RemotelyAnywhere User Guide

March 2009

PUBLISHED BY

LogMeIn, Inc.
500 Unicorn Park Drive
Woburn, MA 01801

Table of Contents

What is RemotelyAnywhere?

RemotelyAnywhere is a remote administration tool that lets you control and administer Microsoft® Windows®-based computers over a local area network or the Internet. Originally designed for network administrators by network administrators, RemotelyAnywhere has since evolved to offer a wide variety of remote computing solutions for an equally wide variety of users. Today, RemotelyAnywhere provides such useful capabilities as Java-based desktop remote control, file transfer protocol (FTP) for downloading and uploading of files, configuration of the Host, remote-to-local printing, advanced scripting, and dozens of other features fully detailed in the rest of this manual.

RemotelyAnywhere acts as the host software on the machine that is to be controlled or accessed. The client requires no special software. The client software is any Java- or ActiveX-enabled web browser, such as Internet Explorer (IE). Many RemotelyAnywhere features can also be accessed and controlled using such client software as that found in handheld PDAs.

RemotelyAnywhere allows secure remote access to and administration of any machine on which it is installed. No special client software is required on your local machine and it is closely integrated with Windows NT/2000/XP security.

Minimize Downtime RemotelyAnywhere helps system administrators keep IT systems up and computer users happy by offering the industry's richest remote-support toolkit. Support staff can often detect, diagnose, and solve problems faster than local support using built-in operating system functions. Background access means the user need not be interrupted during the implementation of solutions.

Deliver the Solution, Not the Person All RemotelyAnywhere's features can be accessed securely and from any Web browser. Support and diagnostics can even be delivered from a PDA or WAP-phone browser. This means you can now offer genuine global support from anywhere, anytime.

Stop Fighting Fires RemotelyAnywhere brings predictability to system management. By giving you monitoring, scripting, and alerts, RemotelyAnywhere allows you to detect potential problems on all your systems before they bring a halt to business. This ensures that you are often the first to know about workstation issues, ranging from attempted security breaches to unstable software installations.

Fast, Simple, Secure Enterprise Deployment RemotelyAnywhere was designed for professionals responsible for large installations of workstations. The product is simple to install and configure on systems of anywhere between a handful and thousands of computers. Five levels of security and built-in event logging give you the confidence that your systems are safe.

Keep Your Company Productive Less downtime means more productivity. What's more, RemotelyAnywhere can dramatically reduce IT operating costs for a surprisingly low price. Contact LogMeIn and download a free trial of our enterprise version enabling you to see these productivity gains for yourself.

Key Features

- Secure Remote Control
- Support Toolset
- Automatic Alerts
- File Transfer
- Disk Mapping
- Folder Synchronization

- Remote-to-local printing
- Remote Deployment
- Accessible via Web Browser
- Enterprise Deployment
- Robust Security
- Centralized Logging
- Port Forwarding (Server Edition Only)
- Supports OpenSSH 5.1
- Supports OpenSLL 0.9.8h

Remote Control

- Complete remote control of keyboard, mouse and monitor
- Can also provide work-from-home and on-the-road access to workstations
- Dynamic resizing of desktop and adjustment of color depth
- File Transfer with delta-file updates
- Host-to-Client printing
- Automatic folder synchronization
- Compression algorithms adapts to bandwidth

Security

- Standards-compliant SSH server
- All events including unauthenticated connection attempts are logged to a central syslog server
- IP lockout of machines with a configurable number of unsuccessful logon attempts
- Security alerts and notification sent to IT managers
- Integrated Windows authentication
- RSA support

Anywhere Access

- RemotelyAnywhere can be accessed without client software
- Remote Control can be accessed using any Java or ActiveX-enabled Web Browser
- All diagnostic and administrative toolset features are presented using simple HTML interfaces
- Fully customizable interfaces support standard, light, and handheld browsers

Easy Enterprise-Wide Deployment

- Network console simplifies workstation management and remote installation
- Standard application installation
- Command line installation

- Scripted mass-deployment support
- Background installation

Support Toolset

- Background access does not interfere with computer users
- Real-time performance, connection, hardware and registry information
- Process manager with detailed info on CPU, memory, registry key and DLL usage
- Service manager with service account and dependencies
- Driver manager with dependencies
- Comprehensive user manager
- Share manager, including admin shares
- Full registry editor with ACL support
- Virtual memory settings
- Resource availability
- Emergency reboot
- Environment variables settings

Reporting and Alerts

- Catch problems before they interrupt work
- Real-time performance, resource, security, and event monitoring
- Script-defined alerts and warnings
- Powerful and flexible scripting language
- Automatic start of recovery procedures
- Alerts can be sent online, by email, or by text messages

Help Desk and Support

- Client keyboard and mouse can be disabled or kept active
- Built-in Help Desk allows interactive support for users from anywhere using your browser
- Background access allows maintenance to be performed without interrupting the user

IPv6 Support

- RemotelyAnywhere supports Internet Protocol Version 6 (IPv6), the protocol designed to replace the current version Internet Protocol, IP Version 4 (IPv4).
- Standard IPv6 address formats are accepted in any IP address field

Additional Features

- Full support for XP Fast User Switching and Terminal Services
- Custom HTTP pages can be delivered from each workstation running RemotelyAnywhere without additional of HTTP server

- Automatic check for upgrades
- User-defined colors and layouts
- User-defined quick links to the features you use most

System Requirements

- RemotelyAnywhere can be used to remotely control and manage any computer running Windows Vista/XP/2000/ NT4.
- RemotelyAnywhere is also compatible with Windows Vista and XP 64-bit operating systems on both the Client and remote machines.
- Computers running RemotelyAnywhere can be accessed from most devices with ActiveX or Java-compatible web browsers, regardless of the operating system. PDA Access is limited to devices running Pocket PC 2000/2002, Microsoft Windows Mobile 2003 for Pocket PC or Microsoft Windows Mobile 2003 Second Edition for Pocket PC.

About this Guide

After reading this guide you should be able to do the following:

- Be able to set up and access your Host through RemotelyAnywhere
- Install the RemotelyAnywhere software on the machine that you wish to control, including:
  - Default installation configurations
  - Custom installation configurations
- Activate the software
- Access the Host from a local area network (LAN) or over the Internet
- Log into the host machine
- Make any special settings required to access RemotelyAnywhere through a firewall
- Know where to locate reference information about all RemotelyAnywhere screens and functionality

Acknowledgements

OpenSSL: RemotelyAnywhere includes cryptographic software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For more information visit: http://www.openssl.org

OpenSSH: RemotelyAnywhere uses cryptographic software developed by the OpenSSH group. For more information visit: http://www.openssh.org

CompuPhase: RemotelyAnywhere includes scripting software developed by ITB CompuPhase. The PAWN language, its interpreter and compiler are copyright © Thiadmer Riemersma, ITB CompuPhase, 1998-2007, The Netherlands. For more information visit: http://www.compuphase.com/pawn/pawn.htm

First Steps

Installing RemotelyAnywhere

Default Installation

1 If you have not already downloaded RemotelyAnywhere, locate and download and execute the remotelyanywhere.msi from http://www.RemotelyAnywhere.com/downloads.htm.

2 On the Welcome screen, select **Next**.

3 On the License Agreement screen, select **I Agree** if you agree to the terms and conditions. If you do not accept these terms, you can exit the setup by clicking the **Cancel** button.

4 The Software Options screen appears next. If the default listening port is acceptable, click **Next**. For more information regarding customizing RemotelyAnywhere during installation, see Custom Installation.

5 The setup will then ask for confirmation of the destination location for the files for RemotelyAnywhere.

6 If you wish to change the destination folder, select the Browse option. Select **Next** to confirm the destination folder.

7 To start copying the files to their destination folder (selected in step 6 above) click **Next**.

8 Select **Finish** to complete the Setup.

Custom Installation

1 Follow steps 1 – 4 above of the Default Installation above.

2 The Software Options screen allows the user to specify the listening port for use by RemotelyAnywhere.

3 If the default port used by RemotelyAnywhere (2000) conflicts with an existing application or service, the user may change it here. If the person installing RemotelyAnywhere is not the Network Administrator, the Network Administrator should be consulted before a port is assigned.

4 This screen also allows the user to copy configuration settings from an existing RemotelyAnywhere installation.

5 After all options have been configured satisfactorily, select **Next**.

6 Continue with steps 6 to 8 outlined above in Default Installation.

Software Activation

Once you have installed RemotelyAnywhere following the instructions above you will need to activate it. If you have already purchased a license, you will be able to paste it into the space provided and activate the software straightaway.

If you have not purchased a license but would like to do so, you will be given the option to do this on the software activation screen. If you purchase online, your license will be delivered immediately, so you can activate your software without delay. Alternatively, you may want to contact our sales department.

If you would prefer to try the software before purchasing, you are entitled to a 30-day evaluation period. Just select "I would like a free trial" on the software activation screen and follow the instructions. You will need to be connected to the Internet to activate your free trial.

The RemotelyAnywhere free trial uses an identifier value from your machine to control the number of evaluation licenses a single computer can receive. It is generated by passing unique data related to your computer through a one-way cryptographic hash function. The ID generated with this algorithm does not identify you or any component of your computer system: Think of this as a unique ticket that your machine receives.

Accessing RemotelyAnywhere

When the installation is complete, the default Internet browser will open with the address of http://MachineName:2000.

To access the host machine from a different machine, open an Internet browser and enter `http://111.111.11.1:2000` in the Location/Address line. `111.111.11.1` represents the IP address of the host machine. `2000` represents the default port shown on the Software Options screen during installation. If you changed this port during installation, then use the specified port when accessing RemotelyAnywhere. On the same network the machine name can also be used.

On the host itself you can also access a machine by entering the loopback address `http://127.0.0.1:2000` at the Location/Address line. This address allows the user to communicate with the RemotelyAnywhere installation only at the machine on which it is installed.

About Dynamic IP Addresses

Many DSL and cable Internet connections assign your machine a new IP address each time you connect to the Internet. This is known as a Dynamic IP address. RemotelyAnywhere will work if you have a dynamic IP (DNS) address, but RemotelyAnywhere needs to be able to track your IP address so that if it changes, the connection can be maintained. There are dynamic DNS solutions available, often for free, which means that your machine can be assigned a fully qualified and static domain name regardless of your IP address.

Alternatively, under **Preferences > Network** you can configure RemotelyAnywhere to send you an email message pointing to the IP address of your remote host every time it detects a change. This way, you always know where to find your Host.

Logging In

After entering the URL into your browser and pressing enter, you will reach the RemotelyAnywhere Login screen.

RemotelyAnywhere will access the user database to authenticate the user. Initially, you will need to log on as someone who is a member of the Administrators group. You can later change this default behavior by granting NT users or NT groups access to RemotelyAnywhere under **Security > Access Control**.

NTLM: By clicking **NTLM** you can use your current Windows login credentials to verify your identity on the Host. This only works when accessing a Windows NT/2000 or XP computer. It will use your current credentials (those you entered at the NT logon prompt on the computer running your browser) to identify you to the Host. This is only available on local networks.

Advanced Login Options

By clicking on **Show Advanced Option**s in the login window a number of additional options become available:

Go directly to Remote Control	Using these buttons you can select whether you want to go directly into Remote Control, to File Transfer & Synchronization or to the Main Menu page - this last option being the default.
Full and Light Interfaces	You can choose between the full and light interfaces. RemotelyAnywhere's full interface is for DHTML capable browsers. The light interface is more suitable for old browsers or users with slow Internet connections.
SSL	If you set up SSL Support for RemotelyAnywhere all traffic between the host and the Host will be encrypted using industry-strength 128-bit ciphers, protecting your passwords and data. You can do this easily by going to Security, clicking on SSL Setup, and following the step-by-step instructions there.
Select Language	You are able to select the language of your choice when logging in.

Bypassing the Login Screen

You can force an NTLM login – and thus bypass the login screen entirely – by appending `/ntlm/` to the URL with which you access RemotelyAnywhere. For example, the URL http://MAILSERVER:2000 would become http://MAILSERVER:2000/ntlm/. Ensure you include the trailing slash.

You can also use this method to bypass the menu system and access certain parts of RemotelyAnywhere directly. Here are some URLs as an example:

- Remote Control: `http://your.machine.here:2000/ntlm/remctrl.html`
- Command Prompt: `http://your.machine.here:2000/ntlm/telnet.html`
- Chat: `http://your.machine.here:2000/ntlm/chat.html`

Similarly, you can specify your username and password in the URL – thus forcing a normal login – by appending the credentials in a `/login:username:password:domain/` form to the URL with which you access RemotelyAnywhere.

For example, the URL `http://MAILSERVER:2000` would become `http://MAILSERVER:2000/login:username:password:domain/`. Yet again, ensure you include the trailing slash.

The Windows NT domain you are logging in to is optional. If omitted, RemotelyAnywhere will try to authenticate you on the computer on which it is running, then in the domain to which it belongs. Here are some URLs as examples:

- Remote Control: `http://your.machine.here:2000/login?username=x&password=y&domain=z&go=r`
- Command Prompt: `http://your.machine.here:2000/login:yourloginname:yourpassword/telnet.html`
- Chat: `http://your.machine.here:2000/login:yourloginname:yourpassword/chat.html`

Accessing RemotelyAnywhere through a Firewall or Router

Most organizations today employ a range of security measures to protect their computer networks from hostile intrusion. One of the common measures includes creating a firewall. A firewall is a system designed to prevent unauthorized access to a private (internal) network. Firewalls can be implemented either as hardware or software, or a combination of the two.

The most common use of a firewall is to prevent unauthorized intrusion from Internet users attempting to access a private network or Intranet. A firewall examines all traffic entering or leaving the internal network/Intranet, ensuring that traffic meets security criteria established by the Network Administrator.

RemotelyAnywhere can be configured to work with a firewall-protected computer. This requires mapping an external, incoming port on the firewall to the internal IP and port on the computer running RemotelyAnywhere. Routers, on the other hand, operate in much the same way as firewalls. They both offer the opportunity to open and map ports to specific computers. For the rest of this explanation, the term "router" can be interchangeable with "firewall."

From outside your LAN, you would gain access to the computer running RemotelyAnywhere by entering the firewall's IP address and the port to which the desired machine is mapped. For example:

Router: External IP address: `111.111.111.111`

RemotelyAnywhere computer: IP address: 192.168.0.10, Port: 2000 (port 2000 is the default but this can also be changed).

Step 1: Mapping a Firewall Port to the Computer

In this case, you would pick a port on the router (say, 5200) and map it to 192.168.0.10:2000.

The procedure for mapping ports from routers to computers is router-specific. Usually your router will have a web-based interface that allows you to configure and maintain it. Sometimes router companies refer to this action as Port Forwarding or Port Mapping.

Step 2: Accessing RemotelyAnywhere through a Firewall

Having done the above, you will now be able to fully access the RemotelyAnywhere computer with the URL http://111.111.111.111:5200 - that is the firewall's external IP, followed by the port you mapped to the RemotelyAnywhere machine.

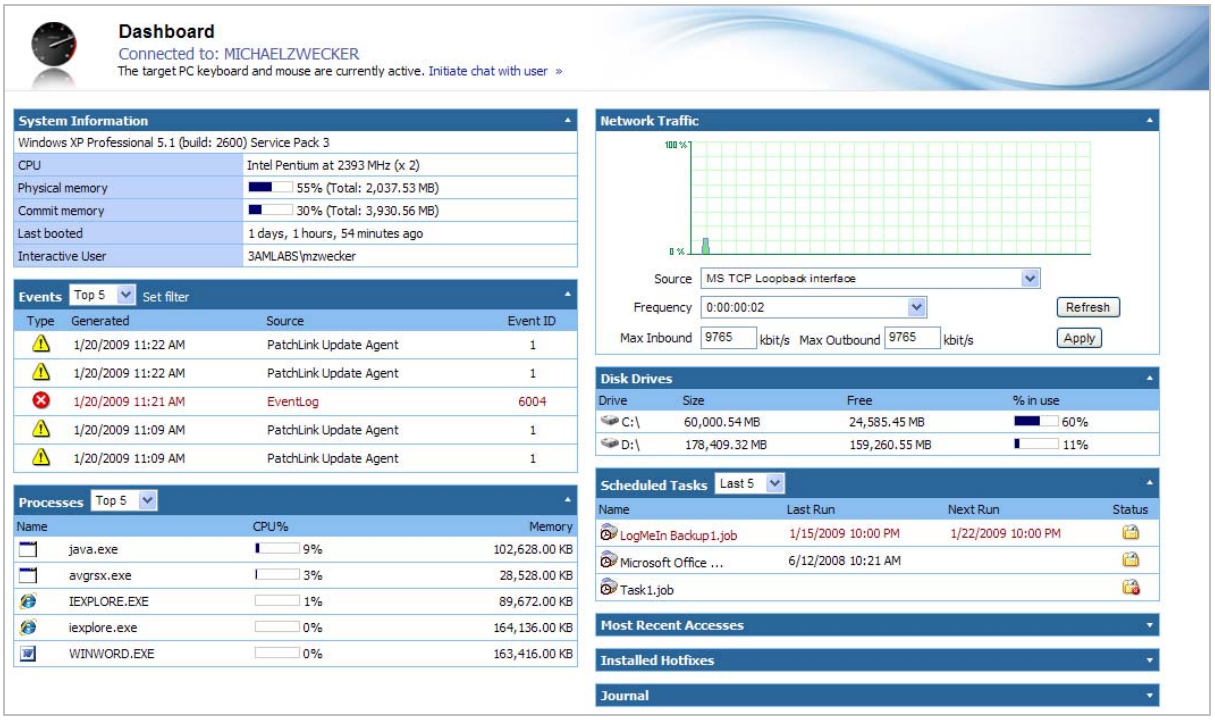
External Resources for Help with Router and Firewall Configuration

No two router models are exactly alike, and this document lacks sufficient space or scope to offer detailed support for all routers and firewalls and RemotelyAnywhere. However, the overarching principles for port forwarding remain the same. Should your router or firewall documentation prove confusing or insufficient, there are several resources available on the Internet that provide exhaustive instruction and help with configuring routers and firewalls.

User Interface

The Dashboard

The Dashboard gives you a detailed, up-to-the-minute diagnostic view of system information for an individual RemotelyAnywhere computer.



Each section of the Dashboard displays a summary of activity.

System Information	Provides details about the Host's operating system; the CPU installed; the amount of physical and virtual memory available and used; when the computer was last booted; and which user is logged in.
Network Traffic	Provides details of network traffic on the selected network interface. The area at the top shows the loading on the network interface: you can redraw this graph to show the latest data by clicking **Refresh**. You may also adjust the sensitivity of the graph by changing the values in the **Max Inbound/Outbound** fields.
Events	Provides an instant view of information that must typically be retrieved using the Administrative Tools/Event Viewer within Windows. It displays the five (default value) most recent events from the Application Event Log, Security Event Log, and System Event Log. You can customize which events are displayed by clicking Set Filter.
Disk Drives	Displays the size and amount of used/free space on each disk drive of the Host.

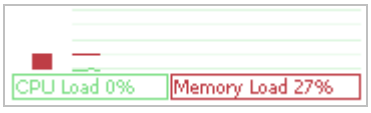
Processes	Provides an instant view of information that must typically be retrieved by running Windows Task Manager/Processes. It displays information about the five (default value) processes using most CPU resources; the percentage of CPU each process is using; and the amount of memory each process is using.
Scheduled Tasks	Provides an instant view of information typically retrieved using the Scheduled Tasks feature in Windows. It lists the most recently executed scheduled tasks.
Most Recent Accesses	Provides details of the most recent accesses to the Host using RemotelyAnywhere.
Installed Hotfixes	Provides details of the Windows Hotfixes (updates, service packs, etc.) installed on the Host.
Journal	Provides a list of the five (default value) most recent Journal entries. The Journal allows you to add useful, time-stamped comments by typing in the input box and clicking **Add**.

Dashboard Features

Section-level details	To view detailed information, click a section heading.
Item-level details	Click any item to view highly detailed information about the event, process, disk drive, etc.
Tool-tips	Hold your mouse over an item to see a tool-tip containing a select set of details about the event, process, disk drive, etc.
Customizable layout	You can drag, drop, minimize, maximize or reposition the various sections. Also, you can change the number of items to be displayed in certain sections (Events, Processes, Scheduled Tasks, and Journal).
Journal	Use this feature to leave notes on the Host's desktop. For example, notes on the current status of scheduled tasks, or the reason the computer was remotely accessed.
Filtering	You can filter Event messages. See the Event Viewer section for details.

Performance Data Viewer

On every page of RemotelyAnywhere you can see a real-time Performance Data Viewer:



This java applet is to the right of the RemotelyAnywhere logo in the top frame. It shows CPU load (green) and Memory load (red) and is updated every few seconds, so you can get instant feedback on the effects of performance intensive processes. This graph can be disabled under **Preferences > Appearance**.

Quicklinks

QuickLinks are accessible from every page of RemotelyAnywhere. You can add your favorite pages to the QuickLinks drop down menu wherever you see the star icon in the tool bar of the page you are viewing. You can also edit your QuickLinks by clicking on Edit your QuickLinks in the QuickLinks drop-down menu.

The QuickLinks menu is situated in the top frame of the page so that your favorite pages are always only a click away. They are also listed on the System Overview tab of Home page.

Log Out and Time

You can Log Out from RemotelyAnywhere via the red Log Out button in the top right corner of the screen, to the right of your computer's name. If you are inactive for 10 minutes you will be logged out automatically. The session timeout time can be modified under **Security > Access Control**.

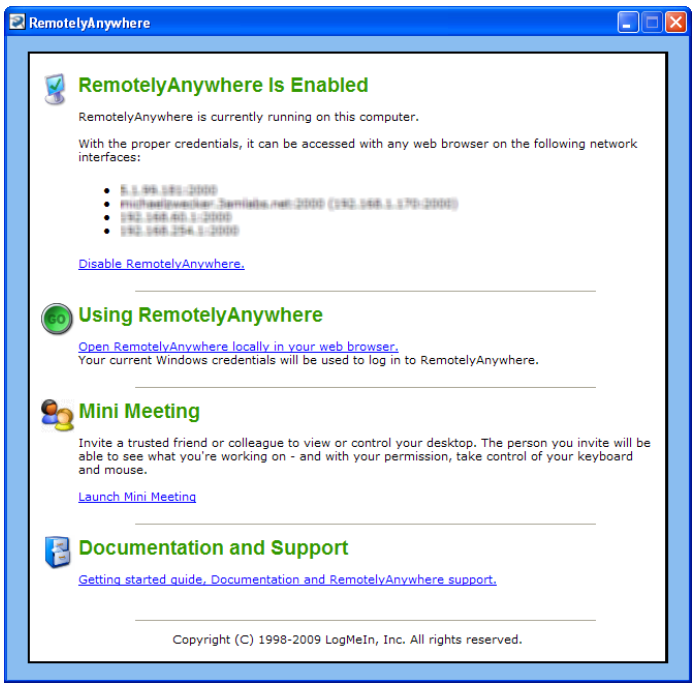
The time on the remote machine is displayed above the log out button.

System Tray Icon

RemotelyAnywhere includes a system tray icon that serves multiple purposes. This icon can be fully configured via the **Preferences > Systray Settings** screen.

Systray menu options

Right-clicking the RemotelyAnywhere icon in the systray will bring up the following options:

Open RemotelyAnywhere	This option will open this dialog box: 

Open RemotelyAnywhere Web Interface	This option will start up RemotelyAnywhere on the local host and log you in using NTLM.
Open Status Window	This option opens a window that updates you on the current status of RemotelyAnywhere.
Enable/Disable RemotelyAnywhere	Here you can turn the RemotelyAnywhere service on and off at will.
About	This command brings up RemotelyAnywhere's HTML About box.
Convert Remote Control Recordings	This wizard will convert RemotelyAnywhere remote control screen recording files into an AVI file for playback in any media player.

The RemotelyAnywhere Toolkit

Every page of RemotelyAnywhere can be reached from the left hand toolkit menu.

The toolkit menu tree expands and collapses so you can find the pages you need quickly.

Remote Control

One of the main features of RemotelyAnywhere is its advanced ability to remotely control the computer on which it is installed, thus enabling you to authentically replicate the experience of sitting in front of the Host.

When you select Remote Control, by default RemotelyAnywhere will attempt to load a small ActiveX control, and, if your browser does not support ActiveX, it will try the Java-based version. Failing that, the HTML screenshot version will load.

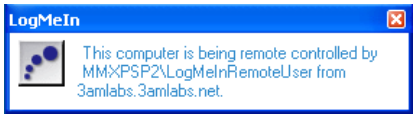
By expanding the left Remote Control menu, it is possible to select any of these three options manually. Depending on your browser settings, you may see a pop-up window asking you to accept or reject the ActiveX control or Java applet. You should accept it in order to use Remote Control.

When typing or using your mouse, it will be exactly as if you were sitting in front of the remote machine. The only real difference will be a number of RemotelyAnywhere-specific tools which appear at the top of the remote control window, detailed below.

On the toolkit, click **Remote Control** to initiate a Remote Control session with the computer to which you are connected.

Remote Control Notification Window

As soon as your remote control session starts, a notification window appears on the screen of the Host. This is a security feature to advise the user that the machine is being remote controlled.



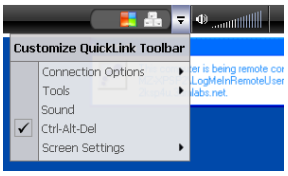
Note: This window always appears. This cannot be changed, nor can the window wording be altered.

The Remote Control Ribbon

The Remote Control interface is called the Remote Control Ribbon. Once you are in a remote control session, there are several features that you can adjust to streamline the experience. You make these adjustments using the remote control ribbon.

***Note**: To change settings impacting how Remote Control functions see the Remote Control Preferences section. These settings determine which Ribbon features will be available.*

QuickLinks



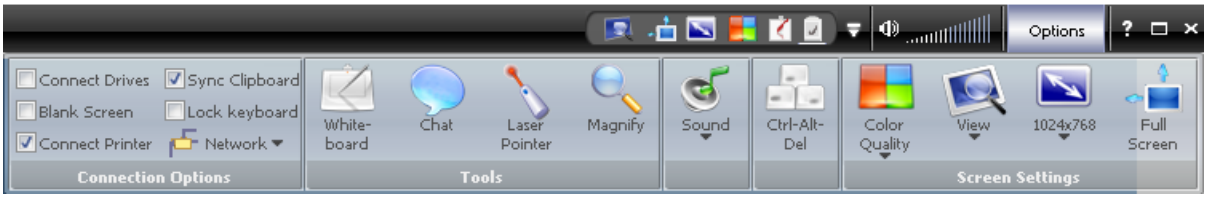
This feature allows you to add icons to the QuickLinks bar. These icons will allow you one click access to all the features available in both the basic and advanced ribbons. Click the down arrow next to the QuickLinks bar to see a list of available features that can be added. All available Options can be added to the QuickLinks bar.

Sound

If Sound is enabled, you can mute the sound (and vice-versa) by clicking on the loudspeaker icon. Adjust the volume by dragging your mouse across the volume bars until you obtain the optimum setting.

Options

Click to access all available Remote Control options.



The following options may be available depending on your computer settings.

Connection Options	
Connect Drives	When selected, drives on the Client will be connected to and appear as network drives on the Host. Once connected you can use files directly on the Client. This option is only available if **Enable Connecting Drives** is selected at **Preferences > Remote Control >** Connecting Drives.
Blank screen	Select this option to blank the Host's screen. This is useful when inputting confidential information that you would not want anyone to see.
Connect Printer	You can print files on the Host using a printer on the Client. Selecting **Print** on the Host machine sends that print job to the Client's default printer. A notification window will appear on the Host informing you that the connection has been established: If you have more than one printer and want to use another printer, uncheck the **Connect Printer** box, and make the desired local printer your default printer and reconnect.
Sync Clipboard	This synchronizes the two machines' clipboards. Anything copied on one machine is automatically available to be pasted on the other.
Lock Keyboard	This locks the keyboard of the Host machine so that it cannot be operated by anyone sitting at the Host machine.
Network	This allows you to select the network connection type. Selecting Slow allows you to optimize your connection on lower speed connections. Selecting Fast lets you exploit high bandwidth connections. The recommended Auto option allows RemotelyAnywhere to set this connection automatically according to the kind of connection it detects.
Terminal Server	This is only visible to users with Terminal Server activated. If the Host is a terminal server (multiple terminals are connected to it using Windows remote desktop) then the terminal server option lets you select whether you want to remote control the Host or one of the connected terminals. Click to switch between sessions.
Tools	
Whiteboard	The Whiteboard feature is invaluable for showing remote users how to detect specific parts of their desktops. It leaves a red track on the screen of the Host. Deactivate the feature to delete the on-screen lines. You will also need to deactivate it to gain control of the Host machine.

Chat	Selecting Chat allows you to open a chat session with the user of the Host. Input text on the Client screen. Select **Send**, or press **Enter** and a chat box opens on the Host's desktop where the remote user can respond. This is a two-way chat. No other participants can be invited to join the session.
Laser Pointer	As with the Whiteboard feature, the Laser Pointer assists you in talking remote users through a complex issue on their machine. A clear red dot can be moved around the screen to highlight features. Deactivate the feature to regain remote control.
Magnifier	This activates a box on the Client that can be dragged around the Host desktop to magnify a small area of the Host screen. This is useful for when you are running screen resolutions of less than 100% and you want to view a specific area of the screen without readjusting your screen resolution.
Sound	
Volume	Click and drag your mouse over the volume bars to adjust the volume setting.
Quality	Select one of three sound quality settings by dragging the slider to the required setting. The higher the sound quality, the greater the bandwidth needed to transmit the sound.
Advanced	Select the sound playback device on the Client.
Ctrl-Alt-Del	
Ctrl-Alt-Del	Click this button to perform the same action as the Ctrl-Alt-Delete button combination on the Host.
Screen Settings	
Color Quality	Adjust the color quality of the displayed remote screen to optimize the amount of information transferred during remote control. Adjusting this setting changes the look of the screen during remote control, but will not be seen by the Host user. We recommend **Automatically adjust color settings**. The Advanced option is to allow your remote control screen to switch to grayscale if focus shifts to another part of your screen. To restore color, move your cursor back onto the remote control screen.
View	Adjust the zoom setting for the viewable screen. Use **Scale to fit** to ensure the Host screen display properly on the Client. If using a set percentage, the remote screen may be larger than the local screen. If so, scroll-bars appear to allow you to navigate the remote screen. If your remote control screen appears fuzzy or unclear, a value of 100% into the **Custom Zoom** field should fix the problem. To view the Host screen as if you were there, we recommend that you select **Scale to Fit** and switch to full-screen.
Resolution settings	To ensure a perfect fit in full-screen mode, select **Match Resolution** to set the Host screen resolution to the same as the Client. On finishing a remote control session, the Host's screen resolution returns to its default.
Full Screen	This performs the same function as the full-screen button on the standard ribbon.

Monitors	Click to switch between screens on computers using more than one monitor. This is only visible to users with multiple monitors on the Host.

Help

? Click to view short movies outlining key Remote Control features.

Full Screen

 Click to go to full screen mode…

 …and back to standard.

Disconnect from Remote Session

 Disconnect from the remote control session. You will be returned to the Dashboard.

To enter text on the remote screen, you should enter it in the send keys field in the toolbar and click send. Checking the box next to this field enables you to enter special characters and simulate special keys. Each key is represented by one or more characters. To specify a single keyboard character, use the character itself. The plus sign +, caret ^, percent sign %, tilde ~, and braces { } have special meanings to this function. To specify one of these characters, enclose it within braces. For example, to specify the plus sign, use {+}. To specify brace characters, use {{} and {}}.

To send special key combinations such as Ctrl+Alt+Delete, use the drop down menu to the right of the send keys field.

To specify characters that are not displayed when you press a key, such as Enter or Tab, and keys that represent actions rather than characters, use the codes shown below:

Key Code	
Backspace	{BACKSPACE}, {BS}, or {BKSP}
Caps Lock	{CAPSLOCK}
Del	{DELETE} or {DEL}
Down Arrow	{DOWN}
End	{END}
Enter	{ENTER} or ~ ESC {ESC}
Home	{HOME}
Insert	{INSERT} or {INS}
Left Arrow	{LEFT}
Num Lock	{NUMLOCK}

Page Down	{PGDN}
Page Up	{PGUP}
Right Arrow	{RIGHT}
Scroll Lock	{SCROLLLOCK}
Tab	{TAB}
Up Arrow	{UP}
F1 to F24	{F1} to {F24}

To specify keys combined with any combination of the Shift, Ctrl, and Alt keys, precede the key code with one or more of the following codes:

Key Code	
Shift	+
Ctrl	^
Alt	%

For example, if you want to go to the beginning of an edit field, select the entire line, place it on the clipboard, and overwrite it with something else then select Enter, you would type:

```
{HOME}+{END}^cThis is the new text {ENTER}
```

This translates into pressing the Home key (going to the beginning to the field), pressing the Shift and the End keys at the same time (selecting the entire field), pressing Ctrl+C (clipboard copy), typing the new text and then selecting Enter.

File Manager

On the RemotelyAnywhere toolkit, click **File Manager** to open the File Manager. The feature allows you to easily and securely transfer files between your Host and Client PCs. You can also synchronize entire folders on both computers with one mouse click. All data transferred between your Host and Client PCs are compressed and encrypted.

Transferring and Synchronizing Files

To transfer or synchronize files, follow these steps:

1 Connect to the Host

2 Click **File Manager** on the navigation bar.

Note: *To perform this function in a new window, right click on File Manager and select* ***Open Link in New Window****.*

3 A dialog box will indicate the progress of your file manager connection to the Host. If the dialog box does not close automatically, click **Continue**.

4 The File Manager mode displays your Host and Client PCs' files in a split screen. The Host's files are displayed in the right frame, the Client's in the left. Use the Tab key to switch between the two frames.

5 Open a Destination Folder. This is the folder to which files will be transferred. This can be any folder on either the Host or Client.

6 Select the files that you want to transfer. The files must be on the opposite computer as the Destination Folder.

Note: *Select files while holding down the Shift key to select multiple folders and files.*

7 On the toolbar at the top of the File Manager window, click **Transfer > Copy**. The selected contents of the Source Folder will be copied to the Destination Folder of the same name on the Client.

File Manager menu

Other options are accessed using the File Manager toolbar.

The File Manager toolbar lists items in the following four categories: Navigate, Edit, Transfer and Select. These actions are available via the drop-down menu shown, the toolbar buttons indicated below, or the keyboard shortcut listed.

Note*: If you are using a Windows computer with Internet Explorer, the default File Manager interface in RemotelyAnywhere is served by an Active X control. Otherwise, Java will be the default. The interface is slightly different, with the actions grouped in drop down menus above the icons, but it is essentially the same, and there is no difference in the available options.*

Navigation

The Navigate and Sort options are accessed via a drop-down menu. Shortcut keys are available for each item.

Refresh	Press **F5** to refresh the folders on both the Client and Host.
Up	You can go up to the parent directory by pressing Backspace.
Drive list	Click to display the available root drives on the selected computer.
Select left drive	Click to select the disk drive you want to view in the left pane of the File Manager window.
Select right drive	Click to select the disk drive you want to view in the right pane of the File Manager window.
Go to folder…	Click this item to open a box where you can type the name of a specific folder or directory you want to view on either the Client or Host.
Sort by…	Use this option to sort directory contents by **name** (Ctrl+1), **type**, (Ctrl +2), **size** (Ctrl+3) and **date** (Ctrl+4).
Show…	Select **Show folders for all users**, **Show hidden files**, and/or **Show system files** in any combination.

Edit

Create Folder		You can create a new folder in the selected location with the **Create folder** button or by pressing Ctrl+N.
Rename		You can rename a selected file or folder with the **Rename** button or by pressing F2.
Delete		You can delete a selected folder or file with the **Delete** button, or by pressing Delete on your keyboard.

Transfer

Copy		You can copy a file or folder with the **Copy** button or by pressing Ctrl+C.
Move		You can move a file or folder with the **Move** button or by pressing Ctrl+X.
Synchronize		By clicking on the **Synchronize current folders** button (or by pressing Ctrl+S) you can update the current folders to the Client and Host so that their contents are the same. Files and folders that exist only on one side are copied normally. If both folders contain one or more files that are different on the Client and Host PCs, the newer version will be copied. The folders must be open, not simply selected.

Replicate		When you click this button (or by pressing Ctrl+R) files and folders that do not exist in the destination folder are copied normally. Files that already exist in the destination folder will be transferred from the source folder. If a destination folder contains a file or a folder that does not exist in the source *it will be deleted*. This is very useful if you update the Source folder and want to push those changes to the Destination.
Connection Details		From the drop down menu you can also select Connection Details to display encryption and authentication details about your current connection.

Select

Select Files		You can select files with the Select files button or by pressing + on the number pad.
Deselect Files		You can also deselect files via the toolbar or with - on the number pad.From the drop-down menu you can also select all the files (Ctrl+A), select none (Ctrl+Num), or invert the selection (Num*).

Mini Meeting

On the RemotelyAnywhere toolkit, click **Mini Meeting** to view instructions on RemotelyAnywhere's Mini Meeting feature. Mini Meeting is allows you to invite another RemotelyAnywhere user to access your computer.

Start a Mini Meeting

1 Right-click on the RemotelyAnywhere system tray icon. Select **Mini Meeting**.

2 In the Contact Your Guest dialog box, choose how you want the invitation to be sent:

   a **Send an email on my behalf** to allow RemotelyAnywhere to send an email.

   b **I will send an invitation myself** to send the invitation using your chosen email program.

3 Click **Next**.

4 In the Invitation Details dialog box, enter a name for the invitation and specify how long the invitation will remain open. The invitation will expire if the invitee does not accept within the given amount of time.

5 Enter the **email address** of the recipient and any **Message** that you want to send with the invitation.

6 Click **Next**.

What the Recipient Must Do

1 The recipient of the invitation will receive an email detailing the invitation and who has sent it.

2 The recipient clicks **Accept Invitation**.

***Note**: If the recipient's computer has never been used to access a computer running RemotelyAnywhere software, then the recipient will be asked to install the RemotelyAnywhere plugin.*

3 The recipient logs in to RemotelyAnywhere.

4 The recipient then selects the profile which relates to the invitation and selects the computers to be accessed.

Chat

From the RemotelyAnywhere interface, click **Chat** to open RemotelyAnywhere's Chat feature.

Simply enter your message in the text box at the bottom of the window and press **Send** to send your message to the recipient at the Host.

***Note:** This is a two-way chat. No other participants can be invited to join the session.*

Computer Management menu

On the RemotelyAnywhere toolkit, click **Computer Management** to access a powerful set of computer management features, including User Manager, Event Viewer, Services, Processes, Drivers, Registry Editor, Command Prompt, Reboot, and Monitor Local (Host) Screen.

These features are available in the background; that is, the RemotelyAnywhere user is able to view and alter a Host machine's settings without having to initiate a Remote Control session and without disturbing the user.

User Manager

On the RemotelyAnywhere toolkit, select **Computer Management > User Manager** to manage the rights of users and groups on the Host.

Click on a user name to change the name or password, assign to groups or to delete from the user list. The User Manager supports all features of Windows' built-in User Manager, with full Active Directory support.

Note: *A disabled account exists, but the user is not permitted to log on. It appears in the list of users but the icon has an X in it. To activate an account, click the name of the account and the cancel the selection in* ***Account Disabled*** *on the Manage User window.*

Event Viewer

On the RemotelyAnywhere toolkit, select **Computer Management > Event Viewer** to view and monitor events recorded in the Application, Security, and System logs of the Host. This feature is very similar to the Windows Event Viewer.

- The Event Viewer lists log entries. You can click on any entry to display its details.
- You can choose to clear the contents of a log file by clicking **Delete** on the toolbar. Specify a filename to back up the event log before it is deleted.
- You can also send email alerts to specified email addresses when log entries matching a given criteria are entered into any of the event logs.

Services

On the RemotelyAnywhere toolkit, select **Computer Management > Services** to view the names and statuses of all the services (or drivers) installed on the Host.

- Click on a name to view more details of the selected Service object and to control it. You can also change a Service object's startup options.
- When specifying a user account to be used by a service, it must be in **DOMAIN\USER** form. Type **.\USER** to use a local account.
- In the objects list, the status field shows **Started**, **Running**, **Stopped**, etc. All listed services and drivers that are not running and not set to start automatically will be shown red.

Processes

On the RemotelyAnywhere toolkit, select **Computer Management > Processes** to view a list of all the processes running on the Host.

The list is hierarchical: a parent process will have its child processes listed beneath it, with indentations indicating relationships. Please note that this is for information purposes only, since Windows reuses process IDs.

Click **Refresh** to retrieve and display the latest process list.

The following information is available in the list by double-clicking an item, or in a tooltip that appears when you hold the mouse over any process in the list.

PID	The internal Windows Process ID.
Hierarchy / Executable / Module	The name of the executable file with full path. This works as a link, and clicking on it will give you some very detailed information on the process. On that page, you have the option of changing the priority class or the processor affinity for the selected process. This data are arranged under the following tabs for easy viewing: General, Windows, Threads, DLLs, Open Files, and Registry Keys in Use.
Version	The version of the program, if specified.
Description	The description of what the program does, if specified.
Memory Used	The amount of memory in use by the process in kilobytes.
Created	The date and time the process was started.
CPU Time	The amount of CPU time (d hh:mm:ss) the process has used.
Priority	The priority class of the process.
Type	The type of the process (service or interactive).
Account	The user account the process is running under.
End Process	Click to terminate the process immediately.

Drivers

On the RemotelyAnywhere toolkit, select **Computer Management > Drivers** to view a list of all programs that control devices. The items displayed work as links. Double-click any item to view detailed information arranged under the tabs General and Dependencies.

Registry Editor

On the RemotelyAnywhere toolkit, select **Computer Management > Registry Editor** to edit the registry for the Host. The registry keys (HKCR, HKCU, HKLM, etc.) are displayed in a tree structure. Click on any item to analyze further available information.

Registry keys are displayed in a hierarchical tree. Key values are also displayed, with their name, type and value. You can edit values that are either of text (REG_SZ, REG_EXPAND_SZ or REG_MULTI_SZ) or integer (REG_DWORD) type and REG_QWORD type values. Binary values are displayed, but cannot be edited. Use the buttons in the toolbar to **Create a New Key** or **Delete** a key.

Command Prompt

On the RemotelyAnywhere toolkit, select **Computer Management > Command prompt** to open the MS-DOS command prompt on the Host.

The Telnet client, written as a Java Applet, provides encryption and data compression for security and speed. It is secure, using the same encryption employed by the remote control module; it is fast, since it uses sophisticated data compression to achieve high throughput; and finally, it lets you transfer keystrokes that terminal emulators do not handle, such as the Alt key. You can also use your mouse in console applications that support it.

Should you disconnect your terminal emulator, or go to a different page in the browser window containing the Telnet client applet, all applications you have running in the Telnet session are left active.

You can reconnect to this Telnet session by simply logging in (or loading the applet) again. There is a timeframe for this though: if you do not reconnect within 60 minutes, all your telnet applications, including the command shell, are terminated. You can change the timeout value from the default value of one hour to anything you want in the configuration dialog boxes.

To set the size of the MS-DOS window, click **Preferences** and then enter the desired size in terms of **Rows** and **Columns**. To terminate the Telnet session, type **Exit** at the command prompt.

Reboot

On the RemotelyAnywhere toolkit, select **Computer Management > Reboot** to view the following six options for rebooting the Host.

Restart RemotelyAnywhere		Restarts the RemotelyAnywhere service. It does not reboot the remote machine. This is useful if you change settings like the listening port and have no physical access to the machine in order to restart the service.
Normal Reboot		Closes all processes and reboots the Host machine in the traditional way.
Emergency Reboot		Does not allow applications and other processes to terminate gracefully, so you might lose unsaved data. Windows will, however, shut down properly and flush all outstanding file operations to disk. This can be useful if there are hung processes that prevent Windows from shutting down normally.
Hard Reboot		Reboots as quickly as possible. This option will not allow Windows to terminate normally, so you might lose unsaved data. Since rebooting is immediate (just like pressing the reset button) you will not receive any RemotelyAnywhere feedback if you select this option.
Safe-mode Reboot		Restart the computer in safe-mode with networking enabled. Safe-mode is a special way for Windows to load when there is a system-critical problem that interferes with the normal operation of Windows. RemotelyAnywhere must be enabled.
Scheduled Reboot		This allows you to schedule a date and time to automatically reboot the computer. This is useful if the reboot is not urgent and can take place during off-peak hours.

Monitor Host Screen

On the RemotelyAnywhere toolkit, select **Computer Management > Monitor Host Screen** to gain view-only access to the Host's screen. The user monitoring the computer remotely can not interact with it. This feature is useful for monitoring screens while waiting for prompts to appear.

A message stating that the computer is being monitored will be displayed on the screen of the Host.

Computer Settings menu

On the RemotelyAnywhere toolkit, use the **Computer Settings** menu to view and modify a number of settings on the Host machine.

Environment Variables

On the RemotelyAnywhere toolkit, select **Computer Settings > Environment Variables** to view and make changes to environment variables on the Host. User environment variables that are defined by you or by programs are listed here, such as the path where files are located. Double-click on any item in the list to view details and make changes. Click the **Create** button on the Environment Variables toolbar to create a new variable.

Virtual Memory

On the RemotelyAnywhere toolkit, select **Computer Settings > Virtual Memory** to change virtual memory settings on the Host. Simply enter a minimum or maximum size for the paging file next to a drive and click **Apply**. Entering zero values both for the minimum and maximum size will remove the paging file from the drive.

Note: *You will need to reboot the computer for any changes to take effect.*

Time

On the RemotelyAnywhere toolkit, select **Computer Settings > Time** to edit the time and date on the Host. Simply enter the desired values and click **Apply**. Please note that the time is displayed according to the time zone settings of the Host.

Automatic Logon

On the RemotelyAnywhere toolkit, select **Computer Settings > Automatic Logon** to enable or disable the Windows auto-logon feature. You can also do this via the register or with other small utilities, similar to the one included in the NT Resource Kit.

Enabling auto-logon will cause the server to bypass the logon dialog after system startup and will log in with the username and password specified here.

Note: *This a potential security risk. The username and password are stored in the registry in clear-text format.*

Shared Resources

On the RemotelyAnywhere toolkit, select **Computer Settings > Shared Resources** to view and manage shared resources on the Host, including shared folders, administrative shares and printers, etc.

- Click the **Path** link to open the linked folder in the RemotelyAnywhere File Manager
- Active **Access permissions** are also shown in detail
- The **Connections** section shows any open files. Click **Close** to close a file
- The **Delete** button removes sharing from the object

- Click the **Change Access Permission** button to open a dialog box where you can add new permissions or remove existing permissions for the chosen object

Automatic Priorities

On the RemotelyAnywhere toolkit, select **Computer Settings > Automatic Priorities** to begin setting automatic change process priorities. This useful if you want to force lengthy, CPU-intensive tasks into the background on a machine where responsiveness of other processes is critical. For example, you may want to archive a huge directory structure using zip/winzip on a live web server without putting additional load on the machine.

1 Click **Create** in the toolbar. The Automatic dialog box is displayed.

2 Enter the Process Name of the executable. The name should not include a path. For example, WinZip is WINZIP.EXE; the Microsoft C compiler is CL.EXE, etc.

3 Select the remote **Priority** from the dropdown box. The priority is usually idle, meaning that the process is the same priority class as the screen saver: it will only be activated if it does not compete with other processes for CPU power.

4 Select the **Process Affinity** box to divide processes amongst CPUs on a multiprocessor system (SMP, ASMP, etc.). The process will execute on the selected processors.

5 Click **Add** to save your work.

If there are entries in the above list, RemotelyAnywhere will scan the process list on your machine every ten seconds, looking for the process names you entered. If RemotelyAnywhere finds one and its priority class does not match the one specified, it will be changed to your preference.

Server Functions (Workstation and Server edition)

On the RemotelyAnywhere toolkit, select **Server Functions** to begin using RemotelyAnywhere's powerful FTP and Port Forwarding capabilities.

RemotelyAnywhere Server Edition comes with an extremely versatile FTP server. You can set up an unlimited amount of FTP servers on one computer, each with its unique IP address and port combination. You can create users and groups for your FTP server, or you can use the built-in Windows accounts for rights management.

If logging has been enabled via Preferences > Log Settings, the FTP Server will log all user activity to the main RemotelyAnywhere log file.

FTP Configuration, FTP Servers tab

Server Functions > FTP Configuration

The options for creating and managing the settings for your FTP servers, users and groups are arranged into three tabs. We will address the content of each tab in turn.

In order to create a new virtual FTP server on your machine you need to define at least one virtual FTP server on the FTP Servers tab of the FTP Configuration screen. If no FTP servers are defined then this screen will be blank, but for the New FTP server button.

Once you have defined a new server it will be shown in a table as in the screen shot above. You can delete a server by clicking on the red cross in the delete column to the right of a given server. The server can be started and stopped by clicking on the status indicator to the left of the virtual server.

A green check mark indicates that the server is running, and a red cross shows that it is stopped. This may be because it was stopped manually, it has been disabled or it was not able to start due to an error.

When you stop an FTP server on this screen its status will change to Disabled. This means that when you reboot the computer the server will not be started automatically. Likewise, if you start a stopped or disabled FTP server it will be Enabled and will start automatically on rebooting.

New FTP Server page

Server Functions > FTP Configuration > New FTP Server

To set up a new FTP server, click on New FTP server at the bottom of the FTP servers tab. This will bring up the New FTP server page.

You can specify the following settings for your new FTP server here:

Name	The name of the virtual FTP server. This is for reference purposes only. You can call your server whatever you want. This is what will be displayed on the FTP configuration screens, the login message from the FTP server, and so on.
TCP/IP port to listen on	The port in use by the virtual FTP server. The default is the standard FTP port, 21.
TCP/IP address to listen on	The IP address to use. You can select one item from the list. If you select All available interfaces the virtual FTP server will listen on all assigned IP addresses.

IP Filter	The IP Filtering drop down lets you specify the IP addresses from which to accept connections. By default, the clients can come from any IP address. The IP filtering engine is the same as that used by RemotelyAnywhere itself. Please see the section on IP filtering under Security for more information.
Port range for passive data transfers (inclusive)	This feature is relevant to passive mode data connections (PMDCs), also known as PASV mode in some clients. In such cases the data channels are opened by the client and the server communicates a PASV reply stating which address and port to connect to. However, servers behind firewalls and/or routers may have problems with the use of the reported address and/or port.

If the server is behind a firewall there may be a problem with the port on which PMDCs are accepted. By default the server tries the port (server port - 1). For example, the server will try port 20 if it is on the default FTP port of 21. If multiple clients were to try to establish simultaneous data connections this would fail and the server would query Windows for an arbitrary free port. Behind a firewall connection to random ports will not work. To avoid this, you can specify a range of ports on which to accept PMDCs. If these ports are open on the firewall then the connection will be established.

IP address of the network interface connecting to NAT router and External IP address of NAT router	By default the server examines the local IP address to which the client is connected and accepts the PMDC on that address. In a NAT environment this is likely to fail, because the server's local IP address is not externally visible for access from the Internet. To avoid this we can configure the FTP server to report a user specified IP address instead of the local one, although only for connections passing through the router. Thus we must specify the IP address of the network interface connecting to the router, and that to report to clients opening PMDCs through this interface. This should be the router's external IP address.
Subnet mask of network interface connecting to NAT router	In the above scenario a problem remains, which is that clients connecting from the LAN, possibly using the same network as the router would be redirected to open the PMDC using the external address. Most routers do not support this. Thus there is a third setting which allows you to specify the subnet mask of the network interface. Clients connected from the same subnet as the router will not be redirected. If the subnet parameter is not specified all connections from the interface will be redirected.

A typical FTP server setup behind an NAT router and a firewall

Imagine a machine on which RemotelyAnywhere has been installed with a local IP address of 192.168.1.2 (subnet mask 255.255.0.0) and the external IP address of 123.45.67.89 (belonging to a NAT router/firewall).

Set up an externally accessible FTP server

Server Functions > FTP Configuration > New FTP Server

Do the following in order to set up an externally accessible FTP server on this machine:

1 Create an FTP server within RemotelyAnywhere with the default settings, listening on all available interfaces, with the default FTP port of 21.

2 On the main configuration page of our new FTP server set the IP address of the network interface connecting to the NAT router as 192.168.1.2, the subnet mask to 255.255.0.0, and the external IP address to 123.45.67.89

3 Set the port range for passive data transfers to 5200-5299

4 Configure your router so that it forwards connections to 123.45.67.89:21 to 192.168.1.2:21 and make sure port 21 is open on the firewall.

5 Configure the router to forward connections to 123.45.67.89:5200-5299 to 192.168.1.2:5200-5299 and make sure that you open the 5200-5299 port range on the firewall.

6 Finish configuring your remaining FTP settings (security, users, etc.)

The server is enabled: If a server is enabled it will start automatically with RemotelyAnywhere; if disabled, you will need to start it manually.

Use implicit SSL encryption: Here you can set your new virtual FTP server to use implicit SSL encryption. Please note that if a server uses implicit SSL connections, it will accept these connections alone and clients must be configured accordingly. Most clients default to port 990 when creating implicit SSL FTP site entries.

Root directory	The root directory for the virtual FTP server. If you leave this field blank the drive list will be used as the root.
Resolve shell links	If you enable this option, shell links (.lnk files) pointing to directories will be displayed as directories, enabling you to use Unix and Windows 2000-style hard links.
Download bandwidth limit	The global download speed limit for the server. No matter how fast users are accepting data, the server will not send it any faster than the speed specified here.
Upload bandwidth limit	The global upload limit to the server. No matter how fast users are sending data, the server will not accept it any faster than the speed specified here.

When you have filled in the required data to define your new server, click **Apply**. The following FTP server configuration pages will become available as buttons at the bottom of the page:

- Security
- Windows Users
- Welcome
- ODBC

Security

Server Functions > FTP Configuration > New FTP Server > Security

Maximum number of simultaneous connections:	The maximum number of simultaneous connections to the FTP server. Setting it to zero means that there are no limits.
Maximum number of failed login attempts	If a user fails to log in with the specified number of tries the connection will be dropped.
Login timeout	The maximum number of seconds the user can take to log in.

No transfer timeout	The connection will be considered idle and will terminate after the specified number of seconds have elapsed on an open connection without a file transfer or directory listing.
Stalled transfer timeout	This is the amount of time a file transfer can spend without sending or receiving any data before it is considered stalled and thus terminated.
Allow keep-alives: FTP clients use various commands to keep the connection from being idle.	When enabled, FTP commands such as CWD, PWD or the ubiquitous NOOP will reset the No transfer timeout counter (described above). If disabled, only an actual file transfer or a directory listing will reset the counter.
Thread priority	You can select the priority of the threads servicing users for the FTP server. If you are running an FTP server on an otherwise busy web server it might be a good idea to set the priority to a lower value than the default Normal setting.
Allow unsecured FTP connections:	If this option is disabled the FTP client must support and utilize SSL.
Allow data connections to go to different IPs than that of the control connection	The FTP protocol uses two connections: The control connection and the data connection. The data connection is where all the raw data is sent, the control connection is used to send commands to the server and receive replies. Normally data connections are set up to the same IP address as that of the control connection, but in order to facilitate server-to-server file transfers it may be desirable to allow data connections to go to different IP addresses. If you are not using server-to-server transfers you can safely disable this option.
Quoted password changes	This determines whether the parameters of the SITE PSWD command are in quotes or simply surrounded by a space. (SITE PSWD oldpwd newpwd vs. SITE PSWD “oldpwd” “newpwd”). Which form is used depends on the Hosted FTP client.
Anti-hammer filter	This feature is similar to RemotelyAnywhere’s IP address lockout settings. By default if 4 bad logins occur from an IP address within one minute, the IP address will be locked out for one hour.
Number of invalid attempts before locking out:	You can change the number of bad login attempts from 4 to anything you want.
Reset invalid attempt count after	You can modify the time before the invalid attempt count is reset to zero.
Lock out for	You can choose the duration for which the user is locked out after the specified number of invalid attempts has been made.

Windows Users

Server Functions > FTP Configuration > New FTP Server > Windows Users

You can connect to the newly defined FTP server with any FTP client, but you are not able to log in until you have created a new FTP user and give them access to the server or you can allow any Windows user to access the new virtual FTP server.

The difference between FTP users and Windows users is simple: Windows users are pre-existing users in the Windows user database. Creating and managing them is done via the User Manager – either the HTML-based one included in RemotelyAnywhere, or the User Manager applet that comes with Windows. You cannot explicitly tell the FTP server the directories and files to which the user has access, but Windows access rights will be enforced. If a user can access a file below the server's root directory locally or over the network, he will be able to do so via FTP as well. If a user has no rights to a file or a directory, he will not be able to access the object with FTP either. This is enforced by the FTP server by having the thread servicing the user impersonate him towards the operating system as soon as login is complete.

FTP users, on the other hand, are created and managed within the FTP configuration pages. You can tell the server which files or folders the user can access, where he can read from, where he can write to. When an FTP user logs on, the thread servicing the user is executing under the LocalSystem account by default. This is rather undesirable, so you can specify an Windows user account on a per-server basis that will be impersonated when servicing FTP users. We will return to FTP users later in this chapter, when discussing the content of the FTP users tab.

The Windows account whose permissions are assigned to FTP users fields let you specify a username, domain and password for an existing Windows account. This is used when an FTP user logs on: the thread servicing the user will be impersonating this account towards the operating system. If you enter an incorrect username or an incorrect password here, the FTP user will receive a 'Login incorrect' message from the FTP server, even if he enters his credentials correctly.

To grant access to a Windows user or group on the FTP server, select its name in the list in the right pane and click the Update button. To revoke access from a user or a group, select its name in the list on the left, and click the Update button.

To list user accounts from a domain rather than from the Client, enter the domain's name in the Default domain field and click Update.

Now that you have granted access to a Windows user, you can use an FTP client to connect and log in to the FTP server. The user will have access to all files and directories below the server's root directory. However, on an NTFS file system, Windows access restrictions will apply. For example, if the user does not have the rights to read or write in a certain directory, he will not be able to do so via FTP either. The FTP server enforces this in a very effective way: the thread servicing the user will impersonate him towards the operating system as soon as login is successful.

Welcome

Server Functions > FTP Configuration > New FTP Server > Welcome

The Welcome page allows you to view and modify the welcome message your users see:

The first message the user will see when they log in will be the RemotelyAnywhere welcome banner. If you do not wish to let the outside world know which FTP server you are running, you can disable this via the checkbox at the bottom of this window.

The next message the user will see is by default:

Welcome to the _!SERVER_NAME!_ FTP server,

running on _!OS_VERSION!_.

The server has been up for _!SERVER_UPTIME!_.

Data downloaded: _!BYTES_DOWN!_

Data uploaded: _!BYTES_UP!_

Sessions serviced: _!TOTAL_LOGINS!_1

You can change this to anything you like, or leave it blank if you would prefer no login message for your users. If you disable both the banner and the welcome note, the FTP Server will just send 'Welcome' whenever somebody connects to the FTP port. This is because the FTP specification requires a server to send a code and some text when a connection is established.

By default, the post-login message is:

Welcome, _!USER_NAME!_, to _!SERVER_NAME!_.

Your last successful login was at _!LAST_LOGIN!_.

Good logins so far: _!GOOD_LOGINS!_.

Bad logins so far: _!BAD_LOGINS!_.

You have uploaded _!BYTES_UP!_ and downloaded

_!BYTES_DOWN!_ in your previous sessions.

The final line (User logged in) cannot be customized, as this is a requirement of FTP protocol. The rest you can change to suit your preferences, or leave blank.

The following variables can be inserted into the welcome messages, and they will be automatically replaced with their corresponding values:

_!SERVER_NAME!_	The name of the FTP server.
_!OS_VERSION!_	The operating system and its version.
_!SERVER_UPTIME!_	The amount of time the server has been up.
_!BYTES_UP!_ and _!BYTES_DOWN!_	The amount of data uploaded and downloaded. These variables behave differently when used in the pre-login or post-login messages. In the pre-login message, they represent a server-wide value, while in the post-login message they represent the amount of data transferred by the user.
_!TOTAL_LOGINS!_	The number of successful logins to the FTP server. Only valid in the pre-login message.
_!GOOD_LOGINS!_ and _!BAD_LOGINS!_	The number of logins and unsuccessful login attempts. Only valid in the post-login message.

`_!LAST_LOGIN!_`	The last successful login by the user. Only valid in the post-login message.

These welcome messages are server-wide settings, and apply to all users and groups. When you specify a welcome message for an FTP group or an FTP user, it will override the post-login message defined here.

ODBC Access

Server Functions > FTP Configuration > New FTP Server > ODBC

The ODBC option allows you to specify a database as a source of user information. With the ODBC Data source settings page you can set up a database to contain user information. This can be any database type: Oracle, SQL Server, Microsoft Access, or even a plain text file. You need to create an ODBC data source that refers to this database so that RemotelyAnywhere can access it. The data source must be a so-called Machine Data Source, as this is the only ODBC source available to processes running in the system context.

When you have your database and ODBC data source ready, we advise you to test it by querying it with a tool that supports ODBC queries, such as a spreadsheet program.

You should have all user information available in one table. If you already have a user database and user information is in separate tables, you should set up a query within your database that contains all user-related fields. RemotelyAnywhere only reads from the database.

Suppose that you have a user database in a data source called FTPUsers. The user information is present in a database table called Users. A database user called ra is able to read from the Users table. You should also supply the password for this user in the above form.

The Users table can have any number of fields in any order, but the above figure assumes that these fields are present:

`login`	(character string)
`password`	(character string)
`homedir`	(character string)
`quota`	(integer, in bytes, optional)
`downstream`	(integer, speed in bytes/sec, optional)
`upstream`	(integer, speed in bytes/sec, optional)
`disabled`	(integer, zero or non-zero, optional)
`maxconns`	(integer, optional)
`maxconnsperip`	(integer, optional)
`welcome`	(character string, optional)

The only three mandatory fields are login, password and homedir. The login and password fields contain the user's login name and password, in clear text. The homedir field must contain the user's home directory, which can be an absolute path (such as z:\ftp\users\~john) or it can be relative to the server root (such as /users/~john).

Notes:

- Users have full access to their home directory, but have neither read nor write permissions outside of it.
- The quota field will not let the user store more data in his home directory and its subdirectories than the number of bytes specified here.
- The downstream and upstream fields restrict download and upload speed. They are optional, and should be an integer number specifying bytes per second.
- The disabled field should be an integer. When it's non-zero, the user is disabled and cannot log in.
- The maxconns field specifies the maximum simultaneous connections to this FTP server for a user.
- The maxconnsperip field specifies the maximum simultaneous connections per unique IP address for a user.
- The welcome string, if used, should contain a custom welcome message for the user.

FTP Configuration, FTP Users tab

Click **Server Functions > FTP Configuration > FTP Users** to view, create or modify your existing FTP users. These are only defined in RemotelyAnywhere and unlike Windows users they do not exist outside of the FTP server.

As on the FTP Servers page, users are shown in a table, with a delete column to the right.

New FTP User

To create a new FTP user click on the **New FTP user** button on the FTP Users tab of the FTP configuration page (**Server Functions > FTP Configuration > FTP Users > New FTP user)**

Enter the desired username and password in the above dialog. You can also specify upload and download speed limits for the user. If not set to zero (meaning disabled) these options override the global FTP server settings.

You can also enable or disable their ability to change this password, and select an IP from the IP filter drop down menu. Click **Apply** to create the user.

When you create a new user the following options become available:

- Groups
- Permissions
- Ratio
- Disable
- Home/Quota
- Max Connections
- Welcome
- Permissions Report

The newly created user cannot log in yet: you have to assign permissions to them for an FTP server and a path so that the user is able to use the account.

To allow anonymous access to an FTP server, you should create an FTP user called anonymous. This user account is special: no password checking is done upon login. You can assign permissions to the anonymous user account as you would to any other user. By default, the newly created anonymous user has no rights to any virtual FTP server defined.

FTP Groups

Server Functions > FTP Configuration > FTP Users (individual user) **> Groups**

This page lets you specify the FTP groups to which the user belongs.

Selecting a group that the user is a member of and clicking the Update button will remove the user from that group. Selecting a group that the user is not a member of and clicking the Update button will add the user to that group.

The **Back** button takes you back to the main user editing page.

Permissions

Server Functions > FTP Configuration > FTP Users (individual user) **> Permissions**

This page lets you edit users' access to directories. To grant access to a directory on a server, select the virtual server from the server list, select the type of rights you wish to assign to the user, enter the path to the directory and click the **Update** button.

The path you specify can be a full path, containing a drive letter, or a path relative to the server's root directory. If you assign rights to a path that is not within the server's root directory, the setting will have no effect at all.

The following rights are possible:

- L – Show directory contents: Allows the user to list the contents of the directory.
- R – Read file: Download files from the directory.
- C – Create subdirectories: Create new directories in the directory.
- D – Delete/rename file: Delete or rename a file or a directory. Also required to be able to overwrite files.
- W – Create/modify file: Create a new file and/or write data to it.
- Full access: All of the above.

The above settings let the user access FTP Server 1 – he has full control over the contents of the server. These rights only apply to the root directory of the server and all directories below that. The user also has list, read and write access to the c:\work directory on FTP Server 2. However, the user has no rights at all to the c:\work\java directory on FTP Server 2. The user has no rights at all on FTP Server 3, meaning he cannot even log on.

The rights you specify for a directory are automatically inherited by its subdirectories, unless you specify different rights for them.

The following method is used when checking access rights to a directory:

1 The current virtual server's access list is enumerated for the current user.

2 When the directory closest to the directory in question is found, the access rights specified for that directory is used. For example, if the user has LRW rights for C:\Work, he has LR rights for C:\Work\CPP, and the directory in question is C:\Work\CPP\Project1, only LR rights are returned – meaning that the user can only list and read files, but not write to them.

3 If a Windows user is specified for the server to run FTP accounts under, further Windows-enforced restrictions might apply, based on file system permissions.

You can also make the user member of one or more groups, and these groups can also be members of one or more groups. For an explanation of this scenario, please see the FTP Groups section of this document.

Ratio

Server Functions > FTP Configuration > FTP Users (individual user) **> Ratio**

This Ratio settings page lets you edit the upload/download ratio settings for the user.

The upload and download ratios let you control how much data the user has to upload before being allowed to download anything.

If the Upload ratio is set to 1, and the Download ratio is set to 5, the user can download 5 bytes for every byte uploaded. If it were vice-versa, the user would have to upload 5 bytes to be able to download one. You can enter any positive integer number in either of these fields.

There are four possible settings for the Ratio type:

None	The user is a normal user, and can download any file he has read access to, without having to upload first.
Per session	When the user logs in, his counters are zeroed. Should he lose connection while uploading or downloading, any remaining credits he has will be lost.
Per user	The user's credits are remembered over sessions. It is not recommended if you want several users to share the same account.
Per IP	Even if the user loses connection, his credits are remembered, if he logs in again from the same IP address. This does not cause a problem, even if the user account is shared by hundreds of concurrent users.

The Per IP ratio information expiration time setting allows you to have the per-IP credits expire after a certain time. If the user logs back from the same IP address after not visiting the server for the specified time, he will have to start building up credits again.

The ratio setting applies to all virtual servers.

To let the user download files without uploading, you can specify a starting credit. The amount given is in kilobytes – the user will be able to download the specified amount of data without uploading.

Disable

Server Functions > FTP Configuration > FTP Users (individual user) **> Disable**

The Disable page lets you explicitly disable (or ban) a user on a virtual FTP server. Disabled users cannot log in, even if they have rights on an FTP server. You can also disable a connected user from the FTP status page.

Home/Quota

Server Functions > FTP Configuration > FTP Users (individual user) **> Home/Quota**

The Home/Quota page lets you specify home directories for the user. A home directory is basically the entry point for a user on an FTP server. When the user logs in, he will find himself in the directory you specify. If no home directory is specified, he will be logged in to the server's root directory. The user can move out from his home directory if he has rights to an outside directory.

You can use a full path, starting with a drive letter, when specifying home directories – or you can enter a relative path to the server's root directory. Home directories specified above the server's root directory are disregarded.

You should make sure that the user has rights to his entry point on the server – either to his home directory, or if the home directory is not specified, to the root directory of the server. If the user has no rights to the entry point, he will not be able to log in.

You can specify quotas for your users. Quotas are only enforced on home directories, and apply to all files contained in the home directory and its subdirectories. If a user has rights to upload files outside of his home directory, he will be able to do so without restrictions – quotas only apply to the home directory and its contents.

Since Windows does not support disk quotas for user accounts, RemotelyAnywhere has to enforce them. When a user starts to upload a file, the FTP server quickly scans the contents of the directory to determine if the user is below or above the quota. If the quota is not exceeded, the upload can be started – however, the FTP server will interrupt the transfer as soon as the file being uploaded starts to exceed the specified quota.

Home directory quotas are entirely optional, by leaving the field empty you choose not to limit the amount of data that can be stored on the server by the user.

Maximum Connections

Server Functions > FTP Configuration > FTP Users (individual user) **> Maximum Conn.**

You can specify the maximum number of simultaneous connections for a user account.

By default, a user account can be used to log in any number of times, until exhausting the maximum number of connections for the virtual FTP server, or exhausting the resources of the computer.

Simply select the server on the right, enter the number of maximum simultaneous connections in the Count field and click Apply. To remove a limitation, select it in the list on the left and click Update.

You can also limit the number of simultaneous connections for the user from a computer or IP address. The Per IP field serves this purpose. When left blank, or a zero is entered, this limitation is disabled. If you enter a numeric value, a single computer can be used to log in that many times with the account.

It is a good idea to limit certain user accounts (for example the Anonymous account) this way. An overall maximum connection limit ensures that the server cannot be overloaded by thousands of Anonymous users, and a Per IP limitation makes sure that no single user can take up all available connections.

Welcome

Server Functions > FTP Configuration > FTP Users (individual user) **> Welcome**

You can compose a custom welcome message for the user in this window.

```
Welcome, _!USER_NAME!_, to _!SERVER_NAME!_.

Your last successful login was at _!LAST_LOGIN!_.

Good logins so far: _!GOOD_LOGINS!_.

Bad logins so far: _!BAD_LOGINS!_.

You have uploaded _!BYTES_UP!_ and downloaded

_!BYTES_DOWN!_ in your previous sessions.

_!QUOTA!_
```

Messages specified here override any post-login message specified for the virtual FTP server. In this case, messages specified for any groups the user belongs to will be disregarded as well. See the equivalent section on welcome messages above for the available variables.

Permissions Report

Server Functions > FTP Configuration > FTP Users (individual user) **> Permissions report**

The permissions report can be retrieved for any FTP user. It will list all FTP servers, and all the rights a user has on the given server.

FTP Configuration, FTP Groups tab

Click **Server Functions > FTP Configuration > FTP Groups** tab to control the resources available to your FTP users. As on the FTP Servers and Users pages, groups are shown in a table, with a delete column to the right.

To add a new FTP Group, click **New FTP Group**.

General Group Settings

You can make a group a member of another group, thus bringing in any permissions or restrictions for its member users from the parent group.

Selecting a group in the Member of list and clicking the Update button will remove it from that group. Selecting a group in the Not member of list and clicking the Update button will add the group to it.

You can also specify a welcome message for a group. Whenever a member logs in, he will see this message instead of the server's general welcome message.

Permissions

Server Functions > FTP Configuration > FTP Groups (individual group) **> Permissions**

With this page you can specify the rights to servers and directories. It works very much like the FTP User Rights page. For a basic description please see the appropriate section of this document.

There are some scenarios, however, that might require further explanation. Let us examine the following, rather complicated scenario:

- User1 is member of Group1.
- Group1 is member of Group2 and Group3. On the membership display, Group2 is shown first and Group3 is shown second.
- User1 is granted LR access to C:\, and LRW access to C:\Work.
- Group1 is granted full access to C:\, LR access to C:\Work, and LRWD access to C:\Work\CPP.
- Group2 is granted LR access to C:\Work\CPP and full access to C:\Work\CPP\Project1
- Group3 is granted LR access to C:\Work\CPP\Project1

So, what exactly can User1 do in the aforementioned directories?

- C:\ He has LR rights. He was explicitly granted LR rights to this directory, and this overrides anything else.
- C:\TEMP He has LR rights. He was explicitly granted LR rights to the directory closest to this one (C:\), and no groups that he is a member of, directly or indirectly, specify anything else for the C:\TEMP directory.
- C:\Work LRW rights again. See the first case.
- C:\Work\CPP LRWD, because Group1 has LRWD rights. Even though Group2, which Group1 is a member of, specifies LR access for this directory, Group1 is the least indirect object that specifies actual rights for the directory. Group2 is one more indirection away, with User1 only being a member of it because he is a member of Group1, and is therefore overridden by Group1.
- C:\Work\CPP\Project1 Full access. Both Group2 and Group3 are two indirections away, they both specify access rights to the same directory, so the deciding factor between Group2 and Group3 is that Group2 is the first one in the list on the membership display of Group1.

FTP Status

When you click on FTP Status under Server Functions in the menu you can view the current status of each of your virtual FTP servers.

For each server, it provides a listing of all current connections and their current activity. The fields in the list are:

Icon	This field shows a small icon, representing the current status of the connection. A green checkmark indicates a ready, or idle connection. An hourglass indicates a connection currently in the process of logging in or becoming ready. An up or down arrow indicates uploading or downloading.
User name	The name of the user associated with the connection. For Windows users, it is in an AUTHORITY\ACCOUNT form. For FTP users, it's simply the username. For connections not yet logged in, it's N/A.
Control address	The IP address of the FTP control connection.

Downloaded Bytes	downloaded during this connection.
Uploaded Bytes	uploaded during this connection.
Data address	The IP address of the FTP data connection, if applicable.
Path	The path and name of the file currently being uploaded or downloaded, if any.
Speed	The speed of the upload or download process.
Bytes left	The amount of data left from the transfer operation. Only applies to download transfers, since the FTP protocol does not let the server know the size of the file being uploaded in advance.
Est. time left	The estimated time remaining from the transfer operation. Only applies to download transfers, for the same reason as the previous item.
Kick	This button kicks the user out – in other words, terminates the connection.
Ban user	This button kicks and then bans the user from the FTP server. Only applies to FTP users, and not to Windows users. The user's properties will show him as disabled on the server he was banned from.
Ban user IP	This option first kicks the user from the server in question, then adds an IP filtering rule to the user object that will prevent him from logging in again from the IP address in question. He will have the ability to log in from other IP addresses (depending on IP filtering setup) and the IP address will only be disabled for this user.
Ban server IP	This button kicks the user, and then adds an IP filtering rule to the server object that will cause the server not to accept connections from the IP address in question. The user will be able to log in from other IP addresses.
Anti-hammering	Information for each server is also shown, where applicable.
IP address	The address the attempted connection came from.
Expires at	The time when the information will be discarded – users will be able to establish connections from the IP address at this time again.
Bad logins	Number of bad logins from the IP address.
Delete	Clicking this button will remove the anti-hammering information from the FTP server's memory, thus making the IP address available for logins, had it been locked out.

The **Refresh** button refreshes the contents of the screen to reflect any changes, while the **Back** button goes back to the main FTP settings screen.

FTP Statistics

If you click **FTP Statistics** under Server Functions in the menu you can view per-server and per-user statistics, such as the last login, number of logins, bytes sent and received, etc.

The red button labeled **Reset for servers and FTP users**, or **Delete for Windows users** will reset or delete statistics kept on that object.

Port Forwarding Server (RemotelyAnywhere Server Edition only)

RemotelyAnywhere Server Edition also comes with Port Forwarding Server. This allows you to forward one or more TCP or UDP ports on one computer to another so that separate networks can be bridged.

Before getting into the details of how you would configure your Port Forwarding Server (PFS) we will look at how it works. Picture the following scenario:

You have a Local Area Network (LAN), connected to the Internet with a firewall / proxy server. The computers on the LAN all have non-Internet IP addresses, and they connect to the outside world via the proxy server.

If you have RemotelyAnywhere installed on any computer on the LAN — for example, the fileserver — you would be able to access it from within the LAN without any problems. However, it is not accessible from the Internet.

If you set up RemotelyAnywhere Server Edition and PFS on the firewall, so that a certain port (say, 3000) on the firewall is forwarded to the fileserver's IP address and RemotelyAnywhere port (2000 by default), accessing port 3000 on the firewall will let you access RemotelyAnywhere on the fileserver - both from within the LAN and from externally.

Server Functions (Server edition only)

Port Forwarding Configuration

Server Functions > Port Forwarding Configuration

In order to understand this feature we will look at a possible scenario:

- The firewall's Internet IP address is 145.236.120.227
- The firewall's LAN IP address is 192.168.0.2
- The fileserver's LAN IP address is 192.168.0.10
- RemotelyAnywhere is installed on both computers, and is listening on port 2000.

The IP addresses used in the foregoing are for demonstration purposes only.

What we need to do is simple: map port 3000 on the firewall computer to port 2000 on the fileserver (dns name: mailserver.company.com).

- Having called up the Port Forwarding Configuration screen from the menu, you can now add a new rule by clicking **Create forwarding rule**.
- The **Incoming Protocol** field will be TCP. Other protocols (SSL, CSSL) will be discussed later. The Incoming IP Address can be "All available", meaning that the port will be forwarded from all IP addresses of the firewall. If you want to use a single IP address instead of all assigned ones, select it here. The Incoming Port can be anything not already in use on the computer – we will use the value 3000 for now.
- The Outgoing Protocol will be TCP. The Outgoing IP Address will be fileserver.company.com (or the actual IP address of the host), and the Outgoing Port will be 2000.
- The **Defer** and the **Timeout** values can be left to their defaults.
- The **Description** field lets you specify a remark associated with the port forwarding item. This will be displayed on the main screen.

- If you fill out the dialog and click **Add**, the item will be listed on the main PFS screen:

Your first port forwarding item has now been configured.

Advanced Options

Server Functions > **Port Forwarding Configuration** (individual rule) > **Modify Rule**

You can edit a port forwarding item by double clicking it, or by selecting on it and clicking on the modify rule button.

You can specify IP address restrictions for the item from the IP filtering drop down. This works exactly like the RemotelyAnywhere IP Address Filtering feature, only it restricts incoming connections to the corresponding port forwarding item only. For more information, please see **Security** > **IP Filtering**.

Timeout	This setting lets you specify how long the PFS will hold a connection open with no data going through it in either direction. When the amount of time specified here is reached and the connection is idle, both ends of the connection will be closed gracefully.
Defer	This setting lets you specify a timeout value for a special condition. When one end of the connection has been closed, but the other is still open, PFS will wait this much time for the open end of the connection to be closed. It will then close the connection itself.
Incoming and Outgoing Protocol	These fields let you specify SSL or CSSL as well as TCP. To translate SSL connections to TCP or TCP to SSL, and thus behave as an SSL proxy for applications that are not SSL-enabled, simply set one end to SSL and the other end to TCP.

There are situations when SSL encryption would be a very nice thing to have, but neither the client nor the server support it. In this case, you can use two installations of RemotelyAnywhere: one to translate the connection from TCP to SSL, the other to translate it back from SSL to TCP.

Let us suppose that you are using a laptop with a dialup account, and your email software does not support SSL. Also suppose that your corporate mail server does not support SSL either. If you still want to keep your email secure, you can install RemotelyAnywhere both on your laptop and on the email server, and set up a port forwarding item on both computers.

On your laptop, you would need to do the following:

- Create a port forwarding item with the incoming IP address as 127.0.0.1 (the loopback address), the incoming port as 3110, the incoming protocol is TCP. The outgoing IP address or host name would be set to that of your email server, the outgoing port would be set to 3110, and the outgoing protocol would be SSL.
- Change your email client's preferences so that the POP3 server is 127.0.0.1 and the port is 3110.

On the mail server, you would need to create a port forwarding item with the incoming IP address set to your mail server's Internet IP address, the incoming port set to 3110, and the incoming protocol set to SSL. The outgoing IP address would be the same (the mail server's Internet IP address), the outgoing port would be 110 (the standard POP3 port), and the outgoing protocol would be set to TCP.

If you performed the above three steps, starting up your email client and checking for mail would actually go through two port forwarding servers; the first one being on your own computer, encrypting all data before it's sent to the mail server. The mail server's port forwarding server would receive the encrypted data, and decrypt it

before sending it on to the actual mail server software. Data flowing in the other direction would be also seamlessly encrypted and decrypted.

However, if you have two RemotelyAnywhere Port Forwarding Servers talking to each other, you could also utilize the proprietary CSSL protocol instead of using plain SSL. CSSL, which stands for Compressed SSL, would also seamlessly compress and uncompress your data as well as encrypt and decrypt it - to keep to the above example, making your mail arrive much faster over a dialup connection. Also, to properly finish the laptop/email example, you would also have to create one additional port forwarding item on both computers for the SMTP protocol that is used to send email as opposed to receiving it. This runs on port 25 by default.

Port Forwarding Status

Server Functions > Port Forwarding Status

If you have configured your Port Forwarding Server as in the examples above, you will be able to view the status of your Port Forwarding connections by clicking on Port Forwarding Status under Server Functions in the menu.

Active Directory

Server Functions > Active Directory

This is an Active Directory browser. It lets the user connect to and browse through the various elements in the Windows domain's active directory tree. It's usually employed as a simple system info tool.

Scheduling & Alerts menu

Go to Scheduling & Alerts on the RemotelyAnywhere toolkit to make use of RemotelyAnywhere's scripting capabilities and work with email alerts that are triggered when certain events occur on the Host.

System Monitoring

On the RemotelyAnywhere toolkit, select **Scheduling & Alerts > System Monitoring** to begin setting up rules (scripts and alerts) that will run on the Host.

If you have C or C++ programming experience, and a basic understanding of HTML, you will be able to create scripts without much difficulty. See Scripting for more information, or for a complete reference of the scripting language used by RemotelyAnywhere, see *The Small Booklet* at https://secure.logmein.com/smalldoc.pdf.

Note: *A condition and an associated action are known as a rule. Rules provide a mechanism for monitoring certain aspects of a computer system. The system administrator can create scripts defining the behavior of the system monitoring module. To view sample scripts, click* ***Edit Rules*** *on the System Monitoring window.*

Email Alerts

On the RemotelyAnywhere toolkit, select **Scheduling & Alerts > Email Alerts** to begin setting up email alerts for a Host.

Note: *Email alerts will not work until you configure your SMTP server under* ***Preferences > Network > SMTP Settings****.*

Once you have set your preferences, you can configure email alerts according to the following criteria:

Event Log name	The event log to watch.
Type	Optional. The type of alert. Can be chosen from the drop-down list.
Event Source	Optional. Type in the source of the message you want to be alerted on. For example, Security, Disk, etc.
Event Category	Optional. Type in the category of the message as it would appear in the event log.
Event ID	Optional. Type in the event code as it would appear in the event log.
Email	The email address to which the notifications are sent. You can only specify a single email address per entry. Specify a group alias if there will be multiple recipients.

Task Scheduler

On the RemotelyAnywhere toolkit, select **Scheduling & Alerts > Task Scheduler** to view and manage the Windows Scheduled Tasks associated with a Host. This feature provides functionality otherwise available using the Windows Scheduled Tasks System Tool.

To add a new scheduled task, click **Create New Task** on the toolbar.

To remove a task from the list, select it and click **Delete** on the toolbar.

To check and modify the attributes of your existing tasks, select an item and click **Change Attributes** on the toolbar. These attributes are organized under three tabs, with the headings Task, Setting, and Schedule. The available options match those found in the Windows Scheduled Tasks System Tool.

***Note**: RemotelyAnywhere supports only those Windows Vista Task Scheduler functions that are compatible with Windows XP and Windows Server 2003.*

Scripting

Select **Scheduling & Alerts > Scripting** to work with RemotelyAnywhere scripts. RemotelyAnywhere provides an extension interface in which you can create custom scripts that interact with the system, RemotelyAnywhere and the user.

- To execute a script, click its **Name**.
- Click **Edit** next to any script to open the script's source code. Edit and compile the script as required.
- Click **Delete** to remove the script.
- To create a new script, type a **Name** for the new script and click **New**. Edit and compile the script in the resulting window.
- You can create three kinds of scripts:
  - Interactive
  - Quiet
  - Hybrid
- If you have C or C++ programming experience, and a basic understanding of HTML, you will very quickly be creating your own scripts.
- For a complete reference of the scripting language used by RemotelyAnywhere, see *The Small Booklet* at https://secure.logmein.com/smalldoc.pdf.

Interactive scripts

Interactive scripts display their output on HTML pages within the RemotelyAnywhere frameset. An example for an interactive script is the File.sma script, which is installed with RemotelyAnywhere. These scripts do not have to return a value from their main function. They communicate with the user via the `htmlBeginOutput()`, `htmlEndOutput()`, and various other `html***()` functions.

Quiet scripts

A Quiet script is one that is usually called from the System Monitoring script. It does not display output. A return value is required at the end of the main function.

Hybrid scripts

Hybrid scripts, on the other hand, are executable interactively and also return a value at the end of their main function. An example for a hybrid script is the WatchProcess.sma file, included with RemotelyAnywhere. Hybrid scripts check the return value of the `htmlBeginOutput()` function, and, if it is a zero value, the script is run in non-interactive mode. That is, it is invoked from the System Monitoring script, via the `Small()` function call.

Performance Info menu

The RemotelyAnywhere toolkit **Performance Info** menu allows you to access performance data collected by RemotelyAnywhere.

CPU Load

On the RemotelyAnywhere toolkit, select **Performance Info > CPU Load** to view CPU utilization with various sampling rates.

Note: *RemotelyAnywhere may require time to gather performance data for these graphs. The Sampling Frequency for the each graph is shown in the format D.HH.MM.SS. If you move your mouse over a line in one of the graphs, the tooltip that pops up tells you exactly when the sample was taken.*

The first graph has a two second sample rate, so the graph spans less than an hour. Use it to see what is happening right now on the Host machine. The other graphs are set to ten seconds and five minutes.

Note: *If you have multiple CPUs, you will see separate graphs for each, as well as a set of graphs showing you the total CPU load.*

The list at the bottom shows the **Most CPU-Intensive Processes** – those that take up most of the processor time. This list is weighted, so younger processes that take up a lot of processing time come closer to the top. If you see a spike on the first graph you can check the **Most CPU-Intensive Processes** list to find out which process is causing the problem.

Click the **Name** of any item in the list to display the relevant data on that process, organized under six separate tabs (General, Threads, Services hosted, DLLs, Open Files, and Registry Keys In Use).

Memory Load

On the RemotelyAnywhere toolkit, select **Performance Info > Memory Load** to view four graphs similar to those on the CPU Load page. These display the memory utilization on the machine. The information is view only.

You can switch between the following:

- Memory Load
- Physical Memory Load
- Commit Memory Load

Disk Space

On the RemotelyAnywhere toolkit, select **Performance Info > Disk Space** to view graphs displaying disk space utilization per logical disk for the Host. The **Sampling Frequency** for the each graph is shown in the format D.HH.MM.SS (days, hours, minutes, seconds).

Drive & Partition Info

On the RemotelyAnywhere toolkit, select **Performance Info > Drive and Partition Info** to view details regarding all physical drives and their partition tables on the Host. These data are organized onto two separate tabs for **Physical Drives and Partitions** and **Logical Drives**.

Click on any listed **Drive** to manage the drive using File Manager.

Open TCP/IP Ports

On the RemotelyAnywhere toolkit, select **Performance Info > Open TCP/IP Ports** to view a list of all open IP endpoints on the computer.

1 Specify the type of port(s) you want to view

   a listening ports (ports that are listening for connections)

   b connected ports (ports that have been connected to another computer)

   c everything else (ports in various stages of being connected and disconnected)

2 Select **resolve IP addresses** to have RemotelyAnywhere resolve IP addresses appearing in the list of Local names. This can take a considerable amount of time to process.

3 Click **Continue** to generate the list.

4 Once you have generated the list, you can change the ports you are viewing using the boxes on the toolbar and clicking **Refresh**.

Network Load

On the RemotelyAnywhere toolkit, select **Performance Info > Network Load** to view network traffic information.

1 Click the name of any listed network to view traffic for a specific network.

or

2 Click **Inbound Network Traffic** or **Outbound Network Traffic** to see total network traffic.

3 Switch between Inbound and Outbound Traffic and between Total Traffic and Individual Traffic using the drop-down lists. Click **Refresh**.

4 You can set the **Maximum Inbound Bandwidth** to a kilobits per second value.

Open Files

On the RemotelyAnywhere toolkit, select **Performance Info > Open Files** to view a list of all files currently open on the Host, along with the names of associated processes. The information is available on several pages. Use the toolbar to explore the data.

Click on any process to view details. To end a process, click **End Process** on the toolbar.

Registry Keys In Use

On the RemotelyAnywhere toolkit, select **Performance Info > Registry Keys In Use** to view a list of registry keys currently open on the Host. Click on any process to view details. To end a process, click **End Process** on the toolbar.

DLLs In Use

On the RemotelyAnywhere toolkit, select **Performance Info > DLLs in Use to** view a list of all currently loaded dynamic link libraries and the processes that use them on the Host.

Click on any process to view details. To end a process, click **End Process** on the toolbar.

RA Connections

On the RemotelyAnywhere toolkit, select **Performance Info > RA Connections** to display all current connections served by RemotelyAnywhere, including IP address and local name of the Host, the type of connection and the name of the Windows user associated with the connection. The connection type can be one of the following:

(Browser) HTTP	A typical browser connection requesting a page.
Remote Control	A Java remote control client.
Upload Status Viewer	A Java applet displaying the progress of a File Manager upload.
Performance Viewer	The Java applet above the menu, displaying CPU and memory utilization.

Telnet/SSH Connections

Performance Info > Telnet/SSH Connections

Selecting this option will display all current Telnet/SSH connections currently being served by RemotelyAnywhere. It will display the IP address, Host name, type of connection, and the name of the Windows user associated with the connection.

Installed Applications

On the RemotelyAnywhere toolkit, select **Performance Info > Installed Applications** to view a list of applications installed on the Host.

The data are for information purposes only, but in addition to the program name and version you will be able to see the Publisher, Installation Directory and frequency of usage, if this information is available. If you roll over a listed application you may also be able to see other data such as estimated size, the installation source, registration data, and the time and date it was last used.

Loaded Device Drivers

Select **Performance Info > Loaded Device Drivers** to view a list of loaded device drivers. This is view-only information.

Security menu

Access Control

On the RemotelyAnywhere toolkit, select **Security > Access Control** to define who can access RemotelyAnywhere.

Users

Security > Access Control

The upper portion of this page lists users with access to RemotelyAnywhere.

Click **Add** to create a new user or group.

Click **Delete** next to any entry to remove that user or group from the access list.

Settings

Security > Access Control

Allow full control to administrators	This is enabled by default. It adds Full Control permission to all administrators of the computer. If you turn it off, only users explicitly granted permission to use RemotelyAnywhere will have access.
NT LAN Manager Authentication	RemotelyAnywhere supports Windows Challenge/Response type authentication. You must use Internet Explorer to take advantage of this feature. You need not worry about exposing your password to eavesdroppers if you are using HTTPS to secure all communications between your browser and RemotelyAnywhere.
Save user name in a cookie	You can configure RemotelyAnywhere to remember your user name in a cookie.
Do Not List Domains on Logon Screen	When logging on to a Host, users will be prompted to enter a username and password for a computer on a given domain. By default, RemotelyAnywhere provides a list of active domains in the **Log on to** field. When the **Do Not List Domains on Logon Screen** box is selected, the list of active domains will not be displayed, thus forcing the user to type the exact name of the chosen domain in the **Log on to** field. This provides an extra layer of security by forcing would-be hackers to know exact domain names.

Adding a New User: Access Control Permissions

Security > Access Control

Permission	R(ead)	W(rite)	D(elete)
Login	Allows the user to log into LogMeIn. By revoking this permission you can temporarily disable a user's access to LogMeIn without having to clear any other permission.		
Configuration	Allows the user to view LogMeIn Preferences. You must be an Administrator to change this setting.	Allows the user to change LogMeIn Preferences. You must be an Administrator to change this setting	
Scripts	Allows the user to view and execute monitoring and maintenance scripts.	Allows the user to edit, compile, enable and disable monitoring and maintenance scripts.	Allows the user to delete monitoring and maintenance scripts.
Event Viewer	Allows the user to read event log entries.		Allows the user to clear and backup event logs.
File System	Allows the user to list drives, folders and files; read and download files; view file attributes; shared folder information and access control lists; and use File Manager.	Allows the user to copy, paste, rename and edit files; create and share folders; edit attributes and access control lists	Allows the user to delete files; remove shares; and disconnect users from shared files.
Registry	Allows the user to view the registry keys and values; and list installed applications.	Allows the user to create and rename registry keys; add and change registry values.	Allows the user to delete registry keys and values.
Performance Data	Allows the user to view system performance data, graphs and detailed hardware information.		
Processes	Allows the user to view running processes, services and drivers; list DLLs and objects that these processes use; and view scheduled tasks.	Allows the user to change process priorities and service startup parameters; control services; create and modify scheduled tasks.	Allows the user to kill running processes and services; delete scheduled tasks

Permission	R(ead)	W(rite)	D(elete)
Reboot		Allows the user to restart the LogMeIn service; initiate and schedule system reboots; and hard-reset the computer.	
Remote Control	Allows the user to view and monitor the remote desktop; and use the chat applet.	Allows the user to view and interact with the remote desktop.	Allows the user to take control over the remote desktop without the interactive user's permission.
Whiteboard		Allows use of the Whiteboard during remote control.	
Chat		Allows the user to chat with the person in front of the computer	
User /Group Accounts	Allows the user to list and view user groups and accounts.	Allows the user to create new user groups and accounts; and modify their details.	Allows the user to delete user groups and accounts.
System Configuration	Allows the user to list and view system configuration data, such as environment variables, virtual memory settings, drive and partition information and network adapters.	Allows the user to modify system configuration data, such as environment variables, virtual memory settings, drive and partition information and network adapters.	Allows the user to delete environmental variables.
SSH Shell	Allows the user to use a command prompt via SSH.		
SSH Port Forward	Allows the user to use port forwarding via SSH.		
SSH Privileged Port Forward	Allows the user to use port forwarding for ports below 1024 via SSH		
SCP	Allows the user to use SFC (Secure File Copy) via SSH.		

Permission	R(ead)	W(rite)	D(elete)
SFTP	Allows the user to use SFTP (Secure File Transfer) via SSH.		
Command Prompt	Allows the user to use the secure LogMeIn telnet applet to open a remote command prompt.		
Telnet	Allows the user to use any unsecured telnet client to open a remote command prompt.		
Mini Meeting			Allows the user to create and delete Mini Meeting invitations.

Other Access options

Security > Access Control

Full Control	Specifying full control is the equivalent of granting all the above permissions to the user. Setting this option overrides the individual options selected above.
Force Basic Interface	Users with this flag set will get a simplified interface of RemotelyAnywhere, which offers only a limited set of features and was designed for novice users. Note; this setting only hides certain RemotelyAnywhere features, but does not disable them, so users can still access them by typing their URLs into the browser's address bar. Members of the Administrators group are not affected by this setting.
SSH Does Not Emulate Stream Mode	Set this flag to disable emulated stream mode for the SSH Server. The option is helpful if you want SSH to execute non-interactive shell scripts which must not include terminal emulation. SSH uses an emulated stream mode when the command shell is cmd.exe. Emulation is turned off by setting this flag, and this allows you to use an alternate shell (such as bash.exe) in stream mode. (You can control the shell interpreter used by changing the ComSpec environment variable for this user.) This flag, when set, overrides the system-wide Console Mode parameter under Telnet Server and will enable Stream Mode for this user. By default, stream mode in RA SSH is emulated, meaning that it does not directly relay I/O between the shell and the SSH client, but does some pre-processing in order to properly display the original command-line shell of Windows (cmd.exe).

RSA SecurID Authentication

RemotelyAnywhere supports RSA SecurID authentication. RSA SecurID offers an extra physical layer of security by demanding conclusive proof of a user's identity.

Regarding setup, configuration, and operation of the RSA Server and Clients, please contact your RSA distributor or support team. For more information about RSA SecurID see http://www.rsa.com/.

To activate this function, follow this procedure:

1 Set up an RSA ACE Server.

2 Set up RSA ACE Client software on each computer that will use RSA authentication.

3 On each computer that will use RSA authentication, click **Start > Control Panel > RSA ACE Client settings**. Configure the service.

4 In RemotelyAnywhere, click **Preferences > Security > RSA SecurID**. The RSA SecurID Authentication window displays. Use this window to set the following options:

   a **Disabled**: When this option is selected, RemotelyAnywhere will not prompt for a SecurID during logon.

   b **Required for all users**: When this option is selected, all users will be prompted for a SecurID during logon.

   c **Required for specific users:** When this option is selected, only specified users will be prompted for a SecurID during logon.

   d **Fail authentication attempts if the RSA ACE/Server is not available**

   e **Force User ID to match Login Name**

   f **Use Domain name in User IDs**

5 Click **Apply** to save your settings.

IP Address Lockout

On the RemotelyAnywhere toolkit, select **Security > IP Address Lockout** to set up features that help detect and temporarily lock out potential intruders. IP Address Lockout is useful if your server is exposed to the Internet.

Denial of Service filter

The Denial of Service filter (DoS) is a precaution against unwanted intruders who slow your Host machine by continuously requesting the same service.

Active	Select **Active** if you want to use the Denial of Service filter.
Number of invalid HTTP Requests allowed from an unauthenticated source before lock out	Specifies the number of HTTP Requests that you will accept from an unauthenticated source before locking out the source IP address. An IP address will be locked out if the number of failed requests from the same IP address reaches the value specified in the **Number of invalid HTTP Requests**… field within the time period specified in the **Reset invalid request counter after** field.
Reset invalid request counter after	After the amount of time specified in this box has elapsed, the invalid request count of the offending IP address will be reset to zero.

Lock out for	All requests from an offending IP address will be rejected for the amount of time specified in this field.

Authentication Attack Filter

The Authentication Attack Filter locks out those who try to get past your logon screen without authorization.

Note: *Failed login attempts and lockouts are logged in the RemotelyAnywhere log file.*

Active	Select **Active** if you want to use the Authentication Attack Filter.
Number of invalid attempts before locking out	Specifies the number of invalid login attempts you will allow from a given IP address before locking out the source IP address. An IP address will be locked out if the number of failed login attempts from the same IP address reaches the value specified in the **Number of invalid attempts before locking out** field within the time period specified in the **Reset invalid attempt counter after** field.
Reset invalid attempt counter after	After the amount of time specified in this box has elapsed, the invalid attempt count of the offending IP address will be reset to zero.
Lock out for	All attempted connections from an offending IP address will be rejected for the amount of time specified in this field.

IP Filtering

On the RemotelyAnywhere toolkit, select **Security > IP Filtering** to specify exactly which computers are allowed to access RemotelyAnywhere on your system by creating profiles to allow or deny connections from specific IP addresses. The IP filtering window is displayed.

- To create a new filtering profile, enter a profile **Name** and click **Add**. You can enter the following:
  - A single IP address
  - An IP address with a subnet mask, essentially granting or denying access for a whole network.
  - An IP address with wildcards and no subnet mask. Accepted wildcards are an asterisk (*) that matches any number of characters, or a question mark (?), that matches a single character only.
  - Use the **Type** dropdown menu to **allow** or **deny** access to the selected IP address.
- To edit an existing filtering profile, select it from the list and click **Edit**.
- The Up, Delete, and Down buttons let you manage already entered filters. Select one item in the list, and move it up or down with the appropriate buttons, or remove it altogether.

Whenever a new connection is established to RemotelyAnywhere, the remote IP addresses are checked against the filter or filters in the list, and access is granted or denied accordingly. The IP filters that you set up here apply to every connection received by RemotelyAnywhere, except for those aimed at the FTP or Port Forwarding Server. To specify IP address restrictions specific to these modules you will need to use their specific IP filtering options.

How IP Filtering Works

When an IP address is checked against a list, RemotelyAnywhere goes from the first element of the list to the last, comparing the IP address against the item. If the item is a single IP address, it only matches the remote IP if they are equal. If the item is an IP address with a subnet mask, a logical AND operation is performed on the subnet mask and the remote IP address, and the result is checked against the item's network address to see if the remote IP address is in fact on the network. If the item is a wildcard, the remote IP address is converted to its dotted textual representation and the two strings are compared.

When a match is found, RemotelyAnywhere checks if it should allow or deny the connection, based on the allow/deny flag belonging to it. This result is then used to decide whether to let the connection proceed.

If no match is found, then the connection is allowed. If you would like all connections that are not listed to be denied, enter `DENY.*` as the last item on the list.

Examples:

Allow connections from IP address 215.43.21.12 and the network 192.168.0.0, and deny all other connections:	`ALLOW:215.43.21.12`
	`ALLOW:192.168.0.0 (255.255.0.0)`
	`OR - ALLOW:192.168.*`
	`DENY:*`

Allow connections from IP address 215.43.21.12 and the network 192.168.0.0, but not from the address 192.168.0.12, and deny everything else	`ALLOW:215.43.21.12`
	`DENY:192.168.0.12`
	`ALLOW:192.168.0.0 (255.255.0.0)`
	`OR`
	`ALLOW;192.168.*`
	`DENY.*`
	
	Note: Denying the connection from 192.168.0.12 comes before allowing connections to the 192.168.0.0 network. This is because if RemotelyAnywhere was to find the ALLOW item first, it would let IP address 192.168.0.12 through, since it matches the condition. To prevent this, we make sure that the address 192.168.0.12 is checked before the network to which it belongs.

Allow all connections, except those coming from 192.168.0.12	`DENY:192.168.0.12`

Deny all connections from the network 192.168.0.0 except for the subnet 192.168.12.0, and allow all other connections	`ALLOW:192.168.12.0(255.255.255.0)`
	`OR`
	`ALLOW:192.168.12.*`
	`DENY:192.168.0.0 (255.255.0.0)`
	`OR`
	`DENY:192.168.*`

Ordering is crucial.

It is not possible for you to lock yourself out by accident when setting up IP address restrictions from afar, i.e. you can not enter a `DENY:*` clause into an empty list.

RemotelyAnywhere Logs

On the RemotelyAnywhere toolkit, select **Security > RemotelyAnywhere Logs** to view the RemotelyAnywhere log files. The RemotelyAnywhere Logs page is displayed.

Click **Download all logs in one compressed file** to access all available logs in a single WinRAR ZIP archive. You will be prompted to open or save the file.

The active log file is named RemotelyAnywhere.log. Older logs are stored with the naming convention LMIYYYYMMDD.log. For example, the RemotelyAnywhere log file for June 1, 2008, would be called RA20080601.log.

You can enable or disable logging to text files, but RemotelyAnywhere will always log the following events to the Windows Application Log:

- Service Start/Stop
- LogIn/Logout
- Remote Control Start/Stop

Service start and stop events are always written to the RemotelyAnywhere log file whether or not logging is enabled or disabled. You can modify the setting for these logs under Preferences > Log Settings.

SSL Setup

On the RemotelyAnywhere toolkit, select **Security > SSL Setup** to view the RemotelyAnywhere SSL Setup options. The SSL Setup page is displayed.

If you set up SSL support for RemotelyAnywhere all traffic between the Client and the Host will be encrypted using industry-strength 128-bit ciphers, protecting your passwords and data. RemotelyAnywhere can detect and use any SSL certificates already installed in Windows on your machine, as long as they have an exportable private key.

You can choose to use an already installed certificate or create a self-signed certificate.

- To select a previously installed certificate, choose one from the list of available certificates and click **Continue**. The chosen certificate will be activated.
- To create your own self-signed certificate select **Create a self-signed certificate** and click **Continue** The Certificate Authority form is displayed. Complete the form. Some default values are provided from the Host's registry. When you have finished, click **Continue**. This will create the CA.
- Optional: Click **Install the CA certificate…** to install the CA certificate to your browser. Follow the instructions in the Windows Certificate Import Wizard.

Windows Password

On the RemotelyAnywhere toolkit, select **Security > Windows Password** to update the Windows Password on the Host. The Windows Password page is displayed. Enter your **Old password**, **New password**, and **Password confirmation**. Click **Apply** to save your changes.

Note: *Fields will not appear if your user account on the Host is configured in a way that does not allow you to change the password.*

Most Recent Accesses

On the RemotelyAnywhere toolkit, select **Security > Most Recent Accesses** to view a list of your most recent remote control sessions. The list includes the following data: Local Name, User, Access Started, Access Finished, and Idle Time.

Preferences menu

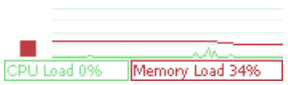
The **Preferences** menu allows you to customize RemotelyAnywhere settings.

Appearance

On the RemotelyAnywhere toolkit, select **Preferences > Appearance** to configure the appearance of RemotelyAnywhere.

General Settings

Preferences > Appearance

Display performance viewer applet at the top of the screen:	Enables/Disables the Java applet showing the current processor and memory utilization in the top frame. 
Enable Tooltips	Cancel this selection to turn-off all RemotelyAnywhere tooltips on the impacted computer.
Enable Icons	Cancel this selection to turn-off most of the icons displayed on RemotelyAnywhere HTML pages.
Default number of items per page for long lists	Sets the number of records displayed per page if there are long lists such as event logs
Default number of items per WAP page	Most WAP devices have very small screens and limited memory. Also, some gateways might enforce size restrictions on the WML documents they compile for their devices. This configuration setting lets you specify the number of records to appear per WAP screen, where applicable. Such screens belong to the Processes, Services, and Drivers menu options.

Systray Settings

Preferences > Appearance

Display the RemotelyAnywhere icon in the System Tray	By default the RemotelyAnywhere icon will be available in the System Tray.  Cancel this selection if you do not want RemotelyAnywhere displayed in the System Tray.
Disable RemotelyAnywhere notification messages	Select this option to supress all RemotelyAnywhere messages communicated from the system tray. This is useful when RemotelyAnywhere is implemented on kiosks or other unattended computers where messages could disrupt the end-user experience.

Custom Pages

Preferences > Appearance

RemotelyAnywhere is able to act as a simple HTTP daemon and serve files from the computer to the Web.

Custom HTTP Directory	Specify the root directory for the HTTP daemon.
Custom HTTP default index file	Define the default index file. This is the file that will open when you select **Custom Pages** from the RemotelyAnywhere Menu.

Network

On the RemotelyAnywhere toolkit, select **Preferences > Network** to update your network's general, proxy, and SMTP settings.

General Settings

Preferences > Network

Use this section to update your general network settings.

TCP/IP port to listen on	By default, RemotelyAnywhere listens on port 2000. However, if this port is already used by a different application or service then you can set a different port for RemotelyAnywhere to use.
TCP/IP address to listen on	Your machine can have several IP addresses assigned to it. By default, RemotelyAnywhere listens on all of those addresses. You can specify just one IP address you want RemotelyAnywhere to use for incoming connections.
IP filter profile to use	Create profiles to allow or deny connections from specific IP addresses.
Accept unsecured HTTP connections (non-SSL)	If this box is unchecked and SSL transport has been set up (Security > SSL Setup) then only HTTPS connections will be allowed.
Allow SSLv2 negotiation if remote insists	If this option is disabled, RemotelyAnywhere will use SSLv3/TLSv1.
Allow export-strength SSL ciphers as a last resort	If this option is disabled, RemotelyAnywhere will not use export-strength ciphers, such as EXP-RC4-MD5.
Allow weaker ciphers as a last resort	If this option is disabled, RemotelyAnywhere will not use ciphers with keys shorter than 128 bits, such as RC4-64-MD5.
Broken proxy server mask	Some proxy servers request pages from web servers using several IP addresses. This can cause RemotelyAnywhere to bounce you back to the login page after you click the Login button. If you are not affected by this problem, you should not change this setting. However, if you experience this problem, please read the following section carefully.

Broken proxy server mask, continued	When you log in, your browser is assigned a session identifier in a cookie. For security reasons, this cookie is only valid when sent from the IP address from which the login originated. Were it not so, an eavesdropping attacker would be able to copy your cookie and gain access to all RemotelyAnywhere resources to which you have access.
	
	Some proxy servers use several IP addresses when requesting data from a remote computer. If this is the case with your proxy server, RemotelyAnywhere sees the original IP address and session identifier as valid, but requests originating from other IP addresses (even if accompanied by a valid cookie) are replied to with the login page. The login page breaks out of frames, and displays itself in your browser - and you are prompted to log in again. A possible workaround is to keep logging in as many times as necessary - most proxy servers only use a few - maybe half a dozen - IP addresses. Once all the IP addresses are logged in, you will no longer be bounced to the login page.
	
	Since version 3.2, RemotelyAnywhere has had a setting called Proxy Problem Fixer. This is essentially a mask that can be applied to IP addresses. Suppose your proxy server uses the following IP addresses to request pages from servers: `192.168.0.33, 192.168.0.34, 192.168.0.35, 192.168.0.36, 192.168.0.37, 192.168.0.38`
	
	In this scenario, if you look at the IP addresses in binary form, you can see that only the last three bits are different:
	
	`11000000.10101000.00000000.00100001`
	`11000000.10101000.00000000.00100010`
	`11000000.10101000.00000000.00100011`
	`11000000.10101000.00000000.00100100`
	`11000000.10101000.00000000.00100101`
	`11000000.10101000.00000000.00100110`
	
	This means that the largest number that can be represented on three bits (111 binary = 7 decimal) has to be masked from the IP addresses when checking them against each other to verify the validity of the session identifier cookie.
	
	RemotelyAnywhere provides a subnet mask-like setting for this purpose. By default, it is set to 255.255.255.255 - this means that no bits are masked off. Given the above scenario, we need to mask off the three least significant bits, thus we subtract 7 (binary form: 111) from 255.255.255.255, which leaves us with 255.255.255.248. By entering this value in the Proxy Problem Fixer field, we are telling RemotelyAnywhere to ignore the last three bits.
	
	This is a rather tedious way of getting around the problem, but short of reconfiguring the proxy server to use only one IP address, there is no easier solution. The latter is the recommended solution, since allowing several IP addresses to share the same session identifier can be a security risk. It is not really significant when you only mask off a few (three or four) bits, but if you need to decrease more and more significant bits of the IP addresses, you are putting yourself in a risky situation. The risk is decreased significantly due to the fact that RemotelyAnywhere now uses HTTPS rather than HTTP by default meaning that the cookie is protected by SSL.

Maximum number of servicing threads	Here you can specify the maximum number of threads RemotelyAnywhere can spawn to service client connections.
Idle time allowed	This is the amount of time that can pass without any activity during a session before the remote connection is dropped.
Stalled transfer timeout	Any file being transferred that fails to complete within the defined period of time will be ended. The time is expressed in days, hours, minutes, and seconds.
File Transfer Compression	Choose **Fast** to use less CPU but also less compression. Use this when you do not want to tie up the CPU. Choose **Normal** for a good balance between effective file compression and balanced CPU utilization. Choose **Best** when you want the CPU to compress the file data as much as possible before transferring it. Choose **No Compression** if you do not compress data.
File Transfer Download Bandwidth Limit	You can set the maximum amount of bandwidth you want to use while downloading files via RemotelyAnywhere File Transfer. This helps you avoid network congestion and poor performance (web pages loading slowly or failing to load).
File Transfer Upload Bandwidth Limit	You can set the maximum amount of bandwidth you want to use while uploading files via RemotelyAnywhere File Transfer. This helps you avoid network congestion and poor performance (web pages loading slowly or failing to load).
Force HTTP Tunneling	HTTP tunneling basically allows the client computer to communicate to the RemotelyAnywhere host from behind a proxy server by issuing HTTP requests to RemotelyAnywhere. Having this option enabled has two advantages and one drawback: Advantage: If you connect to the remote computer via HTTPS, Remote Control, Telnet, and Chat will be tunneled through HTTPS - and SSL is much more secure than the built-in encryption used by these modules when a direct socket connection is established. Advantage: If you can not establish a direct connection to the remote computer (because of, say, a proxy server) you will not have to wait for the direct connection attempt to time out, RemotelyAnywhere will immediately try to connect via the HTTP tunnel. Drawback: You will definitely notice a performance decrease when using these modules with HTTP tunneling since tunneling requires the data to be packed into HTTP packets and usually each packet will need to establish its own connection to RemotelyAnywhere.

Automatically check for latest version on the Web	When enabled, RemotelyAnywhere will attempt to connect to http://www.remotelyanywhere.com every 24 hours to see if there is a newer version of the software available. If there is, it will notify you via the News panel on the About RemotelyAnywhere tab of the home page, as well as place an entry in the RemotelyAnywhere.log file. When RemotelyAnywhere connects to RemotelyAnywhere.com, the following information is recorded on the server: • The version of RemotelyAnywhere making the request • The version and family of the operating system RemotelyAnywhere is running on • The language of the operating system • Whether the instance of RemotelyAnywhere making the request is a trial or a licensed copy This information is recorded for statistical purposes, to help LogMeIn better serve its customers. If you do not wish to provide this information to us, please disable this option.

SMTP Settings

Preferences > Network

When RemotelyAnywhere needs to send an email, it will use the SMTP server you enter in the SMTP Settings page. Leave the **SMTP server address & port** field blank if your SMTP server does not require authentication.

SMTP server address & port	Enter the address and port of the SMTP server you want to use with RemotelyAnywhere.
Force SSL/TLS connection	If this option is enabled, RemotelyAnywhere will be forced to communicate with the SMTP server through an encrypted connection.
SMTP user name	Enter your SMTP user name.
SMTP domain	Enter your SMTP domain name.
SMTP password	Enter your SMTP password.
Default sender address	Email sent using this server will use this address as the default sender address. That is, emails will appear to come from this address.
Test email recipient	Test emails will be sent to this address.

Dynamic IP Support

Preferences > Network

RemotelyAnywhere can send you an email message pointing to the IP address of your remote host every time it detects a change. Use this if your host has a dynamic IP address. Leave the recipient field blank if you do not want to use this feature.

Colors

On the RemotelyAnywhere toolkit, select **Preferences > Colors** to modify RemotelyAnywhere display colors.

Enter standard hexadecimal color codes using the number sign (#) followed by the appropriate six-digit code. You can also select from the pre-defined color schemes in the drop down menu at the bottom of the screen.

Click **Apply** to view changes. Click **Restore** to cancel any changes and return to the default color scheme.

Log Settings

On the RemotelyAnywhere toolkit, select **Preferences > Log Settings** to access log related settings.

General settings

Preferences > Log Settings

Keep log files for this many days	Set the number of days you want to keep log files
Directory for log files	Define the folder where the files are to be saved.

ODBC messages

Preferences > Log Settings

Click the checkbox here to send log events to an ODBC data source.

Syslog Settings

Preferences > Log Settings

Use this section to send log events to a Syslog server. You can also set a Syslog hostname or IP address, Transport protocol (UDP or TCP), UDP port number, TCP port number or Facility code to report.

Remote Control Session Recording

Preferences > Log Settings

Enable Session Recording	Select this field to create a RCREC file during remote control sessions.
Automatically convert to .AVI format	If this field is selected, each new remote control session will automatically be converted to .AVI format. AVI files can be played in any media player with the appropriate codecs installed If this field is not selected, you can convert recordings manually by right-clicking on the RemotelyAnywhere system tray icon and selecting **Tools > Convert Remote Control Recordings**. Follow the instructions in the conversion wizard.
Location for Output Video Files	Specify the folder where video files will be saved.

Maximum Total Size of Output Video Files	Enter a value (expressed in megabytes) if you want to limit the size of your remote session recordings. Set the value to zero to never delete any recorded sessions.

ODBC messages

On the RemotelyAnywhere toolkit, select **Preferences > ODBC messages** to use RemotelyAnywhere's feature for writing messages from System Monitoring and Scripting to a database.

Data Source	Define a data source in Windows using **Control Panel > Administrative Tools > Data Sources (ODBC)**. This can be any database type, such as Oracle, SQL Server, Microsoft Access or Excel.
User name	Enter the user name (including domain) and password required to access the data source. RemotelyAnywhere cannot imitate your database login.
Password	
Table name	The name of an existing table in the database in which the messages are to be stored. You can define specific column names in the database.
Time stamp	Enter the names of the fields that will hold the timestamp.
Computer name	Text field, maximum 16 characters
Message	Text field, maximum 250 characters
Log level	Text field for the severity of message, maximum 10 characters)
Module	Text field for the originating module, maximum 20 characters)
Facility	Text field for the originating facility, maximum 20 characters)
Client	Text field for the address/name of the client, maximum 100 characters)
Write Test Message	Click this button to test your ODBC configuration.

License

On the RemotelyAnywhere toolkit, select **Preferences > License** to view and modify your existing RemotelyAnywhere license options.

Remote Control Preferences

On the RemotelyAnywhere toolkit, select **Preferences > Remote Control** to view and modify a number of options relating to the behavior of remote control sessions.

General Settings

Preferences > Remote Control

Allow Mini Meeting	By checking this box, you enable the Mini Meeting feature. See the relevant section in this document for more details of this feature.

Use mirror display driver	RemotelyAnywhere provides a mirror display driver on the Windows 2000 and XP platforms. This display driver provides a faster and less CPU-intensive remote control session. Should you have any compatibility problems, you can turn off the use of this driver by disabling this option.
Automatically disable wallpaper	By default the wallpaper (desktop background) image on the Host is disabled. Cancel this selection if you need too see the Host's desktop background.
Automatic clipboard transfer maximum size	RemotelyAnywhere features advanced remote clipboard capabilities. Its usage is outlined earlier in this manual. Under preferences you can specify the maximum number of kilobytes to be transferred between machines. The default maximum is 1024kb, but bear in mind that transferring significantly larger amounts may cause problems.
Idle time allowed	If the remote control computer is inactive for the amount of time specified here, it will automatically be disconnected.
Auto panning	If the display area of the Host is too large to display on the Client, then only a part of the screen will be displayed and you will use the scrollbars to view other parts of the Remote screen. With this option enabled, the screen is automatically scrolled for you when the mouse nears the edge of the current display area.
Default Remote Control	Allows the user to specify which technology is used when launching an RemotelyAnywhere Remote Control session (ActiveX, Java or HTML).
Ctrl + Alt + Del Hotkey	Allows you to select which keyboard shortcut to use to enact the Ctrl + Alt + Del Windows function on the Host machine. By default, it is Ctrl + Alt + Insert.

Security

Preferences > Remote Control

Disable Host keyboard and mouse	By disabling the Host keyboard and mouse you can prevent the person sitting in front of the Host (Host) machine from using their mouse or keyboard while a remote control session is in progress.
Blank the Host's monitor	By checking this box, the Host machine's screen is blanked. Anyone sitting at the Host will see a blank screen on the monitor while the remote session is active.
Lock console when connection broken	With this option enabled RemotelyAnywhere will lock the console to protect your work in case the Client loses its connection to the server.
Lock console when connection times out	"Console" refers to the Host that you were controlling remotely With this option enabled RemotelyAnywhere will lock the console to protect your work if your connection times out.

Always lock console when remote control disconnects	"Console" refers to the Host that you were controlling remotely. If the desktop is automatically locked, then anyone physically at the host will not be able to do anything. This is an important security feature. For example, if you are working with your online bank account on the Host, but the connection is dropped because of a problem at the Client, you do not want someone near the Host to be able to access your bank account.
Local keyboard & mouse takes precedence over remote	Select this option if you want all keyboard and mouse actions entered on the Client device to be processed before actions entered on the Host. That is, the actions of the person running the remote control session will be processed before the actions of the person sitting at the computer being controlled.
Allow one click login to desktop	If the Host computer is locked when you initiate a remote control session, LogMeIn will prompt you to unlock the computer with a single click rather than prompting you to re-enter your Windows credentials.
Disable Drag & Drop during Remote Control	Select this option if you do not want to be able to drag and drop files between the Host and Client computers.

Visible & Audible Notification

Preferences > Remote Control

Beep when the remote control session starts or ends	If this is enabled the Client will beep when a remote control session is initiated or ended.
Beep continuously during remote control	With this enabled the Client will beep according to the **Beep interval** when a remote control session is active.
Beep interval	Allows you to define the time period between notification beeps.
Flash Keyboard Indicator Lights	When this field is selected the Number Lock, Caps Lock and Scroll Lock keyboard lights will flash in sequence to indicate that a remote control session is active.

Interactive User's Permission

Preferences > Remote Control

Ask for permission from interactive user	By default, RemotelyAnywhere will prompt the user of the Host to grant permission to the person making a remote connection. Cancel the selection if you want to be able to access a Host without requiring permission from a user. Cancelling the selection will also disable the Chat function.

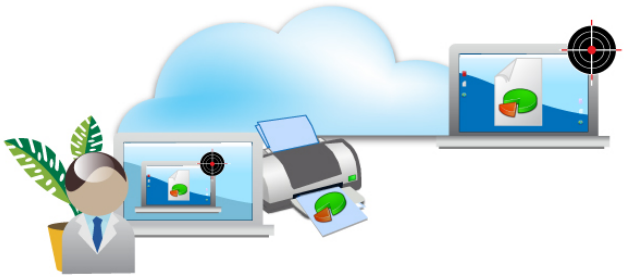
Default answer for confirmation message	If set to **Yes**, then the remote connection will be established even if a user does not respond within the time set in the **Time allowed for the interactive user to give permission** field. If set to **No**, the connection will not be made.
Time allowed for the interactive user to give permission	Enter the amount of time that the Host user has to respond to the notification message. If this time expires, the setting in the **Default answer for confirmation message field** will be applied.
Text to display to the user	This is the text that will be presented to the user in the remote control confirmation page. The string %USER% will be substituted by the name of the user attempting a remote control operation.
Full Control (and Remote Control) access rights bypass interactive user's permission	With this option enabled, users with full Remote Control access rights (Read, Write, Delete, or "R+W+D") will be able to access the Host without first asking the user's permission. If this is enabled it overrides the setting in the **Ask for permission from interactive user** field.
Do not require authorization if user is not present	Select this box is you want be able to initiate a Remote Control session without user permission.

Remote Printing

Preferences > Remote Control

Select **Enable remote printing** to be able to print from the Host to the default printer on the Client. This feature requires no driver installation.

You can only print from the printer assigned to be the default printer on the Host. If a printer you want to use is not the default printer, you must change it to become the default.



Connecting Drives

Preferences > Remote Control

These options control the accessibility of the disk drives on the Client to the Host, allowing you to open Client files on the Host.

Note: *When this feature is enabled the Connect Drives option will be activated in the Remote Control interface. You must select* ***Connect Drives*** *in Remote Control to actually make the connection.*

Scenario: You want to run a Spyware cleaner on the Host, but you *do not* have the software loaded on the Host. You *do* have the software on the Client. Using Windows Explorer on the Remote Device, locate and run the executable file for the Spyware cleaning program directly from its location on the Client.

Note: *Some programs may require additional configuration or a license key before they will run on the Accessible Device.*

Enable connecting drives	Select this box to enable this feature according to rules set in the following fields.
Preferred drive letter…	This is the letter that will be used on the Host to signify the Client drives. Example:"Drives on 'AccessDeviceName' on 'Network Name' (F:)"
Allow connecting local hard drives to the remote computer	Select this box to make disk drives on the Client available to the Host.
Allow connecting removable drives to the remote computer	Select this box to make removable drives (such as a pen drive) connected to the Client available to the Host.
Allow connecting network drives to the remote computer	Select this box to make network drives connected to the Client available to the Host.
Set directory format of connected drives	Example: Description first: winxp32 (C) Drive letter first: (C) winxp32
Write-protect connected drives	Select this box to make all files on the Host read-only when accessed using Remote Control.

Remote Sound

Enable remote sound	With this box selected, the Client will play sounds from the Host.
Mute sound on Remote Computer	With this box selected, the Client will play sounds from the Host, but sounds at the Host will be muted.
Sound capture device	This field lists the sound devices (sound cards) available at the Host. Select the device to be used for capturing sounds.
Input line	This field lists the input lines available at the Host. Select the line to be used for capturing sounds.
Encode quality	Select the quality level of the sound to be recorded from the Host. High quality is recommended for high-speed connections only.

Telnet Server

Preferences > Telnet Server

TCP/IP port to listen on / address to listen on: Here you can specify which port / address you want RemotelyAnywhere to listen on for telnet connections. This defaults to the standard telnet port of 23, and all available interfaces. Changes take effect when the service is restarted.

Accept RemotelyAnywhere connections (secure)	Allow connections from RemotelyAnywhere's built in Command Prompt.
Accept Telnet connections	Allow plaintext terminal emulator connections. If disabled, only the built-in Java client can be used to access Telnet. This does not affect the SSH server.

Show login banner	Enable or disable the logon message sent by the Telnet/SSH servers when a connection is established.
Login	If you do not want to let anybody who connects to the Telnet/SSH ports know the version of the operating system and RemotelyAnywhere, disable this option.
Maximum simultaneous connections	Here you can specify the maximum number of connections to the Telnet/SSH servers. It's a good idea to set a reasonable limit, especially on computers connected to the Internet. Every new connection uses resources on the computer.

Timeouts

Preferences > Telnet Server

Here you can set the login timeout (number of seconds the user may remain idle during the login process), the idle timeout (number of seconds the user may remain idle during a Telnet/SSH session) and the session recovery timeout. When a Telnet connection is broken ungracefully (that is, the user does not type exit at the command prompt) it is possible to reconnect to the session and continue work where it was left off for a period of time. You can specify the amount of time for which you want the lost telnet session to remain available. Any and all running programs started by the user in the Telnet session will be available when the session is resumed.

RemotelyAnywhere Client

Preferences > Telnet Server

Here you can specify the number of columns and rows that the console window will occupy. You can also specify whether you would like to have the client open in a new window, or in a new window in full screen mode.

Telnet/SSH Client Default Parameters

Preferences > Telnet Server

Here you can specify the default parameters for the Telnet/SSH client. You can also select the console mode (Stream, Full ANSI Colors, or Full Monochrome) and enable/disable the console parameters option.

SSH Server

Preferences > SSH Server

This page allows you to view and modify SSH related options.

The IP and address options are the same as for Telnet connections (above), but with the default port of 22, which is standard for SSH connections. Changes will take effect when the service is restarted.

Features enabled section

Preferences > SSH Server

Enable SSH1 or SSH2	The server that will take advantage of these features.
SFTP	This is a secure file transfer method
SCP	This is another secure file transfer method, but non-interactive.
Compression	Compression can be disabled, delayed or enabled in current version Delayed: This delays the start of zlib compression until the user has been authenticated successfully. This eliminates the risk of any zlib vulnerability leading to a compromise of the server from unauthenticated users. Enabled If this is checked data sent over the network will be compressed.
Password authentication	When activated, the user can enter a username / password combination in the terminal emulator client program and use that to gain access.
Keyboard interactive authentication	This is similar to the above option, but it won't allow the saving of the username / password in the terminal client.
Public key authentication	When activated, the user can enter a username and then gain access to the SSH host without entering a password. A private key is used on the client side to authenticate against the matching public key on the host.
Cross-check IP and DNS entry of clients	If this option is activated, and if the client comes from the IP address 192.168.0.10 (for example), and this IP address resolves to COMPUTER1, but COMPUTER1 does not resolve to 192.168.0.10, the connection will be disallowed.
Forwarding of server-side ports	This is SSH Port Forwarding, allowing server-side ports to be forwarded to others, effectively creating a virtual encrypted tunnel for the duration of the SSH session.
Remote connects to the forwarded ports	This allows the ports to be forwarded outside the server; that is, to any computer on the network the server has access to.

Path Mapping in SCP/SFTP

Preferences > SSH Server

Use this feature to create virtual folders for SCP and SFTP.

To create a new path mapping entry, type the **Virtual path** and the **Physical path**. You can use standard Windows path syntax and/or environment variables in the physical path (for example %TEMP% to /tmp).

Sample Virtual Path	Sample Physical Path
/tmp	%TEMP%
/doc	%USERPROFILE%\My Documents

/log	c:\LogFiles

When the connection is made to the Host with SCP or SFTP, virtual folders can be addressed in the same format as physical.

Virtual and physical folders must be referenced UNIX style, using a forward slash mark in place of a back slash Example: `c/Program Files/RemotelyAnywhere/x86/RemotelyAnywhere.exe`

Notes:

- SFTP does not list virtual folders
- It is possible to create virtual folders within physical folders
  `/c/windows/pic` → `d:\Pictures` where `/c/windows` is a physical folder
- It is possible to create virtual folders within existing virtual folders
  `/doc/video` → `d:\Videos` where `/doc` is a previously created virtual folder
- If a virtual and a physical folder are located under the same path, the virtual folder takes precedence
  `/c/windows/system32` → `d:\DataFiles`
  Entering `/c/windows/system32` you will see the contents of `d:\DataFiles` instead of `c:\Windows\system32`
- It is possible to create a virtual folder without creating its parent folder
  `/jpg/2007` → `d:\Images`

Host Keys

Preferences > SSH Server

The SSH Host Keys section lets you re-generate SSH1 and SSH2 host keys used by the SSH server. You can specify the key size, but the larger the key, the longer it takes to generate it. Anything above 2048 bits is excessive, and will take a very long time even on a fast computer.

SSH hosts have keys that can be used to identify them, much like SSL-protected websites have certificates. SSH1 only supports a single host key, while SSH2 supports both RSA and DSA keys. The key length is recommended to be 1024 bits or more, and can be 512, 768, 1024, 2048 or 4096. The SSH1 server key is a key that is relatively short, and has a short lifetime. It is used in conjunction with the host key to negotiate a one-time session key for each connection. SSH2 uses the Diffie-Hellman keyexchange protocol to negotiate the session key and therefore does not need one.

The **Export SSH2 public host keys in SECSH format** button lets you export the host keys and save them in your terminal emulator. This way, you can be sure that when the emulator connects to the RemotelyAnywhere computer and does not put up a warning about an unknown host key, you are still in fact connecting to the intended computer.

Privilege Separation

Preferences > SSH Server

You can enable or disable privilege separation here. A full description of what this means is available within RemotelyAnywhere by clicking **What is it?** The text is reproduced here in full.

On Vista hosts there is an additional checkbox: **Set permissions on objects owned by Trusted Installer**.

For documentation about Windows Resource Protection visit http://msdn2.microsoft.com/en-us/library/aa382503.aspx.

When a user establishes an SSH session, and authentication succeeds, the server executes applications (typically a shell process such as cmd.exe) in the user's security context. The server needs to execute with LocalSystem privileges to access resources required for user authentication and impersonation.

Allowing an anonymous user to directly communicate with code that runs with the same permissions as the operating system itself is the primary reason remote exploits exist.

Privilege separation has been pioneered by the Unix community with the release of OpenSSH 3.2. The main goal of this technology is to prevent anonymous clients from exchanging information with highly privileged software. This is achieved by serving a client with the help of two server-side processes: one that runs with SYSTEM privileges, and another which has practically no privileges (i.e. GUEST privileges). The latter process is automatically spawned by the privileged parent. The unprivileged child processes all network data and handles communications with potentially untrusted clients. It relies on the parent process to perform tasks that need privileges, and communicates these requests through a well defined and very simple interface. This way both sides must agree that the client has authenticated before it is granted further access, and even if the unprivileged child is compromised, the intruder cannot gain access to, let alone modify, valuable information.

OpenSSH runs the unprivileged process in the context of a special user account. When you enable SSH Privilege Separation in RemotelyAnywhere, this user is automatically created and its access rights are minimized on the file system and the registry. This usually requires several minutes, especially on large file systems. This special user has very limited rights: only execute permissions in the System32 directory, and read rights to a minimum set of registry entries. These permissions are required by Windows to execute any and all software. All other access rights are explicitly denied for the special user account.

The Privilege Separation User is created under the name __ra_ssh_privsep__. It is maintained by RemotelyAnywhere and you should not modify the account, its group memberships or any other related security settings. This user is created with GUEST privileges, its password is set to a cryptographically random string that is as long as system policies allow. The user account is disabled by default. When RemotelyAnywhere accepts an SSH connection, it changes the user's password, enables the account, logs the user in, stores it's access token handle, resets the password again - and finally disables the user account until it is needed again.

Warning! Only NTFS file systems allow the required access rights to be set.

When you install a new hard drive in your computer, Windows grants full access to the "everyone" group to the new hard disk and all of its contents. On such occasions you should use the Check rights feature on the SSH Configuration page to set the correct access permissions on your system.

Local or domain security policies might restrict local logins. RemotelyAnywhere attempts to explicitly grant the Privilege Separation User local login privileges in the local security policy - however, if domain policies override the local security policy, the __ra_ssh_privsep__ user might not be allowed to log in. In this case, Privilege Separation should be disabled or the domain security policy should be changed to be less restrictive.

Network Maintenance

Preferences > Network Maintenance

With this feature you can install and configure RemotelyAnywhere on other computers connected to the network.

This option will not work if you have logged on with NTLM authentication. NTLM authentication cannot be delegated over the network, so RemotelyAnywhere would not be able to identify you to other computers.

First, you are asked how you would like to scan the network. You can choose to scan a specified domain only, or you can browse the whole network. On larger networks, this can be a lengthy operation, so looking at single domains at a time is recommended. You also have the option of inspecting and upgrading a single computer.

Second, you are shown the selected part of the network. All computers are listed, and you will be able to see what operating system and which version they are running, what roles they fulfill, and whether or not they have RemotelyAnywhere installed.

If RemotelyAnywhere is installed on a machine in the list, you can quickly open it by clicking on the machine name. You can also see which version of RemotelyAnywhere is running on the computer and you can upgrade it if necessary. If RemotelyAnywhere is not installed on one of the machines on the network you can also quickly do so from here.

Advanced Options

On the RemotelyAnywhere toolkit, select **Preferences > Advanced Options** to set your advanced Remote Control, Log Settings, Network, and Customized Login Message settings.

Remote Control

Preferences > Advanced Options

Disable HTML-based remote control	Select this option if you do not want to use the HTML-based version of RemotelyAnywhere Remote Control when the RemotelyAnywhere ActiveX, Mozilla, or Java plugin is unavailable.
Disconnect an existing remote control session from the same user	If you lose your connection during a Remote Control session and then want to be able to re-connect again before the old session times out.
Block the closing of the Remote Control notification window	Select this field if you want the Remote Control notification window to always be displayed.
Force Bitmap printing	Select **Force Bitmap printing** if material printed using RemotelyAnywhere Remote Printing does not print properly (wrong layout, meaningless characters and content). When this option is selected, all material printed using Remote Printing will be 'printed' locally to a bitmap which is then sent to the remote printer. Bitmap printing is slow, but it is useful since it almost always produces proper printing results.

Log Settings

Preferences > Advanced Options

Log Settings	Click here to enable debug-level logging.

Network

Preferences > Advanced Options

Disable HTTP content compression	Select this option if your browser does not support HTTP compression.

Customized Login Message

Preferences > Advanced Options

Display a customized logo on the login screen	With this box selected, any image saved as “customlogo.jpg” in the RemotelyAnywhere installation directory will be displayed on the RemotelyAnywhere login screen.

Customized Login Message	The customized login message entered here will be displayed on the RemotelyAnywhere IT login screen and as an SSH banner.

General Settings

Preferences > Advanced Options

Select Language	Choose the language used by RemotelyAnywhere. This setting has no impact on operating system settings. RemotelyAnywhere messages on the Host will be displayed in this language.

Custom Pages menu

RemotelyAnywhere is able to act as a simple HTTP daemon and serve files from the computer to the Web. On the RemotelyAnywhere toolkit, select **Custom Pages** to work with this feature.

You will need to assign a **Custom HTTP directory** and **Custom HTTP default index file**.

Appendix 1: Working RemotelyAnywhere from the Command Line

In Windows NT and Windows 2000, you can run RemotelyAnywhere from the command line to perform various actions.

For a complete list of command line options, enter the following command:

```
RemotelyAnywhere -help
```

Install RemotelyAnywhere on the Client

The command for this operation is:

```
Install [-port PORT]
```

You will need to have the RemotelyAnywhere installation files in the current directory, either copied from an existing installation or from the manual installation archive available on RemotelyAnywhere.com.

This command will create the RemotelyAnywhere service and its support driver in the current directory, and start it immediately.

The optional parameter can specify the listener port. For example:

```
RemotelyAnywhere Install -port 2020
```

You will need administrative privileges on the Client to successfully perform this operation.

Install Remotelyanywhere on a Remote (Host) Computer

The command is:

```
Install <–computer COMPUTER> <–path PATH> [-port PORT]
[-minimal] [-license FILENAME]
```

You will need to have the RemotelyAnywhere installation files in the current directory. You will also need administrative rights on the Host.

The first optional parameter is the same as when installing RemotelyAnywhere on the Client; it specifies the HTTP port number. The `[-minimal]` switch allows you to perform a minimal install. This option does not copy the documentation files, thus speeding up the install process over a slow network connection. The two required parameters are the name of the Host and the local path to the intended destination directory on the Host.

The `[-license FILENAME]` option lets you specify a license file to be installed on the Host.

For example, if you want to install RemotelyAnywhere on a computer called KOSSUTH in the C:\RemotelyAnywhere directory, and you do not want the documentation files copied, you will need to enter the following command:

```
RemotelyAnywhere Install –computer \\KOSSUTH -
path
“C:\RemotelyAnywhere” -minimal
```

This will create the destination directory, copy all necessary files, and create and start the RemotelyAnywhere service on \\KOSSUTH.

Uninstall RemotelyAnywhere on a Client

The command is:

```
Uninstall
```

This will stop and remove the RemotelyAnywhere service and its support driver, as well as all registry entries created by RemotelyAnywhere. You will need to delete the RemotelyAnywhere directory and all its contents yourself.

For example:

```
RemotelyAnywhere Uninstall
```

You will need administrative privileges on the Client to successfully perform this operation.

Uninstall Remotelyanywhere On a Host

The command is:

```
Uninstall <-computer COMPUTER>
```

This will stop and remove the RemotelyAnywhere service and its support driver, as well as all registry entries created by RemotelyAnywhere. You will need to delete the RemotelyAnywhere directory and all its contents yourself.

For example:

```
RemotelyAnywhere Uninstall –computer \\KOSSUTH
```

You will need administrative privileges on the Host to successfully perform this operation.

Start or Stop a Service

The command is:

```
start [-service SERVICE] [-computer MACHINE]
stop [-service SERVICE] [-computer MACHINE]
```

The optional parameters are the name of the service (it defaults to RemotelyAnywhere) to be started, and the computer to perform the operation on (defaults to the Client).

For example, this will start the RemotelyAnywhere service on the Client:

```
RemotelyAnywhere start
```

This will stop the W3SVC service on the computer called KOSSUTH. You will need administrative rights on the Host to perform this operation.

```
RemotelyAnywhere stop W3SVC –computer \\KOSSUTH
```

Restart the RemotelyAnywhere Service

The command is:

```
Restart [-computer COMPUTER]
```

The optional parameter is a computer name (defaults to the Client machine). For example:

```
RemotelyAnywhere Restart –computer \\KOSSUTH
```

You will need administrative privileges on the computer to successfully perform this operation.

Export/Import RemotelyAnywhere Configuration Settings To/From a Text File

You can use these commands to quickly copy configuration settings from one RemotelyAnywhere installation to another, usually when installing RemotelyAnywhere to a Host from the command line.

```
CreateIniFile [-inifile FILENAME] [-computer MACHINE]
LoadIniFile [-inifile FILENAME] [-computer MACHINE]
```

The default value for `FILENAME` is RemotelyAnywhere.ini in the directory the RemotelyAnywhere executable is located in. The `COMPUTER` parameter, if not specified, defaults to the Client.

```
RemotelyAnywhere CreateIniFile
RemotelyAnywhere Install –computer SERVER1
RemotelyAnywhere Stop –computer SERVER1
RemotelyAnywhere LoadIniFile –computer SERVER1
RemotelyAnywhere Start –computer SERVER1
```

The first line saves the local RemotelyAnywhere configuration to the default file. The second installs RemotelyAnywhere on the computer named `SERVER1`. The third stops the RemotelyAnywhere service on `SERVER1` – necessary, because the previous command already started RemotelyAnywhere. The fourth will read all settings from the default .ini file, and configure RemotelyAnywhere on `SERVER1`. The last command starts RemotelyAnywhere.

The `CreateIniFile` command will write all RemotelyAnywhere configuration data to the target text file. The `LoadIniFile` command will import all configuration data contained within the text file to the Host. This means that all configuration data is copied, including permissions, FTP Server settings, the license key, etc. If you do not want to import specific configuration items, you will need to edit the generated .ini file and remove these entries. The format of the generated .ini file is shown below. The example is just a small part of the actual file generated. If you do not wish to copy, for example, the `VisitLength` setting, simply remove the `ValueXXXX=VisitLength` line from the `MetaData` section.

```
[MetaData]
Creator=RemotelyAnywhere
CreatorBuildNumber=268
SourceComputer=SERVER2
Value0000=UseGraphRed
Value0001=VisitLength
Values=2
[UseGraphRed]
Type=REG_DWORD
Data=0
[VisitLength]
Type=REG_DWORD
Data=600
```

INSTALL -NOAUTOCERTS

Use this command to install RemotelyAnywhere while preventing RemotelyAnywhere from generating any certificates.

The default installation method includes automatically generating a self-signed CA Certificate and a Server Certificate that is signed by the CA Certificate. After installation RemotelyAnywhere will warn you about the fact that it is not using a Server Certificate and the communication between the browser and the RemotelyAnywhere host is unsecured.

Command	Example
`-NOAUTOCERTS`	`RemotelyAnywhere install –noautocerts`

NOAUTOCERTS MSI

Use this command to install RemotelyAnywhere using the MSI Installer while also preventing RemotelyAnywhere from generating any certificates

Command	Example
`NOAUTOCERTS`	`msiexec /i RA.msi NOAUTOCERTS=1`

INSTALL -USESC

Use this command to install RemotelyAnywhere and instruct RemotelyAnywhere to select the Server Certificate with the given MD5 hash and use it to secure RemotelyAnywhere sessions. Automatic certificate generation will be skipped.

Command	Example
`install –usesc`	`RemotelyAnywhere install –usesc <CERTMD5ID>`

USESC MSI INSTALL

Use this command to install RemotelyAnywhere using the MSI Installer and instruct RemotelyAnywhere to select the Server Certificate with the given MD5 hash and use it to secure RemotelyAnywhere sessions. Automatic certificate generation will be skipped.

Command	Example
`USESC`	`msiexec /i RA.msi USESC=<CERTMD5ID>`

INSTALL -CREATESSSC

Use this command to install RemotelyAnywhere and instruct RemotelyAnywhere to create a Self-Signed Server Certificate and use it to secure RemotelyAnywhere sessions. No CA Certificate is generated. In the example, `<HOSTNAME>` is the common name of the certificate that is being generated. If omitted, the hostname of the computer will be used.

Command	Example
`install –createsssc`	`RemotelyAnywhere install –createsssc <HOSTNAME>`

CREATESSSC MSI INSTALL

Use this command to install RemotelyAnywhere using the MSI Installer and instruct RemotelyAnywhere to create a Self-Signed Server Certificate and use it to secure RemotelyAnywhere sessions. No CA Certificate is generated.

Command	Example
`CREATESSSC`	`msiexec /i RA800735nh.msi CREATESSSC=1`

CREATESSSCHOSTNAME MSI Install Option

If the CREATESSSCHOSTNAME MSI install option is not used then the hostname of the computer will be used for a certificate common name.

Command	Example
CREATESSSCHOSTNAME	msiexec /i RA.msi CREATESSSC=1 CREATESSSCHOSTNAME=<HOSTNAME>

INSTALL -USESCBYCA

Use this command to install RemotelyAnywhere and instruct RemotelyAnywhere to select the first Server Certificate that was signed by the CA with the given MD5 hash and use it to secure RemotelyAnywhere sessions.

Command	Example
-usescbyca	RemotelyAnywhere install –usescbyca <CERTMD5ID>

USESCBYCA MSI Installer

Use this command to install RemotelyAnywhere using the MSI Installer and to instruct RemotelyAnywhere to select the first Server Certificate that was signed by the CA with the given MD5 hash and use it to secure RemotelyAnywhere sessions.

Command	Example
USESCBYCA	msiexec /i RA.msi USESCBYCA=<CERTMD5ID>

CERT –LISTSC

After RemotelyAnywhere has been installed, use this command to list the MD5 hash value of the available Server Certificates.

Command	Example
Cert –LISTSC	RemotelyAnywhere cert –listsc

CERT –USESC

After RemotelyAnywhere has been installed, use this command to select the Server Certificate with the given MD5 hash and use it to secure RemotelyAnywhere sessions.

Command	Example
cert –usesc	RemotelyAnywhere cert –usesc <CERTMD5ID>

CERT –CREATESSSC

Once RemotelyAnywhere has been installed, use this command to instruct RemotelyAnywhere to create a Self-Signed Server Certificate and use it to secure RemotelyAnywhere sessions. No CA Certificate is generated.

Command	Example
`cert –createsssc`	`RemotelyAnywhere cert –createsssc <HOSTNAME>`

CERT –LISTCA

After RemotelyAnywhere has been installed you can list the MD5 hash value of the available CA Certificates using this command.

Command	Example
`cert –listca`	`RemotelyAnywhere cert –listca`

CERT –USESCBYCA

After RemotelyAnywhere has been installed, use this command to select the first Server Certificate that was signed by the CA with the given MD5 hash and use it to secure RemotelyAnywhere sessions.

Command	Example
`cert –usescbyca`	`RemotelyAnywhere cert –usescbyca <CERTMD5ID>`

FTP Start/Stop Commands

Remotelyanywhere.exe ftp start/stop

Use these commands to start or stop the built-in FTP server. If you are running more than one FTP server on the host, all of them will be started or stopped by the command.

Command	Example
`Remotelyanywhere.exe ftp start`	`Remotelyanywhere.exe ftp start`
`Remotelyanywhere.exe ftp stop`	`Remotelyanywhere.exe ftp stop`

Appendix 2: Map of Windows Tools to RemotelyAnywhere Toolkit

RemotelyAnywhere allows easy access to functionality offered by numerous Windows administrative tools. This table maps commonly used Windows tools to their equivalent RemotelyAnywhere feature.

Windows Tool	Equivalent RemotelyAnywhere Feature
Application Event Log	RemotelyAnywhere toolkit > Computer Management > Event Viewer
Command Prompt	RemotelyAnywhere toolkit > Computer Management > Command Prompt
Computer Management > Local Users and Groups	RemotelyAnywhere toolkit > Computer Management > User Manager
Computer Management > Services	RemotelyAnywhere toolkit > Computer Management > Services
Computer Management > Shared Folders	RemotelyAnywhere toolkit > Computer Settings > Shared Resources
Event Viewer	RemotelyAnywhere toolkit > Computer Management > Event Viewer
Performance > Logs and Alerts	RemotelyAnywhere toolkit > Performance Info
Performance > System Monitor	RemotelyAnywhere toolkit > Performance Info
Registry Editor	RemotelyAnywhere toolkit > Computer Management > Registry Editor
Scheduled Tasks	RemotelyAnywhere toolkit > Scheduling & Alerts > Task Scheduler
Security Event Log	RemotelyAnywhere toolkit > Computer Management > Event Viewer
Services	RemotelyAnywhere toolkit > Computer Management > Services
System Event Log	RemotelyAnywhere toolkit > Computer Management > Event Viewer
Task Manager/Processes	RemotelyAnywhere toolkit > Computer Management > Processes

Appendix 3: RemotelyAnywhere on a Mobile Device

RemotelyAnywhere supports access via wireless handheld devices connecting using the http protocol. Not all handheld PDAs are the same. While RemotelyAnywhere is designed to operate on the most popular PDA devices and browsers, some features may appear different from one handheld to the next, and indeed in some cases certain functions have been deactivated altogether due to the limitations of some devices. However, in the case of devices running Pocket PC 2000/2002, Microsoft Windows Mobile 2003 for Pocket PC, or Microsoft Windows Mobile 2003 Second Edition for Pocket PC, RemotelyAnywhere offers the ability to perform desktop remote control.

Logging in to RemotelyAnywhere via a PDA is very similar to logging in via a desktop's web browser. Simply ensure your PDA is connected to your LAN, or, if necessary, the internet, and enter the appropriate IP address or web address and click OK. Authentication with PDA browsers is exactly the same as with other browsers. Enter your Windows username and password and, if necessary, the domain name, click OK, and you will be brought to the main menu.

Security Note: With HTTP and the PDA's browser interface, making secure SSL connections is very similar to the process found on other browsers: simply create an SSL certificate, install the certificate in your browser, and use HTTPS as the protocol.

Main Menu with a Mobile Device

Depending on the browser, you will see a menu with the following clickable links:

- Home
- Remote Control
- Processes
- Services
- Drivers
- Event Viewer
- User Manager
- Registry Editor
- Reboot
- CPU Load
- Memory Load
- File Transfer
- Network Maintenance
- Log Out

Home (Dashboard)

Click Home to see a simplified version of the RemotelyAnywhere Dashboard described earlier in this manual; the PDA interface's Dashboard shows a simple system overview.

Remote Control

If this option is available with your browser, selecting Remote Control downloads an ActiveX control to your PDA.

Using the stylus, you can move the mouse around on the screen. Tapping the screen, as per normal, is like clicking the mouse.

The toolbar, seen at the top left, offers the following buttons in order from left to right:

- Drag: Using this button, the toolbar can be dragged around the edges of the PDA window.
- Menu The menu offers the following options:
- File > Disconnect: Ends the RemotelyAnywhere session
- View > Actual Size: Views the host screen at 100% magnification
- View > Scale to Fit: Scales the host screen to fit the PDA screen
- View > Zoom To >: Manually specify the zoom level
- View > No Rotation: Maintains the remote control screen vertically represented
- View > Rotate Left 90 Degrees: Rotates the remote control screen to the left
- View > Rotate Right 90 Degrees: Rotates the remote control screen to the right
    - (The above two options make better use of the screen geometry of the PDA, thus allowing a larger picture)
- Tools > Send Ctrl-Alt-Del: Sends a Ctrl-Alt-Delete keystroke combination
- Tools > Send Special Keys: See Remote Control section of this manual
- Tools > Change Color Depth: Changes the number of colors shown on the host screen
- Tools > Change Resolution: Changes the screen resolution of the host screen
- Keyboard: Tapping this icon once brings the keyboard interface up, allowing you to type. Tapping it again makes the keyboard disappear.
- Mouse button: Tapping this icon switches between left and right mouse-clicks.
- Exit: Returns to main menu.

Processes

The output of this function will give you a listing of all processes running on the Host. The list is hierarchical: a parent process will have its child processes listed beneath it, with indentation indicating relationships. Please note that this is for information purposes only, since Windows reuses process IDs.

Selecting a process will give you more information about it, as detailed earlier in this manual.

Services & Drivers

The image below shows you what you would see under the services or drivers menu options:

The format of the Services and the Drivers lists are identical. These lists display the names and statuses of all the services (or drivers) installed on the remote machine. Clicking on the name will show you more detail about the selected object and allows you to control it. You can also change its startup options. When specifying a user account to be used by a service, it must be in DOMAIN\USER form. If you want to use a local user account, you can type .\USER.

In the list of objects, the status field shows Stopped, Running, Starting, Stopping, etc. RemotelyAnywhere looks through the list of services and drivers, and if it finds one that is set to start automatically but is not running, a question mark is displayed. This alerts you to the fact that the service should be running, but isn't.

Event Viewer

This option enables you to view RemotelyAnywhere's event viewer. You will be given a list of event viewer options.

User Manager

When you click on User Manager in the menu you will be able to access RemotelyAnywhere's use manager. Supporting all the features of NT's built-in User Manager, its functionality is similar to that of RemotelyAnywhere's regular User Manager.

Registry Editor

This option enables you to edit the registry of the Host. First, the registry roots (HKCR, HKCU, HKLM, etc.) are displayed, and you can drill down into them by clicking on their names. Registry keys are links that open up that key for you. Key values are also displayed here, with their name, type and value. You can edit values that are of either text (REG_SZ, REG_EXPAND_SZ or REG_MULTI_SZ) or integer (REG_DWORD) type. Binary, etc. values are only displayed but cannot be edited. Using the buttons at the bottom of every page you can add a subkey, add a value or delete the currently opened key.

Reboot

This option presents you with a menu similar to that found in the HTML interface.

The first selection restarts the RemotelyAnywhere service. The next four selections reboot the computer. Normal reboot shuts down all applications. Emergency reboot kills all processes then shuts down and restarts the system in an orderly fashion. You might lose data in your running applications. Hard reboot is just like pressing the reset button or toggling the power switch: use this only as a last resort! Scheduled reboot allows you to reboot the remote machine at a specified time.

CPU Load & Memory Load

Here you can view graphs on the CPU and memory load.

File Transfer

When using File Transfer, bear in mind that Palm devices do not really have a "traditional" file system. Under the Windows CE browser, you can hover your stylus over a file and it will give you the option to "Save as" (thus putting the "transfer" in "file transfer") whereas on the Palm OS, all it will do is try to open files in various programs (for example, text files in textpad and jpgs in a picture viewer). This is the fundamental difference between Palm and Windows CE.

Network Maintenance

With this feature you can install and configure RemotelyAnywhere on other computers connected to the network, much as you would with the RemotelyAnywhere Console, as documented in the Preferences chapter of this manual.

Log Out

This menu option ends your RemotelyAnywhere session. It is not strictly necessary to manually log out – your session will eventually time out after the time period specified in the RemotelyAnywhere configuration elapses.