CommView Remote Agent

User Manual

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 can be installed on any Windows 95/98/ME/NT/2000/XP system. It 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 1.1

- This is a maintenance release where we fixed known bugs found in the previous versions and improved Windows .NET compatibility. This release also updates the driver to ensure compatibility with the latest CommView version and other products to be released soon.

License Agreement

Please read the following terms and conditions carefully before using this software. Your use of this software indicates your acceptance of this license agreement. If you do not agree with the terms of this license, you must remove this software from your storage devices and cease to use the product.

Copyright
This software is copyrighted 2001, TamoSoft, Inc. CommView Remote Agent is a trademark of TamoSoft, Inc. The use and copyright of this software is governed by international copyright treaties. TamoSoft, Inc. retains full title and rights to this software and documentation, and in no way does the license granted diminish the intellectual property rights of TamoSoft Inc. You must not redistribute the registration codes provided, on paper, electronically, or in any other form.

Evaluation Version
This is not free software. You are hereby licensed to use this software for evaluation purposes without charge for a period of 30 days. Using this software after the evaluation period violates copyright laws and may result in severe civil and criminal penalties.

Registered Version
A single computer license grants you the right to install and use the program on one computer. If you need to install the program on multiple computers, you need to purchase a multi-computer license.

Disclaimer
THIS SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL TAMOSOFT INC. BE LIABLE TO YOU FOR ANY DAMAGES, INCLUDING INCIDENTAL OR CONSEQUENTIAL DAMAGES, ARISING FROM THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS.

Governing Law
This Agreement will be governed by the laws of the Republic of Cyprus.

Distribution
This software may be distributed freely in its original unmodified and unregistered form. The distribution must include all files of its original distribution. Distributors may not charge any money for it. Anyone distributing this software for any kind of remuneration must first contact us for authorization.

Other Restrictions
You may not modify, reverse engineer, decompile, or disassemble this software in any way, including changing or removing any messages or windows.

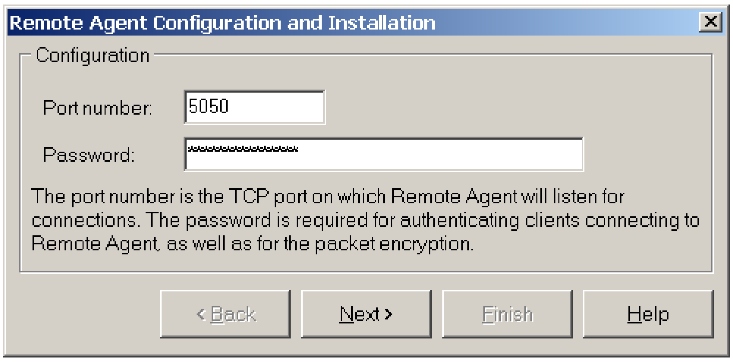
Using the Program

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 under Windows NT/2000/XP, 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.

Configuring The Program

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.



Remote Agent Configuration and Installation

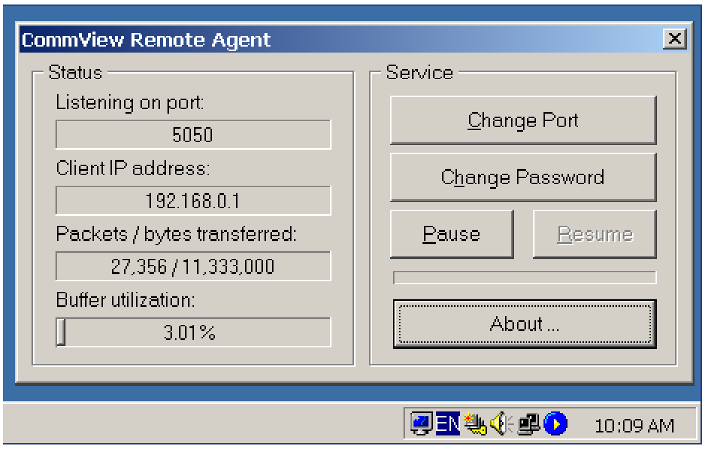
Configuration

Port number: 5050

Password: ***************

The port number is the TCP port on which Remote Agent will listen for connections. The password is required for authenticating clients connecting to Remote Agent, as well as for the packet encryption.

Click **Next** to continue, and the program will install the necessary drivers and launch CommView Remote Agent for the first time. The program's icon should appear in the system tray as shown below. Clicking on the icon will bring up the application window:



CommView Remote Agent

Status

Listening on port: 5050

Client IP address: 192.168.0.1

Packets / bytes transferred: 27,356 / 11,333,000

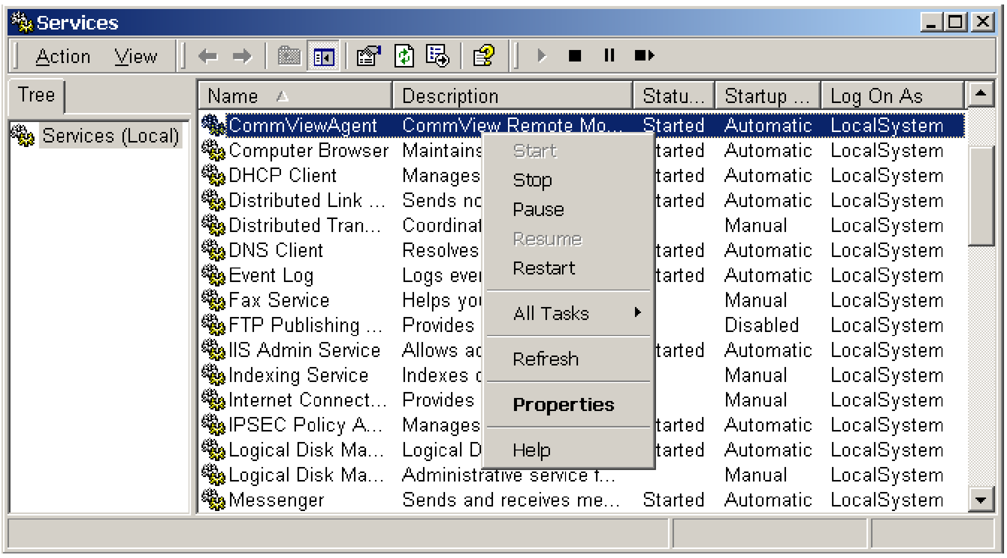
Buffer utilization: 3.01%

The **Status** frame shows 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. The **Service** frame has several program configuration buttons. Click on the **Change Port** button to change the port number that the application listens on. To change the password, click on the **Change Password** button. You can pause or resume the program operation by clicking on the corresponding button. Clicking on the **About** button will display general 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 an **NT 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. 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), or stop/start/pause/resume the service.



Name	Description	Statu...	Startup ...	Log On As
CommViewAgent	CommView Remote Mo...	Started	Automatic	LocalSystem
Computer Browser	Maintains	tarted	Automatic	LocalSystem
DHCP Client	Manages	tarted	Automatic	LocalSystem
Distributed Link ...	Sends nc	tarted	Automatic	LocalSystem
Distributed Tran...	Coordinat		Manual	LocalSystem
DNS Client	Resolves	tarted	Automatic	LocalSystem
Event Log	Logs ever	tarted	Automatic	LocalSystem
Fax Service	Helps you		Manual	LocalSystem
FTP Publishing ...	Provides		Disabled	LocalSystem
IIS Admin Service	Allows ac	tarted	Automatic	LocalSystem
Indexing Service	Indexes c		Manual	LocalSystem
Internet Connect...	Provides		Manual	LocalSystem
IPSEC Policy A...	Manages	tarted	Automatic	LocalSystem
Logical Disk Ma...	Logical D	tarted	Automatic	LocalSystem
Logical Disk Ma...	Administrative service f...		Manual	LocalSystem
Messenger	Sends and receives me...	Started	Automatic	LocalSystem

Under Windows 95/98/ME, CommView Remote Agent emulates a service application and works just like an NT service, i.e. it runs independently of user logons and logoffs.

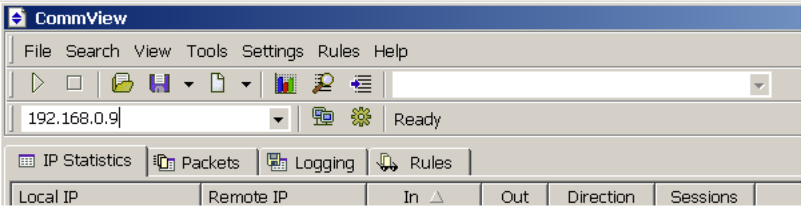
To facilitate the usage of the service, we included a simple utility that allows you to stop/start/pause/resume the service without opening the Services window. This utility is called Service Indicator, and you can find it in the CommView Remote Agent program group (Start => Programs => CommView Remote Agent => Service Indicator).

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

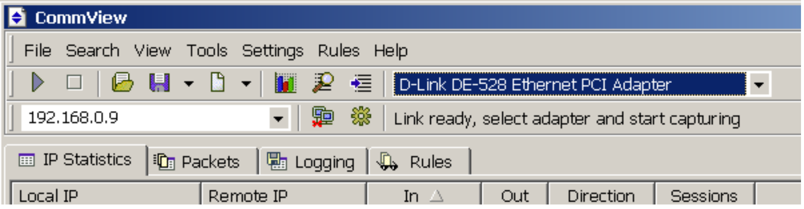
To switch to remote monitoring mode, click **File** => **Remote Monitoring Mode**. An additional toolbar will appear in the CommView main window below the main toolbar. Enter the IP address of the computer running CommView Remote Agent into the IP address input area and click **Connect**. If you are behind a firewall or proxy server, or using a non-standard Remote Agent port, you may need to click on the **Network Settings** button to change the port number and/or enter SOCKS5 proxy server settings.



192.168.0.9

Ready

A window will pop up prompting you to enter the password. Enter the Remote Agent password, and if the password is correct, a connection will be established. You will then see the *Link Ready* message, and the adapter selection box will list the remote computer's adapters.

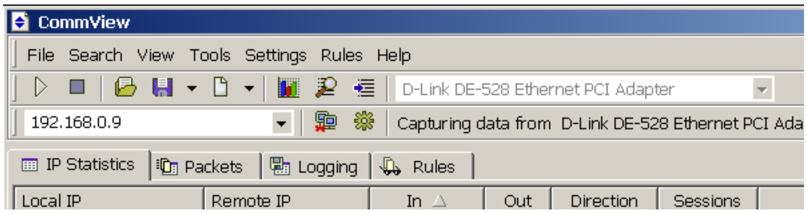


D-Link DE-528 Ethernet PCI Adapter

192.168.0.9

Link ready, select adapter and start capturing

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 Remote Agent and CommView doesn't exceed the bandwidth limit on either side of the connection, or you'll experience a noticeable lag. Be sure to filter out unnecessary packets (see more on this topic below). Once you're ready to start monitoring, select the network adapter from the list and click the **Start Capture** toolbar button.



D-Link DE-528 Ethernet PCI Adapter

192.168.0.9

Capturing data from D-Link DE-528 Ethernet PCI Ada

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.

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) 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. Below are the special introductory prices for the fully functional, unrestricted version of the program:

License	Price, US$
1 Computer	149
5 Computers	499
10 Computers	799

Please note that CommView Remote Agent **is licensed per computer, not per user**. A single computer license grants you the right to install and use CommView Remote Agent on one computer. If you need to install the program on multiple computers, you need to purchase a multi-computer license. You will also need at least one licensed copy of CommView to connect to CommView Remote Agent.

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 (US Server)

http://www.tamosoft.com (UK Server)

E-mail

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

Mail and Fax

Mailing address:

PO Box 1385
Christchurch 8015
New Zealand

Fax: +643 359 0392 (New Zealand)
Fax: +1 503 213-7764 (USA)

Other Products by TamoSoft

CommView

CommView is a program for monitoring Internet and Local Area Network (LAN) activity, capable of capturing and analyzing network packets. It gathers information about data passing through your dial-up connection or Ethernet card and decodes the analyzed data. With CommView you can see the list of network connections and vital IP statistics and examine individual packets. IP packets are decoded down to the lowest layer with full analysis of the main IP protocols: TCP, UDP, and ICMP. Full access to raw data is also provided in real time. CommView is a helpful tool for LAN administrators, security professionals, network programmers, or anyone who wants to have a full picture of the traffic going through one's PC or LAN segment.

More information

SmartWhois

SmartWhois is a handy utility for obtaining information about any IP address, hostname, or domain in the world. Unlike standard whois utilities, it automatically delivers information associated with an IP address or domain, no matter where it is registered geographically. In just a few seconds, you get all you want to know about a user: domain, network name, country, state or province, and city. Even if the IP address cannot be resolved to a hostname, SmartWhois won't fail!

More information

Essential NetTools

Essential NetTools is a set of network tools useful in diagnosing networks and monitoring your computer's network connections. It's a Swiss Army knife for everyone interested in a set of powerful network tools for everyday use. The program includes a NetStat utility that shows your computer's network connections and open ports and maps them to the owning application. It also features a fast NetBIOS scanner, a NetBIOS Auditing Tool for checking LAN security, and a monitor of external connections to your computer's shared resources, as well as a process monitor that displays information about all the programs and services running on your computer and allows you to terminate any process. Other useful tools are included, such as Ping, TraceRoute, and NSLookup. Additional features include report generation in HTML, text, and comma delimited formats and a customizable interface. The program is an easy-to-use and powerful replacement for such Windows utilities as nbtstat, netstat, and NetWatcher. It incorporates many advanced features that standard Windows tools can't offer.

More information

DigiSecret

DigiSecret is an easy-to-use, secure, and powerful application for file encryption and sharing. It utilizes strong and time-proven encryption algorithms for creating encrypted archives, self-extracting EXE files, and P2P sharing of files with your associates and friends. DigiSecret also includes powerful and intelligent file compression; you no longer need .zip files when you can have encrypted and compressed DigiSecret files. The program is integrated with the Windows shell, and you can perform operations on files by right-clicking on them. It also fully supports drag-and-drop operations.

More information