These are the General License Terms and Conditions (hereinafter “General Terms” or “License”) of Men & Mice, plc. (hereinafter “Men & Mice”), having its principal place of business at Hildasmari 15, IS-201 Kopavogur, Iceland. These General Terms of Men & Mice shall be applied to all agreements concluded by Men & Mice with respect to the licensing of The Men & Mice Suite. Men & Mice Suite includes Men & Mice Management Console, Men & Mice Command Line Interface (hereinafter “Men & Mice CLI”), Men & Mice Web Client (hereinafter “Men & Mice Web”), Men & Mice Central, Men & Mice DHCP Server Controller and Men & Mice DNS Server Controller software components (hereinafter “Software”).

YOUR ACCEPTANCE OF THE LICENSE TERMS AND CONDITIONS: By installing, copying, downloading, accessing or otherwise using the Software or any portion of it, you agree to be bound by these General Terms. If you do not agree with the General Terms, do not use the Software and promptly return it to the place of purchase for a full refund.

1. Ownership of the Software and reservation of rights
The enclosed Software is licensed, not sold, to you by Men & Mice for use under the following General Terms, and Men & Mice reserves all rights not expressly granted to you in these General Terms. Men & Mice retains the ownership of all copies of the Software itself.

2. Grant of License
This License grants you the following rights:

2.1. Type of license. Your license is either an Enterprise license or a Small Business License.
An Enterprise license consists of one or more of the following: DNS Module License, IP Address Module License or DHCP Module License. Each of these modules will activate the respective parts of the Software. An Enterprise License may be used on a certain network, as further specified by Men & Mice or its authorized reseller.
A Small Business License is limited to management of a certain number of active IP devices on the network or DNS zones.

2.2. Installation and use for Men & Mice DNS Server Controller. You may install and operate Men & Mice DNS Server Controller on an unlimited number of computers.

2.3. Installation and use for Men & Mice DHCP Server Controller. You may install and operate Men & Mice DHCP Server Controller on an unlimited number of computers.

2.4. Installation and use for Men & Mice Central. You may install and operate Men & Mice Central on an unlimited number of computers.

2.5. Installation and use for Men & Mice Management Console, Men & Mice CLI and Men & Mice Web. Additionally you may install and operate Men & Mice Management Console, Men & Mice CLI and Men & Mice Web on an unlimited number of computers.

2.6. Back-up copy. You may make only a reasonable number of copies of the Software solely for backup or archive purposes, which automatically become the property of Men & Mice and are subject to these General Terms. In any such copy, you must reproduce all copyright notices and other identifying or other legends that appear on the Software as received.

3. Application to updates
This License applies also to updates of the Software made by Men & Mice unless otherwise agreed.

4. Limitations on reverse engineering, decompilation and disassembly
This software contains trade secrets and to protect them you may NOT reverse engineer, decompile, disassemble, or make any attempt to reduce the Software to a human perceivable form.

5. Limitation on renting, leasing or providing services
You may not sub-license, sell, lend, rent or lease the Software or its back-up copy or any portions thereof to another user.

6. Limitations on use and integration
The Men & Mice DNS Server Controller, Men & Mice DHCP Server Controller and Men & Mice Central may only be administered by Men & Mice Management Console, Men & Mice SOAP Interface and Men & Mice CLI, Men & Mice Management Console, Men & Mice SOAP Interface and Men & Mice CLI may only be used in conjunction with the Men & Mice DNS Server Controller, Men & Mice DHCP Server Controller and Men & Mice Central.
You are not allowed to integrate the Software with your products in any manner or form resulting in your products being similar to or competing with the Software.
You are not allowed to integrate the Software with products or computer software programs of third parties in any manner or form for the purpose of avoiding fulfillment of the obligations under these General Terms.

7. Transfer of rights
You may not transfer these General Terms, any rights hereunder, the Software or any of its components to a third party. Any attempted transfer shall be null and void.

8. Intellectual property rights
All title and intellectual property rights in and to the Software and its documentation and any copies of the Software, are owned by Men & Mice or its suppliers.

9. Delivery of the Software
The Software shall be delivered in machine readable code form stored in a DVD- or CD-Rom, discs or diskettes, and Documentation in electronic or printed form. The delivery may also be carried out by the usage of the Internet. The delivery is deemed to be made when the Software and documentation enter into your possession.
10. Inspection of the Software
Men & Mice obliges you to inspect the Software with due care within twenty-one (21) days of the receipt of the first as well as any successive supplementary or corrective delivery of the Software.
Software shall be considered accepted, unless Men & Mice is otherwise notified within thirty (30) days of the receipt of the first delivery of the Software or any successive delivery referred to in the previous section.

11. Governmental approvals
Licensee shall take the proper steps at its own expense to obtain all necessary governmental approvals and validations and other official licenses, permits and certificates for the implementation of this License.
Notwithstanding the provisions of the previous section Men & Mice shall apply for its own export permission in Iceland if needed.

12. Termination
This License is effective until terminated. This License will terminate without prejudice to any other rights immediately without notice from Men & Mice or judicial resolution if you fail to comply with any provisions of this License.
From time to time licenses for the Software are granted for non-retail demonstration purposes and any such licenses shall automatically terminate 15 days after the date of the license being granted.
Upon termination you must destroy the Software, all accompanying written materials and all copies thereof, and Sections 15 (Disclaimer of Warranties) and 18 (Governing Law) will survive any termination.

13. Force Majeure
The General Terms shall be subject to Force Majeure and Men & Mice shall not be responsible for any consequences caused by circumstances beyond his reasonable control, including but without limitation to war (whether declared or not), acts of government or the European Union, export or import prohibitions, breakdown or general unavailability of transport, interruption of data communications, general shortages of energy, fire, explosions, accidents, strikes or other concerted actions of workmen, lockouts, sabotage, civil commotion and riots.
If Men & Mice suffers delay in the execution of its contractual obligations due to such circumstances, Men & Mice shall as soon as possible give you notice in writing of the cause of delay. Men & Mice shall, however, perform said contractual obligations as promptly as reasonably practicable after removal of the cause and/or its effects.

You shall not claim damage or any other compensation from Men & Mice for delays or non-fulfilment of the General Terms caused by Force Majeure.

In the event the delay or non-performance of Men & Mice continues for a period of four (4) months due to reasons of Force Majeure, then Men & Mice and you shall have the right to terminate this License with immediate effect.

14. Waiver
The waiver of any right, power or remedy under this License shall not be effective unless in writing and signed by Men & Mice or you against whom enforcement of such waiver is sought. No delay, neglect or forbearance by either in enforcing against the other any term or condition of this License shall be, or be deemed to be, a waiver nor shall it in any way prejudice any right of that party under this License.

15. Disclaimer of Warranties
THE SOFTWARE IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. MEN & MICE DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR THE RESULTS OF THE USE, OF THE SOFTWARE OR WRITTEN MATERIALS IN THE TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, CURRENTNESS OR OTHERWISE. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE SOFTWARE IS ASSUMED BY YOU. IF THE SOFTWARE OR WRITTEN MATERIALS ARE DEFECTIVE OR INCORRECT, YOU, AND NOT MEN & MICE OR ITS DEALERS, DISTRIBUTORS, AGENTS, OR EMPLOYEES, ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

However, Men & Mice warrants to you that the disk(s) on which the Software is recorded is free from defects in materials and workmanship under normal use and service for a period of thirty (30) days from the date of delivery as evidenced by a copy of the receipt.

THIS IS THE ONLY WARRANT OF ANY KIND, EITHER EXPRESS OR IMPLIED, THAT IS MADE BY MEN & MICE ON THIS SOFTWARE PRODUCT. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY MEN & MICE, IT'S DEALERS, DISTRIBUTORS, AGENTS, OR EMPLOYEES SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY, AND YOU MAY NOT RELY ON SUCH INFORMATION OR ADVICE. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

16. Limitation of Liability
IN NO EVENT SHALL MEN & MICE BE LIABLE FOR ANY PUNITIVE OR EXEMPLARY DAMAGES OR COSTS RESULTING FROM PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES OR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT OR SPECIAL DAMAGES WHATSOEVER (INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF USE, PROFITS, REVENUE, BUSINESS, INFORMATION OR OTHER PECUNIARY LOSS) ARISING FROM, OR IN ANY WAY RELATED TO THIS LICENSE, OR THE MANUFACTURE, SALE, SERVICE, USE OF OR INABILITY TO USE THE PRODUCTS, EVEN IF MEN & MICE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS EXCLUSION SHALL APPLY REGARDLESS OF WHETHER SUCH DAMAGES OR COSTS ARE Sought BASED ON BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY IN TORT, OR ANY OTHER LEGAL OR EQUITABLE THEORY.

THE LIABILITY OF MEN & MICE, IF ANY, FOR DAMAGE RELATING TO ANY MEN & MICE PRODUCT SHALL BE LIMITED TO THE ACTUAL AMOUNT PAID BY YOU FOR THE MEN & MICE PRODUCT.
17. Indemnification

By accepting these terms you agree to indemnify and hold harmless Men & Mice and its officers, directors, employees, and agents from and against any and all claims, demands, costs and liabilities (including all attorneys’ fees) of any kind whatsoever, arising directly or indirectly out of any action or omission by you, including, without limitation, your performance or failure to perform under this License, your breach of this License or your obligations as set forth herein.

18. Governing law

This License will be interpreted and construed in accordance with the laws of Iceland without regard to conflicts of law principles.

Any controversy or claim arising out of or relating to this License shall be primarily settled amicably. If this is not possible, the controversy or claim shall be finally settled by arbitration in accordance with the Rules of the Commercial Arbitration Court of the Iceland Chamber of Commerce. The place of arbitration shall be Reykjavik, Iceland. The language to be used in the proceedings shall be English. The award shall be final and binding on the parties.

If any provision of this License shall be held to be contrary to law or otherwise unenforceable, that provision will be enforced to the maximum extent possible, and the remaining provisions of this License will remain in full force and effect.

If you are a U.S. Government user then the Software is provided with “RESTRICTED RIGHTS” as set forth in subparagraph (c)(1) and (2) of the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19 or subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, as applicable. Manufacturer: Men & Mice Hlidasmari 15, 201 Kopavogur, ICELAND.

© 1996-2012 Men & Mice.
## Contents

### Chapter 1: Introduction ....................................................................................... 1
- What is the Men & Mice Suite? ........................................................................... 1
- Installation/System Requirements ...................................................................... 1

### Chapter 2: Management Console ........................................................................ 3
- Overview .............................................................................................................. 3
- Launching the Men & Mice Suite ....................................................................... 3
- First Use Wizard .................................................................................................. 4
- GUI Interface ....................................................................................................... 4
  - Object Browser .................................................................................................. 5
  - Detail View ......................................................................................................... 5
  - Sorting Records ................................................................................................. 6
- Menu Bars ........................................................................................................... 6
  - File Menu .......................................................................................................... 6
  - Edit Menu .......................................................................................................... 6
  - Query Menu ..................................................................................................... 8
  - Window Menu .................................................................................................. 8
  - Help Menu ....................................................................................................... 8
- Toolbars .............................................................................................................. 9
  - Zone Toolbar ................................................................................................... 9
  - IP Address Range Toolbar ............................................................................... 10
  - Scope Toolbar .................................................................................................. 10
- Quick Filter ......................................................................................................... 11
  - Using Keywords ................................................................................................. 11
  - Using Wildcards and Regular Expressions in Filters ....................................... 11
  - Clearing an Entry .............................................................................................. 12
  - Saving a Filter ................................................................................................. 12
  - Deleting a Filter ............................................................................................... 12
- Program Preferences .......................................................................................... 13
  - Log Window ...................................................................................................... 13
  - New Zone Window ............................................................................................ 13
  - Console ............................................................................................................. 13
- Search/Update Wizard ........................................................................................ 14
- Lease History ...................................................................................................... 14
  - Exporting Search Results ................................................................................ 15
- Object Change History ........................................................................................ 15
  - Accessing via the Menu Bar ........................................................................... 16
  - Accessing via the Object Browser ................................................................. 17
  - Exporting Search Results ................................................................................ 18
- Men & Mice Suite Log ......................................................................................... 18
- Object Folders ..................................................................................................... 19
  - Creating a New Folder ..................................................................................... 19
  - Creating a Subfolder ......................................................................................... 19
  - Renaming a Folder ............................................................................................ 20
  - Specifying Access for Folder Items ............................................................... 20
  - Deleting a Folder .............................................................................................. 20

### Chapter 3: Administration Functions ................................................................... 21
- Overview .............................................................................................................. 21
- System Settings .................................................................................................. 21
  - General ............................................................................................................. 22
  - Logging .............................................................................................................. 23
  - Error Checking ................................................................................................. 24
Chapter 7: IP Address Management ................................................................. 91

Overview ............................................................................................................. 91
Address (A) Records in DNS Zone Windows ....................................................... 91
Range Access ........................................................................................................ 91
Viewing IP Address Ranges .................................................................................. 91
New Ranges .......................................................................................................... 92
Range Configuration .............................................................................................. 93
Range Modifications ............................................................................................. 94
Range Deletions ..................................................................................................... 94
IP Address List ...................................................................................................... 94
Device Dialog Box ................................................................................................. 95
  Adding a DNS Host ............................................................................................. 96
  Editing a DNS Host ............................................................................................ 97
  Removing a DNS Host ......................................................................................... 97
  Adding a Related Host ......................................................................................... 97
  Editing a Related Host ......................................................................................... 97
  Removing a Related Host ..................................................................................... 97
Moving a Device .................................................................................................... 98
Split Range Wizard ............................................................................................... 98
Generate Reverse Zones Wizard ........................................................................... 98
Allocate Ranges Wizard ......................................................................................... 99

Disabling a Zone(s) .............................................................................................. 69
Enabling a Zone(s) ............................................................................................... 70
Duplicate ............................................................................................................... 70
Edit Preferred Servers .......................................................................................... 70
Export ..................................................................................................................... 70
Folders ................................................................................................................... 71
Forward Zone ........................................................................................................ 71
Import ..................................................................................................................... 71
Master Zone .......................................................................................................... 72
DNSSEC Zones ..................................................................................................... 74
DNSSEC Management on Windows Server 2012 ................................................... 74
  Signing Zones using DNSSEC ............................................................................ 74
  UnSigning Zones using DNSSEC ....................................................................... 75
Options .................................................................................................................. 75
Zone Options (Windows and BIND) ...................................................................... 75
BIND Servers ........................................................................................................ 77
Options For ............................................................................................................ 78
Promote Slave to Master ...................................................................................... 79
Properties .............................................................................................................. 79
Reload ...................................................................................................................... 79
Remove from Folder .............................................................................................. 80
Search .................................................................................................................... 80
Slave Zone .............................................................................................................. 81
Slave Server Assignments ..................................................................................... 81
Stub Zone ............................................................................................................... 81
View History ......................................................................................................... 82
Zone Wizard .......................................................................................................... 82

Chapter 6: DNS Resource Records ................................................................. 83

Overview .............................................................................................................. 83
Types of Resource Records .................................................................................. 83
Resource Records ................................................................................................. 87
New Records ......................................................................................................... 87
Create Record Wizard .......................................................................................... 87
Deleting Records ................................................................................................... 88
Clearing Records ................................................................................................. 89
Disable/Enable Records in the Zone Window ....................................................... 89
  How to Disable a Record ..................................................................................... 89
  How to Re-Enable a Record ............................................................................... 89
Cut, Copy, and Paste ............................................................................................. 90
Undo/Redo Commands ......................................................................................... 90
Join Ranges ................................................................. 99
Select Parent............................................................... 100
Host Discovery ............................................................ 100
  Configuring Host Discovery by Querying Routers .......... 101
  Configuring Host Discovery Using Ping ...................... 100
Remove from Folder .................................................... 101
Subnet Monitoring ...................................................... 102
  Set Subnet Monitoring .............................................. 102
  Removing Subnet Monitoring ..................................... 102
Multiple Address Spaces ........................................... 103
Address Space Management ....................................... 103
  Switching to a Different Address Space ...................... 104
  Moving Objects to a Different Address Space ............... 104

Chapter 8: AD Sites and Subnets ................................. 105
Overview .................................................................... 105
Adding an AD Forest .................................................. 105
Changing AD Forest Properties .................................... 106
Removing an AD Forest .............................................. 106
Reloading the Sites in an AD Forest ............................ 106
Managing Subnets in a Site ......................................... 106

Chapter 9: DHCP Servers ............................................ 109
Overview .................................................................... 109
New DHCP Server .................................................... 109
  Server Access on Remote Computers .......................... 110
Edit DHCP Server Name ............................................ 111
Access ........................................................................ 111
Delete ......................................................................... 111
Managing Groups/Hosts ............................................. 112
  Groups/Hosts Toolbar ............................................. 112
  Groups/Hosts Shortcut Menu .................................... 113
Editing Subclasses ..................................................... 114
Options ...................................................................... 115
Defining DHCP Server Options .................................... 116
  Defining Options on MS DHCP Servers ...................... 116
  Defining Options on ISC DHCP Servers .................... 117
Properties .................................................................... 117
  MS Server Properties ............................................. 118
  ISC Server Properties ............................................ 119
  Cisco Server Properties ......................................... 120
Reconcile Scopes ....................................................... 120
Reload Scope List ....................................................... 121
Restart ........................................................................ 121
Set User Name and Password ...................................... 121

Chapter 10: DHCP Scopes ............................................ 123
Overview .................................................................... 123
Viewing Scopes ........................................................ 123
  All DHCP Scopes on All Servers ................................ 123
  Scopes on a Specific DHCP Server ............................. 123
  Selected Scope Menus ............................................. 124
New DHCP Scope ....................................................... 130
  MS DHCP Server ................................................... 131
  ISC DHCP Server .................................................. 133
  Cisco DHCP Server ............................................... 134
Access ........................................................................ 135
Delete ........................................................................ 135
Disable/Enable .......................................................... 135
Scope Migration Wizard ............................................ 136
Duplication Wizard ..................................................... 136
Folders ....................................................................... 136
Reconcile Scope ........................................................ 136
Appendix D: Application Architecture ........................................................... 175
Appendix B: Dynamic Zones .......................................................................... 167
Chapter 11: Web Interface ............................................................................... 157
Overview ........................................................................................................ 157
Appendix A: Command Line Interface (CLI) .................................................. 159
Overview ........................................................................................................ 159
Command List .................................................................................................. 159
Command Descriptions .................................................................................... 161
Example Script ................................................................................................. 161
Appendix B: Dynamic Zones .......................................................................... 167
Overview ........................................................................................................ 167
Static vs. Dynamic Zones ................................................................................ 167
BIND Server Configuration ............................................................................. 167
Windows DNS Server Configuration ............................................................... 168
Appendix C: External Authentication ................................................................. 169
Overview ........................................................................................................ 169
Active Directory User Authentication ............................................................... 169
Active Directory User Authentication vs. Local User Authentication ............. 169
Enabling AD User Authentication Using Active Directory ............................. 169
Configuring Users for AD Authentication ....................................................... 169
Active Directory Single Sign-on ...................................................................... 170
Web Interface .................................................................................................. 170
Application Log In ........................................................................................... 171
Group Level Active Directory User Authentication ........................................ 171
Configuring Groups for AD Group Level Authentication ................................ 171
Configuring Users and Access Privileges ....................................................... 172
RADIUS User Authentication ........................................................................ 172
RADIUS User Authentication vs. Local User Authentication ....................... 172
Enabling RADIUS User Authentication ......................................................... 172
Configuring Users ......................................................................................... 173
Logging into the Men & Mice Suite ................................................................. 173
Appendix D: Application Architecture ............................................................. 175
Overview ........................................................................................................ 175
Management Console ...................................................................................... 175
CLI .................................................................................................................. 175
Web Interface .................................................................................................. 175
DNS Server Controller .................................................................................... 175
DHCP Server Controller .................................................................................. 175
Men & Mice Central .......................................................................................... 175
Men & Mice Suite – High-level Architectural Diagram .................................. 176
User Interfaces ................................................................................................ 176
Appendix E: Central/DNS Server Controller ................................................. 177
  Overview ........................................................................................................ 177
  Men & Mice Central ...................................................................................... 177
    Windows .................................................................................................. 177
    UNIX ..................................................................................................... 177
    Mac OS X .............................................................................................. 178
  DNS Server Controller .................................................................................. 179
    Windows .................................................................................................. 179
    UNIX ..................................................................................................... 179
    Mac OS X .............................................................................................. 180

Appendix F: BIND DNS File Structure ........................................................ 181
  Overview ........................................................................................................ 181
  named.conf ............................................................................................... 181
  Zone Options Files ...................................................................................... 181
  Zone Files .................................................................................................. 181
  Configuration Files Diagram ........................................................................ 182

Appendix G: External Scripts ........................................................................ 183
  Overview ........................................................................................................ 183
  Script Interfaces .......................................................................................... 184
    Property Change Script Interface ............................................................. 184
    Zone Content Change Script Interface .................................................... 186
    Subnet Monitoring Script Interface ........................................................ 187
  Example Script .......................................................................................... 188

Appendix H: Secure64 Integration ................................................................. 191
  Overview ........................................................................................................ 191
  Enabling Support for the Secure64 DNS Signer ......................................... 191
  Creating DNSSEC Signed Zones ............................................................... 192
  Viewing DNSSEC Records ......................................................................... 193

Appendix I: Replacing the Database Engine ................................................ 195
  Overview ........................................................................................................ 195

Appendix J: Backing Up and Restoring the SQLite Database ........................ 197
  Overview ........................................................................................................ 197
  Backing up the Database ............................................................................. 197
  Restoring the Database ................................................................................. 197
    Windows .................................................................................................. 197
    Linux and Solaris ..................................................................................... 198
    Mac OS X .............................................................................................. 198
Chapter 1: Introduction

What is the Men & Mice Suite?

The Men & Mice Suite is an integrated DNS, DHCP, and IP Address Management environment. Using the Men & Mice Suite, you can maintain an overview of your network address space and manage a changing environment with minimum effort. The Men & Mice Suite provides many tools to minimize your effort, including direct views of server data, logical views of diverse data, and a number of wizards.

Installation/System Requirements

The Men & Mice Suite consists of several base components, some of which are available for multiple platforms. As such, the installation instructions and system requirements for some components may vary depending on the platform and the components being installed. Please refer to the online installation instructions for the information that pertains to your environment.
Chapter 2: Management Console

Overview

Prior to starting the Men & Mice Management Console, make sure that you have installed and started the other Men & Mice Suite modules, as required. Refer to the Installation Guide for other components.

The Men & Mice Management Console boasts a very intuitive interface. It is the central organizational tool of the Men & Mice Suite and provides all the tools you need to oversee the management of your DNS and DHCP servers.

NOTE: Be aware that you will only be able to view the servers to which you have access. The administrator user has access to all servers.

Launching the Men & Mice Suite

When logging into the Men & Mice Management Console, you have the option to choose “Single Sign-on.” This allows those users working on a Microsoft Network with Active Directory to sign on one time only to access all your resources.

NOTE: If you are the system administrator, you can choose whether to enable this option. In the Management Console, move to the menu bar and select Tools, System Settings. In the System settings dialog box, click the General tab. Check in the checkbox next to Allow Single Sign-on to enable this option. Then click OK.

To start the Management Console, do the following:

1. Locate and launch the Men & Mice Management Console. The Men & Mice Management Console login dialog box displays.

2. In the Server name field, type the name or IP address (IPv4 or IPv6) of the workstation on which Men & Mice Central is running. This is only required the first time you log in. After a successful connection, this field will be pre-filled with the server name you enter.
3. In the User and Password fields, type the applicable information. The default value for both fields is administrator.

4. If you want to enable Single Sign-on, click in the checkbox.

5. Click the Connect button. If this is the first time any user logs into this particular Men & Mice Central, the First Use Wizard launches. Refer to the section titled, "First Use Wizard." Otherwise, within a few moments, the Men & Mice Management Console will start, and the Manager window will display.

### First Use Wizard

1. Locate and launch the Men & Mice Management Console. If this is the first time you have logged into the Men & Mice Central, the First use wizard launches and the Introduction screen displays.

2. Click Next >.

3. Complete each screen as you move through the wizard.

### GUI Interface

The Men & Mice Management Console is the GUI client of a client/server application that allows you to administer local DNS/DHCP servers and IP Addresses. Specifically, it provides a simple graphical user interface that allows you to manage your domain names and IP addresses.

From the Management Console, you can simultaneously manage DHCP/DNS servers on different platforms. When the Management Console is started up, the Manager Window displays in the center. This window is the heart of the Men & Mice Management Console, providing a single interface with nearly every feature in the Men & Mice Suite.

This window consists of two main areas: the Object Browser and the Detail View.
Object Browser

The Object Browser displays on the left side of the Manager window and contains categories of objects that can be created, modified, and deleted.

- **DNS Zones.** Selecting the DNS Zones object will cause the Detail View to display all DNS zones configured in the system and accessible to the current user. This category is accessible with a valid DNS Module License Key.

- **DNS Servers.** Selecting the DNS Servers category will cause the Detail View to display all DNS servers managed by the system and accessible to the current user. If a DNS server is not reachable, its icon is shown with an exclamation mark. If the DNS Servers category is expanded, the same list of servers will show as sub-categories to the DNS Servers category. Selecting a server subcategory will cause the Detail View to display the zones managed by that server and accessible to the current user. This category is accessible with a valid DNS Module License Key.

- **DNS Views.** The DNS Views category allows you to see zones on DNS servers that are configured with multiple views. If no views are configured on any server, this category will not appear. The Views feature of the BIND name server allows one server to return different data to different clients; each view has its own separate list of zones, often with the same names. This category behaves similarly to the DNS Servers category.

- **IP Address Ranges.** Selecting the IP Address Ranges category will cause the Detail View to display all IP Address Ranges configured in the system and accessible to the current user. This category is accessible with a valid IP Address Management Module License Key.

- **DHCP Scopes.** Selecting the DHCP Scopes category will cause the Detail View to display all DHCP scopes configured in the system and accessible to the current user. This category is accessible with a valid DHCP Module License Key.

- **DHCP Servers.** Selecting the DHCP Servers category causes the Detail View to display all DHCP servers managed by the system and accessible to the current user. If a DHCP server is not reachable, its icon is shown with an exclamation mark. If the DHCP Servers category is expanded, the same list of servers will show as sub-categories to the DHCP Servers category. Selecting a server subcategory causes the Detail View to display the scopes managed by that server and accessible to the current user. This category is accessible with a valid DHCP Module License Key.

- **AD Sites.** This category is only displayed if you have enabled AD Sites and Subnets integration. Selecting this category will show all AD sites that have been selected for integration in the Men & Mice Suite.

Detail View

The Detail View displays on the right side of the Manager window and displays the contents of the selected category in the Object Browser. While in this view, you can do the following:

- Sort and filter to allow a more concise view of the contents. *Refer to Quick Filter.*

- Display a shortcut or “context” menu that gives access to other options. Right-click to view this shortcut menu.

- Open an object by simply double-clicking. This opens either a property window (such as in the case of DNS/DHCP Servers), or brings you to a new view of the data contained within the object (such as in the case of DNS Zones, DHCP Zones, and IP Address Ranges).

- Reorder the columns. Click on the column you want to move and, while holding down the mouse key, drag the column to the new position.

- Display or hide columns. Right-click on a column header. All the column names shown with a checkmark are currently displayed. To hide a column, click on the name to remove the checkmark. To display a hidden column, repeat the process. *Reset all* makes all columns display without having to unhide them individually.
**Sorting Records**

When viewing information in the Object List -- be it DNS zones, Servers, Views, IP Address Ranges, or Scopes -- you can instantly sort the displayed information by clicking on the header of any column shown in that view. For instance, click on the Name header once to sort the displayed objects alphabetically (A-Z) by name. Clicking on the Name header again will resort the list in reverse alphabetic order (Z-A). This can be done with any column of data, including Servers, Addresses, Utilization percentages, etc.

When sorting zone names alphabetically, reverse zones will appear at the bottom of the list (after Z), or at the top of the list when sorted in reverse alphabetic order.

---

**Menu Bars**

The Menu Bar in the Men & Mice Management Console provides access to nearly all of the program’s functionality.

**NOTES**

- You must have sufficient access privileges in order to use some of the menu items discussed below.
- Not every menu option is listed below. Some are detailed in their respective sections. Some of the options discussed below are global across the whole application (e.g., Cut, Copy, and Paste).

**File Menu**

- **Save.** Saves any changes that have been made in the currently active window. This is only available when a zone has been edited and there is some new data to be saved.
- **Change Password.** Use this command to change your login password to the Management Console. Your current password is required in order to change to a new one.
- **Page Setup.** Opens the Print Setup dialog box, from which you can choose the default printer, paper, page orientation, and other properties to be used when printing from Management Console.
- **Print.** Opens the Print dialog box and allows you to print the contents of the currently selected Zone window. This command is only available when a Zone window is open.
- **Exit.** Closes the Management Console window.

**Edit Menu**

The commands available from the Edit menu vary, depending on what is currently selected in the Management Console. When working in the Manager window the following functions are offered:

- **Undo.** Reverses the last edits that you made, in the reverse-order that you made them.
- **Redo.** Reverses the effects of the last Undo command.
- **Cut.** Removes the currently selected item(s) and stores them in the Windows clipboard.
- **Copy.** Makes a copy of the currently selected item(s) and places it into the Windows clipboard.
- **Paste.** Copies the contents of the clipboard at the location of the insertion point.
- **Paste Custom Properties.** Allows pasting of custom property contents into multiple objects. To use this command, select one object and choose **Copy.** Then select the objects whose custom properties you want to populate and choose **Paste Properties.** This will open a dialog box where you can choose which custom properties you want to paste.
- **Clear.** Deletes the currently selected text or record.
- **Select All.** This command selects all of the objects (e.g. zones, servers, scopes, IP address ranges).
- **Find.** This command initiates a new search.
• **Find Next.** This command repeats the last search you performed. For example, if the last search was for A, this automatically locates the next occurrence of A in the object list.

• **Save Filter/Delete Filter.** It is possible to save/delete filters for various object types. Saved filters appear in the list on the left hand side of the Manager Window and in the Create Zone dialog box. Filters can be local or global in scope. Filters created by the Administrator are global and visible to all users. Filters created by any other user are visible only to that user.

• **Preferences.** Opens the Options dialog box where you can make default selections for various Management Console functions.

When working with a zone, the Edit menu changes and includes additional functions.

• **Enable Record.** Makes the currently selected record(s) active in the zone. Use this command to re-enable a zone that has been disabled. All records are active by default unless they have been manually disabled. You cannot enable records in dynamic zones.

• **Disable Record.** Makes the currently selected record inactive. When a record is disabled, it is ignored in the zone. You cannot disable records in dynamic zones.

• **Insert Record.** Opens a popup menu that lets you specify the type of record you want to create. To insert A, CNAME, MX, NS, or PTR records, choose the corresponding option from the menu. The new record is created directly below the currently selected record or field. For other types of records, select Insert Record. This creates a new blank row above the currently selected record or field.

• **Duplicate Record.** Creates a copy of the selected record(s). The new records appear directly underneath the last record being duplicated.

• **Delete Record.** Deletes the entire record from the zone. Unlike the Clear command, the entire record does not need to be selected for this command to work. It will delete the entire record in which the cursor is currently located.

• **Show TTL.** This menu command can be toggled on and off by selecting it repeatedly. This option is enabled by default. If you disable this option, the TTL column will not be displayed in the zone window. This command is only available when a Zone window is open and active.

• **Show Comment.** This menu command can be toggled on and off by selecting it repeatedly. This option is enabled by default. If you disable this option, the Comment column will not be displayed in the zone windows. This command is only available when a Zone window is open and active. This command can only be used for static zones.
Query Menu

- **Lease History.** This function can be enabled through *System Settings, Logging*. When enabled you can search the DHCP lease history and if desired, export the search results to a file.

- **Object History.** Allows you to query the history throughout the system for all objects or a specific object. Refer to *Object Change History for details*. You can search all objects or, using the *Only show objects of type* drop-down list, you can select which object type to search. You can only search all object types or one selected object type.

- **Men & Mice Suite Log.** Displays log messages for the Men & Mice Suite.

- **Search and Update Wizard.** Launches the Search and Update Wizard, a utility that allows you to find, create, modify, or delete records in multiple zones and DHCP Scopes using a single action. Click Next and follow the instructions onscreen to specify the type of records you want to search, the action you want to perform (e.g., create, replace, delete, edit), etc.

- **User Activity.** Users with user administrative privileges can see this menu item. Selecting this menu item displays a window that shows a list of all users including the user name, authentication type, login status, and last login time.

Window Menu

- **Cascade.** Aligns all currently open windows inside the Console window so that they overlap, showing only their title bars. This allows you to access all currently open windows.

- **Show Progress.** This window shows the progress of operation that can take some time, such as opening and saving large zones. When an operation is in progress (and displayed in the progress window) it can be canceled by clicking in the progress window and choosing *Cancel*.

- **Show Console.** Displays errors that may occur during various operations.

- **Show Manager Window.** Displays the Manager Window. Use this function in the event you inadvertently close the Manager window.

- **Revert to Standard Layout.** Returns the program to its standard view, with the Management Console open and the main window displayed on top of any other open windows. Other windows are not affected by this command. Also, shows the progress window if the window is hidden.

- **Active Window List.** At the bottom of the *Window* menu, there will be a list of every window currently open in the Management Console. You can instantly give a window the focus (i.e., bring it to the top) by selecting it from this list.

Help Menu

- **Help.** Launches the online help features of the Men & Mice Suite.

- **About Men and Mice Management Console.** Opens the About window, which contains the full version number of the Men & Mice Management Console that you are running.
Toolbars

The toolbar, which runs along the top of the Object Section and Object List, provides fast access to commonly performed operations. The function of any given button is always in the context of the currently selected object. Some buttons will not be available (i.e., grayed out) when certain objects are selected.

<table>
<thead>
<tr>
<th>BUTTON</th>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>Create</td>
<td>Lets you create a zone, add a name server, a DHCP scope, or a DHCP server based on the currently selected object.</td>
</tr>
<tr>
<td>-</td>
<td>Delete</td>
<td>Lets you delete a zone, a name server, a DHCP scope, or a DHCP server; based on the currently selected object.</td>
</tr>
<tr>
<td>⚙️</td>
<td>Options</td>
<td>Display the options dialog box for the currently selected object, if applicable (e.g., Zone options, Server options, etc.).</td>
</tr>
<tr>
<td>🌐</td>
<td>Server Info</td>
<td>Displays a window that provides general information about the selected server—e.g., server type, IP address, OS, number of zones, number of requests sent/received, etc. Refer to DNS Servers—Viewing Servers, Server Information.</td>
</tr>
<tr>
<td>📜</td>
<td>Server Log</td>
<td>Displays the Server Log window that shows the DNS log of that server. Refer to DNS Servers—Viewing Servers, Server Activity Log.</td>
</tr>
<tr>
<td>⏰</td>
<td>History</td>
<td>Opens the History window and displays a log of all changes that have been made to the selected object, including the date and time of the change, the name of the user who made it, the actions performed, and any comments entered by the user. Refer to Management Console—Object Change History.</td>
</tr>
<tr>
<td>🔍</td>
<td>Zone Wizard</td>
<td>Launches the Zone Wizard, which helps you create the desired type of zone by prompting you with a series of questions. Refer to DNS Zones—Zone Wizard.</td>
</tr>
<tr>
<td>🔍</td>
<td>Views</td>
<td>When selected, toggles between hierarchical and flat view for the IP address range.</td>
</tr>
<tr>
<td>N/A</td>
<td>Quick Filter</td>
<td>This text field lets you instantly filter out objects that you do not want to display. For example, if you type &quot;ex&quot; in the field, only objects that contain &quot;ex&quot; somewhere in their name are displayed in the Object List. When you clear the contents from this field, all available objects are again displayed. Refer to Quick Filter.</td>
</tr>
</tbody>
</table>

Zone Toolbar

<table>
<thead>
<tr>
<th>BUTTON</th>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>📜</td>
<td>Save</td>
<td>Saves the information as entered in the main zone information window.</td>
</tr>
<tr>
<td>🌐</td>
<td>Print</td>
<td>Prints the zone information.</td>
</tr>
<tr>
<td>🔍</td>
<td>Find</td>
<td>Opens the Find Zone dialog box in which you enter criterion to locate specific information for this zone. Refer to DNS Zones—Search in Zone Window.</td>
</tr>
<tr>
<td>⚙️</td>
<td>Options</td>
<td>Opens the Zone Options dialog box. Refer to the DNS Zones—Zone Options.</td>
</tr>
<tr>
<td>⏰</td>
<td>History</td>
<td>Displays the history for the selected zone. Refer to the DNS Zones—Viewing History.</td>
</tr>
<tr>
<td>🔍</td>
<td>Wizard</td>
<td>Launches the Record Creation Wizard. Refer to DNS Resource Records.</td>
</tr>
<tr>
<td>📜</td>
<td>Analyze</td>
<td>Analyzes the contents of the zone. Refer to Zone Analysis.</td>
</tr>
</tbody>
</table>
**IP Address Range Toolbar**

<table>
<thead>
<tr>
<th>BUTTON</th>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Delete</td>
<td>Removes the currently selected host. <em>Refer to IP Address Management.</em></td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td>Opens the Device dialog box in which you can edit device details. <em>Refer to IP Address Management.</em></td>
</tr>
<tr>
<td></td>
<td>Claim</td>
<td>Use this feature to prevent accidental assignment of a reserved address without creating a DNS entry for it. The workflow is as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- A user with &quot;edit data&quot; privileges can select one or more addresses that have no associated A record(s) and choose &quot;Claim&quot; from the menu. Going forward, no one can create A records for the address(es) through the zone window (neither auto-assign nor manually assign).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- A user can select one or more claimed addresses and select &quot;Release.&quot; These addresses are then restored to their previous state.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- A user can edit a Claimed record through the IPAM module. When the user opens a Device Details window for a claimed address, a dialog prompts, &quot;This address has been claimed. Are you sure you want to edit it?&quot; Yes/No? When <strong>Save</strong> is selected in the device details window, one of two things happens:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(1) If the user only entered non-DNS data (custom properties, MAC address, device name), the &quot;claimed&quot; flag stays in place.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(2) If the user entered one or more DNS hosts for the device, the &quot;claimed&quot; flag is cleared.</td>
</tr>
<tr>
<td></td>
<td>Release</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Next Free Address in Range</td>
<td>Finds the first IP address in the range that is not in use. When clicked, opens the Device dialog box in which you enter the IP address info.</td>
</tr>
</tbody>
</table>

**Scope Toolbar**

<table>
<thead>
<tr>
<th>BUTTON</th>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Edit</td>
<td>Allow you to edit the selected host by opening the Device dialog box. <em>Refer to DHCP Scopes</em></td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>Deletes the currently selected device. <em>Refer to DHCP Scopes</em></td>
</tr>
<tr>
<td></td>
<td>Claim</td>
<td>Use this feature to prevent accidental assignment of a reserved address without creating a DNS entry for it. The workflow is as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- A user with &quot;edit data&quot; privileges can select one or more addresses that have no associated A record(s) and choose &quot;Claim&quot; from the menu. Going forward, no one can create A records for the address(es) through the zone window (neither auto-assign nor manually assign).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- A user can select one or more claimed addresses and select &quot;Release.&quot; These addresses are then restored to their previous state.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- A user can edit a Claimed record through the IPAM module. When the user opens a Device Details window for a claimed address, a dialog prompts, &quot;This address has been claimed. Are you sure you want to edit it?&quot; Yes/No?. When <strong>Save</strong> is selected in the device details window, one of two things happens:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(1) If the user only entered non-DNS data (custom properties, MAC address, device name), the &quot;claimed&quot; flag stays in place.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(2) If the user entered one or more DNS hosts for the device, the &quot;claimed&quot; flag is cleared.</td>
</tr>
</tbody>
</table>
Quick Filter

Quick Filters provide a simple way to filter out data records you do not want to see. They can be found in most windows that contain a number of objects.

A Quick Filter works in real time and searches all items in a list by default. It is also possible to narrow the search by using keywords to specify in which field to search.

Using Keywords

- **Column Headers.** It is possible to use column headers as keywords in the Quick Filter and to specify in which field to search. For example, if you enter the following filtering criterion when filtering zones - name:myzone - the filter only searches in the Name field and displays only those results that contain the text myzone.

  When a column header's name contains a space, such as "Lease MAC Address", you can enclose the name in quotes – e.g., “Lease MAC Address”:11. See Colons, below.

- **Colons.** Colons are used to separate a column name from a filter. If the filter contains colons, you can either enclose the filter in quotes or escape the colons with a backslash (\). For example, both "Lease MAC Address":"11:22" and "Lease MAC Address":11\:22 search for a MAC address containing "11:22" in a column with a name containing with the name "Lease MAC Address".

- **Simultaneous Keywords.** You can use several keywords simultaneously simply by leaving a space between each consecutive filtering criterion. An ‘AND’ condition is used when finding records. For example: name:myzone type:slave.

- **Custom Properties.** When custom properties are used, you can use the name of the custom property as a keyword.

Using Wildcards and Regular Expressions in Filters

When using the Quick Filters, it is possible to use the wildcard characters ‘^’ and ‘$’ to narrow the search results.

- **The caret symbol** ^ means starts with. For example, the search string ^server finds server1.zone.com and server-north.anotherzone.com, but not myserver.myzone.com.

- The **dollar symbol** $ means ends with. For example, the search string `server$` finds the.best.server and good.nameserver, but not slow.servers.

- **The ‘!’ operator.** You can use the ‘!’ operator to further narrow the search results. The **exclamation mark** ! means NOT. For example, the search string !^a finds entries that don’t start with ‘a’. The exclamation mark can be used with the other wildcards to find non-empty fields. Entering ‘Description: !^$’ finds all entries where the Description field is not empty.

- **The ‘&’ and ‘|’ operators.** The ampersand is interpreted as an AND operator while the vertical bar is used as an OR operator. Using these operators, you can combine searches for added control. You can use parenthesis in conjunction with these operators. Examples:
  - A | B Finds entries with the text A or the text B
  - A & B Find entries containing both A and B
  - A & (B | C) Finds entries containing A and either B or C
  - (A & B) | C Finds entries containing both A and B or entries containing C

- **For even more control, you can use regular expressions in filters.** **NOTE:** The character ‘:’ must be escaped if it is to be used as a wildcard character. Otherwise, it will be interpreted literally. The same applies to following characters: ( ) { }.
**Clearing an Entry**

At any time, you can clear the text you have in the *Quick Filter* field by click the “X” shown at the end of the field.

![Manager Window](image)

**Saving a Filter**

It is possible to save filters for various object types. Saved filters appear in the list on the left hand side of the Manager Window and in the Create Zone dialog box. Filters can be local or global in scope. Filters created by the Administrator are global and visible to all users. Filters created by any other user are visible only to that user.

To save a filter, do the following:

1. Type the entry you want to filter by in the *Quick Filter* field.
2. Move to the menu bar, and select *Edit, Save Filter*.
3. In the open dialog box, type the desired name for the filter. Then click *OK*.
4. The saved filter shows at the bottom of the Object list.

**Deleting a Filter**

To delete a filter, do the following:

1. Locate the filter name in the Object list.
2. Highlight the filter name and select *Edit, Delete Filter*.
Program Preferences

You can set some default behaviors for the Men & Mice Management Console using the Options dialog box.

- On the menu bar, select Edit, Preferences. The Options dialog box displays.

![Options dialog box]

Log Window

- Initial log size. The server logs are kept by the servers. When the Management Console connects to a server and the log window is opened, the Manager downloads the most recent portions of the server’s log. The amount downloaded (in kilobytes) will be equal to the value set in the Initial log size field.

- Max log size. The maximum log size determines how much of a server’s log can be retained by the Management Console at any one time. Once the maximum size is reached, the Manager will discard old log entries as necessary to make room for the new ones. Log entries discarded by the Manager Console are retained on the log that the server maintains. The Max log size field can be set to any value between 1 and 1024 KBs. The default value is 100 KB.

- Log interval. Whenever the log window is open, it will continually update itself (the log) from the server. The interval between sequential updates can be set to any value between one and thirty seconds. The default value is every five seconds.

New Zone Window

- Show TTL. This checkbox is enabled by default. If you clear this checkbox, the TTL column will not be included in any new zones that you create.

- Show comment. This checkbox is enabled by default. If you clear this checkbox, the Comment column will not be included in any new zones that you create.

Console

You can configure how the Console Window behaves when new entries are added to the window.

- Do nothing. If this option is selected, entries are added ‘silently’ to the console window. If the window is hidden, it is not displayed when new entries are added.

- Display Console if hidden. If this option is selected, the console window will be displayed when new entries are added.

- Bring Console to front. If this option is selected, the console window will be displayed as the front-most window when new entries are added.
Search/Update Wizard

This utility allows you to find, create, modify, or delete records in multiple zones and DHCP Scopes using a single action.

There are three search options available:

- **DNS Resource Records.** Refer to DNS Resource Records for further information.
- **DHCP Scope Options.** Through this function, you replace, delete or search for option values.
- **Devices.** Through this function, you can find a device in any IP address range and display the results in the IP address range window.

To launch the Search and Update Wizard, do the following:

1. From the menu bar, select **Query, Search and Update Wizard.** The Search and Update Wizard dialog box displays.
2. Select the type of search you want to perform.
3. Complete each screen as you move through the wizard.

Lease History

Through this function, you view the lease history for your MS and ISC DHCP servers.

**NOTES**

- You must be a member of the DHCP Administrator group to view the DHCP lease history.
- Lease history collection must be enabled for this function to work. See Logging for information on how to enable lease history collection.

To view the DHCP lease history:

1. From the menu bar, select **Query, Lease History.** The Lease History Query dialog box displays.
2. **Find DHCP leases where.** Select if you want to query by IP Address, MAC Address, Server Address, Hostname or Description.

3. **Starting on/Ending on.** To query based upon a date range, type the starting and ending range dates. For example, to find all changes made in 2007, in the Starting on field type 1/1/2007 and in the Ending on field, type 12/31/07. For example, to find all changes made in 2007, in the Starting on field type 1/1/2007 and in the Ending on field, type 12/31/07.

4. Click **Search.** Any matching results are displayed in the lower portion of the window.

**Exporting Search Results**

To export the results as a CSV file, do the following:

1. Display the lease history.
2. Search for the desired history.
3. When the applicable change history is shown, click the **Export** button. The Export records to CSV file dialog box displays.
4. Select the drive, directory, subdirectory, etc. into which you want to save the CSV file.
5. Click **Save.**

**Object Change History**

Through this function, you can display a log of all changes that have been made to any object such as the date and time of the change, the name of the user who made it, the actions performed, and any comments entered by the user.

There are two ways to search/view the object change history:

- **From the Menu Bar.** With this option, you select the type of object to search change history for.
- **Through the Object Browser.** With this option, you select the object first, and then search for the change history.
Chapter 2: Management Console Men and Mice Suite v6.3.5

Accessing via the Menu Bar

1. From the menu bar, select **Query, Object History**. The History Query dialog box displays.

2. **Where text contains**. Type any words that the text contains.

3. **Made by**. Type the user login name.

4. **Starting on/Ending on**. To query based upon a date range, type the starting and ending range dates. For example, to find all changes made in 2007, in the **Starting on** field type 1/1/2007 and in the **Ending on** field, type 12/31/07. For example, to find all changes made in 2007, in the **Starting on** field type 1/1/2007 and in the **Ending on** field, type 12/31/07.

5. **Only show objects of type**. Click the drop-down list arrow, and select the type of object for which you want to find change history.

6. **Limit to ____ Results**. Enter the maximum number of results to display.

7. Click **Search**. Any matching results are displayed in the lower portion of the window.
Accessing via the Object Browser

1. In the Object Browser, open the desired object category (e.g., DNS Zones, DNS Servers, etc.).
2. Locate the object for which you want to view the history.
3. Right-click and, from the shortcut menu, select View History.

The History window displays showing all the history for the selected object.

4. If you wish to query the results, click the plus sign (+) in the upper left corner of the dialog box.
5. Following the directions under Accessing via the Menu Bar to enter the query information.
**Exporting Search Results**

To export the results as a CSV file, do the following:

1. Display the object change history.
2. Display the Query Change History search criteria fields.
3. Search for the desired change history.
4. When the applicable change history is shown, click the **Export** button. The Export records to CSV file dialog box displays.
5. Select the drive, directory, subdirectory, etc. into which you want to save the CSV file.
6. Click **Save**.

---

**Men & Mice Suite Log**

Through this function, you can display log messages generated by the Men & Mice Suite. **NOTE:** You must be a member of an Administrator group to view the log messages.

To view the log messages, do the following:

1. In the main Men & Mice window, move to the menu bar and select **Query, Men & Mice Suite Log**. The Men & Mice Suite Log window displays.
2. **Search For.** Type the information to query.

3. **Starting on/Ending on.** To query based upon a date range, type the starting and ending range dates. For example, to find all changes made in 2007, in the **Starting on** field type 1/1/2007 and in the **Ending on** field, type 12/31/07.

4. **Log level.** Click the drop-down list, and select the desired level – e.g., **Error, Notice** or **Warning**.

5. When all selections/entries are made, click **Search.** Any matching results are displayed in the lower portion of the window.

6. **Quick Filter.** Allows you to further refine the search results. As you type in the field, results that are not applicable are removed.

7. To export the results as a CSV file, do the following:
   - Click the **Export** button. The Export records to CSV file dialog box displays.
   - Select the drive, directory, subdirectory, etc. into which you want to save the CSV file.
   - Click **Save**.

---

### Object Folders

To help in organizing your IP address ranges, DNS Zones, and DHCP scopes, you can create folders and subfolders into which you can place one or more objects. You can also rename and delete folders, as well as specify access to ranges within the folder (once objects have been moved into it).

#### Creating a New Folder

*NOTE:* When you create a new folder, you can move objects from the “master” list into this new folder. However, the objects always remain in the master list as well.

To create a folder, do the following:

1. In the Object List, right-click on either IP address ranges, DNS Zones, or DHCP scopes.

2. From the shortcut menu, select **New folder.** The Create Folder dialog box displays.

   ![Create Folder Dialog](image)

3. Type a name for the folder.

4. Click **OK.** The new folder now displays in the Object List.

5. To move an object into this new folder, simply highlight it and drag and drop it into this folder.

#### Creating a Subfolder

If desired, you can add a subfolder underneath any existing folder. *NOTE: If you move an object from another folder into a subfolder, the object no longer appears in the original folder. This is not the case, however, when you move an object from the master list. The object always remains in the master list, regardless of what folder/subfolder a copy is moved to.*

1. In the Object List, click the plus (+) sign next to the object type where you want to create the subfolder. The object expands to show any currently defined folders.

2. Right-click on the folder to which you want to add a subfolder.
3. From the shortcut menu, select **New Folder**.
4. In the Create Folder dialog box, type a name for the new subfolder.
5. Click **OK**. You can now move objects into this subfolder by dragging/dropping them from the list on the right.

**Renaming a Folder**

You can rename any folder by doing the following:

1. Select the folder you want to rename.
2. Right-click and, from the shortcut menu, select **Rename**.
3. In the Rename folder dialog box, type the new name for the folder.
4. Click **OK**. The object list refreshes and the new folder name displays.

**Specifying Access for Folder Items**

Once you have created a folder and moved objects into the folder, you can assign permissions to the ranges in the folder to control who can work with those objects.

Choosing access for a folder does not set the access for the folder, but merely selects all objects in the folder and applies the access settings to these objects.

To specify access for item/items in a folder, do the following:

1. Right-click on the folder and, from the shortcut menu, select **Access**.
2. In the Access Control dialog box, select the group/user (or add a new group/user). Then, specify the permissions for the user.
3. Click **OK**.
4. If desired, enter a Save Comment when prompted.

**Deleting a Folder**

When deleting a folder, the objects within the folder are not deleted and remain intact.

To delete a folder/subfolder, do the following:

1. Right-click on the folder and, from the shortcut menu, select **Delete**.
2. When the confirmation message displays, click **Yes**.
Chapter 3: Administration Functions

Overview

This section describes the Administration features in the Men and Mice Management Console. These features include the ability to create and manage user accounts, define user groups, and controlling user/group access. (Group features are accessed through Tools, Users and Groups.)

System Settings

- From the menu bar, select **Tools, System Settings**.

![System Settings Dialog Box](image)

The System Settings dialog box displays and includes these tabs:

- General
- Logging
- Error Checking
Chapter 3: Administration Functions

- Site and Subnets
- Save Comments
- External Commands
- DNS
- Monitoring

**General**

Through this function, you can specify the following:

- Whether to allow single sign-on.
- How the system should handle new subranges if the parent range is in a folder.
- How the system should behave if DHCP scopes are removed outside the Men & Mice Suite.
- How the system should behave when naming conflicts between existing IP address ranges and DHCP scopes occur.
- Whether the system should allow reservations inside address pools on ISC DHCP servers.
- Whether automatic updates of DNS and DHCP server controllers should be enabled.
- Advanced system settings.

To display the General Settings dialog box, do the following:

1. From the menu bar, select **Tools, System Settings**.
2. In the System settings dialog box, click the **General** tab.

![System Settings Dialog Box](image-url)
3. **Allow Single Sign-on.** When selected, Active Directory users do not have to authenticate when logging in through the Management Console or the Command Line Interface.

4. **Allow single sign-on through web interface on IIS.** To enable single sign-on in the web interface, the web server needs to be configured. Refer to Appendix C – Active Directory Single Sign-on.

5. **Subranges.** The selection made here determines what happens when a user creates a subrange of a range in a folder. Click the desired action.

6. **DHCP Scope Deletion.** If a scope is removed directly from a DHCP server (instead of using the Men & Mice Suite), you can select whether to convert it to an IP address range or remove it completely.

7. **Name conflicts between ranges and scopes.** The selection made here determines what happens if the name of an MS DHCP scope does not match the name of an existing IP address range.

8. **Apply same rule for scope description as for scope name above.** When selected, the system will use the same rules to update scope description as it does for updating scope names.

9. **Allow reservations inside pools on ISC DHCP servers.** When selected, the system allows users to create reservations inside pools on ISC DHCP servers. When a reservation is created inside a pool, the pool is split to make space for the reservation. **NOTE:** If a reservation that has been created inside a pool is deleted, the address is not made a part of the pool again.

10. **Show DHCP data in subranges of scopes.** When selected, the system will display contents of subranges of scopes in the same view that is used for scopes and users with the required privileges will be able to work with reservations in these subranges. If the checkbox is not selected, contents of subranges of scopes will be displayed in the regular range view.

11. **Enable automatic updates of DNS and DHCP Server Controllers.** When this checkbox is checked, the system automatically updates the DNS and DHCP server controllers.

   **How the Automatic Update Feature Works**
   When a new version of Men & Mice Central is installed, the installer places the latest version of all controllers and the Management Console in an ‘update’ directory. When automatic updates are turned on, the system uses the files in this directory to update the relevant installed server controllers and the Management Console to the latest version. If automatic updates are turned off the system will not attempt to update the controllers or the Management Console.

   To make automatic updates possible on DNS and DHCP servers, an updater needs to be installed on the relevant server. The updater is installed as a part of the server controller installation. **NOTE:** Installing the updater is optional. The system will work without the updater, but the server controller on the relevant server must then be updated manually.

12. **Advanced system settings.** Click this button to display the dialog box for entering advanced system settings. For more information about the contents of this dialog box, see the Men & Mice Knowledge Base at http://kbase.menandmice.com/.

13. When the desired selections/entries are made, click **OK**.

**Logging**
Through this function, you specify when log messages should be purged and whether lease history for DHCP servers should be collected.

1. From the menu, select **Tools, System Settings.**
2. In the System Settings dialog box, click the **Logging** tab.

![Logging tab](image)

3. **Purge log message after** ____ days. When selected a number is typed in the field indicating the number of days the logs should be kept.

4. **Lease History.** Through this function, you configure the setting that allows for viewing the history of DHCP leases.
   - **Collect lease history for DHCP servers.** Click the checkbox to begin history collection for DHCP servers.
   - **Purge lease history after** ____ days. Click the checkbox to select this option. Then, in the field, type the number of days to retain the history.
   - **Flush lease history to file before purging.** To save the lease history to a comma separated text file before it is purged, click the checkbox, and then type the name of the file.

5. When all selections/entries are made, click **OK**.

---

**Error Checking**

The Error Checking tab allows you to specify how the system reports certain errors related to DHCP and DNS. This tab is also used to enable or disable DHCP scope monitoring.

1. From the menu bar, select **Tools, System Settings**.
2. In the System Settings dialog box, click the **Error Checking** tab.

![Error Checking tab](image)

3. **Ignore missing reverse zones.** An error message displays when the Men & Mice Suite is unable to update a reverse record for a changed address record. It is possible to suppress this error message if no reverse zone exists for the given address record by selecting the Ignore missing reverse zones checkbox.
4. **Warn when creating A/AAAA records with name that already exists.** When enabled, a warning message displays if a user creates an address (A or AAAA) record using the name of an existing record of the same type.

5. **Inconsistencies in DHCP lease names and DNS names.** When enabled, an icon displays for each DHCP lease for which the DNS name does not match the lease name. The user can click on the icon and display a dialog box showing details about the error and (if applicable) how to fix it.

6. **Address pool collisions.** When enabled, an icon displays in split scope entries if the address pool in the scope collides with the address pool of another split scope instance. The user can click on the icon and display a dialog box showing details about the error and (if applicable) how to fix it.

7. **Inconsistencies between reservation names in split scopes.** When enabled, an icon displays in split scope entries if a reservation name in a split scope differs from the reservation name in another split scope instance. The user can click on the icon and display a dialog box showing details about the error and (if applicable) how to fix it.

8. **Inconsistencies between reservation descriptions in split scopes.** When enabled, an icon displays in split scope entries if a reservation description in a split scope differs from the reservation description in another split scope instance. The user can click on the icon and display a dialog box showing details about the error and (if applicable) how to fix it.

9. When all selections/entries are made, click **OK**.

### Sites and Subnets

Use the Sites and Subnets tab to enable integration of sites and subnets in Active Directory. When the integration is active, all sites and their corresponding subnets in Active Directory displays in the Men & Mice Suite, and you can add and remove subnets in sites and move subnets to different sites.

1. From the menu bar, select **Tools, System Settings**.

2. In the System Settings dialog box, click the AD **Sites and Subnets** tab. The Sites and Subnets dialog box displays.

3. **Enable AD sites and subnets integration.** Check this checkbox to enable the integration feature.

4. If you want to synchronize the **Location** and **Description** fields of the subnets in Active Directory against custom properties in the Men & Mice Suite, choose the custom properties to synchronize against. When synchronization is active, any changes made to the fields in Active Directory will update the corresponding fields in the Men & Mice Suite and vice versa.

5. **Enforce AD site inheritance.** Select this checkbox if you want to enforce site inheritance in AD. When site inheritance is enforced, child subnets must reside in the same site as the parent subnet. If site inheritance is not enforced, child subnets can be placed in different sites than the parent subnet.

6. When all selections/entries are made, click **OK**.
Once Sites and Subnets integration has been enabled, an AD Sites object displays in the object list on the left hand side of the Manager window and a new column, AD Site displays in the range list in the Manager window. See also AD Sites and Subnets.

**Save Comments**

When saving changes to various objects, the Save Comment window may display. When this window displays is determined by the selections you make on this tab.

The user simply types comments into the dialog box, explaining a reason for any actions taken (e.g., delete object as it was a duplicate). Then the user clicks OK.

To define when comments can be entered (and this can only be when logged on as a System Administrator), do the following:

1. From the menu bar, select Tools, System Settings.
2. In the System settings dialog box, click the Save Comments tab.
3. Click in the checkbox next to all the instances in which you want the Save Comment dialog box to display.
4. When all selections are made, click OK.

**External Commands**

Refer to the Appendix G: External Scripts.
**DNS**

Use the DNS settings dialog box to specify various DNS related settings. To display the DNS Settings dialog box, do the following:

1. From the menu bar, select **Tools, System Settings**.
2. In the System Settings dialog box, click the **DNS** tab.

3. **Delegation records.** When *automatically create delegation records when creating new zones* is selected, delegation records (NS records) are automatically created in the corresponding parent zones when subzones are created, maintaining a correct delegation chain between parent and subzones.

4. **Secure 64.** Refer to Appendix H: Secure64 Integration.

5. **Adjust Zone Transfer.** Select the checkbox to allow the Men & Mice Suite to automatically adjust zone transfer settings on Microsoft DNS servers to enable management of dynamic and Active Directory integrated zones.

6. When the desired selections/entries are made, click **OK**.

**Monitoring**

Use the Monitoring settings dialog box to specify various monitoring related settings. To display the Monitoring Settings dialog box, do the following:

1. From the menu bar, select **Tools, System Settings**.
2. In the System Settings dialog box, click the **Monitoring** tab.

3. **Ping before automatic assignment.** When selected, when an IP address is being auto-assigned, the system checks as to whether the IP address is responding to a ping request before it is allocated to a new host. If the IP address responds to the ping request, it is not used for auto-assignment.

4. **Automatic assignment ping timeout _____ ms.** Specifies how long the system should wait (in milliseconds) for a response to the ping request. If a response is not received within the specified time, the system considers this to be a non-responding IP address.

5. **Enable subnet monitoring.** When enabled, the system monitors the free addresses in DHCP address pools and subnets, and performs an action if the number of free addresses goes below a user-definable threshold. When subnet monitoring has been enabled, it is possible to configure the global settings for this feature by clicking the **Details** button. **NOTE:** The global subnet monitoring setting can be overridden for individual subnets by changing the setting explicitly for the subnet. See the section **Subnet Monitoring** in chapter 7 for information on how to change monitoring settings for individual subnets.

To change the subnet monitoring settings, do the following:
- Click the **Details** button. A dialog box displays:
- **Enabled.** When checked, all subnets are monitored by default. If you only want to monitor a subset of the subnets in the system, leave this checkbox unchecked and enable monitoring for the individual subnets instead by selecting the subnet and then selecting Set Subnet Monitoring from the Range menu.

- **Script to invoke.** Enter the path of the script to run when the number of free addresses goes below the set threshold. See Appendix G, External Scripts, for information on the script interface and the format for calling the script.

- **Dynamic Threshold.** Enter the threshold for the free addresses in a DHCP scope address pool. **NOTE:** For split scopes and scopes in a superscope (on MS DHCP servers) and address pools using the shared-network feature on ISC DHCP servers, the total number of free addresses in all of the scope instances is used when calculating the number of free addresses.

- **Static Threshold.** Enter the threshold for the free addresses in a subnet.

- **Only perform action once (until fixed).** When checked, the action is performed only once when the number of free addresses goes below the threshold.

- **Perform action when fixed.** When checked, the action is performed when the number of free addresses is no longer below the threshold.

When subnet monitoring is enabled, a new column, Monitoring, displays when viewing the subnet list. To quickly see all subnets that are monitored, you can use the Quick Filter and filter by this column by entering “Monitor:Yes” in the Quick Filter search field. **NOTE:** Only DHCP scopes that are enabled are monitored. Disabled scopes are ignored.

When subnet monitoring is enabled, you must specify the mail server and the sender e-mail address to use if you want the subnet monitor to send an e-mail. Place the appropriate information in the SMTP Server and Mail from fields.

6. **Enable sending SNMP traps.** When enabled, the system will send SNMP traps when certain events occur:
   - When the number of free IP addresses in monitored subnets goes below a user-definable threshold.
   - When a log event of type Error occurs. See Men & Mice Suite Log in Chapter 2 for more information on log events.

7. When enabling sending of SNMP traps, you must provide additional information:
   - **Manager name.** Enter the host name of the computer that should receive the SNMP traps.
   - **Manager port.** Enter the port number the Manager uses for the SNMP traps.
   - **Community.** Enter the community string (password) to use for the SNMP traps.

8. **Enable collection of IP information from routers.** When enabled, the system will query hosts that have been specified as routers for IP information. This feature is used along with the host discovery Ping feature to find active IP addresses on the network. See Host Discovery in Chapter 7 for more information on how to specify hosts as routers.

When this feature is enabled, some additional information must be provided:
   - **SNMP query interval.** Determines how frequently the routers are queried for IP information.
   - **Router SNMP community.** Enter the SNMP community string (password) to use when querying the routers for IP information.
User Management

User Management involves both creating groups as well as creating users to associate with groups.

- From the menu bar, select **Tools, Users and Groups**. The User and Group management dialog box displays.

### User Management

**Users**

Each user defined in the Men & Mice Suite can be a part of one or more groups. Before creating a user, it is recommended to define different groups so you can assign users directly to the desired group as you create their accounts. **NOTE:** “Administrator” is the user already configured for the application. In order to manage users, you have to be logged in as a user who has user management privileges.

#### Adding User Accounts

Through this function, you add new users who can then be assigned to groups.

1. From the menu bar, select **Tools, Users and Groups**. The User and group management dialog box displays. The default administrator account displays here, as well as any other users you have already added.

2. On the Users tab, click the **Add** button. The New user properties dialog box displays.

3. **User Name.** Type the name that you want to assign to this person. **NOTE:** Once you have created the user name, it is not possible to change it.

4. **Full Name** and **Description**. (Optional) Type the user’s first and last name and a description of their duties (i.e., job title, department, etc.), respectively.

5. **Authentication.** Click the drop-down list and specify whether the user’s login will be authenticated by the Men and Mice software or by an external authentication service (such as existing Active Directory account on the network).

6. **Password/Confirm Password.** If the Authentication method selected is Men & Mice Internal, you need to provide a password for the user in the Password field. Passwords must be at least four characters in length and no longer than 20 characters. Passwords can contain any combination of letters and numbers, but cannot include spaces or special characters.

7. In the **Confirm Password** field, re-enter the password exactly as you did in the Password field above.

8. In the **Groups** area, select the user group(s) to which you want to assign this user. Each user can be assigned to none or to multiple groups. There are five default groups defined in Men & Mice Suite:
- **Administrators.** Full access to everything.
- **DNS Administrators.** Full access to all DNS related objects, such as zones, DNS servers, etc.
- **DHCP Administrators.** Full access to DHCP related objects, including DHCP scopes, DHCP servers, etc.
- **IPAM Administrators.** Full access to IPAM related objects, including IPAM ranges, etc.
- **Users Administrators.** Full access to User and Group objects.

**NOTE:** If you have not created your groups, you can always come back and edit the user accounts anytime and change the group assignments.

When all selections/entries are made, click **OK.** The new user is added to the Users list.

### Editing User Accounts

1. From the menu bar, select **Tools, Users and Groups.** The User and group management dialog box displays.
2. To select a single user, click on the user’s name. To select multiple users, press/hold the **Ctrl** key and then click on each user name.
3. Click the **Edit** button. The User properties dialog box displays.
4. Make the desired changes to the user’s information.
5. Click **OK** to save the changes.

### Removing User Accounts

1. From the menu bar, select **Tools, Users and Groups.** The User and group management dialog box displays.
2. To remove a single user, click on the user’s name. To remove multiple users, press/hold the **Ctrl** key and then click on each user name.
3. Click the **Remove** button. A dialog box prompts you to confirm your decision.
4. To remove the user, click the **Yes** button. The user is removed.

### Viewing User Activity

Selecting this menu item displays a window that shows a list of all users including the user name, authentication type, login status, and last login time. Only users with user administrative privileges can see this menu item.

- From the menu bar, select **Query, User Activity.** The User Activity dialog box displays.

- Use the **Quick Filter**, if desired, to refine the list.
Groups

Through this function, you create and manage groups. Groups allow you to manage multiple individual users who have the same access and/or permissions across the system.

Adding a New Group

1. From the menu bar, select Tools, Users and Groups. The User and group management dialog box displays.
2. Click the Groups tab. The default groups are displayed here, as well as any other groups you have already created.
3. From the Groups tab, click the Add button. The New group properties dialog box displays.
4. In the Group name field, enter a name for the group you are creating.
5. (Optional) In the Description field, provide some information that describes the function of this group.
6. Active Directory Integrated. Check this box to define this group as an Active Directory Integrated group. When checked this group name will be matched against groups defined in Active Directory. For more information on this works refer to the Appendix C: External Authentication.

7. When all selections/entries are made, click OK. The new group now displays in the User and Group Management dialog box.

Editing a Group

Through this function, you can edit the group name and/or description, and indicate whether this group is Active Directory integrated.

1. From the menu bar, select Tools, Users and Groups. The User and group management dialog box displays.
2. Click the Groups tab.
3. Highlight the group to which you want to make changes.
4. Click the Edit button. The Users properties dialog box displays.
5. Make the desired changes.
6. When all selections/entries are made, click OK.
Deleting a Group

Through this function, you delete a group.

1. From the menu bar, select **Tools, Users and Groups**. The User and group management dialog box displays.
2. Click the **Groups** tab.
3. Highlight the group you want to delete.
4. Click the **Remove** button.
5. When the confirmation message displays, click **Yes**.

License Management

There are three different keys, one each for the DNS Module, the IPAM Module, and the DHCP Module.

The License Management dialog box shows detailed information about every key entered. It also contains information about license utilization by showing the number of DNS zones and IP addresses in use.

**Adding a License Key**

1. From the menu bar, select **Tools, License Management**. The License Management dialog box displays. All currently entered license keys are displayed.

   ![License Management Dialog Box]

   The Men & Mice Suite is currently managing 0 master DNS zones containing address (A) records for 0 unique IP addresses. Note that each IP address is only counted once. There are 0 IP ranges defined.

2. To add a key, click the **Add Key** button. The Add License Key dialog box displays.

   ![Add License Key Dialog Box]

3. In the **License Key** field, type the license key. Then click **OK**.

**Removing a License Key**

1. From the menu bar, select **Tools, License Management**. The License Management dialog box displays. All currently entered license keys are displayed.
2. Highlight the key you want to remove.
3. Click the **Remove Key** button.
Define Custom Properties

As an administrator, you may find that it is necessary to create some custom properties. These properties are used for entry of any data that you feel is relevant for an object. For example, if you want to specify a server is in a specific location, or indicate who is responsible for a particular server, etc. Custom properties can be defined for various object types.

In addition, various properties can be set when working with custom properties.

**Adding a Custom Property**

1. From the menu bar, select **Tools, Define Custom Properties**. The Define Custom Properties dialog box displays.

2. Select the object type to which you want to add a custom property.

3. Click the **Add** button. The Custom Property dialog box displays.

4. **Name**. Type a name for this custom property.

5. **Type**. Set the type for the property. By default, “Text” is selected. Click the drop-down list and select the desired property type - e.g., Text, Yes/No, IP Address, or Number.

6. **Mandatory**. When selected, a user must enter a value in this field. *If you select this option, you cannot select “Read only.”*

7. **Read only**. When selected, the field is locked for editing. *If you select this option, you cannot select “Mandatory.”*

8. **Multiline**. When selected, the edit field contains multiple lines for entry. *If you select this option, you cannot select “List.”*
9. **Predefined Values.** *NOTE: If you select this option, you cannot select “Multiline.”* When selected, the field displays as a drop-down list. Click the checkbox for **List.** Then click the **Edit List** button. The Custom Property List Items dialog box through which you can add, edit, and remove custom properties displays.

   - To **ADD** an item for this property, click **Add.** The Custom Property List Items dialog box displays.

   ![Custom Property List Items dialog box](image)

   - Type the item in the field provided.
   - Add any additional items. You can move items **Up** and/or **Down** in the list, as desired. This designates the order in which they appear in the list.
   - Then click **OK.** When you return to the Custom Property List Items dialog box, the items entered are shown.

   ![Custom Property dialog box](image)

   - To edit/remove any values, click **Edit List** and make the necessary changes.
   - When all selections are made, click **OK.**

10. **Default value.** Specifies the default field value to use when an object is created. This field is only a drop-down list if the ‘List’ checkbox is selected; otherwise, it is an edit field.

11. When all selections/entries are made, click **OK.** When you return to the Define Custom Properties dialog box, the new field is shown.

12. If there are multiple custom properties for an object, use the **Move Up/Move Down** arrows to change the order in which this display in the object window.

13. When all fields are added, click the **Save** button.
**Editing a Custom Property**

To edit a custom property, do the following:

1. From the menu, select **Tools, Define Custom Properties**.
2. Locate and highlight the property to be edited.
3. Click the **Edit** button.
4. Make the necessary changes.
5. Click **OK**.

**Deleting a Custom Property**

To delete a custom property, do the following:

1. From the menu, select **Tools, Define Custom Properties**.
2. Locate and highlight the property to be deleted.
3. Click the **Delete** button.
4. When the confirmation message displays, click **Yes**.
5. Click **OK**.

**Displaying a Custom Property**

Once a custom property has been defined, it is possible to view and edit its contents by opening the Properties dialog for any object of the type for which the custom property has been defined.

**Opening a Custom Property URL**

Anytime you have specified a URL within a custom property, you can use this option to open the URL.

1. Locate the item containing the URL.
2. Right-click and, from the shortcut menu, select **Properties**.
3. In the Properties dialog box, move to the field containing the URL.
4. Place the cursor anywhere in the field and right-click.
5. From the shortcut menu, select **Open URL**.
6. Your browser will open and the web site for the URL displays.
Scheduled Scripts

The administrator can configure the system to run scripts in a schedule – e.g., to back up the database every night at 3:00 AM, perform changes early in the morning, etc.

To configure this option, do the following:

1. From the menu bar, select **Tools, Scheduled Scripts**. The Scheduled Scripts dialog box displays. Any already defined scripts are displayed.

2. To add a new script, click the **Add** button. The Schedule Script dialog box displays.

3. **Script name**. In the applicable **Script name** field, type the script name and necessary startup parameters. You must enter all information for the script as you would when invoking the script from the command line. It is assumed that the script is located in the same directory as the Men & Mice Central database file (mmsuite.db); however, if the script is stored in a different location, the path for the script must be entered.

   **Example 1:** Running a script named *mytest.vb*. To run a script named *mytest.vb* that is located in the Men & Mice Central directory using the scripting host *cscript*, the following would be placed in the appropriate field: 
   
   ```
cscript /B mytest.vb
   ```

   **Example 2:** Running an executable named *checkdata.exe*. To run an executable named *checkdata.exe* that is located in the Men & Mice Central directory the following would be placed in the appropriate field: 
   
   ```
checkdata.exe
   ```

It is possible to create a special user that has permissions to run scripts. When this user exists, it is possible to execute scripts that access the Men & Mice Suite without having to enter a user name and password in the script itself.

To enable this feature, create a user named **ScriptRunner**. This user must use the Men & Mice Internal authentication method. When this user has been created, you only have to enter $u as a user name and $p as a password when logging in to the Men & Mice Suite through the script.

**NOTE:** This method only works if the script scheduler invokes the script. When running the script, the Men & Mice Suite uses a temporary password that changes every time the script runs.
4. **Example 1:** The following example shows how the command line interface can be invoked by the scheduler to execute a backup. This statement can be entered directly into the **Script name** field:

```
mmcmd -s 127.0.0.1 -u $u -p $p backup;exit
```

**Example 2:** The following Visual Basic script checks which users are logged in and writes the list of logged in users to the file logger.txt. To invoke the script you would enter the following statement into the **Script name** field:

```
cscript /B scripts\test.vbs $u $p
```

```vbs
' Script starts here
Option Explicit
Dim objArgs, objFSO, objShell, objFile, objTextFile
Dim strFile, strUser, strPassword, i
strFile = "logger.txt"
strUser = ""
strPassword = ""

' We should get username and password as arguments
Set objArgs = WScript.Arguments
If objArgs.Count > 0 Then
    strUser = objArgs(0)
End If
If objArgs.Count > 1 Then
    strPassword = objArgs(1)
End If

' First we move into the right directory
set objShell = createobject("wscript.shell")
Set objFSO = CreateObject("Scripting.FileSystemObject")

' write extra info into the log file
If Not objFSO.FileExists(strFile) Then
    Set objFile = objFSO.CreateTextFile(strFile)
End If
set objFile = nothing
Set objTextFile = objFSO.OpenTextFile(strFile, 8, True)
objTextFile.WriteLine("*****")
objTextFile.WriteLine("Date/Time: " & Now())
objTextFile.Close

objShell.Run "cmd /c mmcnd.exe -s 127.0.0.1 -u " & strUser & " -p " & strPassword & " who; exit >> " & strFile, 0, true
set objShell = nothing
WScript.Quit
```

5. **Enabled.** Click the checkbox to enable the scheduling process for the script. Likewise, at any time if you wish to disable the script, return to this dialog box and uncheck this option.

6. **Run on.** Either type the date the script should run, or click the drop-down list field and select the date from the calendar.

7. **At.** Type or use the up/down arrows to select the time.

8. **Repeat every.** If this script should repeat at a designed frequency, click in the checkbox. Then, in the next two fields, select the interval – e.g., 1 week, 1 month, etc.

9. **When all selections/entries are made, click OK.**
Maintenance

The Men & Mice Suite contains several options for cleaning up the network space. To access the network maintenance functions, select **Tools, Maintenance** and then the maintenance operation you want to perform.

**Find Orphaned PTR Records**

The **Find Orphaned PTR Records** maintenance operation allows you to see and remove orphaned PTR records in reverse zones. PTR records that have no corresponding address (A) records in the system are considered orphaned.

To find and remove orphaned PTR records, do the following:

1. From the **Tools** menu, select **Maintenance, Find Orphaned PTR Records**. A dialog box displays.
2. Click **Start** to start looking for orphaned PTR records. **NOTE:** Finding all orphaned PTR records might take a while in large environments.
3. Select the PTR records you want to remove, and click the **Delete** button. The selected PTR records are removed.

**Find Concurrent Leases**

The **Find Concurrent Leases** maintenance operation allows you to see and release concurrent DHCP leases. Concurrent DHCP leases are multiple active leases that are assigned to the same MAC address.

To see and remove concurrent DHCP leases, do the following:

1. From the **Tools** menu, select **Maintenance, Find Concurrent Leases**. A dialog box opens.
2. Click **Start** to start looking for concurrent DHCP leases. **NOTE:** Finding all concurrent leases might take a while in large environments.
3. Select the leases you want to release, and click the Release button. The selected leases are released.

**Show Round Robin Records**

The Show Round Robin Records maintenance operation allows you to see and delete round robin DNS records. Round robin records are multiple address (A / AAAA) records with the same name.

To see and remove round robin records, do the following:

1. From the Tools menu, select Maintenance, Show Round Robin Records. A dialog box displays.
2. Click Start to start looking for round robin records. **NOTE:** Finding all round robin records might take a while in large environments.

   ![Round Robin Records](image)

   Click the Start button to search for Round Robin records. When the search is complete, you can delete individual records from the list below.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
<th>Aging</th>
</tr>
</thead>
</table>
   ...

3. Select the records you want to delete and click the Delete button. The selected records are deleted.

**Show Multiply Defined PTR Records**

The Show Multiply Defined Records maintenance operation allows you to see and delete multiply defined PTR records. Multiply defined PTR records are multiple PTR records with the same name.

To see and remove multiply defined PTR records, do the following:

1. From the Tools menu, select Maintenance, Show Multiply Defined PTR Records. A dialog box displays.
2. Click Start to start looking for multiply defined PTR records. **NOTE:** Finding all multiply defined PTR records might take a while in large environments.

   ![Multiply Defined PTR Records](image)

   Click the Start button to search for multiply defined PTR records. When the search is complete, you can delete individual records from the list below.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
</table>
   ...

3. Select the records you want to delete, and click the Delete button. The selected records are deleted.
Global Access

The Men & Mice Suite access model is object-based. This is similar to mainstream operating system access models such as the Windows Security model, where you choose an object and set access restrictions for particular Users or Groups for the chosen object. We define a set of object types, and a set of Access Flags for each object type. These flags can then be set to Allow or Deny for each User or Group.

The relationship between Groups and Users is as follows:

- Groups can contain Users
- Groups cannot contain Groups
- Users can be a member of any number of Groups

Built-in Groups

A handful of Groups are built-in to the Men & Mice Suite. These groups are special in that they get full access for their respective domains for all Access Flags.

When new objects are created, the Built-in Group that presides over that object, as well as the user that created the object, receives full access to it.

Each administrator group also receives default access to its corresponding module (including an Access Flag set on the Suite object allowing them administrator privileges for their domain). The Administrators group receives default access to all the Access Flags on the Suite object. Default access for each Built-in group is as follows:

- **Administrators.** Full access to all objects
- **DNS Administrators.** Full access to DNS objects, including zones, DNS servers, etc.
- **DHCP Administrators.** Full access to DHCP objects, including scopes, DHCP servers, etc.
- **IPAM Administrators.** Full access to IPAM objects, including IPAM ranges, etc.
- **User Administrators.** Full access to User and Group objects.

It is recommended that our clients use these Groups. These groups are the only groups that can receive default access to new items. User-defined Groups do not receive any access information for new objects and are considered to have “denied” access. To allow a User to receive default full access to a new object, include the User as a member in the corresponding Built-in Group. If you need to reduce this particular User’s access, refer to the section below titled, “Overriding Access Settings.”

When it’s mentioned that a User or Group has Full access to an object we mean that the User or Group has all known Access Flags for the object set to Allow.

The Administrator User

A single user is Built-in to the Men & Mice Suite. The Administrator User exists completely outside of the access model. This User can do everything, and it is not possible to deny any action to this User.

Examples

The **Suite** object will have the following access bits set to **Allow** for the DNS Administrators group:

<table>
<thead>
<tr>
<th>Access Flags</th>
<th>Allow</th>
<th>Deny</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administer DNS servers</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Access DNS Module</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
For every DNS server created, the server will have the following flags set to Allow for the DNS Administrators group:

<table>
<thead>
<tr>
<th>Access Flags</th>
<th>Allow</th>
<th>Deny</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit DNS Server access</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>List (or view) DNS Server</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Edit DNS Server options</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Add Master Zones</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Add non-Master Zones</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>View DNS Server Log</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Clear DNS Server Log</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Edit DNS server properties</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

For every DNS Zone created, the zone will have these flags set to Allow for the DNS Administrators group:

<table>
<thead>
<tr>
<th>Access Flags</th>
<th>Allow</th>
<th>Deny</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Zone access</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>List (or view) Zone</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Enable/disable Zone</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Edit Zone options</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Delete Zone</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Enable/disable apex records</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Edit apex records</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Enable/disable other records</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Edit other records</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Edit zone properties</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Overriding Access Settings**

The Deny setting for an Access Flag allows you to override access settings inherited from Groups. A User’s Access Footprint is calculated from the aggregate access settings of all Groups in which he is a member. In this calculation, the Deny flag overrides the Allow flag. This means that if a User is in several groups where a specific Access Flag is set to Allow, and only a single group where the same Access Flag is set to Deny, the result of the calculation for that Access Flag is Deny.

Let us take an example. Assume you want to add a new user that has DNS Administrator privileges to all servers and zones, but on a particular zone, this user should not be able to view or clear the history, nor should he be able to edit custom properties. To accomplish this, you would first include the new user in the Built-in group named DNS Administrators.
To restrict the user for a particular zone you would locate the zone and set access for your new user to the following:

<table>
<thead>
<tr>
<th>Access Flags</th>
<th>Allow</th>
<th>Deny</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Zone access</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>List (or view) Zone</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Enable/disable Zone</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Edit Zone options</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Delete Zone</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Enable/disable apex records</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Edit apex records</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Enable/disable other records</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Edit other records</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Edit zone properties</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

If you wanted to give similar access to other users, you could instead create a new Group, add the Users to the Group, and apply the aforementioned access to the zone in question for the new Group.

This system allows for a great deal of flexibility when designing your security. Any Group can be extended or overridden for a set of Users by simply adding the Users to another Group with a different access setup, or by directly overriding certain Access Flags on the Users themselves.

If no access is defined for a User or Group on a particular object, the access model assumes that all the Flags are set to Deny.

**New Objects**

When a User creates a new object in the Men & Mice Suite, the object is afforded a certain default access based on the initial access settings for the object type. To define initial access settings for different object types, do the following:

1. From the menu bar, select **Tools, Initial Access For**.
2. Select the object type for which you want to set the initial access. The Access Control dialog box displays.
3. Set the desired access for new objects and click **OK**.

**Edit Access Flag**

Each object type has an Access Flag named **Edit Access**. This flag is special in that it directs a User or Group’s access to the object’s access information. In other words, if a User has this flag set on an object, he may edit the Access Flags for the object. This means that the User could remove a different User or Group from the object completely. He could even remove the User that created the object. In light of this, the Edit Access flag should be treated with care.

Access for Built-in groups is impossible to change. However, it would be possible to shut out all Users in the Men & Mice Suite from a certain object by simply editing access for each User directly. You could even shut yourself out. The Administrator User will always have full access to every object, so if such situations arise, the Administrator User should be used to set things straight.
Access Flags Defined

Each object type in the Men & Mice Suite has a set of Access Flags defined.

**Global.** This is an object referring to the Men & Mice Suite as a whole. It contains flags that define access to the different clients and modules available in the Men & Mice Suite, as well as Administration tasks.

<table>
<thead>
<tr>
<th>OBJECT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administer users/groups</td>
<td>Access to create, edit, and delete users and groups</td>
</tr>
<tr>
<td>Administer IP Address Ranges</td>
<td>Access to admin IPAM ranges</td>
</tr>
<tr>
<td>Administer DNS servers</td>
<td>Access to create, edit, and delete DNS servers</td>
</tr>
<tr>
<td>Administer DHCP servers</td>
<td>Access to create, edit, and delete DHCP servers</td>
</tr>
<tr>
<td>Access IPAM Module</td>
<td>Access to the IPAM Module</td>
</tr>
<tr>
<td>Access DNS Module</td>
<td>Access to the DNS Module</td>
</tr>
<tr>
<td>Access DHCP Module</td>
<td>Access to the DHCP Module</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>Access to the Management Console</td>
</tr>
<tr>
<td>Access CLI</td>
<td>Access to the CLI</td>
</tr>
<tr>
<td>Access to Web Interface</td>
<td>Access to the Men &amp; Mice Web Interface</td>
</tr>
<tr>
<td>Access to basic zone view in Web Interface</td>
<td>Access to the basic zone view in the Men &amp; Mice Web Interface</td>
</tr>
<tr>
<td>Access to advanced zone view in Web Interface</td>
<td>Access to the advanced zone view in the Men &amp; Mice Web Interface</td>
</tr>
<tr>
<td>Access to IPAM view in Web Interface</td>
<td>Access to the IPAM view in the Men &amp; Mice Web Interface</td>
</tr>
<tr>
<td>Access to report view in Web interface</td>
<td>Access to the report view in the Men &amp; Mice Web Interface</td>
</tr>
<tr>
<td>Access to task list view in Web interface</td>
<td>Access to the task list view in the Men &amp; Mice Web Interface</td>
</tr>
<tr>
<td>Access to view history</td>
<td>Access to history window in the Management Console. Also provides access to the history for all objects.</td>
</tr>
<tr>
<td>Access to Host editor</td>
<td>Access to the host editor view in the Men &amp; Mice Web interface</td>
</tr>
<tr>
<td>Access to manage AD Sites and Site Links</td>
<td>Access to work with AD Sites and Site Links. <strong>NOTE:</strong> These actions can only be performed through the SOAP interface.</td>
</tr>
</tbody>
</table>

**DNS Zone**

<table>
<thead>
<tr>
<th>OBJECT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Zone access</td>
<td>Access to edit an object’s access</td>
</tr>
<tr>
<td>List (or view) Zone</td>
<td>Access to list (view) a zone</td>
</tr>
<tr>
<td>View one history</td>
<td>Access to viewing the history for the zone</td>
</tr>
<tr>
<td>Enable/disable Zone</td>
<td>Access to enable/disable the zone</td>
</tr>
<tr>
<td>Edit Zone options</td>
<td>Access to edit zone options</td>
</tr>
<tr>
<td>Delete Zone</td>
<td>Access to delete zone</td>
</tr>
<tr>
<td>Enable/disable apex records</td>
<td>Access to enable/disable zone’s APEX records</td>
</tr>
<tr>
<td>Edit apex records</td>
<td>Access to edit zone’s APEX records</td>
</tr>
<tr>
<td>Enable/disable other records</td>
<td>Access to enable/disable zone records other than APEX</td>
</tr>
<tr>
<td>Edit other records</td>
<td>Access to edit zone records other than APEX</td>
</tr>
<tr>
<td>Edit zone properties</td>
<td>Access to edit properties for the zone</td>
</tr>
</tbody>
</table>
### DHCP Scopes and IP Address Ranges

<table>
<thead>
<tr>
<th>OBJECT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit range Access</td>
<td>Access to edit an object's access</td>
</tr>
<tr>
<td>List (or view) a range</td>
<td>Access to list (view) a range/scope</td>
</tr>
<tr>
<td>View range history</td>
<td>Access to viewing the history for the range/scope</td>
</tr>
<tr>
<td>Delete range</td>
<td>Access to delete a range/scope</td>
</tr>
<tr>
<td>Edit range properties</td>
<td>Access to edit range/scope properties</td>
</tr>
<tr>
<td>Edit device properties</td>
<td>Access to edit the properties for a device in the range/scope</td>
</tr>
<tr>
<td>Use IP address in DNS</td>
<td>Access to create a DNS entry for the selected IP address</td>
</tr>
<tr>
<td>Create a subrange</td>
<td>Access to create a new subrange of the range/scope</td>
</tr>
<tr>
<td>Create multiple hosts per IP address</td>
<td>Access to create multiple address records with the same IP address</td>
</tr>
<tr>
<td>Ping IP address</td>
<td>Access to perform a ping request for hosts in the range/scope</td>
</tr>
<tr>
<td>Edit AD site association</td>
<td>Allows editing of associations for AD sites</td>
</tr>
<tr>
<td>Enable/disable scope</td>
<td>Access to enable/disable scope</td>
</tr>
<tr>
<td>Read scope options</td>
<td>Access to read scope options</td>
</tr>
<tr>
<td>Read/write Scope options</td>
<td>Access to read and write scope options</td>
</tr>
<tr>
<td>Edit Reservations</td>
<td>Access to edit reservations</td>
</tr>
<tr>
<td>Edit address pools</td>
<td>Access to edit address pools</td>
</tr>
<tr>
<td>Edit exclusions</td>
<td>Access to edit exclusions</td>
</tr>
<tr>
<td>Release Leases</td>
<td>Access to release leases</td>
</tr>
<tr>
<td>Add a group</td>
<td>Access to add a DHCP group (ISC DHCP only)</td>
</tr>
</tbody>
</table>

### DNS Server

<table>
<thead>
<tr>
<th>OBJECT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit DNS Server access</td>
<td>Access to edit an object's access</td>
</tr>
<tr>
<td>List (or view) DNS Server</td>
<td>Access to list (or view) server</td>
</tr>
<tr>
<td>View DNS server history</td>
<td>Access to viewing the history for the DNS server</td>
</tr>
<tr>
<td>Edit DNS Server options</td>
<td>Access to server options</td>
</tr>
<tr>
<td>Add Master Zones</td>
<td>Access to add a master zone</td>
</tr>
<tr>
<td>Add non-Master Zones</td>
<td>Access to add a non-master zone</td>
</tr>
<tr>
<td>View DNS Server Log</td>
<td>Access to view the server log</td>
</tr>
<tr>
<td>Clear DNS Server Log</td>
<td>Access to clear the server log</td>
</tr>
<tr>
<td>Edit DNS server properties</td>
<td>Access to edit properties for the DNS Server</td>
</tr>
</tbody>
</table>

### DHCP Server

<table>
<thead>
<tr>
<th>OBJECT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit DHCP Server Access</td>
<td>Access to edit an object's access</td>
</tr>
<tr>
<td>List (or view) DHCP Server</td>
<td>Access to list (or view) server</td>
</tr>
<tr>
<td>View DHCP server history</td>
<td>Access to viewing the history for the DHCP server</td>
</tr>
<tr>
<td>Read DHCP Server options</td>
<td>Access to view server options</td>
</tr>
<tr>
<td>Read/write DHCP Server options</td>
<td>Access to read and write server options</td>
</tr>
<tr>
<td>Add a scope</td>
<td>Access to add a DHCP scope</td>
</tr>
<tr>
<td>Edit DHCP server properties</td>
<td>Access to edit properties for the DHCP Server</td>
</tr>
<tr>
<td>Edit reservations</td>
<td>Access to edit reservations in DHCP scopes</td>
</tr>
<tr>
<td>Add a group</td>
<td>Access to add DHCP groups (ISC DHCP only)</td>
</tr>
<tr>
<td>Read DHCP class data</td>
<td>Access to view DHCP class data on an (ISC DHCP only)</td>
</tr>
<tr>
<td>Read/write DHCP class data</td>
<td>Access to read and write DHCP class data (ISC DHCP only)</td>
</tr>
</tbody>
</table>
DHCP Groups

<table>
<thead>
<tr>
<th>OBJECT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit DHCP group</td>
<td>Access to edit an object’s access</td>
</tr>
<tr>
<td>List (or view) DHCP group</td>
<td>Access to list (or view) DHCP group</td>
</tr>
<tr>
<td>View DHCP group history</td>
<td>Access to viewing the history for the DHCP group</td>
</tr>
<tr>
<td>Edit Reservations</td>
<td>Access to edit reservations</td>
</tr>
<tr>
<td>Read DHCP group options</td>
<td>Access to view group options</td>
</tr>
<tr>
<td>Read/write DHCP group options</td>
<td>Access to read and write group options</td>
</tr>
<tr>
<td>Delete DHCP group</td>
<td>Access to delete a DHCP group</td>
</tr>
</tbody>
</table>

Address Spaces

<table>
<thead>
<tr>
<th>OBJECT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit address space access</td>
<td>Access to edit an object’s access</td>
</tr>
<tr>
<td>List (or view) address space</td>
<td>Access to list (or view) address space</td>
</tr>
<tr>
<td>View address space history</td>
<td>Access to viewing the history for the address space</td>
</tr>
</tbody>
</table>

Access Control Dialog Box

Through the Access Control module, you select groups/users for which you want to manage permissions.

The Access Control dialog box is used to define access to individual objects in the system. To define access for an object, right-click the object and choose Access from the popup menu.

To define access for individual components of the Men & Mice suite, do the following:

- From the menu bar, select **Tools, Global Access**. The Access Control for Men and Mice Suite dialog box displays.

  The default groups/user names are shown. The permissions for any selected group/user are also shown.

Selecting a Group/User

1. While viewing the Access Control dialog box, click the **Add** button. The Select user or group dialog box displays.

2. Highlight the user and/or group for which you want to assign permissions.

3. Click the **Select** button.

4. When you return to the main dialog box, the user/group is highlighted in the list of users and groups.
5. To specify the permissions for this selected group/user, do the following:
   – Move to the Permission for [group/user selected] list.
   – Click in the checkbox for each permission you want to Allow or Deny.

   **NOTE:** It is not necessary to select Deny unless you want to ensure that a user/group does not have permission to a specific object. However, if you do not specify the permission for an individual user, but the group(s) to which the user belong does Allow access to that object, the user (by default) also has access.

6. When all selections are made, click OK. The dialog box closes.

7. Repeat the above for any additional groups/users.

**Initial Access For**

Through this function, you specify access privileges that should be set for objects when they are created. This function is identical to the Access Model and Permissions function except that a new user type – “Creator” (Meta user) - is used to specify the access privileges that should be set for the object creator.

- From the menu bar, select **Tools, Initial Access For**, and then the object type for which you want to set the initial access. The Access Control dialog box displays. Refer to Administration Functions—Global Access/Access Control for details on working with this dialog box.
This page intentionally left blank.
Chapter 4: DNS Servers

Overview

This section shows you how to perform specific actions in the Men & Mice Management Console associated with maintaining your DNS servers, such as adding, and creating and editing zones and records.

The commands associated with server management are located in the Server menu and several are accessible from the toolbar. The Server menu is only available when the DNS Servers object is selected in the Object Section of the Management Console.

NOTE: The functions for this menu option are listed alphabetically after the New DNS Server section.

New DNS Server

You must be logged in as a user with privileges to administer DNS in order to add a DNS server.

To add a new DNS server, do the following:

1. From the menu bar, select File, New, DNS Server. The Add DNS Server dialog box displays.
2. Server Name. Type the name (host name) of the DNS server.
3. Server address (optional). If desired, type the IPv4 or IPv6 address for the server. This is not required, but doing so allows the Management Console to connect to the server by IP address instead of by name. The Server name will still be used when displaying server information and creating NS records.
4. Server Type. Click the drop-down list, and select the desired server type.
   - Microsoft with Agent Installed connects to a Microsoft DNS server that has a DNS Server Controller installed.
   - Microsoft Agent-Free connects to a Microsoft DNS server that does not have a DNS Server Controller installed. For further information regarding this connection method, see the section Server Access on Remote Computers, below
   - BIND connects to BIND DNS server.
5. Use proxy server. If you are adding a Microsoft DNS server you can specify the location of the DNS Server Controller by clicking the Use proxy server checkbox and entering the DNS name or IP address of the machine running the DNS Server controller. This option allows the system to connect to DNS servers in different forests where a cross-forest trust does not exist. It also allows a non-Windows version of Men & Mice Central to manage Microsoft DNS servers.
6. Click OK. You are connected to the server. Once connected, the name of the newly added server displays under DNS Servers in the Object Section. (You may need to click the plus (+) sign next to DNS Servers to see it.)
Server Access on Remote Computers

To manage DNS servers you must have the DNS Server Controller installed. For the BIND DNS server, a DNS Server Controller must be installed on each DNS server you want to manage.

If you plan to use Men & Mice Suite to manage any Microsoft DNS servers, install the DNS Server Controller on a Windows machine that is a member of the same domain or workgroup as the DNS servers. You may install multiple copies of the DNS Server Controller, for example if you want to manage Microsoft DNS Servers that reside in different forests. A single DNS Server Controller for Microsoft DNS Servers can manage multiple DNS servers. The DNS Server Controller must adhere to whatever restrictions and security standards are set forth in Microsoft Windows.

To configure the DNS Server Controller to access DNS servers on remote computers, do the following:

1. Before you can administer DNS servers, verify that the DNS Controller is running as a Windows User and has the necessary privileges.
2. To enable DNS Management in the Men & Mice Suite, start the Windows Services program and open the properties dialog box for Men & Mice DNS Server Controller.
3. Click the Log On tab. The Local System account radio button is most likely selected.
4. Click the This account radio button and enter the name and password of a Windows User that is a member of the Administrators group.
5. Close the dialog box and restart the Men & Mice DNS Server Controller service.

NOTE: Some actions for static zones are not available if you are managing MS DNS servers on remote computers using the DNS Server Controller. The following actions are not available:

- Disable resource record
- Enable resource record
- View and edit resource record comments
- Disable zone

If you need to be able to perform these actions, you must install the DNS Server Controller on the server and use the Microsoft with Agent Installed connection method when connecting to the server.

Edit DNS Server Name

This feature allows you to change the name or IP address used to connect to a DNS server. This is useful if you need to refer to the server by another name or if you are connecting to the server by an IP address and the IP address has changed. You can also use this feature to change the connection method for MS DNS servers.

To access this feature, do the following:

1. Locate the applicable server.
2. Right-click and, from the shortcut menu, select Edit Server Name. The Edit Server name dialog box displays.
3. Change the Server name, Server address (optional), and/or Server Type. If applicable, you can select Use proxy server and enter the relevant information.
4. Click OK.
Access

Refer to Administration Functions—Global Access/Access Control.

Define Work Set

It is possible to define a Work Set for servers. A Work Set contains a subset of all of the servers in the system and when a Work Set is active, only the servers in the Work Set are visible and the zones on the servers in the Work Set are the only zones visible. This feature is useful when many servers are defined, but you only work with a small number of them on a day-to-day basis.

To define a Work Set, do the following:

1. Select the server(s) you want to include in the Work Set
2. Right-click the selected server(s) and choose Define Work Set.

To clear a Work Set, do the following:

- Click the Clear Work Set button in the Manager window. The Work Set is cleared.

Delete

This command is only available with the Administrator account. Use this command to remove a server from the Management Console.

1. In the Object browser of the Management Console, click on DNS Servers.
2. In the Object List, select the Name Server(s) from you want to disconnect. To select multiple servers, hold down the Ctrl key while making your selections.
3. On the toolbar, click the Remove button. A dialog box prompts you to confirm your decision.
4. To disconnect from the Name Server, click Yes. Otherwise, click No to keep the server.

Options

The Server Options dialog box lets you configure settings for each name server individually, including forwarding servers, logging preferences, transfer and query restrictions, and root servers.

NOTE: The server options vary depending on the server environment. In the section that follows, the server options are documented twice: once for those using a Windows DNS server, and again for those using BIND.

Accessing Server Options

1. In the Object Section, select DNS Servers so the servers appear in the Object List.
2. Right-click on the server you want to make changes to and select Options from the context menu. The Server Options dialog box displays.
3. Choose the desired option (Resolution, Logging, Advanced, Interfaces, Event logging, Root hints) from the menu on the left. The corresponding options display in the right panel of the dialog box.
4. Refer to the appropriate section and server environment below for each option.
Windows DNS Servers

This section describes the Server Options as they display in a Windows Server environment.

Resolution (Windows)

The Resolution panel lets you change the method by which this server resolves queries. Three basic modes can be established:

- **Mode 1: The server can be set to resolve queries entirely by itself.** If you do not want to use any forwarders with this server, leave the Use forwarder(s) checkbox unchecked.

- **Mode 2: The server can share the task of resolving queries.** If you want to share the task of resolving requests with one or more forwarding servers, select the Use forwarder(s) checkbox and enter the IP address of the forwarding servers in the Forwarders list.

When you enter the IP addresses to multiple forwarders, all the forwarders are queried simultaneously, and the first response is accepted. Under this shared mode, if a server using a forwarder does not receive a response after a few seconds, it will attempt to resolve the query itself.

- **Mode 3: The server can forward all requests to other servers.** If you want to forward all requests to other servers (and never use this server), select the Use forwarder(s) checkbox, enter the IP address of the forwarding server(s) in the Forwarders list, and check the Only user forwarder(s) checkbox.

After making the desired changes, you can choose another category from the left column, or click OK to close the dialog box.

Logging (Windows)

The Logging options consist of a list of checkbox options. Once you enable Log packets for debugging, the other options in the dialog box become accessible and you can choose which types of information you want the program to record in the server’s log.

After checking the desired options, you can either choose another category from the left column or click OK to close the dialog box.
Advanced (Windows)

Use this panel to set various advanced options for the DNS server. Complete the dialog box based upon the guidelines below. When all selections/entries are made, click OK.
• **Disable recursion.** Determines whether or not the DNS server uses recursion.

• **BIND secondaries.** Enables fast (compressed) zone transfers for compatibility with old BIND servers (older than 4.9.4).

• **Fail on load if bad zone data.** Prevents the server from loading a zone when bad data is found.

• **Enable round robin.** Rotates the order of resource record data returned in query answers when multiple resource records of the same type exist for the queried DNS domain name.

• **Enable netmask ordering.** Determines whether the DNS server reorders A resource records within the same resource record set in its response to a query based on the IP address of the source of the query.

• **Secure cache against pollution.** Determines whether the server attempts to clean up responses to avoid cache pollution.

• **Name Checking.** Determines the type of name checking used for zones on the server. Click the drop-down list and select from the options provided.

• **Load Zone Data on startup.** Determines from where to load the zone data when the server starts up. Click the drop-down list and select from the options provided.

• **Enable automatic scavenging of stale records.** Specifies whether scavenging can occur for the selected server. If automatic scavenging is enabled, the scavenging period can be specified. Type the duration in the first field. In the second field, click the drop-down list and select the duration range – e.g., days.

### Interfaces (Windows)

- Use this panel to specify the IP addresses this server will use to serve DNS requests. When your selection is made, click **OK**.
Event Logging (Windows)

Specifies what event information should be logged and displayed in the Server log.

1. Click next to each of the desired items using the guidelines below:

2. **No events.** Specifies that no events will be logged in the DNS Server log.
3. **Errors only.** Specifies that only errors will be logged in the DNS Server log.
4. **Errors and warnings.** Specifies that only errors and warnings will be logged in the DNS Server log.
5. **All events.** Specifies that all events will be logged in the DNS Server log.
6. When all selections are made, click **OK**.

Root hints

Allows configuration of suggested root servers for the server to use and refer to in resolving names.
1. To **Add** a Root name server, complete the fields as follows:

   **Root hint name server**

   Server fully qualified domain name: 

   IP address

   ![Root hint name server dialog box]

   2. Click the **Add** button.
   3. Server fully qualified domain name. Type the name of the server.
   4. **IP Address.** Type the IP address of this server.
   5. Click **OK**.

To **Edit** the Root hint name server data, do the following:

1. Select the server definition you want to edit.
2. Click the **Edit** button.
3. In the Root hint name server dialog box, type the updated information.
4. Click **OK**.

To **Remove** a Root hint name server, do the following:

1. Select the server definition you want to remove.
2. Click the **Remove** button
**BIND Environment**

This section describes the Server Options as they display in a BIND environment.

**Resolution (BIND)**

The Resolution settings in a BIND environment are the same as in a Windows environment.

Logging (BIND)

The Logging Settings control the type of information that is recorded in a server's log.

- **Channels.** Specifies where your logged data will go. Use the drop-down list to select which log file you want to receive which categories of data.

- **Log Level.** The Log Level allows you to filter messages by severity. Select the level of messages that you want to log by choosing the corresponding radio button. There are eight radio buttons. The top five are the standard severity levels used by syslog. The remaining two settings are Debug and Dynamic.
– **Debug.** Provides name server debugging. When you choose this option, a text box displays next to the radio button allowing you to specify a debug level. If you do not specify a debug level, it is assumed to be 1. If you do specify a level, you will see messages of that level when name server debugging is turned on.

– **Dynamic.** Causes the name server to log messages that match the debug level. For example, if you send two trace commands to the name server, it will log messages from level 1 and level 2.

- **Print Category.** When selected, the category of the message displays with the log entry.
- **Print severity.** When selected, the severity of the message displays with the log entry.
- **Print time.** When selected, the message includes a time stamp.
- **Max file size.** Determines how many versions of the log file are maintained. The log file will grow to the size specified in the Max file size field, after which a new log file is created and the old file is renamed. As this process continues, each file is systematically renamed until it is finally deleted. For example, if the Version field contained the value 2, there would be the ‘active’ log file, and two older versions. When the active log file becomes too big, a new log file would be created and the previously active log file would be renamed as the version 1 file. The old version 1 file would be renamed as the version 2 file, and the old version 2 file would be deleted.

- **Versions.** Enter the maximum size of the log file and the appropriate units. For example, 100K = 100 kilobytes, 2M = 2 megabytes, and 3G = 3 gigabytes. If no value is specified, the default unit bytes are used.

- **Category.** Lists the different types of information that can be logged. The System log typically tracks system-level messages, while the Men & Mice log is much more comprehensive and includes information about server interactions and activity. Check the categories you want to include in the log.

### Query Restrictions (BIND)

The Query restrictions panel allows you to restrict recursive DNS queries to only certain IP addresses or address ranges.

To configure a query restriction, do the following:

1. Click the **Add** button.
2. Enter an IP address in the field provided. You can choose a predefined range from the drop down list, which gives you the option to select **any, none, localhost, or localnets.**
3. Choose whether you want to allow or deny this server access control for recursive queries by selecting the appropriate radio button.
4. Click **OK** to add the new restriction to the list.
Transfer Restrictions (BIND)

The Transfer restrictions panel allows you to restrict zone transfers to only certain IP addresses or address ranges. Restricting access to zone transfers is a marginally effective security measure designed to prevent outsiders from seeing the names and IP addresses of your hosts. All of this information is available from a reverse zone lookup. However, security through obscurity will keep out amateurs and the merely curious.

To configure a transfer restriction, do the following:

1. Click the **Add** button.
2. Enter an IP address in the field provided. You can choose a predefined range from the drop down list, which gives you the option to select **any, none, localhost, or localnets**.
3. Choose whether you want to allow or deny zone transfers to this IP Address by selecting the appropriate radio button.
4. Click **OK** to add the new restriction to the list.

Listen on (BIND)

The Listen on panel allows specify the IP addresses this server will use to serve DNS requests.
To specify the listening interfaces, select the checkboxes for the interfaces you want to listen on, both for IPv4 and IPv6.

- If you select the **any** option, the server will listen on all configured IP addresses.
- If you select the **None** option, the server will not listen on any IP address.

**Advanced Server Options**

DNS Administrators can access the BIND configuration files directly to edit DNS server and zone options that are not available in the GUI.

To access the advanced options, do the following:

1. Log in to Men & Mice as the DNS administrator.
2. For a DNS zone or DNS server, right-click and select **Options** from the shortcut menu.
3. When the Options displays, click the **Advanced** button.
4. When the Advanced Options dialog box displays, you can edit the options for the zone or server in a text document. The dialog for editing server options contains four tabs where each tab contains a section of the server options (logging, user_before, options, user_after).

If the DNS server contains one or more views, each view displays in a separate tab where various settings can be changed for each view. **NOTE: #include statements are not shown and you cannot add #include statements.**

![Advanced Options Dialog](image)

Refer to Appendix F: BIND DNS File Structure for more information on each section.

5. Click **OK**. The contents of the files are verified for correctness. If an error is found during verification, an error message displays and the changes are not saved.

## Properties

**Applies only when custom properties have been defined for DNS servers.** Selecting this menu item will display a dialog box where the custom property values can be modified.

1. In the Object browser, select the server for which you want to manage properties.
2. From the menu bar, select **Server, Properties**.
3. **Location.** Type a location.
4. Click **Apply** or **OK**.
Server Info

This command opens a dialog box that shows information about the history and status of the currently selected server in the Management Console. This includes such things as the server’s IP address, operating system, number of requests & replies received, total uptime, and the number of master and slave zones it has. This command is only available when a server is selected in the Management Console.

- In the Object List, right-click on the desired server name and, from the shortcut menu, select Server Info.

![Server Info dialog box]

An Information window opens for the selected server.

Server Log

To view the activity log for a particular server, do one of the following:

- In the Object List, right-click on the desired server and, from the shortcut menu, select Server Log. A Log window opens for the selected server that contains a list of activity and maintenance that has occurred on that server since the last time the log was cleared.

- You can clear the server log by clicking the Clear log button in the server log window.

![Server Log window]

**NOTE:** For Windows DNS servers, it is not possible to view the server log if connected through an agent-free connection.
Reload/Reload Zone List/Clear Cache

There are two reload commands in the Server context and the commands are quite different:

- **Reload**. This command reloads the DNS server. On Windows this command has the same effect as the **Clear Cache** command, but on BIND servers, the command ‘rndc reload’ is sent to the DNS server.

- **Reload Zone List**. This command reloads the list of zones from the DNS server. It is useful if a zone has been created outside of the Men & Mice Suite.

In addition to the reload commands, it is possible to clear the DNS server cache using the **Clear Cache** command.

To reload the zone list to include zones that have been added/deleted outside of the Men & Mice suite, do the following:

1. Select the desired server.
2. From the menu bar, select Server, Reload Zone List. The window grays as the zones are reloaded then displays with the updated zones.

To **reload** a DNS server, do the following:

1. Select the desired server.
2. From the menu bar, select Server, Reload Zone List.

To **clear** the cache of a DNS server, do the following:

1. Select the desired server.
2. From the menu bar, select Server, Clear Cache.

Backup and Restore (BIND Only)

The Men & Mice Suite will automatically backup configuration for all BIND DNS servers it manages. The backup can then be used to restore the DNS server to the backed-up copy of the configuration.

The backup is fully automatic and there is no configuration needed.

Automatic backup can be disabled by setting the property BackupDNSServers value in Men & Mice central preferences to zero:

```xml
<BackupDNSServers value="0" />
```

If a DNS server machine crashes and has to be replaced with another machine with the same IP address, the Men & Mice Suite will detect the new server and consider it to be in an uninitialized state. To be able to work with the server the administrator needs to initialize the server. To initialize the server right-click on the server and select **Initialize**. This will display a dialog box where the user can choose how the server should be initialized:
• If “Use data from the Men & Mice Suite” is selected, all configurations and DNS zone information on the DNS server will be overwritten with the backed-up data.

• If “Use data from the new server” is selected, all data kept in Men & Mice Central will be ignored and overwritten with current data on the DNS Server.

Basically, the restore scenario is as follows:

1. The DNS server machine crashes and becomes unusable.
2. Configure a new machine to replace the broken machine, using the same IP address as the old machine.
3. Install the DNS Server Controller on the new machine.
4. When the new machine is up and running, in the Management Console, right-click the server and choose Reconnect.

When a connection has been established, the Men & Mice Suite detects that this is a new, uninitialized server. See above for a description on what happens next.
Chapter 5: DNS Zones

Overview

The commands associated with zone management (located in the Zone menu) are only available when a specific DNS server is selected in the Object Section, or when DNS Zones is selected. In other words, the Zone menu is only available when DNS zones are listed in the Object List.

When DNS Zones is selected in the Object Browser, all DNS zones are listed on all servers. However, when a particular name server is selected in the Object Section, only the zones being managed on that server are listed.

NOTE: The functions for this menu option are listed alphabetically after the Zone Icons and Zone Viewing sections.

Zone Icons

When viewing the zones, you will notice the icons that appear to the left of each zone's name. The color of the square (or lack of a square) designates whether the zone is a static master zone, a dynamic master zone, or a slave zone, as described below:

- An icon with a blue dot indicates a static master zone, which is always the original copy of the zone, and always present on that zone's master server.

- An icon with a gold dot indicates a dynamic master zone, which is always the original copy of the zone, and always present on that zone's master server.

- An icon with a purple dot indicates an Active Directory Integrated zone.

- A half page icon represents a stub zone.

- An icon with an arrow pointing to the right represents a forward zone.

- A faded icon without any color marking indicates a slave zone. A slave zone is a duplicate of a master zone that is made on the master zone's slave server(s). Slave zones bring redundancy and stability to the DNS system because it allows more than one server to process domain requests, and allows requests to be processed even if one of the servers becomes unavailable.

NOTE: These indications are not related to which physical server on which the zone is created. Any server can be the master server. The terms master and slave are only relative to the zones. Whichever server the zone was created on is the master server for that zone. This means that a new zone is always created on the master server.
Zone Viewing

All Zones on All Servers

You can use the Management Console to view all of the existing DNS zones at once, regardless of the server to which they belong.

- In the Object Section of the Management Console, click the DNS Zones object. This causes all existing zones (to which you have access) to appear in the Object List.

Single Name Server Zones

- In the Object Section of the Management Console, locate the DNS server that owns the zones you want to view and click on it. (The DNS server(s) will be listed under the DNS Servers object. You may need to click the plus (+) sign in order to see it.) When a server is selected, the zone information for that server displays in the Objects List.

Zone Contents

The Zone Window provides a detailed look at the data inside of a zone, including its resource records. The name of the zone always displays in the title bar. The header record (a.k.a. Start of Authority or SOA record) displays as a collection of fields above the resource records.

- To view the contents of a particular zone, double-click on it. This opens the Zone window.
SOA Panel

Since the SOA record is seldom modified after it is created, the Zone window has a built-in control to allow you to conceal the SOA panel from view. This allows you to view more of the resource record area below. If you look at the left edge of the Zone window, just above the record table, you will notice three short horizontal lines, stacked vertically. This is the Hide/Show SOA panel control. Click on this control once to hide the SOA panel. Click on it again to make it re-appear.

SOA Fields

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master</td>
<td>This field gives the name of the server that acts as master server for the zone.</td>
</tr>
<tr>
<td>Hostmaster</td>
<td>This field is properly formatted by giving the e-mail address of the person responsible for zone with the @ symbol replaced with a period (.). For example, instead of <a href="mailto:hostmaster@example.com">hostmaster@example.com</a> type hostmaster.example.com.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number is a ten-digit number consisting of the year, the month, the day, and a two-digit daily revision number. (Actually, it is any integer between 0 and ~ 4 billion, but the preceding is the standard convention.) To create a unique serial number, the Management Console adds 1 to the daily revision number every time the zone is saved.</td>
</tr>
<tr>
<td>Refresh</td>
<td>This is the period (in seconds) that determines how often slave servers will check with the master server to determine if their zone files are up to date. This is done by checking the serial number. The default value for this field is 28800, which equates to once every 8 hours.</td>
</tr>
<tr>
<td>Retry</td>
<td>This determines the period that a slave server will wait before trying to re-contact the master zone (in the event that an earlier contact attempt is unsuccessful). The default value is 7200 seconds, or once every 2 hours.</td>
</tr>
<tr>
<td>Expire</td>
<td>This value determines how long a slave server will keep serving a zone after its last successful contact to the master name server. Once the zone has expired, the slave stops giving information about the zone because it is deemed unreliable. The default expiration period is 604800 seconds, or 1 week.</td>
</tr>
<tr>
<td>Neg. caching</td>
<td>This field is only available when connected to a BIND server. This value specifies how long a server will retain (cache) the knowledge that something does not exist. The default value is 86400 seconds, 24 hours.</td>
</tr>
<tr>
<td>Default TTL</td>
<td>This value serves as the default time-to-live for all records without an explicit TTL value. The default value is 86400 seconds, 24 hours.</td>
</tr>
<tr>
<td>TTL of SOA</td>
<td>This TTL applies to the SOA record. It represents the maximum time in seconds any outside DNS server should cache this data. The default value is 86400 seconds, 24 hours.</td>
</tr>
</tbody>
</table>

Zone Analysis

The DNS Expert Zone Analysis engine allows zones to be analyzed for correctness.

To analyze a zone, do any of the following:

- Right-click on the zone you want to analyze, and from the shortcut menu select Analyze.
- Choose Zone, Analyze.
- Open the zone and click the Analyze button on the toolbar.
The results of the zone analysis are shown in a new window:

- **Reanalyze.** To perform the analysis again, press F5 or click the Analyze button.
- **Filtering.** It is possible to filter out messages of a certain type. When the checkbox, Don’t show filtered messages is selected, the filtering is active and these messages are not shown in the message list. Deselecting the checkbox disables the filtering and all messages are shown in the message list.
- **Quick Filter.** The Quick filter works the same as it does in other windows.
- **Messages.** The message list shows the results of the zone analysis. Messages are either warnings or errors (as indicated by the icon next to the message). Selecting a message will display detailed information about the message at the bottom of the window.
- **Fix.** When the application can fix an error, the Fix menu item becomes available. Selecting this menu item will display more information about the fix for the error.
- **Filter out messages of this type.** Selecting this item, will suppress the display of the selected error type unless the Don’t show filtered messages checkbox is unselected. **NOTE:** This setting is global and it is applied to all subsequent analysis in all zones. If you right-click a filtered message, this item will read as Don’t filter out messages of this type.

If the zone you are analyzing is open, an icon with an exclamation mark is shown in the bottom left corner of the window. Clicking this icon will display the errors found during the analysis in a list at the bottom of the zone window. Closing the analysis window will clear the error message list in the zone window.

**Access/Access for Non-Master for Zone(s)**

Refer to Administration Functions—Global Access/Access Control.
Delete

Use this command to delete a zone from one or more servers. Before using this command, select the zone you want to delete from the Management Console; the Delete Zone dialog box displays and shows a list of servers on which that zone resides.

By default, the zone will be removed from all servers (i.e., all servers are checked). If you want to keep it on one or more servers, clear the checkbox next to that server. Click the **Delete** button to remove the zone from the selected servers.

1. In the Object Section, select **DNS Zones** to view all zones.
2. Select the zone(s) that you want to delete. To select more than one zone, hold down the **Ctrl** key while making your selections.
3. Right-click on any selected zone and, from the shortcut menu, select Delete. The Delete Zone dialog box displays, showing each zone you selected and a list of servers that currently serve that zone. The zone(s) you selected will be deleted from every server that is checked on this list. To keep the zone on a particular server, clear the checkbox next to that server.
4. To remove the zone(s) from the selected servers, click the **Delete** button. The zone is removed from the servers.

Disable/Enable

**Disabling a Zone(s)**

This function is only available for static master zones that have no slave zones. (For other types of zones (dynamic or AD integrated) the command is not visible. The **Disable** command deactivates the entire zone without deleting it. When disabled, the server ignores the contents of the zone. The zone can still be edited while disabled, but changes will not take effect until the zone is re-enabled.

1. In the Object Section, select DNS Zones to view all zones, or under the DNS Servers object, select the server containing the zone you want to disable. This displays the zones in the Object List.
2. Select the zone(s) that you want to disable. To select more than one zone, hold down the **Ctrl** key while making your selections.
3. From the menu bar, select **Zone, Disable Zone**. A dialog box prompts you to confirm your decision.
4. To disable the selected zone(s), click the Yes button. The zone becomes disabled. Zones that are disabled appear faded in the Object List. They are still fully accessible and editable, but they will not be active until you re-enable them.

**Enabling a Zone(s)**

Use the following procedure to re-activate a zone that has been disabled.

1. In the Object List, locate the zone(s) that you want to re-enable. To select more than one disabled zone, hold down the Ctrl key while making your selections.
2. From the menu bar, select Zone, Enable Zone. A dialog box prompts you to confirm your decision.
3. To enable the zone(s), click the Yes button. The Object List refreshes itself and shows that the zone(s) has been restored to active status.

**Duplicate**

Use the following procedure to create a new zone that is an exact duplicate of an existing one, including master and slave servers, zone data and zone options.

1. In the Object Section, select either DNS Zones, or select a specific server under the DNS Servers object. This lists the zones in the Object List.
2. In the Object List, right-click on the zone you want to duplicate and select Duplicate from the popup menu. The Create Zone dialog box displays.
3. Enter a name for the new zone in the Zone Name field.
4. Click the Create button. A new zone is created with the same records, Master server, and Slave servers as the original.

**Edit Preferred Servers**

This option is only available when working with AD integrated zones. It is used to specify the server to use when opening an AD integrated zone.

It is also possible to specify which server to use if the preferred server becomes unavailable—e.g., the server on the top of the list is tried first and, if that server is unavailable, the second server is tried, and so on.

1. From the menu bar, select Zone, Preferred Server. The Edit preferred server list dialog box displays.
2. Change the order of your servers into the preferred order.
3. Click OK.

**Export**

Use this command to export DNS zone files to standard format.

1. Select the zone you want to export and open the Zone window.
2. From the menu, select File, Export. The Export zone to text file dialog box displays.
3. Provide a name and destination for the file and click the Save button. All exported files are saved in standard, readable format.
Folders

Refer to Management Console: Object Folders for details on this function.

Forward Zone

Through this function, you create a forward zone.

1. In the Object List, right-click on DNS Zones and, from the shortcut menu, select New Forward Zone. The Create forward zone dialog box displays.

2. Zone name. Type the name for this forward zone. You cannot use spaces in the name.

3. Servers. Select all the servers to which this forward zone applies by clicking in the checkbox.

4. IP addresses of forward servers. Type the IP address of any master servers for this zone.

5. Click Create. The new forward zone is created and displays in the Detail View of the main window.

Import

Through this function, you can import multiple DNS zones at one time.

1. From the File menu, select Import Zone. The Import dialog box displays.

2. Locate the zones to be imported. The zones must within the same folder. To select multiple zones, press/hold the Ctrl key. Then click on each zone.

3. Click Open. The files are uploaded and the Import zones dialog box displays.

4. Click Import.
5. If you happen to select an invalid zone, the following error message dialog box displays:

![Image of error message dialog box]

6. Click **OK** and when you return to the Import zones dialog box, clear the field containing the zone.

---

**Master Zone**

This procedure is the fastest way to add a new blank (i.e., empty) zone. If you want to duplicate an existing zone, you should use the Duplicate command instead.

It does not matter which server is currently selected when you add a zone. You always have the option to select the Master Server when you configure the zone.

1. In the Object Section, select either DNS Zones, or select a specific server under the DNS Servers object.

2. On the toolbar, click the **New Zone** button. The Create Zone dialog box displays.

3. To use the Create Zone Wizard from this dialog box, click the Assist me button and follow the instructions found under the section titled, “Zone Wizard.” If you chose not to use the zone wizard, continue with the steps below.

4. In the **Zone Name** field, type a name for the new zone.

5. In the **Master server** field, click the drop-down list, and select the server that you want to designate as the master for this zone. The Slave servers list automatically updates itself based upon your choice of the master server.

6. In the Slave server area, select the slave server(s) onto which you want to place this zone. The slave servers are selected by default, so if you do not want to assign this zone to a slave server, you must clear the associated checkbox. You can select or deselect all slave servers by right-clicking the list of slave servers in the dialog box for creation of master zones, and selecting the appropriate menu item.

7. If you want the zone to be an Active Directory Integrated zone, click the AD Integrated zone checkbox.

8. If the zone is Active Directory Integrated, the **AD Replication** button is enabled. Click this button to display a dialog box where you can set the AD Replication options for the zone.

9. If you want to the zone to use the Secure64 DNS Signer, click in the box next to **Use Secure64 DNS Signer.** See Appendix H: Secure 64 Integration.
10. To finish creating the zone, click the **Create** button. The new zone is created with the appropriate name server (NS) records, and the Zone SOA Panel displays.

11. Make any desired changes to the data shown.

12. When all selections/entries are made, click **Save**.
DNSSEC Zones

Zones containing DNSSEC records are labeled as “Signed” in the DNSSEC column in the zone list.

When DNSSEC zones are opened, the toolbar contains a “Hide DNSSEC Records” checkbox that toggles display of DNSSEC related records.

**NOTE:** All DNSSEC record types, with the exception of the DS and NSEC3PARAM record types, are read-only.

DNSSEC Management on Windows Server 2012

You can use the Men & Mice Suite to manage DNSSEC on Windows Server 2012. You can sign and unsign zones. You can customize the zone signing parameters and add, edit and remove Key Signing Keys (KSK) and Zone Signing Keys (ZSK).

The details of DNSSEC are beyond the scope of this documentation. For more information on Windows Server 2012 and DNSSEC, see the Microsoft web site [http://www.microsoft.com](http://www.microsoft.com).

**Signing Zones using DNSSEC**

To sign a zone on a Windows Server 2012, do the following:

1. With the zones displayed in the Object List, select the zone you wish to sign.
2. Do one of the following to display the Zone Signing dialog box:
   - Right-click on the zone record and select **Sign Zone**.
From the menu bar, select **Zone, Sign Zone**.

3. Select an option for signing the zone:
   - **Customize zone signing parameters**. Signs the zone with a new set of zone signing parameters. When this option is selected you can choose or create new Key Signing Keys (KSK) and Zone Signing Keys (ZSK).
   - **Sign the zone with parameters of an existing zone**. Signs the zone using parameters from an existing signed zone. To use this option, you must enter the name of the zone containing the parameters to use.
   - **Use default settings to sign the zone**. Signs the zone with the default zone signing parameters.

4. Click **Next**. If you chose the **Customize zone signing parameters** option, the zone signing wizard allows you to choose KSK and ZSK for signing the zone. If you chose either of the other options, an overview panel displays in which you can see the zone signing parameters that will be used to sign the zone.

5. Click **Finish** to complete the zone signing process.

**Unsigning Zones using DNSSEC**

To unsign a zone on a Windows Server 2012, do the following:

1. With the zones displayed in the Object List, select the zone you wish to unsign.
2. Do one of the following to unsign the zone:
   - Right-click on the zone record and select **Unsign Zone**.
   - From the menu bar, select **Zone, Unsign Zone**.

The zone is unsigned and all DNSSEC records are removed from the zone.

**Options**

The Zone Options dialog box is where you can configure individual settings for a specific zone on each server.

**Zone Options (Windows and BIND)**

To access the zone options for a specific zone only, do the following:

1. With the zones displayed in the Object List, select the zone you wish to configure.
2. Do one of the following to display the Zone Options dialog box:
Right-click on the zone record and select **Options**.

From the menu bar, select **Zone, Options**.

On the toolbar, click the **Options** button.

Depending on the type of zone you select, the Option dialog box varies.

**Master Zones**

- **Allow Zone Transfers.** When enabled, zone transfers will occur according to the method indicated by the radio buttons below. You must select at least one of these methods.
  - **To any server.** When selected, the zone transfer will be performed to any requester.
  - **Only to listed name servers in the zone.** When selected, the zone will be transferred from the server to any other name server listed in the zone.
  - **Only to the following servers.** When selected, the zone will only be transferred to the servers you specify in the list below. To enter a server, click in the first available row and enter its IP address.

- **Dynamic updates.** Specifies whether dynamic updates are allowed for the zone

- **AD Replication.** Displays a dialog box where you can set the AD Replication options for the zone.

- **Aging/Scavenging.** Displays a dialog box where aging and scavenging options can be set for the zone.

**Slave Zones**

- **Allow Zone Transfers.** When enabled, zone transfers will occur according to the method indicated by the radio buttons below. You must select at least one of these methods.
  - **To any server.** When selected, the zone transfer will be performed to any requester.
  - **Only to listed name servers in the zone.** When selected, the zone will be transferred from the server to any other name server listed in the zone.
  - **Only to the following servers.** When selected, the zone will only be transferred to the servers you specify in the list below. To enter a server, click in the first available row and enter its IP address.

- **IP addresses of master.** Type the IP address of the master servers for the zone.
Stub/Forward Zones

- Type the IP address of the master servers for the zone.

**BIND Servers**

The Zone Options dialog box lets you specify an IP Address (or an address block) from which zone transfers can be allowed, or disallowed.

The top section of the Options dialog box lets you designate the zone as either Static or Dynamic. Newly created zones are static by default, but can be changed to a dynamic zone (and vice versa) using this option. Refer to Appendix B for more information on dynamic zones versus static zones.

Addresses that have already been setup to handle (i.e., allow or disallow) zone transfers are listed in the lower area of the Zone Options dialog box. If you want to change the settings associated with an address that is already listed here, select it and click on the **Edit** button. To remove the access control completely, select it from the list and click the **Remove** button.

To specify a new address (or block) on which you want to implement access controls, do the following:

1. Click the **Add** button. A small dialog box displays, prompting you to enter the server's IP address, an address block, or to use one of the predefined names from the drop-down list (any, none, localhosts, localnets).
2. After entering the address, select either **Allow** or **Deny** to specify whether to permit or disallow access to/from this address.
3. Click **OK** to save the selection. The new address is now listed in the Zone Options dialog box.

**NOTE:** BIND uses journal files to keep track of changes to dynamic zones. The data in the journal files is merged with the zone data file at a designated interval. It is not possible to manually merge the data from the journal files to the zone data file. This means that if there is data in the zone's journal file when the zone type is changed to a static zone, the entries in the journal file will not be visible in the Management Console.
Slave Zones on BIND Servers

When a slave zone is hosted on a BIND server, the Options dialog box will look like the one below.

Besides being able to setup the access control (as described in the previous section), you can also specify the IP address of one or more master servers for the zone.

The master servers are specified in the lower half of the Zone Options dialog box. To add a new server to the list, simply click in the white space and enter the IP address of the master server you are assigning.

- To change the address of an existing server, click on it and make the desired edits.

Advanced Options

DNS Administrators can now access the BIND configuration files directly to edit DNS server and zone options that are not available in the GUI. Refer to Chapter 4: DNS Servers, Options, BIND Environment – Advanced Server Options for details.

Options For

If a zone exists on more than one server (e.g., in a master/slave configuration), it is possible to select the zone instance for which you want to set options.

1. Select the applicable zone.
2. From the menu bar, select Zone, Options for.
3. From the submenu, select the desired zone/zone instance (e.g., Master Zones only, Slave Zone only, etc.). The Zone Options dialog box displays.
4. Allow zone transfers. When selected, enables the zone transfer options.
   - To any server. When selected, the zone transfer will be performed to any requester.
   - Only to listed name servers in the zone. When selected, the zone will be transferred from the server to any other name server listed in the zone.
   - Only to the following servers. When selected, the zone will only be transferred to the servers you specify in the list below. To enter a server, click in the first available row and enter its IP address.
5. Dynamic Updates. Specifies whether dynamic updates are allowed for the zone.
6. Aging/Scavenging. Displays a dialog box where aging and scavenging options can be set for the zone.
7. When all selections/entries are made, click OK.
Promote Slave to Master

The Promote Zone feature makes it possible to change a slave zone to a master zone. This might be necessary in emergency situations, for example if the master zone becomes unavailable for an extended period of time. *This feature is only available for DNS Administrators.*

When a slave zone is promoted, the following actions are performed:

- The Men & Mice Suite checks whether the most recent copy of the zone is found in its internal database or on the server hosting the slave zone and uses the copy that is more recent.
- The server hosting the slave zone is configured so that the zone is saved as a master zone on the server.
- The zone history and access privileges from the old master zone are applied to the new master zone.
- The configurations of other instances of the slave zone are modified so that they will get the updates from the new master zone.

To promote a slave zone to a master zone, do the following:

1. Select the DNS server that contains the slave zone.
2. Right-click the slave zone you want to promote and, from the shortcut menu, select **Promote to master.** An information message displays:

   ![Information Message]

   *The zone test(zone1.test1.com) on server 2.win2003.autotest.devlab will be promoted from a slave zone into a master zone, the current master zone being on server 1.win2003.autotest.devlab. Are you sure you want to continue?*

   - Click **Yes** to continue, or **No** to discontinue the process.

Properties

Applies only when custom properties have been defined for DNS Zones. Selecting this menu item will display a dialog box where the custom property values can be modified.

1. In the Object browser, select the zone for which you want to manage properties.
2. From the menu bar, select **Zone, Properties.**
3. **Location.** Type the application location.
4. Click **Apply** or **OK.**

Reload

Sends a command to the DNS server instructing it to reload the zone data.
**Remove from Folder**

Allows you to remove a zone from a folder. *If you remove a zone from a folder, there is no way to undo this action.*

1. Highlight the zone you want to remove from a folder.
2. Right-click and select **Remove from folder**. The zone is removed from the folder.

**Search**

The Zone window contains a powerful search utility that allows you to search any or all fields in the zone for a particular keyword or numeric value.

1. In the Zone window toolbar, click the **Find** button. The Find in <zone name> dialog box displays.
   
   ![Find in testZone2.test4.com.on central.autotest.dev.lab.](image)

   - The first field (on the left) is a drop-down list. The default setting is **Any field**, which means that every field (i.e., column of data) in the zone is included in the search. If you select a specific field from this list, then only that column will be searched.
   - The middle field is a drop-down list that contains several Boolean operators you can use to further define and narrow your search. The default setting is **Contains**, which will find any occurrence of the search criterion, even if it is nested between other characters. Each operator has a corresponding inverse (e.g. **Does not contain**) that will search for everything but the criterion you entered.
   - The third field is where you enter the text or value you are searching for in this zone.
   - If you check the **Select all matches** checkbox, any records containing information that match the search criterion will automatically be selected. The selected records can then be operated on by other functions, such as Clear, Cut, Copy, Paste, Enable, and Disable. When this option is disabled, only the cell containing the current occurrence of the search criteria is selected.
   - To make your search case sensitive, check the **Case sensitive** checkbox. When checked, a search for ABC will not find fields that contain abc, aBC, AbC, etc.
   - If you check the **Wrap around** checkbox, when you use the Find Again command, the search will start again from the beginning of the zone instead of stopping at the end.
   - To initiate a search, click the **Find** button. The focus will shift to the first cell (or record) that meets the search criteria. If there is no matching information in the zone, a dialog box displays the message, "Nothing found."
   - Shortcut: You can instantly pull up the Find dialog box by pressing **Ctrl+Alt+F**. This will work in any screen where the search tool is available.
Slave Zone

Through this function, you create a slave zone.

1. In the Object List, right-click on DNS Zones and, from the shortcut menu, select New Slave Zone. The Create slave zone dialog box displays.
2. In the Zone name field, type the name for this slave zone.
3. In the Servers list, click all the servers to which this slave applies.
4. In the IP addresses of master servers, click in the field, and type the IP address of any master servers for this zone.
5. When all selections/entries are made, click Create. The new slave zone is created and displays in the Detail View of the main window.

Slave Server Assignments

Use the following procedure to assign a slave server to a particular zone so it will always work from the context of the zone.

1. In the Object Section, under DNS Servers, select the name server containing the zone to which you want to assign a slave server.
2. In the Object List, right-click on the zone to which you want to assign the slave server.
3. From the shortcut menu, select Add slave server.
4. Choose the desired slave server from the submenu that displays. That zone now displays as a slave on the server that was specified.

Stub Zone

Through this function, you create a stub zone.

1. In the Object List, right-click on DNS Zones and, from the shortcut menu, select New Stub Zone. The Create stub zone dialog box displays.
2. In the Zone name field, type the name for this stub zone.
3. In the Servers list, click all the servers to which this stub zone applies.
4. In the IP addresses of master servers, click in the field, and type the IP address of any master servers for this zone.
5. When all selections/entries are made, click Create. The new stub zone is created and displays in the Detail View of the main window.
**View History**

Opens the History window and displays a log of all changes that have been made to the zone, including the date and time of the change, the name of the user who made it, the actions performed, and any comments entered by the user. Refer to Management Console—Object Change History.

**Zone Wizard**

The Create Zone Wizard guides you step-by-step through the process of creating different types of zones, including new zones and reverse zones. In the Zone Wizard, you can have two options available:

- **Create New Zone**
- **Create or Update a Reverse Zone**. Within this wizard, there are options to Create a reverse zone(s) for all addresses, Create a reverse zone for a specific block, or Create a classless reverse zone.

To launch the wizard, do the following:

1. On the toolbar, click the **Wizard** button. This launches the New Zone Wizard. The Introduction screen of the wizard explains how the wizard works. Click **Next>**.
2. Complete each screen as you move through the wizard.
Chapter 6: DNS Resource Records

Overview

Each zone contains DNS resource records that define how requests are processed or delegated by the zone. The Zone Window provides a spreadsheet-like interface that makes it easy to view, edit, and manipulate information within a zone.

Types of Resource Records

There are varieties of resource records that actively affect zones, as well as several informational records that can be used to provide supporting data about a zone. The primary record types are described in the table below.

<table>
<thead>
<tr>
<th>Record Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS</td>
<td>The Name Server record is used to list a name server for this zone. NS records state the domain name of the zone’s name servers. The name of an NS record is the fully qualified domain name of a zone. Every zone must have at least one NS record with the same name as the zone itself.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
</tr>
<tr>
<td>example.com</td>
<td>NS</td>
</tr>
<tr>
<td>example.com</td>
<td>NS</td>
</tr>
<tr>
<td>example.com</td>
<td>NS</td>
</tr>
<tr>
<td>sub.example.zone.com</td>
<td>NS</td>
</tr>
<tr>
<td>ns1.sub.example.zone.com</td>
<td>A</td>
</tr>
<tr>
<td>tcp.example.zone.com</td>
<td>SRV</td>
</tr>
<tr>
<td>server.example.zone.com</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>Also known as an Address record, an A record declares the IP address of a domain name. Defines a Hostname-to-IP Address mapping, or a forward mapping.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
</tr>
<tr>
<td>example.com</td>
<td>A</td>
</tr>
<tr>
<td>PTR</td>
<td>Also known as Pointer records, PTR records define an IP Address-to-Hostname mapping, known as a reverse mapping. A properly configured reverse zone has one PTR record providing the reverse lookup for each IP address. All reverse zones are traditionally part of the .in-addr.arpa. zone. The proper formatting for a PTR record is the 4 octets of the IP address in reverse order, followed by .in-addr.arpa. A properly formatted PTR record for the A record (above) is shown in the following example. In the event that you have multiple A records concerning the same IP address, choose one for the PTR record. If one of the host names is used for a mail server, give that hostname preference because a common use of reverse lookup is to check the source of e-mail.</td>
</tr>
</tbody>
</table>
### Record Type | Description
--- | ---
**Example:** | Name | Type | Data |
--- | --- | --- | --- |
PTR | 1.0.168.192.in-addr.arpa. | PTR | example.com. |
**CNAME** | Canonical Name records are used to define an alias. The canonical or primary DNS domain name used in the data is required and must resolve to a valid DNS domain name in the namespace. The name of the record is the name of the alias. Thus, if you want www.example.com to bring visitors to example.com, you’d need to add the line shown in following example: | Name | Type | Data |
--- | --- | --- | --- |
**MX** | Also known as Mail Exchange records, MX records create mail routes. Each exchanger host must have a corresponding host (A) address resource record in a valid zone. The first field in the record data is the preference number; this is the order in which mail hosts will be used by an outside mail server trying to send mail to a domain. Mail hosts will be contacted from the lowest preference number and work up to higher preference number. If two MX records have the same preference number, they will be used in random order. Mail servers with the same preference number will not forward to each other, nor will they forward to a mail server with a higher preference number. | Name | Type | Data |
--- | --- | --- | --- |
MX | example.com. | MX | 10 mail.example.com. |
**AAAA** | Maps a DNS domain name to an Internet Protocol (IP) version 6 128-bit address. | Name | Type | Data |
--- | --- | --- | --- |
AAAA | host.example.com. | AAAA | 43210:1:2:3:4:567:89ab |
**WKS** | Similar in function to MX records, Well-Known Service (WKS) records describe the well-known IP services supported by a particular protocol on a specific IP address. They provide TCP and UDP availability information for IP servers. Multiple WKS records should be used for servers that support both TCP and UDP for a well-known service or that have multiple IP addresses that support a service. Three fields of data are required: IP address, protocol, and a service list. | Name | Type | Data |
--- | --- | --- | --- |
WKS | host.example.com. | WKS | 10.0.0.1 TCP (ftp smtp telnet) |
**RP** | The Responsible Person record specifies the domain mailbox name for the person responsible for that domain. This name is then mapped to a domain name in for which (TXT) resource records exist in the same zone. When RP records are used in DNS queries, subsequent queries are used to retrieve associated text (TXT) resource record information. Two fields of data are required: the domain name you are searching, the domain where TXT resource records exist. | Name | Type | Data |
--- | --- | --- | --- |
RP | my.example.com. | RP | who.example.com |
| | | | txtrec.example.com |
**AFSDB** | The Andrew File System Database resource record maps a DNS domain name to the host name for a server computer of a server subtype. Two fields of data are required: The first is a subtype, which can have one of two supported numeric values: A 1 indicates that the server is an AFS version 3.0 volume location server for the named AFS cell. A 2 indicates that the server is an authenticated name server holding the cell-root directory node for the server that uses either Open Software Foundation's (OSF) DCE authenticated cell-naming system or HP/Apollo's Network Computing Architecture (NCA). The second field is the server’s host name. | Name | Type | Data |
--- | --- | --- | --- |
AFSDB | | | |
### Record Type Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
</table>

**Example:**

| abc.example.com. | AFSDB | 1 afs-server.example.com. |

**SRV**

Service records are intended to provide information on available services. They allow multiple servers providing a similar TCP/IP-based service to be located using a single DNS query operation.

An SRV record has four fields and a special system for naming. The naming system is an underscore followed by the name of the service, followed by a period, an underscore, and then the protocol (generally TCP or UDP), another dot, and then the name of the domain. The four fields are:

- **Priority.** Used the same way as the preference number in MX records.
- **Weight.** This determines the relative capacity between SRV fields with the same priority. Hits will be assigned proportionately by weight, allowing a powerful and a weak server to share appropriate loads.
- **Port.** The port of the service offered.
- **Hostname.** The name of the domain.

**Example:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
</table>


**HINFO**

The Host information resource record specifies the type of CPU and operating system, respectively, for the host DNS domain name. This information is used by some application protocols, such as FTP, which use special procedures when communicating with computers of a known CPU and operating system type.

Hardware information belongs in the first data field and OS information in the second field, as shown in the example below.

**Example:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
</table>

| compname.example.com. | HINFO | Intel-PIII WIN2K |

**TXT**

A Text Record allows you to include up to 255 characters of free-form descriptive text in your zone file. The order of resource records in zone files is not preserved, so it is best to keep messages confined to one record.

**Example:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
</table>

| random.example.com. | TXT | The quick brown fox jumped over the lazy dog. |

**LOC**

Geographic Location Records provide exact altitude, latitude, and longitude information. There is not much in the way of a practical application for this record, though some industries may find it to be of limited value. The LOC record can accept as few as three or as many as six fields of data:

- Degrees latitude in degrees, minutes, seconds, N or S.
- Degrees longitude in degrees, minutes, seconds, E or W.
- Altitude in meters. This is single value, you may add an M.
- Size of machine in terms of an enclosing sphere in meters radius. Expressed as a number, or a number immediately followed by an M. (Optional.)
- Horizontal precision of the data in meters, with or without an M. (Optional, not available if 4 is blank.)
- Vertical precision of data in meters, with or without an M. (Optional, not available if 5 is blank.)

**NOTE:** The Microsoft DNS server does not support LOC records.

**Example:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
</table>

| geo.example.com. | LOC | 42 21 43.528 N 71 05 06.284 W 12m |
### NAPTR

NAPTR stands for Naming Authority Pointer and is a resource record type that supports regular expression based rewriting. The NAPTR record accepts six fields of data:

- **Preference.** When there are multiple NAPTR records with the same name, the record with the lowest preference number is picked first.
- **Weight (Order).** This field specifies the order in which the NAPTR records MUST be processed to accurately represent the ordered list of Rules. This field is only used when there is more than one record with the same preference.
- **Flags.** This field contains flags to control aspects of the rewriting and interpretation of the fields in the record. Flags are single characters from the set A-Z and 0-9.
- **Service.** This field contains a character-string that specifies the Service Parameters applicable to this delegation path.
- **Regexp.** This field contains a character-string that contains a substitution expression that is applied to the original string held by the client in order to construct the next domain name to lookup.
- **Replacement.** This field contains a domain name, which is the next domain name to query for, depending on the potential values found in the flags field.

**Example:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>104</td>
<td>NAPTR</td>
<td>100 10 u sip+E2U !^.*$!sip:<a href="mailto:info@info.example.test">info@info.example.test</a>!i .</td>
</tr>
</tbody>
</table>

### SSHFP

SSHFP stands for SSH Public Key Fingerprint. This resource record type is used for publishing SSH public host key fingerprints in the DNS System, in order to aid in verifying the authenticity of the host. The SSHFP record accepts 3 fields of data:

- **Algorithm.** Specifies the algorithm number to use.
- **Fingerprint type.** Specifies the fingerprint type to use.
- **Fingerprint.** The fingerprint for the record.

For further information on this record type, see RFC 4255

**Example:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>random.example.com</td>
<td>SSHFP</td>
<td>1 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>23D3C516AAF4C8E867D0A2968B2EB999 B3168216</td>
</tr>
</tbody>
</table>

### SPF

SPF stands for Sender Policy Framework. This record type is used in an e-mail validation system designed to prevent e-mail spam. The SPF record accepts a text string that contains the configuration info that should be used.

For further information on this record type, see RFC 4408

**Example:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com</td>
<td>SPF</td>
<td>v=spf1 a mx -all</td>
</tr>
</tbody>
</table>

In addition to the supported record types in the table, the Men & Mice Suite supports the following DNSSEC resource record types:

- DNSKEY
- NSEC
- NSEC3
- NSEC3PARAM
- RRSIG
- DS
- DLV

**NOTE:** All DNSSEC specific record types, with the exception of the DS and NSEC3PARAM record types, are read only.
It is beyond the scope of this documentation to discuss DNSSEC management so these record types are not explained in detail. For further information on these resource record types and DNSSEC in general, we recommend the DNS Extensions section on the IETF web site (http://www.ietf.org/html.charters/dnsext-charter.html).

### Resource Records

To select a single resource record, do the following:

- Click on the gray square to the left of the record. This highlights the entire record.

Once a record is selected, you can perform various editing actions on it, such as deleting, cutting, or copying. These are discussed in more detail later in this section. Many editing action can be performed on multiple records simultaneously. Simply select the records you want to operate on and perform the editing action as usual.

To select non-consecutive records, do the following:

- Hold down the Ctrl key and select each record as usual.
- When you are done selecting records, release the Ctrl key.

#### New Records

If you are comfortable editing the record table directly, you can use this procedure to insert a new record directly in the zone window. If you need assistance creating basic resource records (A, NS, CNAME, or MX), consider using the Create Record Wizard.

1. Open the Zone window to display the resource records in the zone you want to edit.
2. In the record table, select the record that is directly above where you want to insert the new record. To select a record, click on the square block to the left of the Name column.
3. Right-click anywhere in the selected record and, from the shortcut menu, select Insert Record. A new, blank record is added.
4. Starting with the Name field, enter the domain name. **NOTE:** If you enter a domain name that is not fully qualified (i.e., does not end in a dot). The program will assume that you are using a local name and will automatically append the name of the zone onto the end of the name, making it a fully qualified domain name. That means when adding the name server ns1 to the zone example.com, you should enter either just ns1 or ns1.example.com. If you leave off the period at the end, the program will interpret your intention as ns1.example.com.example.com. The information automatically filled in by the Management Console appears in grey.
5. Press the Tab key to advance the focus to the Type field.
6. Enter the appropriate type classification. The following types of resource records can be created: NS, A, PTR, CNAME, MX, AAAA, WKS, RP, AFSDB, SRV, HINFO, TXT, and NAPTR. The appropriate number of fields is automatically created in the Data field based on the type you entered.

   If you enter the wrong record type, you will be unable to change it. You must delete the record, insert a new one, and re-enter the record information.

7. Press the Tab key to advance the focus to the Data field.

8. Enter the appropriate data for your record type.

9. Click the Save button to save the new record to the zone.

10. An exclamation mark displays at the left edge of a record that is incomplete or improperly entered. The program will not allow you to save the changes to this zone until the record is repaired. Move to the lower right corner of the window and click the exclamation point icon. This expands the window and shows the items in error:

11. Double-click on the error message and it will jump to the record in question.

---

### Create Record Wizard

The Create Record Wizard guides you step-by-step through the process of creating a particular type of resource record.

Within the Create Record Wizard, you have the following options:

- Adding a New Computer to the Zone
- Creating an Alias for an Existing Computer
- Add a New Name Server
- Creating a Mail Route

To launch the Wizard, do the following:

12. In the Management Console, display the DNS zones, and then double-click on the zone you want to edit. This opens the Zone window for that zone.

13. On the Zone toolbar, click the Wizard button. The Create Record Wizard launches. The Introduction screen of the wizard explains how the wizard works. Click Next.

14. For each of the resulting screens, make a selection/entry and move through the wizard.
Deleting Records
Deleting a record removes both the data and the physical record from the Zone window. Records beneath the deleted one are instantly moved up to fill in the space.

1. Select the record(s) that you want to delete. To select multiple records, hold down the Ctrl key while making your selections.
2. Right-click anywhere in the zone window, and select Delete Record from the context menu. The record is immediately deleted from the zone.

Clearing Records
When the whole record is selected, the Clear command works the same as the Delete Record command. The Clear command is really intended for deleting the contents of an individual field of data, leaving the rest of the record's data intact.

1. In the Zone window, select the field (cell) whose contents you want to delete.
2. Right-click anywhere in the zone window and select Clear from the context menu. The data is removed from the field. (The cell is not removed, and the rest of the record is unaffected.)

Disable/Enable Records in the Zone Window
You can disable a record without deleting it. The disabled record performs no function; however, it can be instantly enabled when its services are needed, without having to re-type the record.

**NOTE:** You cannot disable and enable records in dynamic zones.

**How to Disable a Record**

1. In the Zone window, select the record(s) that you want to disable. To select more than one record, hold down the Ctrl key while making your selections.
2. Right-click anywhere in the zone window and select Disable Record. Disabled records are grayed out in the Zone window.

3. In the toolbar, click the Save button to save the changes to the zone.

**How to Re-Enable a Record**

1. Select the disabled record(s) that you want to re-activate. To select multiple records at once, hold down the Ctrl key while making your selections.
2. Right-click anywhere in the zone window and select Enable Record.
3. In the toolbar, click the Save button to save the changes to the zone.
Cut, Copy, and Paste

When working with records in the Management Console, there is no need to enter the same records in different zones. All records can be copied (or moved) to other zones simply by copying and pasting them between different zone windows.

To facilitate this, the Copy and Paste functions do not use fully qualified host names, so it is easy to work with records between zones.

This means that if you copy a record from the domain example.com, such as:


and paste the record to sample.com, it displays as:


To cut, copy, and paste records, do the following:

1. Select the record(s) that you want to move or copy. To select multiple records, hold down the Ctrl key while making your selections.
2. Right-click anywhere in the Zone window and choose either Cut (to move the record) or Copy (to duplicate the record elsewhere) from the context menu.

   NOTE: The Cut, Copy, Paste, and Clear commands can also be selected from the Edit menu in the main window.

3. Open the destination zone in which you want to insert the record(s).
4. In the destination zone, insert a new blank record in the location where you want to paste the records. To do this, right-click on the record immediately above where you want to paste the new one(s), then select Insert Record from the popup menu.
5. Select the blank record.
6. Right-click anywhere in the Zone window and choose Paste from the context menu. The new record(s) are pasted in the destination zone.

Undo/Redo Commands

The Management Console allows you to undo most editing actions, such as deleting, clearing, cutting, and pasting.

When you perform an editing action, the Edit menu’s Undo command is modified to include that action. For example, if you disable a record, the Undo command changes to Undo Disable. Selecting this command will reverse the action and restore the previously deleted record.

When you perform an Undo action, the Redo command becomes active. Selecting this command reverses the previous Undo action.

If you perform multiple editing actions in a row, the Undo command can be used repeatedly to restore each prior action.
Chapter 7: IP Address Management

Overview

Managing IP addresses entails being able to create assignable ranges within the available address space and determining which users and groups have usage rights to that space. The IP ranges can be created with specific properties that also determine the properties of the IP addresses contained within them.

**NOTE:** In order to use the IP Address Management features in the Men & Mice Management Console, you must have entered the license key for the IPAM module.

Address (A) Records in DNS Zone Windows

When the IP Address management component is enabled, you may notice some differences when working with Address (A) records in DNS zone windows, such as:

- **Restriction on allowed IP addresses.** When IPAM is enabled, the system administrator may restrict which IP addresses you are allowed to use. The system administrator can determine an IP address range that you are allowed to work with. In addition, he/she can choose whether you can use an IP address that has already been assigned in DNS.

- **Automatic assignment of IP addresses.** The system administrator can configure the Men & Mice Suite so that you can create address (A) records without entering IP addresses. When the zone is saved, the IP addresses are automatically assigned using free IP addresses in your IP address range. If you want to enter an IP address manually, you can type it in the IP address field, but if you leave the field unchanged, the IP address will be automatically assigned when you save the zone. If you have access to more than one IP address range, a dialog box will be displayed at save time where you can choose the IP address range for your new address records.

Range Access

*Refer to Administration Functions—Global Access/Access Control.*

Viewing IP Address Ranges

The IP Address Range provides a view that shows the section of the IP address space that is accessible to the current user of the system. The Men & Mice Suite allows administrators to manage the IP Address space by dividing it into any number of named sub ranges that can be assigned to specific groups for use by its members.

- In the Object Section, click on **IP Address Ranges.** This shows the name of each IP range that has been created (and the address range it represents) and accessible to the current user.
As indicated by the icons there are two types of ranges listed:

- The icon indicates a user-created range. Any range you create is considered a user-created range.
- The icon represents a DHCP scope, created in the DHCP Scopes area of the Management Console.

You can choose between a flat and a hierarchical view for the Address Ranges scopes by selecting an appropriate button from the toolbar.

You can also toggle between the views by selecting **Toggle Hierarchical View** from the **Range** menu.

The IP Address Range view can display an indicator to show which gaps between IP address ranges. This view is useful if you are looking for free segments in a fragmented IP address space. When active, the view will display a thin blue line below a range if there is unallocated space between that range and the next range in the address space. To display the indicator, choose **Show Trailing Gaps** from the **Range** menu.

While viewing the IP address ranges, the Quick Filter is available. When using the tree view while a filter is active, any parent ranges that don’t fulfill the search criteria are displayed in gray to distinguish them from the found ranges. For example, in the image below, we searched for the string ‘0/26’ and the only range found was ‘10.1.0.0/26’. However, to maintain the tree view, the parent ranges are shown even if they don’t fulfill the search criteria.

### New Ranges

To create a new IP address range, do the following:

1. Make sure that IP Address Ranges is selected in the left hand side of the Manager window.
2. Click the **Add** button. The Properties dialog box displays. *See IP Address Management - Configuration.*
3. Enter the appropriate values in the Properties dialog box and click **OK**.

Once a non-reserved IP address range has been created, it is considered to be managed. A managed IP address range is being managed by the IP address component of the Men & Mice Suite. When the range is managed, the Men & Mice Suite will allow users with appropriate privileges to work with IP addresses from the range.

It is possible to create subranges of existing ranges and DHCP scopes. **NOTE:** When you create a new IP address range, the Men & Mice Suite checks to see if the new range can be logically grouped with other address ranges, and adds the new range in the appropriate address range group.
Range Configuration

When configuring a new IP Address range, you must complete the Properties dialog box.

1. In the Object list, right-click and, from the shortcut menu, select New IP Address Range. The New Range Properties dialog box displays.

   ![Create IP Address Range dialog box]

2. **Subnet.** For IPv4 ranges you can enter the address range in a network/subnet notation, for example 192.168.1/24. You can also enter the address range using a from-to notation, for example 192.168.1.23-192.168.1.77. A range does not have to be defined on network boundaries. For IPv6 ranges you must enter the range in a network/subnet notation and the smallest network you can create is a /64. The actual range displays in the Usable IP addresses field below.

   The network address and the broadcast address for the range are displayed below the Usable IP addresses if the Range is a subnet checkbox is selected. **NOTE:** The boundaries of IP existing address ranges may not overlap.

3. **Title.** Type the name you want to use for this IP address range. This name is for your convenience, so feel free to use whatever name you feel is appropriate.

4. **Description.** Enter a comment for this IP address range.

5. **Reserve Network and Broadcast Address.** This checkbox determines whether the user can use the first and last IP address of the range when creating address records. If the address range is defined on actual network boundaries, you should leave this checkbox checked. If the address range you are defining is used for Administration boundaries rather than network boundaries, you should clear this checkbox. **NOTE:** This checkbox is disabled for IPv6 ranges.

6. **Locked.** Select this checkbox if you want to lock this IP address range. When an IP address range is locked, Men & Mice Suite will not allow using IP addresses from that range. This is useful if you want to lock a certain section of your IP address block.

7. **Allow auto-assignment of IP Addresses.** Select this checkbox if you want to allow automatically assigned IP addresses from this IP address range. If the checkbox is selected, and a user that has access to this address range creates an address record without entering an IP address, Men & Mice Suite automatically assigns a free IP address to the address record. **NOTE:** This checkbox is disabled for IPv6 ranges.
Range Modifications

Once you have created an IP Address Range, it is easy for you to make changes to that IP Address Range. You can do the following:

- Change the name of the IP address range
- Change the boundaries (start and end IP address) of the IP address range
- Change the state of the IP addresses in that IP address range

To modify an IP address range, do the following:

1. Right-click on the IP address ranges.
2. From the shortcut menu, select Properties.
3. Make the desired changes.
4. Click OK.

Range Deletions

You can always delete an IP Address Range definition. If you delete an IP Address Range, the IP addresses that belonged to that range will get the attributes of the parent IP Address Range. If the range you are deleting has subranges, the subranges will become children of the unassigned ranges’ parent.

Use the following procedure to delete an IP Address Range definition:

1. Locate the IP Address Range you want to remove and right-click on it.
2. From the shortcut menu, select Delete. A dialog prompts you to confirm your decision to delete this range
3. Click OK to delete the range, or Cancel to leave it.

IP Address List

To view a list of host entries in a particular range, double-click on the IP Address Range. This opens the IP Address List Window where you can view and edit the properties of individual host entries.

- The Show unassigned addresses checkbox lets you choose whether you want to see all IP addresses in the range or whether you only want to show IP addresses that are assigned.
- The PTR Status column shows the status of the Address (A) record and Pointer (PTR) record mappings. This column can have three values:
  - Empty. The status is empty if there are no DNS records for the host. It is also empty if a PTR record exists where the domain in the data section of the PTR record is not managed by the system.
• **OK.** If there is a match between the A and the corresponding PTR record(s) the status is listed as **OK.**

• **Verify.** If there is not a match between the A and the PTR records for the host, the status is listed as **Verify.** The most common reasons are:
  - There is an A record but the PTR record is missing.
  - There is a PTR record but the A record is missing.
  - The data section in the PTR record does not correspond to the name of the A record.

When the PTR Status for a host entry shows Verify, you can open the Device Dialog box for the host to see more detailed information on which DNS host entry is generating this status message.

**NOTE:** When working with large IP Address ranges (ranges that contain more than 4096 IP Addresses) the **Show unassigned addresses** will no longer be available and the IP Address List window will only display assigned IP addresses.

### Device Dialog Box

When you add or modify an existing entry, the Device Dialog box displays. The entries in this dialog box can vary, depending on the license keys in use, whether the dialog box is accessed from a DHCP scope or an IP Address range, and if any custom properties have been defined (e.g., “Owner” is a custom property in the example shown below).

**Device 10.5.2.10**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
<th>PTR</th>
</tr>
</thead>
<tbody>
<tr>
<td>rec509.testZone2.test4.com</td>
<td>A</td>
<td>10.5.2.10</td>
<td>OK</td>
</tr>
<tr>
<td>...</td>
<td>AAAA</td>
<td>::2</td>
<td></td>
</tr>
</tbody>
</table>

- **DNS Hosts.** If a DNS license key is active, the Device dialog box will contain a DNS Hosts section where you can enter Address (A) records and related CNAME and TXT records. You can also add, edit, and remove hosts/related hosts from this screen. Refer to the Adding a DNS Host/Related DNS Host, Editing a DNS Host/Related DNS Host, and Removing a DNS Host/Related DNS Host. The **PTR** column in the list of DNS hosts shows the PTR status for each A or AAAA record. For more information on PTR status see the **IP Address List** section, above.
• If a discovery schedule has been set for the subnet, the dialog box will show information on when the device was last seen on the network:
  − **Last seen.** Shows the last time this IP address was seen. *This information cannot be edited.*
  − **Last ping.** Shows the last time this IP address was pinged. *This information cannot be edited.*

### Adding a DNS Host
As a shortcut, you can select a valid host name in any field, right-click and select Add Host. The host is automatically added.

1. While viewing the Device dialog box, move to the DNS Hosts section, and click the **Add** button. The Add Host dialog box displays.

   ![Add Host dialog box](image)

   **NOTE:** If the number of available zones does not exceed 100, the Zone area of the window will be a drop-down list instead of the **Browse** button.

2. In the **Zone** field, verify the zone selected is the zone to which you want to add a host. If not, click the **Browse** button. The Select zone dialog box displays, reflecting a list of available zones.

   ![Select zone dialog box](image)

3. If desired, use the **Quick filter** to search for the desired item.
4. Highlight the desired item, and click **Select**.
5. When you return to the Add Host dialog box, the selected item is shown under the **Zone** heading.
6. In the **Name** field, type the host name.
7. Click **OK**. The dialog box closes and the Address record displays in the Device dialog box.
**Editing a DNS Host**

1. Select the host details you want to edit.
2. Double click the host entry you want to edit. A dialog box displays.
3. Make the desired changes and click **OK**. The dialog box closes and the details are updated.

**Removing a DNS Host**

1. Select the host you want to remove.
2. Click **Remove**. The host details are deleted and removed from the list in the Device dialog box.

**Adding a Related Host**

1. Click **Add Related** button. The Add Related Record dialog box displays.

   ![Add Related Record](image)

2. For the **Name** and **Zone** fields, refer to the steps found for “Adding a Host,” above.
3. In the **Type** field, click the drop-down list and select the record type.
   - If the record type is **CNAME**, in the **Zone** field, choose the zone that should contain the record.
   - If the record type is **TXT**, in the **Data** field, type the text for the record.
4. Click **OK**. The dialog box closes and the related record displays in the Device dialog box.

**Editing a Related Host**

1. Double click the related host you want to edit. The Modify Host dialog box displays. **NOTE**: It is not possible to edit all record types.

   ![Modify Related Record](image)

2. Make the desired changes and click **OK**. The dialog box closes and the record is updated.

**Removing a Related Host**

1. Select the related record you want to remove.
2. Click **Remove**. The related record is deleted from the zone and removed from the list in the Device dialog box.
Moving a Device

A device can be moved to a new IP address. When the device is moved, all information about the device is retained, and the associated DNS records are updated.

To move a device, do the following:

1. Locate the IP Address Range containing the device you want to move.
2. Double-click on it to display the list window.
3. Find the applicable device.
4. Right-click and, from the shortcut menu, select **Move**.
5. In the **Move Device to New IP Address** dialog box, type the new IP address.
6. Click **OK**. The device is moved to the new IP address.

Split Range Wizard

This wizard allows you to create multiple subranges of an existing range. The wizard can only be used on ranges that exist on subnet boundaries and have no subranges already in place.

1. From the object list, click on **IP Address Ranges**.
2. From the list of ranges displayed right-click and, from the shortcut menu, select **Split into Subranges**. The Split range wizard displays.
3. For each of the resulting screens, make a selection/entry and move through the wizard.

Generate Reverse Zones Wizard

This wizard allows you to create reverse DNS zones for selected ranges. The wizard can only be used on ranges that exist on subnet boundaries and contain 254 or more IP addresses (/24 or larger)

1. From the object list, click on **IP Address Ranges**.
2. From the list of ranges displayed, select the ranges, right-click and, from the shortcut menu, select **Generate Reverse Zone(s)**. The Reverse zone generation wizard displays.
3. For each of the resulting screens, make a selection/entry and move through the wizard.
Allocate Ranges Wizard

This wizard allows you to create allocate a user-defined number of subranges from an existing range. The wizard can only be used on ranges that exist on subnet.

1. From the object list, click on IP Address Ranges.
2. From the list of ranges displayed right-click and, from the shortcut menu, select Allocate Ranges. The Allocate ranges wizard displays.
3. Follow the instructions provided by the wizard to create the number of subranges that you need.

Join Ranges

This function allows you to select and join a number of ranges. The Join Ranges command is available if the selected ranges can be joined.

1. Display the list of address ranges that you want to join.
2. Select each of the desired ranges.
3. Right-click and, from the shortcut menu, select Join Ranges.

The Join Ranges dialog box displays.

4. Use Access. Click the drop-down list and specify from which range you will gain access.
5. Use Properties. Click the drop-down list and specify from which range you will use the properties.
6. Title. Enter a title for this range.
7. Description. Type a description.

8. Click Join.
Select Parent

This function allows you to view the hierarchy for subnets when filtering is active.

1. Locate the subrange for which you want to view the hierarchy.
2. Right-click on the subrange and, from the shortcut menu, selects Parent. All available parent(s) are shown.
3. Click on the parent and the system automatically moves you to that parent range.

Host Discovery

With this feature, you can see when hosts were last seen on your network. There are two methods you can use for host discovery – using ping or querying routers for host information.

Configuring Host Discovery Using Ping

1. Select one or more IP Address Ranges.
2. Right-click and, from the shortcut menu, select Set Discovery Schedule. The Schedule dialog box displays.
3. Select the Enable discovery schedule option.
4. Schedule ____ every ____ day(s)/week(s)/month(s). Click the drop-down list and select the frequency (e.g., Daily, Weekly, etc.) and the occurrences (e.g., 1 day, 2 weeks, etc.).
5. At ___. Enter the time at which discovery should take place.
6. Starting ___. Click the drop-down list and select the start date.
7. Click OK.

Once the schedule options have been set and saved, a new column called, Last seen, identifies when a host last was last seen on the network.
• **Green.** Host responded to the last PING request. The date and time are shown.

• **Orange.** Host has responded in the past, but did not respond to the last PING request. The date and time of last response is shown.

• **Red.** Host has never responded to a PING request. The text *Never* is shown.

The list of ranges contains a column that shows if a discovery schedule has been set for a range. The name of this column is **Schedule**. To quickly see all ranges that have a schedule set, you can use the Quick Filter and filter by this column by entering **Schedule:Yes** in the Quick Filter search field.

At any time if you wish to **disable** host discovery, do the following:

1. Select the object(s) for which you want to disable discovery.
2. Right-click and, from the shortcut menu, select **Set Discovery Schedule**. The Schedule dialog box displays.
3. Uncheck the **Enable discovery schedule** option.
4. Click **OK**.

### Configuring Host Discovery by Querying Routers

To collect information about hosts by querying routers, you must first enable collection of IP information from routers. *See Monitoring in Chapter 2 for more information.*

To configure host discovery, do the following:

1. Select an IP Address Range.
2. Right-click and, from the shortcut menu, select **Configure IP Address Collection**. The IP Address Collection dialog box displays.
3. Enter the IP address of the router(s) that you want to use to collect information about hosts in the range.
4. Click **OK**.

### Remove from Folder

Removes the currently selected IP Address Range from the current folder. Once you remove a range, there is no “undo” option available.

1. Highlight the range you want to remove.
2. Right-click and, from the shortcut menu, select **Remove from Folder**. The range is removed.
Subnet Monitoring

The Subnet Monitoring is used to monitor the free addresses in subnets and DHCP address pools and perform an action if the number of free addresses goes below a user-definable threshold.

When Subnet Monitoring is enabled a global monitoring setting is applied to all subnets in the system. For information on how to enable the Subnet Monitoring feature, see the Monitoring section in chapter 3. You can change the subnet monitoring settings for individual subnets and scopes, for example if you want to disable monitoring for a certain subnet or if you want to use a different threshold for the free addresses in a DHCP scope. NOTE: Only DHCP scopes that are enabled are monitored. Disabled scopes are ignored.

Set Subnet Monitoring

To change the monitoring settings for a subnet:

1. Select the subnet(s) for which you want to change the monitoring setting.
2. Right-click and, from the shortcut menu, select Set Subnet Monitoring. The Subnet Monitoring dialog box displays.
3. Enabled. When checked, the subnet will be monitored.
4. Script to invoke. Enter the path of the script to run when the number of free addresses goes below the set threshold. See Appendix G, External Scripts, for information on the script interface and the format for calling the script.
5. E-mail addresses. Enter one or more e-mail addresses. An e-mail will be sent to the specified addresses when the number of free addresses goes below the set threshold.
6. Dynamic Threshold. Enter the threshold for the free addresses in a DHCP scope address pool. NOTE: For split scopes and scopes in a superscope (on MS DHCP servers) and address pools using the shared-network feature on ISC DHCP servers, the total number of free addresses in all of the scope instances is used when calculating the number of free addresses.
7. Static Threshold. Enter the threshold for the free addresses in a subnet.
8. Only perform action once (until fixed). When checked, the action is performed only once when the number of free addresses goes below the threshold.
9. Perform action when fixed. When checked, the action is performed when the number of free addresses is no longer below the threshold.
10. Click OK to confirm your settings.

Removing Subnet Monitoring

You can clear the monitor setting for individual subnets if you want to use the global subnet monitoring setting. To clear a monitoring setting for a subnet:

1. Select the subnet(s) for which you want to clear the monitoring setting.
2. Right-click and, from the shortcut menu, select Remove Subnet Monitoring. The custom subnet monitoring setting is removed and the global monitoring setting is used instead.
Multiple Address Spaces

The Men & Mice Suite supports multiple address spaces. Each address space instance contains its own set of DNS servers, DNS zones, DHCP servers, DHCP scopes, IP address ranges (including the IPv4 and IPv6 root ranges), IP address entries and object folders. Changes to data in one address space do not affect data in any other address space.

Items shared between address spaces are the user and group lists and custom property definitions.

Address Space Management

The Address Space Management dialog box allows you to create, modify or delete address spaces as well as set access privileges for existing address spaces. To access the Address Space Management dialog box, you must be logged in as the administrator user.

- To open the Address Space Management dialog box, from the Tools menu, select Define Address Spaces.

- To create a new address space, click the Add button and enter the name and description for the address space.

  NOTE: When more than one address space is defined, the first address space will be named <default>. It is not possible to rename or delete the <default> address space. Also, the <default> address space is the only address space that shows AD sites if AD Site and Subnet integration is enabled.

  NOTE: When a new address space is created, you must set the access for the address space to allow users to access it. When creating your first address space, two address spaces will actually be created, the <default> address space and the address space you created. You must set access for the <default> address space as well as for the new address space.

- To change the name or description for an address space, select the address space and click the Edit button.

- To delete an address space, select the address space and click the Delete button.

  NOTE: When you delete an address space, all objects contained within the address space are removed (DNS servers, DHCP servers, IP Address ranges, IP address entries and folders). This action is not undoable.

  NOTE: You cannot delete the <default> address space or the address space you are currently working in.

- To set access privileges for an address space, select the address space and click the Access button.
Switching to a Different Address Space

You can only work in one address space at a time. You can see the current address space in the Manager window, above the object list.

To switch to a different address space:

1. Select the **IP Address Ranges** object in the object list in the Manager window.
2. Select **Ranges -> Switch Current Address Space**. A dialog box listing all available address spaces displays.
3. Select the address space you want to switch to and click the OK button.

Moving Objects to a Different Address Space

DNS servers, DHCP servers, IP address ranges and individual IP address entries can be moved between address spaces. When an object is moved between address spaces, all properties for the object are retained, including its access settings and change history. You must have the relevant administrator privileges to move objects to a different address space.

**NOTE:** You cannot move folders between address spaces. Individual DHCP scopes cannot be moved between address spaces, but when you move a DHCP server to a different address space, all of its DHCP scopes are moved as well. Likewise, you cannot move individual DNS zones to a different address space, but moving a DNS server to a different address space will move all of its zones as well.
Chapter 8: AD Sites and Subnets

Overview

With this feature, it is possible to integrate Active Directory (AD) sites in the Men & Mice Suite, view subnets within these sites and add, remove and move subnets between the sites.

For information on how to enable the Sites and Subnets integration feature, see the Sites and Subnets section in chapter 3.

Once Sites and Subnets integration has been enabled, an AD Sites object displays in the object list on the left hand side of the Manager window and a new column, AD Site displays in the range list in the Manager window.

A few things to note:

• This feature is only available if Men & Mice Central is running on a Windows machine.

• You can configure the system to view sites and subnets from multiple AD forests.

• If you are using multiple address spaces, you will only be able to view AD Sites in the Default address space.

• To add/remove a subnet to/from a site, the user must have the Can edit range properties flag set for the subnet.

Adding an AD Forest

To manage sites and subnets, you must first add the AD forest. **NOTE:** You can manage sites and subnets from multiple forests.

1. In the Object Browser, right-click on the AD Sites object category.
2. From the shortcut menu, select Add AD Forest. A dialog box displays.

   ![Add AD Forest Dialog Box]

   3. **Use same Global Catalog as the Men and Mice Central server.** If checked, the Men & Mice Suite will use the same Global Catalog server as the Men and Mice Central server is using. If you unselect this checkbox, you must specify the Global Catalog server in the Global Catalog Server field.

   4. **Global Catalog Server.** If you want to specify a non-default Global Catalog server, enter the server name in this field. To enable this field, you must first unselect the Use same Global Catalog as the Men and Mice Central server checkbox.
5. **Use the same credentials as the Men and Mice Central server.** If checked, the Men & Mice Suite uses the same credentials as the Men and Mice Central server when accessing the site information.

6. **User and Password.** If you don’t want to use the default credentials for the machine running Men & Mice Central, enter the desired user name and password in these fields. To enable these fields, you must first **unselect** the **Use the same credentials as the Men and Mice Central server** checkbox.

7. Click OK to save the changes. The forest is added and the sites belonging to the forest are displayed.

### Changing AD Forest Properties

To change the properties for an AD Forest, do the following:

1. In the Object Browser, expand the *AD Sites* object category.
2. Right-click the Forest you want to change, and select **Properties**.
3. Enter the required information in the dialog box.
4. Click OK to save your changes.

### Removing an AD Forest

To remove an AD Forest from the Men & Mice Suite:

1. In the Object Browser, expand the *AD Sites* object category.
2. Right-click the Forest you want to change, and select **Remove AD Forest(s)**.
3. Click OK in the confirmation box to remove the Forest.

### Reloading the Sites in an AD Forest

The list of sites in an AD Forest is reloaded on a regular basis. To manually reload the list of sites:

1. In the Object Browser, expand the *AD Sites* object category.
2. Right-click the Forest you want to reload, and select **Reload AD Sites**.

### Managing Subnets in a Site

- To **view subnets** in a specific site, click the site in the object list. A list of the subnets is shown in the Manager window.
- To **add a subnet** to a site, just drag the subnet from the list of subnets in the Manager window to the site. The subnet is added to the site in AD. When a subnet is placed in a site, all subnets contained within that subnet are placed in the site as well. It is not possible to assign these subnets to a different site.
- To **remove a subnet** from a site, right-click the subnet and choose ‘Remove from AD Site’. The subnet is removed from the site in AD. When a subnet is removed from a site, all subnets contained within that subnet are removed from the site as well.
• To **move a subnet** to a different site, drag the subnet to the new site. The subnet is moved to the site in AD. **NOTES:** Child subnets cannot be moved to a different site than the parent subnet unless the **Enforce site inheritance** checkbox is unchecked in the System Settings dialog box. It is also possible to move a subnet to a different site by selecting the site from a drop-down list in the **Range or Scope Properties** dialog box.

• To **view subnets** that don’t belong to a site, sort the IP address ranges by the **AD Site** column in ascending order. You may want to use the flat view for the IP address ranges when performing this action.
This page intentionally left blank.
Chapter 9: DHCP Servers

Overview

This section shows you how to perform specific actions in the Men & Mice Management Console associated with maintaining your DHCP servers, such as adding and deleting servers and setting DHCP server options. In order to use the DHCP functionality of the Men & Mice Suite you need to have a valid DHCP license key.

NOTE: The functions for this menu option are listed alphabetically after the New DHCP Server section.

New DHCP Server

When adding a DHCP server, the system automatically changes existing IP address ranges to scopes if it finds IP address ranges that contain the same start and end address as a scope on the DHCP server being added.

You must be logged in as a user with privileges to administer DHCP in order to add a DHCP server.

1. From the menu bar, select **File, New, DHCP Server**. The Add DHCP Server dialog box displays.

2. **Server Name**. Type either the DNS name or the IP Address of the DHCP server.

3. **Server address (optional)**. If desired, type the IPv4 or IPv6 address for the server. This is not required, but doing so allows the Management Console to connect to the server by IP address instead of by name.

4. **Server Type**. Click the drop-down list, and select the desired server type.
   - **Microsoft with Agent Installed** connects to a Microsoft DHCP server that has a DHCP Server Controller installed. If you want to gather the lease history from the DHCP server, you must use this connection method.
   - **Microsoft Agent-Free** connects to a Microsoft DHCP server that does not have a DHCP Server Controller installed. When using this connection method, it is not possible to gather the lease history from the DHCP server. For further information regarding this connection method, see the section **Server Access on Remote Computers**, below
   - **ISC** connects to an ISC DHCP server.
Cisco connects to a Cisco Router that is running DHCP server software.

When adding a Cisco DHCP server, the following dialog box displays:

![Image of user interface for entering user name and password]

Type the **User name** and **Password** that should be used to access the server. This is the user name and password that is used when normally accessing the Cisco device from the command line prompt. If the server requires a separate password to enter privilege level 15, enter the required password in the **Enable Password** field. If you select the **Connect using Secure Shell (SSHv2)** checkbox, a secure connection will be used to access the server. If this checkbox is unchecked, the server will be accessed through a telnet connection.

5. **Use proxy server.** If you are adding a Microsoft or a Cisco DHCP server you can specify the location of the DHCP Server Controller by clicking the **Use proxy server** checkbox and entering the DNS name or IP address of the machine running the DHCP Server controller. This option allows the system to connect to DHCP servers in different forests where a cross-forest trust does not exist. It also allows a non-Windows version of Men & Mice Central to manage Microsoft DHCP servers.

6. Click **OK**. You are connected to the server. Once connected, the name of the newly added server displays under DHCP Servers in the Object Section. (You may need to click the plus (+) sign next to DHCP Servers to see it.)

**Server Access on Remote Computers**

To manage DHCP servers you must have the DHCP Server Controller installed. For the ISC DHCP server, a DHCP Server Controller must be installed on each DHCP server you want to manage.

If you plan to use Men & Mice Suite to manage any Microsoft DHCP servers, install the DHCP Server Controller on a Windows machine that is a member of the same domain or workgroup as the DHCP servers. You may install multiple copies of the DHCP Server Controller, for example if you want to manage Microsoft DHCP Servers that reside in different forests. A single DHCP Server Controller for Microsoft DHCP Servers can manage multiple DHCP servers. The DHCP Server Controller must adhere to whatever restrictions and security standards are set forth in Microsoft Windows.

To configure the DHCP Server Controller to access DHCP servers on remote computers, do the following:

1. Before you can administer DHCP servers, verify that the DHCP Controller is running as a Windows User and has the necessary privileges.

2. To enable DHCP Management in the Men & Mice Suite, start the Windows Services program and open the properties dialog box for Men & Mice DHCP Server Controller.
3. Click the Log On tab. The Local System account radio button is most likely selected.

4. Click the This account radio button and enter the name and password of a Windows User that is a member of either the Administrators group or the DHCP Administrators group.

5. Close the dialog box and restart the Men & Mice DHCP Server Controller service.

**NOTE:** Lease history gathering is not possible if you are managing MS DHCP servers on remote computers using the DHCP Server Controller. To gather lease history for a MS DHCP server, you must install the DHCP Server Controller on the server and use the Microsoft with Agent Installed connection method when connecting to the server.

---

### Edit DHCP Server Name

This feature allows you to change the name or IP address used to connect to a DHCP server. This is useful if you need to refer to the server by another name or if you are connecting to the server by an IP address and the IP address has changed. You can also use this feature to change the connection method for MS DHCP servers.

To access this feature, do the following:

1. Locate the applicable server.

2. Right-click and, from the shortcut menu, select **Edit Server Name**. The Edit Server name dialog box displays.

3. Change the **Server name**, **Server address** (optional), and **Server Type**. If applicable, you can select **Use proxy server** and enter the relevant information.

4. Click **OK**.

---

### Access

For complete details on this function, refer to Administration Functions—Global Access/Access Control.

---

### Delete

To remove a DHCP server, do the following:

1. In the Object Section of the Management Console, click on **DHCP Servers**.

2. In the Object List, right-click on the DHCP Server you want to remove.

3. From the shortcut menu, select **Delete**.
4. In the confirmation dialog box, click Yes.

Managing Groups/Hosts

*Applies to ISC DHCP Servers only.* Allows you to manage groups and hosts within groups on an ISC DHCP server. You can also manage host entries that are defined in the global scope.

To manage groups and hosts, do the following:

1. Select the ISC DHCP server for which you want to manage groups and/or hosts.
2. Right-click on the server and, from the shortcut menu, select **Manage Groups and Hosts.** A new menu displays in the menu bar and the DHCP Groups dialog box displays.

**Groups/Hosts Toolbar**

The toolbar that displays in the Groups for DHCP Server contains the following:

<table>
<thead>
<tr>
<th>BUTTON</th>
<th>FUNCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Add" /></td>
<td>Displays the Add Group dialog box. Enter the name for the new group, and click Add.</td>
</tr>
</tbody>
</table>
### Groups/Hosts Shortcut Menu

- **Edit.** Displays the Edit Host dialog box. Make the desired changes to the name for the selected group, and click Save.
- **Add.** Displays the Add Host dialog box. Enter the applicable information, and click Add.
- **Delete.** When selected, displays a confirmation message asking if you want to delete the selected host.
- **Options.** When selected, displays the Host Options dialog. Refer to DHCP Server Options for details on completing this dialog box.
- **Copy.** Copies information about the selected host into the clipboard.
- **Select All.** Selects all groups/hosts. You can then right-click and use the shortcut menu options to manage all the selected items.
Editing Subclasses

Applies to ISC DHCP Servers only. Allows you to edit subclasses on an ISC DHCP server. **NOTE:** You cannot manage DHCP classes – only subclasses of existing DHCP classes.

To edit subclasses, do the following:

1. Select the ISC DHCP server for which you want to edit subclasses.
2. Right-click on the server and, from the shortcut menu, select **Edit Subclasses**. The DHCP class dialog box displays.

![Select DHCP class dialog box](image)

3. Choose a class to edit and click the **Select** button. A new dialog box displays where you can enter the client identifiers or MAC addresses of the hosts that should belong to the selected class.

![DHCP Class dialog box](image)

   The dialog box contains a multi-line edit field where you can quickly add multiple entries. **NOTE:** When entering MAC addresses you must use a colon as a separator. Each line in the dialog box should contain one entry. To delete an entry, simply remove the corresponding line in the dialog box.

4. Click **OK** to confirm your changes and close the dialog box.
Options

The ISC, Cisco and MS DHCP servers offer different types of options: the MS DHCP server allows the user to choose between different option types (Standard, Microsoft Options and Microsoft Windows 2000 options). This drop-down list is only displayed if there are non-standard options defined on the ISC DHCP server.

You can set options for multiple servers by selecting all of the servers for which you want to set options. When setting options for multiple servers all of the servers must be of the same type.

1. In the Object List, right-click on the applicable DHCP Server and, from the shortcut menu, select Options. The DHCP Server Options window displays.

2. In the selection field in the upper left corner, click the drop-down list to select which options you want to display. Based upon your selection, the dialog box changes.

3. To Show only options with non-default values, click this checkbox. The Quick Filter field supports the following keywords: name, value, and option. For example, if you want to quickly find option 51, you could enter the following: option51.

4. To add a value to an option, locate the option item, and click the plus (+) sign at the end of the field. A blank field displays into which you can enter the applicable information. If you enter multiple fields for an option, they are numbered consecutively (e.g., Time Server as two fields.)

5. If applicable, use the scroll bar along the right-hand side of the page to move up/down the option list.

6. When all selections/entries are made, click OK to save your changes.
Defining DHCP Server Options

You can define your own options on ISC and MS DHCP servers.

Defining Options on MS DHCP Servers

1. In the Object List, right-click on the applicable DHCP Server and, from the shortcut menu, select Define Options. The DHCP Server Option definition dialog box displays. The dialog box shows all options defined on the DHCP server.

2. Use the Vendor class drop-down list to select the vendor class for which you want to define options.
   - To Add an option, click the button with the plus sign at the end of the option list. Enter the ID, name and type of data to use for the option. The IP Address and Integer data types can be specified as arrays. To specify an array, click the Array checkbox.
   - To Delete an option, click the button with the minus sign next to the option you want to delete.

3. Click OK to save the option definition.

NOTE: You can only add or delete option definitions. You cannot change the properties of an existing option definition.
Defining Options on ISC DHCP Servers

1. In the Object List, right-click on the applicable DHCP Server and, from the shortcut menu, select Define Options. The DHCP Server Option definition dialog box displays. The dialog box shows all custom defined on the DHCP server.

2. To Add an option, click the button with the plus sign at the end of the option list. Enter the ID, name and type of data to use for the option. The several data types can be specified as arrays and the Array checkbox is enabled when a supported data type is selected. To specify an array, click the Array checkbox.

3. To Delete an option, click the button with the minus sign next to the option you want to delete.

4. To change the ID for an option, enter the new ID in the ID field. **NOTE:** You can only edit the ID property for existing options.

5. Click OK to save the option definition.

Properties

1. From the Object list, expand the DHCP Servers list.

2. Right-click on the server for which you want to manage properties and, from the shortcut menu, select Properties. The Properties dialog box for the selected server displays. **Refer to the applicable section based upon the server type: MS, ISC or Cisco.**
MS Server Properties

1. Complete the General tab using the guidelines below.

   - **Conflict detection attempts.** Specifies the number of conflict detection attempts you want the DHCP server to make before it leases an address to a client.

   - **Audit log file path.** Specifies the location of the DHCP server audit log files.

   - **Database path.** Specifies the location of the DHCP server database.

   - **Backup path.** Specifies the location for the database backup.

2. Click the DNS tab, and complete the fields according to the guidelines below:
3. **Enable DNS dynamic updates according to the settings below.** Specifies whether the DHCP server sends DNS dynamic record updates to the DNS server. Updates are sent to DNS servers configured in TCP/IP client properties for any active network connections at the DHCP server.
   - **Dynamically update DNS A and PTR records.** Specifies that the DHCP server update forward and reverse lookups are based on the type of request made by the client during the lease process.
   - **Always dynamically update DNS A and PTR records.** Specifies that the DHCP server update forward and reverse DNS lookups when a client acquires a lease, regardless of the type of request used to acquire it.

4. **Discard A and PTR records when lease is deleted.** Specifies whether the DHCP server discards forward DNS lookups for clients when a lease expires.

5. **Dynamically update DNS A and PTR records for DHCP clients.** Specifies whether the DHCP server sends dynamic updates to the DNS server for DHCP clients that do not support performing these updates. If selected, clients running earlier versions of Windows are updated by the DHCP server for both their host (A) and pointer (PTR) resource records.

6. When all selections/entries are made, click **OK**.

**ISC Server Properties**

- **Authoritative.** Specifies whether the server is authoritative to determine if a DHCP request from a client is valid
- **DDNS Domain Name.** Specifies the DNS domain name to use to store the A record for a DHCP client.
- **DDNS Reverse Domain Name.** Specifies the DNS reverse domain name to use to store the PTR record for a DHCP client.
- **DDNS Update Style.** Specifies how the DHCP server does DNS updates. The available styles are:
  - **None.** Dynamic DNS updates are not performed
  - **Ad-hoc.** This update scheme is depreciated
  - **Interim.** This is the recommended scheme for dynamic DNS updates
- **DDNS Updates.** Specifies whether to perform DNS updates. This setting has no effect unless DNS updates are enabled globally with the **DDNS Update Style** setting.
- **DDNS TTL.** Specifies (in seconds) the TTL value to use when performing a DNS update.
- **Default Lease Time.** Specifies (in seconds) the default lease time to use for DHCP leases.
• **Log Facility.** Specifies which syslog facility to use when logging DHCP server messages. All possible facilities are listed; however, not all of these facilities are available on all systems.

• **Max/Min Lease Time.** Specifies (in seconds) the maximum/minimum lease time to use for DHCP leases.

• **Get Lease Hostnames.** Specifies whether the DHCP server should perform a reverse DNS lookup for each address assigned to a client and send the result to the client in the **host-name** option.

• **One Lease per Client.** Specifies whether the DHCP server should free any existing leases held by a client when the client requests a new lease.

• **Ping Check.** Specifies whether the DHCP server should send an ICMP echo message to probe an IP address before offering it to a DHCP client.

• **Ping Timeout.** Specifies for how many seconds the DHCP server should wait for an ICMP echo response when **Ping Check** is active.

• **Filename.** Specifies the name of the initial boot file to be used by a client.

• **Server Name.** Specifies the name of the server from which the client should load its boot file.

• **Next Server.** Specifies the host address of the server from which the initial boot file (that is specified by **Filename**) is to be loaded.

**Cisco Server Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Specifies the name of the Cisco router. Refer to Cisco IOS IP Addressing Command Reference document for more information.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Specifies the default domain name that the Cisco IOS software uses to complete unqualified host names. Refer to Cisco IOS IP Addressing Command Reference document for more information.</td>
</tr>
<tr>
<td>Name Server</td>
<td>Specifies the address of a name server to use for name and address resolution. Refer to Cisco IOS IP Addressing Command Reference document for more information.</td>
</tr>
</tbody>
</table>

**Reconcile Scopes**

*Applies to MS DHCP Servers only.* Use this function to fix inconsistencies between information in the registry and the DHCP database.

1. In the Object List, select **DHCP Servers** and then select an MS DHCP server.
2. Right-click the server, and select **Reconcile Scopes**.

![Reconcile Scope(s)](image)

3. Choose the action to perform: **Verify** (only) or **Fix** (any inconsistencies).

4. Click **OK** to complete the action.

---

**Reload Scope List**

Reloads the list of scopes to view additions and/or deletions made by another user.

---

**Restart**

*Applies to ISC DHCP Servers only.* This menu item is only displayed when a user with DHCP administration privileges is logged in. This command restarts the DHCP server.

---

**Set User Name and Password**

This menu item is only displayed when a user with DHCP administration privileges is logged in. This command updates the user name and password that should be used to access the Cisco DHCP server. Use this command if the user name or password on the Cisco DHCP server has changed.
This page intentionally left blank.
Chapter 10: DHCP Scopes

Overview

This section shows you how to perform specific actions in the Men & Mice Management Console associated with maintaining your DHCP scopes, such as creating and modifying reservations, setting scope options and working with split scopes.

NOTE: The functions for this menu option are listed alphabetically after the New DHCP Scope section.

Viewing Scopes

All DHCP Scopes on All Servers

You can use the Management Console to view all of the existing DHCP scopes at once, regardless of the server to which they belong. In the Object Section of the Management Console, click on the DHCP Scopes object. This causes all existing scopes (to which you have access) to appear in the Object List.

![Image of DHCP Scopes list]

The Free column in the scope list displays the number of unassigned addresses within the address pool(s) of each scope. If the number of unassigned addresses within an address pool drops below 10, the scope is listed in a red color.

Disabled scopes are shown as gray. The number of unassigned addresses is always shown as zero for disabled scopes.

Scopes on a Specific DHCP Server

It is easy to view the DHCP scopes that reside on individual DHCP Servers that are being managed by the Management Console. Simply click on the plus (+) sign next to the DHCP Servers object in the Object Section, and select the DHCP server containing the scopes you want to view.
Selected Scope Menus

When working with scopes, a right-click, shortcut menu is offered. The menu options change, based upon the type of DHCP server the scope is hosted on: MS, ISC or Cisco.

MS Shortcut Menu

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>Opens the currently selected device. Refer to Opening/Editing an Existing Scope.</td>
</tr>
<tr>
<td>Delete</td>
<td>This option is enabled when there is an existing DNS entry for the IP address or there is custom property data for the IP address. When Delete is selected, the additional data is removed; however, the IP Address itself remains intact.</td>
</tr>
<tr>
<td>History</td>
<td>Shows any changes made to the selected item. These changes are displayed in a new window.</td>
</tr>
<tr>
<td>Ping</td>
<td>Allows you to ping the selected server. If the ping is successful, a green dot displays; if unsuccessful, a red dot displays.</td>
</tr>
<tr>
<td>Claim</td>
<td>Allows you to &quot;claim&quot; an address to prevent accidental assignment but without creating a DNS entry for it.</td>
</tr>
<tr>
<td>Create Address Pool</td>
<td>Creates an address pool for the selected scope. Complete the From and To fields in the DHCP Address Pool dialog box, typing the range of addresses to be included in the pool. Both of these fields default to the first available address in the range. If this is a split scope (a scope that exists on more than one server) and the address pool overlaps a warning message displays.</td>
</tr>
<tr>
<td>Options for Pool</td>
<td>ISC DHCP only. To set options for a pool, click anywhere in the applicable address pool, right-click, select Options for Pool and, in the Options dialog box, make the desired changes.</td>
</tr>
</tbody>
</table>

### Example Table

<table>
<thead>
<tr>
<th>Address</th>
<th>Genre</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>90.6.0.1</td>
<td>Pool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.2</td>
<td>Pool</td>
<td>Reserved</td>
</tr>
<tr>
<td>90.6.0.3</td>
<td>Pool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.4</td>
<td>Pool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.5</td>
<td>Pool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.6</td>
<td>Pool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.7</td>
<td>Pool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.8</td>
<td>Pool</td>
<td>Excluded</td>
</tr>
<tr>
<td>OPTION</td>
<td>DESCRIPTION</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Permits for Pool</td>
<td><em>ISC DHCP only.</em> Allows you to specify permits for an address pool. To set access pool permits, do the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Click anywhere in the applicable address pool, right-click and select <strong>Permits for Pool</strong>. The Pool Permits dialog box displays.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add</strong> to create a new access pool permit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Enter the permit settings and click OK to save the changes and close the dialog box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Use the <strong>Edit</strong> and <strong>Delete</strong> buttons to modify or delete existing permits.</td>
<td></td>
</tr>
<tr>
<td>Delete Address Pool(s)</td>
<td>To delete an existing pool, click anywhere in the applicable assigned range, right-click and select <strong>Delete Address Pool(s)</strong>.</td>
<td></td>
</tr>
<tr>
<td>Create Excluded Range</td>
<td><em>MS DHCP only.</em> Allows you to exclude a single IP address or an entire range of addresses from being used. You can only exclude addresses that are already part of an address pool.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To create an excluded range, specify the <strong>From</strong> and <strong>To</strong> IP addresses. All the addresses between and including the ones entered will be excluded.</td>
<td></td>
</tr>
<tr>
<td>DHCP Exclude Range</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>From:</strong> 123.0.0.14</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>To:</strong> 123.0.0.14</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>OK</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Cancel</strong></td>
<td></td>
</tr>
<tr>
<td>Edit Excluded Range</td>
<td><em>MS DHCP only.</em> To edit an existing range, click anywhere in the applicable excluded range, right-click, select <strong>Edit Excluded Range</strong> and, in the dialog box, make the desired edits.</td>
<td></td>
</tr>
<tr>
<td>Delete Excluded Range(s)</td>
<td><em>MS DHCP only.</em> To delete an existing range, click anywhere in the applicable excluded range, right-click and select <strong>Delete Excluded Range(s)</strong>. The entire excluded range is removed.</td>
<td></td>
</tr>
<tr>
<td>Create Reservation</td>
<td>Reservations can be created in unassigned address space, address pools, and excluded addresses. It is possible to set options for reserved IP addresses.</td>
<td></td>
</tr>
</tbody>
</table>
To create a reservation, do the following:

1. Locate the IP address you want to reserve, right-click on it, and select **Create Reservation** from the pop-up menu. The DHCP Reservation dialog box displays.

2. **Name.** Assign a name to identify the reserved address.

3. **MAC Address.** Enter the MAC Address (i.e., Media Access Control Address) of the network node for which this address is being reserved.

4. **Description.** (Optional) User defined description.

5. **Supported Types.** Select whether this reservation should support DHCP, BOOTP (i.e., Bootstrap Protocol), or Both (default).

To specify whether the DHCP server automatically updates record in the DNS server or not, click the **DNS** tab.

1. **Enable DNS dynamic updates according to the settings below.** Specifies whether the DHCP server sends DNS dynamic record updates to the DNS server. Updates are sent to DNS servers configured in TCP/IP client properties for any active network connections at the DHCP server.

2. **Dynamically update DNS A and PTR records.** Specifies that the DHCP server update forward and reverse lookups be based on the type of request made by the client during the lease process.
### DHCP Scopes

**OPTION** | **DESCRIPTION**
--- | ---
3. **Always dynamically update DNS A and PTR records.** Specifies that the DHCP server update forward and reverse DNS lookups when a client acquires a lease, regardless of the type of request used to acquire it.
4. **Discard A and PTR records when lease is deleted.** Specifies whether the DHCP server discards forward DNS lookups for clients when a lease expires.
5. **Dynamically update DNS A and PTR records for DHCP clients that do not request updates.** Specifies whether the DHCP server sends dynamic updates to the DNS server for DHCP clients that do not support performing these updates. If selected, clients running earlier versions of Windows are updated by the DHCP server for both their host (A) and pointer (PTR) resource records.
6. **Click OK.** The address is now listed as reserved in the DHCP Scope dialog box.

| **Edit a Reservation** | To edit an existing reservation, right-click on the reservation you want to change and select **Edit a Reservation.** Then, make the necessary edits. |
| **Options for a Reservation** | To select options for a reservation, right-click on the reservation and select **Options for a Reservation.** The DHCP Reservations dialog box displays. **Refer to DHCP Servers—Server Options for details on working with this dialog box.** |
| **Delete Reservation(s)** | To delete an existing reservation, right-click on the reservation you want to remove and select **Delete Reservation(s).** |

### ISC Shortcut Menu

<table>
<thead>
<tr>
<th><strong>OPTION</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Open</strong></td>
<td>Opens the currently selected device. <strong>Refer to Opening/Editing an Existing Scope.</strong></td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>This option is enabled when there is an existing DNS entry for the IP address or there is custom property data for the IP address. When Delete is selected, the additional data is removed; however, the IP Address itself remains intact.</td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>Shows any changes made to the selected item. These changes are displayed in a new window.</td>
</tr>
<tr>
<td><strong>Ping</strong></td>
<td>Allows you to ping the selected server. If the ping is successful, a green dot displays; if unsuccessful, a red dot displays.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address</th>
<th>Genre</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>90.6.0.1</td>
<td>Fool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.2</td>
<td>Fool</td>
<td>Reserved</td>
</tr>
<tr>
<td>90.6.0.3</td>
<td>Fool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.4</td>
<td>Fool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.5</td>
<td>Fool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.6</td>
<td>Fool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.7</td>
<td>Fool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.8</td>
<td>Fool</td>
<td>Excluded</td>
</tr>
</tbody>
</table>

| **Claim** | Allows you to "claim" an address to prevent accidental assignment but without creating a DNS entry for it. |
### OPTION | DESCRIPTION
--- | ---
Create Address Pool | Creates an address pool for the selected scope. Complete the From and To fields in the DHCP Address Pool dialog box, typing the range of addresses to be included in the pool. Both of these fields default to the first available address in the range. If this is a split scope (a scope that exists on more than one server) and the address pool overlaps a warning message displays.

**DHCP Address Pool**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>128.1.0.0</td>
</tr>
<tr>
<td>To</td>
<td>128.1.0.50</td>
</tr>
</tbody>
</table>

**Edit Address Pool** | To edit an existing pool, click anywhere in the applicable assigned range, right-click, select Edit Address Pool and, in the dialog box, make the desired edits.

**Options for Pool** | When selected, the DHCP Options dialog box displays. Refer to DHCP Servers—Server Options for details on working with this dialog box.

**Delete Address Pool(s)** | To delete an existing pool, click anywhere in the applicable assigned range, right-click and select Delete Address Pool(s).

Create Reservation | Reservations can be created in unassigned address space, address pools, and excluded addresses. It is possible to set options for reserved IP addresses. To create an address, do the following:

1. Locate the IP address you want to reserve, right-click on it, and select Create Reservation. The DHCP Reservation dialog box displays.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>MAC Address</td>
<td></td>
</tr>
<tr>
<td>DDNS hostname</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>10.5.0.12</td>
</tr>
</tbody>
</table>

2. **Name.** Assign a name to identify the reserved address.

3. **MAC Address.** Enter the MAC Address (i.e., Media Access Control Address) of the network node for which this address is being reserved.

4. **DDNS hostname.** Specifies the DNS domain name to use to store the A record for a DHCP client.

5. **IP Address.** Enter an IP address for the reservation. You can add additional IP addresses by clicking the plus sign and enter an IP address in the field that displays.

6. Click **OK.**

**Edit a Reservation** | To edit an existing reservation, right-click on the reservation you want to change and select Edit a Reservation. Then, make the necessary edits.

**Options for a Reservation** | To select options for a reservation, right-click on the reservation and select Options for a Reservation. The DHCP Reservations Options dialog box displays. Refer to DHCP Servers—Server Options for details on working with this dialog box.

**Delete Reservation(s)** | To delete an existing reservation, right-click on the reservation you want to remove and select Delete Reservation(s).
Cisco Shortcut Menu

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>Opens the currently selected device. Refer to Opening/Editing an Existing Scope.</td>
</tr>
<tr>
<td>Delete</td>
<td>This option is enabled when there is an existing DNS entry for the IP address or there is custom property data for the IP address. When Delete is selected, the additional data is removed; however, the IP Address itself remains intact.</td>
</tr>
<tr>
<td>History</td>
<td>Shows any changes made to the selected item. These changes are displayed in a new window.</td>
</tr>
<tr>
<td>Ping</td>
<td>Allows you to ping the selected server. If the ping is successful, a green dot displays; if unsuccessful, a red dot displays.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address</th>
<th>Genre</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>90.6.0.1</td>
<td>Pool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.2</td>
<td>Pool</td>
<td>Reserved</td>
</tr>
<tr>
<td>90.6.0.3</td>
<td>Pool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.4</td>
<td>Pool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.5</td>
<td>Pool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.6</td>
<td>Pool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.7</td>
<td>Pool</td>
<td>Available</td>
</tr>
<tr>
<td>90.6.0.8</td>
<td>Pool</td>
<td>Excluded</td>
</tr>
</tbody>
</table>

| Claim | Allows you to “claim” an address to prevent accidental assignment but without creating a DNS entry for it. |
| Create Excluded Range | Allows you to exclude a single IP address or an entire range of addresses from being used. You can only exclude addresses that are already part of an address pool. To create an excluded range, specify the From and To IP addresses. All the addresses between and including the ones entered will be excluded. |

**DHCP Exclude Range**

<table>
<thead>
<tr>
<th>From: 192.168.1.25</th>
<th>OK</th>
</tr>
</thead>
<tbody>
<tr>
<td>To: 192.168.1.27</td>
<td>Cancel</td>
</tr>
</tbody>
</table>

| Edit Excluded Range | To edit an existing range, click anywhere in the applicable excluded range, right-click, select Edit Excluded Range and, in the dialog box, make the desired edits. |
| Delete Excluded Range(s) | To delete an existing range, click anywhere in the applicable excluded range, right-click and select Delete Excluded Range(s). The entire excluded range is removed. |
### OPTION DESCRIPTION

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Reservation</td>
<td>Reservations can be created in address pools, and excluded addresses. It is possible to set options for reserved IP addresses. To create an address, do the following:</td>
</tr>
<tr>
<td></td>
<td>1. Locate the IP address you want to reserve, right-click on it, and select <strong>Create Reservation</strong>. The DHCP Reservation dialog box displays.</td>
</tr>
<tr>
<td></td>
<td>2. <strong>Name</strong>. Assign a name to identify the reserved address.</td>
</tr>
<tr>
<td></td>
<td>3. <strong>Reservation Method</strong>. Choose the reservation method for this reservation. You can choose either <strong>Client Identifier</strong> or <strong>Hardware Address</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. <strong>Client Identifier</strong> / <strong>MAC Address</strong>. Depending on your choice for Reservation Method, enter the <strong>Client Identifier</strong> or <strong>MAC Address</strong> (i.e., Media Access Control Address) of the network node for which this address is being reserved.</td>
</tr>
<tr>
<td></td>
<td>5. <strong>DDNS hostname</strong>. Specifies the DNS domain name to use to store the A record for a DHCP client.</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Edit Reservation</td>
<td>To edit an existing reservation, right-click on the reservation you want to change and select <strong>Edit a Reservation</strong>. Then, make the necessary edits.</td>
</tr>
<tr>
<td>Options for a Reservation</td>
<td>To select options for a reservation, right-click on the reservation and select <strong>Options for a Reservation</strong>. The DHCP Reservations dialog box displays. Refer to <em>Defining DHCP Server Options</em> for details on working with this dialog box.</td>
</tr>
<tr>
<td>Delete Reservation(s)</td>
<td>To delete an existing reservation, right-click on the reservation you want to remove and select <strong>Delete Reservation(s)</strong>.</td>
</tr>
</tbody>
</table>

### New DHCP Scope

This section describes how to create and edit DHCP scopes in the Men & Mice Suite. Whenever you create a new scope, the Men & Mice Suite automatically checks whether the new scope conflicts with an existing scope or an IPAM range.

Adding a new DHCP Scope has three general steps:

- Creating the DHCP scope.
- Setting the desired Options for the scope.
- Enabling the scope. (All new scopes are 'disabled' by default so you can make the necessary configuration changes before the DHCP server starts using it.)

Depending on whether you’re creating a scope on an MS DHCP server or an ISC DHCP server, the process and data you specify are different.
MS DHCP Server

To create a new scope on the MS DHCP server, do the following:

1. In the object list, right-click on **DHCP Scopes** and, from the shortcut menu, and select **New Scope**. The Create DHCP Scope dialog box displays.

![Create DHCP Scope](image)

2. **Subnet/Range.** Type the subnet/range parameters.

3. **Server.** Click the drop-down list arrow, and select the DHCP Server on which you are creating this scope.

4. Once you have made the selections above, the remaining fields (e.g., Usable IP addresses, etc.) are populated.

5. Click **Create**. The DHCP Scope Properties dialog box displays.

![DHCP Scope Properties](image)

6. **Superscope.** If you want to place the scope in a Superscope, type the name of the Superscope.

7. **Name.** Type the name as you want it to appear in the DHCP Scopes list.

8. **Description.** Type information that describes the purpose for this scope.

9. **Lease duration for DHCP client.** Allows you to specify the lease duration of addresses in this scope.
   - **Limited to.** Click the radio button, and then indicate the days, hours, and minutes.
   - **Unlimited.** If you want to specify unlimited lease duration, click this radio button.

10. When all selections/entries are made, click **OK**. The DHCP Scope window displays.
NOTE: Once the scope has been created, you must set access privileges for the scope if you want to allow users to make any changes to it.

Once you have created the scope, you can return to edit the property and then complete the DNS tab.

1. Locate the scope for which you want to add DNS properties.
2. Right-click and, from the shortcut menu, select Properties. When the DHCP Scope Properties dialog box displays, the DNS tab is shown.
3. Click the DNS tab.

4. Enable DNS dynamic updates according to the settings below. Specifies whether the DHCP server sends DNS dynamic record updates to the DNS server. Updates are sent to DNS servers configured in TCP/IP client properties for any active network connections at the DHCP server.
   - Dynamically update DNS A and PTR records. Specifies that the DHCP server update forward and reverse lookups are based on the type of request made by the client during the lease process.
   - Always dynamically update DNS A and PTR records. Specifies that the DHCP server update forward and reverse DNS lookups when a client acquires a lease, regardless of the type of request used to acquire it.
5. Discard A and PTR records when lease is deleted. Specifies whether the DHCP server discards forward DNS lookups for clients when a lease expires.
6. **Dynamically update DNS A and PTR records for DHCP clients.** Specifies whether the DHCP server sends dynamic updates to the DNS server for DHCP clients that do not support performing these updates. If selected, clients running earlier versions of Windows are updated by the DHCP server for both their host (A) and pointer (PTR) resource records.

**ISC DHCP Server**

To create a new scope on an ISC DHCP server, do the following:

1. In the object list, right-click on **DHCP Scopes** and, from the shortcut menu, select **New Scope**. The Create DHCP Scope dialog box displays.

2. **Subnet/Range.** Type the subnet/range parameters.

3. **Server.** Click the drop-down list arrow, and select the DHCP Server on which you are creating this scope.

4. Once you have made the selections above, the remaining fields (e.g., Usable IP addresses, etc.) are populated.

5. Click **Create**. The DHCP Scope Properties dialog box displays.

6. **Authoritative.** Specifies whether the server is authoritative to determine if a DHCP request from a client is valid for the specified scope.

7. **Shared Network.** Specifies the shared network the scope belongs to.
8. **DDNS Updates.** Specifies whether to perform DNS updates. This setting has no effect unless DNS updates are enabled globally with the **DDNS Update Style** setting.

9. **DDNS Domain Name.** Specifies the DNS domain name to use to store the A record for a DHCP client.

10. **DDNS Reverse Domain Name.** Specifies the DNS reverse domain name to use to store the PTR record for a DHCP client.

11. **Default Lease Time.** Specifies (in seconds) the default lease time to use for DHCP leases.

12. **Max/Min Lease Time.** Specifies (in seconds) the maximum/minimum lease time to use for DHCP leases.

13. **Filename.** Specifies the name of the initial boot file to be used by a client.

14. **Server Name.** Specifies the name of the server from which the client should load its boot file.

15. **Next Server.** Specifies the host address of the server from which the initial boot file (that is specified by **Filename**) is to be loaded.

16. **Title.** Indicates a name for this scope.

17. **Description.** Indicates a description for this scope.

18. When all selections/entries are made, click **OK**.

**Cisco DHCP Server**

To create a new scope on a Cisco DHCP server, do the following:

1. In the object list, right-click on **DHCP Scopes** and, from the shortcut menu, and select **New Scope**. The Create DHCP Scope dialog box displays.

2. **Subnet/Range.** Type the subnet/range parameters.

3. **Server.** Click the drop-down list arrow, and select the DHCP Server on which you are creating this scope.

4. Once you have made the selections above, the remaining fields (e.g., Usable IP addresses, etc.) are populated.
5. Click **Create**. The DHCP Scope Properties dialog box displays.

6. **Import All**. When checked, imports Dynamic Host Configuration Protocol (DHCP) option parameters into the DHCP server database. See the *Cisco IOS IP Addressing Command Reference* document for more information.

7. **Name**. Indicates a name for this scope.

8. **Description**. Indicates a description for this scope.

9. When all selections/entries are made, click **OK**.

---

**Access**

*For complete details on this function, refer to Administration Functions—Global Access/Access Control.*

---

**Delete**

Use the following procedure to remove a scope definition from the Management Console.

1. Locate the DHCP Scope you want to remove and right-click on it.

2. From the pop-up menu, select **Delete**. A dialog prompts you to confirm your decision to delete this scope.

3. Click **OK** to delete the scope, or **Cancel** to leave it.

---

**Disable/Enable**

If you are no longer using a particular scope, but do not want to delete it completely because you may need it in the future, you can disable the scope instead. A scope that is disabled will be ignored by the DHCP server until it is re-enabled. Use the following procedure to disable/enable a scope.

1. Locate the DHCP Scope you want to disable/enable and right-click on it. Scopes that are currently disabled have faded icons next to them.

2. From the pop-up menu, select **Disable** to disable this scope, or if the scope is already disabled, select **Enable** to reactivate it.

**NOTE:** New scopes are always disabled by default so you can configure the properties before the DHCP server begins using it.
Scope Migration Wizard

The Scope Migration Wizard allows users to migrate one or more scopes from one server to another, including all data in the scope. This wizard can only be used for DHCP servers.

To migrate a scope, do the following:

1. In the manager window, select one or more scopes.
2. Right-click and, from the shortcut menu, select Migrate Scope. The Migrate Scope(s) Wizard dialog box displays.
3. Server. Click the drop-down list and select onto which you want to migrate this scope(s).
4. Click Next>. The Migration Options dialog box displays.
5. For each of the resulting screens, make a selection/entry and move through the wizard.

Duplication Wizard

To duplicate a DHCP scope you should use the Duplicate Scope wizard. The duplicate will initially have the exact same properties as the original, but you will have the option to assign the duplicate to a different DHCP server and modify the duplicated values.

Within this wizard, you can do the following:

- Create a new scope
- Create a split scope interface

To launch the wizard, do the following:

1. In the Object Section, click on DHCP Scopes.
2. In the Object List, right-click on the DHCP Scope you want to duplicate and, from the shortcut menu, select Duplicate. The Duplicate scope wizard launches.
3. For each of the resulting screens, make a selection/entry and move through the wizard.

Folders

Refer to Management Console: Object Folders for details on this function.

Reconcile Scope

 Applies to MS DHCP Servers only. Use this function to fix inconsistencies between information in the registry and the DHCP database.

1. In the Object List, select DHCP Scopes and then select a scope.
2. Right-click the scope and select Reconcile Scopes.

3. Choose whether you want to verify only or fix any inconsistencies and click OK to complete the action.
Converting a Scope to a Range

Use this function to convert an existing scope to an IP address range while keeping all the settings intact.

1. In the Object List, select **DHCP Scopes** and then select a scope.
2. From the menu bar, select **Range, Convert to IP Address Range**.
3. When the Men & Mice Management Console confirmation dialog box displays, click **Yes** to convert the range.

Converting a Range to a Scope

Use this function to convert an existing IP address range to a scope while keeping all the settings intact.

1. In the Object List, select **IP Address Ranges** and select a range.
2. From the menu bar, select **Range, Convert to DHCP Scope**. The Create DHCP Scope dialog box displays.
3. **Subnet/Range**. Type the subnet/range parameters.
4. **Server**. Click the drop-down list arrow, and select the DHCP Server on which you are creating this scope.
5. Click **Create**. The DHCP Scope Properties for [IP Address Range] dialog box displays.
6. **Superscope**. If you want to place the scope in a Superscope, type the name of the Superscope.
7. **Title**. Type the name as you want it to appear in the DHCP Scopes list.
8. **Description.** Type information that describes the purpose for this scope.

9. **Lease duration for DHCP clients.** Allows you to specify the lease duration of addresses in this scope.
   - **Limited to.** Click the radio button, and then indicate the days, hours, and minutes.
   - **Unlimited.** If you want to specify unlimited lease duration, click this radio button.

10. Click **OK**.

11. When all selections/entries are made, click **OK**. The DHCP Scope window displays.

   ![DHCP Scope Window](image)

**NOTE:** Once the scope has been created, you must set access privileges for the scope if you want to allow users to make any changes to it.

Once you have created the scope, you can return to edit the property and then complete the DNS tab.

1. Locate the scope for which you want to add DNS properties.

2. Right-click and, from the shortcut menu, select **Properties.** When the DHCP Scope Properties dialog box displays, the DNS tab is shown.

3. Click the **DNS** tab.

   ![DHCP Scope Properties](image)
4. **Enable DNS dynamic updates according to the settings below.** Specifies whether the DHCP server sends DNS dynamic record updates to the DNS server. Updates are sent to DNS servers configured in TCP/IP client properties for any active network connections at the DHCP server.
   - **Dynamically update DNS A and PTR records.** Specifies that the DHCP server update forward and reverse lookups are based on the type of request made by the client during the lease process.
   - **Always dynamically update DNS A and PTR records.** Specifies that the DHCP server update forward and reverse DNS lookups when a client acquires a lease, regardless of the type of request used to acquire it.

5. **Discard A and PTR records when lease is deleted.** Specifies whether the DHCP server discards forward DNS lookups for clients when a lease expires.

6. **Dynamically update DNS A and PTR records for DHCP clients.** Specifies whether the DHCP server sends dynamic updates to the DNS server for DHCP clients that do not support performing these updates. If selected, clients running earlier versions of Windows are updated by the DHCP server for both their host (A) and pointer (PTR) resource records.

### Options

You can set options for multiple scopes by selecting all of the scopes for which you want to set options. You cannot change options for multiple scopes that are hosted on different server types.

1. In the Object List, right-click on the applicable DHCP Server and, from the shortcut menu, select **Options**. The DHCP Server Options window displays.
2. To show only options with non-default values, click in the checkbox field.
3. To search for and find a specific option, use the **Quick Filter** field. For example, type the word "servers" and you only see options containing the word "servers". However, type the word "server" (without the "s") and you see both options containing the word "server" or the word "servers".
4. To add an option, locate the option item, and click the **plus (+) sign** at the end of the field. A blank field displays into which you can enter the applicable information. If you enter multiple fields for an option, they are numbered consecutively (e.g., Time Server as two fields).
5. If applicable, use the scroll bar along the right-hand side of the page to move up/down the option list.

![DHCP Server Options](image)

6. When all selections/entries are made, click **OK** to save your changes.
Scope Policies (Windows Server 2012)

If you are managing DHCP servers on Windows Server 2012, you can use the Men & Mice Suite to set scope policies for individual scopes.

**Activate/Deactivate a Scope Policy**

1. In the Scope List, right-click a scope that is stored on a Windows 2012 DHCP server.
2. From the shortcut menu, select Manage Policies. The DHCP Scope Policy Management dialog box displays.

The dialog box shows the current status of DHCP scope policies for the selected scope.

3. To activate DHCP scope policies, click the Activate button. If DHCP scope policies are active, the button text shows, Deactivate. To deactivate the DHCP scope policies, click the Deactivate button.
4. Click Close.

**Add a New Scope Policy**

1. In the Scope List, right-click a scope that is stored on a Windows 2012 DHCP server and, from the shortcut menu, select Manage Policies. The DHCP Scope Policy Management dialog box displays.
2. Click the **Add** button. The DHCP Policy dialog box displays.

3. Enter a **name** and **description** for the DHCP policy in the corresponding fields.

4. Click the **Add** button in the **Conditions** section to add a new condition for the DHCP policy. The DHCP Policy Condition dialog box displays.

5. Specify the condition you want to use and click **OK** to save the condition and close the dialog box. Note that you can enter multiple conditions for a DHCP policy by clicking the **Add** button in the DHCP Policy dialog box.

6. To edit or delete an existing DHCP Policy condition, select the condition from the list of DHCP Policy conditions, and click the corresponding button.

7. If there is more than one condition, you need to specify whether to use the **OR** or **AND** operator when evaluating the conditions. Select the corresponding radio button in the DHCP Policy dialog box.
8. Click the **Add** button in the ranges section to specify an IP address range that should be affected by the policy. The Range specification dialog box displays.

9. Enter the range using the *from* and *to* addresses separated by a hyphen (for example, 192.168.1.10-192.168.1.20).

10. Click the **Add** button to add the range and close the dialog box. **NOTE:** You can enter multiple ranges by using the Add Range dialog box for each range you want to add.

11. To edit or delete an existing range, select the range from the list of ranges, and click the corresponding button.

12. When you have added all conditions and ranges, click the **OK** button to save the DHCP policy.

### Change an Existing Scope Policy

You can edit, delete or disable existing DHCP Scope Policies. You can also change the order of DHCP scope policies.

1. In the Scope List, right-click a scope that is stored on a Windows 2012 DHCP server and, from the shortcut menu, select **Manage Policies**. The DHCP Scope Policy Management dialog box displays.

   ![DHCP Policies dialog box](image)

   2. Select the DHCP Policy you want to work with by clicking it in the list of DHCP Policies.
      - To edit the policy, click the **Edit** button.
      - To delete the policy, click the **Delete** button.
      - To disable the policy, click the **Disable** button. If the policy is already disabled, the button text shows **Enable**. To enable the policy, click the button.
      - To move the policy up or down in the list of DHCP Policies, click the **Move Up** or **Move Down** button.

3. When you have completed your changes, click the **Close** button.
Other Functions

At any time, you can modify the properties for a scope. Simply locate the item, right-click and from the shortcut menu select Properties.

- For scopes on an MS DHCP server, refer to New DHCP Scope, MS DHCP Server.
- For scopes on an ISC DHCP server, refer to New DHCP Scope, ISC DHCP Server.
- For scopes on a Cisco DHCP server, refer to New DHCP Scope, Cisco DHCP Server.
- When a scope is opened, the system displays one tab for each server on which the scope is defined. For split scopes, the scope contents can be examined individually on each server.

In addition to the tabs displaying individual scope contents on each server, the DHCP scope dialog contains an Overview and Statistics tab, with a graphical overview of the scope contents, as well as statistics on pool utilization on all servers.

For each DHCP server containing the scope, there is a bar depicting the placement of reservations, pools, and exclude ranges in different colors.

- The top of the bar represents the IP address at the start of the scope.
- The bottom of the bar represents the IP address at the end of the scope.

This overview is useful in verifying that split scope configurations do not contain conflicts, such as overlapping pools or inconsistent reservations.

The table in the lower part of the window contains aggregate statistics for the scope, i.e., effective pool size, the number of pool clients, and the pool utilization, summed up over all servers containing the scope.

Deleting a Lease

To delete a lease in a DHCP scope, do the following:

1. Open the scope containing the lease you want to delete.
2. Right-click on the lease and, from the shortcut menu, select Release Lease.

Device Details

The Device details window contains all information pertaining to an IP address in the application, including DNS records, DHCP reservations, and custom properties. To access the Device details window from the DHCP scope dialog you need to double click on an IP address in the DHCP scope dialog, or right-click on an IP address and select the Device detail menu item.

The Device details window is documented in IP Address Management—Device Dialog Box. However, when the Device details window is opened from the DHCP scope dialog, information on any DHCP reservation associated with the IP address displays as well.

A reservation can be created by clicking the Create button on the DHCP Panel. You can also create and edit a reservation directly from the DHCP scope dialog by selecting the appropriate menu item when right-clicking on an IP address. The device dialog box is not available if only a DHCP license key has been entered. In this case, the reservation dialog box will be displayed when double clicking an entry in the DHCP scope.
Subranges of Scopes

It is possible to choose whether the contents of ranges that are created under scopes are displayed in a range view or a scope view. Use the Show DHCP data in subranges of scopes checkbox in the System Settings dialog box to choose the preferred display mode.

If the scope view is selected, a window similar to the scope window displays when you open a subrange of a scope. However, the only scope related action available in this window is reservation management. The access dialog box for these subranges will contain an additional access bit, Edit reservations.

If the range view is selected, the subranges are opened in the range view and no scope related actions are available.

Renaming a Scope

It is very simple to change the name and/or description of a scope in the Management Console.

1. Locate the DHCP Scope you want to rename.
2. Right-click and, from the shortcut menu, select Properties. The DHCP Scope Properties dialog box displays. **NOTE:** The dialog box may look different depending on the DHCP server type.
3. Enter the Title and Description.
4. Click OK. The newly renamed scope now displays in the Object List.

Superscopes

- Superscopes are only supported on MS DHCP servers on Windows 2003 and Windows 2008.
- All MS Superscopes are listed in the object section under the heading Superscopes.

- When you click on the Superscope, all scopes within that superscope display. In addition, a new column, Superscope, is shown in the scope list. It is possible to filter by this column.
To assign an existing scope to a superscope, do the following:

1. In the Object list, select a DHCP Scope for which you want to set a Superscope.
2. Right-click and, from the shortcut menu, select Properties. The scope dialog box displays.
3. Enter the name of the superscope in the Superscope field.
4. Click OK. The scope is placed in the superscope. If the superscope did not exist, the new superscope is created and now displays as a new item in the object list.

### Moving a Device

A device in a scope can be moved to a new IP address. When the device is moved, all information about the device is retained, and the associated DNS records are updated. If a reservation is associated with the device, the reservation information is moved with the device if the destination address is in a DHCP scope that is hosted on a DHCP server of the same type. If the destination address is in a scope hosted on a different type of a DHCP server or the destination is in an IP Address range, the reservation information is discarded.

To move a device, do the following:

1. Locate the IP scope containing the device you want to move.
2. Double-click on it to display the scope contents.
3. Find the applicable device.
4. Right-click and, from the shortcut menu, select Move.
5. In the **Move Device to New IP Address** dialog box, type the new IP address.

![Move Device to New IP Address dialog box]

6. Click **OK**. The device is moved to the new IP address.

---

### Host Discovery

With this feature, you can see when hosts were last seen on your network. There are two methods you can use for host discovery – using ping or querying routers for host information.

When host discovery is enabled, two columns are added to the range or scope view.

- **Last Seen.** This column identifies when a host was last seen on the network and which method was used to discover the host.

- **Last Known MAC Address.** This column shows the MAC address used by the host the last time it was seen on the network. This column is only populated if the host was seen using a router query.

### Configuring Host Discovery Using Ping

1. Select one or more scopes.

2. Right-click and, from the shortcut menu, select **Set Discovery Schedule**. The Schedule dialog box displays.

![Schedule dialog box]

3. Select the **Enable discovery schedule** option.

4. **Schedule ____ every ___ day(s)/week(s)/month(s)**. Click the drop-down list and select the frequency (e.g., Daily, Weekly, etc.) and the occurrences (e.g., 1 day, 2 weeks, etc.).

5. **At ____**. Enter the time at which discovery should take place.

6. **Starting ____**. Click the drop-down list and select the start date.

7. **Click OK**.
Once the schedule options have been set and saved, two columns - Last Seen and Last Known MAC Address - are added to the range or scope view. The Last Seen column identifies when a host was last seen on the network.

- **Green.** Host responded to the last PING request. The date and time are shown.
- **Orange.** Host has responded in the past, but did not respond to the last PING request. The date and time of last response is shown.
- **Red.** Host has never responded to a PING request. The text *Never* is shown.

The list of ranges contains a column that shows if a discovery schedule has been set for a range. The name of this column is Schedule. To quickly see all ranges that have a schedule set, you can use the Quick Filter and filter by this column by entering *Schedule:Yes* in the Quick Filter search field.

At any time if you wish to **disable** host discovery, do the following:

1. Select the object(s) for which you want to disable discovery.
2. Right-click and, from the shortcut menu, select **Set Discovery Schedule.** The Schedule dialog box displays.
3. Uncheck the **Enable discovery schedule** option.
4. Click OK.

### Configuring Host Discovery by Querying Routers

To collect information about hosts by querying routers, you must first enable collection of IP information from routers. See *Monitoring* in chapter 2 for more information.

To configure host discovery:

1. Select an IP Address Range.
2. Right-click and, from the shortcut menu, select **Configure IP Address Collection.** The IP Address Collection dialog box displays.
3. Enter the IP address of the router(s) that you want to use to collect information about hosts in the range.
4. Click OK.

Managing Failover Configurations (ISC DHCP)

This function allows you to manage DHCP failover peers on ISC DHCP servers.

**NOTE**: When adding a server's first failover peer, all other address pools on the server will be updated to refer to this failover peer.

1. On the object menu, select the DHCP Server that contains the scope for which you want to setup failover configuration.
2. From the list of scopes, double-click on the applicable one.
3. From the list of IP Addresses, right-click on the applicable one, and select **Create Address Pool** from the shortcut menu. The DHCP Address Pool dialog box displays.
4. Move to the **Failover Peer** field, and click the drop-down list arrow.
5. Select **Add new failover peer**.
6. Click **OK**. The New Failover Peer dialog box displays.

7. **Name.** Specifies the name of the failover peer.

8. **Role.** Specifies the role of the failover peer. The available roles are **Primary** and **Secondary**.

9. **Address.** Specifies the IP address or DNS name on which the server should listen for connections from its failover peer.

10. **Port.** Specifies the port number on which the server should listen for connections from its failover peer.

11. **Peer Address.** Specifies the IP address or DNS name to which the server should connect to reach its failover peer for failover messages.

12. **Peer Port.** Specifies the port number to which the server should connect to reach its failover peer for failover messages.

13. **Max Response Delay.** Specifies the number of seconds that may pass without the server receiving a message from its failover peer before it assumes that the connection has failed.

14. **Max Unacked Updates.** Specifies the number of messages the server can send before receiving an acknowledgement from its failover peer. According to ISC documentation, 10 seems to be a good value.

15. **Max Client Lead Time.** Specifies the number of seconds for which a lease can be renewed by either server without contacting the other. Only specified on the primary failover peer.

16. **Split Index.** Specifies the split between the primary and secondary failover peer for the purposes of load balancing. According to ISC documentation, 128 is really the only meaningful value. Only specified on the primary failover peer.

17. **Load Balance Max Seconds.** Specifies the cutoff in seconds after which load balancing is disabled. According to ISC documentation, a value of 3 or 5 is recommended.
18. Click **OK**. The DHCP Address Pool dialog box displays and shows the updated information.

![DHCP Address Pool dialog box]

19. Click **OK**.

If you need to **EDIT** or **DELETE** an existing failover peer, do the following:

1. Locate the relevant ISC DHCP server.
2. Right-click and, from the shortcut menu, select **Manage Failover Peers**. The Failover Peers for ... dialog box displays. All failover peers are shown.
3. To **EDIT** a failover peer, select it and click the **Edit** button. Then modify the Failover Peers ... properties dialog box, as needed.
4. To **DELETE** a failover peer, select it and click the **Delete** button.

![Failover Peers dialog box]

**NOTES**

- When deleting a failover peer through this dialog, if it is the last failover peer defined on the server, any references to it will be removed from existing address pools on the server. If there is one other failover peer left on the server, references to the failover peer being deleted will be changed to refer to the remaining failover peer. If, however, there are two or more other failover peers left on the server, the user will be prompted with a list of the remaining failover peers where he will have to choose which failover peer should be referenced by address pools currently referring to the failover peer being deleted.

- When changing from one failover peer to another for some specific address pool, if the address pool is the last one referring to the (old) failover peer, the user will be warned that performing the action will result in the deletion of the failover peer.
Managing Failover Configurations (Windows Server 2012)

DHCP failover on Windows Server 2012 enables high availability of DHCP services by synchronizing IP address lease information between two DHCP servers. It is also possible to use DHCP failover to provide load balancing of DHCP requests.

You can configure failover for a single scope or for multiple scopes on the same server.

Setting up a Scope Failover

To setup failover for a scope, do the following:

1. On the object menu, select the DHCP Server that contains the scope(s) for which you want to setup failover configuration.

2. You have two ways to choose the scopes you want to configure.
   - From the list of scopes, select one or more scopes, right-click and select Configure Failover.
   - Right-click the DHCP server and select Configure Failover. A dialog box listing all configurable scopes displays. Select the scopes you want to configure and click Next. The failover configuration dialog box displays.

3. **Relationship Name.** Select the relationship you want to use for the failover configuration or enter a name if you want to create a new relationship. If you choose an existing relationship, you will not be able to change any of the relationship properties and you can simply click OK to complete the failover configuration for the scope.

4. **Partner Server.** Enter the name or IP address of the partner DHCP server with which failover should be configured. You can select from the list of Windows Server 2012 machines or you can type the host name or IP address of the partner server.

5. **Mode.** Select the failover mode you want to use. You can choose between Hot standby and Load balance.

6. **Role of Partner Server.** If you chose the Hot standby mode, you must choose the role of the partner server. You can choose between Standby and Active. If you choose Standby the current server will be Active and vice versa.

7. **Maximum Client Lead Time.** If you don’t want to use the default values, enter the new values in the hours and minutes edit fields.

8. **Addresses reserved for standby server.** If you chose the Hot standby mode, you must enter the percentage of addresses that should be reserved to the standby server.

9. **Local server load balance percentage.** If you chose the Load balance mode, you need to specify the load balance percentage to use on the local server. The remaining percentage will be used on the partner server.

10. **State Switchover Interval.** Select this checkbox if you want to use Automatic State Switchover and specify the interval to use.
11. **Enable Message Authentication.** Select this checkbox if you want to use message authentication between the DHCP servers. If the message authentication is enabled, you must provide a shared secret for the message authentication.

**Removing a Failover Configuration**

1. On the object menu, select the DHCP Server that contains the scope(s) for which you want to remove the failover configuration.
2. Select one or more scopes, right-click the selection and select **Deconfigure Failover.** A confirmation dialog box displays.
3. Click **Yes** to confirm the action. The failover configuration for the selected scope(s) is removed.

**Replicating Failover Scopes**

When using a failover configuration, it is possible to replicate scope information between servers. This is possible for individual scopes, all scopes that share a failover relationship or all scopes on a particular DHCP server.

When a scope replication takes place, the scopes on the selected DHCP are considered the source scopes and the entire scope contents are replaced on the destination server.

*To replicate individual scopes:*

1. On the object menu, select the DHCP Server that contains the scope(s) you want to replicate.
2. Select one or more scopes, right-click the selection and select **Replicate Scope.** A confirmation dialog box displays.
3. Click **OK** to confirm the action. The selected scope is replicated.

*To replicate all scopes that share a failover relationship:*

1. On the object menu, select the DHCP Server that contains the scopes you want to replicate.
2. Right-click a scope using the desired relationship, and select **Replicate Relationship.** A confirmation dialog box displays.
3. Click **OK** to confirm the action. The scopes that use the same relationship as the selected scope are replicated. Note that this action may take some time if multiple scopes use the relationship.

*To replicate all failover scopes on a DHCP server:*

1. On the object menu, right-click the DHCP Server that contains the scopes you want to replicate and select **Replicate Failover Scopes** from the menu. A confirmation dialog box displays.
2. Click **OK** to confirm the action. All failover scopes on the selected server are replicated. Note that this action may take some time if the server contains multiple failover scopes.

**Managing Failover Relationships**

You can view, create, edit and delete existing failover relationships.

*Adding a Failover Relationship*

1. On the object menu, right-click the DHCP Server and select **Manage Failover Relationships** from the menu. A dialog box listing the current failover relationships displays.
2. Click the **Add** button. A dialog box displays, listing all scopes that are available to be configured for high availability.

3. Select the scope(s) you want to configure. To select all scopes, click the **Select all** checkbox. Click **Next**. The failover configuration dialog box displays.

4. Setup the failover configuration for the selected scopes. For more information on setting up the failover configuration, see the section **Setting up Scope Failover**.

*Editing an Existing Failover Relationship*
1. On the object menu, right-click the DHCP Server and select **Manage Failover Relationships** from the menu. A dialog box listing the current failover relationships displays.

![DHCP Failover Relationships](image)

2. Click the **Edit** button. The failover configuration dialog box displays. Note that some properties are disabled and cannot be changed.

![Configure DHCP Failover](image)

3. Edit the failover configuration and click **OK** to save the settings.

You can delete existing failover relationships. When a failover relationship is deleted, the scopes are not removed from the DHCP server, but they are no longer in a failover configuration. After removing the failover relationship the Men & Mice Suite will handle the affected scopes as split scopes.

**Deleting a Failover Relationship**

1. On the object menu, right-click on the DHCP Server, and select **Manage Failover Relationships** from the menu. A dialog box listing the current failover relationships displays.
1. Click the **Delete** button and click **Yes** in the confirmation dialog box.

### Managing Split Scopes

When a scope is hosted on multiple servers, the scope view lists all the servers that contain a copy of the scope. For scopes on MS servers, the line says ‘Split Scope’ and then lists the servers. For the ISC DHCP server, the line says ‘Multiple Instances’ and then lists the servers:

<table>
<thead>
<tr>
<th>Scope Address</th>
<th>Server Name</th>
<th>Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0.0.0/24</td>
<td>win2000.autotest.dev.lab.</td>
<td>N/A</td>
</tr>
<tr>
<td>123.0.0.0/24</td>
<td>Split Scope (1.win2000.autotest.dev.lab, 2.win2003.autotest.dev.lab.)</td>
<td>30</td>
</tr>
<tr>
<td>18.2.0.0/24</td>
<td>win2000.autotest.dev.lab.</td>
<td>N/A</td>
</tr>
<tr>
<td>18.3.0.0/24</td>
<td>win2000.autotest.dev.lab.</td>
<td>N/A</td>
</tr>
<tr>
<td>10.0.0.0/24</td>
<td>win2003.autotest.dev.lab.</td>
<td>N/A</td>
</tr>
<tr>
<td>18.0.0.0/24</td>
<td>win2003.autotest.dev.lab.</td>
<td>N/A</td>
</tr>
<tr>
<td>18.1.0.0/24</td>
<td>win2003.autotest.dev.lab.</td>
<td>N/A</td>
</tr>
<tr>
<td>10.5.0.0/24</td>
<td>Multiple Instances (1.unix.autotest.dev.lab, 2.unix.autotest.dev.lab.)</td>
<td>22</td>
</tr>
<tr>
<td>18.4.0.0/24</td>
<td>unix.autotest.dev.lab.</td>
<td>N/A</td>
</tr>
<tr>
<td>18.5.0.0/24</td>
<td>unix.autotest.dev.lab.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

The Men & Mice Suite detects when a split scope configuration is in place. Split scopes are handled as follows:

- In the scope list, split scopes are shown with a different icon and in the server column, the text "split scope" displays.
- When performing various actions on scopes (for example enable/disable, scope option changes, scope deletion), a dialog box displays where the user is asked to specify to which instances of the split scope the action should be applied.
- The DHCP scope window will show every instance of the split scope in a separate tab, making it possible to work with all instances of the split scope in a single window.
- The Overview and Statistics tab in the DHCP scope window will show a graphical overview for all of the split scope instances.
- Reservations are managed automatically. All changes to reservations (creation, modification, and deletion) are applied to all instances of the split scope.

The servers listed in this dialog box all contain the scope to which the user was applying the change. By pressing the **Enable** button, all instances of the scope would be enabled.

Split scopes are only supported on MS DHCP servers.
Chapter 11: Web Interface

Overview

The Men & Mice Web Interface allows you to perform various operations from your web browser.

To install the Men & Mice Web Interface, refer to the installation document available from our web site at www.menandmice.com.

The Men & Mice Web Interface consists of several modules, each accessed from a separate tab.

- **Advanced Zone View.** The Advanced Zone View allows you to perform basic zone management using your web browser. Using Advanced Zone View, you can perform basic DNS tasks from any workstation.

- **Basic Zone View.** The Basic Zone View contains a simplified web based interface for working with zone information. Using this interface, users with minimal DNS knowledge can make changes to zones in a quick and efficient manner. Users are only allowed to view and work with the information that they have permission to work with.

- **IP Address Management.** The IP Address Management module allows users with sufficient privileges to access the IP Address Ranges that have been assigned to them. Users can add a new host to any address in the range, or edit the properties of an existing host assignment. If the range is a part of a DHCP scope, users can work with reservations within the scope.

- **Reports.** The Report Module allows users with sufficient privileges to generate various reports in the Men & Mice Suite. After running the reports, the results can be displayed in a separate browser window. It is also possible to display the results in an Excel sheet if using Internet Explorer.

To enable this feature, the website for the Men & Mice Web interface must be added to the list of trusted sites from within Internet Explorer:

1. Choose **Tools, Internet Options.** A dialog box displays
2. Click the **Security** tab and click **Trusted Sites.**
3. Click the **Sites** button and add the website to the zone.

After adding the website, the **Export to Excel** button becomes available after running the report. Clicking this button displays the report in an Excel sheet.

**NOTE:** Based on the browser settings, there is a chance that a warning message displays when selecting a report, stating that an ActiveX control want to interact with parts of the page. If you want to suppress this message, use the following instructions:

1. Choose **Tools, Internet Options.** A dialog box displays
2. Click the **Security** tab and click **Trusted Sites.**
3. Click the **Custom Level** button. A dialog box with various settings displays.
4. Locate the setting Initialize and script ActiveX controls not marked as safe for scripting and change the setting to **Enable**.
This page intentionally left blank.
Appendix A: Command Line Interface (CLI)

Overview

The Men & Mice Command Line Interface (CLI) contains various commands to help you manage your network address space from the command line.

You can use the CLI interactively, executing one command at a time, or you can run script files to execute multiple commands in one batch. Script files can be supplied as arguments when starting the CLI and they can be run from within the CLI using the `execute` command.

This document contains a list of the commands supported by the CLI and an example script to help you get started.

Command List

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>Remark</td>
</tr>
<tr>
<td>add</td>
<td>Adds a record to a zone.</td>
</tr>
<tr>
<td>addDevice</td>
<td>Adds a device to the enclosing IP range.</td>
</tr>
<tr>
<td>addDHCPserver</td>
<td>Adds a DHCP server to the list of known DHCP servers.</td>
</tr>
<tr>
<td>addIPRange</td>
<td>Adds an IP range.</td>
</tr>
<tr>
<td>addScope</td>
<td>Adds a scope to a DHCP server.</td>
</tr>
<tr>
<td>addServer</td>
<td>Adds a name server to the list of known name servers.</td>
</tr>
<tr>
<td>addSlaveZone</td>
<td>Adds a slave zone to a server.</td>
</tr>
<tr>
<td>addZone</td>
<td>Adds a zone to a list of servers.</td>
</tr>
<tr>
<td>backup</td>
<td>Creates a backup of the Men &amp; Mice Central database.</td>
</tr>
<tr>
<td>close</td>
<td>Closes a zone without saving changes.</td>
</tr>
<tr>
<td>closeAll</td>
<td>Closes all zones without saving changes.</td>
</tr>
<tr>
<td>defaultTTL</td>
<td>Gets or sets the default TTL for a zone.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a record in a zone.</td>
</tr>
<tr>
<td>deleteZone</td>
<td>Deletes a zone.</td>
</tr>
<tr>
<td>delRec</td>
<td>Deletes a record in a zone.</td>
</tr>
<tr>
<td>DHCPServer</td>
<td>Perform various actions on DHCP servers.</td>
</tr>
<tr>
<td>DHCPServers</td>
<td>Lists all available DHCP servers.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables a record in a zone.</td>
</tr>
<tr>
<td>echo</td>
<td>Echoes text to current output.</td>
</tr>
<tr>
<td>edit</td>
<td>Changes a record in a zone.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables a record in a zone.</td>
</tr>
<tr>
<td>execute</td>
<td>Executes a script file.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>export</td>
<td>Exports a zone to an external file.</td>
</tr>
<tr>
<td>findRec</td>
<td>Finds a record in a zone.</td>
</tr>
<tr>
<td>help</td>
<td>Prints out help information.</td>
</tr>
<tr>
<td>history</td>
<td>Queries the history log.</td>
</tr>
<tr>
<td>import</td>
<td>Imports a zone from an external file.</td>
</tr>
<tr>
<td>ipRanges</td>
<td>Lists all available IP ranges.</td>
</tr>
<tr>
<td>isConnected</td>
<td>Returns true if we are connected to Men &amp; Mice Central.</td>
</tr>
<tr>
<td>listHosts</td>
<td>Lists all hosts in an IP range.</td>
</tr>
<tr>
<td>login</td>
<td>Logs on to Men &amp; Mice Central.</td>
</tr>
<tr>
<td>logMessages</td>
<td>Shows the system log messages.</td>
</tr>
<tr>
<td>modifyDevice</td>
<td>Modifies a device.</td>
</tr>
<tr>
<td>modifyIPRange</td>
<td>Modifies an IP range.</td>
</tr>
<tr>
<td>modifyZoneOptions</td>
<td>Modifies options for a zone.</td>
</tr>
<tr>
<td>open</td>
<td>Opens a zone.</td>
</tr>
<tr>
<td>print</td>
<td>Prints out one or more record from a zone.</td>
</tr>
<tr>
<td>prompt</td>
<td>Changes the prompting mode.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the program.</td>
</tr>
<tr>
<td>refresh</td>
<td>Reloads a zone from a server.</td>
</tr>
<tr>
<td>reloadZones</td>
<td>Reloads the list of zones from a server.</td>
</tr>
<tr>
<td>rem</td>
<td>Remark.</td>
</tr>
<tr>
<td>removeDevice</td>
<td>Removes a device.</td>
</tr>
<tr>
<td>removeDHCPserver</td>
<td>Removes a DHCP server from the list of known DHCP servers.</td>
</tr>
<tr>
<td>removeIPRange</td>
<td>Removes an IP range.</td>
</tr>
<tr>
<td>removeScope</td>
<td>Removes a scope from a DHCP server.</td>
</tr>
<tr>
<td>removeServer</td>
<td>Removes a server from the list of known servers.</td>
</tr>
<tr>
<td>revert</td>
<td>Reverts a DNS event.</td>
</tr>
<tr>
<td>save</td>
<td>Saves a zone.</td>
</tr>
<tr>
<td>sendMessage</td>
<td>Sends a message to all Men &amp; Mice Consoles</td>
</tr>
<tr>
<td>scope</td>
<td>Perform various actions on DHCP scopes.</td>
</tr>
<tr>
<td>scopes</td>
<td>Lists DHCP scopes.</td>
</tr>
<tr>
<td>serverInfo</td>
<td>Lists information about a server.</td>
</tr>
<tr>
<td>servers</td>
<td>Lists all available servers.</td>
</tr>
<tr>
<td>sleep</td>
<td>Sleeps for specified number of seconds.</td>
</tr>
<tr>
<td>verify</td>
<td>Syntax checks a zone.</td>
</tr>
<tr>
<td>version</td>
<td>Returns the version number of the program.</td>
</tr>
<tr>
<td>who</td>
<td>Returns a list of users that are logged in.</td>
</tr>
<tr>
<td>zonehistory</td>
<td>Queries the history log (same as the ‘history’ command).</td>
</tr>
<tr>
<td>zoneInfo</td>
<td>Lists information about a zone.</td>
</tr>
<tr>
<td>zoneModified</td>
<td>Returns indication of whether a zone has been modified.</td>
</tr>
<tr>
<td>zoneOptions</td>
<td>Returns options for a zone.</td>
</tr>
<tr>
<td>zones</td>
<td>Lists all available zones.</td>
</tr>
</tbody>
</table>
Command Descriptions

Below you will find a description of every command supported by the CLI. **NOTE:** In many commands you can use a hyphen (-) instead of `<zonename>` to specify the last zone used. For example, `close -` will close the last zone you worked with. If more than one zone with the same name is available, you might need to refer to it directly by specifying the server name and the view in which it is located. The format is `<server name>:<view name>:<zone name>.

When printing out a zone called azone.com on server mainserv, you would use the command:
```
print mainserv::azone.com.
```

If this is the only known zone named azone.com, you can simply enter:
```
print azone.com.
```

**add** `<zonename>` `<recno>` `<record>`
Adds a record to a zone. Providing `<recno>` as -1 adds the record at the end of the zone.

**addDevice** `<address>` `n=<name>` `[<CFx>=<value>]*`
Adds a device to the enclosing IP range. The IP Address `<address>` is locked for use in DNS. You can set a custom property by the name of `<CFx>` to the value `<value>`. More than one custom property value can be defined in this manner.

**addDHCPserver** `<server>` `[<proxy>]` `type=(MS|ISC|IOS) [user=<value>] [password=<value>] [<CFx>=<value>]*`
Adds a DHCP server to the list of known servers. The user and password parameters are only used for Cisco IOS servers. In case of an MS or a Cisco server, you must specify the location of the dhcpremote proxy (use 127.0.0.1 if it is running on the same machine as Central). You can set a custom property by the name of `<CFx>` to the value `<value>`. More than one custom property value can be defined in this manner.

**addIPRange** `<IP range>` `title="IP Range title" [subnet=t/f] [locked=t/f] [autoassign=t/f] [sc=<save comment>] [<CFx>=<value>]*`
Adds an IP range. The range address `<IP range>` can be in one of the following formats:
- 1.2.3.0/24
- 1.2.3/24
- 1.2.3.1-1.2.3.2
- 1.2.3.0 mask 255.255.255.0
You can set a custom property by the name of `<CFx>` to the value `<value>`. More than one custom property value can be defined in this manner.

**Example:** `addIPRange 10.10.10.0/24 title="Internal" subnet=t custom="My range"`

**addScope** `<subnet>` `<server>` `<title>` `[c=<comment>] [sc=<save comment>] [<CFx>=<value>]*`
Adds a scope to a DHCP server. You can set a custom property by the name of `<CFx>` to the value `<value>`. More than one custom property value can be defined in this manner.

**addServer** `<server>` `[<address>] [<CFx>=<value>]*`
Adds a name server to the list of known servers. You can set a custom property by the name of `<CFx>` to the value `<value>`. More than one custom property value can be defined in this manner.

**addSlaveZone** `<zonename>` `<server>` `<master address>*`
Adds a slave zone to a server. There must be at least one master IP address.

**addZone** `-DS` `<zonename>` `<server>` `[* | <slave>+] [<CFx>=<value>]*`
Adds a zone to a list of servers. The `-DS` argument specifies that the zone created should be an Active Directory zone. Slave servers are optional more than one can be specified. An asterisk (*) can be used instead of explicitly specifying slave servers. If the asterisk is used, a slave zone will be created on all servers besides the master server. You can set a custom property by the name of `<CFx>` to the value `<value>`. More than one custom property value can be defined in this manner.

**backup** `-f` `<path>`
Creates a backup of the Men & Mice Central database. If no pathname is specified, the backup file will be created in the Men & Mice Central data directory. If a backup file already exists and the `-f` argument is not provided the command will fail with an error.
close <zonename>
Closes a zone without saving changes.

closeAll
Closes all zones without saving changes.

defaultTTL <zonename> [value]
Gets or sets the default TTL for a zone. If no value is provided the command returns the current TTL value.
NOTE: This command will only work for static zones on BIND servers.
delete <zonename> <recno>
Deletes a record in a zone.
deleteZone <zonename> [server=]†
Deletes a zone. You can specify more than one server from which to remove the zone. If no servers are provided the zone will be removed from all servers.
delRec <zonename> <recname> <rectype> <recdata>
Deletes all records that match <recname>, <rectype> and <recdata> from the zone <zonename>. Instead of <recdata> you can specify a wildcard * that will match all data values.

DHCPserver <ServerAddress> <command>
Perform various actions on DHCP servers. The following commands are supported:
  show optionvalue [all]
    - Show DHCP server options
  set optionvalue [sc=savecomment] [field=value,value2,*]
    - Set DHCP server option
  delete optionvalue <OptCode>
    - Delete DHCP server option
  show properties [all]
    - Show DHCP server properties
  set property [sc=savecomment] [field1=value1] [field2=value2,*]
    - Set DHCP server properties.

DHCPservers
Lists all available DHCP servers.
disable <zonename> <recno>
Disables a record in a zone.
echo <text>
Echos <text> to current output.
edit <zonename> <recno> <record>
Changes the contents of record <recno>. The new record must be of the same type as the old one.

enable <zonename> <recno>
Enables a record in a zone.
execute <filename>
Executes a script file.
export [-aging] <zonename> <filename>
Exports a zone to an external file. -aging argument specifies that if this is a Windows zone that has scavenging active the zone file will contain the aging values for each record.
findRec <zonename> <recname> <rectype> <recdata>
Finds all records that match <recname>, <rectype> and <recdata> from the zone <zonename>. Instead of <recdata> you can specify a wildcard * that will match all data values.

help [<command>]  
Prints out help information. If a command name is provided as an argument, detailed information about that command will be displayed.

history [zone=<zonename>] [user=<username>] [fmt=(ymd|dmy|mdy)] [from=<fromdate>] [to=<todate>] [data=<text>] [limit=n]
Queries the history log. You can filter the results by zone name, user name, data and a date range. You can also use the limit parameter to specify the maximum number of entries to return (the default limit is 1000 entries).
import [-DS] [-aging] <zonename> <server> [ * | <slave>+ ] <filename>
Imports a zone from an external file. The -DS argument specifies that the zone created should be an Active
Directory zone. The -aging argument specifies that if this zone is created on a Microsoft Windows server and
<br filename> is a zone file that contains aging values for records, those values will be honored when the zone is
created.

ipRanges [-d] [-e] <filter>*
Lists all available IP ranges. If the -d argument is specified, detailed information displays. If the -e argument is
specified all ranges are displayed using the <from>-<to> format. The filters can be one or more specifying
names of a label and values of a custom property. The format of the filter is: [label]:<value>. Example:
[ Responsible Person:Joe]

isConnected
Returns true if we are connected to a Men & Mice Central server.

listHosts [-f] <IP range>
Lists all host in an IP range. If the range contains more than 4096 IP addresses and -f is not provided the
command will warn the user and ask whether it should continue. The IP range can be in one of the following
formats:
1.2.3.0/24
1.2.3/24
1.2.3.1-1.2.3.2
1.2.3.0 mask 255.255.255.0

login <server> <username> [ <password>] 
Logs on to the Men & Mice Central server. If <password> is omitted, you will be prompted for the password.

logMessages [data=<text>] [from=<fromdate>] [to=<todate>] [fmt=(ymd|dmy|mdy)]
Shows the system log messages.

modifyDevice <address> [n=<name>] [ <CFx>=<value>]*
Modifies a device. You can set a custom property by the name of <CFx> to the value <value>. More than one
custom property value can be defined in this manner.

modifyIPRange <IP range> [subnet=t/f] [locked=t/f] [autoassign=t/f] [sc=<save
comment>] [ <CFx>=<value>]*
Modifies an IP range. You can set a custom property by the name of <CFx> to the value <value>. More than one
custom property value can be defined in this manner. The range address <range address> can be in one of
the following formats:
1.2.3.0/24
1.2.3/24
1.2.3.1-1.2.3.2
1.2.3.0 mask 255.255.255.0
Example: modifyIPRange  10.10.10.0/24 locked=t

modifyZoneOptions <zonename> [allow-xfer=all|none|ns|<servers>]
[ notify=all|none|<servers>]
Modifies options for a master zone on a Windows DNS Server. The <servers> argument is a comma separated
list of IP addresses.

open <zonename>
Opens and reads a zone from server.

print [-l] <zonename> [ <range>]
Prints out a zone. <range> is optional and can be on the form <num>-<num>. If the -l argument is specified
line number are printed along with each record.

prompt [on/off]
Changes the prompting mode. With prompting on, the user is questioned about all drastic changes he is about
to make. With prompting off, the user is never prompted. If no argument is given, the program prints out whether
prompting is on or off.

quit
Quits the program.
refresh [zonename]
Reloads a zone from a server. If no zone is specified then the list of known zones and servers is refresh.

reloadZones [server]
Reloads the list of zones from a server. If no server is specified then the list of zones is reloaded from all servers.
This command differs from refresh in that it forces all server configurations to be re-read.

rem
A remark. The rest of the line is ignored. The # character can also be used to indicate a remark.

removeDevice <address>
Removes a device.

removeDHCPServer <server> [sc=save comment]
Removes a DHCP server from the list of known servers.

removeIPRange <IP range> [sc=save comment]
Removes an IP range. The IP range can be in one of the following formats:

- 1.2.3.0/24
- 1.2.3/24
- 1.2.3.1-1.2.3.2
- 1.2.3.0 mask 255.255.255.0

removeScope <ScopeAddress> [server=<ServerAddress>] [sc=savecomment]
Removes a scope from a DHCP server.

removeServer <servername>
Removes a server from the list of known servers.

revert <EventItem ID>+
Reverts a DNS event. You can specify more than one ID of events to be reverted.

save <zonename> [range=<ip range>] [sc=comment]
Saves changes made to a zone. <ip range> is the IP address range to use for auto assignment of IP addresses
for A records.
The IP range can be in one of the following formats:

- 1.2.3.0/24
- 1.2.3/24
- 1.2.3.1-1.2.3.2

sendMessage <message>
Sends a message to all Men & Mice Consoles. You must have administrator privileges to be able to send a
message.

scope <ScopeAddress> <command>
Perform various actions on DHCP scopes. The following commands are supported:

- enable [server=<ServerAddress>]
  Enable a scope on a DHCP server.
- disable [server=<ServerAddress>]
  Disable a scope on a DHCP server.
- show reservedip
  Displays all reservations in a scope.
- show excluderange
  Displays all excluded ranges in a DHCP scope.
- show iprange
  Displays all address pools in a DHCP scope.
- show clients
  Displays all clients in a DHCP scope.
- show properties
  Displays properties and custom properties of a DHCP scope.
<ServerAddress> add excluderange <StartIP> <EndIP> [sc=<savecomment>]
Adds an excluded range to a DHCP scope.

<ServerAddress> delete excluderange <StartIP> <EndIP> [sc=<savecomment>]
Deletes an exclude range from a DHCP scope.

<ServerAddress> add iprange <StartIP> <EndIP> [sc=<savecomment>]
Adds an address pool to a DHCP scope.

<ServerAddress> delete iprange <StartIP> <EndIP> [sc=<savecomment>]
Deletes an address pool from a DHCP scope.

add reservedip <ReservedIP> <MAC_Address> n=<ClientName>
Since=<ClientComment> [t=<ClientType>(DHCP | BOOTP | BOTH)]
[sc=<savecomment>]
Adds a reservation to a DHCP scope. The c=<ClientComment> argument is for MS DHCP only.

delete reservedip <ReservedIP> <MAC_address> [sc=<savecomment>]
Deletes a reservation from a DHCP scope.

set property [sc=<savecomment>] [<field1>=<value1>] [<field2>=<value2>]*
Set properties for scope.

show optionvalue
Shows DHCP scope options.

[<ServerAddress>] set optionvalue [sc=<savecomment>] [<field>=<value>,[<value2>]*]
Set DHCP scope option.

[<ServerAddress>] delete optionvalue <OptCode>
Deletes a DHCP scope option.

show reservedoptionvalue <ReservedIP>
Shows DHCP scope reservation options.

set reservedoptionvalue <ReservedIP> [<field>=<value>[],<value2>]*
[sc=<savecomment>]
Sets a DHCP scope reservation option.

delete reservedoptionvalue <ReservedIP> <OptCode>
Deletes a DHCP scope reservation option.

scopes [-s] [-d] [<server>]
Lists DHCP scopes. If <server> is specified then it will only list scopes on that server. If the -s parameter is used, the command considers split scopes when calculating free addresses in address pools. When the -d parameter is used availability of free addresses for individual split scope instances is also displayed.

serverInfo <server>
Lists information about a server.

servers
Lists all servers available.

sleep <sec>
Sleeps for the specified number of seconds.

verify <zonename>
Syntax checks a zone. Returns a list of syntax errors. If no errors exist within the zone nothing is returned.

version
Returns the version number of the program.

who
Returns a list of users that are logged in.

zonehistory
Queries the history log. For detailed description of the command see the History command.

zoneInfo <zonename>
Displays information about a zone.
zoneModified <zonename>
Returns indication of whether a zone has been modified. Returns true if zone is modified and needs to be saved.

zoneOptions <zonename>
Returns options for a zone.

zones [-n] [<server>]
Lists all available zones. If the -n argument is specified, zones are sorted alphabetically. If omitted, forward zones are listed first, then reverse zones, and finally slave zones. The argument <server> is optional. If provided, the command only lists zones on the specified server.

Example Script

The script below is intended to help you get started using the Men & Mice CLI. You can use it as a starting point when writing your own scripts.

# Demo script for Men & Mice command line interface
# start by logging in to Men & Mice Central
login server.acme.com. user password

zones

import test.zone.com. server.acme.com. zonefile.txt

print test.zone.com.

# view the change history for a single zone
history zone=test.zone.com user=administrator from=2005.2.25

# add one record to it
# NOTE: we can use '-' to refer to the last used zone and -1 means at
# the end of the zone
add - -1 test.record 1d A 10.2.3.4 ; this is comment for the new record

# Disable the third record
disable - 3

save - imported this new zone from a file and added one record

history -

# Then quit and we should be back at the OS command prompt
# NOTE: we could skip this command and return to the
# command prompt of the Men & Mice CLI
quit
Appendix B: Dynamic Zones

Overview
The Men and Mice Suite allows you to work with dynamic zones on BIND and the Windows DNS server.

This section describes how the Men & Mice Suite handles dynamic zones and how to configure your DNS server to allow the program to work with dynamic zones.

Static vs. Dynamic Zones
Due to the nature of dynamic zones, the Management Console must handle such zones differently from static zones. Below, you will find information on how the software handles dynamic zones compared to static zones.

<table>
<thead>
<tr>
<th>Static zones</th>
<th>Dynamic zones</th>
</tr>
</thead>
<tbody>
<tr>
<td>The zone content is read from disk on the server.</td>
<td>The zone content is retrieved from the server via a zone transfer.</td>
</tr>
<tr>
<td>Records can be enabled and disabled. Disabled records are commented out in the zone files.</td>
<td>Disabling records is not possible.</td>
</tr>
<tr>
<td>Specifying a TTL value for individual records is optional.</td>
<td>Every record must have a TTL explicitly set.</td>
</tr>
<tr>
<td>Every resource record can have a comment associated with it.</td>
<td>Comments are not supported for records.</td>
</tr>
</tbody>
</table>

BIND Server Configuration
The Management Console only supports TSIG signed dynamic updates. Therefore, you will have to create a TSIG key on each of your master DNS servers. If a TSIG key already exists, the program will use the first key it finds in the server configuration files (usually in /var/named/conf/user_before)

To create a TSIG key to use with BIND:

1. Check if there is a key already created in /etc/mdc.key (or its equivalent). If there is, simply copy its contents into the file user_before. Then skip the rest of these instructions.
2. Create a new key using the command `rndc-confgen`, like this:
   
   `rndc-confgen -a`

   This will create a file named rndc.key, typically in either /etc or /etc/bind. The contents of the file will look something like this:

   ```
   key rndc-key {
       algorithm hmac-md5;
       secret "Qqn05iUpjzmNoXxLJi5vXw==";
   }
   ```

3. (Re)start named (or signal it with either `kill -HUP <pid>` or `rndc reconfig`) in order to have it reload its configuration files.
4. Restart mmremoted:

    /etc/init.d/mmremote stop
    /etc/init.d/mmremote start

When you have configured the server, you can change the zone type from static to dynamic by opening the zone options in the Management Console and changing the zone type to dynamic.

As dynamic zones are transferred from the DNS server using a zone transfer, you should make sure that zone transfers are allowed to localhost.

Windows DNS Server Configuration

- The Men and Mice Management Console can work with dynamic zones on the Windows DNS server, both AD integrated zones and file-based zones.

- A new column, Record timestamp, is shown for dynamic zones that are hosted on Windows DNS servers. The Record timestamp column will show the creation time for records that are added dynamically (dynamic records). Static records will not have a record timestamp.

- Dynamic zones are transferred from the DNS server using a zone transfer. If you restrict zone transfers from your DNS server, you should make sure that zone transfers are allowed to the IP address of the DNS server itself.

- It is not possible to disable dynamic zones that are hosted on the Windows DNS server. This is the only limitation.
Appendix C: External Authentication

Overview

This section discusses the available user authentication methods available with the Men & Mice Suite.

In addition to Local User Authentication, the Men & Mice Suite currently supports two methods of AD user authentication using the Windows Active Directory user database and authentication through a RADIUS server.

Active Directory User Authentication

The Active Directory (AD) User Authentication mechanism allows you to have users authenticate themselves in the AD login system before allowing them to login to the Men & Mice Suite. In large installations, this system has obvious benefits as the users do not have to maintain their passwords in multiple locations. The password rules (password expiry, minimum password length, etc.) that have been applied within the organization automatically apply to the Men & Mice Suite.

Active Directory User Authentication vs. Local User Authentication

Even when you are using AD User Authentication, you must create users in the Management Console and assign privileges to them using the Men & Mice access system. The only difference between AD vs. local user authentication is that when AD user authentication is used, users are authenticated using the AD User Authentication system before they can access the Management Console. When AD User Authentication is used, the user password is not stored in the Men & Mice software.

NOTE: Only one authentication method can be used per user, but different users can have different authentication methods. That means you can have some users log in using AD user authentication, while other users log in using local user authentication.

Enabling AD User Authentication Using Active Directory

AD user authentication using Active Directory is only possible when you run Men & Mice Central on a Windows machine (Windows 2003/2008). The machine running Men & Mice Central must be a member in an Active Directory domain or forest.

No specific configuration is needed for Men & Mice Central for AD user authentication using Active Directory.

Configuring Users for AD Authentication

To configure a user to use AD user authentication, do the following:

1. From the menu, select Tools, Users and Groups.
2. Select the applicable user from the list. If the desired user is not shown, the user must be added to the application. Refer to Administration Functions: User Management.
3. When the Properties dialog box display, move to the Authentication field, click the drop-down list, and select the applicable authentication method. (If Men & Mice Central is not running on a Windows machine, only the Men & Mice Suite authentication method displays.)

![Image of the Properties dialog box]

4. Click OK. **NOTE:** When the AD authentication method is selected, the Password field is disabled, since the password is not stored in the Men & Mice Suite.

---

### Active Directory Single Sign-on

You can enable the Single Sign-on so that Active Directory users do not have to authenticate when logging in through the Management Console or the Command Line Interface.

To enable Active Directory Single Sign-on, do the following:

1. From the menu bar, select **Tools, System Settings**.
2. In the System Settings dialog box, click the **General Settings** tab.
3. Select the Allow Single Sign-on option.
4. Click **OK**.

---

### Web Interface

When single sign-on is enabled, it is possible to enable sign-on in the web interface if the web application is running on an IIS Server.

To enable single sign-on in the web interface, do the following:

1. Make sure that Single Sign-on and Single Sign-on for web is enabled in the Men & Mice Suite.
2. Using the IIS Administrator application, select an authentication method other than **Anonymous** and **Basic** for the MenandMice web folder.
3. Edit the file **Index.htm** in the MenandMice web folder, and change the redirection so **SSO=1** argument is specified.
4. Make **Index.htm** the default document for the site.
Application Log In

Logging into the Men & Mice Suite will not change when AD user authentication is used and Single Sign-on is disabled. The only thing to keep in mind is that the user name that is entered must match the user name stored in the Men & Mice Suite. If a distinguished user name is used, it must be entered in the same way when logging in.

Group Level Active Directory User Authentication

The Group Level Active Directory (AD) User Authentication mechanism allows you to set user access privileges by group membership in the AD. In large installations, this system has obvious benefits as the users do not have to maintain their passwords in multiple locations. The password rules (i.e., password expiry, minimum password length, etc.) that have been applied within the organization automatically apply to the Men & Mice Suite.

The login sequence is as follows for users with Group Level AD authentication:

- The user enters his/her user name and password in the Men & Mice Suite.
- The Men & Mice Suite uses the AD authentication mechanism to validate the user name and password. If the user name and password is correct, the Men & Mice Suite retrieves the group membership of the user from the AD.
- The AD group list of the user is compared (by group name) to the local group list in the Men & Mice Suite. If a match is found, the user is logged in with the privileges specified in the local group list. If no match is found, the login fails.

To allow a user to log in to the Men & Mice Suite, you must create a group in the AD that has the same name as a group in the Men & Mice Suite and place the AD user in that group. You may create multiple groups in the AD that match group names in the Men & Mice Suite.

Configuring Groups for AD Group Level Authentication

When using AD Group level authentication, you must specify which groups in the Men & Mice Suite should be used to verify group membership.

1. From the menu, select Tools, Users and Groups. The Users and groups management dialog box displays.
2. Click the Groups tab.
3. Select the group to which you want to configure AD and click the Edit button. If the desired group is not shown, you will need to add the group. Refer to Administration Features: User Management—Groups.
4. **Group Name.** Ensure that the group name is prefixed with the name of the owning domain name. Example: The Active Directory domain "MYDOMAIN" contains the group "MM-ReadOnly". The group name must then be "MYDOMAIN/MM-ReadOnly".

5. Click the checkbox for Active Directory Integrated.

6. Click OK.

Group Level Active Directory user authentication is only possible when you run Men & Mice Central on a Windows machine (Windows 2003/2008 Server). The machine running Men & Mice Central must be a member in an Active Directory domain or forest.

**Configuring Users and Access Privileges**

You do not have to create users in the Men & Mice Suite when the Group Level AD authentication is used. Instead, user access is controlled by the group membership of the user in the AD.

---

**RADIUS User Authentication**

The Men & Mice Suite can authenticate using an external RADIUS server. In large installations, this system has obvious benefits as the users do not have to maintain their passwords in multiple locations. The password rules (i.e., password expiry, minimum password length, etc.) that have been applied within the organization automatically apply to the Men & Mice Suite.

**RADIUS User Authentication vs. Local User Authentication**

Even when you are using RADIUS User Authentication, you must create users in the Management Console and assign privileges to them using the Men & Mice access system. The only difference between RADIUS vs. local user authentication is that when RADIUS user authentication is used, users are authenticated using the RADIUS User Authentication system before they can access the Management Console. When RADIUS User Authentication is used, the user password is not stored in the Men & Mice software.

*NOTE:* Only one authentication method can be used per user, but different users can have different authentication methods. That means you can have some users log in using RADIUS user authentication, while other users log in using local user authentication.

**Enabling RADIUS User Authentication**

To enable RADIUS authentication, you must add several properties to the Men & Mice Central configuration file `preferences.cfg`. This file is located in the `data` folder inside the Men & Mice Central data directory:

**Windows:** `C:\Program Files\Men & Mice\Central\data`  
**Mac OS X:** `/var/mmsuite/mmcentral`  
**All others:**  
Set during installation. Usually `/var/mmsuite/mmcentral` or `/chroot/var/mmsuite/mmcentral`, where `/chroot` is the location used as a chroot jail for named.

The properties to be added are:

- **RADIUServer**  
  Defines the address of the RADIUS server that will do RADIUS authentication.

- **RADIUSPort**  
  Defines the port that the RADIUS server is listening on. The default value is 1812, which is the port normally used by RADIUS.

- **RADIUSSharedSecret**  
  The shared secret between the RADIUS server and the Men & Mice Suite.

- **RADIUSAuthentication**  
  The type of authentication used. 0 = PAP, 1 = CHAP.
Example:

```xml
<RADIUSServer value="192.168.1.3"/>
<RADIUSPort value="1515"/>
<RADIUSSharedSecret value="MyBigSecret"/>
<RADIUSAuthentication value="1"/>
```

After editing the file, restart Men & Mice Central.

**Windows:** Use Administration Tools > Services to restart Men & Mice Central.

**Mac OS X:** Execute the following shell command in a Terminal window (/Applications/Utilities/Terminal):
```
sudo /Library/StartupItems/mmSuite/mmcentral restart
```

**All others:** Execute the `mmcentral` init script with the 'restart' argument.

### Configuring Users

To allow a user to log in to the Men & Mice system, the user must exist in the Men & Mice user database. If the user does not exist in the Men & Mice user database, they are not allowed to log in, even if they provide a valid user name and password in the RADIUS login system.

To configure a user to use AD user authentication, do the following:

1. From the menu bar, select **Tools, Users and Groups**. The User and group management dialog box displays.
2. To add a new user, click the **Add** button. **Refer to Administration Functions: User Account Management.** Follow the instructions with one exception: in the **Authentication** field, click the drop-down list and select **RADIUS**.
3. To modify an existing user, double-click on the user’s name to display the user Properties dialog box, and in the **Authentication** field, click the drop-down list and select **RADIUS**.

**NOTE:** When the RADIUS authentication method is selected, the **Password** field is disabled, since the password is not stored in the Men & Mice Suite.

### Logging into the Men & Mice Suite

Logging in to the Men & Mice Suite will not change when RADIUS user authentication is used. The only thing to keep in mind is that the user name that is entered must match the user name stored in the Men & Mice Suite.
This page intentionally left blank.
Appendix D: Application Architecture

Overview

The Men & Mice Suite consists of several components. Below, you will find a short description on each component and a high-level architectural diagram of the Men & Mice Suite architecture.

Management Console

The Men & Mice Management Console is the application you use to administer your DNS server. The Management Console runs on Windows XP or later.

CLI

The Men & Mice Management Console’s Command Line Interface contains various commands to help you manage your zones from the command line.

Web Interface

The Men & Mice Web Interface is a web interface for the Men & Mice Suite. The Men & Mice Web Interface is an AJAX Web Application that can run on top of Microsoft IIS or an Apache web server.

DNS Server Controller

The Men & Mice DNS Server Controller is used to control the DNS server and must be installed on each DNS server machine you want to control. The Men & Mice DNS Server controller reads and writes zone data and option files, and sends commands to the DNS server. The Men & Mice DNS Server Controller listens on TCP port 1337.

DHCP Server Controller

The Men & Mice DHCP Server Controller is used to control the DHCP server. For ISC DHCP, a copy should be installed on each DHCP server machine. For MS DHCP, a copy can be installed on each DHCP server machine, or in certain circumstances it can be installed on another server and connect to the DHCP service over the network. In order for this remote DHCP management to work, the DHCP Server Controller must be installed on a Windows server and must run under an account that has privileges to manage the DHCP service over the network. Operating this way, one DHCP Server Controller can manage several different DHCP servers. To manage the DHCP server on a Cisco router, the DHCP Server Controller can be installed on any machine. The DHCP Server Controller listens for connections from Men & Mice Central on port 4151/TCP.

Men & Mice Central

Men & Mice Central stores all user specific information as well as centrally stored information. One copy of Men & Mice Central needs to be installed. When a user logs into the system, they start by connecting to Men & Mice Central. Men & Mice Central handles user authentication and contains information about access privileges for the user. If the Men & Mice IP Address Management component is installed, Men & Mice Central is responsible for management and allocation of IP addresses. Men & Mice Central listens on TCP port 1231.
All communications between Men & Mice Management Console and the other Men & Mice components are encrypted.

**User Interfaces**

The Management Console and Command Line Interface connects directly to Men & Mice Central using TCP/IP connecting to through port 1231. The Men & Mice Web Interface talks directly to the Web Server (IIS or Apache) which redirects its request to Men & Mice Central also through port 1231.

**Middle Layer**

The middle layer is responsible for collecting and synchronizing data and handle requests from different Interfaces. Men & Mice Central has its own database to store all related data. The authoritative data is always the data source itself (i.e., the DNS Server). To retrieve data from the different data sources it uses various methods. It connects to Men & Mice DNS Server Controller using TCP/IP port 1337 to get and set DNS Server information. It might also communicate to other services in order to get or set information—e.g., Microsoft Active Directory to authenticate users.

**Data Layer**

The Men & Mice DNS Server Controller communicates with the DNS server using RNDC (BIND) or DNSCMD.EXE (Windows 2003/2008).
Appendix E: Central/DNS Server Controller

Overview
The Men & Mice DNS Server Controller and Men & Mice Central can be configured using command line parameters. This section describes the configuration options for Men & Mice Central and the Men & Mice DNS Server Controller.

Men & Mice Central
Men & Mice Central is available for Windows, various flavors of UNIX, and Mac OS X.

Windows
Men & Mice Central runs as a service and you can start and stop Men & Mice Central using the Services application. You can also control Men & Mice Central using these command line options:

- `mmcentral -i` Installs Men & Mice Central as a service
- `mmcentral -u` Uninstalls Men & Mice Central
- `mmcentral -start` Starts the Men & Mice Central service
- `mmcentral -stop` Stops the Men & Mice Central service
- `mmcentral -v` Displays version information
- `mmcentral -h` Displays available command line options for Men & Mice Central

UNIX
Men & Mice Central runs as a daemon on UNIX. You can use the `mmcentral` script to start and stop the Men & Mice Central daemon. The script is located in the startup scripts directory of the machine running Men & Mice Central.

- `mmcentral start` Starts the Men & Mice Central daemon
- `mmcentral stop` Stops the Men & Mice Central daemon
- `mmcentral restart` Stops and then restarts the Men & Mice Central daemon
- `mmcentral status` Displays the running state of Men & Mice Central

The Men & Mice Central binary is by default stored at the following location: `/usr/sbin/mmcentrald`
You can set several options when starting Men & Mice Central:

- **-ll <level>**  
  Men & Mice Central sends event messages to the system log. You can change the log level for Men & Mice Central by using the `–ll` command-line option when starting the daemon. Possible levels are 0 - 5 (the default value is 3)

- **-p <port>**  
  Set port number to listen to (default 1231)

- **-u <user>**  
  Specifies the user name or user id that the program should run as

- **-g <group>**  
  Specifies the group name or group id that the program should run as

- **-d <path>**  
  Sets the path where the data files should be located (the default path is /var/mmsuite/mmcentral)

- **-v**  
  Displays version information

- **-h**  
  Displays available command line options for Men & Mice Central

**Example:** `mmcentrald -p 9876 -ll 5 -d /temp/data`

**Mac OS X**

Men & Mice Central runs as a daemon on Mac OS X. You can use the `mmcentral` script to start and stop the Men & Mice Central daemon. The script is located in the `/Library/StartupItems/` directory.

- **mmcentral start**  
  Starts the Men & Mice Central daemon

- **mmcentral stop**  
  Stops the Men & Mice Central daemon

- **mmcentral restart**  
  Stops and then restarts the Men & Mice Central daemon

- **mmcentral status**  
  Displays the running state of Men & Mice Central

The Men & Mice Central binary stored at the following location: `/usr/sbin/mmcentrald`

You can set several options when starting Men & Mice Central:

- **-ll <level>**  
  Men & Mice Central sends event messages to the system log. You can change the log level for Men & Mice Central by using the `–ll` command-line option when starting the daemon. Possible levels are 0 - 5 (the default value is 3)

- **-p <port>**  
  Set port number to listen to (default 1231)

- **-u <user>**  
  Specifies the user name or user id that the program should run as

- **-g <group>**  
  Specifies the group name or group id that the program should run as

- **-d <path>**  
  Sets the path where the data files should be located (the default path is /var/mmsuite/mmcentral)

- **-v**  
  Displays version information

- **-h**  
  Displays available command line options for Men & Mice Central

**Example:** `mmcentrald -p 9876 -ll 5 -d /temp/data`
DNS Server Controller

The Men & Mice DNS Server Controller is available for Windows, various flavors of UNIX, and Mac OS X.

Windows

The Men & Mice DNS Server Controller runs as a service and you can start and stop the Server Controller using the Services application. You can also control the Men & Mice DNS Server Controller using these command line options:

- `mmremote -i` Installs the Men & Mice DNS Server Controller as a service
- `mmremote -u` Uninstalls the Men & Mice DNS Server Controller
- `mmremote -start` Starts the Men & Mice DNS Server Controller service
- `mmremote -stop` Stops the Men & Mice DNS Server Controller service
- `mmremote -v` Displays version information
- `mmremote -h` Displays available command line options for the Men & Mice DNS Server Controller

UNIX

The Men & Mice DNS Server Controller runs as a daemon on Unix. You can use the `mmremote` script to start and stop the Men & Mice DNS Server Controller daemon. The script is located in the startup scripts directory of the machine running the Men & Mice DNS Server Controller.

- `mmremote start` Starts the Men & Mice DNS Server Controller daemon
- `mmremote stop` Stops the Men & Mice DNS Server Controller daemon
- `mmremote restart` Stops and then restarts the Men & Mice DNS Server Controller daemon
- `mmremote status` Displays the running state of the Men & Mice DNS Server Controller

The Men & Mice DNS Server Controller binary is by default stored at the following location:

```
/usr/sbin/mmremoted
```

You can set several options when starting the Men & Mice DNS Server Controller:

- `-ll <level>` The Men & Mice DNS Server Controller sends event messages to the system log. You can change the log level for the Men & Mice DNS Server Controller by using the `-ll` command-line option when starting the daemon. Possible levels are 0 - 5 (the default value is 3)
- `-p <port>` Set port number to listen to (default 1337)
- `-u <user>` Specifies the user name or user id that the program should run as
- `-g <group>` Specifies the group name or group id that the program should run as
- `-t <path>` Specifies the directory for the program to chroot() to in a jailroot configuration
- `-c <file>` Location of the BIND configuration file (the default location is /etc/named.conf)
- `-v` Displays version information
- `-h` Displays available command line options for the Men & Mice DNS Server Controller

Example: `mmremoted -p 9876 -ll 5`
Mac OS X

The Men & Mice DNS Server Controller runs as a daemon on Mac OS X. You can use the mmremote script to start and stop the Men & Mice DNS Server Controller daemon. The script is located in the /Library/StartupItems/ directory.

mmremote start     Starts the Men & Mice DNS Server Controller daemon
mmremote stop      Stops the Men & Mice DNS Server Controller daemon
mmremote restart   Stops and then restarts the Men & Mice DNS Server Controller daemon
mmremote status    Displays the running state of the Men & Mice DNS Server Controller

The Men & Mice DNS Server Controller binary is by default stored at the following location:
/usr/sbin/mmremoted

You can set several options when starting the Men & Mice DNS Server Controller:

-ll                   The Men & Mice DNS Server Controller sends event messages to the system log. You can change the log level for the Men & Mice DNS Server Controller by using the –ll command-line option when starting the daemon. Possible levels are 0 - 5 (the default value is 3)
-ll <level>            The Men & Mice DNS Server Controller sends event messages to the system log. You can change the log level for the Men & Mice DNS Server Controller by using the –ll command-line option when starting the daemon. Possible levels are 0 - 5 (the default value is 3)
-p <port>             Set port number to listen to (default 1337)
-u <user>             Specifies the user name or user id that the program should run as
-g <group>            Specifies the group name or group id that the program should run as
-t <path>             Specifies the directory for the program to chroot() to in a jailroot configuration
-c <file>             Location of the BIND configuration file (the default location is /etc/named.conf)
-v                    Displays version information
-h                    Displays available command line options for the Men & Mice DNS Server Controller

Example: mmremoted -p 9876 -ll 5
Appendix F: BIND DNS File Structure

Overview

When the Men & Mice Suite is installed on a server running BIND, it needs to perform several changes to the server configuration file structure. This section describes these changes and includes an overview diagram that shows how the server configuration files are processed after the Men & Mice Suite has updated the structure.

named.conf

- named.conf is split into several files. A new named.conf file that includes statements for all the new files is created.
- When named.conf is split up, a new file is created for each zone statement (see Zone options files, below).
- The options statement goes into a separate file. That file is modified when the user makes changes to the server options in the Men & Mice Management Console.
- The current version of the Men & Mice Management Console has no interface to change the values of the following statements: key, acl, controls, server, trusted-keys. Therefore, they are kept in separate files, user_before and user_after. The Men & Mice Suite does not modify these files.
- The hint zone is copied to /var/named/conf/root.hint. That file is modified when the user makes changes in the Root servers tab in the server options in the Men & Mice Management Console.

Zone Options Files

A new file, /var/named/conf/zones is created. It contains a list of includes for zone option files which are stored in the directory /var/named/conf/zoneopt/, one for each zone. The zone options (or definitions) files are called <zonename>.opt

Zone Files

No changes are made to the zone files themselves. The installer copies the zone files to different directories, depending on their types:

- master and forward zones are copied to /var/named/hosts/masters/
- slave and stub zones are copied to /var/named/hosts/slaves/

The new zone file is named <zonename>-hosts
The following diagram provides an overview on how the configuration files are processed after the file structure has been updated by the Men & Mice Suite.

File: `/etc/named.conf`
- include /var/named/conf/logging;
- include /var/named/conf/user_before;
- include /var/named/conf/options;
- include /var/named/conf/user_after;
- include /var/named/conf/zones;

Directory: `/var/named/conf`
- File: `logging`
  Contains the logging statement
- File: `user_before`
  Contains all acl and key statement. It may not contain any other statements.
  Note: Men & Mice Suite does not modify this file so the user can change it, as applicable.
- File: `options`
  Contains the options statement
- File: `user_after`
  Contains the root.hint. zone statement. It can also contain controls, server, and trusted keys statements.
  Note: Men & Mice Suite does not modify this file so the user can change it, as applicable.
- File: `zones`
  Contains include statements for all the zones on the server.
  Example
  include conf/zoneopt/text.com.opt;
  include conf/zoneopt/dynamic.net.opt;

Directory: `/var/named/conf/zoneopt`
- File: `<zonename>.opt`
  Contains zone definition and options for `<zonename>`.
  Example:
  zone test.com. IN {
  type master;
  file hosts/masters/test.com-hosts;
  allow-query { any; };
  };

Directory: `/var/named/hosts/masters`
- File: `test.com-hosts`
  The actual zone file (hosts file).
Appendix G: External Scripts

Overview

The system can be configured to run external scripts under several conditions:

- When object properties are modified.
- When zone contents are changed.
- When the number of free addresses in subnets go below a set threshold.

Scripts associated with object types are often used to perform lookups in external data sources and return data from these sources. To configure the system to run a script when properties for an object are modified or when zone contents are changed, do the following:

1. Log in as Administrator.
2. From the menu, select **Tools, System Settings**.
3. In the System settings dialog box, click the **External Commands** tab.
4. In the applicable field (e.g., Range script, IP address script, etc.), type the script name and necessary startup parameters. You must enter all information for the script as you would when invoking the script from the command line. It is assumed that the script is located in the same directory as Men & Mice Central; however, if the script is stored in a different location, the path for the script must be entered.

   **Example 1:** Running a script named mytest.vb. To run a script named mytest.vb that is located in the Men & Mice Central directory using the scripting host cscript, the following would be placed in the appropriate field: `cscript /B mytest.vb`

   **Example 2:** Running an executable named checkdata.exe. To run an executable named checkdata.exe that is located in the Men & Mice Central directory the following would be placed in the appropriate field: `checkdata.exe`.

5. Click **OK**.

To configure the system to run a script when the number of free addresses in a subnet goes below a user-definable threshold, see **Subnet Monitoring** in chapter 7.
Script Interfaces

When Men & Mice Central runs an external script, it sends an XML structure as an argument to the script being called. The XML structure contains information about all custom properties that are defined for the object type. The XML structure also contains the login name of the user that triggered the script.

The XML structures differ a little depending on the type of script (property change, zone contents change, scope monitoring).

Property Change Script Interface

The XML schema for a property change script is as follows:

```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema targetNamespace="http://tempuri.org/XMLSchema.xsd" elementFormDefault="qualified"
xmlns:xmns="http://www.w3.org/2001/XMLSchema">
<xs:element name="externalScriptParameters">
<xs:complexType>
<xs:sequence>
<xs:element ref="customFields" minOccurs="1" maxOccurs="1" />
</xs:sequence>
<xs:attribute name="userName" type="xs:string" />
</xs:complexType>
</xs:element>
<xs:element name="customFields">
<xs:complexType>
<xs:sequence>
<xs:element ref="customField" minOccurs="1" maxOccurs="unbounded" />
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="customField">
<xs:complexType>
<xs:sequence>
<xs:attribute name="customFieldID" type="xs:string" />
<xs:attribute name="customFieldName" type="xs:string" />
<xs:attribute name="objectId" type="xs:string" />
<xs:attribute name="objectType" type="xs:string" />
<xs:attribute name="value" type="xs:string" />
</xs:complexType>
</xs:element>
</xs:schema>
```

An example XML structure with three custom properties named Location, Country and Region might look as follows:

```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<externalScriptParameters username="administrator">
<customFields>
<customField customFieldID="24" customFieldName="Location" objectId="27" objectType="4" value="location1"></customField>
<customField customFieldID="25" customFieldName="Country" objectId="27" objectType="4" value=""></customField>
<customField customFieldID="26" customFieldName="Region" objectId="27" objectType="4" value=""></customField>
</customFields>
</externalScriptParameters>
```

Upon completion, the script must create a new XML structure and return it to Men & Mice Central. The schema for the XML structure that is returned is as follows:

```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
```
An example XML structure with three custom properties named Location, Country and region might look as follows:

```xml
<?xml version="1.0"?>
<result success="1">
  <customFields>
    <customField customFieldID="24" customFieldName="loc" objectID="27" objectType="4" value="location1"/>
    <customField customFieldID="25" customFieldName="Country" objectID="27" objectType="4" value="USA"/>
    <customField customFieldID="26" customFieldName="Region" objectID="27" objectType="4" value="Texas"/>
  </customFields>
</result>
```

Men & Mice Central uses the information in the XML structure to update other custom properties or to display an error message if the success attribute on the result element is set to 0. The following XML example shows how an error message can be returned by the external script.

```xml
<?xml version="1.0"?>
<result success="0">
  <error code="1" message="The error message."/>
</result>
```
The XML structure is not required to return information about all custom properties, only fields that the script has changed. Unknown property fields are ignored by Men & Mice Central.

**Zone Content Change Script Interface**

The XML schema for a zone content change script is as follows:

```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema targetNamespace="http://tempuri.org/XMLSchema.xsd" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="externalScriptParameters">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="object" minOccurs="1" maxOccurs="1" />
    </xs:sequence>
    <xs:attribute name="userName" type="xs:string" />
  </xs:complexType>
</xs:element>
<xs:element name="object">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="id" type="xs:integer" minOccurs="1" maxOccurs="1" />
      <xs:element name="type" type="xs:integer" minOccurs="1" maxOccurs="1" />
      <xs:element name="server" type="xs:string" minOccurs="1" maxOccurs="1" />
      <xs:element name="view" type="xs:string" minOccurs="1" maxOccurs="1" />
      <xs:element name="zone" type="xs:string" minOccurs="1" maxOccurs="1" />
      <xs:element name="fqName" type="xs:string" minOccurs="1" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
</xs:schema>
```

An example XML structure for a zone change script might look as follows for a zone that exists in a view:

```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<externalScriptParameters userName="administrator">
  <object>
    <id>2534</id>
    <type>13</type>
    <server>bind1.corp.net.</server>
    <view>internal</view>
    <zone>zone.com.</zone>
    <fqName>bind1.corp.net::internal:zone.com.</fqName>
  </object>
</externalScriptParameters>
```

An example XML structure for a zone change script might look as follows for a zone that is not in a view:

```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<externalScriptParameters userName="administrator">
  <object>
    <id>2635</id>
    <type>13</type>
    <server>dns1.corp.net.</server>
    <view />
    <zone>my.zone.com.</zone>
    <fqName>dns1.corp.net.:my.zone.com.</fqName>
  </object>
</externalScriptParameters>
```

A zone content change script does not have any return value.
**Subnet Monitoring Script Interface**

The XML schema for a subnet monitoring script is as follows:

```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema targetNamespace="http://tempuri.org/XMLSchema.xsd" elementFormDefault="qualified"
  xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="scopeMonitor">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="scope" type="xs:string" minOccurs="0" maxOccurs="1" />  
        <xs:element name="server" type="xs:string" minOccurs="0" maxOccurs="1" />  
        <xs:element name="superscope" type="xs:string" minOccurs="0" maxOccurs="1" />  
        <xs:element name="threshold" type="xs:integer" minOccurs="1" maxOccurs="1" />  
        <xs:element name="available" type="xs:integer" minOccurs="1" maxOccurs="1" />  
        <xs:element name="fixed" type="xs:boolean" minOccurs="1" maxOccurs="1" />  
        <xs:element name="thresholdType" type="xs:string" minOccurs="1" maxOccurs="1" />  
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

The value of the `thresholdType` element will be either static or dynamic depending on whether the threshold being crossed is one of dynamically allocatable addresses (i.e. available addresses in address pools) or if it is a threshold set for static addresses (i.e. available addresses outside of address pools).

**NOTE:** The global subnet monitor, set through the system settings dialog, is the only one that takes superscopes into account. When the global subnet monitor actions are performed, due to the conditions being met for a superscope, the XML generated will contain a `<server>` tag and a `<superscope>` tag.

An example XML structure for a subnet monitoring script might look as follows for scope:

```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<scopeMonitor>
  <scope>123.45.67.0/24</scope>
  <threshold>20</threshold>
  <available>8</available>
  <fixed>0</fixed>
  <thresholdType>dynamic</thresholdType>
</scopeMonitor>
```

The XML structure is slightly different if a superscope (MS DHCP) or a shared-network (ISC DHCP) configuration is used. An example XML structure for a scope monitoring script might look as follows for a superscope / shared-network configuration:

```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<scopeMonitor>
  <server>dhcp1.corp.net.</server>
  <superscope>office</superscope>
  <threshold>20</threshold>
  <available>22</available>
  <fixed>1</fixed>
  <thresholdType>dynamic</thresholdType>
</scopeMonitor>
```

A subnet monitoring script does not have any return value.
Example Script

The following example script, written in Visual Basic, shows how a script could return different values depending on the user that is running the script. The script is called when an object property changes.

```vba
Dim fso, stdin, stdout, stderr, xmlDoc

' The next four lines connect the script and the "Men & Mice Suite"
Set fso = CreateObject("Scripting.FileSystemObject")
Set stdin = fso.GetStandardStream (0)
Set stdout = fso.GetStandardStream (1)
Set stderr = fso.GetStandardStream (2)

Set xmlDoc=CreateObject("Microsoft.XMLDOM")
xmlDoc.async="false"

' read xml from MMSuite
xmlDoc.loadXml(stdin.ReadAll)

Dim xElLocationCodeField, theCode, xElCustomFields, theUser

' Get the username
theUser = xmlDoc.selectSingleNode("/externalScriptParameters").getAttribute("userName")

' Select all the customfields
Set xElCustomFields = xmlDoc.selectSingleNode("/externalScriptParameters/customFields")

' Get the current value of the location code field
Set xElLocationCodeField =
  xElCustomFields.selectSingleNode("customField[@customFieldName='Location']")
theCode = xElLocationCodeField.getAttribute("value")

Dim success, retVal1, retVal2
success = false

' Very simple logic, here a DB query could be performed or some other lookup
if theCode = "l1" then
  retVal1 = "USA"
  retVal2 = "Washington"
  success = true
elseif theCode = "l2" then
  retVal1 = "UK"
  retVal2 = "London"
  success = true
end if

Dim xReturnDoc, xElResult
' create return document
Set xReturnDoc = CreateObject("Microsoft.XMLDOM")
Set xElResult = xReturnDoc.createElement("result")

if success then
  xElResult.setAttribute "success", "1"
  ' set the value of xml that we return. It is OK to omit fields that are not changed by script
  xElResult.appendChild xElCustomFields.cloneNode(true)
  Dim xElChange
  Set xElChange =
    xElResult.selectSingleNode("/customFields/customField[@customFieldName='Country']")
  xElChange.setAttribute "value", retVal1
  Set xElChange = xElResult.selectSingleNode("/customFields/customField[@customFieldName='City']")
  xElChange.setAttribute "value", retVal2
```

---

Example Script

The following example script, written in Visual Basic, shows how a script could return different values depending on the user that is running the script. The script is called when an object property changes.

```vba
Dim fso, stdin, stdout, stderr, xmlDoc

' The next four lines connect the script and the "Men & Mice Suite"
Set fso = CreateObject("Scripting.FileSystemObject")
Set stdin = fso.GetStandardStream (0)
Set stdout = fso.GetStandardStream (1)
Set stderr = fso.GetStandardStream (2)

Set xmlDoc=CreateObject("Microsoft.XMLDOM")
xmlDoc.async="false"

' read xml from MMSuite
xmlDoc.loadXml(stdin.ReadAll)

Dim xElLocationCodeField, theCode, xElCustomFields, theUser

' Get the username
theUser = xmlDoc.selectSingleNode("/externalScriptParameters").getAttribute("userName")

' Select all the customfields
Set xElCustomFields = xmlDoc.selectSingleNode("/externalScriptParameters/customFields")

' Get the current value of the location code field
Set xElLocationCodeField =
  xElCustomFields.selectSingleNode("customField[@customFieldName='Location']")
theCode = xElLocationCodeField.getAttribute("value")

Dim success, retVal1, retVal2
success = false

' Very simple logic, here a DB query could be performed or some other lookup
if theCode = "l1" then
  retVal1 = "USA"
  retVal2 = "Washington"
  success = true
elseif theCode = "l2" then
  retVal1 = "UK"
  retVal2 = "London"
  success = true
end if

Dim xReturnDoc, xElResult
' create return document
Set xReturnDoc = CreateObject("Microsoft.XMLDOM")
Set xElResult = xReturnDoc.createElement("result")

if success then
  xElResult.setAttribute "success", "1"
  ' set the value of xml that we return. It is OK to omit fields that are not changed by script
  xElResult.appendChild xElCustomFields.cloneNode(true)
  Dim xElChange
  Set xElChange =
    xElResult.selectSingleNode("/customFields/customField[@customFieldName='Country']")
  xElChange.setAttribute "value", retVal1
  Set xElChange = xElResult.selectSingleNode("/customFields/customField[@customFieldName='City']")
  xElChange.setAttribute "value", retVal2
```
else
    xElResult.setAttribute "success", "0"
    'add error element
    Dim xElError
    Set xElError = xReturnDoc.createElement("error")
    xElError.setAttribute "code", "1"
    xElError.setAttribute "message", "Unknown location."
    xElResult.appendChild xElError
end if

xReturnDoc.appendChild xElResult

'finally return the xml
stdout.WriteLine xReturnDoc.xml
This page intentionally left blank.
Appendix H: Secure64 Integration

Overview

This section explains how to enable support for the Secure64 DNS Signer in the Men & Mice Suite.

The following components are required for Secure64 DNS Signer integration:

- A Secure64 DNS Signer
- At least two DNS servers. These can be BIND or MS Windows servers. One will be a hidden master and the other servers will be slave servers

Enabling Support for the Secure64 DNS Signer

To create a zone and have the Men & Mice Suite automatically configure the zone for signing on the Secure64 DNS Signer, you first have to enable the Secure64 integration.

1. From the Tools menu, select System Settings. The System Settings dialog box displays.
2. Click the DNS tab.
3. **Enable Secure64 integration.** Click in the checkbox to enable this feature.
4. **Server name.** Type the name of the server.
5. **User.** Type the username. This must be the user name of someone who has the appropriate credentials for a user account that exists on the Secure64 server and is allowed to manage the server.
6. **Password.** Type the password.
7. Click OK.
Creating DNSSEC Signed Zones

Next, you create zones in the Men & Mice Suite and have the system create the zone on the hidden master, the Secure64 DNS Signer, and the slaves.

1. From the menu bar, select **New, Master Zone**. The Create Zone dialog box displays.

2. In this dialog box, select which server should be the (hidden) master and which server(s) should be the slave(s).

3. Click the **Create** button. A new zone window displays in which you can create new records for the zone and/or paste records from other zones.

4. Once you have created the new records, click **File, Save**. The application displays what changes have been made to the zone, and asks you for a Save comment.

5. Click **OK** and all the servers will be configured.
Viewing DNSSEC Records

To see all the DNSSEC records that were added to the zone you need to open the zone from one of the slave servers by doing the following:

1. Expand the **DNS Servers** in the left side panel.
2. Select the slave server. This will display all the zones on the server.
3. Double-click on the zone to see the records in the zone.
4. Make sure the **Hide DNSSEC records** checkbox is unchecked in the toolbar to see the DNSSEC records. It may take a few moments for the zone to be created, sign onto the Secure64 DNS Signer, and transfer to the slaves.
This page intentionally left blank.
Appendix I: Replacing the Database Engine

Overview

The default database engine for the Men & Mice Suite can be replaced and the MS SQL Server or Oracle 11g can be used instead. Using either of these database servers is preferred for large installations.

See the Men & Mice knowledgebase, http://kbase.menandmice.com/ for more information on the database Server configuration options for the Men & Mice Suite.
Appendix J: Backing Up and Restoring the SQLite Database

Overview

This section explains how to backup and restore the database file when using the SQLite database engine.

Backing up the Database

SQLite stores all database information for the Men & Mice Suite in a single file named mmsuite.db. On Windows this file can be found at C:\Program Files\Men and Mice\Central\ or at C:\ProgramData\Men and Mice\Central\ On Unix based systems, the database file can be found at /var/mmsuite/central

When Men & Mice Central is running, the database file is open so copying the file directly can result in a corrupt backup of the file. The best way to back up the database file is to use the Command Line Interface (CLI). The CLI contains a backup command that allows backing up a running database.

To backup the database using the CLI you need to execute these commands within the command line shell:

```
login server administrator password
backup /some/path
exit
```

For more information on the backup command, see the CLI documentation in Appendix A.

**NOTE:** You can use a scheduled script to backup the database automatically. The Scheduled Scripts section in this user manual contains an example on how to backup the database using a script.

Restoring the Database

To restore the database, you must first stop Men & Mice Central and then replace the database file. The process for restoring the database differs a little depending on the OS running Men & Mice Central.

**Windows**

To restore the SQLite database file on Windows, do the following:

1. Install Men & Mice Central, if necessary.
2. Stop the Men & Mice Central service.
3. Restore the mmsuite.db data file by copying it to the correct location. The default location for the data file is either C:\Program Files\Men and Mice\Central\ or C:\ProgramData\Men and Mice\Central\ If an older mmsuite.db file is already present, you might want to rename it before restoring.
4. Start the Men & Mice Central service.
**Linux and Solaris**

To restore the SQLite database file on Linux and Solaris:

1. Install Men & Mice Central, if necessary.
2. Stop Men & Mice Central by issuing the following command:

   ```sh
sudo /etc/init.d/mmcentral stop
   ```
3. Restore the mmsuite.db data file by copying it to the correct location. The default location for the data file is `/var/mmsuite/central/` If an older mmsuite.db file is already present, you might want to rename it before restoring.
4. Start Men & Mice Central by issuing the following command:

   ```sh
   sudo /etc/init.d/mmcentral start
   ```

**Mac OS X**

To restore the SQLite database file on Mac OS X:

1. Install Men & Mice Central, if necessary.
2. Stop Men & Mice Central by issuing the following command:

   ```sh
   sudo /Library/StartupItems/mmCentral/mmCentral stop
   ```
3. Restore the mmsuite.db data file by copying it to the correct location. The default location for the data file is `/var/mmsuite/central/` If an older mmsuite.db file is already present, you might want to rename it before restoring.
4. Start Men & Mice Central by issuing the following command:

   ```sh
   sudo /Library/StartupItems/mmCentral/mmCentral start
   ```
Index

A
About Menu, 8
Active Directory Single Sign-on, 170
Active Directory User Authentication, 169
AD Sites and Subnets, 105
AD Sites/Subnets
adding AD forest, 105
changing AD forest properties, 106
managing, 106
overview, 105
reloading AD forest, 106
removing AD forest, 106
Administration Functions, 21
Advanced Options, 78
Application Architecture, 175
Application Log In, 171

B
Backing Up and Restoring the SQLite Database, 197
BIND
DNS File Structure, 181
server configuration, 167

C
Central/DNS Server Controller, 177
CLI, 175
Command Descriptions, 161
Command Line Interface, 159
Command List, 159
Example Script, 166
Configuring Groups for AD Group Level Authentication, 171
Configuring Users, 173
access privileges, 172
AD authentication, 169
Custom Properties
adding, 34
define, 34
deleting, 36
displaying, 36
editing, 36
opening, 36

D
Data Layer, 176
Database Engine
replacing, 195
Detail View, 5
DHCP Scope, 123
access, 135
delete, 135
device details, 143
disable, 135
duplication wizard, 136
enable, 135
delete, 51edit name, 50
info, 62
log, 62
new, 49
options, 51
overview, 49
properties, 61
reload, 63
reload zone list, 63
Windows, 52
DNS Zone, 65
access, 68
analysis, 67
BIND servers, 77
delete, 69
disable/enable, 69
DNSSEC management, 74
DNSSEC zones, 74
duplicate, 70
edit preferred servers, 70
export, 70
folders, 71
forward zone, 71
icons, 65
import, 71
master zone, 72
options, 75
options for, 78
overview, 65
promote slave to master, 79
properties, 79
reload, 79
remove from folder, 80
searching, 80
slave zone, 81
stub zone, 81
view history, 82
viewing, 66
Windows and BIND, 75
zone wizard, 82
Dynamic Zones, 167

E
Edit Menu, 6
Enabling AD User Authentication Using Active Directory, 169
Enabling RADIUS User Authentication, 172
Example Script, 188
External Authentication, 169
External Commands, 27
External Scripts, 183

F
File Menu, 6
Filter
clearing an entry, 12
deleting, 12
saving, 12

G
Global Access
selecting users, 46
Global Access, 41
access control dialog box, 46
access flags defined, 44
administrator, 41
built-in groups, 41
edit access flag, 43
new objects, 43
overriding access settings, 42
selecting groups, 46
Group Level Active Directory User Authentication, 171
Groups, 32
adding new, 32
deleting, 33
editing, 32

H
High-level Architectural Diagram, 176

I
Initial Access for, 47
Installation, 1
IP Address Management, 91
address records, 91
allocate ranges wizard, 99
device dialog box, 95
generate reverse zones wizard, 98
host discovery, 100
join ranges, 99
list, 94
moving a device, 98
multiple address spaces, 103
new ranges, 92
overview, 91
range access, 91
range configuration, 93
range deletions, 94
range modifications, 94
range toolbar, 10
remove from folder, 101
select parent, 100
split range wizard, 98
subnet monitoring, 102
viewing, 91
ISC DHCP Scope
managing failover configurations, 148

K
Keywords, 11

L
Lease History, 14
License Key
adding, 33
removing, 33
License Management, 33
Logging into the Men & Mice Suite, 173

M
Maintenance, 39
find concurrent leases, 39
find orphaned PTR records, 39
show multiply defined PTR records, 40
show round robin records, 40
Management Console, 3, 175
first use wizard, 4
GUI interface, 4
launching, 3
Men & Mice Central, 175
Men & Mice Suite, 1
Menu Bar, 6
Middle Layer, 176
O
Object Browser, 5
Object Change History, 15
Object Folders, 19
creating new, 19
creating subfolder, 19
deleting, 20
renaming, 20
specifying items access, 20
P
Preferences, 13
Program Preferences
console, 13
new zone window, 13
Program Preferences
log window, 13
Property Change Script Interface, 184
Q
Query Menu, 8
Quick Filter, 11
R
RADIUS User Authentication, 172
RADIUS User Authentication vs. Local User Authentication, 172
Regular Expressions, 11
Resource Records, 83
S
Scheduled Scripts, 37
Scope Toolbar, 10
Script Interface, 184
Search/Update Wizard, 14
Secure64 Integration, 191
Select All, 113
Slave Zones
BIND Servers, 78
Sorting Records, 6
Static Zones, 167
Subnet Monitoring Script Interface, 187
System Requirements, 1
System Settings, 21
DNS, 27
error checking, 24
external commands, 26
general, 22
logging, 23
monitoring, 27
save comments, 26
sites and subnets, 25
T
_toolbar, 9
U
User Interfaces, 176
User Management, 30
Users, 30
adding, 30
editing, 31
removing, 31
viewing activity, 31
W
Web Interface, 170, 175
Web User Interface, 157
Wildcards, 11
Window Menu, 8
Windows DNS Server Configuration, 168
Z
Zone Content Change Script Interface, 186
Zone Toolbar, 9

Men and Mice Suite v6.3.5  Index  201