CommView® Remote Agent

Help Documentation

Introduction

About CommView Remote Agent

CommView Remote Agent is an application for remote network traffic monitoring. It allows CommView users to capture network traffic on any computer where Remote Agent is running, regardless of the computer's physical location. This new, unique technology broadens your horizons: you are no longer limited by your LAN segment or personal computer. If you are in Tokyo and want to troubleshoot a complex software installation in Amsterdam, just install CommView Remote Agent on the target system and watch the important TCP/IP traffic from the comfort of your office, as if you were there!

After the installation and simple configuration, CommView Remote Agent is ready to accept connections from CommView. Once the connection is established and the authentication is successful, CommView Remote Agent is ready to capture packets in its network segment and transmit them to CommView. The transmitted packets are compressed to save bandwidth and encrypted to ensure safe transmission over insecure network channels. CommView has a flexible system of filters that is capable of filtering out all undesired packets, thus minimizing the bandwidth used for the TCP link between CommView and CommView Remote Agent.

CommView Remote Agent is an indispensable tool for networking, software, and security professionals that can solve a wide range of problems, such as monitoring multi-segment LANs or remote software and network troubleshooting.

CommView Remote Agent requires an Ethernet or Wireless Ethernet network card supporting the NDIS 3.0 driver standard, or a standard dial-up adapter.

What's New

Version 2.3

- Windows 8 support

Version 2.2

- New operating systems supported: Windows Server 2008 32-bit and 64-bit Editions.

Version 2.1

- Windows Vista support.

Version 2.0

- High resolution time stamping (up to microseconds, available under Windows 2000/XP/2003).
- Windows XP 64-bit Edition on AMD processors is now supported.
- You can now capture loopback packets being sent from/to local IP addresses, e.g. 127.0.0.1 (this functionality is available under Windows 2000/XP/2003).
- Improved performance.

Using the Program

Installation and Configuration

CommView Remote Agent should be installed on the compute(s) whose traffic you would like to monitor. Just like CommView, the agent can capture all traffic that passes through a network interface card (NIC) or dial-up adapter. CommView Remote Agent can be installed on computers that are part of a LAN or on stand-alone computers. You must have administrative privileges to install the program, although such privileges are no longer required after the initial installation and configuration. You should NOT install both CommView and CommView Remote Agent on the same computer; doing so makes no sense.

Installation

To install the program, run SETUP.EXE and follow the instructions on the screen. Once the program files are copied to the destination folder, you will see the Installation and Configuration window that will prompt you to enter two initial settings. You should select a TCP port number and password. The TCP port number (5050 by default) will be used by the program to accept client connections from CommView. The password is required for client authentication and subsequent packet encryption. Be sure to choose a long, hard-to-guess password, using alphanumeric upper and lower case characters, because if somebody guesses your password, he/she will be able to gain access to the network traffic of the computer on which you are installing CommView Remote Agent.
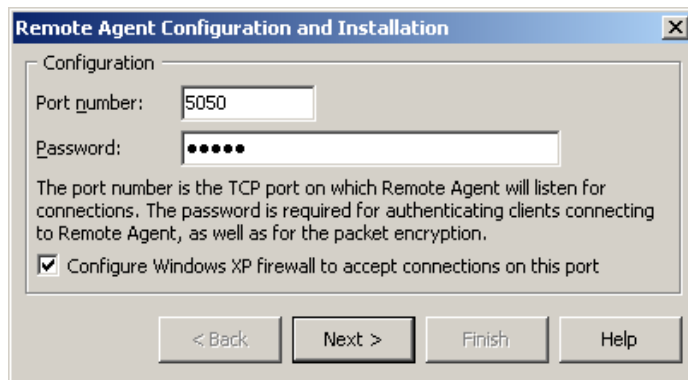
Click **Next** to continue, and the program will install the necessary drivers and launch CommView Remote Agent for the first time.

Batch Mode Installation

When performing mass deployment of CommView Remote Agent, batch mode installation and configuration can be used. In batch mode installation, the required installation parameters are supplied as command line switches, and the installation process is performed silently, without any user interaction. To perform batch installation, SETUP.EXE must be run with the following switches:

/s – silent installation. This switch is required.
/port=xxx – port number, where xxx is any numeric value between 1 and 65536. This switch is required.
/pass="xxx" – password, where xxx is a password string. The password string must be enclosed in quotation marks. This switch is required.
/du – installs the driver for monitoring the dial-up adapter in addition to the standard set of drivers. This switch is optional. Do not use this switch if you don't need to monitor dial-up connections. Note that depending on the target system driver installation policy, you may be prompted to confirm this driver installation manually, so the installation process may not be silent.
/lb – installs the driver for monitoring loopback packets being sent from/to local IP addresses, e.g. 127.0.0.1. This switch is optional. Do not use this switch if you don't need to capture loopback traffic.

Usage example:

SETUP.EXE /s /port=5050 /pass="ZdU34 ! Hny536" /lb

Interface

Once the installation and initial configuration has been completed, the program's icon should appear in the system tray as shown below. Clicking on the icon will bring up the application window that displays the program status – the port number that the CommView Remote Agent listens on, the IP address of a client that is connected to it, packet transmission statistics, and buffer utilization.
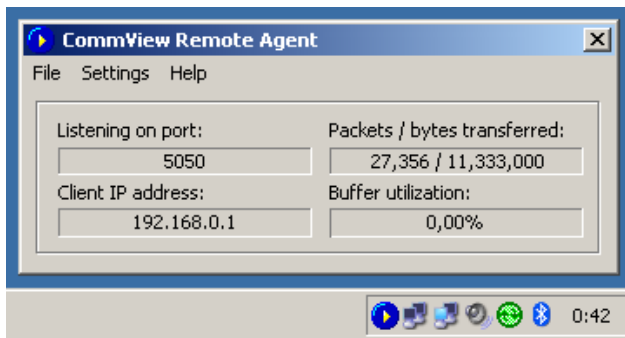
Main Menu

File

Start/Resume Service – starts or resumes CommView Remote Agent service if it has been stopped or paused.
Stop Service – stops CommView Remote Agent service.
Pause Service – pauses the Remote Agent service.
Exit – closes CommView Remote Agent console. Please note that the Remote Agent service continues to run and accept connections from CommView.

Settings

Change Port – allows you to change the port number that the application listens on.
Change Password – allows you to change the connection password.
Language – allows you to change the interface language.

Help

Contents – launches CommView Remote Agent help.
About – shows information about the program.

Note that CommView Remote Agent can accept only one client connection at any given time.

Controlling The Program

CommView Remote Agent is a **service application**. This means that it starts automatically when the computer is booted up and runs even if no one is logged on to the system. The service can be controlled using the **File** menu described above. Additionally, as with any other service application, it can be controlled using Control Panel => Administrative Tools => Services. There you can also change the start-up mode (automatic/manual).

Monitoring Traffic

This chapter describes how to use CommView to connect to CommView Remote Agent and capture traffic remotely. To monitor network traffic on remote computers, you need to have CommView Remote Agent running on the remote host and CommView running on your computer. It is assumed that Remote Agent is already installed and running (see the previous chapter for instructions) and that you are already familiar with CommView and know how to use it. If you have no experience with CommView, please download it and familiarize yourself with CommView prior to using CommView Remote Agent.

Using CommView to Connect to CommView Remote Agent

To switch to remote monitoring mode, click **File** => **Remote Monitoring Mode**. An additional toolbar will appear in the CommView main window next to the main toolbar. If you are behind a firewall or proxy server, or using a non-standard Remote Agent port, you may need to click on the **Advanced Network Settings** button to change the port number and/or enter SOCKS5 proxy server settings.
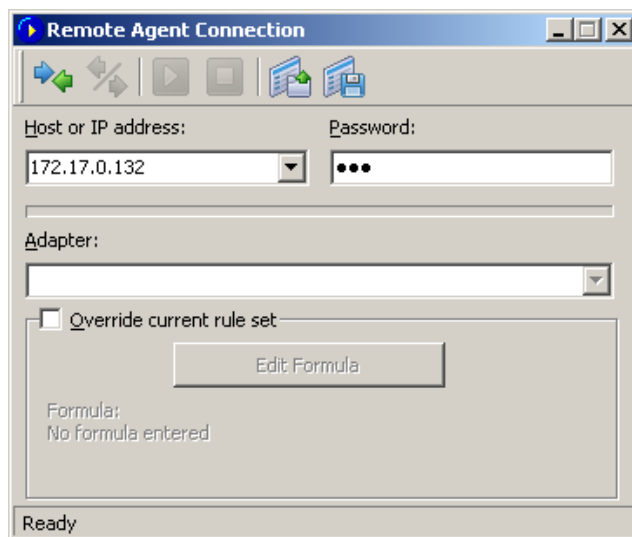
Click on the **New Remote Agent Connection** button to establish a new connection, or click on the **Load Remote Agent Profile** toolbar button to load a previously saved Remote Agent connection profile. A previously saved profile may also be loaded from the New Remote Agent Connection window.

A Remote Agent Connection window will appear where you can enter the IP address of the computer running CommView Remote Agent into the IP address input area, enter the connection password and click on the **Connect** button, and if the password is correct, a connection will be established. You will then see the *Link Ready* message in the status bar, and the adapter selection box will list the remote computer's adapters.
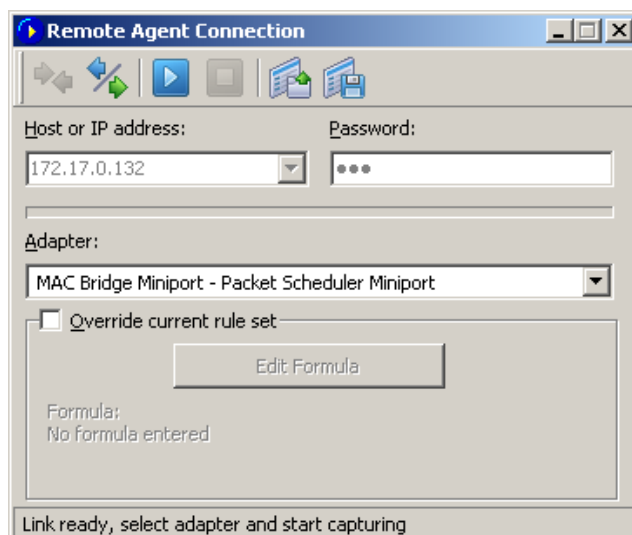
Now is the best time to configure the capturing rules using the **Rules** tab. It's very important to configure the rules correctly so that the volume of traffic between the Remote Agent and CommView doesn't exceed the bandwidth limit on either side of the connection, or you will experience noticeable lag. Be sure to filter out unnecessary packets (see more on this topic below). You can also apply a custom set of capturing rules to this connection and override the current rules defined in CommView by checking the **Override current rule set** box, clicking on the **Edit Formula** button and entering the rules formula in the field below. The formula syntax is the same as the one used in Advanced Rules. Once you're ready to start monitoring, select the network adapter from the list and click the **Start Capture** toolbar button. CommView allows you to save the Remote Agent Connection settings as a connection profile for quick

and easy access in the future. Click on the **Save Remote Agent profile** toolbar button in the New Remote Agent Connection window and enter a name for the file.
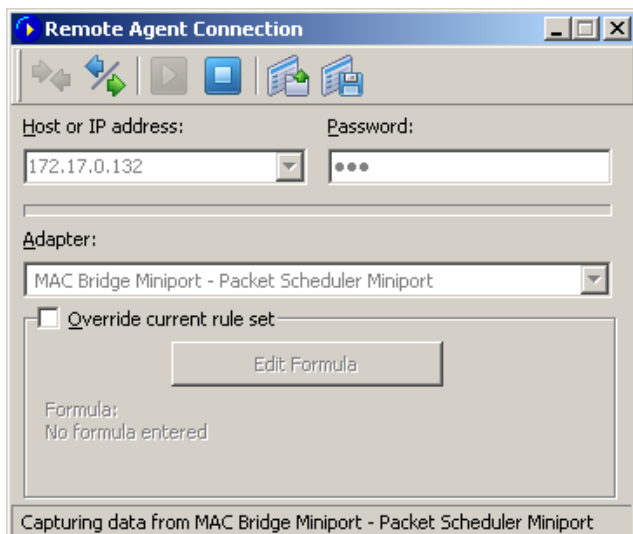
CommView will start to capture the remote computer's traffic as if it's your local network traffic; there is virtually no difference between using CommView locally and remotely. When you are done with remote monitoring, just click on the **Stop Capture** toolbar button. You can then change the adapter or disconnect from Remote Agent by clicking the **Disconnect** toolbar button. To return to the standard mode, click **File** => **Remote Monitoring Mode**, and the additional toolbar will disappear.

Please note that CommView can work with multiple Remote Agents simultaneously. You can open several remote connections, each having its own settings and an independent set of rules and collect the traffic from remote network segments in one CommView instance.

How to Use CommView Remote Agent Efficiently

We encourage you to pay special attention to setting the capturing rules (the Rules tab in the CommView main window, or in the Remote Agent window using Advanced Rules syntax) to best suit your monitoring needs. The bandwidth that you use to connect to the remote computer has limits; in many cases, if CommView Remote Agent is installed on a computer with high network payload, it can take up all available bandwidth trying to transmit all packets to the computer running CommView. If you do not set the capturing rules carefully to filter out the traffic that you do not need to see, it is likely that the channel that connects CommView and CommView Remote Agent computer might be overloaded. For example, even if you are connecting to the CommView Remote Agent via T1 or T3 channel (1.5 or 4.5 Mb/s correspondingly), the remote computer may be connected to the local area network at 100 Mb/s; therefore, under a heavy load your bandwidth will be far from adequate to transmit all the remote LAN traffic being captured.

If CommView Remote Agent captures more data than it can send to CommView, it used an internal buffer to store the packets that cannot be sent immediately. The buffer size is 5Mbytes. The **Buffer utilization** indicator in the Remote Agent window shows the current status of the buffer. For example, if the program has buffered 2.5 Mbytes of data, the buffer utilization is 50%. If/when the buffer utilization reaches 100%, the program stops buffering data and discards captured packets until some buffer spaced is freed. To avoid data loss, you should set the capturing rules so that the buffer is never full.

Security

CommView Remote Agent was made with security in mind. It can be accessed only by using a password that is never transmitted in plain text and that is ensured by using a challenge-response protocol with a secure hash function. If the authentication is successful, all transmitted traffic is compressed and then encrypted with the same password. Please take precautions to keep your password secret. Once it is revealed to an unauthorized person, that person will have broad capabilities to study your network and intercept network traffic on the remote computer.

Information

How to Purchase CommView Remote Agent

This program is a 30-day evaluation version. You can purchase the fully functional, unrestricted version of the program by visiting our Web site.

Check our Web site for current pricing on single-user and multi-user licenses. One licensed copy of CommView Remote Agent may be used by a single person who uses the software personally on one computer. A second copy may be installed on one additional portable computer. Please refer to the End User License Agreement that is displayed when you install the application for the official, detailed description of our licensing policy.

As a registered user, you will receive:

- Fully functional, unrestricted copy of the software
- Free updates that will be released within 1 year from the date of purchase
- Information on updates and new products
- Free technical support

We accept credit card orders, orders by phone and fax, checks, purchase orders, and wire transfers. Prices, terms, and conditions are subject to change without notice: please check our Web site for the latest product offerings and prices.

http://www.tamos.com/order/

Contacting Us

Web

http://www.tamos.com

E-mail

sales@tamos.com (Sales-related questions)
support@tamos.com (All other questions)

Mail and Fax

Mailing address:

TamoSoft
PO Box 1385
Christchurch 8140
New Zealand

Fax: +643 359 0392 (New Zealand)
Fax: +1 917 591-6567 (USA)