Admin Guide

RED COM Management

8.1.1
Contents

CHAPTER 1  INTRODUCTION .............................................................................................................1
  1.1  Overview ...............................................................................................................................1
  1.2  How does the Program Work? .............................................................................................1
  1.3  License Agreement ...............................................................................................................2
  1.4  Limited Warranty ..................................................................................................................3

CHAPTER 2  GETTING STARTED .................................................................................................5
  2.1  Main Dialog ..........................................................................................................................6
    2.1.1  Main Dialog Pull-Down Menus .....................................................................................7
  2.2  Managed Systems Lists .......................................................................................................9
    2.2.1  Create Management Sets ............................................................................................10
    2.2.2  Adding Systems to a Simple Management Set ............................................................12
      2.2.2.1  Add From Domain Systems List ...........................................................................13
      2.2.2.2  Add From Network Browse List ...........................................................................15
      2.2.2.3  Add From Shell Network Browse List ..................................................................17
      2.2.2.4  Add Systems Manually .........................................................................................18
      2.2.2.5  Add From Active Directory .................................................................................20
      2.2.2.6  Add From IP Scanned Range ...............................................................................24
      2.2.2.7  Import/Export Systems List ...................................................................................42
    2.2.3  Backup System Sets .......................................................................................................43
      2.2.3.1  Backup Internal Database .....................................................................................43
      2.2.3.2  Export Systems List to a Comma-Delimited File .....................................................43
    2.2.4  Import Groups ...............................................................................................................44
      2.2.4.1  Import from ODBC Datasource ..........................................................................45
      2.2.4.2  Import from a Comma-Delimited File ...................................................................49
      2.2.4.3  Import from a Scanned IP Range .........................................................................49
      2.2.4.4  Restore from a Binary File .....................................................................................49
    2.2.5  Change the System Set Comment ..................................................................................49
    2.2.6  Delete a System Set .......................................................................................................50
    2.2.7  Delete Internal Database ..............................................................................................50
  2.3  Program Settings & Options ...............................................................................................51
    2.3.1  Logging Options .............................................................................................................51
    2.3.2  Configuring Email Server Settings ...............................................................................53
      2.3.2.1  SMTP Settings: General .......................................................................................54
      2.3.2.2  SMTP Settings: Outgoing Server .........................................................................57
      2.3.2.3  SMTP Settings: SMTP Logging ............................................................................60
    2.3.3  Alternate Administrators ...............................................................................................63
      2.3.3.1  Administrator Accounts Editor .............................................................................64
  2.4  Configuring Reports.............................................................................................................67
## Contents

**CHAPTER 3 WORKING WITH SYSTEMS**

3.1 Manage Systems Dialog ........................................ 88  
  3.1.1 Manage Systems Pull-Down Menus .......................... 89  
  3.1.2 Manage Systems Dialog Systems List Columns .......... 92  
    3.1.2.1 View Systems Only .................................. 92  
    3.1.2.2 View MTS/COM+ Objects ............................. 94  
    3.1.2.3 View DCOM Applications ............................. 95  
    3.1.2.4 View Custom DCOM Permissions .................... 95  
  3.1.3 System Name Resolution .................................. 96  
  3.1.4 View Filter Options .................................... 97  
3.2 Manage Systems Context Menu ................................ 97  
3.3 Selecting Machines .......................................... 98  
3.4 Highlight Lists ............................................. 99  
3.5 Refresh ..................................................... 99  
3.6 Reboot and Abort Reboot .................................... 100  
3.7 Send Message ............................................. 101  
3.8 Send Wake on LAN Packet .................................. 101  
3.9 Remove Systems from a System Set ......................... 102  

**CHAPTER 4 MANAGING COM OBJECTS** ................................ 103  

**CHAPTER 5 REMOTE CONTROL** .................................... 105  
5.1 Setting up VNCPass ........................................... 105  
5.2 Open VNC Connection ....................................... 105  
5.3 VNC Options ............................................... 106  
5.4 Import Settings from a .RCM File ............................ 114  
5.5 Install/Remove VNC on System ............................... 114  
5.6 Start/Stop/Restart the VNC service ......................... 114  
5.7 Set VNC Password .......................................... 114
**CHAPTER 6  HELP INFORMATION**

6.1 License Token Assignment ................................................................................. 117

6.2 Registration Dialog ........................................................................................... 120
  6.2.1 Use Remote License ..................................................................................... 121

6.3 Logon Information Dialog .................................................................................. 122

6.4 About ................................................................................................................... 124

**CHAPTER 7  INDEX** ................................................................................................ 125
Welcome to RED COM Management! This manual contains information to help an administrator use RED COM Management including creating and managing systems lists and working with identity information as well as descriptions of its many features.

IN THIS CHAPTER
- Overview .............................................................. 1
- How does the Program Work? .................................. 1
- License Agreement .................................................. 2
- Limited Warranty ..................................................... 3

1.1 OVERVIEW

Thank you for purchasing RED COM Management. If you are evaluating the product, we think you will be very pleased with its capabilities.

RED COM Management allows management of COM+/MTS and DCOM applications. Use this program to see what COM+/MTS and DCOM applications are present on systems as well as settings and UUIDs for those applications. RED COM Management also allows changing the identity that the COM+/MTS and DCOM applications runs as on all managed systems in just a few clicks, making account changes easy and efficient.

1.2 HOW DOES THE PROGRAM WORK?

This program uses the COM+ components and tools built into Microsoft Windows to pull information about COM+ applications from managed systems. Using these same tools, it is possible make changes to those COM+ applications allowing the objects to run as a specified identity or as a part of the system. The program also allows access to the built in configuration tools Windows offers for local COM+ applications and extends that functionality over the network.
1.3 LICENSE AGREEMENT

This is a legal and binding contract between you, the end user, and Lieberman Software. By using this software, you agree to be bound by the terms of this agreement. If you do not agree to the terms of this agreement, you should return the software and documentation as well as all accompanying items promptly for a refund.

1. Your Rights: Lieberman Software hereby grants you the right to use a single copy of RED COM Management to manage the licensed number of systems. This software is licensed for operation on only one machine unless other license arrangements have been made in writing between Lieberman Software and your organization.

2. Copyright. The SOFTWARE is owned by Lieberman Software and is protected by United States copyright law and international treaty provisions. Therefore, you must treat the software like any other copyrighted material (e.g. a book or musical recording) except that you may either (a) make one copy of the SOFTWARE solely for backup and archival purposes, or (b) transfer the SOFTWARE to a single hard disk provided you keep the original solely for backup and archival purposes. The manual is a copyrighted work also--you may not make copies of the manual for any purpose other than the use of the software.

3. Other Restrictions: You may not rent, lease, or transfer the SOFTWARE to any other entity. You may not reverse engineer, de-compile, or disassemble the SOFTWARE that is provided solely as executable programs (EXE files). If the SOFTWARE is an update, any transfer must include the update and all prior versions.

4. Notice: This software contains functionality designed to periodically notify Lieberman Software of demo usage and of the detection of suspected pirated license keys. By using this software, you consent to allow the software to send information to Lieberman Software under these circumstances, and you agree to not hold Lieberman Software responsible for the use of any or all of the information by Lieberman Software or any third party.
1.4 LIMITED WARRANTY

The media (optional) and manual that make up this software are warranted by Lieberman Software Corporation to be free of defects in materials and workmanship for a period of 30-days from the date of your purchase. If you notify us within the warranty period of such defects in material and workmanship, we will replace the defective manual or media (if either were supplied).

The sole remedy for breach of this warranty is limited to replacement of defective materials and/or refund of purchase price and does not include any other kinds of damages.

Apart from the foregoing limited warranty, the software programs are provided "AS-IS," without warranty of any kind, either expressed or implied. The entire risk as to the performance of the programs is with the purchaser. Lieberman Software does not warrant that the operation will be uninterrupted or error-free. Lieberman Software assumes no responsibility or liability of any kind for errors in the programs or documentation or for consequences of any such errors.

This agreement is governed by the laws of the State of California.

Should you have any questions concerning this Agreement, or if you wish to contact Lieberman Software, please write:

Lieberman Software Corporation
1875 Century Park East, Suite 1200
Los Angeles, CA 90067

You can also keep up to date on the latest upgrades via our website at http://www.liebsoft.com or e-mail us at: sales@liebsoft.com.
Chapter 2  Getting Started

This section will provide additional information that would be configured after RED COM Management is installed, such as configuring systems lists, job scheduling service configuration and more. The installation of RED COM Management is addressed in the installation guide which may be downloaded from the documentation section on Lieberman Software's website at http://www.liebsoft.com/Support_Documentation. The installation guide also covers port requirements and supported host operating systems as well as the installation of pre-requisites.

IN THIS CHAPTER

Main Dialog ........................................................................................................... 6
Managed Systems Lists ....................................................................................... 9
Program Settings & Options ............................................................................. 51
Configuring Reports .......................................................................................... 67
Deferred Processing in Lieberman RED COM Management ...................... 74
2.1 MAIN DIALOG

The initial or main screen of RED COM Management displays lists of system sets that can be activated for systems management. Create an unlimited number of machine sets based on the network or organizational topology. Many customers add sets for domain controllers, web servers, other servers, workstations, and different physical locations on the WAN.

The purpose of this dialog is to display, edit and activate groups of systems for management. From the menus of this dialog are additional windows and menus to control licensing as well as backup and restore the internal database of the program.

To do useful work with this program it is essential to create at least one group and then activate it. Once a group is activated, add systems to the group and then perform a refresh to get the current state of the systems in the list.

On the bottom right side of the screen is the License Mode. Local Machine means a license is installed for the local machine. If the entry is Remote: ServerXXX then a shared the license key is installed on ServerXXX.
Just to the left of the License Mode field are options to manage groups of systems. **Activate** opens the selected group, while **Add** creates a new empty group, and **Delete** deletes the highlighted group from the list of managed groups.

### 2.1.1 Main Dialog Pull-Down Menus

**DATABASE**

- **Backup to Binary File** - Copies the internal database used by the program to a binary file.
- **Import from Binary File** - Restores the internal database from a backup file.
- **Export to Comma-Delimited File** - Copies the internal database to a comma-delimited file.
- **Import from Comma-Delimited File** - Restores the internal database from a comma-delimited backup file.
- **Import from ODBC Database** - Updates the list of systems, groups from an ODBC data source.
- **Scan IP Range for Groups/Machines** - Use the IP Scanner to add systems to the group.
- **Delete Internal Database** - Removes all traces of the internal database.

**JOBS**

- **Jobs Monitor** - Opens the Jobs Monitor Dialog.
- **Retry Policy** - Opens the Retry Policy Dialog.

**LOGGING**

- Opens the logging settings dialog

**HELP**

- **Contents** - Displays this help file.
- **License Keys** - The License Token Dialog allows manual assignment or release license keys to systems.
- **Register** - view and enter registration information.
- **Logon Info** - Displays current logon information.
- **About** - Displays version, product, and license information.
2.2 MANAGED SYSTEMS LISTS

Systems that will be managed are organized into lists called management sets. This allows creation of logical groupings of systems based on their type, operating system version, physical location, or any other personal organization scheme.

This chapter describes how to create and manage lists of systems. A system must be located in one or more management set before performing operations on it. This chapter includes all the ways to add or remove systems from the program as well as the ways to backup system list and program data.

There are multiple ways to add systems to the current management set.

To access these features, either select them off the context menu (right click in the systems list window) or click on the SystemsList menu option.

Add From Domain Systems List (on page 13) - This is the fastest way of adding systems that have joined a trusted domain. This uses the NT4 style domain browser.

Add From Network Browse List (on page 15) - The easiest way to find machines using the network browse list.

Add From Shell Network Browse List (on page 17) - Add systems from the Windows shell network browser.

Add Systems Manually (on page 18) - For machines that are not visible or have not joined the domain.

Add From Active Directory (on page 20) - To add machines using the Object Picker under Windows 2000 and later.

Add from IP Scanner - Add machines by specifying IP Address ranges or domains.

Import Systems List from a Text File - Import a list of systems from a text File.

Export Systems List to a Text File - Export a list of systems to a text File.
IN THIS CHAPTER

Create Management Sets ............................................................................. 10
Adding Systems to a Simple Management Set ............................................ 12
Backup System Sets ................................................................................. 43
Import Groups ............................................................................................. 44
Change the System Set Comment ................................................................. 49
Delete a System Set ..................................................................................... 50
Delete Internal Database ............................................................................. 50

2.2.1 Create Management Sets

To create a new management set, click Add.
Next, provide a name and an optional comment for the new group.

When finished, click **OK** to return to the Manage Groups Dialog. The new group will be in the list of groups to perform operations on.
2.2.2 Adding Systems to a Simple Management Set

There are various different ways to add systems to a management set manually once the set has been created:

- Add from domain systems list.
- Add from network browse list.
- Add from shell network browse list.
- Add systems manually by name
- Add from Active Directory
- Add from scanned IP ranges.
- Import/Export Systems List from text file.

These methods are in addition to the IP Scanner and ODBC query, which can both be used to create a new management set.
2.2.2.1 ADD FROM DOMAIN SYSTEMS LIST

Shown below is the Add from Domain List dialog.

The fastest method of adding Windows systems to this program is to inquire at the Domain Controller for the list of machines which have joined the domain. There are a few confusing cases when viewing servers in the domain list. The machine list may not represent all of the machines on the network (some machines may not have joined the domain). The list usually contains systems that have left the domain, but have not been purged from the domain database.
After adding machines to the Selected Systems list, use the **Platform?** button to verify the connectivity, credentials, and version of the selected systems. The **Platform?** feature contacts each machine on the list and inquires as to what version of the operating system it is running, as well as, which network services (Type) are running on the machine. This feature is an excellent way to verify that only live appropriate systems are added.

The Platform field indicates what operating system type is running.

The system name and system comment are both shown in the available systems list. After systems have been selected and checked (by pressing **Platform?**), there are columns to display the Platform, Version, Role, and Net Services.

The Net Services field indicates which network services are running on each system. It is normal for both a Workstation and Server to both have the Workstation and Server services running.

When performing domain lookups and platform checks the status, progress, and thread count are all updated in real time. The status box displays messages about the status of current the operation, and the active thread count displays how many threads have yet to complete for this operation.
2.2.2.2 ADD FROM NETWORK BROWSE LIST

Shown below is the Add From Network Browse dialog.

To add a machine using the Network Neighborhood browsing architecture of the operating system, press the **Insert** key on the keyboard or the **Browse** button on the Manage Systems dialog. Information can only be populated here is the Computer Browser services are started on your systems. If the Computer Browser services are not started, no information will be present in this list.

After adding machines to the Selected Systems list, use the **Platform?** button to verify the connectivity, credentials, and version of the selected systems. The **Platform?** feature contacts each machine on the list and inquires as to what version of the operating system it is running, as well as,
which network services (Type) are running on the machine. This feature is an excellent way to verify that only live appropriate systems are added.

The Platform field indicates what operating system type is running.

The system name and system comment are both shown in the available systems list. After systems have been selected and checked (by pressing Platform?), there are columns to display the Platform, Version, Role, and Net Services.

The Net Services field indicates which network services are running on each system. It is normal for both a Workstation and Server to both have the Workstation and Server services running.

When performing domain lookups and platform checks the status, progress, and thread count are all updated in real time. The status box displays messages about the status of current the operation, and the active thread count displays how many threads have yet to complete for this operation.
2.2.2.3 ADD FROM SHELL NETWORK BROWSE LIST

The Shell Network Browser dialog allows browsing the network for systems to add using the shell’s browse functionality. This may be helpful for adding machines from organizational units in Active Directory, since the shell allows browsing of the Active Directory hierarchy. In this view, organizational units are represented as folders in the hierarchy. If creating a separate set for each organizational unit in the company, populate the sets easily using this dialog.

After adding machines to the Selected Systems list, use the Platform? button to verify the connectivity, credentials, and version of the selected systems. The Platform? feature contacts each machine on the list and inquires as to what version of the operating system it is running, as well as,
which network services (Type) are running on the machine. This feature is an excellent way to verify that only live appropriate systems are added.

The Platform field indicates what operating system type is running.

The system name and system comment are both shown in the available systems list. After systems have been selected and checked (by pressing Platform?), there are columns to display the Platform, Version (4.0 is NT, 5.0 is Windows 2000, 5.1 is Windows XP, 5.2 is Server 2003, 6.0 is Windows Vista/2008, 6.1 is 7/2008R2, 6.2 is 8/2012, 6.3 is 8.1/2012R2), Role, and Net Services.

The Net Services field indicates which network services are running on each system. It is normal for both a Workstation and Server to both have the Workstation and Server services running.

When performing domain lookups and platform checks the status, progress, and thread count are all updated in real time. The status box displays messages about the status of current the operation, and the active thread count displays how many threads have yet to complete for this operation.

### 2.2.2.4 ADD SYSTEMS MANUALLY

Shown below is the Add Systems Manually dialog.

In cases where machines cannot be discovered, systems may need to be added manually.

After adding machines to the Selected Systems list, use the Platform? button to verify the connectivity, credentials, and version of the selected systems. The Platform? feature contacts each
machine on the list and inquires as to what version of the operating system it is running, as well as, which network services (Type) are running on the machine. This feature is an excellent way to verify that only live appropriate systems are added.

The Platform field indicates what operating system type is running.

The system name and system comment are both shown in the available systems list. After systems have been selected and checked (by pressing Platform?), there are columns to display the Platform, Version, Role, and Net Services.

The Net Services field indicates which network services are running on each system. It is normal for both a Workstation and Server to both have the Workstation and Server services running.

When performing domain lookups and platform checks the status, progress, and thread count are all updated in real time. The status box displays messages about the status of current the operation, and the active thread count displays how many threads have yet to complete for this operation.
2.2.2.5 ADD FROM ACTIVE DIRECTORY

Shown Below is the Add Systems from Active Directory dialog on the Active Directory Browse page.

The default options for the control are to show both up-level (native and mixed mode) systems, as well as, down level systems (NT). Options to search any desired domain controller or selection of a desired directory can be specified here.

The Browse Options (on page 21) page is detailed in the following section.
2.2.2.5.1 **BROWSE OPTIONS**

Shown below is the Browse Options page of the Add From Active Directory Dialog.

The **Browse Options** page shows the available options to put into effect when the "Browse..." button is clicked on the first page. There is typically no need to change the browse options, but if changes are made on the "Browse Options" page and then return to the first page and then click on the "Browse" button to see the results of the new options.

The default options are to browse for machines in up level and down level domains to which the host system is joined. The default domain is the currently logged on user account is authenticated with and the search is performed from the local machine.

▶ **ACTIVE DIRECTORY BROWSE OPTIONS – TARGET COMPUTER**

These options allow controlling where searches are to be performed. Normally these options should be ignored. Use these options to extract machine lists from foreign/non-Active Directory domains.
• **Skip Target Domain Controller Check** - Set this flag if the computer is not a domain controller, to save time. However, if the machine is a domain controller, this flag would not typically be set. It is usually best to select domain objects from the domain scope rather than from the domain controller itself.

• **Target Computer (optional)** – Allows specifying where to execute the search via the text entry field below the check box. Set the check box and set the field to a non-Active Directory domain controller to see a list of machines that have joined that domain (The "Skip Target Domain Controller Check" should be unchecked in this scenario). If the "Target Computer" entry field is blank, the current machine is the target computer.

### Active Directory Scope of Provider Search

These options allow controlling which data source is to be used for the machine search. Generally, leave all of these options unchecked.

• **Force Starting Scope as** - Sets the first entry in the "Look in" drop down to the option selection. Normally the drop down will default to its own choice.

• **Provider** - These options are different data sources for searches.

### Look-In Options

• **Up level Joined Domain** - Search the up level domain to which the target computer is joined. If this flag is set, use the "Up level Domain Controller" entry field to specify the name of a domain controller in the joined domain.

• **Up level Domain Controller Field** - This field can be blank even if the "Up level Joined Domain" is checked, in which case, the dialog box looks up the domain controller. This entry field enables specifying a domain controller in a multi-master domain. For example, an administrative application might make changes on a domain controller in a multi-master domain, and then open the object picker dialog box before the changes have been replicated on the other domain controllers.

• **Down level Joined Domain** - Search the down level domain to which the Lieberman RED Systems Management host computer is joined.

• **Enterprise Domain** - Search all Active Directory domains in the enterprise to which the target computer belongs. If the Up level Joined Domain check box is set, then the results represent all Active Directory domains in the enterprise except the joined domain.

• **External Up level Domain** - Search all up level domains external to the enterprise but trusted by the domain to which the target computer is joined.
• **External Down level Domain** - Search all down level domains external to the enterprise but trusted by the domain to which the target computer is joined.

• **Workgroup** - Search the workgroup to which the target computer is joined. Applies only if the target computer is not joined to a domain.

• **User Entered Up level Scope** - Enables entry of an up level scope. If neither of the "USER ENTERED..." types is specified, the dialog box restricts the query to the scopes in the "Look in" drop-down list.

• **User Entered Down level Scope** - Enables entering a down level scope.
2.2.2.6 ADD FROM IP SCANNED RANGE

This option will open up the IP Scanner Dialog (on page 27) to scan TCP/IP Address Ranges for systems that respond to the currently logged on credentials. Once the ranges are defined systems found, use the IP Scanner’s export options to add systems to system sets.
### IP Address Range Machine Add

<table>
<thead>
<tr>
<th>Subnets/IP Address Ranges to Scan</th>
<th>Count</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enb/ID #</td>
<td>AddrType</td>
<td>NetAddr</td>
</tr>
</tbody>
</table>

#### Systems Found:

<table>
<thead>
<tr>
<th>Enb/IP Addr</th>
<th>System</th>
<th>Domain</th>
<th>Comment</th>
<th>Subnet#</th>
<th>Role</th>
<th>Ver</th>
<th>AdminType</th>
<th>Alt#</th>
<th>AdminID</th>
</tr>
</thead>
</table>

#### Optional Alternate Administrator

<table>
<thead>
<tr>
<th>ID #</th>
<th>Description</th>
<th>Type</th>
<th>UserName</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default win...</td>
<td>Windows</td>
<td>%system%</td>
</tr>
</tbody>
</table>

### Log File:

- **Status:**

- **Progress:**

- **Current Logon Account:**
  - [UserAccount]

This dialog allows you to specify which Subnets and/or access machines to include in the scan.
As this feature successfully contacts each machine on the list it inquires as to what version of the operating system it is running, as well as, which network services (Type) are running on the machine. This feature is an excellent way to verify that only live appropriate systems are added.
2.2.2.6.1 IP SCANNER DIALOG

The IP Scanner allows one or more IP address ranges to be scanned for machines. By default, only systems that grant the currently logged on account or an alternate administrator account access will be added. A Configuring Reports (on page 67) package allows exporting the results of the IP scan to a text file, Excel spreadsheet, or database. The results can also be used to build system sets or add to an existing system set for further action.
The main dialog is shown below.
The main sections of the dialog are:

Subnets/IP Ranges to Scan panel at the top of the screen. This panel lists the ranges that will be scanned to search for systems to add to the current system set. Add, edit, or delete ranges by using the buttons underneath the panel labeled: Add, Edit, Delete.

Scanned IP Addresses. This panel displays the list of systems found in the range of the scan.

Exclusion List. Not all machines returned by the IP Scanner should be imported into a system set. Certain machines may be already known as untouchable/critical where settings should not be changed under any circumstances. The program provides an editable Exclusion List to enter the NETBIOS names of the machines to exclude.

When performing an IP scan, all machines capable of administrative access are added to the "Scanned IP Addresses with administrator level access" list, however, any machines that also appear on the Exclusion List are disabled (unchecked) by default. Unchecked systems will not be exported.

To edit the Exclusion List, click on the "Edit" button to the right of the "Exclusion List."

Optional Administrator Account. This is the list of alternate administrator accounts. This list can be edited through the menu.

Log File. This is where the log of actions is displayed to the screen.

Clicking on the "Add" button under the top Panel brings up the dialog box shown below. The "IP Address Range Type" radio buttons allow entering the address format in either Network Address format or IP Stop/Start format. If using the Network Address format, click on the "Calculate >>" button to see the range of address generated by the subnet of the Network Address. Alternatively, click on the "Analyze Entries" button to examine the address range and report on the class and format of the address range.

Clicking on the "Edit" button will display the same dialog, but any changes will be made to the selected entry in the panel.

Enable or disable any address range by checking/un-checking the "Enable Entry" check box.
The name of the subnet or address can be entered in the "Description" field.

In the middle of the main dialog you will be buttons to "Set Fields". Highlighting one or more entries in the Subnets list (top list) and then clicking on the "Subnet" or "Skip" buttons will change the subnets and skipped address ranges for all of the highlighted entries. This is useful feature when needing to modify a range of imported network address ranges.

The "Select" group of buttons will highlight all or none of the address ranges. The "Enable" buttons allow will enable (check) or disable (un-check) all highlighted entries. This is useful when only scanning a subset of all addresses available is desired.

To perform the scan, click on the "Scan Now" button or use the menu option: "Scan Subnet | Start." Notice that the "Status" field (lower right) will show the highest IP address currently being
scanned. The "Progress" bar will also show the percentage of addresses processed (or in process). To see when the process is complete, keep an eye on the "Active Threads" number. When this number goes to zero, the scan is completed.

A "Log File" list box display any unusual return codes from your systems. One common error code is 1723. This error can mean that the local protocol stack is getting confused (this should be corrected in a Microsoft Service Pack). This error can be ignored without any worry since the scanner will continue to retry until the protocol stack gets back into proper operation.

When the scan is completed, a list of entries that fully identifies each machine will display. These results can be sorted result by clicking on the column headers. Any entries which should not be exported can be disabled by highlighting entries and clicking on the "Yes" or "No" button in the "Enable" button group below the list of scanned machines.

IN THIS CHAPTER

IP Scanner Menu - File.................................................................................................. 33
IP Scanner Menu - Options.......................................................................................... 37
IP Scanner Menu - Scan Subnet.................................................................................... 37
IP Scanner Menu - Report Generator............................................................................ 37
IP Scanner Menu - Alternate Administrators ............................................................... 39
IP Scanner Menu - Exclusion List.................................................................................. 41
Vulnerability Testing...................................................................................................... 41
IP SCANNER MENU - FILE

Options on this Menu:

- **Import Subnet List** - Allows you to import a list of subnet addresses to scan.
- **Export Scanned Entries** - Allows you to export a list of systems from the results of the scan.

**Import Subnet List**

Import a range of subnets into the scanner for scanning if the file format is organized as:

```
Network Address1
;Comment
Network Address2
;Comment
```

To import a range, click **File | Import Subnet List**. This will activate the following dialog to confirm that the file being imported is in the correct format.
Click **Next**. Specify the path to the file containing a list of network addresses. After selecting the file to use, the following dialog which confirms the selection will appear.

Click **Next**. Specify the default subnet mask for each imported network address. The subnet mask helps limit the range of addresses to be scanned. If some of the network addresses are different, go back later and edit the subnet masks.
After clicking on the **Next** button, a final dialog box will pop-up that will prompt to skip the first, last and gateway (start+1) addresses in the subnet range. Normally leave these check boxes to be unchecked. The state of these check boxes is shown in the "NetSkip" column of the main dialog.

Click the **Import** button to add the subnets to scan to the list. Notice that all of the entries have a check box next to them that is checked. By default, all address ranges are enabled.

*Export Scanned Entries*

Before exporting any of the scanned systems, make sure any systems that should not be exported are disabled (unchecked). To disable any excluded systems, click on the **Apply** button within the *Exclude Systems List* area (normally step is not necessary unless the Exclusion List is loaded after completing the scan and the Exclusion List to needs to take effect on the results already in the list.

To export, click on the **Export** button located to the right and button of the list of systems. This may also be done by clicking the **File | Export Scanned Entries.**
The following dialog will now appear:

![Export Scan List Options](image)

It is possible to export the NetBIOS names or the raw IP addresses to the management set. The NetBIOS name export is the preferred format. The distribution of the scanned machines can be as follows:

Automatically creates a new system set where the name is composed of the combination of the number of the subnet/address range in the list combined with a description. This is a good option if a router table with address as the source of the address ranges to scan was imported. Populate the created management sets with those machines that are in the IP range of the management set (same subnet/IP range).

Automatically creates a system set for each unique domain/workgroup retrieved from the scanned systems. Use this option to manage machines by domain where the machines are spread across multiple network segments.

Import all of the enabled (checked) scanned systems into the current management set.

Click on the **OK** button to perform the export. The operation is very fast. Then go into the current system set or go back to the main program dialog select a different system set.
IP SCANNER MENU - OPTIONS

Options for this Menu:

Thread Maximum Override

Once a list of IP address ranges to scan is set, the next logical step is to begin the actual scanning. The scanning step uses as many threads up to the maximum (configurable, but 100 by default). This value can be overridden by clicking on the Options | Thread Maximum Override.

The upside of increasing the number of threads is that a large address range can be scanned quickly. The downside is that stopping a scan can take an extended period of time as all outstanding network requests must finish or timeout. Increasing thread count can also set off an intrusion detection/prevention system. When working with this feature, set the number to 10 for a relatively quick stop time, and increase the number to 1000 or 5000 to scan large ranges of systems.

IP SCANNER MENU - SCAN SUBNET

Start - Begins the scan of the selected subnet range.

Stop - Tells all the threads working on scanning the subnet range to stop.

Validate Subnet Table Values - verifies that the given range is able to be scanned. This would detect bad input from imported lists of subnet ranges.

IP SCANNER MENU - REPORT GENERATOR

Options on this menu:

- SUBNET/IP ADDRESS RANGE LIST - tells the Report Generator to output the Subnets/IP Address Range List panel including all systems in the list and all columns in the list.

- IP SCAN RESULTS - tells the Report Generator to output the Scanned IP Addresses panel including all the systems in the list and all the columns in the list.

Note that both of these features make use of the Configuring Reports (on page 67) feature.
IP SCANNER MENU - ALTERNATE ADMINISTRATORS

The options for Alternate Administrators are shown in the bottom of the dialog box of the IP Scanner. The List of available alternate administrator accounts is in the lower left. Options from this menu can be used to add, edit, and delete alternate administrators from this list.

All previously entered alternate administrator accounts (if any) are used by the IP Scanner. To use the default (current) logon credentials, un-check the Enable Alternate Administrators check box on the right bottom side of the dialog. To add additional alternate administrators, right click on the list in the lower left hand corners or use the Alternate Administrators menu options to add, edit, or delete alternate administrator accounts.

If using the wild card of %SYSTEM% for impersonating accounts, the IP address will be prefixed onto the account. This may or may not work with some systems. Generally the prefix information for the system will be safely ignored.

Administrator Accounts Menu - Add

The adding and editing of alternate administrators is handled by a simple dialog shown below.

- **Add** - To add another alternate administrator account, fill out the user name and both password fields, then select whether the alternate administrator is local or a domain administrator. Click **OK** to add to the Alternate Administrator List.
• **Edit** - To edit an alternate administrator account, simply make any changes to the current alternate administrator account and click **OK** to update the Alternate Administrator List.

• **Delete** - A dialog asking for confirmation to delete the alternate administrator account will appear.
**IP SCANNER MENU - EXCLUSION LIST**

Options for this Menu:

- **SYSTEMS EXCLUDED FROM ALL OPERATIONS** - Access to the Exclusion List.
- **APPLY TO IP RESULTS** - Masks the excluded systems from those found in the IP scan.

*Systems Excluded From all Operations*

Use the **Add** and **Delete** buttons to manually change the Exclusion List. It is possible to provide a text file containing critical systems that should not normally be modified, use the **Import List**... button to load the list. The format of the imported list is simply to put each machine name on a line by itself.

![Exclusion List dialog]

**VULNERABILITY TESTING**

One use of the IP Scanner is to find system on the network that are vulnerable to attack using the default administrator setting of built-in administrator account being named "administrator" with a blank password.

To perform this test, do a local logon to the host system with a local administrator account that is unique. Make sure that the account chosen for the local logon does not appear on any of the remote machines. Next, enter the alternate credentials of: an account being named "administrator" with its password as blank. Make sure that the check box for **Enable Alternate Administrators** is checked. Now perform a scan of the network. What is returned is a list of all machines that can be connected to with the default administrator credentials and a blank password.
If these systems are directly connected to the Internet, this scan is especially important to perform.

### 2.2.2.7 IMPORT/EXPORT SYSTEMS LIST

There are following methods listed under the SystemsList | Import/Export Systems List menu item to import or export systems lists:

- Import System List from Text File
- Export System List to a Text File

These methods make it easy to import systems lists from text files. An import will require a previously created list of systems that is properly formatted. Properly formatted text files of systems lists have one system name per line.
2.2.3 Backup System Sets

There are various ways to backup system sets and/or program information:

1) Backup Internal Database to Binary File.
2) Backup Systems list to a Text File.

2.2.3.1 BACKUP INTERNAL DATABASE

To backup all RED COM Management information including system set to a binary file, choose the Backup to Binary File from the Database menu on the main dialog. Supply a path to save the file. The resultant file is NOT human readable and can be used to backup system sets for disaster recovery or to transfer group information from one computer to another.

2.2.3.2 EXPORT SYSTEMS LIST TO A COMMA-DELIMITED FILE

To backup all program information including system sets to a CSV file, choose the Export to Comma-Delimited File from the Database menu on the main dialog. This will save the system list database to a comma-delimited text file. Specify a path and a file name for the new backup file. The text file is human readable and can be used to backup system sets for disaster recovery or to transfer group information from one computer to another.
2.2.4 Import Groups

*RED COM Management* allows importing a systems list from a text file (CSV), an ODBC data source, or a generated binary backup file. A properly formatted system list text file contains one system name per line.
2.2.4.1 IMPORT FROM ODBC DATASOURCE

Many organizations are more than happy manually setting up system sets and populating those system sets manually from domain or browse lists. On the other hand, large companies that have a constantly changing inventory of machines under management will find manual methods cumbersome. The ODBC import capability allows this program to set-up its management sets and machine members from a database of systems. Source databases can be comma-delimited files, Excel spreadsheets, and SQL Server databases. In fact, almost every database today has an ODBC interface that is compatible with this program.

To use this feature, system set data should be located in three columns within the data source: one column for corresponds to set name, another to set comment, and a third to system name.

Getting Started

Before using this feature, permission to access to the database containing the information is required. Next, set up a ‘data source’ (also known as a DSN). This is under administrative tools. Lastly, identify which table contains the system set and machine name information as well as the column names for that information.

Remember that the machine name must be the NetBIOS machine name or the TCP/IP address (although this is not nearly as friendly).

The last part is to set up the program to perform the import and create a little snippet of SQL code to do the retrieval.
To start, on the main dialog of the program (not in a management set), go to **Groups | Import from ODBC Datasource**.

![Get ODBC Data dialog](image)

Each part of the dialog and example steps to set up a simple interaction is described below.

- **Set the Database Connection String** *(on page 47)*
- **SQL Statement** *(on page 48)*
- **Retrieving the Data using the Database** *(on page 48)*
2.2.4.1.1 SET THE DATABASE CONNECTION STRING

Click on the button ‘...’ to the right of the Database Connection String entry field. Select the tab for **Machine Data Source**.

If the data source is already configured, select it from the list and click on the **OK** button. If the data source is not created, click on the **New** button.

Using the wizard, create a data source to point to the database. This will involve picking a device driver, giving the data source a name, and finding it (attaching to it). **Make sure an ODBC compatible data source is configured.**

When all of the steps are completed correctly, the database connection string will become available:

```
DSN=SYZCORP;DBQ=D:\SysMgr\xyz.mdb;DriverId=25;FIL=MS Access;
MaxBufferSize=2048;PageTimeout=5;
```
2.2.4.1.2 SQL STATEMENT

Now write a simple piece of SQL code into the ‘SQL Statement’ field. This is nothing more than a single line of text that tells the ODBC driver what table to use in your database as well as which fields to retrieve. The format of the code is:

```
Select "field1", "field2", "field3" from Table
```

Optionally, add a second line containing a qualifier such as:

```
Select "field1", "field2", "field3" from Table
Where Table.field4 = 'Windows Servers'
```

or other such qualification to make sure that only the correct records are retrieved.

The returned fields are used as follows:

- **field1** – Group Name
- **field2** – Group Comment
- **field3** – Machine Name or IP Address

When retrieving data from an Excel database, put the ‘Table’ portion of the SQL statement in square brackets ‘[Table]’.

2.2.4.1.3 RETRIEVING THE DATA USING THE DATABASE

To execute the SQL code against the data source, click on the **Get Data** button. In the log at the bottom of the dialog note the statistics of the retrieval (example statistics):

- Unique Groups: 244
- Unique Comments: 5
- Unique Machines: 1569

At the top of the dialog are the retrieved records. The retrieved records show which system sets will be created as well as the machine names that will be added to those sets. To import all of these sets and machines, click on the **Apply** button.

To merge into an existing system sets, leave the check box: **Replace all existing sets and machines with this data** unchecked. If the existing data should be purged and replaced with the retrieved data, set the box to the checked state.
2.2.4.2 IMPORT FROM A COMMA-DELIMITED FILE

To create a set from a comma-delimited list of systems, select the properly formatted list of systems and then click OK. This feature can be used to transfer sets from one machine to another, to backup sets, or to copy entire sets.

A CSV file used for system set importation will be formatted as:
System_Set_Name,System_Set_Comment,System_Name.

2.2.4.3 IMPORT FROM A SCANNED IP RANGE

This allows the IP Scanner to scan IP Ranges for systems and then use the scanned systems to create a new system set. To perform this operation:

1) Click on the Scan IP Ranges for Groups/Machines from the Database menu.
2) Define the IP range to include in the group.
3) Click on Export Scanned Entries from the File menu in the IP Scanner.
4) Select either option for creating new groups according to Domain Name.
5) Click OK.

The system will tell how many total machines were added. There should now be new system sets for all the machines scanned. The machines will be in sets according to their domain or subnet and subnet description.

2.2.4.4 RESTORE FROM A BINARY FILE

Use this option to Restore the internal database and all associated system sets and systems. The file must have been previously created using the Database | Export to a Binary File option. Select the backup file and click OK to restore Lieberman RED COM Management’s internal database.

2.2.5 Change the System Set Comment

To change a comment field for a system set, open the system set and choose Set Group Comment from the File menu. This will display the Group Comment Editor shown below.
The name of a management set cannot be changed.

Click **OK** to set the new group comment.

### 2.2.6 Delete a System Set

To delete a system set, form the main dialog, select the system set(s) and click the **Delete** button.

### 2.2.7 Delete Internal Database

Select this option from the **Database** menu to remove all traces of the RED COM Management internal database from the system. This will remove all system sets, and all information about all managed systems.
2.3 PROGRAM SETTINGS & OPTIONS

This chapter outlines the program-wide settings. Things in this chapter include, General Options, logging settings, scheduling and retry settings, and more. Most options described are available when viewing a systems list.

IN THIS CHAPTER

Logging Options................................................................. 51
Configuring Email Server Settings .................................... 53
Alternate Administrators..................................................... 63

2.3.1 Logging Options

Before using the product, examine the log file settings. The log file settings are on the main dialog on the Logging menu.

By default, the log file will be created in the location recommended by Microsoft for application log files. This location will vary by operating system. If log files should be kept elsewhere, specify a new log file location/name.

There are two levels of logging normally available: extended and normal. The extended (verbose) mode includes normal log information as well as information on the internal phases the product goes through. In normal operation, the extended logging option should not be used due to the large amount of normally useless information that is produced (the information is useful for debugging should it become necessary).
The log file is always appended too. It is always safe to read/copy the log file when changes are not in progress. To delete the log file will require the program first be stopped.

- **Enable Logging** - When enabled, logging is enabled for all operations.
- **Extended Logging** - When logging is enabled, this adds verbose information to the logs.
- **Log Statistics** - By checking the Log Statistics check box, the log will receive the pre and post transaction counts for the following categories: users, groups and group memberships.
- **View** - View the event log in a text file.
- **Print** - Print the text log file.
- **Delete** - Delete the current log file.
- **Log Size** - Displays the current size of the log file in bytes.
- **Windows Event Log** - These options tell the program to log to the computer’s application log. The remote computer is the computer that is being changed by the program and the local machine is the machine that the program is running on. This makes possible logging to the application event log for both machines affected by the program.
2.3.2 Configuring Email Server Settings

Email settings are found at Settings > Email Settings.

This product can send email via SMTP for reporting and alerting purposes. Access to an SMTP email server is required. This topic documents how to configure the "SMTP Email Settings" dialog.
2.3.2.1 SMTP SETTINGS: GENERAL

Use the **General** tab to configure settings for sending SMTP email messages, including sender information; priority, sensitivity, and importance settings; and custom message headers.

![SMTP Email Settings](image)
Email Profile

- **Profile Name** – While multiple email profiles may be created, only one may be used. The default profile name is called **Default**.

- **Description** - Text field that may be edited and used to enter a short note or description regarding the email profile.

Sender Information

This information is sent with each email in its header and will appear when the recipient reads the mail. Some email servers will reject messages that lack the proper address information for these fields (i.e. wrong domain name).

- **Name** - The friendly name of the email sender.
- **Organization** - Enter the name of your organization.
- **Sender Email** - Enter an email address that tells the recipient who this is message is "From".
- **Reply-to Email** - If a user replied to the email, this is the address the email will be sent back "To".

  **Read Receipts Email** - Optional. Enter the address that a read receipt should be sent to. Adds the Disposition-Notification-To header field to the email message. The read receipt is a request for the receiving email client to send a delivery status notification as soon as the person opens the email. If the reader approves the read receipt be returned, the reader's email client will send a reply email to the reply-to email address specified in the profile settings.

- **Return Receipt To Email** - Optional. Enter the address that a delivery receipt for the message should be sent to. Adds the Return-Receipt-To header field to the email message. The delivery receipt is a request for the receiving mail server to send a delivery status notification as soon as it receives the email.

Priority / Sensitivity / Importance

- (Optional) For each property, select the value that should be applied to email messages sent by this product. How these settings are processed depends on the client application that receives the email. For example, in Microsoft Outlook, a message with a Priority setting of Urgent displays with an exclamation mark (!) next to the message.

Advanced Message Settings

This section should not be confused with email subject lines. Do not enter any information in these fields if you are not comfortable writing customer MIME headers for email. Use this section to enter
a custom message header (MIME header) to be included in all email messages. Message headers are special text added to the message before the body of the message appears. Leave this section blank if special headers are not needed.

- **Name** - The attribute name to include in the message header.
- **Value** - The attribute value to include in the message header.
2.3.2.2 SMTP SETTINGS: OUTGOING SERVER

Use the **Outgoing Server** tab to configure SMTP server settings.

![SMTP Email Settings](image)

**Outgoing SMTP Server Settings**
- **Outgoing SMTP Server Name**: symail
- **Port**: 25
- **Server Timeout (seconds)**: 30
- **Authentication Method**: USER_PASSWORD
- **SSL/TLS Channel Encryption**: AUTOMATIC

**Email Server Authentication**
- **Use Authentication Credentials** (DISABLED=Anonymous)
  - **User Name**: lsadmin
  - **Password**: ******

**Email Server SSL Settings**
- **Use SSL Client Certificate Authentication**
  - **User Certificate File**: ...
  - **User Authentication Certificate Store**: ...
  - **User Certificate Password**: ...
Outgoing SMTP Server Settings

How you configure these settings will depend on how your SMTP server is configured.

- **Outgoing SMTP Server Name** – Enter the DNS name or IP address of the server.

- **Port** – Port 25 is standard for email. For SSL/TLS Encrypted email it may be port 25 or port 465 or 587.

- **Default (Button)** – Resets the port number value to port 25.

- **Server Timeout** – The default value of 30 seconds work in most cases. Increase this time if necessary.

- **Authentication Method** – Choose the authentication option that your SMTP server is configured to use. Incorrect method settings can prevent connectivity with a mail server even when the credentials are correct.
  - USER_PASSWORD - basic username and password as spelled out in the Email Server Authentication section.
  - CRAMMD5 - challenge-response authentication mechanism protects the password in transit.
  - NTLM - NTLM challenge-response authentication to email server which never actually sends a user password.
  - SASLPLAIN - challenge-response authentication that does not protect the password in transit.
  - KERBEROS - Kerberos authentication with the email server.
  - XOAUTH2 - Use XOAUTH2 method to authenticate to the email server. This will also require configuration of the OAUTH2 Authentication tab.

- **SSL/TLS Channel Encryption** – If using SSL/TLS encryption, choose the option that your SMTP server is configured to use.
  - AUTOMATIC - negotiate with the email server to find a supported SSL/TLS or plain text method. Not all email servers support negotiation.
  - IMPLICIT - the mail server expects the initial connection to already be encrypted.
  - EXPLICIT - the mail server does not require the initial connection be made with SSL/TLS but may use SSL/TLS after the connection is initiated.
  - NONE - use when automatic negotiation does not work and SSL/TLS is not configured on the email server.
Email Server Authentication

Use Authentication Credentials – Select this option if your SMTP server requires authentication; otherwise, clear it to use Anonymous authentication.

The following settings are required if Use Authentication Credentials is enabled.

- **User Name** – The user name configured to authenticate to the SMTP server.
- **Password** – The password required to authenticate to the SMTP server.

Email Server SSL Settings

Use SSL Client Certificate Authentication – Select this option if your SMTP server is configured to use SSL encryption. SSL encryption allows both logon credentials and data to be encrypted during the SMTP transaction. The server must be already set up to use SSL encryption for this option to work. Test the SSL functionality with an email client to confirm that all SSL components are configured correctly.

The following settings are required if Use SSL Client Certificate Authentication is enabled.

- Choose one of the following options:
  - **User Certificate File** – Enter the path to the security certificate file.
  - **User Authentication Certificate Store** – Enter the path to the certificate store if one is configured.
- **User Certificate Password** – If required, enter the password that further secures the certificate file.
- **Enable Cached Certificate** – Select to allow caching of the certificate information.

Test Options

- **Test Connection** – Click to verify connectivity to the SMTP server and that the server accepts the configured credentials. This feature completes the handshake with the server to test that mail can be sent, but it does not send mail.

  The program log records the transaction details:
  
  SetMailServer error: 11001, [11001] Host not found
  Failed to fill SMTP settings
  Failed to send email message error: Host not found.

- **Send Test Email** – Sends a test email message.
2.3.2.3 SMTP SETTINGS: SMTP LOGGING

Use the **SMTP Logging** tab to configure logging options for SMTP email. Communication transaction details are logged as SMTP operations are performed. These options are useful for debugging problems with SMTP traffic.
• **Enable Event Log Logging** – Select this option if the solution should write SMTP log events to the Windows event log.

• **Enable SMTP File Logging** – Select this option if the solution should write SMTP application log events to a text file. Configure the following setting if **Enable SMTP File Logging** is enabled:
  - **Log File Name** – Provide the path to the .txt file where SMTP events should be logged.
2.3.3 Alternate Administrators

This feature allows specifying additional sets of credentials that can be used to administer systems in multiple [un-]trusted domains and work groups. The program will automatically use the current login credentials or any of the alternate administrator credentials when it performs operations.

When Alternate Administrators are enabled, it is normal to experience delays on some machines during operations because the program must wait for bad credentials to time-out before trying alternate credentials.

To access the Alternate Administrators dialog, open any set of systems and click the Alternate Administrators Accounts options from either the Settings menu or ConnectAs menu.

In newer versions of Microsoft operating systems, there may be issues using Alternate Administrators (impersonation) to manage any reliant COM+/DCOM interfaces and applications. This is a Microsoft imposed limitation.

IN THIS CHAPTER

Administrator Accounts Editor ........................................................................................................... 64
2.3.3.1 ADMINISTRATOR ACCOUNTS EDITOR

Shown below is the Administrator Accounts Editor Dialog.

The top list shows the list of systems in the current set and any previous information recorded about the systems. The lower left of the dialog lists the alternate administrator accounts. The Status field shows the current status of any task that has begun and has not yet completed. The Active Threads box shows how many threads are working on the current task (zero when work is completed/no operation in progress). The progress bar is an approximation of task completion. The Current Logon Account is the account the solution is opened as. The check box titled Enable
**Alternate Administrators** is a program wide option that allows the use of alternate administrative credentials for all connections made through the tool.

Alternate administrator accounts can be edited by using the Administrator Accounts Editor menu option.

**Alternate Administrator Accounts…**

When choosing to edit and or delete one of the entries, first highlight an entry and use either the **Edit** or **Delete** menu option. To add a new alternate administrator, use the **Add** option (Also available through the Alternate Administrators menu item). These options are also available through the context menu (right-click menu) of the Alternate Administrators List.

Enter the name of the alternate administrator (use the "domain\account format" or "account" formats) by manual entry, or via the **Local** or **Domain** browse buttons. Substitution, such as '%system%' to replace the system name for local account changes to multiple machines may also be used.

For example: The local machine name is DCTR1, is a domain controller in domain DOMAIN, and has an account named CustomUser. The target machines each have local accounts named CustomUser, but can also be accessed by the account DOMAIN\CustomUser. By specifying %system%\CustomUser, the local CustomUser account on each machine is specified, rather than the domain account DOMAIN\CustomUser account on each machine.
TESTING ADMINISTRATOR ACCOUNT ACCESS

Check the Enable Alternate Administrators check box to use all alternate credentials when accessing systems.

To test access, highlight one or more systems (if none are selected, all systems in the list are tested for access) and click on the Test Access button (or go to the menu item Test Access | Start). This test will identify which systems are on-line in and which credentials worked with which systems. The testing is completed when the threads counter equals zero.

The columns for AdminID and AdminPwd show which account/password provided administrator access to each remote system. If there is a number in the ALT# field, this corresponds the ID# of the alternate administrator account that successfully connected. If a dash (-) is in the ALT# field, it means that an alternate administrator account was not used to connect to the computer. If none of the entries worked, this will be reflected in the Access Status field. Lack of appropriate administrator credentials is shown by an error code of 5 - Access Denied. Other error codes (i.e. 53, 1722) usually indicate an off-line system.

ENABLE ALTERNATE ADMINISTRATORS

Typically, the logon account will be used for connections. To have the program try alternates in case of problems authenticating, set the check box: Enable Alternate Administrators. Be aware that not every feature in the solution may work through alternate administrators as there may be limitations on impersonation imposed by Microsoft.

REPORT GENERATOR - ALTERNATE ADMINISTRATORS

Export the results of an authentication test using the built in Configuring Reports (on page 67).
2.4 CONFIGURING REPORTS

You can create reports from many places in RED Systems Management. For example, ways to open the "Report Generator" dialog in the management console include the following:

- From the main screen, choose **SystemsList > Create Report from Display List**
- From the "Stored Jobs" dialog, choose **Report > Generate Report**
- From the "Enroll Identities" dialog, click **Report**
- From the "Web Application Self-Recovery" Rules dialog, click **Report**
- And so on.

Regardless of where the report is generated from, the "Report Generator" dialog (shown below) and functionality are the same.
Configuring the "Report Generator" Dialog

To create a report output file and launch an appropriate viewer for the file, click Generate Report located at the bottom of the dialog.

Normally, after a report is generated, the report dialog window will save its settings and close. To prevent the dialog from closing after completing the generation of a report, select the Do not close
dialog after report generation option. To save new dialog settings without generating a report, click the Save Settings button. To abort the report generation click Cancel.

The Export Data Columns list shows the columns in the list for which the report is being generated (in this case, the managed set list in the main window). Change if a particular column will be exported by double-clicking on it. Check/un-check all columns by using the All and None buttons to the right of the list. Columns with an X to the left of the column will be exported.

The Export Status Columns section will add a status column to the output that indicates the rows in the source list box that were highlighted (selected). If this option is selected, the generated report will have an additional column; the new column rows that were selected will be labeled Yes and rows that were not selected will be labeled No.

The Limit Output to Rows with section will export only those rows that were highlighted in the previous list (requires the report to be run from a dialog with a list of items that are selectable).

The No Column Headers option exports just the results without including the data column header titles.

The File Name box shows the file name for the generated report. A valid output file for the report must exist, even if no action is taken based on the report. The extension of the file is automatically adjusted to be a valid extension based on the report type. The file extension can be overwritten in the file name box.

The Report File Output Type defines the output type. There are four file types that the Report Generator can generate:

- **Comma Delimited** – Column data is separated with a comma with the first row containing the column names. This can be read into a spreadsheet program, such as Microsoft Excel.
- **Tab Delimited** – Similar to comma-delimited except tab characters are used instead of commas.
- **Fixed Column Width** – Columns are space padded to the fixed width. Specify how wide (in characters) each column should be. This is useful for fixed size viewing and printing, and in some displays that may have limited space. Information that does not fit within the fixed size is truncated on generation. This format is useful for generating human readable output.
- **HTML** – Customizable HTML reports. The HTML output in the HTML Edit Dialog (on page 72) may be edited.

The Post-Generation Action section shows the actions to be taken after the output file is generated.

- **Create File Only** simply generates the output file.
- **View** or **Print** the report to invoke the View or Print shell actions on the resulting report file (the actual program invoked to view or print is dependent on shell settings for actions based on the extension of the report file).

- Choose **Execute Program** to execute an arbitrary program after the report is generated. Click the ellipses (…) button to pull up the executable editing window.

- Choose **Email** to email the resulting report file (inline or as an attachment). Click the ellipses (…) button to pull up the [Configuring Email Server Settings](#) on page 53.

- If the **Show Dialog on Success** option is selected, the program will display a dialog box when the report action is complete. (This may be useful if the action produces no visible feedback itself.) The program will always show a dialog box if an error occurs during the report generation/action.

The **Title** field allows editing the title of the report. This is only valid for HTML reports. The **Edit** setting generates a window that allows the addition of replaceable report-specific variables to the report title.
2.4.1 Report File Output Type

There are four file types that the Report Generator can generate:

- **Comma Delimited** - Column data is separated with a comma with the first row containing the column names. This can be read into a spreadsheet such as Excel.

- **Tab Delimited** - Similar to comma delimited except tab characters are used rather than commas.

- **Fixed Column Width** - Specify how wide each column is in characters. This is useful for fixed size viewing, printing, and some displays that may have limited space. Information that does not fit within the fixed size is truncated on generation. This format is useful for generating human readable output.

- **HTML** - Customizable HTML reports.
2.4.1.1 HTML EDIT DIALOG

Configure the HTML report output in the "Edit" dialog. The HTML output template is set to the default template the first time the report generator is run. It is always possible to revert to the default template by pressing the Default button.

It is possible to create many template files for HTML reports. Use the file name editor to select which template file is currently being editing. The file menu allows opening or saving templates. The current template file is shown in the template editing window and can be edited directly. Alternatively, the template may be edited outside of the program by any other HTML editor.
The top of the edit window shows the variables that can be used in the report that will be automatically populated with data specific to the actual report being generated. These variables can be inserted into the template file at the current cursor position by using the **Insert** button, double-clicking the variable that should be inserted, or simply entering the variable name directly into the template.

The look of the generated report data is controlled by several CSS style elements. The default template has default styles for these elements and these styles can be edited. The look of the report title elements is set directly in the HTML (which can also be modified).

### 2.4.2 Post-Generation Action

The Report Generator allows actions when the generation of the report is complete. The following options are currently available:

- **CREATE FILE ONLY** - Only create the file.
- **VIEW** - View the file using the default shell viewer based on the file extension.
- **PRINT** - Generate the report and use the default shell printing application based on the report file extension.
- **EXECUTE PROGRAM** - Allows specifying a program to be run upon the completion of report file generation. With this option, specify the path to the program and any additional command line arguments to run with the program with.
- **E-MAIL** - Email the report file in the body of an email or as an attachment. Specify a list of email addresses to send the report to and append a custom subject line to the report.
2.5 DEFERRED PROCESSING IN LIEBERMAN RED COM MANAGEMENT

RED COM Management does not provide a full featured scheduling system where jobs can be scheduled to occur at future dates and times. Rather, RED COM Management does provide a scheduling program to retry jobs that may have failed during an interactive job run. When a job failure occurs, a failure dialog will pop-up and present the option to retry the failed operation:

The job process is handled by a scheduling service (Windows Service) that runs on the RED COM Management host system. The service runs under an administrator level account due to the accesses required on target systems. It is best to use a domain administrator account for this service given that it will be accessing many if not all systems in the network. The program periodically (default is 60 seconds) checks for any jobs that need action as well as if any retry jobs are ready to be tried again. The job dispatching mechanism works as a queue, so older jobs will always run before newer jobs if more than one job should be dispatched. Only one deferred job will run at a time. Install and start the deferred processing service to permit any deferred processing to take place. The setup and management of the deferred processing service is handled through the Jobs Monitor dialog.

The Jobs Monitor dialog can be launched either from the main program dialog or from the systems list dialog. The jobs monitor shows the current jobs; get more details on any job by double-clicking on it. These jobs may be edited, deleted, restarted or paused. The scheduler job log can also be viewed, printed, or erased. The retry policy (wait between retries, which errors to ignore, etc.) can also be set from this dialog.
Note: If the system that is running the deferred processing service is restarted, make sure that the scheduler is restarted when the system comes back up.
2.5.1 Jobs Monitor Dialog

Shown Below is the Jobs Monitor dialog. The Job Monitor allows viewing and managing jobs that have not yet completed or jobs that are set to run in the future. The Jobs Monitor will also show the status of any jobs that have failed and are being retried.

<table>
<thead>
<tr>
<th>JobID</th>
<th>Comment</th>
<th>Action</th>
<th>SysCnt/Todo</th>
<th>State</th>
<th>Retries</th>
<th>Last Run</th>
<th>Last El</th>
<th>RtnErr</th>
<th>Next Run</th>
<th>Hourly: XX:XX</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000000D</td>
<td></td>
<td></td>
<td>42/42</td>
<td>Running</td>
<td>0</td>
<td></td>
<td>00:00:00</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The top list shows the current list of jobs and each job's status. In the dialog shown, there are currently no pending jobs. The columns of the list show the job type, the number of machines the job was originally run on (and the number remaining to complete), the current state of the job, the
number of retries attempted, the time and result of the last run, the time of the next attempt, and
the status of the job.

The middle section of this window has three parts. On the top left, there is a section which shows
the status of the scheduler service. From here, it is possible to adjust the scheduler service state
(and the Job Scheduler Service Installation (on page 84)), the sleep time between runs, and the
general Retry Settings Dialog. If the service is running, the numbers in the countdown box will
count down to 0.

The top right box has controls for manipulating the jobs. Edit Job Properties, pause and resume
jobs, delete jobs from the list, or restart jobs from here.

The bottom section has controls for the Job Scheduler Log File Dialog (on page 82). Adjust the log
file name and location, as well as view and erase the log from here.

**Note:** the scheduler’s log file contains entries for the scheduler service operation; entries
related to specific jobs are contained in the specific job’s log file. Access these log
files by editing the particular job.

The top list box provides summary information about all of the pending and completed jobs. The
entire dialog may be resized or any column may be resized by using the mouse to drag the right
border of any column heading.

**Note:** that some of the columns appear to be truncated. This was done on purpose to
display the most important information on each line, yet allow the option of
opening up partial columns that may contain infrequently used information.

The function of each column is described below:

- **JOBID** is the number of each job. The numbers start at 00000000 and go up to FFFFFFFF counting
in hexadecimal (0-9, then A-F before carrying to the next digit).

- **COMMENT** is an optional comment which can be given each job. This column has been
intentionally narrowed to provide enough space for other columns. The column can be resized
by dragging the right side of the column to the right.

- **ACTION** is the type of job. This will normally correspond to Get, Set, Replace etc.

- **SYS_CNT/ToDo** provides a count of the number of system in the job and the count of systems yet
to be processed.
• **STATE** shows the state of the job. Jobs can be scheduled for a run (sked), retrying (retry), completed (done) and a few other states.

• **RETRIES** shows how many times this job had to be restarted to handle a returned error. If any part of a job fails, the entire job is re-run.

• **LAST RUN** shows the date and time of the last run of the job. This is useful when tracking jobs that are retrying.

• **LAST ELAPSED** shows the amount of time it took for Lieberman RED Services Management to complete the last task.

• **RTNERR** shows the last returned error code number. Successful jobs always return zero (0) if there were not errors. Ignore certain errors by using the "Retry" dialog to edit the ignore errors list.

• **NEXT RUN** shows when the job is scheduled to next run again.

• **STATUS** shows the current return status message for the job. Get more details by double-clicking on any job to get detailed information on any system or service in the job.

### 2.5.2 Jobs Monitor Menu Items

**FILE**

- **Log** - Set up, view or print the log file of all the program's activities.

**JOB**

- **View/Edit Details** - Edit selected job(s).
- **Restart** - Restart the selected job(s).
- **Pause** - Pause the selected job(s).
- **Delete** - Delete the selected job(s).
- **Retry Policy** - Open up and edit the Retry Policy.

**SCHEDULER SERVICE**

- **Configure** - Open up and configure the scheduler service.
- **Sleep Time** - Set up the sleep time between checks for scheduled services.

**COMPONENTS**

- **View Components** - View components that are used by this program.

**HELP**
2.5.3 Editing a Job

View/edit any job by either double-clicking on the job entry, or by highlighting an entry and clicking on the Edit button on the dialog (it is located in the Job Control group outline box).

IMPORTANT DETAIL: Clicking Cancel after viewing a job will cancel any changes made to a job. Clicking OK will save changes and reset the job to run again.

Shown below is the Edit Job dialog:
Above is a typical per-job notebook. At the top of the dialog is the name of the job. There are also see three tabbed pages: Job Systems, Schedule Event, and Job Log.

*Job Systems* – Shows the list of systems managed by this job. Remove any system from the job by highlighting one or more entries and clicking on the corresponding **Delete** button located beneath the list. The list is a list of all systems that are being affected by the current job.

The number of jobs that have yet to be run are listed below each list of systems.
**Getting Started**

*Schedule Event* – Shows when the job is to be run and allows modification of the running criteria. The **How often should this job run?** list determines how often and when this job should be run. The options are: One-Shot (meaning just once), disabled, hourly, days of the week, monthly, or yearly. Delete job on completion will remove the job from the job list upon completion. The Scheduled Run Time box will allows setting the time for the job to run. The job comment text field allows provides for a job comment that appears in the Job Monitor Dialog.

*Job Log* – Displays the detailed log information regarding this job. View the file using Windows built-in Notepad application (via **View Log File** button) as well as print the file (via **Print Log File** button).
button). The file size is displayed and the file can be deleted if desired. If there is nothing in the log, the display will be blank as it is in the screen shot.

2.5.4 Job Scheduler Log File Dialog

The Job Scheduler Log File dialog is shown below. This can be accessed through the File menu in the Job Scheduler dialog. This dialog allows the user to view the log file in a text editor, print the log file, or delete the log file. It also displays the size and location of the log file.
The log file for the deferred processor service will contain messages related to the operation of the scheduling service. It will show service startup, stop, and job dispatches as well as abnormal return codes from dispatched jobs. For log information pertaining to a specific job, look into specific job log file by editing the job and browsing to the log tab.

2.5.5 Job Scheduling Check Interval

The job scheduler periodically checks all existing jobs to determine if it is now time to start their job. The period between polls is set in the **Sleep Max** field. Edit this time by clicking on the ellipses (...) button to the right of the **Sleep Max** field. The default time is 60 seconds. Between checks, the scheduler is in a sleep state and will not dispatch jobs. Only one job will be dispatched at a time.
2.5.6 Job Scheduler Service Installation

Shown below is the Scheduler Service Installation dialog:

The status display shows the current status of the scheduler service. Use the refresh button to cause the program to query for the status manually. The start and stop buttons control the startup and shutdown of the service. The path to the scheduler service may be changed from this dialog.

Before the service can run, it needs to be installed. When installing the service, the installation dialog will prompt for the account to run the service under. To later remove the service, use the Remove button.

Note: The account the service runs as will be granted the necessary rights to run as a service if it does not already have these rights. The relevant rights are Log On as a Service. Remove will not revoke any rights which are granted as a result of this operation. When installing the service, it will be installed as a regular service on the host machine under the name of this application. The service can also be configured via the Service Configuration control. To reconfigure the service through the tools dialogs, first remove the service, and then use install. At this time, reconfigure is functionally equivalent to install.
2.5.7 Retry Policy

The Retry Options dialog allows configuring options for automatic retry of failed jobs.

From this dialog, configure the default behavior when an error occurs, as well as errors to ignore during processing (by number), the maximum number of retries to attempt, and the interval between retry attempts. The default settings are shown in the dialog above.
Chapter 3  Working With Systems

This chapter describes how to handle systems in a system set such as refreshing system information, how to resolve the system names to actual machines, and how to get information about the machines in a system set.

IN THIS CHAPTER

Manage Systems Dialog ................................................................. 88
Manage Systems Context Menu ..................................................... 97
Selecting Machines ........................................................................ 98
Highlight Lists .............................................................................. 99
Refresh ......................................................................................... 99
Reboot and Abort Reboot ............................................................... 100
Send Message .............................................................................. 101
Send Wake on LAN Packet ............................................................. 101
Remove Systems from a System Set .............................................. 102
3.1 MANAGE SYSTEMS DIALOG

The Managed Systems Dialog is shown below. It is the launching point for most operation within RED COM Management.

Almost all the features of RED COM Management can be accessed through the menu at the top of this screen.

Below the menu is the systems list. This is the list of all the systems that are a part of the current system set. By default there are several columns displayed that each show relevant information about the system. Detailed explanations of what each column name means can be found in a
following subsection. The systems can be sorted by any of the columns by clicking on the corresponding column to toggle between ascending and descending order.

In the middle of the screen is the systems list which contains all the systems in the system set with each system's COM objects.

Below this list to the left is the Active Job Panel. To the center and right of the Active Job Panel is the Select buttons and a count of the current number of items in the systems list. The Active Job panel shows the job that the program is currently working on as well as the number of active threads that are working on that job. There is also a status bar that shows an approximation of progressed based on how much of the current job has been completed already.

At the bottom of the screen is the log file which records the status and progress of operations performed by Lieberman RED COM Management.

Here are what the buttons in the dialog do:

**SELECT:**
- All - Highlights/selects all entries in the list
- None – Removes highlight from all entries
- Invert - De-selects all selected items and selects all de-selected.

**ACTIVE JOB:**
- Kill Job - Tells all active threads to stop working on the current job.

### 3.1.1 Manage Systems Pull-Down Menus

**FILE**
- **Logging** - Options for logging COM+ Manager's tasks.
- **Set Group Comment** - Set the group properties.
- **Email Settings** - Set up SMTP email settings for automatic reporting.
- **Report Generator** - Use the report generator to export information about systems in the group.

**VIEW**
- **Refresh** - Refresh the system information about the selected systems and COM objects.
- **Systems Apps** - View only system applications.
- **MTS/COM+ Apps** - View only MTS/COM+ applications.
- **DCOM Apps** - View only Distributed COM applications.
• **Custom DCOM Permissions** - View only Distributed COM applications that have custom permissions.

• **Filter Options** - Hide or show certain items which generally should not be modified.

**SYSTEMS LIST**

• **Add from Domain Systems List** - Add systems from the domain.

• **Add from Browse List** - Add systems from the network.

• **Add Systems Manually** - Add systems by manually entering the system name.

• **Add from Active Directory** - Add systems using the built-in Active Directory Object Picker.

• **Resolve By** - Set the way which system names are resolved.

• **Edit Exclusion List** - Edit the Exclusion list containing systems that are not modified by COM+ Manager.

• **Delete Systems from List** - Remove the selected machines from the group.

• **Eliminate Duplicates from the List** - Remove multiple instances of the same machine from the group.

• **Export Systems list to a Text File** - Export a systems list to a text file.

• **Import Systems list from a Text File** - Import a systems list from a text file.

• **Highlight Connected Machines** - Highlight machines connected to selected machines.

• **Scan IP Range for Groups/Machines** - Use the IP Scanner to add systems.

**SET MISC**

• **Reboot** - Reboot selected machines.

• **Abort Reboot** - Abort any pending reboot commands for selected machines.

• **Send Message** - Send a text message to selected machines.

• **Send Wake on LAN Packet** - Send a Wake on LAN Packet to the selected machines.

**CONNECT AS**

• **Alternate Administrator Accounts** - Set up accounts with additional administration rights that COM+ Manager can use along with the current logon rights to administrate systems.

**JOBS**

• **Jobs Monitor** - Monitor, edit, add, stop current jobs.

• **Retry Policy** - Edit the global retry policy for jobs.
HELP

- **Contents** - Opens this help file.
- **License Keys** - Assign and release license keys as well as view license token information and statistics.
- **Logon Info** - Show the current logon information.
- **About** - Opens the about box for license, version, and product information.
3.1.2 Manage Systems Dialog Systems List Columns

The main window has one line for each machine in the current system set and one line for each application that is in the view. The columns that show information about the systems and applications are dependant on the view mode. The four view modes are:

- Systems Only
- MTS/COM+ Applications
- Distributed COM Applications
- Custom Distributed COM Permissions

The following sub-sections describe the information shown based on the chosen view.

3.1.2.1 VIEW SYSTEMS ONLY

This view will show only the systems in the group. Each system will be on a separate line. The columns in this view are:

COLUMN DEFINITIONS:

- **System Name (with status)** - This is the name of the system for addressing and display purposes. When the product attempts operations on this system, it will use this name to identify the system on the network (unless a different System Name Resolution (on page 96) is specified). The status shows the last connection or operation result (green = good, yellow = unknown/intermediate, red = failed).

- **License Status** - This column shows whether or not the system has a license token assigned to it. If a system has just been added to a group, this column will show ?.

- **Role** - This is the main role for the system. This can be WS (Workstation), SRV (Server), PDC (Primary Domain Controller), or BDC (Backup Domain Controller). The role determines the operations which are possible on that server (for example, BDCs cannot accept user/group changes).

- **Version** - The internal version of the operating system. Following are operating system version numbers:
  - 4.0 = Windows NT
  - 5.0 = Windows 2000 Pro or Windows 2000 Server
  - 5.1 = Windows XP
- 5.2  = Windows Server 2003
- 6.0 = Windows Vista or Windows Server 2008
- 6.1 = Windows 7 or Windows Server 2008 R2
- 6.2 = Windows 8 or Windows Server 2012
- 6.3 = Windows 8.1 or Windows Server 2012 R2
- 10 = Windows 10 or Server 2016

- **Resolve By** - This is the network identifier which is used to resolve the system on the network. For more information, see the [System Name Resolution](#) (on page 96).

- **NetBIOS Name** - The NetBIOS name of the machine, usually set in the system properties. NetBIOS names must be unique on local area networks, but may be duplicated on different NetBIOS networks.

- **IP Address** - The IP address of the system. This is normally found by doing a `gethostbyname` call, which uses the same mechanism Windows uses to resolve network names to IP addresses.

- **Subnet Mask** - The subnet mask for the IP address. If this is blank, the remote machine could not be accessed, or could not find the IP address in the machine's network configuration information or the remote registry service is not running on the target system.

- **DHCP** - This indicates whether the IP address was dynamically obtained (through DHCP), or was statically assigned.

- **MAC Address** - This is the hardware address of the network card to which the IP address is assigned. This value is hard coded in the card itself, but may be overridden in Windows. If this is blank, the remote machine could not be accessed or the other resolution methods failed.

- **Checked** - This is the last time User Manager Pro attempted to access the machine.

- **Status** - The last status for the last operation which was done against the machine. This value updates dynamically as operations are in progress, and will often indicate what step of an operation is currently in progress on that machine.

The columns can be resized to accommodate viewing requirements (for example, reduce the size of columns not wanted/needed to hide the information). The product will remember the last sizes for all the columns of the main window, so the next time the app is started it will have the same column sizes.
**3.1.2.2 VIEW MTS/COM+ OBJECTS**

This view will show both systems and MTS/COM+ Objects. Each COM+ application will be listed with the name of the system that it is on.

**COLUMN DEFINITIONS:**

- **System** - the name of system being queried. Both systems and service entries share this column. The initial sort order is by system, but this can be reordered by clicking on any column heading.

- **Version** – version of the COM+ application.

- **UUID** - Universally Unique Identifier. This is the identifier used to identify each different instance of an object. This is basically another way of saying a Globally Unique Identifier (GUID).

- **App Name** - Name of the application that is using the COM+ application.

- **Description** - A description of the COM+ application and its purpose.

- **Identity** - The identity that the COM+ application is running under. The COM+ application is granted all the rights of its identity.

- **System App?** - Indicates whether or not the application is running as a system application or not.

- **Enabled?** - Indicates whether or not the current COM+ application is available for use.

- **Changeable?** - Indicates whether or not the identity this COM+ application runs under can be changed.

- **Deleteable?** - Indicates whether or not the COM+ application can be deleted from the system.

- **Auth Lvl** - One of several defined security levels of communication between the caller and the COM+ application.

- **Shutdown Delay** - The amount of time to wait before shutting down the COM+ application after all the objects in its resource pool are no longer being used.

- **Run Forever?** - Indicates whether or not the COM+ application will continue to run indefinitely.

- **Security?** - Indicates whether or not this COM+ application verifies roles for each user trying to access or start the COM+ application.

- **Activation Type** - This field indicates whether the object is created in the caller's process (library) or out of process in a separate dedicated process (server).
• **Created By** - A string used to indicate who created the process. This label could be a user name, a name of a program or completely absent, it is only meant to help identify who started the application.

### 3.1.2.3 VIEW DCOM APPLICATIONS

This view shows only systems and Distributed COM applications on those systems. Each DCOM object will be listed with the name of the system that it is on.

**COLUMN DEFINITIONS:**

- **System** - the name of system being queried. Both systems and service entries share this column. The initial sort order is by system but may be reordered by clicking on any column heading.

- **Enabled?** - Indicates whether or not the current DCOM object is available for use.

- **AppID** - Unique Application ID that is used to identify each instance of the DCOM object.

- **App Name** - Name of the application that is using the DCOM object.

- **Run At** - This is either:
  - local system - which means that the DCOM object is created on the local system
  - none - the DCOM object runs as a part of the system.
  - remote system - the DCOM object runs on a different machine.

- **Run As** - The user rights that this DCOM object is allowed.

- **ProgID** - The program ID that is calling and using this DCOM object.

- **App Type** - Application Type. Either running as a server (an application is calling and using the DCOM object), or as a service (a service is using the DCOM object).

- **Module Path** - The location of the DCOM object.

- **Auth Level** - One of the built in authorization levels given to the DCOM object to perform operations.

### 3.1.2.4 VIEW CUSTOM DCOM PERMISSIONS

This view shows only systems and Distributed COM objects that have custom permissions. Each DCOM object will be listed with the name of the system that it is on.
COLUMN DEFINITIONS:

- **System** - the name of system being queried. Both systems and service entries share this column. The initial sort order is by system, which can be reordered by clicking on any column heading.

- **App Name** - Name of the application that is using the COM+ application.

- **Permission** - One of the built in permission types allowed to access and perform operations on this DCOM object.

- **Type** - Either an Allow or Deny assigned to the App Name and Permission for the user or group specified in the Principle column.

- **Principle** - The users or groups that each specific rule applies to.

- **Principle SID** - The secure identifier assigned to each Principle to uniquely identify each one.

### 3.1.3 System Name Resolution

When adding systems to a management set, you can resolve computer names using several methods. This product supports NetBIOS names, system names (fully-qualified DNS or simple), and IP addresses. There are valid reasons to use each depending on network configuration.

IP addresses can be used, but they have two problems: (1) They do not necessarily provide a meaningful identification for a machine, and (2) IP addresses can be re-assigned using DHCP. These problems could result in an administrator making changes to the wrong machine.

With a DNS name, a machine can be specified in both an easily identifiable way, and a way that is insensitive to changes to the machine's IP address via DHCP as long as DHCP and dynamic DNS are linked together.

To check if a name is resolvable, try pinging the machine by name from the command line interface. If the ping resolves to the correct machine, This product may be able to use that name to manage the machine (because it uses the same resolution mechanism as ping does).

**Note:** Being able to ping a computer is not an indication that the computer will be manageable. It only indicates that name is responsive on the network. Management of the computer is dependent on other systems, such as SSH, RPCs, and so on that are not tested with a simple ping.

When the program does a Get Role/Version (Refresh) operation, it retrieves the NetBIOS name and IP address of each managed machine. By default, the computer is resolved by whatever name is in the System column (which can be a NetBIOS name, an IP address, or a DNS name). The resolution method can be changed by right-clicking on the computer(s) and selecting a Resolve By option. This
will cause the product to use the alternate name of the computer for name resolution. In most cases, however, the computer name should be sufficient for name resolution. In addition, the other information can then be examined to make sure operations will affect the correct system(s).

### 3.1.4 View Filter Options

The view filter is active when viewing MTS/COM+ applications or DCOM applications. This filter allows limiting what is shown on the systems list.

When viewing COM+/MTS applications, choose to hide applications that are read only, system modules, running as system accounts, or running as the interactive user.

When viewing DCOM applications, choose to hide applications running as the launching user, an interactive user, or as the local system

### 3.2 MANAGE SYSTEMS CONTEXT MENU

The Manage Systems context menu (Right-Click Menu) contains a few of the most common operations to perform on systems and COM objects. The following options are available on the context menu:
• **REFRESH** - refresh information about the selected machine(s)/COM object(s).
• **SET IDENTITY** - Set the identity that a COM object runs under.
• **REBOOT** - Reboot the selected machine.
• **ABORT REBOOT** - Abort any pending reboots for the selected machine.
• **SEND MESSAGE** - Send a text message to a selected machine or domain.
• **SEND WAKE ON LAN PACKET** - Send a Wake on LAN packet to selected machine(s).
• **STOP** - Stop the current operation.
• **BROWSE SYSTEMS ADD** - Add systems using the Network Browse.
• **JOINED DOMAIN SYSTEMS ADD** - Add systems that have joined the domain.
• **MANUAL SYSTEMS ADD** - Add systems by specifying a system name.
• **ACTIVE DIRECTORY SYSTEMS ADD** - Add systems using Active Directory.
• **RESOLVE BY** - Set the system name resolution mechanism.
• **EDIT EXCLUSION LIST** - Edit the list of systems that are excluded from all operations.
• **DELETE SYSTEMS** - Delete the selected system(s) from the systems list.
• **ELIMINATE DUPLICATES FROM LIST** - Remove multiple instances of the same machine from the systems list.

### 3.3 SELECTING MACHINES

Select machines in the systems list by clicking on them. Select multiple machines by using CTRL+Click to select multiple specific systems or SHIFT+Click to select a range of systems.
3.4 HIGHLIGHT LISTS

This feature allows saving and recalling lists of highlighted systems within a set. Use multiple selection lists together to combine sets. The Highlight Lists panel is located in the Manage Systems dialog on the right side of the dialog in the section labeled Select/Highlight System Lists.

To save a list of highlighted systems, first highlight the machines that should be a part of the list and then click on New. Enter the new name for the list of selected machines and click OK. The list created will appear on the Highlight Lists panel. To select the systems in the list, simply highlight the name of the list and click Select or double-click on the name. To edit a highlight list, simply select the machines that will make up the new list and then highlight the highlight-list-name and click Save. To delete highlight lists, just select the lists and click Delete. Note that this list is additive in nature and that highlighting a list of systems using the highlight list feature does not de-select any currently selected systems.

3.5 REFRESH

The refresh command retrieves or updates the information for the selected system(s) and/or object(s). If nothing is selected, the refresh command refreshes everything listed in the systems list. The refresh command can be accessed by clicking "Refresh" from the "Systems List" menu or by clicking "Refresh" from the context menu (right-click menu) in the Manage Systems Dialog.
3.6 REBOOT AND ABORT REBOOT

This product gives the ability to remotely reboot systems. Shown below is the Reboot Systems dialog:

Set the **Time to display message before forced reboot**, as well the **Message to send to system** field. When everything is set, click on the **Apply** to start the shutdown process. Use the **Schedule** button to schedule periodic rebooting without any further actions.

The systems that are to be rebooted are listed on the right. This list corresponds to all the selected systems in the Manage Systems dialog.

The options allow forcing all applications to close in order to ensure that the reboot takes place. Systems may also be shutdown down without restarting. The **Message to send to** field will be sent to the machines as soon as the reboot is scheduled. This message will give any users on the machine a chance to finish what they are doing before the reboot.

Once a reboot command is issued, the way to stop the reboot from occurring os to right-click on the system and choose **Abort Reboot** or from the affected system, open a run menu or command prompt and type: shutdown /a
3.7 SEND MESSAGE

The product allows sending messages using the Windows Messenger service. Shown below is the Send Message to Systems dialog:

The Send Message settings are limited to those which are valid for the Windows Messenger service; see the Windows documentation for details. If options are specified which are invalid, the Send Message operation will fail with the error code received from the operating system.

If the Messenger service is stopped on the remote system, messages cannot be sent to the remote system. The Messenger Service can be started on target systems and then optionally shut it down again after the message is sent.

Note: Using the current scheduler, Domain sends cannot be scheduled.

3.8 SEND WAKE ON LAN PACKET

This sends a message to the selected machine to wake itself up from sleep mode.

Wake on LAN requires that all of the following conditions be met:
• Wake on LAN be supported by the remote system and be enabled on the remote system.
• Product has the MAC address of the remote system.
• Interim routers, switches and firewalls must support and allow the passing of UDP traffic over port 7.

3.9 REMOVE SYSTEMS FROM A SYSTEM SET

There are three ways to remove systems from a set:

1) Highlight the system(s) you wish to remove and click "Delete Systems from List" from the "Systems List" menu in the Manage Systems Dialog.
2) Highlight the system(s) to remove and Click "Delete Systems" from the context menu (right-click menu).
3) Highlight the system(s) to remove and press the "Delete" key on your keyboard.
Chapter 4  Managing COM Objects

The main purpose of Lieberman RED COM Management is to manage COM+/MTS/DCOM applications. From Lieberman RED COM Management, all COM+/MTS/DCOM applications and properties for any system in a set may be viewed. Right-click on an application and use the Set Identity feature from the context menu to manage the COM+/MTS/DCOM application identities.

Using this dialog, set or change the identity property of COM+/MTS/DCOM components for the selected systems. There are four main options for the identity property:

- **Interactive User** - This will run the selected COM+/MTS/DCOM component as the current user on the machine which is running the COM+/MTS/DCOM component. This means that if an administrator is logged in, the COM+/MTS/DCOM component will run with administrative rights. If a guest is logged in, the COM+/MTS/DCOM component will only have the rights of a
guest to the machine. If no user is logged in, then the object will not be created and an error will be returned.

- **Launching User** - This will run the selected DCOM applications with the rights of the account which called the DCOM object. This means that if an application calls the DCOM object, then the DCOM object will have the rights that the calling application would have on the remote system. If the local program runs as local system and calls a DCOM object, it is granted the same rights as an anonymous user.

- **This User** - This will run the selected COM+/MTS/DCOM components as a user that is specified in the fields below. It is possible to browse for users from a local system or from the domain. If a user is specified that is not recognized by the system then the object will not be created and the call will return an error. If a user with insufficient access rights to perform an operation that the COM+/MTS/DCOM application attempts to perform an operation, the COM+/MTS/DCOM component will fail at that time and an error code will be returned.

- **System Account** - This option is available only to services. It allows the DCOM (not MTS/COM+) components to run as a part of the local system and gain local system access.

- **Verify ability to launch DCOM component remotely after account change** - attempts to start the DCOM component to verify it was updated properly following a change.
Chapter 5  Remote Control

The remote control support allows integration with VNC and Terminal Services to provide remote control for systems.

IN THIS CHAPTER

Setting up VNCPass ................................................................. 105
Open VNC Connection ............................................................. 105
VNC Options .......................................................................... 106
Import Settings from a .RCM File ............................................ 114
Install/Remove VNC on System ............................................... 114
Start/Stop/Restart the VNC service ......................................... 114
Set VNC Password ................................................................. 114

5.1 SETTING UP VNCPASS

Before using VNC functionality, first download and install the open source VNCPass application from Lieberman Software’s website at https://www.liebsoft.com/VNCPass/. This separate application will allow getting and settings options for VNC. This application will also allow launching VNC and starting a logon session on a remote machine.

5.2 OPEN VNC CONNECTION

This option will attempt to create a VNC connection with all selected systems. By default, the application will attempt to connect to the VNC service running on the remote machine. If the service cannot be found, it will attempt to copy the service to the remote machine, install the service, and start the service. The connection will then be retried.

During this process, if required information cannot be found (such as a path to the service or any of the required files), a message box will be displayed to inform the user of the missing components. If copying VNC to a remote system, make sure to specify a logon password for the service. If the password is left blank, VNC will not allow connections using the logon password mechanism.
Open VNC Connection also does not require knowing the password for the VNC installation on the target system. The VNC connection password can be gathered as part of the connection process.

If a different version of VNC installed on the local system than the version that is running on the remote system, VNC may not be able to connect. The easiest way to get around this issue is to remove the remote version and push out the local version to remote systems when you attempt to make connections.

### 5.3 VNC OPTIONS

To configure the VNC options, go to Remote Connections | VNC | VNC Options. This dialog is used to fill in the required information for pushing VNC to a remote system and connecting to it. These options are filled in automatically, but you may need to be adjusted. The case where this dialog will be necessary is if VNC has been installed and it cannot be found. In the previous case, Lieberman RED Systems Management will prompt to locate the required files when a VNC connection is attempted.

In the dialog shown, the VNC Service Remote Push Settings section provides the location of the VNC service that will be copied to remote systems if VNC is not found. Along with the full path the service EXE file, also specify any files on which that service is dependent. These dependent files are filled in by default, but different instances of VNC which depends on different files. In all cases, default files must be located in the same directory as the service EXE file.
add files to the list that are not in the same location, a warning will appear and then those files which cannot be found will be removed from the list of dependent files.

The Local Viewer Settings is the full path to the client viewer used to connect to VNC on the remote systems.

The VNC Session Password that is required in order for clients to open sessions with the VNC service. By default, existing passwords will not be overwritten when connecting to pre-existing instances of VNC on remote systems, this password is used when copying the service to a system that does not already have it. It will still be possible to access systems for which no password has been set as long as administrative access to that system is available. Select to use a fixed password or assign a random password to each instance of the VNC service. VNCPass provides a randomization of this password for increased security so that each system will receive a different random password for its VNC service. There is no need to know this VNC password because administrative access allows the process to retrieve it on demand.

The Advanced button provides additional pages with more fields to fine tune:

- The installation parameters of the VNC service when pushing VNC out to remote systems.
- The VNC application settings that will be applied to new installs of the VNC client.
- Actions to take before and/or after the VNC session, such as installation and removal or service start and stop.
- Additional viewer command line parameters or a customer viewer application path.
- Application specific VNC parameters for optimal use of different versions of VNC.
**VNC Service** - This page allows configuring the service settings for copying to and installing the VNC service on remote systems.

The Remote Service Installation Settings all deal with copying the VNC service to the remote system if the service cannot be found. If **Install Remote Service** is unchecked, then VNC will not be installed on remote systems. The **Service Short Name** and **Service Display Name** fields are both used for installing the service on the remote system. The **Service EXE Name** field is the name of the executable file that will be copied to the remote systems and run as the VNC service. This field can be set manually or is set automatically when browsing to the file using the "Name and Path to
Service EXE" edit field.  The **Service Startup Type** options also deal with installing the service on the remote system.

Using the file list, specify any additional files the service EXE is dependent on to be copied along with the service.  Finally, the **Service Destination Location** field specifies the remote folder to which the service EXE file and any dependent files will be copied to on the remote system.  The **Viewer Application Name and Location** field refers to the path and name of the viewer application on the local system that will be used to make the connection to the service on the remote system.
**VNC Settings** - This page allows setting the VNC options for new installs of the VNC service. These options can also be used to overwrite the options for existing instances of VNC.

The top options tune which events on the remote system cause the screen to redrawn. If **Allow Socket Connections** is un-checked, the VNC service on the remote machine will not allow clients to make socket connections. Configure which port the service uses for connections. The **Connection Password Settings** section controls the client connection password to the VNC service. This password must be entered in order to start a VNC session with a remote system. VNC does not allow blank passwords.
The **Random Password** option allows creating a secure, pseudo-random, un-typeable password for each installation of the VNC service on remote systems or create random passwords that can be entered via keyboard.

**Auto-Configuration** - This page shows the options that can be taken before starting a VNC session and directly after ending a VNC session.

The options at the top allows configuration of whether or not the VNC service will be copied out to remote systems, started before a connection is made, and stopped and/or removed after a session is ended.
VNC Viewer - On this dialog, set the path to the VNC viewer application. This is the path on the local system that will be used to connect to the VNC service running on remote systems.

Using this page, supply additional command line arguments to the viewer application on launch. These command line arguments will be used every time a VNC connection is opened from within our tool.

Application Preferences - These settings customize how VNC interacts with specific applications on the remote system. These registry settings can be used to define custom behaviors for the VNC viewer client interacting with specific applications. For example, the VNC viewer normally hooks
the paint method, but for an application like the system clock, specify for the VNC viewer to refresh on the OnTimer call instead.

Some versions of VNC ship with registry files for specific application configuration. See the VNC documentation of the VNC distribution for more details about details of application preferences.
5.4 IMPORT SETTINGS FROM A .RCM FILE
This option allows importing previous settings from a .RCM file. This format is used to store VNC connection settings. Just browse to the file and VNC settings will be imported from the existing format. Check the settings using the VNC Options menu item.

5.5 INSTALL/REMOVE VNC ON SYSTEM
These options allow installing or removing the VNC service from selected systems. If installing the service, the settings specified through VNC Options will be used to configure the service. If one or more required components cannot be found, a notification as to which components are missing will be displayed. Use the VNC Options Pages to locate these components. The default settings will assume default paths for a VNC install.

5.6 START/STOP/RESTART THE VNC SERVICE
Start, stop, and restart the VNC service running on remote systems. This can be useful when changing the password or explicitly enabling or disabling VNC. Some changes to options in VNC require a restart of the VNC service to take effect (like changing passwords).

5.7 SET VNC PASSWORD
This dialog allows the password to be set for VNC services running on one or more systems at the same time.
First, select one or more target systems. Then go to **RemoteConnection | VNC | Set VNC Password**. Either supply a fixed password or choose to generate a random password for each instance of VNC. By default, the random passwords that are generated cannot be typed on a keyboard, which will prevent non-administrators from being able open a VNC session through the VNC client logon window. It is also possible to generate typeable passwords but un-typeable is the default for increased security. It will always be possible to open a VNC session on the system as long as credentials are supplied that are valid administrator credentials on that system (whether the password is typeable or not).

A service must be restarted after updating a password. Choose to restart the VNC services after the password change, as the password change will not take effect until the service is restarted. Keep in mind that restarting the service will end any active sessions.

**Note:** If supplying a blank password for VNC, VNC will not permit a connection. Depending on the version of VNC, it may use alternate methods to authenticate, but a blank password will not work. Specifying a blank password may also cause a failure when opening a VNC connection to a remote system.
Chapter 6 Help Information

This section contains information about the items listed under the Help menu.

IN THIS CHAPTER

License Token Assignment ................................................................. 117
Registration Dialog ........................................................................... 120
Logon Information Dialog ................................................................. 122
About ................................................................................................. 124

6.1 LICENSE TOKEN ASSIGNMENT

When a commercial version of the product is purchased, a serial number will be sent which will allow managing a fixed number of systems.

Use the following dialog to manually assign/release the purchased tokens to/from the systems of your choice. Alternatively, simply perform operations on systems, whereupon one or more available license tokens will be assigned automatically to each system being managed (refresh does not cause a system to be licensed). The primary use of this dialog is to release tokens from abandoned systems that are no longer part of the network so those tokens can be reassigned to new systems on the network.
To access the License Token Assignment Dialog, click the "License Keys" option from the "Help" menu in the main dialog or any system set.

License tokens are assigned to machine names. This means that if a system is decommissioned and is replaced with new hardware but give it the same name, it may use the same license; there is no reason to release and re-assign the license.

In the systems list on this dialog, the "Licensed" column displays the current licensing status of a machine as either YES or NO. The "#Rekeys" column displays the number of times a machine has had its license released and re-assigned. The "InAGroup" column displays whether or not a system is found in any systems list as either "Active" if it is in a group, or "Abandoned" if it is not in any groups.

As stated previously, if retiring a system but the replacement has same exact NetBIOS name, it is not necessary to release the license. However, if the NetBIOS will never be managed again and there is a need to reclaim licenses, select those systems here and elect to RELEASE their license.
Whenever a machine's token is released, the "Rekeyed Systems" counter will increment for that system. If the name is later re-added and the token re-assigned, the "Rekeyed Systems" field will decrement and the "#Rekeys" column for the given system will increment. If this process is repeated more times than the allowed number of "Maximum Rekeys", the system will be "Locked-Out" of management.

An easy way to find systems that you may wish to remove licenses from is to sort by the "InAGroup" column and look for systems that are abandoned. Abandoned systems are not found in any systems list.

IMPORTANT: License tokens are currently assigned for each unique system name in the System column of the main dialog. If the same system listed multiple times by different names (ie: by NetBIOS name and by IP Address), multiple tokens will be used for the same system. To ensure that this does not happen, use the following steps when adding systems using multiple naming conventions:

1) Add the systems to the group.
2) Select all the systems, then select the Refresh Info (Get Role/Version) operation (this does not cause systems to be licensed).
3) From the system list's SystemsList menu, select Eliminate Duplicates from the list.
6.2 REGISTRATION DIALOG

Shown below is the Registration dialog. This dialog can be accessed through the Help menu in the main dialog (not the Manage Systems dialog). This dialog is also shown as a part of the installation process.

The serial number entered is customized specifically to the machine that is running the software, not the machines being managed. The number of systems the license allows management of and the name of the system that is allowed to run this software is embedded in the serial number.

If the software has been running in demo mode and a commercial license is purchased, send Lieberman Software the machine name (which is located on the About dialog screen). We use this to generate the appropriate serial number.

If more systems must be managed or the tool needs to be moved to a machine with a different name, contact Lieberman Software for a new serial number.
6.2.1 Use Remote License

Multiple administrators can share a single license from multiple workstations or servers. This option does not share system set or system information (each system set and system information is maintained locally). General application data is also not shared. This essentially means that each instance of the install is a complete version which maintains its own separate program data.

If needing to transfer set information from one instance of the tool to another, use the Import/Export Systems List (on page 42) features for system lists or use Import Settings to import program settings from a Remote Licensed Server if available.

To enable the use of a shared license key, a commercial version of the software must be installed and accessible. Go to the registration screen and set the check box: Use Remote License. It is also possible to connect as an Administrator Accounts Editor (on page 64). Enter the name or browse to find the name of the machine that has the license. Enter the name of the licensed machine in the Remote Licensed Machine Name field. Finally, click on the OK button.

**Note:** On the remote system, the provided credentials must have administrative credentials, otherwise remote licensing will not work.

In order to continue using a remote license, the licensed system must always be online and accessible.

**Note:** Remote Licensing will not function without a commercial key being installed on the licensing server.
6.3 LOGON INFORMATION DIALOG

The Logon information shows the current logon credentials and program environment variables. These current logon credentials can be supplemented using the Administrator Accounts Editor (on page 64) feature to perform operations within the product. Shown below is the Logon Information dialog.

- **USER NAME** - The current user's login name.
- **SYSTEM NAME** - The name of this system.
- **ROLE** - The role of this system.
- **LOGON DOMAIN** - The name of the domain that this machine is logged into.
• **DEFAULT DOMAIN** - The name of the domain that this machine is a part of.
• **LOGON DC** - The name of the machine that is the domain controller for this machine.
• **OP SYS VERSION** - The current version of the operating system that is running on this machine.
• **ADMINISTRATOR ACCOUNT** - Whether or not the current user account an administrator account.
• **LAUNCH.EXE** - The path to the file that launched this instance of the product.
• **RIGHTS** - Any additional rights granted to the current user beyond rights inherited by groups to which the current user belongs.
6.4 ABOUT

This dialog contains version information and decoded information based on the installed serial number. Use this dialog to obtain the computer name, serial number, support information, and version information for this tool. This screen will be updated after using the Register dialog to install a new serial number.
## Chapter 7 Index

<table>
<thead>
<tr>
<th>A</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ABOUT • 124</td>
<td>ALTERNATE ADMINISTRATORS • 63</td>
</tr>
<tr>
<td>ADD FROM ACTIVE DIRECTORY • 9</td>
<td>BACKUP INTERNAL DATABASE • 43</td>
</tr>
<tr>
<td>ADD FROM ACTIVE DIRECTORY • 20</td>
<td>BACKUP SYSTEM SETS • 43</td>
</tr>
<tr>
<td>ADD FROM DOMAIN SYSTEMS LIST • 9</td>
<td>BROWSE OPTIONS • 20</td>
</tr>
<tr>
<td>ADD FROM DOMAIN SYSTEMS LIST • 13</td>
<td>BROWSE OPTIONS • 21</td>
</tr>
<tr>
<td>ADD FROM IP SCANNED RANGE • 24</td>
<td></td>
</tr>
<tr>
<td>ADD FROM NETWORK BROWSE LIST • 9</td>
<td></td>
</tr>
<tr>
<td>ADD FROM NETWORK BROWSE LIST • 15</td>
<td></td>
</tr>
<tr>
<td>ADD FROM SHELL NETWORK BROWSE LIST • 9</td>
<td></td>
</tr>
<tr>
<td>ADD FROM SHELL NETWORK BROWSE LIST • 17</td>
<td></td>
</tr>
<tr>
<td>ADD SYSTEMS MANUALLY • 9</td>
<td></td>
</tr>
<tr>
<td>ADD SYSTEMS MANUALLY • 18</td>
<td></td>
</tr>
<tr>
<td>ADDING SYSTEMS TO A SIMPLE MANAGEMENT SET • 12</td>
<td></td>
</tr>
<tr>
<td>ADMINISTRATOR ACCOUNTS EDITOR • 121, 122</td>
<td></td>
</tr>
<tr>
<td>ADMINISTRATOR ACCOUNTS EDITOR • 64</td>
<td></td>
</tr>
<tr>
<td>ADMINISTRATOR ACCOUNTS MENU - ADD • 39</td>
<td></td>
</tr>
<tr>
<td>BACKUP INTERNAL DATABASE • 43</td>
<td></td>
</tr>
<tr>
<td>BACKUP SYSTEM SETS • 43</td>
<td></td>
</tr>
<tr>
<td>BROWSE OPTIONS • 20</td>
<td></td>
</tr>
<tr>
<td>BROWSE OPTIONS • 21</td>
<td></td>
</tr>
<tr>
<td>CHANGE THE SYSTEM SET COMMENT • 49</td>
<td></td>
</tr>
<tr>
<td>CONFIGURING EMAIL SERVER SETTINGS • 53, 70</td>
<td></td>
</tr>
<tr>
<td>CONFIGURING REPORTS • 27, 37, 66</td>
<td></td>
</tr>
<tr>
<td>CONFIGURING REPORTS • 67</td>
<td></td>
</tr>
<tr>
<td>CREATE MANAGEMENT SETS • 10</td>
<td></td>
</tr>
<tr>
<td>DEFERRED PROCESSING IN LIEBERMAN REDCOM MANAGEMENT • 74</td>
<td></td>
</tr>
<tr>
<td>DELETE A SYSTEM SET • 50</td>
<td></td>
</tr>
<tr>
<td>DELETE INTERNAL DATABASE • 50</td>
<td></td>
</tr>
<tr>
<td>EDITING A JOB • 79</td>
<td></td>
</tr>
<tr>
<td>EXPORT SCANNED ENTRIES • 35</td>
<td></td>
</tr>
</tbody>
</table>
EXPORT SYSTEMS LIST TO A COMMA-DELIMITED FILE • 43

G
GETTING STARTED • 5

H
HELP INFORMATION • 117
HIGHLIGHT LISTS • 99
HOW DOES THE PROGRAM WORK? • 1
HTML EDIT DIALOG • 69
HTML EDIT DIALOG • 72

I
IMPORT FROM A COMMA-DELIMITED FILE • 49
IMPORT FROM A SCANNED IP RANGE • 49
IMPORT FROM ODBC DATASOURCE • 45
IMPORT GROUPS • 44
IMPORT SETTINGS FROM A .RCM FILE • 114
IMPORT SUBNET LIST • 33
IMPORT/EXPORT SYSTEMS LIST • 121
IMPORT/EXPORT SYSTEMS LIST • 42
INSTALL/REMOVE VNC ON SYSTEM • 114
INTRODUCTION • 1
IP SCANNER DIALOG • 24
IP SCANNER DIALOG • 27
IP SCANNER MENU - ALTERNATE ADMINISTRATORS • 39
IP SCANNER MENU - EXCLUSION LIST • 41
IP SCANNER MENU - FILE • 33
IP SCANNER MENU - OPTIONS • 37
IP SCANNER MENU - REPORT GENERATOR • 37
IP SCANNER MENU - SCAN SUBNET • 37
J
JOB SCHEDULER LOG FILE DIALOG • 77, 82
JOB SCHEDULER SERVICE INSTALLATION • 77, 84
JOB SCHEDULING CHECK INTERVAL • 83
JOBS MONITOR DIALOG • 76
JOBS MONITOR MENU ITEMS • 78
L
LICENSE AGREEMENT • 2
LICENSE TOKEN ASSIGNMENT • 117
LIMITED WARRANTY • 3
LOGGING OPTIONS • 51
LOGON INFORMATION DIALOG • 122
M
MAIN DIALOG • 6
MAIN DIALOG PULL-DOWN MENUS • 7
MANAGE SYSTEMS CONTEXT MENU • 97
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MANAGE SYSTEMS DIALOG</strong> • 88</td>
</tr>
<tr>
<td><strong>MANAGE SYSTEMS DIALOG SYSTEMS LIST COLUMNS</strong> • 92</td>
</tr>
<tr>
<td><strong>MANAGE SYSTEMS PULL-DOWN MENUS</strong> • 89</td>
</tr>
<tr>
<td><strong>MANAGED SYSTEMS LISTS</strong> • 9</td>
</tr>
<tr>
<td><strong>MANAGING COM OBJECTS</strong> • 103</td>
</tr>
<tr>
<td><strong>OPEN VNC CONNECTION</strong> • 105</td>
</tr>
<tr>
<td><strong>OVERVIEW</strong> • 1</td>
</tr>
<tr>
<td><strong>POST-GENERATION ACTION</strong> • 73</td>
</tr>
<tr>
<td><strong>PROGRAM SETTINGS &amp; OPTIONS</strong> • 51</td>
</tr>
<tr>
<td><strong>REBOOT AND ABORT REBOOT</strong> • 100</td>
</tr>
<tr>
<td><strong>REFRESH</strong> • 99</td>
</tr>
<tr>
<td><strong>REGISTRATION DIALOG</strong> • 120</td>
</tr>
<tr>
<td><strong>REMOTE CONTROL</strong> • 105</td>
</tr>
<tr>
<td><strong>REMOVE SYSTEMS FROM A SYSTEM SET</strong> • 102</td>
</tr>
<tr>
<td><strong>REPORT FILE OUTPUT TYPE</strong> • 71</td>
</tr>
<tr>
<td><strong>RESTORE FROM A BINARY FILE</strong> • 49</td>
</tr>
<tr>
<td><strong>RETRIEVING THE DATA USING THE DATABASE</strong> • 46</td>
</tr>
<tr>
<td><strong>RETRY POLICY</strong> • 85</td>
</tr>
<tr>
<td><strong>SELECTING MACHINES</strong> • 98</td>
</tr>
<tr>
<td><strong>SEND MESSAGE</strong> • 101</td>
</tr>
<tr>
<td><strong>SEND WAKE ON LAN PACKET</strong> • 101</td>
</tr>
<tr>
<td><strong>SET THE DATABASE CONNECTION STRING</strong> • 46</td>
</tr>
<tr>
<td><strong>SET THE DATABASE CONNECTION STRING</strong> • 47</td>
</tr>
<tr>
<td><strong>SET VNC PASSWORD</strong> • 114</td>
</tr>
<tr>
<td><strong>SETTING UP VNCPASS</strong> • 105</td>
</tr>
<tr>
<td><strong>SMTP SETTINGS</strong></td>
</tr>
<tr>
<td><strong>GENERAL</strong> • 54</td>
</tr>
<tr>
<td><strong>OUTGOING SERVER</strong> • 57</td>
</tr>
<tr>
<td><strong>SMTP LOGGING</strong> • 60</td>
</tr>
<tr>
<td><strong>SQL STATEMENT</strong> • 46</td>
</tr>
<tr>
<td><strong>SQL STATEMENT</strong> • 48</td>
</tr>
<tr>
<td><strong>START/STOP/RESTART THE VNC SERVICE</strong> • 114</td>
</tr>
<tr>
<td><strong>SYSTEM NAME RESOLUTION</strong> • 92, 93, 96</td>
</tr>
<tr>
<td><strong>SYSTEMS EXCLUDED FROM ALL OPERATIONS</strong> • 41</td>
</tr>
<tr>
<td><strong>THREAD MAXIMUM OVERRIDE</strong> • 37</td>
</tr>
<tr>
<td><strong>USE REMOTE LICENSE</strong> • 121</td>
</tr>
</tbody>
</table>
V
VIEW CUSTOM DCOM PERMISSIONS • 95
VIEW DCOM APPLICATIONS • 95
VIEW FILTER OPTIONS • 97
VIEW MTS/COM+ OBJECTS • 94
VIEW SYSTEMS ONLY • 92
VNC OPTIONS • 106
VULNERABILITY TESTING • 41

W
WORKING WITH SYSTEMS • 87