

Winternals[®]

Administrator's Pak[™]

GETTING STARTED



Administrator's Pak™

Getting Started



Table of Contents

I.	Introduction	2
II.	Installation and Setup	4
III.	Booting from the Administrator's Pak CD	5
IV.	Creating a Custom Boot CD	7
V.	Booting from a Custom Boot CD	9
VI.	ERD Commander 2005	10
VII.	Remote Recover	12
VIII.	Crash Analyzer Wizard	14
IX.	FileRestore	15
X.	Filemon Enterprise Edition	16
XI.	Regmon Enterprise Edition	17
XII.	AD Explorer	18
XIII.	Insight for Active Directory	19
XIV.	TCP Tools	20
XV.	Technical Support	21



SYSTEM REPAIR



DATA RECOVERY



TROUBLESHOOTING

I. Introduction

Welcome to Winternals Software's Administrator's Pak™. Administrator's Pak is a comprehensive suite of powerful, versatile tools that allow you to repair a damaged or unbootable system, restore lost or corrupt data, and diagnose and troubleshoot problems associated with Windows® operating systems and file systems.

What's Inside Administrator's Pak:

Administrator's Pak Navigator™

Administrator's Pak Navigator helps users select and utilize the appropriate Administrator's Pak tool to solve a particular Windows system emergency. It also provides a centralized starting point for creating various boot media (diskettes and CDs).

ERD Commander 2005™

ERD Commander 2005 boots a dead system directly from the product CD to a Windows XP-like interface with an array of powerful diagnostic and repair tools, including Disk Commander, FileRestore, Crash Analyzer Wizard, and Locksmith.

Remote Recover™

Remote Recover accesses volumes and files on a dead Windows NT®, Windows® 2000, Windows® XP and Windows™ Server 2003 system remotely via TCP/IP. Volumes and files appear as if they were mounted locally, allowing you to quickly repair problems, remove viruses and malware, salvage data, and more.

Crash Analyzer Wizard™

The Crash Analyzer Wizard allows you to quickly and easily diagnose the cause of a Windows crash dump by identifying the driver that caused the problem.

FileRestore™

FileRestore recovers files that have been lost or deleted from your computer, including files emptied from the Recycle Bin, deleted by applications, programs, or remote processes, lost with removed directories, or deleted via a command prompt.

Filemon Enterprise Edition™

With Filemon Enterprise Edition you can track file system activity on a local or remote system. Quickly find file accesses that coincide with error messages to identify missing, corrupt, duplicate, and out-of-date files in real-time.

Regmon Enterprise Edition™

Regmon Enterprise Edition provides real-time reports of registry accesses, modifications, and deletions that help you pinpoint and correct faulty registry settings, learn where registry settings are stored, and learn which keys affect application behavior.

Insight™ for Active Directory

By displaying the LDAP calls made from any computer to Active Directory, Insight for Active Directory allows you to pinpoint AD configuration issues, analyze application usage of AD, and guide troubleshooting of applications and services that depend on AD.

AD Explorer™

AD Explorer enables you to find, modify, add, and delete Active Directory® objects and attributes within a two-pane window.

TCP Tools™

With TCP Tools (TCPView Professional™ and TCPVStat™) you can easily monitor TCP/IP network activity on a Windows system. It shows you the process associated with each TCP/IP address in real-time, making it easy to determine the application responsible for specific connections and activity. It also lets you see the amount of data sent and received over a network connection.

II. Installation and Setup

1. If your Administrator's Pak is licensed by Administrative User, install the USB-port dongle or parallel-port dongle into the correct computer port. If your Administrator's Pak was licensed to your entire enterprise, no dongle is required.
2. Insert the Administrator's Pak CD into the CD-ROM drive of your computer.
3. If the autoplay feature for your system is enabled, the Administrator's Pak CD will automatically begin the installation process. If the autoplay feature is disabled, navigate to **ADMINPAK.EXE** and double-click to begin installation.
4. The Installation Wizard will guide you through the installation process. Follow the instructions on each screen.
5. Choose either a custom or typical installation. (By default, TCP Tools is not installed with the typical installation. It has to be chosen from the custom setup menu.)
6. During installation you will be prompted for an Activation Key. Your Activation Key was sent by email after your product order was processed. For help with activation issues, please contact customerservice@winternals.com. Please provide your license number.
7. Click Finish to complete the installation procedure.
8. To begin using the tools you have installed, click **Start**, then **Programs**, then **Winternals Administrator's Pak**. If you know which Administrator's Pak tool you wish to use, you may select it directly. (Selecting ERD Commander 2005 will launch a wizard to create the necessary boot media for this tool.) Otherwise, choose **Administrator's Pak Navigator**, which will help you select and utilize the best Administrator's Pak tool for your needs.

III. Booting from the Administrator's Pak CD

The original Administrator's Pak Installation CD is bootable so you can repair or recover a system that cannot start normally. From the Installation CD, you can run either ERD Commander 2005 or the Remote Recover boot client. The system must have a CD-ROM drive and a floppy disk drive to access the Activation Key information.

If your Administrator's Pak license requires a USB-Port Dongle:

1. Copy your Activation Key text file to a floppy disk. You should have received your Activation Key by email after your order was processed. If you did not receive your Activation Key please email Winternals Customer Service at custo_merservice@winternals.com
2. Do NOT insert the dongle yet.
3. Start the computer from the Administrator's Pak Installation CD. You may need to adjust your BIOS settings to allow the computer to boot to the CD first.
4. After ERD Commander loads networking components, you will be prompted to accept the terms of the software license agreement. Click **Yes**. Click **OK**.
5. From the Administrator's Pak Installation CD you can run either ERD Commander 2005 or the Remote Recover client. Click **Run ERD Commander** or **Run Remote Recover client**.
6. If you selected to run ERD Commander, you will be prompted to enter your Activation Key.
7. Insert the floppy disk containing your Activation Key text file, browse to the Activation Key text file and click **OK**.
8. Click **Activate**.
9. After a short delay, you will be notified that the license requires a dongle. Insert the dongle and click **Retry**.
10. ERD Commander will validate the license key and the dongle and then display a list of the operating system(s) installed on the computer.
11. From the list, select the operating system installation you wish to repair and click **OK**.

If your Administrator's Pak license requires a Parallel-Port Dongle:

1. Copy your Activation Key text file to a floppy disk. You should have received your Activation Key by email after your order was processed. If you did not receive your Activation Key please email Winternals Customer Service at customerservice@winternals.com
2. Insert the dongle into the parallel port.

3. Start the computer from the Administrator's Pak Installation CD. You may need to adjust your BIOS settings to allow the computer to boot to the CD first.
4. After ERD Commander loads networking components, you will be prompted to accept the terms of the software license agreement. Click **Yes**. Click **OK**.
5. From the Administrator's Pak Installation CD you can run either ERD Commander 2005 or the Remote Recover client. Click **Run ERD Commander** or **Run Remote Recover client**.
6. If you selected to run ERD Commander, you will be prompted to enter your Activation Key.
7. Insert the floppy disk containing your Activation Key text file, browse to the Activation Key text file and click **OK**.
8. Click **Activate**.
9. ERD Commander will validate the license key and dongle and then display a list of the operating system(s) installed on the computer.
10. From the list, select the operating system installation you wish to repair and click **OK**.

If your Administrator's Pak license does not require a dongle:

1. Copy your Activation Key text file to a floppy disk. You should have received your Activation Key by email after your order was processed. If you did not receive your Activation Key please email Winternals Customer Service at custo_merservice@winternals.com
2. Start the computer from the Administrator's Pak Installation CD. You may need to adjust your BIOS settings to allow the computer to boot to the CD first.
3. After ERD Commander loads networking components, you will be prompted to accept the terms of the software license agreement. Click **Yes**. Click **OK**.
4. From the Administrator's Pak Installation CD you can run either ERD Commander 2005 or the Remote Recover client. Click **Run ERD Commander** or **Run Remote Recover client**.
5. If you selected to run ERD Commander, you will be prompted to enter your Activation Key.
6. Insert the floppy disk containing your Activation Key text file, browse to the Activation Key text file and click **OK**.
7. Click **Activate**.
8. ERD Commander will validate the license key and then display a list of the operating system(s) installed on the computer.
9. From the list, select the operating system installation you wish to repair and click **OK**.

IV. Creating a Custom Boot CD

The Administrator's Pak Installation CD is a bootable image that also includes an installer for the Administrator's Pak itself, which installs the ERD Commander 2005 Boot CD Wizard. The Boot CD Wizard is used to create a bootable CD (ISO) image, which is a file that represents the raw contents of a CD, ready to be written to recordable CD media.

You will need several other items to successfully create a bootable CD from the ISO image the Boot CD Wizard creates:

- CD recordable drive
- CD recordable media (as supported by your recordable drive)
- CD burning software that supports your recordable drive and supports burning an ISO image directly to CD

Note that you can utilize whatever recordable media type (CD-R/+R/-RW/+RW, etc.) that your recordable drive supports, but you should test the resulting media on all systems you intend to support with it, as some systems are not capable of booting from all types of CD recordable media.

-
1. From the **Start** menu, click **Programs**, then **Winternals Administrator's Pak**, then **ERD Commander 2005 Boot CD Wizard**. Follow the onscreen prompts until you are presented with a dialog box asking you to enter your licensing information. The ERD Commander 2005 Boot CD Wizard verifies the license information and embeds it into the ISO image.
 2. The Boot CD Wizard will then extract the files needed to build the bootable CD image. This may take several minutes.
 3. You will be prompted to select the functionality included on the Boot CD.
 - Include only ERD Commander 2005 functionality.
 - Include only Remote Recover 3.0 client functionality.
 - Include both, and allow the user to decide which to use at run-time.
 4. If you choose to include Remote Recover functionality, the Boot CD Wizard will prompt you to customize settings related to network connectivity and security.
 5. You will then be prompted to customize the set of components included on the ERD Commander 2005 CD. (You may wish to limit the tools on the CD.)
 6. Next you will be asked to specify the location of a current copy of the debugging tools for Windows, which will be added to your ERD Commander 2005 CD. (Although you can also later utilize a copy on any system where you are diagnosing a crash, it is recommended that you include them on your boot CD to ensure that they are always available when needed for an emergency diagnosis.)
 7. The wizard will prompt you to create a password. Providing a password for your boot CD limits access to it, for increased security.

8. The wizard will prompt you to add OEM SCSI drivers to your ERD Commander 2005 Boot CD. You must add an OEM SCSI driver if your system uses SCSI devices that Windows XP does not recognize natively.
9. The wizard will prompt you to add network adapter drivers to your ERD Commander 2005 Boot CD. You must add an OEM network adapter driver if your system uses a network adapter that Windows XP does not recognize natively.
10. The wizard will prompt you to add any additional files that you would like to be included on the CD.
11. The wizard will then prompt you to specify the destination of the generated ISO image. The image can range from 150MB to 250MB of disk storage and requires an .iso file extension.
12. In the final step, the Boot CD Wizard will search your system for a compatible CD recordable drive. If a supported drive is found, it will offer to burn the ISO image to disk for you. You can then use a CD duplicator, duplicating service, or CD-burning software to make any additional copies you may need as permitted within the license agreement.

If the wizard does not find a supported drive, you will need to utilize the CD-burning software that came with your drive or use third party software that supports burning an ISO to CD. Most popular CD burning applications offer the option to write a CD from an ISO file. Check with your CD recording software's documentation for information on how to do so. **Note that you cannot use the CD burning software built into Windows XP for this task**

NOTE: For more detailed information on any of the steps above, please refer to the ERD Commander 2005 Help File.

V. Booting from a Custom Boot CD

If your Administrator's Pak license requires a USB-Port Dongle:

1. Do NOT insert the dongle yet.
2. Start the computer.
3. Insert the ERD Commander 2005 Boot CD.
4. After a short delay, you will be notified that the license requires a dongle.
5. Insert the USB-port dongle and click **Retry**.
6. If the Activation Key file is valid and the dongle is properly attached, the logon screen will be displayed and ERD Commander 2005 will function normally.

If your Administrator's Pak license requires a Parallel-Port Dongle:

1. Plug the dongle into the parallel port.
2. Insert the ERD Commander 2005 Boot CD.
3. Start the computer.
4. If the Activation Key file is valid and the dongle is properly attached, the logon screen will be displayed and ERD Commander 2005 will function normally.

If your Administrator's Pak license does not require a dongle:

1. Insert the ERD Commander 2005 Boot CD.
2. Start the computer.
3. If the Activation Key file is valid, the logon screen will be displayed and ERD Commander 2005 will function normally.

VI. ERD Commander 2005



With ERD Commander 2005, you can access and repair an otherwise unbootable system in a familiar, Windows XP-like environment. It provides flexible diagnostic and troubleshooting tools to help you determine why a system will not boot and powerful repair tools to correct a wide range of problems.

Requirements

ERD Commander 2005 requires that the target system have a bootable CD-ROM drive, and one of the following operating systems:

- Windows NT 4 Service Pack 6a
- Windows 2000
- Windows XP (x86 versions)
- Windows Server 2003 (x86 versions)

Regardless of the operating system, ERD Commander 2005 requires a minimum of 64MB (128MB recommended) of system RAM and an Intel Pentium (or compatible) 166 MHz or faster processor, as well as a CD-ROM drive and a computer with BIOS that supports booting from that CD-ROM drive.

The ERD Commander 2005 Boot CD Wizard runs on x86 versions of Windows 2000, Windows XP and Windows Server 2003. It is not supported on earlier versions of Windows, or 64-bit versions of Windows XP or Windows Server 2003 running on Intel Itanium or 64-bit Extended systems.

For more specific information about the requirements for the individual utilities included in ERD Commander 2005, refer to the documentation available at <http://www.winternals.com/support/>.

Using ERD Commander 2005

Once the ERD Commander 2005 environment has started you may use the diagnostic and repair tools, accessible directly from the Start menu, to troubleshoot and repair the dead system or to move files to or from the system. The following built-in utilities are specially designed for the pre-boot repair environment:

- Autoruns: View programs configured to start automatically when the system boots or at user login.
- Console: Run batch files or CHKDSK from a command prompt.
- Crash Analyzer Wizard: Diagnose the cause of a system crash.
- Disk Commander™: Repair damaged partition tables, rewrite the MBR, and retrieve data from corrupted or deleted volumes.

- Disk Management: Partition disks and create or format volumes.
- Disk Wipe: Erase disks or volumes via single pass or four-pass secure overwrite with verification.
- Event Log Viewer: Review System, Security, and Application logs.
- Explorer: Copy and move files.
- FileRestore™: Find and recover deleted files.
- File Sharing: Copy files to or from a system via the network.
- Hotfix Uninstall Wizard: Remove a Windows hotfix or service pack.
- Locksmith™: Change Administrator or other local user account passwords.
- Map Network Drive: Assign a drive letter to a network computer or folder.
- Notepad: Edit/create text-based files such as INI files.
- RegEdit: Import and export registry files, and modify registry settings.
- Search: Locate files and folders.
- Service and Driver Manager: Enable or disable services and drivers.
- Solution Wizard: Determine which ERD Commander 2005 utility can best solve your system problem.
- System Compare: Compare the files and registry settings of an unbootable system and a functioning system for differences.
- System File Repair Wizard: Examines Windows system files to ensure they are not corrupt.
- System Info: View OS info, service packs, and configuration.
- System Restore: Roll back Windows XP systems to a working state.
- TCP/IP Configuration: Customize NIC settings for network access.
- Volumes: View detailed info on logical and physical drives.

NOTE: For detailed information on using these tools, please refer to the ERD Commander 2005 integrated Help File or User's Manual.

VII. Remote Recover



Remote Recover allows users to boot a system via a CD or diskette in order to access FAT or NTFS drives from a remote Windows NT/2000/XP/Server 2003 system. With Remote Recover, you can perform any repair or recovery operation on the remote disk that you can perform on your local disks. An operating system does not have to be installed on the target machine in order for Remote Recover to operate, making it an ideal tool for repairing/restoring dead systems throughout the network that are accessible via TCP/IP.

Requirements

You must have the following components in order to install and run Remote Recover:

- A system running Windows 2000, a 32-bit version of Windows XP, or Windows Server 2003.
- A network using the TCP/IP protocol.
- A network interface card and corresponding Windows 2000, Windows XP, or Windows Server 2003 driver for each client system (if using CD-based boot clients). If your clients utilize mass storage controller drivers not supported by Windows (referred to as an OEM storage controller) then you need to provide drivers at client boot disk creation time.
- A network interface card and corresponding NDIS2 drivers for each client system (if using floppy disk-based boot clients).

If you choose to boot client systems using a Remote Recover client CD:

- Recordable CD media for each client boot CD you require.

If you choose to boot client systems using a Remote Recover client diskette:

- A formatted floppy diskette for each client boot diskette you require.

Using Remote Recover

1. Before Remote Recover can be used to recover a dead system, you must run the Client Wizard, accessible from the Tools menu of the host client, to create a boot CD or boot diskette. For detailed instructions, please refer to the Remote Recover integrated Help File or User's Manual.
2. Once you have created a CD, or one or more client diskettes, you are ready to begin making connections to client machines. To make a connection to a client machine:
 - If you created a boot CD insert it into the bootable CD drive of the client machine and boot it.

- If you created a client diskette insert it in drive A:\ of the client machine and boot it. It will load several network drivers and then start the Remote Recover client program.
3. Start the Remote Recover host software by going to the **Start** menu, then **Programs**, then **Winternals Administrator's Pak**, then the **Remote Recover Program Group**, then **Remote Recover**. Once started, Remote Recover broadcasts a query on your network and any clients receiving the broadcast should automatically respond and appear in the left-hand Remote Recover window.
 4. If your client machines are not accessible to the host via network broadcast (for example, if they are on a different subnet), then use the **Add IP** option in the **File** menu to specify the IP address of the machine you wish to connect. Select the **Refresh** button to check again whether the machines are visible.
 5. Connect to the system you want to repair by clicking **Connect** on the **File** menu or the context menu. A list of physical disks attached to the system will appear beneath it in the left side of the Remote Recover window.
 6. To mount one or more drives for access by the host machine, select a partition, disk, or system in the left-side window and click **Mount** in the **File** menu. The selected drives are assigned drive letters and appear in the disk management window on the right. You can then access them from any Windows application — including Explorer, the command prompt, or diskpart — just as you do with any other drive on your system.
 7. When you are finished, click the system from the right-side window and click **Unmount** from the **File** or shortcut menu. If you are accessing mounted volumes as you exit, an error message will appear.

VIII. Crash Analyzer Wizard

With Crash Analyzer Wizard you can quickly and easily diagnose the cause of a Windows crash. It analyzes the crash dump, pinpoints the driver most likely responsible for a crashed system, and helps you take action to resolve the problem. Crash Analyzer Wizard utilizes a copy of the Microsoft Debugging Tools for Windows and can also be run from within the ERD Commander 2005 environment.

Requirements Crash Analyzer requires Internet access and a writable volume formatted with NTFS or FAT.

Using Crash Analyzer Wizard

1. Click the Start menu, then **Programs**, then **Winternals Administrator's Pak**, then **Crash Analyzer Wizard**. Click **Next** at the introductory screen.
2. Select the directory that contains the Microsoft Debugging Tools for Windows package; a link will be provided if you need to download it. Then click **Next**.
3. Select the directory containing symbol files; unless you have previously downloaded them you will need to use the Microsoft Symbol Server to download the symbols. Then click **Next**.
4. Specify the dump file you wish to analyze, then click **Next**. C:\%systemroot%\minidump is the default directory for dump files to be placed. If none have occurred on your system, specify the location where you have copied dump files from another system.
5. The wizard will display information indicating the driver that may have caused the crash you chose to analyze. You can adjust the driver using the Service and Driver Manager, then reboot the system.

IX. FileRestore



With FileRestore you can salvage lost or deleted files. It recovers files emptied from the Recycle Bin, deleted by application programs and remote processes, lost with removed directories, or deleted via the Command Prompt. FileRestore works without modifying the Windows environment, and leaves the Recycle Bin intact. It supports all Windows file systems - NTFS, FAT, and FAT32 - and even recovers compressed files and files deleted from Jaz®, Zip®, floppy drives, and CompactFlash® photo cards.

Requirements

FileRestore runs on all Windows platforms. It recovers files from local drives only; in order to recover files on a network drive the application must run on the file server. Because FileRestore provides access to all deleted files on a system, regardless of which user they originally belonged to, you must have Administrator privilege in order to run it.

Using FileRestore

1. FileRestore can be accessed from either the Windows **Start** menu or from the ERD Commander 2005 **Start** menu. To access FileRestore from Windows, click the **Start** menu, then **Programs**, then **Winternals Administrator's Pak**, then the **FileRestore** icon. To access FileRestore from within the ERD Commander 2005 environment, click the **Start** menu, then **System Tools**, then the **FileRestore** icon.
2. Enter search parameters such as file name, date last modified, size, type, or location, then click **Search Now**.
3. Sort results by selecting the appropriate column heading.
4. Once you have located the deleted file(s) you wish to recover, highlight the files, and select **Copy To Folder...** from the **Menu** bar, select the corresponding tool bar button, or select **Copy To Folder...** from the shortcut menu. You will then be prompted to select a folder as a location for the copied files.



With Filemon Enterprise Edition you can monitor all file system-related activity on your local system or any computer on your network that you can reach via TCP/IP. Data is collected and presented in real-time, so you can see exactly which process is performing an access, when it occurs, the data that is read or modified, and the result of the access. This data will help you isolate problems, so that you can quickly repair faulty systems on your network.

Requirements Filemon Enterprise Edition runs on all Windows platforms. You need a network using the TCP/IP protocol to access other computers on your network. If you wish to run Filemon Enterprise Edition on Windows 95 you must install the WinSock 2 update.

Using Filemon Enterprise Edition

1. Launch the Filemon Enterprise Edition program file from the **Start** menu and it will immediately start capturing file system output. If you run Filemon Enterprise Edition on Windows NT/2000/XP/Server 2003, FILEMON.EXE must be located on a non-network drive and you must have administrative privileges.
2. When Filemon Enterprise Edition is started for the first time it monitors all local hard drives. Accesses that coincide with error messages and unsuccessful accesses allow you to immediately identify missing, corrupt, duplicate, or out-of-date files.
3. Menus, hot-keys, or toolbar buttons can be used to clear the window, select and deselect monitored drives, save the monitored data to a file, and filter and search output. As events are printed to the output, they are tagged with a sequence number.
4. Use the **Filter** dialog, accessed with a toolbar button or from the **Edit** menu, to select the data to be shown in the list view.
5. Use the highlight filter to specify output that you want highlighted in the list view output. Select highlighting colors from the **Edit** menu.



With Regmon Enterprise Edition you can track registry-related configuration problems and analyze application registry usage on your local system, or any computer on your network that you can reach via TCP/IP. Data is collected and presented in real-time, so you can see exactly which process is performing an access, when it occurs, the data that is read or modified, and the result of the access. This data will help you diagnose problems, so that you can quickly repair faulty systems on your network.

Requirements

Regmon Enterprise Edition runs on all Windows platforms. You need a network using the TCP/IP protocol to access other computers on your network. If you wish to run Regmon Enterprise Edition on Windows 95 you must install the WinSock 2 update.

Using Regmon Enterprise Edition

1. Launch the Regmon Enterprise Edition program file from the **Start** menu and it will immediately start capturing registry output. If you run Regmon Enterprise Edition on Windows NT/2000/XP/Server 2003, REGMON.EXE must be located on a non-network drive and you must have administrative privileges.
2. Regmon Enterprise Edition monitors the local registry when it is started for the first time. With the real-time report of successful and failed accesses to the registry you can pinpoint and correct faulty registry settings. You can also learn the location of the registry settings and determine the registry keys affecting application behavior.
3. Menus, hot-keys, or toolbar buttons can be used to clear the window, select and deselect monitored drives, save the monitored data to a file, and to filter and search output. As events are printed to the output, they are tagged with a sequence number.
4. Use the **Filter** dialog, accessed with a toolbar button or from the **Edit** menu, to select the data to be shown in the list view.
5. Use the highlight filter to specify output that you want highlighted in the list view output. Select highlighting colors from the **Edit** menu.

XII. AD Explorer



With AD Explorer you can browse your Active Directory infrastructure, and quickly and easily locate, modify, add, and delete AD objects and attributes.

Requirements AD Explorer runs on Windows 2000/XP/Server 2003. You must have an account with Administrator rights to view or log activity on a system.

Using AD Explorer

1. Click the **Start** menu, then **Programs**, then **Winternals Administrator's Pak**, then **AD Explorer**.
2. AD Explorer displays information in two panes. The Object Pane is the left-hand pane that displays Active Directory objects. The Attribute Pane is the right-hand pane that displays attributes of the object selected in the Object Pane.
3. Use AD Explorer to connect to Active Directory domains; search for objects in the AD; inspect the properties and edit the security permissions of objects; rename, insert, and delete objects; and modify, insert, and delete object attributes.

XIII. Insight for Active Directory



Insight for Active Directory is a real-time Active Directory diagnostic tool that identifies the causes of application and service failures resulting from AD configuration, corruption, and communication issues. This tool displays continuous LDAP communication between any computer and the AD, helping guide the troubleshooting of applications and services that depend on AD.

Requirements Insight for Active Directory runs on Windows 2000/XP/Server 2003. You must have an account with Administrator rights to view or log activity on a system.

Using Insight for Active Directory

1. Click the **Start** menu, then **Programs**, then **Winternals Administrator's Pak**, then **Insight for Active Directory**. It will immediately begin capturing and displaying LDAP traffic.
2. Insight for Active Directory presents activity in two sub-windows. The top sub-window displays a real-time view of LDAP activity on the local system. The bottom sub-window displays detailed information about any LDAP action selected in the top sub-window.
3. By default, the dynamic view scrolls so that it always displays the most recent event. Auto scrolling can be disabled.



With TCPView Professional and TCPVStat, the two components of TCP Tools, you can monitor TCP/IP network activity on Windows systems. TCP Tools shows which process is associated with each TCP/IP address in real-time, so that you can determine the application responsible for specific connections and activity. It also displays the amount of data sent and received over a network connection, which makes it a useful tool for performance diagnostics.

Requirements TCP Tools runs on all Windows platforms; on Windows 95 you will need COMCTL32.DLL version 4.7 or higher and the Windows 95 WinSock 2 update.

Using TCPView Professional

1. To access TCPView Professional click the **Start** menu, then **Programs**, then **Winternals Administrator's Pak**, then **TCPView Professional**. It will immediately begin capturing and displaying TCP/IP network activity.
2. TCPView Professional presents network activity in two sub-windows. The top sub-window shows a static view snapshot of existing TCP/IP endpoints on the system. The bottom sub-window displays a dynamic real-time view of TCP/IP activity.
3. By default, TCPView Professional refreshes the contents of both the static view and the dynamic view once every second. The refresh rate can be changed or disabled.

Using TCPVStat

1. To access TCPVStat click the **Start** menu, then **Programs**, then **Winternals Administrator's Pak**, then **TCPVStat**.
2. TCPVStat is a command-line tool that will immediately begin displaying data such as the process that controls a TCP/IP address, and the amount of data transferred over an endpoint.

NOTE: By default, TCPView Professional and TCPVStat are not included in the typical Administrator's Pak installation. To install them, choose a custom installation.

XV. Technical Support

To view Online Help, press **F1** or click **Help** from within the Administrator's Pak application that you are using.

For a complete User's Guide for Winternals Administrator's Pak, as well as access to the Winternals Support Knowledge Base, visit our support web site at: <http://www.winternals.com/support>.

You may also request help by email for issues not covered in the Online Help or Support Knowledge Base.

- CVisit <http://www.winternals.com/support/getsupport.aspx>
- CSend an email to: support@winternals.com
- CContact your Winternals Partner

Customers who have purchased Product Assurance may receive phone support by calling 512-330-9861. Please have your license number available.

Winternals®

3101 Bee Caves Road

Suite 150

Austin, TX 78746

www.winternals.com

Ph 512.330.9130

Fax 512.330.9131

v.211105