Symantec pcAnywhere™ Solution 12.6 SP2 User Guide

Symantec

Symantec pcAnywhere™ Solution 12.6 SP2 User Guide

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

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

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 features and functionality. The Technical Support group also creates 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 support 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
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

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

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

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/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as 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 assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

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

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

Contents

Chapter 1

Introducing pcA Solution

This chapter includes the following topics:

About pcAnywhere Solution

Symantec pcAnywhere Solution provides secure, remote access to computers and servers. This remote access lets you quickly resolve help desk and server support issues or stay productive while you work away from your office. You can use your desktop computer or laptop to work across multiple platforms, including the Windows OS, Linux OS, and Macintosh OS.

Connectivity features help facilitate connections through firewalls, routers, and other types of network address translation (NAT) devices. Robust security features help protect your computers and servers from unauthorized access.

You can use pcAnywhere Solution in the following ways:

Manage computers remotely	pcAnywhere Solution lets help desk providers and administrators troubleshoot and quickly resolve computer problems. You can remotely perform diagnostics, check and modify settings, and deploy and install software. See "Running a remote control session" on page 22.
Support and maintain servers	pcAnywhere Solution lets administrators connect to servers across their organizations to perform routine maintenance. It also helps administrators deploy and install software patches and upgrades, assess performance, and troubleshoot network problems. See "Starting a remote control session" on page 28.
Transfer files between computers	pcAnywhere Solution lets you connect to your home computer or office computer to quickly get the files that you need. You can perform automatic file transfers from one computer to another or exchange multimedia and other files that are too large to send by email. See "File transfer options" on page 39.
Work from a remote location	pcAnywhere Solution lets you remotely connect to another computer. You can then work as though you are sitting in front of that computer. You can view and edit files, run software, print files to a printer at your location or at the host's location, or give demonstrations. See "Remote control options" on page 33.

See "*Establishing remote connections*" on page 21.

See "Running a remote control session" on page 22.

See "Starting a remote control session" on page 28.

See "File transfer options" on page 39.

What's new in pcAnywhere Solution

- The initiation of remote control sessions on Mac OS X 10.5 and Mac OS X 10.6 computers even when a user is not logged on is now supported on pcAnywhere.

How the Symantec Management Platform works

Products that are designed to plug into the Symantec Management Platform are known as solutions. Multiple solutions that are installed as a unit are known as

suites. When you install a solution or suite, the platform is also installed if it is not already installed.

During the platform installation, each of the platform services is installed. These services include the Notification Server service. The services are installed on a single computer that is known as the Notification Server computer. This computer is the computer you access, through the Symantec Management Console, to perform your administration and your management work.

The Symantec Management Console is a browser-based console that can be accessed from the Notification Server computer or remotely. When you access the console remotely, the computer must be on the network, running Microsoft Internet Explorer, and have access to the Notification Server computer.

As part of the platform installation, you set up the Configuration Management Database (CMDB). The CMDB stores the data that the platform and your solutions collect. The CMDB is a Microsoft SQL Server database.

After the platform and solutions are installed, you need to do some configuration. If any of the solutions manage other computers (most solutions do), you must install the Symantec Management Agent on the computers to be managed. The agent facilitates communications between the managed computer and the platform and solutions. The agent also receives tasks from the platform and solutions, helps install software, and sends collected data from the managed computer to the platform. There is an agent for managing UNIX, Linux, and Mac OS computers and one for managing Windows computers.

As solutions and the agent collect data, the data is stored in the CMDB, where it can be used in numerous ways. The data is used to generate the reports that help you manage your network. The data can also be used to trigger the actions that help prevent or address issues automatically.

The data that is collected and the tasks that are performed depend on the solutions and suites you install. The platform lets you run a single solution or numerous solutions. Regardless of the number of solutions installed, they are all managed through the Symantec Management Console. A single console means there is no need to learn new interfaces as you add new solutions to your environment.

System requirements

The pcAnywhere Solution comprise of components that are supported on different operating systems.

The support matrix of the pcAnywhere Solution components against the different operating systems are as follows:

Table 1-1 Support matrix of components

Component	Windows	Macintosh	Linux
Client software (Host)	Supported	Supported	Supported
Console software (Remote)	Supported	-	-
Access Server	Supported **Note:** Access Server is not supprted on Windows Vista, Windows Server 2008, or Windows 7 operating systems.	-	-

The supported operating systems by pcAnywhere Solution, the pcAnywhere Solution plug-in that comprises of the agent and host, and the remote accessibility support are as follows:

Table 1-2 Operating system support matrix

Operating System	pcAnywhere Solution 12.6	pcAnywhere Agent/Host/Remote 12.6
Windows XP SP2	-	Supported
Windows XP SP3	-	Supported
Windows XP Tablet PC Edition 2005	-	Supported
Windows XP 64-bit	-	Supported
Windows XP 64-bit SP2	-	Supported
Windows Vista 32-bit	-	Supported
Windows Vista 32-bit SP1	-	Supported
Windows Vista 32-bit SP2	-	Supported

Table 1-2 Operating system support matrix *(continued)*

Operating System	pcAnywhere Solution 12.6	pcAnywhere Agent/Host/Remote 12.6
Windows Vista 64-bit	-	Supported
Windows Vista 64-bit SP1	-	Supported
Windows Vista 64-bit SP2	-	Supported
Windows Server 2003 32-bit	-	Supported
Windows Server 2003 64-bit	-	Supported
Windows Server 2003 SP1	-	Supported
Windows Server 2003 32-bit SP2	-	Supported
Windows Server 2003 64-bit SP2	-	Supported
Windows Server 2003 R2	-	Supported
Windows Server 2003 R2 SP1	-	Supported
Windows Server 2008 SP1	-	Supported
Windows Server 2008 SP1 64-bit (64EMT)	-	Supported
Windows Server 2008 SP2	-	Supported
Windows Server 2008 SP2 64-bit (64EMT)	-	Supported
Windows Server 2008 R2	Supported	Supported
Windows 7 32-bit	-	Supported

Table 1-2 Operating system support matrix *(continued)*

Operating System	pcAnywhere Solution 12.6	pcAnywhere Agent/Host/Remote 12.6
Windows 7 64-bit	-	Supported
Mac OS X (10.4) x86 / PPC	-	Supported on the pcAnywhere host component only
Mac OS X (10.5) x86 / PPC	-	Supported on the pcAnywhere host component only
Mac OS X (10.6)	-	Supported on the pcAnywhere host component only
Mac OS X Server (10.4) x86 / PPC	-	Supported on the pcAnywhere host component only
Mac OS X Server (10.5) x86 / PPC	-	Supported on the pcAnywhere host component only
Mac OS X Server (10.6)	-	Supported on the pcAnywhere host component only
RHEL 4 WS x86/x86_64	-	Supported on the pcAnywhere host component only
RHEL 4 ES x86/x86_64	-	Supported on the pcAnywhere host component only
RHEL 4 AS x86/x86_64	-	Supported on the pcAnywhere host component only
RHEL 5 x86/x86_64	-	-
RHEL 5 Server x86/x86_64	-	-
SLES 10 (x86/x86_64)	-	Supported on the pcAnywhere host component only
SLES 11 (x86/x86_64)	-	-
VMware ESX 3.01	-	-
VMware ESX 3.02	-	-
VMware ESX 3.5	-	-
VMware ESX 3i	-	-

Table 1-2 Operating system support matrix *(continued)*

Operating System	pcAnywhere Solution 12.6	pcAnywhere Agent/Host/Remote 12.6
VMware ESX Hyper-V	-	-
Solaris 9 Sparc	-	-
Solaris 10 Sparc	-	-
Solaris 10 x86	-	-
Solaris 10 x64	-	-

Role-based security

Role-based administration and security are provided on two levels with pcAnywhere Solution.

The administrator can decide which roles have access to pcAnywhere Solution by configuring those roles in the Symantec Management Console. You can choose which roles have the ability to launch remote control sessions.

The administrator who configures the remote control clients can choose which remote control privileges are available to specified Active Directory users or other users. These choices are made when the host authentication is configured. Scope-based administration is controlled through the Symantec Management Console.

See "Approve connection user states" on page 32.

See "Setting platform-specific configuration options" on page 26.

Settings on different platform

Several differences exist in how pcAnywhere Solution operates on the Windows, Linux, and Macintosh platforms. For example, the Windows platform uses a mirror driver.

For authentication on the Linux and the Macintosh platforms, you cannot have more than one caller at a time if the authentication type is pcAnywhere.

For the Linux and the Macintosh platforms, the Host window is always hidden from the user.

Table 1-3 Differences in platform settings

Settings	Windows	Linux	Macintosh
Connection	Requires the user to approve connections. Includes support for encryption. Supports a connection to a host that is behind a firewall and NAT devices. Customizes the host data port number.	Requires the user to approve connections. Includes support for encryption	Requires the user to approve connections. Includes support for encryption.
Authentication	pcAnywhere authentication. Native NT authentication. ADS authentication.	pcAnywhere authentication. PAM authentication.	pcAnywhere authentication. Open Directory authentication.
Security	Logs off host on connection. Restarts the host on disconnect. Hides the host tray icon. Locks out for offending systems. Tracks the maximum number of logon attempts. Includes a timeout setting. Supports the remote control mode.	NA	NA
Access Server	Docks to pcAnywhere Access Server. Connects to a specific group.	Docks to pcAnywhere Access Server. Connects to a specific group.	Docks to pcAnywhere Access Server. Connects to a specific group.

See "Setting platform-specific configuration options" on page 26.

Where to get more information

Use the following documentation resources to learn about and use this product.

Table 1-4 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues.	The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Release Notes**.
User Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. ■ The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Documentation**.
Help	Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: ■ The F1 key when the page is active. ■ The Context command, which is available in the Symantec Management Console on the **Help** menu.

In addition to the product documentation, you can use the following resources to learn about Symantec products.

Table 1-5 Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	http://www.symantec.com/business/theme.jsp?themeid=support-knowledgebase

Table 1-5 Symantec product information resources *(continued)*

Resource	Description	Location
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	http://www.symantec.com/connect/endpoint-management

Chapter 2

Establishing remote connections

This chapter includes the following topics:

Running a remote control session

You can use the pcAnywhere Solution to start a remote control session and choose the display options and communication options for the session.

During a remote control session, you can move or copy files to the remote computer. You can also decide the order for when different jobs and tasks complete.

Global configuration settings apply to all future remote control sessions.Symantec Management Agent should be installed on the managed machines to roll out pcAnywhere plug-in.

Table 2-1 Process for running a remote control session

Step	Action	Description
Step 1	Install the pcAnywhere plug-in on managed computers.	You can select the managed computers on which to install the pcAnywhere Solution plug-in. See "Installing the pcAnywhere plug-in from the managed computers" on page 24.
Step 2	Select the platform-specific configuration settings.	You can choose what options are applied to all host computers that are running on a specific platform. See "Setting platform-specific configuration options" on page 26.
Step 3	Start a remote control session.	You can select a computer in your network, connect to it, and start a remote control session with that computer. See "Starting a remote control session" on page 28.

Table 2-1 Process for running a remote control session *(continued)*

Step	Action	Description
Step 4	Choose the options that you want for the current session.	You can choose the options that let you decide how your remote control session is displayed. You can also choose how you communicate with the user of the remote computer. See "Approve connection user states" on page 32.
Step 5	(Optional) Perform a file transfer.	You can copy or move a file to and from the remote computer. See "File transfer options" on page 39.
Step 6	(Optional) Create a command queue.	You can order jobs and tasks by creating a command queue. See "Command queue options" on page 41.
Step 7	End the session.	You can end your remote control session. See "Ending a remote control session" on page 43.

See "Starting a remote control session" on page 28.

Services and Processes for pcAnywhere Solution plug-in Installation

Several services and processes are in running mode after the pcAnywhere Solution plug-in is installed.

Following are the processes that run Mac, linux and Windows computers after the installation of pcAnywhere plug-in.

Table 2-2 Process

Operating system	Name of the process
Mac	ThinHost process On installation of pcAnywhere plug-in on Mac Agent, the ThinHost and ThinHost Agent processes run in Activity monitor of Mac computer.

Table 2-2 Process *(continued)*

Operating system	Name of the process
Linux	ThinHost process On installation of pcAnywhere plug-in on Linux Agent, the ThinHost process run in the activity monitor of Linux computer.
Windows	Awhost32.exe process The AWHost32.exe process runs in Task Manager.

Following is the process that runs Windows computers after the installation of pcAnywhere plug-in:

Table 2-3 Service

Operating system	Name of the process
Windows	pcAnywhere has services that let you install host service. ■ Symantec pcAnywhere Host Service On installation of pcAnywhere plug-in on Windows agent, the Symantec pcAnywhere host Service gets installed. ■ pcAEvents.exe pcAEvents.exe runs in task manager

Installing the pcAnywhere plug-in from the managed computers

Several installation policies are defined for the Windows, Linux, and Macintosh operating sytems. These installation policies let you install the pcAnywhere Solution plug-in on the managed computers that you select. Do ensure that Symantec Management Agent is installed on the managed machines to roll out pcAnywhere plug-in.

You can also choose to use a pcAnywhere Plug-in package for each operating systems.

See "Running a remote control session" on page 22.

To install the plug-in on managed computers

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, expand the **Settings** > **Agents/Plug-ins** > **Remote Management** > **Remote Control** folders.
3. Expand the **Linux**, **Mac**, or **Windows** folder.
4. Click one of the policies or packages.
5. In the right pane, choose the options that you want.
6. Enable the 'ON'option
7. Click **Save Changes**.

Uninstalling the pcAnywhere plug-in from the managed computers

pcAnywhere has distinct uninstallation policies for the Linux, Windows, and Macintosh platforms.

These uninstallation policies let you uninstall the pcAnywhere Solution plug-in from the selected managed computers.

See "Running a remote control session" on page 22.

To uninstall the plug-in from managed computers

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, expand the **Settings** > **Agents/Plug-ins** >**Remote Management** > **Remote Control** folders.
3. Expand the **Linux**, **Mac**,or **Windows** folder.
4. Click one of the policies or packages.
5. In the right pane, choose either the **Target** or the **Computers** option.
6. Click **ON** on the right pane.
7. Click **Save Changes.**

See "Running a remote control session" on page 22.

Upgrading the pcAnywhere plug-in on the managed computers

You can upgrade the pcAnywhere plug-in policy through different policies defined for Windows, Linux, and Macintosh operating systems.

The upgrade policies help you upgrade the pcAnywhere Solution plug-in from the managed computers that you select.

You can also choose to use a pcAnywhere Plug-in package for each operating system.

To upgrade the plug-in on the managed computers

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings.**
2. In the left pane, expand the **Settings** > **Agents/Plug-ins** > **Remote Management** > **Remote Control** folders.
3. Choose the respective **Windows** or **Linux** or **Mac** pcAnywhere Plug-in - Upgrade package to upgrade the pcA plug-in.
4. Click one of the policies or packages.
5. In the right pane, choose the options from the**View** pane.
6. In the right pane,click **ON**.
7. Click **Save Changes.**

See "*Establishing remote connections*" on page ?.

Setting platform-specific configuration options

You can use Notification Server to create configuration policies for pcAnywhere Solution.

If the Notification Server administrator sends new configuration settings, the new settings are applied when the Altiris Agent is updated.

See "Settings on different platform" on page 17.

See "Running a remote control session" on page 22.

To set platform-specific configuration options

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, expand the **Settings** > **Agents/Plug-ins** > **Remote Management** > **Remote Control** folders.

3 Expand the **Linux**, **Mac**, or **Windows** folder.

4 Click the **pcAnywhere Settings** policy for your platform.

The corresponding **pcAnywhere Settings** page displays in the right pane.

5 In the right pane, choose from the following options (depending on the platform that you selected):

Tab	Options
Connection	Require user to approve connection. Sends a message to the host computer that requires the user to allow the remote control connection within the specific timeout number of seconds. Customized approval message. Lets you create a custom connection approval message. Use encryption. The host computer uses this option. If this box is checked, the encryption type is symmetric AES with 128-bit key length. Allow connections to hosts behind firewalls and NAT devices. Customize the host data port or use the default setting. If no entry is found in the database for the default value, it is read from the TCPIPDataPort value in the HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\pcAnywhereSolution registry entry.
Authentication	Select the authentication type (pcAnywhere, NT, Active Directory). The Macintosh platform includes pcAnywhere and Open Directory authentication. The Linux platform includes pcAnywhere and PAM authentication. For the Linux and the Macintosh platforms, the pcAnywhere authentication type supports only one caller at a time. The Windows platform supports multiple callers. Lists the active users or groups. Lets you add or remove users. Enable the Local Administrators group. Support the global NT users and the groups that are defined in local NT groups.

Tab	Options
Security (Windows only)	Log off host computer on connect. Restart host computer on disconnect. Hide host tray icon. Enable lockout for offending systems for the specified number of minutes. Maximum number of logon attempts. Timeout connection attempts after the specified number of minutes. Remote control mode: ■ **Full control**. Lets both users control the mouse and keyboard of the host computer. ■ **View only**. Lets the administrator observe a user's actions at the host computer. The administrator's keyboard and mouse are disabled in this view. ■ **Lock Host keyboard/mouse**. Locks the keyboard and mouse on the host computer. ■ **Blank Host screen**. Disables the view on the host computer. This functionality prevents the host user from using their keyboard and mouse.
Access Server	Dock to an Access Server with the specified name or IP address. Connect to a group with the specified name.

6 On the bottom bar, click the down arrow next to **Apply to**.

7 Select the option that you want.

8 In the top corner, click the drop-down menu next to the **Off** icon.

9 Click **On**.

10 Click **Save Changes**.

Starting a remote control session

Using pcAnywhere Solution, you can select a computer in your network and establish a remote control connection to that computer. pcAnywhere Solution also supports VNC and RDP connections.

See "About VNC and RDP connections" on page 30.

The host computer usually displays a message that prompts the user to approve the remote control session. This functionality can be changed in the configuration policies. After the session is established, the background color of the remote computer changes to blue to indicate that it is controlled. The desktop theme and background on the host computer are disabled during the session.

A yellow tray icon that has a picture of a computer on it also appears on the host computer. The lower left corner of the tray icon includes some green animation dots that continually flash if there is an active remote control session. Otherwise, the tray icon is a complete yellow circle without any animation. If you mouse over the tray icon during an active session, it displays the name of the computer that has control of that computer.

By right-clicking the tray icon, the host user can choose to end the session, start a chat session, access Help, and enable the pen option. Each of these options can be used during an active remote session. A remote user can access all of these functions from the left pane of a remote session window.

If the remote computer does not have pcAnywhere Solution installed on it, that computer displays a prompt. If you approve the prompt, an ActiveX component installs the pcAnywhere remote viewer.

See "Running a remote control session" on page 22.

To remotely control a computer

1. In the Symantec Management Console, on the **Actions** menu, click **Remote Mangement** > **Remote Control**.
2. On the **Remote Control** page, enter the computer name or the IP address for the computer that you want to control.

   You can click **Browse** to find a list of available computers. Then, you can select the computers that you want to control.

   For more information, view topics about selecting computers in the Symantec Management Platform Help.
3. From the **Connect Using** drop-down menu, select pcAnywhere.

   If you choose a connection method other than pcAnywhere Solution, you must ensure that the software for that method is installed and configured properly.
4. (Optional) Click **Advanced** to choose other options.

   See "Advanced options" on page 32.
5. Click **Connect**.

6 On the **Host Login** page, enter the credentials for the computer that you want to control.

If the authentication policy has not been applied to the host computer, the default authentication uses each computer's local administrators group account.

You can also choose to connect to a remote control session as a standard user or as a superuser

See "Approve connection user states" on page 32.

7 Click **OK**.

After you establish a connection, the **Session Manager** window appears on your computer. The navigation bar on the left of the window lets you switch modes. You can also perform the tasks that are related to the mode that you have selected and view details about the connection. The arrow icons let you expand and collapse each section in the navigation bar.

The right pane displays the host computer screen. If you are connected to multiple remote control sessions, the right pane also displays each of those sessions in a separate tab.

About VNC and RDP connections

pcAnywhere Solution supports VNC connections and RDP connections from its remote control Web pages. For the remote computers that are running Windows or Linux, you can choose to connect to host computers using either technology.

See "Connecting with VNC" on page 30.

See "Connecting with RDP" on page 31.

See "Starting a remote control session" on page 28.

Connecting with VNC

You can install Virtual Network Computing (VNC) on your remote computer and then use it to connect to a host computer. pcAnywhere Solution supports VNC connections from Windows and Linux remote computers.

You must install the VNC server to run on port 5800. pcAnywhere supports VNC connections only if the VNC server is running on port 5800.

By default, a VNC server listens for connections from a Web browser on TCP port 5800. If you point a Web browser to this port, the VNC server automatically provides a Java VNC viewer that runs in your Web browser. This Java Viewer

exchanges data with the VNC Server on the same ports that a normal VNC viewer uses.

See "About VNC and RDP connections" on page 30.

To connect with VNC

1. On the host computer, install a VNC server.
2. On the computer on which you want to access Symantec Management Console, install JRE 1.4.2 or later.
3. On the Symantec Management Console, on the **Actions** menu, click **Remote Control**.
4. Select **VNC** as the remote control method.
5. Connect to the host computer.

See "About VNC and RDP connections" on page 30.

Connecting with RDP

You can install Remote Desktop (RDP) on your remote computer and then use it to connect to a host computer. pcAnywhere Solution supports RDP connections.

See "About VNC and RDP connections" on page 30.

To connect with RDP

1. On the host computer, enable RDP using one of the following options:
   - For Vista and 2K8, right-click **My Computer** > **Properties** > **Remote Settings** > **Remote** tab, and then click **Allow connections from computers running any version of Remote Desktop**.
   - For XP, right-click **My Computer** > **Properties** > **Remote** tab, and then click **Allow users to connect remotely to this computer**.
   - For 2K3, right-click **My Computer** > **Properties** > **Remote** tab, and then click **Enable remote desktop on this computer**.
2. On the Symantec Management Console, on the **Actions** menu, click **Remote Control**.
3. Select **Microsoft Remote desktop** as the remote control method.
4. Connect to the host computer.

See "About VNC and RDP connections" on page 30.

Advanced options

You can choose the options that let you select the connection options for your remote control session.

See "Starting a remote control session" on page 28.

Table 2-4 Advanced options

Option	Description
Remote control	Click this option to start the session in remote control mode.
File transfer	Click this option to start the session in file transfer mode. See "File transfer options" on page 39.
Data port	Do not change the default setting. For the managed computers that have updated inventories, the data port setting is read from the CMDB. If the data port setting is not found, it is read from the registry entry. If the registry entry is not found, the setting defaults to 5631.
Use encryption	Click this box to use symmetric AES 128-bit encryption while you are connected.

See "Starting a remote control session" on page 28.

See "File transfer options" on page 39.

Approve connection user states

You can choose to connect to a remote control session as a standard user or as a superuser. When you connect as a standard user, the host machine can deny the connection.

When you connect as a superuser, the host machine is given only the option to approve the connection. If the host computer displays a login message, the remote control connection is established after the timeout period.

See "Starting a remote control session" on page 28.

Table 2-5 Approve connection user states

Machine state	Standard user	Superuser
Ctrl+Alt+Delete	Display message box with the ability for the host user to only accept the connection. After timeout, the connection is established.	Display message box with the ability for host user to only accept the connection. After timeout, the connection is established.
Machine locked	Display message box with the ability for the host user to only accept the connection. After timeout, the connection is established.	Display message box with the ability for the host user to only accept the connection. After timeout, the connection is established.
Logged in	Display message box with the ability for the host user to deny the connection. After timeout, the session is terminated.	Display message box with the ability for the host user to only accept the connection. After timeout, the connection is established.

See "Starting a remote control session" on page 28.

Remote control options

You can choose from the many options that let you change the display of your remote session. You can also choose how you communicate with the remote user during your session.

All of these options are available on the Windows platform.

The pcAnywhere product and the pcAnywhere Solution share the same agent and viewer. However, the **Power off** host and **Explore** shared devices options are disabled in the pcAnywhere Solution viewer. If you need to turn off, turn on, or reboot individual computers, use the Real-Time System Manager interface.

See "Running a remote control session" on page 22.

Table 2-6 Remote control options

Option	Mac/Linux platform	Description
Full Screen	No	Displays the host screen fully on the remote computer screen. This option is available only if both computers are set to the same resolution.
Screen Scaling	Yes	Sizes the host screen to fit in the display area of the Session Manager window. Use this option when the host computer uses a higher screen resolution than the remote computer.
View/Edit Online Options	No	Changes display settings during a remote control session. See "Changing online options" on page 35.
Start/Stop Session Recording	Yes	Records the remote session to a file to play back later. See "Recording a remote session" on page 37.
Take Snapshot	Yes	Saves a screen shot of the session to view later. See "Taking a snapshot" on page 38.
Send Ctrl+Alt+Del	No	Sends the Ctrl+Alt+Delete command to the host computer.
Restart Host Computer	No	Restarts the host computer.
Enable Pen	No	Lets you draw on your screen so that both computers can see your annotations, figures, and text. After the pen is enabled, both the host computer screen and the remote computer screen display a palette. A user at either computer can then select **Draw** on the palette to launch the pen application. Any other mouse clicks do not work while in the draw mode.

Table 2-6 Remote control options *(continued)*

Option	Mac/Linux platform	Description
Power Off Host Computer	No	Turns off the host computer. This option is available only when the remote session is established with the Superuser caller type.
Lock Host Keyboard and Mouse	No	Locks the keyboard and mouse on the host computer.
Lock Remote Keyboard and Mouse	No	Locks the keyboard and mouse on the remote computer.
Explore Shared Devices	No	Lets you examine any devices that both computers share. This option is supported only in the pcAnywhere boxed product.
Show chat	No	Displays a chat window. See "Starting a chat session" on page 39.

See "Changing online options" on page 35.

See "Starting a chat session" on page 39.

See "Taking a snapshot" on page 38.

See "Running a remote control session" on page 22.

Changing online options

You can change display settings or temporarily blank the host computer screen during a session.

Video quality and ColorScale options affect product performance, image resolution, and color depth. For high-bandwidth connections, you can adjust the video quality to increase performance. For low-bandwidth connections, you can adjust the color levels to increase performance. If a sharper display is more important to you than color, use the four colors setting. This setting changes the color to gray scale, but provides sharper resolution.

These changes affect only the current session.

See "Remote control options" on page 33.

To change display settings during a remote control session

1. In the **Session Manager** window, on the left navigation bar, under **Remote Control**, click **View/Edit Online Options**.
2. In the **Online Options** window, select from the following options:

Reduce host desktop to match remote	Synchronizes the resolution settings on the host computer to match the settings on the remote computer.
Host active window tracking	Automatically moves any active window that appears on the host computer screen to a visible part of the remote screen. For example, a dialog box that requires an action from you might appear out of the viewing area on your computer. Because you cannot see the message, you might think the session has locked. By checking this option, you ensure that such dialog messages appear in a visible part of your screen.
Display Revert and End Session buttons in full screen mode	When you operate in full-screen mode, this option places command icons in the top left corner of the remote control window. The command icons let you end the session or return to the two-paned window.
High bandwidth	Optimizes the performance for high-speed connections, such as LAN connections and cable modems. You can adjust the video quality settings. Move the slider to the left to increase performance. Move the slider to the right to increase video quality. A lower setting increases performance, but reduces the video quality. A higher setting increases the video quality, but reduces performance.
Low bandwidth	Optimizes the performance for low-speed connections, such as modems. You can adjust the ColorScale settings. When you lower the number of colors that are displayed, you increase performance. If a sharper display is more important to you than color, use the four colors setting.
Blank Host Screen	Prevents other users at the host site from viewing the session. This option is not available for virtual computers. This option is also not available if the computer was not restarted after the pcAnywhere agent was installed.

Automatically transfer host and remote clipboard content	Automatically transfers the text or graphics that are contained in the clipboard between the host and remote computers.
Multi Monitor	Lets you select the monitor that you want to view from the host computer. This option is enabled only if the host computer has multiple monitors. You can view multiple monitors on a host computer by using the following keyboard shortcuts: ■ Ctrl+m+0—View all monitors. ■ Ctrl+m+*n*—View a single monitor, where *n* is the number that corresponds with the monitor that you want to view.

3 Click **Apply**.

4 Click **OK**.

See "Remote control options" on page 33.

Recording a remote session

You can record a remote session at any point during the session. You can save the session in a new file or add the recording to the end of an existing file.

See "Playing a recorded session" on page 38.

See "Remote control options" on page 33.

To record a remote session

1 In the **Session Manager** window, in the left pane, under **Remote Control**, click **Start/Stop Session Recording**.

2 Complete one of the following options:

- To add the recording to the end of an existing file, select the `.rdc` file that you want to append.
- To create a new file, type the file name.

3 Click **Save**.

After this point, any actions that you perform on the host computer are recorded in the specified file.

4 When you are finished recording, click **Start/Stop Session Recording**.

Playing a recorded session

You can view a recorded session using pcAnywhere Manager. The recorded session file is in a proprietary format that can be viewed only from the computers that can physically access the Notification Server computer.

On the Windows platform, you can play back a session that you previously recorded.

See "Recording a remote session" on page 37.

To play back a recorded session

1. Launch the pcAnywhere Manager application.

   This 32-bit Windows application installs with the Symantec Management Console. It creates a Symantec pcAnywhere shortcut icon on your Windows desktop.
2. In the pcAnywhere Manager console, in the left pane, click **Go to Advanced View**.
3. Under the pcAnywhere Manager section, click **pcAnywhere Tools**.
4. In the right pane, click **Playback Sessions**.
5. Browse for and select the file that you want to play back.
6. Click **Open**.

See "Recording a remote session" on page 37.

Taking a snapshot

You can capture and save an image of the host computer screen during a session. You can capture and save multiple screen shots. Each screen shot must be saved in a separate file.

See "Remote control options" on page 33.

To take a snapshot

1. In the **Session Manager** window, on the left navigation bar, under **Remote Control**, click **Take Snapshot**.
2. In the **Take Snapshot** window, select one of the following:

Visible Display	Takes a snapshot of only the visible part of the host screen.
Entire Display	Takes a snapshot of the entire host screen.

3 Click **OK**.

4 In the **Select Save Screen File** window, select the location where you want to save the snapshot.

5 In the **File name** field, type a file name.

6 In the **Save as type** field, select jpg or bmp.

7 Click **Save**.

See "Remote control options" on page 33.

Starting a chat session

During a remote control session, the host and remote users can have a typed conversation in a chat window. Either the host or remote user can initiate a chat session. This feature is helpful for sending brief messages or instructions.

This option is located in the **Session Manager** options in the top left corner of your screen.

See "Remote control options" on page 33.

To chat online with the host user

1 In the **Session Manager** window, on the left navigation bar, under **Remote Control**, click **Show Chat**.

2 In the **Chat** window, in the lower pane, type your message.

3 Click **Send**.

Your messages and the other user's responses appear in the upper portion of the chat window.

4 (Optional) Check the **Always on top** option to keep the chat window in front of any other remote session activities.

5 Click **Save** to save your chat session.

See "Remote control options" on page 33.

File transfer options

You can copy and move files from either the host computer or the remote computer. You can also delete files, rename files, or check the properties of a file on either computer.

You can select files and folders by their dates, file type, or a wildcard.

File transfer supports writing to and from a computer using the computer name, IP address, or UNC path.

pcAnywhere Solution saves the last nine locations that you browsed to.

If you are connected to a Linux or a Macintosh host, the file transfer options do not work. These platforms do not support the file transfer options.

See "Edit preferences while in Command Queue or File Transfer mode" on page 42.

See "Running a remote control session" on page 22.

See "Advanced options" on page 32.

Table 2-7 File transfer options

Option	Description
Transfer =>	Moves the selected files from the remote computer to the host computer. You can browse through the directories of both computers to select the file to move and to choose where the file resides.
Transfer <=	Moves the selected files from the host computer to the remote computer.
Synchronize	Synchronizes the current directories that are selected for the host computer and the remote computer.
Clone =>	Copies the selected files from the remote computer to the host computer.
Clone <=	Copies the selected files from the host computer to the remote computer.
Compare Folders	Determines any differences in the selected directories.
Delete	Deletes the selected files.
Rename	Renames the selected file.
Properties	Lets you view the properties for the selected file.

See "Running a remote control session" on page 22.

See "Advanced options" on page 32.

Command queue options

You can create and order commands, such as copy, move, delete, create a folder, rename, synchronize, and run using these options.

The run command is the same as using the **Start** > **Run** option in Windows. Using it, you can connect to a drive, folder, document, or Web site. You can also perform generic commands, such as regedit.

See "Edit preferences while in Command Queue or File Transfer mode" on page 42.

Table 2-8 Command queue options

Option	Description
Pause Queue	Temporarily stops the command queue.
Restart Queue	Restarts the command queue.
Open Queue	Opens a command queue.
Save Queue As	Lets you specify where to save a command queue.
Cancel Command	Cancels the specified command in the command queue list from currently executing.
Remove Command	Deletes the specified command in the command queue list.
Move Command Up	Moves up the specified command in the command queue list. The commands execute in the order they are listed, top to bottom.
Move Command Down	Moves down the specified command in the command queue list.
Cancel All Commands	Cancels all of the commands that are currently in the command queue list from executing.
Remove All Commands	Deletes all of the commands that are currently in the command queue list.
Remove Completed Commands	Deletes all of the commands that have executed from the command queue list.
Generate Report	Runs a report.

See "Edit preferences while in Command Queue or File Transfer mode" on page 42.

See "Running a remote control session" on page 22.

Edit preferences while in Command Queue or File Transfer mode

The options in this window control the file handling options and the end-of-session options for command queue sessions and file transfer sessions.

See "Command queue options" on page 41.

See "File transfer options" on page 39.

You can choose from the following file handling options:

Table 2-9 File handling options

Option	Description
Use compression	Compresses the files during file transfer. Selecting this option can speed up the file transfer. You might want to use this option if you transfer a large, uncompressed text file.
Confirm deletion of read-only/system/hidden files	Prompts you to confirm the action before you delete specific types of files. Select this option only if you will be present to respond to the prompt.
Use SpeedSend	Compares the contents of files with duplicate file names in the source directory and the destination directory. This option transfers only the portions of the source file that differ.
Suppress error messages	Automatically skips over a file that cannot be processed. No error message is generated, so no user intervention is required. To find this tab, click the left arrow and the right arrow in the pcAnywhere Options window to scroll through the tabs.
If destination file exists	Lists the following overwrite options if a file with the same name exists in the destination folder: ■ Never overwrite. ■ Always overwrite. ■ Verify before overwriting. ■ Overwrite older files only. Select Verify before overwriting only if you will be present to respond to the prompt.

You can choose from the following end-of-session options:

Table 2-10 Session end options

Option	Description
After queue ends	Lists the following options for ending a session: ■ Remain connected ■ Disconnect ■ Disconnect and lock host computer ■ Disconnect and log off host computer ■ Restart host computer ■ Shut down host computer The lock computer option is available on Windows 2000, 2003 Server, XP, and Vista only. If the host computer is running Windows 98/Me, this command starts the Windows screen saver if one is configured on the host computer. For added security, the host user can password-protect the screen saver.
Generate report	Automatically creates a report that contains the commands that were executed during the session and their status. You can save the report in HTML (.html) or comma-separated values (.csv) format.
Prompt user	Notifies the user about the action that you are about to perform. Select the number of seconds that the user has to respond to the prompt. If the timeout period expires, the action is carried out automatically.
Allow user to cancel	Sends a confirmation prompt to the host user. This option is available only if you select **Prompt user**.
Message to display	Lets you type a message to send to the host user. This option is available only if you select **Prompt user**.
Close open programs without saving data	Closes any programs that are running. The user loses any unsaved data.

See "Command queue options" on page 41.

See "File transfer options" on page 39.

Ending a remote control session

Either the host or remote user can end a session. After a session ends, you return to the main Symantec Management Console window.

See "Running a remote control session" on page 22.

To end a remote control session

1. In the **Session Manager** window, on the left navigation bar, under **Session Manager**, click **End Session**.
2. In the confirmation window, click **Yes**.

   If you have permission to restart the host computer, you can choose whether the host should accept other connections. You can also cancel the host by restarting the computer.

See "Running a remote control session" on page 22.

Chapter 3

Generating reports

This chapter includes the following topics:

About pcAnywhere logs

pcAnywhere uses different logs and reports to help you troubleshoot any problems that you encounter. Log is an essential tool to know the summary of the event.

See “Viewing reports” on page ?.

A log report is a chronological listing of the session events that are contained in a pcAnywhere-generated log file. This information is useful for security and troubleshooting,The logs location and file names are listed below:

Linux

For Linux information is as following:

- Logs location-`/Opt/altiris/notification/SymantecpcAplugin/bin`
- Logs file name- `thinhostd.log`

Windows

For Windows, the information is as follows:

- Logs location- `C:\Program Data\Symantec pcASolutionLog`

- Log Files name- pcAHostInstall generates the following log files:
  pcAHostInstall
  pcAPluginAgentInstall
  pcASolInstaller-pcAClientInstallManager-TRACE

Mac

For Mac, the information is as follows:

- Logs location- /Opt/altiris/notification/SymantecpcAplugin/bin/thinhostd.log
- Log File name- thinhostd.log

About pcAnywhere reports

Notification Server automatically generates several standard reports on various pcAnywhere Solution details. These reports contain detailed information on the authentication process and connection processes. For example, some of the reports include the user name and IP address that attempted to initiate a remote control session.

If you have multiple sessions that are active, the pcAnywhere Solution reports might not reflect the current status of each session.

You can also create custom reports in Notification Server.

For more information, view topics about creating custom reports in the Symantec Management Platform user guide.

See "Viewing reports" on page 49.

See "Report actions" on page 48.

See "pcAnywhere events" on page 50.

Table 3-1 pcAnywhere Solution reports

Report	Changeable parameters	Description
pcAnywhere Connection Activity Audit	**Time Period** (in days) **Host Machine Name** **Connection Status** **Time\date** **Remote Machine (Console)** **User Name** **OS**	Provides a history of all of the connections to any managed hosts The report contains the host and remote computer names, IP addresses, and OS type. It also provides the user's name that started the remote session, and the date and time of each attempt. Time and date provides the login time and login date Remote Machine provides information about the Console on which the application is running User name requires the credentials of the user Displays the Operating Systems
pcAnywhere Host Security and Encryption	**Host Machine** (Target) **Authentication Type** **User\User Groups** **Encryption** **Approve Connect** **Notify on Connect** **OS**	Provides the information about the configuration settings for each computer Displays the credentials to authenticate the host computer User name requires the credentials of the user Specifies certificate information required for public key encryption Provides information whether or not the host machine is connected Notification whether or not the host machine is connected Displays the Operating Systems
pcAnywhere Hosts by Version	**Collection** **Host Machine** **pcAnywhere Host** **OS**	Provides the version information on the different pcAnywhere Solution hosts that are running in the current environment. The report contains the host and remote computer names, IP addresses, and OS type. It also provides the user's name that started the remote session, and the date and time of each attempt. Name of the host computer Displays the Operating Systems

Table 3-1 pcAnywhere Solution reports *(continued)*

Report	Changeable parameters	Description
pcAnywhere Session Activity Audit	**Time Period** (in days) **Host Machine** (Target) **Remote Machine(Console)** **Host Machine** **Time\Date** **Category** **Description**	Provides the information on the connections and remote tools activity that occurred over a specified period of time Displays the IP address and name of the console of the Remote machine Displays the Operating system and IP address of the Host machine User name requires the credentials of the user Time and date provides the login time and login date Provides information about the activity of the session Provides the description of the activity

See "Viewing reports" on page 49.

Report actions

You can perform different actions on each report.

See "About pcAnywhere reports" on page 46.

Table 3-2 Report actions

Action	Description
View	Look at the detailed information that is contained in each report. See "Viewing reports" on page 49.
Print	Print each report.
Refresh	Refresh each report and update it with the latest, current information.
Search in	Search in each report for specific values.
Save	Save the report as a Web part, spreadsheet, XML file, HTML file, or static filter. You can also choose the location where the report is saved.
Change the display format	Change how the details of each report are grouped.

Table 3-2 Report actions *(continued)*

Action	Description
Change the parameter values	Change the values for some parameters that are included in the report. See "Changing report parameters" on page 49.

Viewing reports

You can view the information that is available in the standard reports.

See "Report actions" on page 48.

See "About pcAnywhere reports" on page 46.

To view a report

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand the **Reports** > **Remote Management** > **Remote Control** folders.
3. Click the report that you want to view.

   The report opens in the right pane.

Changing report parameters

You can change some of values for the parameters that are included in the standard reports.

See "Report actions" on page 48.

See "About pcAnywhere reports" on page 46.

To change the parameters for a report

1. In the Symantec Management Console, on Reports menu, click **All Reports**.
2. In the left pane, expand the **Reports** > **Remote Management** > **Remote Control** folders.
3. Click the report that you want to change.
4. In the right pane, in the Parameters section, in the right corner, click the down arrow.

5 For each field that you want to change, enter the new value or select the new value from the drop-down list.

A percentage character (%) indicates to include all options.

6 In the Parameters section, in the right corner, click the Refresh symbol.

Your report is updated with the new values that you entered.

pcAnywhere events

pcAnywhere Solution captures information from many events.

This information is stored in an event log file that is named `AW.PL9`.

The file is stored on the agent machine in the following locations:

- XP, 2K, 2K3 platforms: `C:\Documents and Settings\All Users\Application Date\Symantec\pcAnywhere\`
- Vista, 2K8 platforms: `C:\ProgramData\Symantec\pcAnywhere\`

See "About pcAnywhere reports" on page 46.

Table 3-3 pcAnywhere events

Category	Description
Session	Status: **Remote Logged Off Session**
Session	Status: **Host Ended Session**
Host	Entry: `bhf` file path Device: [TCP/IP,Modem]
File Transfer	File name [source path] [destination path] File Operation [Sent/Received] File Termination Reason [Normal/Abnormal]
Login Failure	**Remote PC**: **Machine Name** **Remote User**: **Remote User Name**

Chapter 4

Managing Access Server

This chapter includes the following topics:

About Symantec pcAnywhere Access Server

Symantec pcAnywhere Access Server provides secure, centralized pcAnywhere connectivity for your organization. It facilitates the process of finding and connecting to multiple pcAnywhere host computers that are behind a firewall, router, or other NAT device.

The Access Server can discover any pcAnywhere host that is docked to it, regardless of network or physical location. You can set up host groups to logically arrange the hosts that dock to the Access Server (for example, by customer, organization, or department). You can connect through the Access Server to any platform that pcAnywhere supports, including the Windows, Linux, and Mac OS X platforms.

Each Access Server installation supports up 1,000 docked hosts and 30 concurrent remote sessions.

See "Installing Symantec pcAnywhere Access Server" on page 55.

How the Access Server works

The Access Server uses the registered pcAnywhere TCP/IP ports to support access by existing pcAnywhere remote and host computers. If necessary, you can configure the Access Server to use alternative ports.

See "Specifying the port numbers for the Access Server" on page 63.

A router or firewall can filter traffic to the Access Server. If this functionality occurs, you need to open the corresponding ports on the router or firewall to enable the incoming connections. For more information about mapping the ports on your device, see the documentation for the router or firewall.

When a pcAnywhere host docks, it registers its name and IP address with the Access Server. The host then waits for an incoming connection from a remote. When a host is docked, it is bound to the Access Server. The host can accept the connections that come through the Access Server only. Docked hosts are not included in the pcAnywhere host discovery lists.

Remote users must connect to the Access Server to view and connect to a docked host. To connect to a docked host, remote users first must connect to the Access Server. They can then browse the list of available hosts and select the one to which they want to connect.

A pcAnywhere remote computer can connect to a host through the Access Server. When that happens, the Access Server proxies all of the data that is exchanged between the host and remote computers. It also records statistics during the session. Either the host, the remote user, or the Access Server administrator can end a session. At the end of a session, the remote is disconnected. The host re-docks to the Access Server, unless the host is configured to cancel at the end of a session.

See "Docking a pcAnywhere host to the Access Server" on page 68.

See "Connecting to a host through the Access Server" on page 69.

About Access Server security

You must set up a user password for the Access Server when you install the product. You can change the password through the Access Server Manager. Symantec Management Console users must also supply user credentials to log on to the pcAnywhere host. The authentication process is handled through the caller properties that are configured on the pcAnywhere host. Symantec pcAnywhere uses symmetric encryption to encrypt the exchange of the logon credentials between the console and the host.

The Access Server is a bridge between the console computer and the host computer. It performs no data encryption or authentication. Both users set their own encryption levels and settings when they configure their connection item properties in pcAnywhere.

You can create host groups to control access to the Access Server. You can configure the Access Server to accept docking requests only from the hosts that are configured to join a group. These groups must already be configured on the Access Server. You can also control access by blocking console connections from specific IP addresses.

See “Blocking IP addresses from docking” on page 64.

See “Setting up host groups” on page 66.

About Access Server scalability

Each Access Server can support up to a maximum of 1,000 docked hosts.

Your license determines the maximum number of hosts that can dock to your Access Server at one time. This limit is set in the license file that you receive from Symantec. If you need to increase the number of docked hosts, you can obtain additional licenses from Symantec.

See “About hosts docked to the Access Server” on page 68.

What you can do with the Access Server

The Access Server lets you perform the following tasks:

- View details about the docked hosts and active sessions.
  See “Opening the Access Server Manager” on page 59.
- End a remote session that is running.
  See “Ending an active session” on page 60.
- Stop and restart the Access Server.
  See “Starting and stopping the Access Server” on page 60.
- Set up passwords to control user and administrator access to the Access Server.
  See “Setting a user password for the Access Server” on page 64.
  See “Setting a password for the Access Server Manager” on page 65.
- Protect the Access Server from unauthorized host connections.
  See “Blocking IP addresses from docking” on page 64.
- Set up password-protected groups to control and manage the docked hosts.
  See “Setting up host groups” on page 66.

Preparing for installation

Before you install the Access Server, you should do the following:

- Verify that the computer on which you want to install the Access Server meets the minimum system requirements.
  See “About system requirements of Access Server” on page 55.
- Ensure that you have the necessary license file.

See "About system requirements of Access Server" on page 55.

About system requirements of Access Server

Your computer must meet several system requirements before your install the Access Server.

See "Preparing for installation" on page 54.

Table 4-1 System requirements

Component	Minimum requirement
Operating system	Any of the following: Windows XP Professional x32/x64 Windows 2000 Server/Advanced Server Windows Server 2003/x64 AMD64/EM64T
Processor	800 MHz or faster (2 GHz recommended)
RAM	256 MB or more (2 GB recommended)
Hard disk space	20 MB
Drives	CD-ROM or DVD-ROM
Network	TCP/IP network connection
Software	Internet Explorer 6 SP1 or later

See "Preparing for installation" on page 54.

Installing Symantec pcAnywhere Access Server

Symantec pcAnywhere Access Server requires a license to run. After the installation process is complete, you are prompted to import your license file. This step is not required. However, the license file must be imported for the Access Server service to run.

The Access Server service starts automatically after you install the Access Server and import a valid license file. The Access Server icon appears in the system tray.

See "Uninstalling Symantec pcAnywhere Access Server" on page 58.

To install Symantec pcAnywhere Access Server

1. Insert the Symantec pcAnywhere Access Server CD into the CD-ROM drive.
2. In the installation window, click **Install Symantec pcAnywhere Access Server**.
3. In the **Welcome** panel, click **Next**.
4. In the **License Agreement** panel, read and accept the terms of the license agreement, and then click **Next**.
5. In the **Destination Folder** panel, do one of the following:
   - To install Symantec pcAnywhere Access Server in the default folder, click **Next**.
   - To change the installation folder, click **Change**.
     In the **Change Current Destination Folder** panel, browse to the folder location in which you want to install the Access Server, and then click **OK**. Then, in the **Change Current Destination Folder** panel, click **Next**.
6. In the **Access Server Security** panel, in the **Password and Confirm Password** boxes, type the Access Server user password.

   This password is required to dock a host to the Access Server. It is also required to remotely connect to the Access Server to access the docked hosts.
7. Click **Next**.
8. In the **Ready to Install the Program** panel, if you do not want to place a shortcut on your desktop, uncheck **Symantec pcAnywhere Access Server**.

   This shortcut opens the Access Server Manager, which lets you configure the Access Server, manage docked hosts, and monitor active pcAnywhere sessions.
9. Click **Install**.
10. In the **Installation Completed** panel, click **Finish**.

    If a valid license file is not found on your computer, you are prompted to import one.

    See "Importing a license file through the Access Server Manager" on page 57.
11. Do one of the following:
    - If you have a license file available, click **Yes**.
      In the **Open** dialog, select the license file (`.slf`) that you want to import, and then click **Open**.
    - If you do not have a license file available, click **No**.
      You need to obtain a license file and import it through the Access Server Manager. You cannot run the Access Server service until you have imported a license file.

See "Uninstalling Symantec pcAnywhere Access Server" on page 58.

See "Importing a license file through the Access Server Manager" on page 57.

Post-installation tasks

After you install Symantec pcAnywhere Access Server, you might need to do the following:

- Configure the Access Server to meet the requirements of your organization.
  You can specify the ports to use and the subnets and IP addresses that you want to block from docking. You can also specify the host groups that you want to use to manage docked hosts.
  See "Configuring the Access Server" on page 61.
- Set up your hosts to dock to the Access Server.
  You can configure hosts to dock to a particular host group on the Access Server. You use Symantec pcAnywhere to configure the hosts.
  See "Docking a pcAnywhere host to the Access Server" on page 68.
- Manually specify the name of your Access Server or IP address.

See "Configuring the Access Server" on page 61.

See "Docking a pcAnywhere host to the Access Server" on page 68.

Importing a license file through the Access Server Manager

You must import a license file to run the Access Server service. If you installed the Access Server without importing a license file, you can import the license file through the Access Server Manager.

See "Installing Symantec pcAnywhere Access Server" on page 55.

See "About managing the Access Server" on page 58.

To import a license file through the Access Server Manager

1. Open the Access Server Manager.
2. In the pcAnywhere Access Server window, on the **Help** menu, click **About pcAnywhere Access Server**.

3 In the Symantec pcAnywhere Access Server window, click **Import License**.

The Host License Count shows the number of hosts that can dock to the Access Server. The license files that are currently stored on your computer determine this number.

4 In the **Open** dialog, select the license file (`.slf`) that you want to import, and then click **Open**.

5 Click **OK**.

Uninstalling Symantec pcAnywhere Access Server

You can uninstall Symantec pcAnywhere Access Server through the Windows Control Panel. The removal process removes the program files and registry key settings for the Access Server. It does not remove your Access Server license files. If you reinstall the Access Server on the same computer, the same license files are reused automatically.

See "Installing Symantec pcAnywhere Access Server" on page 55.

To uninstall Symantec pcAnywhere Access Server

1 In the Windows Control Panel, click **Add or Remove Programs**.

2 In the **Add or Remove Programs** window, click **Symantec pcAnywhere Access Server**.

3 Click **Remove**.

4 In the confirmation dialog, click **Yes**.

See "Installing Symantec pcAnywhere Access Server" on page 55.

About managing the Access Server

You can perform the following management tasks:

- Start and stop the Access Server.
  See "Starting and stopping the Access Server" on page 60.
- View the list of docked hosts, and undock a host when necessary.
  See "Undocking a host" on page 59.
- View details about all active sessions, and end a session when necessary.
  See "Ending an active session" on page 60.
- Import a license file.
- Configure the Access Server.

See "Configuring the Access Server" on page 61.

- Set up host groups to control and manage the hosts that dock to the Access Server.

Opening the Access Server Manager

The Access Server Manager lets you start and stop the Access Server. You can also view the status of the docked hosts and active sessions and configure the Access Server. The Access Server Manager can be password-protected. You need to supply the password to open the Access Server Manager.

See "What you can do with the Access Server" on page 54.

The Access Server Manager runs independently of the Access Server service. Opening and closing the Access Server Manager does not affect the host computers that are docked or the active sessions.

You can use the Access Server Manager to view the host groups that have been set up. You can also see the status of each docked host. The Access Server Manager also displays details about the active sessions. You can see the session duration and the amount of data that has been transferred between the console and host.

The Access Server Manager window is refreshed automatically, but there can be delays. You can manually refresh the window to ensure that you see the most current information.

To open the Access Server Manager

1. On the **Start** menu, click **Programs** > **Symantec** > **Symantec pcAnywhere Access Server** > **pcAnywhere Access Server**.
2. If necessary, in the Symantec pcAnywhere Access Server dialog box, type the password for the Access Server Manager, and then click **OK**.

Undocking a host

You can undock a host from the Access Server. When you undock a host from the Access Server, the host does not attempt to reconnect automatically. To re-establish a connection with the Access Server, the host user must manually dock to the Access Server again.

For example, if you reach the maximum number of docked hosts that your license allows, you can use this feature to temporarily manage connections. You can undock a host that is less critical to allow a more critical host to dock.

For security purposes, you can undock a host that appears to be unauthorized. You can then add the IP address to the host blocking list to prevent the host from re-docking.

See "About managing the Access Server" on page 58.

To undock a host

1. In the Access Server Manager, select the host that you want to undock.
2. In the left navigation pane, under **Actions**, click **Undock Host**.
3. In the confirmation dialog, click **Yes**.

Ending an active session

You can end a remote session that is running. Ending an active session does not affect the other active sessions that are running through the Access Server. When an active session is ended, the host automatically docks again to the Access Server.

See "What you can do with the Access Server" on page 54.

See "About managing the Access Server" on page 58.

To end an active session

1. In the Access Server Manager, select the host session that you want to end.
2. In the left navigation pane, under **Actions**, click **End Session**.
3. In the confirmation dialog, click **Yes**.

Starting and stopping the Access Server

You can manually stop the Access Server if you want to prevent it from accepting connections at a particular time. Stopping the Access Server ends all connections and releases all of the docked hosts.

For example, if the Access Server becomes unstable for any reason, you can try to manually stop and restart the service to regain stability.

If you change a configuration setting for the Access Server, you must stop and restart the Access Server for the changes to take effect.

See "What you can do with the Access Server" on page 54.

See "About managing the Access Server" on page 58.

To start the Access Server

- In the Access Server Manager, in the left navigation pane, under **Actions**, click **Start Server**.

  This option is available only if the Access Server is not running.

To stop the Access Server

1. In the Access Server Manager, in the left navigation pane, under **Actions**, click **Stop Server**.

   This option is available only if the Access Server is running.

2. In the confirmation dialog box, click **OK**.

Configuring the Access Server

When you install the Access Server, you need to specify some of the configuration options during the installation process. You can change these configuration settings.

See "Post-installation tasks" on page 57.

See "About managing the Access Server" on page 58.

Table 4-2 Access Server settings

Tab name	Description
General	Lets you specify a name for the Access Server and set the launch options.
Connectivity	Lets you select custom ports, if necessary, and change the modem configuration settings. You can also specify any IP addresses or subnets that you want to prevent from docking to the Access Server.
Security	Lets you set the Access Server security options. You can change the user password and set an administrator password to control access to the Access Server configuration settings. You can hide the Access Server from TCP/IP searches to prevent it from being displayed in the host list in the Symantec Management Console. You can also specify where to log Access Server events.
Groups	Lets you set up and maintain host groups to control access to the Access Server and simplify the management of docked hosts.

If you change a configuration setting for the Access Server, you must stop and restart the Access Server for the changes to take effect.

To configure the Access Server

1. In the Access Server Manager, on the **Edit** menu, click **Preferences**.
2. In the **Preferences** window, select a tab and make the appropriate configuration changes.
3. When you are finished, click **OK** to close the **Preferences** window.

Naming the Access Server

Symantec pcAnywhere Access Server automatically uses the name of the computer on which it is installed. The Access Server name is the display name of the Access Server. You can use a custom name to make it easier for users to find the Access Server.

See "Configuring the Access Server" on page 61.

Note: Changing the Access Server name does not affect the computer name.

To name the Access Server

1. In the **Preferences** window, on the **General** tab, under **Access Server Name**, select one of the following:

User Defined	The Access Server uses the name that you specify.
Use Computer Name	The Access Server uses the computer name that is defined in Windows.

2. If you select **User Defined**, in the adjacent box, type the name that you want to use.

   You can use a maximum of 24 characters.
3. Click **Apply**.

Setting the launch options for the Access Server

The Access Server launches automatically when Windows starts, and the Access Server program icon appears in the Windows system tray. The Access Server program icon indicates whether the server is running or stopped.

See "Configuring the Access Server" on page 61.

To set the launch options for the Access Server

1 In the **Preferences** window, on the **General** tab, select any of the following:

Launch with Windows	The Access Server starts automatically when you start Windows.
Display Access Server icon in taskbar	The Access Server icon is displayed in the Windows system tray.

2 Click **Apply**.

Specifying the port numbers for the Access Server

Symantec pcAnywhere and the Access Server are configured to use ports 5631 (TCP Data port) and 5632 (UDP Status port) by default. To dock to the Access Server, the port settings on the host and the Access Server must match. You can change the port settings on the Access Server. However, host users who want to dock to the Access Server must change their port settings to match. If you want to connect through the Access Server, you must also change your port numbers to match.

You can run a pcAnywhere host on the Access Server computer. However, the port numbers for the pcAnywhere host must be unique to avoid a port conflict. When you start the pcAnywhere host on the Access Server computer, it does not dock to the Access Server. Instead, it waits for an incoming connection from the Symantec Management Console. The management console must be configured to use the same port numbers as the host.

See "How the Access Server works" on page 52.

See "Configuring the Access Server" on page 61.

To specify the port numbers for the Access Server

1 In the **Preferences** window, on the **Connectivity** tab, click **TCP/IP Settings**.

2 In the **Port Settings** window, in the **Data port** and **Status port** boxes, type the port numbers that you want to use.

3 If you want to restore the default setting for a port, click **Reset Default** next to the appropriate box.

4 Click **OK**.

5 Click **Apply**.

Blocking IP addresses from docking

The Access Server lets a host dock from any network address. If necessary, you can specify the subnets or IP addresses that you want to prevent from docking to the Access Server.

For security purposes, you can undock a host that appears to be unauthorized. You can then add the IP address to the host blocking list to prevent the host from re-docking.

See "About Access Server security" on page 53.

See "What you can do with the Access Server" on page 54.

See "Configuring the Access Server" on page 61.

To block IP addresses from docking

1. In the **Preferences** window, on the **Connectivity** tab, under **Prevent the following IP address or subnets from docking**, do either one of the following:
   - To add a new subnet or IP address, type the subnet mask or IP address, and then click **Add**.
   - To remove a subnet or IP address, select it, and then click **Remove**.
2. Click **Apply**.

Setting a user password for the Access Server

You can set a user password to control connections to the Access Server. Host users must supply the password to dock to the Access Server. You must supply the password to connect to a docked host through the Access Server. You set the user password during the installation process. You can change it when necessary to maintain security.

You can configure the host or Symantec Management Console to automatically supply the user password to connect to the Access Server.

See "What you can do with the Access Server" on page 54.

See "Docking a pcAnywhere host to the Access Server" on page 68.

See "Configuring the Access Server" on page 61.

To set a user password for the Access Server

1. In the **Preferences** window, on the **Security** tab, under **Enter password for Access Server connections**, in the **Password** box, type the password.
2. In the Confirm password box, type the password again.
3. Click **Apply**.

Setting a password for the Access Server Manager

You can set a password for the Access Server Manager to control access to connection information and configuration settings. When this password is set, you must supply the password to open the Access Server Manager.

See "What you can do with the Access Server" on page 54.

See "Configuring the Access Server" on page 61.

To set a password for the Access Server Manager

1. In the **Preferences** window, on the **Security** tab, check **Require a password to open the Access Server Manager**.
2. In the Password box, type the password.
3. In the Confirm password box, type the password again.
4. Click **Apply**.

Logging Access Server events

You can log Access Server events to the Windows Event Viewer. You can view the event log to review the operation of the Access Server, and then make any necessary configuration changes. For example, you can view the log to determine the number of hosts that were blocked from docking because the maximum limit had been reached. If you notice a significant number of these events, you may want to upgrade your license to increase the number of hosts.

You can log events to the Access Server computer. You can also log events to another computer to which you have access. For example, you can log Access Server events to a secure, central computer.

The following events are logged:

- The Access Server started.
- A host connection to the Access Server was blocked because the maximum number of docked hosts was reached.
  Your license agreement determines the maximum number of docked hosts.

- A remote user failed to supply the correct Access Server password in three attempts.
- The Access Server stopped.

See "Configuring the Access Server" on page 61.

To log Access Server events to the local computer

1. In the **Preferences** window, on the **Security** tab, under **Logging Options**, check **Enable logging to the Windows Event Viewer**.
2. Check **Log to the Event Viewer on this computer**.
3. Click **Apply**.

To log Access Server events to another computer

1. In the **Preferences** window, on the **Security** tab, under **Logging Options**, check **Enable logging to the Windows Event Viewer**.
2. Check **Log to the Event Viewer on another computer**.
3. In the text box, type the computer name.

   You must use UNC syntax.
4. Click **Advanced**.
5. In the User name box, type the user name.
6. In the Password box, type the password.
7. In the Domain box, type the domain name.
8. Click **OK**.
9. Click **Apply**.

Setting up host groups

You can set up host groups to control access to the Access Server and to simplify management of the hosts that are docked. When remote users connect to the **Access Server through the host** list, they can view the groups of docked hosts and select the host they want to connect to.

You can hide individual host groups from TCP/IP searches to protect the hosts from unauthorized access. Remote users must provide the group name to connect to any of the docked hosts that are contained in the group.

You can configure the Access Server to require the host computers to dock to a specific host group. Host users must supply a valid group name and the appropriate password to dock to the Access Server.

You can choose not to require host computers to dock to a group. Any hosts that do not specify a group name or password are assigned to the Default group.

You can set a password for the host group. The host user must supply the password to dock to the group. The group password does not apply to remote connections. Remote users only need to supply the group name to access the docked hosts that are contained in the group.

See "About Access Server security" on page 53.

See "What you can do with the Access Server" on page 54.

See "About managing the Access Server" on page 58.

See "Configuring the Access Server" on page 61.

To set up host groups

1. In the **Preferences** window, on the **Groups** tab, do either of the following:
   - To add a new group, click **Add**.
   - To modify a group, in the **Groups** list, select the group that you want to modify, and then click **Modify**.
2. In the **Group Properties** window, in the **Name** box, type the name that you want to give the group.

   All group names must be unique.
3. If you want to assign a password to the group, in the **Password** box, type the password.
4. In the **Confirm Password** box, type the password again.
5. If you want to prevent the group from being displayed in the host list when a remote user connects to the Access Server, uncheck **Display this group in TCP/IP search results**.
6. Click **OK**.
7. If you want to require hosts to dock to a specific group, check **Require hosts to dock to a group**.

   If you select this option, the Access Server blocks docking attempts from a host that is not configured to join a group.
8. Click **Apply**.

About hosts docked to the Access Server

When a pcAnywhere host docks to the Access Server, it connects to the Access Server and waits for connections. The host can accept only the remote connections that come through the Access Server.

To dock to the Access Server, the host computer must be running pcAnywhere Solution 12.5.

If a host computer is configured to dock to an Access Server, it automatically docks when Windows starts.

See "Docking a pcAnywhere host to the Access Server" on page 68.

Docking a pcAnywhere host to the Access Server

When a host is configured to use the Access Server, it automatically docks to the Access Server when the host is launched. The host usually re-docks to the Access Server at the end of a session. However, you can configure the host to cancel at the end of a session. After the Access Server service is restarted, the host also automatically re-docks when it goes back into a waiting state.

If you have set up host groups on the Access Server, the host user must supply a group name and password. Host users can configure the pcAnywhere host to automatically dock to the assigned group.

See "How the Access Server works" on page 52.

See "Post-installation tasks" on page 57.

See "About hosts docked to the Access Server" on page 68.

To dock a pcAnywhere host to the Access Server

1. In the Symantec Management Console, in the **Settings** menu, click **All Settings**.
2. In the left pane, expand the **Settings** > **Remote Management** > **pcAnywhere** folders.
3. Click the **pcAnywhere Settings** policy for your platform.
4. In the right pane, click the **Access Server** tab.
5. Check **Dock to pcAnywhere Access Server**.
6. Enter the credentials for the Access Server.

7 (Optional) If you want to also connect directly to a group on the Access Server, check **Connect to a group**.

If you don't select a group, the host connects as a member of the default group on the Access Server.

8 (Optional) Enter the credentials for the group.

9 In the upper right corner, ensure that the policy is **On**.

10 Click **Save changes**.

Connecting to a host through the Access Server

Before you connect to a host through an Access Server, those hosts must be configured to be docked to the Access Server.

A single host can be configured to dock to the Access Server or a direct TCP/IP standard connection. You cannot configure a specific host to simultaneously dock to both an Access Server and a TCP/IP connection. If you want to change this functionality, you must distribute an updated policy.

pcAnywhere Solution Host can be sucessfully docked to the Access Server with a 24character or longer FQDN.

Each instance of an Access Server installation can support up to 1,000 docked hosts and 30 concurrent remote control sessions. pcAnywhere Solution Host can be sucessfully docked to the Access Server with a 24character or longer FQDN. The limit on the Access Server FQDN length was increased from 24 characters to 32 characters.

See "How the Access Server works" on page 52.

See "Manually connecting to a host computer" on page 70.

To connect to a host through the Access Server

1 In the Symantec Management Console, in the **Actions** menu, click **Remote Control**.

2 In the **Computer** box, enter the computer name or IP address of the Access Server that your host is docked to.

3 Click **Connect**.

4 Provide the appropriate credentials for the Access Server.

5 Click **OK**.

6 From the list, select the group that your host computer is docked to.

7 Select the computer that you want to connect to.

8 Click **OK**.

9 Enter the credentials for the host computer.

10 Click **OK**.

Manually connecting to a host computer

You can view the docked host computers and then start a pcAnywhere session with a selected host computer.

See "Connecting to a host through the Access Server" on page 69.

To manually connect to a host computer

1 In the Symantec Management Console, on the **Actions** menu, click **Remote Management** > **Remote Control**.

2 Type the Access Server name or IP address.

3 Click **Connect**.

4 In the **pcAnywhere Access Server Authentication** dialog box, type the Access Server user password.

5 Click **OK**.

6 From the list, select the group that your host computer is docked to.

7 Select the computer that you want to connect to.

8 Click **OK**.

9 Enter the credentials for the host computer.

10 Click **OK**.

11 Click **OK**.

Index