









Diese Option weist VShield an, alle Dateien nach Viren zu durchsuchen. Diese Option gewährt einen optimalen Schutz.

Diese Option weist VShield an, nur Programmdateien nach Viren zu durchsuchen. Mit dieser Option kann der Benutzer VShield so einrichten, daß er eine zufriedenstellende Leistung erhält, ohne gleichzeitig auf angemessenen Schutz verzichten zu müssen.

Diese Option weist VShield an, in mit PkLite und LZEXE komprimierten ausführbaren Dateien nach Viren zu suchen.

Klicken Sie hier, um Programmdateierweiterungen anzugeben.

Geben Sie in diesem Feld an, welche Aktion bei Auffinden eines Virus ausgeführt werden soll.

Diese Option weist VShield an, bei Auffinden eines Virus eine benutzerdefinierte Meldung anzuzeigen. Damit die Meldung angezeigt wird, muß die darüber angezeigte Option "Aktion" auf **Benutzeraktion anfordern** gesetzt sein.

Geben Sie die Meldung ein, die bei Auffinden eines Virus angezeigt werden soll.

Diese Option weist VShield an, Informationen in der angegebenen Protokolldatei aufzuzeichnen.

Geben Sie die gewünschte Protokolldatei in das angegebene Textfeld ein.

Diese Option weist VShield an, eine Protokolldatei mit höchstens der angegebenen Größe zu erstellen und beizubehalten. Deaktivieren Sie diese Option, um die Beschränkung der Protokolldateigröße aufzuheben.

Geben Sie die gewünschte Protokolldateigröße in das entsprechende Feld ein.

Zeigt eine Liste der Dateierweiterungen an, die VShield scannt.

Klicken Sie hier, um eine weitere Dateierweiterung hinzuzufügen.

Klicken Sie hier, um die ausgewählte Dateierweiterung zu löschen.

Klicken Sie hier, um die Standarddateierweiterungen von VShield wiederherzustellen.

Geben Sie hier eine neue Dateierweiterung ein.

Klicken Sie hier, um den Speicherort der VShield-Protokolldatei anzugeben.

Diese Option weist VShield an, einen Protokolleintrag mit den VShield-Einstellungen für die Rechensitzung zu erstellen.

Diese Option weist VShield an, einen Protokolleintrag mit der Zusammenfassung der Aktivitäten während der Rechensitzung zu erstellen.

Diese Option weist VShield an, während des Systemabschlusses auf Disketten nach Viren zu suchen.

Diese Option weist VShield an, bei der Erstellung von Protokolleinträgen den Windows-Benutzernamen mit aufzunehmen.

Geben Sie den Pfad des gewünschten Verschiebeordners an, in den infizierte Dateien verschoben werden sollen. Dieser Ordner wird automatisch aus den VShield-Scanvorgängen ausgeschlossen.

Klicken Sie hier, um einen Ordner zu suchen.

Diese Option weist VShield an, auf den Disketten, auf die zugegriffen wird, nach Viren zu suchen.

Mit dieser Option kann der Benutzer den VShield-Schutz deaktivieren.

Diese Option weist VShield an, als Symbol auf dem Desktop zu erscheinen.

Diese Option weist VShield an, einen Protokolleintrag zu erstellen, wenn eine infizierte Datei gefunden wurde.

Diese Option weist VShield an, einen Protokolleintrag zu erstellen, wenn eine infizierte Datei erfolgreich gesäubert wurde.

Diese Option weist VShield an, einen Protokolleintrag zu erstellen, wenn eine infizierte Datei gelöscht wurde. Durch die Aktivierung dieser Option können Sie verfolgen, welche Dateien von Originaldisketten oder aus Sicherungen wiederhergestellt werden müssen.

Diese Option weist VShield an, einen Protokolleintrag zu erstellen, wenn eine infizierte Datei in einen Verschiebeordner verschoben wurde.

Diese Option weist VShield an, jedem Protokolleintrag einen Datums- und Zeitstempel hinzuzufügen.

Diese Option weist VShield an, in Dateien, die ausgeführt werden, nach Viren zu suchen.

Diese Option weist VShield an, in Dateien, die zum Kopieren auf das lokale System geöffnet werden, nach Viren zu suchen.

Diese Option weist VShield an, in Dateien, die auf dem lokalen System erstellt werden, nach Viren zu suchen.

Diese Option weist VShield an, in Dateien, die im lokalen System umbenannt werden, nach Viren zu suchen.

Diese Option weist VShield an, bei Auffinden infizierter Dateien die Option "Säubern" bereitzustellen. Mit "Säubern" erhalten der Benutzer und VShield eine Möglichkeit, die infizierte Datei zu bereinigen. Wenn der Säuberungsvorgang erfolglos verläuft, werden weitere Optionen zur Verfügung gestellt.

Diese Option weist VShield an, beim Auffinden infizierter Dateien die Option "Löschen" bereitzustellen. Mit "Löschen" erhalten der Benutzer und VShield die Möglichkeit, die infizierte Datei zu löschen.

Diese Option weist VShield an, beim Auffinden infizierter Dateien die Option "Ausschließen" bereitzustellen. "Ausschließen" entfernt diese Datei für die aktuelle Sitzung aus zukünftigen Scanvorgängen. Dauerhafte Ausschlüsse sind in der Eigenschaftsseite **Ausschlüsse** enthalten.

Diese Option weist VShield an, beim Auffinden infizierter Dateien die Option "Stoppen" bereitzustellen. "Stoppen" bricht den Zugriff auf die Datei ab.

Diese Option weist VShield an, beim Auffinden infizierter Dateien die Option "Fortsetzen" bereitzustellen. "Fortsetzen" umgeht die VShield-Warnungen und ermöglicht es dem Benutzer, den Zugriff auf die Datei fortzusetzen.

In dieser Liste definierte Objekte, wie zum Beispiel Dateien, Ordner oder Laufwerke, werden von der Viruserkennung ausgeschlossen. Stellen Sie sicher, daß dieser Liste hinzugefügte Objekte virenfrei sind.

Klicken Sie hier, um ein Objekt für den Ausschluß aus VShield-Scanvorgängen hinzuzufügen.

Klicken Sie hier, um den markierten Eintrag aus der Liste "Ausschlüsse" zu löschen.

Klicken Sie hier, um den markierten Eintrag zu bearbeiten.

Klicken Sie hier, um VShield während des Systemstarts automatisch zu laden.

