4

Managing the Network Systems

ENlighten/DSM provides powerful tools for managing systems on your network.

This chapter contains basic information about how to manage systems on your network using the following ENlighten/DSM program features:

- Locking and unlocking user accounts
- Building disk snapshots, viewing usage, file searching, and displaying currently running processes
- Managing Network Filesystems (NFS) for clients and servers
- Managing cron jobs

- Configuring archive devices, backing up files, restoring files, and scheduling backups
- Configuring and managing Network Information Servers (NIS) on a network

For information about other management tasks not covered in this chapter, refer to the *ENlighten/DSM Reference Manual*.

Managing a User's System Access

You can deny a specific user access to the system without deleting the account through the ENlighten/DSM user module. ENlighten/DSM also provides tools to check files, passwords, and other network functions. Refer to the *ENlighten/DSM Reference Manual* and Chapter 5, "Monitoring Your Network Systems," for information about those security features.

To lock user access,

1) Choose Configure from the User menu. The User Configuration window appears.

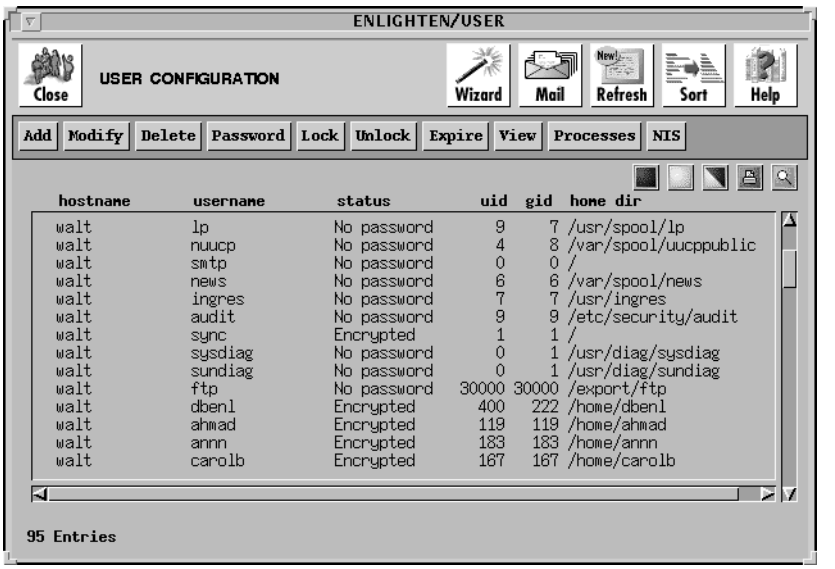

Figure 4-1 User Configuration window

2) Select the user whose access you want to deny.

3) Click the Lock button. A pop-up window will prompt you to confirm this action.

You must assign a new password to unlock a user, or the existing password will be lost!

To unlock a user account,

1) Highlight the user for whom you want to resume access privileges from the User Configuration window.

2) Click the Unlock button.

Because locking and unlocking user accounts is considered part of system security, you are prompted for a new password when ENlighten/DSM unlocks a User Account.

Managing Disk Partitions

ENlighten/DSM provides you with tools to easily and efficiently manage your network's disk space. You can get disk filesystem information summaries for users, groups, and disk filesystems, and perform specific file searches. To decrease the time required to generate these summaries, ENlighten/DSM creates a database, or *snapshot*, of the files in the requested filesystem and then uses this database to perform the required tasks.

This section briefly describes how to view usage by filesystem, username, and groupname; build snapshots; perform file searches; and display processes. For more detailed information about these options, refer to Chapter 5, "Disk," in the *ENlighten/DSM Reference Manual*.

Viewing Usage by Filesystem

To view disk usage by filesystems,

1) Choose Usage by Filesystem from the Disk menu. The Usage by Filesystem window appears.

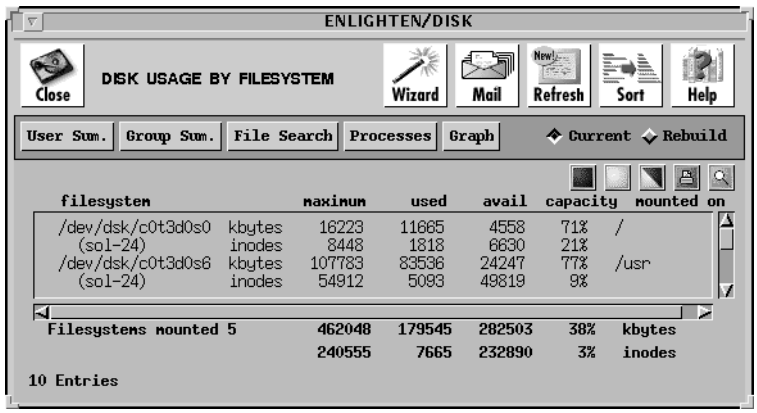

Figure 4-2 Usage by Filesystem window

2) Highlight the filesystem(s) that you want to summarize and then you can:

- Click the User Sum. button for a summary of disk usage by username.
- Click the Group Sum. button for a summary of disk usage by user group.
- Click the File Search button to search files based on a search criterion.
- Click the Processes button to view the processes using a filesystem.
- Click the Graph button to graph disk usage.

Viewing Disk Usage by User Name

To view at a glance a summary of disk usage by user for currently mounted filesystems,

1) Choose Usage by Username from the Disk menu. The Select Disk Partitions window appears.

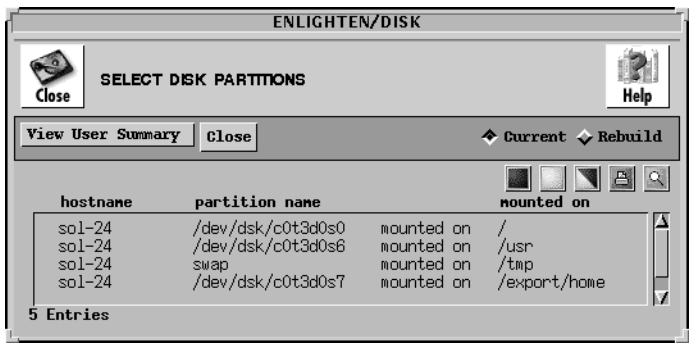

Figure 4-3 Select Disk Partitions window

2) Highlight the disk partition that you want a summary of.

3) Click the View User Summary button. The Disk Usage Information by Users window appears.

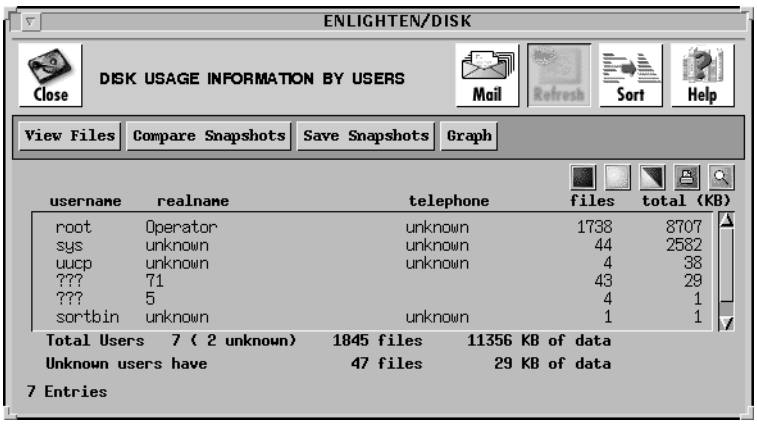

Figure 4-4 Disk Usage Information by Users window

4) Highlight the user names you want a summary of, then

- Click the View Files button to view a list of files owned by the user(s) and perform further operations on them.
- Click the Compare Snapshots button to compare the current snapshot to a previously saved one.
- Click the Save Snapshots button to save the current snapshot.
- Click the Graph button to graph the disk usage summary of the user(s).

Viewing Disk Usage by Group Name

To view at a glance a summary of disk usage by user group for currently mounted filesystems,

1) Choose Usage by Groupname from the Disk menu. The Select Disk Partitions window appears.

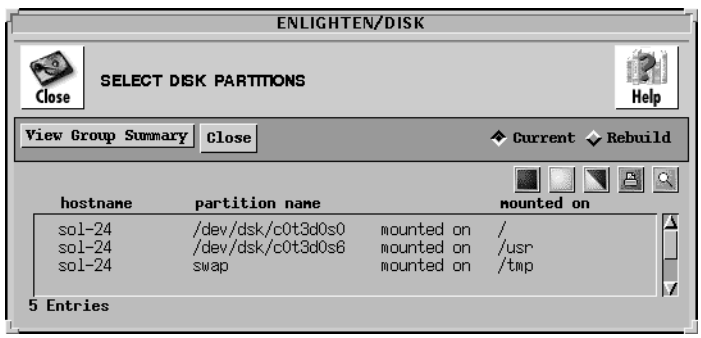

Figure 4-5 Select Disk Partitions window

2) Highlight the disk partitions that you want to view from the list and then click the View Group Summary button. The Disk Usage Information by Groups window appears.

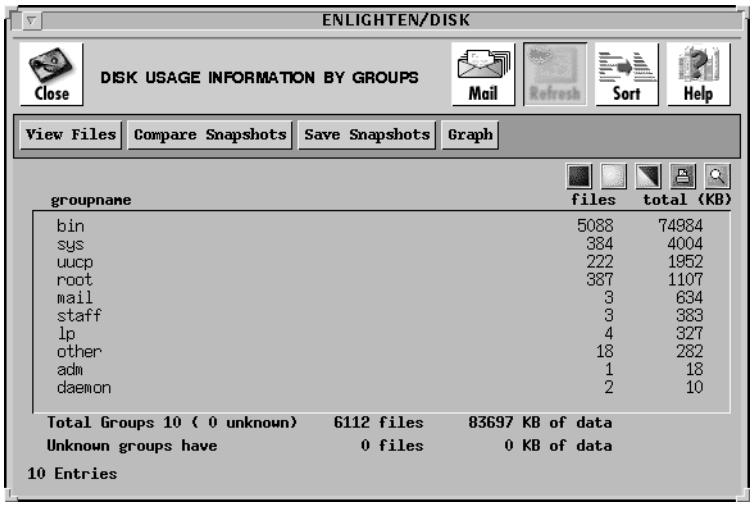

Figure 4-6 Disk Usage Information by Groups window

3) Highlight the group name entries you want and then:

- Click the View Files button to view a list of files owned by the group(s) and perform further operations on them.
- Click the Compare Snapshots button to compare the current snapshot to a previously saved one.
- Click the Save Snapshots button to save the current snapshot. See the next section, "Building Snapshots," for more information.
- Click the Graph button to graph the disk usage of the group(s).

Building Snapshots

Disk snapshots provide a detailed description of a disk partition at a given moment that you can use to monitor disk usage and determine if changes have been made to a partition from time to time. You can save and store these snapshots, and update them with the rebuild function.

Master snapshots are not automatically created during installation, so you must first create a snapshot and save it as a master that you can compare with later snapshots.

Creating a Master Snapshot

You can store a snapshot as a master snapshot that represents a secure system state. You usually create a master snapshot after installing the software and before giving users access to partitions, or after a system cleanup to track changes made over time. You can assign a meaningful name to a snapshot to represent interim states.

To save a current snapshot,

1) Choose Save Current Snapshots from the Disk menu. The Select Disk Partitions window appears.

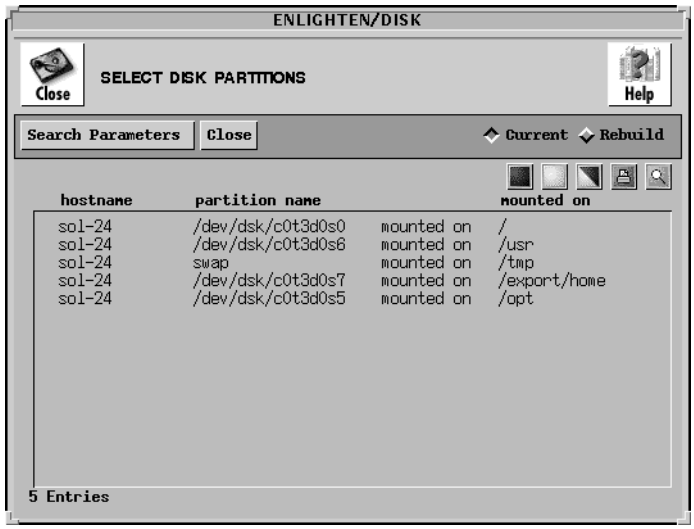

Figure 4-7 Select Disk Partitions window

2) Highlight the disk partitions for which you want to make a snapshot from the list of currently mounted filesystems.

3) Click the Save Snapshot button. The Save Selected Disk Snapshots window appears. The names of the selected partitions are imported into the Snapshot from Partition column. You can add other partition names or modify existing ones.

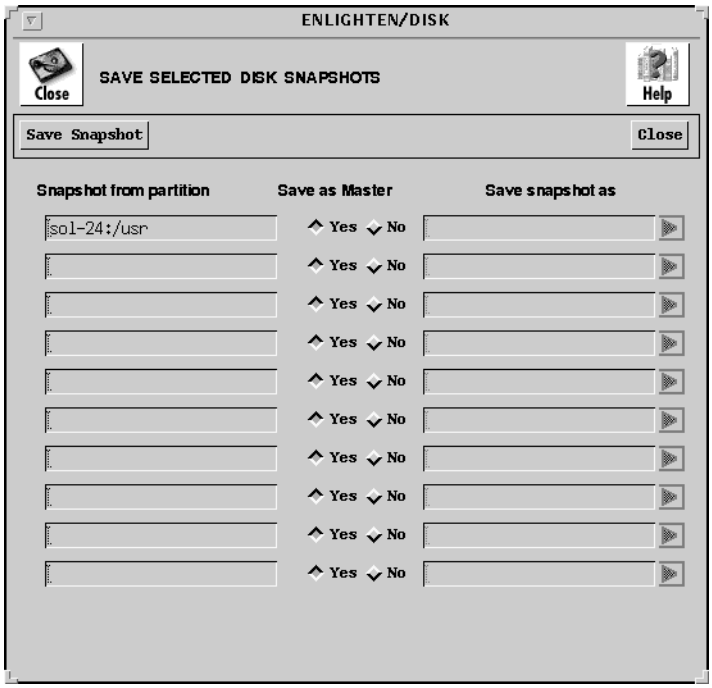

Figure 4-8 Save Selected Disk Snapshots window

4) For each partition,

- To assign the snapshot a unique name, click the No button and then enter the new name in the Save Snapshot As field.
- To save the snapshot as the Master, leave the Yes button enabled.

5) Click the Save Snapshot button when you are finished.

Comparing Snapshots

To create a new snapshot and then compare it with the master snapshot,

1) Choose one of the Disk Usage commands:

   - Disk—>Usage by Filesystem
   - Disk—>Usage by Username
   - Disk—>Usage by Groupname

2) Highlight the disk partitions (filesystems) for which you would like to perform a comparison.

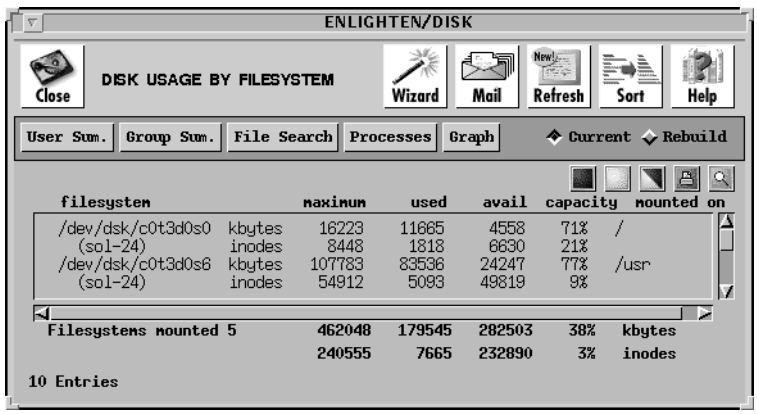

Figure 4-9 Currently Mounted Filesystems

3) Click the Rebuild radio button in the upper right part of the window, and then click one of the functional buttons; for example, the User Sum. button.

   A new snapshot of the current filesystem is created that you can use to compare with the master or interim snapshots.

4) Click the Compare Snapshot button. The Select Saved Snapshots window appears. You can look at a summary of the changes, view a detailed list of the changes, or search for changes based on a query process.

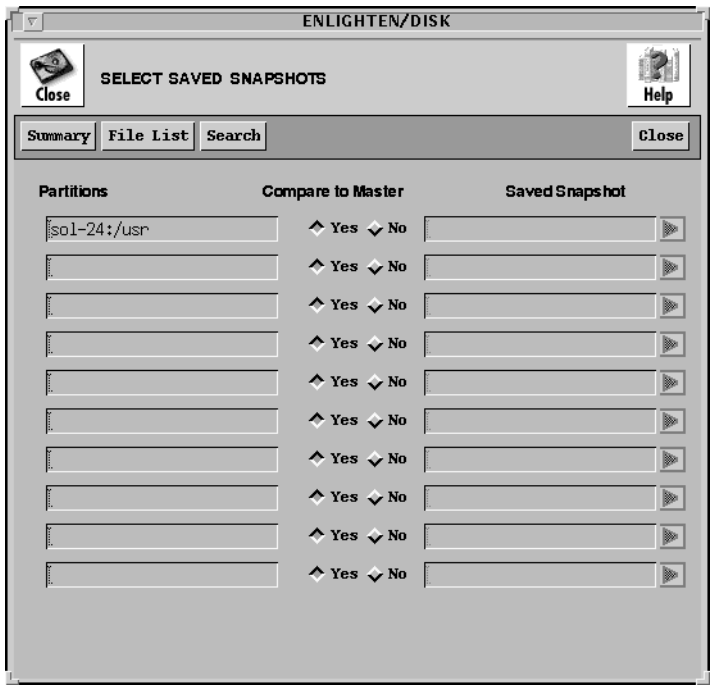

Figure 4-10 Select Saved Snapshots window

5) To compare against a named snapshot, click the No button under the Compare to Master column. Then, enter the name of the previously saved snapshot in the appropriate Saved Snapshot field.

Partitions of the same name, but from different systems, can be compared. For example, the / partition from the host `athens` can be compared to the / partition from the host `paris`. You can use this to help maintain consistency of static partitions (partitions that do not change) across hosts.

6) Choose how you want to compare the snapshots by selecting one of the following options:

   - Click the Summary button to get a summary of the changes.
   - Click the File List button to get a list of all the changes.
   - Click the Search button to search further for certain types of changes.

Updating

From the Disk Usage by Filesystem and Select Disk Partitions windows, you can update the snapshot of a selected filesystem. When you do this, it replaces the old disk partition information with current information.

To update the snapshot of a filesystem,

1) Highlight it in the list of filesystems and click the Rebuild button.

2) Click one of the buttons: User Sum. or Group Sum.

   ENlighten/DSM displays a window indicating when the last request was taken.

3) Click the Save Snapshot button to save the snapshot as the new master, or save it and name it as an interim snapshot for future reference.

Because disk summaries and searches are performed on this snapshot, you should rebuild your snapshots periodically to reflect a more current state of the disk. This can be done with the cli and cron commands.

Managing Network File Systems (NFS)

ENlighten/DSM provides you with tools to mount or unmount filesystems on any host or make server directories available for export by a host. Mounting NFS partitions attaches a named resource to the filesystem hierarchy at the pathname location mount point, which already exists.

This section explains how to mount and export directories, or *partitions*. For more information about NFS options not explained here, refer to Chapter 5, "Disk," in the *ENlighten/DSM Reference Manual*.

Mounting Directories on Hosts

You can mount partitions on the host(s) immediately, when the hosts are booted, or both.

To add an NFS partition on one or more hosts,

1) Choose NFS from the Disk menu and then Mounted Directories. The Network Filesystem Configuration window appears, displaying the mounted filesystems on all hosts in the current pool.

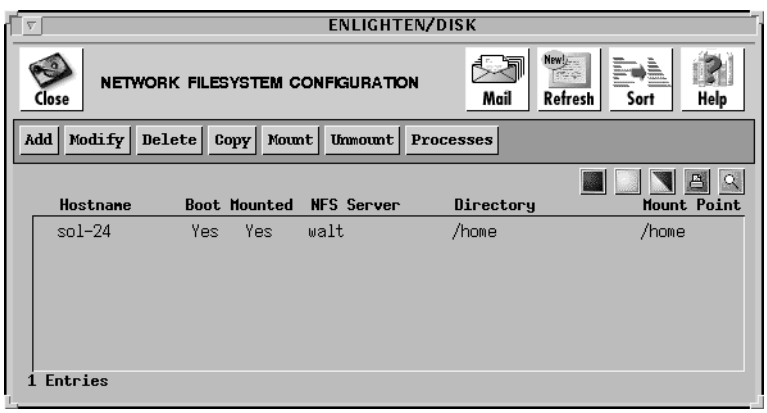

Figure 4-11 Network Filesystem Configuration window

Each line in the list box displays the hostname, whether the filesystem is currently mounted and/or automatically mounted at boot time, the NFS Server name, the remote partition (directory) name, and the local mount point name.

2) Click the Add button. The Add an NFS Partition window appears.

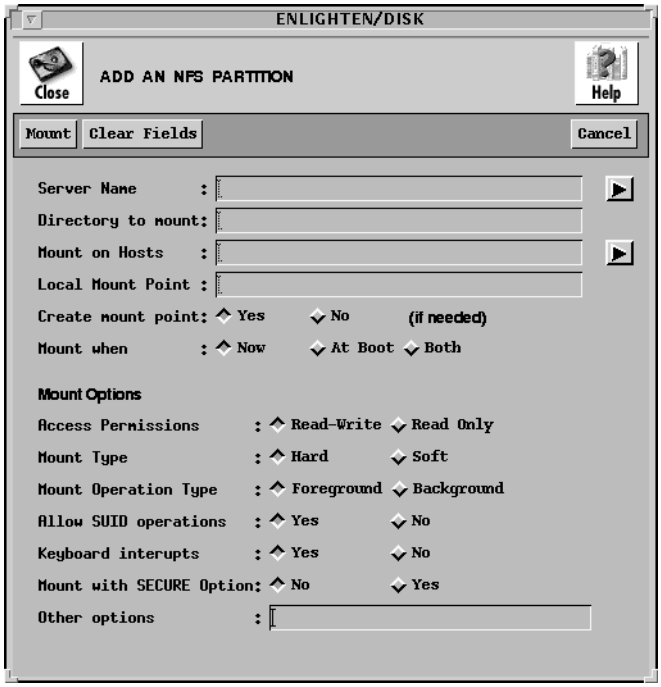

Figure 4-12 Add an NFS Partition window

3) Enter the server and directory information in the fields and select the mount options you want. For information about all of the options in the window, refer to the next section, "Add and Modify NFS Partition Options," on page 4-18.

4) Click the Mount button to initiate the mount you defined.

To modify the mount parameters for an existing configuration,

1) Choose NFS from the Disk menu and then Mounted Directories. The Mounted Filesystems on Host window appears, displaying the mounted filesystems on all hosts in the current pool (see Figure 4-11).

2) Highlight the NFS partition(s) you want to modify.

3) Click the Modify button. The Modify an NFS Partition window appears.

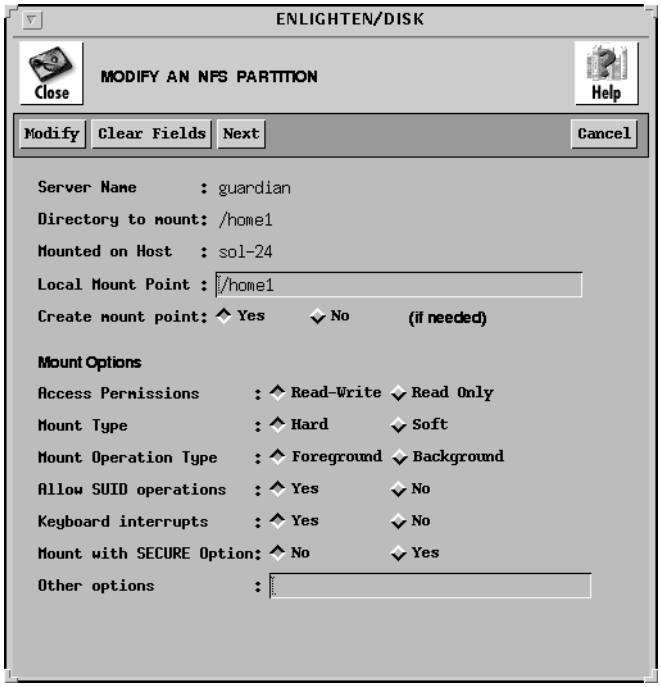

Figure 4-13 Modify an NFS Partition window

4) Change the options that you want. A description of each option is listed in the next section, "Add and Modify NFS Partition Options."

5) Click the Modify button to save the changes you have made to the selected partition.

6) If you selected more than one partition to change, click the Next button to modify the next NFS partition that you selected from the list.

Add and Modify NFS Partition Options

The Add an NFS Partition and Modify an NFS Partition windows are similar except the Modify an NFS Partition window does not allow you to modify the Server Name, Directory to Mount, or Mounted on Host fields. Each field or option in these windows is listed and described in the following sections.

Server Name field

Use this field to specify the NFS server from which the partition will be mounted. You can also click the arrow button to the right to pop up a pick list of all hosts within the current pool that may have partitions you can mount.

Directory to Mount field

Use this field to specify the remote directory to mount. Leave a blank space between directory names for multiple entries.

Mount on Hosts field

Use this field to specify the hosts where the directory will be mounted. Leave a blank space between hostnames for multiple entries. You can also click the arrow button to the right to pop up a pick list of all hosts within the current pool that may mount the partition specified and make your selection(s) from there.

Local Mount Point field

Use this field to specify the directory name where the exported partition will be mounted.

Create Mount Point option

Use this option to specify if the local mount point directory should be created during a mount if that directory does not already exist. The default setting is Yes.

Access Permissions option

Use this option to specify how the remote partition should be mounted: Read-Write (the default) or Read Only.

Mount Type option

Use this option to specify if the mount should be a Hard (the default) or a Soft mount. Filesystems that are mounted read-write or that contain executable files should be mounted with the Hard setting. Applications using soft-mounted filesystems may produce unexpected I/O errors. Soft-mounted filesystems return errors on request; hard-mounted filesystems display a warning message and continue to try the request.

Mount Operation Type option

Use this option to specify whether the mount should be performed in Foreground (the default) or Background. Filesystems mounted with the Background setting specify that the mount is to retry in the background if the server's mount daemon does not respond.

Allow SUID operations option

Use this option to specify if setuid execution is allowed for this mount. The No setting causes the filesystem to be mounted but silently ignores the request to set the suid bit. The default setting is Yes.

Keyboard Interrupts option

Use this option to specify if keyboard interrupts are allowed to kill a process that is hung while waiting for a response on a hard-mounted filesystem. The default setting is Yes.

Mount with Secure option

Use this option to specify whether to mount with the authentication at RPC option. The default setting is No.

Other Options field

You can use this field to specify other NFS options. This field is not pre-checked for syntax errors.

Mounting and Unmounting NFS Partitions

To mount or unmount NFS partitions immediately, highlight the partition(s) you want to mount or unmount in the Network Filesystem Configuration window (see Figure 4-11) and then click the Mount or Unmount button.

Exporting Directories

This section describes how to re-export a directory, define new export criteria, export a directory, and modify export parameters for an existing NFS partition and export it.

To export a directory,

1) Choose NFS from the Disk menu and then Exported Directories. The Export a Directory window appears displaying all of the currently exportable directories.

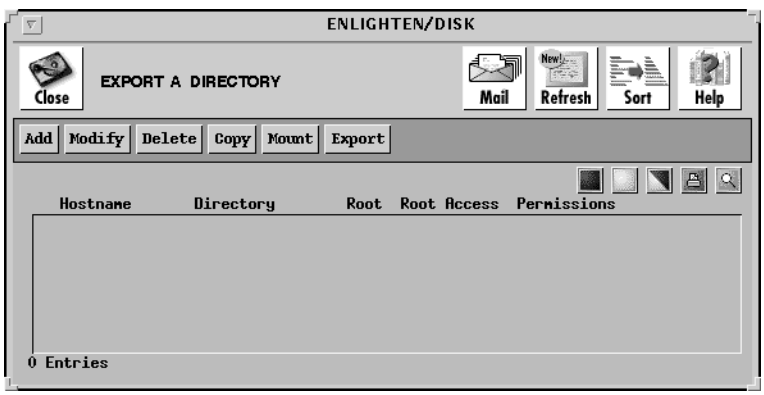

Figure 4-14 Export a Directory window

Each line in the list displays the hostname, exported partition, number of hosts with root access, root access, and permissions.

2) Select the directory you want to export.

3) Click the Export button.

To define new export criteria for a directory,

1) Choose NFS from the Disk menu and then Exported Directories. The Export a Directory window appears displaying all of the currently exportable directories.

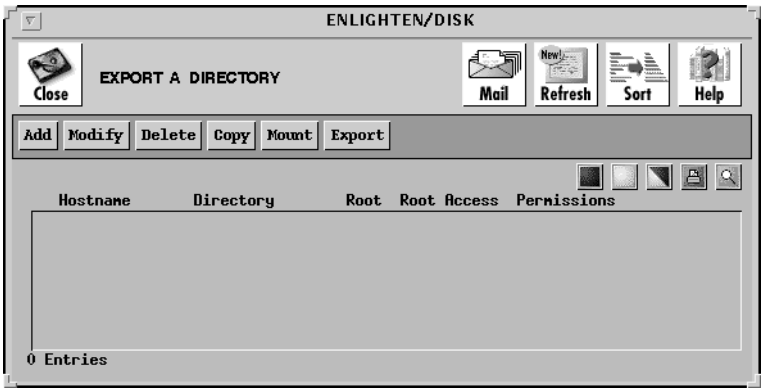

Figure 4-15 Export a Directory window

2) Click the Add button. The NFS: Export a Filesystem window appears.

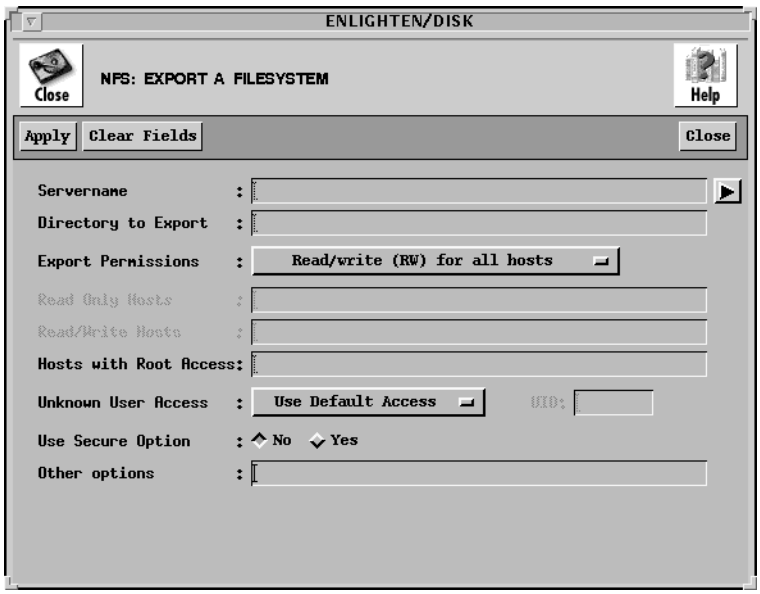

Figure 4-16 NFS: Export a Filesystem window

3) Modify the export parameters you want to use. Refer to the next section, "Add and Modify Export Fields," for information about each one of the parameters.

4) Click Apply to export the directory.

To modify the export parameters for an existing NFS partition,

1) Choose NFS from the Disk menu and then Exported Directories. A window appears displaying the exportable directories on all hosts in the current pool.

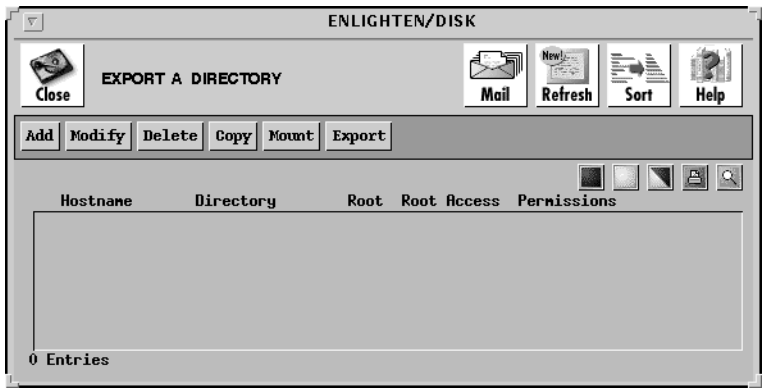

Figure 4-17 Export a Directory window

Each line in the list will display the hostname, exported partition, number of hosts exported to, root access, and permissions.

The Modify an Exported Filesystem window is similar to the Export a Filesystem window, except you cannot modify the Servername or Directory to Export fields.

2) Highlight one or more partitions that you want to modify and then click the Modify button. The Modify an Exported Filesystem window appears.

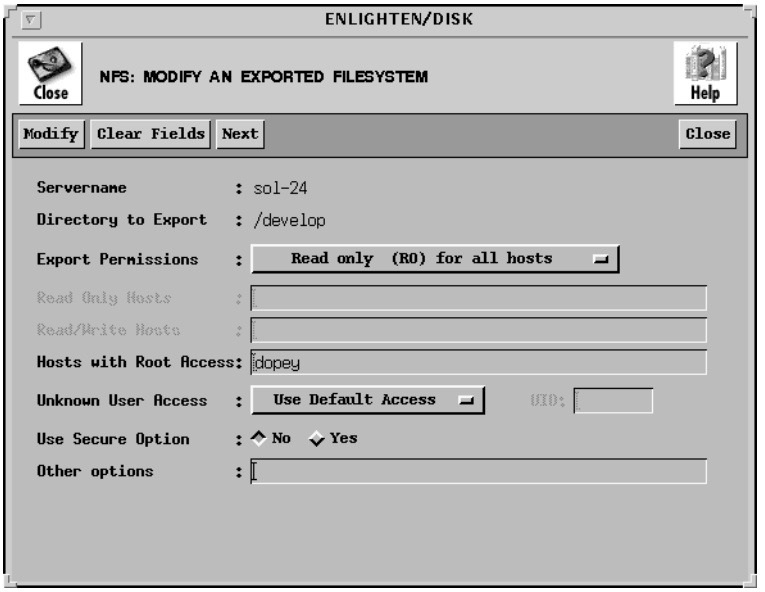

Figure 4-18 Modify an Exported Filesystem window

3) Change the parameters you want. Refer to the next section, "Add and Modify Export Fields," for information about each parameter.

4) Click the Modify button to save the changes you made.

5) If you selected more than one partition in the Network File Configuration window, click the Next button to display the parameters of the next selected partition.

Add and Modify Export Fields

Server Name field

Use this field to specify the NFS server from which the partition will be exported. You can also click the arrow button to the right to pop up a pick list of all hosts within the current pool.

Directory to Export field

Use this field to specify the full pathname for the directory to export. Leave a blank space between directory names for multiple entries.

Export Permissions option

Use these toggles to specify what access permissions the client machines will have to the directory. The options are:

- Read/write (RW) for all hosts (the default)
- Read only (RO) for all hosts
- RW for specific hosts and RO for rest
- Read/write for specific hosts
- Read only for specific hosts

Read Only Hosts field

This field is active only if you selected the Read Only for Specific Hosts option in the Export Permissions field. Use this field to specify the read only hosts. Leave a blank space between hostnames for multiple entries.

Read/Write Hosts field

This field is active only if you selected the RW for Specific Hosts and RO for Rest or Read/Write for Specific Hosts options in the Export Permissions field. Use this field to specify the read/write hosts. Leave a blank space between hostnames for multiple entries.

Hosts with Root Access field

Use this field to specify which hosts have root equivalency permissions on this partition. Leave a blank space between hostnames for multiple entries.

Unknown User Access option

Use these toggles to determine how unknown user (UID) access should be handled. This will also determine how any root access (other than those hosts specified in the previous Hosts with Root Access field) should be handled. The options are:

- Use Default Access (the default). If the default is unknown, it puts UID_NOBODY in the file.
- Disable Unknown Access. –1 access is denied.
- Select own UID. Only the specified UID has access.

UID field

This field is active only if you selected the Select Own UID option in the Unknown User Access field. Use this field to enter a UID to which unknown users will be mapped.

Use Secure Option

Use this toggle to specify if the filesystem should be exported with the Secure option. The default setting is No.

This does not work on all systems (for example, SCO and HP-UX). Both the server and the client must be configured to be “secure” for this to work properly.

Other Options field

You can use this field to specify other NFS options. This field is not pre-checked for syntax errors.

Managing Cron Jobs

This section describes how to manage crontab entries on multiple heterogeneous hosts. The Cron Management options in the System menu allow you to configure cron jobs, perform a query on all cron jobs, or manage user access to crontab.

Configuring Cron Jobs

The Crontab Configuration window (Figure 4-19) displays current cron jobs for all users on all hosts in the current pool and allows you to:

- Create a new crontab job.
- Modify an existing crontab entry.
- Delete selected crontab jobs.
- Create another cron job using the settings of an existing cron job (copy).

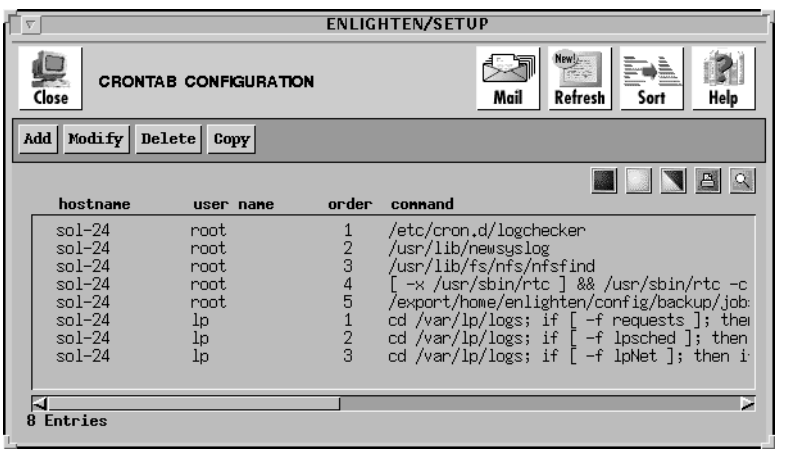

Figure 4-19 Crontab Configuration window

Adding New Crontab Jobs

This feature is system dependent; you may not be able to use all combinations of time settings on your system. Check your local cron for its precise workings.

To create a new crontab job,

1) Choose Cron Management from the System menu and then choose Configure.

2) Click the Add button in the Crontab Configuration window. The Add Crontab Entry window appears (Figure 4-20).

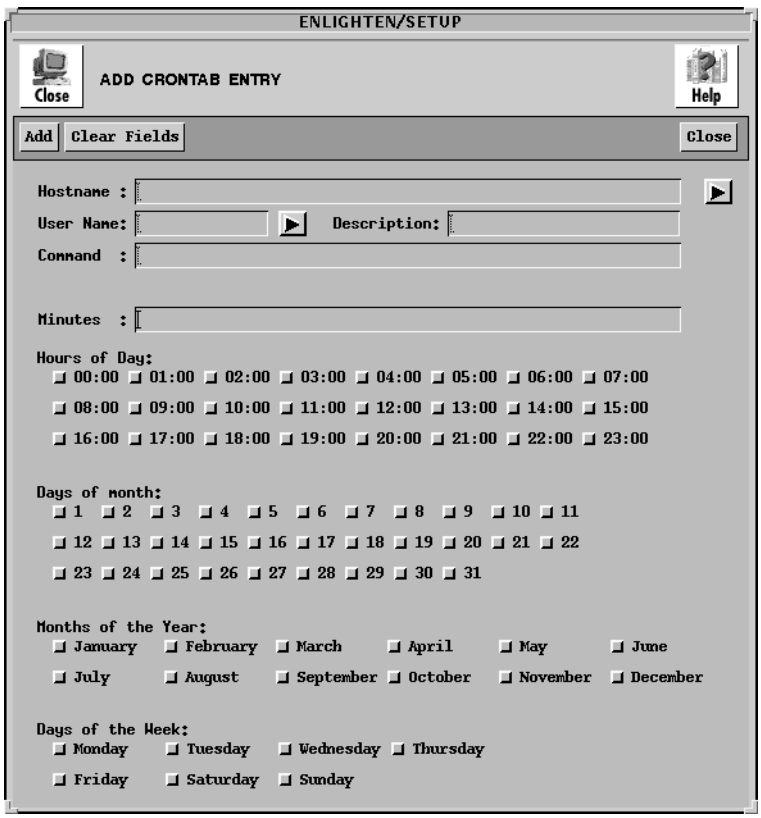

Figure 4-20 Add Crontab Entry window

A crontab entry consists of six fields. Any combination of the five time fields (minutes, hours, days, months, and/or days of the week) define when the command (sixth field) will execute. By default, the job will run every hour if all the time fields are left blank.

3) Enter the Add Crontab Entry parameters. See the section, "Add/Modify Crontab Entry Parameters," on page 4-29 for information about any of the fields in this window.

4) Click the Add button to selectively create the crontab job.

Modifying a Crontab Entry

To modify a crontab entry,

1) Choose Cron Management from the System menu and then choose Configure.

2) Highlight the entries you want to modify in the Crontab Configuration window (Figure 4-19).

3) Click the Modify button. The Modify Crontab Entry window appears.

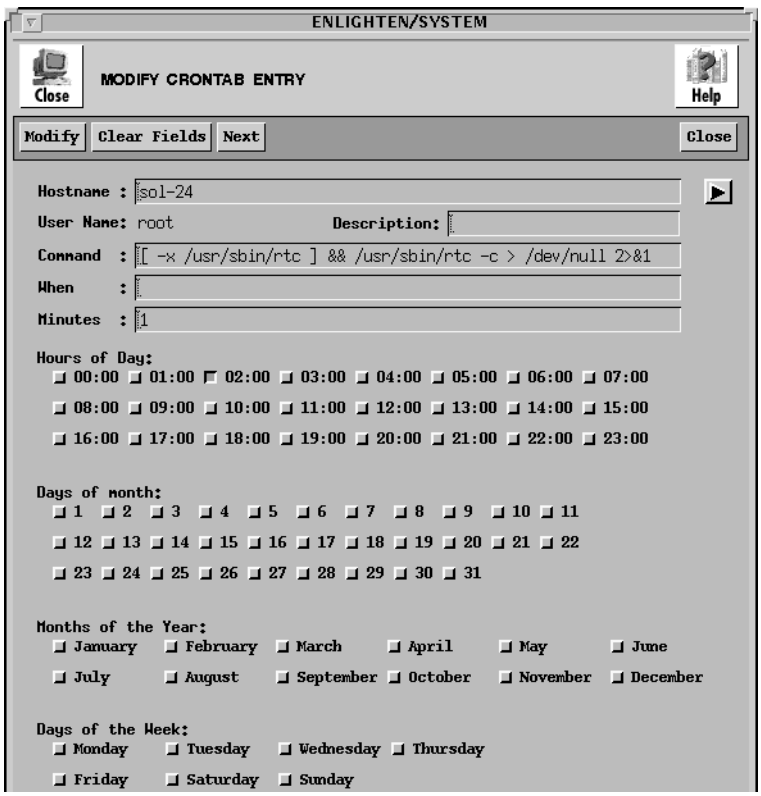

Figure 4-21 Modify Crontab Entry window

4) Change the entry parameters that you want. See the next section, "Add/Modify Crontab Entry Parameters," for information about each field.

5) Click the Modify button.

6) If you selected more than one entry in the Crontab Configuration window, click the Next button to modify the next entry.

Add/Modify Crontab Entry Parameters

The Modify Crontab Entry window is similar to the Add Crontab Entry window except that you cannot change the User Name field.

Hostname field

If you want to limit this job to specific hostnames within a pool, enter those hostnames in this field. If you are using multiple entries, leave a blank between each entry. You can also use the arrow button to the right to select the available hosts from the current pool.

User Name field

You can use this field to specify which user will run this job. You can also click the arrow button on the right to display a list of users and select one.

Description field

You can use this field to briefly describe this job's purpose.

Command field

Use this field to specify the cron command (and arguments) to be run at the time established by the remaining five fields.You can use a maximum of 256 characters to specify this command.

Minutes field

Use this field to specify what point in the specified hour(s) the job will run. Enter a whole number between 0 and 59. Or you can specify a range by using a hyphen (-), for example, 0-20. If you are using multiple entries, leave a blank between each entry.

Hours of Day
Days of month
Months of the Year
Days of the Week options

Click the appropriate boxes to further define when this job will run. You may select multiple values per field.

Querying Cron Jobs

You can find specific cron jobs by searching for hostnames, usernames, the command itself, the time settings, and so on. Once your query is successful, you can then modify, delete, or copy the cron job.

To query a cron job,

1) Choose Cron Management from the System menu, then Query. The Cron Entry Query window appears.

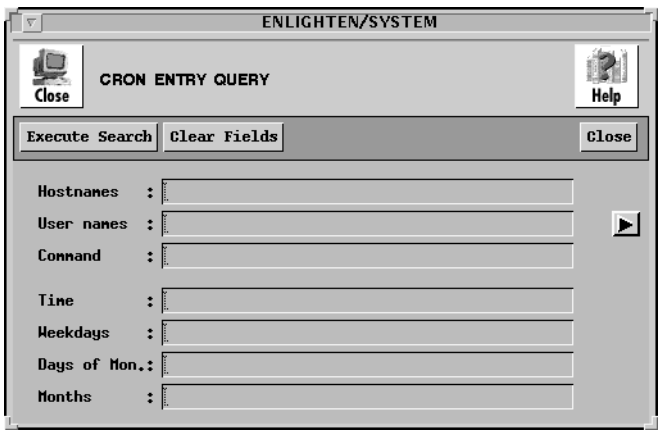

Figure 4-22 Cron Entry Query window

The cron job must match all fields to get a successful match. The fields in this window have a logical *and* relationship. Blank fields always match and you can also negate fields with the `!` character (for example, `!Monday`).

2) To limit the search to specific hostnames within a pool, enter those hostnames in the Hostnames field. If you are using multiple entries, leave a blank between each entry.

3) To limit the search to specific users, specify which one(s) in the User Names field. If you are using multiple entries, leave a blank between each entry. You can also use the arrow button to the right to select from a pick list of the users.

4) To limit the search to a specific cron command (or any of its options), enter it in the Command field. You can use a maximum of 256 characters in this field, including the standard UNIX wildcards.

5) To specify times or time ranges, enter parameters in the Time, Weekdays, Days on Mon., and Months fields. This limits the search to find jobs executing at/between the times entered in these field.

6) After selecting your search criteria, click the Execute Search button. If you click this button without entering values in any of the fields, all current cron jobs will be displayed. A window similar to the Crontab Configuration window appears with the results listed.

You can modify, delete, or copy the current cron jobs listed in the Crontab Configuration list.

Managing Cron Users

Cron has built-in security features allowing you to control which users are allowed to execute cron jobs. There are five possible user access states:

- Only root is allowed to execute cron jobs.
- Only selected users are allowed to execute cron jobs.
- All users are allowed to execute cron jobs.
- All users except specified users are allowed to execute cron jobs.
- No users are allowed to execute cron jobs.

To control user access,

1) Choose Cron Management from the System menu and then Cron Users to display the cron security status of all hosts (Figure 4-23).

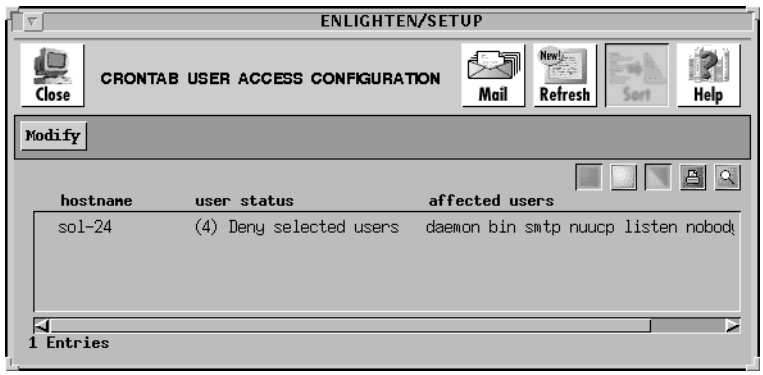

Figure 4-23 Crontab User Access Configuration window

2) Highlight which users' accessibility you want to change and click the Modify button. The Modify Crontab window (Figure 4-24) appears.

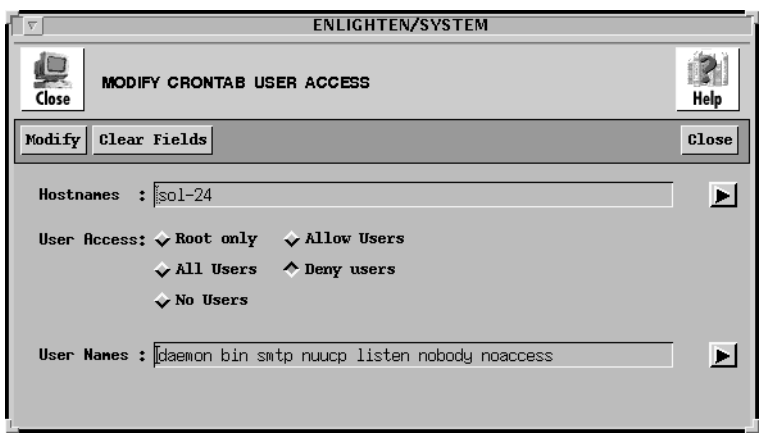

Figure 4-24 Modify Crontab window

3) Use this window to modify the cron user access for multiple hosts.

4) To limit this modification to specific hostnames within a pool, enter those hostnames in the Hostnames field. If you are using multiple entries, leave a blank between each entry. You can also use the arrow button to the right to select the available hosts from the current pool.

5) Set the User Access option to specify what type of user cron access you want to allow.

6) To allow or exclude (deny) specific users, enter the user name(s) in the User Names field. If you are using multiple entries, leave a blank between each entry. You can also use the arrow button to the right to select from a pick list of the users.

7) Click the Modify button to make the crontab user access modifications.

Archiving Files

Essential to every network manager is the ability to automatically back up and archive in order to safeguard files. ENlighten/DSM provides you with the ability to configure devices, perform tape operations, restore files, and schedule full and incremental backups.

This section provides basic information about configuring devices and performing backups. For information about backing up to tape drives, restoring files, and cataloging backup files, refer to Chapter 6, "Archive," in the *ENlighten/DSM Reference Manual*.

Adding Backup Devices

You can use a variety of different devices to back up system files, including custom devices, reel-to-reel tapes, 1/4-inch cartridge tapes, or a raw device types.

To add a new device,

1) Choose Configure Devices from the Archive menu. The Archive Device Configuration window appears, listing which devices are available for archiving data.

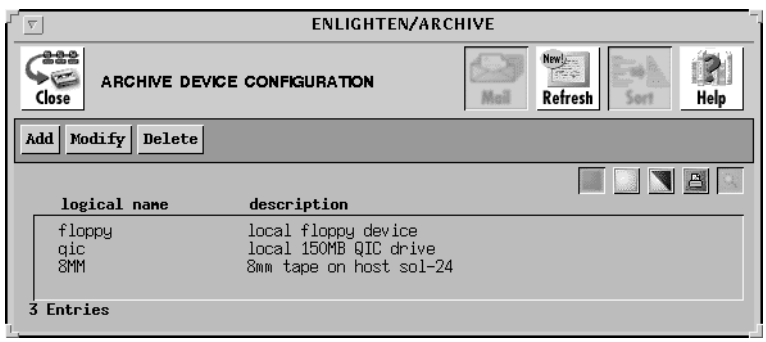

Figure 4-25 Archive Device Configuration window

2) To add a new device, click the Add button. The Archive Device Add window appears (Figure 4-26).

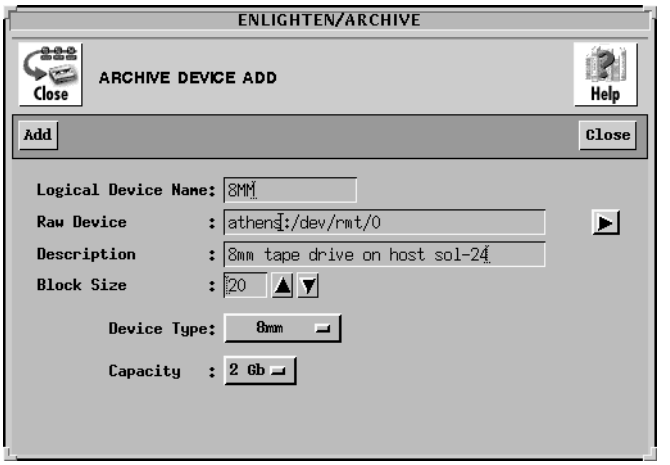

Figure 4-26 Archive Device Add Window

3) Enter the device name that the user specifies when accessing this backup device in the Logical Device Name field.

4) Enter a UNIX device name in the Raw Device field, using the form: `hostname:/dev/rmt0`. You can click the Select button to choose from a list of possible tape device names. You need to prefix the device name with its hostname, followed by a colon (:).

   For example, if you have a device `/dev/rmt/0h` on host `athens`, the name of the device would be:

   ```
   athens:/dev/rmt/0h
   ```

   Note that this host must have an active renld daemon for a successful backup.

5) Enter a device description or name in the Description field.

6) Choose a block size from the Block Size option.

   Each type of device has a blocking factor associated with it. The blocking factor is the size of each data block written to the device. The most common blocking factor is 20 blocks; however, you can back up data using a blocking factor of up to 2000 blocks. Block size is O/S dependent. On Solaris 2.4, the block size is 1024 bytes (1K). On SCO 5 platform, the default block size is 1K.

7) Choose the device type from the Device Type option. The Device Type specifies the device's capacity. The options are:

   - The Cartridge Tape option displays tape length and density. For length, click the left mouse button and then drag the cursor to the appropriate value: 300, 450, or 600 feet. For density, click QIC 24 (low) or QIC 120 (high).
   - The Reel option displays tape length and density line. For length, click the left mouse button and then drag the cursor to the appropriate value: 600, 1200, or 2400 feet. For density, click 1600 (low) or 6250 (high).
   - The Custom option allows you to define your own device. You will be prompted to enter the capacity for the new device in KB.
   - The Raw option allows you to quickly add an entry to the device list. Use this option to add a device with no capacity or a new piece of media. Eventually, you should redefine this storage device.
   - Click the 8 MM button to define an 8mm cartridge tape device. You are prompted to select the capacity of the tape. The options are 2GB (default) and 5GB. If neither of these options applies, create a custom backup device and manually set the device capacity. Or you can create a raw device and then define the device capacity.

8) Click the Add button to save the parameters.

Modifying Backup Devices

To view and/or modify the backup devices configured on your system,

1) Highlight the device name you wish to modify from the Archive Device Configuration window (Figure 4-25).

2) Click the Modify button. A window will appear similar to the Archive Device Add window, except the Logical Device Name field is view-only.

3) Change the parameters that you want to modify.

4) Click the Modify button to save the changes you have made.

5) Click the Next button to modify additional backup schedules if you've selected more than one backup to modify from the Add Device Configuration list.

Deleting Backup Devices

To remove an ENlighten/DSM backup device from ENlighten/DSM, highlight the devices you want to delete from the Archive Device Configuration window (Figure 4-25), then click the Delete button. To ensure the correct backup device is being deleted, ENlighten/DSM will prompt you for confirmation before deleting it. After an entry has been removed, the only way to add it again is to recreate the entry.

Performing Backups

You can schedule and perform incremental or full backups on filesystems (disk partitions). Full backups contain all files in the selected partition you choose, while incremental backups contain only selected files in the partition that have been modified since the last backup. You may want to use incremental backups as your daily backup since it is generally much faster. You do not need to know specific UNIX commands; ENlighten/DSM prompts you for the information needed to create the backup. For both types you use the Backup Partitions window shown in Figure 4-27.

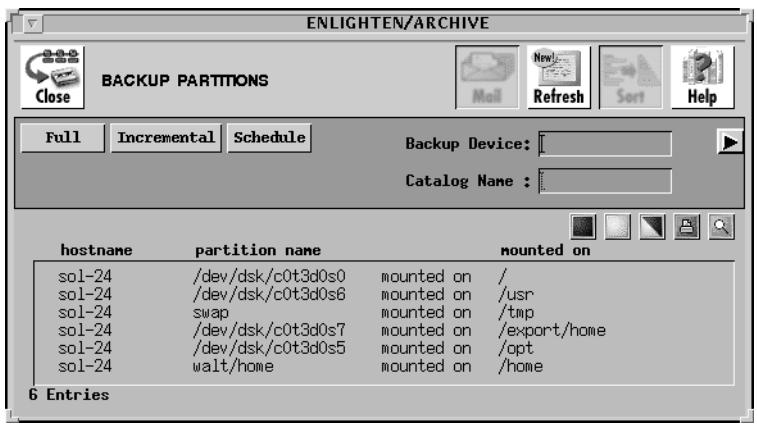

Figure 4-27 Backup Partitions window

ENlighten/DSM can catalog the backed-up files. To do so, turn on the catalog function in the Session Preferences menu item. These catalogs can be queried at a later time to help find instances of backed-up files. The default setting does *not* keep a catalog of backed-up files.

If the Catalog option is enabled, enter a catalog name in the Catalog Name field. This can be a filename or just an identifying tag. If no name is entered, ENlighten/DSM uses the default name of `NONAME`.

Full Backup

To perform a full backup,

1) Choose Backup Partitions from the Archive menu. A list of all current local mounted partitions is displayed. If session preferences is set to Include NSF Parts, then NFS mounted parts is displayed also.

2) Highlight the partitions you wish to back up.

3) Enter the logical device name or click the arrow button on the right for a pick list of defined backup devices.

4) Click the Full button. A window will appear asking for confirmation of your action. Once the backup is completed, the names of the files will be displayed on the screen.

Incremental Backup

To perform an incremental backup,

1) Choose Backup Partitions from the Archive menu. A list of all current local and NFS mounted partitions is displayed.

2) Highlight the partition names you want to back up and enter the desired backup device. (You can also click the arrow button on the right for a pick list of available backup devices.)

3) Then, click the Incremental button. A window will prompt you for the type of incremental backup to run (Figure 4-28).

Figure 4-28 Incremental Backup window

You can back up the following selected partitions:

- Since the last full backup (the default setting).
- Since the last incremental backup.
- Within a specific time period (the last n days).

4) Choose one option.

5) Once you've made all your selections, click the Apply button. As ENlighten/DSM does the backup, a listing of each file it archives will be displayed in a window.

Scheduling Backups

You can automatically schedule full or incremental backups of selected files and partitions.

The Scheduled Backup window (Figure 4-29) displays a list of all currently defined scheduled backups, their schedule types, and their descriptions.

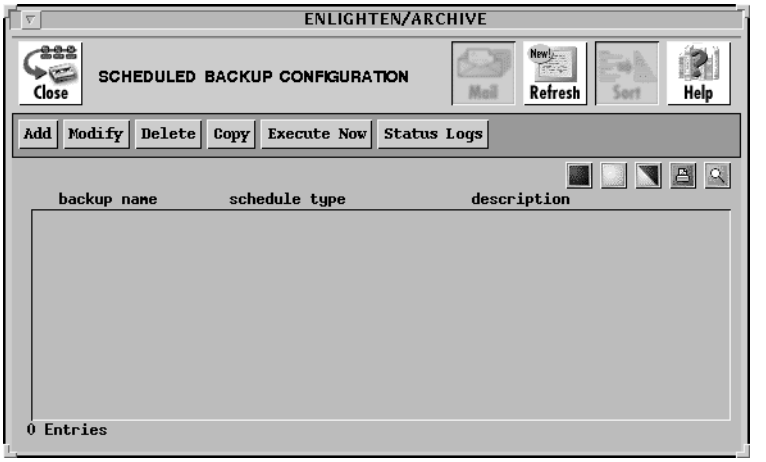

Figure 4-29 Scheduled Backup Configuration window

The rest of this section explains the backup windows' functionality.

To add a scheduled backup,

1) Choose Schedule Backup from the Archive menu.
2) Click the Add button. The Add Scheduled Backup window appears.

Figure 4-30 Add Scheduled Backup window

3) Enter the parameters in each field. For information about each field, see "Scheduled Backup Fields," on page 4-43.

4) Click the Add button to create the scheduled backup defined by the rest of this window's fields.

5) Click the Execute Now button to execute the highlighted backup immediately. This occurs regardless of the backup's defined schedule time.

Modifying Scheduled Backups

To modify a scheduled backup,

1) Choose Scheduled Backup from the Archive menu.
2) Highlight the backup that you want to change.
3) Click the Modify button. The Modify Scheduled Backup window appears.
4) Change the parameters you want. See the next section, "Scheduled Backup Fields," for a description of each option in the window.
5) Click the Modify button to save your changes.
6) Click the Next button to modify additional backup schedules if you've selected more than one backup to modify from the Scheduled Backup Configuration list.

Scheduled Backup Fields

The Add Scheduled Backup and Modify Scheduled Backup windows are the same, except the Backup Name field in the Modify window is a display-only field.

The Add Scheduled Backup window contains the following fields:

Backup Name field

Use this field to specify the backup's name.

Description field

Use this field to provide a brief description of the backup.

Backup Device field

Use this field to specify the logical device name for the backup. Logical device names are defined via the Configure Device window. You can also click the arrow button to the right to bring up a list of all defined device names and select one of them.

Catalog Name field

If you have enabled backup catalogs, specify in this field a catalog name that will be used to keep a record of this backup. See the Catalog option in the Session Preferences menu item.

Backup Type option

These toggle buttons specify whether to run an Incremental or Full backup. The Incremental setting also activates the Backup Files CHANGED toggle buttons.

Backup Files Changed options

This set of toggle buttons specifies which files should be backed up during an Incremental backup. You can back up the following selected files:

- Since the last full backup (the default setting).
- Since the last incremental backup.
- Within a specific time period (the last n days).

Choosing the Within Time Period setting displays the Number of Days field so you can specify a time period.

Number of Days field

You can use this field to specify how many days back ENlighten/DSM will check to see if a file has changed and therefore should be backed up. The arrow buttons to the right will automatically increment or decrement the number displayed in the text field.

Remain in Partition option

Choose the Yes setting to backup only the immediately defined partition for a particular directory. Choose the No setting to backup all partitions listed under that directory. The default setting is Yes.

File List option

If you are incrementally backing up, this option allows you to choose the directories and files to be backed up. Enter which files will be checked for changes. Those that have changed will then be backed up as specified in the preceding fields. Remote files need the hostname followed by the directory name.

Time of Backup field

You can use this field with the Schedule Type toggle buttons to determine when a backup should be executed. See the following Schedule Type field description for more details on how this field is used.

Schedule Type

This set of toggle buttons determines how and when the backup will occur. The choices are:

- Weekly — The days of the week will be displayed. Select which days the backups should occur. Enter when the backup will occur in the Time of Backup field.
- Monthly — The days of the month will be displayed. Select which days the backups should occur. Enter when the backup will occur in the Time of Backup field.
- Manual — This option does not schedule a time to perform the backup; you run it by selecting the Execute Now button in the Scheduled Backup Configuration parent window or the current window.
- One Time — Specify a (one time) date and time to run the backup in the Time of Backup field.

Status Logs

When backups are run in the background at their scheduled times, they create a backup log. Click the Status Logs button to access these status logs in the Backup Logs window (Figure 4-31).

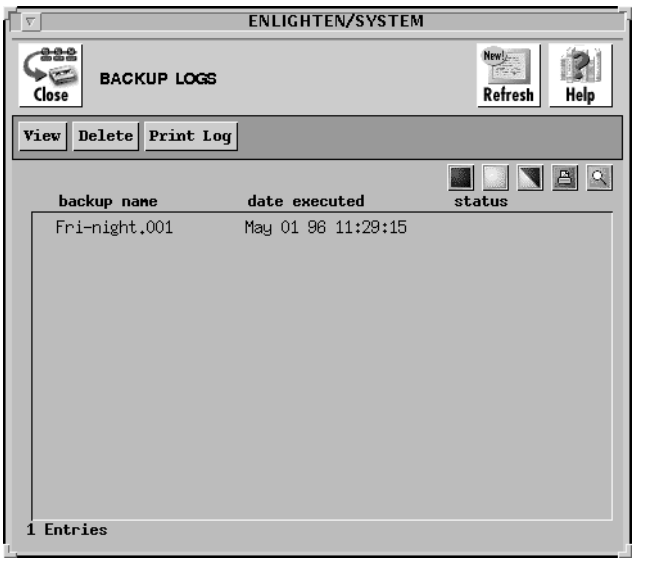

Figure 4-31 Backup Logs window

Click the Print Log button to print a copy of the selected backup logs. The output is sent to the printer defined in the Print field in the Session Preferences configuration window.

Click the View button to view the selected backup logs.

Click the Delete button to remove the selected backup logs.

Configuring NIS and NIS+ Servers

ENlighten/DSM provides you with the tools to configure master Network Information Servers (NIS and NIS+), slave servers (NIS), and replica servers (NIS+).

You must first disable a host as an NIS server or client before reconfiguring that host as an NIS+ server or client.

Adding an NIS Server

To add an NIS server or slave to your network,

1) Choose NIS and NIS+ from the Network menu. The NIS Servers window appears displaying all configured NIS and NIS+ servers. Each line in the list will show the type, domain, and hostname for each server.

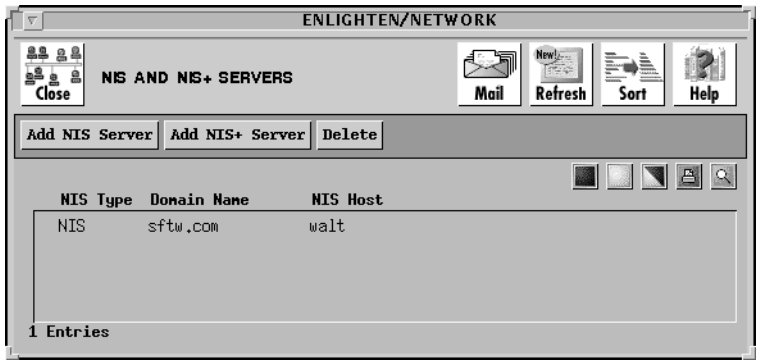

Figure 4-32 NIS and NIS+ Servers window

2) Click the Add NIS Server button to configure NIS master servers or NIS slave servers. The Add NIS Server window appears.

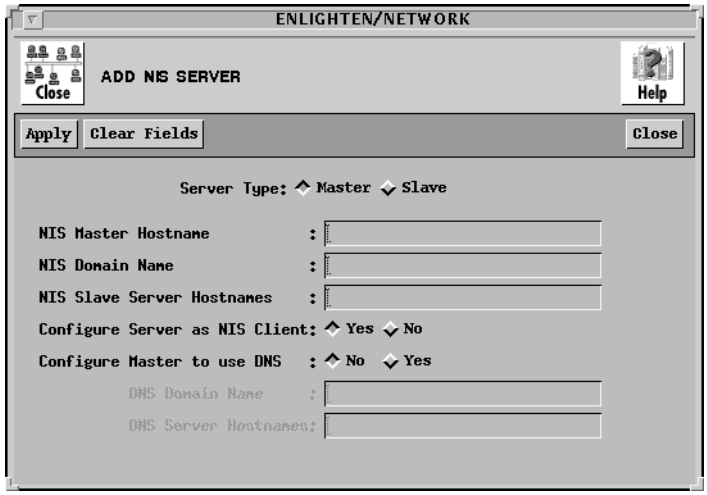

Figure 4-33 Add NIS Server window

3) Click the Master Server Type or Slave Server Type button to select the server type. The Add NIS Server window changes depending on the Server Type option that you choose.

4) Enter the field parameters for either the master or slave server. The master and slave fields are described in the next two sections.

5) Click the Apply button to add the new NIS server shown in the window.

NIS Master Fields

When you choose the Master Server Type option, the Add NIS Server window has the following fields (see Figure 4-33):

NIS Master Hostname field

Use this field to specify the hostname of the NIS master server.

NIS Domain Name field

Use this field to specify the domain name for this server.

NIS Slave Server Hostnames field

You can use this field to specify any NIS slave servers for this domain.

Configure Server as NIS Client

Use this toggle to specify if this server should also be configured as an NIS client. The default setting is Yes.

Configure Master to use DNS

Use this toggle to specify if the NIS master server should use DNS as a fall back. The default setting is No.

DNS Domain Name field

You can only use this field if you set the Configure Master to use DNS field to Yes. If so, you can use this field to specify the domain name of the DNS servers the NIS master should reference.

DNS Server Hostnames field

You can only use this field if you set the Configure Master to use DNS field setting to Yes. Then, you can use this field to specify the domain name and hostnames of the DNS servers the NIS master should reference.

NIS Slave Fields

When you choose the Slave Server Type option, the Add NIS Server window (Figure 4-34) has the following fields:

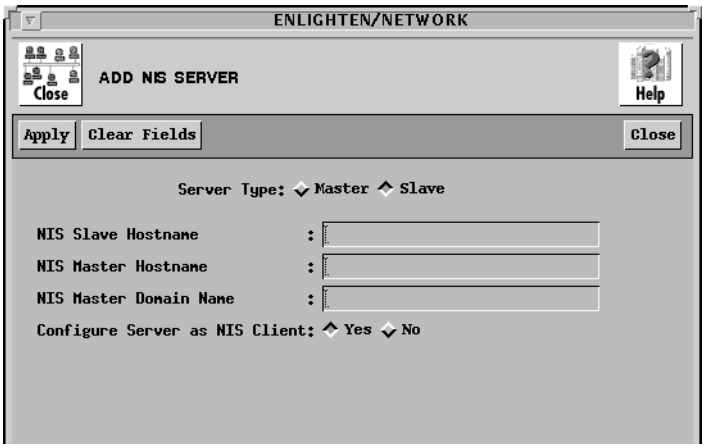

Figure 4-34 Slave Add NIS Server window

NIS Slave Hostname field

Use this field to specify the hostname of the NIS slave server.

NIS Master Hostname field

Use this field to specify the hostname of the NIS master server.

NIS Master Domain Name field

Use this field to specify the domain name for the NIS master server.

Configure Server as NIS Client option

Use this toggle to specify if this server should also be configured as an NIS client. The default setting is Yes.

Adding an NIS+ Server

To add an NIS+ server,

1) Choose NIS and NIS+ from the Network menu. The NIS and NIS+ Servers window appears displaying all configured NIS and NIS+ servers. Each line in the list will show the type, domain, and hostname for each server.

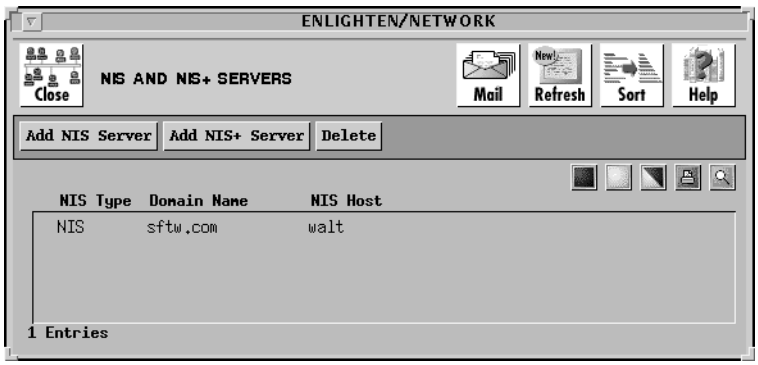

Figure 4-35 NIS and NIS+ Servers window

2) Click the Add NIS+ Server button. The Add NIS+ Server window appears.

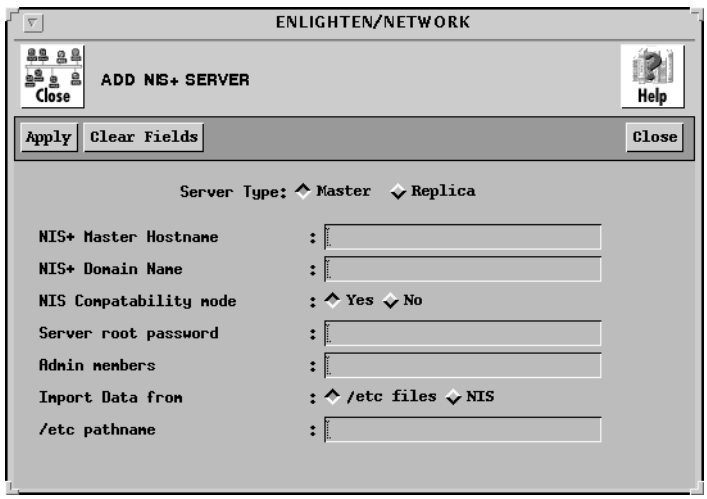

Figure 4-36 Add NIS+ Server window

3) Choose the NIS+ server type you want: a Master (the default) or Replica server. If you choose the Replica server option, the window will be redrawn to show the fields listed in "Replica Fields," on page 4-53.

4) Enter the remaining field parameters. See the next two sections for information about NIS+ master and replica configurations.

5) Click the Apply button.

NIS+ Master Fields

When you choose the Master Server Type, the following fields are displayed on the Add NIS+ Server window:

NIS+ Master Hostname field

Use this field to specify the hostname of the NIS+ master server.

NIS+ Domain Name field

Enter the domain name for the NIS+ master server.The domain name is used to uniquely identify users and hosts that are making NIS+ requests.

NIS Compatibility mode

Use this toggle to specify if this NIS+ should be made backwards compatible with NIS. The default setting is Yes.

Server Root Password field

Use this field to specify the root password for the NIS+ master server.

Admin Members field

Use this field to specify which users are allowed to administer this NIS+ host. Leave a blank space between names for multiple entries.

Import Data From field

Use this toggle to specify if any existing imported data should come from the servers' /etc files or from an NIS server. The default is /etc.

/etc pathname field

You can use this field only if you set the Import Data From field to /etc files. If so, you can use this field to specify these files' pathname.

NIS Domain field

You can use this field only if you set the Import Data from field to NIS. If so, you can use this field to specify the domain name of the NIS server from which to import the data.

NIS Server field

You can use this field only if you set the Import Data from field to NIS. If so, you can use this field to specify the hostname of the NIS server.

Replica Fields

This window is similar to the Add NIS+ Server window for a master server shown in Figure 4-36. It contains the following fields:

Server Type option

Use this toggle to specify what type of NIS+ server to configure, a Master (the default) or Replica server. If you set this to be a Master server, the window will be redrawn to show the fields listed in "NIS+ Master Fields," on page 4-52.

NIS+ Master Hostname field

Use this field to specify the hostname of the NIS+ master server.

NIS+ Domain Name field

Use this field to specify the domain name for the NIS+ master server.

Replica Hostname field

Use this field to specify the hostname of the NIS+ replica server.

Replica Server Root Password field

Use this field to specify the root password for the NIS+ replica server.

NIS Compatibility mode

Use this toggle to specify if this NIS+ server can also interact with NIS servers. The default is Yes.

Deleting Server Configurations

To delete an NIS or NIS+ server configuration,

1) Select the server you want to delete from the NIS and NIS+ Servers window.

2) Click the Delete button. The Delete NIS/NIS+ Server window appears.

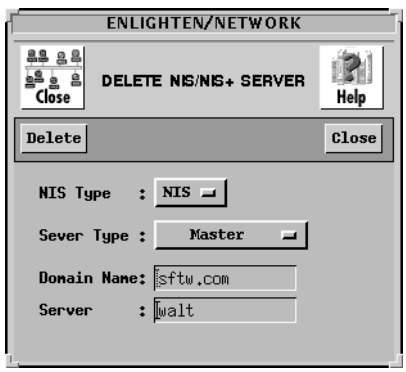

Figure 4-37 Delete NIS/NIS+ Server window

3) Click the NIS Type button to specify what type of server to delete, an NIS (the default) or NIS+ server.

4) Click the Server Type button to specify what type of server to delete, a Master (the default) or Slave/Replica server.

5) Enter the domain name for the server in the Domain Name field.

6) Enter the hostname in the Server field if you set the Server Type field to Slave/Replica. If so, you can use this field to specify the hostname of the NIS/NIS+ master server.

7) Select a Remain as Client option if you set the Server Type field to Slave/Replica. If so, you can use this toggle to specify if this server should remain as an NIS client after deletion. The default is Yes.

8) Click the Delete button.

ENlighten/DSM does not automatically detect whether a server is a master or slave/replica server.