Users Help Manual

Lepide Active Directory Management and Reporting

Warranty Disclaimers and Liability Limitation

Lepide Active Directory Management and Reporting, and any and all accompanying software, files, data and materials, are distributed and provided AS IS and with no warranties of any kind, whether expressed or implied. In particular, there is no warranty for any harm, destruction, impairment caused to the system where Lepide Active Directory Management and Reporting is installed. You acknowledge that good data processing procedure dictates that any program, including Lepide Active Directory Management and Reporting, must be thoroughly tested with non-critical data before there is any reliance on it, and you hereby assume the entire risk of all use of the copies of Lepide Active Directory Management and Reporting covered by this License. This disclaimer of warranty constitutes an essential part of this License.

In addition, in no event does Lepide Software Private Limited authorize you or anyone else to use Lepide Active Directory Management and Reporting in applications or systems where Lepide Active Directory Management and Reporting failure to perform can reasonably be expected to result in a significant physical injury, or in loss of life. Any such use is entirely at your own risk, and you agree to hold Lepide Software Private Limited harmless from any and all claims or losses relating to such unauthorized use.

Trademarks

Lepide Active Directory Management and Reporting is a copyright work of Lepide Software Private Limited. Windows 95®, Windows 98®, Windows ME®, Windows NT®, Windows 2000 Server®, Windows 2000 Advanced Server®, Windows 2003 Server®, Windows XP®, Windows Vista, Windows 7, and MS-DOS, are registered trademarks of Microsoft Corporation.

Contact Information

Email: sales@lepide.com

Website: http://www.lepide.com

Table of Contents

Table of Figures

Users Help Manual for Lepide Active Directory Management and Reporting

1. About Lepide Active Directory Management and Reporting

In this section, you will be acquainted with the various sections covered in this user guide for better use of the Lepide Active Directory Management and Reporting software. You also know about the purpose of developing the Lepide Active Directory Management and Reporting software and how it helps organizations. Apart from this, the software key features are also provided in this section along with the system requirements for proper installation and use of the software.

1.1 Brief about this User Guide

Welcome to the user guide of Lepide Active Directory Management and Reporting – a prominent, professional, and output-driven Active Directory management software. The user guide has been designed to provide system administrators systematic information for effectively using the Lepide Active Directory Management and Reporting software. Therefore, we suggest you to carefully read the user guide before using the software. The user guide comprises the following main sections:

Introduction: Provides overview of the Lepide Active Directory Management and Reporting software, key features, and abbreviations. This section also provides information about the system requirements for successful installation and execution of the software.

Install and Uninstall: Describes the processes to install and uninstall the Lepide Active Directory Management and Reporting software.

Launching the Software: Depicts the processes to start the Lepide Active Directory Management and Reporting software.

Understanding the User Interface: Explores the user interface of Lepide Active Directory Management and Reporting software for its easy and perfect use. In this section, you experience accessing various options for managing Active Directory objects with ease and effectiveness.

Sections of Lepide Active Directory Management and Reporting: Explores the sections covered in the software.

Working with Active Directory: Explores the process using which the administrator can manage Active Directory objects in domains from a central location.

Creating Active Directory Reports: Describes the process to generate, view, customize, save, and print Active Directory reports.

Download Purchase and Register: Provides information about downloading, purchasing, and registering the Lepide Active Directory Management and Reporting software. Apart from this, the information regarding technical support is also provided in this section.

Legal Notices: Provides information about copyright notices, trademarks, disclaimer, and license agreement related to the Lepide Active Directory Management and Reporting software.

1.2 List of Abbreviations

Certain abbreviations have been used throughout this user manual. Please go through the list of abbreviations mentioned below before proceeding to read this user manual. Abbreviations used are:

- **LADMR**: Lepide Active Directory Management and Reporting

- **AD**: Active Directory

- **DC**: Domain Controller

- **AD Queries**: Active Directory Queries

- **WMI Queries**: Windows Management Instrumentation Queries

- **OUs**: Organizational Units

- **DFS**: Distributed File Systems

- **Net APIs**: Network Application Programming Interface

- **WMI**: Windows Management Instrumentation

- **CPU**: Central Processing Unit

- **DNS**: Domain Name System

- **VPN**: Virtual Private Network

- **NAT**: Network Address Translator

- **IPC**: Inter Process Communication

- **I/O System**: Input/output System

- **OS**: Operating System

- **GB**: Gigabyte

- **MB**: Megabyte

- **PDC**: Primary Domain Controller

- **BDC**: Backup Domain Controller

- **DES**: Data Encryption Standard

- **GPO**: Group Policy Object

- **MMC**: Microsoft Management Console

- **SID**: Security Identifier

1.3 Keyboard Shortcuts

Keyboard shortcuts that you can use while using the software are listed in Table 1.1:

Keys combination	Description
Ctrl+ Shift+ D	To clear the list view
Ctrl+ F	To find items in list view
F3	To find items in the Tree view
F5	To refresh tree view as well as list view
Ctrl+ C	To copy contents in list view
Ctrl+ Shift+ F	To Toggle, Enable/Disable filter in list view
Ctrl+ A	To select all in list view
Ctrl+ D	To open "Add Domain" dialog box
Ctrl+ O	To open "Object Manager" dialog box
Ctrl+ P	To print the contents of list view
Ctrl+ S	To open "Save As"dialog box for saving contents of list view.
F1	To open Help Contents of Lepide Active Directory Management and Reporting
Ctrl+ Q	To open dialog box to query Active Directory objects
Ctrl+ Shift+ T	To view settings of Lepide Active Directory Management and Reporting

1.4 Introducing Lepide Active Directory Management and Reporting

Microsoft Active Directory (AD) is a directory structure developed by Microsoft Corporation to store objects and their attributes in hierarchical format. Active Directory stores three types of objects that incorporate **Resources** like printers, **Services** like email, and **Users** including users' accounts and groups. In small as well as large organizations, Active Directory serves the purpose of organizing information about objects at a central location. In organizations, system administrator/help desk looks after managing objects in Active Directory.

Managing Active Directory is a challenging task for an administrator who deals with it on regular basis. Adding and managing domains in Active Directory, managing computers, and managing users' accounts and password are extremely time-consuming, error-prone, and tiresome processes especially in large and

complex Windows environment. The administrator must have vast knowledge about executing Active Directory management related tasks using native Microsoft Management Console (MMC) snap-ins.

Lepide Active Directory Management and Reporting simplifies managing Windows Active Directory by providing the administrator a Windows explorer like user interface. The software provides the administrator a central location to easily and impeccably manage all Active Directory objects across multiple domains. Incorporating the advance domain management functions in one tool, LADMR meets all AD management related requirements.

The administrator can save a considerable amount of time by accessing all the AD management options and Microsoft Management Console (MMC) snap-ins by using this centralized tool. Moreover, central administration of AD helps you exercise an effective control over computers and devices in a domain by simplifying the process of auditing networks. You can use LADMR to manage and administer users, groups, files, resources, etc. on both local and remote computers in your domain.

Advanced AD management features like object management, schema management and WMI management make LADMR the most comprehensive AD administration tool available. Moreover, the software helps the administrator to have a quick overview about the status of AD objects through its automatically generated AD reports.

1.5 Key Features

LADMR – a complete tool for performing all AD management related operations comprises following outstanding features:

- **Domain Management**: Adding domains in Windows Active Directory has been much simplified with LADMR. The administrator can now add a domain in AD in just few mouse clicks instead of executing complex commands. In addition, performing the tasks, such as creating and managing containers/OUs, adding computers in domains, managing available computers in domain, and so on are no more time-consuming and error-prone, as these tasks can now be performed using simple and self-explaining graphical user interface of LADMR.

- **Computers Management**: While managing computers in a domain, the administrator has to perform various tasks in his day-to-day life for effective management of computers. Some of those tasks are moving computers from one OU to another, enable the disabled computers, changing group of a computer, and modifying general details of computers. LADMR eases the life of the administrator by offering bulk computer management that is the multiple tasks can be performed concurrently on various computers in a domain. Through, bulk computer management LADMR not only simplifies computers management but also saves a considerable amount of the administrator's time.

- **Users Management**: Creating and managing users' accounts, configuring users' attributes, doing password reset, enabling/disabling users' accounts, and moving users from one organizational unit to another are some of the daily activities of the administrator. Effectively doing all these tasks on a large scale and in timely manner is difficult, tedious, and error prone as well. Besides that, good knowledge about Active Directory and the native tools used for users management is must. But, with LADMR novice administrator can also effectively perform users management related task. The software enables the administrator to quickly and flawlessly manage users' accounts on both local and remote computers by performing mass users' management. By performing the mass users' management, the administrator can concurrently execute operations (like password reset, move users between OUs, unlock users accounts, etc.) on all users accounts in a domain.

- **Groups Management:** In Active Directory, groups are divided into two categories – Security and Distribution. Groups help the administrator to manage AD objects flexibly. But, creating groups and assigning their scope is very time-consuming and difficult. LADMR provides a simple-to-use wizard for

creating group, specifying group's type, and assigning group's scope. In addition, the administrator can easily move a group from one container to another, rename group, add members in a group, and send an email to group.

- **Policies Management**: System administrator is often tasked to apply stringent accounts password, accounts lockout, and audit policies. LADMR helps the administrator to quickly apply tough accounts' password, account lockout, and audit policies on all users' accounts in a domain.

- **Tasks Management**: The native task-scheduling tool does not provide any option to view, schedule, and manage tasks on remote computers in a domain; therefore, the administrator has to visit every remote computer to schedule and manage tasks. Thus, using native task-scheduling tool is very time consuming. LADMR enables the administrator to perform all tasks management related operations on any computer within a domain without letting him to stop over every computer.

- **Printers Management**: Every version of the Windows operating system including Windows Server 2000, 2003, and above, provides built-in tool to manage printers on a local computer. But, there is not much functionality available in built-in printer's management tool to effectively manage printers on remote computers from a central location. To manage printers on remote computers within a local network, the administrator has to move on every computer, which becomes tedious especially in large network. Furthermore, a significant amount of the administrator's time, which can be used in some other prolific task, gets wasted. LADMR saves the administrator's time by centralizing the printers' management.

- **Shares Management**: Users often need to create shared directories for sharing objects in network and for that; they contact the administrator/help desk staff. The administrator/help desk staff has to personally visit the users' computers, which consumes a lot of time. LADMR eases shares management by enabling the administrator to manage shared objects from a central location.

- **Services and Device Management**: Managing services and devices on both local and remote computers is a tough job, as MMC snap-in does not provide the facility to manage services and devices on remote computers. LADMR has simplified managing services and devices on local and remote computers. Now, the administrator can easily view and manage services and devices without moving from one computer to another.

- **Events Management**: Effective events management helps the administrator to gather relevant information about the activities performed in Windows operating system. LADMR contains its own events management function using which event logs for any number of computers in a domain can be easily managed.

- **Quick Access of System Tools**: Every version of Windows operating system incorporates some administrative tools that help the administrator to properly manage users account, password, services, events, etc. Accessing those tools is a lengthy process; therefore, time consuming too. LADMR has made accessing system tools fast; opening an administrative tool is now just a single step process instead of lengthy multi-steps process.

- **Centralized Registry Management**: Windows registry plays an important role in storing and managing configuration settings and options on Windows operating system. However, accessing Windows registry is a difficult task. The administrator needs to remember typical command for accessing Windows registry. Now, accessing Windows registry has been made simple. There is no need to execute any command for getting an access to Windows registry. LADMR offers an easiest way to access Windows registry from within the software interface and this is possible in just a single mouse click.

- **Exchange Management**: LADMR also eases the task of the administrator by providing him options to manage users' mailboxes on Exchange server from a centralized location. The administrator can now easily create users mailboxes on Exchange Server, view properties of the users mailboxes, and delete mailboxes. The administrator can perform all these functions through a centralized location.

- **Automatic AD Reports**: In addition with helping the administrator to manage AD objects, LADMR facilitates him to audit activities and status of AD objects. The software automatically generates more than 65 customizable reports using which the administrator can grab updated information about users accounts, accounts password, accounts lockout, GPOs, etc. The software also allows you to print and/or save the reports. Using this amazing AD management and reporting tool, reports can be saved in various formats, such as RTF, TXT, CSV, PDF, and HTML.

- **Intuitive User Interface**: Simplicity of the user interface of LADMR ties the administrator with it. Its Windows explorer like user interface gives a familiar look to the administrator. Moreover, the embedded help content and tips given in the software interface guides its users at every step thus, using the software becomes so easy.

- **Support**: Round the clock technical support is provided to the users of LADMR software.

- **Free Demo**: LADMR is also available for a free trial. One can take advantage of the trial version for 30 days. However, the trial version has some limitations like does not save and print AD reports; it is fully functional.

1.6 System Requirements

Before you start installing Lepide Active Directory Management and Reporting software, make sure that your computer meets the following system requirements:

Basic System Requirements

- Pentium Class Processor

- 128 MB RAM (256 recommended)

- 20 MB of Disk Space for Software installation

Supported Platforms

- Windows 2000

- Windows 2003

- Windows XP

- Windows Vista and later versions

  > ✎ Note: Admin pack should be installed on client computer(s)

2. Install and Uninstall

After being familiar with the software overview, key features, and system requirements, you can move ahead to install the software. In this section, you acquire information about the process to install the Lepide Active Directory Management and Reporting software.

2.1 Install the Software

Before you start installing LADMR, makes you sure that the software installer file is available on your computer. If the file is not available then you can download the file from our Website - http://www.lepide.com

After you have downloaded the installer file, execute the following steps to install the software:

1. Double-click the Lepide Active Directory Management and Reporting's installer file.

2. Follow the on-screen instructions. When the installation process completes "Completing the Lepide Active Directory Management and Reporting Wizard" message appears on the software installation window.

3. Click the **Finish** button to launch the software.

2.2 Uninstall the Software

There can be a situation when you need to uninstall the LADMR software. The software can be uninstalled from your system in following two ways:

- Uninstall through Windows Start Menu

- Uninstall through Control Panel

  ✎ Before you start uninstalling the LADMR software makes you sure that the software is not running.

2.2.1 Uninstall through Windows Start Menu

Execute the following steps to uninstall LADMR through Windows Start menu:

1. Click **Start > All Programs** > **Lepide Active Directory Management and Reporting** > **Uninstall Lepide Active Directory Management and Reporting.** A confirmation message appears to let you affirm the un-installation process.

2. Click the **Yes** button to uninstall the software.

3. Click the **OK** button to finish the un-installation process.

LADMR is successfully uninstalled from your computer system.

2.2.2 Uninstall through Control Panel

Execute the following steps to uninstall LADMR through Control Panel:

1. Click **Start** -> **Control Panel**. **Control Panel** window appears.

2. Double-click the **Add or Remove Programs** icon. A list of the programs installed on your computer appears.

3. Select Lepide Active Directory Management and Reporting and click the **Remove** button. A confirmation message before un-installing the software appears on the screen.

4. Click the **Yes** button to un-install the software.

5. Click the **OK** button to complete the un-installation process.

LADMR is successfully uninstalled from your computer system.

3. Launching the Software

Now, when you have successfully installed the Lepide Active Directory Management and Reporting software, let us see the process to start the software. Execute the following steps to launch the software through Windows Start menu:

1. Click **Start** > **All Programs**.

2. Select **Lepide Active Directory Management and Reporting** > **Lepide Active Directory Management and Reporting**.

Home page of the Lepide Active Directory Management and Reporting appears, as shown in Figure 3.1:
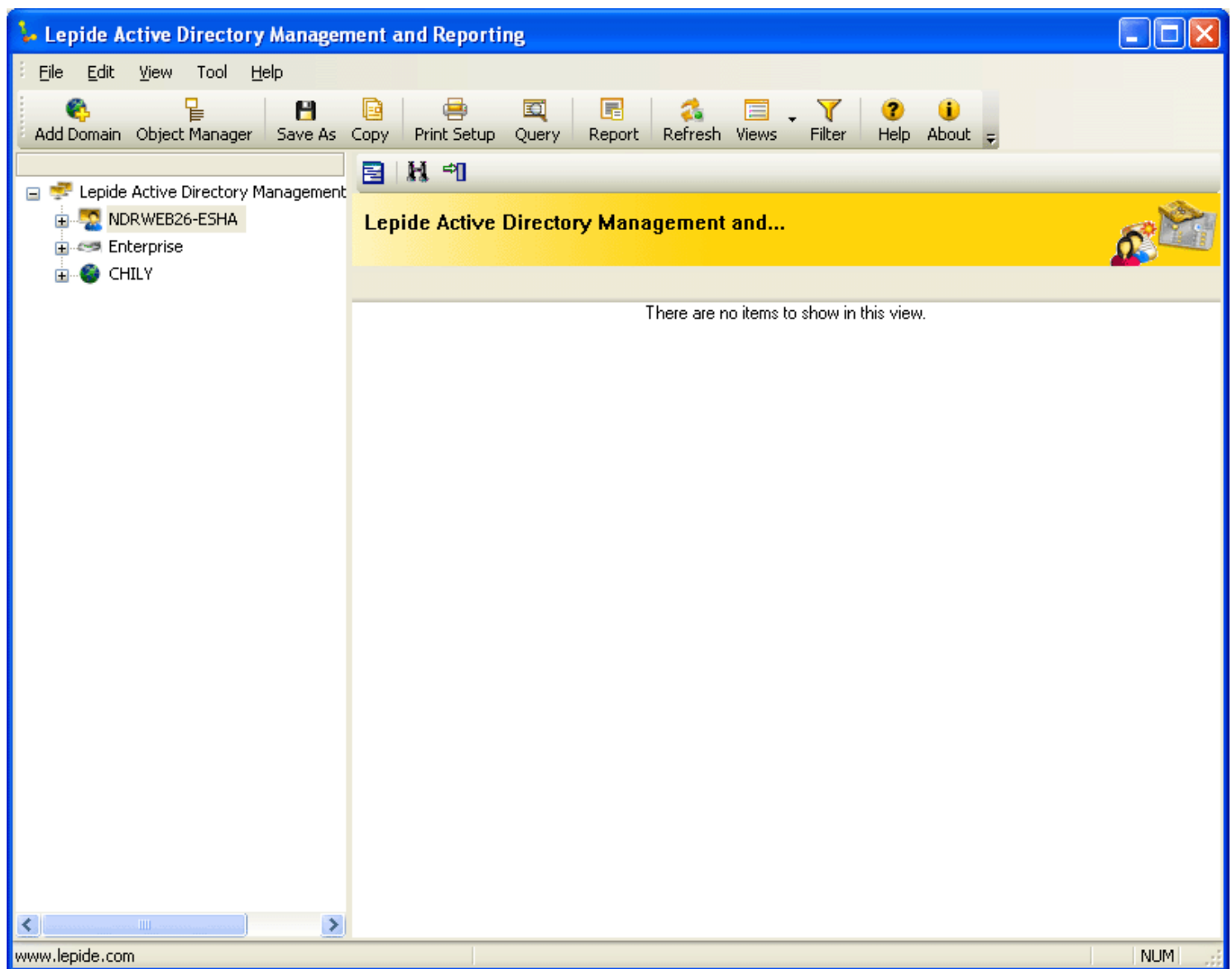
Figure 3.1: Software Home Window at Launch

4. Understanding the User Interface

After you have become familiar with the process to launch the software let us have a look on the software GUI. The software has self-descriptive interface with various easy-to-use options that make the process of AD Management fast, simple, and accurate. In this section, we explore the software GUI in following sub-headings:

- Menu Bar

- Tool Bar

- Top Panel

- Left Panel

- Right Panel

Figure 4.1 is displaying various sections on the software GUI:
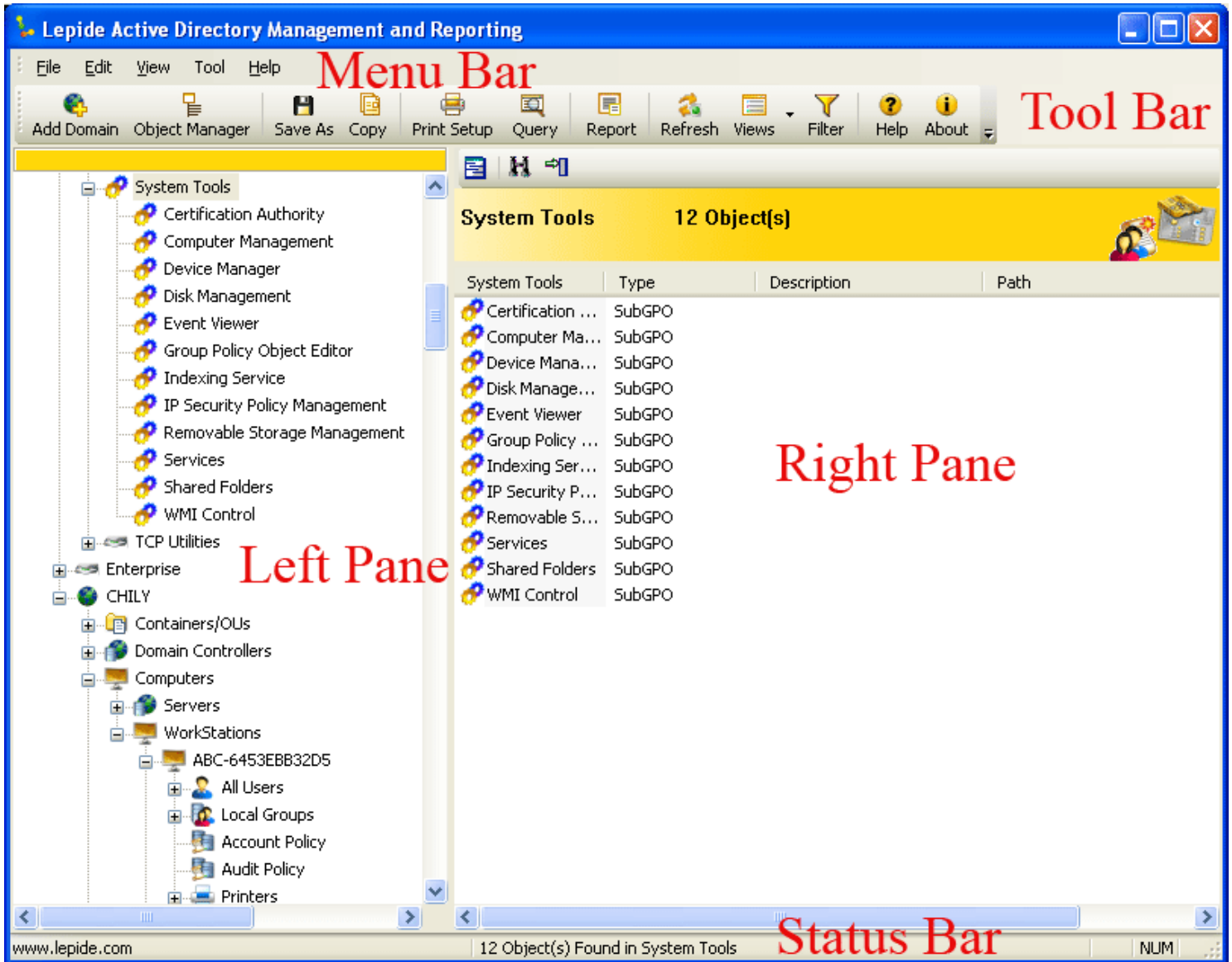
Figure 4.1: Displaying Various Sections of the Software GUI

When you launch the software, it displays the current computer and user's domain in left panel.

4.1 Menu Bar

Menu bar of LADMR comprises following main menus:

- File Menu

- Edit Menu

- View Menu

- Tool Menu

- Help Menu

File Menu

File menu of LADMR is shown in Figure 4.2:
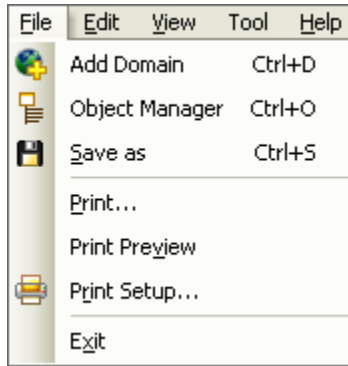
Figure 4.2: File Menu

Table 4.1 lists the options of **File** menu:

Option	Description
Add Domain	Click to add a new domain to administer. LADMR always includes user's current domain in the left tree pane. More domains can be added with this option.
Object Manager	Click to access the "Object Manager" dialog box, which helps to view and modify Performance Counters, AD Queries, and WMI Queries.
Save As	Click to save listed items of right panel in desired format i.e. .html, .csv, .pdf, .rtf, and .txt.
Print	Click to print the listed items of right panel through the default printer.
Print Preview	Click to preview before printing.
Print Setup	Click to configure printing properties.
Exit	Click to close Lepide Active Directory Management and Reporting software.

Edit Menu

Edit menu of LADMR is shown in Figure 4.3:
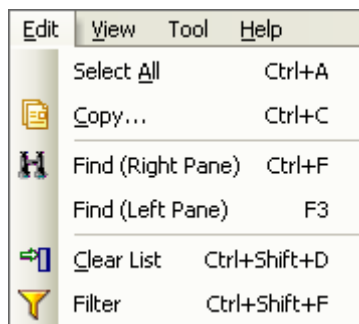
Figure 4.3: Edit Menu

Table 4.2 lists the options of **Edit** menu:

Option	Description
Select All	Click to select all the objects listed in the right panel.
Copy	Select to copy selected objects from the right panel. Copied objects can then be inserted/pasted to a text file, excel file, or a document file.
Find (Right List Pane)	Click to search desired objects in the right panel.
Find (Left Tree Pane)	Click to search desired objects in the left tree pane.
Clear List	Click to clear/remove the list of objects in the right panel.
Filter	Click to display and hide the filter option for the list displayed in the right panel.

View Menu

View menu of LADMR is shown in Figure 4.4:
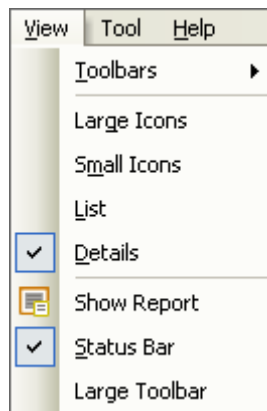
Figure 4.4: View Menu

Table 4.3 lists the options of **View** menu:

Option	Description
Toolbars	Click Toolbars > Standard to display/hide toolbar.
Large Icons	Click to view objects in right panel as large icons.
Small Icons	Click to view objects in right panel as small icons.

List	Click to view objects in right panel as a list.
Details	Click to view objects in right panel as a detailed list.
Show Report	Click to open the reporting console of LADMR. The report section displays various reports for the selected domain.
Status Bar	Click to display/hide status bar.
Large Toolbar	Click to view the toolbar icons in large view.

Tool Menu

Tool menu of LADMR is shown in Figure 4.5:
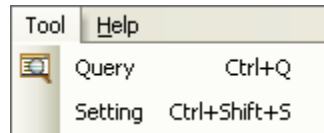
Figure 4.5: Tools Menu

Table 4.4 lists the options of **Tool** menu:

Option	Description
Query	Click to open the dialog box to run queries to search objects in a network: groups, printers, users, contacts, computers, OUs, shared folders, people and other objects.
Setting	Click to manage display settings of Lepide Active Directory Management and Reporting. Display settings can be configured for Printers, Services, Shares, Print Jobs, Disk Space, Events, Scheduled Jobs and Directory Security.

Help Menu

Help menu of LADMR is shown in Figure 4.6:
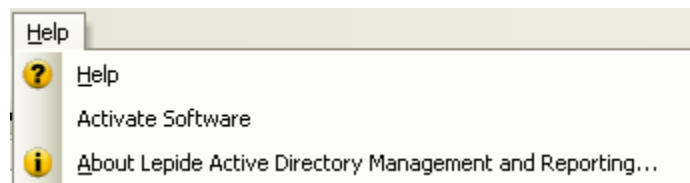
Figure 4.6: Help Menu

Table 4.5 lists the options of **Help** menu:

Option	Description
Help	Click to view help contents for Lepide Active Directory Management and Reporting software.
Activate Software	Click to activate Lepide Active Directory and Management Reporting software.
About Lepide Active Directory Management and Reporting...	Click to view version and support related information of Lepide Active Directory Management and Reporting software.

4.2 Tool Bar

The toolbar comprises several buttons that can be used to quickly perform operations that can otherwise be performed by using the menu bar. Table 4.6 lists the buttons available in the Tool bar:

Button	Description
Add Domain	Click to add a new domain to administer. Local domain is included by default in LADMR. More domains can be added with this option.
Object Manager	Click to access the "Object Manager" dialog box, which helps to view and modify Performance Counters, AD Queries, and WMI Queries.
Save As	Click to save listed items of right panel in desired format i.e. .html, .csv, .pdf, .rtf, and .txt.
Copy	Click to copy selected text from the right panel. Copied objects can then be inserted/pasted to a text file, excel file or a document file.
Print Setup	Click to configure printing properties.
Query	Click to open the window to run queries to search objects in a network: groups, printers, users, contacts, computers, OUs, shared folders, people and other objects.
Report	Click to open the reporting console of LADMR. The reporting console displays various reports for the selected domain.
Refresh	Click to refresh all the panes in the software.

Views	Click to change the view of listed items of right panel.
Filter	Click to display and hide the filter option for the list displayed in the right panel.
Help	Click to view help contents for Lepide Active Directory Management and Reporting software.
About	Click to view version and support related information of Lepide Active Directory Management and Reporting software.

4.3 Top Panel

Buttons available in the top panel enable you to perform operations pertaining to the contents of the right panel. Table 4.7 lists the buttons available in the Top panel:

Button	Description
	Click to select all objects listed in the right panel. After selection, right click and select "Copy to Clipboard" option to copy the selected items to any text editor.
	Click to search desired objects in the right panel.
	Click to clear the list of objects in the right panel.

4.4 Left Panel

The left panel of the software displays a hierarchical tree "Lepide Active Directory Management and Reporting." The tree comprises three expandable nodes:

1. The first node corresponds to the local computer (computer where Lepide Active Directory Management and Reporting is installed).

2. The second node corresponds to "Enterprise," which can be expanded to view workgroup computers in Windows style network browser.

3. The third node "Domain" corresponds to domain name in which the local computer exists. This node can be expanded to view and manage all other users, groups, etc. on the domain.

Figure 4.7 displays the left panel of LADMR:

Figure 4.7: Left Panel of LADMR

4.5 Right Panel

The right panel of LADMR displays contents corresponding to the objects selected from the hierarchical tree displayed in the left panel. Figure 4.8 displays the right panel of LADMR:

Figure 4.8: Right Panel of LADMR

5. Sections of Lepide Active Directory Management and Reporting

The management options available in Lepide Active Directory Management and Reporting software can be divided into following major categories:

- Local Computer

- Workgroup

- Domain

- Reports

5.1 Local Computer

The name of the local computer appears as the first node in the tree displayed in the left panel of the software. The node corresponding to local computer can be expanded by clicking the + sign displayed to the left of the node. Once expanded, various child nodes corresponding to users, groups, etc. are displayed.

The child nodes of the local computer node may vary depending upon the class of computers that the local computer belongs to. If the local computer is a domain controller or a member server, it will display additional nodes, such as, DFS, which will not be displayed otherwise. LADMR uses Net API to display the configuration options for the local computer.

You can right click the local computer node in the left panel and select **Properties** to view the properties of the computer. When you right click the local computer node in the left panel and select the Properties option, the **System Properties** dialog box appears. This dialog box has seven tabs that are described below:

- **Directory**: Description, Directory Path, and Names are displayed in this tab.

- **Object**: Creation, modification, category, logon - logoff information, password set time information is displayed in this tab.

- **MemberOf**: Information about the domain of which the local computer is a member is displayed in this tab.

- **Software**: List of installed software applications on the local computer is displayed in this tab.

- **System**: CPU Information, Operating System information, Logged On Users, and Other System Information is displayed in this tab.

- **Environment**: Environment variables, with property names and their values, are displayed in this tab.

- **Network**: Network transports, DNS host name, network card properties, IP address, subnet mask information, and WINS Server information is displayed in this tab.

> ✎ Note: Of the various tabs displayed on the **Properties** screen, **Directory**, **Object**, and **Memberof** will not be displayed if the computer is not a part of any domain.

5.2 Workgroup

You can use Lepide Active Directory Management and Reporting software to manage your workgroup resources. You will need to expand the **Enterprise** node under the root node in the left panel to view a Windows style display of your workgroup computers. The Networks node under the Enterprise node can be further expanded to display the following three nodes:

- Microsoft Terminal Services

- Microsoft Windows Network

- Web Client Network

To access workgroup computers, you will need to expand the **Microsoft Windows Networks** node.

5.3 Domain

The domain node appears after the **Enterprise** node in the left panel of the software. The node corresponding to domain can be expanded by clicking the + sign displayed to the left of the node. Once expanded, various child nodes corresponding to Organizational Units, Domain Controllers, Groups (local, global, universal), Schema management etc. are displayed.

Currently configured domain gets automatically added in LADMR. You can remove this domain from the software but it will reappear when **Refresh** button is clicked or software is re-opened.

'N' number of domains can be added to LADMR. Feature rich LADMR helps you to manage local and remote domain from one central place. You can right click the domain name node in the left panel and view shell properties with other options for a domain. On right clicking the Domain node in left panel, you see the following options to manage objects:

- **Shell Properties**: View shell properties of the domain. You can easily manage the General, Managed by, Object and Security attributes for a domain.

  > ✎ **Note:** Shell properties will be available only for Local and Trusted domains.

- **View FSMO Roles**: View Domain-wide and Forest-wide FSMO roles for the domain.

- **Container/OUs**: Displays containers/organizational units of the domain.

- **Show Trusts**: View details of trusted domains and trusting domains. This presents a list of domains, which have been termed as trusted by you and those domains, which have termed you as trusted.

- **Send Messages**: Send message to all users in domain.

- **View Deleted Objects**: View list of all objects, which were recently deleted from active directory. Deleted objects remain in the active directory until the TombStone time arrives for individual objects. Before this time, the deleted objects are restorable. After the TombStone time is crossed, the deleted object is permanently deleted from the active directory. **(Restore deleted object function is available for local and trusted domains only).**

- **Delete Domain Entry**: This will delete the domain added in LADMR. New or Same domain can be added again using the **Add Domain** option.

- **Authentication Credentials**: This will display the user credentials dialog box for the domain server, which can be modified.

- **Synchronize Objects**: This will help to synchronize objects of PDCs and BDCs. LADMR asks your confirmation before starting the synchronization process.

- **Browse Group Policy Objects**: This will help to view and edit various group policy objects, which are linked or not linked to the Domain or Organizational Unit

5.4 Reports

Reports section in Lepide Active Directory Management and Reporting contains all the domain reports for:

- Users

- Groups

- Passwords

- Computers

- OUs

- GPOs

- Accounts

- Logon Reports

- Other Reports

5.4.1 Understanding the User Interface of Reporting Console

Graphical user interface of reporting console of Lepide Active Directory Management and Reporting software is user friendly, easy to understand with attractive interface. To access the reporting console of LADMR, execute the following steps:

1. Select a domain in the left panel.

2. Click the **Reports** button in the **Tool** bar. Reporting console of LADMR appears, as shown in Figure 5.1:
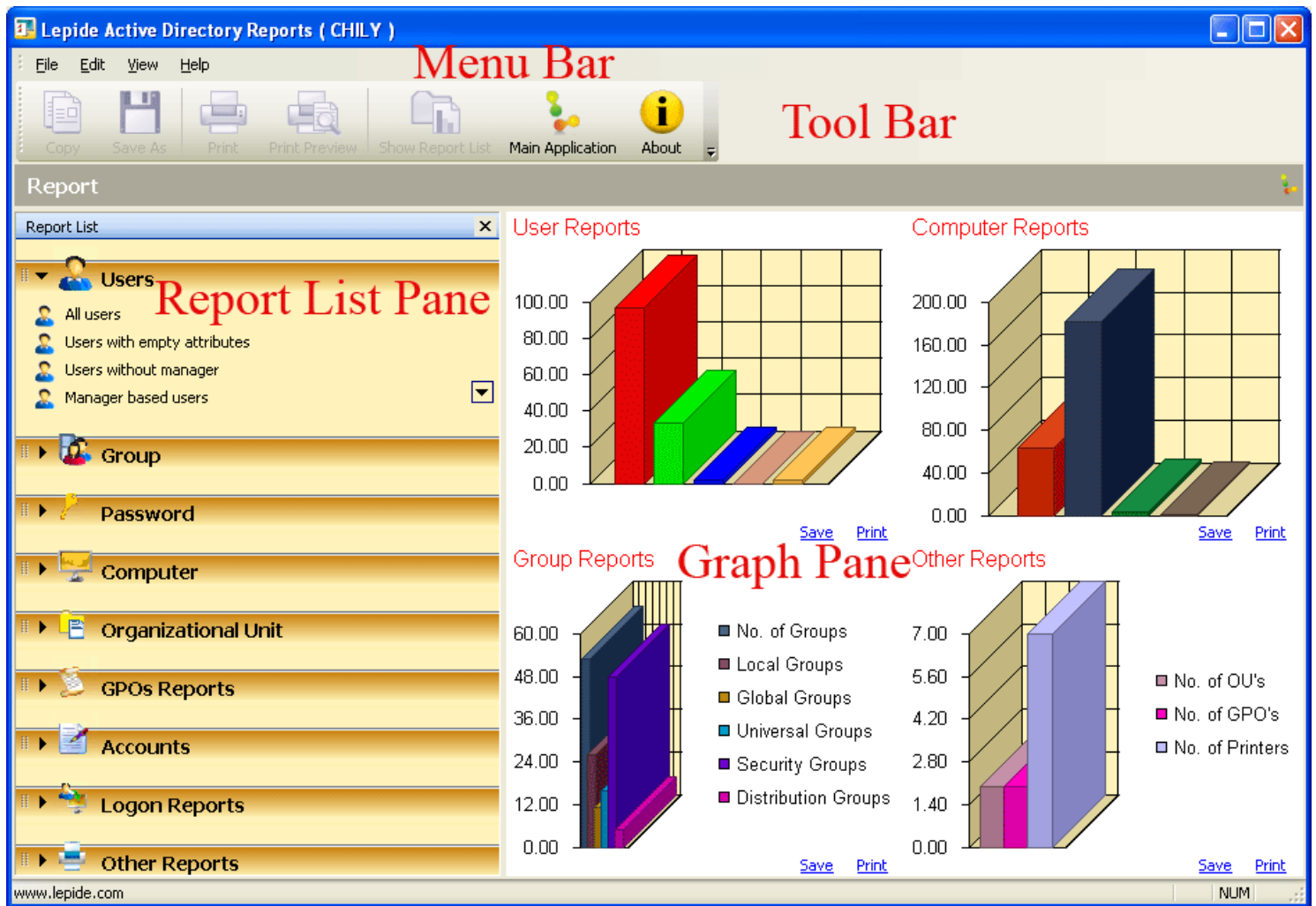
Figure 5.1: Displaying Reporting Console

Reporting console of the software is explored in the following sections:

- Menu Bar

- Tool Bar

- Top Panel

- Report List Panel

- Graph and Report Panel

5.4.4.1 Menu Bar

Menu bar of LADMR reporting console comprises following main menus:

- File Menu

- Edit Menu

- View Menu

- Help Menu

File Menu

File menu of LADMR reporting console is shown in Figure 5.2:
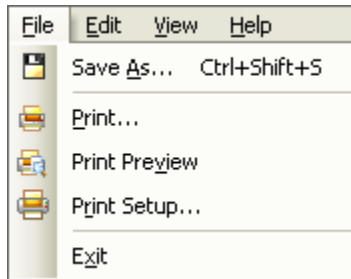
Figure 5.2: File Menu

Table 5.1 lists the options of **File** menu:

Option	Description
Save As	Select to save the report in desired format: HTML, CSV, PDF, RTF, and TXT
Print	Select to print the report
Print Preview	Select to preview the report before printing
Print Setup	Select to manage printer and page setup properties for printing the report
Exit	Select to close Lepide Active Directory Reporting console

Edit Menu

Edit menu of LADMR reporting console is shown in Figure 5.3:
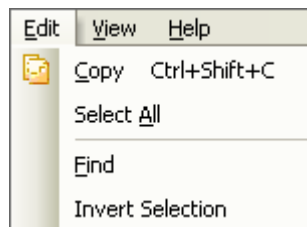
Figure 5.3:Edit Menu

Table 5.2 lists the options of **Edit** menu:

Option	Description
Copy	Select to copy the selected field items from right panel

Select All	Select to select all the items listed in right panel
Find	Select to find any object from the right panel
Invert Selection	Choose to select or deselect the listed items from right panel

View Menu

View menu of LADMR reporting console is shown in Figure 5.4:
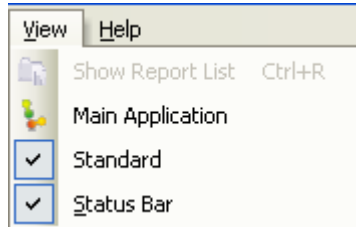
Figure 5.4: View Menu

Table 5.3 lists the options of **View** menu:

Option	Description
Show Report List	Select to view and hide the report list panel
Main Application	Select to switch to main application "Lepide Active Directory Management and Reporting"
Standard	Select to view and hide the toolbar
Status Bar	Select to view and hide the status bar

Help Menu

Help menu of LADMR reporting console is shown in Figure 5.5:
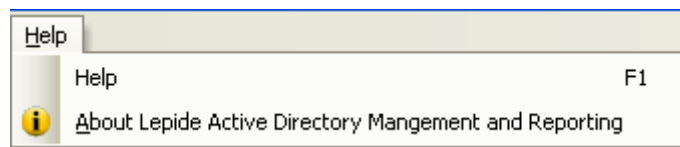
Figure 5.5: Help Menu

Table 5.4 lists the options of **Help** menu:

Option	Description
Help	Select to view help contents of Lepide Active Directory Reports

About Lepide Active Directory Management and Reporting…	Select to view version and support related information of Lepide Active Directory Management and Reporting

5.4.4.2 Tool Bar

The toolbar comprises several buttons that can be used to quickly perform operations that can otherwise be performed by using the menu bar. Table 5.5 lists the buttons available in the Tool bar:

Button	Description
Copy	Click to copy the selected field items from right panel.
Save As	Click to save the report in desired format: HTML, CSV, PDF, RTF, and TXT
Print	Click to print the report
Print Preview	Click to view preview before printing the report
Show Report List	Click to view and hide the report list pane
Main Application	Click to minimize Lepide Active Directory Reporting console and access Lepide Active Directory Management and Reporting window
About	Click to view version and support related information of Lepide Active Directory Reports

5.4.4.3 Top Panel

The top panel of the software displays information related to selected report for viewing purposes. You can also filter your report according to the number of days by entering a numeric value in **Enter the no. of days** field and clicking the **Generate** link.

The **Graph View** link enables you to view displayed report in graphical format in right panel. The **Add/Remove Columns** links helps you to add or remove any desired or unwanted columns to view in the right panel for the generation of any report.
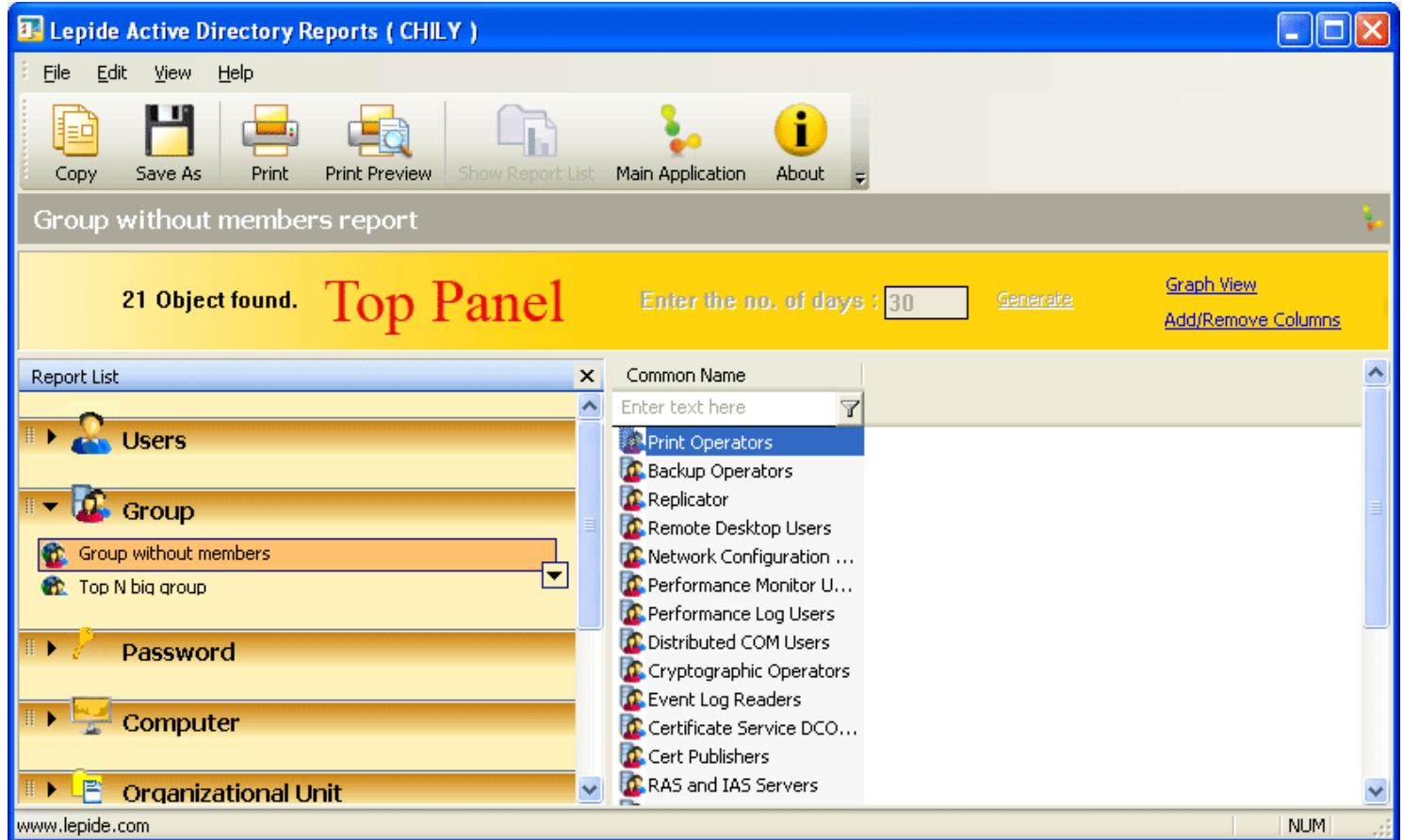
Figure 5.6: Displaying Top Panel

Add/Remove Columns

Click the Add/Remove Columns link if you want to add more columns to the generated reports. Attribute Customization.. dialog box appears which contains following two sections:

- **Available Attributes**: This section contains predefined attributes for the selected report for generation. Select the attribute name and click **Add**. Selected attributes will get transferred to the "Selected Attributes section". You can remove any attribute with **Remove** button.

  "The list of pre-defined attributes displayed in this section keeps on changing as per the selected report in the left panel."

- **Selected Attributes**: This section contains the pre-defined attributes for report generation. Order of these attributes can be changed with **Up** and **Down** buttons and these attributes can be removed with **Remove** button.
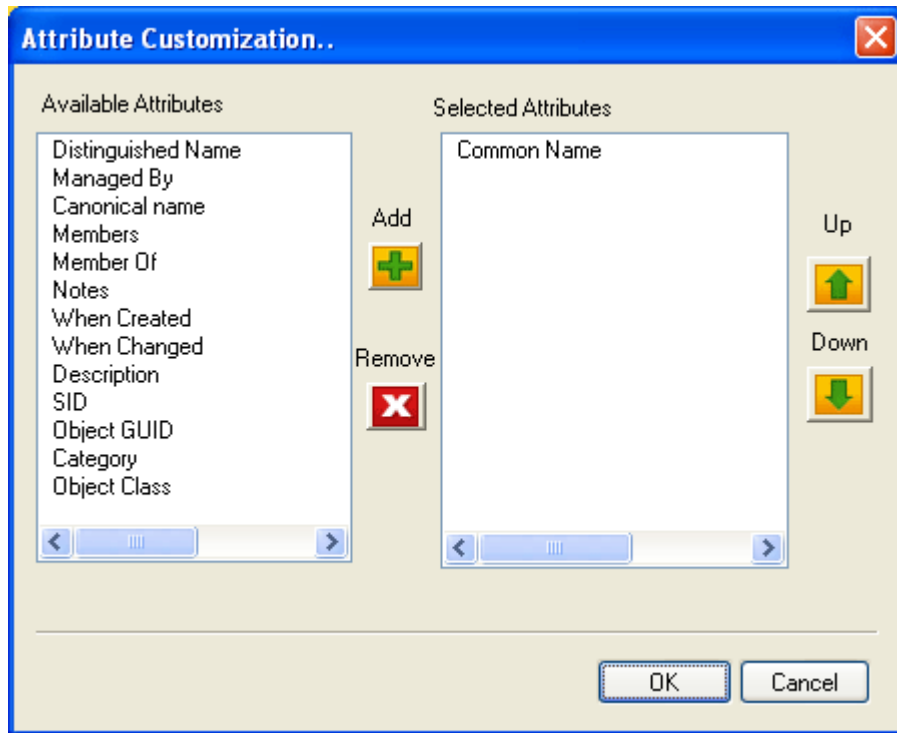
Figure 5.7: Customizing Report

5.4.4.4 Report List Panel

The left panel of the software is termed as **Report List Panel** of Lepide Active Directory Reports. This panel displays complete report list, which is available and can be viewed to gather entire information. This panel can be hided and viewed by selecting **View >> Show Report List** or clicking the **Show Report List button** from the toolbar.

LADMR will display the domain name in its title section. Title of the Reporting console displays **Lepide Active Directory Reports (LEPIDE)**, where LEPIDE is name of the domain for which reports are being generated.

Figure 5.8: Displaying Report List Panel

5.4.4.5 Graph and Report Panel

The right panel of the LADMR reporting console is termed as **Graph and Report Panel**. This panel displays graphical and tabular reports for the selected report items in the report list panel.

You can easily "Save" and "Print" reports in .BMP format with **Save** and **Print** links in the panel. LADMR provides the feature to change the graph view from 2D view to 3D view. Press **Ctrl**, move the mouse cursor on top of the graph, and rotate it to have 2D or 3D view.
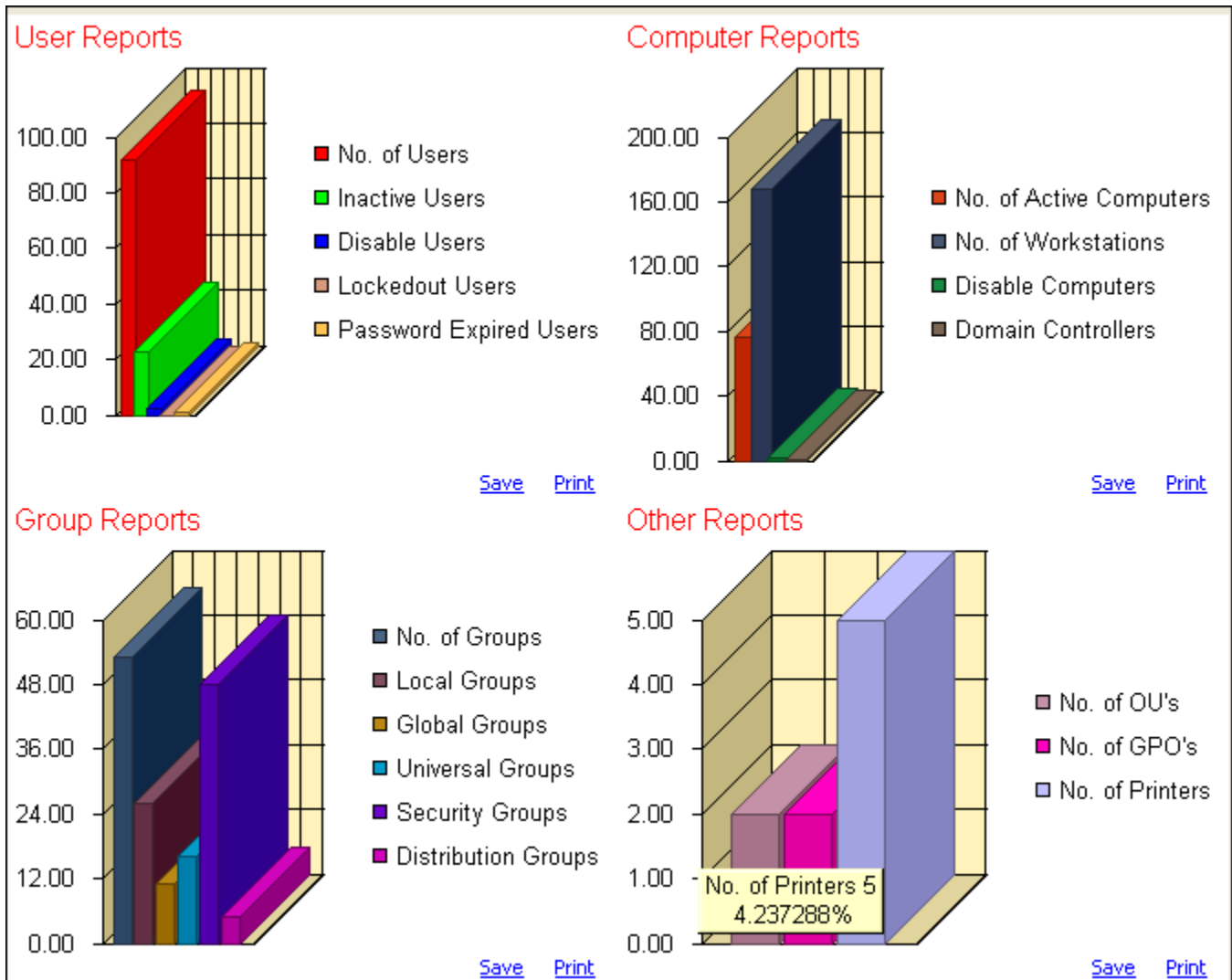
Figure 5.9: Displaying Graph and Report Panel

6. Working with Active Directory

LADMR is a complete, powerful, and centralized tool for all your Active Directory management and reporting needs. Using this amazing utility, the administrator/help desk personnel (with admin rights) can manage all AD objects from a central platform. In this section, you learn about managing AD objects under following sub-headings:

- Domain Management

- Manage Workgroup Computers

- Manage Local Computer

6.1 Domain Management

Using LADMR, the administrator can administer and manage 'n' number of domains from a central location. By default, software allows you to manage the local computer where you install the software and its domain. To manage more domains, containers, domain controllers, groups, etc. the administrator has to add domains in the software.

6.1.1 Add/Remove Domain

The "Add Domain" dialog box is used to add a new domain to the software database. The dialog box can be accessed by clicking **File > Add Domain** or by clicking the **Add Domain** button in the software toolbar on the main Window of LADMR. The domain on which the user exists is always included as the default domain in LADMR. Apart from the local domain, you can also add remote domains for administering in LADMR. You can add any domain in the software database; however, you will need to login as the administrator of a domain to administer the domain.

The "Add Domain" dialog box provides you with two methods to add a domain.

- **Method 1:** Type the name of the domain in the **Domain Name** text field and click **OK**.

- **Method 2:** Click **Find All Domains** to search for domains and populate the **Domain List**, select the domain name and click **OK** to add it to the **Domain Name** text field and click **OK**.

    ✍ Note: Workgroup names also get listed while performing the domain search.

Let us execute following steps to add a remote domain in the software database:

1. Select the **Add Domain** option in the **File** menu. The "Add Domain" dialog box appears.

2. Click the **Find All Domains** button to list out all available domains.

    All available domains get listed in the **Domain List** section. If any domain does not appear in the list then type the NETBIOS name of domain in the edit box above the **Domain List** section. Also make sure that the domain and its domain controller are in connection with the computer on which LADMR is installed.

3. After selecting a domain in the list or specifying the domain name, click the **OK** button.

On clicking the **OK** button, LADMR will try to find the domain controller (preferably primary domain controller) for that DOMAIN, if LADMR is able to find Domain Controller then it will add a new node in the tree view otherwise it will display an error message.

> ✍ Note: Following are the restrictions faced while working in remote domains with Lepide Active Directory Management and Reporting:
>
> ● All shell functions related to domain objects will be disabled. (This includes shell properties, object creation wizards, RSOP etc.)
>
> ● Not ALL functions of DFS will be available.
>
> ● Restore deleted objects Function is not available.

> ✍ Note: To delete a domain from the software database, right click the domain name in the left panel and select the **Delete Entry** option.

6.1.2 Containers/ OUs

Containers or Organizational Units (OUs) are used in Windows AD to implement objects as logical business units. OUs in AD logically comprise AD objects including other OUs. The **Containers/OUs** node in the left tree panel can be expanded to display all user-defined and in-built OUs in the left tree panel. Each OU can be further expanded to display all AD objects that are logically grouped under it.

Operations that can be performed by right clicking the **Containers/OU** node are described in the table 6.1:

Task	Description
View	Select to view all OUs in the right panel
New OUs	Select to create a new OU
Find OUs	Select to search for OUs
Browse for GPOs	Select to find a Group Policy Object (GPO) in domain
Reports	Select to view reports pertaining to OUs

You can double-click an OU name to view its contents in the right panel. Alternatively, you can view the content in the left panel by expanding the OU name node. Certain other operations that can be performed on OUs by right clicking the OU node are described in the table 6.2:

Task	Description
View Contents	Select to view the contents of OU in the right panel
Properties	Select to view OU properties. You can change various settings for an OU with this option
List Permissions	Select to view AD permissions for the contents of the OU
Manage Directory Attributes	Select to manage AD attributes with Lepide Active Directory Management and Reporting
New	Select to add a new object to the OU
Find	Select to find OU object
Delete	Select to delete OU and its respective child objects

Let us move ahead in the section with following processes:

- Create New OU

- Manage Directory Attributes

- Add New Objects in OU

6.1.2.1 Create New OU

Execute the following steps to create a new OU:

1. Right click the **Container/OUs** node in the left panel and select the **New OUs** option. The "Create (Copy) New" dialog box opens.

2. Type the desired location (LDAP path) for the new OU in the **Create In** text field or click the **Browse** button to select location. You can create the new OU either in the AD root directory or within another OU.

3. Type the desired OU name in the **Name** text field.

4. Select the **Run Active Directory Creation Wizard** checkbox if you want to use the AD creation wizard.

5. Select the **Display Object Properties dialog box after wizard completes** checkbox if you want to view properties of OU objects once the new OU is created.

6. Click the **OK** button.

Newly created OU will be displayed with other OUs in the list.

6.1.2.2 Manage Directory Attributes

You can apply common functions to every object in active directory with LADMR. Let us execute the following steps to manage directory attributes.

1. Right click a container/OU in the **Container/OUs** node and select the **Manage Directory Attributes** option. Software will open "Select Active Directory Attribute" dialog box, as shown in Figure 6.1:
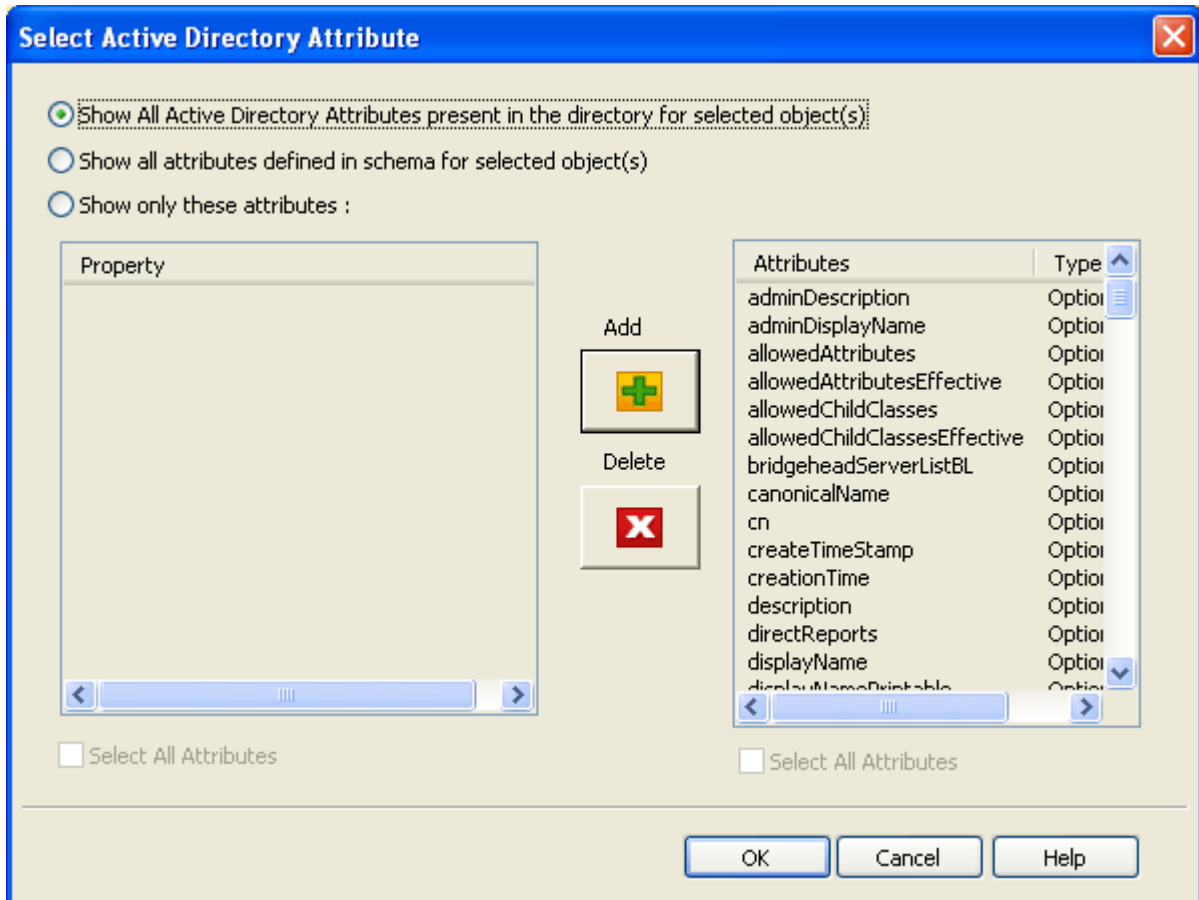
Figure 6.1: Displaying Options to Manage Directory Attributes

The "Select Active Directory Attribute" dialog box comprises following options to help you manage directory attributes:

- **Show All Active Directory Attributes present in the directory for selected object(s):** This option will display all the attributes of the selected object, which are not empty and have been assigned some value.

- **Show all attributes defined in schema for selected object(s):** This option will display all the attributes defined in schema for the selected object, related class that has any value (even the empty ones).

- **Show only these attributes:** This option will display only those attributes, which are pre-defined in the list.

2. Select the desired option to select the directory attribute(s).

3. Click the **OK** button. The "Properties" dialog box appears, which displays the properties of the selected attribute and also enables you to edit the attribute:
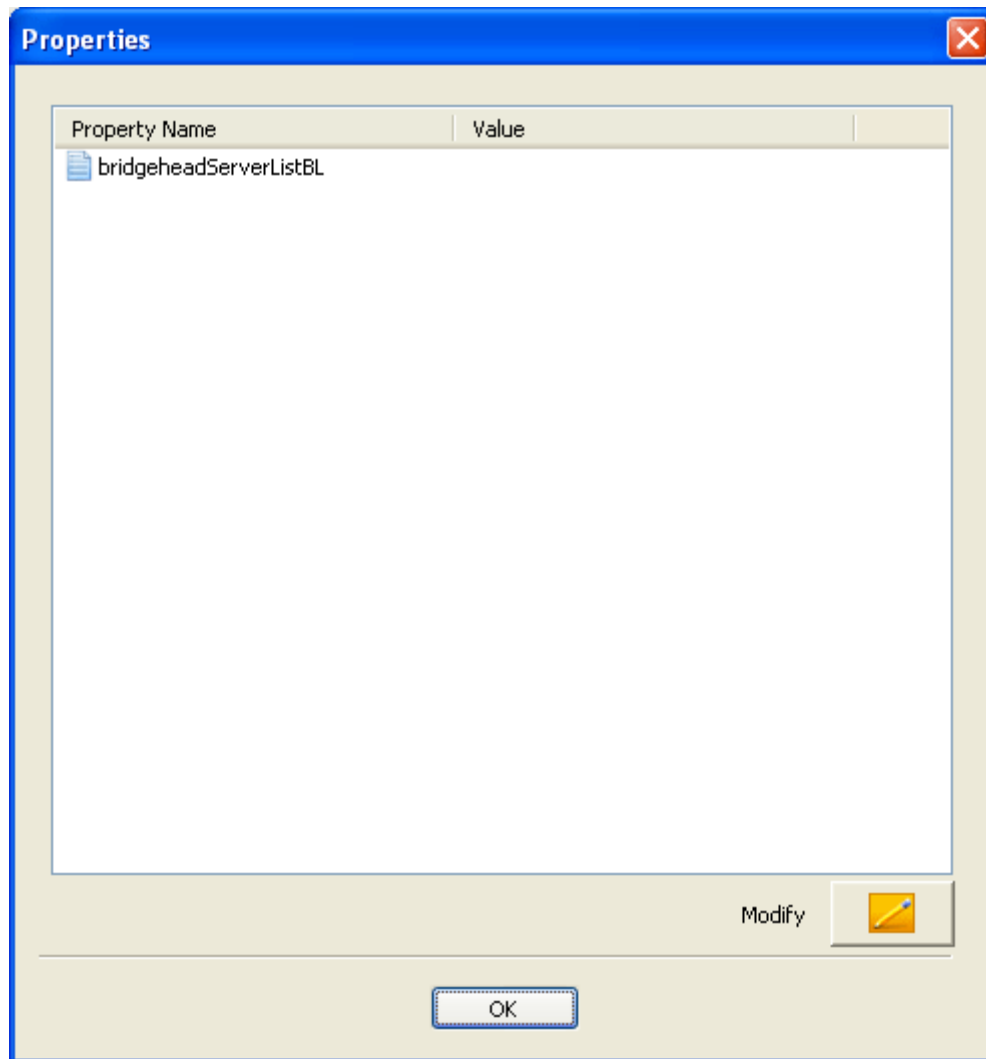
Figure 6.2: Displaying Properties of the Selected Attribute

Lepide Active Directory Management and Reporting software supports 10 data types, which are as follows:

- ADSTYPE_DN_STRING

- ADSTYPE_CASE_EXACT_STRING

- ADSTYPE_IGNORE_STRING

- ADSTYPE_PRINTABLE_STRING

- ADSTYPE_NUMERIC_STRING

- ADSTYPE_OBJECT_CLASS

- ADSTYPE_BOOLEAN

- ADSTYPE_INTEGER

- ADSOBJECT_STRING

- ADS_LARGE_INTEGER

These data types are easily editable for Single Value and Multiple Values.

4. Select the attribute and click the **Modify** button. The "Modify Directory Attribute Value" dialog box appears:
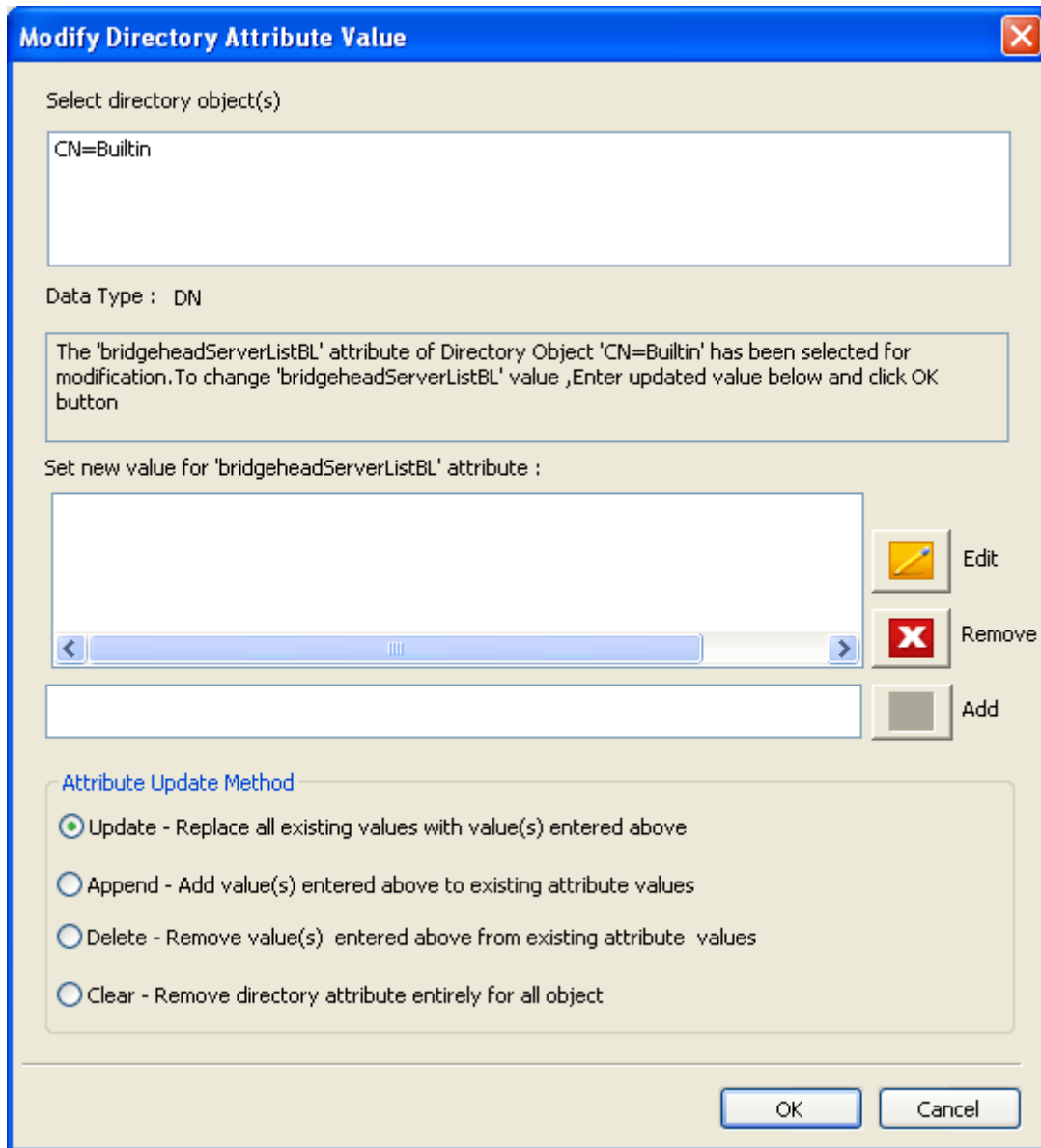
Figure 6.3: Modifying Properties of the Selected Attribute (Multiple Values)

Appearance of the dialog box varies depending on the attributes value (single value or multiple values). The "Modify Directory Attribute Value" dialog box in Figure 6.3 is for multiple values. Using the dialog box, you can change existing values with **Edit** button and remove or add them with the **Remove** and **Add** buttons. Attributes can be updated with four provided options to Update, Append, Delete, and Clear options.

If you select the single valued attribute in the "Properties" dialog box then the "Modify Directory Attribute Value" dialog box looks, as shown in Figure 6.4:
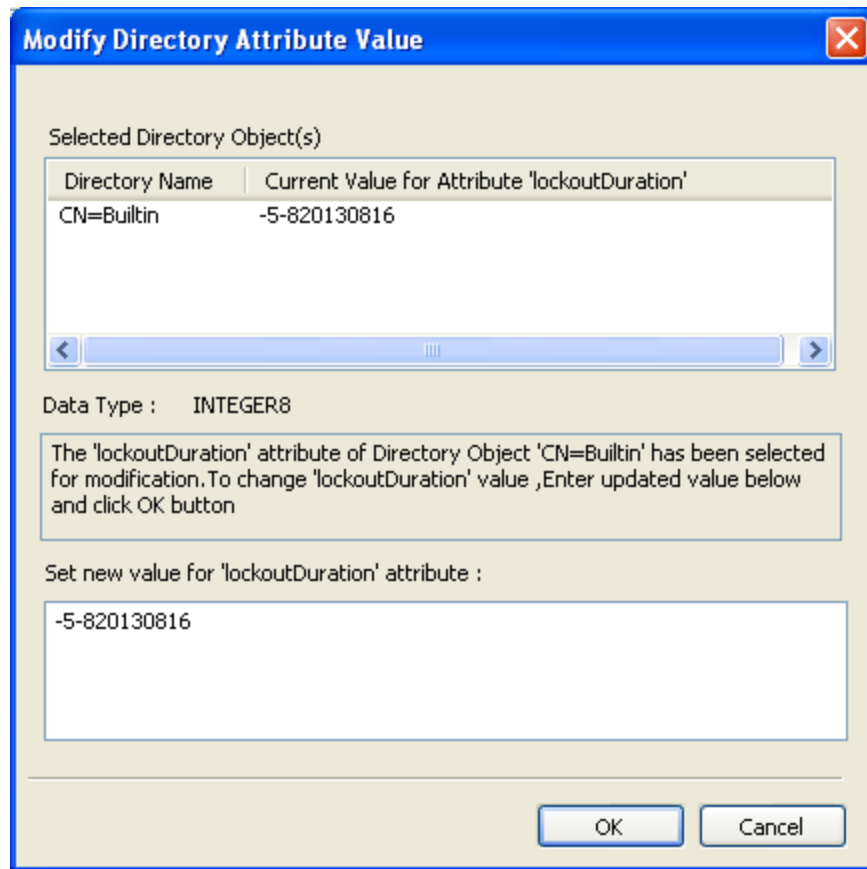
Figure 6.4: Modifying Properties of the Selected Attribute (Single Value)

> ✎ Note: On unsuccessful operation, LADMR will display a message box with actual error code and other details.

6.1.2.3 Add New Objects in OU

Execute the following steps to add an object in selected OU:

1. Right click a container/OU in the **Container/OUs** node.

2. Select **New** > **object**. LADMR allows you to add one of the following objects:

   - Computer

   - Group

   - User

   - Contact

   - OU

   - Shared Folders

   - Printers

   Wizard to add new object under the selected OU appears.

3. Follow the onscreen instructions to create new object in OU.

When the process is completed, a new object appears in the selected container/OU as a child node.

6.1.3 Domain Controllers

You can use LADMR software to view and manage various types of domain controllers. LADMR software provides many options to manage the DC, which otherwise takes more time in administering. On expanding the Domain Controllers node, you can view all the controllers configured as domain controllers. BDC(s) will also get listed here (if any). Software provides following functions for a DC:

- Properties

- Directory Functions

- Account Policy

- Audit Policy

- Printers

- Shares

- DFS

- Sessions

- Open Files

- Services

- Devices

- Events

- Disk Space

- Performance

- Scheduled Jobs

- User Rights

- Registry

- WMI

- Software

- System Tools

- TCP Utilities

All these functions can also be executed on local computer. You can right click the DC node in the left panel and select **Properties** to view the properties of the DC. When you right click the DC node in the left panel

and select the Properties option, the **System Properties** dialog box appears. This window has seven tabs that are described below:

- **Directory**: Description, Directory Path, and Names are displayed in this tab.

- **Object**: Creation, modification, category, logon - logoff information, password set time information is displayed in this tab.

- **MemberOf**: Information about the domain of which the DC is a member is displayed in this tab.

- **Software**: List of installed software applications on the DC is displayed in this tab.

- **System**: CPU Information, Operating System information, Logged On Users, and Other System Information is displayed in this tab.

- **Environment**: Environment variables, with property names and their values, are displayed in this tab.

- **Network**: Network transports, DNS host name, network card properties, IP address, subnet mask information, and WINS Server information is displayed in this tab.

In addition with displaying the properties, the software also enables you to execute various directory functions. To view and execute directory functions, right click the DC node in the left panel and select **Directory** Function. This displays the directory functions that can be performed on the selected DC. Table 6.3 lists those functions:

Function	Description
Shell Properties	Select to view shell properties of domain controller
List Permissions	Select to list and view all permissions of the object in right panel
Manage	Select to open Computer Management dialog box
Manage Directory Attributes	Select to manage AD attributes with Lepide Active Directory Management and Reporting
Reset Account	Select to reset computer account properties
Move	Select to move a DC object to new OU
Add to Group	Select to change group membership of any DC object
Name Mapping	Select to manage name mapping attributes for a DC

6.1.4 Computers

Every registered computer in a domain is listed here. The **Computers** node in the left panel can be expanded to view categories under which all computers in domain are arranged. Categories in the Computer node are:

- **Servers**: Expand the **Servers** node to view associated domain controllers of the domain. Right click the domain controller name to view respective properties and functions. Properties and functions are same as discussed in the section 6.1.3, Domain Controllers.

- **Workstations**: Expand the **Workstations** node to view registered workstation names in domain. Double-click, expand, or right click any workstation name to view respective properties.

LADMR enables you to perform bulk operations on all or selected workstations in the domain. For example, you can move computers from one container to another, add computer(s) to a group, etc. In addition, you can generate AD reports for all computers in the domain. Right click the **Computer** node in the left panel and select one of the following based on your requirement:

1. **View**: Displays Server and Workstations in the right panel.

2. **Task**: Displays the bulk operations that can be performed on selected or all computers in a domain. Bulk operations that you can perform using LADMR are:

    - **Move Computer(s):** Helps to move computer(s) to another container.

    - **Enable Computer(s):** Helps to enable the disabled computers in domain. Only the disabled computer(s) will get displayed in the list.

    - **Disable Computer(s):** Helps to disable any computer in domain. Only the enabled computers, which can be disabled, are listed here.

    - **Add Computer(s) to a Group**: Helps to change group of any computer(s) in domain. You can also change the associated Server for a particular computer.

    - **Remove Computer(s) from a Group**: Helps to remove any computer(s) from its group and allocate it to another group in domain.

    - **Set Primary group of Computer(s):** Helps to set primary group for the selected computers in domain.

    - **Change Common Details of Computer(s):** Helps to change common details of computer(s). Location, Managed By, and Description for selected computers is modifiable.

    > ✎ Note: LADMR displays failure message if the action is not performed.

3. **Reports**: Displays a list of the reports that you can generate to get the updated status. Reports that you can generated from here are:

    - All Workstation Computers

    - Domain Controllers

    - OS Based Reports

    - Computers Trusted For Delegation

- Recently Modified Computers

- Managed Computers

- Unmanaged Computers

- Inactive Computers

- Active Computers

6.1.5 Users

Lepide Active Directory Management and Reporting software helps to authenticate, grant authorizations, log on to a computer or domain. You can view list of all users, which are registered in a domain. Right click the All Users node to view the tasks that can be performed on all users' accounts in the domain. Following are the tasks that you can perform on domain users' accounts:

1. **View**: Displays all associated users of a domain in right panel.

2. **New User**: Adds a new user in the domain.

3. **Task**: Displays the bulk operations that can be performed on selected or all users in a domain. Bulk operations that you can perform using LADMR are:

   - **Reset Password:** Enables you to reset password of selected domain users.

   - **Unlock Users:** Enables you to unlock accounts of the selected domain users.

   - **Move Users:** Enables you to move selected domain users from one container to another.

   - **Delete Users**: Enables you to delete account of the selected domain users.

   - **Move Home Folders**: Enables you to move home folders of the selected domain users.

   - **Naming Attributes:** Enables you to modify the naming attributes of the selected domain users.

   - **Group Attributes:** Enables you to modify the group attributes of the selected domain users.

   - **Contact Attributes:** Enables you to modify the contact attributes of the selected domain users.

   - **Custom Attributes:** Enables you to modify the custom attributes of the selected domain users.

   - **Address/Organization Attributes:** Enables you to modify the address/organization attributes of the selected domain users.

   - **Enables Users:** Helps to enable the disable user accounts.

   - **Disable Users:** Enables you to disable the users' accounts.

   - **Profile Attributes:** Enables you to modify the profile attributes of the selected domain users.

   - **User Workstation:** Enables you to modify the users workstations.

> ✎ Note: LADMR displays failure message if the action is not performed.

4. **Reports**: Displays a list of the reports that you can generate to get the updated status. Reports that you can generate from here are:

- All Users

- Enabled Users

- Inactive Users

- Users with Empty Attributes

- Users without Manager

- Manager based Users

- Users in more than one group

- Recently Deleted Users

- Recently Created Users

- Recently Modified Users

- Dial-in Allow Access

- Dial-in Deny Access

- Users with Logon Script

- Users without Logon Script

- Account Status Report

- Logon Reports

- Nested Report

5. **Password Reports**: Displays the password reports under following categories:

- General Password Reports

- Password Status Reports

6. **Query Active Directory**: Enables you to query Active Directory.

6.1.5.1 AD Queries

The configuration options available on the **AD Queries** tab of the Object Manager dialog box enable you to view and edit query attributes comprised in different types of queries. The query types are generally defined on the basis of the type of group they are associated with. To start configuring queries you can select the type of queries from the **Query Type** drop-down menu. When you select a query type, all the queries associated with the type will be displayed in the **Existing Queries** section. You can select a query from the list and click the **Delete** button to remove the query. You can create a new query

by clicking **New** and typing the name of the query in the window that opens. Two lists are displayed below the list of queries:

- **Query Directory Attributes:** This list displays the attributes of the selected query directory. You can select an attribute from this list and click the **Delete** button to remove it from the list. You can edit the display name of any attribute displayed in this list by selecting it and clicking **Edit** or by double-clicking it. You can use the **Up** and **Down** button to move up or down in the list.

- **Schema Attributes:** This list displays the schema attributes that can be added to the query directory. You can select an attribute from this list and click **Add to** add the attribute to the query directory.

6.1.5.2 Create New AD Query

Execute the following steps to create a new AD query:

1. Select the **Object Manager** option in the **File** menu. The "Object Manager" dialog box opens up.

2. Select the **AD Queries** tab.

3. Click the **New** button. Software displays the "Active Directory Query Settings" dialog box.

4. Type the Query Name in **Query Name / Description** text box.

5. Click the **OK** button.

Newly created query name will be added to the list of existing queries. Now you can assign desired attributes to it.

6.1.5.3 Modify an Existing AD Query

Execute the following steps to modify an existing AD query:

1. Select the **Object Manager** option in the **File** menu. The "Object Manager" dialog box opens up.

2. Select the **AD Queries** tab. You see lots of fields in the dialog box that are described below:

    - **Query Type**: Select the query type from drop-down list to create or modify AD Queries. All Users, All Groups, Global Groups, Local Groups, and Universal Groups can be selected for assigning queries.

    - **Existing Queries**: This section displays the associated directory attribute(s) for the selected query in Existing Queries section. New attribute can be added with the **Add** button (from Schema Attributes section) or any existing query can be deleted with **Delete** button.

    - **Query Directory Attributes**: Specify the minimum number of characters you want the password to comprise. Select the **Permit Blank Password** option if you want the user to be able to set blank password. Select the **Atleast -- characters** option and specify the number of characters in the text field if you want to specify the number of characters that password should comprise.

    - **Schema Attributes:** This section displays the default query attributes available in Lepide Active Directory Management and Reporting. Click the **Add** button to transfer queries to Query Directory Attributes section for any existing selected query name.

6.1.5.4 View Properties of a Domain User

Double-click or right click a domain user name to view respective properties for a user. LADMR displays "User Properties" dialog box, as shown in Figure 6.5:
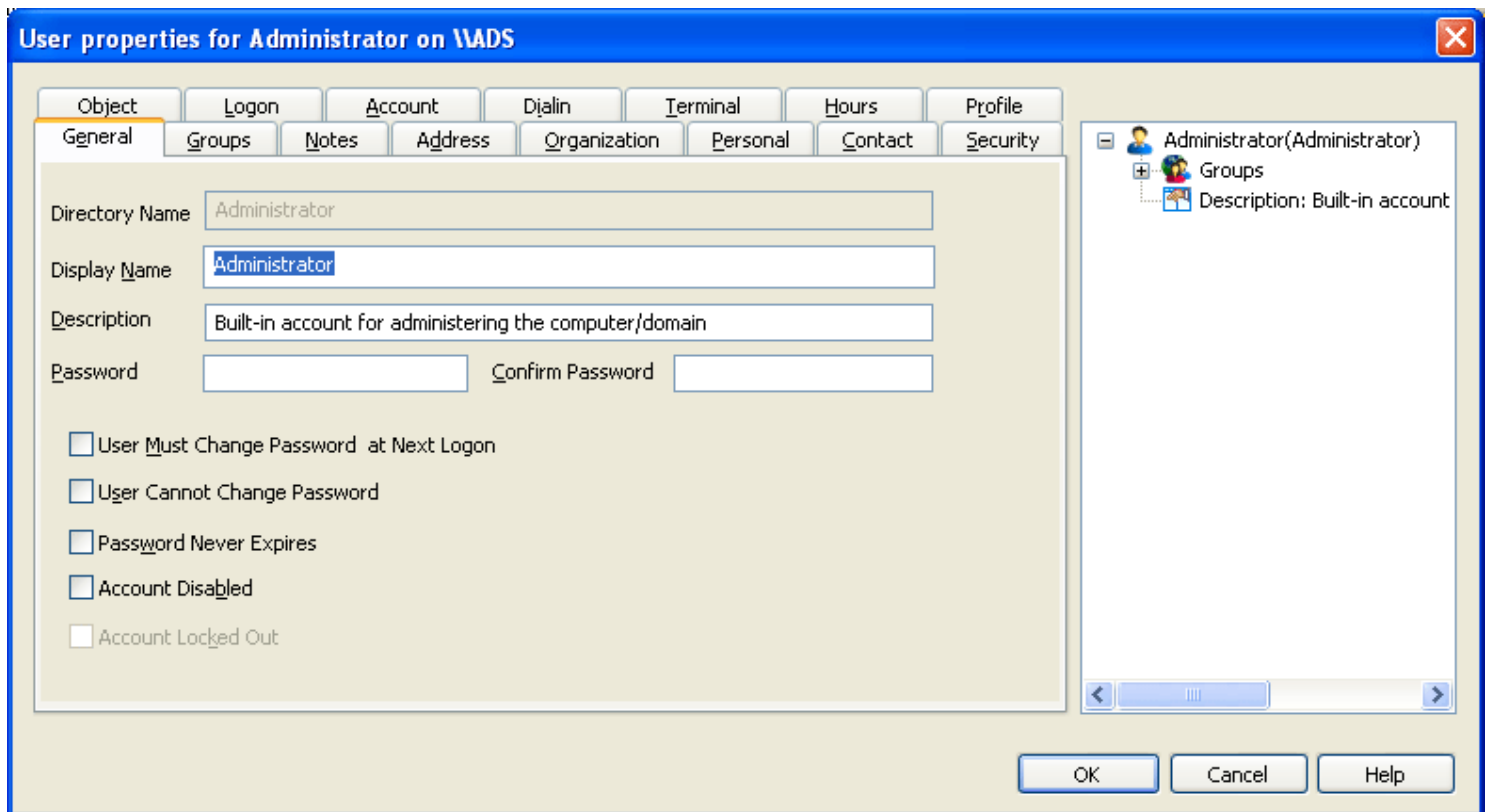
Figure 6.5: Domain User's Properties Dialog Box

The "User's Properties" dialog box comprises following tabs:

- **General**: This tab displays crucial information about the user attributes. User name, description, user password policies are displayed here.

- **Groups**: This tab displays information on group memberships of the user. You can modify the group membership of users with the **Add** and **Remove** buttons.

- **Notes**: This tab allows you to add notes/comments for a specific user.

- **Address**: This tab displays contact information of the user such as street address, city, state, country, pin code, etc.

- **Organization**: This tab displays company information of the user such as title, department, office, company etc.

- **Personal**: This tab displays personal information of the user such as first name, last name, user's picture, etc. These attributes are hidden in Active Directory and no MMC snap-in allows an administrator to change or set these attributes but with LADMR, you can easily and quickly modify these attributes.

- **Contact**: This tab displays contact attributes of the user. You can add or remove any contact or phone attribute. LADMR provides 16 attributes to add for a user. Click the **Add** button to assign more attributes and click the **Remove** button to remove any attribute for the selected user. You can modify the details with **Modify** button.

- **Security**: This tab displays information pertaining to the security and authentication of the user. You can view the details of account creation, password modification, lockout time and configure account security settings. LADMR provides following account security settings option:

  - **Store password using reversible encryption:** Select the checkbox if you want to allow a user to log on to a Windows network from Apple computers. If a user is not logging on from an Apple computer, this option should not be used.

  - **Smart card is required for interactive logon:** Select the checkbox if you require that a user possess a smart card to log on to the network interactively. The user must also have a smart card reader attached to their computer and a valid personal identification number (PIN) for the smart card. When this option is selected, the password for the user account is automatically set to a random and complex value and the Password never expires account option is set.

  - **Account is trusted for delegation:** Select the checkbox if you want to allow a service running under this account to perform operations on behalf of other user accounts on the network. A service running under a user account (otherwise known as a service account) that is trusted for delegation can impersonate a client to gain access to resources on the computer where the service is running or on other computers. This is a security-sensitive capability and should be cautiously assigned.

  - **Use DES encryption for this account:** Select this checkbox if you want to provide support for the Data Encryption Standard (DES).

  - **Do not require Kerberos preauthentication:** Select this checkbox if you want to provide support for alternate implementations of the Kerberos protocol.

- **Profile**: The tab contains two sections: User Profile and Home Directory. It displays configuration information for a specific user; desktop settings, and persistent network connection and application settings.

- **Hours**: This tab displays the logon hours section for a user. You can set the valid logon hours of users. It helps to avoid employee security breach cases with high end security at workplace. No one can logon after the valid hours been set with LADMR. This beneficial feature of the software helps to restrict the user working hours strictly.

✎ This feature is available for domain users only but can be performed on local user computer as well.
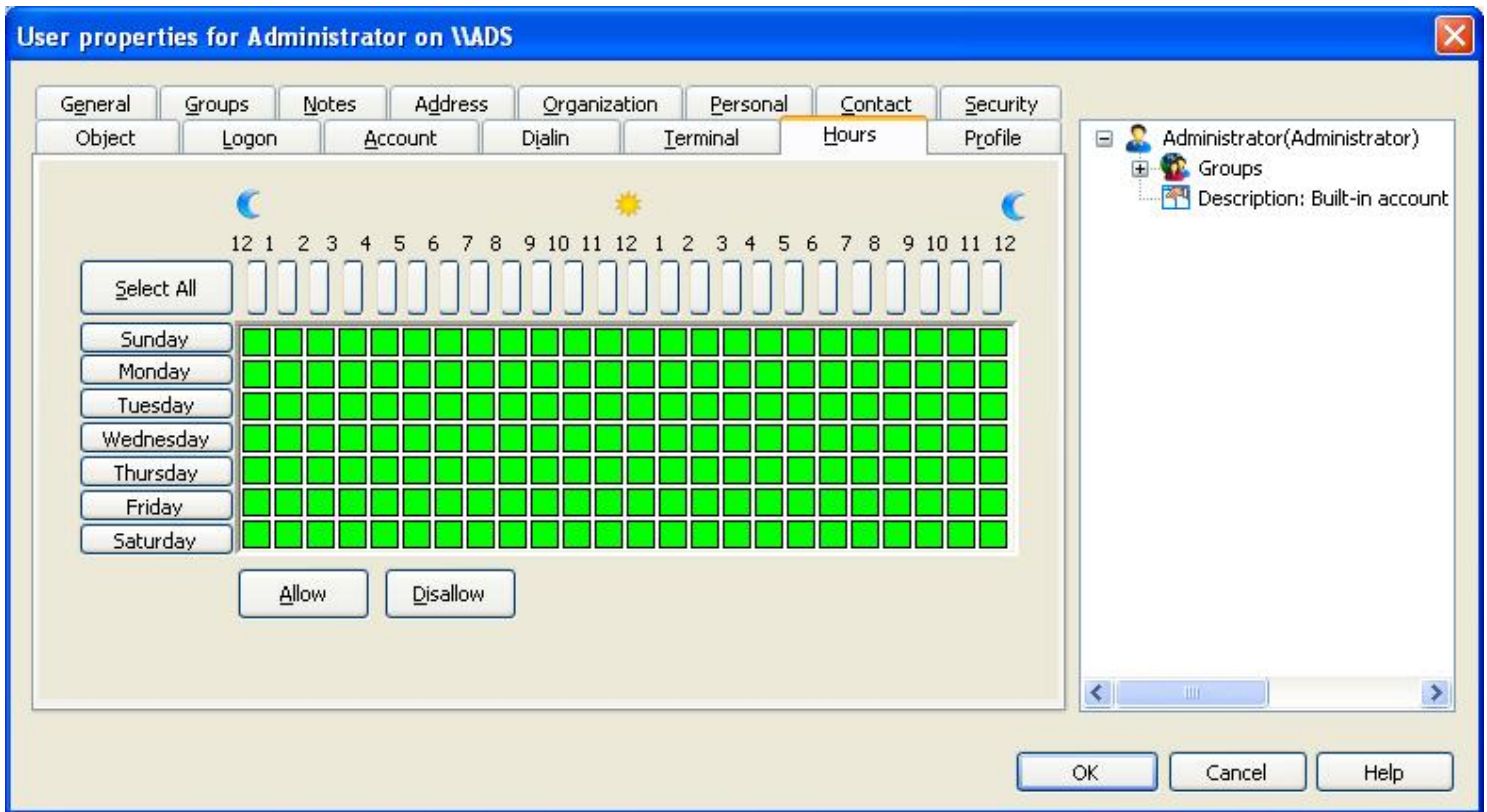
Figure 6.6: Displaying Logon Hours

Figure 6.6 displays logon hours, which can be configured for different users. Select the weekday(s) and hours and click the **Allow** button to allow access to the computer in selected criterion. LADMR will show Green color, which signifies that a user can login to the system on, selected days and hours. To disallow any user, select the weekdays and hours and click the **Disallow** button. This will restrict the user from logging on the selected day or hour. LADMR displays Red color for disallowed days and hours. Following operations are performed, if a user logs in after the valid logon hours:

- o **Forcible Disconnection**: You can set Window policy to forcibly disconnect when logon hours expire. Computer system will automatically get disconnected from all network resources and system will be logged off.

- o **Restricted Usage**: Users are not disconnected from the network when they logon after valid hours. Instead, with the help of set account policies, user is not allowed to make any new network connection.

- **Logon**: This tab provides two options wherein you can define the settings for a user, where user can **Logon to All Computers** or **Logon to Specific Computers only**.

- **Account**: This tab allows you to set account expiration date for a user. After the set date, user will not be able to logon to that computer.

- **Dialin**: This tab displays **Remote Access Permissions** and **Callback** options for a user. RAS enables remote or mobile workers who use dial-up communication links to access corporate computers or network as if they were directly connected. Remote access also provides virtual private network (VPN) services so that users can access corporate networks or computers over the Internet. Once Routing and remote access service is started and running then as administrator you need to change the dial-in properties of user. RAS provides many facilities which include:

  - o Dial-up remote access server

- Virtual private network (VPN) remote access server

- Internet Protocol (IP) router for connecting subnets of a private network

- Network address translator (NAT) for connecting a private network to the Internet

- Dial-up and VPN site-to-site demand-dial router

Lepide Active Directory Management and Reporting provides two options: **Remote Access Permissions** and **Callback options**.

- **Remote Access Permissions**: Allow or Deny access to user on dial-in server, besides this you can control this through remote access policy.

- **Callback Options**: Following are the call back options:

  - "No Callback" indicates that server will not callback a user, user has to make connection from his site.

  - "Set By Caller" indicates that server will callback to user on the telephone number as specified by the user on his side.

  - "Preset to" indicates that server will call back on a specific number as defined in this setting.

- **Terminal**: This tab allows you to configure the user profile environment when a user remotely connects to a terminal server.

  - **Profile Path**: Specify the profile path assigned to the user when the user connects to a terminal server. Assign the user a separate profile for Terminal Services sessions. Many of the common options that are stored in profiles such as screen savers and animated menu affects, are not desirable when using Terminal Services.

  - **Terminal Server Home Directory**: Specify a path to a home folder to be used for Terminal Services sessions. The folder can be either a local folder or a network share. Click the **CONFIG** button to view more properties of terminal services.

  - **Allow log on to Terminal Server**: Specify if the user can connect to terminal servers. Even if this check box is cleared, the user still needs to be given permission to connect to a terminal server. The **Remote Desktop Users** group on the terminal server is used to give users and groups permission to log on remotely to a terminal server.

  Further manageable options include:

  - Time out settings for connections

  - Client devices like drives and printer settings

  - Initial program to run and working directory setting

  - On broken or timeout disconnect or reset the session

  - Enable or disable modem callback and callback number

  - Settings regarding shadowing

- **Object**: This tab displays crucial information of the user object such as GUID, SID USN etc. Besides these, you can modify the "Managed by User" of the selected user.

6.1.5.5 Functions for Managing Domain User

Right click a domain user name to view respective functions for a domain user. As you right click the domain user, you see following functions:

- **Shell Properties**: Displays shell properties for the selected user. If ADMINPAK is installed on the user system then LADMR will displays various properties otherwise the properties will get limited to two or three.

- **Manage Directory Attributes**: Displays directory attributes to manage for a user. From here, you can easily modify the attributes.

- **Shell Functions**: View shell functions for a User. Following are the shell functions, you can work with:

    o **Resultant Set of Policy(Planning)...:** Resultant Set of Policy (RSoP) planning mode helps you to plan for growth and reorganization. With RSoP planning mode, you can poll existing Group Policy objects (GPOs) for all of the policy settings that can be applied. Then, you can use the results to construct a "What if?" scenario to predict the effect of changes in policy settings. Planning mode is most helpful in following situations:

        ▪ Administrator wants to simulate the affect of specific policy settings on a computer or user, domain, organizational unit, or site.

        ▪ The user is in Active Directory only (for example, a new account).

        ▪ Administrator wants to test policy precedence in the following situations:

            • User and the computer are in different security groups.

            • User and the computer are in different organizational units.

            • User or the computer is moving to a new location.

            • Administrator wants to create a slow network simulation.

            • Administrator wants to create a loop back simulation.

    After you have decided that a change is necessary, a series can be run of RSoP planning simulations to see what will happen to a user or a group of users if they are moved to another location or security group, or even to another computer.

    o **Resultant Set of Policy(Logging)...:** Resultant Set of Policy (RSoP) logging mode helps you to review existing policy settings that have been applied to computers and users. Logging mode is most helpful in following situations:

        ▪ Need to discover which policy settings are applied to a computer or user.

        ▪ Need to discover failed or overwritten policy settings.

        ▪ Need to see how security groups affect policy settings.

> ✍ To run RSoP logging mode on a remote computer, Administrator must be a member of the Domain Admin security group, Enterprise Admin security group, or be delegated Generate Resultant Set of Policy (logging) rights.

- o **Name Mappings...:** View mapped user accounts. You can also add certificates to the mapped accounts. This magnificent feature of LADMR helps to associate user names in two networks with different identities in Windows-based and UNIX-based domains. You can map user name with a certificate(x.509) or can give a kerberos name to it. For more information; http://technet.microsoft.com/hi-in/library/bb463221(en-us).aspx#ESH

- **Exchange Functions**: Exchange functions help you to manage user mailboxes. LADMR provides 4 manageable options in respect to this:

  - o **Create Mailbox:** Create user mailbox in domain exchange server

  - o **Mailbox Properties:** Displays shell properties of user mailbox

  - o **Delete Mailbox:** Delete user mailbox in domain exchange server

  - o **Move Mailbox:** Move user mailbox amongst two domain exchange server(s)

- **Account Functions**: Account functions prove helpful in managing user accounts for daily operations like password reset, disable, or unlock the account. LADMR provides following three options to manage users accounts:

  - o **Reset Password:** Allows to reset the password of selected user.

  - o **Enable/Disable Account:** Enable/disable user account. If the account is disabled then the menu item becomes "Enable Account" and vice versa.

  - o **Unlock Account:** Unlock any user account, which has been locked out because of the account lockout policy.

- **List Permissions**: Displays all the permissions allowed for the user in right panel.

- **View Details**: View details of the user in right panel.

- **Copy User**: Copy user settings such as personal, contact, dialin, etc. to a container. You will need to assign a different name (SAM account) for this.

- **Copy User To**: Useful function of LADMR, which helps to copy user to a different server with same attributes. You can also copy the group memberships of user by selecting the **Copy user group memberships** checkbox. This do not affect current status of the user.

- **Add New User**: Adds new user to the selected user. LADMR will display the "Create New" dialog box wherein you need to define user name and password of the user. New added user will get added to the selected user in domain.

- **Move User**: Move user object from one container to another.

- **Rename User**: Change or rename directory name, logon name and "Pre-windows 2000 name" of the selected user. Besides these, you can also change first name, last name and display name.

- **Delete User**: Deletes the user account.

- **Send Message**: Sends message to user where messenger service is active and running on sender and receiver computer(s).

- **View Logon Information**: View the logon or logoff information of the user. You can also check all Domain Controllers and PDS emulators to get the actual logon and logoff time.

- **Query Active Directory**: Customize or select a query for selected/all users.

6.1.6 Groups

Lepide Active Directory Management and Reporting software helps to create groups in root domain, any other domain, any OU, or in any container class object. You can also nest different groups. LADMR facilitates you to perform various tasks on groups associated with the domain. To view the tasks, right click the **All Groups** node in the left panel. Table 6.4 lists those functions:

Function	Description
View	Select to view all the associated groups of domain in right panel
New	Select to add a new group to the domain. You can define the scope and type of the group
Reports	Select to view Group reports and Group type reports
Query Active Directory	Select to customize or select a query for selected/all groups

In addition with enabling you to perform tasks on all groups in domain, LADMR allows you to manage individual group. Table 6.5 lists the functions using which you can manage an individual group:

Function	Description
Properties	View properties of the selected group
Manage Directory Attributes	Select to manage AD attributes with Lepide Active Directory Management and Reporting
View Group Details	View details of the selected group
Shell Functions	View shell functions of the selected group. • Shell Properties: View shell properties. • Send Mail: Send email to the entire group
List Permissions	View list of permissions applied on selected object in right panel
New	Add new group to the selected group
Move	Select to move a group object from one container to another
Rename	Select to rename the group

View Group Members	Select to view direct and indirect group members
Delete	Select to delete the selected group
Copy	Select to copy the group
Copy to Server...	Select to copy group from one server to another server
Copy Members to Group	Select to copy members from one group to another group
Add Members	Select to add members to the selected group
Query Active Directory	Select to customize or select a query for selected/all groups

6.1.7 Local Groups

LADMR software helps to view and manage built-in local domain groups and other domain local groups. Expand the **Local Groups** node to view list of all the local groups in domain underneath. LADMR facilitates you to perform various tasks on local groups. To view the tasks, right click the Local Groups node in the left panel. Table 6.6 lists those functions:

Function	Description
View	Select to view all the local groups of domain in right panel
New	Select to add a new group to the domain. You can define the scope and type of the group
Reports	Select to view Group reports and Group type reports
Query Active Directory	Select to customize or select a query for selected/all groups

Right click the local group name to view the respective properties. These properties are similar to All Groups options.

6.1.8 Global Groups

LADMR software helps to view and manage global groups. The Global Groups node displays all the available groups, which are of global nature in a domain. Expand the **Global Groups** node to view list of all the global groups in domain underneath. LADMR facilitates you to perform various tasks on global groups. To view the tasks, right click the Global Groups node in the left panel. Table 6.7 lists those functions:

Function	Description

View	Select to view all the associated global groups of domain in right panel
New	Select to add a new group to the domain. You can define the scope and type of the group
Reports	Select to view Group reports and Group type reports
Query Active Directory	Select to customize or select a query for selected/all groups

Right click the global group name to view the respective properties. These properties are similar to All Groups options.

6.1.9 Universal Groups

Lepide Active Directory Management and Reporting software helps to view and manage universal groups. The **Universal Groups** node displays all the available groups, which are of universal scope in a domain. Expand the **Universal Groups** node to view list of all the universal groups in domain underneath. LADMR facilitates you to perform various tasks on universal groups. To view the tasks, right click the Universal Groups node in the left panel. Table 6.8 lists those tasks:

Function	Description
View	Select to view all the associated universal groups of domain in right panel
New	Select to add a new group in the domain. You can define the scope and type of the group
Reports	Select to view Group reports and Group type reports
Query Active Directory	Select to customize or select a query for selected/all groups

Right click the universal group name to view the respective properties. These properties are similar to All Group options.

6.1.10 Schema

The Active Directory schema contains the definitions for all objects in the directory. Every new directory object created, is validated against the appropriate object definition in the schema before being written to the directory. The schema is made up of object classes and attributes.

Every directory object that is created is an instance of an object class contained in the schema. Each object class contains a list of associated attributes that determines information the object can contain. Classes and attributes are defined independently so that a single attribute can be associated with multiple classes. All schema classes and attributes are defined by the **classSchema** and **attributeSchema** objects, respectively. Classes that exist in schema are listed in Table 6.9:

Function	Description

Structural	Used to instantiate objects (users, servers and so on) in the directory
Abstract	Provides templates for deriving structural classes
Auxiliary	Contains pre-defined list of attributes that can be included in structural and abstract classes

While working with schema in LADMR, you perform following tasks:

- o **Single and Multi valued attributes**: Attributes can be single-valued or multi-valued. An instance of a single-valued attribute can only contain a single value. An instance of a multi-valued attribute can contain multiple values of uniform syntax. A multi-valued attribute stores no information about ordering of the attributes it contains. Each value of a multi value attribute must be unique.

- o **Indexed attributes**: Both multi-valued and single-valued attributes can be indexed to help improve the performance of queries on that attribute. (Indexing does not apply to classes.)

- o **View Class**: Double-click **Classes** node under Schema Management node. All classes will be displayed in the right panel.

- o **Create New Class**: Right click **Classes** node and select **"Create new class"** option, "Create New Schema dialog box" appears. Provide all the information and click the **OK** button to create a new class.

- o **View Properties of classes**: Double-click on any class to view properties.

- o **Manage Attributes**: LADMR schema management option allows administrator to change optional attributes of any class. Despite administrative credentials, changes will be honored only if they do not violate the basic constraints of Active Directory Schema.

- o **Manage Classes**: LADMR schema management option allows administrator to change Possible Superiors of any class. Despite administrative credentials, changes will be honored only if they do not violate the basic constraints of Active Directory Schema.

- o **View Attributes**: Double-click on **Attributes** node under **Schema Management** node, all attributes will be listed in right panel of the software.

- o **Create New Attribute**: Right click **Attributes** node and select Create New Attribute from the drop-down menu. After clicking, a message box will appear, which provides general warning about the consequences of changes in Schema, click the **Yes** button to proceed. "Create New Attribute" dialog box appears where you need to provide all information and click the **OK** button to create the new attribute.

- o **View Properties of Attribute**: Right click any attribute and select the Properties option from the drop-down menu. A dialog box appears which displays properties of the attribute. Administrator can perform various settings in order to enhance the responsiveness of Domain Controller.

6.2 Manage Workgroup Computers

A node corresponding to your workgroup will be displayed in the left panel when you expand the **Microsoft Windows Network** node. You can view all computers on the workgroup in the left panel by expanding the node. Each computer node can be expanded to access management options similar to the options that are displayed when you expand the local computer node. Certain other operations on workgroup computers can be performed by right clicking a computer and selecting appropriate options. However, to manage a workgroup computer remotely, you will need to log on to the computer with the credentials of an administrator authorized for that computer. To logon to a workgroup computer remotely:

1. Right click the computer node from the left panel and select the **Logon As** option.

2. Provide the **User Name** and **Password** in their respective fields and click the **OK** button. After you have logged in, you can perform all operations that can be performed on local computer along with following additional operations:

   - Send Wakeup Request

   - Remotely Shut Down a Computer

   - Send Message

   - Verify Logged on User

   - Ping

   - Net Logon Status

6.2.1 Send Wakeup Request

This option enables you to remotely turn on a computer, which has been turned off. However, computers without an automatic power supply will not respond to this feature. To send a wakeup request:

1. Right click the computer that you want to turn on and select the **Send Wakeup Request** option.

2. Click the **Browse** button to select the Wake-On LAN (WOL) configuration file. You can use the **Computer Name** drop-down list to select a computer before browsing for WOL file on it.

3. Type the MAC address of the computer in the **Mac Address** text field. You can use the **Edit** and **Reload** buttons to edit MAC address in notepad and reload MAC address respectively.

4. Type the default port number that you want to use for sending the request in the **Default Port** text field.

5. Click the **Send** button.

Pre-requisites to use WOL

- An ATX motherboard with an onboard, 3-pin "WOL" connector and ATX power supply.

- A network card that can support WOL with its cable to the motherboard properly installed.

- In the BIOS Power Management, you must enable the LAN Wakeup option.

- In Windows, "Device Manager" > "Network Card" properties Wakeup should be also enabled.

  > ✎ Note: The "Good Connection" light (green LED) on the back of the Network Card should be lit when machine is OFF. This helps in waking up the machine.

To accomplish WOL with Lepide Active Directory Management and Reporting, you need to manage a separate file, which consists of various computer names and their MAC address in the following format:

- ELECTRON,2EFAFC2312EA

- ELECTRON1,2EFSDFC2312E

{Where 'ELECTRON' is the computer name and '2EFAFC2312EA' is the MAC Address. In case of many computer listings, separate the individual entities with Return option}

LADMR recognizes this format and lists all the computers from where you can easily choose computers and their MAC addresses You can edit and reload the file by clicking **Reload**. Default port is 4000, which can change from machine to machine. Click **OK** to send the magic packets to target computer.

6.2.2 Remotely Shut Down a Computer

This option enables you to remotely shut down a computer. To shut down a computer on workgroup:

1. Right click the computer that you want to turn off and select the **Shut Down** option.

2. Type a message in the **Shut Down Message** text field that you want to display on the computer screen while the computer turns off.

3. Type the number of second after which the computer should be turned off in the **Timeout (In Seconds)** text field.

4. Select the **Force open applications to be closed** checkbox if you want the computer to be turned off despite running applications.

5. Select the **Reboot automatically after shutting down** checkbox if you want to restart the computer.

6. Click the **OK** button.

6.2.3 Send Message

To send a message to a workgroup computer, execute the following steps:

1. Right click the computer you want to send a message to and select the **Send Message** option.

2. Type the desired message in the **Message Text** field and click the **OK** button.

> ✍ Note: Messenger Service should be up and running in both computers to successfully send and receive messages

6.2.4 Verify Logged on User

The **Verify Logged on User** option enables you to view the user (if any) logged on to the computer. You can right click a computer and select **Verify Logged On User** option to view the logged on user along with the computer name, logon time, and the user's full name. You can thereafter click **Send Message** button to send a message to the computer, **Copy to Clipboard** to copy the data displayed, or **OK** to close the window.

6.2.5 Ping

The **Ping** option enables you to ping a computer. You can perform the ping operation by right clicking a computer node and selecting the **Ping** option. Execute the following steps to ping a workgroup computer:

1. Right click the workgroup computer and select the Ping option. The "Ping" dialog box appears.

2. Type the computer name in **Host** textbox.

3. Select or type the number of retries to ping for a machine.

4. Click **Ping** to start pinging.

6.2.6 Net Logon Status

The **Net Logon Status** option enables you to view the status of Net Logon service on a computer. You will need to right click a computer node and select **Net Logon Status** option to view, whether the Net Logon service is running or stopped.

6.3 Manage Local Computer

LADMR allows you to manage local computer along with the domain computers. When you expand the local user node then you see following child nodes that help you manage local computer:

- All Users

- Local Groups

- Local Connections

- Account Policy

- Audit Policy

- Printers

- Shares

- Distributed File System

- Sessions

- Open Files

- Services

- Devices

- Events

- Disk Space

- Performance

- Scheduled Jobs

- User Rights

- Registry

- Windows Management Instrumentation

- Software

- System Tools

- TCP Utilities

Let us explore these nodes.

6.3.1 All Users

All Users node displays hierarchy of all the users available for the computer. Group information and other information can be viewed when the node is expanded. This node also displays all the group name(s) of which the selected user is member of.

> ✎ Note: Local Users section is not available on Domain Controllers

Using LADMR, you can quickly view all users account on local computer and can add a new user account on local computer. Right click the **All Users** node to view the tasks that you can perform. Table 6.10 lists the tasks that can be performed using LADMR:

Function	Description
View All Users	Click to view all users in right panel.
New User	Click to add new user. LADMR will display the "Create New" dialog box wherein you need to define user name and password of the user. Newly added user will be added to the selected user in local computer.

Along with providing functions to apply on all users, LADMR provides various functions to manage individual user account. Table 6.11 lists those functions:

Function	Description
Properties	Displays the properties for the selected user. Properties for a local user are similar to that of domain user except that the domain user carries some additional properties.
Account Functions	**Reset Password**: Reset user account password. **Enable Account**: Enable or disable a user account. After being disabled, user cannot logon to the account. User can logon if the account is enabled from here again.

	A RED cross appears in case if user account is disabled. **Unlock Account**: Unlock user account.
Add New	Creates new local user. After creation, it gets listed under All Users node. ✎ Note: The username may be up to 20 characters, upper or lowercase or a combination. • To avoid confusion with special syntax characters, usernames should not include any of the following: " / \ [ ] : ; | = , + * ? < > • The name may include spaces and periods, but should not consist entirely spaces or periods. • Avoid use of spaces
Rename	Renames user name, which is not modifiable from user properties window.
Delete	Deletes user account. LADMR will display confirmation dialog box to perform the delete operation.
Copy	Creates a duplicate copy of reference user with a different name. All properties except name and password are copied to new user.
Copy To	Copies user from one system to another or to a computer/server. For this, you must create and maintain a valid admin session between the source and target server. New password is required to be set for the copied user.
View Logon Information	Displays logon information about the selected user.
View Details	Displays some common attributes of user in a tabular format.
Send Message	Send message to user where messenger service is active and running on sender and receiver computer(s).

6.3.2 Local Groups

The **Local Groups** node is displayed under the local computer node in the left panel. This node, when expanded, displays all in-built and user defined local groups that exist on the local computer. You can alternatively double-click Local Groups or right click Local Groups node and select the **View** option to display all local groups in the right panel.

6.3.2.1 View Properties and functions of Local Group

Double-click Local Groups node to view complete list of existing local groups on local computer with complete information. Select appropriate group name and right-click to view respective properties and functions. Table 6.12 lists the properties and functions of local group:

Function	Description

Properties	Displays the properties of the selected group. The properties dialog box also enables you to change group description and modify membership in the selected group.
View Group Members	Displays members of the selected group.
New	Enables you to create new group.
Rename	Renames the selected group name.
Delete	Deletes the selected group.
Copy	Creates a copy of the selected local group and create a similar group on the local computer or on the server.
Copy to server...	Copy the selected local group and its members to another server. This unique feature of LADMR helps to copy groups with complete membership details to any server or workstation. To perform this, the target computer should have authenticated sessions with this computer.
Copy Members to Group	Copies the members of this group to another group in same domain.
Add Members	Add or remove members from a domain or workgroup to selected local group.
Copy to Clipboard	Copy the selected local group details to a text editor like notepad, MS word, MS excel etc.

6.3.2.2 Add a New Local Group

Execute the following steps to add a new local group:

1. Right click the **Local Groups** node and select the **New Group** option.

2. Type desired group name in the **New Group Name** text field and click the **OK** button.

You can alternatively create a new group by right clicking an existing group in the right panel and selecting the **New** option.

6.3.3 Local Connections

The Local Connections node, which displays all local connections established with other computers in workgroup, displays sub node. Under this node, you see IPL Connections node, which is established when you access shared folders on any other computer in a workgroup. An open connection is a major security concern on a network, where unauthorized access can result into data and security breach. All such connections are listed under the IPC Connections node.

You can right click this node and select **Disconnect All** to end all IPC sessions immediately or right click a particular connection and select **Disconnect** to end the selected IPC session.

6.3.4 Account Policy

The **Account Policy** option enables you to manage account policy for the computer. This window is divided into two sections: **Password Restriction** and **Account Lockout**.

Password Restriction

In this section, you can configure settings to control the properties of passwords that can be used in user accounts. The configurable settings under this section are described in the table 6.13:

Function	Description
Maximum Password Age	Specify the time period before expiry of password. Select the Password Never Expires option if you do not want password to expire. Select the Password Expires in -- Days option and type the number of days in the text field provided if you want to specify the time period after which password should expire.
Minimum Password Age	Specify the minimum time period after which password can be changed. Select the Allow Changes Immediately option if you want the user to be able to modify password immediately. Select the Allow Changes in -- Days option and type the number of days in the text field provided if you want to specify the number of days after which the user should be able to change password.
Minimum Password Length	Specify the minimum number of characters you want password to be comprised of. Select the Permit Blank Password option if you want the user to be able to set blank password. Select the At least -- characters option and specify the number of characters in the text field if you want to specify the number of characters that password should comprise.
Password History	Specify the number of old passwords that you want the system to remember. Select the Do Not Keep Password History option if you do not want the system to store old passwords. Select the Remember -- Passwords option and specify the number of passwords in the text field if you want to specify the number of passwords that you want to be saved on the system.

Account Lockout

In this section, you can define the conditions under which an account should be locked. You will need to select the **No Account Lockout** option if you do not want any of the user's actions to result in account lockout.

To enable account lockout, you will need to select the **Lockout After** option and specify the number of bad attempts after which account should be locked in the text field that follows the option. Type the number of minutes after which you want the bad attempt count to be reset in the **Reset count after -- Minutes** text field. You can also specify the lockout duration by selecting the **Duration** option and typing the number of minutes in the text field that follows. The number of minutes defined here signifies the number of minutes after which a locked account will automatically get unlocked. You can disable automatic unlocking of accounts by selecting the **Forever (until admin unlocks)** option.

A checkbox, **Forcibly disconnect remote users from server after logon hours expire**, is displayed at the bottom of the **Account Policy** window. You will need to select this checkbox if you want to disconnect logged on users from server once their login hours expire. If you do not select this checkbox, the users who are logged on to the server will continue using the server; however, logged out users will not be able to establish connection to the server once logon hours expire. After making desired changes to the account policy, you will need to click the **OK** button to save the changes.

6.3.5 Audit Policy

The audit policy determines the events that are audited and logged. You can double-click the Audit Policy node to view or modify existing audit policy. Auditing for a computer can be enabled by selecting the **Enable Auditing** check box and then activating the events to view their success and failure logs. No events will be audited if the **Enable Auditing** check box is not selected.

Logs of events, which are enabled for auditing, can be viewed in Event Viewer. Lepide Active Directory Management and Reporting provides the following events for auditing:

- Logon and Logoff

- File and Object Access

- Use of User Rights

- User and Group Management

- Security Policy Changes

- Restart, Shutdown, and System

- Process Tracking

- Privileged Logons

- Directory Service Access

6.3.6 Printers

The **Printers** node in the left panel, when expanded, displays all the printers that are installed on the computer. You can also double-click this node or right click it and select **View Printers** to see all the installed printers in the right panel. All the print jobs associated with a printer can be viewed in the right panel by double-clicking the printer. LADMR enables you to manage the local as well network printers on domain.

You can use the configuration options available in the Printers node to view printer properties, connect to a printer, view or modify printer or printer server properties, etc. LADMR offers various operations that can be performed to manage printers. Table 6.14 lists those operations:

Function	Description
View printers	You can open the Windows view of a printer by right clicking the printer and selecting **Shell Functions > Open Printer**. You can view or modify the printing preferences of a printer by right clicking the printer and selecting **Shell Functions > Document Default**.
View Shell Properties of Printer Server	You can view the shell properties of the printer server by right-clicking **Printers** and selecting **Shell Properties** > **Server Properties**. Alternatively, you can right click any printer name > select **Shell Functions > Server Properties**.
Add a New Printer	To add a new printer, right click the **Printers** node, select **Shell Properties** option, and then select the **Add New printer** option to launch Windows Add Printer Wizard. Now, follow on screen instructions to add printer.
Connect to a Printer in Network	To connect to a printer in network, right click the **Printers** node and select the **Connect To** option. Type name of the printer in the **Printer** text field and click the **OK** button.
Copy Printer(s) to	Select to copy printer to a server. Copy Printer(s) window appears to define the target server location: Target Server(s): Type the target server name or click the **Find** button to search for it. Copy Printer Security: Select to copy the printer security settings Share Printers: Select to share the Printer Use existing assigned Ports: Select to utilize the existing ports
View Print Jobs	Select to view print jobs in process
Resume Printing	Select to resume paused printing job(s)
Pause Printing	Select to pause print job(s)
Purge All Print Jobs	Select to remove all scheduled print jobs
Connect to printer	Select to connect to a printer

Delete Printer	Select to delete selected printer(s)
Copy to Clipboard	Select to copy printer information listed in the right list pane to a text editor

6.3.7 Shares

The Shares node enables you to view and manage all shared folders and files on the local and remote computer(s). You can expand this node to view all the shared folders in the left panel and further expand the listed folders to view their sub-folders and constituent files in the right panel. You can view the shared folders in the right panel by double-clicking the **Shares** panel.

> ✎ Note: Admin shares are ended with '$' sign.

When you right click the **Shares** node, following operations can be performed:

- View Shares

- Create New Shares

6.3.7.1 View Shares

Execute the following steps to view shares:

1. Right click the **Shares** node and select the **View Shares** option. LADMR will list the shared folders of local and remote computers in the right panel with the information, such as File Name, Type, Size, Attribute, Last Access Time, Last Written Time, and Last Creation Time.

2. Double-click any **File Name** to view contents of that particular shared folder.

6.3.7.2 Create New Shares

Execute the following steps to create new shares:

1. Right click the **Shares** node and select the **Create New Share** option. The **Create New Share** dialog box appears.

2. Provide value for the following fields:

   - Share Name: Type the share name of the folder, which you want to create for sharing.

   - Path: Click the **Find** button to browse for path of the share and populate the path text field. This path should be a local path on the target computer.

   - Comment: Type a comment in the **Comment** text field.

   - User Limit: Define the maximum number of user(s) that you want to provide access permission to the shared folder.

> ✎ **Note:** If you check the **Maximum Allowed** option in this section, the user limit will be set to the default limit in Windows.
>
> Alternatively, you can define the number of users by selecting the **Allow** option.

3. Click the **OK** button.

In addition with allowing you to view shares and create new shares, LADMR allows to perform various operations on every shared item. Table 6.15 lists the tasks that can be performed on shared items:

Function	Description
View Files	Select to view objects (files, folders etc.) of the selected share.
Share Properties	Select to view selected share properties in terms of General, Security and Customization.
Show Connections	Select to view the connection dialog box for the target share. The dialog box will display the computer name/IP address and the user name of the computer who is currently accessing that share.
View NTFS Permissions	Displays the list of object level permissions for the selected share.
Open	Select to open the folder in explorer and view constituent files.
Explore	Select to view the content of the folder in Windows Explorer
Connect Drive	Select to create a network drive on local computer. The network drive will be linked to the selected shared folder.
Create Directory	Select to create a new directory / folder in the selected shared folder.
Stop Sharing	Select to stop sharing the selected folder
Copy Share To...	Select to copy all contents of the selected shared folder in new shared folder on another computer. For this operation to execute, the target computer should contain at least one share. To execute this operation, LADMR opens the **Copy Share To** window, where you will need to configure the following settings: Target Server: Type or browse the target server name with an active admin session. Select shared directory on remote server: Select the drive letter or any share name of the target server, where LADMR will create a new shared folder. New base path: Type the name of the folder, which will be created in the selected drive, and where all the files of the folder will get copied to.

6.3.8 Distributed File System

Distributed File System, or DFS, is a set of client and server services that helps to organize many distributed file shares into a distributed file system. When users try to access a share that exists off the DFS root, the user is really looking at a DFS link and the DFS server transparently redirects them to the correct file server and share. There are two ways of implementing DFS on Windows 2000 and Windows Server 2003:

1. Stand-alone DFS roots allow for a DFS root that exists only on the local computer, and thus does not use Active Directory. A Standalone DFS can only be accessed on the computer, which it is created. It does not offer any fault tolerance and cannot be linked to any other DFS.

2. Domain-based DFS roots exist within Active Directory and can have their information distributed to other domain controllers within the domain — this provides fault tolerance to DFS. DFS roots that exist on a domain must be hosted on a domain controller. This is to ensure that links with the same target get all their information replicated over the network. The file and root information is replicated via the Microsoft File Replication Service (FRS).

Administrator can create DFS domain root and DFS standalone root. New links can be created further in those roots. Various Targets can be assigned to a root.

DFS with Lepide Active Directory Management and Reporting

The DFS node in the left panel corresponds to the Distributed File System (DFS) root. You can expand this node to view the DFS root – domain or standalone. You can change the configuration of both domain and standalone roots by selecting appropriate options from the right click menu.

> ✍ **Note:** The DFS node will be displayed only if you run Lepide Active Directory Management and Reporting on a Domain Controller.

6.3.8.1 Create a New DFS root (Domain root and Stand alone root)

Execute the following steps to create a new DFS root:

1. Right click the **DFS** node.

2. Select **New Domain Root** or **New Standalone Root** depending upon the type of root that you want to create.

3. Enter the desired name in the **Root Name** text field.

4. Click the **Find** button to browse for path and populate the **Share Folder** path field.

5. Type any comments – if required.

6. Click the **OK** button.

6.3.8.2 Create a New Link in the Domain or Standalone root

Execute the following steps to create a new link in the domain or standalone root:

1. Expand the **DFS** node to display all roots.

2. Right click the root, you want to create a new link for, and select the **New Link** option.

3. Enter the desired name of the link in the **Link Name** text field.

4. Click the **Browse** button and select the target folder for the link.

5. Click the **OK** button.

You can delete a DFS root by right clicking the root and selecting **Delete Root** and delete all links of a root by right clicking the root and selecting **Delete All Links**.

> ✍ **Note:** It is advisable to right-click DFS and select **Refresh** to update any newly configured DFS settings.

6.3.8.3 Create a New Target

Execute the following steps to create a new target:

1. Right click the DFS node and select the **New Target** option from the drop-down menu. New Target dialog box will appear.

2. Provide "Unique Target Name" and "UNC path" of the shared folder, which will be the target of the DFS link.

> ✍ **Note:** If there is only one target in a link, which is removed, then the link will also get removed automatically.

Lepide Active Directory Management and Reporting has some limitations in regards of DFS management. Those limitations are:

- With LADMR, you cannot create or access domain type DFS root on remote domain.

- Number of roots supported by LADMR depends on the target server type and policies.

6.3.9 Sessions

The **Sessions** node displays all the users connected to the system. Double-click the **Sessions** node to view the list of connected users in the right panel of LADMR. Software displays following information for the connected users:

- Computer

- User

- Transport

- Time Active

- Time Idle

- Open Handles

- ID

To disconnect and delete any session from the list, select and right click the session and select the **Disconnect Session** option.

To copy the listed items of any session, select and right click the session and select the **Copy to Clipboard** option. Copied content then can be pasted/inserted to any text editor.

6.3.10 Open Files

The **Open Files** node under a computer can be double-clicked to view and manage all the open files on the local and remote computer(s) in domain. Lepide Active Directory Management and Reporting displays the list of open files in its right panel, where Path, User, Permissions Locks, and Id information of every file is displayed. Select and right click a **Path Name** in the right panel to view the operation, you can perform to manage open files. When you right click a path, following functions can be seen:

- **Disconnect**: Select to close the open file handle on network.

- **Send Message**: Select to send message to the user who is using that file.

- **Copy to Clipboard**: Select to copy the listed information. The copied information then can be added/inserted to any text editor.

6.3.11 Services

Services node enables you to view and manage all the Windows services related to local and remote computer(s). You can use the configuration options available under this node to start or stop a service, delete a service, and perform all services configuration operations that you are authorized for. You can view all the services running on the computer in the right panel by double-clicking the **Services** node. LADMR allows you to perform various operations on services. Right click the Services node to view the functions that can be executed to manage services. Following are the operations that you can perform to manage services:

- View All Services

- View Active Services

- View Inactive Services

- Install Services

6.3.11.1 View All Services

To view services, right click the **Services** node and select the **View** option. The software lists all services in right panel. Apart from displaying services, LADMR allow you to manage every individual service. To manage an individual service, right click the service. On right clicking the service, a list of the operations that can be performed on the selected service pops up. Table 6.16 lists those tasks:

Function	Description
Start	Select to start a stopped service
Stop	Select to stop a running service
Pause	Select to pause a running service
Resume	Select to resume a paused service
Restart	Select to restart an already running service
Refresh	Select to refresh a service

Delete	Select to delete the service and remove it from the list of services
Properties	Select to view the properties of the services in a different window
Copy To Clipboard	Select to copy the row information from the right list pane to any text editor

6.3.11.2 View Active Services

To view all active services right click the **Services** node and select the **View Active (Running) Only** option**.** LADMR will list all the active services for the computer in its right panel. Table 6.17 lists the fields on the right panel:

Field	Description
Name	Displays the name of the service
Startup	Displays the method by which the service starts up– manual or automatic
Display Name	Displays the name of the service that is displayed in the Windows services settings
Status	Displays whether the service is running or stopped
Type	Displays the service type, such as, Windows Own Process, Windows Shared Process, etc
Executable	Displays the path to the associated executable file
Dependencies	Displays other services on which the service depends
Account	Displays user account information

6.3.11.3 View Inactive Services

To view all inactive services right click the **Services** node and select the **View Inactive (Stopped) Only** option**.** LADMR will list the inactive services for the computer in its right panel.

6.3.11.4 Install Services

With LADMR, you can easily install any service to the remote computer(s) with some basic information. Execute the following steps to install services:

1. Right click the **Services** node and select the **Install Services** option. The "Install Service" dialog box appears.

2. Provide value for the fields given in the box. Table 6.18 describes the fields in the "Install Service" dialog box:

Field	Description
Service Name	Name of the service to installed. The maximum string length is 256 characters. The service control manager database preserves the case of the characters, but service name comparisons are always case insensitive. Forward-slash (/) and back-slash (\\) are invalid service name characters.
Display Name	Display name to be used by user interface programs to identify the service. The string has a maximum length of 256 characters. The name is case-preserved in the service control manager. Display name comparisons are always case-insensitive.
Service Type	Select the type of service: • Service runs in its own process • Service shares a process • Driver service • File system driver service
Startup Type	Select the service start up type: • Auto: Service started automatically by the service control manager during system startup. • Demand: Service started by the service control manager when a process demands that service. • Disabled: A service that cannot be started. Attempts to start the service result in the error • Boot: A device driver started by the system loader. This value is valid only for driver services. • System: A device driver started by the IoInitSystem function. This value is valid only for driver services.
Error Control Type	The severity of the error, and action taken, if this service fails to start. • Ignore: The startup program ignores the error and continues the startup operation. • Normal: The startup program logs the error in the event log but continues the startup operation. • Critical: The startup program logs the error in the event log, if possible. If the last-known-good configuration is being started, the startup operation fails. Otherwise, the system is restarted with the last-known good configuration. • Severe: The startup program logs the error in the event log. If the last-known-good configuration is being started, the startup operation continues.

	Otherwise, the system is restarted with the last-known-good configuration.
Path to binary file	The fully qualified path to the service's binary file. If the path contains a space, it must be quoted so that it is correctly interpreted. The path can also include arguments for an auto-start service. like, "d:\\myshare\\myservice.exe arg1 arg2". These arguments are passed to the service entry point (typically the main function). If you specify a path on another computer, the share must be accessible by the computer account of the local computer because this is the security context used in the remote call.
Load ordering group(optional)	The names of the load ordering group of which this service is a member. Leave empty string if the service does not belong to a group. The startup program uses load ordering groups to load groups of services in a specified order with respect to the other groups. The list of load ordering groups is contained in the following registry value: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ServiceGroupOrder
Service Account	The name of the account under which the service should run. If the service type is "Service run in its own process", use an account name in the form *DomainName\UserName*. The service process will be logged on as this user. If the account belongs to the built-in domain, you can specify *.\UserName* > ✎ If this is NT AUTHORITY\LocalService, it uses the LocalService account. If this is NT AUTHORITY\NetworkService, it uses the NetworkService account. A shared process can run as any user. If the service type is "Driver Service" or "File System Driver Service", the name is the driver object name that the system uses to load the device driver. Leave empty if the driver is to use a default object name created by the I/O system. Passwords are ignored for driver services.

3. Click the **Install Service** button.

After successfully installing a service, installed service will get displayed in right panel.

6.3.12 Devices

All the devices installed on a system are displayed in the right panel when you double-click the **Devices** node or right click the node and select the **View** option.

You can view all device driver services by right clicking **Devices** node and selecting the **Driver Services** option. You can select various rows of data in the right panel and copy it by right clicking the selection and selecting **Copy to Clipboard** to any text editor. Double-click the Device name in right list pane to view device properties.

6.3.13 Events

Events log helps an administrator to determine those conditions, which caused any error in the user system. It helps to record important events such as low memory conditions, restart operations, failing hard drive, etc. Events prove to be fruitful and save any big occurrence for data loss, disk damages, disk corruptions, OS errors etc.

All events configured for auditing in the Audit Policy section are registered in Windows event logs and can be viewed by using the **Events** node. You can expand this node to view various categories of events in the right list pane. Each of the sub nodes can be double-clicked to view related events in the right list pane.

Double-click the **Events** node to view "Event Filter" dialog box. LADMR provides this helpful feature to view events according to your requirements. In the "Event Filter" dialog box, you get options to filter your search for event logs. With this feature, you can easily view logs of multiple events at a time and also clear them. Table 6.19 lists the options to manage events that appear when you right click the **Events** node:

Option	Description
Event Viewer	Select to view the Windows Event Viewer
Filter Events	Select to filter the list of events displayed in the right list pane
Clear Logs	Select to clear event logs
Open Log File	Select to open the event log file. LADMR provides filter function to filter the event logs for time range, event types, and other filter types
Backup Event Log	Select to backup event logs. The file backup saving location should be on target computer

To copy the information from right panel, select and right click the row information and then select **Copy To Clipboard** to copy it to any text editor.

6.3.14 Disk Space

Under the Disk Space node, you can view the disk space available on the various hard disk drives installed on the computer. This section will display entire information related to the logical drives: Server name, Drive name, Format type, Total Space, % Free space, % Used space, Free space in terms of Gigabyte, Used space in terms of Gigabyte, Volume name, and Serial number.

You can copy the selected information displayed in right list pane to any text editor by right clicking and selecting **Copy To Clipboard.**

6.3.15 performance

LADMR helps to view performance counters of operating system functioning, applications, services, or drivers. Data received from performance helps to determine problems, functioning, and performance of the applications for a computer. You can also view performance object and counters of remote domain and manage them.

Double-click or expand the **Performance** node to view all the objects to be analyzed for a computer in right list pane of LADMR. Double-click any performance object name to view respective performance counters in the right panel.

6.3.15.1 Create Performance Counters

LADMR helps to create templates for performance objects, which are then assigned to the objects for monitoring purposes. Execute the following steps to create performance counters:

1. On the **File** menu, click **Object Manager** or **Object Manager** button from the toolbar. The Object Manager dialog box opens up.

2. Click the **Performance** tab (it is default first tab of the window).

3. Select **Use Local Computer Counters** or **Use Counters From This Computer** option.

   - **Use Local Computer Counters**: this will use counters of the local computer. You must authenticate the user credentials to view and enumerate performance objects and their counters for target computers. This can also be performed by creating authenticated sessions between both the computer(s).

   - **Use Counters From This Computer:** this will apply counters defined for the selected computer for monitoring. It also helps in monitoring performance of IIS, MS Exchange Server, MSSQL Server etc. You will need to provide authenticate yourself on the remote computer if you want to load the counters available on it.

4. Select the **Recall this computer by default** checkbox if you want to recall the listed computer every time for enumeration of performance counters.

5. Select appropriate object name from **Performance Object Name** drop-down for which you want to select counters. Select the **Automatic Update** checkbox if you want LADMR to refresh the performance object list in every 3 seconds.

   As the object name is selected from the list, **Current Query Performance Counters** and **Available Performance Counters** sections gets updated with the pre-defined and set counters for the selected object name.

6. Click the **Add** button to add selected counters from the "Available Performance Counters section" to "Current Query Performance Counters section". Click the **Delete** button to remove any assigned counter to the object. You can also modify the counters by clicking the **Edit** button. The edit option provides options to modify counter display title, display title in MB, GB or Bytes and Data Divisor value.

7. Click the **OK** button to complete the process. Now you can view the added performance counters with their value in right list pane of the selected object name.

6.3.16 Scheduled Jobs

The Scheduled Jobs node can be double-clicked to view all the scheduled Windows jobs in the right panel. All scheduled jobs can be divided into following categories:

- Administrative Tasks

- Normal Tasks

6.3.16.1 Add Administrative Task

Execute the following steps to add an administrative task:

1. Right click the **Scheduled Jobs** node and select the **New Job (AT)** option.

1. Populate the **Active Filename** text field or click the **Browse** button to select appropriate file.

2. Click appropriate option from the **Run Job** section as per your scheduling requirements and use the subsequent sections to schedule the job.

6.3.16.2 Add Normal Task

Execute the following steps to add a normal task:

1. Right click the **Scheduled Jobs** node and select the **Add New Job (Task)...** option**.** The "Create New Task" dialog box appears.

2. Type the name of the task and click the **OK** button. The Job Scheduler will then display the **Task Properties** dialog box.

3. Click the **Browse** button from the **Task tab** to select the job file to run from the saved location. LADMR displays the job save location in the top location*.*

4. Populate the **Start In** and **Comments** text fields.

5. Populate the **Run As** text field with the account that you want to use to run the task.

6. Click the **Set Password** button to provide credentials of the mentioned user account. You can select the **Run only if logged on** checkbox if you want to run the task only when you are logged on to Windows.

7. Select the **Enabled** option (scheduled task runs at specified time).

8. Select the **Schedule tab** and click the **New** button to schedule the task.

9. Select the **Settings** tab to configure task settings.

10. Click the **Apply** button to save changes.

Scheduled jobs can be configured by right clicking any of the jobs displayed in the right panel and selecting appropriate option. The configuration options available on right clicking a job are displayed in the table 6.20:

Option	Description
Properties	Select to view or modify task properties
Add New Job (AT)	Select to add a new administrator task
Add New Job (Task)	Select to add a new task
Delete Selected Job	Select to delete job
Run	Select to run the job immediately

6.3.17 User Rights

The **User Rights** node can be expanded to list all available user rights in the left panel. Each user rights node can be expanded to display all the users who have been granted that particular right.

To assign a right to more users:

1. Double-click the user right from the left panel to open the Rights on 'Computer' dialog box.

2. Use the tree in the left section (Available Users and Groups) of the dialog box to select and add users by clicking the **Add** button.

3. Click the **OK** button.

6.3.18 Registry

You can view or modify software registries on a computer by double-clicking the **Registry** node in the left panel. To view or modify a registry value, execute the following steps:

1. Double-click the **Registry** node in the left panel to launch the Registry Editor.

2. Use the tree in the left panel of the Registry Editor to browse the location of the registry.

3. Double click the registry file in the left panel to view the registry value name and registry value data.

4. Make the required changes and click the **OK** button.

6.3.19 Windows Management Instrumentation

Windows Management Instrumentation (WMI) is a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notifications. WMI is Microsoft's implementation of the Web-Based Enterprise Management (WBEM) and Common Information Model (CIM) standards from the Distributed Management Task Force (DMTF). The purpose of WMI is to define a non-proprietary set of environment-independent specifications, which allow management information to be shared between management applications.

WMI allows scripting languages like VBScript or Windows PowerShell to manage Microsoft Windows personal computers and servers, both locally and remotely, But besides these WMI functionality is difficult to use for even an experienced administrator. Lepide Active Directory Management and Reporting provides an intuitive way to fetch information from WMI.

LADMR use WQL (SQL like query for WMI) in order to fetch information from WMI repository. LADMR performs this in a very user friendly way and represents output in the GUI in comparison of other WMI tools. You can create query templates and view WMI instances in result of those queries. Also view details of those WMI instances and perform those actions, which are defined by their class.

WMI module in LADMR is a very flexible way, which is fully functional and dynamic to serve all WMI classes. LADMR Dynamically enumerates classes & their descriptions from the NameSpaces, dynamically enumerates Properties, their Qualifiers & their descriptions from those classes. All these are done without any dependencies of local and remote system. With the help of these dynamically enumerated classes, their properties and WQL, you can create very complex and powerful queries to fetch information from network resources.

However, before explaining the WMI system in LADMR, we must understand some basic concepts about WMI:

Namespaces

A categorization of classes and instances used to control their scope and visibility. Namespaces are not physical locations. They are more like logical databases containing specific classes and instances. Namespaces are represented by the __Namespace system class or a class derived from it. Each namespace contains a set of providers with their related classes specific to a management area (i.e. RootDirectoryDAP for Active Directory, RootSNMP for SNMP information or RootMicrosoftIISv2 for Internet Information Services information).

WMI Classes

As part of the installation process, most of the Microsoft applications available today extend the standard CIM object model to add the representation of their manageable entities in the CIM repository. This representation is called a WMI class, and it exposes information through properties and allows the execution of some actions via methods.

Provider

WMI providers act as intermediaries between the CIM Object Manager and one or more managed objects. When the CIM Object Manager receives a request from a management application for information that is not available from the CIM repository or for notification of events that it does not supports, it forwards the request to the provider. The provider then supplies the information or event notification requested.

System Classes

The WMI system classes are a collection of predefined classes based on the Common Information Model (CIM). Unlike classes supplied by providers, the system classes are not declared in a Managed Object Format (MOF) file. WMI creates a set of these classes whenever a new WMI namespace is created. Objects from the system classes are used to support WMI activities, such as event and provider registration, security, and event notification. Some objects are temporary, and some are stored in the repository as instances of the system classes. System classes follow a naming convention that consists of a double-underscore (__) followed by the class name.

WQL

To locate huge amount of management information available from the CIM repository, WMI comes with a SQL- like language called the WMI Query Language (WQL). Windows Management Instrumentation Query Language (WQL) is a subset of the standard ANSI SQL with minor semantic changes. A basic WQL query remains fairly understandable for people with basic SQL knowledge. WQL is dedicated to WMI and is designed to perform queries against the CIM repository to retrieve information.

6.3.19.1 WMI and Lepide Active Directory Management and Reporting

In LADMR, WMI node appears under every Computer node, as this is an individual computer property. Various WMI classes (which are configured in Object Manager) get displayed underneath. Every Class Node host individual Query Templates, which allows you to view the output of those query.

The WMI node (Windows Management Instrumentation) displays all the Win32 processes running on the selected computer under the Win32_Process sub node of this node. The management options available in this section enable you to manage all windows processes and execute WMI queries easily. You can expand the Win32_Process node to view all the processes running on the computer in the left tree pane. Alternatively you can double click Win32_Process to view all the processes in the right list pane.

6.3.19.2 Execute Method

LADMR enables you to execute methods for WMI Classes and WMI Instances. Lets us follow the below mentioned steps to execute method for WMI classes:

1. Double-click WMI class node. The default query will execute and all instances will appear in the right panel. Expand the WMI node to view list of WMI classes.

2. Right click a class name and select the **Execute Method** option. LADMR will open the "Execute Method" dialog box. LADMR provides various data type support for input (used as parameters in Methods). Supported data types are:

   - CIM_SINT8

   - CIM_UINT8

   - CIM_SINT16

   - CIM_UINT16

   - CIM_UINT32

   - CIM_SINT32

   - CIM_SINT64

   - CIM_UINT64

   - CIM_REAL32

   - CIM_REAL64

   - CIM_BOOLEAN

   - CIM_STRING

   - CIM_DATETIME

   - CIM_STRING | CIM_FLAG_ARRAY

   - CIM_SINT8 | CIM_FLAG_ARRAY

   - CIM_UINT8 | CIM_FLAG_ARRAY

   - CIM_SINT16 | CIM_FLAG_ARRAY

   - CIM_UINT16 | CIM_FLAG_ARRAY

   - CIM_SINT32 | CIM_FLAG_ARRAY

   - CIM_UINT32 | CIM_FLAG_ARRAY

   - CIM_SINT64 | CIM_FLAG_ARRAY

   - CIM_UINT64 | CIM_FLAG_ARRAY

REFRENCE and OBJECT data type are not supported by LADMR.

3. Double-click the **Parameter** name to edit/enter value.

4. Enter the value type and click the **OK** button.

5. Click the **OK** button.

Let us see how to execute method for WMI Instance.

1. Double-click WMI class node. The default query will execute and all instances will appear in the right list pane. LADMR will display Object properties dialog box on double-clicking any instance, which will display all properties of the instance. You can view next or previous instance properties with "Previous" and "Next" buttons.

2. Right click individual instance to view Properties, Execute Method, and Copy To Clipboard options. LADMR provides various data type support for input (used as parameters in Methods). Supported data types are listed above in this section.

6.3.19.2 Execute WMI Query

Follow the below given steps to execute a WMI query:

1. Right click the WMI node and select the **Execute Query** option. The "WMI Query Template Properties" dialog box appears.

2. Click the **New** button to browse for a new class.

3. Select required properties from the available properties and provide appropriate "Where" clause.

4. Click the **Execute Query** button to execute the query where output will be displayed in the right panel.

5. Double-click the WMI instance in right list pane to view detailed properties. This process helps to execute new queries without creating "Query Templates."

6.3.19.3 Create WMI Query for Local Computer

You can create various templates as per your requirements. Templates are grouped according to the WMI Class Name. Let us execute the following steps to create WMI query:

1. Click the **Object Manager** button from the toolbar and select the **WMI Queries** tab. This tab displays WMI query classes and enables you to add new query or modify query properties.

2. Select the Query Class and click the **New** button. The "Create New WMI Query" dialog box appears.

3. Type the new **WMI Query Name** with **WMI Namespace**.

4. Select the WMI Class by clicking the **Lookup Class** button**.**

5. Click the **OK** button. LADMR will open **WMI Query Template Properties** dialog box.

6. Perform the desired modifications and click the **Add Query** button. New WMI template will then appear in WMI Queries.

6.3.19.4 Create WMI Query for Other Computer

You can create WMI query templates for other computer(s) also. For this, the target computer must be available in the LADMR tree and must be authenticated in LADMR. Authentication session outside LADMR will not work for WMI. Two options are displayed on the WMI Queries tab for creating query:

Use Local Computer WMI Interface

Select this to create the query for the local computer.

Use WMI Interface from This Computer

1. Select this option to add a remote computer to create WMI Queries for that computer.

2. When you select a remote computer for loading WMI Queries, you will need to provide logon credentials for that computer. Type the computer name in the text field provided with the option or click the adjoining button to browse a computer.

3. Select the **Recall this computer by default** checkbox if you want the WMI Interface from the selected computer to be loaded by default instead of the local computer.

6.3.20 Software

The **Software** node can be double-clicked to display information pertaining to all the software applications installed on the computer. LADMR displays the following information in this tab:

- Name

- Version

- Publisher

- Help Link

- Help Telephone

- Info Link

- Modify Path

- Source

- Location

- Date

- About Link for the list of software installed

6.3.21 System Tools

The **System Tools** node can be expanded to display the list system tools available in Windows for computer administration. The following system tools are displayed in the list:

- Certification Authority

- Computer Management

- Device Manager

- Disk Management

- Event Viewer

- Group policy Object Editor

- Indexing Service

- IP Security Policy Management

- Removable Storage Management

- Services

- Shared Folders

- WMI Controls

Each of the tools can be opened by double-clicking the corresponding node.

> ✎ There can be events when the installed anti virus might block the MMC snap-in. In such cases, you need to unblock and add them to trusted region.

6.3.22 TCP Utilities

The **TCP Utilities** node can be expanded to list network utilities provided in Lepide Active Directory Management and Reporting. The utilities available are:

- Trace Route

- Ping

- Telnet

- FTP

6.3.22.1 Trace Route

Execute the following steps to use the Trace Route utility:

1. Double-click the **Trace Route** utility.

2. Type the tame of the destination computer in the **Target** text field.

3. Populate the **Maximum Hops, Timeout, and Ping** text-fields depending on your requirements.

4. Click the **Trace** button.

6.3.22.2 Ping

Execute the following steps to use the Ping utility:

1. Double-click the **Ping** utility in left panel.

2. Type the name of the computer to ping in the **Host** text field.

3. Click the **Ping** button.

6.3.22.3 Telnet

Execute the following steps to use the Telnet utility:

1. Double-click the **Telnet** utility in left panel. LADMR starts the utility in just few seconds.

2. Use the utility as per your need.

6.3.22.4 FTP

Execute the following steps to use the FTP utility:

1. Double-click the **FTP** utility in left panel. LADMR starts the utility in just few seconds.

2. Use the utility as per your need.

7. Creating Active Directory Reports

Reports section in Lepide Active Directory Management and Reporting contains all the domain reports based on following report types:

- Users
- Group
- Passwords
- Computers
- OUs
- GPOs
- Accounts
- Logon Reports
- Other Reports

7.1 User Reports

User Reports section displays reports related to the users in domain. You can select the report list from left panel and view its report in right panel. To save any report, click the **Save As** button in toolbar and to print any report click the **Print** button in the toolbar. Following is the description of the reports listed in left panel:

- **All users**: Click this to view list of all users that exist in domain.

- **Users with empty attributes**: Click this to view list of those users on which empty attribute criteria is applied. Click the report name, software displays "Select Empty Attributes..." dialog box. Table 7.1 provides description of fields on the dialog box:

Field	Description
Match all of the selected attributes	Select the option to generate report for all the selected attributes from the "Selected Attributes" section.
Match any of the selected attributes	Select the option to generate report for any of the selected attributes from the "Selected Attributes" section.
Available attributes	List of available attributes, which can be selected and transferred to the "Selected Attributes" section with **Add** button.
Selected Attributes	List of transferred attributes from the "Available attributes" section, which can be selected for report generation.

Assign the attributes for report generation and click the **OK** button. Software will generate and display the report in its right panel.

- **Users without manager**: Click this to view report for those users who are not managed by a manager in domain.

- **Manager based users**: Click this to view report for those users who are managed by a manager in domain.

- **Users in more than one group**: Click this to view report for those users who exist in more than one group created in domain. You can view the group name by adding the "MemberOf" column through **Add/Remove Columns** link.

- **Recently deleted users:** Click this to view report of user accounts that have been deleted recently. You can customize your search based on the number of days in the "Enter the no. of days" field and clicking the **Generate** button to view reports for the specified number of days.

- **Recently created users**: Click this to view report of user accounts, which have been created recently. You can customize your search based on the number of days in the "Enter the no. of days" field and clicking the **Generate** button to view reports for the specified number of days.

- **Recently modified users**: Click this to view report of those user accounts, which have been modified recently. You can customize your search based on the number of days in the "Enter the no. of days" field and clicking the **Generate** button to view reports for the specified number of days.

- **Dial-in allow access**: Click this to view report of those users who are allowed for Dial-in access.

- **Dial-in deny access**: Click this to view report of those users who are specially denied for Dial-in access.

- **Users with logon script**: Click this to view report of those users who are assigned with a Logon Script.

- **Users without logon script**: Click this to view report of those users who have not been assigned with a Logon Script.

- **Users in a group**: Click this to view report of those users who exist in the specified group in domain. "Select" dialog box to select a group name gets displayed. Select the group and click the **OK** button to generate the report.

- **Inactive users**: Click this to view report of those user accounts, which are inactive in domain.

- **Disable users**: Click this to view report of those user accounts, which are disabled in domain.

- **Enable users**: Click this to view report of those user accounts, which are enabled in domain.

7.2 Group Reports

Group Reports section displays reports related to the groups in domain. You can select the report list from left panel and view its report in right panel. To save any report, click the **Save As** button in toolbar and to print any report click the **Print** button from the toolbar. Following is the description of the reports listed in left panel:

- **Group without members**: View report of those group names, which are without any members.

- **Top N big group:** View report of groups in hierarchical manner, which rank higher in its member count than other groups in domain. Double click the report name and **Search settings for groups..** dialog box will appear which contains the fields listed in Table 7.2:

Field	Description
Enter a Number to find the Top Big Groups in the domain:	Enter the number to list that number of groups which are as per their member count: Security or Distribution To view the count of users in a group, click **Add/Remove Columns** and select **Member Count**.
Select the Type & Scope of the Group to filter:	**Group Type:** Select the group type to filter the search for type of group. **Group Scope:** Select the group scope to filter the search for group scope: Global, Domain or Universal (*These options alternatively get enabled in "Groups types and scopes" section*)

Define the appropriate option and click the **OK** button to generate the report.

- **All groups**: View report of all existing group(s) in a domain.

- **Managed groups**: View list of those groups, which are managed.

- **Unmanaged groups**: View list of those groups, which are not managed.

- **Group members in a user**: View the group(s) in which the selected user is a member of. As you click the report link, the **Select** dialog box appears which contains the list of users registered in domain. Select the user from list and view the group(s) of which it is a member.

- **Security groups**: View the list of security groups in domain.

- **Distribution groups**: View the list of distribution groups in domain.

- **Groups types and scopes**: View the list of groups in domain according to the group type and group scope.

7.3 Password Reports

Password Reports section displays reports related to the user account passwords in domain. You can select the report list from left panel and view its report in right panel. To save any report, click the **Save As** button in toolbar and to print any report click the **Print** button in the toolbar. Following is the description of the reports listed in left panel:

- **Users can't change password**: View list of the user(s) who cannot change their passwords.

- **Users whose password never expires**: View list of the user accounts whose passwords will never expire.

- **Password expired users**: View list of the user accounts whose passwords have been expired.

- **Soon-to-expire user password**: View list of the user accounts whose password will expire soon. Password expiry depends on the days defined in "Maximum Password Age" field for a user, domain, or group in the account policy section.

- **Password changed users**: View list of the users who have changed their passwords in the number of days entered in **Enter the no. of days:** field.

- **Password unchanged users**: View list of those users who have not changed their passwords in the number of days entered in **Enter the no. of days** field.

7.4 Computer Reports

Computer Reports section displays reports related to the workstations registered in domain. You can select the report list from left panel and view its report in right panel. To save any report, click the **Save As** button in toolbar and to print any report click the **Print** button in the toolbar. Following is the description of the reports listed in left panel:

- **All workstations**: View list of workstations registered in domain with their Organizational Unit name and other properties like common name, display name, managed by, when created, when changed etc. Servers and Domain Controllers are not termed as workstation.

- **Domain controllers**: View list of domain controllers in domain.

- **OS based**: View list of the workstations where a specific OS has been installed. Double click the report name. The "Select" dialog box will open from which you can select the Operating System version. Select the OS version and click the **OK** button to view the generated report.

- **Computer trusted for delegation**: View list of computers, which are trusted for delegation. User with trusted workstation can easily use the network services.

- **Recently modified computers**: View list of workstations, which were modified recently for any attribute. You can filter the days search by entering number of days in **Enter the no. of days** field and clicking **Generate** to view the filtered report.

- **Managed computers**: View list of computers, which are managed by any user in domain. You can view the name of managing person by clicking **Add/Remove Columns** and adding the 'Managed By' column to the report to be generated.

- **Unmanaged computers**: View list of computers, which are not managed by any user in domain.

- **Inactive computers**: View list of inactive computers for a specified number of days entered in **Enter the no. of day** field. This report is generated on the basis of last logon time on that computer. LADMR thoroughly scans the Domain Controllers to retrieve last logon time. Data might be incomplete in an event when LADMR is unable to get connected and scan all domain controllers.

- **Disabled computers**: View list of disabled computer accounts in domain.

- **Active computers**: View list of active computers in domain. This report is generated on the basis of last logon time on that computer.

7.5 OU Reports

Organizational Unit Reports section displays reports related to the OUs in domain. You can select the report list from left panel and view its report in right panel. To save any report, click the **Save As** button in the

toolbar and to print any report click the **Print** button in the toolbar. Following is the description of the reports listed in left panel:

- **All OUs**: View list of OUs present in domain.

- **Empty OUs**: View list of empty OUs in domain

- **Recently modified OUs**: List of all OUs, which have been modified in specified number of days. Specify the number of days in **Enter the no. of day** field and click **Generate** to view the report.

- **Recently created OUs**: List of all OUs, which have been created in specified number of days. Specify the number of days in **Enter the no. of day** field and click **Generate** to view the report.

- **User only OUs**: View list of all the OUs that contain only the users. Report will be generated for the OUs existing in the selected domain.

- **Computer only OUs**: View list of all the OUs that contain only the computers. Report will be generated for the OUs existing in the selected domain.

- **GPO linked OUs**: View list of OUs that are linked with Group Policy Objects. Report will be generated for the OUs existing in the selected domain.

- **GPO blocked inheritance OUs**: View list of OUs with Group Policy Objects, which are blocked from inheritance.

7.6 GPOs Reports

Group Policy Object Reports section displays reports related to the GPOs in Active Directory. You can select the report list from left panel and view its report in right panel. To save any report, click the **Save As** button in the toolbar and to print any report click the **Print** button in the toolbar. Following is the description of the reports listed in left panel:

- **All GPOs**: View list of all GPOs present in active directory.

- **Recently created GPOs**: View list of GPOs, which are created recently. Specify the number of days in **Enter the no. of day** field and click **Generate** to view the report.

- **Recently modified GPOs**: View list of GPOs, which are modified recently. Specify the number of days in **Enter the no. of day** field and click **Generate** to view the report.

- **Disabled GPOs**: View list of all GPOs, which are disabled. Both the computer configuration and user configuration settings are disabled.

- **Unused GPOs**: View list of Group Policy Objects, which are not in use since they are linked to a GPO.

- **Frequently modified computers settings GPOs**: View list of GPOs with frequently modified computer settings.

- **Frequently modified user settings GPOs**: View list of GPOs with frequently modified user settings.

- **Domain linked GPOs**: View list of GPOs, which are linked with domain.

- **OU linked GPOs**: View list of GPOs, which are linked with Organizational Units.

- **Site linked GPOs**: View list of GPOs, which are linked to any site.

- **GPO blocked inheritance containers**: View list of GPOs whose inheritance is blocked.

- **Computer settings disabled GPOs**: View list of GPOs with disabled computer settings.

- **User settings disabled GPOs**: View list of GPOs with disabled user settings.

- **Frequently modified GPOs**: View list of GPOs, which are frequently modified.

7.7 Accounts Reports

Account Reports section displays reports related to the user accounts in domain. You can select the report list from left panel and view its report in right panel. To save any report, click the **Save As** button in the toolbar and to print any report click the **Print** button in the toolbar. Following is the description of the reports listed in left panel:

- **Recently account expired user:** View details of those user accounts, which have been expired recently in domain. Specify the number of days in **Enter the no. of day** field and click **Generate** to view the report.

- **Soon-to-expire user account**: View details of those user accounts, which will expire within the specified number of days. Specify the number of days in **Enter the no. of day** field and click **Generate** to view the report.

- **Account never expiry users**: View details of those user accounts, which will never expire in domain.

- **Account expired users**: View details of those user accounts that have been expired in domain.

- **Locked out users**: View details of those user accounts that have been locked out. Generally, frequent bad login attempts locks out the user accounts. Configured account lockout policy determines the account lockouts.

7.8 Logon Reports

Logon Reports section displays reports related to the user logons in domain. You can select the report list from left panel and view its report in right panel. To save any report, click the **Save As** button in the toolbar and to print any report click the **Print** button in the toolbar. Following is the description of the reports listed in left panel:

- **Recently bad logged on users:** View list of those users who have experienced bad logon due to incorrect password value, which results in to unsuccessful login. Specify the number of days in **Enter the no. of day** field and click **Generate** to view the report.

- **Recently logged on users**: View list of those users who have logged on recently in domain. Specify the number of days in the **Enter the no. of day** field and click the **Generate** button to view the report. Report for the recently logged on users is generated with the help of users last logon time. LADMR scans all the domain controllers to retrieve the time information. If in an event, LADMR is unable to get connected to any Domain Controller, it might display incomplete data.

- **User never logged on**: View list of those users who have never logged on in the domain.

7.9 Other Reports

Other Reports section displays reports related to the other items in domain. You can select the report list from left panel and view its report in right panel. To save any report, click the **Save As** button in the toolbar and to print any report click the **Print** button in the toolbar. Following is the description of the reports listed in left panel:

Printers: View the list of printers, which are linked to active directory.

8. Troubleshooting

Troubleshooting questions with their answers for Lepide Active Directory Management and Reporting:

Q1. I am getting an error "GDIplus32.dll is missing" and software did not start. Why?

Ans. LADMR uses GDI+ for its Graphics and it is required for proper working of the software. In XP/2003 it is pre-installed but previous OS require a separate installation for this DLL. Read Microsoft KB957096 for further reference.

Q2. Does LADMR supports 2000/2003/XP/Vista?

Yes, LADMR fully support these Operating Systems.

Q3. Why am I getting errors while working on Windows 95/98?

Ans. LADMR is an advance tool to manage servers and their clients. Some functions used in LADMR are not compatible with Windows 95/98, so you might see some errors while managing these systems.

Q4. I am getting error:"some number" with error description "Description". What is this and how can I identify the root cause?

Ans. LADMR is designed to manage enterprises and there are so many errors, which can occur due to various reasons. Windows standard errors are informed LADMR which can be resolved by referring Microsoft documentation.

Q5. "Shell Property sheet" of AD objects on some systems display various tabs and in some system only few tabs are displayed. Why?

Ans. Shell Property functions do not work as usual in the absence of ADMINPAK and limited tabs are displayed when it is not installed. ADMINPAK is required but not necessary for the functioning of LADMR. It is recommended to install ADMINPAK for properties to work as expected.

Q6. Why is it the case that Shell Properties are available for some domains and not available for other domains?

Ans. Shell properties require native authentication to fetch and display attributes of required objects and this type of authentication is available only on child and trusted domains, so **Shell Properties and functions related to domain will be available for child and trusted domains only**. Rest of the functionalities does not abide by this rule and work properly as expected.

Q7. I am unable to view all Printer reports in the domain. Why is it so?

Ans. Printer report shows all the printer connected with active directory. Printers, which are installed on client machine and not connected with active directory will be not get displayed in reports section.

Q8. While working on Vista, I m not able to set the RAS properties of some users.

Ans. It is unusual behavior of Vista as it allows RAS property to get modified and sometime is available as read only.

Q9. All WMI data types are not supported while executing WMI functions. Why is it so?

Ans. Some WMI functions are very simple as they expect simple data types to work, where as some functions require complex structure which are not possible to implement in a user input type scenario. So all data types are not supported only the simple one are allowed.

Q10. I am unable to create another DFS root in 2000 server. Why?

Ans. It is known limitation of 2000 family of servers. Only one DFS root is allowed at a time.

Q11. I am administrating a remote domain (which is not child nor trusted by current domain) but I am not able to access Domain type DFS root of target remote domain. Why is it so?

Ans. LADMR cannot manage domain root of remote domains. But it works very well in local or trusted domains.

Q12. I am unable to enumerate performance counters in Object Manager. Why?

Ans. There are two cases where performance counter enumeration fails:

> 1. If user has selected a remote computer to enumerate performance object and their counters but somehow remote machine is not available.

> 2. A prior session is not established.

Choose another machine or create proper authentication session and after that re-open Object Manager.

Q13. AD Queries tab is not working and taking a long time to open on client machine. Why is it happening?

Ans. AD queries enumerate attributes of users and groups from domain itself. It requires at least one domain, which has at least read access to active directory. Therefore, if LADMR runs on a computer, which is not a part of domain nor is added in any domain, it will fail to run.

Q14. "Copy Share" function is not working on target computer.

Ans. "Copy share" function requires shared folder on target computer or admin shares to be enabled. In absence of these "Copy Share" function will fail. Check the target computer for shared folder.

Q15. I want to enumerate WMI classes of remote computer in Object Manager and LADMR is showing "RPC server is not available". How to resolve this?

Ans. If you have selected a remote computer as a default to enumerate WMI classes but some how remote machine is not available or a prior session is not established in both cases it fails to enumerate class. Choose another machine and create proper authentication session and after that re-open Object Manager. You must check target machine and ensure that WMI service is running properly.

Q16. Wake-On-LAN (WOL) is not working for my network. Why?

Ans. WOL needs hardware support for its functionality. Check the hardware requirements. If network has various hardware firewalls then they must be configured to forward "Magic packet" to flow.

Q17. Why am I not able to disconnect every session of computer?

Ans. Operating system can fail the attempts to close sessions, which are active, and which are under heavy usage, closing or terminating those sessions can hamper OS stability. The termination of sessions is under the discretion of OS and if OS understands that termination of the session is not going to disturb its stability then it simply allows to terminate.

Q18. "Send Message" function is not working properly.

Ans. Send Message function depends on the "Microsoft Messenger" services. Check that the service is running.

Q19. "Send Message to user" function is not behaving properly.

Ans. This functionality depends upon "Microsoft Messenger" service and LADMR behaves according to the MS Messenger behavior.

Q20. "Server Busy" dialog box opens while opening or closing user properties.

Ans. It is a normal scenario because LADMR uses standard COM interfaces to get/set properties of AD objects and if target server is very busy or loaded then sometimes client computer can display "server busy" dialog box.

Q21. I am viewing devices for VISTA but device list is different when LADMR is running on VISTA and VISTA computer is being administered from other computer. Why is it so?

Ans. It is a known issue that VISTA does not allow to enumerate devices from remote computer. LADMR displays device service for Vista devices. On local Vista system devices are enumerated properly.

Q22. I want to take backup of events (for remote computer) on local system where LADMR is installed. But the software is displaying errors, Why?

Ans. This is a known limitation of event services that Backup service of remote computer accepts only local path as a backup location. After taking backup on local system it can be copied on desired system.

Q23. I am trying to administrate VISTA client and before that I have successfully authenticated the session but even after that I am not able to access anything. Why is it so?

Ans. From VISTA onwards, Microsoft has introduced a new type of authentication session named as "NULL session". This type of connection requires no username or password. Even when user provides wrong username or password, it does not display any errors and Vista silently creates a NULL session with very limited credentials, these credentials are similar to Anonymous user.

Q24. Active Directory Creation Wizards are not working for some domains?

Ans. Active directory creation wizard exploit the features of Shell and for this administrator need to install ADMINPAK on the workstation on which LADMR is installed. Besides this, shell features require native authentication and will work only for self, child and trusted domains.

Q25. I am using LADMR on a machine, which is client of a domain to which I administrate, but I am not able to view Shell Properties of various objects.

Ans. You need to install ADMINPAK on the workstation from which you are administrating whole domain.

Q26. I am trying to access Event Log / Registry / Software of remote computer from LADMR, but the software is displaying error that "server is not operational".

Ans. Accessing remote registry requires "Remote Registry" service to be up and running. If this is stopped it might effect "Event Log" also.

Q27. Sometimes, I see "Server Busy" dialog box while accessing items under "System tools".

Ans. LADMR exploits the functionalities of MMC to get these system tool working. It invokes MMC with desired parameters and rest are done by MMC. This dialog box occurs because server is "Busy or Overloaded" and target system's response is slow.

Q28. I administrate domain from client computer and try to view "System Tools" from LADMR but some items do not show appropriate snap-ins instead some other snap-ins get opened. Why is it happening?

Ans. This happens because ADMINPAK is not installed, so all SNAP-INS are not installed on local system.

Q29. am trying to view "Open Connections" of shares but I am unable to view "user name" attribute. I m viewing shares of 2000 server.

Ans. It is a known limitation of 2000 family of OSs where user name is not displayed.

Q30. I am trying but not able to set User Rights for some users. Why?

Ans. It is a system dependent problem because LADMR requests the user SID to the target computer and if target computer has no idea about that user, in such case no SID is returned, that is why on some users, rights cannot be forced.
Although this is a very rare combination and usually occurs when we try to set user rights on such users which do not belong to the domain or those users who have same SAM account name on local machine or on domain.

Q31. I am trying to change schema attributes but changes are not honored by active directory. Why?

Ans. This happens because you need to tweak registry in order to change schema. To modify the registry to allow write operations to the schema, create a new REG_DWORD value named "Schema Update Allowed" with a data value of "1" in the following registry key: " HKEY LOCAL MACHINE\System\CurrentControlSet\Services\NTDS\Parameters "

Q32. I am unable to remove some attributes and superior classes from schema classes. Why?

Active directory does not allow certain change like these even if user has administrative rights. If you try to apply these changes then these changes are dishonored by active directory.

Q33. I am trying to change "Minimum Password Length" in account policy of a computer but I am not able to see any effect of that.

If "Password Complexity" requirement is enabled by group policy then "Minimum Password Length" and "blank password" setting will not work.

9. Download Purchase and Register

9.1 Free Trial Download

Download the free trial version of Lepide Active Directory Management and Reporting software to evaluate its features. The free trial version of the software is fully functional for 30 days with only one limitation that it the trial version does not allow to save and print the Active Directory reports.

9.2 Purchase and Register

To overcome the limitations of the free trial version and to use the software for a longer period, you need to purchase the Lepide Active Directory Management and Reporting software. The software is available in various license packs that you can purchase as per your organization's requirement.

You can purchase the software through Lepide Active Directory Management and Reporting Software from our Website:

http://www.lepide.com (encrypted and secure site)

Payment and Delivery

Purchase the Lepide Active Directory Management and Reporting software from our authorized resellers, which provide number of payment options for your ease - Paypal, FAX, Credit Card, E-cheque, Pay Order, etc.

After making the purchase transaction with our resellers, we send you an email, which consists of activation details and download link of the Full version comprising of the activation code. This email is sent to the email address, which you have used while processing the purchase transaction with our resellers.

We suggest you not to use false e-mail address while making the purchase transaction

For any other details related to purchase process, software activation process, email us at: sales@lepide.com

9.3 Support

Lepide Software provides **Round the Clock Support** to solve the technical and software related issues.

Telephone Support:

Software Help line: **+91-9818718513**

Indian Help line: **+91-9818718513**

Email Support:

For General Queries: **support@lepide.com**

For Sales: **sales@lepide.com**

For Technical Support: **support@lepide.com**

Documentation Center:

You can access the documentation of Lepide Software range at - http://www.lepide.com

10. Legal Notices

10.1 Copyright Notice

Lepide Software Private Limited, Lepide, accompanied user manual and documentation are copyright of Lepide Software Private Limited, with all rights reserved under the copyright laws. This user manual cannot be reproduced in any form without the prior written permission of Lepide Software Private Limited. No Patent Liability is assumed, however, with respect to the use of the information contained herein.

© LEPIDE SOFTWARE PRIVATE LIMITED. All rights reserved.

10.2 Trademarks

The Information contained in this manual including but not limited to any product specifications is subject to change without notice. Lepide Software Private Limited provides no warranty with regard to this manual or any other information contained herein and here by expressly disclaims any implied warranties of merchantability or fitness for any particular purpose with regard to any of the foregoing. Lepide Software Private Limited assumes no liability for any damages incurred directly or indirectly from any technical or typographical errors or omissions contained herein or for discrepancies between the product and the manual.

In no event shall Lepide Software Private Limited be liable for any incidental, consequential special or exemplary damages, whether based on tort, contract or otherwise, arising out of or in connection with this manual or any other information contained herein or the use there of.

10.3 Disclaimer Notice

Lepide Active Directory Management and Reporting is a copyright work of LEPIDE SOFTWARE PRIVATE LIMITED

Windows 95®, Windows 98®, Windows ME®, Windows NT®, Windows 2000 Server®, Windows 2000 Advanced Server®, Windows 2003 Server®, Windows XP®, and MS-DOS, are registered trademarks of Microsoft Corporation.

All other brand and product names are trademarks or registered trademarks of their respective companies.

10.4 License Agreement

Lepide Active Directory Management and Reporting is Copyright © by Lepide Software Private Limited. All Rights Reserved

Your Agreement to this License

You should carefully read the following terms and conditions before using, installing or distributing this software, unless you have a different license agreement signed by Lepide Software Pvt Ltd. If you do not agree to all of the terms and conditions of this License, then: do not copy, install, distribute or use any copy of Lepide Active Directory Management and Reporting with which this License is included.

The terms and conditions of this License describe the permitted use and users of each Licensed Copy of Lepide Active Directory Management and Reporting. For purposes of this License, if you have a valid single-copy license, you have the right to use a single Licensed Copy of Lepide Active Directory Management and Reporting; if you or your organization has a valid multi-user license, then you or your organization have - has the right to use up to a number of Licensed Copies of Lepide Active Directory Management and Reporting equal to the number of copies indicated in the documents issued by Lepide Software Pvt Ltd when granting the license.

Scope of the License

Each Licensed Copy of Lepide Active Directory Management and Reporting may either be used by a single person or used non-simultaneously by multiple people who use the software personally installed on a single workstation. This is not a concurrent user license.

All rights of any kind in Lepide Active Directory Management and Reporting, which are not expressly granted in this License, are entirely and exclusively reserved to and by Lepide Software Pvt Ltd. You may not rent, lease, modify, translate, reverse engineer, decompile, disassemble, or create derivative works based on, Lepide Active Directory Management and Reporting, nor permit anyone else to do so. You may not make access to Lepide Active Directory Management and Reporting available to others in connection with a service bureau, application service provider, or similar business, nor permit anyone else to do so.

Warranty Disclaimers and Liability Limitations

Lepide Active Directory Management and Reporting, and any and all accompanying software, files, data and materials, are distributed and provided AS IS and with no warranties of any kind, whether expressed or implied. In particular, there is no warranty for any harm, destruction, impairment caused to the system where Lepide Active Directory Management and Reporting is installed. You acknowledge that good data processing procedure dictates that any program, including Lepide Active Directory Management and Reporting, must be thoroughly tested with non-critical data before there is any reliance on it, and you hereby assume the entire risk of all use of the copies of Lepide Active Directory Management and Reporting covered by this License. This disclaimer of warranty constitutes an essential part of this License

In addition, in no event does Lepide Software Pvt Ltd authorize you or anyone else to use Lepide Active Directory Management and Reporting in applications or systems where Lepide Active Directory Management and Reporting's failure to perform can reasonably be expected to result in a significant physical injury, or in loss of life. Any such use is entirely at your own risk, and you agree to hold Lepide Software Pvt Ltd harmless from any and all claims or losses relating to such unauthorized use.

General

This License is the complete statement of the agreement between the parties on the subject matter, and merges and supersedes all other or prior understandings, purchase orders, agreements and arrangements. This License shall be governed by the laws of the State of Delhi. Exclusive jurisdiction and venue for all matters relating to this License shall be in courts and for a located in the State of Delhi, and you consent to such jurisdiction and venue. There are no third party beneficiaries of any promises, obligations or representations made by Lepide Software Pvt Ltd herein. Any waiver by Lepide Software Pvt Ltd of any violation of this License by you shall not constitute, nor contribute to, a waiver by Lepide Software Pvt Ltd of any other or future violation of the same provision, or any other provision, of this License.