

The VirusScan Enterprise software depends on information in the virus definition (DAT) files to identify viruses. Without updated files, the product software might not detect new virus strains or respond to them effectively. Software that is not using current DAT files can compromise your virus-protection program.

New viruses appear at the rate of more than 500 per month. To meet this challenge, McAfee releases new DAT files every week, incorporating the results of its on-going research into the characteristics of new or mutated viruses. The update task that is provided with the VirusScan Enterprise software makes it easy to take advantage of this service.

The AutoUpdate feature has been improved to provide easier, more flexible updating. This feature allows you to download the latest DAT files, scanning engine, and EXTRA.DAT simultaneously, using an immediate update or a scheduled update. You can also use this feature to download HotFixes and product upgrades.

The following topics are covered in this section:

- Update strategies
- AutoUpdate
- Mirror tasks
- AutoUpdate repository list
- Rollback DAT files
- Manual updates

## Update strategies

There are many methods available for performing updates. You can use update tasks, manual updates, login scripts, or schedule updates with management tools. This document discusses using AutoUpdate and updating manually. Any other implementations are beyond of the scope of this document.

An efficient updating strategy generally requires that at least one client or server in your organization retrieve the updates from the Network Associates download site. From there, the files can be replicated throughout your organization, providing access for all other computers. Ideally, you should automate the process of copying the updated files to your share points, while minimizing the amount of data transferred across your network.

The main factors to consider for efficient updating are the number of clients and the number of sites. There may be additional considerations that affect your update schema, for example, the number of systems at each remote site and how remote sites access the internet. However the basic concepts of populating your share points and scheduling updates apply to any size organization.

Using an update task to perform updates allows you to:

- Schedule network-wide DAT file roll-outs and product upgrades for convenient times and with minimal intervention from either administrators or network users. You might, for example, stagger your update tasks, or set a schedule that phases in or rotates DAT file updates and product upgrades among different parts of the network.
- Split roll-out administration duties among different servers or domain controllers, among different regions of wide-area networks, or across other network divisions. Keeping update traffic primarily internal can also reduce the potential for network security breaches.
- Reduce the likelihood that you will need to wait to download new DAT or upgrade files. Traffic on McAfee computers increases dramatically on regular DAT file publishing dates and whenever new product versions appear. Avoiding the competition for network bandwidth enables you to deploy your new software with minimal interruptions.

## AutoUpdate

This version of VirusScan Enterprise uses the AutoUpdate 7.0 component to schedule tasks and to perform updating functions.

- The AutoUpdate 7.0 scheduling feature is used to schedule all tasks, including on-demand, update, and mirror tasks. See [Scheduling tasks on page 200](#) for more information.
- The AutoUpdate 7.0 updating feature is used to perform scheduled or immediate update tasks. You can update DAT files, scanning engine, HotFixes, EXTRA.DAT, and product upgrades.

The VirusScan Enterprise product provides a default update task that is scheduled to update every Friday at 5:00 p.m. with one-hour randomization. The default update task is named **AutoUpdate**. You can rename and reconfigure the default **AutoUpdate** task. You can also create additional update tasks to meet your updating requirements.

Update tasks are resumable as follows:

- **Tasks that are updating from an HTTP, UNC, or local site.** If the update task is interrupted for any reason during the update, the task resumes where it left off the next time the update task starts.
- **Tasks that are updating from an FTP site.** The task does not resume if interrupted during a single file download. However, if a task is downloading several files and it is interrupted, then the task resumes before the file that was being downloaded at the time of the interruption.

The following topics are covered in this section:

- Creating an AutoUpdate task
- Configuring an AutoUpdate task
- Running AutoUpdate tasks
- Viewing the activity log

## Creating an AutoUpdate task

To create a new AutoUpdate task:


- 1 Open the **VirusScan Console**. See [VirusScan Console on page 19](#) for instructions.
- 2 Create a new update task using one of these methods:
  - ◆ Right-click a blank area in the Console, without selecting an item in the task list, then select **New Update Task**.
  - ◆ Select **New Update task** from the **Task** menu.

A new update task appears, highlighted, in the **VirusScan Console** task list.

- 3 Accept the default task name or type a new name for your task, then press ENTER to open the **AutoUpdate Properties** dialog box. See [Configuring an AutoUpdate task on page 174](#) for detailed configuration information.

## Configuring an AutoUpdate task

You can configure and schedule an AutoUpdate task to meet your requirements.

- 1 Open the **VirusScan Console**. See [VirusScan Console on page 19](#) for instructions.
- 2 Open the **AutoUpdate Properties** dialog box using one of these methods:
  - ◆ Highlight the task in the Console task list, then select **Properties** from the **Task** menu.
  - ◆ Double-click the task in the task list.
  - ◆ Right-click the task in the task list, then select **Properties**.
  - ◆ Highlight the task in the task list, then click .

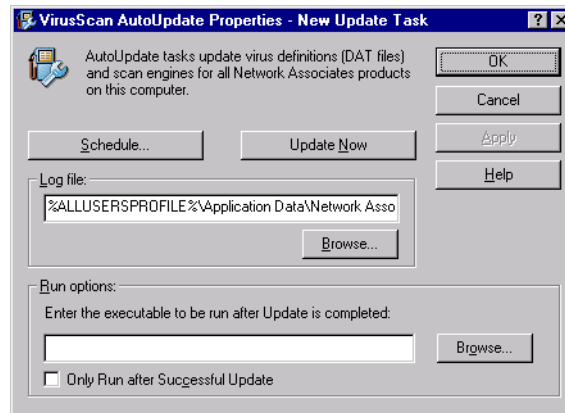


Figure 7-1. AutoUpdate Properties — New Update Task

**NOTE**

Configure the update task before you **Schedule** it or perform an **Update Now**.

- 3 In the **Log file** text box, accept the default log file name and location, enter a different log file name and location, or click **Browse** to locate a suitable location.

**NOTE**

By default, log information is written to the UPDATELOG.TXT file in the following directory:

```
<drive>:\Winnt\Profiles\All Users\Application Data\Network Associates\Virusscan
```

- 4 In the **Run options** area, you can specify an executable file to start after the **AutoUpdate** task finishes running. For example, you might use this option to start a network message utility that notifies the administrator that the update operation completed successfully.
  - ◆ **Enter the executable to be run after Update is completed.** Enter the path of the executable you want to run, or click **Browse** to locate it.
  - ◆ **Only Run after Successful Update.** Run the executable program only after a successful update. If the update is not successful, the program you selected does not run.

**NOTE**

The program file that you specify must be executable by the currently logged on user. If the currently logged on user does not have access to the folder containing the program files, or if there is no currently logged on user, the program does not run.

- 5 Click **Schedule** to schedule the update task. See [Scheduling Tasks on page 199](#) for more information.
- 6 Click **Apply** to save your changes.
- 7 If you want to run the update task immediately, click **Update Now**.
- 8 Click **OK** to close the **AutoUpdate Properties** dialog box.

### NOTE

The update task uses the configuration settings in the AutoUpdate repository list to perform the update. See [AutoUpdate repository list on page 184](#) for more information.

## Running AutoUpdate tasks

Once you have configured your task with the update properties you want, you can run the update task. The following topics are covered in this section:

- Running the update task
- Update activities that occur during an update task

### Running the update task

- 1 Open the **VirusScan Console**. See [VirusScan Console on page 19](#) for instructions.
- 2 Run the update task using one of these methods:
  - ◆ **Update as scheduled**. If you scheduled the update, allow the task to run unattended.

### NOTE

Your computer must be active to run an update task. If your computer is not operating when the task is scheduled to start, the task starts at the next scheduled time if the computer is active, or when the computer starts if you selected the **Run missed task** option on the **Schedule Settings, Schedule** tab.


- ◆ **Update immediately**. There are three methods of starting update tasks immediately:
  - ◆ **Update Now** command for default update task.
  - ◆ **Start** command for all update tasks.
  - ◆ **Update Now** command for all update tasks.

### Update Now command for default update task

You can use **Update Now** to immediately start the default update task.


#### NOTE

**Update Now** only works with the default update task which was created when you installed the product. You can rename and reconfigure the default update task, but if you delete the default task, **Update Now** becomes disabled.

- 1 Open the **VirusScan Console**. See [VirusScan Console on page 19](#) for instructions.
- 2 Use one of these methods to perform an immediate update using **Update Now**:
  - ◆ From the **VirusScan Console** select **Update Now** from the **Task** menu.
  - ◆ Right-click  in the system tray, then select **Update Now**.
  - ◆ When the task finishes, click **Close** to exit the **McAfee Updater** dialog box, or wait for the dialog box to close automatically.

### Start command for all update tasks

You can use **Start** from the **VirusScan Console** to immediately start any update task.

- 1 Open the **VirusScan Console**. See [VirusScan Console on page 19](#) for instructions.
- 2 Use one of these methods to start an immediate update from the **VirusScan Console**:
  - ◆ Highlight the task in the Console task list, then select **Start** from the **Task** menu.
  - ◆ Right-click the task in the task list, then select **Start**.
  - ◆ Highlight the task in the task list, then click .
  - ◆ When the task finishes, click **Close** to exit the **McAfee Updater** dialog box, or wait for the dialog box to close automatically.

### Update Now command for all update tasks

You can use **Update Now** in the **AutoUpdate Properties** dialog box to immediately start any update task.

- 1 Open the **VirusScan Console**. See [VirusScan Console on page 19](#) for instructions.

- 2 Open the **AutoUpdate Properties** dialog box for the selected update task. See [Configuring an AutoUpdate task on page 174](#) for detailed information about opening the **AutoUpdate Properties** dialog box.
- 3 Click **Update Now** in the **AutoUpdate Properties** dialog box.
- 4 When the task finishes, click **Close** to exit the **McAfee Updater** dialog box, or wait for the dialog box to close automatically.

### Update activities that occur during an update task

Products using the AutoUpdate 7.0 component download a CATALOG.Z file from the download repository. The CATALOG.Z file is used to perform incremental updates of the updated files.

## Viewing the activity log

The update task activity log shows specific details about the updating operation. For example, it shows the updated DAT file and engine version numbers.

To view the activity log:

- 1 Open the **VirusScan Console**. See [VirusScan Console on page 19](#) for instructions.
- 2 Use either of the following methods to open the activity log file:
  - ◆ Highlight the task, then select **Activity Log** from the **Task** menu.
  - ◆ Right-click the task in the task list and select **View Log**.
- 3 To close the activity log, select **Exit** from the **File** menu.

## Mirror tasks

The mirror task allows you to download update files from the first accessible download repository defined in the repository list, to a mirror site on your network. Each mirror site replicates the Network Associates site that contains the update files. Computers on your network can then download the files from the mirror site. This approach is *practical* because it allows you to update any computer on your network, whether or not it has Internet access, and *efficient* because your computers are communicating with a server that is probably closer than a Network Associates Internet site, therefore economizing access and download time. The most common use of this task is to *mirror* the contents of the Network Associates download site to a local server.

The following topics are covered in this section:

- Creating a mirror task
- Running mirror tasks
- Viewing the mirror task activity log

## Creating a mirror task

You can create a mirror task for each mirror location you need:

To create a new mirror task:


- 1 Open the **VirusScan Console**. See [VirusScan Console on page 19](#) for instructions.
- 2 Create a mirror task using one of these methods:
  - ◆ Right-click a blank area in the Console, without selecting an item in the task list, then select **New Mirror Task**.
  - ◆ Select **New Mirror task** from the **Task** menu.

A new mirror task appears, highlighted, in the **VirusScan Console** task list.

- 3 Accept the default task name or type a new name for your task, then press ENTER to open the **AutoUpdate Properties** dialog box. See [Configuring a mirror task on page 180](#) for detailed configuration information.

## Configuring a mirror task

You can configure and schedule a mirror task to meet your requirements.

- 1 Open the **VirusScan Console**. See *VirusScan Console* on page 19 for instructions.
- 2 Open the **AutoUpdate Properties** dialog box using one of these methods:
  - ◆ Highlight the task in the Console task list, then select **Properties** from the **Task** menu.
  - ◆ Double-click the task in the task list.
  - ◆ Right-click the task in the task list, then select **Properties**.
  - ◆ Highlight the task in the task list, then click .

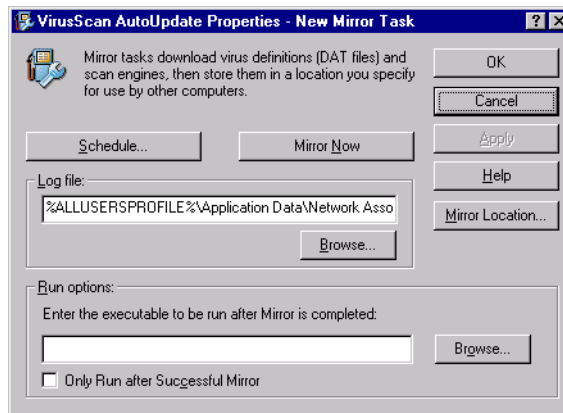


Figure 7-2. AutoUpdate Properties — New Mirror Task

### NOTE

Configure the mirror task before you **Schedule** it or perform a **Mirror Now** update.

- 3 In the **Log file** text box, accept the default log file name and location, enter a different log file name and location, or click **Browse** to locate a suitable location.

### NOTE

By default, log information is written to the VSEMIRRORLOG.TXT file in the following directory:

```
<drive>:\Winnt\Profiles\All Users\Application Data\Network Associates\Virusscan
```

- 4 Click **Mirror Location** to open the **Mirror Location Settings** dialog box:

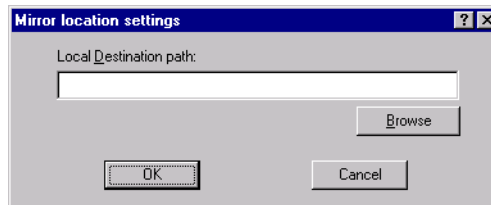


Figure 7-3. Mirror Location Settings

- a Enter the path to the destination on the local system that you are using for the mirror site, or click **Browse** to navigate to the desired location.
  - b Click **OK** to return to the **AutoUpdate Properties** dialog box.
- 5 In the **Run options** area, you can specify an executable file to start after the **mirror** task finishes running. For example, you might use this option to start a network message utility that notifies the administrator that the update operation completed successfully.

- ◆ **Enter the executable to be run after Mirror is completed.** Enter the path of the executable you want to run, or click **Browse** to locate it.
- ◆ **Only Run after Successful Mirror.** Run the executable program only after a successful update. If the update is not successful, the program you selected does not run.

**NOTE**

The program file that you specify must be executable by the currently logged on user. If the currently logged on user does not have access to the folder containing the program files, or if there is no currently logged on user, the program does not run.

- 6 Click **Schedule** to schedule the mirror task. See [Scheduling Tasks on page 199](#) for more information about scheduling tasks.
- 7 Click **Apply** to save your changes.
- 8 If you want to run the mirror task immediately, click **Mirror Now**.
- 9 Click **OK** to close the **AutoUpdate Properties** dialog box.

**NOTE**

The **Mirror** task uses the configuration settings in the repository list to perform the update. See [AutoUpdate repository list on page 184](#) for more information.

## Running mirror tasks

Once you have configured the mirror task with the properties you want, you can run the mirror task using one of these methods:

- **Mirror as scheduled.** If you scheduled the mirror task, allow it to run unattended.


### NOTE

Your computer must be active to run a mirror task. If your computer is not operating when the task is scheduled to start, the task starts at the next scheduled time if the computer is active, or when the computer starts if you selected the **Run missed task** option on the **Schedule Settings, Schedule** tab.

- **Mirror immediately.** There are two methods of starting mirror tasks immediately:
  - ◆ Start command for mirror tasks.
  - ◆ Mirror Now command for mirror tasks.

### Start command for mirror tasks

You can use **Start** from the **VirusScan Console** to immediately start any mirror task.

- 1 Open the **VirusScan Console**. See [VirusScan Console on page 19](#) for instructions.
- 2 Use one of these methods to start an immediate mirror update from the **VirusScan Console**:
  - ◆ Highlight the task in the Console task list, then select **Start** from the **Task** menu.
  - ◆ Right-click the task in the task list, then select **Start**.
  - ◆ Highlight the task in the task list, then click .
  - ◆ When the task finishes, click **Close** to exit the **McAfee Updater** dialog box, or wait for the dialog box to close automatically.

### Mirror Now command for mirror tasks

You can use **Mirror Now** in the **AutoUpdate Properties** dialog box to immediately start any mirror task.

- 1 Open the **VirusScan Console**. See [VirusScan Console on page 19](#) for instructions.
- 2 Open the **AutoUpdate Properties** dialog box for the selected mirror task. See [Configuring a mirror task on page 180](#) for detailed information about opening the **AutoUpdate Properties** dialog box.
- 3 Click **Mirror Now** in the **AutoUpdate Properties** dialog box.
- 4 When the task finishes, click **Close** to exit the **McAfee Updater** dialog box, or wait for the dialog box to close automatically.

## Viewing the mirror task activity log

The mirror task activity log shows specific details about the updating operation. For example, it shows the updated DAT file and engine version numbers.

- 1 Open the **VirusScan Console**. See [VirusScan Console on page 19](#) for instructions.
- 2 Use either of these methods to open the activity log file:
  - ◆ Highlight the task, then select **Activity Log** from the **Task** menu.
  - ◆ Right-click the task in the task list and select **View Log**.
- 3 To close the activity log, select **Exit** from the **File** menu.

## AutoUpdate repository list

You can use the AutoUpdate repository list to download the most recent DAT file updates, scanning engine upgrades, HotFixes, and/or product upgrades.

The AutoUpdate repository list specifies repositories and configuration information necessary to perform an update task. For example:

- Update repository information and location.
- Proxy server information.
- Logon credentials for client computers to access the repositories and retrieve updates.

The VirusScan Enterprise software comes with two repository lists which are configured to download from the following sites:

<ftp://ftp.nai.com/commonupdater>

<http://download.nai.com/products/commonupdater>

You can use either of these sites to download the latest updates if you are using VirusScan Enterprise 7.0 exclusively, or if you are using VirusScan Enterprise 7.0 in a mixed environment with VirusScan 4.5.1 or NetShield 4.5.

The FTP repository is the default site. The HTTP repository is the fallback site. If you use the AutoUpdate repository list the way it comes configured, updates tasks will try to download from the FTP site first. If the update from the FTP site fails, it will try to download from the HTTP site. You can move the sites in the list, change the configuration, or remove one or both of the FTP and HTTP sites.

If you want to import a customized AutoUpdate repository list, specify source repositories to obtain software from, or use multiple update locations that can replicate from a master repository, you must use the McAfee AutoUpdate Architect™ utility in conjunction with VirusScan Enterprise. Refer to the *McAfee AutoUpdate Architect Product Guide* for more information.

The following topics are covered in this section:

- Importing the AutoUpdate repository list
- Editing the AutoUpdate repository list

## Importing the AutoUpdate repository list

To import an AutoUpdate repository list from another location:

- 1 Open the **VirusScan Console**. See *VirusScan Console* on page 19 for instructions.
- 2 Select **Tools | Import AutoUpdate Repository List**.

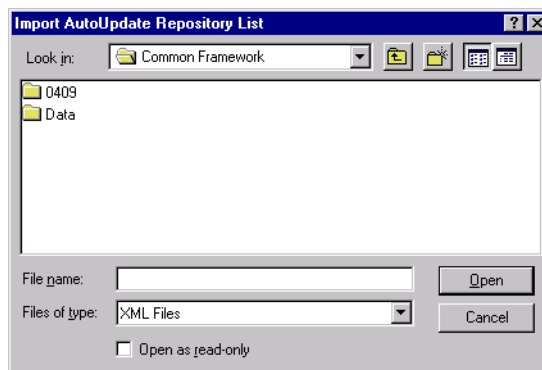



Figure 7-4. Import AutoUpdate Repository List

- 3 In the **Look in** box, enter the location for the .XML file, or click  to navigate to the location, then select the file.
- 4 Click **Open** to import the AutoUpdate repository list.

## Editing the AutoUpdate repository list

Use the **Edit AutoUpdate Repository List** dialog box to add new AutoUpdate repositories to the list, configure them, edit and remove existing repositories, and organize the repositories in the list.

The following topics are covered in this section:

- Adding and editing AutoUpdate repositories
- Removing and reorganizing repositories
- Specifying proxy settings

### Adding and editing AutoUpdate repositories

AutoUpdate repositories can be added to the list from this dialog box. You can also create repositories using McAfee AutoUpdate Architect™ and export them to VirusScan Enterprise. See the *McAfee AutoUpdate Architect Product Guide* for more information about using it to create and export AutoUpdate repositories.

AutoUpdate repositories can have a state of *Enabled* or *Disabled*. Each repository can have an additional state of *Fallback* or *read-only*.

- A fallback repository can be used to update if other AutoUpdate repositories are not available. A fallback repository is always listed at the bottom of the list. The Network Associates HTTP download site is a fallback repository by default.
- A read-only repository cannot be edited. Read-only repositories are only visible in the list if McAfee AutoUpdate Architect™ was used to create the repository.

### NOTE

The McAfee AutoUpdate Architect utility also has the ability to hide repositories so that they do not show in the VirusScan Enterprise AutoUpdate repository list.

To add or edit a repository in the AutoUpdate repository list:

- 1 Open the **VirusScan Console**. See [VirusScan Console on page 19](#) for instructions.
- 2 Select **Tools | Edit AutoUpdate Repository List**.

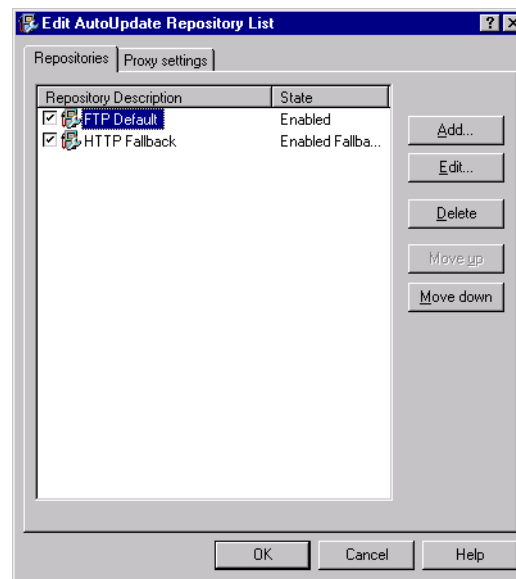


Figure 7-5. Edit AutoUpdate Repository List — Repositories tab

- 3 Select the **Repositories** tab. *The FTP repository is the default site. The HTTP repository is the fallback site.*

- 4 To add or edit an AutoUpdate repository list, choose from the following:
  - ◆ To add a repository, click **Add** to open the **Repository Settings** dialog box.
  - ◆ To edit a repository, highlight it in the **Repository Description** list, then click **Edit** to open the **Repository Settings** dialog box.

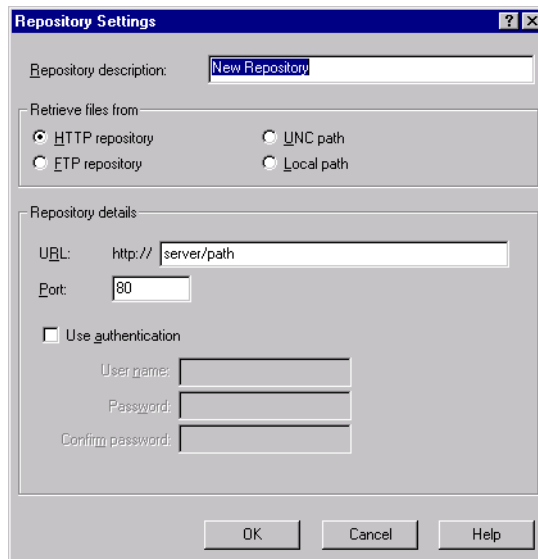


Figure 7-6. Repository Settings

- 5 In the **Repository description** box, enter the name or description for this repository.
- 6 In the **Retrieve files from** area, select the repository type or path from the following choices:
  - ◆ **HTTP repository.** *This option is selected by default.* Use the HTTP repository location you designate below as the repository from which you retrieve the update files.
  - ◆ **FTP repository.** Use the FTP repository location you designate below as the repository from which you retrieve the update files.
  - ◆ **UNC path.** Use the UNC path you designate below as the repository from which you retrieve the update files.
  - ◆ **Local path.** Use the local site you designate below as the repository from which you retrieve the update files.

- 7 In the **Repository details** area, the information you enter depends on the repository type or path you selected in the **Retrieve files from** area. Choose from the following:
  - ◆ If you selected **HTTP repository** or **FTP repository** see [HTTP or FTP repository details on page 188](#) for detailed instructions.
  - ◆ If you selected **UNC path** or **Local path** see [UNC path or Local path repository details on page 190](#) for detailed instructions.

### HTTP or FTP repository details

If you selected HTTP or FTP repository, follow these steps.

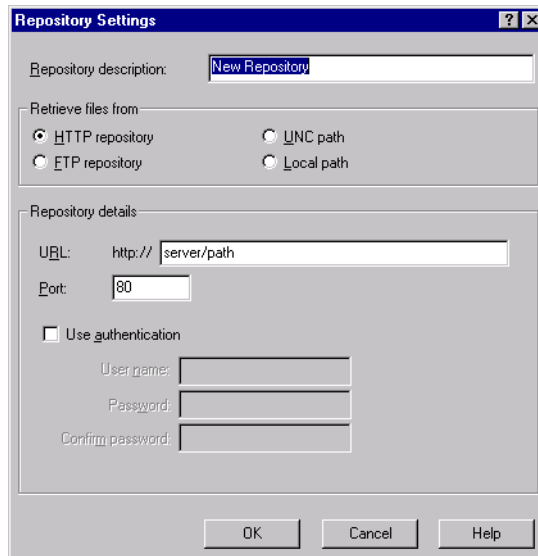


Figure 7-7. Repository details — HTTP or FTP site

- 1 In the **Repository details** area, enter the path to the repository you selected, the port number, and specify security credentials for accessing the repository.
  - ◆ **URL.** Enter the path to the HTTP or FTP repository location as follows:
    - ◆ **HTTP.** Enter the location for the HTTP server and directory where the update files are located. The default McAfee HTTP repository for DAT file updates is located at:  
<http://download.nai.com/products/commonupdater>
    - ◆ **FTP.** Enter the location for the FTP server and directory where the update files are located. The default McAfee FTP repository for DAT file updates is located at:  
<ftp://ftp.nai.com/commonupdater>
  - ◆ **Port.** Enter the port number for the HTTP or FTP server you selected.
  - ◆ **Use authentication or Use anonymous login.** *The title differs depending on whether you have selected HTTP path or FTP path.* Specify security credentials for accessing the repository. Next enter a **User name** and **Password**, then **Confirm password**.
- 2 Click **OK** to save your changes and return to the **AutoUpdate Repositories List** dialog box.

### UNC path or Local path repository details

If you selected UNC or Local path, follow these steps.

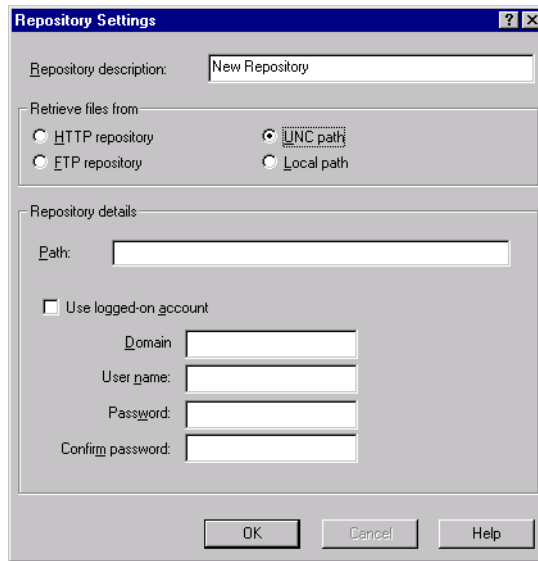


Figure 7-8. Repository details — UNC or Local path

- 1 In the **Repository details** area, enter the path to the repository you selected and determine if you want to use the logged on account or add security by specifying a user name and password.
  - ◆ **Path.** Enter path to the location from which you want to retrieve the update files.
    - ◆ **UNC path.** Using UNC notation (`\\servername\path\`), enter the path of the repository where the update files are located.
    - ◆ **Local path.** Enter the path of the local folder in which you have placed the update files, or click **Browse** to navigate to the folder.
  - ◆ **Use logged on account.** Determine which account you want to use. Choose from these options:
    - ◆ Select **Use logged on account** to use the account that is currently logged on.
    - ◆ Deselect **Use logged on account** to use a different account, then enter the **Domain**, **User name**, **Password**, and **Confirm password**.
- 2 Click **OK** to save your changes and return to the **AutoUpdate Repositories List** dialog box.

## Removing and reorganizing repositories

To remove or reorganize repositories in the repository list, follow these steps:

- 1 Open the **VirusScan Console**. See [VirusScan Console on page 19](#) for instructions.
- 2 Select **Tools | Edit AutoUpdate Repository List**.

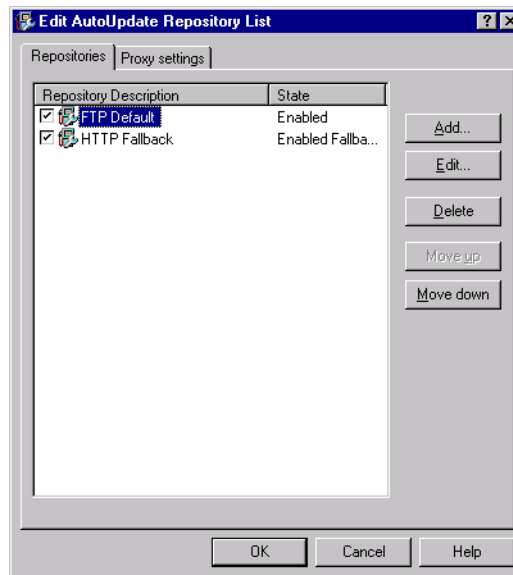


Figure 7-9. Edit AutoUpdate Repository List — Repositories tab

- 3 Select the **Repositories** tab.
- 4 To remove or reorganize repositories in the repository list, choose from the following:
  - ◆ To remove a repository, highlight it in the list, then click **Delete**.
  - ◆ To reorganize the repositories in the list, highlight a repository, then click **Move up** or **Move down** repeatedly until the repository has moved to the place in the list that you want it.

### NOTE

The order in which the repositories are listed, is the order in which they are accessed during an update operation.

## Specifying proxy settings

If your network uses a proxy server, you can specify which proxy settings to use, the address of the proxy server, and determine if you want to use authentication. The proxy settings you configure here apply to all the repositories in this repository list.

To specify proxy settings, follow these steps:

- 1 Open the **VirusScan Console**. See [VirusScan Console on page 19](#) for instructions.
- 2 Select **Tools | Edit AutoUpdate Repository List**.
- 3 Select the **Proxy settings** tab.

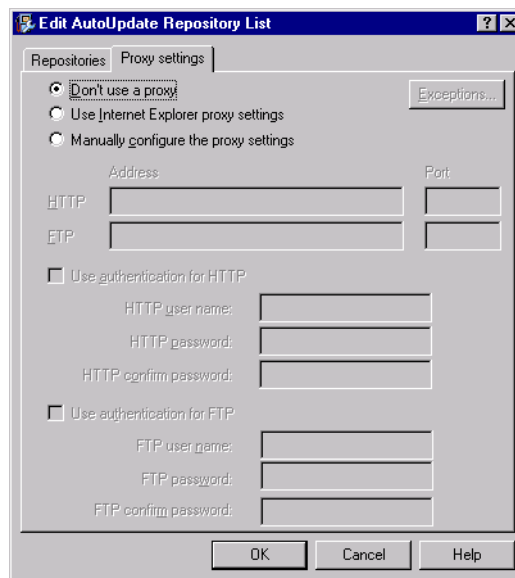


Figure 7-10. Edit AutoUpdate Repository List — Proxy settings tab

- 4 Determine whether you want to use a proxy, and if you do, which settings do you want to use. Choose from these options:
  - ◆ **Don't use a proxy.** *This option is selected by default.* Do not specify a proxy server. Select this option then click **OK** to save your settings and close the **Edit AutoUpdate Repository List** dialog box.
  - ◆ **Use Internet Explorer proxy settings.** Use the proxy settings for the currently installed version of Internet Explorer. Select this option then click **OK** to save your settings and close the **Edit AutoUpdate Repository List** dialog box.
  - ◆ **Manually configure the proxy settings.** Configure the proxy settings to meet your specific needs.

Select this option, then enter the address and port, information for the repository you selected as follows:

- ◆ **HTTP Address.** Enter the address of the HTTP proxy server.
- ◆ **HTTP Port.** Enter the port number of the HTTP proxy server.
- ◆ **FTP Address.** Enter the address of the FTP proxy server.
- ◆ **FTP Port.** Enter the port number of the FTP proxy server.

Determine if you want to use authentication for either the HTTP or FTP proxy server you specified. Choose from these options:

- ◆ **Use authentication for HTTP.** Select this option to add authentication to the HTTP proxy then enter the **HTTP user name**, **HTTP password**, and **HTTP confirm password**.
  - ◆ **Use authentication for FTP.** Select this option to add authentication to the FTP proxy server, then enter the **FTP user name**, **FTP password**, and **FTP confirm password**.
- 5 Click **Exceptions** to specify proxy exceptions. If you do not want to specify exceptions, skip this step and go to [Step 6](#).

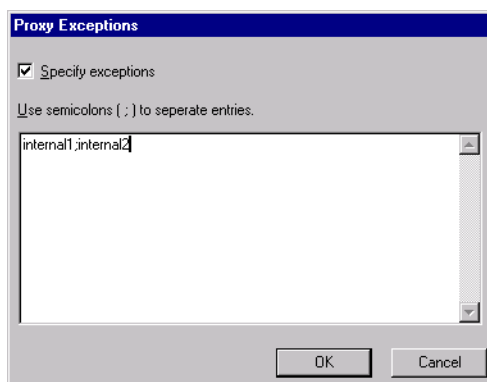


Figure 7-11. Proxy Exceptions

- a Select **Specify exceptions**, then enter the exceptions using semicolons to separate the entries.
  - b Click **OK** to save your changes and return to the **Proxy settings** tab.
- 6 Click **OK** to save your changes and close the **Edit AutoUpdate Repository List** dialog box.

## Rollback DAT files

You can use this feature to roll back the DAT files to the last backed up version, if you find that the current DAT files are corrupt or incompatible for some reason. Whenever DAT files are rolled back, the rejected DAT version is stored in the registry. The next time an update is performed, the DAT version in the registry is compared with the DAT files on the update repository. If the new DAT files are the same as the ones marked as rejected, no update occurs.

To roll back the DAT files, follow these steps:

- 1 Open the **VirusScan Console**. See [VirusScan Console on page 19](#) for instructions.
- 2 Select **Tools | Rollback DATs**. The **McAfee Updater** dialog box opens.

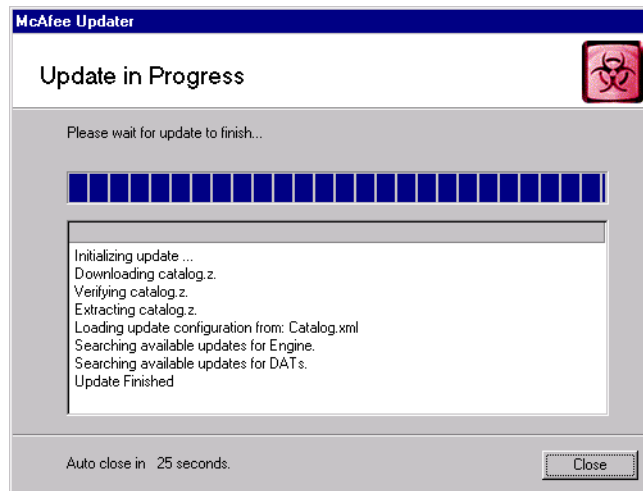


Figure 7-12. Rollback DATs — Update in Progress

- 3 The roll back appears to be the same as an update, except that the details show *Performing DAT rollback*. When the roll back finishes, click **Close** to exit the **McAfee Updater** dialog box, or wait for the dialog box to close automatically.

### NOTE

When you perform a rollback, the last backup of the DAT files is restored.

## Manual updates

McAfee recommends that you use the AutoUpdate task supplied with the VirusScan Enterprise software to install new DAT file versions. This utility offers an easy method for correctly updating DAT files. If you want to install DAT files yourself, however, you can download DAT files manually from the following update sites:

<http://www.mcafeeb2b.com/naicommon/download/dats/find.asp>

<ftp://ftp.nai.com/pub/antivirus/datfiles/4.x>

- **Regular DAT files.** McAfee stores these files on its FTP site as .ZIP archives with the name DAT-XXX.ZIP. The XXXX in the file name is a series number that changes with each DAT file release. To download these files, use a web browser or FTP client to connect with:

<ftp://ftp.nai.com/pub/antivirus/datfiles/4.x>

- **Installable .EXE files.** McAfee stores these files on its website as a self-executing setup file named XXXXUPDT.EXE. Here, too, the XXXX is a series number that changes with each new virus definition file release. To download these files, use a web browser to connect with:

<http://www.mcafeeb2b.com/naicommon/download/dats/find.asp>

Both files contain exactly the same virus definition files. The difference between them is in how you use them to update your copy of the VirusScan Enterprise software.

To use the DAT-XXXX.ZIP archive, you must download the file, extract it from its archive, copy the files into the DAT directory, then restart the on-access scanner. See [Updating from DAT file archives on page 197](#) for detailed steps.

To install DAT files that come with their own setup utility, you need only to download the files to a temporary directory on your hard disk, then run or double-click the XXXUPDT.EXE file. The setup utility stops the on-access scanner, copies the files to the correct directory, then restarts the on-access scanner.

### NOTE

You may need administrator rights to write to the DAT directory.

Once updated, the new DAT files are picked up by the on-access scanner, the on-demand scanner, and the e-mail scanner, the next time each scanner starts.

---

## Updating from DAT file archives

To install DAT file updates directly from a .ZIP archive *without* using AutoUpdate, follow the steps below.

- 1 Create a temporary directory on your hard disk, then copy the DAT file .ZIP archive you downloaded to that directory.
- 2 Back up or rename these existing DAT files.
  - ◆ CLEAN.DAT
  - ◆ NAMES.DAT
  - ◆ SCAN.DAT

If you accepted the default installation path, these files are located in:

drive:\Program Files\Common Files\Network Associates\Engine

- 3 Use WINZIP, PKUNZIP, or a similar utility to open the .ZIP archive and extract the updated DAT files.
- 4 Log on to the server you want to update. You must have Administrator rights for the destination computer.
- 5 Copy the DAT files to the DAT directory.
- 6 Disable on-access scanning, then re-enable it.
- 7 Stop Microsoft Outlook, then restart it.
- 8 Stop on-demand scan tasks, then restart them.