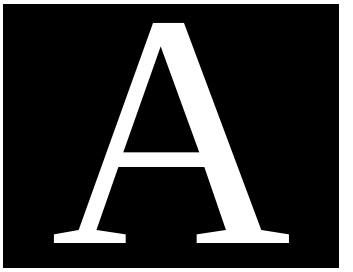

Wizard

The Wizard function exists in the Disk Usage Information by Filesystem, the User Configuration, the Configured Printers, and the Host Configuration windows. These Wizards analyze, with a focus on security, various system aspects.

Click the Wizard button to pop up the appropriate analysis window. Select the type of security evaluations you want, then click the Apply button. Be aware the evaluations marked by a star (*) are relatively time-consuming.

Once the evaluation is complete, a summary of findings will be displayed in the top right portion of the window, as shown in Figure A-1. You can use the window buttons for further analysis.

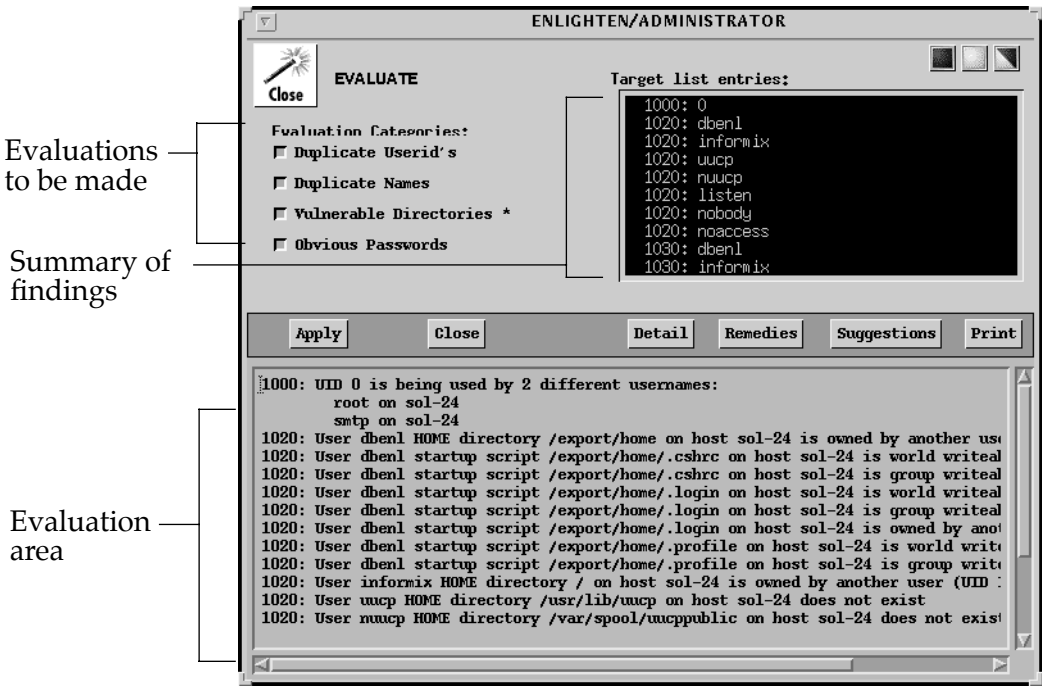

Figure A-1 Evaluation window

Detail

Use this button to display (in the evaluation area) a detailed list of findings for those entries highlighted in the summary window.

Remedies

Just knowing that there is a potential problem does not necessarily solve it. You can use this button to get a brief description of the problems encountered for the entries highlighted in the summary window. Furthermore, the Wizard will also make suggestions on how to remedy the problems using ENlighten/DSM.

Suggestions

Use this button to see suggestions on how to avoid the problem in the future for any entries highlighted in the summary window.

Print

You can use this button to print the contents of the explanation area, as defined in the default print command field in the Session Preferences window. See "Session Preferences" on page 2-2 for more details on setting up this command.

The remaining sections of this chapter detail the security check options within each of the four Wizards.

Disk Wizard

The Disk Wizard performs a series of disk checks with an emphasis on security needs.

Full Disk Partitions

This is a simple test to check if disk usage on any of the partitions has surpassed 85% capacity.

Set UID/GID Problems

When a set UID or GID (setuid) program is executed, it gains the permissions of the owner/group of the program. Consequently, a setuid program owned by root will give the user super user privileges when executed. This concept is fine as long as these programs have the proper built-in safety mechanisms. Without the proper safety mechanisms, these programs can create a major security risk.

Wizard runs several checks on setuid programs when this option is selected. It performs the checks against the current disk snapshots of all partitions. Furthermore, some of the checks involve the use of the associated Master snapshot. Make sure the disk snapshots for all partitions are relatively new. See "Save Current Snapshots" on page 5-27 for more information on re-creating snapshots and creating Master Snapshots.

First, the Wizard checks if each setuid program found is in what it considers to be a system directory. If not, this will be reported. The current system directories are:

```
/bin        /sbin       /etc
/usr/bin    /usr/sbin   /usr/lib
/usr/ucb    /usr/kvm    /etc
```

Next, the Wizard checks the permissions of the program. If the program is world-writable, that is, may be replaceable, this will be reported.

Finally, if a master snapshot for the partition being checked exists, the Wizard checks if the setuid program existed at the time the master snapshot was created. If the setuid program has been newly created

since the master snapshot was taken, this will be reported. If the program did previously exist, Wizard checks if it is still the same file by looking for a difference in the file's size, permissions, or date of last modification.

Devices not in /dev

Device files are used in UNIX as an interface to the hardware and kernel memory. These device files should only be found in the directory `/dev` (and on some systems `/devices`). If a device file is found outside of these directories, it should be considered a serious threat.

Wizard scans the existing disk snapshots looking for devices not in the `/dev` or `/devices` (where appropriate) directories when this option is selected. If any files are found, they are reported.

User Wizard

The User Wizard helps with user-related problems.

Duplicate UserID's

This operation searches for users with different names sharing the same UID. There may be times when this usage is necessary.

Duplicate Names

This operation searches for users with the same name using different UIDs on different hosts. Typically a user should have a consistent UID on all hosts.

Vulnerable Directories

This operation is similar to the User Home Directory security check in the security menu. See "User Home Directories" on page 3-9 for more information on this check.

Obvious Passwords

This operation is a subset of the obvious password checking in the security menu. It checks if the user has a password, if the password is the same as the username, or if the password is zero length (just press Enter to get in). For more detailed password checking, see "Obvious Passwords" on page 3-11.

Printer Wizard

The Printer Wizard checks for printer-related problems.

Downed Printers

This checks if any of the printers are disabled. If any are, they are reported.

Long Print Queues

This checks if a print queue for any of the printers has more than 15 print jobs queued. If so, this is reported. If a print queue gets too long you might want to move some of the jobs to other compatible printers. See "Move" on page 7-10 for more details.

Large Print Jobs

This checks if any queued print job is larger than 400 KB. If so, this is reported.

Host Wizard

The Host Wizard checks for potential host conflicts.

Host Address Conflicts

This check looks at all hostnames and their associated TCP/IP addresses and verifies all hosts of a given name have the same network address. If a hostname is found on one host with a different address than on another host, this is reported.

Host Entry Name Conflicts

This check looks at all hostnames and their associated TCP/IP addresses and verifies a given address only has one hostname associated with it. If an address is found to have more than one hostname associated with it on any host, this is reported.

Host Aliasing Conflicts

This check looks at all host alias names and verifies each alias name is used uniquely for a single hostname. If an alias is found to apply to more than one hostname, this is reported.