## Introduzione

Il grande successo delle reti di comunicazione negli ultimi anni, e in particolar modo la vertiginosa crescita di Internet, hanno reso enormemente popolare l'uso della posta elettronica.

Uno dei maggiori vantaggi della posta elettronica è la possibilità di spedire e ricevere dei file. Ma, proprio per questo motivo, la posta elettronica costituisce anche una nuova porta di entrata per i virus.

Lo scambio di documenti per posta elettronica è molto frequente. Ciò ha reso possibile, in grande misura, l'enorme espansione di virus di Word e Excel. Ma non va dimenticato che attraverso la posta elettronica è possibile spedire e ricevere anche qualsiasi tipo di virus, e non solamente quelli di Word e Excel.

Gli antivirus convenzionali non sono stati preparati per poter realizzare una individuazione e disinfezione efficace dei virus veicolati dai messaggi di posta elettronica, e questo per i seguenti motivi:

1. Normalmente i messaggi di posta elettronica vengono immagazzinati in una base di dati della posta con un formato proprio e con tecniche di compressione e/o codificazione che rendono impossibile l'analisi mediante antivirus convenzionali.

2. È molto frequente che i messaggi di posta elettronica con i realtivi file vengano salvati in un server a cui un antivirus convenzionale non può avere accesso.

Per questi motivi, un antivirus per posta elettronica deve essere disegnato specificamente per individuare e eliminare virus nell'ambito della posta elettronica. Le caratteristiche principali che deve avere un antivirus per posta elettronica sono:

- Analisi dei messaggi nel momento stesso della loro ricezione in modo totalmente automatico.
- Analisi automatica di ogni messaggio nel momento in cui viene aperto.
- Analisi automatica del messaggio che si cerca di spedire. In questo modo si evita la possibilità di inviare messaggi contaminati da virus.
- Analisi automatica di ogni messaggio salvato.
- Analisi di tutti i messaggi della posta in qualsiasi momento su richiesta dell'utente.
- Integrazione con il programma di posta elettronica.
- Possibilità di analizzare file compressi.
- Possibilità di analizzare messaggi nascosti (messaggi dentro altri messaggi).

Panda Antivirus per Exchange/Outlook è un antivirus per posta elettronica che possiede tutte le caratteristiche descritte e molte altre che ne completano la funzionalità, facendo di esso uno strumento potente anche se con molte possibilità di essere configurato, e che evita ogni rischio nel lavoro con i messaggi di posta elettronica.

NOTA
In questo manuale vengono spiegati i seguenti prodotti:

- Panda Antivirus Exchange/Outlook
- Panda Antivirus Exchange/Outlook Network Client

Il primo permette di installare Panda Antivirus Exchange/Outlook in un computer in modo diretto. Il secondo permette la distribuzione del menzionato antivirus a tutte le stazioni di una rete semplificando così il compito dell'amministratore della rete.

Fare riferimento alla parte del manuale corrispondente al prodotto acquistato.

## Installazione

### Requisiti

Panda Antivirus Exchange/Outlook richiede:

- Computer IBM compatibile in grado di eseguire Windows 95, 98 o Windows NT Workstation 3.51 o 4.0.
- MS-Exchange e/o MS-Outlook
- 3 Mb disponibili su disco rigido.

### Installazione

Per installare Panda Antivirus Exchange/Outlook bisogna inserire il disco numero 1 nel floppy e eseguire il programma SETUP.EXE.

Il processo di installazione è costituito da una serie di finestre in cui vengono chiesti i dati necessari per portare a termine l'installazione.

Una volta terminata l'installazione, si consiglia di riavviare il computer. L'antivirus per Exchange/Outlook non entrerà in funzionamento fino a quando verrà nuovamente avviato Exchange/Outlook.

### Disinstallazione

Per disinstallare Panda Antivirus Exchange/Outlook è necessario chiudere il programma di posta Exchange/Outlook, andare nel *Pannello di Controllo*, scegliere l'opzione *Installazione applicazioni* e scegliere dalla lista Panda Antivirus Exchange/Outlook. Una volta fatto ciò, premere il pulsante *Aggiungi/Rimuovi*. In brevi istanti verrà portata a termine la disinstallazione. Non bisogna cercare di disinstallare questa versione cancellando la cartella in cui è stata installata, ma effettuare la disinstallazione sempre seguendo il procedimento indicato.

## Come analizzare con Panda Antivirus Exchange/Outlook

### Analisi su richiesta

Per analizzare una determinata cartella, bisogna selezionarla. Se si sceglie una cartella che contiene altre cartelle (per esempio, una casella), verranno analizzate tutte le cartelle che dipendono da quella scelta. Una volta selezionata la cartella, premere il pulsante Analizza nella barra degli strumenti standard del programma MS-Exchange/Outlook o selezionare l'opzione Analizza per individuare virus nell'opzione "Strumenti" nel menù principale di MS- Exchange/Outlook.

Una volta terminata l'analisi, sarà possibile vedere un resoconto dei risultati in cui viene specificata qualsiasi incidenza riscontrata durante l'analisi.

Panda Antivirus Exchange/Outlook permette inoltre di analizzare uno o più messaggi. Per fare ciò, selezionare il messaggio o messaggi che si vogliono analizzare. Una volta selezionati, premere il pulsante di analisi su richiesta per iniziare l'analisi.

Per selezionare più messaggi, cliccare su questi mantenendo premuto il tasto Control. Se si desidera selezionare un gruppo di messaggi, selezionare il primo e cliccare sull'ultimo mantenendo premuto il tasto Shift.

## Protezione in tempo reale

La protezione permanente permette di lavorare con la massima tranquillità con la propria posta senza preoccuparsi dei virus, dal momento che Panda Antivirus Exchange/Outlook controllerà tutte le operazioni sospette realizzate.

La protezione permanente si preoccupa di analizzare per individuare virus in:

- Tutti i nuovi messaggi che si ricevono.
- Tutti i messaggi che si desidera spedire.
- Tutti i messaggi che vengono aperti, indipendentemente dal fatto che siano stati ricevuti prima o dopo l'installazione dell'antivirus.
- Tutti i messaggi che si desidera salvare.

La protezione permanente può essere attivata o disattivata con facilità, premendo o rilasciando il pulsante dedicato a tale scopo nella barra degli strumenti standard di MS-Exchange/Outlook.

Panda Antivirus Exchange/Outlook è in grado di analizzare file compressi e messaggi nascosti (messaggi dentro altri messaggi), offrendo in tal modo i più alti livelli di protezione.

## Funzionamento di Panda Antivirus Exchange/Outlook

Panda Antivirus Exchange/Outlook si integra completamente con il programma MS-Exchange/Outlook. Pertanto, tutta la gestione dell'antivirus viene condotta dallo stesso programma di posta.

Panda Antivirus Exchange/Outlook aggiunge quattro pulsanti alla barra degli strumenti standard di MS-Exchange/Outlook. Questi quattro pulsanti sono:

**Analizza**: questo pulsante inizia un'analisi della cartella o dei messaggi selezionati nel momento in cui bisogna iniziare l'analisi. Verranno analizzate tutte le cartelle secondarie che verranno trovate all'interno della cartella scelta. È possibile seguire il processo di analisi attraverso una finestra che visualizza l'insieme di cartelle oggetto di analisi, la cartella che si sta analizzando in quel momento e una barra di avanzamento.

**Resoconto dei risultati**: questo pulsante visualizza il resoconto delle incidenze riscontrate dall'antivirus. Questo resoconto viene conservato fra una sessione all'altra fino a quando l'utente decide di cancellarla.

**Attiva o disattiva l'antivirus**: questo pulsante permette di attivare o disattivare la protezione permanente di Panda Antivirus. Se si disattiva tale protezione, il programma Panda Antivirus Exchange/Outlook non analizzerà i nuovi messaggi in arrivo e in uscita per individuarne gli eventuali virus. Non effettuerà nemmeno l'analisi per individuare i virus di quei messaggi che vengono aperti per essere letti. Tuttavia potrà continuare ad analizzare una determinata cartella o messaggio in qualsiasi momento mediante il pulsante *Analizza*. L'analisi all'avvio del programma Exchange/Outlook verrà portata a termine anche se è stata disattivata la protezione permanente.

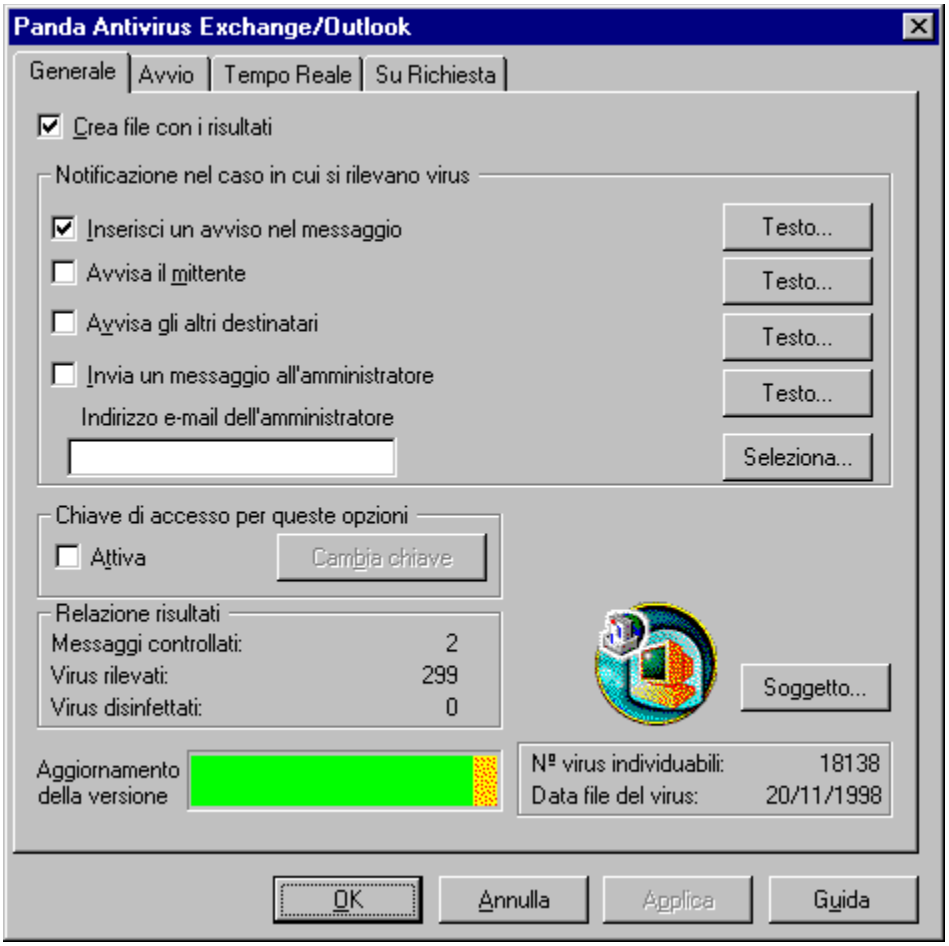
**Configura**: questo pulsante visualizza la finestra di configurazione di Panda Antivirus Exchange/Outlook. Mediante questa finestra, è possibile configurare il comportamento generale dell'antivirus, il suo comportamento all'avvio del programma di posta e il suo comportamento come protezione permanente e come protezione su richiesta. Inoltre è possibile procedere alla configurazione di Panda Antivirus Exchange/Outlook scegliendo *Opzioni* in *Strumenti* dal menù principale di MS-Exchange/Outlook. In questa finestra appare una pagina chiamata Panda Antivirus Exchange/Outlook mediante la quale è possibile configurare l'antivirus.

### Configurazione di Panda Antivirus Exchange/Outlook

Panda Antivirus Exchange/Outlook permette un'ampia configurazione per ciascuna delle sue funzioni. La finestra di configurazione è divisa in varie pagine, e ciascuna di esse si riferisce a una parte in concreto dell'antivirus.

### Generale

Le opzioni raggruppate in questa pagina sono di ambito generale e condizionano il comportamento dell'antivirus in tutti i casi. Sono le seguenti:




**Crea file dei risultati**. Se si seleziona questa opzione, tutte le operazioni di analisi dell'antivirus registreranno le varie incidenze in un file dei risultati.

**Inserisci un avviso nel messaggio**. Se si seleziona questa opzione, ogni volta che si individua un virus in un messaggio verrà aggiunto un testo a tale messaggio come avvertimento. Tale messaggio verrà aggiunto indipendentemente dalla azione che si è deciso di compiere una volta individuato un virus. Il messaggio può essere personalizzato, e quindi permette all'utente di inserire ciò che desidera.

**Avvisa il mittente**. Se si seleziona questa opzione, ogni volta che viene individuato un virus in un messaggio verrà inviato un messaggio al mittente del messaggio infetto per informarlo in merito. Il testo del messaggio che riceverà il mittente è totalmente configurabile e può quindi essere personalizzato.

**Avvisa gli altri destinatari**. Se si seleziona questa opzione, quando si individua un virus in un messaggio verrà inviato un messaggio agli altri destinatari del messaggio contaminato, se ve ne sono. In questo modo è possibile avvertire utenti che forse non sono protetti da virus. Il testo del messaggio che riceveranno gli altri destinatari può essere personalizzato.

**Invia un messaggio all'amministratore**. Se si seleziona questa opzione e si specifica l'indirizzo di posta elettronica dell'amministratore, ogni volta che si individua un virus in un messaggio verrà inviato un messaggio di avvertimento all'amministratore del sistema. Il testo del menzionato messaggio di avvertimento può essere completamente personalizzato.

**Attiva chiave**. Se si seleziona questa opzione, la configurazione di Panda Antivirus Exchange/Outlook rimarrà protetta mediante una chiave. In questo modo, nessun utente non autorizzato potrà modificare la configurazione dell'antivirus.

**Cambia chiave**. Questo pulsante permette di cambiare la chiave con cui è stata protetta la configurazione Panda Antivirus Exchange/Outlook.

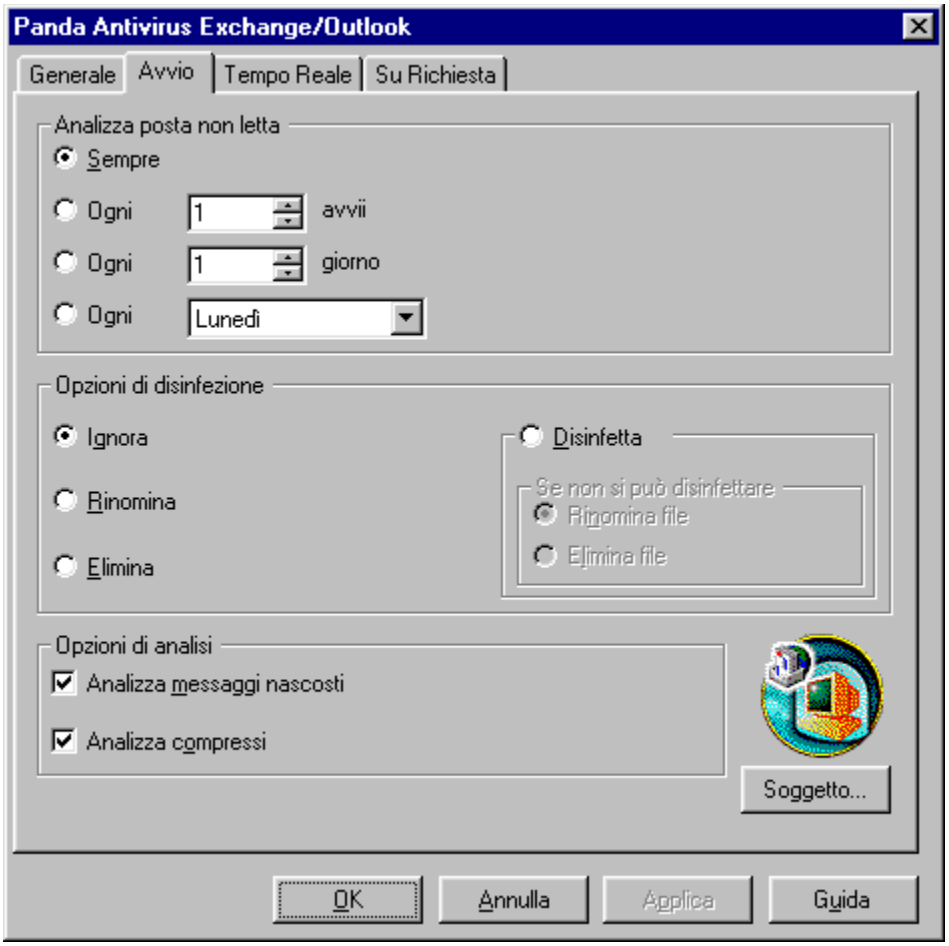
**Resoconto dei risultati**. In tale opzione vengono visualizzate delle informazioni circa i messaggi analizzati, il numero dei virus individuati e di quelli disinfettati.

**Aggiornamento della versione**. Qui viene mostrato in modo grafico il livello di aggiornamento dell'antivirus.

**Dati relativi alla versione**. Il numero di virus individuabili e la data del file dei virus forniscono informazioni circa la versione dell'antivirus installata.

## Avvio

Da qui è possibile configurare il comportamento dell'antivirus nel momento in cui si avvia il programma di posta elettronica MS-Exchange/Outlook. Le opzioni disponibili sono le seguenti:




**Analizza sempre la posta non letta:** Se si seleziona questa opzione, ogni volta che viene avviato MS-Exchange/Outlook verranno analizzati tutti i messaggi della cartella della posta in arrivo non ancora letti.

**Analizza la posta non letta dopo un certo numero di avvii:** Se si seleziona questa opzione, i messaggi non letti della cartella della posta in arrivo verranno analizzati ogni volta che si raggiunge il numero indicato di avvii del programma di posta.

**Analizza la posta non letta dopo un determinato periodo di tempo:** Se si seleziona questa opzione, l'analisi dei messaggi non letti della cartella della posta in arrivo verrà effettuata solamente quando sarà trascorso il numero di giorni indicato.

**Analizza la posta in determinati giorni:** Se si seleziona questa opzione, verranno analizzati i messaggi non letti della cartella della posta in arrivo solo il giorno della settimana scelto.

**Disinfezione** – **Ignora:** se si seleziona questa opzione, quando si individua un virus l'antivirus non compirá nessuna azione.

**Disinfezione** – **Rinomina:** se si seleziona questa opzione, quando si individua un virus l'antivirus rinominerà il file contaminato da virus.

**Disinfezione** – **Elimina:** se si seleziona questa opzione, quando si individua un virus l'antivirus procederà all'eliminazione del file infetto.

**Disinfezione** – **Disinfetta:** se si seleziona questa opzione, quando si individua un virus l'antivirus cercherà di disinfettare il file infetto.

**Disinfezione - Se non si può disinfettare, rinomina:** se l'antivirus non può disinfettare un fileinfetto, procederà a rinominare tale file.

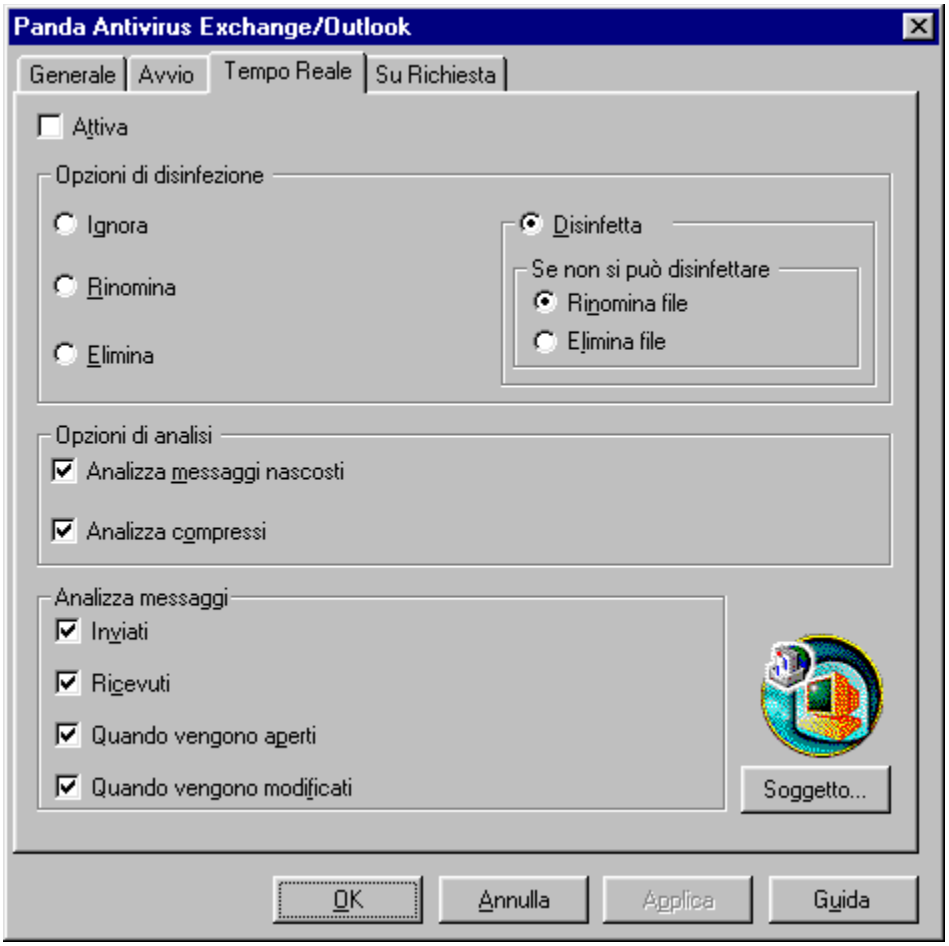
**Disinfezione - Se non si può disinfettare, elimina:** se l'antivirus non può disinfettare un file infetto, procederà alla sua eliminazione.

**Analizza messaggi nascosti:** se si seleziona questa opzione verranno analizzati i messaggi nascosti. In altre parole, se si individua un messaggio all'interno di un altro messaggio, entrambi verranno analizzati. Il numero di livelli di messaggi che si possono analizzare dipende dalle risorse del computer.

**Analizza compressi:** se si seleziona questa opzione e si individua un file compresso si procederà alla sua analisi come se si trattasse di un file normale.

### Tempo reale

Permette di configurare la protezione permanente offerta dall'antivirus. Le opzioni disponibili sono le seguenti:




**Attiva**: se si seleziona questa opzione verrà attivata la protezione permanente. Vale a dire che verranno automaticamente analizzati tutti i messaggi in arrivo e in uscita, aperti o salvati.

**Disinfezione - Ignora**: se si seleziona questa opzione e si individua un virus l'antivirus non porterà a termine nessuna azione.

**Disinfezione - Rinomina**: se si seleziona questa opzione e si individua un virus l'antivirus rinominerà il file contaminato da virus.

**Disinfezione - Elimina**: se si seleziona questa opzione e si individua un virus l'antivirus procederà all'eliminazione del file infetto.

**Disinfezione - Disinfetta**: se si seleziona questa opzione e si individua un virus l'antivirus cercherà di disinfettare il file infetto.

**Disinfezione - Se non si può disinfettare, rinomina**: se l'antivirus non può disinfettare un file contaminato procederà a rinominare tale file.

**Disinfezione - Se non si può disinfettare, elimina**: se l'antivirus non può disinfettare un file infetto procederà all'eliminazione del menzionato file.

**Analizza messaggi nascosti**: se si seleziona questa opzione verranno analizzati i messaggi nascosti. Vale a dire, se si individua un messaggio dentro un altro verranno analizzati entrambi i messaggi. Il numero di livelli di messaggi che si possono analizzare dipende dalle risorse del computer.

**Analizza compressi**: se si seleziona questa opzione e si individua un file compresso si procederà alla sua analisi come se si trattasse di un file normale.

**Analizza messaggi spediti**: se si seleziona questa opzione verranno analizzati i messaggi che si desidera inviare prima che vengano spediti. In questo modo si evita la spedizione di file contaminati.

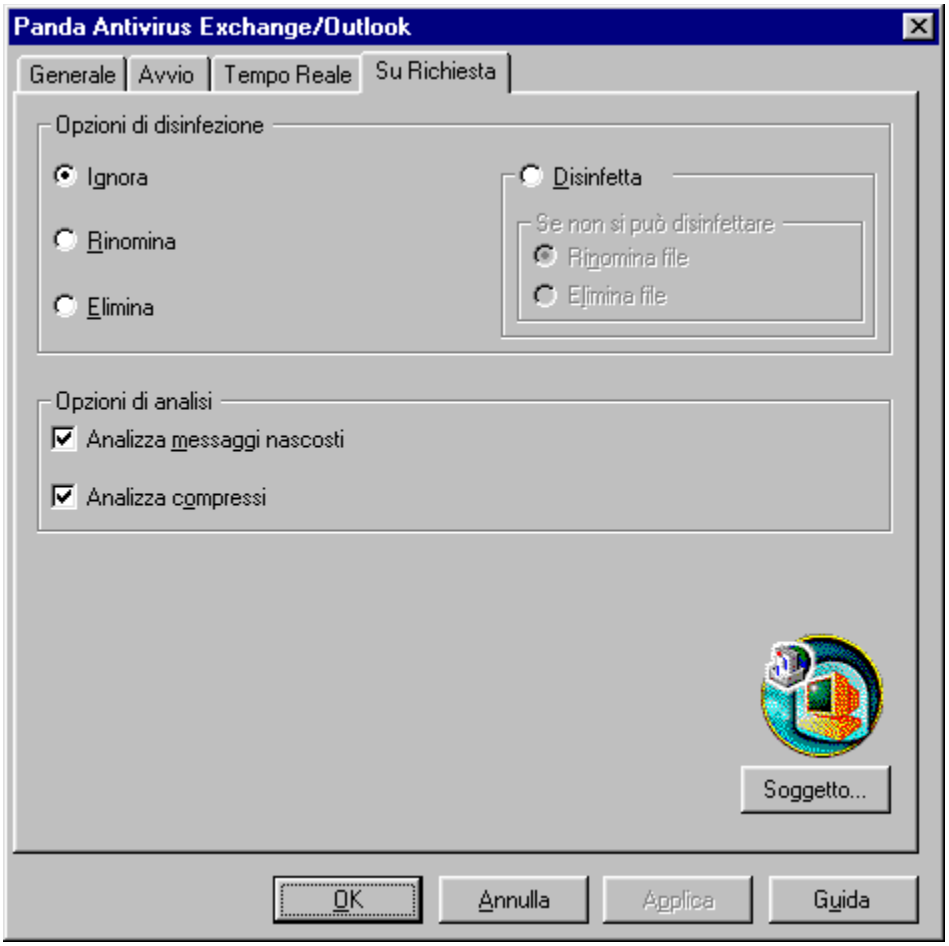
**Analizza messaggi ricevuti**: se si seleziona questa opzione verranno analizzati tutti i messaggi che vengono ricevuti nel momento stesso della loro ricezione, ancor prima che vengano aperti.

**Analizza messaggi quando si aprono**: se si seleziona questa opzione verranno analizzati tutti quei messaggi che si aprono, indipendentemente da quando siano stati ricevuti.

**Analizza messaggi quando si modificano**: se si seleziona questa opzione verranno analizzati tutti i messaggi che vengono salvati.

### Su richiesta

In questa pagina è possibile configurare l'analisi su richiesta che offre l'antivirus. Le opzioni disponibili sono le seguenti:




**Disinfezione - Ignora**: se si seleziona questa opzione e si individua un virus l'antivirus non porterà a termine nessuna azione.

**Disinfezione - Rinomina**: se si seleziona questa opzione e si individua un virus l'antivirus rinominerà il file infetto.

**Disinfezione - Elimina**: se si seleziona questa opzione e si individua un virus l'antivirus procederà all'eliminazione del file infetto.

**Disinfezione - Disinfetta**: se si seleziona questa opzione e si individua un virus l'antivirus cercherà di disinfettare il file infetto.

**Disinfezione - Se non si può disinfettare, rinomina**: se l'antivirus non può disinfettare un file contaminato, procederà a rinominare tale file.

**Disinfezione - Se non si può disinfettare, elimina**: se l'antivirus non può disinfettare un file infetto, procederà all'eliminazione del menzionato file.

**Analizza messaggi nascosti**: se si seleziona questa opzione verranno analizzati i messaggi nascosti. Vale a dire, se si individua un messaggio all'interno di un altro verranno analizzati entrambi. Il numero di livelli di messaggi che si possono analizzare dipende dalle risorse del computer.

**Analizza compressi**: se si seleziona questa opzione e si individua un file compresso si procederà alla sua analisi come se si trattasse di un file normale.

## Introduzione alla distribuzione mediante una rete

L'idea di distribuire l'antivirus mediante una rete nasce per rendere più semplice il lavoro di un amministratore di rete che desideri proteggere un insieme di postazioni in modo comodo e rapido.

Il funzionamento è il seguente:

1. L'amministratore della rete copia l'antivirus in una directory nel server o in una directory condivisa a cui abbiano accesso tutti gli utenti. Questa copia viene realizzata mediante un programma di installazione disegnato a tale proposito. Bisogna tenere in conto che NON si sta installando l'antivirus nel server, ma che semplicemente si stanno copiando i file necessari per installare l'antivirus nelle postazioni.

2. Ogni volta che una postazione viene collegata alla rete, si verificherà se possiede l'antivirus installato e aggiornato. Se è così non si farà nulla, mentre se non possiede l'antivirus installato o aggiornato si procederà all'installazione o aggiornamento dello stesso in modo totalmente automatico.

Come si può notare, il server (o risorsa condivisa) funge unicamente da mezzo di distribuzione dell'antivirus alle stazioni.

Questo procedimento globale serve praticamente per ogni genere di rete. Tuttavia in ciascuna di queste esso avviene in modo leggermente diverso. In questa documentazione si spiegherà tale procedimento per i tipi di rete più comuni oggigiorno.

## Come distribuire l'antivirus attraverso una rete

### Requisiti

Per la distribuzione di Panda Antivirus Exchange/Outlook attraverso una rete è necessario:

- Computer IBM compatibile in grado di eseguire Windows 95, 98 o Windows NT Workstation 3.51 o 4.0.
- 3 Mb disponibili sul disco rigido del server che fungerà da mezzo di distribuzione.
- 3 Mb disponibili sul disco rigido del computer in cui verrà installato l'antivirus.

### Come distribuire l'antivirus a tutti le postazioni della rete facilmente

Il processo di distribuzione dell'antivirus a tutte le postazioni della rete è costituito da due parti:

1. Copia dell'antivirus in una directory a cui possano accedere tutti gli utenti.

2. Distribuzione dell'antivirus a tutte le postazioni a mano a mano che si collegano alla rete mediante il programma RINSTALL.

Di seguito viene spiegato dettagliatamente come realizzare i due passaggi menzionati. Alcuni aspetti di questo processo di installazione richiedono delle nozioni circa il tipo di rete mediante cui verrà distribuito l'antivirus. Tutte queste nozioni vengono spiegate in dettaglio per i principali tipi di rete nelle sezioni corrispondenti, quindi si consiglia di consultarle in caso di dubbio.

### Copia dell'antivirus a una directory a cui possano accedere tutti gli utenti

Il primo passaggio nella distribuzione dell'antivirus attraverso la rete è la copia dei file in una directory di uno dei dischi rigidi del server. È molto importante tener conto del fatto che la copia dei file nel server deve essere realizzata in un ambiente privo di virus. Se così non fosse potrebbero venire contaminati i file dell'antivirus. Poihé tali file verranno distribuiti a tutte le postazioni che si collegano alla rete, anche il virus verrebbe distribuito assieme a loro. Per ottenere una copia sicura dei file e per essere sicuri che tali file non vengano contaminati in futuro da nessuna stazione, è necessario effettuare la copia in base ai seguenti passaggi:

1. L'amministratore deve assicurarsi che il suo computer sia privo di virus. Sarebbe conveniente che l'amministratore installasse l'antivirus adeguato di Panda Software nel suo computer e attivasse la relativa protezione permanente. Non si dovrebbe continuare l'installazione fino a quando non si è sicuri che il computer da cui si sta installando l'antivirus è privo virus.

2. Bisogna scegliere una directory del server corrispondente in cui copiare i file. Si consiglia di creare una nuova directory chiamata PAVEXCLI a cui abbiano diritto di lettura tutti gli utenti. È importante che nessun utente abbia diritto di *scrittura* o *cancellazione* in questa directory dal momento che se così non fosse, qualsiasi utente potrebbe, in modo accidentale o di proposito, infettare o cancellare i file dell'antivirus con le gravi conseguenze che ciò comporta.

3. Una volta creata la directory di arrivo, è sufficiente introdurre il disco numero 1 o il CD-Rom, collocarsi nell'unità corrispondente ed eseguire il programma SETUP.EXE.

Il processo di installazione è costituito da una serie di finestre in cui verranno richiesti i diversi dati necessari per portare a termine l'installazione nel computer. Uno dei dati che verranno richiesti sarà la directory d'arrivo. Bisognerà scegliere la directory creata a tale proposito affinché vengano copiati

in questa i file dell'antivirus.

**Distribuzione dell'antivirus**

È in questa fase che si può constatare il vantaggio del nostro antivirus per PC in rete. Invece di dover andare di stazione in stazione per installare l'antivirus, questo viene installato automaticamente nel momento in cui una stazione viene collegata alla rete.

Normalmente, quando una stazione si collega a una rete vengono eseguiti una serie di comandi o programmi per preparare il lavoro in rete nello stesso modo in cui si eseguono una serie di comandi o programmi una volta che viene avviato un computer. Questa serie di comandi e/o programmi è conosciuta come *Login Script* (o script di accesso).

Il nostro antivirus con capacità di distribuzione attraverso una rete, è accompagnato da un programma chiamato **RINSTALL**, che si occupa della distribuzione automatica dell'antivirus. Quindi ottenere la distribuzione automatica dell'antivirus è molto facile, basta inserire nel *Login Script* l'esecuzione di **RINSTALL**.

**RINSTALL** verrà eseguito ogni volta che una stazione si collega alla rete. La prima cosa che **RINSTALL** verifica è che la stazione collegata abbia installato l'antivirus. Se questo è installato e aggiornato non fa nulla, e prosegue l'esecuzione dei comandi rimanenti del *Login Script* normalmente. Se la stazione non ha installato l'antivirus o non lo ha aggiornato, **RINSTALL** installerà l'antivirus. Una volta fatto ciò, l'esecuzione dei comandi rimanenti del *Login Script* continuerà normalmente.

Poiché il funzionamento del **RINSTALL** è totalmente automatico, l'amministratore della rete deve solo copiare il file e modificare il *Login Script* per installare la protezione antivirus che si propagherà alle stazioni mano a mano che si collegano.

**Distribuzione dell'antivirus in una rete Novell NetWare**

Affinché l'antivirus venga distribuito automaticamente in tutte le stazioni a mano a mano che si collegano a una rete Novell NetWare, è necessario inserire la seguente stringa nel *System Login Script*:

```
#F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Consultare la sezione Novell NetWare per ottenere una spiegazione più dettagliata circa questi aspetti.

Come si può notare nell'esempio, è necessario indicare il luogo del server in cui risiedono i file dell'antivirus. Per questo la stringa dovrà essere collocata *dopo* la mappatura delle unità, per cui questa parte del *System Login Script* risulta come segue:

```
MAP ROOT F:=ALFA\SYS:
#F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

(supponendo che il server venga chiamato Alfa e che i file risiedano nel volume SYS).

**Distribuzione dell'antivirus in una rete Windows NT**

Affinché l'antivirus venga distribuito automaticamente alle stazioni della rete mano a mano che questi si collegano, è necessario aggiungere la seguente stringa al *File dei comandi di inizio sessione*

utilizzando il programma Profile Manager:

Consultare la sezione Windows NT per ottenere una spiegazione più dettagliata circa questi aspetti.

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Come si può notare nell'esempio, è necessario indicare il luogo in cui sono stati copiati i file dell'antivirus. Per questo, la stringa dovrà essere posta *dopo* la mappatura delle risorse condivise, per cui questa parte del *File dei comandi di inizio sessione* sarà:

```
NET USE F: \\ALFA\SYS
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

(supponendo che il server venga chiamato Alfa e che la risorsa condivisa venga chiamata Sys).

**Distribuzione dell'antivirus in una rete OS/2**

Affinché l'antivirus venga distribuito automaticamente alle stazioni della rete a mano a mano che questi si collegano, è necessario aggiungere la seguente stringa al file PROFILE.BAT (o PROFILE.CMD):

Consultare la sezione OS/2 per ottenere una spiegazione più dettagliata circa questi aspetti.

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Come si può notare nell'esempio, è necessario indicare il luogo in cui sono stati copiati i file dell'antivirus. Per questo la stringa dovrà essere posta *dopo* la mappatura delle risorse condivise e quindi questa parte del file PROFILE.BAT sarà:

```
NET USE F: \\ALFA\SYS
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

(supponendo che il server venga chiamato Alfa e che la risorsa condivisa venga chiamata Sys).

**Distribuzione dell'antivirus in una rete Pathworks**

Affinché l'antivirus venga distribuito automaticamente alle stazioni della rete mano a mano che questi si collegano, è necessario aggiungere la seguente stringa nella sequenza di connessione di un gruppo in cui si trovino tutti gli utenti a cui si desidera installare l'antivirus:

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Come si può notare nell'esempio, è necessario indicare il luogo in cui sono stati copiati i file dell'antivirus. Per questo, è opportuno avere definito la mappa delle unità prima di eseguire RINSTALL.

**Distribuzione dell'antivirus in una rete Banyan-Vines**

Affinché l'antivirus venga distribuito automaticamente alle stazioni della rete a mano a mano che queste si collegano, è necessario aggiungere la seguente stringa nel profilo di ciascun utente il cui computer si desidera proteggere. Il profilo di un utente è la sequenza degli ordini che vengono eseguiti ogni volta che tale utente si collega alla rete.

È sufficiente modificare questo profilo con l'ordine MUSER e aggiungere la stringa:

```
POSTLOGIN F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

se l'unità del server è stata *mappata* come F e sono stati copiati i file nella directory **PAVEXCLI**.

È particolarmente conveniente avere definito la mappa delle unità prima di eseguire **RINSTALL** per assicurarsi che il disco rigido del server sia caratterizzato da uno stesso riferimento da parte di tutte le stazioni.

Modificare uno a uno di tutti i profili dell'utente può diventare un compito molto laborioso se esistono molti utenti. Normalmente esiste un profilo comune utilizzato da tutti gli utenti. Tale profilo viene definito in base ai diversi profili degli utenti. Il comando che bisogna utilizzare per chiamare un profilo da un altro è:

```
USE Sample_Profile@gruppo@organizzazione
```

In cui *Sample_Profile* è un utente fittizio e *gruppo* e *organizzazione* sono quelli corrispondenti nella struttura di ogni impresa.

In questo modo è sufficiente apportare le adeguate modifiche al profilo *Sample_Profile* affinché abbiano effetto su tutti gli utenti che chiamano tale profilo dal loro.

**Installazione dell'antivirus in una postazione non collegata alla rete.**

Se si desidera installare Panda Antivirus Exchange/Outlook in una postazione non collegata alla rete è necessario realizzare il seguente procedimento:

1. Inserire il disco numero 1 o il CD-Rom di Panda Antivirus Exchange/Outlook, situarsi nell'unità corrispondente ed eseguire il programma SETUP.EXE. Il processo di installazione è costituito da una serie di finestre in cui vengono richiesti i dati necessari per portare a termine l'installazione nel computer. Uno dei dati che verranno richiesti sarà la directory di arrivo. Bisognerà scegliere una directory nel computer in cui si sta effettuando la installazione, e non una directory del server come è stato descritto in precedenza.

2. Una volta terminato il processo di installazione, eseguire il seguente comando:

   C:\PAVEXCLI\RINSTALL PAVEX.SCR

   (se è stato installato l'antivirus in un'altra unità o directory, indicare quella adeguata).

3. Una volta terminato il processo di distribuzione, il programma antivirus per MS-Exchange/Outlook sarà installato nel computer.

4. Eliminare la directory dove è stato installato l'antivirus nel passaggio 1, poiché non sarà più necessaria.

**Soluzione dei problemi di distribuzione**

Se l'antivirus non viene distribuito adeguatamente in uno o più computer è necessario recarsi presso tale o tali computer e verificare quanto segue:

1. Che dal computer in questione è possibile collegarsi al server in cui è stato copiato l'antivirus.

2. Provare a eseguire **RINSTALL** direttamente. Situarsi nella directory del server in cui è stato copiato l'antivirus e eseguire **RINSTALL** PAVEX.SCR.

3. Se le due verifiche precedenti non hanno dato nessun risultato, controllare lo script di accesso, e assicurarsi che sia stato modificato lo script adeguato e che la stringa corrisponda a quella specificata in questo manuale.

## Caratteristiche avanzate

### Come evitare che gli utenti modifichino la configurazione di Panda Antivirus Exchange/Outlook

Se si desidera evitare che gli utenti a cui verrà installato automaticamente Panda Antivirus Exchange/Outlook possano modificare la configurazione dello stesso, è necessario seguire il procedimento descritto di seguito:

1. Installare Panda Antivirus Exchange/Outlook nel computer dell'amministratore della rete.

2. Aprire il programma di posta MS-Exchange/Outlook e configurare l'antivirus nel modo desiderato.

3. Proteggere la configurazione con chiave. Ciò si realizza nella finestra di configurazione dell'antivirus.

4. Copiare il file PAVEXCLI.CFG che si trova nella directory WINDOWS/SYSTEM nel computer dell'amministratore nella directory della rete da cui si distribuirà l'antivirus.

5. Procedere alla modifica del *login script* affinché abbia inizio la distribuzione dell'antivirus a tutte le postazioni della rete.

È importante tener presente che il procedimento descritto deve essere realizzato prima che abbia inizio la distribuzione dell'antivirus attraverso la rete.

## Nozioni necessarie circa Novell NetWare

La distribuzione dell'antivirus attraverso una rete Novell NetWare richiede una serie di nozioni minime su tale sistema. Qui di seguito verranno descritte le nozioni necessarie, spiegate con esempi sul come preparare il sistema in modo adeguato.

### Comandi che si eseguono quando si inizia una sessione di rete

Normalmente, quando un computer viene avviato si eseguono una serie di comandi definiti in un file. Nel caso di MS-DOS o Windows, tale file è l'AUTOEXEC.BAT.

Analogamente, è anche normale che, quando un computer si collega a una rete, vengano eseguiti una serie di comandi. Questa serie di comandi e/o programmi è conosciuta come *login script* o script di accesso.

Il *login script* può essere generale (uguale per tutti gli utenti) o privato (uno per ciascun utente). Può esistere anche una soluzione mista, con un *login script* generale comune a tutti gli utenti e uno privato per ognuno di loro.

Dal momento che il *login script* viene eseguito ogni volta che un utente si collega alla rete, esso costituisce il luogo più adatto per ottenere la distribuzione dell'antivirus alle postazioni. Sarà sufficiente eseguire nel *login script* il programma di distribuzione dell'antivirus di Panda Software affinché questo antivirus venga distribuito a tutte le postazioni a mano a mano che si collegano alla rete.

### System Login Script

Nel caso di Novell NetWare, il *login script* generale comune a tutti gli utenti è conosciuto come *System Login Script*. È necessario modificare tale file per aggiungervi l'esecuzione del programma di distribuzione antivirus di Panda Software. Per modificare il *System Login Script* bisogna effettuare i seguenti passaggi:

1. Se si possiede una versione Novell NetWare 3.x bisogna utilizzare il programma SYSCON. Se si possiede una versione Novell NetWare 4.x bisogna utilizzare il programma NETADMIN. Tutti i server Novell NetWare possiedono un volume chiamato SYS, e all'interno di esso si trova sempre una directory PUBLIC. I due programmi citati (SYSCON e NETADMIN) si trovano in tale directory.

2. Per modificare il *System Login Script* con il programma SYSCON, è necessario eseguire il programma, selezionare l'opzione *Supervisor Options* e quindi l'opzione *System Login Script*.

3. Per modificare il *System Login Script* con il programma NETADMIN, è necessario eseguire il programma e selezionare i due punti (..) nel riquadro a sinistra fino a che appare tale opzione. In quel momento verrà visualizzata una sola opzione (sulla destra sarà descritta come una *organizzazione*). Fatto ciò, è necessario selezionare questa unica opzione e premere il tasto F10. Nel menù che appare bisogna selezionare l'opzione *Vedi o modifica proprietà dell'oggetto*, e nel successivo menù l'opzione *Script di accesso*. Una volta effettuata questa operazione è già possibile modificare il *System Login Script*.

Nel *System Login Script* bisogna inserire due stringhe: la stringa relativa alla *mappatura* (questo concetto viene spiegato nella seguente sezione) e la stringa relativa alla distribuzione automatica dell'antivirus.

**Associazione di una lettera di unità**

In questa sezione verrà spiegato il concetto di *mappatura*. In un computer, il disco rigido viene normalmente identificato con la lettera C, il floppy con la lettera A o B e il CD-ROM con la D, la E, ecc. a seconda dei dischi rigidi installati.

I volumi ("dischi rigidi") del server Novell NetWare devono essere anche identificati con una lettera di unità per poter così fare riferimento a directory e file di questi volumi dalle stazioni senza problemi. L'operazione di associazione di una lettera di unità a un volume è conosciuta come *mappatura*.

E molto interessante il fatto che tutte le postazioni abbiano le stesse *mappature* per essere sicuri che i vari volumi del server abbiano lo stesso riferimento. A questo scopo è sufficiente indicare il comando di mappatura nel *System Login Script*. Generalmente i volumi si iniziano a definire a partire dalla lettera F, ma è possibile utilizzare qualsiasi altra lettera di unità che non sia già in uso. Il comando di mappatura, considerando quanto detto, sarebbe:

```
MAP ROOT F:=NOME_SERVER\NOME_VOLUME
```

Se il nome del server è ALFA e il nome del volume è SYS, il comando sarebbe:

```
MAP ROOT F:=ALFA\SYS:
```

## Nozioni necessarie circa Windows NT

La distribuzione dell'antivirus attraverso una rete Windows NT richiede una serie di nozioni minime su tale sistema. Qui di seguito verranno descritte le nozioni necessarie, spiegate con esempi sul come preparare il sistema in modo adeguato.

### Comandi che si eseguono quando si inizia una sessione di rete

Normalmente quando un computer viene avviato si eseguono una serie di comandi definiti in un file. Nel caso di MS-DOS o Windows, tale file è l'AUTOEXEC.BAT.

Analogamente, è anche normale che quando un computer si collega a una rete vengano eseguiti una serie di comandi. Questa serie di comandi e/o programmi è conosciuta come *login script* o script di accesso. Nel caso di Windows NT si usa il nome di *File di comandi di inizio sessione*.

Nel caso di Windows NT, ogni utente ha il proprio file di comandi di inizio sessione. Ciò fa sì che in generale sia necessario modificare i file di comando di inizio sessione di tutti gli utenti a cui si desidera distribuire l'antivirus. Per evitare questo compito laborioso Panda Software ha sviluppato un'utilità chiamata Profile Manager, il cui funzionamento viene spiegato qui di seguito.

Dal momento che il file di comandi di inizio sessione viene eseguito ogni volta che un utente si collega alla rete, esso è il luogo più adeguato per ottenere la distribuzione dell'antivirus alle postazioni. Sarà sufficiente eseguire nel file di comandi di inizio sessione il programma di distribuzione di antivirus di Panda Software affinché l' antivirus venga distribuito a tutte le postazioni a mano a mano che si collegano alla rete.

### File di comandi di inizio sessione - Profile Manager

Per installare il programma Profile Manager, che permette di modificare in modo congiunto tutti i file di comandi di inizio sessione, è necessario inserire il disco etichettato come *Editor di comandi di avvio per Windows NT* o collocarsi nella directory corrispondente del CD-Rom, e eseguire il programma **SETUP.EXE**. Per esempio:

```
A:\SETUP
```

Una volta installato, effettuare i seguenti passaggi:

1. Eseguire il programma.
2. Selezionare la modalità semplificata.
3. Selezionare *Modifica comandi di inizio di dominio* nel menù File.
4. Nella parte inferiore della finestra verrà visualizzata un editor di testo. È qui che si realizzano le modifiche corrispondenti che andranno a interessare tutti i file di comandi di inizio sessione.
5. Uscire dal programma salvando le modifiche.

Nel *File di comandi di inizio sessione* devono essere inserite due stringhe: la stringa relativa alla *mappatura* (questo concetto viene spiegato nella seguente sezione) e la stringa relativa alla distribuzione automatica dell'antivirus.

### Associazione di una lettera di unità

In questa sezione verrà spiegato il concetto di *mappatura*. In un computer, il disco rigido viene normalmente identificato con la lettera C, il floppy con la lettera A o B e il CD-ROM con la D, la E, ecc.

a seconda dei dischi rigidi installati.

Nel caso di una rete Windows NT, il concetto di *mappatura* deve essere messo in relazione con il concetto di *risorsa condivisa*. La totalità o una parte qualsiasi del disco rigido del server (o dei dischi, se ve n'è più d'uno) può essere in comune, diventando quindi una *risorsa condivisa*. Queste risorse condivise sono quelle che devono essere mappate per poi poter fare riferimento alle stesse dalle stazioni.

È particolarmente interessante che tutte le stazioni abbiano la stessa *mappatura*, per essere sicuri che tutte le diverse risorse condivise del server abbiano lo stesso riferimento. Per fare ciò è sufficiente inserire il comando di mappatura nel *File di comandi di inizio sessione*. Generalmente le risorse condivise vengono chiamate a partire dalla lettera F, ma si può utilizzare qualsiasi altra lettera di unità che non sia già in uso. Il comando di mappatura, considerando quanto detto, sarebbe:

```
NET USE F:= \\NOME_SERV\NOME_RISORSA
```

Se il nome del server è ALFA e il nome della risorsa condivisa è SYS, il comando sarebbe:

```
NET USE F: \\ALFA\SYS
```

## Nozioni necessarie circa OS/2

La distribuzione dell'antivirus attraverso una rete OS/2 richiede una serie di nozioni minime su tale sistema. Qui di seguito verranno descritte le nozioni necessarie, spiegate con esempi sul come preparare il sistema in modo adeguato.

### Comandi che si eseguono quando si inizia una sessione di rete

Normalmente, quando un computer viene avviato si eseguono una serie di comandi definiti in un file. Nel caso di MS-DOS o Windows, tale file è l'AUTOEXEC.BAT.

Analogamente, è anche normale che quando un computer si collega a una rete vengano eseguiti una serie di comandi. Questa serie di comandi e/o programmi è conosciuta come *login script* o script di accesso. Nel caso di OS/2, ogni utente possiede un file chiamato PROFILE.BAT (o PROFILE.CMD) che viene eseguito ogni volta che l'utente si collega alla rete.

Poiché ogni utente possiede un proprio file di comandi di inizio sessione, è necessario modificare il file PROFILE.BAT di ognuno degli utenti a cui si desidera effettuare la distribuzione. L'inconveniente è che le future modifiche richiedono anch'esse la modifica di tutti i file PROFILE.BAT. Ciò si può evitare creando un file BAT che contenga le stringhe necessarie per la distribuzione dell'antivirus, e chiamando tale file dai corrispondenti file PROFILE.BAT. In questo modo qualsiasi modifica futura potrà essere effettuata semplicemente nel file BAT creato, che interessa così tutti gli utenti.

Poiché il *login script* viene eseguito ogni volta che un utente si collega alla rete, esso è il luogo più adatto per ottenere la distribuzione dell'antivirus alle postazioni. Sarà sufficiente eseguire nel *login script* il programma di distribuzione di antivirus di Panda Software affinché l'antivirus venga distribuito a tutte le postazioni a mano a mano che queste si collegano alla rete.

### Associazione di una lettera di unità

In questa sezione verrà spiegato il concetto di *mappatura*. In un computer, il disco rigido viene normalmente identificato con la lettera C, il floppy con la lettera A o B e il CD-ROM con la D, la E, ecc. a seconda dei dischi rigidi installati.

Nel caso di una rete OS/2, il concetto di *mappatura* deve essere messo in relazione con il concetto di *risorsa condivisa*. La totalità o una parte qualsiasi del disco rigido del server (o dei dischi se ve n'è più d'uno) può essere in comune, e diventare quindi una *risorsa condivisa*. Queste risorse condivise sono quelle che devono essere mappate per poi poter fare riferimento alle stesse dalle stazioni.

È particolarmente interessante che tutte le stazioni abbiano la stessa *mappatura,* per essere sicuri che tutte le diverse risorse condivise del server abbiano lo stesso riferimento. Per fare ciò è sufficiente inserire il comando di mappatura nel file PROFILE. Generalmente le risorse condivise vengono chiamate a partire dalla lettera F, ma si può utilizzare qualsiasi altra lettera di unità che non sia già in uso. Il comando di mappatura, considerando quanto detto, sarebbe:

```
NET USE F: \\NOME_SERV\NOME_RISORSA
```

Se il nome del server è ALFA e il nome della risorsa condivisa è SYS, il comando sarebbe:

```
NET USE F: \\ALFA\SYS
```

## Sintassi dei comandi degli script (.SCR)

Nel leggere questa documentazione ci si sarà resi conto che viene sempre attribuito un parametro al programma **RINSTALL**. Tale parametro è il nome di un file con estensione SCR (file di script). Un file di script è un file di testo diviso in sezioni in cui si indica un comando per ogni stringa. Il file di script è quello che determina il comportamento del programma **RINSTALL**.

I file SCR adeguati per **RINSTALL** possono avere 6 sezioni differenti:

Sezione comune **[COMMON]**: questi comandi vengono sempre eseguiti.

Sezione DOS **[DOS]**: i comandi di questa sezione vengono eseguiti in DOS, Windows 3.1x e Windows 95.

Sezione Windows 3.1x **[WIN]**: i comandi di questa sezione vengono eseguiti in DOS, Windows 3.1x e Windows 95, ma viene localizzata solo la directory di Windows 3.1x nel disco rigido della postazione di lavoro.

Sezione Windows 95 **[WIN95]**: i comandi di questa sezione vengono eseguiti in DOS, Windows 3.1x e Windows 95, ma viene localizzata solo la directory di Windows 95 nel disco rigido della postazione di lavoro.

Sezione Windows NT **[WINNT]**: i comandi di questa sezione vengono eseguiti solo in Windows NT.

Sezione OS/2 **[OS/2]**: i comandi di questa sezione vengono eseguiti unicamente in OS/2.

Esistono tre tipi di comandi:

1. **File da copiare**: tutte le stringhe che NON iniziano con il carattere # indicano un file che dovrà essere presente nella directory di partenza e che dovrà essere copiato nella directory di arrivo. Secondo i parametri predefiniti, i file verranno copiati solo se non esistono già nella directory di arrivo o se il file presente nella directory di arrivo è meno recente di quello che si trova nella directory di partenza.

2. **Assegnazioni**: questi comandi iniziano con il carattere # e hanno la seguente struttura: # Variabile = valore. Servono per assegnare un determinato valore a una variabile. Di seguito vengono elencate le diverse variabili disponibili nei file script (SCR).

| **Nome della variabile** | **Descrizione** |
|---|---|
| Win3xDir | Directory di Windows 3.1x |
| Win95Dir | Directory di Windows 95 |
| WinNTDir | Directory di Windows NT |
| BaseSourcePath | Directory di partenza base |

| | |
|---|---|
| BaseTargetPath | Directory di arrivo base |
| RelSourcePath | Directory di partenza relativa |
| RelTargetPath | Directory di arrivo relativa |
| | |
| SourcePath | BaseSourcePath + RelSourcePath |
| TargetPath | BaseTargetPath + RelTargetPath |
| | |
| Copy Mode | Indica le condizioni di copiatura dei file. Ammette tre valori. COPY significa che verranno copiati i file solo se non esistono già nella directory di arrivo. UPDATE significa che verranno copiati i file solo se la versione da copiare è più recente di quella esistente nella directory di arrivo. OVERWRITE significa che i file verranno copiati sempre. |
| | |
| ErrorMode | Indica se devono essere visualizzati o meno i messaggi di errore. È possibile assegnare un valore 0 (non verranno visualizzati i messaggi) o un valore 1 (verranno visualizzati i messaggi). |

3. **Funzioni**: questi comandi cominciano anch'essi con il carattere #, e servono per portare a termine determinate operazioni. La loro sintassi è la seguente: # Funzione parametro 1, parametro 2, .... Le varie funzioni disponibili sono:

**AddProfileEntry**
Questa funzione aggiunge una voce in una sezione di un file tipo INI. Ammette 4 parametri:

| | |
|---|---|
| Parametro 1: | indica la sezione in cui creare la voce. |
| Parametro 2: | indica il campo (la 1ª parte della voce). |
| Parametro 3: | indica il valore (la 2ª parte della voce). |
| Parametro 4: | indica il percorso al file INI. |

Esempio:

```
#AddProfileEntry Windows, Load,
f:\pavfn\winkir.exe, c:\windows\win.ini
```

**AppendLine**
Questa funzione aggiunge una stringa a un file di testo. Ammette 3 parametri:

| | |
|---|---|
| Parametro 1: | indica il percorso al file di testo. |
| Parametro 2: | indica la stringa di testo da aggiungere. |
| Parametro 3: | LETTERALE (è facoltativo). Indicando questo parametro ci si assicura che la stringa di testo appaia proprio come è stata scritta, eliminando qualsiasi modifica che possa essere stata introdotta. |

Esempio:

```
#AppendLine c:\autoexec.bat,
c:\pavfn\sentinel.com
```

**AppendLineBefore**
Questa funzione aggiunge una stringa a un file di testo, ma sempre prima di un'altra stringa specificata. Ammette 4 parametri:

Parametro 1: indica il percorso al file di testo.
Parametro 2: indica la stringa di testo da aggiungere.
Parametro 3: indica la stringa di testo successiva a quella che viene inserita.
Parametro 4: LETTERALE (è facoltativo). Indicando questo parametro ci si assicura che la stringa di testo appaia proprio come è stata scritta, eliminando qualsiasi modifica che possa essere stata introdotta.

Esempio:

```
#AppendLineBefore c:\autoexec.bat,
c:\pavfn\sentinel.com, win, LITERAL
```

**DeleteLine**
Questa funzione serve per cancellare una stringa di un file di testo. Ammette 2 parametri:

Parametro 1: indica il percorso al file di testo.
Parametro 2: indica la stringa di testo da cancellare.

Esempio:

```
#DeleteLine c:\autoexec.bat,
c:\pavfn\sentinel.com
```

**InsertLine**
Questa funzione serve per inserire una stringa all'inizio di un file di testo. Ammette 3 parametri:

Parametro 1: indica il percorso al file di testo.
Parametro 2: indica la stringa di testo da inserire.
Parametro 3: LETTERALE (è facoltativo). Indicando questo parametro ci si assicura che la stringa di testo appaia proprio come è stata scritta, eliminando qualsiasi modifica che possa essere stata introdotta.

Esempio:

```
#InsertLine c:\autoexec.bat,
c:\pavfn\sentinel.com
```

**MakeDir**
Questa funzione crea una directory. Ammette un parametro:

Parametro 1: indica il percorso alla directory da creare.

Esempio:

```
#MakeDir c:\pavfn
```

**NoWinLoad**
All'interno del file WIN.INI esiste una sezione [Windows ] che ha una voce chiamata Load. Tale comando fa sì che vengano caricati una serie di programmi quando si entra in Windows. Nello stesso comando Load possono esserci più programmi. Il comando NoWinLoad elimina il programma che si desidera dal comando Load. Ammette un parametro:

Parametro 1: indica il programma che non si desidera caricare.

Esempio:

```
#NoWinLoad c:\pavfn\winkir.exe
```

**ReplaceLine**
Questa funzione sostituisce una stringa di un file di testo. Ammette 3 parametri:

Parametro 1: indica il percorso al file di testo.
Parametro 2: indica la stringa di testo da sostituire.
Parametro 3: indica la nuova stringa di testo.

Esempio:

```
#ReplaceLine c:\autoexec.bat,
«TargetPath»SENTINEL.COM,
«TargetPath»SENTINEL.COM /OE
```

**SetProfileEntry**
Questa funzione assegna un valore a una voce in una certa sezione di un file INI. La funzione cerca di trovare questa sezione. Se la trova le attribuisce un valore; altrimenti crea la voce e le assegna il valore. Anche se non esiste la sezione viene creata. Ammette 4 parametri:

Parametro 1: indica la sezione del file INI
Parametro 2: indica il campo (la 1ª parte della voce)
Parametro 3: indica il valore (la 2ª parte della voce)
Parametro 4: indica il percorso al file INI.

Esempio:

```
#SetProfileEntry Windows, Load,
c:\pavfn\winkir.exe, c:\windows\win.ini
```

**WinLoad**
All'interno del file WIN.INI esiste una sezione [Windows ] che ha una voce chiamata Load. Tale comando fa sì che vengano caricati una serie di programmi quando si entra in Windows. Nello stesso comando Load possono esserci più programmi. Il comando WinLoad aggiunge il programma che si desidera al comando Load. Ammette un parametro:

Parametro 1: indica il programma che si desidera caricare.

Esempio:

```
#WinLoad c:\pavfn\winkir.exe
```

**AdminRequired**

Tramite questa funzione si indica che da quel momento finché non appare una linea con la funzione EndAdminRequired, è necessario essere administrator per poter eseguire tutto il blocco di comandi (quelli che si trovano tra #AdminRequired e #EndAdminRequired). La funzione ha effetto solo quando RInstall si esegue con il parametro /Local. Questa funzione non prevede parametri.

Esempio:

```
#AdminRequired
```

**EndAdminRequired**

Quando appare questa funzione si indica che tutti i comandi seguenti si potranno eseguire senza la necessità di essere administrator. Hanno effetto solo quando RInstall si esegue con il parametro /Local. Questa funzione non prevede parametri.

Esempio:

```
#EndAdminRequired
```

**ResetMode**

Indica se il PC verrà riavviato in quel momento o se non verrà riavviato. Il valore 0 significa che non viene eseguito il riavvio, mentre il valore 1 significa che il riavvio deve verificarsi in quel momento. In ogni caso varrà visualizzato un avviso.

**CheckSpace**

Tramite questo comando si verifica l'esistenza di spazio (in Mb) esistente nella destinazione. In caso di spazio insufficiente verrà presentato un messaggio e non si procederà alla copia dei file.

Parametro 1: indica la dimensione necessaria in Mb.

Esempio:

```
#CheckSpace 8
```

**CopyFileAs**

Realizza la copia di un file da un'origine alla sua destinazione indicando la modalità di copia e rendendo possibile il cambiamento di nome del file. Prevede tre parametri:

Parametro 1: indica il percorso originale del file.

Parametro 1: indica la destinazione del file.

Parametro 1: indica la modalità di copia tramite le seguenti possibilità: COPY (il file verrà copiato solo se non è già presente nella destinazione), UPDATE (il file verrà copiato solo se la versione da copiare è più recente di quella presente nella destinazione), OVERWRITE (il file verrà comunque copiato anche se uguale a quello presente nella destinazione) e ONCHANGE (si effettuerà la copia sempre che i file di origine e destinazione siano

diversi). ONCHANGE indica che verrà realizzata la copia solo se il file di origine è diverso da quello di destinazione, non tenendo conto se il primo risulta precedente.

**DeteleDirDelayed**

Al termine dell'esecuzione di RInstall (dopo i comandi #Run), questo comando cancella una directory completa, comprese le subdirectory.

Parametro 1: indica la directory da cancellare.

Esempio:

```
#DeleteDirDelayed c:\pavfn
```

**ExchangeRequired**

Tramite questo comando si indica la necessità di avere installato un cliente di Exchange/Outlook per proseguire il procedimento della sezione in cui si trova. Non prevede nessun parametro.

Esempio:

```
#ExchangeRequired
```

**EndExchangeRequired**

Tramite questo comando si indica che non è più necessario avere installato un cliente di Exchange/Outlook per proseguire il procedimento della sezione in cui si trova. Non prevede nessun parametro.

Esempio:

```
#EndExchangeRequired
```