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**.

The System Settings dialog box displays and includes these tabs:

- General
- Logging
- Error Checking
- Save Comments
- External Commands
- DNS
- IPAM
- Monitoring

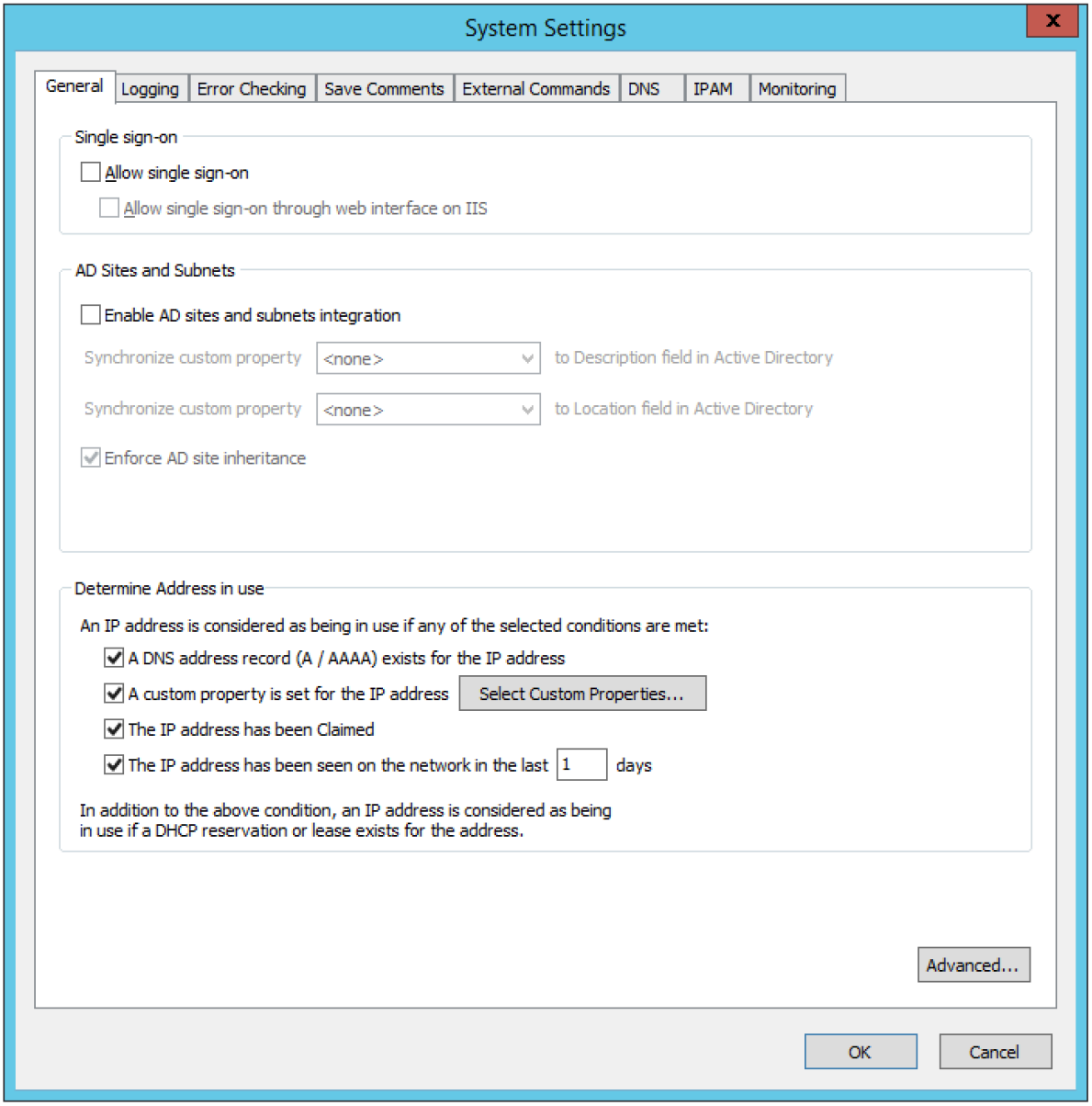
General

Through this function, you can specify the following:

- Whether to allow single sign-on
- Settings for AD Sites and Subnets integration
- Rules to determine when an IP address is considered as being in use
- Advanced system settings

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

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

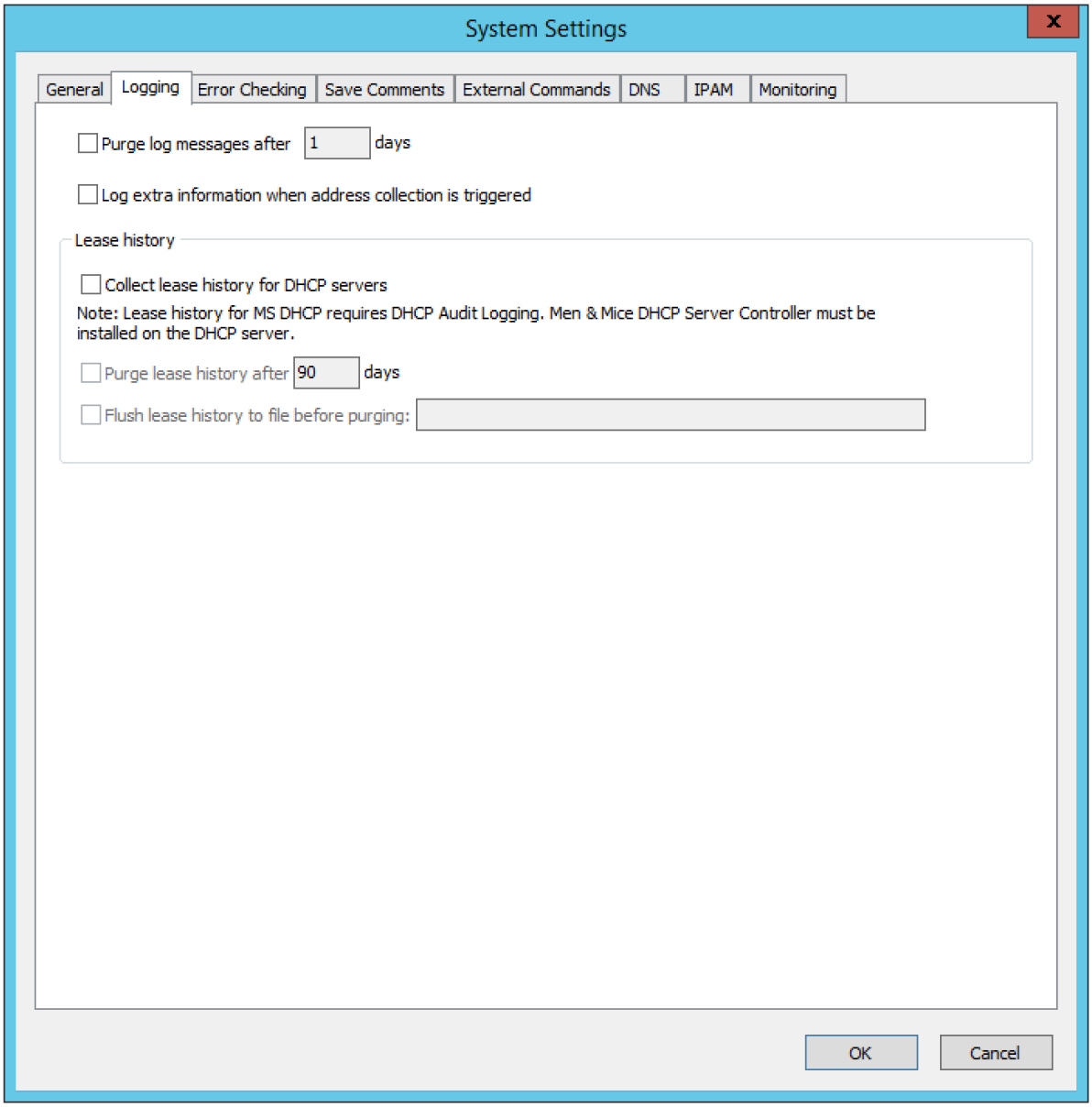


2. In the System settings dialog box, click the **General** tab.
3. **Allow Single Sign-on.** When selected, Active Directory users do not have to authenticate when logging in through the Management Console or the Command Line Interface.
4. **Allow single sign-on through web interface on IIS**. To enable single sign-on in the web interface, the web server needs to be configured. *Refer to Appendix C – Active Directory Single Sign-on .*
5. **Enable AD sites and subnets integration** . Check this checkbox to enable the integration feature. 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. 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. 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.
6. **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.
7. **Determine Address in use** . This section contains several checkboxes that determine whether an IP Address should be considered as being in use. Check the appropriate checkboxes to specify which rules should be applied to the IP Addresses.
8. **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.
9. 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**.

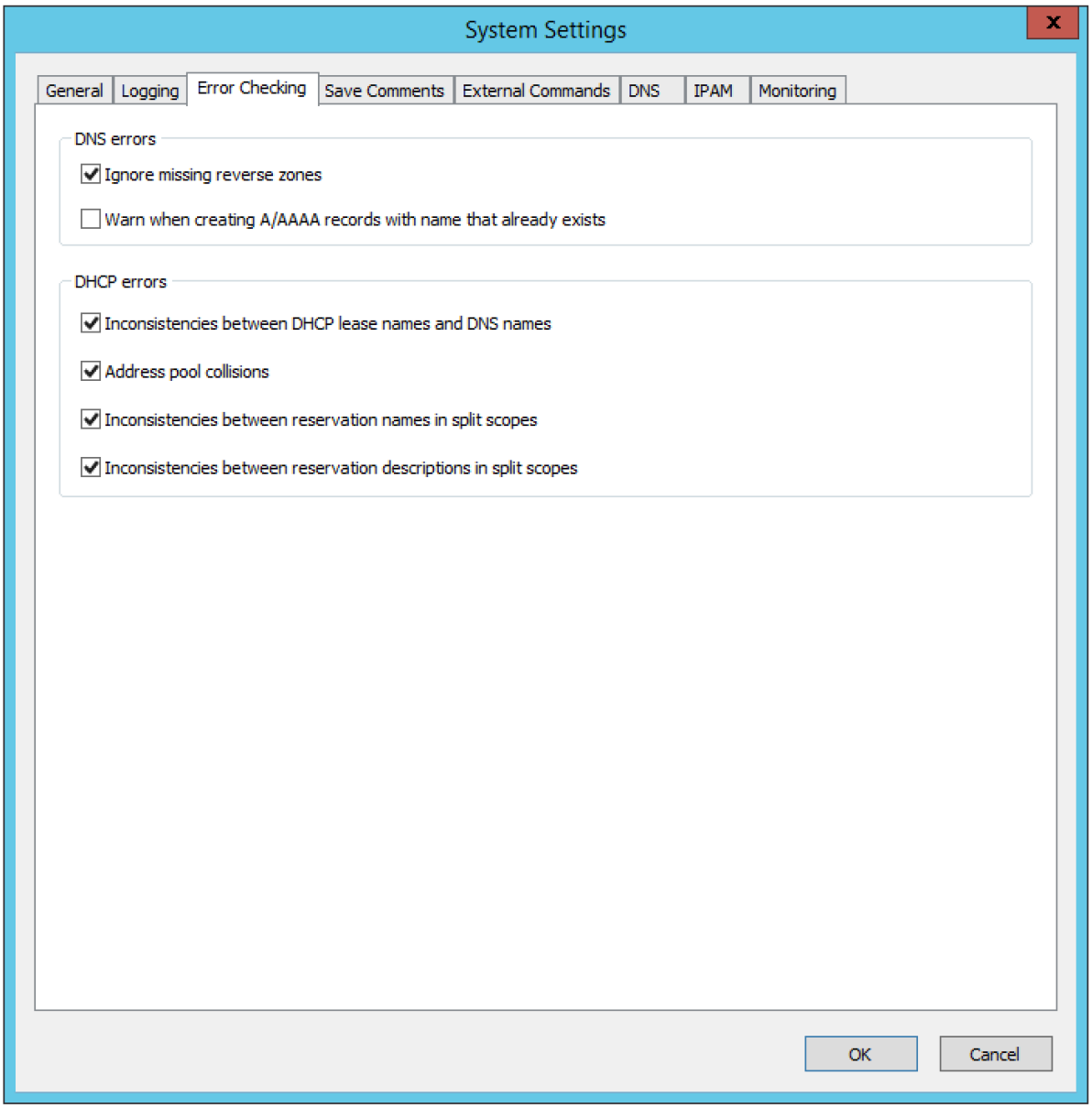


2. In the System Settings dialog box, click the **Logging** tab.
3. **Purge log message after** ____ days. When selected a number is typed in the field indicating the number of days the logs should be kept.
4. **Log extra information when address collection is triggered** . When selected, information about the start and duration of the address collection is written in the Men & Mice Suite log file.
5. **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.
6. 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**.



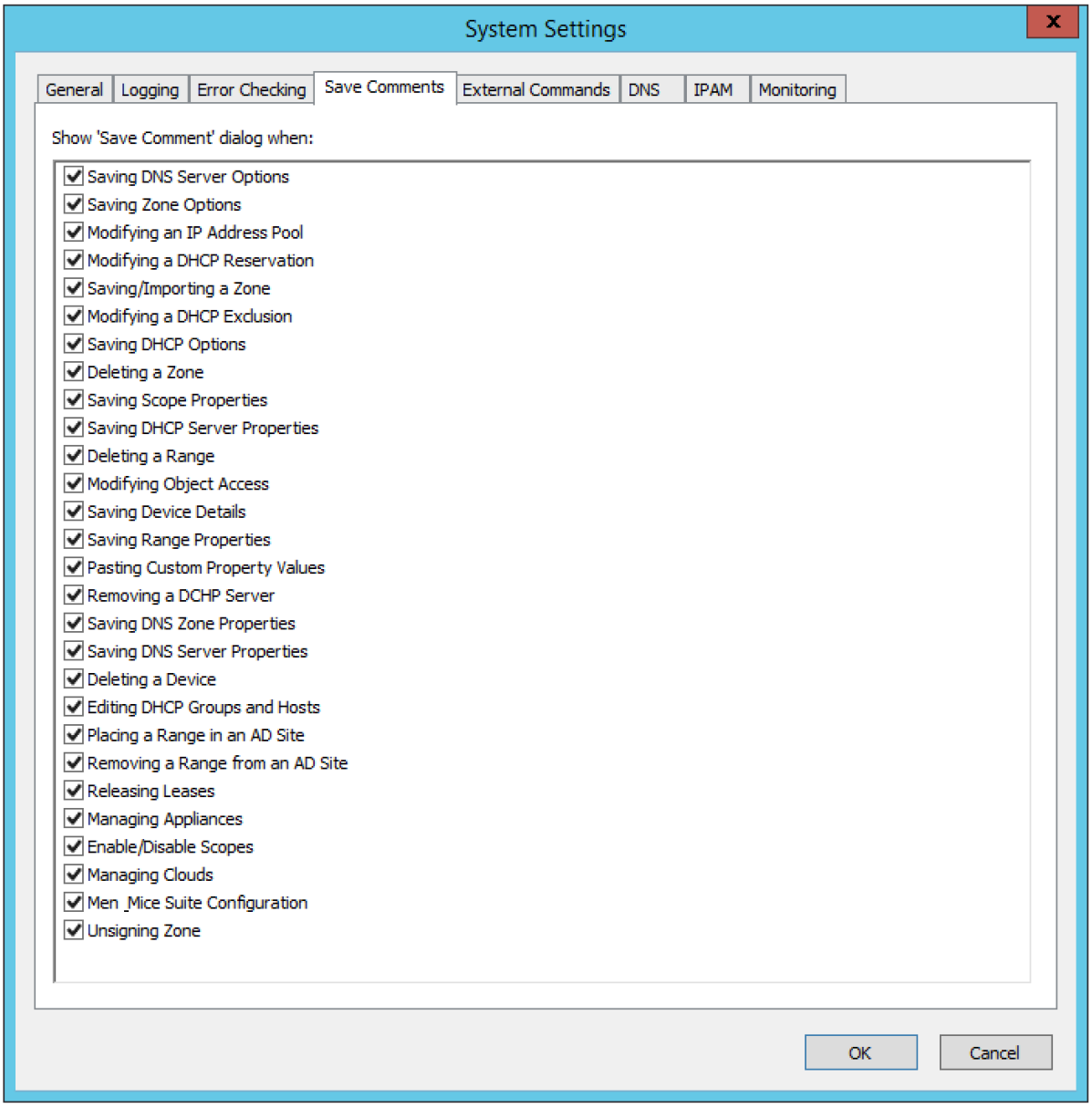
2. In the System Settings dialog box, click the **Error Checking** tab.
3. **Ignore missing reverse zones.** An error message displays when the Men & Mice Suite is unable to update a reverse record for a changed address record. It is possible to suppress this error message if no reverse zone exists for 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** .

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**.

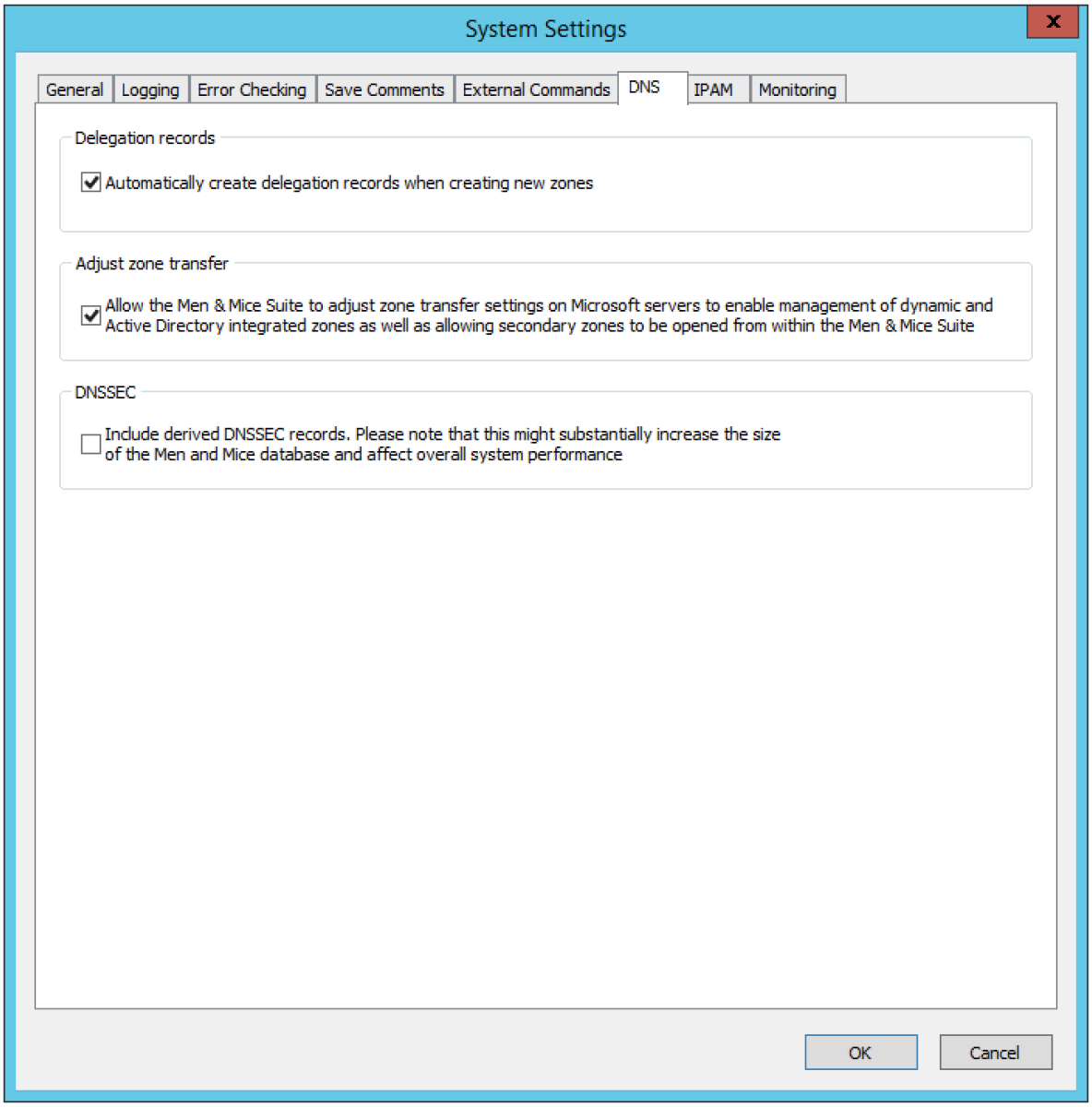
External Commands

Refer to the 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**.



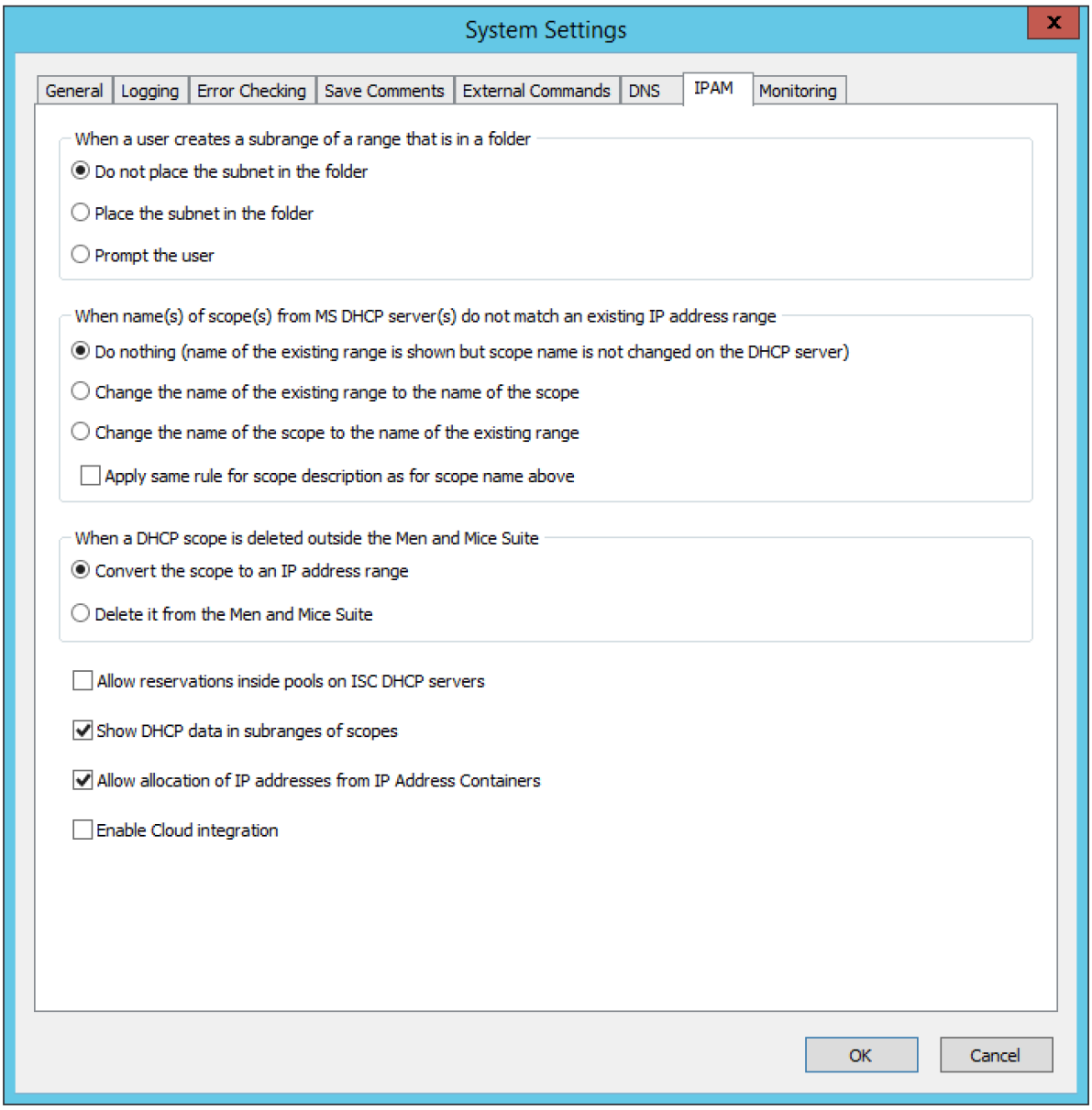
2. In the System Settings dialog box, click the **DNS** tab.
3. **Delegation records**. When *automatically create delegation records when creating new zones* is selected, delegation records (NS records) are automatically created in the corresponding parent zones when subzones are created, maintaining a correct delegation chain between parent and subzones.
4. **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.
5. **DNSSEC**. Select the checkbox to include derived DNSSEC records when viewing DNSSEC signed zones in the Men & Mice Suite. Note that this will increase the size of the Men & Mice Suite database significantly and may affect overall system performance.
6. When the desired selections/entries are made, click **OK**.

IPAM

The IPAM tab allows you to specify various IPAM related settings:

- 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.

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



2. In the System Settings dialog box, click the **IPAM** tab.
3. **Subranges**. The selection made here determines what happens when a user creates a subrange of a range in a folder. Click the desired action.
4. **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.
5. **Name conflicts between ranges and scopes**. The selection made her determines what happens if the name of an MS DHCP scope does not match the name of an existing IP Address range.
6. **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.

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.

> ⚠ *If a reservation that has been created inside a pool is deleted, the address is not made a part of the pool again.*

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.

Allow allocation of IP Addresses from IP Address Containers. When selected, the system will allow allocation of IP Addresses that reside in IP Address Containers. For more information on IP Address Containers, *refer to* IPAM Settings.

Enable Cloud integration. Check this checkbox to enable the Cloud integration feature. When Cloud integration is active you can add

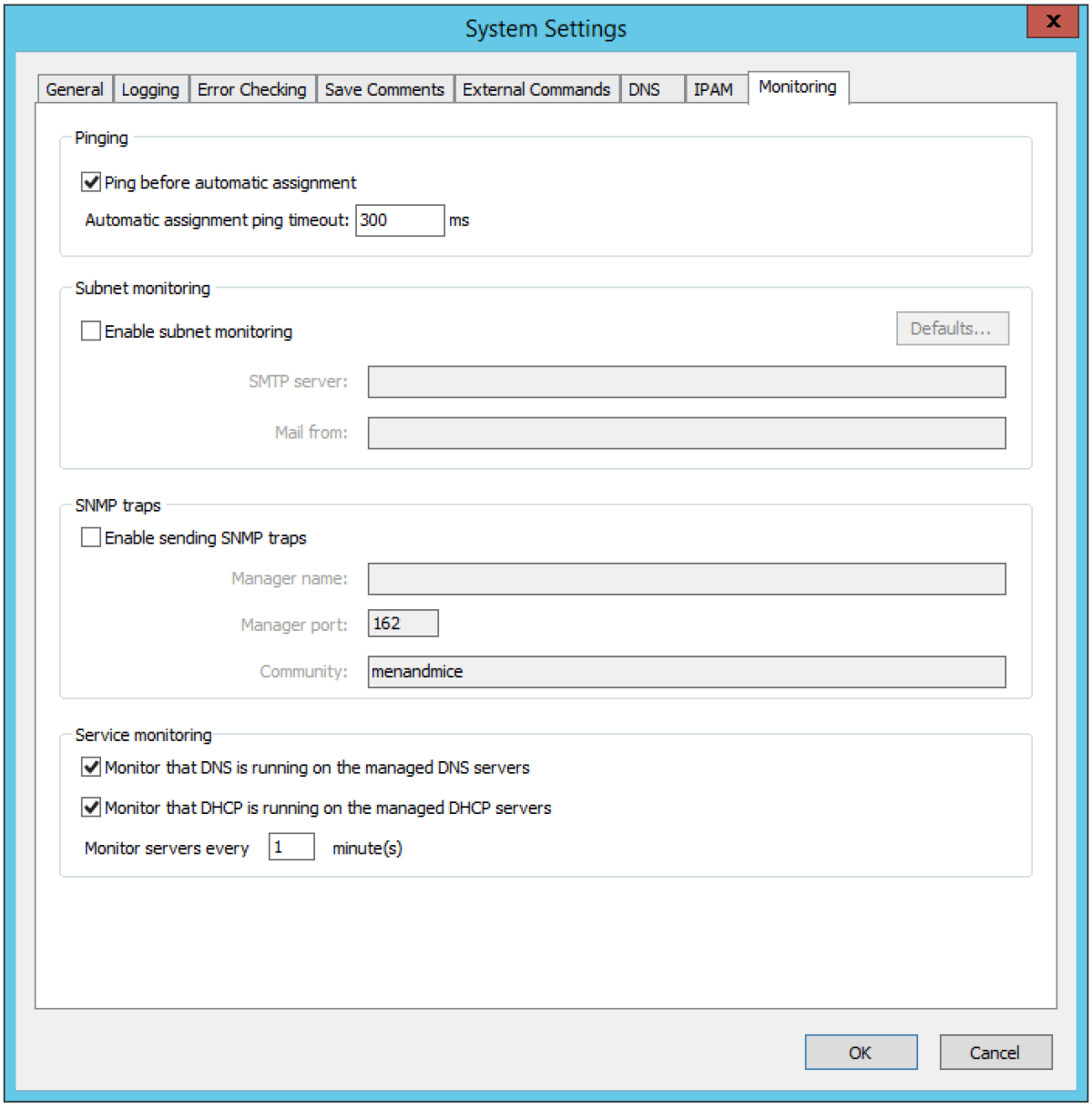
OpenStack clouds to the Men & Mice Suite. You can manage cloud networks and and you can add and remove subnets from cloud networks and move subnets to cloud networks. Cloud integration has been enabled, a **Cloud** object displays in the object list on the left hand side of the Manager window and a new column, **Cloud Network** displays in the range list in the Manager window.

7. When all 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**.



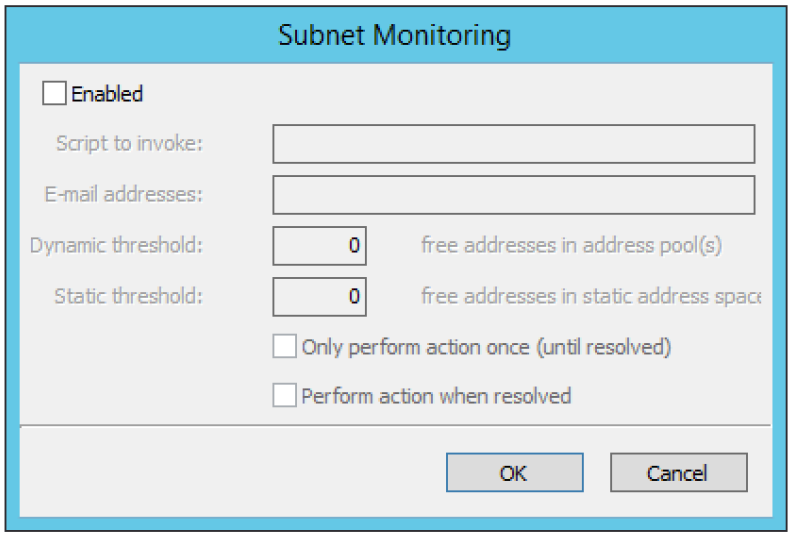
2. In the System Settings dialog box, click the **Monitoring** tab.
3. **Ping before automatic assignment.** When selected, when an IP Address is being auto-assigned, the system checks as to whether the IP Address is responding to a ping request *before* it is allocated to a new host. If the IP Address 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.

> ⚠ *The global subnet monitoring setting can be overridden for individual subnets by changing the setting explicitly for the subnet. Refer to IP Address Management—Subnet Monitoring and Utilization History for information on how to change monitoring*

settings for individual subnets.

To change the subnet monitoring settings, do the following:

- Click the **Defaults...** button. The Subnet Monitoring 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. *Refer to* 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.

> ⚠ *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.

> ⚠ *Only DHCP scopes that are enabled are monitored. Disabled scopes are ignored.*

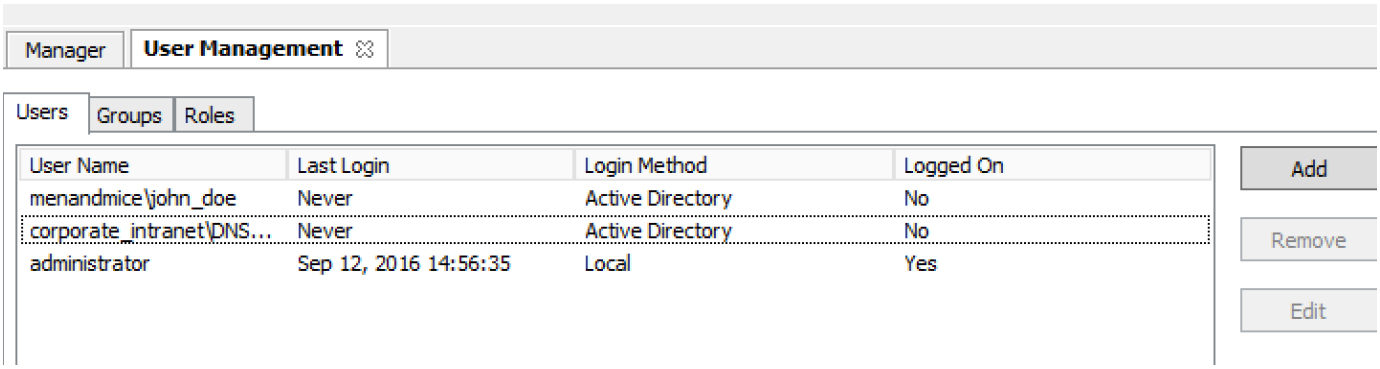
When subnet monitoring is enabled, you must specify the mail server and the sender e-mail address to use if you want the subnet monitor to send an e-mail. Place the appropriate information in the **SMTP Server** and **Mail from** fields.

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. *Refer to Management Console—Men and Mice Suite Log for more information on log events*.

   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.
7. **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. *Refer to IP Address Management—Host Discovery 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 tab.

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.

> ⚠ *"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* a ccount 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 as assign to this person.

   > ⚠ *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.

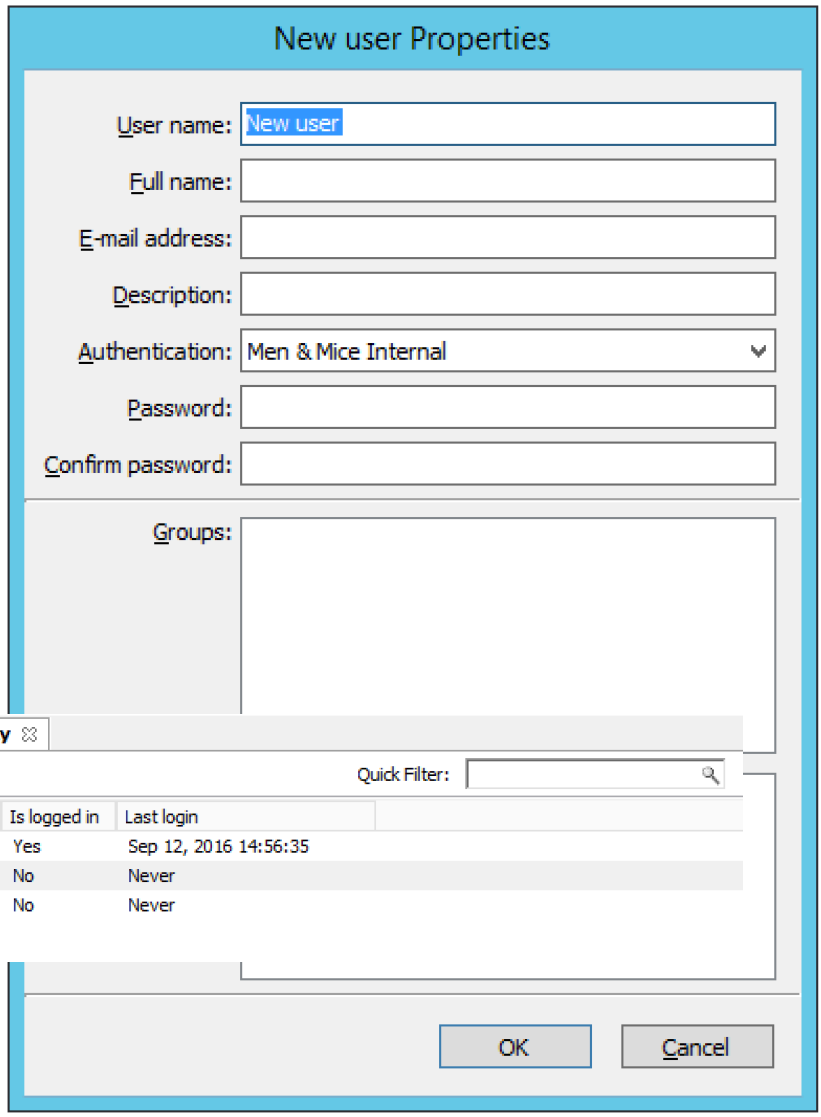
   > ⚠ *If you have not created your groups, you can always come back and edit the user accounts anytime and change the group assignments.*

9. 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 tabdisplays.

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 tab displays.

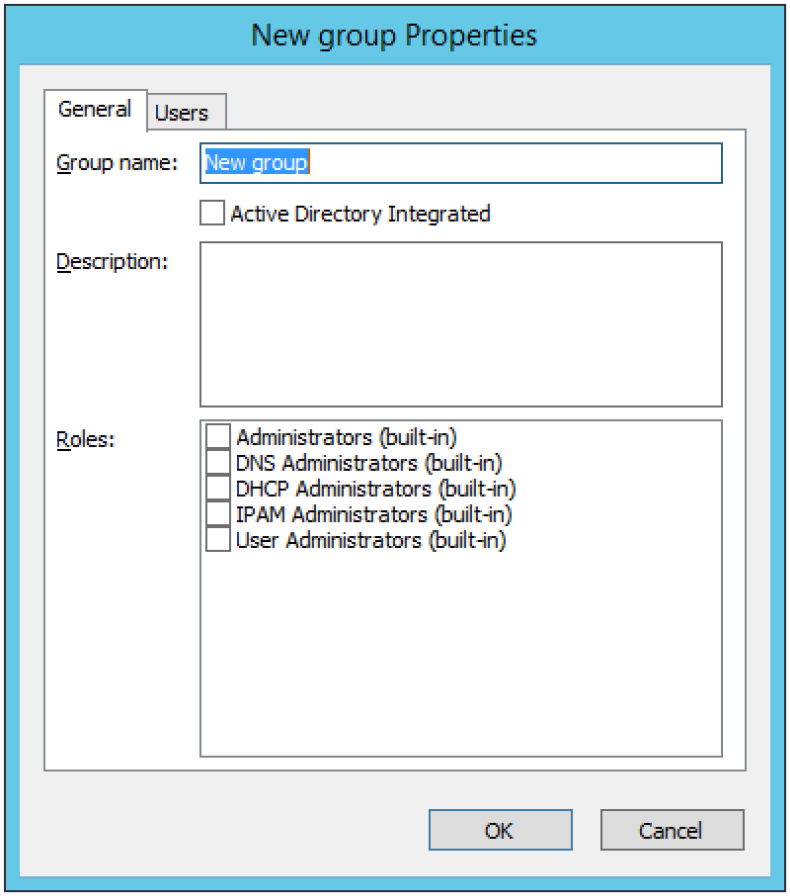
- Use the **Quick Filter**, if desired, to refine the list.

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 how on this works *refer to 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.

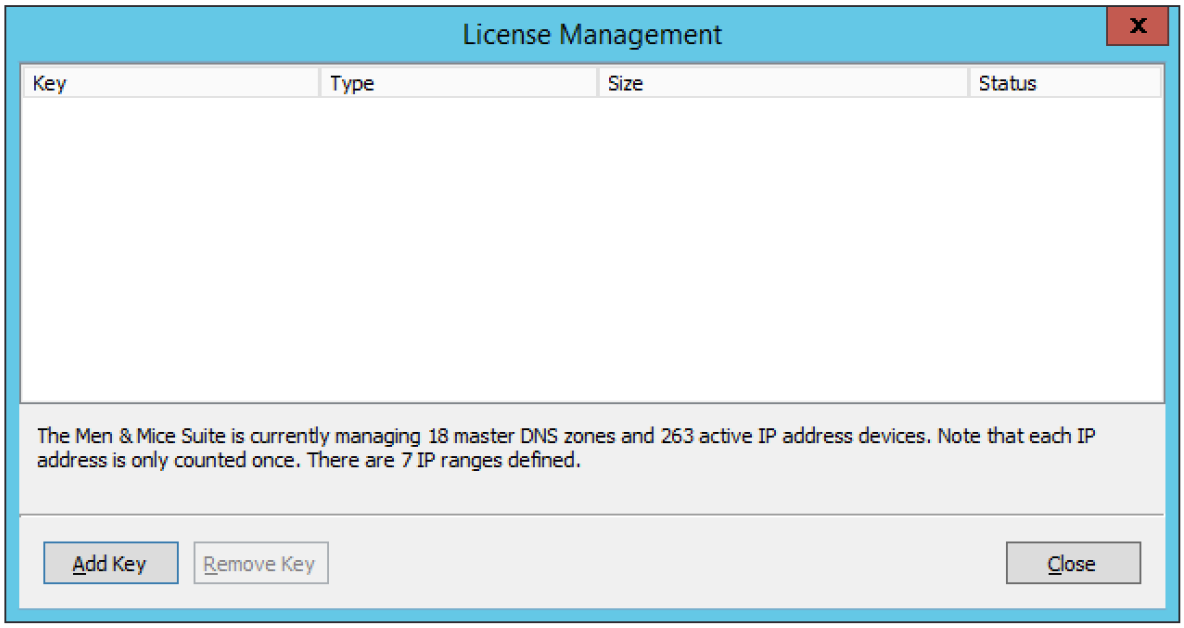
1. From the menu bar, select **Tools, Users and Groups**. The User and group management dialog box displays.
2. Click the **Groups** tab.
3. Highlight the group you want to delete.
4. Click the **Remove** button.
5. When the confirmation message displays, click **Yes**.

License Management

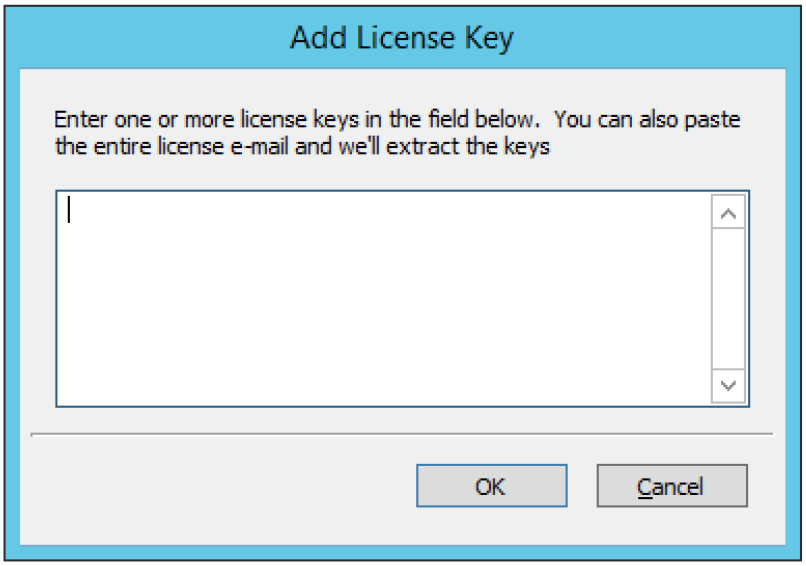
There are four different keys, one each for the DNS Module, the IPAM Module, and the DHCP Module and one key for enabling management of Appliances.
The License Management dialog box shows detailed information about every key entered. It also contains information about license utilization by showing the 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.



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



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

Removing a License Key

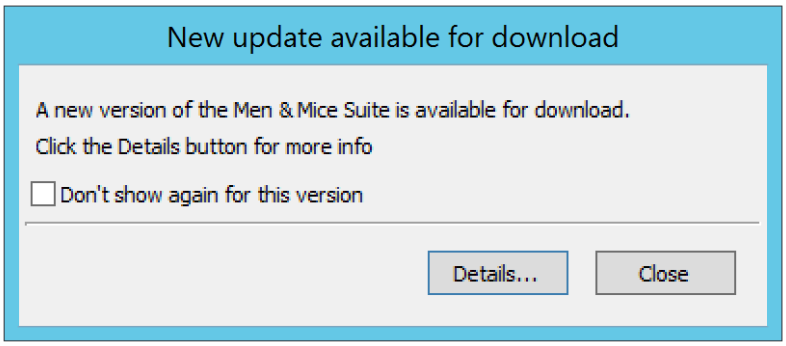
1. From the menu bar, select **Tools, License Management**. The License Management dialog box displays. All currently entered license keys are displayed.
2. Highlight the key you want to remove.
3. Click the **Remove Key** button.

Update Management

The Update Manager notifies you when a new version of the Men & Mice Suite is available and simplifies the update process for the Men & Mice Suite. Using the Update Manager you can update Men & Mice Central, the Men & Mice Suite Server Controllers and the Men & Mice Suite Appliance with minimal downtime.

Checking and Downloading an Update

When you log into the system using the Management Console, an update notification is displayed when a new version of the Men & Mice Suite is available.

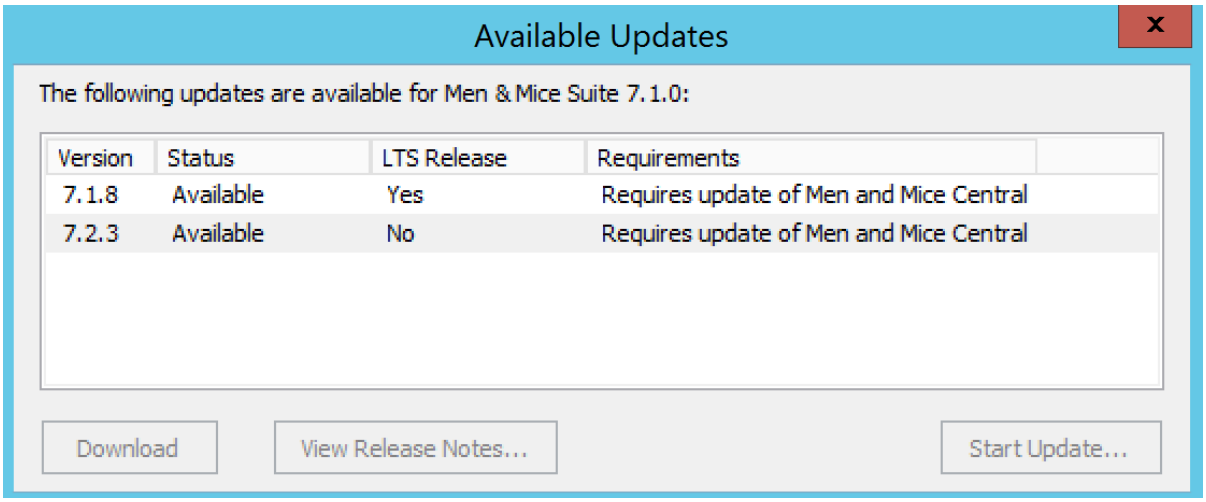


You can also check if an update is available by selecting **Tools, Check for Updates.**

> ⚠ *To receive update notifications and check for updates, you must be in a group with administration privileges. Only the Administrator user can perform the actual update.*

If you are not interested in receiving notifications for the update, select the **Don't show again for this version** checkbox. When the checkbox is checked, a notification for the specific update is no longer displayed, however, if a later update becomes available, the dialog box is displayed again.

Click the **Details** button to get more information on the update. This displays a dialog box that shows all available updates.



- To view the release notes for an update, select the corresponding update and then click the **View Release Notes** button. This will show the release notes in a web browser.
- To download the new version, select the version and click the **Download** button. The new version is downloaded and stored on the Men & Mice Central server. Once the download has completed, you can start the update.

> ⚠ *To download and perform the actual update you must be logged in as Administrator. If you are not logged in as Administrator, the Download button is disabled.*

Installing an Update

Once the update has been downloaded, you can start the actual update process. The Update Manager can update Men & Mice Central, the Server Controllers and the Men & Mice Appliance. The Men & Mice Web interface must be updated manually.

If you want to perform the update at a later time, you can close the dialog box. To display the dialog box again, select **Tools, Check for Updates**.

The following instructions contain information on how to update the Men & Mice Suite after the update has been downloaded using the Update Manager.

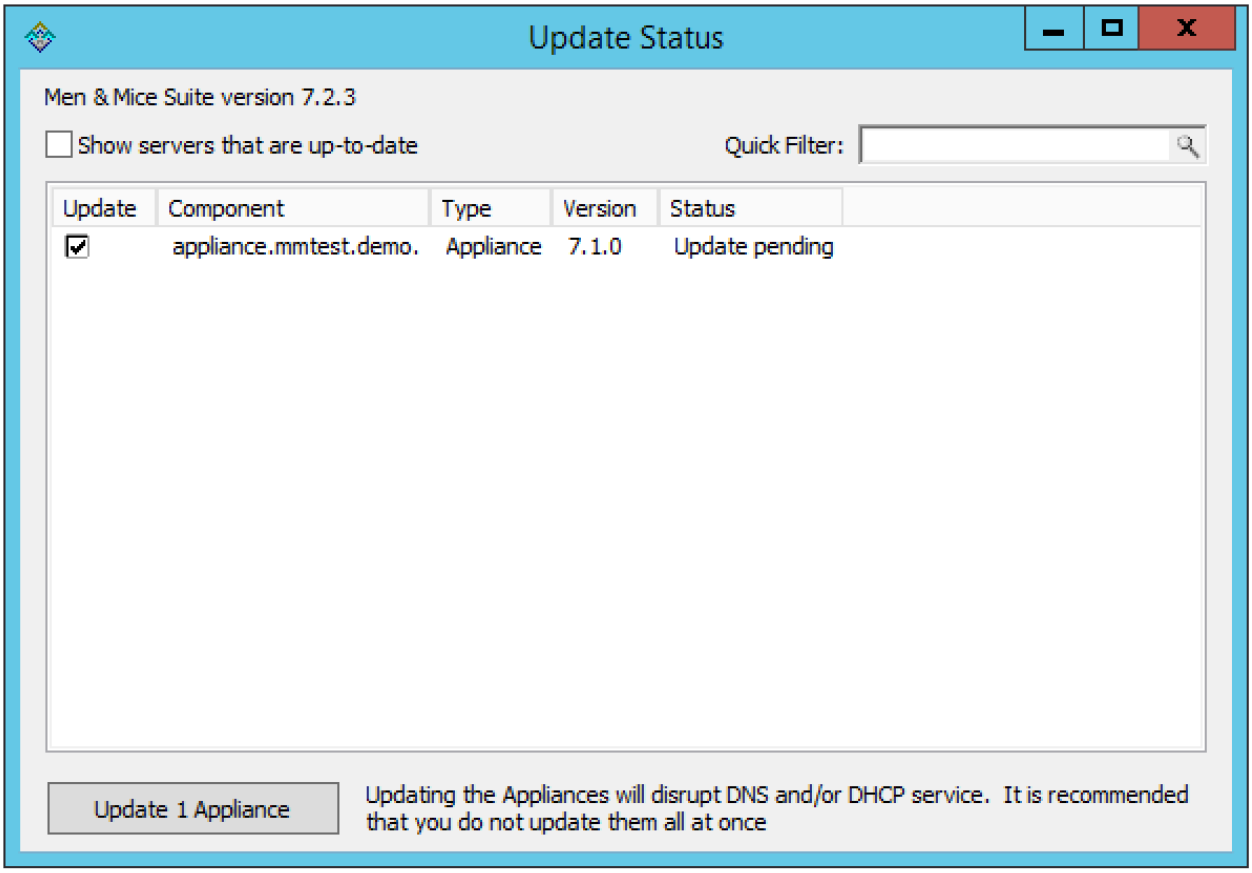
To start the update process, click the **Start Update** button in the update details dialog box. When you click **Start Update** the following happens:

- Men & Mice Central and the DNS and DHCP server controllers are updated.
- If the update contains a new version of the Men & Mice web interface, a dialog box is displayed where you can find instructions on manually updating the Men & Mice Web interface.
- If your setup contains a Men & Mice Appliance, the latest version of the Men & Mice Appliance software is uploaded to the Appliance. Note that the update is not applied automatically.

Updating an Appliance

As an update to the Men & Mice Appliance sometimes requires that the Appliance is restarted, the update is not applied automatically. To complete an Appliance update, you must manually initiate the update. To minimize service disruption you might want to update your Appliances in several batches.

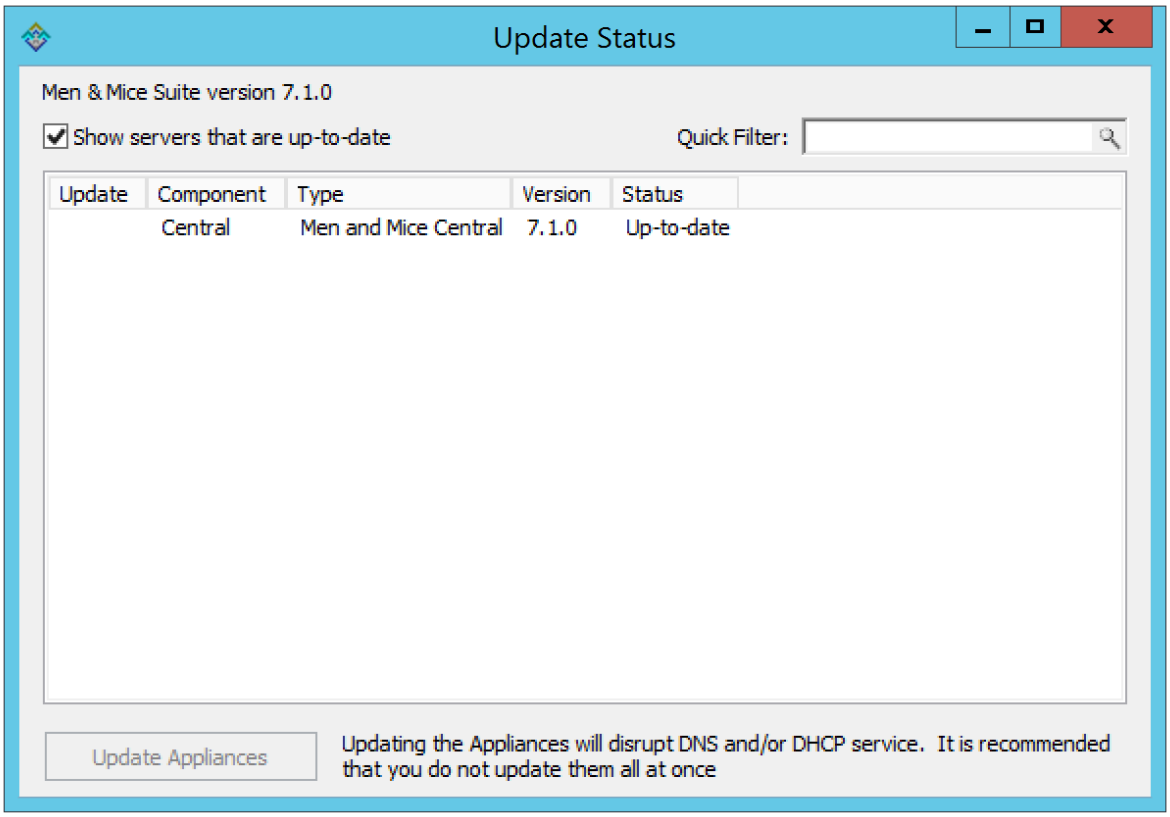
1. From the menu bar, select **Tools, Update Status**. The Update Status dialog box displays. The dialog box shows the update status for all DNS and DHCP server controllers as well as all Men & Mice Appliances. If an update is pending for an Appliance, the status is listed as **Update pending** and a checkbox is displayed in the **Update** column.



2. Click the checkbox to select the Appliance(s) you want to update.
3. Click the **Update Appliances** button. This will update the selected appliance(s).

Viewing Update Status

Through the Update Status dialog box, you can always view the update status for the Men & Mice Suite components. To display the Update Status dialog box, select **Tools, Update Status**.



The dialog box shows the update status for all DNS and DHCP server controllers as well as all Men & Mice Appliances. If an update is pending for an Appliance, the status is listed as **Update pending** and a checkbox is displayed in the **Update** column.

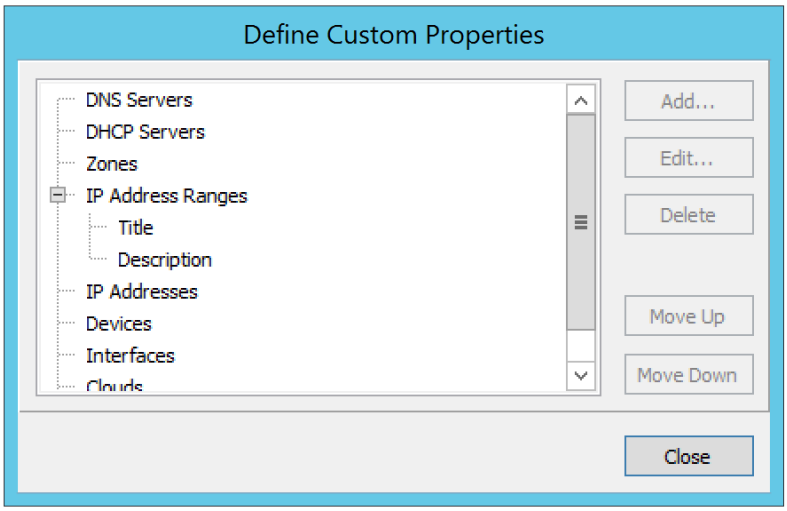
- Uncheck the **Show servers that are up-to-date** checkbox to only show servers that need to be updated.

Define Custom Properties

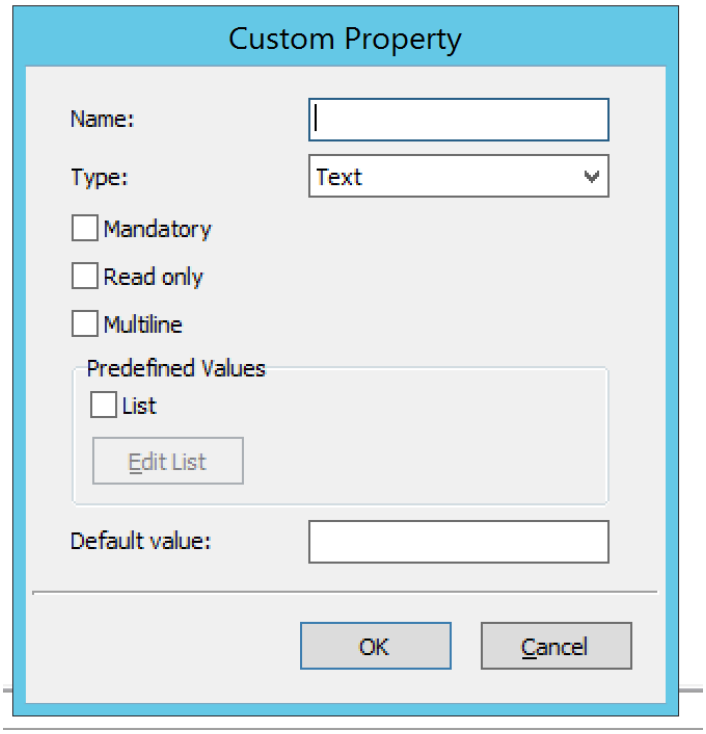
As an administrator, you may find that it is necessary to create some custom properties. These properties are used for entry of any data that you feel is relevant for an object. For example, if you want to specify a server is in a specific location, or indicate who is responsible for a particular server,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



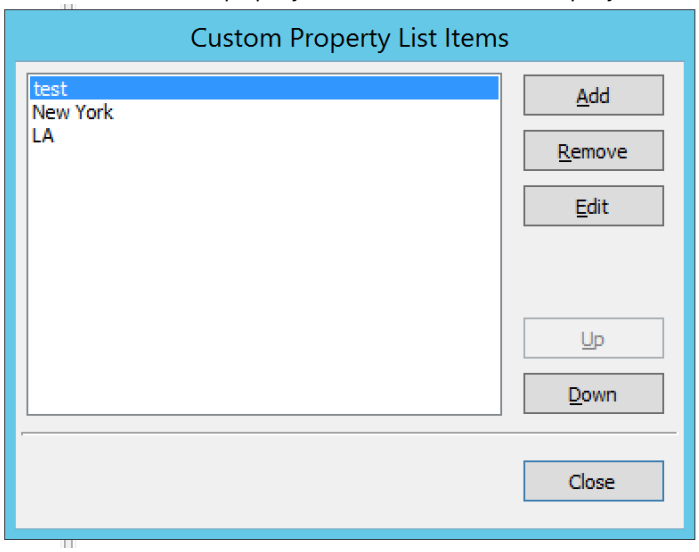
2. Select the object type to which you want to add a custom property.
3. Click the **Add** button. The Custom Property dialog box displays.



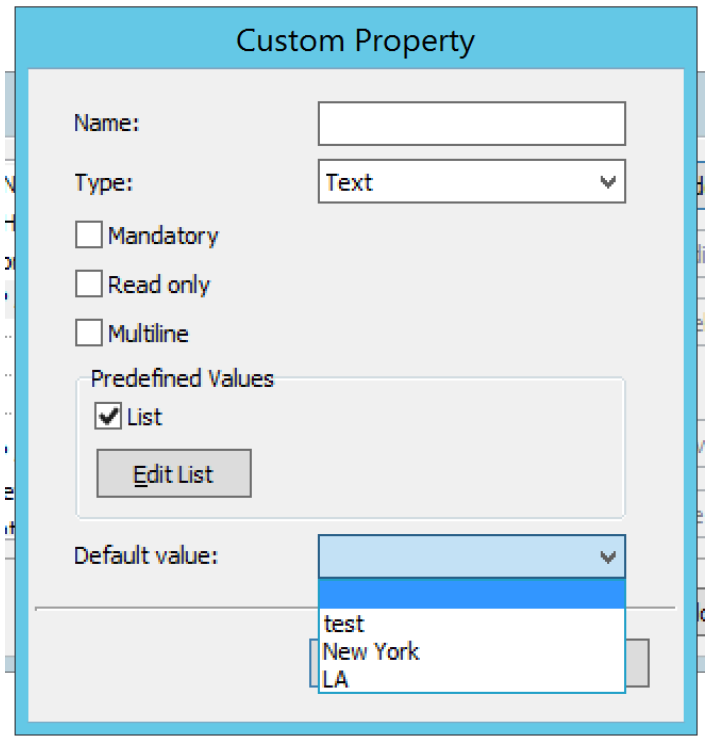
4. **Name**. Type a name for this custom property.
5. **Type**. Set the type for the property. By default, "Text" is selected. Click the drop-down list and select the desired property type - e.g., Text, Yes/No, IP Address, or Number.
6. **Mandatory**. When selected, a user must enter a value in this 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.** 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.

> ⚠ *If you select this option, you cannot select "Multiline"*

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



- 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.



- 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

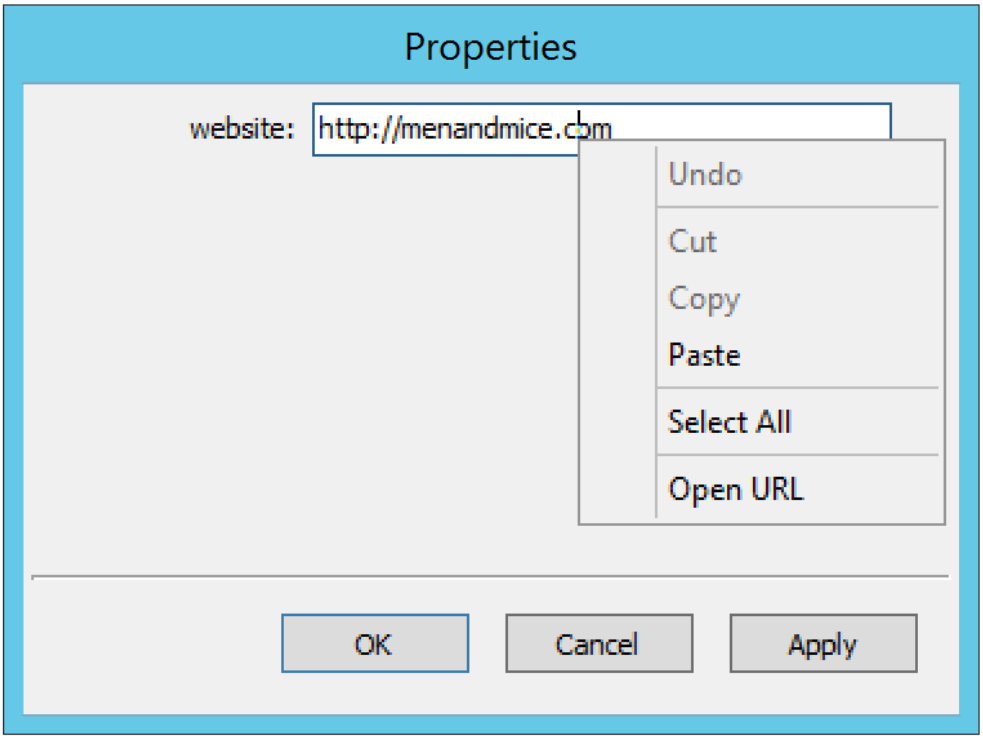
Once a custom property has been defined, it is possible to view and edit its contents by opening the Properties dialog for any object of the type for which the custom property has been defined.

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**.

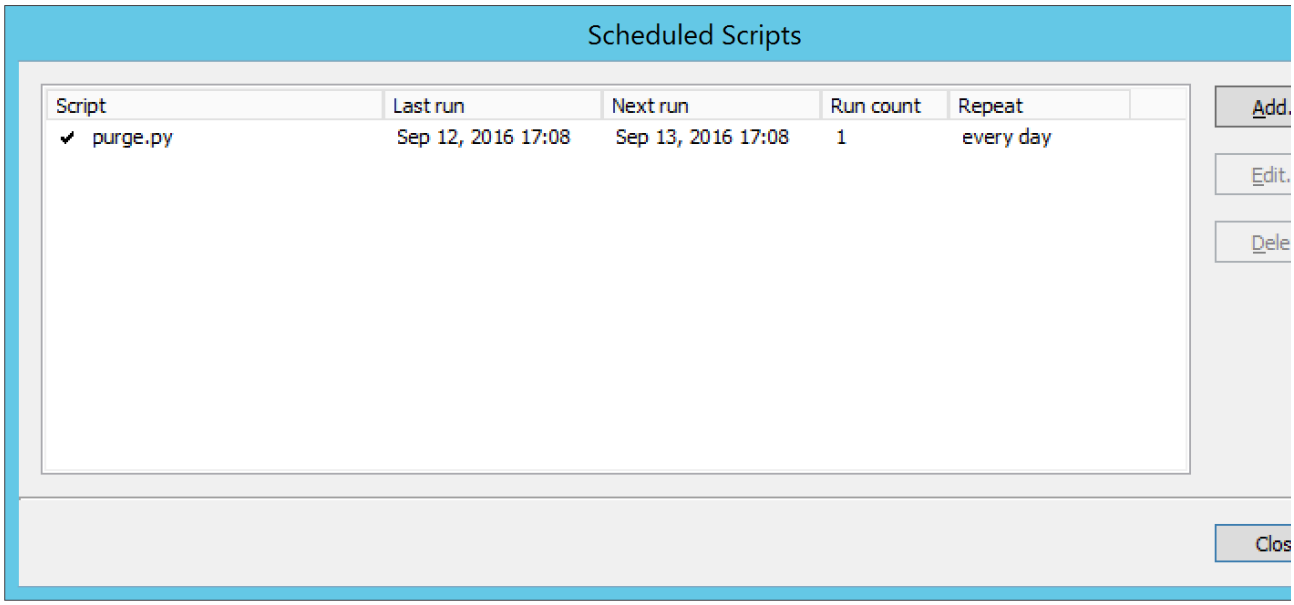


6. Your browser will open and the web site for the URL displays.

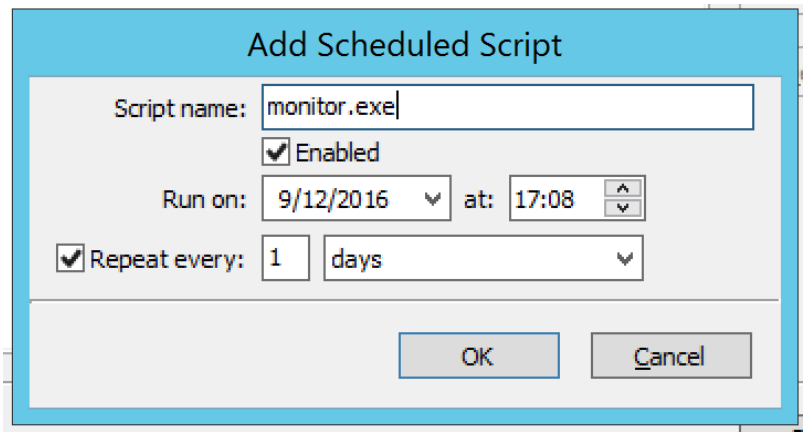
Scheduled Scripts

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.

   ⚠ *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

' 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 str
 User = 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")
objShell.CurrentDirectory = objShell.CurrentDirectory & "\scripts"

' 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 mmcmd.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.

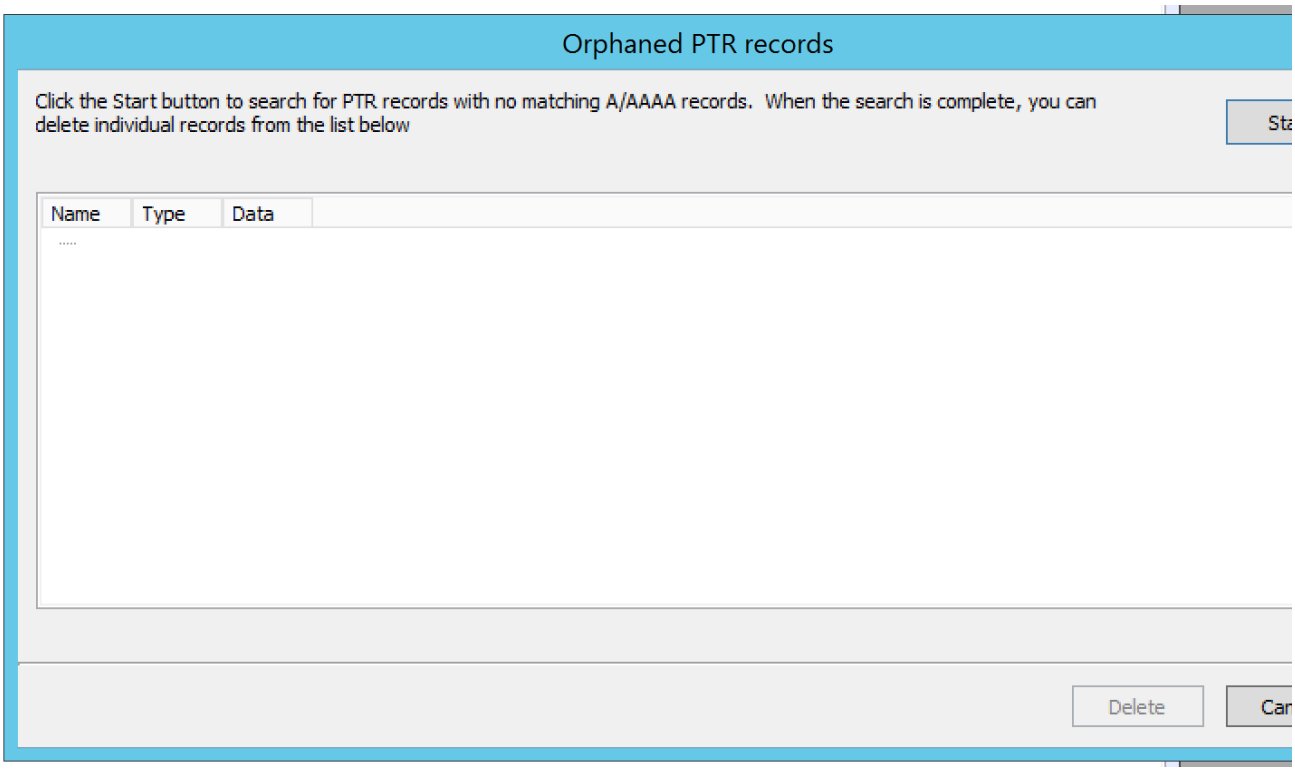
Find Orphaned PTR Records

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.

> ⚠ *Due to the fact that the result could be a large number of records, there is now a limit of 1000 records being shown.*



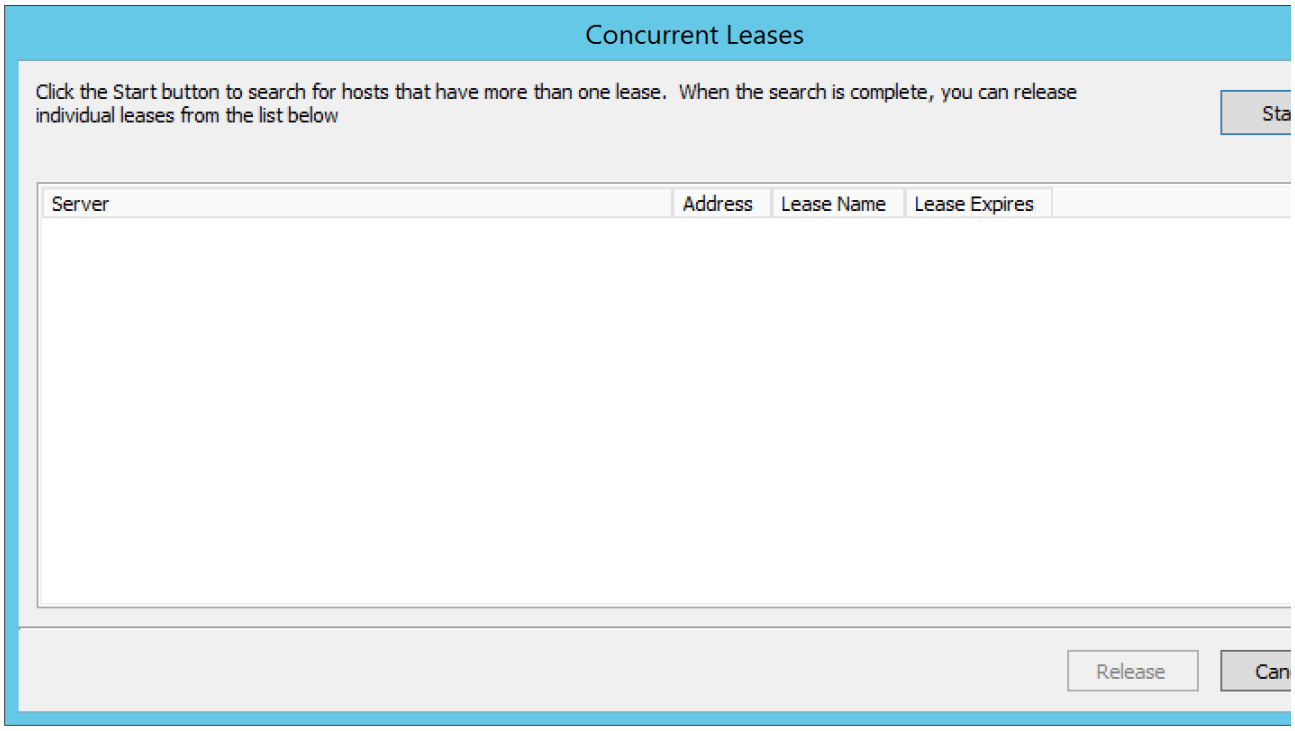
3. Select the PTR records you want to remove, and click the **Delete** button. The selected PTR records are removed.

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.

> ⚠ *Finding all concurrent leases might take a while in large environments.*



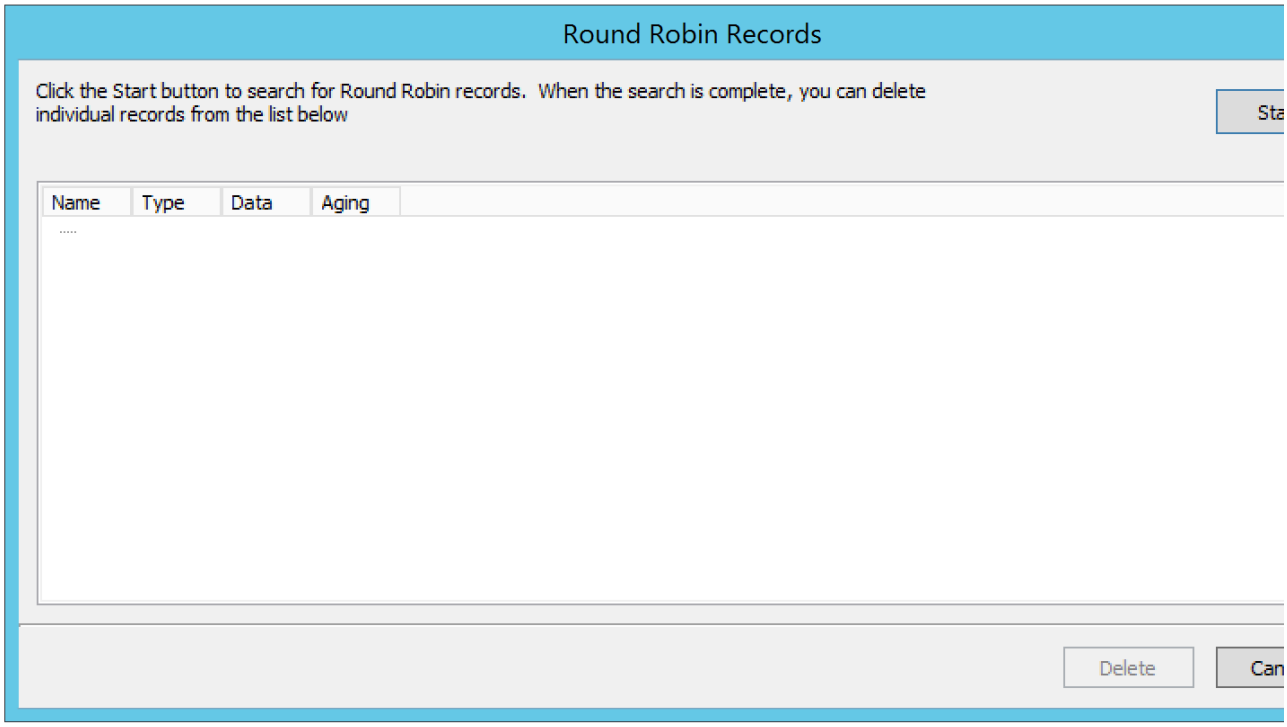
3. Select the leases you want to release, and click the **Release** button. The selected leases are released.

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.

> ⚠ *Finding all round robin records might take a while in large environments.*



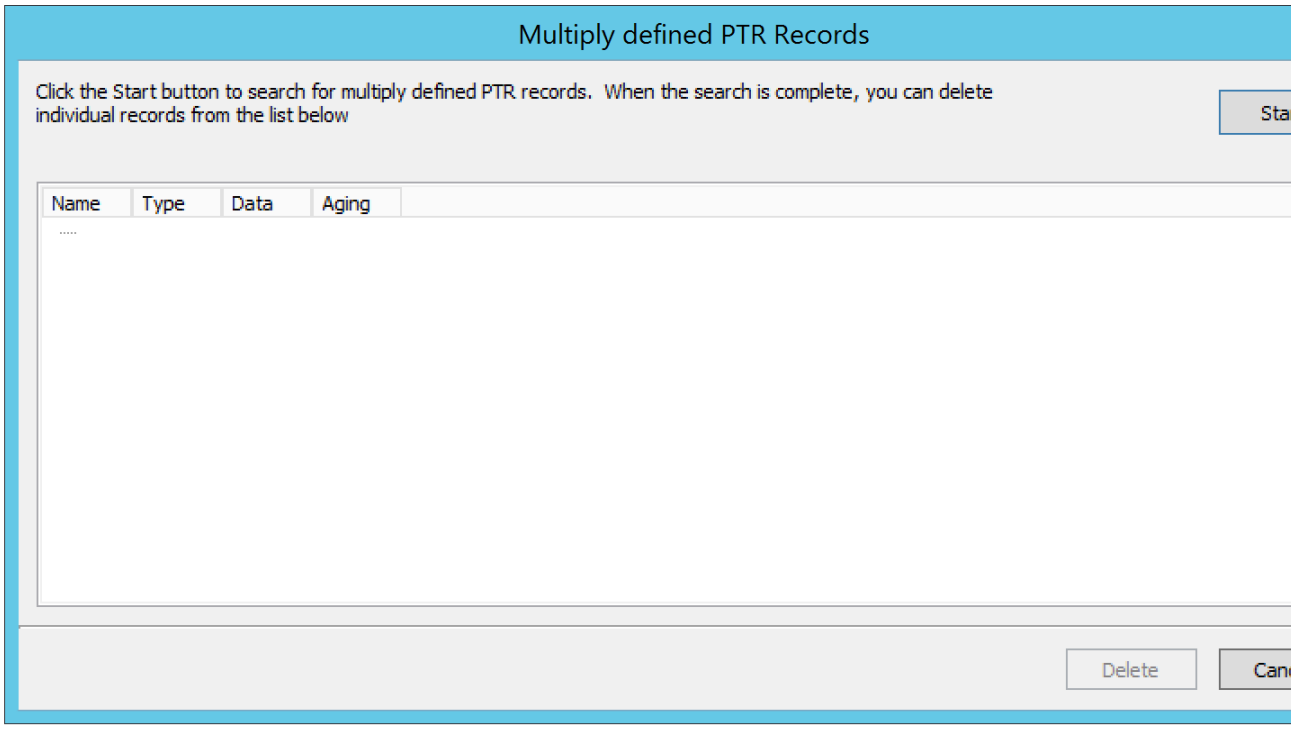
3. Select the records you want to delete and click the **Delete** button. The selected records are deleted.

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.

> ⚠ *Finding all multiply defined PTR records might take a while in large environments.*



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, Groups or Roles 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, Group or Role.

The relationship between Groups, Users and Roles is as follows:

- Groups can contain Users
- Groups cannot contain Groups
- Users can be a member of any number of Groups
- Users and Groups can be assigned to Roles.

Built-in Roles

> ⚠ Please note that in previous versions (< 6.7) roles did not exist and the built-in roles described below were previously built-in groups. All of the users that were members in specific built-in groups are now assigned to the corresponding built-in roles.

Five Roles are built-in to the Men & Mice Suite. These roles are special in that they get full access for their respective domains for all Access Flags.
When new objects are created, the Built-in Role that presides over that object, as well as the user or group that created the object, receives full access to it.
Each administrator role 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 role receives default access to all the Access Flags on the Suite object. Default access for each Built-in role 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 Roles. These roles are the only roles that can receive default access to new items. User-defined Roles do not receive any access information for new objects and are considered to have "denied" access. To allow a User or a Group to receive default full access to a new object, include the User or Group as a member in the corresponding Built-in Role. 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 Role:

Access Flags	Allow	Deny
Administer DNS servers	1	0
Access DNS Module	1	0

For every **DNS server** created, the server will have the following flags set to *Allow* for the DNS Administrators Role:

Access Flags	Allow	Deny
Edit DNS Server access	1	0
List (or view) DNS Server	1	0
Edit DNS Server options	1	0
Add Master Zones	1	0
Add non-Master Zones	1	0
View DNS Server Log	1	0
Clear DNS Server Log	1	0
Edit DNS server properties	1	0

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

Access Flags	Allow	Deny
Edit Zone access	1	0
List (or view) Zone	1	0
Enable/disable Zone	1	0
Edit Zone options	1	0
Delete Zone	1	0
Enable/disable apex records	1	0
Edit apex records	1	0
Enable/disable wildcard records	1	0
Edit wildcard records	1	0
Enable/disable other records	1	0
Edit other records	1	0
Edit zone properties	1	0

Overriding Access Settings

The **Deny** setting for an Access Flag allows you to override access settings inherited from Roles. A User's Access Footprint is calculated from the aggregate access settings of all Roles 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 Roles where a specific Access Flag is set to **Allow,** and only a single Role 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 Role 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:

Access Flags	Allow	Deny
Edit Zone access	1	0
List (or view) Zone	1	0
Enable/disable Zone	1	0
Edit Zone options	1	0
Delete Zone	1	0
Enable/disable apex records	1	0
Edit apex records	1	0
Enable/disable wildcard records	1	0
Edit wildcard records	1	0
Enable/disable other records	1	0
Edit other records	1	0
Edit zone properties	0	1

If you wanted to give similar access to other users, you could instead create a new Role, add the Users to the Role, and apply the aforementioned access to the zone in question for the new Role.
This system allows for a great deal of flexibility when designing your security. Any Role can be extended or overridden for a set of Users by simply adding the Users to another Role 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 Role 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, Group's or Role'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.

OBJECT	DESCRIPTION

Administer users/groups	Access to create, edit, and delete users and groups
Administer IP Address Ranges	Access to admin IPAM ranges
Administer DNS servers	Access to create, edit, and delete DNS servers
Administer DHCP servers	Access to create, edit, and delete DHCP servers
Access IPAM Module	Access to the IPAM Module
Access DNS Module	Access to the DNS Module
Access DHCP Module	Access to the DHCP Module
Access Management Console	Access to the Management Console
Access CLI	Access to the CLI
Access to Web Interface	Access to the Men & Mice Web Interface
Access to basic zone view in Web Interface	Access to the basic zone view in the Men & Mice Web Interface
Access to advanced zone view in Web Interface	Access to the advanced zone view in the Men & Mice Web Interface
Access to IPAM view in Web Interface	Access to the IPAM view in the Men & Mice Web Interface
Access to report view in Web interface	Access to the report view in the Men & Mice Web Interface
Access to task list view in Web interface	Access to the task list view in the Men & Mice Web Interface
Access to view history	Access to history window in the Management Console. Also provides access to the history for all objects.
Access to Host editor	Access to the host editor view in the Men & Mice Web interface
Access to manage AD Sites and Site Links	Access to work with AD Sites and Site Links. ⚠ *Finding all multiply defined PTR records might take a while in large environments.*

DNS Zone

OBJECT	DESCRIPTION
Edit Zone access	Access to edit an object's access
List (or view) Zone	Access to list (view) a zone
View one history	Access to viewing the history for the zone
Enable/disable Zone	Access to enable/disable the zone
Edit Zone options	Access to edit zone options
Delete Zone	Access to delete zone
Enable/disable apex records	Access to enable/disable zone's APEX records
Edit apex records	Access to edit zone's APEX records
Enable/disable wildcard records	Access to enable/disable zone's wildcard records
Edit wildcard records	Access to edit zone's wildcard records
Enable/disable other records	Access to enable/disable zone records other than APEX
Edit other records	Access to edit zone records other than APEX records
Edit zone properties	Access to edit properties for the zone

DHCP Scopes and IP Address Ranges

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

DNS Server

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

DHCP Server

OBJECT	DESCRIPTION

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

DHCP Groups

OBJECT	DESCRIPTION
Edit DHCP group	Access to edit an object's access
List (or view) DHCP group	Access to list (or view) DHCP group
View DHCP group history	Access to viewing the history for the DHCP group
Edit Reservations	Access to edit reservations
Read DHCP group options	Access to view group options
Read/write DHCP group options	Access to read and write group options
Delete DHCP group	Access to delete a DHCP group

Address Spaces

OBJECT	DESCRIPTION
Edit address space access	Access to edit an object's access
List (or view) address space	Access to list (or view) address space
View address space history	Access to viewing the history for the address space

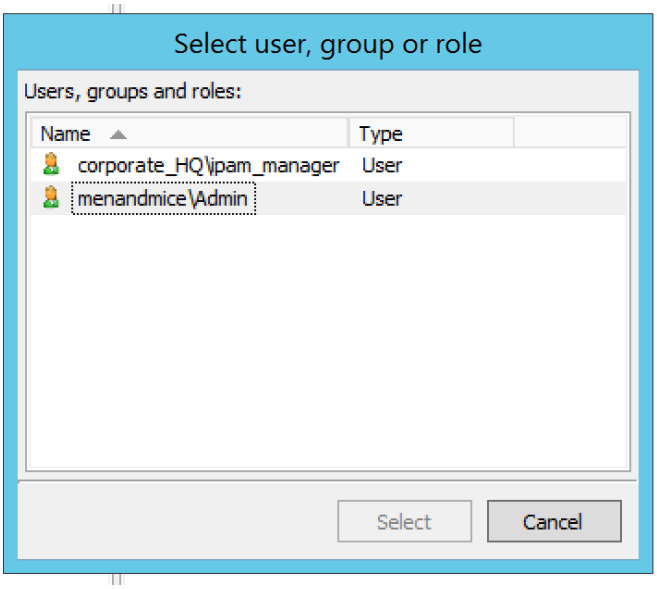
Access Control Dialog Box

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:

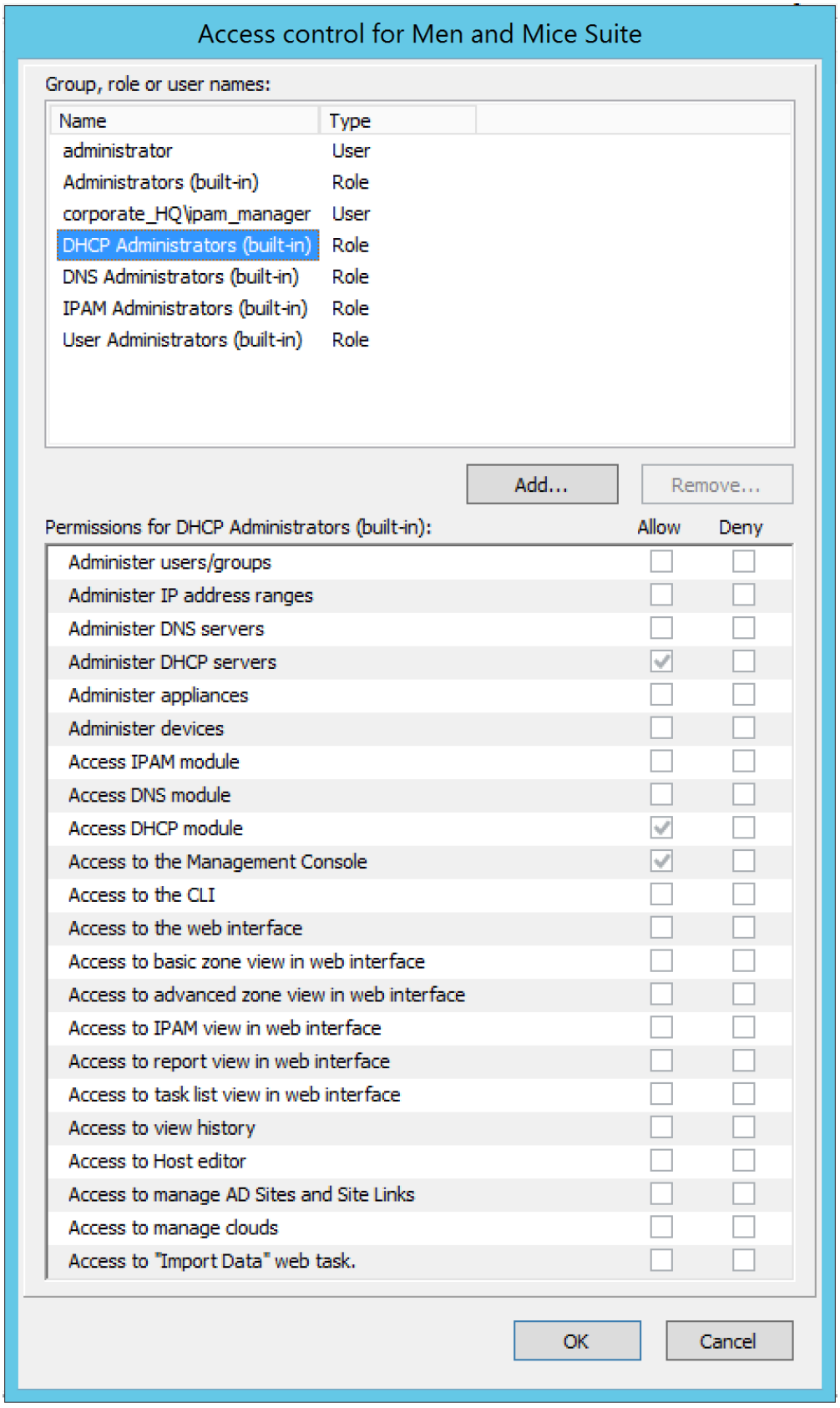
- From the menu bar, select **Tools, Global Access**. The Access Control for Men and Mice Suite dialog box displays. The default groups/user names are shown. The permissions for any selected group/user are also shown.

Selecting a Group/User

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



2. Highlight the user, group and/or role 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/role, do the following:
    - Move to the Permission for [group/user/role selected] list.
    - Click in the checkbox for each permission you want to **Allow** or **Deny**.

> ⚠ *It is not necessary to select **Deny** unless you want to ensure that a user/group/role does not have permission to a*

specific object. However, if you do not specify the permission for an individual user, but the group(s) or role(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.

The access control dialog box for IP Address Ranges and Scopes contains a checkbox, 'IP Address Ranges/Scopes inherit access by default'. If this checkbox is checked, a new range or scope will inherit all access bits from its parent. For more information on inherited access, refer to IP Address Management—Range Access.

- 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 for details on working with this dialog box.*