NetIQ® iManager
Administration Guide

October 2019

Legal Notice

Contents

About this Book and the Library

The *Administratin Guide* provides conceptual information about the NetIQ iManager (iManager) product. This book defines terminology and includes implementation scenarios.

For the most current version of the *NetIQ iManager Administration Guide*, see the English version of the documentation at the NetIQ iManager online documentation site.

Intended Audience

This guide is intended for network administrators.

Other Information in the Library

The library provides the following information resources:

Installation Guide

Describes how to install iManager. The book is intended for network administrators.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

1 Overview

NetIQ iManager is a Web-based administration console that provides secure, customized access to network administration utilities and content from virtually anywhere you have access to the Internet and a Web browser.

iManager provides the following:

- Single point of administration for NetIQ eDirectory objects, schema, partitions, and replicas
- Single point of administration for many other network resources
- Management of many other NetIQ and Novell products using iManager plug-ins
- Role-Based Services (RBS) for delegated administration

Because iManager is a Web-based tool, it enjoys several advantages over client-based administrative tools:

- Upgrade once, on the server, for all administrative users
- Changes to iManager look, feel, and functionality are immediately available to all administrative users
- Do not need to open additional administrative ports for remote access. iManager leverages standard HTTP ports (80/443). With iManager, you can pass non- standard HTTP ports.
- Not necessary to download and maintain an administrative client
- Not necessary to keep client software synchronized with changes to server software

2 Accessing iManager

You can access iManager and the complete set of features that it provides from any supported web browser. Although you might be able to access iManager via a web browser not listed, we do not guarantee or support full functionality with any browser that is not officially supported.

IMPORTANT: For information about supported web browsers for this version, review the NetIQ iManager Installation Guide.

For some iManager wizards and help to work, you must enable pop-up windows in your web browser. If you use an application that blocks pop-up windows, disable the blocking feature while working in iManager or allow pop-ups from the iManager host.

If you have configured your web browser to not display Web site images, the iManager interface might become garbled and unusable.

Accessing iManager varies based on the iManager version (server-based or workstation) and the platform on which iManager is running. For information on installing iManager, see the *NetIQ iManager Installation Guide*.

This section includes the following topics:

Accessing Server-Based iManager

To access server-based iManager:

1 Enter one of the following in the Address (URL) field of a supported Web browser.

- To access stand alone iManager:

  Secure URL: `https://<server ip address>:8443/nps/iManager.html`

  NOTE: iManager uses only Tomcat 9 for its Web server requirements. You must specify the Tomcat port in the URL on your browser.

  In the examples, the IP address in *<server ip address>* can be either IPv4 or IPv6. For example, when accessing iManager the URL can be the following:

- **IPv6**: `https://[2001:db8::6]/nps/iManager.html`

  Although slightly different iManager URLs might work on some platforms, NetIQ recommends using these URLs for consistency.

2 Log in using your user name, password and tree name or IP.

iManager login only accepts lowercase tree names. Make sure that you enter the tree name in lower case.

Accessing iManager Workstation

To access iManager Workstation:

1 Execute the appropriate iManager Workstation startup script.

Linux: Navigate to the `imanager/bin` directory and execute `./iManager.sh`.

NOTE: If you plan to run iManager Workstation as a non-root user in the future, do not run iManager as root the first time.

Windows: Execute `imanager\bin\iManager.bat`.

2 Log in by using your user name, password, and tree name or IP.

iManager login only accepts lowercase tree names. Make sure that you enter the tree name in lower case.

Understanding Access Modes

When you start iManager, you are granted an *access mode* based on the rights you've been assigned. iManager has three access modes. The mode you are in is displayed on the iManager home page.

Unrestricted Access: This is the default mode before RBS is configured. It displays all of the roles and tasks installed. Although all roles and tasks are visible, the authenticated user still needs the necessary rights to perform the tasks.

There is a setting that you can add to the `config.xml` file which forces Unrestricted Access, even if Role-Based Services is installed. To force Unrestricted Access for all users, add this setting to <*TOMCAT_HOME*>`\webapps\nps\WEB-INF\config.xml`, then restart Tomcat:

```
<setting>
<name><![CDATA[RBS.forceUnrestricted]]></name>
<value><![CDATA[true]]></value>
</setting>
```

For information about restarting Tomcat, see "Starting and Stopping Tomcat" on page 101.

NOTE: When using iManager in Unrestricted mode, you typically see the following message on the iManager Home Page: `Notice: Some of the roles and tasks are not available.` Clicking **View Details** might display a `Not supported by current authenticators` message for several of the tasks, even though the tasks work correctly. This message is misleading, and iManager removes these messages after you configure RBS.

Assigned Access: Displays only the roles and tasks assigned to the authenticated user. This mode takes full advantage of the Role-Based Services technology.

Collection Owner: Displays all of the roles and tasks installed in the collection. If you are a collection owner, though you are not assigned specific roles, it allows you to use all the roles and tasks in the collection. Role-Based Services must be installed in order to use this mode. Adding a group or user as a collection owner does not assign any RBS rights. To assign rights you must make explicit RBS role assignments or make trustee assignments.

NOTE: When collection is assigned to a group, all the members of that group get the collection ownership. The collection owner sees all roles and tasks, regardless of role membership.

Authenticating to an EBA-Enabled eDirectory Server

To access an EBA-enabled eDirectory from an EBA-enabled iManager, the EBA CA certificate must reside in the EBA trusted certificate store of iManager. The `.eba.p12` file contains the EBA CA certificate of the tree. To download the EBA CA certificate on the computer running iManager, use ebaclientinit. ebaclientinit is a new command line utility bundled in the iManager installation package.

When you run ebaclientinit, this utility generates an `.eba.p12` file for a particular user for a particular tree. This file is hidden and resides in the user's home directory ($HOME) on Linux and user's profile directory (%USERPROFILE%) on Windows.

IMPORTANT: EBA requires that the time is synchronized on all EBA-enabled servers and clients in your eDirectory environment. If you do not synchronize the time, EBA might not function properly.

The following table lists the command line options available with the `ebaclientinit` utility:

Command Line Options	Description
`--user-dn`	DN of the user in dot format.
`--password`	Password of the EBA-enabled user.
`--address`	Address of an NCP server in the tree. The syntax is `<IP address>:<port>`.

For example, `ebaclientinit --mechanism ebatls --user-dn john.foo.org --password p@$$w0rd --address 111.111.11.1:524`

Depending on your platform, run `ebaclientinit` by using one of the following methods:

Linux: iManager runs as a `novlwww` user on Linux. Therefore, run ebaclientinit as a `novlwww` user by using this command:

```
sudo -u novlwww -H LD_LIBRARY_PATH=/var/opt/novell/iManager/nps/WEB-INF/bin/linux/:/opt/netiq/common/openssl/lib64/  /var/opt/novell/iManager/nps/WEB-INF/bin/linux/ebaclientinit --mechanism ebatls
```

RHEL: On RHEL, use the following command:

```
sudo -u novlwww -H LD_LIBRARY_PATH=/var/opt/novell/iManager/nps/WEB-INF/bin/linux/:/opt/netiq/common/openssl/lib64/:/opt/novell/lib64/  /var/opt/novell/iManager/nps/WEB-INF/bin/linux/ebaclientinit --mechanism ebatls
```

Windows: Perform the following actions:

1. Log in to iManager as any user other than the `System` user.
2. Run ebaclientinit from `C:\Program Files\Novell\Tomcat\webapps\nps\WEBINF\bin\windows\ebaclientinit.exe --mechanism ebatls`.

   This will place the `.eba.p12` file in the user's home directory.
3. Copy the `.eba.p12` file to `C:\Windows\System32\config\systemprofile`.

   You need to perform this because iManager runs as a `novlwww` user in Windows.

Alternatively, you can run ebaclientinit by using the psexec tool as a `system` user.

1. Download the psexec tool from the Microsoft Download page.
2. From the command prompt, navigate to the directory containing psexec and run the following command:

   ```
   psexec -i -s -d cmd
   ```
3. In the command prompt, run ebaclientinit by using the following command:

   ```
   C:\Windows\system32\Program Files\Novell\Tomcat\webapps\nps\WEBINF\bin\windows\ebaclientinit.exe --mechanism ebatls
   ```

NOTE: If iManager does not find the EBA CA certificate for the tree in the `.eba.p12` file or if `.eba.p12` file is not present, the EBA plug-in of iManager prompts you for the `sadmin` credentials of the server acting as EBA CA. However, NetIQ does not recommend you to use `sadmin`.

Managing Multiple eDirectory Trees

iManager provides an easy way to manage multiple eDirectory trees from a single interface. You can login to the tree that you want to connect to and also switch among the trees that you are currently logged into. After connecting to a tree, iManager provides the tree-specific content, such as tree administration and tasks, and allows you to configure the required options. It relies on the default settings for the other configuration options. You can log in to upto 20 eDirectory trees at the same time.

To manage multiple eDirectory connections:

1. Launch iManager.
2. Log in to an eDirectory tree as an administrator with the appropriate rights.

   After a successful login, iManager displays the **Manage Connections** icon in the right corner of the iManager header.
3. Click the **Manage Connections** icon.

   iManager displays a list of currently logged-in trees under **Manage Connections**. You can also sign into another eDirectory tree from the **Manage Connections** page.
4. To switch to a different tree, click on the respective tree from the list.

5 To **Login** to a different tree, click **Sign in to another directory tree** option and provide the username, password and the tree name or IP and click **Sign in**.

   The iManager home page displays. To verify whether the page displays correct information for this tree, look at the top right side of the page. You will see the user name that you used to log in to this tree and name of the logged in tree.

6 Repeat Step 3 through Step 5 for every tree for which you want to manage connection.

7 To logout from the individual logged in trees, click on the logout icon displayed next to the respective trees listed under the **Manage Connections**.

3 Navigating the iManager Interface

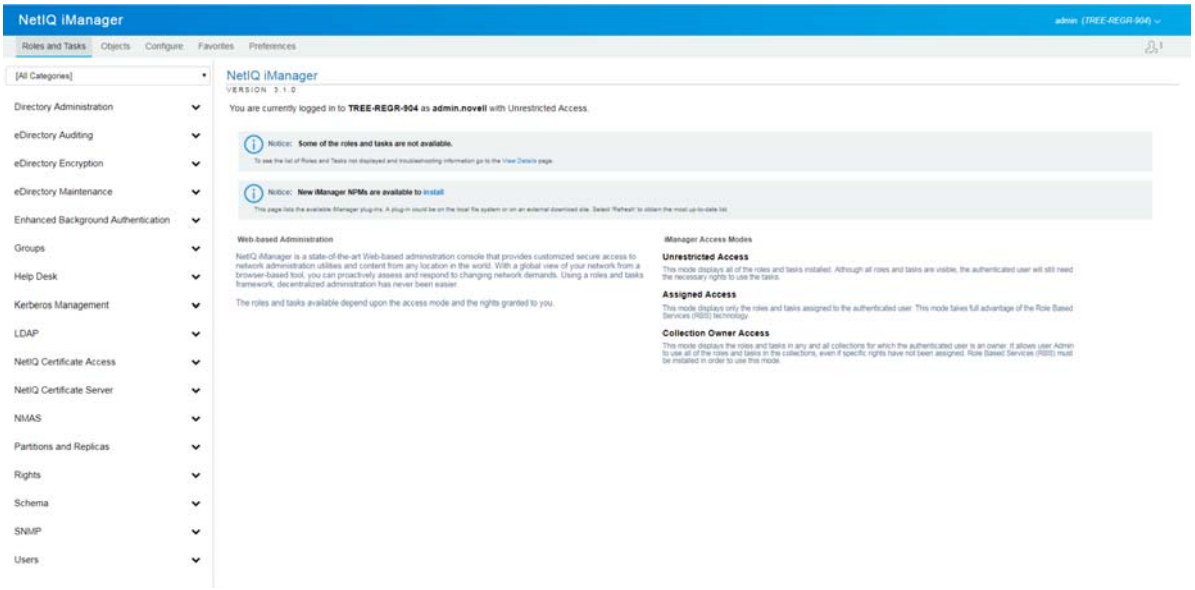
This section describes how to navigate through the NetIQ iManager interface.

iManager Interface

The iManager interface comprises three main regions, or frames.

- Header Frame
- Navigation Frame
- Content Frame

Figure 3-1 *iManager interface with default Roles and Tasks view*



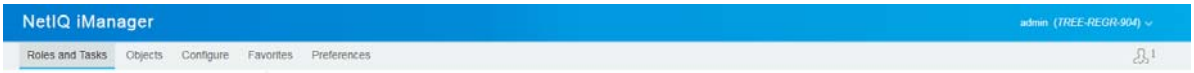
NOTE: Use only the buttons within the interface when you are navigating in iManager. Do not use the Web browser's navigation buttons (**Back**, **Next**, etc.)

To change the default view in Preferences, see "Set Initial View" on page 90.

Header Frame

The Header frame is a largely static frame that occupies the top of the iManager interface. It provides icons with which you can access iManager's various views. A *view* is a combination of Navigation and Content frames that deliver specific management functionality. For example, the default Roles and Tasks view lets you select a given task in the Navigation frame, and then perform the selected task in the Content frame.

Figure 3-2 *iManager Header frame*



The iManager Header frame includes the following icons:

- Home: Returns the Content frame to its default view (as in Figure 3-1).
- Exit: Logs you out of all the eDirectory trees.
- Roles and Tasks: This view displays all the tasks you are authorized to perform in the Navigation frame. This is iManager's default view. For more information, see Chapter 5, "Roles and Tasks," on page 35.
- Objects: This view contains browsing and searching functionality to find objects, including a Tree View feature similar to that used in ConsoleOne. For more information, see Chapter 4, "Browsing Objects," on page 25.
- Configure: This view contains Role-Based Services, iManager Server, Object Creation List, Plug-in Installation, E-mail Notification, and Views, all of which you can configure as you want.
- Favorites: This view displays your most frequent tasks, selected from the Preferences > Favorites page.
- Preferences: This view sets your preferences according to your most frequent tasks, how the Object Selector displays, how your Object View displays, what view appears after logging in to iManager, and what language iManager displays in.
- Manage Connections: This view displays all the logged in eDirectory trees.
- Help: Displays applicable context-sensitive help information, as determined by the current Content frame.

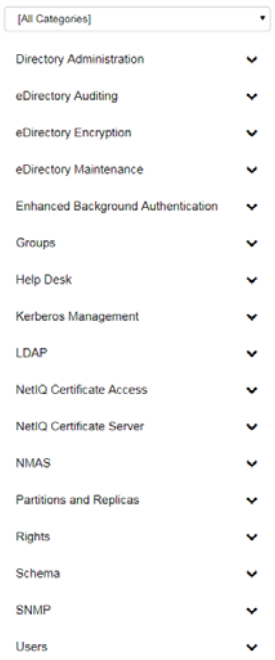
Additionally, the Header frame identifies the currently authenticated user and the tree name to iManager in the upper left.

For information on how to change iManager's default view, see Chapter 6, "Configuring and Customizing iManager," on page 55.

Navigation Frame

The Navigation frame resides along the left side of the iManager UI. It displays task and functionality options related to the currently selected view. For example, the default Roles and Tasks view lists all the tasks your are authorized to perform. Tasks are organized into categories. The list of categories and tasks varies based on the installed plug-ins and the rights granted to you as an authenticated iManager user.

Figure 3-3 *Contents of the Navigation frame when in the Roles and Tasks view*

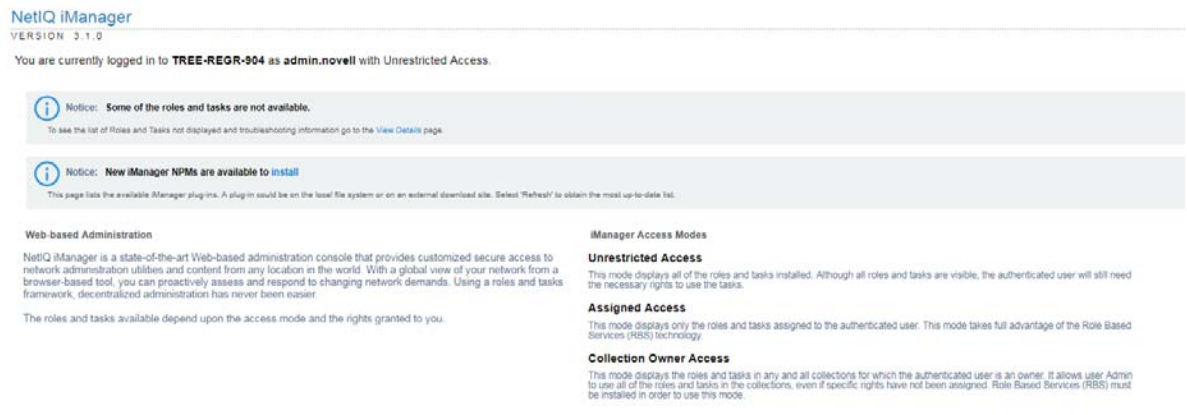


The ordering of tasks within each category is determined by the author of the applicable iManager plug-in. Base plug-in tasks (those that are included with iManager) typically display before tasks from other plug-ins.

Content Frame

The Content frame provides the specific task or object interface, based on the current selection in the Navigation frame.

Figure 3-4 *The default contents of the iManager Content view*



When a task is not selected, the Content frame displays the iManager homepage with general information related to your iManager access rights.

Special Characters

In iManager, some characters have special significance and must be escaped with the backslash (\) character:

NDAP (eDirectory):

- Period (.)
- Equal sign (=)
- Plus sign (+)
- Backslash (\)

LDAP:

- Distinguished names (DNs) and = + \ @; < >
- Leading #
- Leading or trailing spaces

For LDAP, any character can be specified with *xx*. See RFC 2253 (http://www.faqs.org/rfcs/rfc2253.html) for more information.

4 Browsing Objects

iManager lets you manipulate and manage directory objects. There are two paradigms for doing this. First, you can browse for and select the objects with which you want to work, and then specify the task you want to perform on those objects (object-then-task.) Second, you can select the task you want to perform, and then specify the objects to which you want to apply the task (task-then-object.) Either way of doing things is valid, and iManager lets you use the method with which you are most comfortable.

iManager provides the Object View for those from the object-then-task school, and the Object Selector for those from the task-then-object school. The Object Selector is used extensively in the Roles and Tasks view. For more information, see Chapter 5, “Roles and Tasks,” on page 35.

This chapter includes the following sections:

NOTE: iManager supports browsing and selecting objects in an NCP-enabled file system. It allows you to access file system objects through Server and Volume objects in the directory tree.

The ability to browse and select file system objects is available from both the Object View and the Object Selector. However, the actual tasks available for file system objects is provided by the NSS iManager plug-in, which is available separately.

Regardless of the tool you are using, remember the following guidelines when specifying object names:

- If the following characters are part of a dotted eDirectory name, escape them with a backslash (\). You don't need escape characters in most values, but you do need them when the name is a distinguished name or relative distinguished name.
  - Period (.)
  - Equal sign (=)
  - Plus sign (+)
  - Backslash (\)
- If the following characters are part of a name you want to specify in a search, escape them with a backslash (\):
  - Asterisk (*)
  - Backslash (\)

  For example:
  - To search for all objects containing a period, use = *.* as the search filter
  - To search for all objects containing a plus, use = *+* as the search filter
  - To search for all objects containing a backslash, use = ** as the search filter

Using the Object View

The Object view is designed to let you browse for and locate objects in the directory. Once you have selected the objects with which you want to work, you can then specify the tasks to perform on those objects. Open the Object view by selecting the View Objects icon in the Header frame.

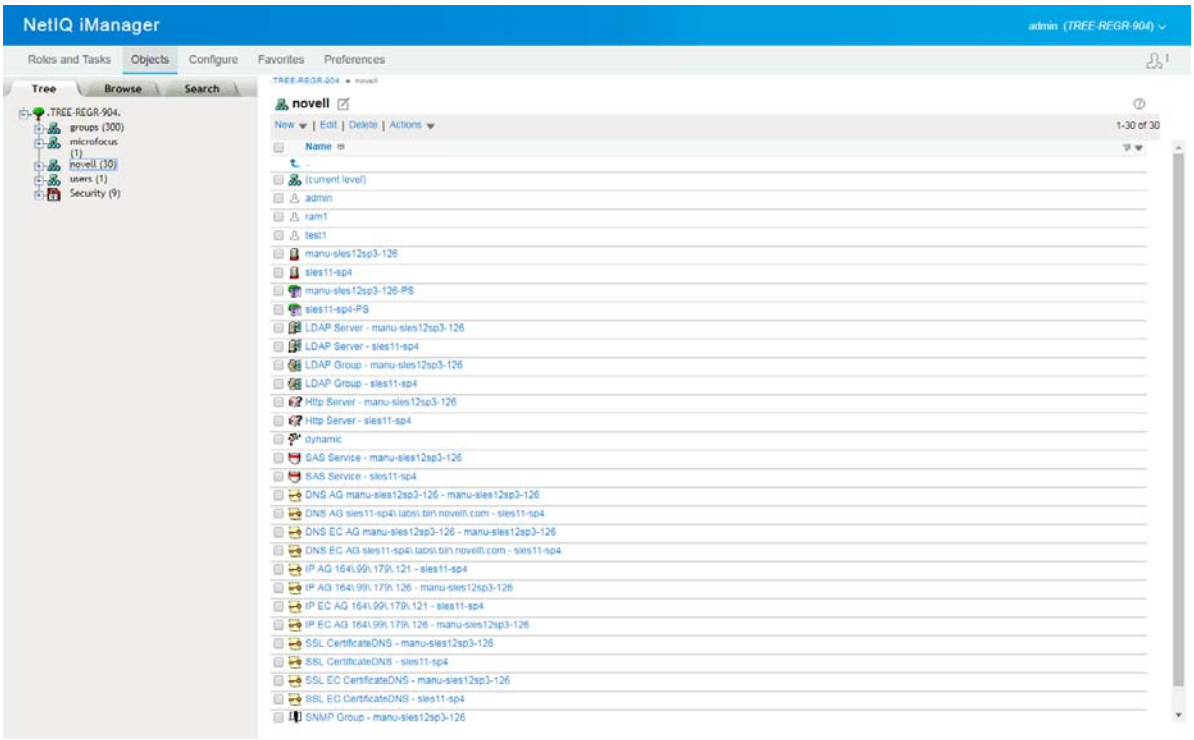
The Object View includes the following tabs in the Navigation frame, each of which give you a different way to browse for and locate directory objects:

- Tree
- Browse
- Search

Tree

The Tree tab lets you browse a directory tree with a look and feel similar to ConsoleOne™. Tree view uses both the Navigation frame and the Content frame to provide its functionality.

Figure 4-1 *The Tree Tab in iManager's Object View*



Tree View Navigation Frame

In the Tree view, the Navigation frame displays the directory structure in the familiar ConsoleOne format. The Navigation frame displays Container, including Volume (file system), objects. Click on the plus and minus icons to expand and collapse the container objects and browse the directory tree.

By default, Tree View displays up to 100 subordinate objects per container, but you can change this setting in the Object View Preferences.

Tree View Content Frame

Selecting one of the container objects in the Navigation frame causes the Content frame to display all the objects in that container. The Content frame is where you actually manipulate directory objects. The Content frame includes a header from which you can select from among several available actions:

Bread Crumbs: At the very top of the Content frame, Tree view provides a bread crumb feature that lets you navigate along the containers in the current context.

Title Bar: The Content frame's title bar displays the name of the currently selected container object. Click the Pencil icon to edit the properties of this container.

Object List Header: The object list header provides access to the following:

- Menu Bar: The Content frame's menu bar provides access to the object-related actions you can perform. Options include the following:
  - **New**: Opens a drop-down menu of "create" tasks.
  - **Edit**: Opens the property book for the selected objects so you can modify their attributes. Selecting multiple objects of the same type lets you set attributes for all the objects to the same value.

    NOTE: You can also open a leaf object's property book by selecting it in the object list. Selecting a container object in the object list opens the selected container and displays all that container's subordinate. To edit the attributes of a container object, you must select its checkbox, then click **Edit**.

  - **Delete**: Deletes the selected objects. To select an object to edit, select its checkbox in the object list.
  - **Actions**: Opens a drop-down menu of supported tasks for the selected objects. To perform a task, select it from the drop-down menu and provide the required information.

    NOTE: If you have configured RBS, the Actions menu displays only those tasks in your assigned roles.

- **Object Count**: To the right of the menu bar, Tree view lists the number of objects in the current page and the total number of objects in the selected container.
- **Select All**: The checkbox in the header functions as a "select all" checkbox for the current page of objects.
- **Sort**: Directly above the Object list is a "Name" column heading and a sort icon. Click either of these to toggle the object sort between ascending and descending alphabetical order.
- **Define Filter**: At the far right of the header, under the object count, is the object filter icon. Select this icon to create a filter that limits the objects displayed in the object list. You can filter on object type and object name, as needed.

  Select **Show All Containers** to display container objects in the Object List regardless of the defined filter.

  Select Advanced Filter to open the Advanced Filter dialog that lets you create a filter using almost any object attribute. For more information, see "Advanced Selection" on page 37.

NOTE: When a filter is active, the filter icon changes to a colored icon , and the filter setting is listed next to the icon. If you configure an advanced filter, iManager displays a checkmark icon next to the filter icon.

Object List: The Content frame's object list displays all objects in the container currently selected in the Navigation frame. By default, the object list displays 100 objects on a page, but you can change this setting in the Object View Preferences.

To perform an action on an object, select its checkbox, then select the action from the Object List header. Select the (current level) object to perform an action on the container in which you are currently browsing.

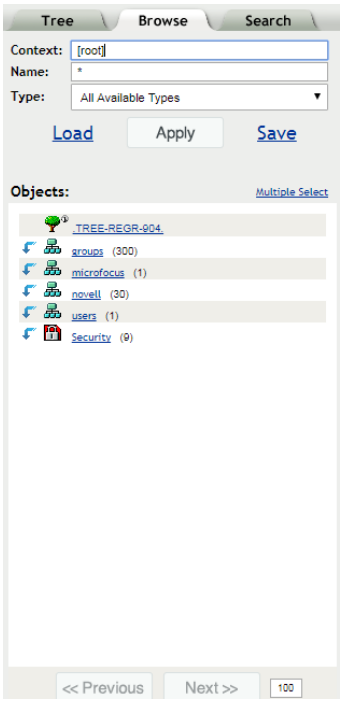
Select the double-period object to navigate up one level to the parent container.

IMPORTANT: Tree view does not support selecting objects across multiple pages in the object list. If you need to do this, use Object View's Browse tab to perform the multiple object action. For more information, see "Browse" on page 28.

Browse

The Browse tab leverages a user interface and functionality similar to the Object Selector to provide a directory browsing tool. For information on navigating the Browse user interface, see "Using the Object Selector" on page 31.

Figure 4-2 *The Browse tab in iManager's Object View*



The Browse tab uses only the Navigation frame to provide its functionality. It includes the following primary components:

Object Filter: Located at the top of the Navigation frame, the object filter lets you limit the objects displayed in the object list. Once defined, click **Apply** to use the filter.

IMPORTANT: The object filtering in the Browse tab only applies to directory objects. It does not filter file system objects, even though they might be visible in the Browse tab.

The object filter uses the following fields:

- Context: Displays only those objects in the specified context. This is identical to opening the container from the object list.
- Name: Displays only those objects that conform to the specified name filter. Use the asterisk (*) wildcard to specify a partial name. For example: `ldap*`, `*cert`, `*server*`.
- Type: Displays only those objects of the type specified.

  NOTE: If you select a specific object type, a plus icon [+] appears that lets you open the Advanced Selection tool, from which you can specify additional, attribute-level filter settings. For more information, see "Advanced Selection" on page 37.

- Load/Save: These two links let you load a previously defined filter definition and save the current filter so it can be re-used, respectively.

Multiple Select / Single Select: Located above the right side of the object list, this link lets you toggle between selecting a single object or multiple objects against which you want to perform a task. The default option is Single Select. For more information, see "Selecting and Filtering Objects" on page 35.

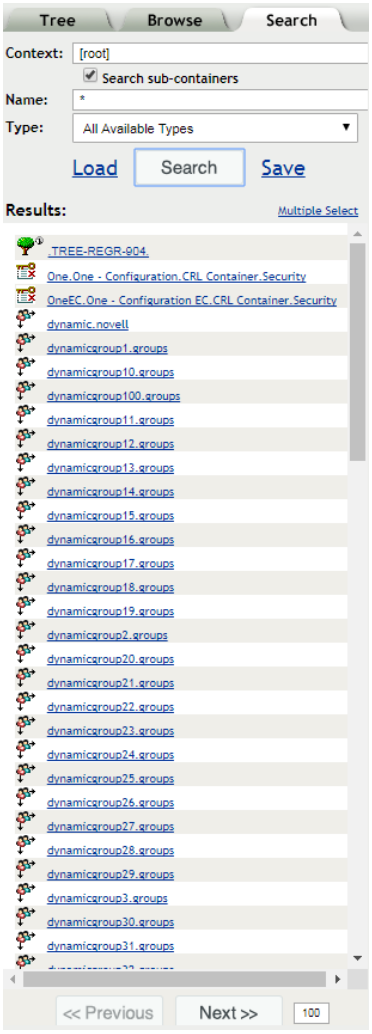
Object List: Displays a list of directory objects, as defined by the criteria in the Object Filter. By default, the object list displays 100 objects on a page, but you can change this value in the Object View Preferences. Use the `Previous` and `Next` buttons to navigate between object pages. You can navigate amongst the objects in the object list by doing the following:

- Select the down arrow icon next to a container object to open that container and view its objects in the object list.
- Select the up arrow icon at the top of the object list to view the contents of the current container's parent. This moves you up one level in the directory tree.
- Select an object, either container or leaf, to open a window with the available tasks for that type of object. Selecting a task opens that tasks UI in the Content frame.

Search

The Search tab is similar to the Browse tab, but instead of displaying a tree structure in the Navigation frame, it displays only those objects resulting from the specified search.

Figure 4-3 *The Search tab in iManager's Object view*



The Search tab uses only the Navigation frame to provide its functionality. It includes the following primary components:

Object Search: Located at the top of the Navigation frame, the object search lets you define the search criteria. Once defined, click **Search** to perform the specified search operation.

IMPORTANT: The object filtering in the Search tab only applies to directory objects. It does not filter file system objects, even though they might be visible in the Search tab.

You can define your search using the following fields:

- Context: Specifies the starting container for the search operation. If you want the search to include subordinate containers, select **Search sub-containers**.
- Name: Defines the object name filter for this search. Use the asterisk wildcard to specify a partial name. For example: `ldap*`, `*cert`, `*server*`.
- Type: Defines the object type filter for this search. iManager only displays objects of the specified type.

NOTE: If you select a specific object type, a plus icon [+] appears that lets you open the Advanced Selection tool, from which you can specify additional, attribute-level filter settings. For more information, see "Advanced Selection" on page 37.

- Load/Save: These links let you load a previously defined search definition and save the current search so it can be re-used, respectively.

Multiple Select / Single Select: Located above the right side of the results list, this link lets you toggle between selecting a single object or multiple objects against which you want to perform a task. The default option is Single Select. For more information, see "Selecting and Filtering Objects" on page 35.

Results List: Displays the results of the search operation. By default, the object list displays 100 objects on a page, but you can change this value in the Object View Preferences. Use the `Previous` and `Next` buttons to navigate between results pages. Select an object, either container or leaf, to open a window with the available tasks for that type of object. Selecting a task opens that tasks UI in the Content frame.

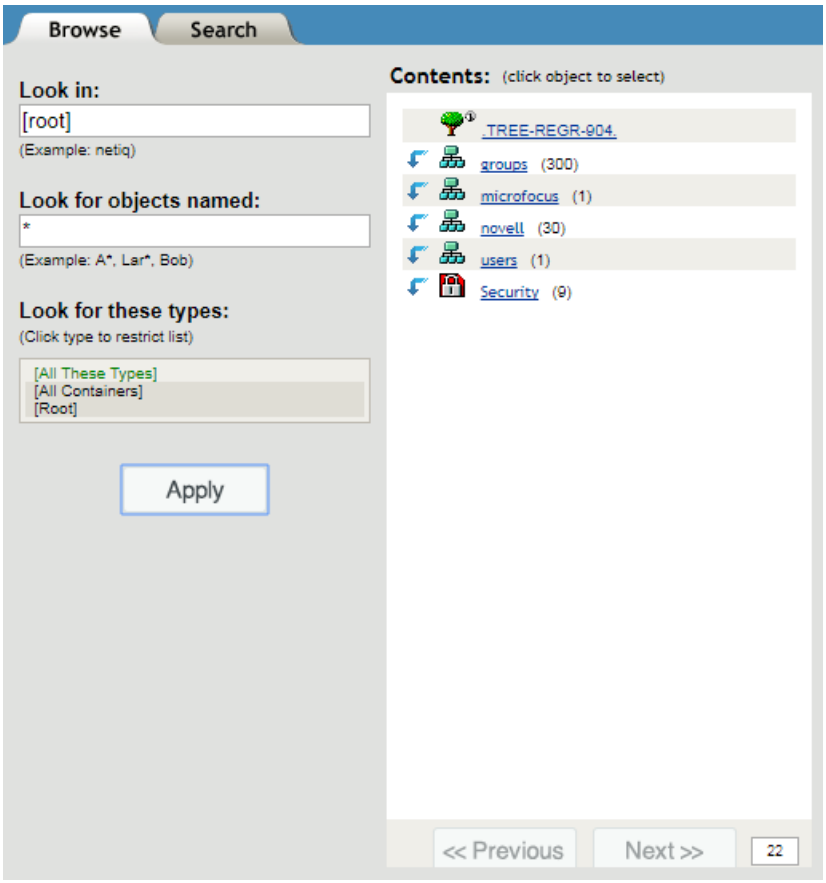
NOTE: The Search tab does not let you navigate objects, such as opening container objects, in the results list. If you want to be able to do this, use the Tree tab or the Browse tab.

Using the Object Selector

The Object Selector lets you select the objects with which you want to work in the current task. iManager provides this tool in any situation where you are selecting a task or action before specifying the objects to which the task or action is applied.

Access the Object Selector by selecting the magnifying glass icon  anywhere it appears in the Content frame. The Object Selector opens in its own window on top of iManager.

Figure 4-4 *iManager's Object Selector*



Object Selector includes two tabs for locating target objects for the tasks you want to perform:

- "Browse" on page 32
- "Search" on page 33

Browse

The Browse tab (default) lets you navigate the directory tree to search for the desired objects. It includes the following primary components:

Object Filter: Located on the left side of the Object Selector, the object filter lets you limit the objects displayed in the Contents list. Once defined, click Apply to use the filter. The object filter uses the following fields:

- Look in: Displays only those objects in the specified context. This is identical to opening the container from the Contents list.
- Look for objects named: Displays only those objects that conform to the specified name filter. Use the asterisk (*) wildcard to specify a partial name. For example: `ldap*`, `*cert`, `*server*`.

- Advanced Browsing: This link opens the Advanced Selection tool, from which you can specify additional, attribute-level filter settings. For more information, see “Advanced Selection” on page 37.
- Load Criteria/Save Criteria: These two links let you load a previously defined filter definition and save the current filter so it can be re-used, respectively.

Contents List: Displays a list of directory objects, as defined by the criteria in the object filter. By default, the object list displays 100 objects on a page, but you can change this number, if desired. Use the `Previous` and `Next` buttons to navigate between object pages. You can navigate amongst the objects in the Contents list by doing the following:

-  Select the down arrow icon next to a container object to open that container and view its objects in the Contents list.
-  Select the up arrow icon at the top of the object list to view the contents of the current container’s parent. This moves you up one level in the directory tree.
- Selecting an object causes iManager to identify that object as one on which you want to perform the current task.

Selected Objects: This component only appears when you are selecting multiple objects for the current task. The Selected Objects field lists the objects currently selected for the task. Click **OK** when the list is complete. Click Clear All if you want to empty the selected objects list and start over.

For more information about selecting single or multiple objects for a task, see “Selecting and Filtering Objects” on page 35.

Search

The Search tab lets you specify a search operation to perform on the directory tree and display the results. It includes the following primary components:

Object Search: Located on the left side of the Object Selector, the object search lets you define the search criteria. Once defined, click Search to perform the specified search operation. You can define your search using the following fields:

- Start search in: Specifies the starting container for the search operation. If you want the search to include subordinate containers, select `Search sub-containers`.
- Search for objects named: Defines the object name filter for this search. Use the asterisk wildcard to specify a partial name. For example: `ldap*`, `*cert`, `*server*`.
- Advanced Browsing: This link opens the Advanced Selection tool, from which you can specify additional, attribute-level search settings. For more information, see “Advanced Selection” on page 37.
- Load Criteria/Save Criteria: These two links let you load a previously defined search definition and save the current filter so it can be re-used, respectively.

Multiple Select / Single Select: Located above the right side of the results list, this link lets you toggle between selecting a single object or multiple objects against which you want to perform a task. The default option is Single Select. For more information, see “Selecting and Filtering Objects” on page 35.

Results List: Displays the results of the search operation. By default, the results list displays 100 objects on a page, but you can change this number, if desired. Use the `Previous` and `Next` buttons to navigate between results pages.

NOTE: The Search tab does not let you navigate objects, such as opening container objects, in the results list. If you want to be able to do this, use Object Selector's Browse tab.

Selected Objects: This component only appears when you are selecting multiple objects for the current task. The Selected Objects field lists the objects currently selected for the task. Click **OK** when the list is complete. Click Clear All if you want to empty the selected objects list and start over.

For more information about selecting single or multiple objects for a task, see "Selecting and Filtering Objects" on page 35.

5 Roles and Tasks

Selecting the Roles and Tasks option in the Header frame displays all of iManager's available roles and tasks in the Navigation frame. iManager groups related roles and tasks into categories. However, you can create custom category groups and assign roles and tasks to them. For more information, see "The Category Tab" on page 65.

This section includes the following topics:

The first section in this chapter introduces Roles and Tasks navigation. The remaining sections provide a detailed description of the tasks available in iManager's core set of roles and tasks. For information about the roles and tasks provided by a product-specific plug-in, consult that product's documentation.

In addition to the Roles and Tasks view, you can configure iManager's Favorites view to display your most frequently used tasks. For more information, see "Manage Favorites" on page 89.

Navigating Roles and Tasks

Navigating iManager's tasks is a straight-forward process that includes the following general steps:

1. (Navigation frame) Open the category that contains the desired task.
2. (Navigation frame) Select the desired task from the category's list of tasks.
3. (Content frame) Provide the necessary information to complete the task. When applicable, this includes specifying those objects to which the task is applied.

   For information about selecting objects to which the task will apply, see "Selecting and Filtering Objects" on page 35.
4. (Content frame) Click **OK** to perform the task.

Selecting and Filtering Objects

For those tasks that can be applied to more than one object at a time (for example, Modify User), iManager provides options, selectable in the Content frame, for locating the desired objects.

Figure 5-1 *Object selection options in a task*

Select a Single Object

This is the default object selection method. Select a Single Object lets you specify a single object to which the task is applied. When using the Object Selector to locate the object, selecting an object automatically closes the Object Selector and inserts the selected object in the task's object name field. For more information about the Object Selector, see "Using the Object Selector" on page 31.

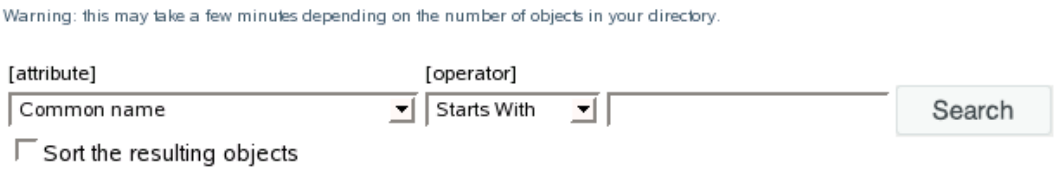
Select Multiple Objects

Select Multiple Objects modifies the tasks object name field to accept a list of objects instead of only one object. The Object Selector also runs in "multiple object" mode so that you can select more than one object at a time. For more information about the Object Selector, see "Using the Object Selector" on page 31.

Simple Selection

Simple Selection opens a basic search tool in the Content frame. With this tool, you can search for objects in the directory tree based on a specified property value.

Figure 5-2 *Basic object filter in a task*



The **attribute** list has a list of attributes on which you can perform the Search operation.

The **operator** list has a list of various operators to be used for the Search operation.

If you want the objects, which result after performing the search operation, to be sorted, select **Sort the resulting objects**.

Simple Selection includes the following limitations:

- Searches the entire directory tree
- Does not support wildcards in the search criteria
- Supports only "starts with" and "equals" filters for property values

Advanced Selection

Advanced Selection provides a more configurable environment for searching the directory for the desired objects.

Advanced Selection gives you more granular control over the object filter used during the search operation. You can configure advanced selection options using the following fields:

Object Type: Specifies the object base class for which you are searching. For example, User.

Container: Specifies the container at which you want to start the search. To search subordinate containers, select **Include sub-containers**.

Filter: Specifies a filter to apply to the search. Select the Filter icon to open a separate window from which you can define the filter. Click **OK** when the filter is done.

The Filter interface includes the following fields:

Aux Classes: Specifies an Auxiliary Class to include in the search.

Attribute: Specifies an attribute (property) that you want to utilize as part of the filter.

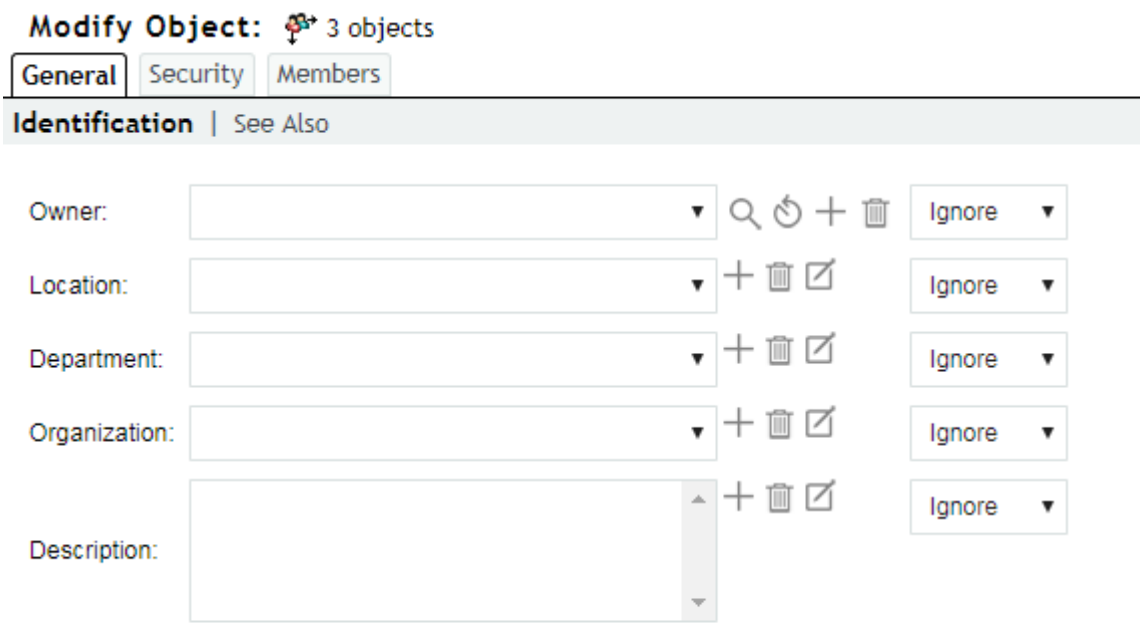
Operator: Specifies the logical operator to apply to the filter. Options include

Value: Specifies the attribute value you are using as a filter. You can use the asterisk (*) as a wildcard to indicate part of a value. For example, smi*, *th, and *mit*.

Additionally, you can chain multiple attribute filters together into a filter group by using the + icon to add a second attribute to the list. When using multiple attribute filters, link them together with a logical AND or logical OR.

After you define a filter, click **Preview**, and click **OK**, the Modify Object screen is displayed. It displays the attributes defined for the objects in the container. The common attribute values are also listed. For example, as per Figure 5-3 the First name, Last name, and Full name attributes have common value (s) for all the objects in the specified container. The attributes whose fields are empty indicate that those attributes does not hold a common value for all the objects. You can add values to these attributes, as well.

Figure 5-3 *The Modify Object Screen*



You can do the following tasks to the attributes and all the objects in the container are updated:

Ignore: Is used not to update any changes to the objects.

Replace: Is used to replace an existing attribute value in the list. To replace, double-click the value, make the changes, and press **Enter.** Then, click **Replace**.

Add: Is used to add values to an attribute. You can add more than one value to an attribute. For example, you have more than one First Names for all the objects.

Remove: Is used to remove attribute values. To remove an attribute value (s):

1. If the attribute has more than one values, you must first hide the values that you do not want to remove by pressing the **Delete** key on your keyboard. This is done because the **Remove** option removes all the values listed. So, you must first hide the values that need not be removed.

   Only the values that have to be deleted are displayed in the attribute list.
2. Click **Remove** from the drop-down list.

   The specified values are deleted and the values that you hide are displayed in the list.

Directory Administration

Directory administration involves the management of objects in your directory tree. You can create, edit, and organize objects.

- "Copying an Object" on page 39
- "Creating an Object" on page 39

- “Deleting an Object” on page 40
- “Modifying an Object” on page 40
- “Moving an Object” on page 40
- “Renaming an Object” on page 40

For more information about eDirectory objects, see the *NetIQ eDirectory 9.0 Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html).

Copying an Object

You can either create a new object with the same attribute values as an existing object, or copy attribute values from one object to another.

1. In Roles and Tasks, click **Directory Administration** > **Copy Object**.
2. In the **Object to Copy From** field, type the name and context of the object or use the Object Selector to find it.
3. Select one of the following options:
   - **Create New Object and Copy Attribute Values**
   - **Copy Attribute Values to an Existing Object**

     The attributes whose class is not extended by the copied object, are not copied.
4. Select **Copy ACL Rights** if you want to copy access control list (ACL) rights to this object.

   This step might take additional processing time, depending on your system and networking environment.

NOTE: The copy object operation does not copy the following object attributes:

- ACL (unless you select **Copy ACL Rights**)
- CN
- DirXML-Associations
- Equivalent To Me
- Group Membership
- Member
- Security Equals
- Any naming attribute
- Any Read Only attribute
- Any RBS attribute

Creating an Object

1. In Roles and Tasks, click **Directory Administration** > **Create Object**.
2. Select the object class from the list that appears, then click **OK**.
3. Specify the requested information that appears according to the object class you selected, then click **OK**.

If you are using Firefox, click the + symbol to add information instead of typing directly in the field.

4 When the confirmation message appears, click **OK**, **Repeat Task**, or **Modify**.

Deleting an Object

1 In Roles and Tasks, click **Directory Administration** > **Delete Object**.

2 Type the name and context of the object, or use the Object Selector to find it, and click **OK**.

A confirmation message appears indicating the object was successfully deleted.

Modifying an Object

1 In Roles and Tasks, click **Directory Administration** > **Modify Object**.

2 Type the name and context of the object or use the Object Selector to find it, then click **OK**.

The Modify Object page displays pages with the selected object's attributes.

3 Modify the object as desired, then click **OK**.

If you are using Firefox, click the + symbol to add information instead of typing directly in the field.

Moving an Object

1 In Roles and Tasks, select **Directory Administration** > **Move Object**.

Type the name and context of the object or use the Object Selector to find it, then click **OK**.

2 In the **Move To** field, select the container to which you want to move the object.

3 Select **Create an Alias in Place of Moved Object** to create an alias in an old location for each object being moved.

4 Click **OK**.

A confirmation message appears indicating the move object operation was successful.

Renaming an Object

1 In Roles and Tasks, select **Directory Administration** > **Rename Object**.

2 Type the name and context of the object or use the search feature to find it.

Type only the name of the new object. Do not include a context.

3 Select to save the old name, if you want to save it.

This saves the old name as an additional unofficial value of the Name property. Saving the old name lets users search for the object based on that name. After renaming the object, you can view the old name in the **Other Name** field on the object's **General Identification** tab.

4 Select **Create an Alias in Place of Renamed Object**, if you want to create an alias for the object being named.

This allows any operations that are dependent on the old object name to continue uninterrupted until you can update those operations to use the new object name.

5 Click **OK**.

A confirmation message appears indicating that the object renaming operation was successful.

Groups

Any user who creates a group automatically becomes the owner of the group. Available group operations include the following:

- "Creating a Group" on page 41
- "Deleting a Group" on page 42
- "Modifying a Group" on page 42
- "Modifying Members of Group" on page 42
- "Move Group" on page 42
- "Rename Group" on page 42
- "Viewing My Groups" on page 42

For more information about using and configuring Group objects, see the *NetIQ eDirectory 9.0 Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html).

Creating a Group

1 In Roles and Tasks, select **Groups** > **Create Group**.

2 In the Create Group page, provide the required information, then click **OK**.

Select **Dynamic Group** to make the new group a dynamic group, of the class dynamicGroup. Otherwise, the group is created as a static group, or the class Group.

Select **Set Owner** to make the creator of a group object the group owner. The group's Owner attribute is set to the DN of iManager's logged-in user. Deselect **Set Owner** to leave the Owner attribute undefined.

Select **Nested Group** to make the new group a nested group so that the group is created with auxiliary class `nestedGroupAux`.

NOTE: You can convert a static group to a dynamic group after the fact by using the Modifying a Group option. This extends the selected Group object to belong to the dynamicGroupAux class.

A group can be either nested or dynamic. You cannot create a group that is both nested and dynamic.

You can convert a static group to a nested group by using the **Modify Group** option. This makes the selected group object belong to the `nestedGroupAux` class.

Deleting a Group

1. In Roles and Tasks, select **Groups** > **Delete Group**.
2. In the Delete Group page, specify the name of the group object to delete, or use the Object Selector to locate it, then click **OK**.

   The Delete Group page lets you Select a single object, Select multiple objects, or use Advanced Selection option to specify the object to delete.

Modifying a Group

1. In Roles and Tasks, select **Groups** > **Modify Group**.
2. In the Modify Group page, specify the name of a Group object, or use the Object Selector to locate it, then click **OK**.
3. Make the desired changes to the Group object's attributes, then click **OK**.

NOTE: If you modify a static group to be a dynamic group, and you are using RBS, you must enable dynamicGroupAux class support. To do this, open **Configure** > **iManager Server** > **Configure iManager** > **RBS** > **Dynamic Group Search Type**. Select **DynamicGroupObjects&AuxClasses** from the drop-down menu, then click **Save**.

You cannot convert a dynamic group to a nested group and vice-versa.

Modifying Members of Group

This task lets you make simultaneous identical modifications to the attributes of all member objects of a specified group.

1. In Roles and Tasks, select **Groups** > **Modify Members of Group**.
2. In the Modify Members of Group page, specify the name of a Group object, or use the Object Selector to locate it, then click **OK**.
3. Make the desired changes to the member object's attributes, then click **OK**.

Move Group

This link redirects you to the Move an Object task. For more information, see "Moving an Object" on page 40.

Rename Group

This option is identical to the Rename an Object task. For more information, see "Renaming an Object" on page 40.

Viewing My Groups

This page displays the groups that you own. From it, you can create a new group, and edit or delete an existing group.

Help Desk

Help Desk provides access to a limited number of user-related tasks. The user who owns this role can do the following:

- "Clearing a Lockout" on page 43
- "Creating a User" on page 43
- "Setting a Password" on page 43

For more information about User objects, see the *NetIQ eDirectory 9.0 Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html).

Clearing a Lockout

A user can be locked out for entering the wrong password too many times or trying to log in with an expired password.

1. In Roles and Tasks, select **Help Desk** > **Clear Lockout**.
2. In the Clear Lockout page, specify the name of a User object, or use the Object Selector to locate it, then click **OK**.

Creating a User

To create a new user object:

1. In Roles and Tasks, select **Help Desk** > **Create User**.

   Fill out the necessary user information, as described in "Creating a User" on page 51.

Setting a Password

1. In Roles and Tasks, select **Help Desk** > **Set Password**.
2. In the Set Password page, specify the name of the User Object. Use the Object Selector to browse for the User Object or use Simple Selection to search for it.
3. Specify the new password for the selected User object (twice), then click **OK**.

   Select **Set simple password** to define a simple password, which is required for native file access for Windows* and Macintosh* users. It is not necessary when Universal Password is enabled.

   NOTE: Password should not exceed 127 characters. If your password contains more than 127 characters, iManager truncates the password to 127 characters automatically.

Partitions and Replicas

Partition and replica operations let you manage eDirectory's physical design and distribution across your directory servers, and includes the following tasks:

- "Creating a Partition" on page 44
- "Merging a Partition" on page 44

- "Moving a Partition" on page 44
- "Viewing Replica Information" on page 45
- "Viewing Partition Information" on page 45
- "Using the Filtered Replica Wizard" on page 46

For information about partitions and replicas, see the *NetIQ eDirectory 9.0 Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html).

Creating a Partition

Partitions create logical divisions of the eDirectory tree. For example, if you choose an Organizational Unit and create it as a new partition, you split the Organizational Unit and all of its subordinate objects from its parent partition. The Organizational Unit you choose becomes the root of a new partition. The replicas of the new partition exist on the same servers as the replicas of the parent, and objects in the new partition belong to the new partition's root object.

1. In Roles and Tasks, select **Partitions and Replicas** > **Create Partition**.
2. In the Create Partition page, specify the container to use as the root of the new partition, or use the Object Selector to locate it, then click **OK**.

   A confirmation message appears indicating that the partition create operation was successful.

Merging a Partition

Merging a partition effectively recombines it with its parent partition. Creating and merging partitions is how you determine how the directory is logically divided.

1. In Roles and Tasks, select **Partitions and Replicas** > **Merge Partition**.
2. In the Merge Partition page, specify the partition to merge with its parent, or use the Object Selector to locate it, then click **OK**.

   To specify a partition, specify the Container object that acts as the partition root.

   A confirmation message appears indicating that the partition create operation was successful.

Moving a Partition

Moving a partition lets you move a subtree in your directory tree. This is also known as a prune and graft operation. You can only move partitions that have no subordinate partitions. If subordinate partitions exist, you must first merge those partitions before performing the move operation.

When you move a partition, eDirectory changes all references to the partition Root object. Although the object's common name remains unchanged, the complete name of the container (and of all its subordinates) changes.

NOTE: When you move a partition, you must follow the eDirectory containment rules. For example, you cannot move an Organizational Unit directly under the root of the directory tree, because the root's containment rules permit only Locality, Country, or Organization objects, but not Organizational Unit objects.

1 In Roles and Tasks, select **Partitions and Replicas** > **Merge Partition**.

2 In the Move partition page, specify the required information, then click **OK**.

- The **Object name** field specifies the partition to move, or use the Object Selector to locate i
- The **Move to** field specifies the Container object into which you want to move the specified partition.
- The Create an alias in place of moved object creates a pointer to the partition's new location. This allows any operations that are dependent on the old location to continue uninterrupted until you can update those operations to reflect the new location. Users can continue to log in to the network and find objects in the original directory location.

WARNING: Make sure your directory tree is synchronizing correctly before you move a partition. If you have any errors in synchronization in either the partition you want to move or the destination partition, do not perform a move partition operation. First, fix the synchronization errors. After moving the partition, if you don't want the partition to remain a partition, merge it with its parent partition.

Viewing Replica Information

Viewing a replica tells you about its current state. An eDirectory replica can be in various states depending on the partition or replication operations it is undergoing.

1 In Roles and Tasks, click **Partitions and Replicas** > **Replica View**.

2 In the Replica View page, specify the partition or server whose replica table you want to view, then click **OK**.

A table appears listing the replica Partition, Type, Filter, and State. For information about replica states, see the *NetIQ eDirectory 9.0 Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html).

Viewing Partition Information

1 In Roles and Tasks, select **Partitions and Replicas** > **View Partition Information**.

2 In the Partition Information page, specify the partition for which you want to view information, then click **OK**.

To specify a partition, specify the Container object that acts as the partition root.

Using the Filtered Replica Wizard

Filtered replicas maintain a filtered subset of information from an eDirectory partition (objects or object classes along with a filtered set of attributes and values for those objects). The Filtered Replica Wizard steps you through the configuration of the filtered replicas on the selected server.

1. In Roles and Tasks, select **Partitions and Replicas** > **Filtered Replica Wizard**.
2. Specify the name and context of the server on which you want to configure a filtered replica, or use the Object Selector to find it, then click **Next**.
3. Click Define the Filter Set to specify the classes and attributes for a filter set on the selected server, then click **Next**.

   The replication filter contains the set of eDirectory classes and attributes you want to host on this server's set of filtered replicas.
4. Click **Finish**.

For more information about filtered replicas, see the *NetIQ eDirectory 9.0 Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html).

Rights

Rights refers to eDirectory trustee rights and trustees. When you create a tree, the default rights assignments give your network generalized access and security. iManager lets you perform the following rights-related tasks:

- "Modifying the Inherited Rights Filter" on page 46
- "Modifying Trustee Rights" on page 47
- "Rights to Other Objects" on page 47
- "Viewing Effective Rights" on page 47

For more information about eDirectory rights, see the *NetIQ eDirectory 9.0 Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html).

Modifying the Inherited Rights Filter

Both eDirectory and the NetWare file system provide an Inherited Rights Filter (IRF) mechanism to block rights inheritance on individual subordinate items. One exception is that the Supervisor right can't be blocked in the NetWare file system.

For more information about Inherited Rights Filters, see the *NetIQ eDirectory 9.0 Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html).

1. In Roles and Tasks, select **Rights** > **Modify Inherited Rights Filter**.
2. Specify the full name of the object whose inherited rights filter you want to modify, or use the Object Selector to find it, then click **OK**.

   This displays a list of the inherited rights filters that have already been set on the object.

3 On the property page, edit the list of inherited rights filters as needed, then click **OK**.

To edit the list of filters, you must have the Supervisor or Access Control right to the ACL property of the object. You can set filters that block inherited rights to the object as a whole, to all the properties of the object, and to individual properties.

Modifying Trustee Rights

A trustee is one object that has been granted explicit rights to another object in your directory tree. To modify the trustee list for a given object:

1 In Roles and Tasks, select **Rights** > **Modify Trustees**.

2 Specify, or use the Object Selector to find, the name of the object whose trustee list you want to view, then click **OK**.

This opens a list of the object's currently assigned trustees.

3 Modify the trustee list as needed, then click **OK**.

- Add a trustee by clicking **Add Trustee**.
- Remove a trustee by selecting its check box and clicking **Remove Selected**.
- Modify a trustee's rights assignment by selecting the **Assigned Rights** link for that trustee.

Rights to Other Objects

This task allows you to view and modify the list of objects to which an object is a trustee.

1 In Roles and Tasks, select **Rights** > **Rights To Other Objects**.

2 In the Rights To Other Objects page, provide the required information, then click **OK**.

- Specify the name of the object in **Trustee name**.
- Specify the context in which you want to search for objects that have this trustee in **Context to search from**.

  Select **Search entire subtree** to search all containers under the specified context.

3 Modify the object list as needed, then click **OK**.

- Add explicit rights to another object by clicking **Add Object**.
- Remove explicit rights to an object by selecting its check box and clicking **Remove Selected**.
- Modify the explicit rights granted to an object by selecting the **Assigned Rights** link for that object.

Viewing Effective Rights

Effective rights is the combination of explicit and inherited rights that an object has at any point in the directory tree. To view an object's effective rights to another object:

1 In Roles and Tasks, select **Rights** > **View Effective Rights**.

2 Specify, or use the Object Selector to find, the name of the trustee whose rights you want to view, then click **OK**.

3 In the Object name field, specify the name of the object for which you want to calculate the trustee's effective rights.

eDirectory calculates the effective rights and displays them in the **Effective Rights** field.

4 Click **Done** when finished.

Schema

The directory schema defines the types of objects that can be created in your tree (such as Users, Printers, and Groups) and what information is required or optional at the time the object is created.

NOTE: You should not use underscore in the attribute names. Only alphanumeric values and hyphens are allowed in attribute names.

---

iManager provides the following schema-related tasks:

- “Adding an Attribute” on page 48
- “Viewing Attribute Information” on page 49
- “Viewing Class Information” on page 49
- “Creating an Attribute” on page 49
- “Creating a Class” on page 49
- “Deleting an Attribute” on page 50
- “Deleting a Class” on page 50
- “Extending a Schema” on page 50
- “Extending an Object” on page 50

For more information about eDirectory schema, see the *NetIQ eDirectory 9.0 Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html).

Adding an Attribute

You can add optional attributes to existing classes if your organization’s information needs change or if you are preparing to merge trees. To add an attribute to an existing class:

NOTE: Mandatory attributes can be defined only while creating a class. A mandatory attribute is one that must be completed when an object is being created.

---

1 In Roles and Tasks, select **Schema** > **Add Attribute**.

2 Select the class you want to add an attribute to, then click **OK**.

3 Select the attributes you want to add, then click **OK**.

Select the desired attributes from the **Available Optional Attributes** list, then click the **Right-arrow** to add these attributes to the **Add These Optional Attributes** list. Use the **Left-arrow** to remove attributes from **Add These Optional Attributes**.

Objects you create of this class now have the properties you added. To set values for the added properties, use the generic Other property page of the object.

Viewing Attribute Information

You can view an attribute's structural details such as Syntax, flags and Classes that use the attribute. To see an attribute's information:

1. In Roles and Tasks, select **Schema** > **Attribute Information**.
2. Select the attribute for which you want to see information, then click **View**.

   The Content frame displays information related to the selected attribute.
3. When finished, click **Close**.

Viewing Class Information

The Class Information page displays information about the selected class and lets you add attributes. During class creation, if the class is specified to inherit attributes from another class, the inherited attributes are classified as they are in the parent class. For instance, if Object Class is a mandatory attribute for the parent class, then it displays on this screen as a mandatory attribute for the selected class.

To see a Class's information:

1. In Roles and Tasks, select **Schema** > **Class Information**.
2. Select the class for which you want to see information, then click **View**.

   The Content frame displays information related to the selected class. To add an attribute to the class, select **Add a new attribute**. To view the class's parent class, select **View superclass**.
3. When finished, click **Close**.

Creating an Attribute

You can define your own custom types of attributes and add them as optional attributes to existing object classes. However, you cannot add mandatory attributes to existing classes. To create an attribute:

1. In Roles and Tasks, click **Schema** > **Create Attribute**.
2. Follow the steps in the Create Attribute Wizard to complete the attribute creation procedure.

Creating a Class

An auxiliary class is a set of properties (attributes) added to particular object rather than to an entire class of objects. For example, an e-mail application could extend the schema of your eDirectory tree to include an E-Mail Properties auxiliary class and then extend individual objects with those properties as needed.

Using Schema Manager, you can define your own auxiliary classes. You can then extend individual objects with the properties defined in your auxiliary classes. To create an auxiliary class:

1. In Roles and Tasks, click **Schema** > **Create Class**.
2. Follow the steps in the Create Class Wizard to define the new class.

Deleting an Attribute

You can delete unused attributes that are not part of the base schema of your eDirectory tree. This might be useful after merging two directory trees, or if an attribute has become obsolete over time. To delete an attribute:

1. In Roles and Tasks, click **Schema** > **Delete Attribute**.
2. Select the attribute you want to delete, then click **Delete**.

   Only attributes that you can delete are displayed.

Deleting a Class

You can delete unused classes that are not part of the base schema of your eDirectory tree. iManager prevents you from deleting classes that are currently being used in locally replicated partitions. To delete a class:

1. In Roles and Tasks, click **Schema** > **Delete Class**.
2. Select the class you want to delete, then click **Delete**.

   Only classes that are allowed to be deleted are shown.

Extending a Schema

You can extend the schema of a tree by creating a new class or attribute. To extend the schema of your eDirectory tree, you need Administrator/Supervisor right to the entire tree. To extend the schema:

1. In Roles and Tasks, click **Schema** > **Extend Schema**.
2. Follow the ICE Wizard through the import, export, migration of data, or schema update and compare operations.

Extending an Object

1. In Roles and Tasks, click **Schema** > **Object Extensions**.
2. Specify the name and context of the object you want to extend, then click **OK**.
3. Depending on whether the auxiliary class that you want to use is already listed under Current Auxiliary Class Extensions, click one of the following:
   - **Yes**: Quit this procedure. See Modifying an Object's Auxiliary Properties in the *NetIQ eDirectory 9.0 Administration Guide (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html)*, instead.
   - **No**: Click **Add**, select the auxiliary class, then click **OK**.
4. Click **Close**.

You can also add or remove auxiliary classes at once for multiple objects.

1. In Roles and Tasks, click **Schema > Object Extensions**.
2. Click the **Select Multiple Objects** tab.

   2a Select the objects that you want to extend, then click **OK**.

The list of auxiliary class extensions is displayed which are common to all the selected objects.

2b To add an auxiliary class, click **Add**, select the required auxiliary class, then click **OK**.

2c To delete an existing auxiliary class, select the class, then click **Remove**.

3 Click **Close** to exit the page.

Users

Managing users and their network access is a central purpose of the directory. iManager provides the following user-related tasks:

- "Creating a User" on page 51
- "Deleting a User" on page 52
- "Disabling an Account" on page 52
- "Enabling an Account" on page 52
- "Modifying a User" on page 52
- "Moving a User" on page 53
- "Renaming a User" on page 53

For more information about user objects in the directory, see the *NetIQ eDirectory 9.0 Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html).

Creating a User

To create a new user object:

1 In Roles and Tasks, select **User** > **Create User**.

2 In the Create User page provide, at a minimum, the required user-related information, then click **OK**.

- **Username**
- **Last Name**
- **Context**
- **Password** (twice)

IMPORTANT: If you do not enter a password, you are prompted to either allow the user to log in without a password (not recommended) or require a password for login.

Select **Set simple password** to define a simple password, which is required for native file access for Windows* and Macintosh* users. It is not necessary when Universal Password is enabled.

Select **Copy from template or user object** to create a user based on an existing Template or User object. When copying from a user object, iManager allows only a copy of the New Object NDS rights instead of a copy of NDS rights, to prevent users from receiving the same rights as the administrator.

Select **Create home directory** to specify a location for the user's home directory, which is created when the user object is created. If you specify a path that doesn't exist, a message appears stating that the user's home directory has not been created.

Deleting a User

To delete a user object:

1. In Roles and Tasks, select **Users** > **Delete User**.
2. Type the name and context of the object or use the search feature to find it, then click **OK**.
3. Click **Delete**.

   A confirmation appears indicating the user object has been deleted.

Disabling an Account

To disable a user account, thereby preventing the user from authenticating to the directory:

NOTE: This only prevents a user from authenticating subsequent to disabling the account. If they are logged in when the account is disabled, their access continues unchanged until they log out.

---

1. In Roles and Tasks, select **Users** > **Disable Account**.
2. Specify, or use the Object Selector to find, the name and context of the object, then click **OK**.
3. Click **Disable**.

Enabling an Account

To enable a previously disabled user account:

1. In Roles and Tasks, select **Users** > **Enable Account**.
2. Specify, or use the Object Selector to find, the name and context of the object, then click **OK**.
3. Click **Enable**.

Modifying a User

To modify an existing user object's properties:

1. In Roles and Tasks, select **Users** > **Modify User**.
2. Specify, or use the Object Selector to find, the name and context of the object, then click **OK**.

   The Content frame displays the user object's property book.
3. Make your changes, then click **Apply** or **OK** to save the changes.

Moving a User

To move a user object:

1. In Roles and Tasks, select **Users** > **Move User**.
2. Provide the required information, as described in “Moving an Object” on page 40.

Renaming a User

To rename a user object:

1. In Roles and Tasks, select **Users** > **Rename User**.
2. Provide the required information, as described in “Renaming an Object” on page 40.

6 Configuring and Customizing iManager

This section describes the various features of NetIQ iManager configuration. You configure iManager from the Configure view. This section discusses the following topics:

IMPORTANT: Using Role-Based Services is optional, although we recommend setting it up for the optimal use of iManager. RBS must be configured in the eDirectory tree in order to use the Plug-In Studio.

Do not use Novell ConsoleOne to modify or delete any RBS objects. RBS objects should be managed using only iManager.

If desired, you can prevent non-admin and non-collection-owner users from accessing iManager's Configure view. For more information see the following topics:

- iManager Views: "Views" on page 86.
- User Preferences: "Preferences" on page 89.
- Authorized Users: "Authorized Users and Groups" on page 75.

Role-Based Services

iManager gives you the ability to assign specific responsibilities to users and to present them with the tools (and their accompanying rights) necessary to perform those sets of responsibilities. This functionality is called Role-Based Services (RBS).

Role-Based Services is a set of extensions to the eDirectory schema. RBS defines several object classes and attributes that provide a mechanism for administrators to grant a user access to management tasks based on the user's role in the organization. This gives users access to only those tasks that the users need to perform. RBS grants only the rights necessary to perform assigned tasks.

NOTE: NetIQ iManager Role-Based Services (RBS) grants rights based upon the Access Control List (ACL) capability of NetIQ eDirectory. The ACLs allow a trustee to be granted rights to a specific object or its subordinate objects. ACLs are not granted based upon specific object types. Each NetIQ

iManager task defines its applicable object types and necessary ACLs. However, these ACLs allow the user to perform those operations with other object types through eDirectory APIs or other tools such as Novell ConsoleOne or NWAdmin.

Use RBS to create specific roles within your organization. The roles contain tasks that an assigned user can perform within iManager, such as creating a new user or changing a password. Tasks are preassigned to roles but can be replaced, reassigned, or removed altogether.

Furthermore, users are associated with roles in a specified scope, which is a container in the tree in which the user has the requisite permissions to perform a task. A role requires this threefold association of role, members, and scope to be complete.

An RBS Role object creates an association between users and tasks. An administrator grants a user access to a task by making the user a member of the role to which the task is assigned.

A user can be assigned to a role in the following ways:

- Directly as a user
- Through group and dynamic group assignments

  If a user is a member of a group or a dynamic group that is assigned to a role, then the user has access to the role.
- Through organizational role assignments

  If a user is an occupant of a organizational role that is assigned a role, then the user has access to the role.
- Through container assignment

  A User object has access to all of the roles that its parent container is assigned. This could also include other containers up to the root of the tree.

A user can be associated with a role multiple times, each with a different scope.

RBS Objects in eDirectory

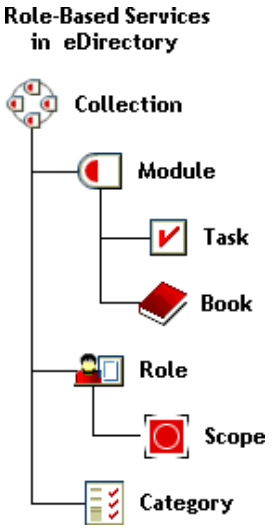
The following table lists the RBS objects. iManager extends the eDirectory schema to include these objects when you install RBS. For more information, see “Installing RBS” on page 58.

Object	Description
rbsCollection	A container object that holds all RBS Role and Module objects. rbsCollection objects are the uppermost containers for all RBS objects. A tree can have any number of rbsCollection objects. These objects have owners, which are users who have management rights over the collection. rbsCollection objects can be created in any of the following containers: ◆ Country ◆ Domain ◆ Locality ◆ Organization ◆ Organizational Unit

Object	Description
rbsRole	Defining a role includes creating an rbsRole object and specifying the tasks that the role can perform. rbsRoles are container objects that can be created only in an rbsCollection container. Role members can be Users, Groups, Organizations, Organization Roles, or Organizational Units, and role members are associated to a role in a specific scope of the tree. The rbsTask and rbsBook objects are assigned to rbsRole objects.
rbsTask	A leaf object that holds a specific function, such as resetting login passwords. rbsTask objects are located only in rbsModule containers.
rbsBook (aka Property Book)	A book is a leaf object that displays a group of pages that allow a user to view or modify the properties of an object or set of objects of the same type. Each page of the book has a tab that you click, to view a different page. A book object resides only in rbsModule containers and can be assigned to one or more roles and to one or more object class types.
rbsScope	A leaf object used for ACL assignments (instead of making assignments for each User object). rbsScope objects represent the context in the tree where a role is performed and are associated with rbsRole objects. They inherit from the Group class. User objects are assigned to an rbsScope object. These objects have a reference to the scope of the tree that they are associated with. The objects are dynamically created when needed, then automatically deleted when no longer needed. They are located only in rbsRole containers. **WARNING:** Never change the configuration of an rbsScope object. Doing so has serious consequences and could possibly break the system.
rbs Module	Represents a container object that holds rbsTask and rbsBook objects. rbsModule objects have a module name attribute that represents the name of the product that defines the tasks or books (for example, eDirectory Maintenance Utilities, NMAS Management, or NetIQ Certificate Server Access). rbsModule objects can be created only in rbsCollection containers.
rbs Category	A category groups roles and tasks together which are specific to a particular function. iManager has 14 default categories: Authentication & Passwords, Collaboration, Directory, File Management, Identity Manager, Infrastructure, Install & Upgrade, Network, Novell Audit, Printing, Security, Servers, Software Licenses & Network, Usage, and Users & Groups. The All Categories selection displays all available roles and tasks. You can also create new categories and assign roles and tasks to them.

RBS objects reside in the eDirectory tree as depicted in the following figure:

Figure 6-1 *Role-Based Services in eDirectory*



Installing RBS

RBS is installed using the iManager Configuration Wizard.

1. In the Configure view, select **Role Based Services** > **RBS Configuration**.
2. Select **Configure iManager**.
3. Follow the on-screen instructions.

Removing RBS

If Role-Based Services is no longer needed in the tree, the RBS Collection object can be safely deleted through iManager. Deleting the RBS collection automatically cleans up all user role associations and scopes in the tree. Do not delete the RBS collection using other utilities, such as ConsoleOne.

To remove Roll-based Services:

1. In the Configure view, select **Role Based Services** > **RBS Configuration**.
2. Select the collection to be deleted.
3. Click **Delete**.

After the RBS collection is deleted, all users logging in to iManager enter in Assigned Access mode even though there is no RBS collection object in the tree.

To switch back to Unrestricted mode (the default mode):

1. In the Configure view, select **iManager Server** > **Configure iManager**.
2. Select the **RBS** tab.
3. Select the appropriate tree name in the **RBS Tree List** field, then click the **minus** button.
4. Click **Save**.

NOTE: When using iManager in Unrestricted mode, you typically see the following message on the iManager Home Page: `Notice: Some of the roles and tasks are not available.` Clicking **View Details** might display a `Not supported by current authenticators` message for several of the tasks, even though the tasks work correctly. This message is misleading, and iManager removes these messages after you configure RBS.

RBS Configuration

The RBS Configuration task provides complete control over RBS objects. It is a central place for managing and configuring RBS objects. You can list and modify RBS objects by type. The task also gives you useful information about the RBS system, such as the number of modules in a collection, how many are installed, how many are not installed, and how many are outdated. Some tasks let you operate on multiple objects simultaneously. For example, you can associate or disassociate multiple members from a role at the same time.

From the Configure view, select **Role-Based Services** > **RBS Configuration** to open the RBS Configuration page in the Content frame.

The page includes two tabs:

iManager 2.x Collection: Displays current RBS collections.

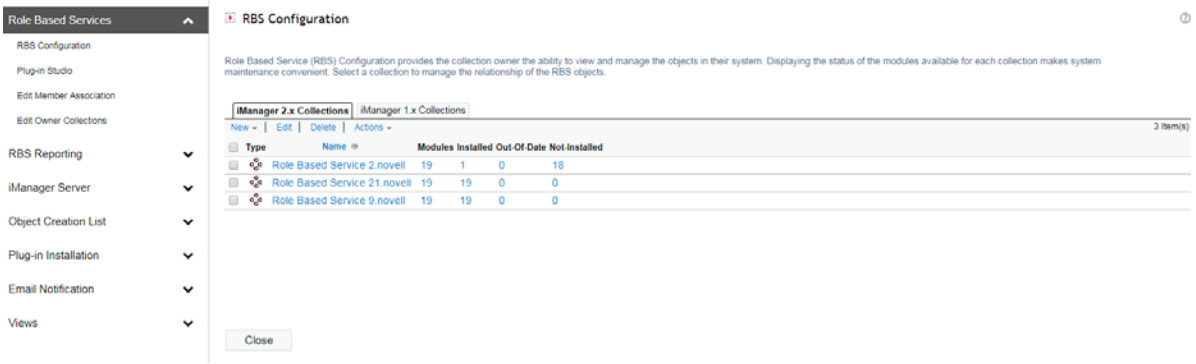
iManager 1.x Collections: Displays older RBS collections that you can either delete or migrate to iManager 2.*x*. If you select Migrate, a wizard steps you through the migration process.

iManager displays only those collections you own, and includes the following information about each collection:

- Module: Indicates the number of modules on the Web server that you are logged in to.
- Installed: Indicates the number of modules that are currently installed.
- Outdated: Indicates the number of outdated modules currently installed.
- Not-Installed: Indicates the number of modules that are available but not installed.

To work with a particular collection, select it from the list. This opens a collection-specific view, as shown in Figure 6-2.

Figure 6-2 *Working with RBS collections in iManager*



The remainder of this section describes the various tabs in the RBS Collection page as well as the other RBS-related tasks in the Role Based Services category.

The Role Tab

The RBS Collection Role tab lets you manage the RBS roles in the collection. From this tab you can do the following:

NOTE: To select a role, select the checkbox to the left of the role name.

Create a New Role

To create a new role in the collection:

1. In the **Role** tab, select **New** > **iManager Role**.
2. Complete the steps in the iManager Role Wizard.

   The wizard steps you through naming the role, assigning tasks and categories to the role, and assigning role members and scopes to the role.

Edit a Role

To edit an existing role in the collection:

1. In the **Role** tab, select the role, then click **Edit**.

   The role's task list appears.
2. Add or remove a task from this page as needed, then click **OK**.

Delete a Role

To delete a role in the collection:

1. In the **Role** tab select the role, then click **Delete**.

   A message appears: `This operation will delete all of the selected roles. Do you want to continue?`
2. Click **OK** to delete the role.

Set a Member Association

To add a member to an existing role:

1. In the **Role** tab select the role, then select **Actions** > **Member Associations**.
2. Provide the required member information, then click **Add**.
   - **Name**: Specify, or use the Object Selector to find, the desired object to be a role member.
   - **Scope**: Specify, or use the Object Selector to find, the container that defines the scope within which this member can perform the role.
3. In the members list, specify how you want rights related to this role assigned to the member, then click **OK**.
   - **Assign Rights**: Instructs eDirectory to automatically grant the member rights necessary to perform the assigned role. When not selected, the member is assigned the role but might not have rights to perform all tasks associated with the role. The member's rights assignments are handled separately.
   - **Inheritable**: Select **subtree** to indicate that the member's scope includes all sub-containers in the specified context. Select **base object** to indicate that the member can perform the role only in the specified container.

NOTE: If a user is a collection owner, and has a member association set, then he/she can manage all the RBS objects within the defined scope. For a list of RBS objects in eDirectory and their description, see "RBS Objects in eDirectory" on page 56.

Assign a Category

To add a category assignment to an existing role:

1. In the **Role** tab, select the role, then select **Actions** > **Category Assignment**.

   The Category Assignment page appears.
2. Select a category, then click the right-arrow to assign it to the role.
3. Click **OK**.

Add a Description to a Role

To add a description to an existing role:

1. In the **Role** tab, select the role and click **Actions** > **Description**.
2. Specify the description in the text box, then click **OK**.

The Task Tab

A task is a plug-in that performs a distinct management function, such as creating a user or setting a password. iManager lists the tasks by group in the navigation area on the left side of the window.

The RBS Collection Task tab lets you do the following operations:

- "Creating a New Task" on page 62
- "Deleting a Task" on page 62
- "Editing the Role Assignment of a Task" on page 62
- "Adding a Description to a Task" on page 63

Creating a New Task

To create a new task:

1. In the **Task** tab, select **New** > **iManager Task**.
2. Complete the steps in the Create iManager Task Wizard.

   The wizard steps you through providing the necessary detail about the new task you are creating.

For information on creating tasks in the Plug-in Studio, see "Creating a New Task from Plug-In Studio" on page 66.

Deleting a Task

To delete an existing task:

1. In the **Task** tab, select the task, then select **Delete**.

   A message appears: `This operation will delete all of the selected tasks. Do you want to continue?`
2. Click **OK**.

Editing the Role Assignment of a Task

To edit the list of roles to which a task is assigned:

1. In the **Task** tab, select the task, then select **Actions** > **Role Assignment**.
2. On the Edit Role Assignment page, add or remove roles from the **Assigned Roles** field, then click **OK**.

Adding a Description to a Task

To add a description to an existing task:

1. In the **Task** tab, select the task, then select **Actions** > **Description**.
2. Specify the description in the text box, then click **OK**.

The Property Book Tab

A property book displays the attributes of a specific object type that you can modify. These properties are of an object or set of objects of the same type.

Property books can be assigned to roles and appear in the list of tasks for a role. For example, a property book that modifies the attributes of User objects might have a page that lets you to specify a user's login script. Another page could let you change a user's e-mail address and telephone number.

Property book pages are similar to tasks. However, they are for displaying and modifying attributes in a single view. For a more complex, wizard-like UI, you should create a task.

The RBS Collection Property Book tab lets you perform the following operations:

Creating a New Property Book

To create a new property book:

1. In the **Property Book** tab, select **New**.
2. Complete the steps in the Create Property Book Wizard.

   The wizard steps you through providing the necessary detail for the property book you are creating.

   IMPORTANT: In iManager, some characters have special significance and must be escaped with the backslash (\) character. For more information, see "Special Characters" on page 24.

Deleting a Property Book.

To delete a property book:

1. Under the **Property Book** tab, select the property book, then select **Delete**.

A message appears: `This operation will delete all of the selected property books. Do you want to continue?`

2 Click **OK**.

Editing the Role Assignment in a Property Book

To modify the list of roles to which a property book is assigned:

1 Under the **Property Book** tab, select the property book, then select **Actions** > **Role Assignment**.

2 On the Edit Role Assignment page, add or remove roles from the **Assigned Roles** field, then click **OK**.

Modifying the Page List for a Property Book

To modify the attribute pages associated with a property book:

1 Under the **Property Book** tab, select the property book, then select **Actions** > **Page List**.

2 On the Edit Page List page, add or remove roles from the **Assigned Pages** field. To change the order of the pages, select a page and click **Move Up** or **Move Down** buttons.

Modifying the Object Type Assignment of a Property Book

To modify the list of object types associated with a property book:

1 Under the **Property Book** tab, select the property book, then select **Actions** > **Object Type**.

2 On the Edit Object Type page, add or remove roles from the **Assigned Object Types** field, then click **OK**.

Adding/Modifying the Description of a Property Book

To add/modify a description to an existing task:

1 In the **Property Book** tab, select the property book, then select **Actions** > **Description**.

2 Specify/modify the description in the text box, then click **OK**.

Defining/Modifying a Preferred Object Selection Method for a Task of a Property Book

To define/modify a preferred object selection method for an existing task:

1 Under the **Property Book** tab, select the property book, then select **Actions** > **Target Chooser Mode**.

2 From the Mode list, select the appropriate mode: **single**, **multiple**, **simple**, or **advanced** and click **OK**.

A successful message is displayed. Click **OK**.

NOTE: For the changes to iManager Base Content module to take effect, restart Tomcat.

The Module Tab

The Module page lists the RBS modules currently installed on a selected collection. Each module contains RBS property books and tasks. From this page, you can add (if you want to create a custom property book) and delete modules, and also type a description for a selected plug-in module.

The RBS Collection Module tab lets you perform the following operations:

- "Adding a New Plug-in Module" on page 65
- "Deleting an RBS Module" on page 65
- "Adding a Description" on page 65

Adding a New Plug-in Module

To add a new plug-in module:

1. In the **Module** tab, select **New**.
2. Specify the RBS module name and a destination context, then click **OK**.

   iManager displays a message indicating the module has been added.

Deleting an RBS Module

To delete an existing plug-in module:

1. In the **Module** tab, select a module to delete, then select **Delete**.
2. Click **OK** to confirm the module deletion.

Adding a Description

To add a description to an existing plug-in module:

1. In the **Module** tab, select a module, then select **Actions** > **Description**.
2. Specify the module description, then click **OK**.

The Category Tab

Category tab groups the related roles and tasks together. The RBS Collection Category tab lets you perform the following operations:

- "Adding a New Category" on page 65
- "Deleting a Category" on page 66
- "Adding a Description" on page 66

Adding a New Category

To add a description to an existing plug-in module:

1. In the **Category** tab, select **New**.

This launches the Create Category Wizard.

2. Specify category name and description (optional), then click **Next**.
3. Select the roles to be associated with the new category, then click **Next**.
4. Review the new category summary, then click **Finish**.

Deleting a Category

To delete an existing category:

1. In the **Category** tab, select a module to delete, then select **Delete**.
2. Click **OK** to confirm the category deletion.

Adding a Description

To add or modify the description of an existing category:

1. In the **Category** tab, select a category, then select **Actions** > **Description**.
2. Specify the category description, then click **OK**.

Plug-In Studio

Plug-In Studio offers a quick and easy way to streamline the tasks that you do several times a day. Use Plug-in Studio to dynamically create tasks for your most frequently used operations. You can also edit and delete tasks here.

For example, to modify a user, instead of selecting **Modify Object**, you can create a dynamic UI to edit only the attributes you have selected, such as first name or title. Data is stored in the `TOMCAT_HOME/webapps/nps/portal/modules/custom` directory.

NOTE: While using the Plug-In Studio, NetIQ recommends that you do not run multiple iManager servers using the same RBS. The Plug-In Studio does not correctly update the plug-ins in eDirectory.

From the Plug-in Studio task, you can perform the following operations:

- "Creating a New Task from Plug-In Studio" on page 66
- "Editing a Task" on page 67
- "Deleting a Task" on page 67
- "Copying Custom Tasks" on page 68
- "Exporting Custom Tasks" on page 68
- "Importing Custom Tasks" on page 68

Creating a New Task from Plug-In Studio

To create a new task with Plug-In Studio:

1. In the Configure view, select **Role-Based Services** > **Plug-in Studio**.
2. Select **New**.

The Task Builder appears to help you build custom tasks and property pages.

NOTE: If a new page is added to the book with certain attributes, rights to these attributes are not granted by default. You must remove the role member and scope and add them back to grant rights.

3 Specify the object type and platform information, then click **Next**.

Available classes: Specify the object class associated with the new task.

Target device: Specify the platform on which the task is used. Typically, the default selection (Default) works fine.

Plug-in type: Specify the type of task you are creating.

Add Auxiliary Classes: Select this option to add aux class support to the task.

4 In the Plug-in Fields screen, provide the necessary information, then click **Install**.

When you click **Install**, iManager dynamically builds the task's `.xml` file, `.jsp` file, and the Java files that execute the task, then it installs those files into the system.

Attributes: Select an attribute to associate with the task from the list of available attributes.

Double-click the attribute to move it to the **Plug-in Fields** field, using the default control.

Controls: Displays the available controls for the attribute selected in the **Attributes** field.

Double-click a control to move the current attribute to the **Plug-in Fields** field, using the selected control.

Plug-in Fields: Displays each attribute/control currently associated with the task. From this field, you can remove attributes from the task, change the control associated with an attribute, and modify the control properties for the attribute.

Plug-in Properties: Lets you specify a **Plug-in ID**, assign the task to an **RBS collection**, and assign the task to a **Role**. The role you assign determines where this task appears in the Roles and Tasks Navigation frame.

Editing a Task

To edit an existing plug-in with Plug-in Studio:

1 In the Configure view, select **Role-Based Services** > **Plug-in Studio**.

2 Select the task, then select **Edit**.

3 Modify the settings described in "Creating a New Task" on page 62, then click **Install**.

iManager displays a confirmation message indicating the plug-in was successfully created and installed.

Deleting a Task

To delete an existing plug-in with Plug-in Studio:

1 In the Configure view, select **Role-Based Services** > **Plug-in Studio**.

2 Select the plug-in from the list of installed custom plug-ins, then click **Delete**.

A message appears: `Are you sure you want to delete this plug-in?`

3 Click **OK** to delete the plug-in.

iManager displays a confirmation message indicating the plug-in was successfully deleted.

Copying Custom Tasks

To copy an existing plug-in with Plug-in Studio:

1 In the Configure view, select **Role-Based Services** > **Plug-in Studio**.

2 Select the plug-in from the list of installed custom plug-ins, then click **Actions > Copy**.

3 Specify a name for the copied plug-in, then click **OK**.

Exporting Custom Tasks

Use this task to export your custom tasks, making them deployable to other iManager servers.

1 In the Configure view, select **Role-Based Services** > **Plug-in Studio**.

2 Select the custom plug-in to export, then click **Actions** > **Export**.

Importing Custom Tasks

Use this task to deploy an exported custom tasks onto multiple iManager servers.

1 In the Configure view, select **Role-Based Services** > **Plug-in Studio**.

2 Select **Actions** > **Import**.

3 Specify, or use the Object Selector to find, the RBS collection into which you want to import the custom plug-ins.

4 Specify, or browse to, the NPM file that you previously exported.

5 Click **Import**.

Editing Member Associations

There are two ways to associate members with roles:

- Select a member, then assign it to a role within a scope as described in "Set a Member Association" on page 61.
- Select a role, then assign members and a scope to it as described below.

To assign an existing role to a selected member

1 In the Configure view, select **Role Based Services** > **Edit Member Association**.

2 Specify, or use the Object Selector to find, a member, then click **OK**.

A list appears displaying the roles to which this member is assigned.

3 Specify a role and role scope to add to this member, then click **OK**.

This data is saved to eDirectory. After login, the newly assigned role appears in the left column of the member who owns it.

Editing Owner Collections

Use this task to change the owner assigned to a collection.

1. In the Configure view, select **Role Based Services** > **Edit Owner Collections**.
2. Specify, or use the Object Selector to find, a collection owner, then click **OK**.
3. Add or remove collections this person can own, then click **OK**.

RBS Reporting

The RBS Reporting feature lets you generate reports about RBS objects in the directory and their configuration. Reports are in chart format and can be exported to other formats and printed. RBS Reporting generates the following reports:

Role Assignments	Unassigned Tasks
Role Tasks Assignments	Unassigned Categories
User Roles Assignments	Custom Roles
User Task Assignments	Custom Tasks
Role Rights Assignments	Custom Categories
Unassigned Roles	Collections

Creating Reports

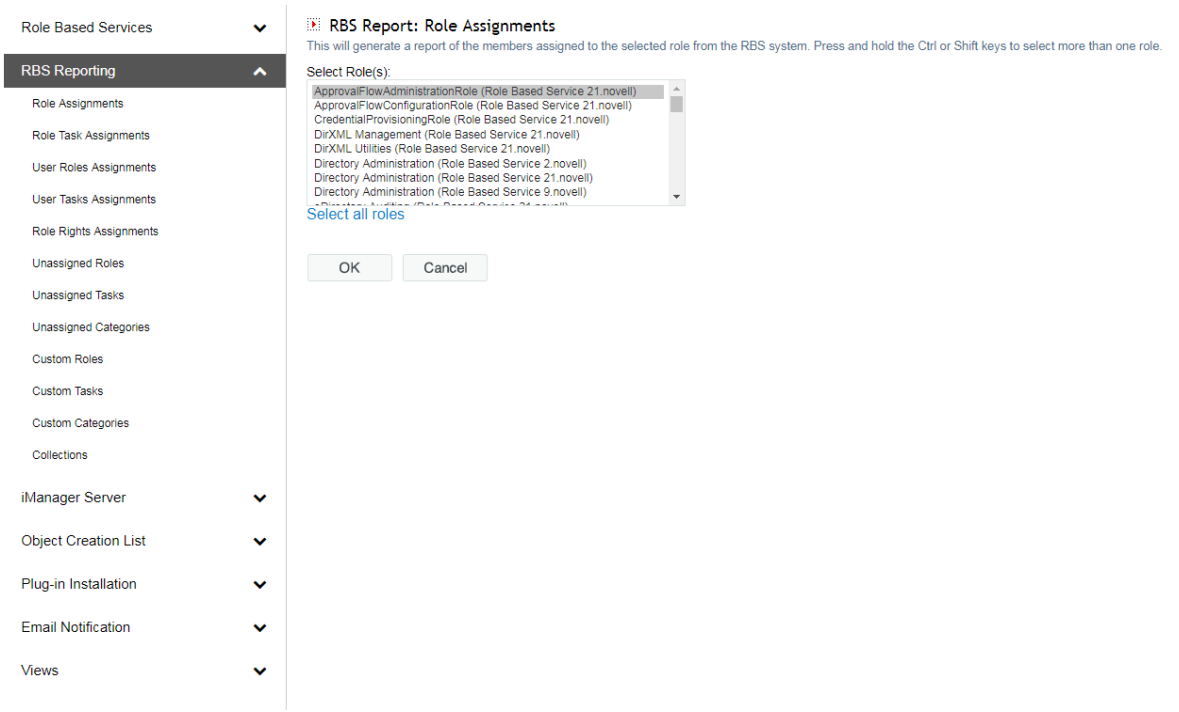
To create an RBS Report:

1. In the Configure view, select **RBS Reporting**.

   Each type of report is implemented as a task.
2. Select the desired report, provide the necessary information, then click **OK**.

   Each report requires that you provide some initial information, such as the roles for which you want to generate a list of assigned members.

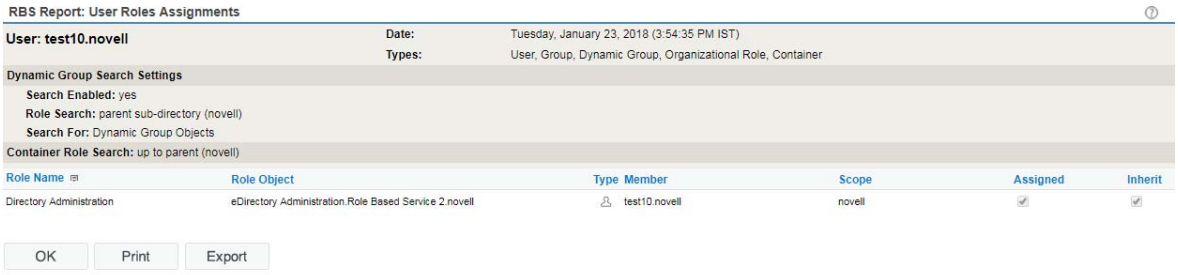
Figure 6-3 *iManager Configure View Showing the Role Assignments Task*



Using Reports

The RBS Reporting tasks generate reports that you can sort, print, and export. The following figure shows an example of an iManager report.

Figure 6-4 *Members Assigned to a Role*



Sorting Reports

By default, the items listed in a report are sorted alphabetically in ascending order on the first column. To indicate the column in which items are sorted, iManager displays a small icon next to the column name, and the icon indicates the sort order. To change the column in which items are sorted, click the name of the column you want.To change the sort order, click the name of the column in which items are currently sorted.

Printing Reports

You can easily print RBS reports by clicking the **Print** button. This opens your browser's print dialog box, where you can select a printer and other printing options. This feature prints only the browser frame that contains the report and it prints the report as displayed in the frame, so you should make sure the items are sorted in the order you want before you click **Print**.

Exporting Reports

You can export report data to XML, CSV, and plain text files to use in other applications such as spreadsheets and databases. The export files contain only data and enough metadata to describe the report columns. Other information, such as the report title and date, is not exported. Items in a report are exported in the currently displayed sort order.

1. Click the **Export** button.
2. In the RBS Report Export window, select the format for the exported data, then click **Export**.
3. When your browser prompts you to open or save the file generated by iManager, select the option you prefer and proceed as required by your browser.

The following are examples of XML, CSV, and plain text files exported from the same RBS report:

XML:

```
<?xml version="1.0"?>
  <rbs-report>
    <rbs-report-header>
     <user>admin.novell</user>
     <report-time>Thursday, June 26, 2008 (10:33:17 AM IST)</report-time>
     <selected-member-types>User, Group, Dynamic Group, Organizational
Role, Container</selected-member-types>
     <dynamic-group>
       <search-enabled>yes</search-enabled>
       <role-search>parent sub-directory (novell)</role-search>
       <search-for>Dynamic Group Objects</search-for>
     </dynamic-group>
     <container-role-search>up to parent (novell)</container-role-search>
    </rbs-report-header>
    <rbs-record>
      <role-name>eDirectory Administration</role-name>
      <role-object>eDirectory Administration.Role Based Service 2.novell</
role-object>
      <member-type>User</member-type>
      <member-object>admin.novell</member-object>
      <scope>.MY_TREE.</scope>
```

```
      <rights-assigned>true</rights-assigned>
      <rights-inherit>true</rights-inherit>
    </rbs-record>
    <rbs-record>
      <role-name>eDirectory Administration</role-name>
      <role-object>eDirectory Administration.Role Based Service 2.novell</
role-object>
      <member-type>User</member-type>
      <member-object>jdoe.novell</member-object>
      <scope>novell</scope>
      <rights-assigned>true</rights-assigned>
      <rights-inherit>true</rights-inherit>
    </rbs-record>
  </rbs-report>
```

CSV:

```
RBS Report Query Settings
User:,"admin.novell"
Date:,"Thursday, June 26, 2008 (10:33:17 AM IST)"
Types:,"User, Group, Dynamic Group, Organizational Role, Container"
Dynamic Group Search Settings:,
Search Enabled:,"yes"
Role Search:,"parent sub-directory (novell)"
Role Search:,"Dynamic Group Objects"
Container Role Search:,"up to parent (novell)"
```

RBS Report: User Roles Assignments

```
User,"Role Name","Role
Object","Type","Member","Scope","Assigned","Inherit",
admin.novell,"Archive Version Management","Archive Version Management.Role
Based Service 2.novell","User","admin.novell",".BLR-ANIL-
TREE.","true","true",
admin.novell,"DFS Management","DFS Management.RBS 270
akpal.08","User","admin.novell",".BLR-ANIL-TREE.","true","true",
admin.novell,"Directory Administration","eDirectory Administration.Role
Based Service 2.novell","User","admin.novell",".BLR-ANIL-
TREE.","true","true",
admin.novell,"Directory Administration","eDirectory Administration.RBS 270
akpal.08","User","admin.novell",".BLR-ANIL-TREE.","true","true",
admin.novell,"eDirectory Maintenance Utilities","eDirectory Maintenance
Utilities.Role Based Service 2.novell","User","admin.novell",".BLR-ANIL-
TREE.","true","true",
admin.novell,"File Protocols","File Protocols.RBS 270
akpal.08","User","admin.novell",".BLR-ANIL-TREE.","true","true",
admin.novell,"Groups","Group Management.Role Based Service
2.novell","User","admin.novell",".BLR-ANIL-TREE.","true","true",
admin.novell,"Groups","Group Management.RBS 270
akpal.08","User","admin.novell",".BLR-ANIL-TREE.","true","true",
admin.novell,"Help Desk","Help Desk Management.Role Based Service
2.novell","User","admin.novell",".BLR-ANIL-TREE.","true","true",
admin.novell,"Help Desk","Help Desk Management.RBS 270
akpal.08","User","admin.novell",".BLR-ANIL-TREE.","true","true",
admin.novell,"IDE Demo Role","IDE Demo Role.Role Based Service
2.novell","User","admin.novell",".BLR-ANIL-TREE.","true","true",
```

```
admin.novell,"Novell Certificate Access","Novell Certificate Access.RBS
270 akpal.08","User","admin.novell",".BLR-ANIL-TREE.","true","true",
admin.novell,"Novell Certificate Server Management","Novell Certificate
Server Management.RBS 270 akpal.08","User","admin.novell",".BLR-ANIL-
TREE.","true","true",
admin.novell,"Partitions and Replicas","Partition and Replica
Management.Role Based Service 2.novell","User","admin.novell",".BLR-ANIL-
TREE.","true","true",
admin.novell,"Partitions and Replicas","Partition and Replica
Management.RBS 270 akpal.08","User","admin.novell",".BLR-ANIL-
TREE.","true","true",
admin.novell,"QuickFinder Administration","QuickFinder Administration.RBS
270 akpal.08","User","admin.novell",".BLR-ANIL-TREE.","true","true",
admin.novell,"Rights","Rights Management.Role Based Service
2.novell","User","admin.novell",".BLR-ANIL-TREE.","true","true",
admin.novell,"Rights","Rights Management.RBS 270
akpal.08","User","admin.novell",".BLR-ANIL-TREE.","true","true",
admin.novell,"Schema","Schema Management.Role Based Service
2.novell","User","admin.novell",".BLR-ANIL-TREE.","true","true",
admin.novell,"Schema","Schema Management.RBS 270
akpal.08","User","admin.novell",".BLR-ANIL-TREE.","true","true",
admin.novell,"Storage Management","Storage Management.RBS 270
akpal.08","User","admin.novell",".BLR-ANIL-
TREE.","true","true",admin.novell,"Users","User Management.Role Based
Service 2.novell","User","admin.novell",".BLR-ANIL-TREE.","true","true",
admin.novell,"Users","User Management.RBS 270
akpal.08","User","admin.novell",".BLR-ANIL-TREE.","true","true",
```

Plain Text:

```
RBS Report Query Settings
User: admin.novell
Date: Thursday, June 26, 2008 (10:33:17 AM IST)
Types: User, Group, Dynamic Group, Organizational Role, Container
-------------------------------------------------
Dynamic Group Search Settings:
Search Enabled: yes
Role Search: parent sub-directory (novell)
Role Search: Dynamic Group Objects
Container Role Search: up to parent (novell)
-------------------------------------------------
Role Name: eDirectory Administration Role Object: eDirectory
Administration.Role Based Service 2.novell Type: User Member: jdoe.novell
Scope: novell Assigned: true Inherit: true
-------------------------------------------------
```

iManager Server

If you do not see this task, you are not an authorized user. See “Authorized Users and Groups” on page 75. This topic includes the following information:

- “Configure iManager” on page 74
- “Security” on page 74

Configure iManager

There are three settings in the `config.xml` file that control the security and the certificates used when iManager creates an LDAP SSL connection:

Security.Keystore.AutoUpdate: If the value of AutoUpdate is `True`, when a user successfully logs in to iManager, the certificate from that eDirectory server might automatically be imported into the iManager-specific keystore. Select the setting **Auto Import Tree Certificate for Secure LDAP** (**Configure iManager** > **Security**).

Security.Keystore.UpdateAllowAll: When UpdateAllowAll is `True`, then any successful user login imports/updates a certificate into the iManager certificate keystore. If the setting is false, only an authorized user login imports/updates certificates.

Security.Keystore.Priority: The priority setting contains two words that define the search order for certificates during a connection: *system,* and *imanager*.*system* uses the default JVM* keystore to locate certificates when created the SSL context. If that fails, it then goes to the iManager keystore.

You can change the search order of *system* and *iManager* by removing either word from the entry.

To further tighten security, do not allow AutoUpdate and use only the system keystore. If you do this, you must manually import the certificates that you want to reside in the default system keystore by using the tools that come with Java. If you disable UpdateAllowAll, then certificate imports occur only from a successful iManager authorized user login.

Security

These settings affect your entire Web server configuration and are saved in the `config.xml` file. You can either save as you go or click **Save** once after you have made all your changes.

Warn When Using a Nonsecure Connection

Select this option if you want users without a secure connection between the Web browser and the Web server to receive the following warning: `You are using a non-secure connection`.

Auto Import Tree Certificate for Secure LDAP

Secure LDAP connections require a certificate. If you select this feature, the system automatically imports a public tree certificate for secure LDAP.

Authorized Users and Groups

Authorized users and groups are those that iManager permits to perform its various administrative tasks. Authorized user data is saved in *TOMCAT_HOME*\webapps\nps\WEB-INF\configiman.properties. The iManager installation process creates this file only if authorized user and group information is provided, but doing it, is not required. If you do not provide the required information, iManager allows any user to install iManager plug-ins and modify iManager server settings (not recommended for long-term.)

When a group or an organizational role is added to this list, all members of the group or the organizational role become authorized users. Adding a nested group supports only first level of members. But adding a dynamic group is not supported because it can have any type of objects as its members.

After installing iManager, you can add an authorized user, group, or organizational role by specifying, or by using the Objector Selector icon next to the **Authorized Users and Groups** list. Doing this modifies the configiman.properties file.

To designate all users of the tree as authorized users, type AllUsers.

NOTE: You can add and save only valid users to the **Authorized Users and Groups** list. If you add invalid users and click **Save**, an error message, which says that the object is not found, is displayed. If you add only invalid users to the list and click **Save**, the error message is displayed and the list of invalid users is automatically replaced by AllUsers. If you do not want all the users of the tree to be authorized users, remove AllUsers from the list, add desired valid users to the list, and click **Save**.

IMPORTANT: If you have installed iManager for the first time, the Authorized Users and Groups list is empty. As an Admin user, you must immediately add users and groups to the list to make them authorized, and to have rights to modify the list. Otherwise, a non-admin user might add users and groups to the list by which he/she acquires the rights to modify the list. You (Admin) might lose the rights to modify the list.

For security-related information about the configiman.properties file, see "iManager Authorized Users and Groups" on page 127.

Enable NetIQ Audit

Make sure you have met the Audit Prerequisites. Select the Enable NetIQ Audit option and select specific iManager logging events, then click **Save**.

Look and Feel

The **Look and Feel** tab lets you customize the appearance of the iManager interface. This information is stored in TOMCAT_HOME\webapps\nps\WEB-INF\config.xml.

Title Name

Specify your organization name in this text box. It then appears in the title bar of the Web browser in place of the default text (NetIQ iManager).

Title Bar Color

You can customize the color of the title bar:

- **Title Color:** Let's you select the color in which your organization name will be displayed in the title bar.
- **Left Color:** Let's you select the color for the left panel of the title bar.
- **Right Color:** Let's you select the color of the right panel of the title bar.

  You can select the color by entering the hexadecimal values in the text field. Entries do not need to be case sensitive.

Logo Image Location

The title bar can also contain the logo of your organization. Your own logos must conform to the dimensions given in the interface.

Store the logo images in `/portal/modules/fw/images`. Specify the path of each image in its respective text field.

By default, logo is not displayed in the header. Check the **Showing a logo in the header is option. Uncheck the box to hide the image** box to display the logo in the header.

Click **Reset** to return to default colors and images.

Click **Save** to save the settings. You can see the preview of all your changes under the **Preview** section.

Logging Events

The **Logging Events** tab lets you configure iManager's logging environment. There are two logging settings:

Logging Level: Select the types of messages you want to log, from four options: **No Logging**, **Errors**, **Errors and Warnings**, and **Errors, Warnings and Debug Information messages**.

NOTE: The **view debug log** and the **clear debug log** options will be visible in the iManager header if the **Logging Level** is set to **Errors, Warnings and Debug Information messages**.

Select your logging output options.

Logging Output: Select the destination for logged messages, from three options: **Send Log Output to Standard Error Device**, **Send Log Output to Standard output Device**, and **Send Log Output to Debug.html File**.

The log file path and log file size both appear on this page. Select **View** to display the current log file in HTML format. Select **Clear** to clear the current log file and reset the log file size to 0 (zero) bytes.

Authentication

The **Authentication** tab configures iManager's login page. It contains the following options:

Remember login credentials: When selected, users must only enter a password to log in.

Use Secure LDAP for auto-connection: When selected, iManager performs LDAP communications using SSL. Some plug-ins, such as Dynamic Groups and NMAS, do not work if this option is not selected. This setting does not take effect until you log out of iManager.

Hide specific reason for login failure: When selected, iManager replaces authentication-related eDirectory messages with a generic error message that reads: `Login Failure. Invalid Username or Password`. For more information, see "Preventing User Name Discovery" on page 127.

Allow 'Tree' selection on Login page: When selected, iManager's login page displays the **Tree** field. If you do not select this option, you must have a default tree name specified or you cannot log in.

Contextless Login: Contextless login allows users to log in with only user name and password, without knowing their entire User object context. For example, `.admin.support.sales.netiq`.

If there are multiple users with the same user name in the tree, contextless login allows to log in by using the first user account it finds with the supplied password within the container order list that the user has specified. User can re-arrange and set the container order list.

If there are multiple users with the same user name in the tree, to log in with a specific user name, a user should provide full context when logging in, or limit the search containers that contextless login searches.

Select **Search from Root** to perform the user search from the root of the directory tree. Select **Search Containers** to specify one or more containers where User objects can be found.

By default, iManager connects with public access, requiring no specific credentials. You can specify a user with specific credentials to do the search for the contextless lookup. The iManager public user is used if you don't specify a user.

IMPORTANT: If you specify a public user, consider carefully the implications of password expiration settings. If the password is set to expire for the public user, you do not have the opportunity to change the password during login after it expires.

---

iManager Server Timeout Settings: If you want the iManager server to time out after a certain period, specify the number of days, hours, and minutes in the respective fields, in the Authentication page.

If you never want the server to time out, select the Never Timeout option.

Redirection After Logout: In the Authentication page, you have to enable this option if you want to be redirected to a desired page after logging out of iManager. You have to specify the desired URL in the **URL:** field. If you do not specify any URL, when you click Exit, you are logged out of iManager. By default, the Login page is displayed.

Redirection After Logout

The **Redirection After Logout** option allows you to specify the URL to be redirected to, after you log out of iManager. If you have not selected this option, when you click Exit, you are logged out of iManager. By default, the Login page is displayed.

Enable: Select this option to enable Redirection After Logout feature.

URL: Specify the URL to be redirected to, after you log out of iManager.

RBS

Role-Based Services (RBS) assigns the rights within eDirectory to perform tasks. When you assign a role to a user, by default RBS assigns the rights necessary to perform the tasks included with that role.

The **RBS** tab lets you configure the following settings:

Enable Dynamic Groups: When selected, RBS allows dynamic groups to be members of a role. For more information about dynamic groups, see the *NetIQ eDirectory Administration Guide*.

Show Roles in Owned Collections: When selected, collection owners see all roles and tasks whether they are members of them or not. De-select this option to force collection owners to see only their assigned roles.

Role Discovery Domain: Indicates where in the tree iManager is to search for roles that are assigned to a member.

- Parent, iManager searches for Dynamic Groups up to the parent container.
- Partition, iManager searches for Dynamic Groups up to the first eDirectory partition.
- Root, iManager searches for Dynamic Groups in the entire tree.

Dynamic Group Discovery Domain: Indicates where in the tree iManager is to search for Dynamic Group membership. Role membership is then checked in the Dynamic Groups found.

- Parent, iManager searches for roles in the user's parent container.
- Partition, iManager searches for roles up to the first eDirectory partition.
- Root, iManager searches for roles in the entire tree.

Dynamic Group Search Type: Selects which type of Dynamic Groups should be searched for role membership.

- Dynamic Groups only, searches for objects that are of the Dynamic Group class type.
- Dynamic Group Objects and Aux classes, searches for objects that are either of the dynamicGroup class type or have been extended with the dynamicGroupAux class. This includes group objects that were later converted to Dynamic Groups.

RBS Tree List: Auto-populated with the eDirectory tree's name when a collection owner or a role member authenticates. If RBS is removed from an eDirectory tree, remove that tree's entry in this list in order to return to Unassigned Access mode.

Plug-In Download

The **Plug-in Download** tab lets you configure the following settings:

Query Novell download site for new NetIQ Plug-in Modules (NPM): Indicates that the iManager Server should query the NetIQ Download site (http://download.novell.com/index.jsp?product_id=&search=Search&build_type=SDBuildBean&families=&date_range=&keywords=iManager&x=23&y=4) for new plug-in modules (NPMs).

Two radio buttons let you configure the query for every available NPM, or query only for updates to already-installed NPMs.

Downloading Plug-In Modules from a Custom Site: You can download the plug-in modules from a custom site by specifying the URL of the custom site in the Download URL field, in the Plug-in Download page.

Downloading Plug-In Modules Through Proxy: If iManager Servers are running under the firewall proxy, the client can access the Internet through a proxy server. Only HTTP Proxy is supported. It is a Web proxy HTTP. To download the plug-ins, the user has to do the following in the Plug-in Download page:

1. Select **Enable Proxy**.
2. Enter in the following fields:
   - **Proxy Host**: Specify the proxy host IP address in this field.
   - **Proxy Port**: Specify the proxy port number in this field.
   - **Username**: Specify the user name in this field.
   - **Password**: Specify the password in this field.
   - **Retype Password**: Specify the same password that you have specified in the **Retype Password** field.

IMPORTANT: iManager plug-ins are not compatible with previous versions of iManager. Additionally, any custom plug-ins you want to use with iManager must be re-compiled in the iManager environment.

Misc

The **Misc** tab lets you configure the following settings:

Enable [this]: You can safely ignore this option. Enable [this] was added to iManager to allow some internal teams to modify their own objects. [this] is an attribute in the tree that enables specific self-management functionality. If [this] is enabled, all eDirectory servers in the tree must be version 8.6.2 or later.

eGuide URL: Specifies the URL to eGuide. This is used in the eGuide launch button in the header and in the eGuide role and task management tasks. This must be a full URL, for example, `https://my.dns.name/eGuide/servlet/eGuide`, or the keyword `EMFRAME_SERVER`. Using `EMFRAME_SERVER` causes eMFrame to look for eGuide on the same server on which eMFrame is located.

For more information on eGuide, see the Novell eGuide documentation Web site (http://www.novell.com/documentation/eguide212/index.html).

Certificate

To choose the cipher level based on your security requirement, use the **Certificate** tab. iManager provides the following certificates to choose from:

- **RSA:** The certificate uses a 2048 RSA key pair. iManager allows the following cipher levels for RSA:
  - **NONE**: Allows any type of cipher.
  - **LOW**: Allows a 56-bit or a 64-bit cipher.

- **MEDIUM:** Allows a 128-bit cipher.
- **HIGH:** Allows ciphers that are greater than 128-bit.

- **ECDSA 256:** The certificate uses an ECDSA key pair with curve secp256r1. iManager allows only one cipher level for ECDSA 256:
  - **SUITEB 128 ONLY:** Allows any type of cipher.
- **ECDSA 384:** The certificate uses an ECDSA key pair with curve secp384r1.

NOTE: By default Java does not support the AES 256-bit encryption. Perform the following steps to use the ECDSA 384 certificates:

1. Download and extract the `Java Cryptography Extension (JCE) Unlimited Strength Policy Files 8`.
2. Replace the `local_policy.jar` and the `US_export_policy.jar` files in the Java security folder (`jdk1.8.xx/jre/lib/security`) with the extracted files respectively.
3. Restart Tomcat.

- SUITEB 128: Allows any type of cipher.
- SUITEB 192: Allows a 56-bit or a 64-bit cipher.

By default, **RSA** is selected and the cipher level is set to **NONE**. For ECDSA certificates, iManager allows only Suite B ciphers. If you change the certificate, ensure that Tomcat server is restarted for the change to take effect.

IMPORTANT: By default, Firefox does not allow **LOW** cipher level.

To enable the **LOW** cipher algorithms in your Firefox browser:

1. Open Firefox, type `about:config` in the location bar, then press **Enter**.
2. (Conditional) If a warning appears, click the **I'll be careful, I promise!** button to continue to the `about:config` page.
3. In the `about:config` page, under the Preference Name list, double-click the **security.ssl3.rsa_rc4_128_md5** preference to change the value to `True`.

   This enables the **LOW** cipher algorithms in your Firefox browser.

For example, to configure only `HIGH` cipher level, modify the `SSLCipherSuite` parameter as follows:

```
<VirtualHost _default_:443>
  --------------
    ----------------
SSLCipherSuite
ALL:ADH:EXPORT56:RC4+RSA:+HIGH:!MEDIUM:!LOW:+SSLv2:+EXP:+eNULL
    -------------
 ---------------
<VirtualHost>
```

You can use the following prefixes to modify the cipher levels:

- **+** : adds ciphers to the list of ciphers and pulls them to the current location in the list.
- **-** : removes a cipher from the list (can be added later again).

- **!** : kills a cipher from the list completely (cannot be added later again).

For more information, see the Apache Module mod_ssl (http://httpd.apache.org/docs/2.0/mod/mod_ssl.html) documentation.

Object Creation List

When you create an object, a pre-configured list of object classes is registered with the Create Object task. The Object Creation List Category contains the following tasks:

- "Adding an Object Class to the Creation List" on page 81
- "Removing an Object Class from the Creation List" on page 81

Adding an Object Class to the Creation List

Use this task to add more objects to the Object Creation List, which is the list of objects that can be created in iManager, using the Directory Administration > Create Object task.

1. In the Configure view, select **Object Creation List** > **Add Object Class to Creation List**.
2. Select the object to add, then click **Next**.
3. Review the XML definition information, then click Finish to create the `.xml` file.

Removing an Object Class from the Creation List

Use this task to remove an object from the Object Creation List, which is the list of objects that can be created in iManager, using the Directory Administration > Create Object task.

1. In the Configure view, select **Object Creation List** > **Delete Object Class from Creation List**.
2. Select the object to remove, then click **Next**.
3. Review the XML definition information, then click Finish to remove the object from the Object Creation List.

Plug-In Module Installation

If you do not see this role in your iManager interface, you are probably not an authorized user. See "Authorized Users and Groups" on page 75.

There are two types of modules used in iManager:

NetIQ Plug-in Module (NPM): These are archives that contain the files for plug-ins to iManager. When you install an NPM using the Available NetIQ Plug-in Modules task, you are installing a plug-in to iManager to add to its functionality.

RBS Module: These are objects in eDirectory that contain RBS Tasks and RBS Book objects. When Role-Based Services has been configured in an eDirectory tree, click **Configure** > **RBS Configuration** to install the RBS Module after the NPM in order for the new tasks associated with the plug-in to become available for use.

Module Installation relates to NPMs only. For information about installing NPMs during the iManager installation process, see "Understanding Installation for iManager Plug-ins" in the *NetIQ iManager Installation Guide*.

Available NetIQ Plug-in Modules

The Available NetIQ Plug-in Modules (NPM) page lists all the available NPMs contained in the packages directory or on the download site. For more information, see "Plug-In Download" on page 78. The name, version, and description of each module are in their respective manifest files.

You can hide the plug-ins by selecting the plug-in modules and clicking the **Hide** button. You can also hide all the plug-in modules so that the Home page doesn't display the `New iManager NPMs are available to install` notice.

You can also view the list of the hidden plug-in modules by clicking the **Show Hidden** button. You can view the hidden plug-in modules if required.

Installed NetIQ Plug-in Modules

This list contains the NPMs that have been installed in iManager. Each NPM is listed by name, local version, and description found in the current manifest files.

iManager does not include all plug-in modules as part of the base product. You must separately download most of the iManager plug-ins. However, the following plug-ins are included in the `base.npm` module that ships with iManager:

- Directory Administration
- Partitions and Replicas
- Help Desk
- Schema
- Rights
- Users
- Groups

For more information, see Chapter 5, "Roles and Tasks," on page 35.

IMPORTANT: To function properly, a plug-in module's version must be compatible with the version of iManager on which it is running. Refer to the specific product documentation for information about iManager version requirements for a particular plug-in module.

For example, iManager plug-ins are not compatible with previous versions of iManager. Additionally, any custom plug-ins you want to use with iManager must be re-compiled in the iManager environment.

Downloading and Installing Plug-in Modules

iManager lets you download and install updates to existing and new plug-ins from within iManager. iManager automatically queries the NetIQ Download Web site once a week for plug-ins.

NOTE: Plug-in modules are not replicated between iManager servers. We recommend that you install the plug-in modules you want on each iManager server.

To download and install one or more plug-in modules:

1. Launch iManager and log in.
2. In the Configure view, select **Plug-in Installation** > **Available NetIQ Plug-in Modules**.

   The Content frame lists all the available iManager plug-ins. iManager automatically checks the Novell download site once a week for updated plug-ins. However, you can update the list at any time by clicking the **Refresh** link.
3. (Optional) If you have downloaded a plug-in, or have one locally that you want to install, click **Add**, then browse for the appropriate plug-in NPM file.
4. Click **OK**.

   This returns you to the Available NetIQ Plug-in Modules page.
5. Select the plug-in you want, then click **Install**.

   The file location shows whether the plug-in is from Local Directory or the Novell Download site. If you select at least one plug-in that has the **File Location** as **NetIQ Downloads** for installation, the NetIQ iManager Plug-in Modules License Agreement page is displayed. Select **I Agree**, then click **OK** to proceed with the installation.

   NOTE: Installing a plug-in from the Novell download site can take several minutes, depending on your connection speed and number of plug-ins being installed. A status bar indicates the download time.
6. After the installation is completed, restart Tomcat.

   Tomcat sometimes requires several minutes to fully initialize. Wait at least 5 minutes before trying to log in to iManager.

   For information about restarting Tomcat, see "Starting and Stopping Tomcat" on page 101.
7. Verify that the new Role appears in the Roles and Tasks page.

   To add members to the new Role, use the Modify Member Association task.

If RBS is Configured

IMPORTANT: In order to reinstall an existing plug-in, you must first delete the rbsModule object for that plug-in from eDirectory using the **Module Configuration** > **Delete RBS Module** task.

1. From the Configure view, select **Role-Based Services** > **RBS Configuration**.

   The table on the 2.x Collections tab displays any out-of-date modules.
2. To update them, select the number in the Out-of-Date column for the Collection you want to update.

   The list of outdated modules is displayed.
3. Select the modules you want to update, then click Update at the top of the table.

Uninstalling a Plug-in Module

1. In the Configure view, select **Plug-in Installation** > **Installed NetIQ Plug-in Modules**.
2. Select the plug-in, then click Uninstall.
3. Restart Tomcat.

   For information about restarting Tomcat, see "Starting and Stopping Tomcat" on page 101.

The steps for manually removing a plug-in module are available in TID #7006125 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=7006125&sliceId=1&docTypeID=DT_TID_1_1&dialogID=790607&stateId=0%200%20792657).

Customizing the Plug-In Download Location

You can create a plug-in download repository if a proxy server or firewall prevents iManager from contacting the NetIQ Download site. This lets you host plug-in modules on a local Web server or a common file system location.

The best way to do this is to use the XML descriptor file from the Download site (http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml) as a template. For more information about the iManager descriptor file, see "Understanding Installation for iManager Plug-ins" in the *NetIQ iManager Installation Guide*.

To set up a local plug-in repository, save the descriptor file locally, then open the file and copy the URL for each plug-in module you want to make available locally and paste it in a Web browser address bar to download the file. After downloading all desired plug-in modules, edit the local copy of the descriptor file to reflect the new URL for each downloaded plug-in module.

A plug-in module URL can be an HTTP link or a file system location. For example:

Windows File System

```
<url><![CDATA[file:///c:\iManager_plugins\NMAS.npm]]></url>
```

Linux File System

```
<url><![CDATA[file:///home/admin/iManager_plugins/NMAS.npm]]></url>
```

HTTP Link

```
<url><![CDATA[http://192.168.0.136/iManager_plugins/NMAS.npm]]></url>
```

Specifying a Local Descriptor File

You can specify a custom descriptor file either during the iManager installation, or after iManager has been installed.

During the installation process, the iManager plug-in download URL can be redirected to a custom descriptor file. To do this, simply change the URL on the Select Plug-ins to Download and Install page to the location of the custom descriptor file and click **Go**.

NOTE: If the message `No plug-ins found or server not available` appears in the Plug-in download area, one or both of the following conditions can exist: There are no updated plug-ins available on the Novell download site, or the connection to download. novell.com from the install program was not successful. Verify your Internet connection.

When iManager is installed, you can change the plug-in module download URL by modifying <*TOMCAT_HOME*>`\webapps\nps\WEB-INF\config.xml`. For example:

Windows File System

```
<setting>
  <name><![CDATA[ModuleDownloadDescriptorURL]]></name>
  <value><![CDATA[file:///c:\iManager_plugins\custom.xml]]></value>
</setting>
```

Linux File System

```
<setting>
  <name><![CDATA[ModuleDownloadDescriptorURL]]></name>
  <value><![CDATA[file:///home/admin/iManager_plugins/custom.xml]]></
value>
</setting>
```

HTTP Link

```
<setting>
  <name><![CDATA[ModuleDownloadDescriptorURL]]></name>
  <value><![CDATA[http://192.168.0.136/iManager_plugins/custom.xml]]></
value>
</setting>
```

IMPORTANT: If you use iManager Workstation to access a custom plug-in URL over an SSL connection (HTTPS), make sure to import the target Web server's certificate or you won't be able to set up a secure connection.

E-Mail Notification

This role enables you to select plug-in-specific tasks that users want to be notified of whenever that specific task occurs. The tasks are set up by the plug-in itself. You decide whether or not to be notified, and specify who should be notified of selected events. Your first task is to set up the mail server.

TIP: Depending on what you select, you could receive a *lot* of e-mails!

Mail Server Configuration

The mail server configuration specifies the SMTP server settings for event notification.

1. In the Configure view, select **Email Notification** > **Mail Server Configuration**.
2. Specify the mail server settings, then click **OK**.

   From Address: Specifies the address that appears in the From field of the iManager e-mail message.

   Primary Mail Server: Specifies an IP address or server name (for example: smtp.novell.com) of a mail server. You must also provide the user name and password for iManager to use to access the SMTP server.

   Secondary Mail Server: Specifies an optional backup mail server. Provide the same information as that for the primary mail server.

Task Event Notification

Plug-ins whose tasks are listed in their `.xml` files automatically register task events on this page.

1. In the Configure view, select **Email Notification** > **Task Event Notification**.
2. In the **Email Address** field, specify the E-mail addresses you want to receive this notification, separated by commas.
3. Select an event.

   The Task Event Properties screen appears.
4. Specify the e-mail subject and the E-mail message in the appropriate fields.
5. In the **Additional Email Addresses** field, type any additional e-mail addresses (separated by commas) you want to notify.
6. Select **Override Default and Notify Only These Addresses** if you want the message to ignore the E-mail list in step 2 and go only to the e-mail addresses specified on this page.

Views

If you do not see this role in your iManager interface, you are probably not an authorized user. See "Authorized Users and Groups" on page 75.

iManager Views are management pages accessed from buttons in iManager's Header frame. You might want to prevent users from accessing certain views, such as **View Objects** or **Configure**.

By default, all views inherit the settings of the parent set.

Showing and Hiding iManager Views

1. In the Configure view, select **Views** > **iManager Views**.
2. Specify, or use the Object Selector to find, a container at which you want to restrict access to Views, then click **OK**.
3. Specify the appropriate view settings, then click **OK**.

There are three view settings from which you can choose:

- Do not set: Does not explicitly set the view state. This is the default setting.
- Hide: Hides the view.
- Show: Displays the view.

Select **Read parent containers of this object** to use the settings of the object's parent container for this object. When selected, the parent settings take precedence over the object's local settings.

Enabling and Disabling Identity Manager view as Default view in iManager on Identity Manager Installed Servers

To enable iManager views:

1. Stop Tomcat.
2. Open the `/var/opt/novell/iManager/nps/WEB-INF/config.xml` file.
3. Add the following configuration details in the xml file:

```
<setting>
        <name><![CDATA[IS_IDM_VIEW_AS_DEFAULT]]></name>
         <value><![CDATA[true]]></value>
    </setting>
```

4. Start tomcat.

NOTE: By default, "IS_IDM_VIEW_AS_DEFAULT"is set to "true".

To disable iManager views:

1. Stop Tomcat.
2. Open the `/var/opt/novell/iManager/nps/WEB-INF/config.xml` file.
3. Add the following configuration details in the xml file:

```
    <setting>
       <name><![CDATA[IS_IDM_VIEW_AS_DEFAULT]]></name>
        <value><![CDATA[false]]></value>
    </setting>
```

4. Start tomcat.

7 Preferences

The Preferences view lets you configure iManager settings related to the application's look and feel. It provides access to the following tasks:

Manage Favorites

Configures the Favorites view, which displays a custom set of often-used tasks together in a special view.

1. From the Preferences view, select **Manage Favorites**.
2. Select the desired tasks from the **Tasks** field and move them to the **Favorites** field.

   Double click tasks to move them, or select them and use the arrow icons to move them.

   Select **Make favorites my initial view** to use the Favorites view as your iManager "Home page".
3. Click **OK**.

Object Selector

Configures the Object Selector settings:

Window Size: Specify Object Selector's window width, height, and left column width, in pixels.

User-Specified Defaults: Specify Object Selector's default settings, including

- Startup Mode: Specifies whether the **Browse** tab or **Search** tab is displayed initially.
- Results per Page: Specifies the number or results to display per page.
- Starting Context: Specifies the default container to which Object Selector opens.
- Search on Startup: Specifies initial search actions when Object Selector opens to the **Search** tab.
- Show Subordinate Count: Enables/disables displaying the total number of objects next to each container object displayed in the Object Selector. When selected, iManager displays the subordinate object count, in parentheses, next to the container name.

NOTE: The subordinate count does not take into account your assigned rights when calculating the subordinate object count, so the number of objects you can see might differ from the count specified.

Object View

Configures the Object View settings:

Column Width: Specifies Object View's column width, in pixels.

Startup Mode: Specifies whether the **Browse**, **Search, or Tree** tab is displayed initially.

Selection Mode: Specifies Object View's initial object selection mode: single object, or multiple objects.

Navigation Pane (Left Side): Specifies the number of results to display in the Navigation frame. This setting applies to all tabs in the Object View. Valid settings include 1 - 500.

Tree Content Pane (Right Side): Specifies the number of results to display one page in the Content frame. This setting applies only to the Tree tab in the Object View. Valid settings include 1 - 500.

Starting Context: Specifies the default directory container to which Object View opens. You can have it open to the last container used, or have it always open to the same container.

Search on Startup: Specifies initial search actions when Object View opens to the **Search** tab.

Show Subordinate Count: Enables/disables displaying the total number of objects next to each container object displayed in the Object Selector. When selected, iManager displays the subordinate object count, in parentheses, next to the container name.

This applies to the Navigation frame in the Tree tab, and the results window in the Browse and Search tabs in the Object View.

NOTE: The subordinate count does not take into account your assigned rights when calculating the subordinate object count, so the number of objects you can see might differ from the count specified.

Set Initial View

Specifies the view that displays when you first log in to iManager. If nothing is selected, the **Roles and Tasks** view defaults to the initial view. Your selection determines the initial view after you log in to iManager.

Language

Specifies the language in which you want iManager to display. You must select the check box to remember the language will remember the language setting between iManager sessions. To make the language setting permanent, set your preferred default language in the Web browser.

NOTE: Plug-ins cannot work properly if the first language (top position) listed in your Web browser's Language setting is not set to a supported language for iManager.

To avoid problems, in your Web browser, click **Tools** > **Options** > **Languages** or a sequence similar to this, then set the first language preference in the list to a supported language.

---

8 Troubleshooting

This section provides some troubleshooting tips resulting from NetIQ's testing of iManager. These tips are arranged alphabetically in the following topics:

Authentication Issues

Authentication is a complex topic, and your existing network infrastructure can affect your ability to successfully perform an initial iManager login. The following facts can help you minimize authentication-related difficulties. For more information about authentication-related topics, see the NetIQ Modular Authentication Service (NMAS) documentation (https://www.netiq.com/documentation/edir88/nmas88/data/bookinfo.html) and NetIQ eDirectory documentation (https://www.netiq.com/documentation/edir88/).

- iManager authentication is a platform-dependent operation, meaning that it functions differently depending on the platform on which iManager is running

  Linux and Windows servers: When iManager runs on a Linux or Windows server it utilizes eDirectory's legacy authentication mechanism and the regular eDirectory password. This mechanism supports eDirectory's Universal Password option but does not support the Simple Password option.

  iManager Workstation: iManager Workstation runs on a client workstation, either Linux or Windows, and leverages the NMAS client that allows it to use Universal Password, if configured.
- iManager does not use LDAP for the initial iManager authentication process. It utilizes eDirectory's proprietary authentication protocol. However, following initial authentication, iManager can, create LDAP connections to eDirectory as needed to support directory access for the installed plug-ins that require LDAP access.
- iManager does not support authenticating with eDirectory's Simple Password.

You might encounter the following error messages when authenticating to iManager. Each error message section discusses possible causes.

HTTP 404 Errors

If you receive a 404 error the first time you attempt to access iManager, you need to verify the ports that Apache is running on. Depending on how you installed iManager and whether you chose to use Apache or IIS, the configuration file locations vary. Apache uses either the `httpd.conf` file or the `ssl.conf` file. Refer to the Microsoft documentation for information on IIS port settings.

HTTP 500 Errors

If you receive an internal server error or servlet container error (either unavailable or being upgraded), iManager is having one of two problems with Tomcat:

- Tomcat has not fully initialized after a reboot.
- Tomcat has failed to start.

Wait a few minutes and try again to access iManager. If you still receive the same errors, verify the status of Tomcat.

Checking the Status of Tomcat

1. Restart Tomcat.

   For information about restarting Tomcat, see "Starting and Stopping Tomcat" on page 101.
2. Check the Tomcat logs for any errors.

   The log file is located in the `$tomcat_home$/logs` directory on the UNIX, Linux, and Windows platforms. On UNIX and Linux, the logs are named `catalina.out` or `localhost_log.date.txt`. On Windows, the log files are named `stderr` and `stdout`.

601 Error Messages

The object name entered could not be found in the context specified.

Some possible causes:

- Contextless login might be disabled.
- Your User object might not be in the configured search containers list. Either ask your administrator to add your user location to the contextless login search containers or log in with a full context.

622 Error Messages

The NDS password has been disabled in the Universal Password policy. This may also manifest itself with a 222 Error Message.

You can avoid this error with iManager Workstation by installing the client, which allows iManager to utilize the Universal Password authentication mechanism rather than eDirectory's legacy authentication process.

632 Error Messages

This error is a system failure with several possible causes (http://www.novell.com/documentation/nwec/).

634 Error Messages

The target server does not have a copy of what the source server is requesting, or the source server has no objects that match the request and has no referrals on which to search for the object.

Some possible causes:

- You entered an incorrect tree or IP address. If you are using the IP address, make sure you include the port if eDirectory is installed on a nonstandard (524) port.
- iManager cannot locate your tree or IP address before timing out. If the tree name fails, use the IP address.

669 Error Messages

An invalid password was used, authentication failed, one server tried to synchronize with another one but the target server's database was locked, or a problem exists with the remote ID or public key.

Some possible causes:

- You typed an incorrect password
- There are multiple users with the same user name in the tree. Contextless login tries to log in using the first user account it finds with the supplied password. In this case, provide a full context when you log in or limit the search containers that contextless login searches.

Tree Name Field

If eDirectory is installed and running on another port besides the default port 524, you can use the IP address or DNS name of the eDirectory server to log in if you also specify the port. For example:

- For an IPv4 address:

  ```
  https://127.0.0.1/nps/servlet/
  webacc?taskId=fw.Startup&forceMaster=true
  ```

- For an IPv6 address:

  ```
  https://[2001:db8::6]:1080/nps/servlet/
  webacc?taskId=fw.Startup&forceMaster=true
  ```

If you use the tree name to log in, you do not have to specify a port.

Possible values for the Tree Name field are the tree name, the server IP address, and the server DNS name. For best results, use the IP address.

Logging in to a Server without a Replica

If necessary, iManager can log in to the eDirectory tree using a server that does not host an eDirectory replica. To do this, iManager maintains a connection cache with the information it needs to successfully log in. To populate the connection cache, the first time you login to an eDirectory tree with iManager you must log in to a server that hosts a replica.

Restarting Tomcat or the iManager server clears the connection cache, so the first time iManager logs in following one of these events, you must log in to a server that hosts a replica.

Unsuccessful Authentication

Login failures occur for a variety of reasons. Authentication error messages are addressed in "Authentication Issues" on page 92.

For information about limiting the error messages that iManager displays upon a failed authentication attempt, see "Preventing User Name Discovery" on page 127.

Expired Password Information

If a password expires, the user sees a message to this effect. However, users might not be aware that grace logins can be quickly consumed, depending on certain operations such as modifying a dynamic group, simple find, and setting a simple password.

These operations consume additional grace logins each time a user performs a task. We highly recommend that you encourage users to change their passwords the first time they are prompted.

Contextless Login Using Alternate Object Classes and/or Alternate Attributes

To enable contextless authentication using an alternate object type, do the following:

1. Open iManager and browse to **Configure > iManager Server > Configure iManager > Authentication**.

   If you do not see this task, you are not an authorized user. See "Authorized Users and Groups" on page 75.
2. Set **Public Username** and **Password** to a user that has rights to read the desired attributes.
3. Modify <*TOMCAT_HOME*>\webapps\nps\WEB-INF\config.xml to include a <Setting> property that lists the attributes you want to add to the contextless search, and then restart Tomcat.

   For information about restarting Tomcat, see "Starting and Stopping Tomcat" on page 101.

For example, the following XML adds the Alias and User objects to the contextless search:

```
<setting>
<name><![CDATA[Authenticate.Form.ContextlessLoginClass.NDAP.treename]]></
name>
  <value><![CDATA[User]]></value>
  <value><![CDATA[Alias]]></value>
</setting>
```

Similarly, the following XML allows users to log in with the CN or uniqueID attribute:

```
<setting>
<name><![CDATA[Authenticate.Form.ContextlessLoginSearchAttributes.NDAP.treename]]></name>
  <value><![CDATA[CN]]></value>
  <value><![CDATA[uniqueID]]></value>
</setting>
```

IMPORTANT:

- In the sample code above, replace *treename* with the name of the appropriate directory tree in lower case.
- If you save any iManager Server settings from the **Configure iManager** task after editing the config.xml file, verify that the tree name is still in lowercase or customized contextless login will fail.

Accessing NCP Server Objects

To improve the performance of the NCP server objects, the **Modify Index Location** option must be disabled.

To disable the **Modify index Location** option:

1. Open the config.xml file from <*TOMCAT_HOME*>/webapps/nps/WEB-INF/.
2. Add the following content to the config.xml file.

   ```
   <setting>
      <name><![CDATA[IndexManagerPlugin_ModifyObjectTask_Disabled]]></name>
      <value><![CDATA[true]]></value>
   </setting>
   ```

3. Save the changes and restart Tomcat.

   For information about restarting Tomcat, see "Starting and Stopping Tomcat" on page 101.

NOTE: To modify the indexes of the NCP server objects, goto **Roles and Tasks** > **eDirectory Maintenance** > **Indexes** > **NCP Server Object** > **Indexes** > **Modify Index Location**.

Deleting and Re-creating User Accounts with the Same Name (Windows XP/2000)

If you have deleted one or more Windows user accounts, and then re-created them with the same name, do the following to use iManager Workstation with the re-created account:

1. Log in as a member of the Administrator group.
2. Take ownership of the `\system32\novell\nici\username` directory. The absolute path varies between Windows 2000 and Windows XP.
3. Delete the folder.

When the user next logs in, this folder is automatically recreated using Novell International Cryptographic Infrastructure (NICI) keys of the re-created user account, and the user can then run iManager Workstation.

DNS 630 Error Message Appears When Creating a Property Book with Invalid Characters in Name

If you create a Property Book and name it using special characters that are invalid, a DNS Error 603 message might be returned. For more information about naming a Property Book, see "Creating a New Property Book" on page 63.

eDirectory Maintenance Task Errors

Running eDirectory Maintenance Tasks requires that Role-Based Services (RBS) must be configured through iManager for the tree that is being administered. For RBS configuration information, see Chapter 4, "Browsing Objects," on page 25.

For additional information, see *The eDirectory Management Toolbox* in the *NetIQ eDirectory 9.0 Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html).

Enabling Debug Messages for Install and Configure

If installation fails, you must enable some debugging messages to help determine what is wrong.

- Linux: Export LAX_DEBUG=true in the terminal session that you start the iManager InstallAnywhere program from.
- Windows: Hold the Ctrl key down as you start the iManager InstallAnywhere program and continue holding it until the debugging screen appears.

History Does Not Automatically Sync Across Multiple Simultaneous User Logins

Using two instances of the same browser (such as two Firefox browsers but not Internet Explorer) avoids the problem. The history book is shared by the two instances.

iManager Does Not Work After Installing Groupwise 7.0 WebAccess (Windows Server 2000/2003)

On Windows 2000 and 2003 Server with IIS 5 or 6, installing Groupwise 7.0 WebAccess to IIS automatically installs Tomcat 5.5.

As the iManager installation begins, the iManager installer program detects that IIS and Tomcat are available for use. The installer reports the inability to stop the iisadmin service. Near the end of the install, the installer reports the inability to start Tomcat.

After the install is completed, Groupwise WebAccess still works, but iManager does not (HTTP 404: Page not found).

Workaround: Do not install iManager and Groupwise on the same server.

Missing Attribute, Object, or Value Errors

If you have a large installation with synchronization delays, you can force iManager to communicate with the master replica. This ensures that you have access to any attributes, objects, or values that have been recently added or modified. This is not recommended for regular use of iManager, but can be helpful when you are experiencing synchronization delays.

To use this parameter when logging in to iManager, add `&forceMaster=true` to the end of the URL after you have loaded the login page. This setting can also be enabled in *`TOMCAT_HOME`*`\webapps\nps\WEB-INF\config.xml`. For example:

- For an IPv4 address:

  ```
  https://127.0.0.1/nps/servlet/
  webacc?taskId=fw.Startup&forceMaster=true
  ```

- For an IPv6 address:

  ```
  https://[2001:db8::6]:1080/nps/servlet/
  webacc?taskId=fw.Startup&forceMaster=true
  ```

You must restart Tomcat after making any changes to the `config.xml` file. For information about restarting Tomcat, see “Starting and Stopping Tomcat” on page 101.

Missing Roles or Tasks in the Configure View

If the following Roles or Tasks are not present on the Configure view, you need to verify that you are an authorized user. For more information, see “Authorized Users and Groups” on page 75.

Possible Missing Roles or Tasks

- Configure iManager task
- Object Creation List role
- Plug-in Installation role
- E-mail Notification role
- View role

Possible Reasons Why You Are Not an Authorized User

- You renamed your tree.

  Edit the `configiman.properties` file and change the tree name for each user.
- Information entered during the iManager installation for the authorized user was incorrect.

  Edit the `configiman.properties` file and add the correct user name including the tree name.
- The `configiman.properties` file is corrupted for some unknown reason.

  Delete the `configiman.properties` file and either re-create the file with the correct information or log in to iManager and go to **Configure view** > **iManager Server** > **Configure iManger**. On the Security page, add the Authorized Users for the system by browsing the tree, or if you are sure of the full path to the user, you can manually enter it.
- The permissions on the `configiman.properties` file have been changed to prevent iManager from reading the file.

  Change the permissions on the file to match the files in the same directory.
- Your administrator has not added you as an authorized user.

  Request to be added to the Authorized Users list. For more information, see "Authorized Users and Groups" on page 75.

Running eDirectory and iManager on the Same Computer (Windows only)

If iManager was installed before eDirectory, you might experience any of the following errors when using iManager, LDAP(S), or HTTP(S) to access eDirectory.

```
-340 error when trying to access encrypted attributes with iManager

 LDAP : SSL_CTX_use_KMO failed. Error stack: error:1412D0D4:SSL
  routines:SSL_CTX_use_KMO:read wrong packet type (err = -1418)
 HTTP : 0016 TLS operation failed, err: 1, result: -1 --
  HTTP : -- error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared
  cipher
 HTTP : 0017 TLS operation failed, err: 1, result: -1 --
  HTTP : -- error:1406B0BD:SSL routines:GET_CLIENT_MASTER_KEY:no p
  rivatekey
```

```
HTTP : Unable to access server certificate and key, handshakes will fail -
 - HTTP : -- error:1412D0D4:SSL routines:SSL_CTX_use_KMO:read wrong packet
 type
Limber : Error while setting NCP Key Material Name SSL CertificateDNS to
 server, Err: failed, -340 (0xfffffeac)...
 Limber : Error During syncKeyMaterialInfo -340 (0xfffffeac)
```

It could be that eDirectory's initial system configuration has not occurred. The user who installed eDirectory and the user who is running the eDirectory server must coordinate the eDirectory configuration. Generally, eDirectory is installed as administrator and is run as SYSTEM. You can manually correct this issue, but an understanding of eDirectory, iManager, NICI, and other currently installed products is necessary. You must determine if the following steps are safe to perform. You should also check the product's documentation and dependencies to see if any long-term encrypted data or secrets are used.

If eDirectory and iManager are installed on the same computer, you can manually configure eDirectory after eDirectory installation.

NOTE: You should not do this if eDirectory was installed at a previous time and has been successfully running on the current machine.

---

1. Log in as an administrator.
2. Stop the eDirectory server and the Tomcat service.

   Also stop any other service that may be using NICI.
3. Take ownership of the `%systemroot%\system32\novell\NICI\SYSTEM` directory.

   Do this from the file properties' **Security** > **Advanced Options**.
4. Save the contents of the SYSTEM directory in a backup directory.
5. Delete the contents of the SYSTEM directory.
6. Copy the contents of `%systemroot%\system32\novell\NICI\Administrator` to `%systemroot%\system32\novell\NICI\SYSTEM`.
7. You can reset the permissions of `%systemroot%\system32\novell\NICI\SYSTEM` and its contents so that only SYSTEM has access.
8. Restart the NDS Server and Tomcat services and any other service you may have stopped.

"Service Unavailable" Message Appears During Multiple Plug-In Installs

This situation occurs when you select several plug-ins to install, all at the same time. While the plug-in installation continues over several minutes, the browser page times out and returns a 503 Error.

Although you probably don't need to do anything but wait, you can monitor plug-in installations through the Tomcat log files.

Tomcat

The following general Tomcat information can be useful in your troubleshooting efforts.

Starting and Stopping Tomcat

The following tables describe how to start and stop Tomcat on the platforms supported by iManager

Table 8-1 *Stopping and Starting Tomcat*

Platform	Restart Command
Linux	• **`init.d` process:** Enter `/etc/init.d/novell-tomcat8 stop`, then enter `/etc/init.d/novell-tomcat8 start`. • **`systemd` process:** Enter `systemctl stop novell-tomcat8-service.service`, then enter `systemctl start novell-tomcat8-service.service`.
iManager Workstation	Shut down and restart iManager Workstation.
Windows	Stop and start the Tomcat service.

Tomcat Ports

If you experience port conflicts while upgrading to iManager, or need to know the ports that Tomcat is using, consult the platform-specific information in this section.

Linux

View Tomcat ports in the `/var/opt/novell/tomcat8/conf/server.xml` file.

The non-SSL port section of the file begins with `Define a non-SSL Coyote HTTP/1.1 Connector` on port *n*, while the SSL port section begins with `Define an SSL Coyote HTTP/1.1 Connector` on port *n*.

Windows

Windows allows for relocation of all files. If you accept the defaults in the iManager installation, look for Tomcat configuration files in the *`rootdir`*`\novell\tomcat8\conf\server.xml` file.

If you can't find a configuration file, search the Windows registry for the Tomcat settings.

“Unable to Determine Universal Password Status” Error

If a UNIX eDirectory server is configured to use SSL for LDAP communications, you might receive the following error when you select the option in iManager to set a Simple Password:

```
Unable to determine universal password status
```

To resolve this error, run the `/usr/bin/nmasinst/nmasinst` utility on the eDirectory server. This utility lets you install login methods into eDirectory from a UNIX machine and is required to run the Universal Password feature.

For more information, see the *NMAS Chapter* in the *eDirectory 9.0 Administration Guide*.

iManager Workstation Does Not Display Information

iManager workstation might not display error messages, and load pages such as Tree View, Object Browse, Create Objects, and page after clicking the Refresh button. This happens when the XULRunner browser cache contains old data of the previous build of iManager workstation.

Work around: You must manually clear the data from browser cache.

For Windows:

1. Exit iManager.
2. Browse for `C:\Users\<username>\AppData\<Profile>\Mozilla\eclipse\Cache` (the path varies depending on the configuration and OS).
3. Delete all the data from the `Cache` directory.
4. Restart iManager.

For Linux:

1. Exit iManager.
2. Browse for one of the following:
   - `/root/.mozilla/eclipse/Cache` (for root user)
   - `/$HOME/.mozilla/eclipse/Cache` (for non-root user)
3. Delete all the data from the `Cache` directory.
4. Restart iManager.

Sometimes Refresh Button Does Not Function

Sometimes the Refresh button in various pages does not function when you click it.

Work around:

1. Log out from iManager.
2. Clear the browser's cache.
   - For Internet Explorer,
     1. Click **Tools > Internet Options**. The Internet Options dialog box is displayed.
     2. Under the **General** tab, under **Browsing history**, click Delete.
   - For Firefox,
     1. Press **Alt + F >** select **History** and click **Clear Recent History**.
     2. Select **Cache** and click **Clear Now**.
3. Log in to iManager.

iManager Plug-in Installation Hangs or Plug-ins Are Not Properly Installed

When you install iManager plug-ins, sometimes either the installation hangs or the plug-ins are not properly installed.

Work around

For iManager Standalone:

1. Log out from iManager.
2. Clear the browser's cache.
   - For Internet Explorer, do the following:
     1. Click **Tools > Internet Options**. The Internet Options dialog box is displayed.
     2. Under the **General** tab, under **Browsing history**, click Delete.
   - For Firefox, do the following:
     1. Press **Alt + F > > Select History**.
     2. Click **Clear Recent History**.
     3. Select **Cache** and click **Clear Now**.
3. Log in to iManager.
4. Re-install the plug-ins.

For iManager workstation:

- For Windows:
  1. Exit iManager.
  2. Browse for `C:\Users\<username>\AppData\<Profile>\Mozilla\eclipse\Cache` (the path varies depending on the configuration and OS).
  3. Delete all the data from the `Cache` directory.
  4. Restart iManager.
- For Linux:
  1. Exit iManager.
  2. Browse for one of the following:
     - `/root/.mozilla/eclipse/Cache` (for root user)
     - `/$HOME/.mozilla/eclipse/Cache` (for non-root user)
  3. Delete all the data from the `Cache` directory.
  4. Restart iManager.

Login Issue with Tree IP Address Change

Consider the following scenario:

1. Your IP address is <*xxx.xx.xx.xx*>, you have configured eDirectory on it, and your tree name is <XXX_TREE>.
2. You have a login cache that maps <XXX_TREE> to <*xxx.xx.xx.xx*>.
3. Because of network movement, you have got a new IP address <*yyy.yy.yy.yy*>, configured eDirectory on it, and the tree name remains same (<XXX_TREE>).
4. Another user has taken your previous IP address <*xxx.xx.xx.xx*>, and configured a new eDirectory tree <YYY_TREE>.

Now, if you log in to iManager with <XXX_TREE> tree name, you would log in to <YYY_TREE> because <XXX_TREE> maps to <*xxx.xx.xx.xx*>, but <*xxx.xx.xx.xx*> is currently configured with <YYY_TREE>.

Work around:

- For Windows,
  1. Go to `...\Program Files\Novell\Tomcat\webapps\nps\WEB-INF\`.
  2. Open `config.xml` file.
  3. In the file, search for the `Cached-Tree` setting and delete your `Tree Name` value from the setting.
  4. Delete the setting that starts with your tree name.
- For Linux,
  1. Go to `/var/opt/novell/iManager/nps/WEB-INF`.
  2. Open `config.xml` file.
  3. In the file, search for the `Cached-Tree` setting and delete your `Tree Name` value from the setting.
  4. Delete the setting that starts with your tree name.

Insufficient Java Heap Size Results in Failed Login

To increase the heap size on a Linux server running Tomcat, stop Tomcat and open a terminal window. In the terminal, run the following command, then restart Tomcat:

```
export CATALINA_OPTS="-Xms128m -Xmx1024m"
```

To increase the heap size on a Windows server running Tomcat, stop the Tomcat service, create a new environment variable called `JAVA_OPTS`, and set the value of the variable to `-Xms128m -Xmx1024m`, then restart the Tomcat service.

For information about stopping and starting Tomcat, see “Starting and Stopping Tomcat” on page 101.

Java Error Messages are Displayed After Closing the Browser of iManager Workstation

After logging out of iManager, when you close the browser, the following java error message is displayed.

```
#

# An unexpected error has been detected by Java Runtime Environment:

#

#  SIGSEGV (0xb) at pc=0x8e4c6944, pid=4106, tid=3085011872

#

# Java VM: Java HotSpot(TM) Server VM (11.3-b02 mixed mode linux-x86)

# Problematic frame:

# C  [libmozjs.so+0x2944]  strftime+0x2944
```

Work around: Ignore the error message and the `hs_err_pid####.log` files because they don't affect the iManager workstation.

iManager and LDAP Use Different Date Ranges

If you create an attribute in iManager using the Time syntax, populate the attribute value, and then search for that value using LDAP, LDAP returns a value different from the value populated by iManager.

iManager and LDAP both natively store date values using the first 31 bits of a 32-bit unsigned integer. However, the two applications interpret the most significant bit (MSB) in the integer differently, with iManager using the MSB to store dates earlier than 1970 and LDAP using the MSB to store dates later than 2038. Therefore, the date range used by iManager is 1903-2038, while the date range used by LDAP is 1970-2106.

Creating Secure SSL LDAP Context Fails While Modifying a Dynamic Group

If you configure eDirectory with a non-default LDAP port, iManager displays the following error message while modifying a dynamic group in the **Dynamic** tab.

```
Creating Secure SSL LDAP Context Failed
```

To troubleshoot this issue, add the IP address of the LDAP server to the LDAP URL in the ldapInterfaces attribute by using the ldapconfig utility or LDAP plug-in of iManager.

iManager Plug-In for eDirectory Fails If The LDAP Server Uses a Certificate Issued By Third Party CA

The iManager Java keystore only has the tree CA certificates by default and does not have any third party CA certificates. Hence various plug-ins such as Groups, NMAS, Password Policy are unable to connect to eDirectory over LDAPS and displays error messages when eDirectory uses a certificate issued by a third party CA.

To troubleshoot this issue, perform the following steps:

- **Linux:**
  1. Import the external CA certificate into the JRE keystore file in the following location: `/opt/novell/jdk1.8.0_66/jre/lib/security/cacerts`

     For more information about importing the external CA certificates, see "Secure LDAP Certificates" on page 125.
  2. Restart the Tomcat service.
- **Windows:**
  1. Import the external CA certificate into the JRE keystore file in the following location: `C:\Program Files\Novell\jre\lib\security\cacerts`

     For more information about importing the external CA certificates, see "Secure LDAP Certificates" on page 125.
  2. Restart the Tomcat service.

iManager Is Vulnerable to Cross-Domain Referer Leakage

When a web browser makes a request for a resource, it typically adds an HTTP header, called the Referer header, indicating the URL of the resource from which the request originated. If the resource being requested resides on a different domain, then the Referer header is still generally included in the cross-domain request. If the originating URL contains any sensitive information within its query string, such as a session token, then this information will be transmitted to the other domain. If the other domain is not fully trusted by the application, then this may lead to a security compromise.

To troubleshoot this issue, perform the following steps:

1. Stop Tomcat.
2. Open the `/var/opt/novell/iManager/nps/WEB-INF/web.xml` file.
3. Under `<description>Novell's Management Console</description>`, add the following:

```
<filter>
  <filter-name>CorsFilter</filter-name>
  <filter-class>org.apache.catalina.filters.CorsFilter</filter-class>
    <init-param>
      <param-name>cors.allowed.origins</param-name>
      <param-value>https://164.99.1.1:8443</param-value>
  </init-param>
      <init-param>
       <param-name>cors.allowed.methods</param-name>
        <param-value>GET,POST,HEAD,DELETE,OPTIONS,PUT</param-value>
        </init-param>
  <init-param>
    <param-name>cors.allowed.headers</param-name>
    <param-value>Content-Type,X-Requested-With,accept,Origin,Access-
Control-Request-Method,Access-Control-Request-Headers</param-value>
  </init-param>
  <init-param>
  <param-name>cors.exposed.headers</param-name>
  <param-value>Access-Control-Allow-Origin</param-value>
  </init-param>
  <init-param>
    <param-name>cors.support.credentials</param-name>
    <param-value>false</param-value>
  </init-param>
  <init-param>
    <param-name>cors.preflight.maxage</param-name>
    <param-value>10</param-value>
  </init-param>
  </filter>
  <filter-mapping>
  <filter-name>CorsFilter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

NOTE: The `param-value` is the value for the allowed URL. In this case, the `param-value` tag contains the iManager server details.

4 Start Tomcat.

Additionally, you can also add custom referrer header in the `web.xml` file for the existing filter class `AntiCsrfServletFilter`. For example, you can add the `init parameters` with `param-name` `referrer-header` as shown in the below sample xml file:

```
<filter>
      <filter-name>iManagerAntiCsrfFilter</filter-name>
        <display-name>iManagerAntiCsrfFilter</display-name>
        <description>Filter to prevent Cross Site Request Forgeries</
description>
      <filter-class>com.novell.emframe.fw.filter.AntiCsrfServletFilter</
filter-class>

<init-param>
                        <param-name>Referrer-Policy</param-name>
                       <param-value>"As per document link referral-policy
can be added here"</param-value>
</init-param>

</filter>
```

For a list of all the custm referrer header, see Referrer-Policy.

iManager Fails to Display the Replica View of a Server

On Windows, if you go to **Partitions and Replicas** > **Replica View** > select a server, iManager, fails to display any information related to the replica view of the selected server.

There is no workaround at this moment.

9 Auditing iManager Events

Use Novell Audit for auditing iManager events. For more information, see the *Novell Audit 2.0 Administration Guide* (http://www.novell.com/documentation/novellaudit20/index.html).

Audit has the following prerequisites:

- ❒ A server (Windows, Linux) in your directory tree with Audit.
- ❒ Novell Audit Platform Agent installed on the iManager server or iManager Workstation desktop and configured to point to the Secure Logging Server.

Audit captures data about the following events:

Table 9-1 *iManager Events*

Event ID	Event Name	Description
150013	Added Authorized User	An authorized user is added to eDirectory
150004	Successful Login	The login to eDirectory from iManager was successful
150009	Successful NPM Install	The NPM install was successful
150001	Startup iManager	Tomcat has started
150011	Failed SSL Connection	An SSL connection to eDirectory has failed
150006	Logout	Logged out of iManager
150012	Changed Configuration	The configuration has changed
150015	Successful NPM Upload	The NPM upload was successful
150006	Failed Login	The login to eDirectory from iManager has failed
150010	Failed NPM Install	The NPM installation has failed
150002	Shutdown iManager	Tomcat has stopped

Enabling Novell Auditing in iManager

To configure Novell Audit, do the following:

1. Install iManager 3.2.
2. Login to iManager and navigate to **Configure** > **iManager Server** > **Configure iManager** and click **Add Authorized Users**.
3. Select **Enable NetIQ Audit**, and select the required iManager events to audit.
4. From the eDirectory 9.2 installation package, install Platform Agent.

NOTE: If your server already has a consumer of `nauditpa.jar`, perform the following steps:

- Do not modify the logevent file (skip step 5).
- Do not change the ownership of the `naudit` folder.
- Add `novlwww` user to the `idvadmin` group and create a `.profile` for `novlwww` user with umask setting of `0002`.

5 Modify the logevent file depending on your platform.

- **Linux:** Perform the following actions:

  1. Edit the following entries in the `/etc/logevent.conf` file:

     ```
     LogHost=IP_Address_of_secure_logging_server
     JLogCacheDir=/var/opt/novell/naudit/jcache
     JLogCachePort=1287
     LogCachePort=1288
     LogJavaClassPath=/var/opt/novell/iManager/nps/WEB-INF/lib/
     NAuditPA.jar
     LogMaxBigData=8192
     LogEnginePort=1289
     LogCacheUnload=no
     LogCacheSecure=no
     LogCacheLimitAction=keep logging
     ```

  2. (Conditional) Manually create the naudit folder in the `/var/opt/novell/` location.

     Change the permission to `novlwww` for the `/var/opt/novell/naudit` folder by running the following command:

     ```
     chown -R novlwww:novlwww naudit/
     ```

- **Windows:** Edit the following entries in the `logevent.cfg` from `C:\Windows` location:

  ```
  LogHost=IP_Address_of_secure_logging_server
  JLogCacheDir=/var/opt/novell/naudit/jcache
  JLogCachePort=1287
  LogCachePort=1288
  LogJavaClassPath=/var/opt/novell/iManager/nps/WEB-INF/lib/
  NAuditPA.jar
  LogMaxBigData=8192
  LogEnginePort=1289
  LogCacheUnload=no
  LogCacheSecure=no
  LogCacheLimitAction=keep logging
  ```

6 Depending on your platform, uncomment the following entries in the `imanager_logging.xml` file:

- **Linux:** Uncomment `<appender-ref ref="NAUDIT_APPENDER"/>` entry.

  The `imanager_logging.xml` file is located in the `/var/opt/novell/iManager/nps/WEB-INF/` directory.

NOTE: The iManager 3.2 SP6 uses a different version of the `imanager_logging.xml` file. If you are on iManager 3.2 SP6, uncomment the following entries:

- The audit log appender `<NauditAppender name="NAUDIT_APPENDER"> </NauditAppender>` entry
- The appender `<AppenderRef ref="NAUDIT_APPENDER" />` entry under both loggers

- **Windows:** Uncomment `<appender-ref ref="NAUDIT_APPENDER"/>` entry.

  The `imanager_logging.xml` file is located in the `C:\Program Files (x86)\Novell\Tomcat\webapps\nps\WEB-INF\`directory.

NOTE: The iManager 3.2 SP6 uses a different version of the `imanager_logging.xml` file. If you are on iManager 3.2 SP6, uncomment the following entries:

- The audit log appender `<NauditAppender name="NAUDIT_APPENDER"> </NauditAppender>` entry
- The appender `<AppenderRef ref="NAUDIT_APPENDER" />` entry under both loggers

NOTE: Perform Step 7 to Step 9 if you are using iManager 3.0 SP3 or above. If you are using any previous version of iManager, skip to Step 10.

7. Create an user certificate for iManager using eDirectory. For more information, see Creating User Certificates in the *NetIQ eDirectory Administration Guide*.
8. Export the certificate to .pfx format. For more information, see Importing a Public Key Certificate into a User Object in the *NetIQ eDirectory Administration Guide*.
9. Extract the private key to `imanipkey.pem` and certificate to `imanicert.pem` files. Copy the generated certificate files (`imanicert.pem` and `imanipkey.pem`) to the respective folders of iManager server.

   For Windows:

   - `c:\windows\imanicert.pem`
   - `c:\windows\imanipkey.pem`

   For Linux:

   - `/etc/imanicert.pem`
   - `/etc/imanipkey.pem`

   Use the following command to extract the Private key and Certificate:

   - To extract private key: `openssl pkcs12 -in imanP12File.pfx -nocerts -out imanipkey.pem -nodes`
   - To extract certificate: `openssl pkcs12 -in imanP12File.pfx -clcerts -nokeys -out imanicert.pem`
10. Restart Tomcat.
11. Verify if the events are logged into the logging server.
    - **Linux:** Stop jcache and restart Tomcat. Generate events and check the logging server.
    - **Windows:** Generate events and check the logging server.

Enabling XDAS Auditing in iManager

XDAS Audit comes with iManager by default. XDAS Audit captures data about the following events:

- Added Authorized User
- Successful Login
- Successful NPM Install
- Startup iManager
- Failed SSL Connection
- Logout
- Changed Configuration
- Successful NPM Upload
- Failed Login
- Failed NPM Install
- Shutdown iManager

To enable XDAS audit for iManager:

1. Log in to iManager.
2. Click **Configure > iManager Server > Configure iManager**.
3. In the Configure iManager page, on the **Security** tab, select **Enable XDAS Audit**.
4. Select the events you want to record, and then click **Save**.

NOTE: The Failed SSL connection XDAS event is logged multiple times because internally several attempts are made to establish an LDAP connection.

Configuring XDAS Audit for iManager

Table 9-2 lists the default location of the `xdasconfig.properties` file in different operating systems. You can customize the file according to your requirements.

Table 9-2 *Location of the XDAS Configuration File*

Operating System	File
Linux	`/var/opt/novell/iManager/nps/WEB-INF/imanager_logging.xml`
Windows	`c:\Program Files\Novell\Tomcat\webapps\nps\WEB-INF\imanager_logging.xml`
Linux and Windows Workstation	`<unzipped workstation folder>\imanager\tomcat\webapps\nps\WEB-INF\imanager_logging.xml`

Table 9-3 lists the XDAS configuration files.

Table 9-3 *XDAS Configuration File*

Options	Name
Syslog Appender	`syslog`
Rolling File Appender	`file_appender`

The following table provides an explanation of each setting in the `imanager_logging.xml` file.

Table 9-4 *Syslog Settings*

Setting	Description
syslogHost	IP address of the host in which the Audit server is running.
syslogProtocol	The protocol that must be used for communication (UDP/TCP/SSL).
syslogSslKeystoreFile	Location of the key store file.(Used only for SSL).
syslogSslKeystorePassword	Password for the keystore file.(Used only for SSL).
Threshold	Specifies the minimum log level allowed in the Syslog appender. Currently, INFO log level is supported.
Facility=USER	Specifies the type of facility. The facility is used to try to classify the message.Currently, USER facility is supported. These values may be specified as upper or lower case characters.
Layout	Layout setting for Syslog appender.

Table 9-5 *File Appender Settings*

Setting	Description
File= ${catalina.home}/logs/imanager.log	The default location of the log file for a File appender
MaxFileSize=10MB	The maximum size, in MBs, of the log file for a File appender. Set this value to the maximum size that the client allows.
MaxBackupIndex=10	Specifies the maximum number of backup files for a File appender. The maximum number of the backup files can be 10. If the value of MaxBackupIndex is set to 0, no backup file will be created.
layout class=org.apache.log4j.PatternLayout	Layout setting for File appender.
ConversionPattern="%t %d %-5p [%c:%M] %m%n”	Layout setting for File appender.
For information about the conversion patters and their descriptions, see logging.apache.org.	

For iManager 3.2 SP5 and previous versions, make the following changes to the `imanager_logging.xml` file:

1. To enable the Syslog appender:

   1a Edit the following entries:

   ```
   <param name="Facility" value="user"/>

   <param name="syslogHost" value=" 192.168.1.5:1468 "/

   <param name="syslogProtocol" value="tcp"/>

   <param name="syslogSslKeystoreFile" value="/root/Desktop/sentinel/
   mykeystore.jks"/>

   param name="syslogSslKeystorePassword" value="novell"/>

   <param name="Threshold" value="INFO"/>
   ```

   1b Log into iManager and change the log events.

2. To enable the File appender:

   2a Edit the following entries:

   ```
   <param name="File" value="${catalina.home}/logs/imanager.log"/>

   <param name="Append" value="true" />

   <param name="MaxFileSize" value="10MB" />

   <param name="MaxBackupIndex" value="10" />
   ```

   You can customize the `File` value in either of the following platforms:

   `Linux: /home/imanager.log`

   `Windows: C:\\<directory>\\imanager.log`

   2b Select the desired event from iManager and save changes.

In iManager 3.2 SP6, the installer creates a new `imanager_logging.xml` file that includes the latest log4j 2.17.1 capabilities. If you are on iManager 3.2 SP6, make the following changes to the logging XML file:

1. To enable XDAS logging in Syslog server,

   1a Locate the `Syslog appender with XDAS JSON Layout` comment and uncomment the following entry:

   ```
     <iManSyslogAppender name="SysLog" facility="user"
   syslogProtocol="tcp"
         syslogHost="##.##.##.##" port="####" syslogSslKeystoreFile="/
   root/Desktop/sentinel/mykeystore.jks"
   syslogSslKeystorePassword="novell" newLine="true">
         <SSL>
              <KeyStore />
                <TrustStore />
          </SSL>
       <PatternLayout>
   ```

```
        <Pattern>%c</Pattern>
    </PatternLayout>
</iManSyslogAppender>
```

NOTE: Uncommenting SSL will allow servers to communicate over a secure connection. Uncomment only if required.

1b Provide the Syslog host server IP address and port number.

2 To enable XDAS appenders, uncomment the `<AppenderRef ref="FILE_APPENDER" />` and `<AppenderRef ref="SysLog" />` entries under both loggers.

3 Save the file and restart Tomcat.

Enabling CEF Auditing in iManager

Common Event Format (CEF) Audit comes with iManager by default. CEF Audit captures data about the following events:

- Added Authorized User
- Successful Login
- Successful NPM Install
- Startup iManager
- Failed SSL Connection
- Logout
- Changed Configuration
- Successful NPM Upload
- Failed Login
- Failed NPM Install
- Shutdown iManager

To enable CEF audit for iManager:

1 Log in to iManager.

2 Click **Configure > iManager Server > Configure iManager**.

3 In the Configure iManager page, on the **Security** tab, select **Enable CEF Audit**.

4 Select the events you want to record, and then click **Save**.

NOTE: The Failed SSL connection CEF event is logged multiple times because internally several attempts are made to establish an LDAP connection.

Configuring CEF Audit for iManager

Table 9-6 lists the default location of the `auditconfig.properties` file in different operating systems. You can customize the file according to your requirements.

Table 9-6 *Location of the CEF Configuration File*

Operating System	File
Linux	`/var/opt/novell/iManager/nps/WEB-INF/imanager_logging.xml`
Windows	`c:\Program Files\Novell\Tomcat\webapps\nps\WEB-INF\imanager_logging.xml`
Linux and Windows Workstation	*<unzipped workstation folder>*`\imanager\tomcat\webapps\nps\WEB-INF\imanager_logging.xml`

Table 9-7 lists the CEF configuration files.

Table 9-7 *CEF Configuration File*

Options	Name
Syslog Appender	`CEFSyslog`
Rolling File Appender	`CEF_FILE_APPENDER`

The following table provides an explanation of each setting in the `imanager_logging.xml` file.

Table 9-8 *CEF Syslog Settings*

Setting	Description
syslogHost	IP address of the host in which the Audit server is running.
syslogProtocol	The protocol that must be used for communication (UDP/TCP/SSL).
syslogSslKeystoreFile	Location of the key store file.(Used only for SSL).
syslogSslKeystorePassword	Password for the keystore file.(Used only for SSL).
Threshold	Specifies the minimum log level allowed in the Syslog appender. Currently, INFO log level is supported.
Facility=USER	Specifies the type of facility. The facility is used to try to classify the message.Currently, USER facility is supported. These values may be specified as upper or lower case characters.
Layout	Layout setting for Syslog appender.

Table 9-9 *CEF File Appender Settings*

Setting	Description
File= ${catalina.home}/logs/imanager_cef.log	The default location of the log file for a File appender
MaxFileSize=10MB	The maximum size, in MBs, of the log file for a File appender. Set this value to the maximum size that the client allows.
MaxBackupIndex=10	Specifies the maximum number of backup files for a File appender. The maximum number of the backup files can be 10. If the value of MaxBackupIndex is set to 0, no backup file will be created.
layout class=org.apache.log4j.PatternLayout	Layout setting for File appender.
ConversionPattern="%d{MMM dd yyyy HH:mm:ss} %m%n”	Layout setting for File appender.
For information about the conversion patterns and their descriptions, see logging.apache.org.	

For iManager 3.2 SP5 and previous versions, make the following changes to the `imanager_logging.xml` file:

1. To enable the CEFSyslog appender:

   1a Edit the following entries:

   ```
   <param name="Facility" value="user"/>

   <param name="syslogHost" value=" 192.168.1.5:1468 "/

   <param name="syslogProtocol" value="tcp"/>

   <param name="syslogSslKeystoreFile" value="/root/Desktop/sentinel/
   mykeystore.jks"/>

   param name="syslogSslKeystorePassword" value="novell"/>

   <param name="Threshold" value="INFO"/>
   ```

   1b Log into iManager and change the log events.

2. To enable the File appender:

   2a Edit the following entries:

   ```
   <param name="File" value="${catalina.home}/logs/imanager.log"/>

   <param name="Append" value="true" />

   <param name="MaxFileSize" value="10MB" />

   <param name="MaxBackupIndex" value="10" />
   ```

   You can customize the `File` value in either of the following platforms:

   ```
   Linux: /home/imanager_cef.log

   Windows: C:\\<directory>\\imanager_cef.log
   ```

   2b Select the desired event from iManager and save changes.

In iManager 3.2 SP6, the installer creates a new `imanager_logging.xml` file that includes the latest log4j 2.17.1 capabilities. If you are on iManager 3.2 SP6, make the following changes to the logging XML file:

1. To enable CEF Rolling forward log, locate the `Rolling file appender` comment and uncomment the following entry:

```
<IManRollingCEFFileAppender name="CEF_FILE_APPENDER"
fileName="${sys:catalina.base}/logs/imanager_cef.log"
filePattern="${sys:catalina.base}/logs/$${date:yyyy-MM}/app-
%d{MM-dd-yyyy}-%i.log.gz"
```

2. To enable CEF Syslog:

   2a Uncomment the following entry:

```
<IManCEFlogAppender name="CEFSyslog" facility="user"
syslogProtocol="tcp"
syslogHost="##.##.##.##" port="####" syslogSslKeystoreFile="/
root/Desktop/sentinel/mykeystore.jks"
syslogSslKeystorePassword="novel"  newLine="true">
```

   2b Provide the Syslog host server IP address and port number.

3. To enable CEF appenders, uncomment the `<AppenderRef ref="CEF_FILE_APPENDER" />` and `<AppenderRef ref="CEFSyslog" />` entries under both loggers.

4. Save the file and restart Tomcat.

Configuring Audit for iManager with Third-Party Certificates

1. Enable NAudit in iManager. For more information, see "Enabling Novell Auditing in iManager" on page 109.

2. Type the following command to create a Logging Application Certificate for auditing iManager events in the Audit Server:

```
audcgen -app:iManagerInst -cert:c:\cacert.pem -pkey:c:\capkey.pem -f -
bits:2048 -serial:12345 -appcert:c:\imanicert.pem -
apppkey:c:\imanipkey.pem
```

3. Copy the generated certificate files (`imanicert.pem` and `imanipkey.pem`) to the respective folders of iManager server.

   For Windows:

   - `c:\windows\imanicert.pem`
   - `c:\windows\imanipkey.pem`

   For Linux:

   - `/etc/imanicert.pem`
   - `/etc/imanipkey.pem`

4. Restart Tomcat.

Configuring Audit for iManager in Strict Mode

1. Create an user certificate for iManager using eDirectory. For more information, see Creating User Certificates in the *NetIQ eDirectory Administration Guide*.
2. Export the certificate to .pfx format. For more information, see Importing a Public Key Certificate into a User Object in the *NetIQ eDirectory Administration Guide*.
3. Extract the private key to `imanipkey.pem` and certificate to `imanicert.pem` files. Copy the generated certificate files (`imanicert.pem` and `imanipkey.pem`) to the respective folders of iManager server.

   For Windows:

   - `c:\windows\imanicert.pem`
   - `c:\windows\imanipkey.pem`

   For Linux:

   - `/etc/imanicert.pem`
   - `/etc/imanipkey.pem`

   Use the following command to extract the Private key and Certificate:

   - To extract private key: `openssl pkcs12 -in imanP12File.pfx -nocerts -out imanipkey.pem -nodes`
   - To extract certificate: `openssl pkcs12 -in imanP12File.pfx -clcerts -nokeys -out imanicert.pem`
4. Copy the CA certificate (`SSCert.pem`) of the eDirectory server from `/var/opt/novell/eDirectory/data` and add it to the Keysotre file of the Audit Connector using the following command:

   ```
   /keytool -importcert -file SSCert.pem -keystore audit_keystore -alias "eDir-CA"
   ```
5. Import the `audit_keystore` file to Audit Connector which is set to Strict Mode in Sentinel server.
6. Configure iManager for auditing and restart Tomcat. For more information, see "Enabling Novell Auditing in iManager" on page 109.

10 Best Practices and Common Questions

This section contains recommendations about the following topics from some of our experts. If you find something that works well for you, please share it at Cool Solutions (http://www.novell.com/coolsolutions).

Backup and Restore Options

There is no automatic backup and restore feature included with iManager. iManager is composed of two parts: the local files on the server and the Role-Based Services objects in eDirectory.

To make a full backup of iManager, make sure you have a valid backup of the RBS collection and all subordinate objects in the tree, either through replica redundancy or with an eDirectory backup solution.

All local iManager files on the file system are stored in the Tomcat directory. As long as you have a backup of the Tomcat directory, all iManager content is preserved. If the Tomcat directory is somehow compromised on the server, shutting down Tomcat and recopying the directory allows you to recover iManager. If you are not using RBS, backing up the Tomcat directory is all that is needed.

Coexistence with previous versions of iManager 2.x and Role-Based Services

You should update your RBS collection to version 2.7. Otherwise, if you use iManager to access a tree that has an RBS collection from a previous version of iManager 2.x, you won't see all of the roles and tasks that should display.

1. In the Configure view, click **Role Based Services** > **RBS Configuration**.
2. Click the link in the **Out-of-Date** column for a module that needs updating.
3. On the Out-Of-Date Modules page, select a module, then click **Update**.

   A message appears that confirms a successful update.

Updated plug-ins are visible in all versions of iManager 2.x.

Collections

It is important to recognize that one configuration is not ideal for all companies. We recommend multiple collections in a tree only if you use a hierarchical structure using geographical or functional organizations with different administrators in each location. Following are the most common situations together with suggestions for managing their respective collections:

- A hierarchical tree organized to reflect a geographical organization

  Create a collection in every geographical location and have one or more iManager servers per location. Login time is faster and tree navigation is simplified. Each geographical administrator manages the collection of a specified location.

- A hierarchical tree that reflects the company's organizational structure

  Create one collection at the same level as the organization and have one or more iManager servers as company size requires. You manage only one collection.

- A flat tree in which all objects are in a unique container

  Create one collection as a sibling of the unique container and have one or more iManager servers as company size requires. You manage only one collection.

Failed Installs

To avoid failed installs, make sure that your operating system is updated to the most current version and that all system requirements are met. For more information, see "Prerequisites and Considerations for Installing iManager" in the *NetIQ iManager Installation Guide*.

To recover from a failed install, assess the problem from the error message generated during installation.

- "Windows" on page 122
- "Linux" on page 123

Windows

1. If the error involves one of these components, check the specified log files for errors:

   NICI: *`installed directory`*`\temp\wcniciu0.log`

   Tomcat: *`tomcat install directory`*`\Apache_Tomcat_InstallLog.log`. For example, `C:\Program Files\Novell\Tomcat\Apache_Tomcat_InstallLog.log`.

2. Check the iManager install log file (`C:\Program Files\Novell\Tomcat\webapps\nps\WEB-INF\logs\install\iManager_Install_3.2.0_InstallLog.log`) for any errors.

3. If the log file does not give sufficient information to identify the problem, re-run the install in debug mode.

To view or capture the debug output from an installer, open and copy the console output to a text file for later review.

3a Immediately after launching the installer, hold down the Ctrl key until a console window appears.

3b After the install has completed, click the icon in the upper left corner of the console window and select **Properties** > **Layout**.

3c Change the buffer size to 3000, then click **OK**.

3d In the Layout window, select **Edit** > **Select All** > **Edit** > **Copy**.

3e Open a text editor and paste the output of the debug in it.

4 Identify and correct any errors or stack traces, then rerun the install.

Linux

1 Check the iManager install log file (`/var/log/NetIQ_iManager_3.2.0_InstallLog.log`) for any errors.

2 If the log file does not give sufficient information to identify the problem, re-run the install in debug mode.

At the command line, type the following:

```
export LAX_DEBUG=true
```

3 Identify and correct any errors or stack traces, then re-run the install.

Performance Tuning

The following are tips for enhancing speed and efficiency.

Disabling Dynamic Group Support for RBS

Disable Dynamic Group support for RBS if you are not using this feature. By default, Dynamic Group support is enabled and, when used, significantly taxes resources because of the extensive searches it conducts.

1 In the Configure view, click **iManager Server** > **Configure iManager**.

2 Select the **RBS** tab, then de-select **Enable Dynamic Groups**.

Role Assignments

If you have assigned more than five users to a role within the same scope, consider using Group objects to reduce the number of role assignments and make RBS administration more efficient. By doing so, you have fewer objects to update and you can manage the Group object by adding and removing members.

Also, consider using Dynamic Group objects. You can set up User objects to match a Dynamic Group search criteria.

Configuring Referral Costing Manually

If a server-based instance of iManager does not hold the entire tree, it will connect to other servers at random to resolve objects that it does not have. For example, when resolving the root of the tree, iManager resolves to replica holders in remote locations rather than a local replica. This can cause long login delays in a large tree. Because iManager uses JClient application, neither Advanced Referral Costing (ARC) nor the `hosts.nds` file have any effect on its resolving behavior.

To address this issue, the iManager lets you manually configure the costing of remote servers to which it may connect. This feature is available in iManager 2.7 SP4 Patch 4 and later, as well eDirectory 8.8 SP6 Patch 5 and later (requires both). For more information about the steps for manually configuring costing referrals to other servers, see TID# 7000773 (https://support.microfocus.com/kb/doc.php?id=7000773).

iManager AppArmor Profile

Novell Open Enterprise Server —Linux includes an AppArmor profile for iManager. The profile name is `etc.opt.novell.tomcat5.init.d.tomcat5` and is installed at `/etc/apparmor/profiles/extras/iManager`.

The iManager AppArmor profile is not enabled by default. To enable it, copy the profile into the `/etc/apparmor.d` folder.

For more information about AppArmor and AppArmor profiles, see the Novell AppArmor documentation (http://www.novell.com/documentation/apparmor/).

Allocating Additional Tomcat Memory in Windows

1. Go to Tomcat/bin folder (For example, `c:\Program Files\Novell\Tomcat\bin`)
2. Right-click on `tomcat9w.exe` file.
3. Open **Tomcat9 Properties** window.
4. Click **Java** tab.
5. Specify the Initial & Maximum memory pool sizes.

   IMPORTANT: Ensure that the Initial & Maximum memory pool sizes that you specify is less than your physical RAM's size, otherwise it may cause more performance issues.

6. Click **Apply**, then click **Ok**.
7. Restart Tomcat Service.

   TIP: To verify the new settings, go to the URL of Tomcat server and click **Server Status**.

A iManager Security Issues

This section provides information about potential security issues related to iManager, and includes information about the following topics:

Secure LDAP Certificates

iManager can create secure LDAP connections behind the scenes without any user intervention. If the LDAP server's SSL certificate is updated for any reason (for example, new Organizational CA), iManager should automatically retrieve the new certificate using the authenticated connection and import it into its own keystore database.

If this does not happen correctly, you must delete the private key store that iManager uses, in order to force iManager and Tomcat to re-create the database and re-acquire the certificate:

1. Shut down Tomcat.
2. Delete the *TOMCAT_HOME*\webapps\nps\WEB-INF\iMKS file.
3. Restart Tomcat.

   For information about restarting Tomcat, see "Starting and Stopping Tomcat" on page 101.
4. Open iManager in a browser and log back in to the tree, to automatically re-acquire the new certificate and re-create the database store.

Alternately, you can also manually import the required certificate into Tomcat's JVM default keystore using the keytool certificate management utility available in the JDK. When creating secure SSL connections, iManager first tries the JVM default keystore, then uses the iManager specific keystore database.

After you have an eDirectory certificate saved in DER format, you must import the trusted root certificate into the iManager keystore. To do this, you need a JDK to use keytool. If a JRE was installed with iManager, you must download a JDK to use the keytool.

NOTE: For information about creating a `.der` certificate file, see "Exporting a Trusted Root or Public Key Certificate". You will want to export the trusted root certificate.

1. Open a command window.
2. Change to the `\bin` directory where you have installed the JDK.
3. Import the certificate into the keystore with the keytool, executing the following keytool commands (platform specific):

   - Linux

     ```
     keytool -import -alias [alias_name] -file [full_path]/
     trustedrootcert.der -keystore [full_path]/jre/lib/security/cacerts
     ```

   - Windows

     ```
     keytool -import -alias [alias_name] -file
     [full_path]\trustedrootcert.der -keystore
     [full_path]\jre\lib\security\cacerts
     ```

   Replace *alias_name* with a unique name for this certificate and make sure you include the full path to `trustedrootcert.der` and `cacerts`.

   The last path in the command specifies the keystore location. This varies from system to system because it is based on where iManager is installed. The following are the examples of default locations for iManager on Windows and Linux:

   On Windows: `C:\Program Files\Novell\jre\lib\security\cacerts`

   On Linux: `/<JAVA_HOME>/jre/lib/security/cacerts`
4. Enter `changeit` for the keystore password.
5. Click **Yes** to trust this certificate.

NOTE: This process must be repeated for each eDirectory tree you will be accessing with iManager. If LDAP has been configured to use a certificate not signed by the tree's Organizational CA, you must import that certificate's Trusted Root. This is necessary, for example, if LDAP is configured to use a VeriSign*-signed certificate.

Self-Signed Certificates

iManager includes a temporary, self-signed certificate that you use when installing iManager on Linux or Windows platform. It has an expiration date of one year. For more information, see "Prerequisites and Considerations for Installing iManager" in the *NetIQ iManager Installation Guide*.

iManager Authorized Users and Groups

Authorized Users and Groups are those that iManager permits to perform its various administrative tasks. For more information about specifying and configuring Authorized Users and Groups, see "Authorized Users and Groups" on page 75.

Authorized Users and Groups data is stored in the `configiman.properties` file, which must be secured to prevent unauthorized modification. To do this, modify the access controls for `configiman.properties` to restrict those users authorized to manually edit the file.

NOTE: Not specifying an Authorized User or Group, which prevents the `configiman.properties` file from being created, or specifying an Authorized User or Group of `AllUsers`, allows any user to install iManager plug-ins and modify iManager server settings. This is a security risk for server-based iManager environments.

Preventing User Name Discovery

In some installations, the eDirectory server is protected behind a firewall, but the iManager server is open to the outside world to allow management from home or on the road. Access to iManager is controlled with **Username**, **Password**, and **Treename** fields on the login screen. In such installations, it is often desirable to tighten security to avoid revealing any information about the system.

Standard iManager configurations pass through eDirectory messages related to invalid user names and passwords during iManager authentication. These messages can inadvertently provide too much information to potential crackers. To avoid this, iManager includes a configuration option to hide the specific reason for login failure. When enabled, the following error messages are replaced with a generic error message that reads: `Login Failure. Invalid Username or Password`.

- Invalid Username (-601)
- Incorrect password (-669)
- Expired password or disabled account (-220)

To enable this setting, open the **Configure** view and select **iManager Server** > **Configure iManager**. On the **Authentication** tab, select **Hide specific reason for login failure**. This sets `Authenticate.Form.HideLoginFailReason=true` in iManager's `config.xml` file.

Additionally, iManager does not support the asterisk (*) character as a wildcard in the **Username** field. This prevents unauthorized users from discovering valid user names. It also prevents possible denial-of-service attacks that attempt to overload the eDirectory server by continually attempting a login using only the wildcard (*), which forces eDirectory to search for and return all matching user names.

Tomcat Settings

Because iManager makes use of Tomcat Servlet Container, iManager administrators should be aware of the encryption-related configuration options of those resources as part of their overall security strategy. Of particular interest are cipher suites and trusted certificates, which directly impact the quality of your wire-level encryption. Consider the following rules when configuring your Tomcat environment:

- Do not use SSL 2.0 cipher suites, which are outdated and not guaranteed to be secure.
- Do not use the NULL cipher suite in a production environment.
- Do not use any cipher suite classified as LOW or EXPORT quality, because these are less secure.
- Regularly review the list of trusted certificates, and limit the list of accepted Certificate Authorities to only those you are actually using

More information for Tomcat is available at the Apache Tomcat Documentation Web site (http://tomcat.apache.org/tomcat-9.0-doc/).

Encrypted Attributes

iManager is able to securely read eDirectory encrypted attributes. However, because of the way it determines if an attribute is encrypted, iManager does not securely modify or delete these encrypted attributes. The impact of this, which can result in some wire-level data exposure, can be mitigated through normal network security practices such as the following:

- Locating all iManager servers behind the firewall
- Locating iManager servers physically near their associated eDirectory servers
- Physically securing iManager and eDirectory servers
- Requiring remote administrators to use a VPN to access iManager and eDirectory servers

Secure Connections

Although iManager leverages secure HTTP (SSL) for client communications, and secure LDAP connections between iManager and eDirectory servers, iManager does not, with the exception of reading encrypted attributes, utilize secure NCP connections for communications between iManager servers and eDirectory servers.

This is also true for the NCP connection used by Mobile iManager. The impact of this, which can result in some wire-level data exposure, can be mitigated through normal network security practices such as the following:

- Locating all iManager servers behind the firewall
- Locating iManager servers physically near their associated eDirectory servers
- Physically securing iManager and eDirectory servers
- Requiring remote administrators to use a VPN to access iManager and eDirectory servers

NOTE: Regardless of the wire-level encryption being used, passwords are always encrypted and protected as part of the iManager authentication process.

B NetIQ Plug-in Modules

iManager ships with the following roles as part of the `base.npm` plug-in. Additional plug-in modules must be downloaded separately.

- Directory Administration
- Partitions and Replicas
- Help Desk
- Schema
- Rights
- Users
- Groups

The best place to locate and download iManager plug-ins is within iManager on the **Available NetIQ Plug-in Module** page. Alternately, you can download plug-ins from the NetIQ download site (https://dl.netiq.com/index.jsp). Select iManager as the product in the search criteria.

Additionally, NetIQ occasionally releases iManager plug-in updates. These updates are available on the NetIQ iManager Plug-ins download site (https://www.netiq.com/support/imanager/plugins/).

iManager base plug-ins are only available as part of the complete iManager software download. Unless there are specific updates to these plug-ins, they can only be downloaded and installed with the entire iManager product.

For more information about downloading iManager plug-ins, see "Understanding Installation for iManager Plug-ins" in the *NetIQ iManager Installation Guide*.

NOTE: By default, the plug-in modules are not replicated between iManager servers. NetIQ recommends that you install the plug-in modules you want on each iManager server.
