **Individual caller rights**
When applicable, limit the level of access that a caller has to the host. pcAnywhere lets you restrict users from performing certain functions on the host, such as restarting the host computer, transferring files to or from the host, or cancelling the host.
- **Time limits for individual users or user groups**
Protect the host from malicious users intent on disrupting service, as well as from innocent users who inadvertently forget to end a session, by setting time limits for sessions and configuring the host to automatically end the session after a specified length of inactivity. These options are configured at the caller level.
- **Secure end-of-session options**
Securely end host sessions to prevent potential security breaches. You can handle normal end of sessions and abnormal end of sessions differently, choosing to cancel the host or continue to wait for connections, log off the host user, restart the host computer, or lock the computer.

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

Maintaining audit trails

Symantec pcAnywhere event logging helps you monitor session activities and track information for auditing purposes. You can track who connected to a host, session duration, what files were accessed as well as important security information such as authentication or logon failures.

Depending on your environment, you can send information about events that occurred during a session to a pcAnywhere generated log file, the Windows Event

Log, or a Simple Network Management Protocol (SNMP) console. Symantec pcAnywhere supports centralized logging, so you can archive the logs on a secure, central server.

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. You should also remember to periodically archive log files.

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

Implementing policy-based administration

Administrators can securely customize the look and behavior of pcAnywhere through centralized policy-based administration. Symantec pcAnywhere supports Group Policy in Windows 2000/XP and operating system policy integration in Windows 98/Me/NT4.

Administrator rights are required to modify policy settings in Windows NT4/2000/XP.

Implementing Group Policy in Windows 2000/XP

You must use the Microsoft Management Console (MMC) Group Policy snap-in to administer group policy in Windows 2000/XP. To manage policy for a site, domain, or organizational unit, you should open Group Policy from Active Directory, then link the Group Policy object to the appropriate Active Directory container. The operating system provides a software wizard to guide you through this process.

For more information about adding the Group Policy snap-in to MMC, see the online documentation for your operating system.

Symantec pcAnywhere defines policy settings in an administrative template. After you add the Group Policy snap-in to MMC, you must import the pcAnywhere.adm file into MMC.

See [“Importing the pcAnywhere administrative template”](#) on page 137.

Implementing system policy in Windows 98/Me/NT4

The System Policy Editor in Windows 98/Me/NT4 lets you manage policy settings on these systems. Policy settings in Windows 98/Me can be modified by any user and are not as secure as Group Policy in Windows 2000/XP.

For more information about the System Policy Editor, see the online documentation for your operating system.

Symantec pcAnywhere defines policy settings in an administrative template. After you start the System Policy Editor, you can import the pcAnywhere.adm file.

See [“Importing the pcAnywhere administrative template”](#) on page 137.

Importing the pcAnywhere administrative template

Symantec pcAnywhere provides administrative templates for Windows 2000/XP and Windows 98/Me/NT4 to support registry-based policy management. The pcAnywhere.adm files define the policy settings for certain components in pcAnywhere and include registry keys and values, the location in which the registry settings will be written, and other descriptive information.

Importing the pcAnywhere.adm file for Windows 2000/XP

The pcAnywhere.adm file for Windows 2000/XP is located on the pcAnywhere CD in the Tools\Policy folder. You can copy this file to a secure location, then import it into MMC. Before you import this file, ensure that you have added the Group Policy snap-in to MMC.

To import the pcAnywhere.adm file for Windows 2000/XP

- 1 To start MMC, on the Windows taskbar, click **Start > Run**, then type **mmc**
- 2 In the console window, in the left pane, select the Group Policy object for which you want to set policies.
- 3 Under the Group Policy object, right-click Administrative Templates, then click **Add/Remove Templates**.
- 4 In the Add/Remove Templates window, click **Add**.
- 5 Browse to the location of the pcAnywhere.adm file, select it, then click **Open**.
- 6 In the Add/Remove Templates window, click **Close**.

Importing the pcAnywhere.adm file for Windows 98/Me/NT4

The pcAnywhere.adm file for Windows 98/Me/NT is located on the pcAnywhere CD in the Tools\Policy\NT4_9x_Me folder. You can copy this file to a secure location, then import it into the System Policy Editor. Ensure that you select the correct pcAnywhere.adm file.

To import the pcAnywhere.adm file for Windows 98/Me/NT4

- 1 To start the System Policy Editor, on the Windows taskbar, click **Start > Run**, then type **poledit.exe**
- 2 In the System Policy Editor window, on the Options menu, click **Policy Template**.
- 3 In the Policy Template Options window, click **Add**.
- 4 Browse to the location of the pcAnywhere.adm file, select it, then click **Open**.
- 5 In the Policy Template Options window, click **OK**.

For more information about running the System Policy Editor and importing administrative template files, see the online documentation for your operating system.

Managing user policies

Symantec pcAnywhere lets you control whether users can access certain portions of the user interface or perform certain functions in pcAnywhere. [Table 6-4](#) provides information about the policy settings that pcAnywhere lets you control.

Table 6-4 Location of pcAnywhere policy settings

Folder	Description
Actions	Contains policy settings to prohibit users from doing the following: ■ Launching the pcAnywhere Manager window, which is the main user interface for pcAnywhere ■ Launching host objects, thereby starting a host session ■ Launching remote objects, thereby connecting to a host computer ■ Cancelling a host computer that is running ■ Using the keyboard or mouse on the host computer during a session ■ Using LiveUpdate to download product updates ■ Registering the product online ■ Starting a chat session ■ Using file transfer and command queue features

Table 6-4 Location of pcAnywhere policy settings

Folder	Description
Actions\pcAnywhere Tools	Contains policy settings to prohibit users from using the following tools in pcAnywhere: ■ Package Deployment Tool ■ Host Administrator ■ Remote Access Perimeter Scanner ■ Activity Log Processing
Actions\Remote Management	Contains policy settings to prohibit users from using all Remote Management features or from using individual features
UI Changes\Host Objects	Contains policy settings to prohibit users from doing the following: ■ Editing host objects ■ Creating host objects ■ Changing the directory location of host objects ■ Viewing or editing specific property pages ■ Customizing the host name, which is used to identify the host computer
UI Changes\Remote Objects	Contains policy settings to prohibit users from doing the following: ■ Editing remote objects ■ Creating remote objects ■ Changing the directory location of remote objects ■ Viewing or editing specific property pages
UI Changes\Option Sets	Contains policy settings to prohibit users from doing the following: ■ Editing option set objects and global pcAnywhere preferences ■ Creating option set objects ■ Changing the directory location of object set objects ■ Viewing or editing specific property pages for option sets and global pcAnywhere preferences
UI Changes\Device Visibility	Contains policy settings to remove specific device types (for example, Infrared, TAPI) from the list of available connection types

Table 6-4 Location of pcAnywhere policy settings

Folder	Description
UI Changes\Help	Lets you use a custom URL for the Service and Support option on the Help menu

Managing user policies in Windows 2000/XP

To manage user policies in Windows 2000/XP, you must run MMC with the Group Policy snap-in. Ensure that you have imported the appropriate pcAnywhere administrative template.

See [“Importing the pcAnywhere administrative template”](#) on page 137.

To manage user policies in Windows 2000/XP

- 1 To start MMC, on the Windows taskbar, click **Start > Run**, then type **mmc**
- 2 In the console window, in the left pane, click the plus sign next to the group policy object that you want to manage to expand the list.
- 3 Under User Configuration, click the plus sign next to Administrative Templates to expand the list.
- 4 Click the plus sign next to Symantec pcAnywhere to expand the list.
- 5 Open the folder that contains the policy settings that you want to edit.
See [Table 6-4, “Location of pcAnywhere policy settings,”](#) on page 138.
- 6 In the right pane, under Policy, double-click the policy setting that you want to edit.
- 7 In the properties window, on the Policy tab, select one of the following:
 - Enabled: Sets the policy, which typically prevents a user from viewing or performing a task
 - Disabled: Unsets the policy, which typically allows a user to view or perform a task
- 8 Click OK.

Managing user policies in Windows 98/Me/NT4

To manage user policies in Windows 98/Me/NT4, you must run the System Policy Editor. On Windows 98/Me/NT 4 workstation, you might need to install this tool separately. To apply policy settings to users upon system logon, you must create a directory share in the Windows or NT system32\imports\scripts folder called Netlogon.

For more information, see the documentation for your operating system.

Before you begin, ensure that you have imported the appropriate pcAnywhere administrative template.

See [“Importing the pcAnywhere administrative template”](#) on page 137.

To manage user policies in Windows 98/Me/NT4

- 1** To start the System Policy Editor, on the Windows taskbar, click **Start > Run**, then type **poedit.exe**
- 2** In the System Policy Editor window, on the File menu, click **New Policy**.
- 3** Double-click the icon that represents the user or group for which you want to set policies.
- 4** In the properties window, click the plus sign next to Symantec pcAnywhere to expand the list.
- 5** Under Symantec pcAnywhere, click the plus sign next to the policy type that you want to edit.
- 6** Check the policy settings that you want to enable.
Enabling a policy setting typically prevents users from viewing or performing a task.
- 7** Click **OK**.
- 8** Save the policy file in the Windows or NT system32\imports\scripts folder using the file name NTconfig.pol.

Identifying security risks

This chapter includes the following topics:

- [About the Remote Access Perimeter Scanner](#)
- [Installing the Remote Access Perimeter Scanner](#)
- [Opening the Remote Access Perimeter Scanner](#)
- [Setting global options](#)
- [Logging Remote Access Perimeter Scanner events](#)
- [Creating a custom scan file](#)
- [Running a Remote Access Perimeter Scanner scan](#)
- [Viewing scan results](#)

About the Remote Access Perimeter Scanner

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 scans your network for remote access products and identifies potential security risks. The Remote Access Perimeter Scanner is available only in Symantec pcAnywhere Corporate Edition.

The Remote Access Perimeter Scanner lets you do the following:

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

Disclaimer

The Remote Access Perimeter Scanner is intended to help you identify security risks in your own organization. Using the Remote Access Perimeter Scanner 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 the Remote Access Perimeter Scanner.

When you use the Remote Access Perimeter Scanner to scan TCP/IP connections, the Remote Access Perimeter Scanner sends a packet to the computer to which you are connecting that states, “The Remote Access Perimeter Scanner is scanning your system from” and identifies your TCP/IP address, user name, and computer name.

Products included in a scan

The Remote Access Perimeter Scanner scans for the following remote access products:

- Symantec pcAnywhere
The Remote Access Perimeter Scanner searches for pcAnywhere for DOS 5.0, pcAnywhere 2.0, and pcAnywhere versions 7.5 through 11.0.
The Remote Access Perimeter Scanner can automatically shut down pcAnywhere hosts that do not require a logon.
For more information, see [“Setting global options”](#) on page 147.

- 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

Installing the Remote Access Perimeter Scanner

The Remote Access Perimeter Scanner is available as a custom setup option in the full product installation. Follow this procedure to install the Remote Access Perimeter Scanner after pcAnywhere installation.

To install the Remote Access Perimeter Scanner

- 1 On the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 In the Control Panel window, double-click **Add/Remove Programs**.
- 3 In the Add/Remove Programs window, click **Symantec pcAnywhere**.
- 4 Click **Change**.
- 5 In the Modify or Remove Symantec pcAnywhere window, click **Next**.
- 6 In the Program Maintenance window, click **Modify**.
- 7 Click **Next**.
- 8 In the Custom Setup window, under pcAnywhere Tools, click the down arrow next to Remote Access Perimeter Scanner, then click **This feature will be installed on local hard drive**.
- 9 Click **Next**.

- 10
- To include the program icon on the Windows desktop, check **Remote Access Perimeter Scanner**.
- 11
- Click **Install**.
- 12
- Follow the on-screen instructions to continue the installation process. When the installation is complete, click **Finish**.
- 13
- If your computer requires updates to system files, you will be prompted to restart your computer. This step is necessary to ensure proper functionality.

Opening the Remote Access Perimeter Scanner

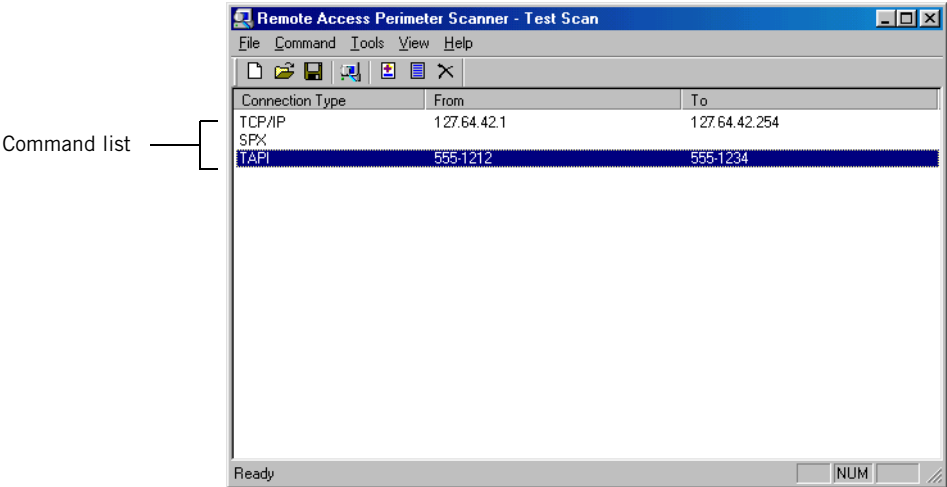
The instructions in the remainder of this chapter assume that you know how to open the Remote Access Perimeter Scanner.

Every time that you open the Remote Access Perimeter Scanner, you are prompted to read the Remote Access Perimeter Scanner license agreement.

To open the Remote Access Perimeter Scanner

- ◆
- On the Windows taskbar, click **Start > Programs > Remote Access Perimeter Scanner**.
- Figure 7-1
- shows the contents of a scan file as displayed in the Remote Access Perimeter Scanner window.

Figure 7-1 Remote Access Perimeter Scanner scan results



Running the Remote Access Perimeter Scanner from a command line

You can use the Remote Access Perimeter Scanner command line to run a scan from a program scheduler or batch file.

To run the Remote Access Perimeter Scanner from a 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, the Remote Access Perimeter Scanner uses the last scan file you opened. If you don't include `/s`, Remote Access Perimeter Scanner opens the scan file, but doesn't start the scan.

It might be necessary to include the fully qualified path to the Remote Access Perimeter Scanner executable and scan file name.

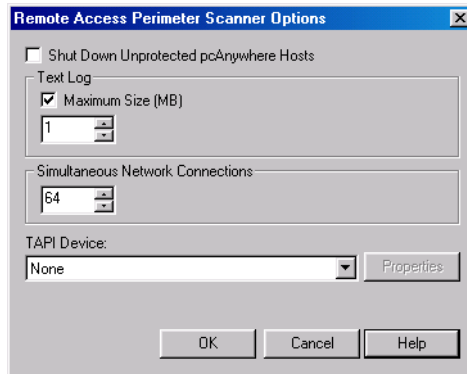
Setting global options

You can configure the Remote Access Perimeter Scanner to automatically shut down unsecured pcAnywhere hosts and place limits on the maximum size of the text log file that 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 Remote Access Perimeter Scanner Tools menu, click **Options**.



- 2 If you want to shut down unprotected pcAnywhere hosts, in the Remote Access Perimeter Scanner Options window, check **Shut Down Unprotected pcAnywhere Hosts**.
- 3 Check **Maximum Size (MB)** and type a number in MB to restrict how large the text log grows.
- 4 In the Simultaneous Network Connections box, set the network usage. 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.
- 5 In the TAPI Device list, select the modem you want to use to make TAPI connections.
- 6 Click OK.

Logging Remote Access Perimeter Scanner events

The Remote Access Perimeter Scanner logs events separately from pcAnywhere, but uses the same methods. This section covers the procedures for setting up SNMP traps, Windows Event Logging, and local text file logging.

SNMP traps and Windows Event Logging are more robust than simple text file logging. Text logging on the local computer is always enabled during Remote Access Perimeter Scanner scanning.

About event log classifications

The Remote Access Perimeter Scanner classifies events in two ways: Potential Vulnerability and Product Found.

When the Remote Access Perimeter Scanner 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:

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

When the Remote Access Perimeter Scanner 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:

- The Remote Access Perimeter Scanner finds an unknown product. (Unknown means that the product is not detected by Remote Access Perimeter Scanner.)
- The Remote Access Perimeter Scanner looks for one product and finds another. For example, if Remote Access Perimeter Scanner is looking for pcAnywhere and finds LapLink, then LapLink is “unknown” for that scan.

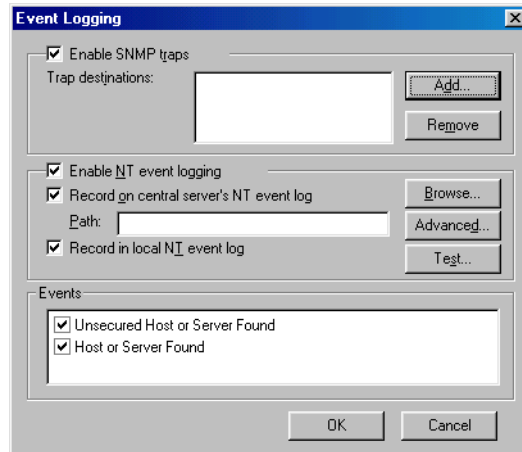
Setting SNMP traps

Follow this procedure to set up SNMP traps to log Remote Access Perimeter Scanner events.

See [“About centralized logging”](#) on page 79.

To set SNMP traps

- 1 On the Remote Access Perimeter Scanner Tools menu, click **SNMP** and **NT Event Logging**.
- 2 In the Event Logging window, check **Enable SNMP traps**.



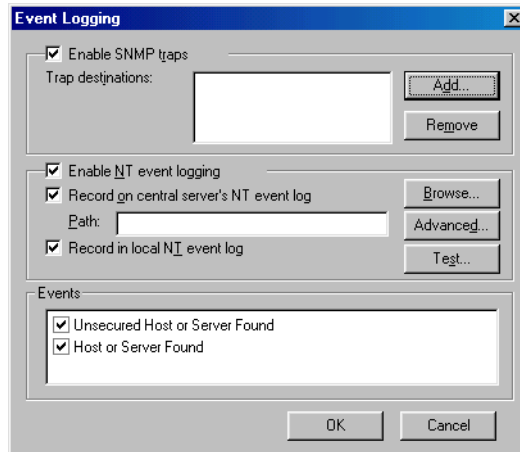
- 3 Do one of the following:
 - Click **Add** to enter trap destinations.
New trap destinations appear in the Trap destination window.
 - Click **Remove** to remove selected trap destinations from the list.
- 4 Check the events that you want to include in the log.
- 5 Click **OK**.

Setting up Windows Event Logging

Follow this procedure to log Remote Access Perimeter Scanner events in the Windows Event Log on your local computer or on a central server.

To set up Windows Event Logging

- 1 On the Remote Access Perimeter Scanner Tools menu, click **SNMP and NT Event Logging**.
- 2 In the Event Logging window, check **Enable NT event logging**.



- 3 Check **Record on central server's NT event log** to save the events in a central location.
- 4 Type 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 Under **Events**, 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 the Remote Access Perimeter Scanner 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 Remote Access Perimeter Scanner 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

The Remote Access Perimeter Scanner 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 and save a scan file

- 1 On the Remote Access Perimeter Scanner 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 Remote Access Perimeter Scanner 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, you can 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 Remote Access Perimeter Scanner Command menu, click **New**.
- 3 On the General tab, select 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.

Table 7-1 Remote Access Perimeter Scanner connection settings

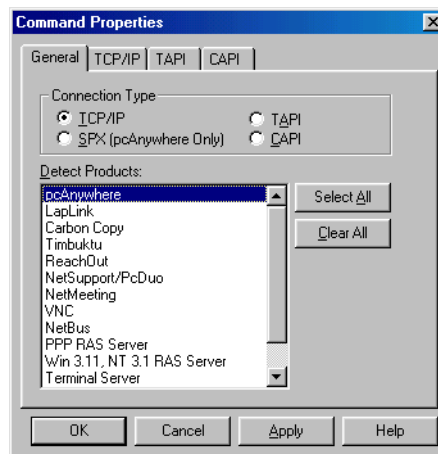
Tab	Lets you	For more information, see
General	Select the connection type and the remote access products that you want to detect. You also use this tab to set up an SPX command.	“Configuring SPX scan settings” on page 156.
TCP/IP	Specify the IP addresses that you want to scan. You can specify the IP address by the full subnet or partial subnet address. You can also include additional ports in the scan.	“Configuring TCP/IP scan settings” on page 154.
TAPI	Specify the numbers that you want to dial, including the country code.	“Configuring TAPI scan settings” on page 157.
CAPI	Specify the numbers that you want to dial.	“Configuring CAPI scan settings” on page 158.

Configuring TCP/IP scan settings

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

To configure TCP/IP scan settings

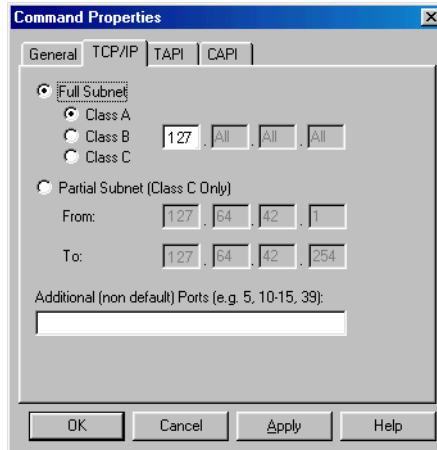
- 1 Open the scan file that you want to customize or create a new scan file.
- 2 On the Remote Access Perimeter Scanner Command menu, click **New**.
- 3 In the Command Properties window, on the General tab, under Connection Type, click TCP/IP.



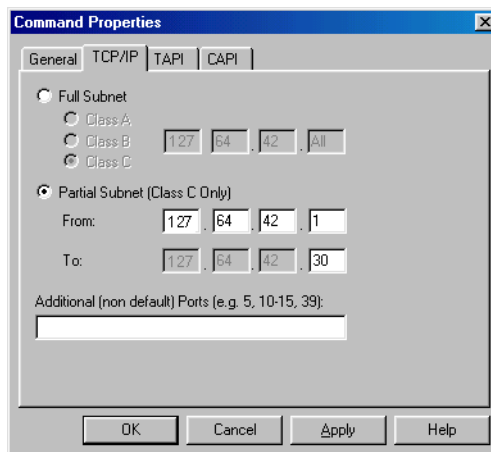
- 4 Under Detect Products, select the products that you want to detect.

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.



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



6 Type any additional ports that you want to scan.

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

Configuring SPX scan settings

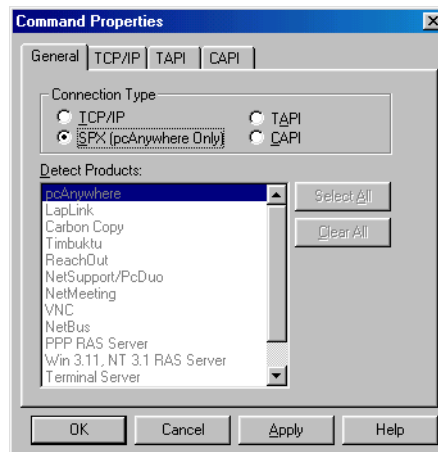
To scan for remote access products using an SPX connection, add an SPX command to your scan file.

On SPX connections, Remote Access Perimeter Scanner only scans for pcAnywhere.

To configure SPX scan settings

- 1 On the Remote Access Perimeter Scanner Command menu, click **New**.
- 2 In the Command Properties window, on the General tab, under Connection Type, click **SPX (pcAnywhere Only)**.

When you click SPX, Remote Access Perimeter Scanner automatically selects pcAnywhere and disables the remainder of the Detect Products list.



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

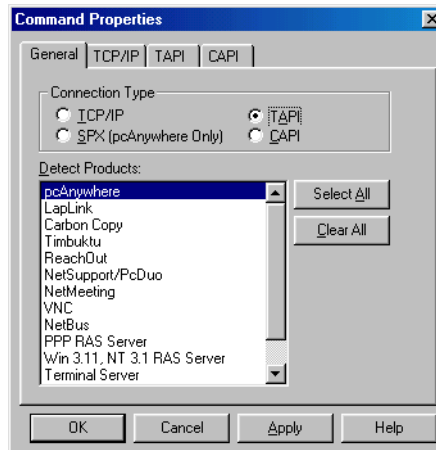
Configuring TAPI scan settings

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 Remote Access Perimeter Scanner scan.

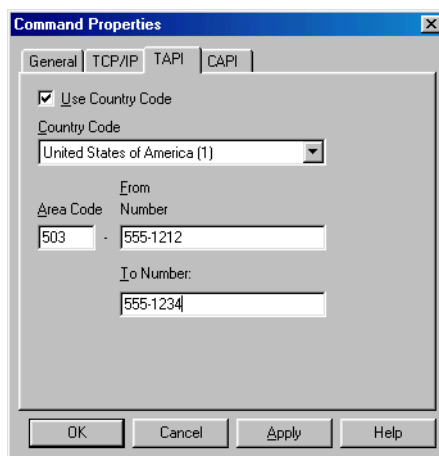
To configure TAPI scan settings

- 1 Open a scan file that you want to customize or create a new scan file.
- 2 On the Remote Access Perimeter Scanner Command menu, click **New**.
- 3 In the Command Properties window, on the General tab, under Connection Type, click **TAPI**.



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

- 5 On the TAPI tab, type 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. Type the ending number in the To Number box.



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

Configuring CAPI scan settings

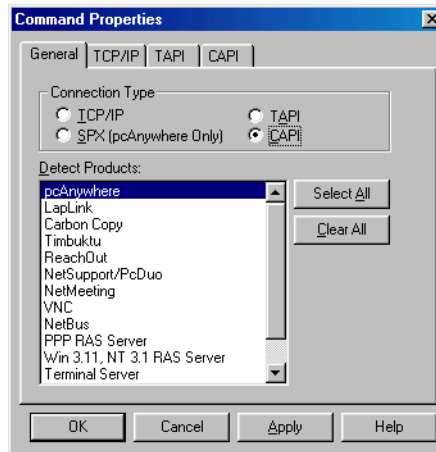
To scan for remote access products using a CAPI connection, add a CAPI command to your scan file.

Symantec is not responsible for telephone charges incurred during a Remote Access Perimeter Scanner scan.

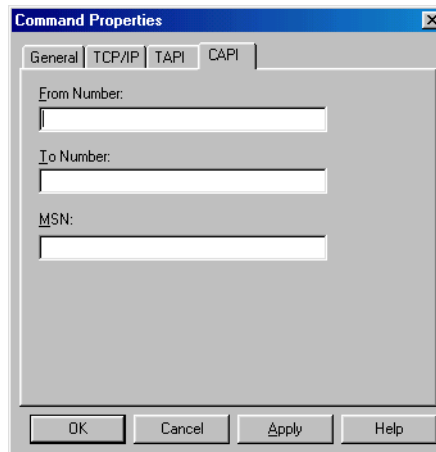
To configure CAPI scan settings

- 1 Open the scan file you want to customize or create a new scan file.
- 2 On the Remote Access Perimeter Scanner Command menu, click **New**.

- 3 In the Command Properties window, on the General tab, under Connection Type, click CAPI.



- 4 Under Detect Products, 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 Select the command, then press **Delete**.

Running a Remote Access Perimeter Scanner scan

When you run a Remote Access Perimeter Scanner 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 dialog box shows when the Remote Access Perimeter Scanner starts a connection. It takes time to make the connection, detect the remote access products, and return that information to the Remote Access Perimeter Scanner. The status might not change for a few moments while the Remote Access Perimeter Scanner processes the information.

To run a Remote Access Perimeter Scanner scan

- ◆ On the Remote Access Perimeter Scanner File menu, click **Start Scan**. You can also press **F5**.
The Scan Results window displays status information.

Viewing scan results

Upon 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 view scan results

- ◆ On the Remote Access Perimeter Scanner View menu, click **Text Log**.

Index

Symbols

.atf files 15
.bhf files 27, 72
.chf files 27, 71
.cif files 27, 72
.cqf files 27
.sid files 30

A

ACE/Agent. *See* SecurID
ACE/Server. *See* SecurID
Active Directory Services 120
Admin.bhf file 71
Admin11.chf file 71
administrative template 137
alias 58
ATF Converter tool 15
authentication
 centralized types 130
 configuring global users 132
 Microsoft Windows-based methods 131
 Novell-based methods 133
 two-factor 130
 Web-based methods 134
AutoTransfer files, converting 15
awshim.exe 78

B

building
 packages 44
 product configuration files 24

C

caller files 27
CAPI, scanning ports 158
command configuration files. *See* custom commands
command queue files 27
computer names, restricting connections 130

configuration files
 adding to packages 26
 distributing 74
configuration groups 70
conflicts, viewing 42
connection item files
 host 27
 remote 27
connection items
 host 37
 remote 38
custom commands
 adding to package definition files 42
 overview 40
custom installations. *See* packages

D

DCOM
 modifying security settings 77
 overview 76
 requirements
 Windows 98/Me 77
 Windows NT/2000/XP 77
dcomcnfg.exe file 78
dependencies, viewing 42
deployment
 customizing files 53
 over the Web 49
 testing 57
 using NetWare login scripts 64
 using SMS 59
 using Windows login scripts 62
directory services
 configuring
 host settings 125
 LDAP servers 114
 Netscape Directory Server 3.1 114
 Netscape Directory Server 4.0 115
 Novell Directory Server 116

- directory services (*continued*)
 - configuring (*continued*)
 - pcAnywhere settings 124
 - remote settings 126
 - Windows Active Directory 120
 - LDAP overview 112
- DynIP custom package 13

E

- event logging 135
 - building automated responses 80
 - on central server 79
 - SNMP traps 79

F

- Files.ini file 54, 55

G

- Group Policy 136

H

- Host Administrator
 - adding computers 70
 - adding computers to groups 71
 - adding configuration groups 70
 - adding host configuration items 74
 - adding to MMC 69, 70
 - connection item templates 71
 - distributing configuration files 74
 - installing 68
 - managing a host 75
 - sending commands 74
 - using AwShim 78
- host computers
 - limiting connections 130
 - securing 128
 - shutting down 148
- host items
 - adding to packages 27
 - configuring 71
- Host Only product 12
- host sessions, securing 134

I

- installation
 - over previous versions 13
 - system requirements 10
 - user rights 11
- installation files *See* packages
- installation options
 - custom products 34
 - installation packages 42
- integrity management 28
- IP addresses, limiting connections by 130
- ISDN connections, scanning ports 158

L

- LAN Host product 12
- LDAP, overview 112
- license agreements
 - Remote Access Perimeter Scanner 144
 - Symantec Packager 20
- limited users 11
- LiveUpdate 39
- logging
 - on central server 79
 - Remote Access Perimeter Scanner 148
 - SNMP traps 79
- login scripts
 - for Novell deployment 64
 - for Windows deployment 62
 - testing 64, 66

M

- management shims 78
- MIB 80
- Microsoft Management Console. *See* MMC
- migration
 - about 13
 - from pcAnywhere 10.x 14
 - of AutoTransfer files 15
 - of configuration data 13
 - of packages 15
 - of pcAnywhere 10.x 15
- MMC
 - about Group Policy snap-in 136
 - adding computers 70
 - adding configuration groups 70
 - adding Host Administrator snap-in 70

MMC (*continued*)
 managing policies 140
 modem connections, scanning ports 157

N

Netscape Directory Server 114, 115
 NetWare login scripts
 deploying packages 64
 testing 66
 network connections
 restricting IP address 130
 scanning
 SPX ports 156
 TCP/IP ports 154
 Novell Directory Server 116
 NT authentication, configuring global users 132

O

option sets
 adding to packages 33
 applying locally 34
 overview 32

P

package definition files
 adding custom commands 42
 adding products to 42
 building 44
 importing into SMS 75
 viewing product requirements 42
 Packager. *See* Symantec Packager
 packages
 adding configuring files 26
 adding custom commands 40
 configuring product installation settings 34
 configuring products 23
 defining 41
 deployment
 over Web 49
 testing 57
 using SMS 59
 integrity stamping 28
 product dependencies 25
 product settings
 host templates 37
 installation directory 36

packages (*continued*)
 product settings (*continued*)
 online registration 36
 preserving 39
 product updates 39
 remote templates 38
 serializing 30
 setting global options 32
 testing 45
 pcAnywhere Express 12
 pcAnywhere Tools
 Host Administrator 68
 Remote Access Perimeter Scanner 144
 pcAnywhere.adm file 137
 PMI file 22
 policy management
 settings 138
 user rights 136
 Windows 2000/XP
 editing policies 140
 implementing 136
 importing administrative template 137
 Windows 98/Me/NT4
 editing policies 140
 implementing 136
 importing administrative template 137
 product configuration files
 adding to package definitions 42
 building 24
 product definition files, building 43
 product modules, importing 22
 product requirements 42

R

RAPS. *See* Remote Access Perimeter Scanner
 Readme file 10
 registry keys 28
 Remote Access Perimeter Scanner
 adding commands 152
 creating a scan file 152
 installing 145
 logging 148
 modifying commands 160
 opening 146
 overview 144
 remote access products 144
 setting preferences 147

- Remote Access Perimeter Scanner (*continued*)
 - setting SNMP traps 149
 - shutting down hosts 148
 - using from the command line 147
 - viewing scan results 161
- remote items
 - adding to packages 27
 - configuring 71
- remote management 68
- Remote Only product 12

S

- SecurID 130
- security ID
 - adding to packages 30
 - generating 30
- serial ID
 - adding to packages 30
 - generating 30
- shim 78
- SMS
 - deployment of packages 59
 - importing pcAnywhere files 75
 - using AwShim 78
 - using MIB 80
- SNMP traps 79, 135, 149
- SPX, scanning ports 156
- Start.htm file 54
- Symantec Packager
 - customizing products 23
 - importing product modules 22
 - process overview 21
 - system requirements 20
 - using for migrations and upgrades 17
- Symantec pcAnywhere
 - location of configuration files 27
 - migrating and upgrading 13
- system requirements 10

T

- TAPI, scanning ports 157
- TCP/IP
 - restricting access 130
 - scanning ports 154
- templates, Host Administrator 71

U

- unprotected hosts, identifying 143
- upgrades
 - about 13
 - from pcAnywhere 9.2x 16
- user rights 11

W

- Web server
 - configuring 52
 - copying installation files 50
- Web-based authentication 134
- Windows Active Directory 120

Symantec pcAnywhere™

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 distributor.

Briefly describe the problem:

CD Replacement Price \$ 10.00

Sales Tax (See Table) \$ 9.95

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 ☐ AMEX

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

555 International Way

Springfield, OR 97477 (800) 441-7234

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

Symantec and Symantec pcAnywhere are trademarks of Symantec Corporation.
Other brands and products are trademarks of their respective holder/s.
© 2003 Symantec Corporation. All rights reserved. Printed in the U.S.A.

