Symantec pcAnywhere™ Administrator's Guide

Symantec pcAnywhere™ Administrator's Guide

Documentation version 12.0

Legal Notice

Symantec Corporation 20330 Stevens Creek Blvd. Cupertino, CA 95014 USA

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product feature and function, installation, and configuration. The Technical Support group also authors content for our online 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 and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- A telephone and web-based support that provides rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week worldwide. Support is provided in a variety of languages for those customers that are enrolled in the Platinum Support program
- Advanced features, including Technical Account Management

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/ent/enterprise.html

Select your country or language under Global Support. The specific features that are available may vary based on the level of maintenance that was purchased and the specific product that you are using.

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/techsupp/ent/enterprise.html

Select your region or language under Global Support, and then select the Licensing and Registration page.

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/ent/enterprise.html

Select your country or language under Global 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 about product updates and upgrades
- Information about upgrade insurance and maintenance contracts
- Information about the Symantec Value License Program
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

- Asia-Pacific and Japan: contractsadmin@symantec.com
- Europe, Middle-East, and Africa: semea@symantec.com
- North America and Latin America: supportsolutions@symantec.com

Additional Enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively. Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.

Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring and management capabilities, each focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Chapter 3 Deploying Symantec pcAnywhere custom installations

Chapter 4 Performing centralized management

Chapter 1

Planning a migration and upgrade strategy

This chapter includes the following topics:

About migrations and upgrades

Symantec pcAnywhere supports migration from versions 10.x to version 12.0 on Windows 98/Me/NT/2000/2003 Server/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 9.2.x to version 12.0 on Windows 98/Me/NT/2000/2003 Server/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 14.

Table 1-1 includes information that you can use as a reference in planning your migration and upgrade strategy.

Table 1-1 Migration and upgrade strategy matrix

Symantec pcAnywhere version	Operating system	Restart required	Data preserved automatically
11.x	Windows NT/2000/2003 Server/XP	No	Host items Caller items Remote items Option sets Registry settings AutoTransfer files (must be converted) Serial ID sets
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)
9.2.x	Windows NT/2000/XP	No Uninstalls previous version	None
9.2.x	Windows 98/Me	Yes Uninstalls previous version	None

Migrating from pcAnywhere 11.x in Windows NT/2000/2003 Server/XP

Symantec pcAnywhere supports full migration of the full product version and host-only version of pcAnywhere 11.x to version 12.0 in Windows NT/2000/2000/2003 Server/XP.

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.

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

Migrating from pcAnywhere 10.x in Windows NT/2000/ 2003 Server/XP

Symantec pcAnywhere supports full migration of the full product version and host-only version of pcAnywhere 10.x to 12.0 in Windows NT/2000/2003 Server/XP.

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.

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 of the full product version and host-only version of pcAnywhere 10.x to pcAnywhere 12.0 in Windows 98/Me.

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.

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 14.

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

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

Symantec pcAnywhere supports upgrades of the full product and host-only versions of pcAnywhere 9.2.x to version 12.0 in Windows NT/2000/XP.

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 14.

Upgrading from pcAnywhere 9.2.x in Windows 98/Me

If you are installing pcAnywhere version 12.0 on a Windows 98/Me computer that has version 9.2.x 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 uninstallation 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 14.

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 installation 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 that you need.

See "Using Symantec Packager to streamline migrations and upgrades" on page 14.

Chapter 2

Creating custom installation packages

This chapter includes the following topics:

About Symantec Packager

Symantec Packager lets you create, modify, and build custom installation packages that you can distribute to target systems. You can use Symantec Packager to tailor installations to fit your corporate environment by 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/2000/2003 Server/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 shows the process for creating custom installation packages with Symantec Packager.

Figure 2-1 Overview of Symantec Packager phases

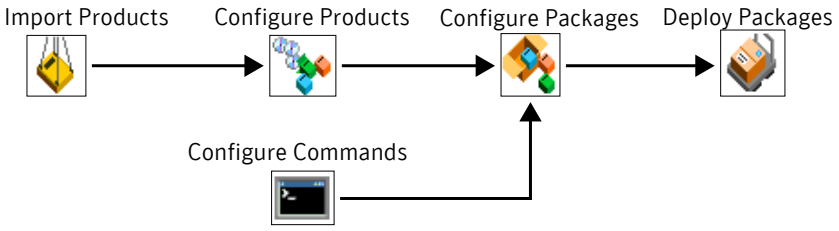

Table 2-1 outlines the process for creating packages.

Table 2-1 Package creation process

Task	Description	Reference
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 20.
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 21.
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 38.
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 39.
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 40.

Table 2-1 Package creation process *(continued)*

Task	Description	Reference
Test the package.	You should test packages before deploying them to end users to ensure proper functionality.	See "Testing packages" on page 42.
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 "About deployment" on page 43.

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, and 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 2-2 includes information about the configuration options that are available in the default pcAnywhere product configuration file.

Table 2-2 Symantec pcAnywhere product configuration options

Tab	Settings
Features	You can customize the following features in pcAnywhere such as: ■ User interface (pcAnywhere Manager) ■ Remote components ■ Host components ■ Communications protocols ■ Documentation (online manuals and Help) ■ Symantec installation utilities
Configuration Files	The pcAnywhere product template includes default remote and host configuration items that you can configure after you install the package or custom product. You can add configuration files that you create in pcAnywhere to the package or custom product configuration for further customization.

Table 2-2 Symantec pcAnywhere product configuration options *(continued)*

Tab	Settings
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 41.

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 2-3 lists some of the key product dependencies.

Table 2-3 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 communication 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 communication protocol.
Remote Control	Required for all custom product installations.
File Transfer	Requires at least one communication protocol.
Remote Management	Requires at least one communication protocol.
Chat	Requires at least one communication 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 window, on the Features tab, do any of the following:
   - Select the product features that you want to include in the custom product.
   - Clear 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 window
Apply	Saves your changes and lets you continue the product configuration

4 If prompted, type a file name, and 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, and 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.HST)	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)	Provides default settings to support connections to a host computer over a modem, network, or direct connection. Also provides default settings to start a connection in file transfer or remote management mode.
Host connection item files (.bhf)	Provides 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	Lets you configure global options for pcAnywhere to accommodate unique configuration requirements.
Host Security IDs	Lets you serialize the pcAnywhere installation.

Remote connection item files (.chf)	Lets you preconfigure the connection and security settings needed to connect to another computer remotely. For more information, see the *Symantec pcAnywhere User's Guide*.
Command queue files	Lets you automate file transfer, command-line, and end-of-session tasks. For more information, see the *Symantec pcAnywhere User's Guide*.
Host connection item files (.bhf)	Lets you preconfigure the connection and security settings needed to allow a connection from another computer. For more information, see the *Symantec pcAnywhere User's Guide*.
Caller files (.cif)	Lets 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 *Symantec pcAnywhere User's Guide*.

Symantec pcAnywhere configuration files are located in the following folders:

Windows 2000/2003 Server/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 window, on the Configuration Files tab, do one of the following:
   - Select the type of preconfigured file that you want to add, and then click **Add**.
   - Browse to the configuration file that you want to include, and 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, and 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 window, do one of the following:
   - Click **OK** to save your changes and close the Product Editor window.
   - Click **Apply** to save your changes and continue the product configuration.
4. If prompted, type a file name, and then click **Save**.

Integrity stamping a product configuration

You can prevent unauthorized changes to the installed product by using integrity management. 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 use integrity management, 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 using 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 management in conjunction with

policy management and overall strong security practices, such as hardening the operating system.

See "Implementing policy-based administration" on page 99.

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 Features tab, click the plus sign next to Symantec installation utilities to expand the listing.
3. Select **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 32.
6. Select one of the following:

OK	Saves your changes and closes the Product Editor window
Apply	Saves your changes and lets you continue the product configuration

7. If prompted, type a file name, and then click **Save**.
8. Do one of the following:
   - Build the product.
     Building a product configuration file creates an .msi file that contains the single product.
   - Create a package that includes the product, and then build the package.
     Building a package creates a self-extracting .exe file.

   See "Building product installations and packages" on page 40.

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, and 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. Serial IDs must be a numeric value between 0 and 4,294,967,296.

To let a remote user connect to one or more host computers that use different serial IDs, you must include the serial ID 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 dialog box, under Limit host connections by using the following serial IDs, type the serial ID number that you want to use.

   Serial IDs must be a numeric value between 0 and 4,294,967,296.
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 in Symantec Packager. 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 window, 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)** , and then click **Add**.
4. Browse to the folder that contains the serial ID file (*.sid) that you generated in pcAnywhere, select the file, and 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 32.
6. Select one of the following:

OK	Saves your changes and closes the Product Editor window
Apply	Saves your changes and lets you continue the product configuration

7. If prompted, type a file name, and then click **Save**.
8. Do one of the following:
   - Build the product.
     Building a product configuration file creates an .msi file that contains the single product.
   - Create a package that includes the product, and then build the package.
     Building a package creates a self-extracting .exe file.

See "Building product installations and packages" on page 40.

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 2-4 lists the properties that are available.

Table 2-4 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 computer
Remote Communications	Contains customization options for modem and network connections on the remote computer
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

Table 2-4 Symantec pcAnywhere option set properties *(continued)*

Tab	Description
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, and 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 2-4 on page 30.
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)**, and then click **Add**.

3 Browse to the folder that contains the option set files (*.opt) that you created in pcAnywhere, select the one that you want to use, and 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 window.
- Click **Apply** to save your changes and continue the product configuration.

5 If prompted, type a file name, and 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, and 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, and 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 Packager 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 33.

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 34.
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 35.
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 35.
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 35.
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 36.
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 by default in the Program Files directory under Symantec\pcAnywhere. 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 dialog box, select one of the following:

- Program Files directory
- Root of system drive
- Custom path

4 Under Folder specification, type the full path to the location in which you want to install the product.

5 Click **OK**.

6 In the Product Editor window, do one of the following:

- Click **OK** to save your changes and close the Product Editor window.
- Click **Apply** to save your changes and continue the product configuration.

7 If prompted, type a file name, and 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 dialog box, select**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 window.

- Click **Apply** to save your changes and continue the product configuration.

6 If prompted, type a file name, and 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 dialog box, 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 dialog box, 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 window.
- Click **Apply** to save your changes and continue the product configuration.

8 If prompted, type a file name, and 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 dialog box, 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 window.
   - Click **Apply** to save your changes and continue the product configuration.
6. If prompted, type a file name, and 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 dialog box, select **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 window.
- Click **Apply** to save your changes and continue the product configuration.

6 If prompted, type a file name, and 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.

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 39.

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 window.
- Click **Apply** to save your changes and continue the product configuration.

6 If prompted, type a file name, and 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 dialog box, 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 dialog box, under Command line and switches, type the command-line arguments and switches that are required to run the command.

For example, to run the uninstallation 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. For example:

“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**.

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 window, as well as any product requirements or conflicts.

To add products and commands 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 window, on the Product Selection tab, click **Add**.
3. In the Open dialog box, 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 window.
   - Click **Apply** to save your changes and continue the package definition.
7. If prompted, type a file name, and 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 as follows:

   Product was built successfully.
3. In the Product Build Status dialog box, 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 as follows:

   Package was built successfully.
3. In the Build Status dialog box, click **Close**.

Testing packages

It is important to test packages before you deploy 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 customize 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 users.

Chapter 3

Deploying Symantec pcAnywhere custom installations

This chapter includes the following topics:

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/2000/2003 Server/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 45.
- 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 54.
- Logon scripts
  Package and product installations created with Symantec Packager can be distributed to Windows NT/2000/2003 Server/XP and Novell NetWare target computers using a logon script.
  See "Using Windows NT/2000/2003 Server/XP logon scripts" on page 58.
  See "Using NetWare logon scripts" on page 60.

About package 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 a self-extracting executable (.exe) file or create a custom product installation for a single product as an .msi file.

About Web-based deployment requirements

Table 3-1 lists the minimum requirements that the server or computer must meet before you implement Web-based deployment on a Web server or target computer.

Table 3-1 Web server and target computer requirements

Deployment	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.

Table 3-1 Web server and target computer requirements *(continued)*

Deployment	Requirements
Target computer	■ Internet Explorer 4.0 or later. Symantec pcAnywhere requires Internet Explorer 6.x 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.

File names are case-sensitive. The following is an example of the folder structure on the Web server:

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

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 49.

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 46.

Creating a virtual directory on the Web server

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

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**, and 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), and then click **Next**.
6. Type the location of the installation folder (for example, C:\Client\Webinst), and then click **Next**.
7. For access permissions, select **Read only**, and 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**, and then click **Finish**.

To create a virtual directory on an Apache Web Server

1. In a text editor, do one of the following:
   - If you are using Apache Web Server 2.0 or later, open **httd.conf**. This file is installed by default in C:\Program Files\ Apache Group\Apache2\conf.
   - If you are using Apache Web Server 1.3, open **srm.conf**.

This file is installed by default in C:\Program Files\ Apache Group\Apache\conf.

2 Type the following lines at the end of the 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 are located near the bottom of the Start.htm file, inside the <object> tags.

Table 3-2 describes the configuration parameters.

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 have 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 on page 50.
3. Save and close the file.

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 51.

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 and close the file.

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 52.

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 and close the file.

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 msiexec.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 51.

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
4. Save and close the file.

Testing the installation on the Web server

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

If the installation fails, note any error messages that are displayed. Use the following guidelines to troubleshoot the problem:

- 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 package, users must have Internet Explorer 6.0 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/2000/2003 Server/XP must have administrator rights on their own computers and must be logged on with administrator rights.

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 the 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 You can create an installation package or custom product installation as a self-extracting .exe file or as 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 using SMS.
Package Definition File	An SMS-specific information file used by SMS to create and deploy SMS packages The default package definition file (PDF) that is supplied with pcAnywhere is named pcAnywhere.pdf

See "Deploying with SMS" on page 55.

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 later
- 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 be members of the same domain as the SMS distribution server, or have a trust relationship set up between the domains with appropriate permissions that allow 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.

For more information about SMS requirements and updates, visit the Microsoft Web site at the following URL:

//www.microsoft.com/sms

Deploying with SMS

An SMS deployment requires the following 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=UserLoggedOn
- AdminRightsRequired=TRUE

Creating an SMS deployment package

You must create an SMS Package and configure a distribution 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, and 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**.

Do not select This package does not contain any files.

7 Click **Browse** to locate the folder that contains the pcAnywhere package that you created with 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**, and then click **New > Distribution point**.

2 Select 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 installations must be created.

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.

To advertise the package

1 Right-click **Advertisements**, and 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:

- 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 then 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.

Using Windows NT/2000/2003 Server/XP logon scripts

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

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

Windows NT/2000/2003 Server/XP users must have local administrative rights on their computers to install the pcAnywhere package.

Setting up the Windows 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 Windows 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 Windows logon script

You can use the following sample logon script to deploy pcAnywhere packages to Windows NT/2000/2003 Server/XP clients. The script is a simple batch file that copies the pcAnywhere package to the workstation, launches the pcAnywhere package installation, and then cleans up the installation files when complete.

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

```
@echo off
setlocal


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


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


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


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


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


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


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


REM ***** Cleanup *****
del %Package%
CD ..
```

```
rd pcapkg
Net Use Z: /DELETE


:End
endlocal
```

Testing the Windows logon script

Test the completed script on one or two workstations before setting up the script for all users. Windows NT/2000/2003 Server/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. The following steps are required:

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

Windows NT/2000/2003 Server/XP users must have local administrative rights on their computers to install the pcAnywhere package.

Setting up the Novell NetWare 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.
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 NetWare 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 msiexec -i %Package%
IF %PkgType% == EXE %Package%


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


:End
endlocal
```

Testing the NetWare logon script

Test the completed script on one or two workstations before setting up the script for all users. Windows NT/2000/2003 Server/XP users must have local administrative rights on their computers to install the pcAnywhere package.

Chapter 4

Performing centralized management

This chapter includes the following topics:

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.

Symantec pcAnywhere supports integration with Microsoft Systems Management Server. It also supports centralized event logging using the SNMP monitor.

See "Integrating with Microsoft Systems Management Server" on page 71.

See "About centralized logging" on page 74.

Managing pcAnywhere hosts remotely

The pcAnywhere Host Administrator tool lets you remotely manage the hosts on your network. It 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 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/2000/2003 Server/XP.

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

To install the pcAnywhere 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 panel, click **Next**.
6. In the Program Maintenance panel, click **Modify**, and then click **Next**.
7. In the Custom Setup panel, under pcAnywhere Tools, click the down arrow next to Host Administrator, and then click **This feature will be installed on local hard drive**.
8. Click the down arrow next to Host Administrator Agent, and 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.
9. Click **Next**.
10. To include the program icon on the Windows desktop, select **pcAnywhere Host Administrator**.

11 Click **Install**.

12 Follow the on-screen instructions to continue the installation process. When the installation is complete, click **Finish**.

If your computer requires updates to system files, you will be prompted to restart your computer. The restart 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 2000/2003 Server/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**, and then type `mmc`

3 Click **OK**.

4 On the Console menu, click **Add/Remove Snap-in**.

5 In the Add/Remove Snap-in dialog box, on the Standalone tab, click **Add**.

6 In the Add Standalone Snap-in dialog box, click **pcAnywhere Host Administrator**.

7 Click **Add**.

8 Click **Close**.

9 In the Add/Remove Snap-in window, click **OK**.

Creating a configuration group

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

See "Adding computers to a configuration group" on page 66.

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**, and 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, and then click **Add Systems to Configuration Groups**.
3. In the Add Systems to Configuration Groups dialog box, 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 tool 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 tool 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, and 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, and 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, and 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, and then click **Rename**.

9 Type a name.

For example:

Admin

Configuring a host item in pcAnywhere Host Administrator

The pcAnywhere Host Administrator tool 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**, and 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 to Configuration Groups to expand it.

2 Under Configuration Groups, right-click the configuration group to which you want to send the files, and then click **Distribute pcAnywhere Files**.

3 In the Distribute pcAnywhere Files dialog box, 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, and 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 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.

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

To import the package definition file into SMS

1. Insert the Symantec pcAnywhere CD into the CD-ROM drive.
2. In the SMS Administrator console, in the left pane, right-click Packages, and 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 on the installation CD is as follows:

   \tools\SMS folder
4. Click **Open**.
5. In the Package Definition panel, click **Next**.
6. When you complete all of the steps in the wizard, click **Finish**.

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/2000/2003 Server/XP

To remotely configure and control pcAnywhere on Windows NT/2000/2003 Server/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, callers who do not have 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

- Do one of the following:
  - In Windows NT/2000/2003 Server/XP, open the \WinNT\System32 folder, and then run dcomcnfg.exe.
  - In Windows 98/Me, open the \Windows\System folder, and then run dcomcnfg.exe.

About AwShim

AwShim is the management component that bridges 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 as follows:

- 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 that 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 . You can then 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 that 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 75.

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

Chapter 5

Integrating pcAnywhere with directory services

This chapter includes the following topics:

About directory services

The directory services capability 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.

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. You can then select the host to which you want to connect from this list.

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. The configuration instruction depends on 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 that 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.

For example:

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, and 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 then click **Add** to include it in the Required Attributes list.

12 In the Available Attributes list, locate the pcaHostEntry attribute, and then 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**, and 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 the following procedures:

- 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 the following location:

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

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

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

5 Click **Next**.

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

All entries are case-sensitive.

7 Click **Next**.

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

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

10 Click **Next**.

11 Click **Finish**.

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 the following location:

   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 then 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 typed exactly.

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 lines for each user:

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

Changetype:modify

Add:objectclass

Objectclass:pcaHost
```

2. Save this file locally, and then copy it to the following location:

   sys:system\schema\

3. At the server prompt, type the following:

```
Load Bulkload.nlm
```

4. Click **Apply LDIF file**.
5. At the prompt, type the following 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, and 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, and then click **New > Group**.
3. Type a name for the group.
4. Right-click the group name, and 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, and 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 following 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**, and 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**, and then click **Operations Master**.
10. Select **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, and then click **Create Attribute** .

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

   This is case-sensitive.
4. In the LDAP Display Name field, type **pcaHostEntry**
5. In the Unique X500 Object ID field, type the following:

   `1.3.6.1.4.1.393.100.9.8.1`
6. In the syntax list, click **Octet string**.
7. Select **Multi-Valued**.
8. Click **OK**.
9. In the left pane, right-click the Classes folder, and 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.
2. In the LDAP Display Name field, type `pcaHost`
3. In the Unique X500 Object ID field, type the following:

   `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, next to the Optional attribute box, click **Add**.
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, and then click **Properties**.
3. Select the Relationship tab, and then next to the Auxiliary Classes box, click **Add**.
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 edit 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 that Advanced Features is selected.

   This enables the Security tab in the property pages.

   You can set the following rights at any organizational unit. You should set these rights at the level that contains the pcAnywhere users.
3. Right-click the organizational unit, and 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, select **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, select **Write**.
6. Click **Advanced**.
7. Select the Self group that you just added, and 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 this 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.

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.

Configure the directory server entries before beginning this procedure.

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, and then click **Properties**.

3 On the Settings tab, check **Use directory services**.

4 Select the appropriate directory server in the list.

The directory server that you select is used to register the host when it starts.

5 Click **OK**.

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. Configure the directory server entries before beginning this procedure.

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, and 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 wildcard characters in these fields. For example, A* returns entries that have a name beginning with the letter A.
6. Click **OK**.
7. On the Settings tab, click **OK**.

Chapter 6

Managing security in Symantec pcAnywhere

This chapter includes the following topics:

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 by implementing secure, remote access server (RAS) and Virtual Private Network (VPN) solutions in place of individual dial-up devices.

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

- Limit connections to specific computer names or IP addresses.
  See "Limiting connections to specific computer names or IP addresses" on page 92.
- Serialize pcAnywhere installations.
  Symantec pcAnywhere lets you create custom installation packages 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 27.

- Implement 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 93.
- Limit 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*.
- Limit the 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*.
- Prompt 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 the following URL:

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.x or later.

Using Microsoft Windows-based authentication types

Table 6-1 includes information about 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.
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, and then they can browse for user names.
NT (For Windows NT/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, and 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 includes information about 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.

Table 6-2 Novell-based authentication types *(continued)*

Novell-based authentication types	Explanation	Implementation in pcAnywhere
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, and then they can browse for user names.

Using Web-based authentication types

Table 6-3 includes information about 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.

Table 6-3 Web-based authentication types *(continued)*

Web-based authentication methods	Explanation	Implementation in pcAnywhere
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, and then they 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.

Table 6-4 includes information about the ways in which pcAnywhere can protect session security.

Table 6-4 Session security options

Option	Description
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. When connecting with a host or remote that is running pcAnywhere 11.0.x or earlier, either user can deny a connection if the other is using a lower level of encryption. If the connection is not denied, pcAnywhere automatically lowers the encryption of the computer with the higher encryption level to match the encryption of the computer with the lower encryption level. When both the host and remote are running pcAnywhere 11.5 or later, pcAnywhere automatically raises the encryption of the computer with the lower encryption level to match the encryption of the computer with the higher encryption level.

Table 6-4 Session security options *(continued)*

Option	Description
Logon encryption	Symantec pcAnywhere automatically secures logon information by using symmetric encryption to encrypt the user ID and password. Logon information might not be encrypted if either the host or remote uses a previous version of pcAnywhere that is not configured to use symmetric 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, cancelling the host, or using the mouse and keyboard.
Time limits for individual users or user groups	Protect the host from a malicious user's 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. You can do the following: ■ Cancel the host or continue to wait for connections. ■ Log off the host user. ■ Restart the host computer. ■ Lock the computer.

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

Maintaining audit trails

Event logging helps you monitor session activities and track information for auditing purposes. You can track who connected to a host and session duration, 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 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 2000/2003 Server/XP and operating system policy integration in Windows 98/Me/NT4.

Administrator rights are required to modify policy settings in Windows NT4/2000/2003 Server/XP.

Implementing Group Policy in Windows 2000/2003 Server/XP

You must use the Microsoft Management Console (MMC) Group Policy snap-in to administer group policy in Windows 2000/2003 Server/XP. To manage policy for a site, domain, or organizational unit, you should open Group Policy from Active Directory, and 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 100.

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 2000/2003 Server/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 100.

Importing the pcAnywhere administrative template

Symantec pcAnywhere provides administrative templates for Windows 2000/2003 Server/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. These settings 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 2000/2003 Server/XP

The pcAnywhere.adm file for Windows 2000/2003 Server/XP is located on the pcAnywhere CD in the Tools\Policy folder. You can copy this file to a secure location, and then import it into MMC. Before you import this file, ensure that you have added the Group Policy snap-in to MMC.

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

To import the pcAnywhere.adm file for Windows 2000/2003 Server/XP

1. On the Windows taskbar, click **Start > Run**, and then type the following:

   ```
   gpedit.msc
   ```

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, and 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, and 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, and then import it into the System Policy Editor. Ensure that you select the correct pcAnywhere.adm file.

Before you begin these procedures, ensure that you have configured the system policy for your operating system.

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

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**, and 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, and then click **Open**.

5 In the Policy Template Options window, click **OK**.

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 6-5 lists information about the policy settings that pcAnywhere lets you control.

Table 6-5 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
Actions\pcAnywhere Tools	Contains policy settings to prohibit users from using the following tools in pcAnywhere: ■ Package Deployment Tool ■ Host Administrator ■ 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

Table 6-5 Location of pcAnywhere policy settings *(continued)*

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

Managing user policies in Windows 2000/2003 Server/XP

To manage user policies in Windows 2000/2003 Server/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 100.

To manage user policies in Windows 2000/2003 Server/XP

1 On the Windows taskbar, click **Start > Run**, and then type the following:

```
gpedit.msc
```

2 In the console window, in the left pane, select the Group Policy object for which you want to set policies.

3 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.

4 Under User Configuration, click the plus sign next to Administrative Templates to expand the list.

5 Click the plus sign next to Symantec pcAnywhere to expand the list.

6 Open the folder that contains the policy settings that you want to edit.

See Table 6-5 on page 102.

7 In the right pane, under Policy, double-click the policy setting that you want to edit.

8 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

9 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 computers, 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 100.

To manage user policies in Windows 98/Me/NT4

1 To start the System Policy Editor, on the Windows taskbar, click **Start > Run**, and then type `poledit.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, expand a list by clicking the plus sign next to the policy type that you want to edit.

6 Select 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

Index

R

S

T

U

W