
GFI EndPointSecurity 4.0

Manuale

a cura di GFI Software Ltd.



<http://www.gfi-italia.com>

Email: info@gfi.com

Le informazioni contenute nel presente documento sono soggette a modifica senza preavviso. Le società, i nomi e i dati adoperati negli esempi sono fittizi salvo diversamente indicato. Nessuna parte del presente documento può essere riprodotta o trasmessa in alcuna forma, elettronica o meccanica, per qualsiasi scopo, senza esplicita autorizzazione scritta di GFI SOFTWARE Ltd.

Versione 4.0 – Ultimo aggiornamento: 10 marzo 2008

Indice

Introduzione	4
Informazioni sulle minacce rappresentate dai dispositivi di supporto portatili.....	4
Introduzione a GFI EndPointSecurity.....	4
Classi di dispositivi supportati	5
Porte per la connessione dei dispositivi supportati.....	6
Caratteristiche principali.....	6
Componenti di GFI EndPointSecurity	8
Modalità di funzionamento di GFI EndPointSecurity: distribuzione e monitoraggio	9
Modalità di funzionamento di GFI EndPointSecurity: accesso al dispositivo	11
Modalità di funzionamento di GFI EndPointSecurity: accesso temporaneo	12
Schema delle licenze	13
Installazione di GFI EndPointSecurity	14
Introduzione	14
Requisiti di sistema	14
Requisiti hardware	14
Requisiti software.....	14
Agente GFI EndPointSecurity: requisiti hardware	14
Agente GFI EndPointSecurity: requisiti software.....	14
Procedura d'installazione	15
Aggiornamento da precedenti versioni	17
Aggiornamento da GFI EndPointSecurity 3.....	17
Aggiornamento da GFI LANGuard Portable Storage Control	17
Guida introduttiva	19
Avvio di GFI EndPointSecurity.....	19
Utilizzo della finestra di dialogo dell'Avvio rapido	19
Configurazione dei gruppi utenti locali o di dominio	20
Configurazione del terminale database	21
Configurazione delle opzioni di avviso.....	21
Configurazione dell'account amministratore di GFI EndPointSecurity	22
Configurazione dei criteri di protezione predefiniti.....	22
Navigazione nella consolle di gestione di GFI EndPointSecurity	23
Guida introduttiva: distribuzione del criterio di protezione predefinito	25
Introduzione	25
Preparazione della distribuzione del criterio di protezione	25
Configurazione dei computer da proteggere	25
Credenziali di configurazione.....	27
Distribuzione di un criterio di protezione predefinito	28
Distribuzione immediata.....	28
Pianificazione della distribuzione	30
La distribuzione di un criterio di protezione attraverso Active Directory	31
Verifica dello stato di distribuzione del criterio di protezione	31

Cronologia della distribuzione	31
Stato degli agenti	32
Monitoraggio dell'attività di utilizzo del dispositivo	33
Introduzione	33
Utilizzo della visualizzazione delle Statistiche	33
Stato della protezione	34
Utilizzo del dispositivo secondo il tipo	35
Utilizzo del dispositivo secondo la porta di connessione	35
Utilizzo della scansione dispositivi	36
Risultati di scansione	39
Utilizzo del Browser dei log	42
Creazione delle query di eventi	43
Utilizzo di avvisi	44
Rapporti	44
Monitoraggio dello stato	45
Introduzione	45
Accesso al monitor di stato	45
Utilizzo della visualizzazione di stato Generale	46
Stato del Servizio	47
Stato del terminale database	47
Stato Generale	48
Stato della protezione	48
Stato in linea	49
Stato degli agenti	49
Utilizzo del dispositivo	50
Utilizzo della visualizzazione Stato agenti	51
Utilizzo della visualizzazione Stato distribuzione	52
Distribuzioni correnti	53
Distribuzioni in attesa	53
Distribuzioni pianificate	53
Cronologia della distribuzione	54
Utilizzo della visualizzazione delle Statistiche	54
Personalizzazione del criterio di protezione predefinito	55
Introduzione	55
Configurazione dei dispositivi portatili da controllare	55
Configurazione delle porte di connessione da controllare	57
Configurazione degli utenti autorizzati	58
Configurazione delle autorizzazioni di accesso alla categoria di dispositivi	59
Configurazione autorizzazioni di utilizzo della porta di connessione	62
Configurazione autorizzazioni di accesso per un determinato dispositivo	65
Visualizzazione autorizzazioni	69
Configurazione priorità autorizzazioni	70
Configurazione blacklist dispositivi portatili	70
Configurazione whitelist dispositivi portatili	73
Configurazione privilegi di accesso temporaneo	76
Richiesta di accesso temporaneo per un computer protetto	77
Concessione accesso temporaneo a un computer protetto	78
Configurazione dei filtri dei tipi di file	80
Configurazione della registrazione eventi	81
Configurazione notifiche	83
Configurazione delle impostazioni predefinite di GFI EndPointSecurity	87
Introduzione	87

Configurazione account amministratore di GFI EndPointSecurity	87
Configurazione opzioni di avviso	91
Avvisi via email.....	92
Avvisi mediante messaggi di rete	93
Avvisi SMS	93
Configurazione utenti da avvisare.....	94
Creazione utenti.....	94
Modifica proprietà dell'utente	94
Rimozione di utenti	94
Configurazione gruppi da avvisare	94
Creazione di gruppi.....	94
Modifica delle proprietà di gruppo.....	95
Rimozione di gruppi	95
Configurazione del database terminale	96
Creazione del nuovo database	96
Modifica del terminale database	97
Manutenzione database.....	97
Personalizzazione messaggi utenti.....	98
Opzioni avanzate	99

Opzioni varie **101**

Introduzione	101
Inserimento del codice di licenza dopo l'installazione	101
Ricerca di build più recenti.....	101

Risoluzione dei problemi **102**

Introduzione	102
Knowledgebase.....	102
Richiesta di assistenza tecnica via email.....	102
Richiesta di assistenza tecnica telefonica	103
Forum su internet.....	103
Notifiche relative alle build	103

Indice analitico **105**

Introduzione

Informazioni sulle minacce rappresentate dai dispositivi di supporto portatili

Il vantaggio principale dei dispositivi di supporto portatili (o dispositivi portatili) è il facile accesso. In teoria, ciò potrebbe essere molto vantaggioso per le organizzazioni. Tuttavia, è noto che gli elementi "accesso" e "protezione" sono situati agli estremi opposti del segmento "sicurezza".

Gli sviluppi tecnologici dei supporti rimovibili vanno intensificandosi. Le versioni di dispositivi portatili più nuove, come le memorie flash, hanno visto un incremento di capacità e prestazioni tali da rendere detti dispositivi:

- facili e veloci da installare
- capaci di memorizzare quantità enormi di dati
- sufficientemente piccoli da poterli mettere in tasca.

Di conseguenza, gli utenti interni possono, deliberatamente o accidentalmente:

- rimuovere dati sensibili o esporre informazioni riservate
- introdurre codici maligni (ad esempio, virus e trojan) in grado di bloccare l'intera rete aziendale
- trasferire materiale inopportuno od offensivo su un'apparecchiatura aziendale
- produrre copie personali di informazioni e proprietà intellettuale aziendale
- collegare dispositivi portatili alle apparecchiature aziendali e, di conseguenza, distrarsi durante l'orario lavorativo.

Nel tentativo di controllare queste minacce, le organizzazioni hanno cominciato a proibire l'utilizzo di dispositivi portatili personali sul posto di lavoro. Tuttavia, la *best practice* richiede che non si faccia mai affidamento sulla "compiacenza" volontaria. Il miglior modo per garantire il controllo completo sui dispositivi portatili consiste nel porre barriere tecnologiche.

Introduzione a GFI EndPointSecurity

GFI EndPointSecurity è la soluzione di protezione che aiuta a mantenere l'integrità dei dati impedendo l'accesso e il trasferimento non autorizzati di contenuto da e verso i seguenti dispositivi di supporto portatili:

- porte USB (per esempio, lettori di schede flash e di memoria, chiavi USB)
- porte FireWire (ad esempio, foto e videocamere digitali, lettori di schede FireWire)
- connessioni dati wireless (per esempio, adattatori Bluetooth, infrarossi)
- unità floppy (interne ed esterne)
- unità ottiche come CD, DVD e unità MO (magneto-ottiche), interne ed esterne
- unità disco rigido USB rimovibili
- altre unità, quali le unità Zip e a nastro (interne ed esterne).

Attraverso la sua tecnologia, GFI EndPointSecurity consente di autorizzare o negare l'accesso a un dispositivo e di assegnare (ove possibile) privilegi "completi" o di "sola lettura":

- su ogni dispositivo supportato (ad esempio, unità CD/DVD e PDA)
- a qualsiasi utente o gruppo di utenti locali o di Active Directory.

Con GFI EndPointSecurity è inoltre possibile registrare l'attività di tutti i dispositivi portatili utilizzati sui computer target (compresi, data e ora di utilizzo e utenti dei dispositivi stessi).

Classi di dispositivi supportati

In GFI EndPointSecurity, le classi di dispositivi portatili sono organizzate nelle seguenti categorie:

Floppy disk

CD o DVD ROM

- CD R/W ROM
- DVD R/W ROM

Dispositivi di memoria

- pen drive USB
- lettori digitali (ad esempio, MP3, iPod, Creative Zen)
- lettori di schede flash e di schede di memoria
- dispositivi USB a più unità, cioè dispositivi che non si montano come un'unica unità (spoofing)
- altri dispositivi di memoria portatili

Stampanti

PDA

- PC tascabili
- dispositivi BlackBerry RIM
- smartphone

Adattatori di rete

- WiFi
- adattatori e/o connessioni Bluetooth
- adattatori e/o connessioni ad infrarossi

Modem

- smartphone
- telefoni cellulari

Dispositivi per l'acquisizione di immagini

- foto e videocamere digitali
- webcam
- scanner

Periferiche Human Interface

- tastiere
- mouse
- game controller

Altri dispositivi

- adattatori e/o porte Bluetooth
- adattatori e/o porte ad infrarossi
- unità magneto-ottiche (MO) interne ed esterne
- unità ZIP
- unità a nastro.

Porte per la connessione dei dispositivi supportati

EndPointScan esegue la scansione alla ricerca di dispositivi collegati, o che siano stati collegati in passato, alle seguenti porte:

- USB
- Firewire
- PCMCIA
- Bluetooth
- Secure Digital (SD)
- seriali e parallele
- a infrarossi
- interne (es. unità ottiche e floppy).

Caratteristiche principali

Controllo di protezione basato sui gruppi

In GFI EndPointSecurity è possibile configurare e collocare i computer in gruppi regolati da un criterio di protezione. In questo modo, è possibile configurare un unico criterio di protezione e applicarlo a tutti i computer appartenenti a quel gruppo.

Controllo di accesso granulare

GFI EndPointSecurity consente di autorizzare o negare l'accesso a un dispositivo specifico e di attribuire (ove possibile) privilegi di "accesso completo" o di "sola lettura" su ogni dispositivo supportato (ad esempio, PDA), utente per utente.

Distribuzione pianificata

Quando l'amministratore apporta modifiche ai criteri o alla configurazione mediante la consolle di gestione di GFI EndPointSecurity, è possibile chiudere la consolle e permettere la distribuzione automatica dell'agente in base a una pianificazione. La distribuzione viene gestita dallo stesso servizio GFI EndPointSecurity che si occupa delle distribuzioni non riuscite attraverso la riprogrammazione.

Controllo di accesso

Oltre a bloccare una gamma di classi di dispositivi, GFI EndPointSecurity consente inoltre il blocco:

- per tipo di file, ad esempio, consente all'utente di leggere i file ".doc", ma blocca l'accesso a tutti i file ".exe";
- per porta fisica, cioè blocca tutti i dispositivi collegati a una determinata porta fisica, comprese USB, Firewire, Bluetooth, a infrarossi, Wi-Fi, PCMCIA, parallele, seriali, S-ATA ed SD;
- per ID del dispositivo, impostando l'autorizzazione per singolo dispositivo in base all'ID hardware esclusivo del dispositivo stesso.

Whitelist e blacklist dei dispositivi

L'amministratore può definire un elenco di determinati dispositivi sempre consentiti e di altri sempre vietati.

Utenti autorizzati

L'amministratore può specificare utenti o gruppi che avranno sempre pieno accesso ai dispositivi protetti da GFI EndPointSecurity.

Accesso temporaneo

L'amministratore è in grado di conferire l'accesso temporaneo a un dispositivo (o gruppo di dispositivi) su un determinato computer. Questa nuova funzionalità consente all'amministratore di generare un codice di sblocco utilizzabile dall'utente finale per ottenere un accesso, temporalmente limitato, a un particolare dispositivo o porta, persino quando l'agente GFI EndPointSecurity non è collegato alla rete.

Dashboard di stato

Un'interfaccia utente rinnovata mostra ora lo stato degli agenti "dal vivo", quello della distribuzione degli agenti, del database, del servizio GFI EndPointSecurity e dati statistici completi di grafici.

L'applicazione principale tiene traccia dello stato dell'agente "dal vivo", comunicando con i suoi agenti distribuiti. Vengono automaticamente eseguite operazioni di manutenzione una volta che un agente va in linea.

Distribuzione di Active Directory di attraverso MSI

Dalla consolle di gestione di GFI EndPointSecurity è possibile generare un singolo file MSI che, successivamente, potrà essere distribuito con l'apposito strumento di Active Directory o tramite altre opzioni di distribuzione. Il file MSI conterrà tutte impostazioni di sicurezza configurate in un particolare criterio di protezione.

Password di gestione dell'agente

Le funzioni di gestione dell'agente (ad esempio un aggiornamento o la disinstallazione) sono protetti da una password configurata dall'utente.

Pertanto, tutte le altre istanze di GFI EndPointSecurity non avranno accesso alle opzioni di gestione dell'agente.

Scoperta del dispositivo

Il motore di GFI EndPointSecurity può essere adoperato per eseguire la scansione e individuare la presenza di dispositivi sulla rete. Le informazioni relative ai dispositivi individuati possono essere adoperate per creare criteri di sicurezza e attribuire diritti di accesso per dispositivi specifici.

Browser dei log

An in-built tool allows the administrator to browse user activity and device usage that is detected by GFI EndPointSecurity and logged in the backend database.

Avvisi

È possibile inviare notifiche standard quando vengono collegati o adoperati dispositivi ovvero quando viene bloccato o autorizzato l'accesso a un dispositivo.

Messaggi personalizzati

Quando agli utenti viene impedito di utilizzare un dispositivo, vengono visualizzati messaggi pop-up personalizzati illustranti i motivi del blocco del dispositivo.

Gestione del database

Semplice manutenzione automatica del terminale database, ad esempio, l'opzione di eliminare le informazioni più vecchie di "x" giorni.

Componenti di GFI EndPointSecurity

Nell'installazione di GFI EndPointSecurity, vengono installati i seguenti componenti:

- Agente di GFI EndPointSecurity
- Applicazione della consolle di gestione di GFI EndPointSecurity.

Agente di GFI EndPointSecurity

L'agente di GFI EndPointSecurity è un servizio client responsabile dell'implementazione/applicazione dei criteri di protezione sui computer target. Il servizio è installato automaticamente su target di rete remoti durante la primissima distribuzione di un criterio di protezione. Dopo le distribuzioni successive (cioè dopo aver apportato modifiche al criterio di protezione iniziale), l'agente non verrà reinstallato, ma soltanto aggiornato.

NOTA: l'applicazione della consolle di gestione di GFI EndPointSecurity terrà traccia dei computer dotati di agente e verificherà la necessità di distribuire eventuali aggiornamenti nel momento in cui si aggiorna la configurazione.

Consolle di gestione di GFI EndPointSecurity

La consolle di gestione di GFI EndPointSecurity è l'applicazione tramite la quale è possibile:

- creare e configurare il criterio di protezione di ogni categoria di dispositivi e di ogni porta di connessione supportata dal prodotto
- distribuire in remoto criteri di protezione sui computer target (cioè distribuire e/o aggiornare gli agenti GFI EndPointSecurity)

- conferire l'accesso temporaneo a computer client affinché possano utilizzare determinati dispositivi
- visualizzare lo stato della protezione del dispositivo di ogni computer monitorato
- eseguire scansioni su computer target per identificare i dispositivi collegati attualmente o in precedenza
- controllare i log e analizzare i dispositivi portatili che sono stati connessi a ogni computer della rete.

Modalità di funzionamento di GFI EndPointSecurity: distribuzione e monitoraggio

Le operazioni di distribuzione e monitoraggio dei criteri di protezione di GFI EndPointSecurity possono essere suddivise in 4 fasi logiche:

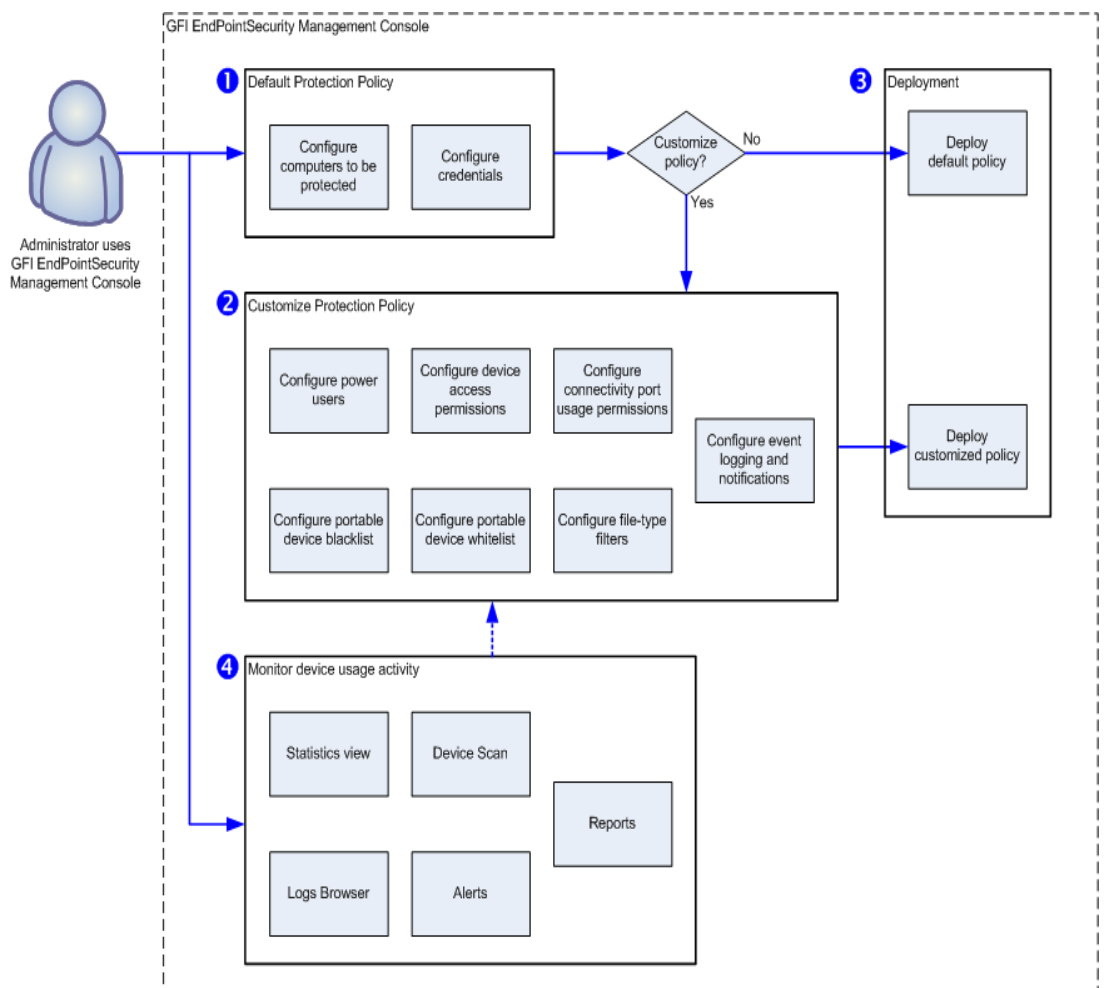


Figura 1 – Distribuzione e monitoraggio del criterio di protezione

Fase 1: configurazione del criterio di protezione predefinito In questa fase l'amministratore specifica i computer che devono essere aggiunti a un criterio di protezione e le credenziali di accesso che GFI EndPointSecurity dovrà adoperare per accedere ai computer e distribuire gli agenti.

Fase 2: personalizzazione del criterio di protezione predefinito L'amministratore può personalizzare un criterio di protezione predefinito prima di distribuirlo. Tra le opzioni di personalizzazione,

figurano la creazione di utenti autorizzati, l'aggiunta di dispositivi inseriti nella blacklist o nella whitelist e le autorizzazioni di accesso al dispositivo.

Fase 3: distribuzione del criterio di protezione In questa fase l'amministratore distribuisce il criterio di protezione (predefinito o personalizzato), attraverso l'installazione di agenti su computer target. Le successive personalizzazioni dei criteri di protezione richiedono esclusivamente l'invio di aggiornamenti agli agenti.

Fase 4: controllo di accesso al dispositivo Una volta che gli agenti sono stati distribuiti, l'amministratore è in grado di controllare tutti i tentativi di accesso al dispositivo, grazie alle visualizzazioni della console di gestione, agli avvisi e ai rapporti del ReportPack di GFI EndPointSecurity.

Modalità di funzionamento di GFI EndPointSecurity: accesso al dispositivo

Le operazioni di accesso al dispositivo di GFI EndPointSecurity possono essere suddivise in 3 fasi logiche:

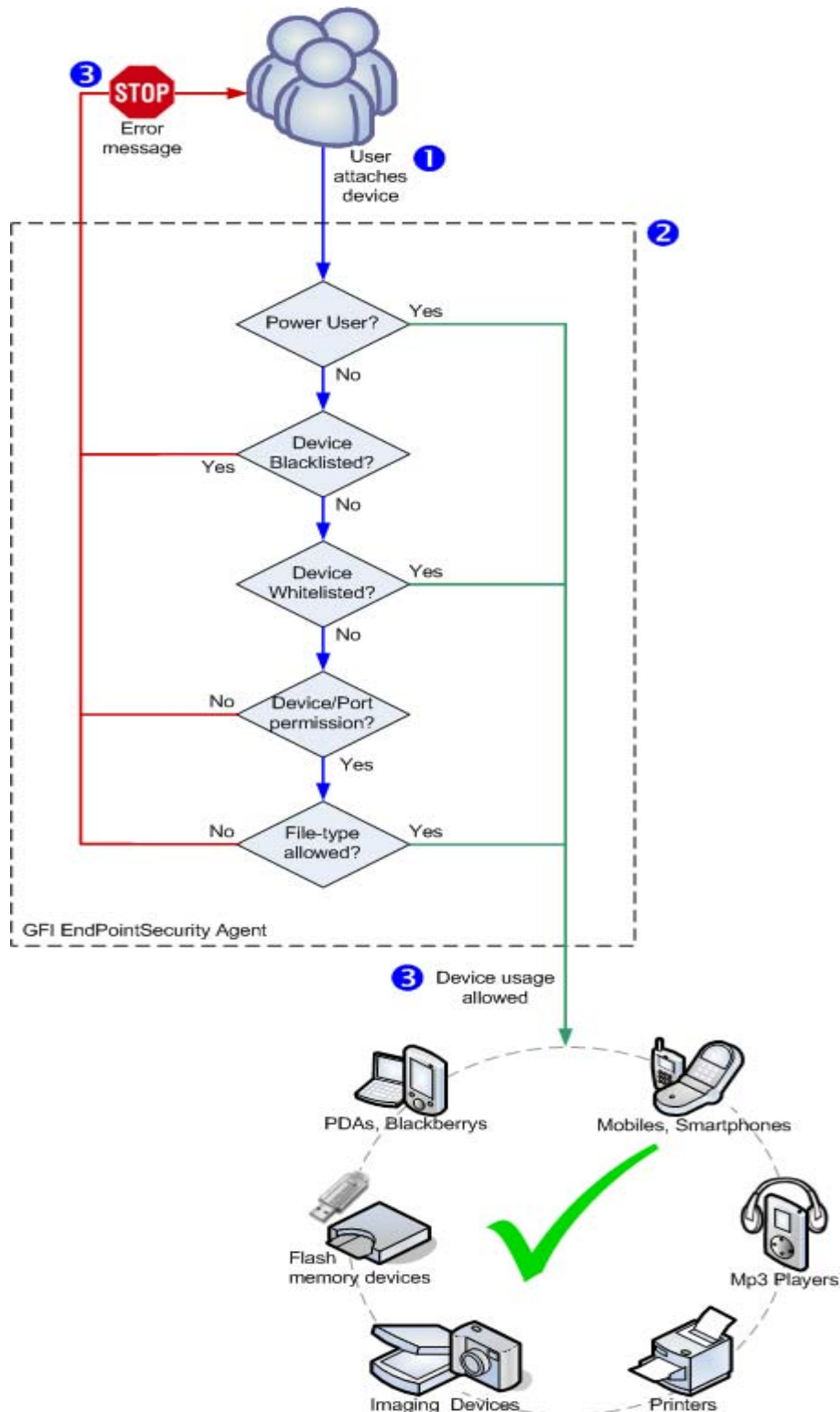


Figura 2 – Accesso al dispositivo

Fase 1: dispositivo collegato al computer In questa fase, l'utente collega un dispositivo di comunicazione portatile a un computer protetto da GFI EndPointSecurity.

Fase 2: applicazione del criterio di protezione In questa fase l'agente GFI EndPointSecurity installato sul computer rileva il dispositivo collegato e analizza le regole del criterio di protezione applicabili al computer o all'utente. L'operazione determina se è possibile accedere al dispositivo e il livello di accesso consentito.

Fase 3: autorizzazione/divieto di utilizzo del dispositivo In questa fase l'utente riceve un messaggio un messaggio di errore indicante che è stato bloccato l'utilizzo del dispositivo oppure uno che gli comunica di poter accedere al dispositivo stesso.

Modalità di funzionamento di GFI EndPointSecurity: accesso temporaneo

Le operazioni di accesso temporaneo di GFI EndPointSecurity possono essere suddivise in 2 fasi logiche:

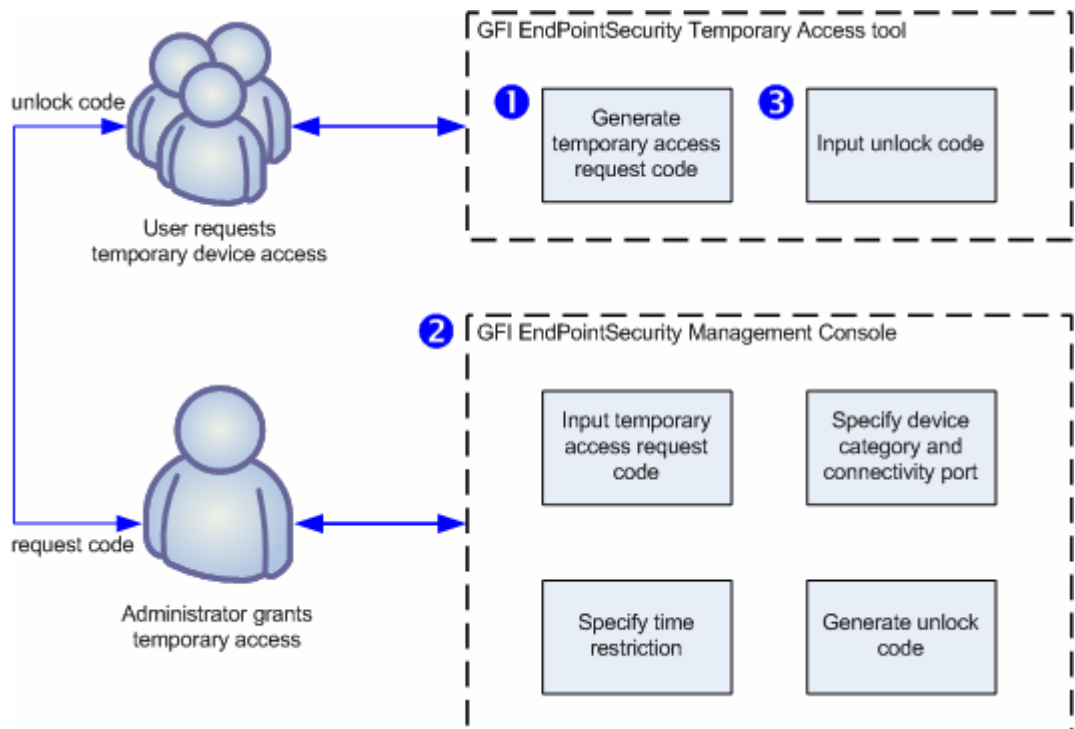


Figura 3 – Richiesta/attribuzione dell'accesso temporaneo

Fase 1: l'utente richiede un accesso temporaneo In questa fase l'utente esegue il tool di accesso temporaneo di GFI EndPointSecurity (GFI EndPointSecurity Temporary Access) dal computer dal quale si deve accedere al dispositivo di supporto portatile. Il tool è adoperato per generare un codice di richiesta, che l'utente comunicherà all'amministratore. L'utente dovrà inoltre informare l'amministratore in merito al tipo di dispositivo cui desidera accedere e per quanto tempo.

Fase 2: l'amministratore concede l'accesso temporaneo In questa fase, l'amministratore si avvale della funzione di accesso temporaneo di GFI EndPointSecurity (GFI EndPointSecurity Temporary Access) per inserire il codice di richiesta e per specificare i dispositivi o le porte

e la durata dell'accesso temporaneo. Viene così generato un codice di sblocco che l'amministratore comunica all'utente.

Schema delle licenze

La licenza di GFI EndPointSecurity dipende dal numero di computer che saranno controllati ai fini dell'accesso a dispositivi portatili. Ad esempio, per controllare l'accesso a dispositivi portatili su 25 computer, è necessario acquistare una licenza da 25 computer.

Per impostazione predefinita, GFI EndPointSecurity ha un periodo di valutazione di 10 giorni con tutte le funzionalità attive. Se i dati forniti nel modulo di download sono corretti, si riceve un'email contenente un codice di licenza che consente di valutare GFI EndPointSecurity per un totale di 30 giorni.

Installazione di GFI EndPointSecurity

Introduzione

Il presente capitolo fornisce le seguenti informazioni:

- i requisiti di sistema richiesti per l'installazione di GFI EndPointSecurity 4
- le modalità per effettuare l'aggiornamento da GFI LANguard Portable Storage Control o da GFI EndPointSecurity 3
- le modalità d'installazione di GFI EndPointSecurity 4.

Requisiti di sistema

I requisiti di sistema di GFI EndPointSecurity sono i seguenti:

Requisiti hardware

- Processore: con velocità di clock pari a 2GHz
- RAM: almeno 512MB; 1 GB (consigliata)
- Disco rigido: 100Mb di spazio disponibile

Requisiti software

- Sistema operativo: Windows 2000 (SP4), XP, 2003, Vista e 2008 (versioni a 86 e 64 bit)
- Internet Explorer 5.5 o successivi
- .NET Framework versione 2.0.
- Terminale database: SQL Server 2000, 2005, 2008
- Porta: TCP 1116 (predefinita)

NOTA 1: il firewall deve essere configurato in modo da consentire a GFI EndPointSecurity di "ascoltare" la porta TCP configurata.

NOTA 2: GFI EndPointSecurity può essere installato e avviato esclusivamente se si utilizzano privilegi amministrativi.

Agente GFI EndPointSecurity: requisiti hardware

- Processore: con velocità di clock pari a 1GHz
- RAM: almeno 256MB; 512MB (consigliata)
- Disco rigido: 50Mb di spazio disponibile

Agente GFI EndPointSecurity: requisiti software

- Sistema operativo: Windows 2000 (SP4), XP, 2003, Vista e 2008 (versioni a 86 e 64 bit)

Procedura d'installazione

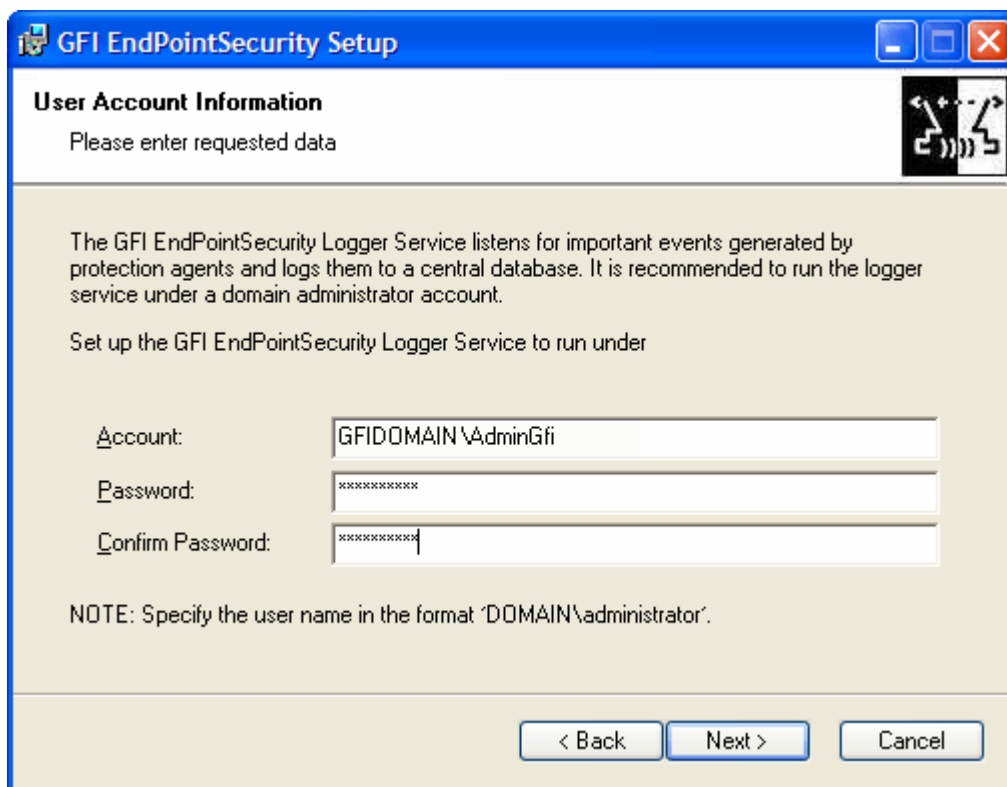
Per installare GFI EndPointSecurity 4, seguire questa procedura:

1. Fare doppio clic su **endpointsecurity4.exe** e poi clic su **Next (Avanti)**.



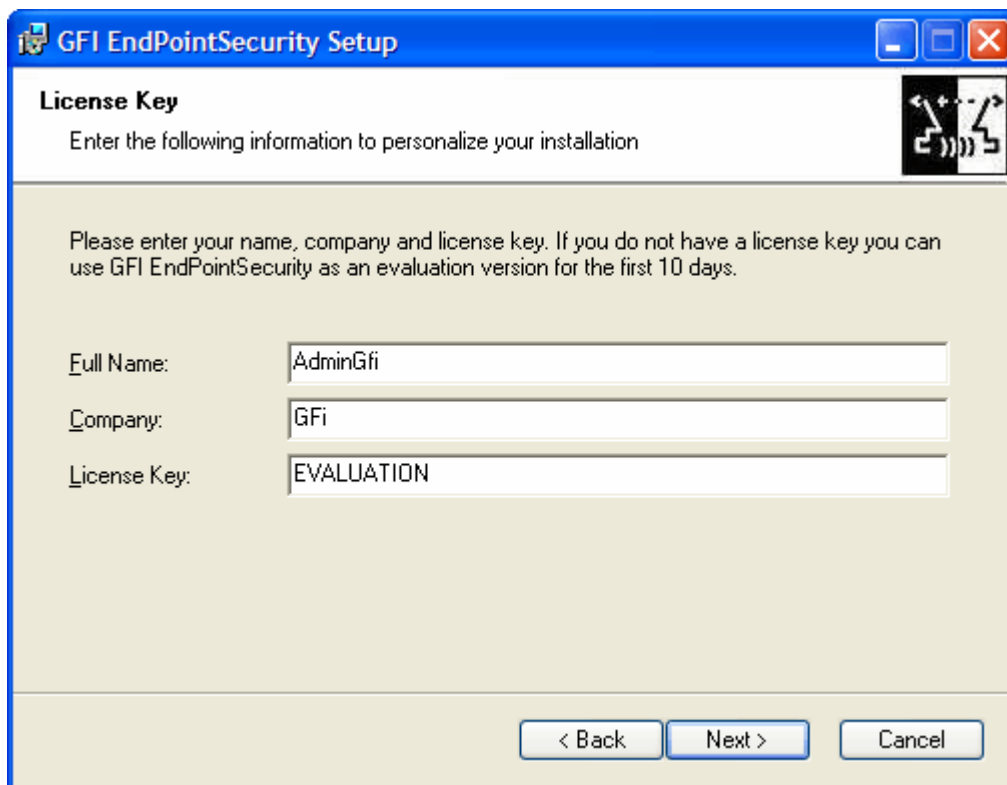
Schermata 1 – Contratto di licenza di GFI EndPointSecurity

2. Leggere attentamente il contratto di licenza. Per procedere con l'installazione del prodotto, selezionare l'opzione *I accept the terms in the license agreement* (Accetto) e fare clic su **Next (Avanti)**.



Schermata 2 – Impostazione dell'account amministratore di dominio di GFI EndPointSecurity

3. Specificare l'account amministratore di dominio con il quale eseguire il servizio GFI EndPointSecurity Logger. Fare clic su **Next (Avanti)** per continuare.



Schermata 3 – Dettagli del codice di licenza di GFI EndPointSecurity

4. Indicare nome utente, organizzazione e dati del codice di licenza. Se si sta valutando il prodotto per il periodo di 10 giorni, lasciare il codice di valutazione predefinito "Valutazione". Fare clic su **Next (Avanti)** per continuare.

5. Indicare un percorso d'installazione alternativo o fare clic su **Next (Avanti)** per utilizzare il percorso predefinito e proseguire l'installazione.

6. Fare clic su **Indietro** per inserire nuovamente le informazioni d'installazione. Fare clic su **Next (Avanti)** per completare l'installazione.

Aggiornamento da precedenti versioni

Se si è in possesso GFI LANguard Portable Storage Control o una versione precedente di GFI EndPointSecurity, è possibile eseguire l'aggiornamento a GFI EndPointSecurity 4.

Aggiornamento da GFI EndPointSecurity 3

Aggiornamento facile e diretto da GFI EndPointSecurity 3 a GFI EndPointSecurity 4. Il processo di aggiornamento rientra nella procedura d'installazione di GFI EndPointSecurity 4 e comprende:

- la disinstallazione di GFI EndPointSecurity 3
- l'importazione delle impostazioni di configurazione di GFI EndPointSecurity 3.

Importazione delle impostazioni di configurazione di GFI EndPointSecurity 3

Quando s'installa GFI EndPointSecurity 4, viene richiesto di confermare se importare le configurazioni dalla versione precedente. Fare clic su **Yes (Sì)** per importare le configurazioni. Viene quindi richiesto di specificare quale delle seguenti configurazioni importare:

- Criteri di protezione
 - Computer
 - Impostazioni di sicurezza
- Opzioni
 - Opzioni di registrazione
 - Opzioni del database

Aggiornamento da GFI LANguard Portable Storage Control

Se il computer sul quale si sta installando GFI EndPointSecurity 4 è protetto da un agente GFI LANguard Portable Storage Control, è necessario innanzitutto disinstallare l'agente. A questo scopo, procedere come segue:

1. aprire la console di configurazione di GFI LANguard Portable Storage Control
2. eliminare l'agente dal computer su cui verrà installato GFI EndPointSecurity.

NOTA: questa procedura va eseguita soltanto sul computer su cui sarà installato GFI EndPointSecurity 4.

3. Chiudere l'applicazione della consolle di configurazione di GFI LANguard Portable Storage Control e procedere con l'installazione di GFI EndPointSecurity 4.

4. Quando s'installa GFI EndPointSecurity 4, viene richiesto di confermare se importare le configurazioni dalla versione precedente. Fare clic su **Yes (Si)** per importare le configurazioni.

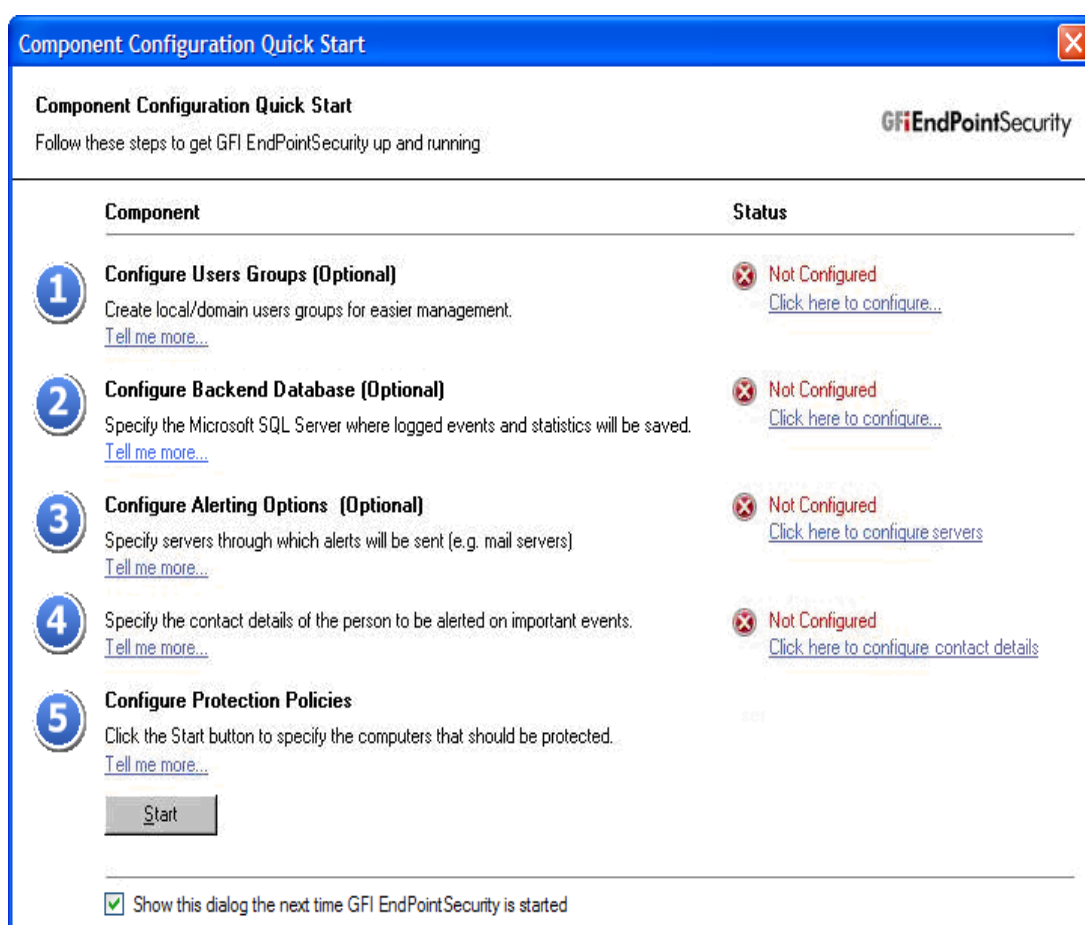
NOTA: gli agenti GFI LANguard Portable Storage Control che proteggevano i computer verranno aggiunti automaticamente a un criterio di protezione di GFI EndPointSecurity 4 chiamato **LegacyAgents (Agenti ereditati)**.

Guida introduttiva

Avvio di GFI EndPointSecurity

Tutte le impostazioni di configurazione di GFI EndPointSecurity sono eseguite con la console di gestione omonima. Per aprire la console di gestione, fare clic su: **Start ▶ Tutti i programmi ▶ GFI EndPointSecurity 4.0 ▶ GFI EndPointSecurity 4.0**

Utilizzo della finestra di dialogo dell'Avvio rapido



Schermata 4 – Finestra di dialogo dell'Avvio rapido di GFI EndPointSecurity

Per impostazione predefinita, la prima volta che viene avviata la console di gestione si apre la finestra di dialogo "Avvio rapido". La finestra aiuta l'utente nella configurazione dei parametri operativi essenziali richiesti da GFI EndPointSecurity in occasione del primo avvio.

I parametri da configurare all'avvio sono:

Gruppi utenti locali o di dominio

Questo parametro crea i gruppi utenti di dominio secondo le categorie dei dispositivi e le porte di connessione, per una gestione più agevole.

Terminale database

Tra i parametri richiesti figurano il nome o l'IP del server SQL e i dati del terminale database da utilizzare per l'archiviazione degli eventi.

Opzioni di avviso

Tra i parametri richiesti figurano i dati del server SMTP e del gateway SMS o del service provider degli avvisi via email o sms.

Dettagli dell'account amministratore di GFI EndPointSecurity

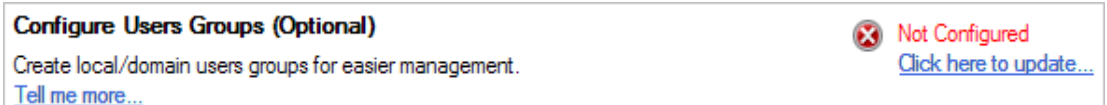
Tra i parametri richiesti figurano l'indirizzo email, il numero di cellulare e il nome o l'IP dei computer cui inviare gli avvisi.

Criteri di protezione

Tra i parametri richiesti figurano i computer da aggiungere al criterio e le credenziali di accesso.

La finestra di dialogo dell'Avvio rapido contiene link alle finestre di dialogo di configurazione da cui impostare direttamente i parametri operativi essenziali.

Configurazione dei gruppi utenti locali o di dominio



Schermata 5 – Finestra di dialogo Avvio rapido: link ai Gruppi utenti

Per creare i gruppi utenti locali o di dominio secondo le categorie di dispositivi e le porte di connessione, fare clic sul link fornito nella finestra di dialogo dell'Avvio rapido. Viene visualizzata la finestra di dialogo "Configure Users Groups (Configurare gruppi utenti)".

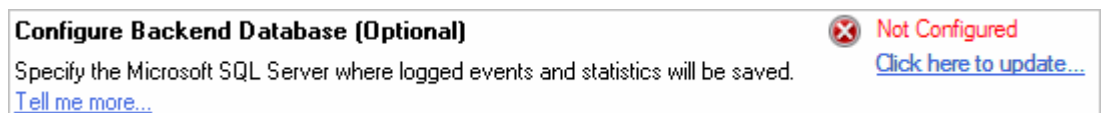


Schermata 6 – Finestra di dialogo della configurazione dei gruppi utenti

1. Selezionare i gruppi utenti da creare per le categorie di dispositivi e le porte di connessione.
2. Fare clic su **Create (Crea)** per creare i gruppi.

NOTA: adesso è quindi possibile gestire le autorizzazioni di accesso al dispositivo o alla porta per determinati utenti, rendendoli membri di uno o più gruppi creati.

Configurazione del terminale database

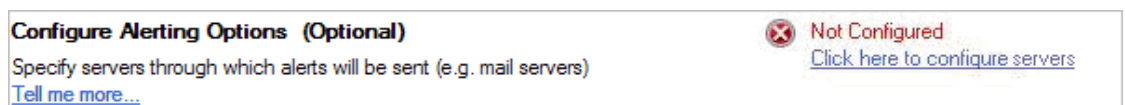


Schermata 7 – Finestra di dialogo Avvio rapido: collegamento alle impostazioni del terminale database

Per configurare le impostazioni del terminale database la prima volta, fare clic sul collegamento fornito nella finestra di dialogo dell'Avvio rapido. Viene visualizzata la finestra di dialogo "Database Options (Opzioni database)".

Per informazioni sulla configurazione del terminale database, si rinvia alla sezione "Configurazione del database terminale" del capitolo "Configurazione delle impostazioni predefinite di GFI EndPointSecurity".

Configurazione delle opzioni di avviso

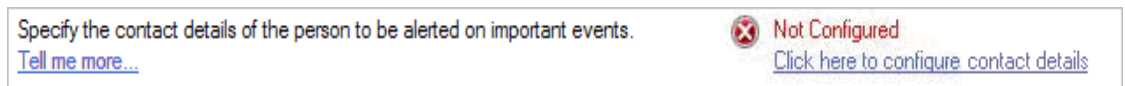


Schermata 8 – Finestra di dialogo Avvio rapido: collegamento alle opzioni di avviso

Per configurare le impostazioni delle opzioni di avviso la prima volta, fare clic sul collegamento **Click here to configure servers (Fare clic qui per configurare i server)** fornito nella finestra di dialogo dell'Avvio rapido. Viene visualizzata la finestra di dialogo "Alerting Options (Opzioni di avviso)".

Per informazioni sulla configurazione delle opzioni di avviso, si rinvia alla sezione "Configurazione delle opzioni di avviso" del capitolo "Configurazione delle impostazioni predefinite di GFI EndPointSecurity".

Configurazione dell'account amministratore di GFI EndPointSecurity

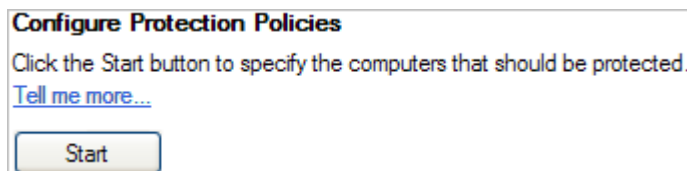


Schermata 9 – Finestra di dialogo Avvio rapido: collegamento alle impostazioni dell'account amministratore

Per configurare le impostazioni del terminale database la prima volta, fare clic sul collegamento **Click here to configure contact details (Fare clic per configurare i dettagli dei contatti)** fornito nella finestra di dialogo dell'Avvio rapido. Viene visualizzata la finestra di dialogo "Proprietà EndPointSecurityAdministrator".

Per informazioni sulla configurazione dell'account amministratore, si rinvia alla sezione "Configurazione dell'account amministratore di GFI EndPointSecurity" del capitolo "Configurazione delle impostazioni predefinite di GFI EndPointSecurity".

Configurazione dei criteri di protezione predefiniti

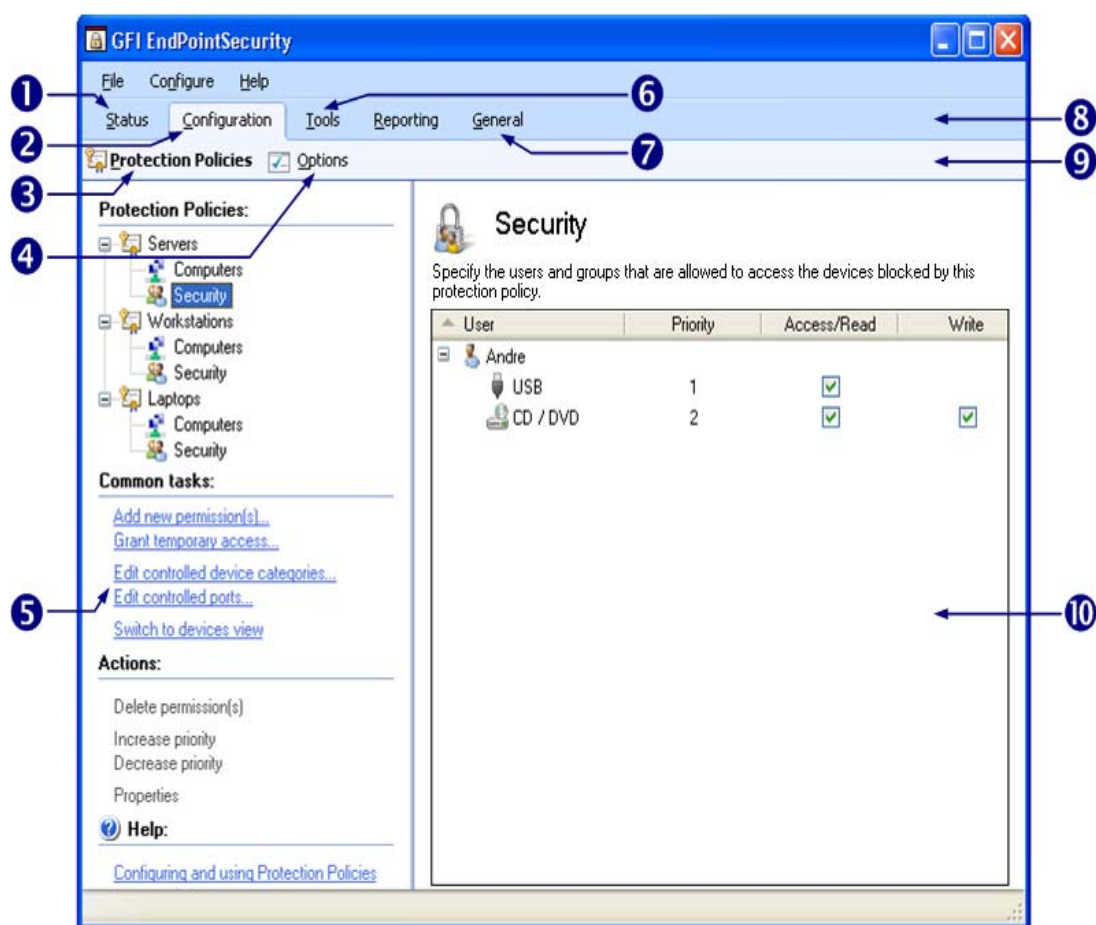


Schermata 10 – Finestra di dialogo Avvio rapido: pulsante Start per la configurazione di criteri di protezione

Per configurare e distribuire i criteri di protezione predefiniti la prima volta, fare clic sul pulsante **Start** fornito nella finestra di dialogo dell'Avvio rapido.

Per informazioni sulla configurazione dei criteri di protezione predefiniti, si rinvia al capitolo "Guida introduttiva: distribuzione del criterio di protezione predefinito".

Navigazione nella consolle di gestione di GFI EndPointSecurity



Schermata 11 – La consolle di gestione GFI EndPointSecurity

1	Opzione <i>Status</i> (Stato): adoperare questa opzione per visualizzare lo stato di GFI EndPointSecurity e le informazioni statistiche sull'accesso al dispositivo.
2	Opzione <i>Configuration</i> (Configurazione): adoperare questa opzione per accedere e configurare i criteri di protezione predefiniti.
3	Opzione <i>Protection policies</i> (Criteri di protezione): adoperare questa opzione per configurare i criteri di protezione, compresi i computer da aggiungere e la sicurezza del dispositivo da applicare.
4	Opzione <i>Options</i>: adoperare questa opzione per configurare impostazioni generali, quali i parametri di avviso predefiniti e i parametri del terminale database.
5	Opzione <i>Left pane</i> (Pannello di sinistra): adoperare questa opzione per navigare nelle opzioni di configurazione supplementari fornite in GFI EndPointSecurity.
6	Opzione <i>Tools</i> (Strumenti): adoperare questa opzione per visualizzare e analizzare gli eventi con il Browser di log ed eseguire scansioni dei dispositivi sulla rete.
7	Opzione <i>General</i> (Generale): adoperare questa opzione per ricercare aggiornamenti del prodotto o visualizzare la

	versione e le informazioni di licenza.
8	Tabs (Schede): queste schede contengono le opzioni di configurazione principali fornite in GFI EndPointSecurity.
9	Options Tab (Scheda opzioni): la scheda Opzioni contiene le opzioni di configurazione facendo clic sulle schede.
10	Right Pane (Pannello di destra): adoperare questo pannello per sfogliare i computer di un criterio di protezione, la sicurezza dei dispositivi configurata, i risultati di scansione dei dispositivi, gli eventi generati dal servizio e dall'accesso ai dispositivi, le informazioni di licenza e sulla versione del prodotto.

Guida introduttiva: distribuzione del criterio di protezione predefinito

Introduzione

GFI EndPointSecurity contiene tre criteri di protezione predefiniti, distribuibili immediatamente sui computer target subito dopo l'installazione:

- criterio di protezione server
- criterio di protezione stazioni di lavoro
- criterio di protezione computer portatili.

I criteri di protezione predefiniti bloccano l'accesso a tutti i dispositivi su tutte le porte di connessione. Per distribuire un criterio di protezione è necessario specificare i seguenti dettagli:

- i computer su cui il criterio verrà distribuito
- le credenziali di accesso con cui distribuire il criterio.

GFI EndPointSecurity consente inoltre di personalizzare i criteri di protezione predefiniti e di crearne di nuovi. Per informazioni sulle modalità di esecuzione di tali operazioni, si rinvia al capitolo "Personalizzazione del criterio di protezione predefinito".

Preparazione della distribuzione del criterio di protezione

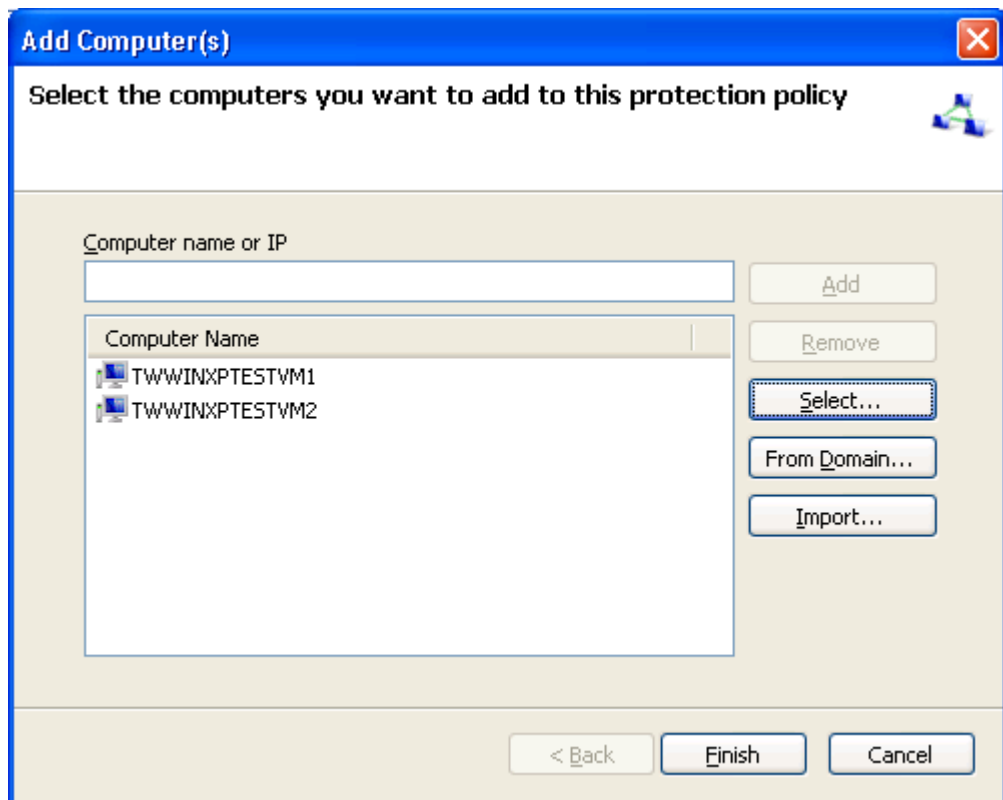
Per accedere ai criteri di protezione predefiniti, seguire questa procedura:

1. Fare clic sulla scheda **Configuration (Configurazione)**
2. Fare clic su **Protection Policies (Criteri di protezione)**
3. Nel pannello di sinistra, selezionare il criterio di protezione da distribuire.

Configurazione dei computer da proteggere

Per aggiungere computer al criterio di protezione selezionato, seguire questa procedura:

1. Nel pannello di destra, fare clic sull'opzione **Add computers to this policy (Aggiungi computer a questo criterio)** della sezione **Computers**.

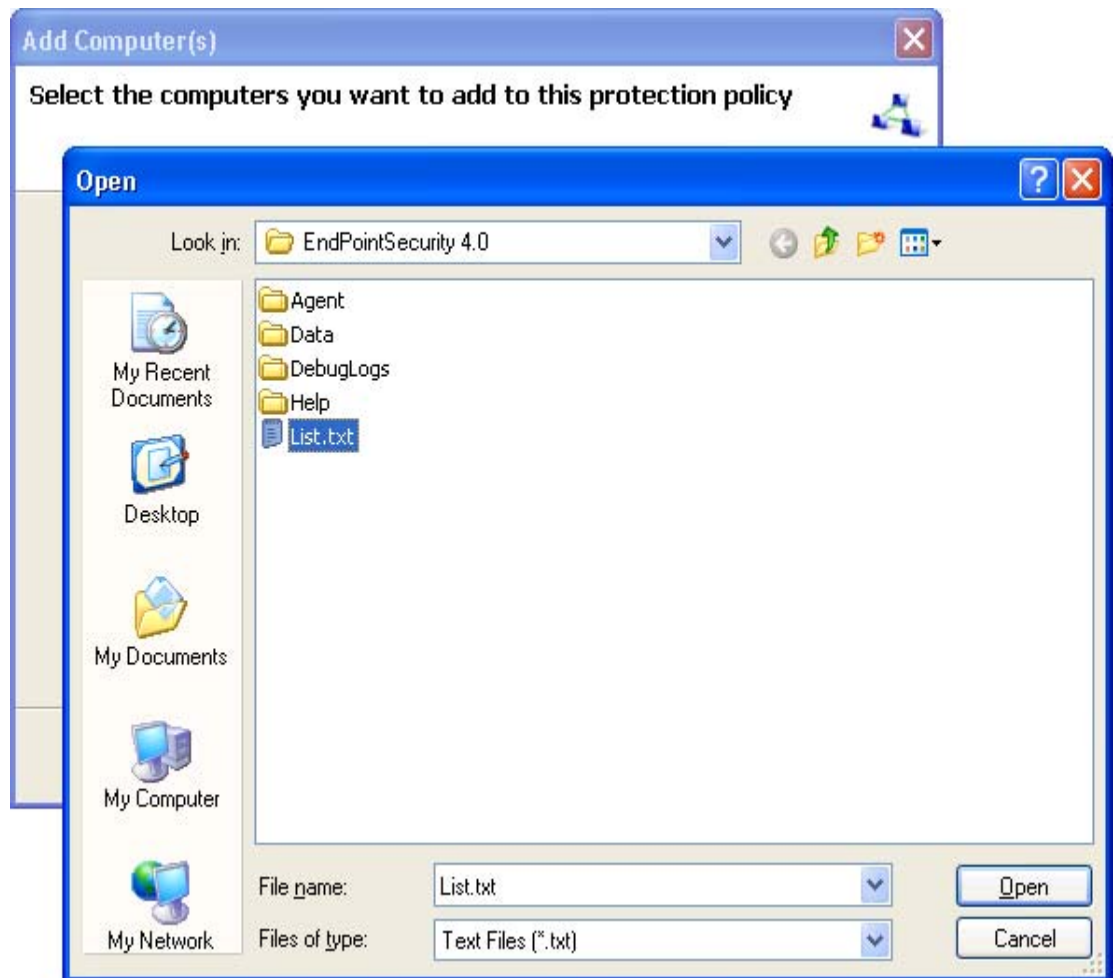


Schermata 12 – Selezione dei computer da aggiungere al criterio

2. Indicare il nome o IP del computer da aggiungere e fare clic su **Add (Aggiungi)**. Ripetere l'operazione finché sono stati specificati tutti i computer da aggiungere al criterio di protezione interessato.

NOTA 1: al fine di selezionare i target da un elenco, fare clic su **Select (Seleziona)** per visualizzare la finestra di dialogo *Select Computer* (Seleziona computer). Fare quindi clic su **Search (Cerca)** in questa finestra di dialogo per elencare i computer di uno dominio specifico.

NOTA 2: per selezionare i computer del dominio su cui risiede la console di gestione di GFI EndPointSecurity, fare clic su **From Domain (Dal dominio)**.



Schermata 13 – Importazione dei computer da aggiungere al criterio

NOTA 3: per importare l'elenco di computer da un file di testo, fare clic su **Import (Importa)**.

3. Fare clic su **Finish (Fine)** per completare le impostazioni.

Credenziali di configurazione

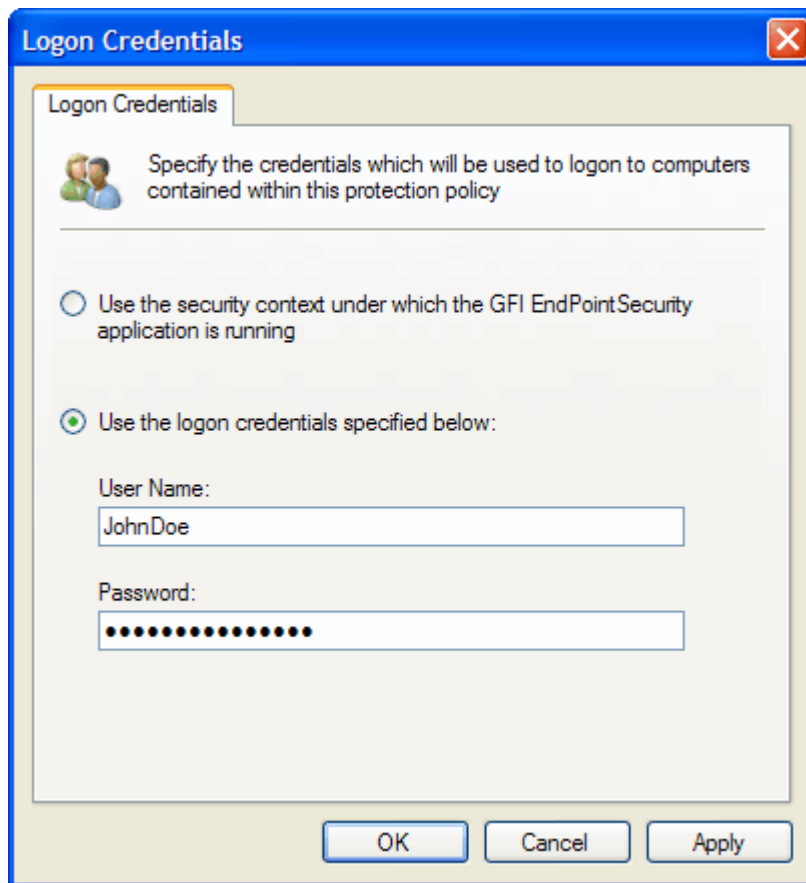
GFI EndPointSecurity richiede di accedere fisicamente ai computer target per:

- distribuire gli agenti e gli aggiornamenti dei criteri di protezione;
- tenere sotto controllo lo stato della protezione di tutti i computer target.

Il prodotto deve perciò essere eseguito con un account munito di privilegi amministrativi sui target della rete (per esempio, l'account dell'amministratore di dominio).

NOTA: per impostazione predefinita, GFI EndPointSecurity è configurato per utilizzare il contesto di sicurezza in cui è eseguito (cioè, le credenziali dell'utente collegato in quel momento).

Per indicare credenziali diverse da quelle del contesto di sicurezza corrente:



Schermata 14 – Impostazione credenziali di accesso

1. Nel pannello di destra, fare clic su **Set Log-on Credentials (Impostare credenziali di accesso)** della sezione **Computers**.
2. indicare il nome e la password di login da adoperare per collegarsi ai computer target.
3. Fare clic su **OK** per completare le impostazioni.

Distribuzione di un criterio di protezione predefinito

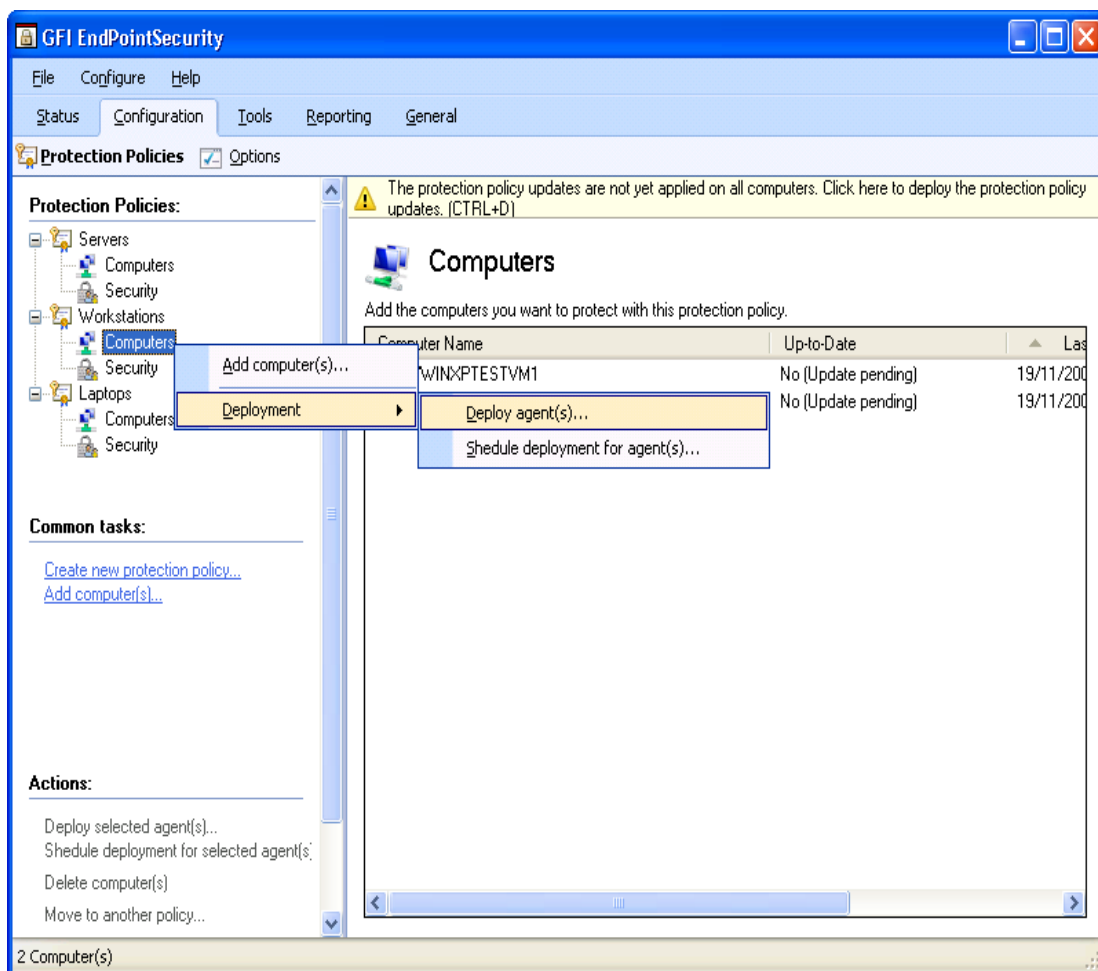
Dopo aver aggiunto i computer a un criterio di protezione e specificato le credenziali di accesso, è quindi possibile distribuire il criterio sui computer target. Si può distribuire il criterio immediatamente ovvero se ne può pianificare la distribuzione.

NOTA: quando distribuisce il criterio su un computer target per la prima volta, GFI EndPointSecurity installa automaticamente un agente su quel computer. L'agente elabora tutte le richieste di lettura e scrittura effettuate ai dispositivi portatili, adoperando come riferimento il criterio di protezione distribuito. Questo vale anche per i computer i cui agenti erano stati disinstallati in precedenza.

Distribuzione immediata

Per distribuire immediatamente un criterio di protezione sui target selezionati, seguire questa procedura:

1. Fare clic sulla scheda **Configuration (Configurazione)**.
2. Fare clic su **Protection Policies (Criteri di protezione)**



Schermata 15 – Distribuzione di agenti

3. Nel pannello di sinistra, fare clic con il pulsante destro del mouse sul criterio di protezione da distribuire e selezionare **Deployment ► Deploy agent(s) (Distribuzione ► Distribuisci agenti)**.

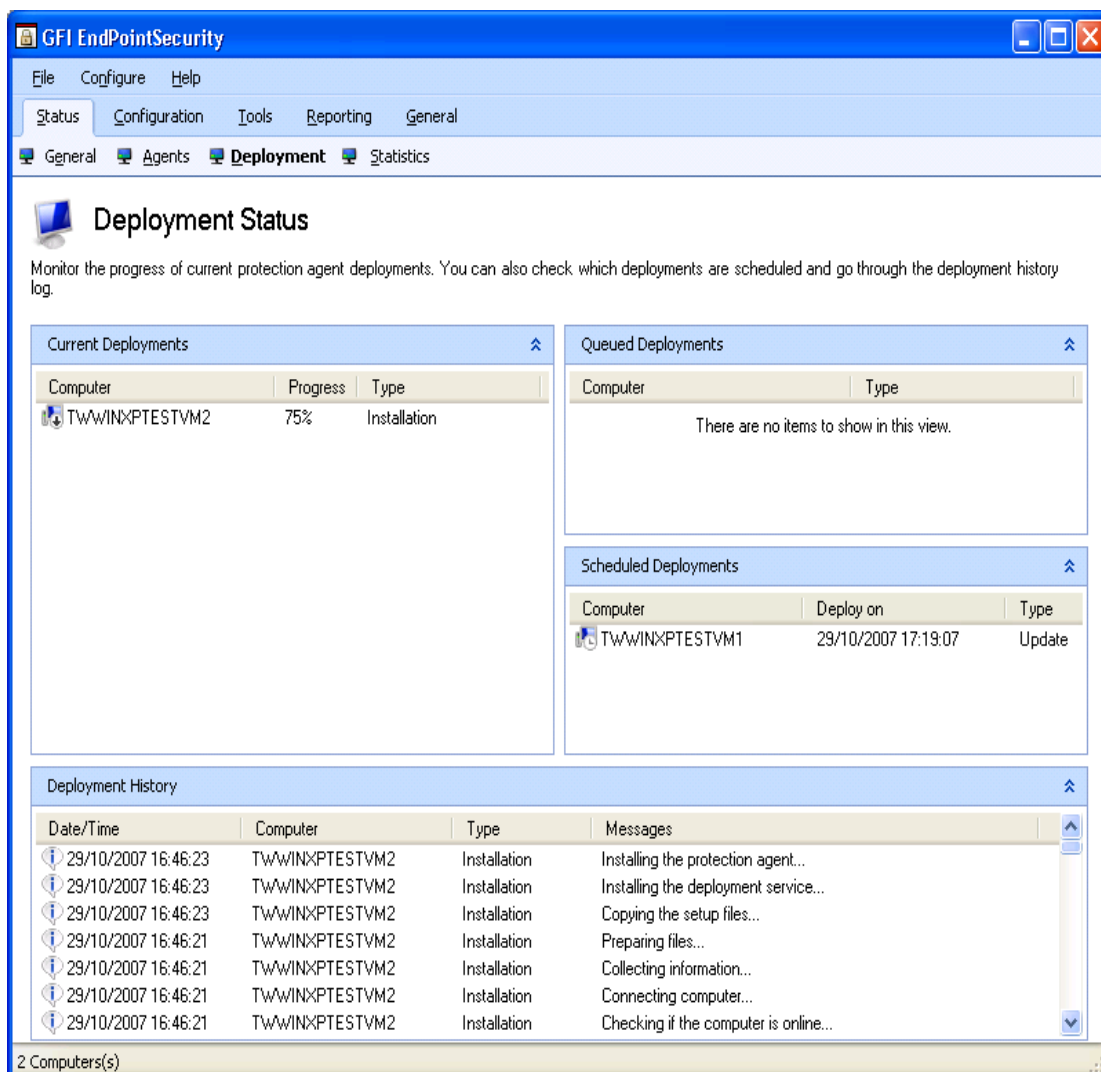
NOTA: per eseguire questo passaggio, è anche possibile adoperare la scelta rapida di tastiera **CTRL + D**.

4. Dalla finestra di dialogo *Select computers for deployment* (Selezionare i computer per la distribuzione), selezionare i computer sui quali distribuire il criterio.

NOTA 1: i computer target elencati sono quelli che sono stati aggiunti al criterio di protezione.

NOTA 2: per impostazione predefinita vengono selezionati tutti i computer selezionati.

5. Fare clic su **OK** per iniziare la distribuzione.



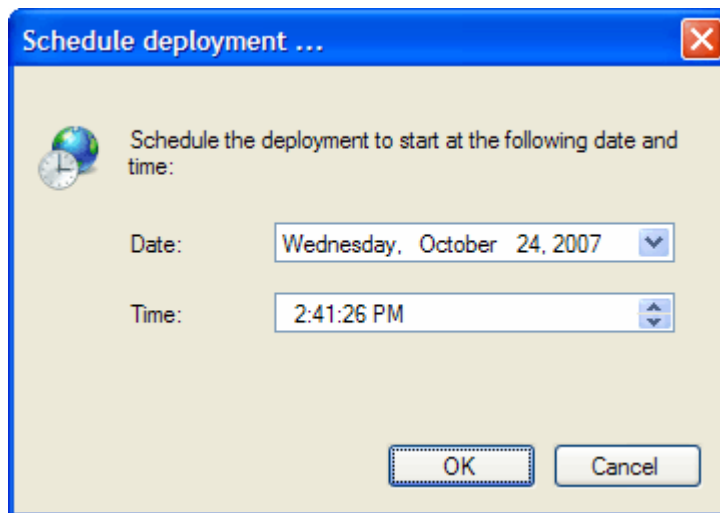
Schermata 16 – Visualizzazione stato della distribuzione

NOTA: GFI EndPointSecurity va automaticamente sulla visualizzazione *Deployment Status* (Stato distribuzione) della console di gestione, dove è possibile vedere il progresso della distribuzione.

Pianificazione della distribuzione

Per pianificare la distribuzione di un criterio di protezione sui target selezionati, seguire questa procedura:

1. Fare clic sulla scheda **Configuration (Configurazione)**.
2. Fare clic su **Protection Policies (Criteri di protezione)**
3. Nel pannello di sinistra, fare clic on il pulsante destro del mouse sul criterio di protezione da distribuire e selezionare **Deployment ► Schedule deployment for agent(s) (Distribuzione ► Pianifica distribuzione per gli agenti)**.
4. Dalla finestra di dialogo *Select computers for deployment* (Selezionare i computer per la distribuzione), selezionare i computer sui quali distribuire il criterio.



Schermata 17 – Impostazione distribuzione pianificata

5. Indicare la data e l'ora dell'avvio della distribuzione.

NOTA: la distribuzione pianificata continuerà anche se l'applicazione della consolle di gestione di GFI EndPointSecurity non è in esecuzione.

La distribuzione di un criterio di protezione attraverso Active Directory

È possibile creare un pacchetto d'installazione Windows (file MSI) che è possibile poi distribuire tramite Active Directory Group Policies (Criteri di gruppo di Active Directory) sui client del dominio.

Per creare il pacchetto d'installazione di Windows, seguire questa procedura:

1. Fare clic sulla scheda **Configuration (Configurazione)**.
2. Fare clic su **Protection Policies (Criteri di protezione)**
3. Nel pannello di sinistra, selezionare il criterio di protezione da distribuire tramite Active Directory.
4. Nel pannello di destra, fare clic su **Deploy through Active Directory (Distribuisci tramite Active Directory)** della sezione **Computers**.
5. Indicare il nome file MSI e fare clic su **Save (Salva)**.

Per informazioni sulle modalità di utilizzare i Criteri di gruppo di Active Directory per distribuire software, si rinvia all'articolo di knowledgebase intitolato "Utilizzo dei Criteri di gruppo per l'installazione remota di software in Windows Server 2003" all'indirizzo <http://support.microsoft.com/kb/816102>.

Verifica dello stato di distribuzione del criterio di protezione

Cronologia della distribuzione

Date/Time	Computer	Type	Messages
19/11/2007 12:51:39	TWWINXPTESTVM1	Installation	The deployment was completed.
19/11/2007 12:50:32	TWWINXPTESTVM1	Installation	Installing the protection agent...
19/11/2007 12:50:31	TWWINXPTESTVM1	Installation	Installing the deployment service...
19/11/2007 12:50:31	TWWINXPTESTVM1	Installation	Copying the setup files...
19/11/2007 12:50:28	TWWINXPTESTVM1	Installation	Preparing files...
19/11/2007 12:50:28	TWWINXPTESTVM1	Installation	An older version of GFI EndPointSecurity agent (version 4 build 20071022) detected. Reinstallation is required.
19/11/2007 12:48:55	TWWINXPTESTVM1	Update	Collecting information...
19/11/2007 12:48:55	TWWINXPTESTVM1	Update	Connecting computer...

Schermata 18 – Cronologia della distribuzione

Il processo di distribuzione del criterio genera un audit trail per ciascuna fase del processo. È possibile visualizzare l'audit trail mediante la sezione "Cronologia della distribuzione" situata in fondo alla visualizzazione "Stato della distribuzione".

Utilizzare le informazioni visualizzate per determinare se la distribuzione è stata completata correttamente su ogni computer target o se si sono verificati degli errori.

Per visualizzare la cronologia della visualizzazione:

1. Fare clic sulla scheda **Status (Stato)**.
2. Fare clic su **Deployment (Distribuzione)**.

Stato degli agenti

Computer	Protection Policy	Up-to-date	Status
TMJASON-CLIENT1	Servers	Yes	Online (Last message received at: 30/10/2007 10:05:18)
TWWINXPTESTVM1	Workstations	Yes	Online (Last message received at: 30/10/2007 10:05:38)
TWWINXPTESTVM2	Workstations	Yes	Online (Last message received at: 30/10/2007 10:05:48)

Schermata 19 – Visualizzazione stato degli agenti

Adoperare la visualizzazione "Stato degli agenti" per determinare lo stato di tutte le operazioni di distribuzione eseguite sui target della propria rete. Per ogni computer target, le informazioni visualizzate illustrano:

- se la distribuzione è aggiornata
- se la distribuzione è stata pianificata
- se il computer target è in linea.

NOTA 1: se la distribuzione di un criterio sul computer target non riesce, viene automaticamente pianificato un altro tentativo di distribuzione un'ora più tardi.

NOTA 2: viene utilizzato il "ping" per determinare se un computer target è in linea.

Per visualizzare lo stato degli agenti, seguire questa procedura:

1. Fare clic sulla scheda **Status (Stato)**.
2. Fare clic su **Agents (Agenti)**.

Monitoraggio dell'attività di utilizzo del dispositivo

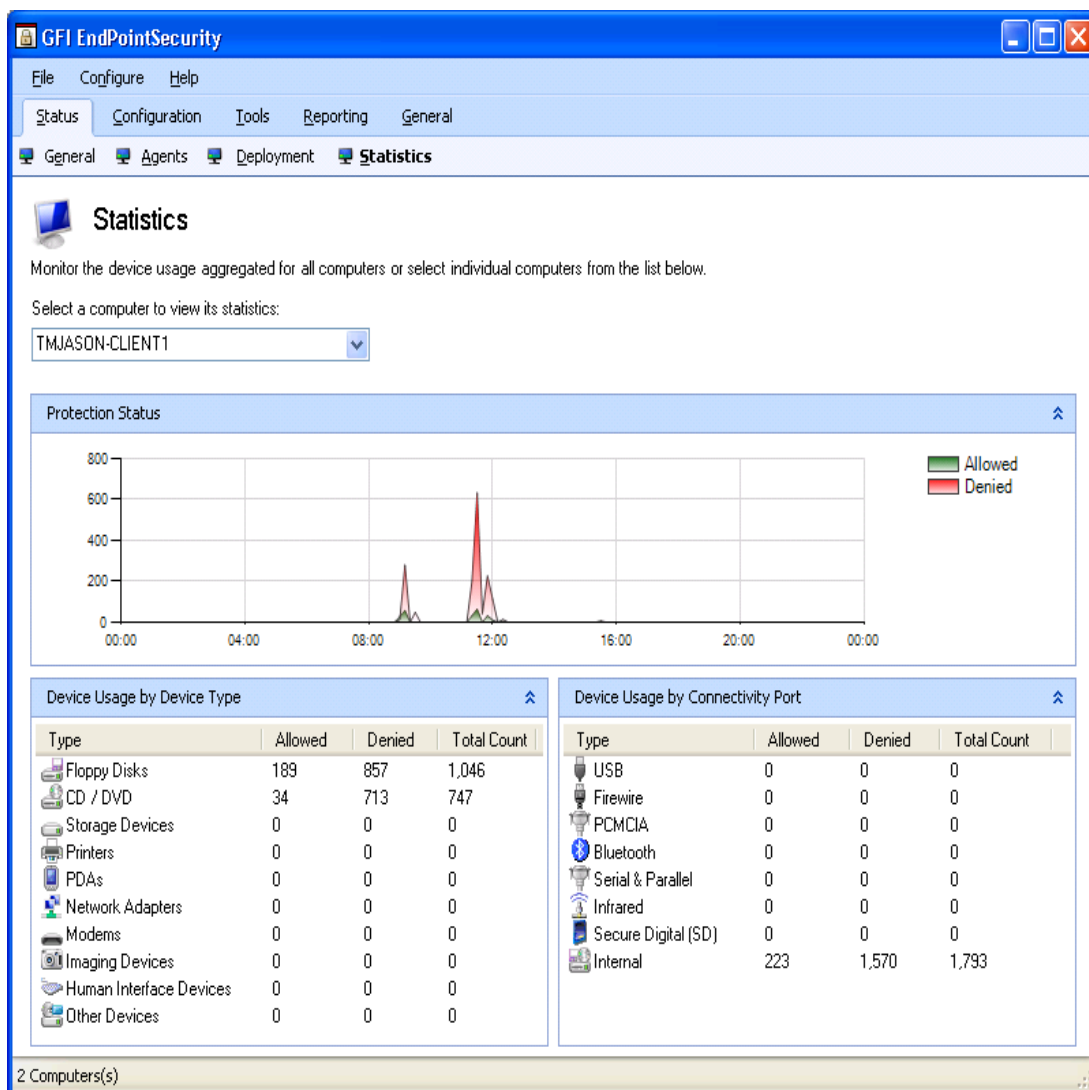
Introduzione

GFI EndPointSecurity consente di controllare l'attività dell'uso del dispositivo sui computer protetti quasi in tempo reale. È possibile effettuare questa operazione attraverso:

- la visualizzazione delle Statistiche
- scansioni del dispositivo
- il browser dei log
- avvisi
- i rapporti creati dal ReportPack di GFI EndPointSecurity.

Utilizzo della visualizzazione delle Statistiche

Adoperare l'opzione **Statistics (Statistiche)** per visualizzare gli andamenti e statistiche dell'attività quotidiana del dispositivo relativi a un computer specifico o a tutti i computer della rete. Le informazioni fornite con questa modalità di visualizzazione sono riportate in apposite sezioni separate. Di seguito si forniscono informazioni più dettagliate su dette sezioni.

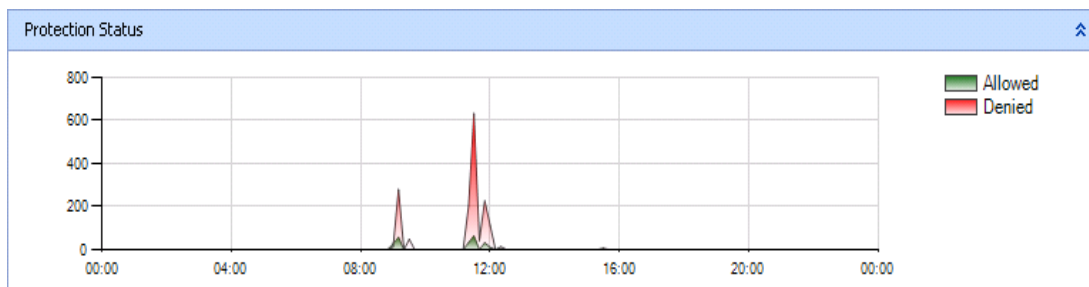


Schermata 20 – Visualizzazione delle Statistiche

Per accedere alla visualizzazione delle Statistiche, seguire questa procedura:

1. Fare clic sulla scheda **Status (Stato)**.
2. Fare clic su **Statistics (Statistiche)**.

Stato della protezione



Schermata 21 – Visualizzazione dello stato della protezione

La presente sezione illustra graficamente i tentativi di connessione al dispositivo autorizzati o negati, sia per singolo computer che in base

alla rete. Viene adoperato uno schema di colori per distinguere le connessioni autorizzate da quelle negate.

Utilizzo del dispositivo secondo il tipo

Type	Allowed	Denied	Total Count
Floppy Disks	189	857	1,046
CD / DVD	34	713	747
Storage Devices	0	0	0
Printers	0	0	0
PDA's	0	0	0
Network Adapters	0	0	0
Modems	0	0	0
Imaging Devices	0	0	0
Human Interface Devices	0	0	0
Other Devices	0	0	0

Schermata 22 – Utilizzo del dispositivo secondo il tipo

La presente sezione elenca i tentativi di connessione al dispositivo, autorizzati o negativi, secondo il tipo del dispositivo. Si forniscono informazioni per un computer specifico o per tutti i computer della rete.

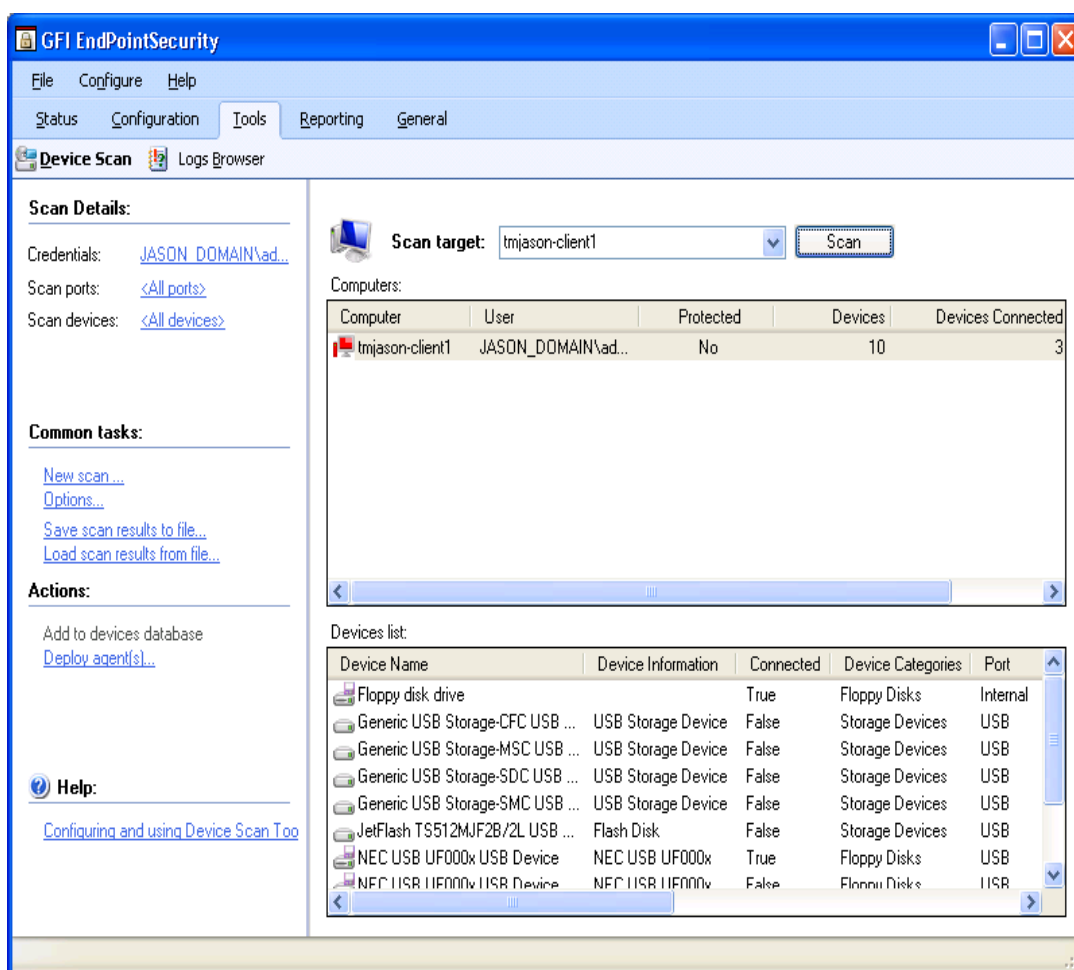
Utilizzo del dispositivo secondo la porta di connessione

Type	Allowed	Denied	Total Count
USB	0	0	0
Firewire	0	0	0
PCMCIA	0	0	0
Bluetooth	0	0	0
Serial & Parallel	0	0	0
Infrared	0	0	0
Secure Digital (SD)	0	0	0
Internal	223	1,570	1,793

Schermata 23 – Utilizzo del dispositivo secondo la porta di connessione

La presente sezione elenca i tentativi di connessione al dispositivo, autorizzati o negativi, secondo la porta di connessione. Si forniscono informazioni per un computer specifico o per tutti i computer della rete.

Utilizzo della scansione dispositivi



Schermata 24 – Scansione dispositivi di GFI EndPointSecurity

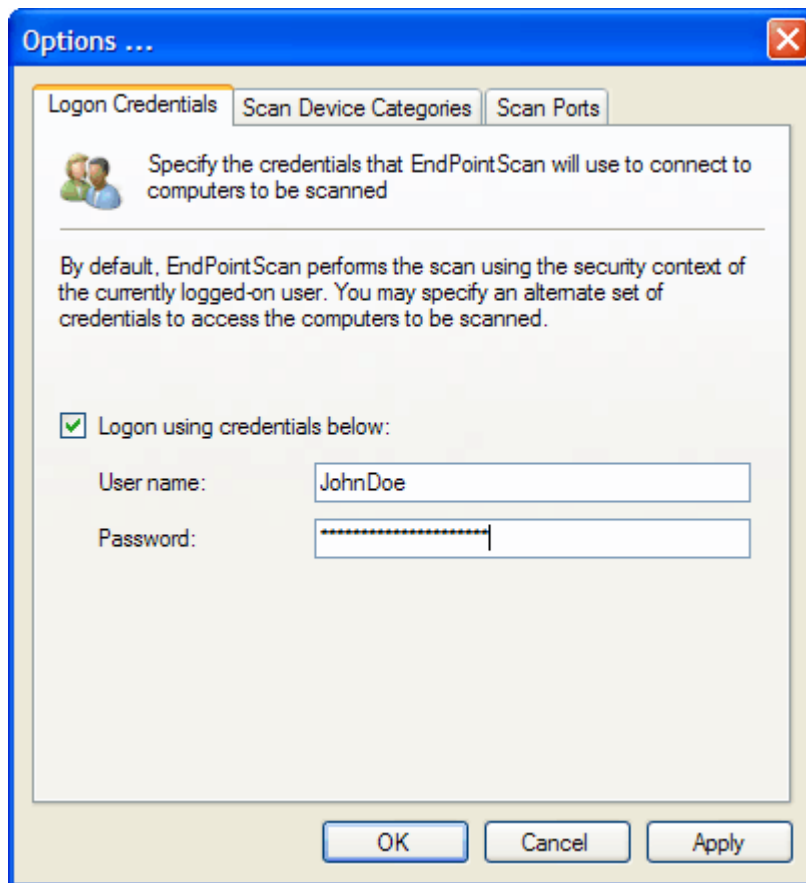
Adoperare l'opzione *Device Scan* (Scansione dispositivi) per interrogare, in modo trasparente e rapido, endpoint (punti finali) della rete aziendale, localizzare e riportare tutti i dispositivi che sono correntemente connessi al target di scansione o che lo sono stati. L'applicazione identifica in modo granulare i dispositivi endpoint connessi al target, sia correntemente che in passato, e visualizza informazioni dettagliate sullo schermo una volta completata la scansione.

NOTA 1: il target di scansione può essere qualsiasi computer della rete, anche se non compreso nel criterio di protezione di GFI EndPointSecurity.

NOTA 2: la scansione del dispositivo va eseguita con un account munito di privilegi amministrativi sul target di scansione.

Per eseguire una scansione di dispositivi, seguire questa procedura:

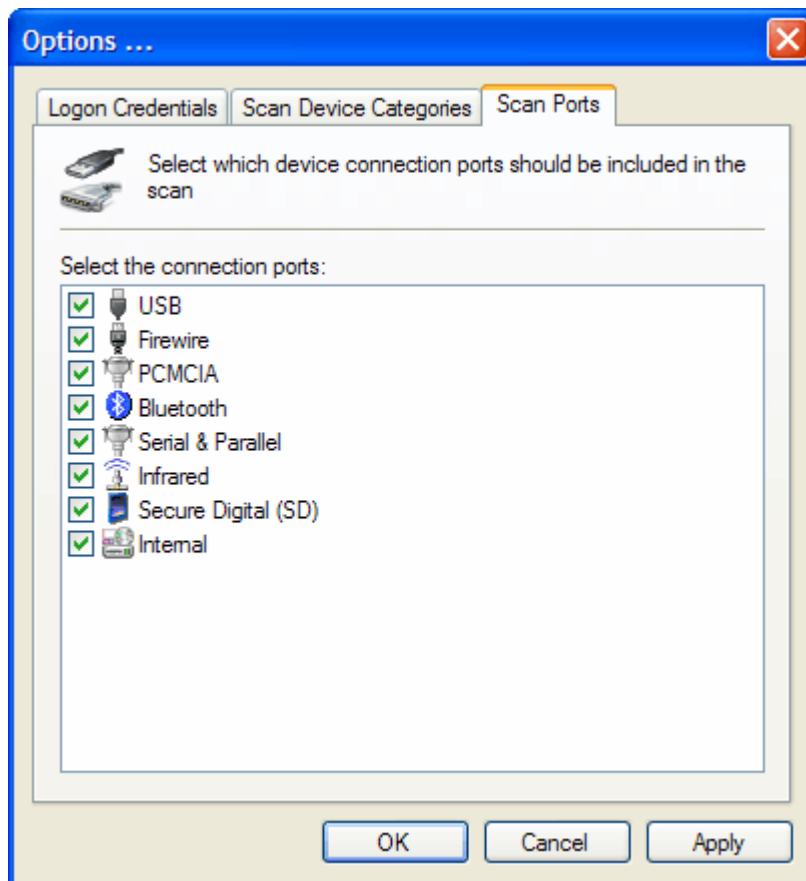
1. Selezionare la scheda **Tools (Strumenti)**.
2. Fare clic su **Device Scan (Scansione dispositivi)**.
3. Nel pannello di destra, specificare il target di scansione.



Schermata 25 – Credenziali del target di scansione

4. Nel pannello di sinistra, fare clic sul link *Credentials* (Credenziali) della sezione *Scan Details* (Dettagli scansione). Indicare le credenziali che GFI EndPointSecurity dovrà utilizzare per collegarsi al target di scansione e fare clic su **OK**.

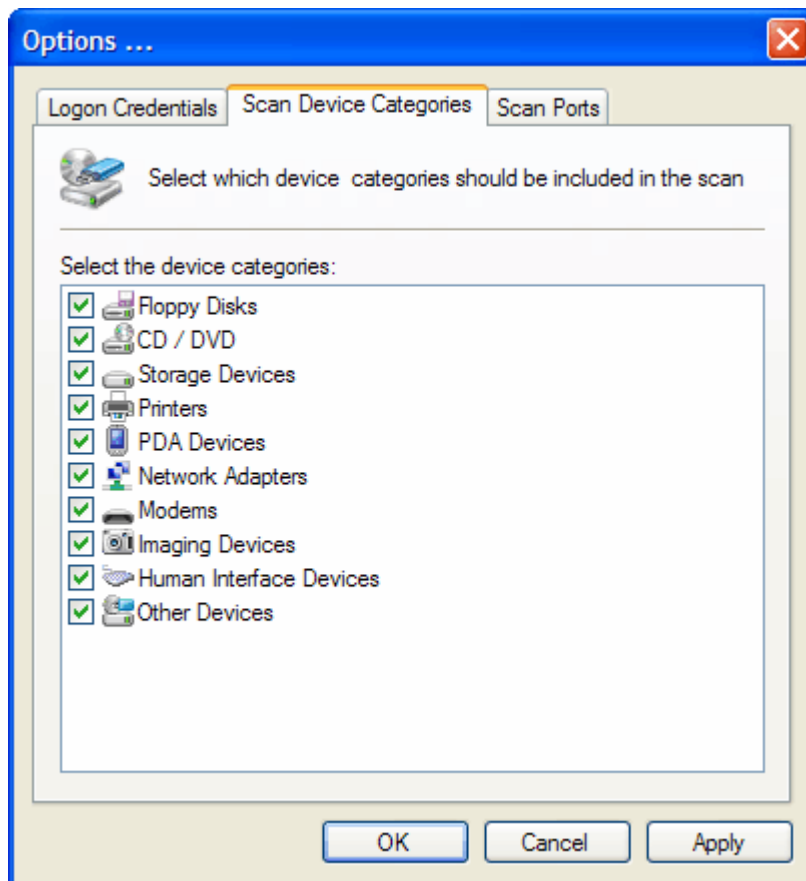
NOTA: per impostazione predefinita, GFI EndPointSecurity esegue la scansione adoperando il contesto di sicurezza su cui il software gira (cioè, le credenziali dell'utente collegato in quel momento).



Schermata 26 – Porte del target di scansione

5. Nel pannello di sinistra, fare clic sul link *Scan ports* (Porte di scansione) della sezione *Scan Details* (Dettagli scansione). Indicare le porte di connessione al dispositivo da includere nella scansione.

NOTA: per impostazione predefinita, GFI EndPointSecurity esegue la scansione di tutte le porte di connessione supportate.



Schermata 27 – Porte di connessione del target di scansione

6. Nel pannello di sinistra, fare clic sul link *Scan Device Categories* (Categorie dispositivi di scansione) della sezione *Scan Details* (Dettagli scansione). Indicare le categorie di dispositivi da includere nella scansione.

NOTA: per impostazione predefinita, GFI EndPointSecurity esegue la scansione di tutte le categorie di dispositivi supportate.

7. Nel pannello di destra, fare clic su **Scan (Esegui scansione)** per avviare il processo.

Risultati di scansione

I risultati di scansione vengono visualizzati in due sezioni:

- Computer
- Elenco dispositivi

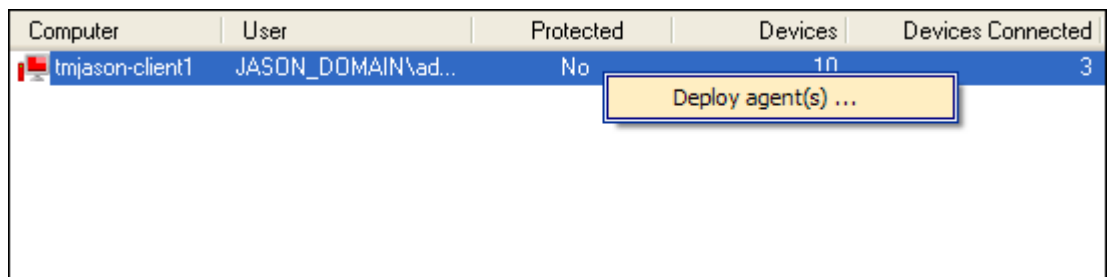
Computer	User	Protected	Devices	Devices Connected
tmjason-client1	JASON_DOMAIN\ad...	No	10	3

Schermata 28 – Risultati di scansione del dispositivo – sezione Computer

La sezione Computer visualizza risultati di scansione riepilogativi, compresi:

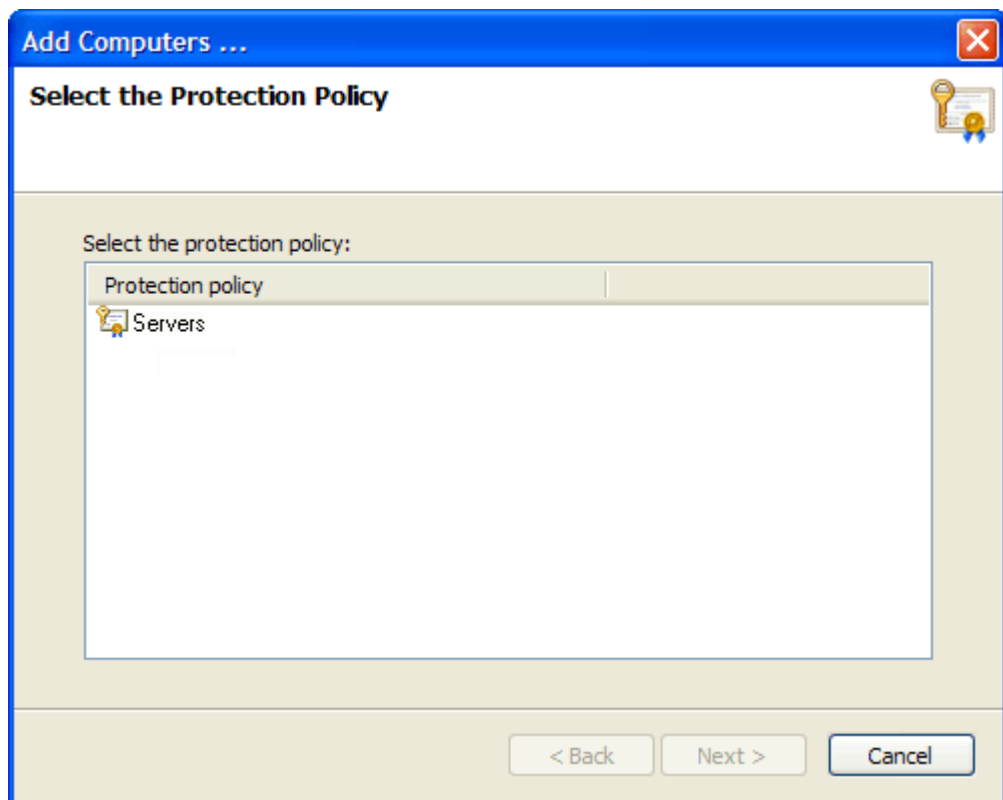
- il nome o l'IP del target di scansione
- l'utente collegato in quel momento
- lo stato della protezione, ossia, se il computer è incluso in un criterio di protezione di GFI EndPointSecurity
- il numero totale di dispositivi collegati in quel momento o che lo siano stati in precedenza
- il numero di dispositivi collegati in quel momento.

Se il target di scansione non è compreso in nessun criterio di protezione di GFI EndPointSecurity, è possibile scegliere di distribuirne uno sul computer. A questo scopo, seguire questa procedura:



Schermata 29 – Distribuzione agenti

1. Fare clic sul computer con il pulsante destro del mouse
2. Selezionare **Deploy agent(s) (Distribuisci agente/i)**



Schermata 30 – Selezione del criterio di protezione da distribuzione

3. Selezionare il criterio di protezione da distribuire. Fare clic su **Next (Avanti)** per continuare e su **Finish (Fine)** per avviare la distribuzione.

Device Name	Device Information	Connected	Device Categories	Port
Floppy disk drive		True	Floppy Disks	Internal
Generic USB Storage-CFC USB ...	USB Storage Device	False	Storage Devices	USB
Generic USB Storage-MSC USB ...	USB Storage Device	False	Storage Devices	USB
Generic USB Storage-SDC USB ...	USB Storage Device	False	Storage Devices	USB
Generic USB Storage-SMC USB ...	USB Storage Device	False	Storage Devices	USB
JetFlash TS512MJF2B/2L USB ...	Flash Disk	False	Storage Devices	USB
NEC USB UF000x USB Device	NEC USB UF000x	True	Floppy Disks	USB

Schermata 31 – Sezione Elenco dispositivi

La sezione Elenco dispositivi visualizza risultati di scansione dettagliati, compresi:

- nome dispositivo, descrizione e categoria
- porta di connessione
- stato di connessione, ossia, se il dispositivo è collegato in quel momento.

È possibile selezionare uno o più dispositivi forniti nell'elenco e aggiungerli al database di dispositivi. Il database è adoperato quando si specificano i dispositivi da inserire nelle blacklist o nelle whitelist. Per informazioni sulle blacklist e whitelist, si rinvia alle apposite sezioni del capitolo "Personalizzazione del criterio di protezione predefinito".

Per aggiungere dispositivi all'apposito database, seguire questa procedura:

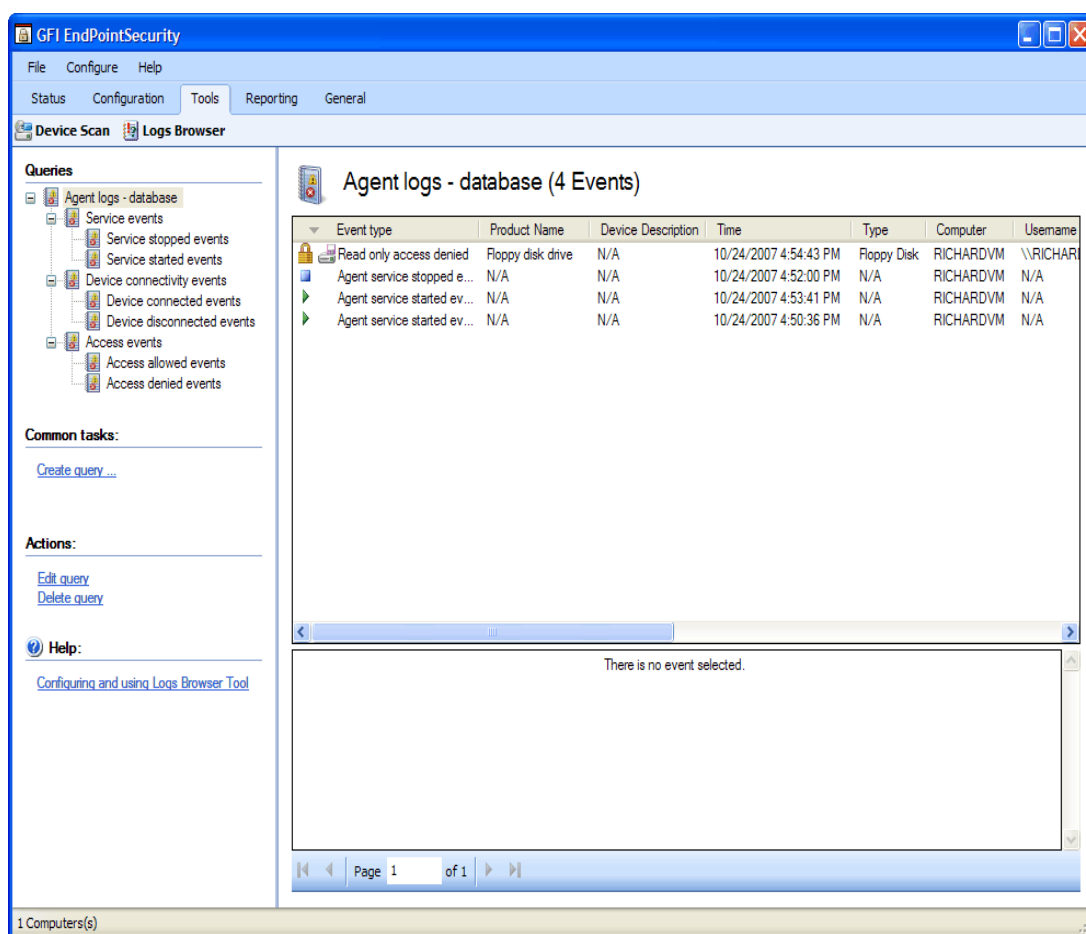
Device Name	Device Information	Connected	Device Categories	Port
Floppy disk drive		True	Floppy Disks	Internal
Generic USB Storage-CFC USB ...	USB Storage Device	False	Storage Devices	USB
Generic USB Storage-MSC USB ...	USB Storage Device	False	Storage Devices	USB
Generic USB Storage-SDC USB ...	USB Storage Device	False	Storage Devices	USB
Generic USB Storage-SMC USB ...	USB Storage Device	False	Storage Devices	USB
JetFlash TS512MJF2B/2L USB ...	Flash Disk			USB
NEC USB UF000x USB Device	NEC USB UF000x			USB

Add to devices database

Schermata 32 – Aggiunta di un dispositivo all'apposito database

1. Nella sezione *Devices list* (Elenco dispositivi), selezionare uno o più dispositivi da aggiungere.
2. Fare clic con il pulsante destro del mouse sui dispositivi scelti e selezionare **Add to devices database (Aggiungi a database dispositivi)**.

Utilizzo del Browser dei log



Schermata 33 – Browser dei log di GFI EndPointSecurity

GFI EndPointSecurity consente di tenere un audit trail di tutti gli eventi generati dagli agenti GFI EndPointSecurity distribuiti sui computer della rete. È possibile archiviare gli eventi in un log di eventi di Windows e/o su un terminale database Microsoft SQL Server.

NOTA: per tenere l'audit trail, è necessario abilitare la registrazione (logging). Per informazioni a questo proposito, si rinvia alla sezione "Configurazione registrazione e notifiche di eventi" del capitolo "Personalizzazione del criterio di protezione predefinito".

Adoperare la visualizzazione "Browser dei log" per accedere e sfogliare gli eventi archiviati in quel momento sul terminale database. I dati degli eventi sono organizzati in colonne e, facendo clic su un dato evento, verranno visualizzate ulteriori informazioni in un apposito pannello descrittivo degli eventi.

GFI EndPointSecurity comprende inoltre un query builder per semplificare la ricerca di eventi specifici. Adoperando il query builder degli eventi, è possibile creare filtri personali che vagliano i dati degli eventi e visualizzano soltanto le informazioni da sfogliare ricercate, senza eliminare un singolo record dal terminale database.

Per accedere alla visualizzazione "Browser dei log", seguire questa procedura:

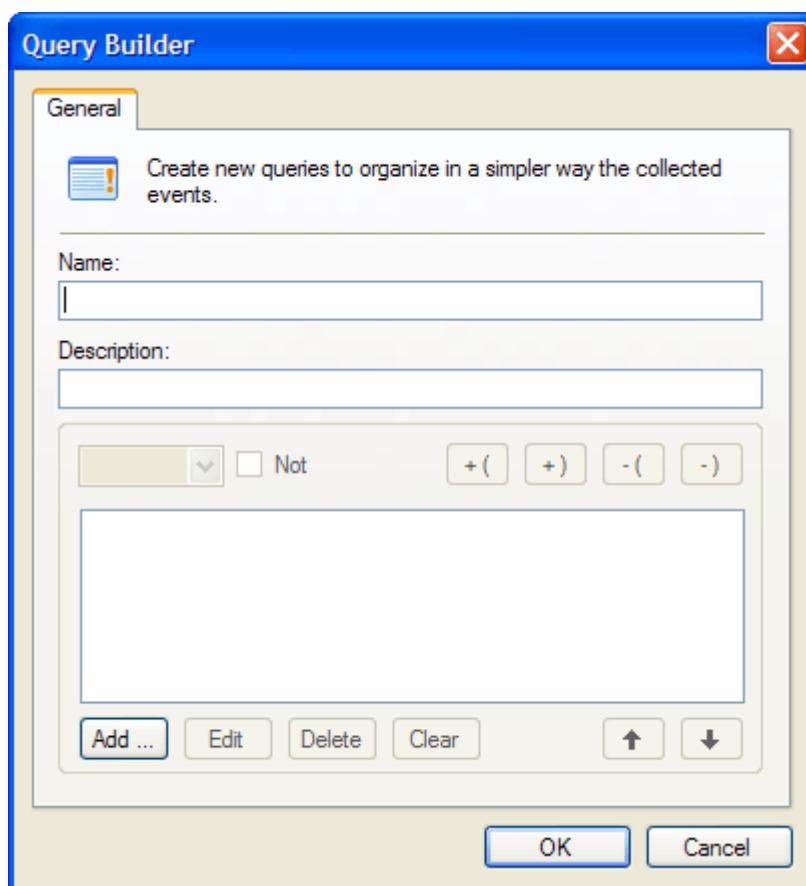
1. Selezionare la scheda **Tools (Strumenti)**.

2. Fare clic su **Logs Browser (Browser dei log)**.
3. Nel pannello di sinistra, selezionare l'opzione **Agent logs – database (Log agenti: database)** per elencare tutti gli eventi archiviati in quel momento sul terminale database.

Creazione delle query di eventi

Per creare query di eventi personalizzate, seguire questa procedura:

1. Selezionare la scheda **Tools (Strumenti)**.
2. Fare clic su **Logs Browser (Browser dei log)**.
3. Nel pannello di sinistra, selezionare l'opzione **Agent logs – database (Log agenti: database)**.
4. Fare clic con il pulsante destro del mouse e selezionare **Create query... (Crea query)**. Verrà visualizzato il query builder degli eventi.



Schermata 34 – Creazione di una nuova query

5. Indicare un nome e una descrizione per la nuova query.
6. Fare clic su **Add (Aggiungi)**, configurare le condizioni richieste per la query e fare clic su **OK**. Ripetere la procedura finché si sono specificate tutte condizioni di query.
7. Fare clic su **OK** per completare le impostazioni. La query personalizzata viene aggiunta a un sub-nodo di **Agent logs – database (Log agenti: database)**.

Utilizzo di avvisi

Quando viene generato un determinato evento, GFI EndPointSecurity può inviare avvisi a specifici destinatari. È possibile configurare avvisi da inviare mediante:

- Email
- Messaggi di rete
- Messaggi SMS

È altresì possibile indicare i tipi di eventi in relazione ai quali si desidera inviare gli avvisi:

- Eventi di servizio
- Eventi relativi alla connessione al dispositivo
- Eventi relativi alla disconnessione del dispositivo
- Eventi relativi agli accessi autorizzati
- Eventi relativi agli accessi non autorizzati.

È possibile indicare opzioni di avviso per singoli criteri di protezione.

Per informazioni sulle modalità di configurazione, si rinvia alla sezione "Configurazione delle opzioni d avviso" del capitolo "Personalizzazione del criterio di protezione predefinito".

Rapporti

Il ReportPack di GFI EndPointSecurity rappresenta un prodotto complementare, del tutto sviluppato, per GFI EndPointSecurity. Questo pacchetto per la generazione di rapporti può essere programmato per generare, in maniera automatica, rapporti grafici a livello di personale tecnico informatico e dirigente, sulla base dei dati raccolti da GFI EndPointSecurity, consentendo di ottenere rapporti sui dispositivi connessi alla rete, sull'andamento dell'utilizzo del dispositivo per computer o per utente, sui file copiati da e verso i dispositivi (compresi i veri nomi di file copiati) e molto altro.

NOTA: per poter generare i rapporti, è necessario scaricare e installare il componente aggiuntivo ReportPack di GFI EndPointSecurity

Per maggiori informazioni, visitare la pagina:

<http://www.gfi-italia.com/italia/endpointsecurity/esecreportpack.htm>.

Monitoraggio dello stato

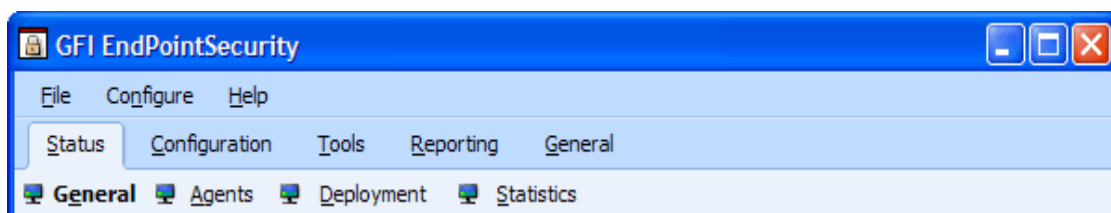
Introduzione

Il monitor di stato è una dashboard che mostra lo stato di GFI EndPointSecurity e lo stato degli agenti distribuiti sui computer di rete. Fornisce inoltre grafici e informazioni statistiche correlati all'utilizzo del dispositivo. Il monitor di stato si compone di quattro visualizzazioni dashboard: Generale, Agenti, Distribuzione e Statistiche.

Accesso al monitor di stato

Per accedere al monitor di stato, seguire questa procedura:

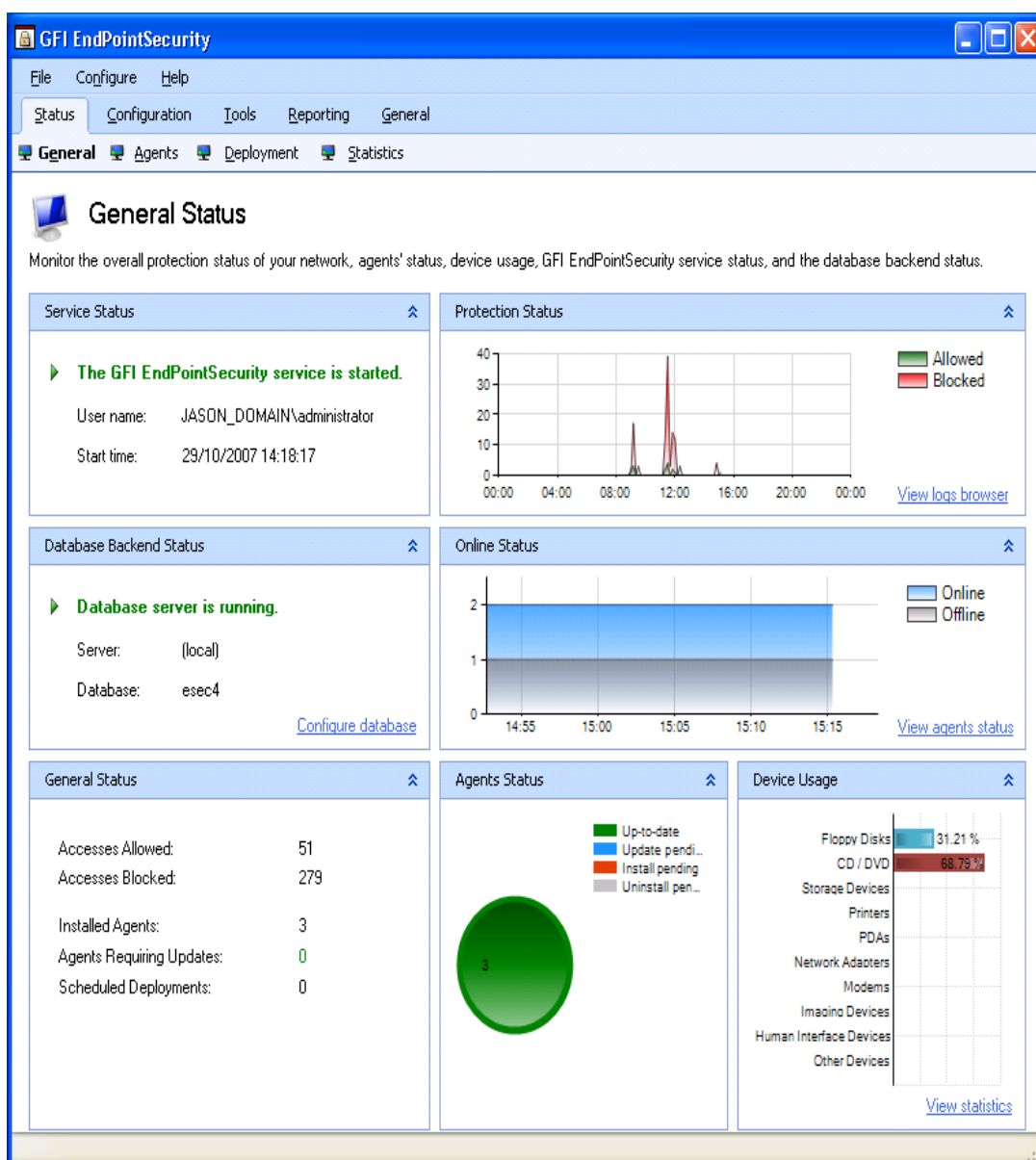
1. Fare clic sulla scheda **Status (Stato)**.



Schermata 35 – Scheda dello Stato

2. Selezionare la visualizzazione dashboard desiderata facendo rispettivamente clic sulle opzioni *General* (Generale), *Agents* (Agenti), *Deployment* (Distribuzione) o *Statistics* (Statistiche).

Utilizzo della visualizzazione di stato Generale



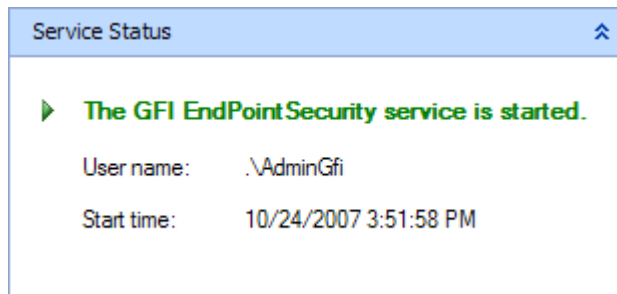
Schermata 36 – Visualizzazione di stato Generale

Adoperare l'opzione **Generale** per visualizzare:

- lo stato del servizio GFI EndPointSecurity e del terminale database
- lo stato degli agenti GFI EndPointSecurity distribuiti sui computer della rete
- l'utilizzo del dispositivo, come il numero di dispositivi bloccati o autorizzati.

Le informazioni fornite con questa modalità di visualizzazione sono riportate in sezioni separate. Di seguito sono fornite ulteriori informazioni su dette sezioni.

Stato del Servizio

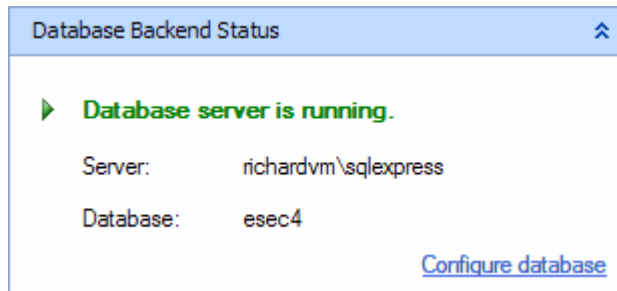


Schermata 37 – Visualizzazione dello stato del Servizio

La presente sezione illustra:

- lo stato operativo del servizio GFI EndPointSecurity
- l'account utente sotto il quale viene eseguito il servizio GFI EndPointSecurity
- l'ora in cui il servizio è stato avviato l'ultima volta.

Stato del terminale database



Schermata 38 – Visualizzazione dello stato del Terminale database

La presente sezione illustra:

- lo stato operativo del server database adoperato in quel momento da GFI EndPointSecurity
- il nome del server database adoperato in quel momento da GFI EndPointSecurity
- il nome del database in cui GFI EndPointSecurity archivia gli eventi.

Fare clic sul collegamento **Configure database (Configurazione database)** per visualizzare la finestra di configurazione del terminale database.

Stato Generale

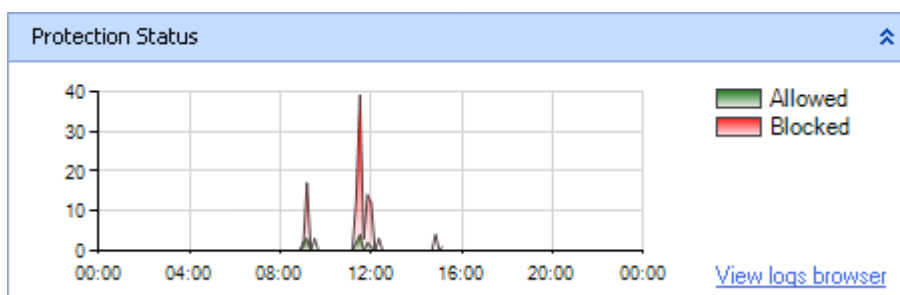
General Status	
Accesses Allowed:	51
Accesses Blocked:	279
Installed Agents:	3
Agents Requiring Updates:	0
Scheduled Deployments:	0

Schermata 39 – Visualizzazione di stato Generale

La presente sezione illustra il numero di:

- dispositivi bloccati sui computer della rete
- dispositivi autorizzati sui computer della rete
- agenti installati sui computer della rete
- agenti da aggiornare, compresi:
 - agenti da installare
 - agenti da disinstallare
 - aggiornamenti criterio di protezione
- distribuzioni pianificate, compresi:
 - agenti da installare
 - agenti da disinstallare
 - aggiornamenti criterio di protezione.

Stato della protezione

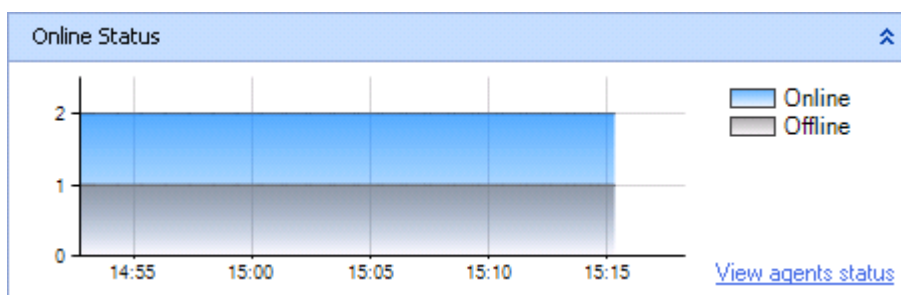


Schermata 40 – Visualizzazione dello stato della protezione

La presente sezione illustra graficamente l'utilizzo giornaliero del dispositivo sui computer della rete, distinguendo i dispositivi bloccati da quelli autorizzati.

Fare clic sul collegamento **View logs browser (Visualizza il browser dei log)** per un'analisi approfondita degli eventi, compresi quelli relativi ai dispositivi bloccati o autorizzati.

Stato in linea

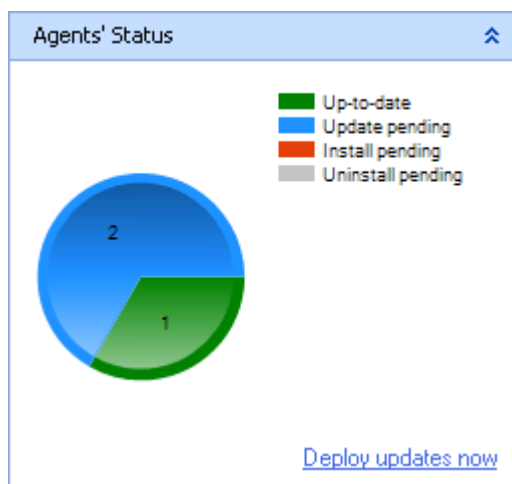


Schermata 41 – Visualizzazione dello stato in linea

La presente sezione illustra graficamente tutti gli agenti distribuiti sui computer della rete, distinguendo quelli attualmente in linea da quelli fuori linea.

Fare clic sul collegamento **View agents status (Visualizza stato agenti)** per vedere le informazioni di stato degli agenti.

Stato degli agenti

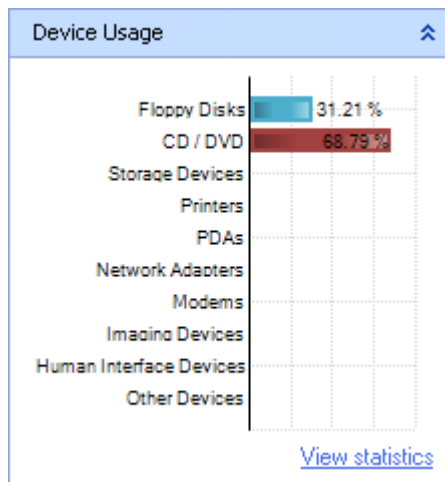


Schermata 42 – Visualizzazione stato degli agenti

La presente sezione illustra graficamente il numero di agenti che:

- sono sincronizzati con il criterio di protezione
- necessitano di aggiornamenti con le modifiche del criterio di protezione
- sono in attesa di installazione sui computer della rete
- sono in attesa di essere disinstallati dai computer della rete.

Utilizzo del dispositivo

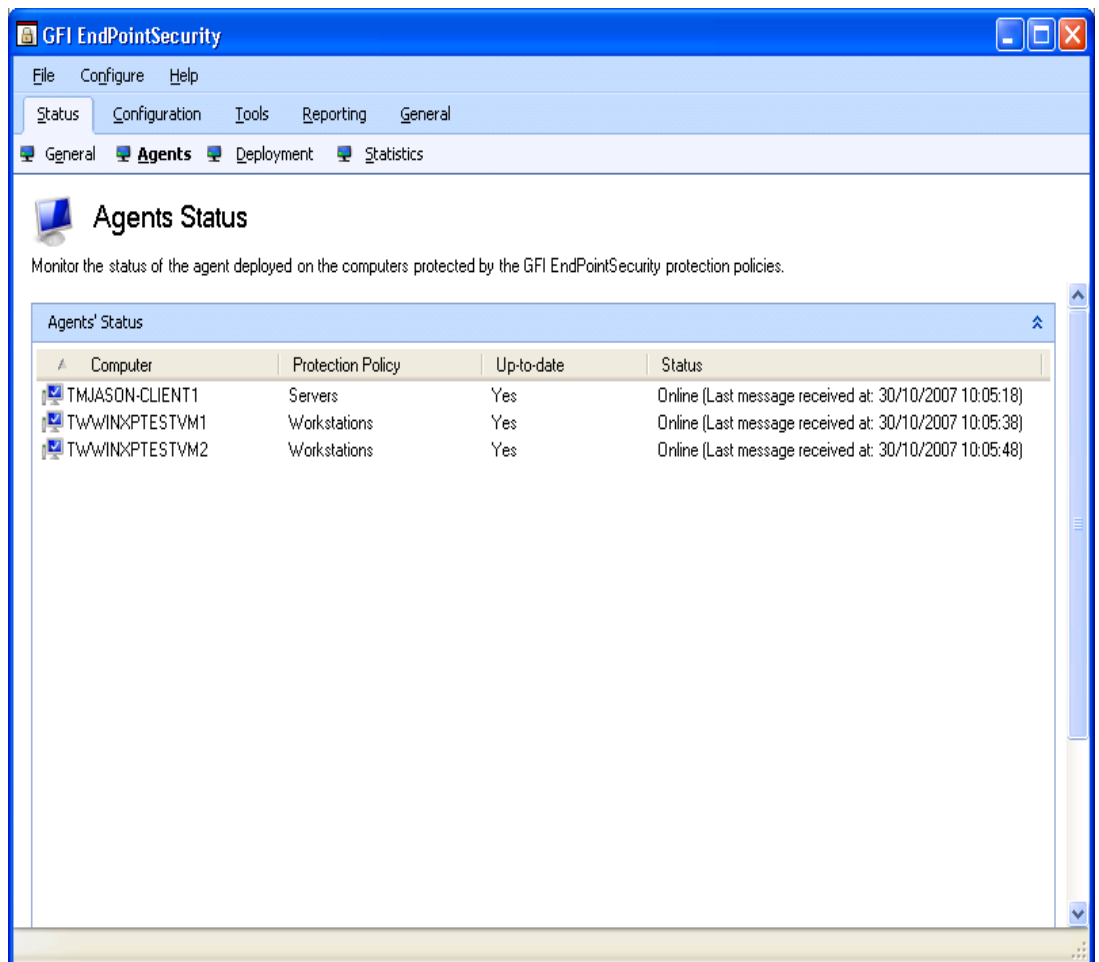


Schermata 43 – Visualizzazione utilizzo del dispositivo

La presente sezione illustra graficamente il numero di dispositivi per singolo tipo.

Fare clic sul collegamento **View statistics (Visualizza statistiche)** per vedere una suddivisione statistica dell'utilizzo del dispositivo, indicante quelli che sono stati bloccati o autorizzati per un determinato computer oppure per tutti i computer della rete.

Utilizzo della visualizzazione Stato agenti

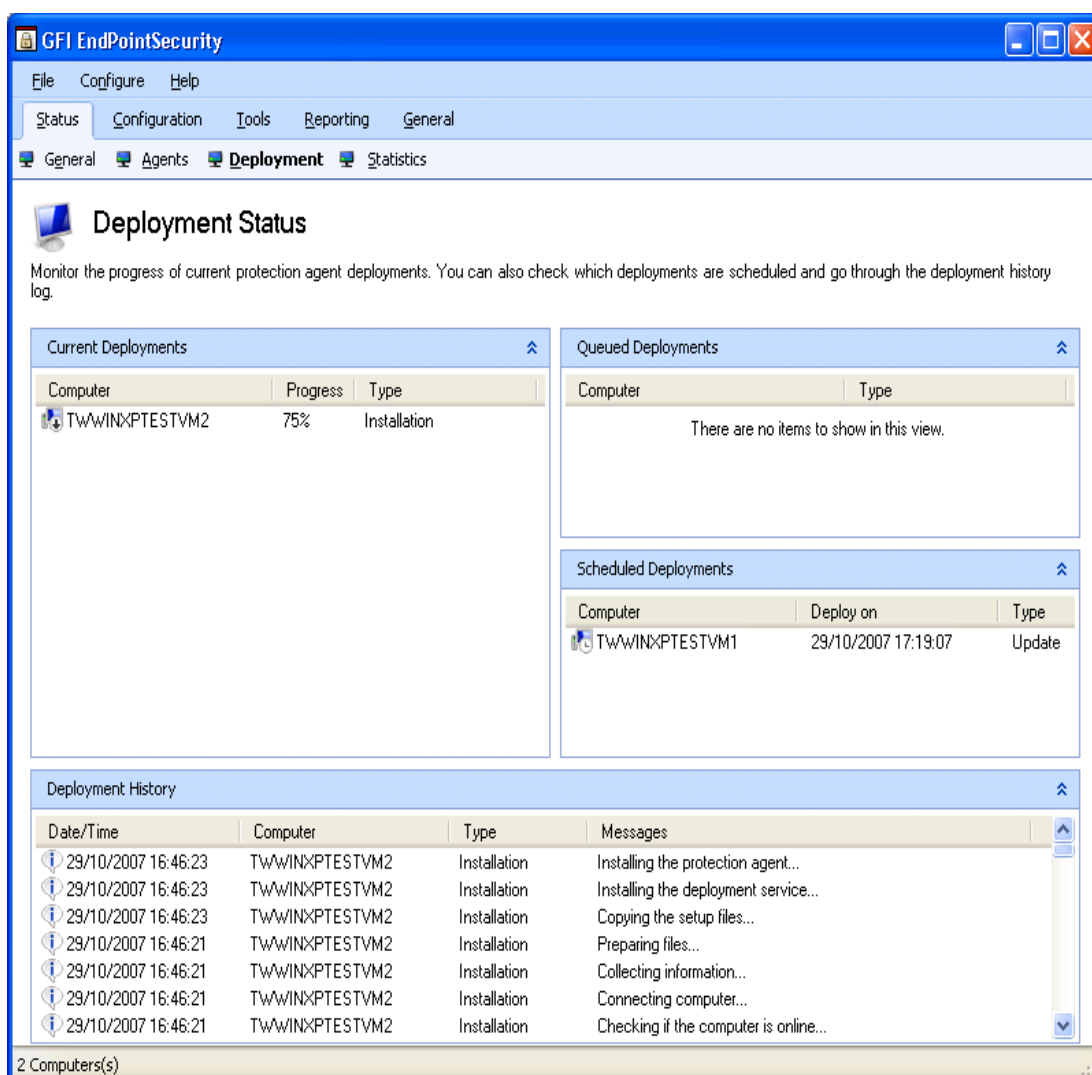


Schermata 44 – Opzioni stato degli agenti

Adoperare l'opzione **Agents Status (Stato agenti)** per visualizzare:

- lo stato di tutti gli agenti GFI EndPointSecurity attualmente distribuiti oppure in attesa di distribuzione
- il nome del computer target e il criterio di protezione applicabile.

Utilizzo della visualizzazione Stato distribuzione



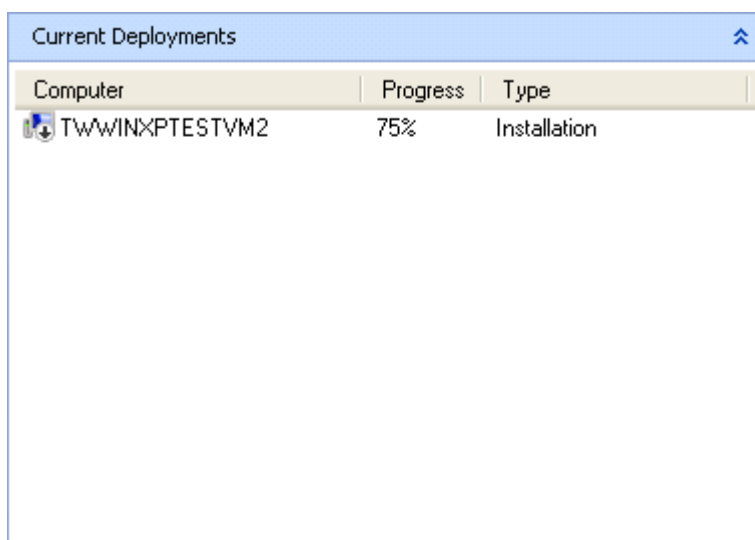
Schermata 45 – Visualizzazione stato della distribuzione


Adoperare l'opzione **Deployment Status (Stato distribuzione)** per visualizzare:

- l'attività di distribuzione corrente
- le distribuzioni pendenti
- la cronologia della distribuzione.

Le informazioni fornite con questa modalità di visualizzazione sono riportate in sezioni separate. Di seguito sono fornite ulteriori informazioni su dette sezioni.

Distribuzioni correnti

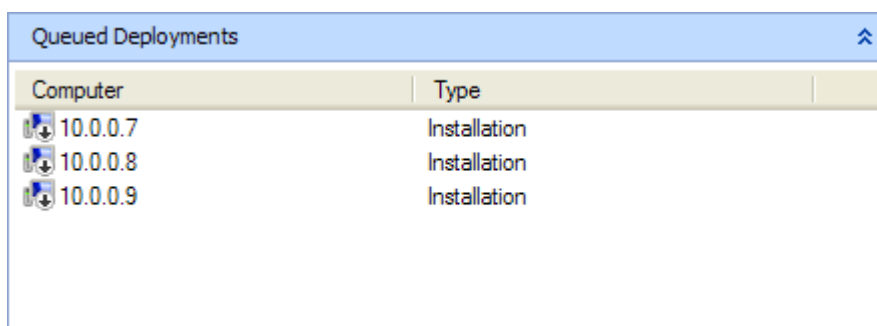





Computer	Progress	Type
 Tw\WINXPTESTVM2	75%	Installation

Schermata 46 – Visualizzazione distribuzioni attive

La presente sezione illustra un elenco delle distribuzioni in corso. Tra le informazioni fornite, figurano il nome del computer, lo stato di avanzamento e il tipo di distribuzione, cioè se la distribuzione è un'installazione, una disinstallazione o un aggiornamento.

Distribuzioni in attesa

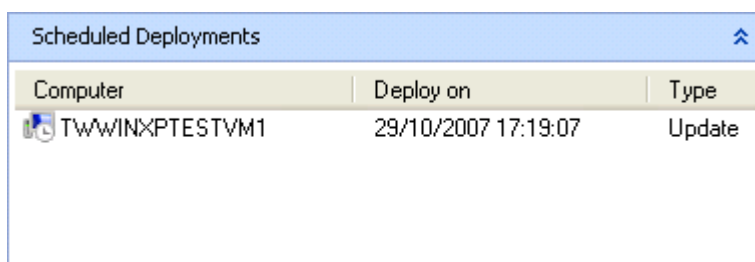



Computer	Type
 10.0.0.7	Installation
 10.0.0.8	Installation
 10.0.0.9	Installation

Schermata 47 – Visualizzazione distribuzioni in attesa

La presente sezione illustra un elenco di distribuzioni pendenti. Tra le informazioni fornite, figurano il nome computer e il tipo di distribuzione.

Distribuzioni pianificate

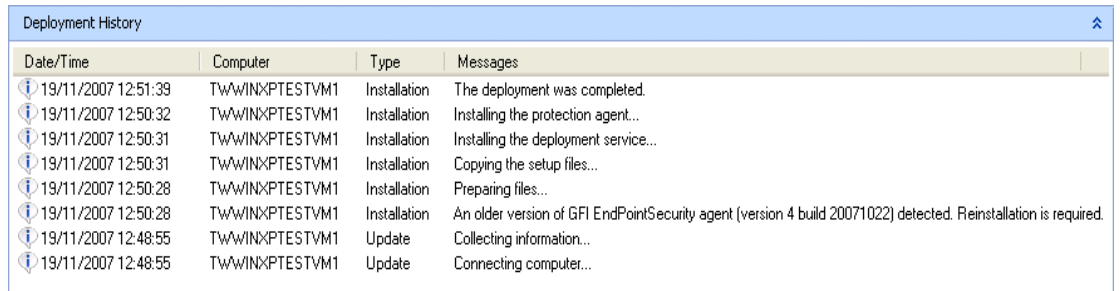


Computer	Deploy on	Type
 Tw\WINXPTESTVM1	29/10/2007 17:19:07	Update

Schermata 48 – Visualizzazione distribuzioni pianificate

La presente sezione illustra un elenco di distribuzioni pianificate. Tra le informazioni fornite, figurano il nome computer, il tipo di distribuzione e l'ora programmata.

Cronologia della distribuzione



Date/Time	Computer	Type	Messages
19/11/2007 12:51:39	TWWINXPTESTVM1	Installation	The deployment was completed.
19/11/2007 12:50:32	TWWINXPTESTVM1	Installation	Installing the protection agent...
19/11/2007 12:50:31	TWWINXPTESTVM1	Installation	Installing the deployment service...
19/11/2007 12:50:31	TWWINXPTESTVM1	Installation	Copying the setup files...
19/11/2007 12:50:28	TWWINXPTESTVM1	Installation	Preparing files...
19/11/2007 12:50:28	TWWINXPTESTVM1	Installation	An older version of GFI EndPointSecurity agent (version 4 build 20071022) detected. Reinstallation is required.
19/11/2007 12:48:55	TWWINXPTESTVM1	Update	Collecting information...
19/11/2007 12:48:55	TWWINXPTESTVM1	Update	Connecting computer...

Schermata 49 – Visualizzazione cronologia della distribuzione

La presente sezione illustra un audit trail di tutte le distribuzioni eseguite da GFI EndPointSecurity. Tra le informazioni fornite, figurano messaggi di errori e informativi generati durante il processo di distribuzione, nonché il tipo di distribuzione.

Utilizzo della visualizzazione delle Statistiche

Per informazioni sulla visualizzazione "Statistiche", si rinvia alla sezione "Utilizzo della visualizzazione delle statistiche" del capitolo "Monitoraggio dell'attività di utilizzo del dispositivo".

Personalizzazione del criterio di protezione predefinito

Introduzione

I criteri di protezione predefiniti inclusi in GFI EndPointSecurity sono del tutto personalizzabili e possono perciò essere configurati per adattarsi alla politica di sicurezza dei dispositivi portatili della propria azienda.

Nel presente capitolo, si impareranno le modalità per eseguire le modifiche di configurazione in tutte le sezioni dei criteri di protezione predefiniti. Le informazioni contenute in questo capitolo consentono inoltre di creare da zero il proprio criterio di protezione.

Presentazione del capitolo

In questo capitolo verranno coperte le seguenti sezioni di criteri di protezione:

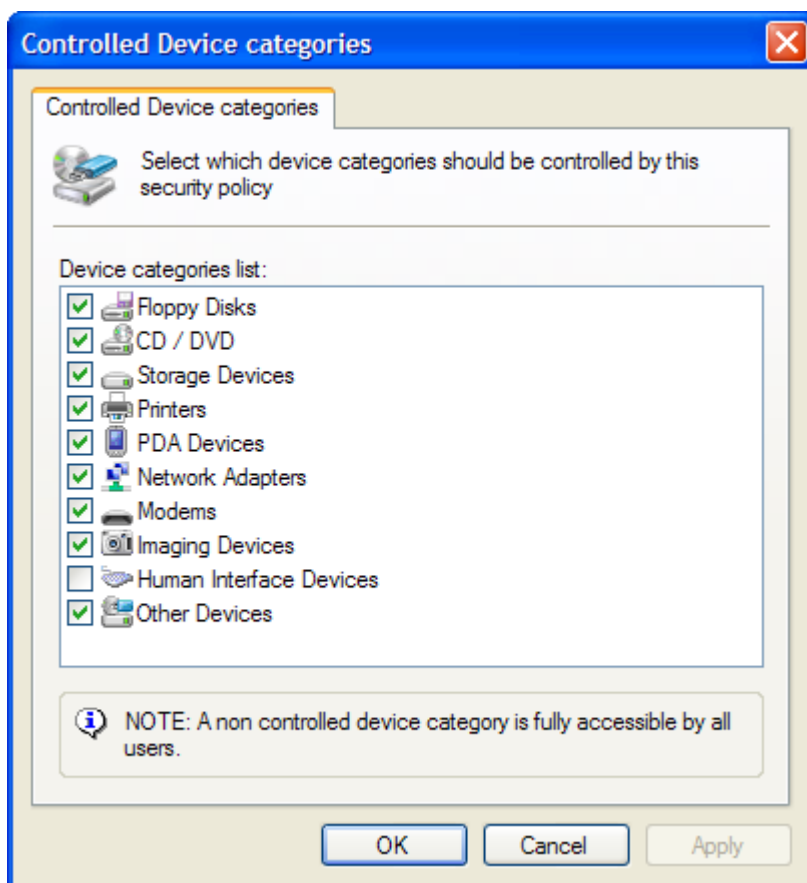
- Configurazione dei dispositivi portatili da controllare
- Configurazione delle porte di connessione da controllare
- Configurazione degli utenti autorizzati
- Configurazione autorizzazioni di accesso alla categoria del dispositivo
- Configurazione autorizzazioni di utilizzo della porta di connessione
- Configurazione autorizzazioni di accesso per un determinato dispositivo
- Visualizzazione autorizzazioni
- Configurazione priorità autorizzazioni
- Configurazione blacklist dispositivi portatili
- Configurazione whitelist dispositivi portatili
- Configurazione privilegi di accesso temporaneo
- Configurazione dei filtri dei tipi di file
- Configurazione della registrazione e delle notifiche eventi.

Configurazione dei dispositivi portatili da controllare

In GFI EndPointSecurity, è possibile specificare quali dispositivi portatili supportati devono essere controllati ovvero esclusi da un criterio di protezione. Questa operazione può essere eseguita per singolo criterio di protezione.

Per configurare i dispositivi che dovranno essere controllati da un dato criterio di protezione, seguire questa procedura:

1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Protection Policies (Criteri di protezione)**
3. Nel pannello di sinistra, selezionare il criterio di protezione da configurare
4. Fare clic sul sub-nodo **Security (Sicurezza)**
5. Nel pannello di sinistra, fare clic sull'opzione **Edit controlled device categories (Modifica categorie dispositivi controllati)**



Schermata 50 – Selezione delle categorie di dispositivi da controllare

6. Selezionare le categorie di dispositivi che saranno controllate dal criterio di protezione e fare clic su **OK**.

NOTA: le categorie di dispositivi non controllate dal criterio di protezione sono del tutto accessibili sui computer inclusi nel criterio.

7. Distribuire gli aggiornamenti del criterio di protezione sui computer compresi nel criterio. Nel pannello di sinistra, fare clic con il pulsante destro del mouse sul criterio di protezione configurato e selezionare **Deployment ▶ Deploy agent(s) (Distribuzione ▶ Distribuisci agenti)**.

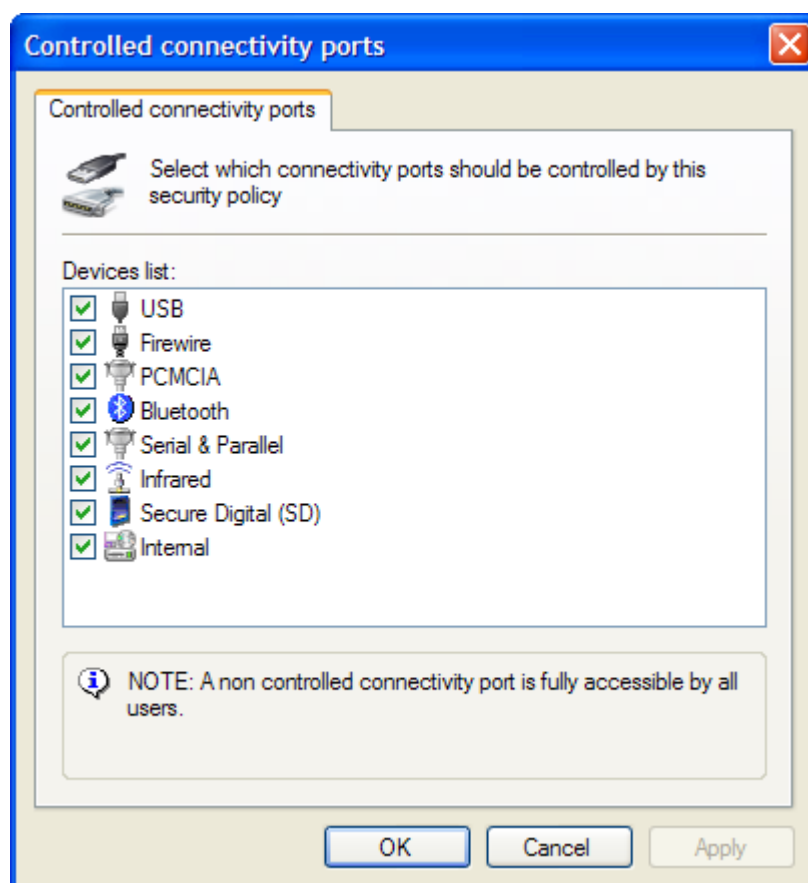
NOTA: per eseguire questo passaggio, è anche possibile adoperare la scelta rapida di tastiera **CTRL + D**.

Configurazione delle porte di connessione da controllare

In GFI EndPointSecurity, è possibile specificare quali porte di connessione supportate devono essere controllate ovvero escluse da un criterio di protezione. Questa operazione può essere eseguita per singolo criterio di protezione.

Per configurare le porte che dovranno essere controllate da un dato criterio di protezione, seguire questa procedura:

1. Selezionare la scheda **Configuration (Configurazione)**
2. Fare clic su **Protection Policies (Criteri di protezione)**
3. Nel pannello di sinistra, selezionare il criterio di protezione da configurare
4. Fare clic sul sub-nodo **Security (Sicurezza)**
5. Nel pannello di sinistra, fare clic sull'opzione **Edit controlled ports (Modifica porte controllate)**



Schermata 51 – Selezione delle porte da controllare

6. Selezionare le porte di connessione che saranno controllate dal criterio di protezione e fare clic su **OK**.

NOTA: le porte di connessione non controllate dal criterio di protezione sono del tutto accessibili sui computer inclusi nel criterio.

7. Distribuire gli aggiornamenti del criterio di protezione sui computer compresi nel criterio. Nel pannello di sinistra, fare clic con il pulsante destro del mouse sul criterio di protezione configurato e selezionare **Deployment ▶ Deploy agent(s) (Distribuzione ▶ Distribuisci agenti)**.

NOTA: per eseguire questo passaggio, è anche possibile adoperare la scelta rapida di tastiera **CTRL + D**.

Configurazione degli utenti autorizzati

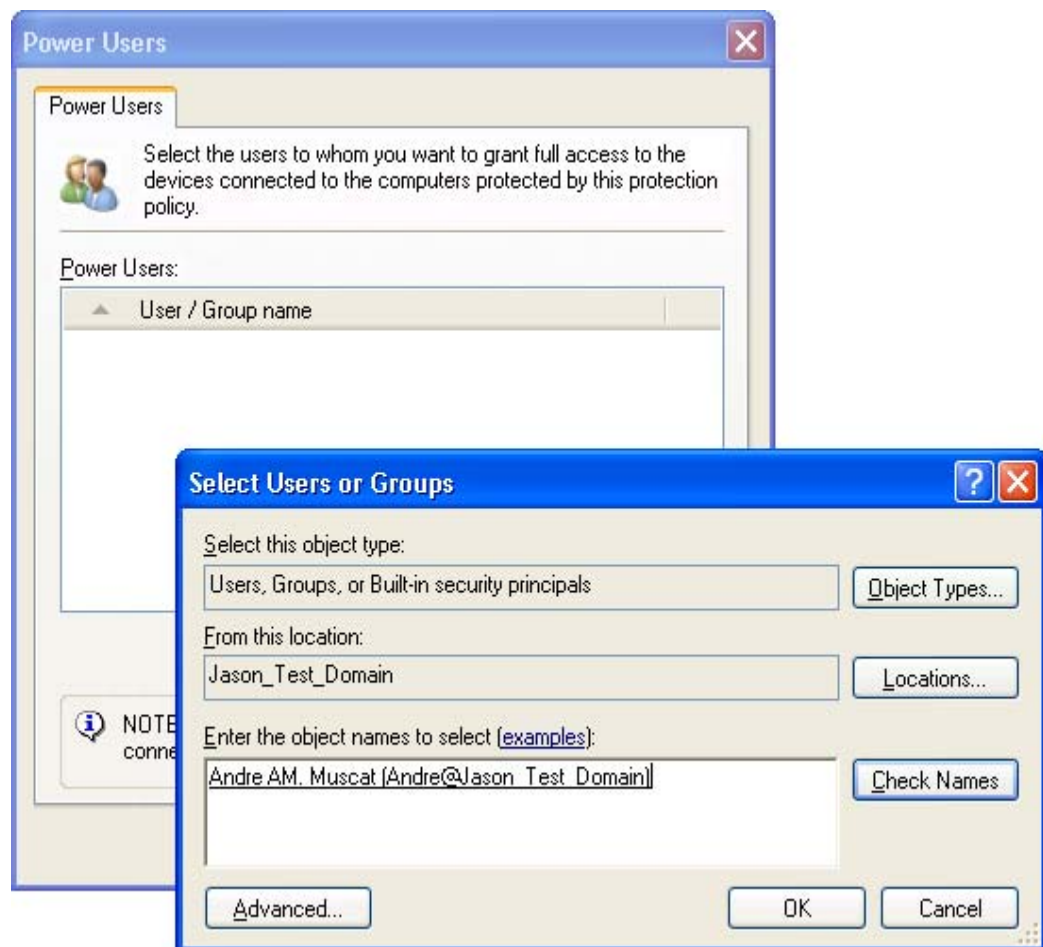
GFI EndPointSecurity consente di specificare come utenti autorizzati qualsiasi utente o gruppo di utenti di Active Directory (AD) oppure utenti locali o schemi di gruppi. Questa operazione può essere eseguita per singolo criterio di protezione.

Gli utenti autorizzati di un dato criterio di protezione sono provvisti del pieno controllo sui dispositivi collegati ai computer di quel criterio, indipendentemente dalle limitazioni eventualmente impostate.

NOTA: adoperare questa funzione con prudenza, in quanto l'errata indicazione di un utente come utente autorizzato può comportare il rischio che quell'utente superi tutte le limitazioni del criterio di protezione.

Per indicare gli utenti autorizzati, seguire questa procedura:

1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Protection Policies (Criteri di protezione)**
3. Nel pannello di sinistra, selezionare il criterio di protezione di cui si desidera specificare Utenti autorizzati
4. Nel pannello di destra, fare clic su **Power Users (Utenti autorizzati)** della sezione **Security (Sicurezza)**



Schermata 52 – Indicazione degli utenti autorizzati

5. Fare clic su **Add (Aggiungi)** per specificare gli utenti/gruppi da indicare come utenti autorizzati. fare clic su **OK** per completare le impostazioni
6. Distribuire gli aggiornamenti del criterio di protezione sui computer compresi nel criterio. Nel pannello di sinistra, fare clic con il pulsante destro del mouse sul criterio di protezione configurato e selezionare **Deployment ▶ Deploy agent(s) (Distribuzione ▶ Distribuisci agenti)**.

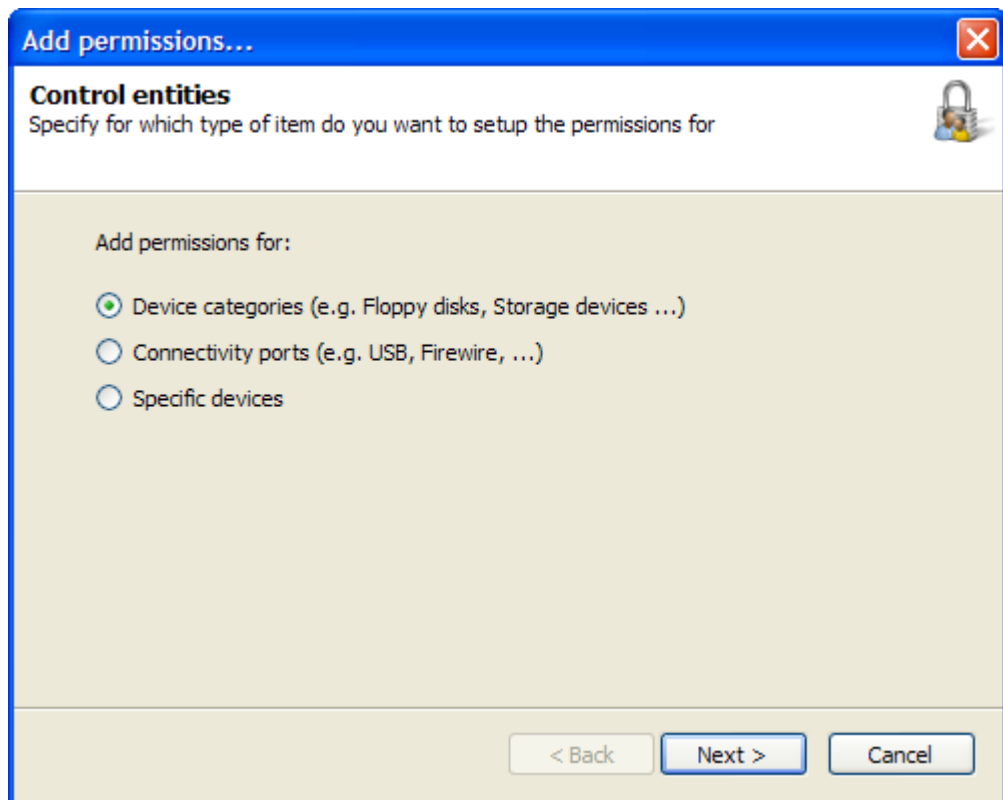
Configurazione delle autorizzazioni di accesso alla categoria di dispositivi

Per impostazione predefinita, non sono preconfigurati utenti e privilegi nei criteri di protezione inclusi in GFI EndPointSecurity. Di conseguenza, dopo aver distribuito un criterio di protezione predefinito su un computer target, l'accesso ai dispositivi portatili sarà negato a tutti gli utenti.

GFI EndPointSecurity consente di assegnare privilegi di accesso, lettura e scrittura (sui dispositivi portatile supportati) a qualsiasi utente o gruppo utenti appartenente ad Active Directory (AD) o a utenti e schemi di gruppo locali. Questa operazione può essere eseguita per singolo criterio di protezione.

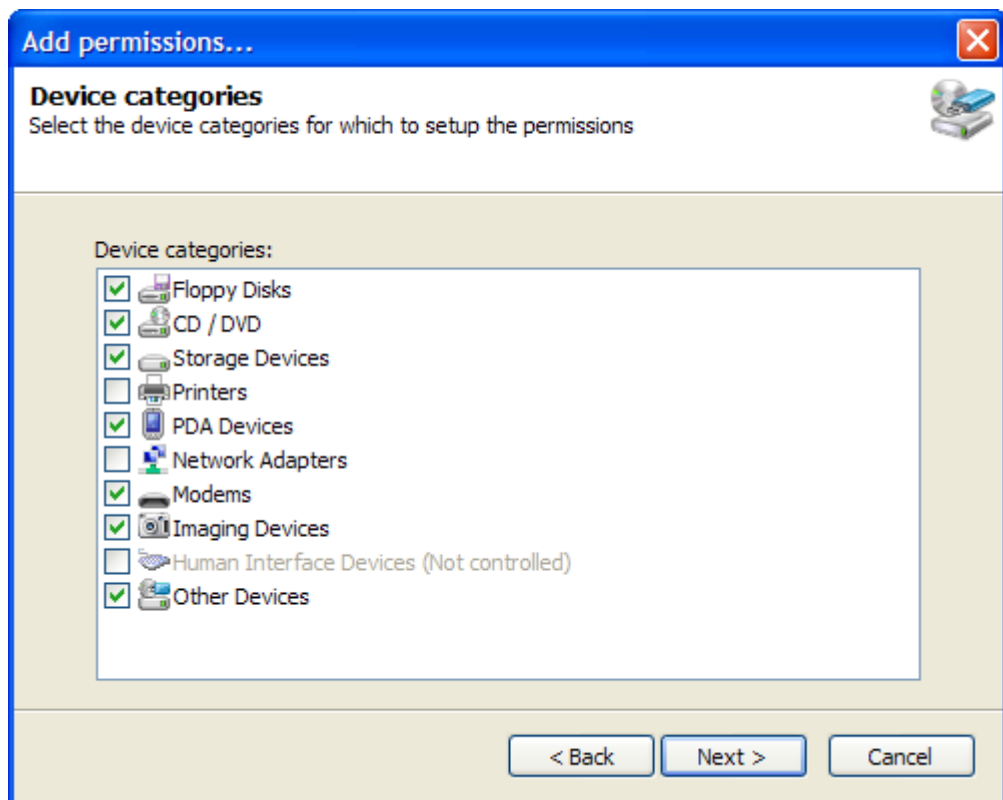
Per configurare gli utenti e i privilegi delle categorie di dispositivi, seguire questa procedura:

1. Selezionare la scheda **Configuration (Configurazione)**
2. Fare clic su **Protection Policies (Criteri di protezione)**
3. Nel pannello di sinistra, selezionare il criterio di protezione da configurare
4. Fare clic sul sub-nodo **Security (Sicurezza)**
5. Nel pannello di sinistra, fare clic su **Add new permission(s) (Aggiungi nuove autorizzazioni)**



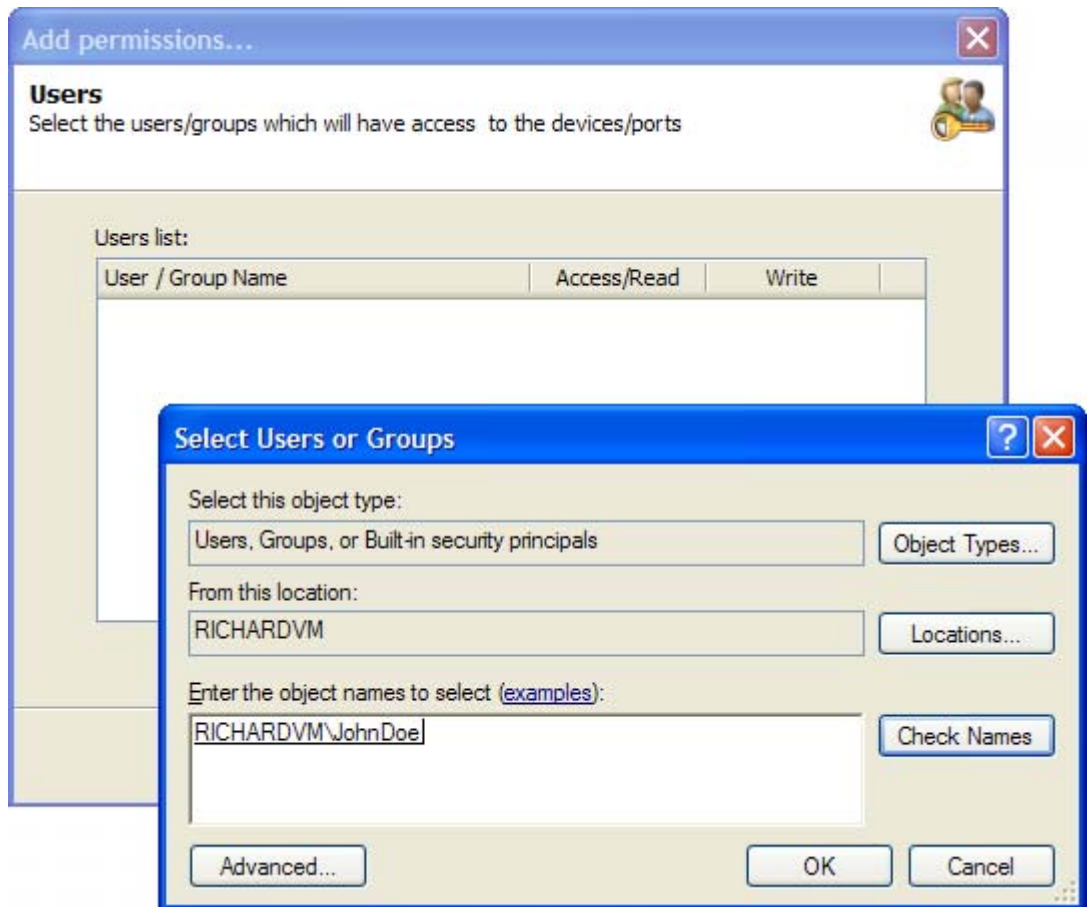
Schermata 53 – Aggiunta di autorizzazioni a categorie di dispositivi

6. Selezionare l'opzione **Device categories (Categorie di dispositivi)** e fare clic su **Next (Avanti)** per continuare.



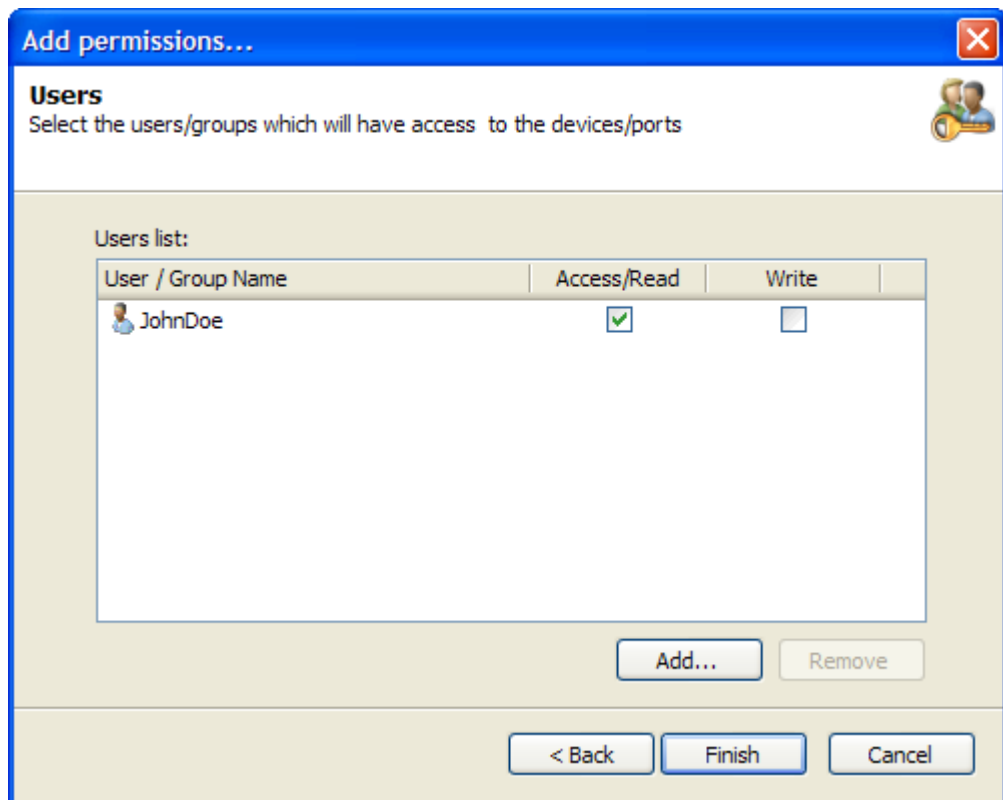
Schermata 54 – Selezione delle categorie di dispositivi

7. Selezionare le categorie di dispositivi di cui configurare le autorizzazioni e fare clic su **Next (Avanti)** per continuare



Schermata 55 – Aggiunta di utenti o gruppi

8. Fare clic su **Add (Aggiungi)** per specificare utenti o gruppi che hanno accesso alle categorie di dispositivi indicate



Schermata 56 – Aggiunta autorizzazioni

9. Assegnare privilegi di lettura/scrittura a ciascun utente o gruppo indicati. Fare clic su **Finish (Fine)** per completare le impostazioni.

10. Distribuire gli aggiornamenti del criterio di protezione sui computer compresi nel criterio. Nel pannello di sinistra, fare clic con il pulsante destro del mouse sul criterio di protezione configurato e selezionare **Deployment ▶ Deploy agent(s) (Distribuzione ▶ Distribuisci agenti)**.

NOTA: per eseguire questo passaggio, è anche possibile adoperare la scelta rapida di tastiera **CTRL + D**.

Configurazione autorizzazioni di utilizzo della porta di connessione

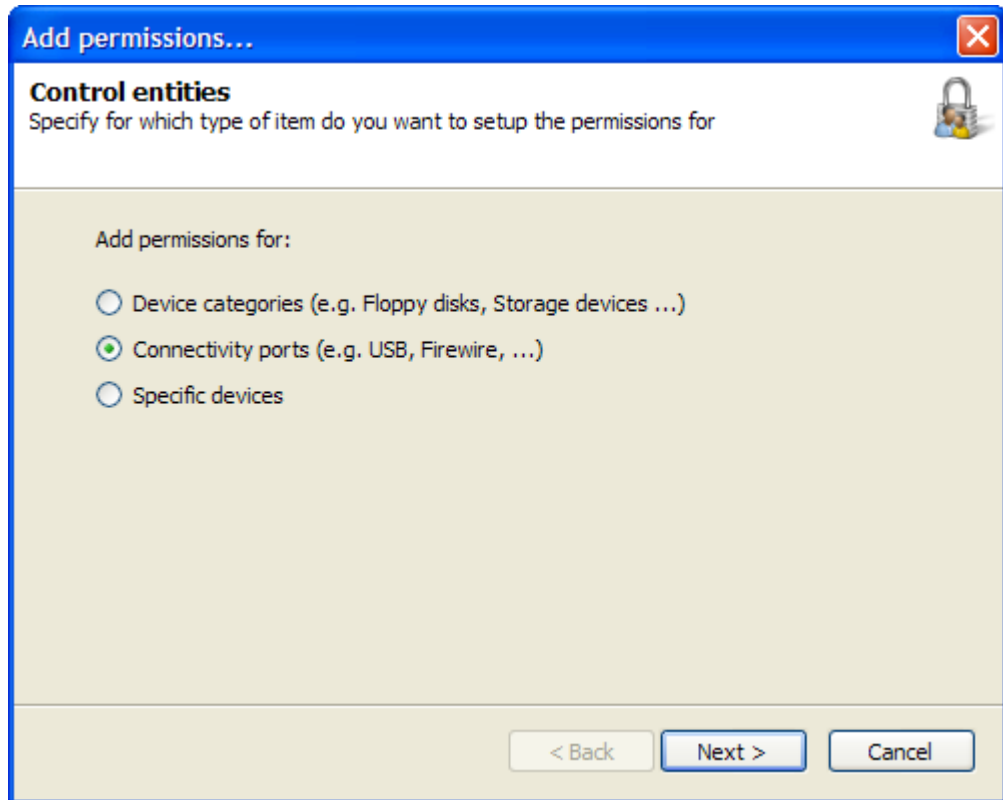
Per impostazione predefinita, non sono preconfigurati utenti e privilegi nei criteri di protezione inclusi in GFI EndPointSecurity. Di conseguenza, dopo aver distribuito un criterio di protezione su un computer target, l'accesso ai dispositivi portatili sarà negato a tutti gli utenti.

GFI EndPointSecurity consente di assegnare privilegi di accesso, lettura e scrittura (sulle porte di connessione supportate) a qualsiasi utente o gruppo utenti appartenente ad Active Directory (AD) o a utenti e schemi di gruppo locali. Questa operazione può essere eseguita per singolo criterio di protezione.

Per configurare gli utenti e i privilegi per le porte di connessione di un criterio di protezione, seguire questa procedura:

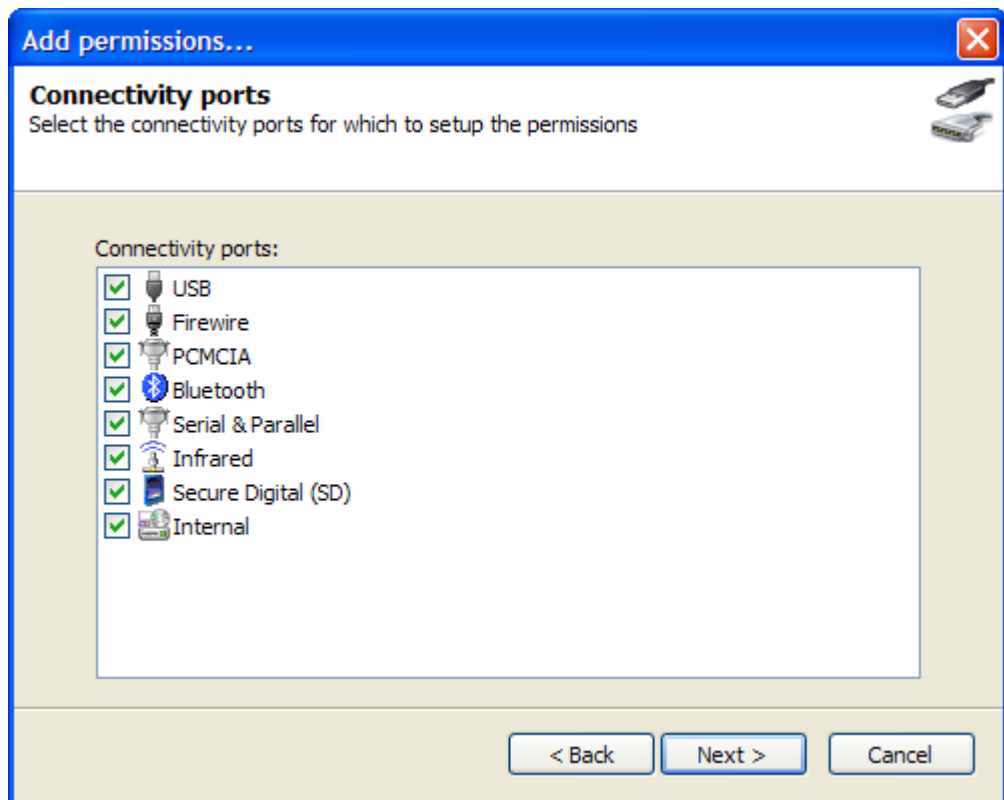
1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Protection Policies (Criteri di protezione)**.

3. Nel pannello di sinistra, selezionare il criterio di protezione da configurare.
4. Fare clic sul sub-nodo **Security (Sicurezza)**.
5. Nel pannello di sinistra, fare clic su **Add new permission(s) (Aggiungi nuove autorizzazioni)**.



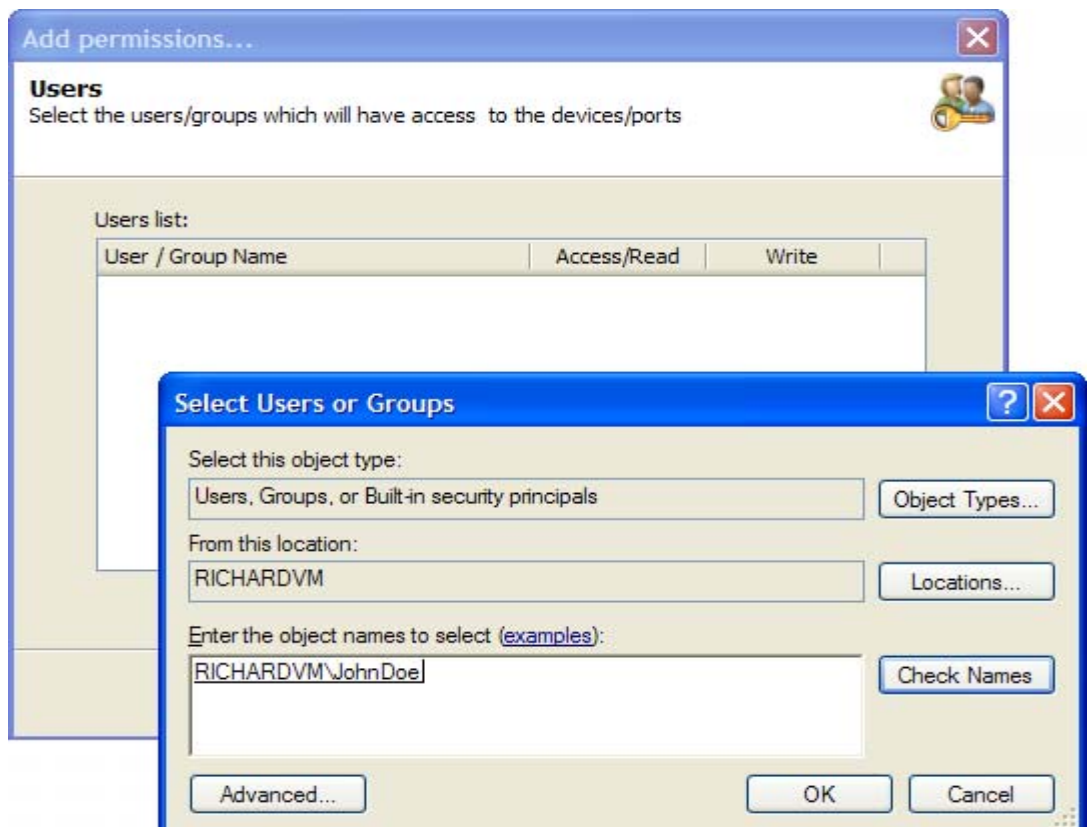
Schermata 57 – Impostazione dell'opzione relativa alle porte di connessione

6. Selezionare l'opzione **Connectivity ports (Porte di connessione)** e fare clic su **Next (Avanti)** per continuare.



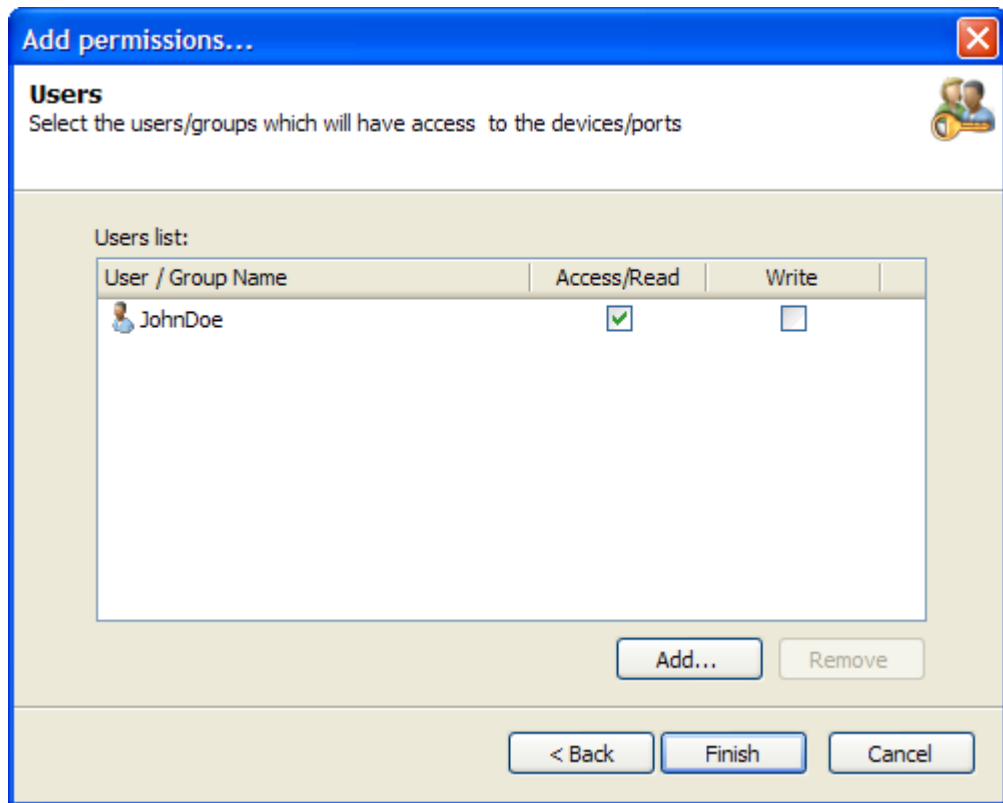
Schermata 58 – Selezione delle porte di connessione

7. Selezionare le porte di connessione di cui configurare le autorizzazioni e fare clic su **Next (Avanti)** per continuare.



Schermata 59 – Aggiunta di utenti o gruppi

8. Fare clic su **Add (Aggiungi)** per specificare utenti o gruppi che avranno accesso alle porte di connessione indicate.



Schermata 60 – Aggiunta autorizzazioni

9. Assegnare privilegi di accesso a ciascun utente o gruppo indicati. Fare clic su **Finish (Fine)** per completare le impostazioni.

10. Distribuire gli aggiornamenti del criterio di protezione sui computer compresi nel criterio. Nel pannello di sinistra, fare clic con il pulsante destro del mouse sul criterio di protezione configurato e selezionare **Deployment ▶ Deploy agent(s) (Distribuzione ▶ Distribuisci agenti)**.

NOTA: per eseguire questo passaggio, è anche possibile adoperare la scelta rapida di tastiera **CTRL + D**.

Configurazione autorizzazioni di accesso per un determinato dispositivo

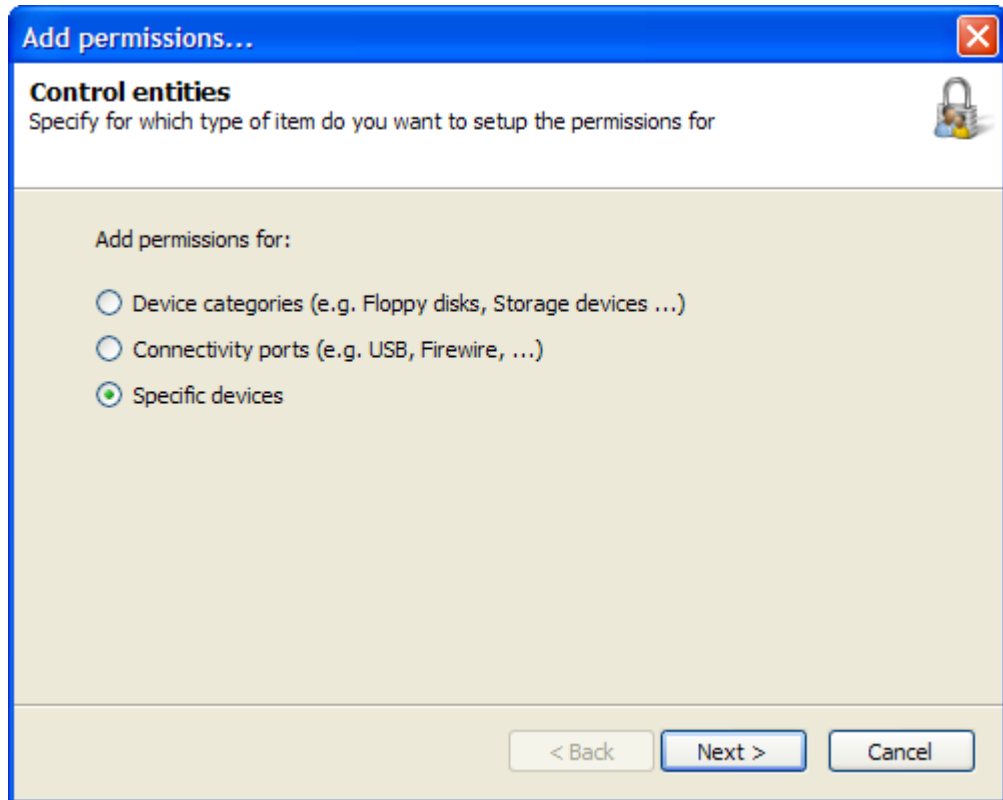
GFI EndPointSecurity consente di assegnare privilegi di accesso, lettura e scrittura su un determinato dispositivo elencato nel database di dispositivi, a qualsiasi utente o gruppo utenti appartenente ad Active Directory (AD) o a utenti e schemi di gruppo locali. Questa operazione può essere eseguita per singolo criterio di protezione.

Per esempio, è possibile assegnare privilegi di sola lettura a una pen-drive USB di una determinata società. Verranno bloccati tutti i tentativi di utilizzare una pen-drive USB non approvata.

Per configurare gli utenti e i privilegi di un determinato dispositivo presente nel criterio di protezione, seguire questa procedura:

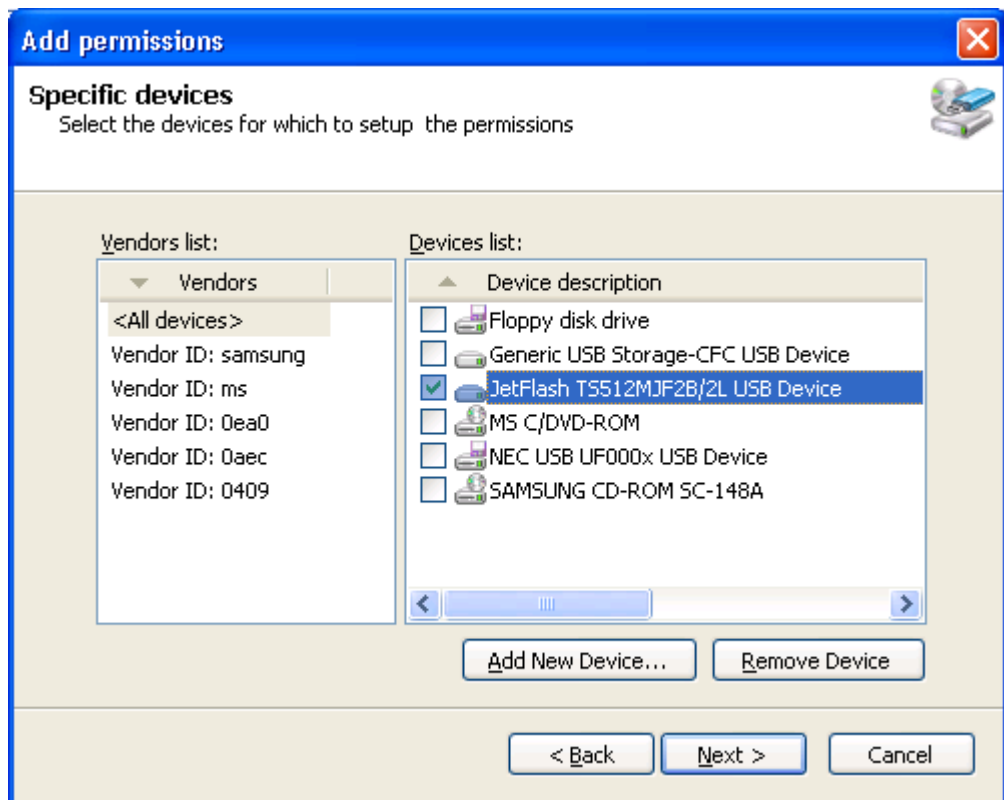
1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Protection Policies (Criteri di protezione)**.

3. Nel pannello di sinistra, selezionare il criterio di protezione da configurare.
4. Fare clic sul sub-nodo **Security (Sicurezza)**.
5. Nel pannello di sinistra, fare clic su **Add new permission(s) (Aggiungi nuove autorizzazioni)**.



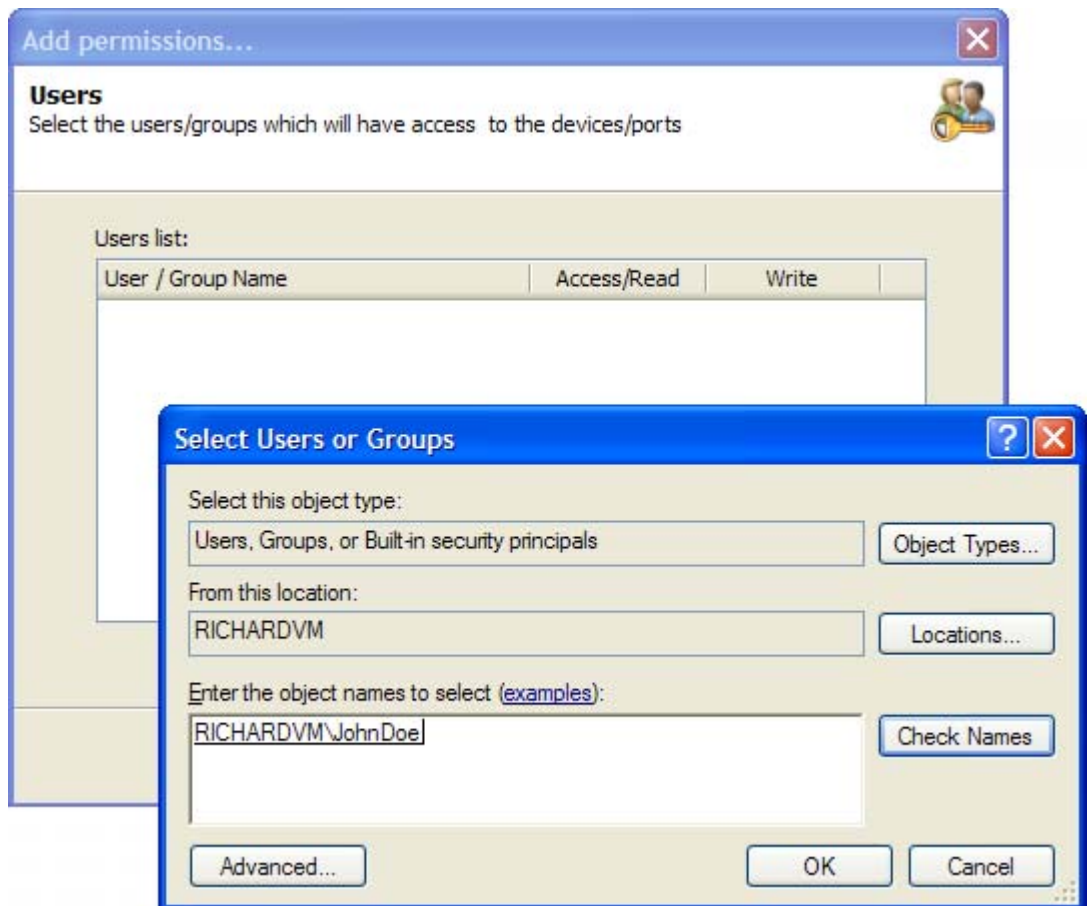
Schermata 61 – Selezione dell'opzione dei dispositivi specifici

6. Selezionare l'opzione **Specific Devices (Dispositivi specifici)** e fare clic su **Next (Avanti)** per continuare.



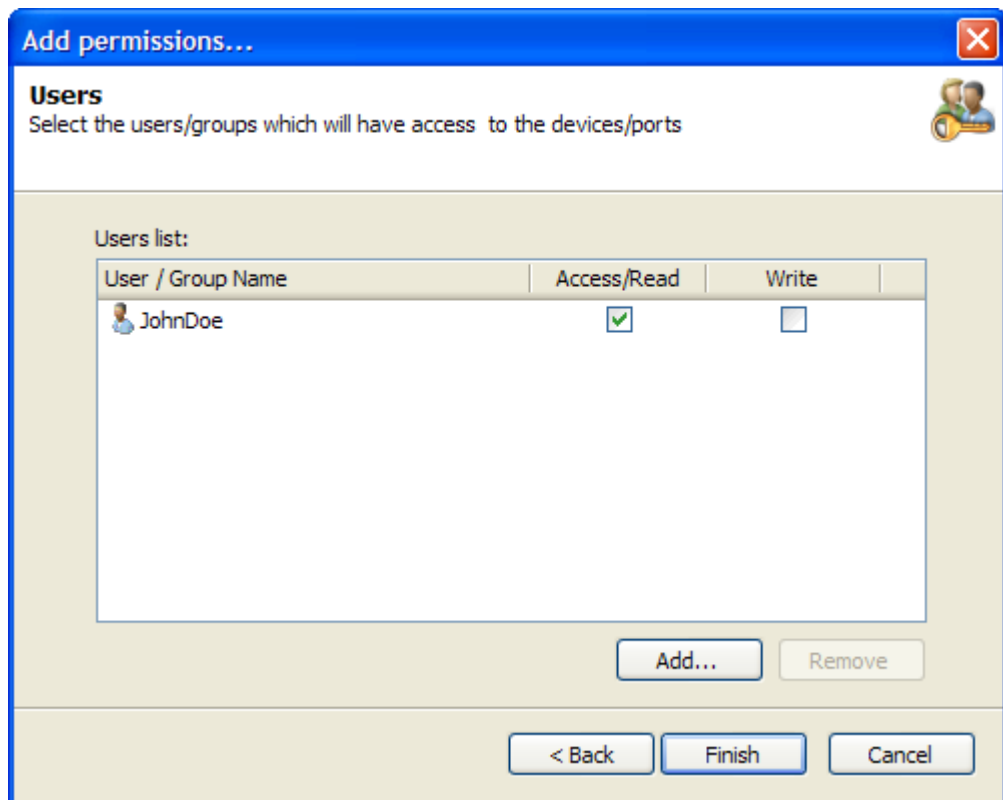
Schermata 62 – Selezione dei dispositivi

7. Selezionare nel relativo database i dispositivi di cui configurare le autorizzazioni e fare clic su **Next (Avanti)** per continuare.



Schermata 63 – Aggiunta di utenti o gruppi

8. Fare clic su **Add (Aggiungi)** per specificare utenti o gruppi che avranno accesso ai dispositivi indicati.



Schermata 64 – Aggiunta autorizzazioni

9. Assegnare privilegi di lettura/scrittura a ciascun utente o gruppo indicati. Fare clic su **Finish (Fine)** per completare le impostazioni.

10. Distribuire gli aggiornamenti del criterio di protezione sui computer compresi nel criterio. Nel pannello di sinistra, fare clic con il pulsante destro del mouse sul criterio di protezione configurato e selezionare **Deployment ▶ Deploy agent(s) (Distribuzione ▶ Distribuisci agenti)**.

NOTA: per eseguire questo passaggio, è anche possibile adoperare la scelta rapida di tastiera **CTRL + D**.

Visualizzazione autorizzazioni

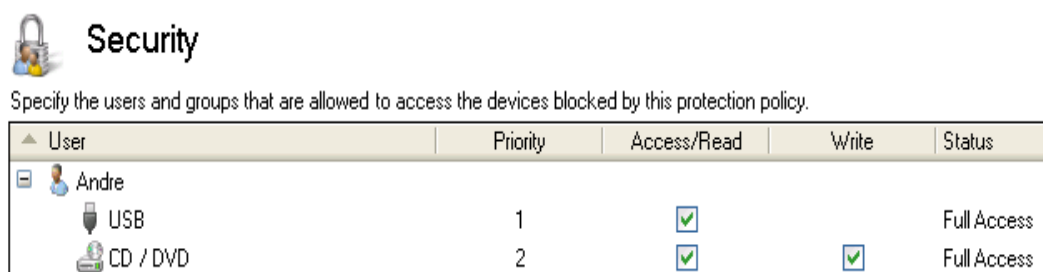
È possibile visualizzare tutte le autorizzazioni di un determinato criterio di protezione. A questo scopo, procedere come segue:

1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Protection Policies (Criteri di protezione)**.
3. Nel pannello di sinistra, selezionare il criterio di protezione di cui si desidera visualizzare le autorizzazioni.
4. Fare clic sul sub-nodo **Security (Sicurezza)**. Nel pannello di destra è possibile visualizzare tutte le autorizzazioni impostate per il criterio di protezione interessato.
5. Nel pannello di sinistra, fare clic su **Switch to devices view (Passare alla visualizzazione dispositivi)** o **Switch to users view (Passare alla visualizzazione utenti)** per cambiare il raggruppamento delle autorizzazioni per dispositivi, porta o utente.

NOTA: nella visualizzazione utenti è inoltre possibile vedere gli utenti autorizzati creati nel criterio.

Configurazione priorità autorizzazioni

Quando si osservano le autorizzazioni della visualizzazione utenti, è possibile impostare priorità di dispositivo o porta per le autorizzazioni di dispositivo o porta definiti dall'amministratore, oppure per singolo utente.



Schermata 65 – Impostazione priorità per le autorizzazioni di dispositivo o porta

Per esempio, è possibile attribuire a un determinato utente la priorità 1 alle autorizzazioni di porta USB e la priorità 2 alle autorizzazioni dell'unità CD/DVD. Pertanto, se l'utente collega al computer un'unità CD/DVD esterna tramite la porta USB, le autorizzazioni della porta USB hanno la precedenza su quelle dell'unità CD/DVD.

Per impostare le priorità, seguire questa procedura:

1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Protection Policies (Criteri di protezione)**.
3. Nel pannello di sinistra, selezionare il criterio di protezione di cui si desidera impostare le priorità per le autorizzazioni.
4. Nel pannello di destra, selezionare l'autorizzazione di cui modificare la priorità.
5. Nel pannello di sinistra, fare clic su **Increase priority (Aumenta priorità)** o **Decrease priority (Riduci priorità)**.
6. Distribuire gli aggiornamenti del criterio di protezione sui computer compresi nel criterio. Nel pannello di sinistra, fare clic con il pulsante destro del mouse sul criterio di protezione configurato e selezionare **Deployment ▶ Deploy agent(s) (Distribuzione ▶ Distribuisci agenti)**.

NOTA: per eseguire questo passaggio, è anche possibile adoperare la scelta rapida di tastiera **CTRL + D**.

Configurazione blacklist dispositivi portatili

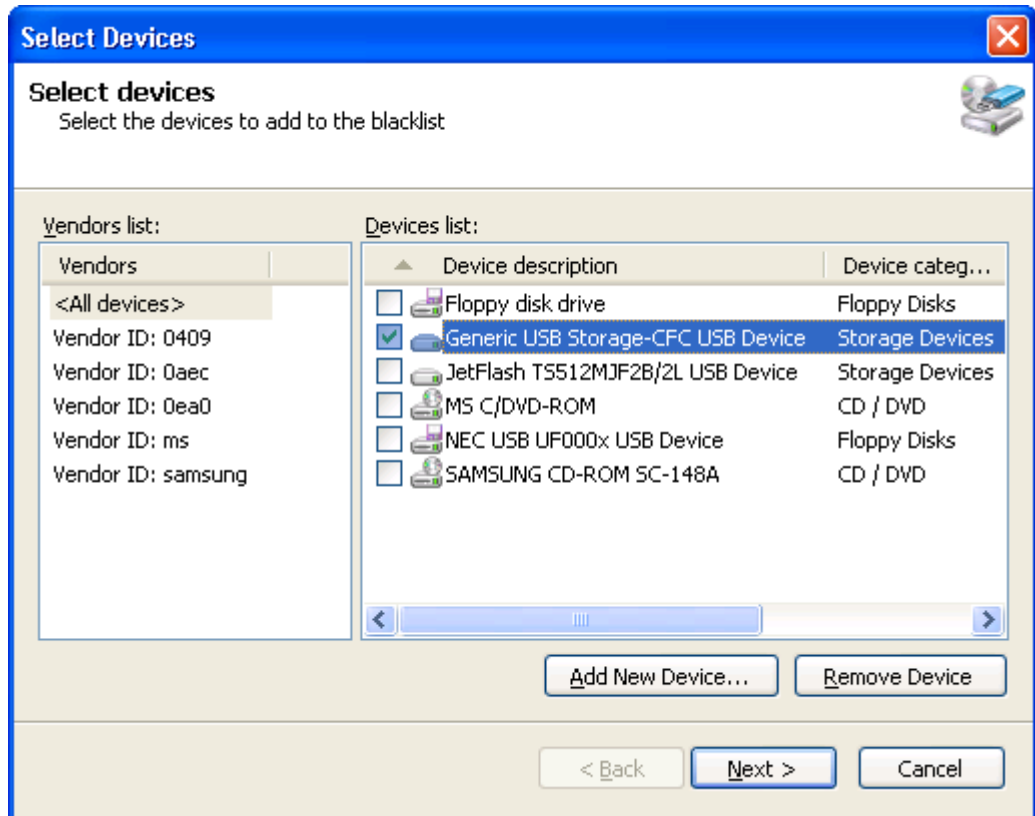
GFI EndPointSecurity consente di indicare i dispositivi da rendere inaccessibili a tutti. La blacklist è granulare, il che significa che è possibile persino inserirvi un dispositivo con numero seriale specifico. È possibile specificare le blacklist per singolo criterio di protezione.

NOTA: gli Utenti autorizzati potranno derogare a qualunque dispositivo inserito nella blacklist.

Per aggiungere dispositivi alla blacklist, seguire questa procedura.

1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Protection Policies (Criteri di protezione)**.

3. Nel pannello di sinistra, selezionare il criterio di protezione da configurare.
4. Nel pannello di destra, fare clic su **Devices Blacklist (Blacklist dispositivi)** della sezione **Security (Sicurezza)**.
5. Fare clic su **Add (Aggiungi)** per selezionare dispositivi da aggiungere alla blacklist.

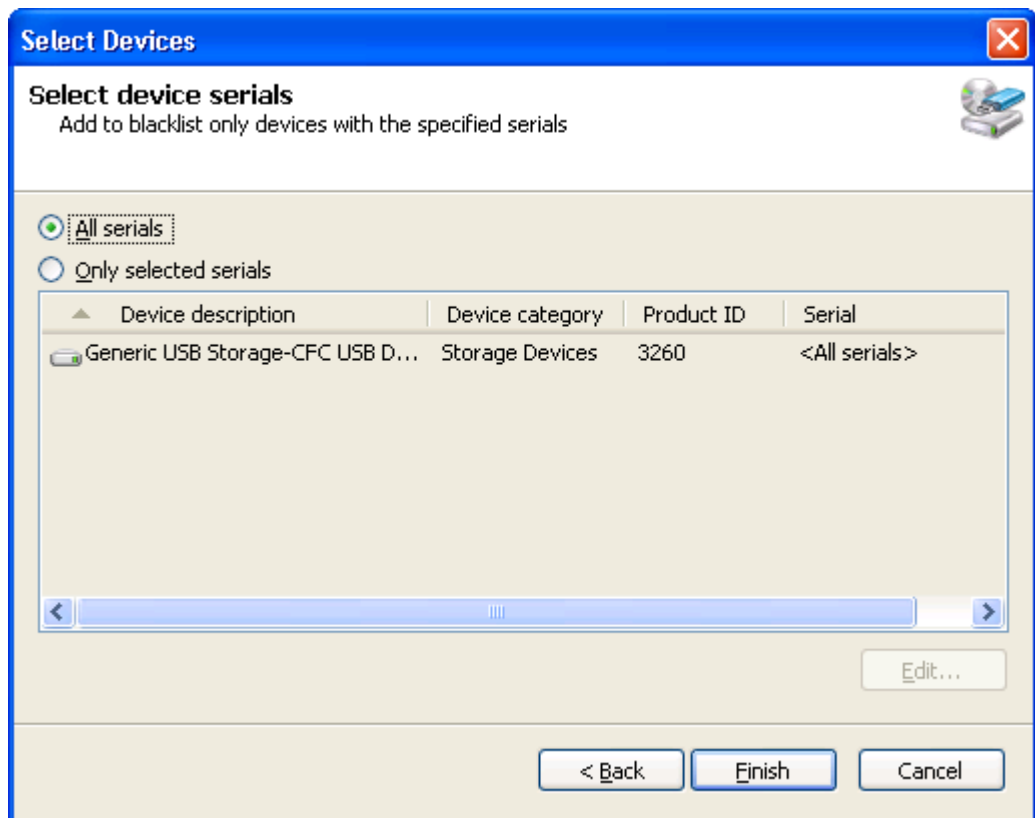


Schermata 66 – Aggiunta di dispositivi alla blacklist

6. Nell'apposito database, selezionare i dispositivi da aggiungere alla blacklist.

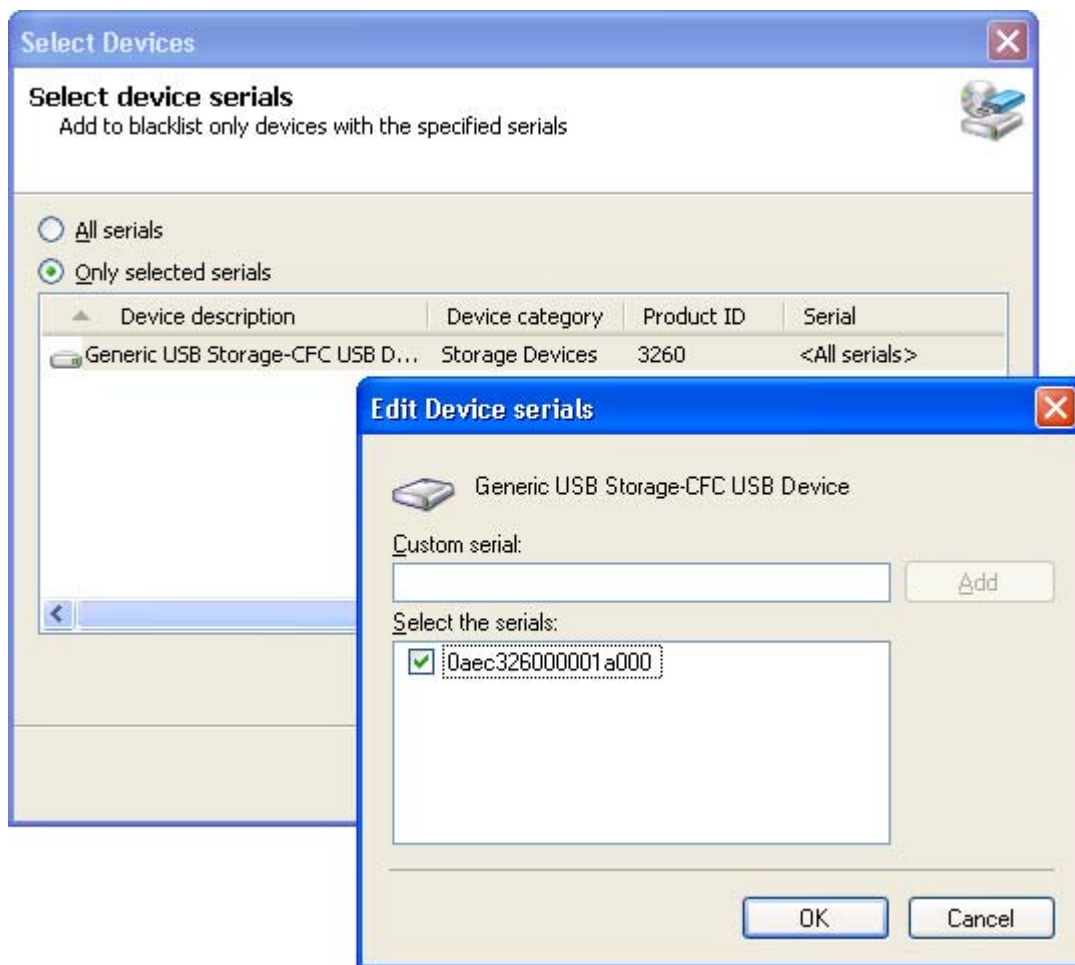
NOTA: se un dispositivo non è elencato, è possibile aggiungerlo facendo clic sul pulsante **Add (Aggiungi)** e inserendone i dettagli.

Fare clic su **Next (Avanti)** per continuare.



Schermata 67 – Inserimento nella blacklist di tutti i numeri seriali

7. Per inserire nella blacklist tutti i numeri seriali di un determinato dispositivo, selezionare l'opzione **All serials (Tutti i numeri seriali)**.



Schermata 68 – Aggiunta di numeri seriali agli elementi inseriti nella blacklist

Per specificare solo determinati numeri seriali del dispositivo da aggiungere alla blacklist, selezionare l'opzione **Only selected serials (Soltanto i numeri seriali selezionati)**. Evidenziare quindi il dispositivo e fare clic su **Edit (Modifica)** per selezionare i numeri seriali da inserire nella blacklist.

Fare clic su **OK** e poi su **Finish (Fine)** per completare le impostazioni.

8. Distribuire gli aggiornamenti del criterio di protezione sui computer compresi nel criterio. Nel pannello di sinistra, fare clic con il pulsante destro del mouse sul criterio di protezione configurato e selezionare **Deployment ▶ Deploy agent(s) (Distribuzione ▶ Distribuisci agenti)**.

NOTA: per eseguire questo passaggio, è anche possibile adoperare la scelta rapida di tastiera **CTRL + D**.

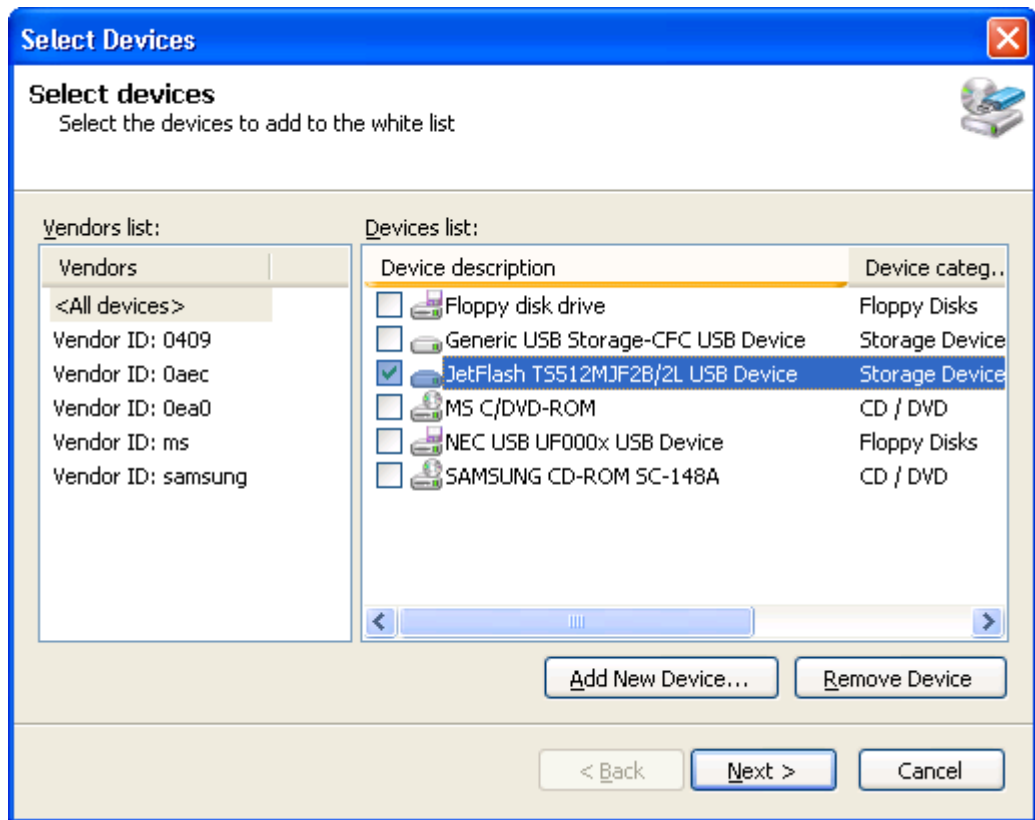
Configurazione whitelist dispositivi portatili

GFI EndPointSecurity consente di indicare i dispositivi da rendere accessibili a tutti. La whitelist è granulare, il che significa che è possibile persino inserirvi un dispositivo con numero seriale specifico. È possibile specificare le whitelist per singolo criterio di protezione.

Per aggiungere dispositivi alla whitelist, seguire questa procedura.

1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Protection Policies (Criteri di protezione)**.

3. Nel pannello di sinistra, selezionare il criterio di protezione da configurare.
4. Nel pannello di destra, fare clic su **Devices Whitelist (Whitelist dispositivi)** della sezione **Security (Sicurezza)**.
5. Fare clic su **Add (Aggiungi)** per selezionare dispositivi da aggiungere alla whitelist.

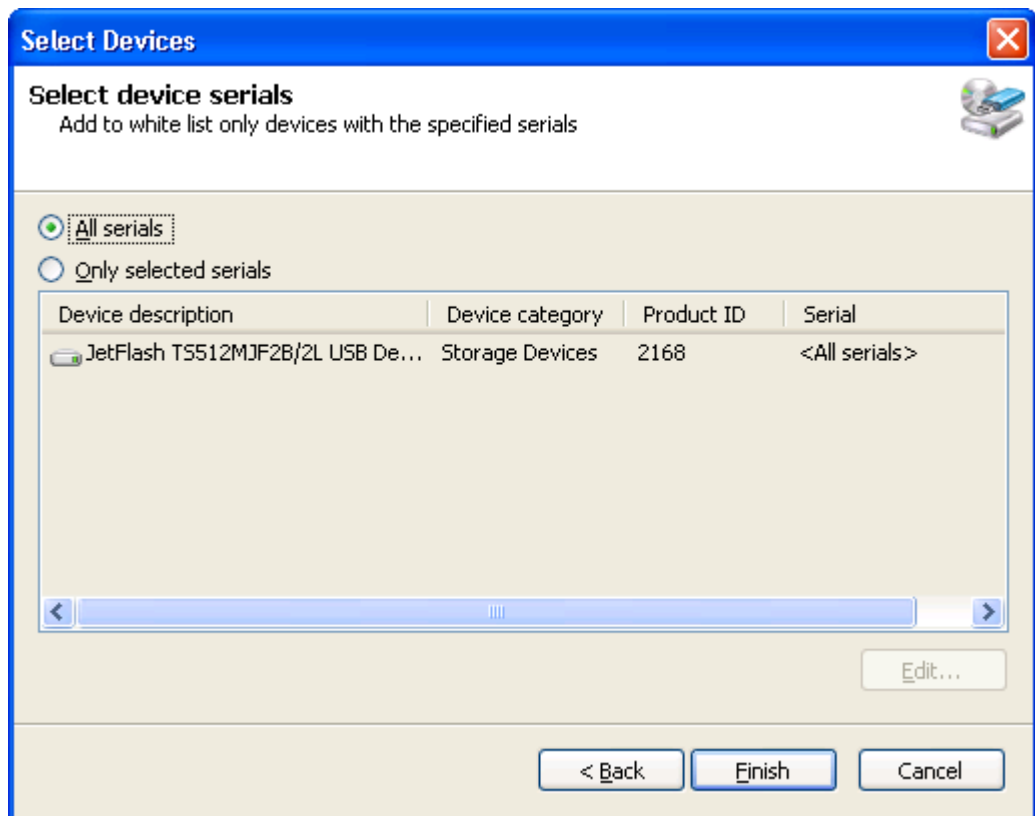


Schermata 69 – Aggiunta dispositivo alla whitelist

6. Nell'apposito database, selezionare i dispositivi da aggiungere alla whitelist.

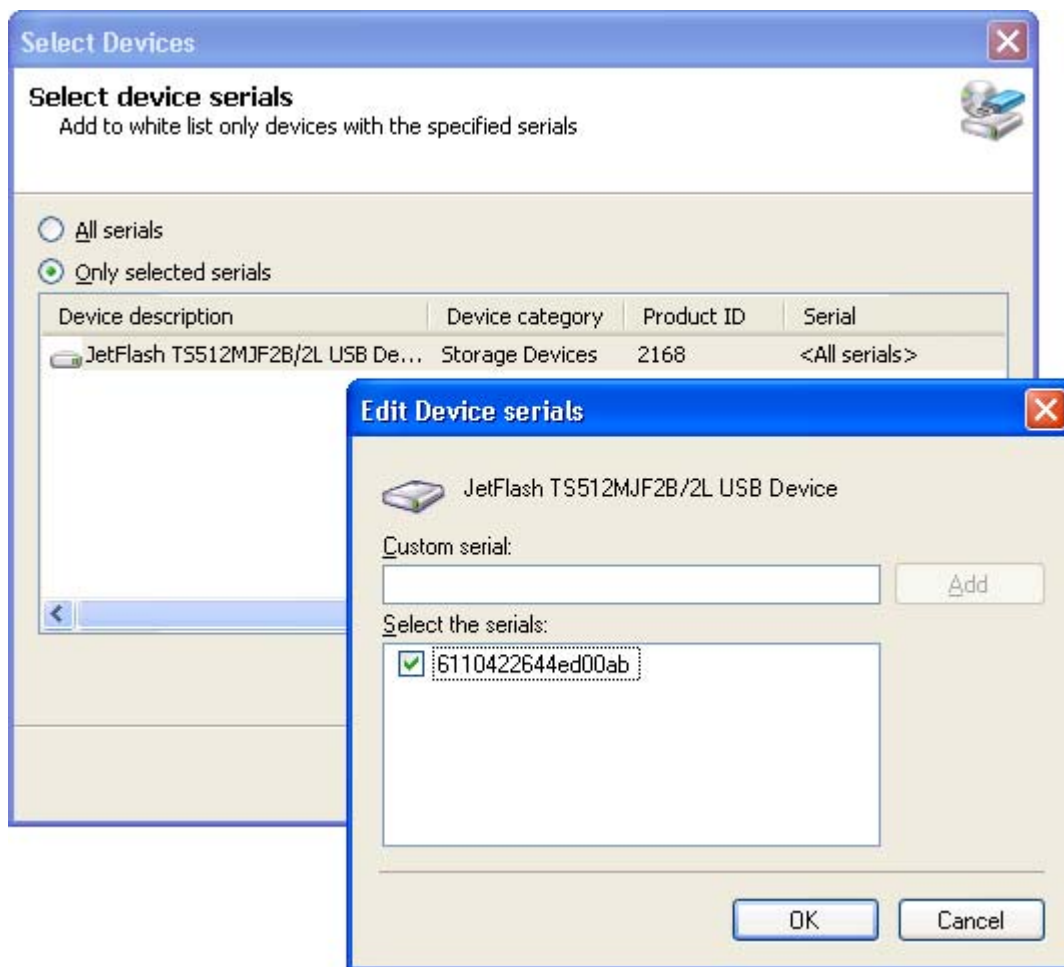
NOTA: se un dispositivo non è elencato, è possibile aggiungerlo facendo clic sul pulsante **Add (Aggiungi)** e inserendone i dettagli.

Fare clic su **Next (Avanti)** per continuare.



Schermata 70 – Inserimento nella whitelist di tutti i numeri seriali

7. Per inserire nella whitelist tutti i numeri seriali di un determinato dispositivo, selezionare l'opzione **All serials (Tutti i numeri seriali)**.



Schermata 71 – Aggiunta di numeri seriali agli elementi inseriti nella whitelist

Per specificare solo determinati numeri seriali del dispositivo da aggiungere alla whitelist, selezionare l'opzione **Only selected serials (Soltanto i numeri seriali selezionati)**. Evidenziare quindi il dispositivo e fare clic su **Edit (Modifica)** per selezionare i numeri seriali da inserire nella whitelist.

Fare clic su **OK** e poi su **Finish (Fine)** per completare le impostazioni.

8. Distribuire gli aggiornamenti del criterio di protezione sui computer compresi nel criterio. Nel pannello di sinistra, fare clic con il pulsante destro del mouse sul criterio di protezione configurato e selezionare **Deployment ▶ Deploy agent(s) (Distribuzione ▶ Distribuisci agenti)**.

NOTA: per eseguire questo passaggio, è anche possibile adoperare la scelta rapida di tastiera **CTRL + D**.

Configurazione privilegi di accesso temporaneo

GFI EndPointSecurity permette agli amministratori di concedere un accesso temporaneo agli utenti, consentendo a questi ultimi di accedere a dispositivi portatili su computer protetti quando il normale accesso agli stessi è bloccato. È possibile concedere l'accesso temporaneo per singolo criterio di protezione.

I passaggi necessari per richiedere e poi concedere l'accesso temporaneo sono i seguenti:

1. L'utente richiede l'accesso temporaneo generando un codice di richiesta con lo strumento GFI EndPointSecurity Temporary Access localizzato sul computer protetto.
 2. L'utente comunica il codice di richiesta all'amministratore, via email, SMS o altri metodi di comunicazione.
- NOTA:** l'utente dovrà inoltre informare l'amministratore in merito al tipo di dispositivo cui desidera accedere e per quanto tempo.
3. L'amministratore inserisce il codice di richiesta nella consolle di gestione di GFI EndPointSecurity Temporary Access.
 4. L'amministratore seleziona le categorie di dispositivi e le porte di connessione cui concedere l'accesso temporaneo, specificandone i limiti temporali.
 5. L'amministratore genera un codice di sblocco.
 6. L'amministratore comunica il codice di sblocco all'utente, via email, SMS o altri metodi di comunicazione.
 7. L'utente inserisce il codice di sblocco nello strumento GFI EndPointSecurity Temporary Access.

Richiesta di accesso temporaneo per un computer protetto

Per generare il codice di richiesta, seguire questa procedura:

Schermata 72 – Gruppo di accesso temporaneo

1. Avviare lo strumento GFI EndPointSecurity Temporary Access dal menu **Start ▶ Pannello di controllo ▶ Accesso temporaneo ai dispositivi**.
2. Annotare il codice di richiesta generato e comunicarlo all'amministratore di sistema. Tenere aperto lo strumento di accesso temporaneo.

3. Quando l'amministratore invia il codice di sblocco, inserirlo nell'apposito campo. Fare clic su **Unlock (Sblocca)** per attivare l'accesso temporaneo.

Concessione accesso temporaneo a un computer protetto

Per concedere un accesso temporaneo, seguire questa procedura:

1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Protection Policies (Criteri di protezione)**.
3. Nel pannello di sinistra, selezionare il criterio di protezione che comprende il computer cui verrà concesso l'accesso temporaneo.
4. Nel pannello di destra, fare clic sull'opzione **Grant temporary access (Concedi accesso temporaneo)** della sezione **Temporary Access (Accesso temporaneo)**.

Grant temporary access

Request code
Enter request code

The user has to use the "GFI EndPointSecurity Temporary Access" tool which is installed on the client computer to generate the request code.

Request code:

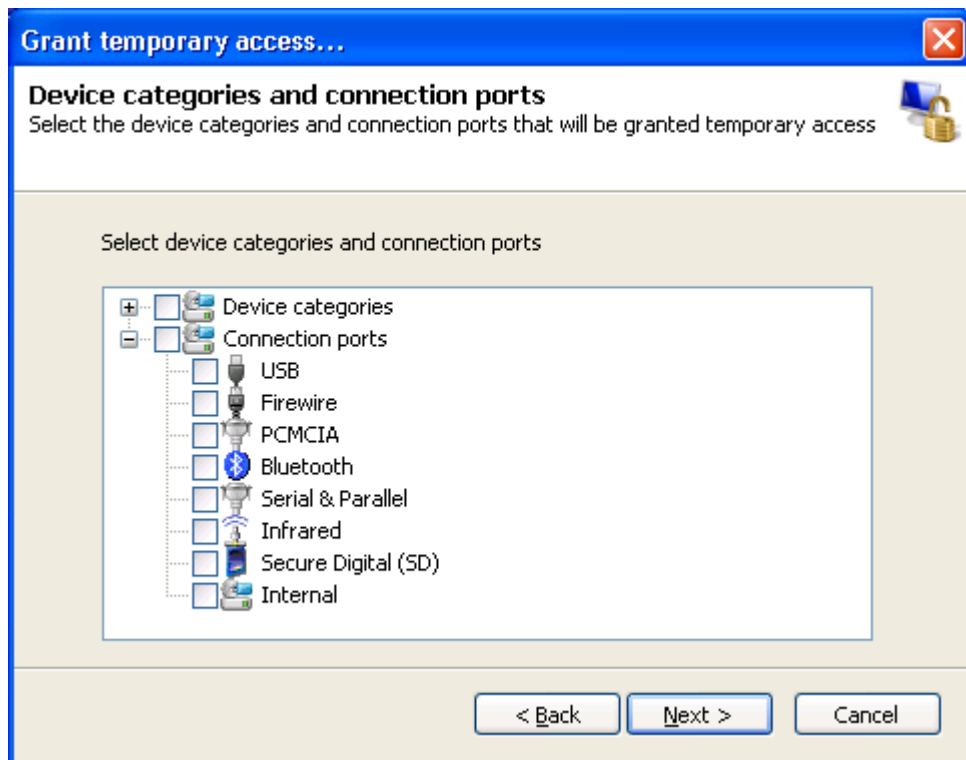
EcHP6n cmR5L\$ 4#Ed8K RivU8G 3P*

Computer Name:
TWWINXPTESTVM1

< Back Next > Cancel

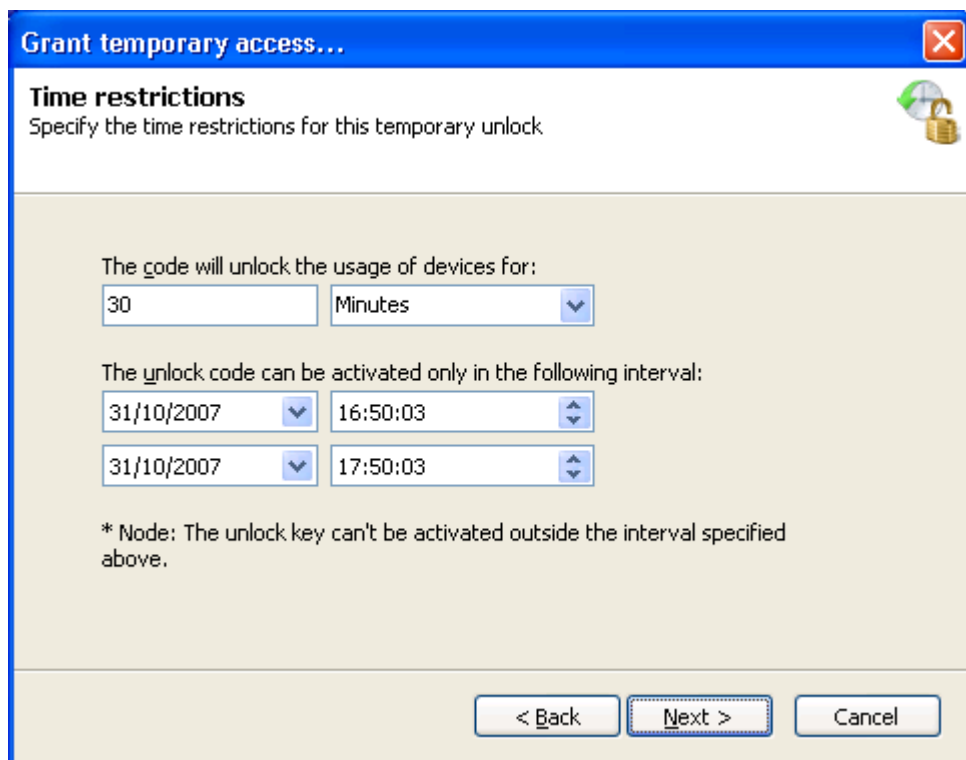
Schermata 73 – Connessione accesso temporaneo

5. Inserire il codice di richiesta ricevuto dall'utente nel campo **Request code (Codice di richiesta)**. Viene quindi visualizzato il nome computer da cui è stata generata la richiesta. Fare clic su **Next (Avanti)** per continuare.



Schermata 74 – Indicazione delle categorie o porte cui attribuire l'accesso temporaneo

6. Selezione delle categorie di dispositivi e/o porte di connessione cui concedere l'accesso temporaneo.



Schermata 75 – Indicazione dei limiti temporali di accesso temporaneo

7. Indicare la durata dell'accesso consentito e il periodo di validità del codice di sblocco.

NOTA: un codice di sblocco inserito sul computer protetto al di là del periodo di validità specificato non attiverà l'accesso temporaneo.

8. Annotare il codice di sblocco generato e comunicarlo all'utente che richiede l'accesso temporaneo. Fare clic su **Finish (Fine)** per completare le impostazioni.

Configurazione dei filtri dei tipi di file

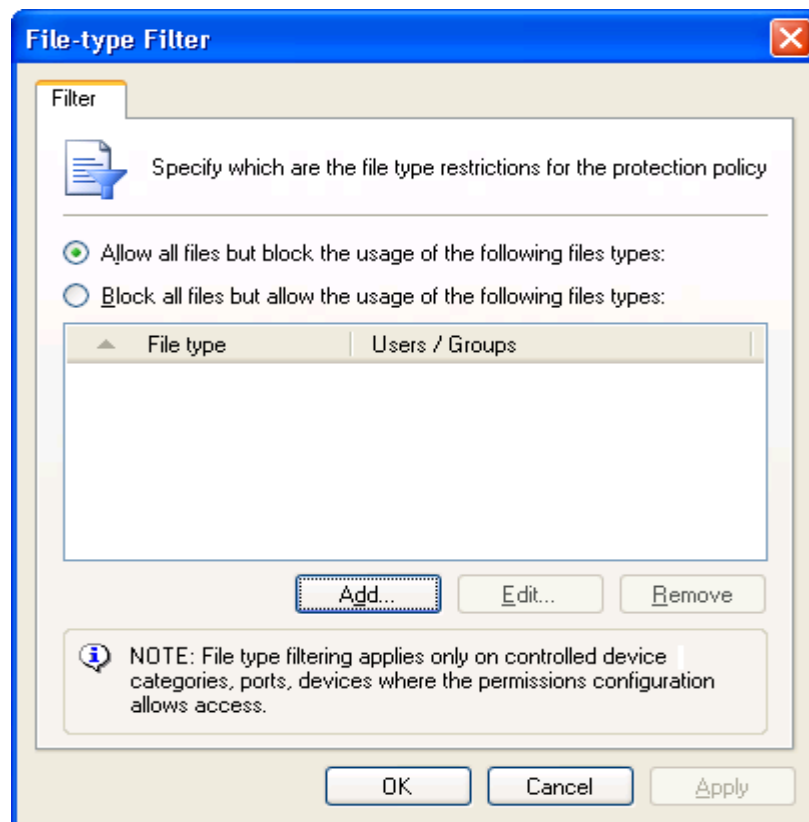
GFI EndPointSecurity consente di specificare limiti in termini di tipi di file, ad esempio, .DOC O .XLS, copiati da/verso dispositivi autorizzati. È possibile applicare tali limiti a qualsiasi utente o gruppo di utenti appartenente ad Active Directory (AD) o a utenti locali o schemi di gruppi. Questa operazione può essere eseguita per singolo criterio di protezione.

NOTA 1: il filtraggio è basato solo sul controllo dell'estensione file, non su quello della firma effettiva del tipo di file.

NOTA 2: il filtraggio del tipo di file si applica unicamente a categorie di dispositivi e/o porte per i quali sono state impostate autorizzazioni di accesso.

Per specificare i limiti di tipi di file, seguire questa procedura:

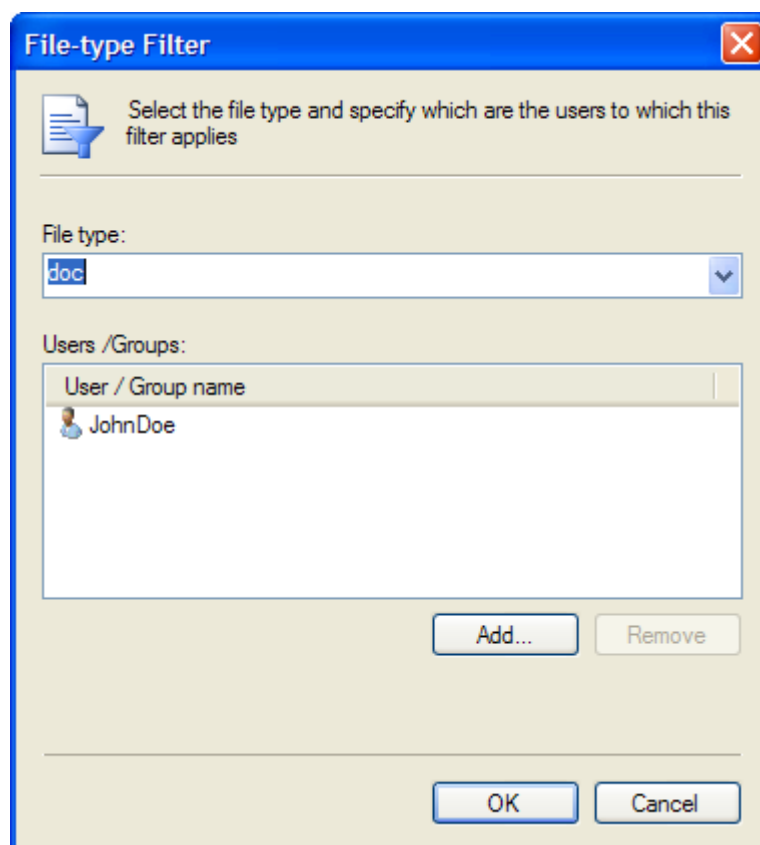
1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Protection Policies (Criteri di protezione)**.
3. Nel pannello di sinistra, selezionare il criterio di protezione di cui si desidera specificare i limiti dei tipi di file.
4. Nel pannello di destra, fare clic sull'opzione **File-type Filter (Filtro tipo di file)** della sezione **File control (Controllo file)**.



Schermata 76 – Selezione dei limiti da applicare

5. Selezionare il limite da applicare.

- Autorizzare tutti i file, ma bloccare l'utilizzo di specifici tipi di file
- Bloccare tutti i file, ma consentire l'utilizzo di specifici tipi di file



Schermata 77 – Indicare tipo di file e utente

Fare clic su **Add (Aggiungi)** per selezionare il tipo di file e gli utenti/gruppi cui applicare la restrizione. Ripetere l'operazione per ogni tipo di file cui applicare il limite.

Fare clic due volte su **OK** per completare le impostazioni.

6. Distribuire gli aggiornamenti del criterio di protezione sui computer compresi nel criterio. Nel pannello di sinistra, fare clic con il pulsante destro del mouse sul criterio di protezione configurato e selezionare **Deployment ▶ Deploy agent(s) (Distribuzione ▶ Distribuisci agenti)**.

NOTA: per eseguire questo passaggio, è anche possibile adoperare la scelta rapida di tastiera **CTRL + D**.

Configurazione della registrazione eventi

Gli agenti di GFI EndPointSecurity registrano eventi correlati ai tentativi di accesso effettuati a dispositivi di supporto portatili. Gli agenti registrano inoltre eventi relativi a operazioni di servizio. È possibile indicare la locazione (o entrambe le locazioni) seguenti in cui archiviare tali eventi:

- i log degli eventi di sicurezza di Windows del computer protetto. È possibile visualizzare gli eventi con il Visualizzatore eventi di Windows oppure raccogliere tutti gli eventi in una locazione centrale con GFI EventsManager
- un database centrale Microsoft SQL Server. È possibile visualizzare gli eventi con il Browser di log della consolle di gestione di GFI EndPointSecurity.

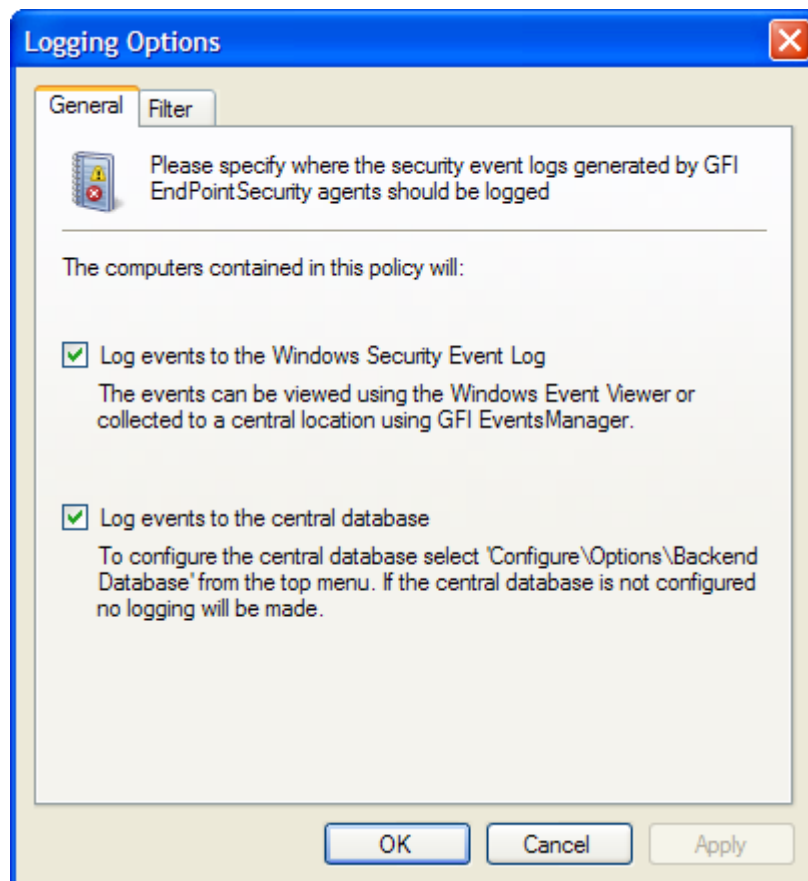
È altresì possibile indicare i tipi di eventi da registrare:

- Eventi di servizio
- Eventi relativi alla connessione al dispositivo
- Eventi relativi alla disconnessione del dispositivo
- Eventi relativi agli accessi autorizzati
- Eventi relativi agli accessi non autorizzati.

È possibile indicare la locazione e i tipi di eventi per singolo criterio di protezione.

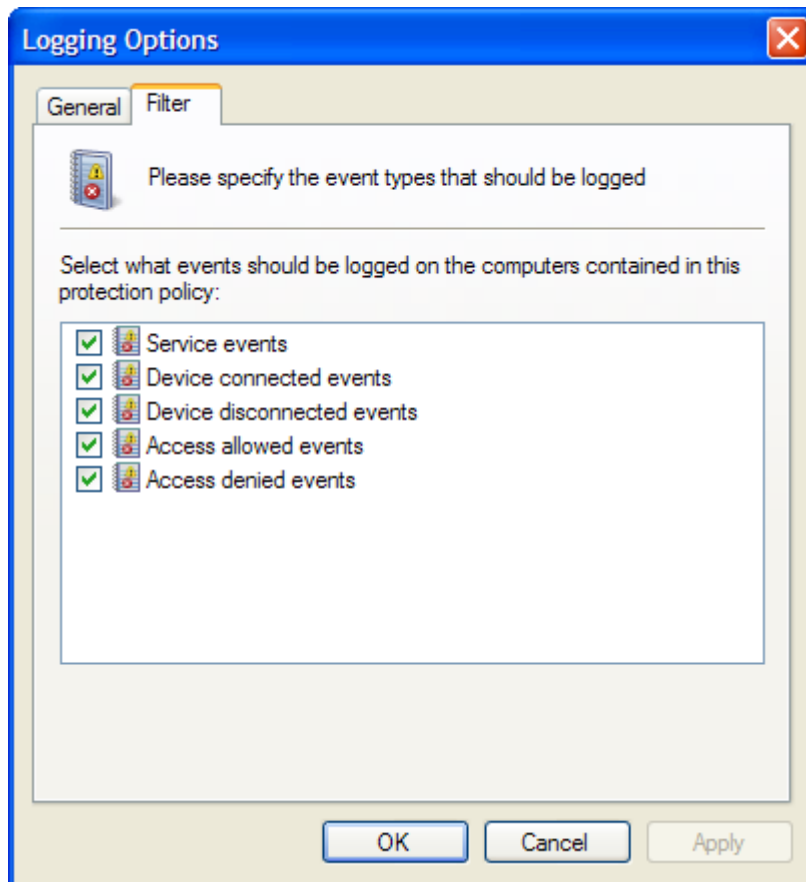
Per specificare le opzioni di registrazione, seguire questa procedura:

1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Protection Policies (Criteri di protezione)**.
3. Nel pannello di sinistra, selezionare il criterio di protezione di cui si desidera specificare le opzioni di registrazione.
4. Nel pannello di destra, fare clic su **Set logging options (Impostare opzioni di registrazione)** della sezione **Logging and Alerting (Registrazione e avvisi)**.



Schermata 78 – Opzioni di registrazione: scheda Generale

5. Fare clic sulla scheda **General (Generale)** per specificare le locazioni in cui archiviare gli eventi del criterio di protezione.



Schermata 79 – Opzioni di registrazione: scheda Filtro

6. Fare clic sulla scheda **Filter (Filtro)** per indicare gli eventi da registrare per il criterio di protezione.

7. Fare clic su **OK** per completare le impostazioni.

8. Distribuire gli aggiornamenti del criterio di protezione sui computer compresi nel criterio. Nel pannello di sinistra, fare clic con il pulsante destro del mouse sul criterio di protezione configurato e selezionare **Deployment ▶ Deploy agent(s) (Distribuzione ▶ Distribuisci agenti)**.

NOTA: per eseguire questo passaggio, è anche possibile adoperare la scelta rapida di tastiera **CTRL + D**.

Configurazione notifiche

Quando viene generato un determinato evento, GFI EndPointSecurity può inviare avvisi a specifici destinatari. È possibile configurare avvisi da inviare mediante:

- Email
- Messaggi di rete
- SMS.

È altresì possibile indicare i tipi di eventi in relazione ai quali si desidera inviare gli avvisi:

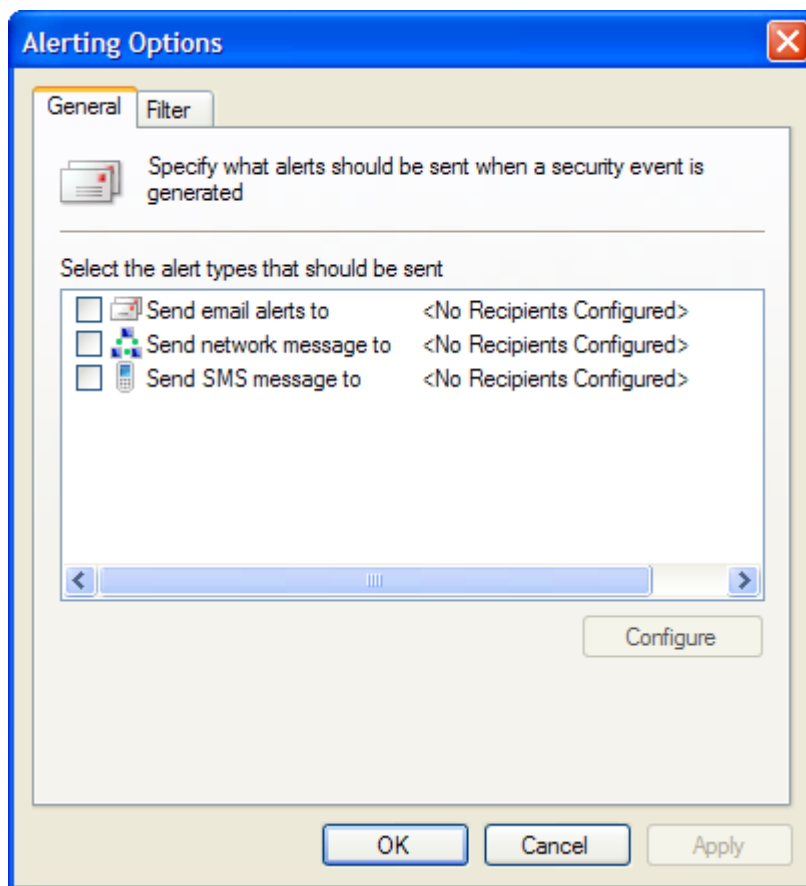
- Eventi di servizio

- Eventi relativi alla connessione al dispositivo
- Eventi relativi alla disconnessione del dispositivo
- Eventi relativi agli accessi autorizzati
- Eventi relativi agli accessi non autorizzati.

È possibile indicare opzioni di avviso per singoli criteri di protezione.

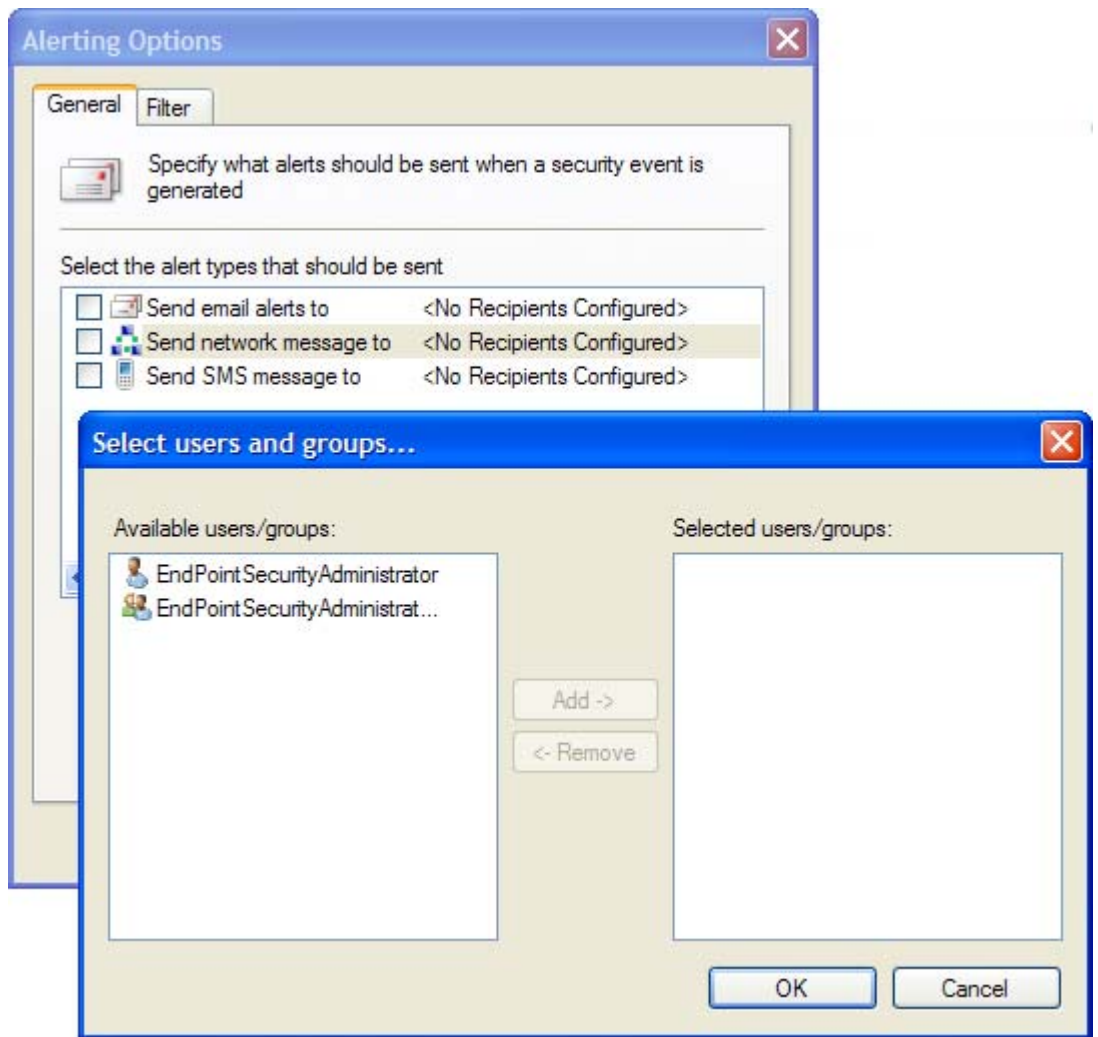
Per specificare le opzioni di avviso, seguire questa procedura:

1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Protection Policies (Criteri di protezione)**.
3. Nel pannello di sinistra, selezionare il criterio di protezione di cui si desidera specificare le opzioni di registrazione.
4. Nel pannello di destra, fare clic su **Alerting options (Opzioni di avviso)** della sezione **Logging and Alerting (Registrazione e avvisi)**.



Schermata 80 – Opzioni di avviso: scheda Generale

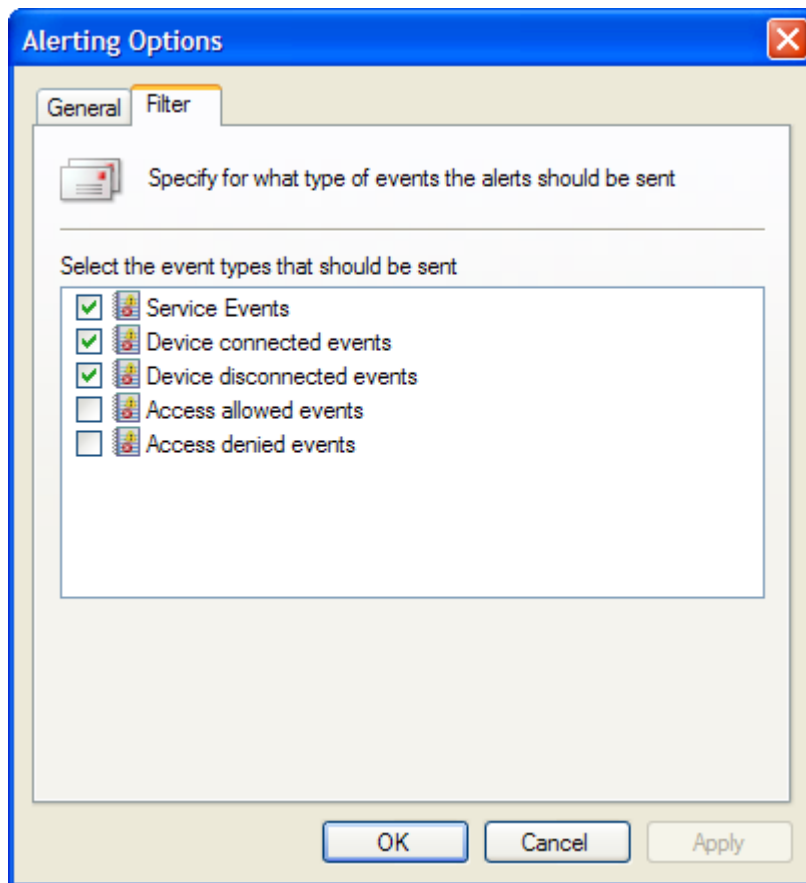
5. Fare clic sulla scheda **General (Generale)** per indicare il tipo di avvisi da inviare.



Schermata 81 - Configurazione utenti e gruppi

6. Per ogni tipo di avviso selezionato, fare clic su **Configure (Configura)** per indicare gli utenti/gruppi cui inviare l'avviso.

NOTA: non si tratta di Active Directory (AD) o utenti locali e schemi di gruppi (gli utenti e gruppi vengono creati mediante **Configurazione ▶ Opzioni ▶ Opzioni di avviso**).



Schermata 82 – Opzioni di avviso: scheda Filtro

7. Fare clic sulla scheda **Filter (Filtro)** per specificare i tipi di eventi in relazione ai quali inviare avvisi.
8. Fare clic su **OK** per completare le impostazioni.
9. Distribuire gli aggiornamenti del criterio di protezione sui computer compresi nel criterio. Nel pannello di sinistra, fare clic con il pulsante destro del mouse sul criterio di protezione configurato e selezionare **Deployment ▶ Deploy agent(s) (Distribuzione ▶ Distribuisci agenti)**.

NOTA: per eseguire questo passaggio, è anche possibile adoperare la scelta rapida di tastiera **CTRL + D**.

Configurazione delle impostazioni predefinite di GFI EndPointSecurity

Introduzione

GFI EndPointSecurity consente di configurare una serie di parametri predefiniti.

Presentazione del capitolo

Verranno coperte le seguenti sezioni:

- configurazione account amministratore di GFI EndPointSecurity
- configurazione opzioni di avviso
- configurazione utenti da avvisare
- configurazione gruppi da avvisare
- configurazione terminale database di SQL Server
- personalizzazione messaggi utenti
- opzioni avanzate.

Configurazione account amministratore di GFI EndPointSecurity

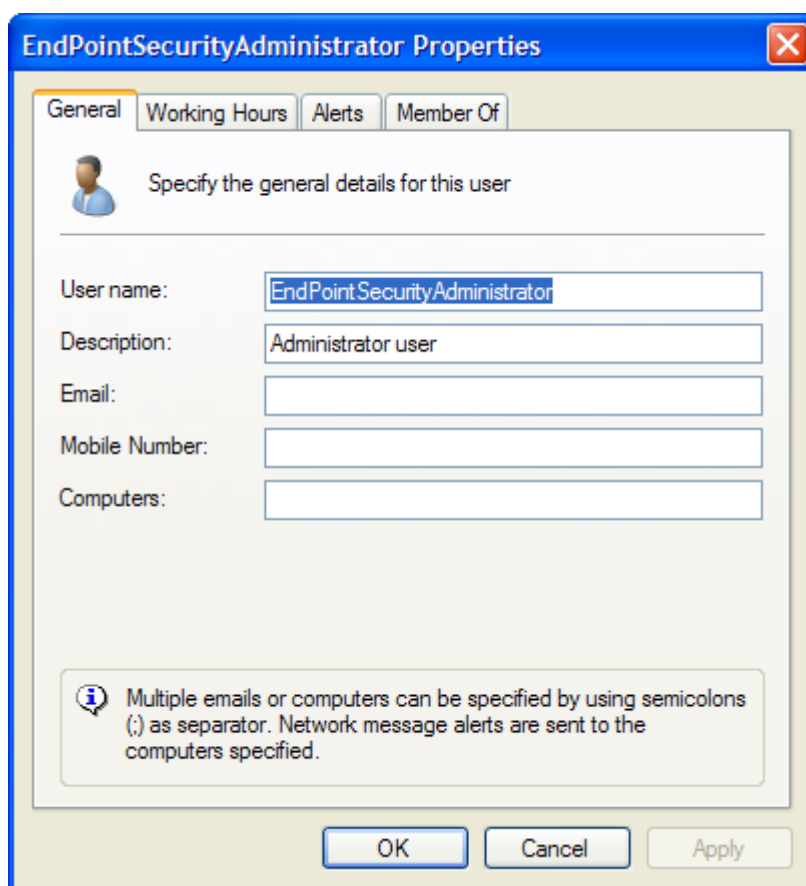
Ogni volta che scopre eventi particolari, GFI EndPointSecurity invia automaticamente avvisi a destinatari specifici tramite email, messaggi di rete o SMS. Pertanto, è necessario configurare i recapiti dei destinatari desiderati per distribuire gli avvisi in modo efficace. Per esempio, è necessario configurare l'indirizzo email dei destinatari per poter inviare loro gli avvisi via email.

GFI EndPointSecurity consente di creare un elenco personalizzato di destinatari, che è possibile organizzare in gruppi per velocizzare le operazioni amministrative. Per impostazione predefinita, GFI EndPointSecurity crea automaticamente l'account "EndPointSecurityAdministrator". Tuttavia, vanno ancora configurati informazioni specifiche degli utenti, quali l'indirizzo email e il numero di cellulare dell'amministratore di GFI EndPointSecurity. Per tutti gli utenti, è possibile configurare i seguenti parametri:

- le informazioni di recapito, compresi indirizzo email e numero di telefono
- il normale orario di lavoro
- il tipo di avviso da inviare durante e al di fuori dell'orario di lavoro
- il gruppo di notifica di appartenenza dell'utente.

Per configurare la prima volta l'account GFI EndPointSecurityAdministrator, fare clic sul collegamento fornito nella

sezione **Configure Alerting Options (Configura opzioni di avviso)**
finestra di dialogo dell'Avvio rapido.

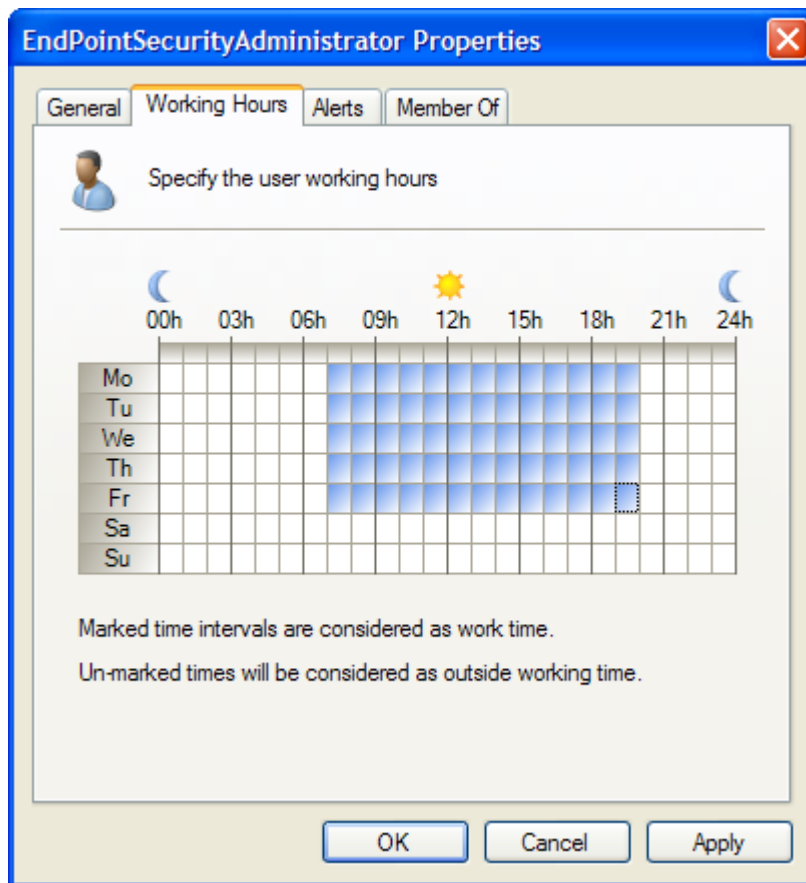


The screenshot shows a Windows-style dialog box titled "EndPointSecurityAdministrator Properties". It has four tabs: "General", "Working Hours", "Alerts", and "Member Of". The "General" tab is selected. Below the tabs, there is a user icon and the text "Specify the general details for this user". The form contains five input fields: "User name:" with the value "EndPointSecurityAdministrator", "Description:" with the value "Administrator user", "Email:", "Mobile Number:", and "Computers:". At the bottom, there is an information icon and a text box stating: "Multiple emails or computers can be specified by using semicolons (;) as separator. Network message alerts are sent to the computers specified." Below the information box are three buttons: "OK", "Cancel", and "Apply".

Schermata 83 – Finestra di dialogo delle proprietà di EndPointSecurityAdministrator

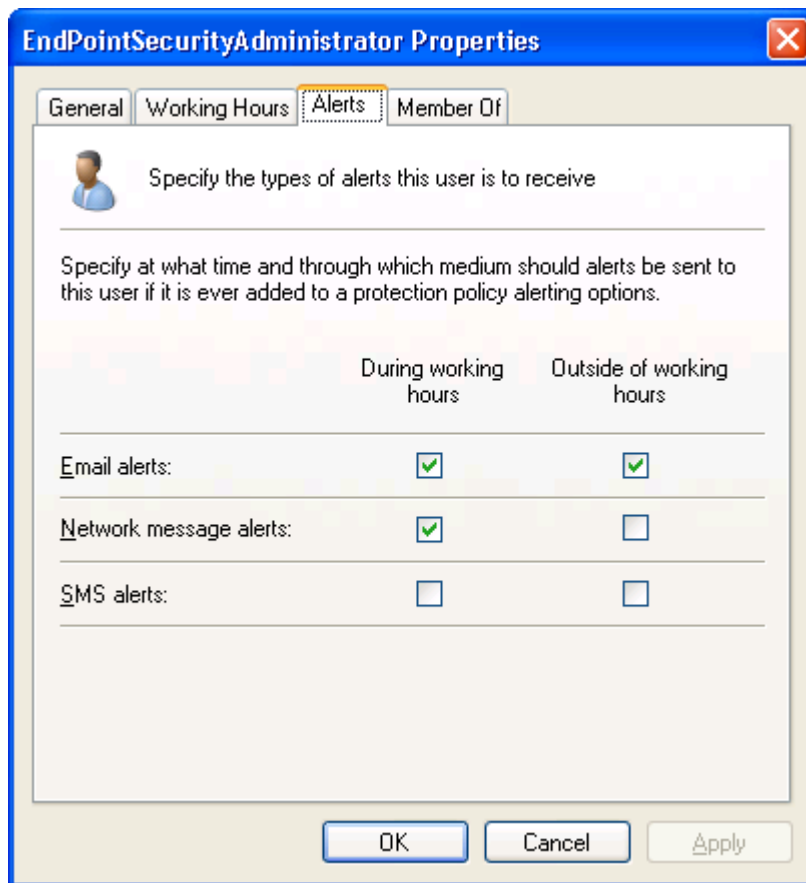
Viene visualizzata la finestra di dialogo "EndPointSecurityAdministrator". Per configurare l'account, seguire questa procedura:

1. Indicare le informazioni di recapito richieste, ad esempio indirizzo email e numero di cellulare.
2. Indicare i computer cui inviare gli avvisi di rete indirizzati all'amministratore.
3. Fare clic sulla scheda **Working Hours (Orario di lavoro)**.



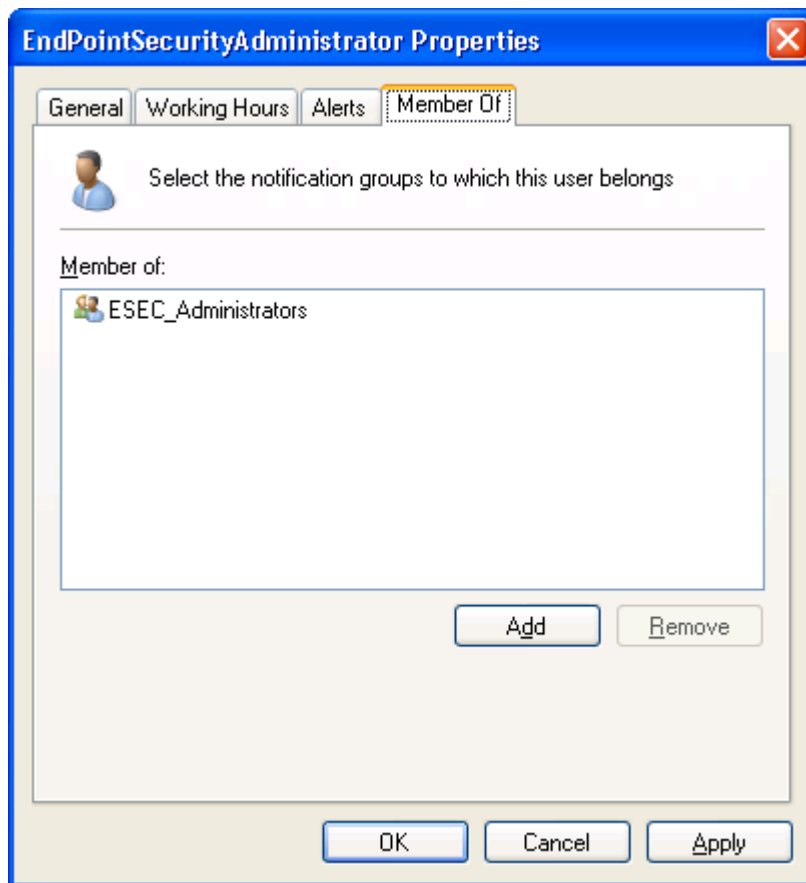
Schermata 84 – Scheda Orario di lavoro

4. Selezionare il normale orario di lavoro dell'amministratore o dell'utente.



Schermata 85 – Scheda degli Avvisi

5. Fare clic sulla scheda **Alerts (Avvisi)** e selezionare gli avvisi da inviare durante e al di fuori dell'orario di lavoro.



Schermata 86 – Scheda Appartenenti a

6. Fare clic sulla scheda **Member Of (Appartenente a)** e selezionare i gruppi di notifica di appartenenza dell'utente. Per impostazione predefinita, l'amministratore appartiene al gruppo di notifica "EndPointSecurityAdministrators (Amministratori di EndPointSecurity)".

7. Fare clic sul pulsante **OK** per completare le impostazioni.

È ancora possibile apportare modifiche alle proprietà dell'account amministratore anche dopo averle configurate. Per maggiori informazioni in proposito, si rinvia alla sezione "Configurazione utenti da avvisare" di questo capitolo.

Configurazione opzioni di avviso

Adoperare la sezione delle opzioni di avviso per configurare:

- le impostazioni del server di posta e il messaggio email da utilizzare nell'invio degli avvisi via email
- il gateway SMS e il messaggio SMS da adoperare nell'invio degli avvisi via SMS
- il messaggio di rete da adoperare nell'invio degli avvisi di rete
- gli utenti destinatari degli avvisi
- i gruppi destinatari degli avvisi.

Per configurare i parametri di avviso generali la prima volta, fare clic sul collegamento **Configure Alerting options (Configura opzioni di avviso)** forniti nella finestra di dialogo dell'Avvio rapido.

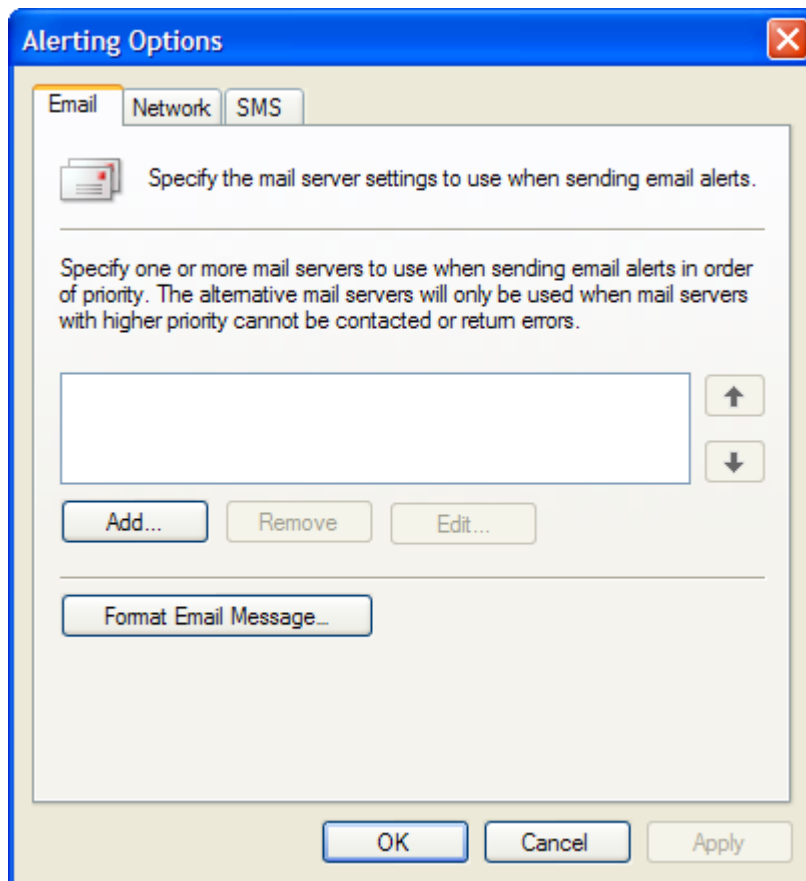
Viene visualizzata la finestra di dialogo "Alerting Options (Opzioni di avviso)". Adoperare le schede **Email**, **Network** e **SMS (Email, Rete e SMS)** presenti in questa finestra di dialogo per configurare le impostazioni di avviso predefinite. Di seguito vengono fornite maggiori informazioni sulle modalità di configurazione di dette impostazioni.

Per accedere alle opzioni di avviso dalla consolle di gestione, seguire questa procedura:

1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Options (Opzioni)**.
3. Nel pannello di sinistra, selezionare **Alerting Options (Opzioni di avvisi)**.
4. Nel pannello di destra, selezionare l'opzione da configurare.

Avvisi via email

Per configurare le opzioni di avviso email, seguire questa procedura:



Schermata 87 – Opzioni di avviso via mail

1. Nella finestra di dialogo delle Opzioni di avviso, fare clic sul pulsante **Add (Aggiungi)** della scheda **Email** che si apre per impostazione predefinita, per configurare le impostazioni del server di posta.
2. Indicare il nome o l'IP del proprio server di posta. Se necessario, indicare inoltre i dati di autenticazione sul server di posta.
3. Indicare l'indirizzo email e il nome visualizzato da adoperare per l'invio di avvisi via email.

4. Fare clic su **OK** per completare le impostazioni.
5. Per personalizzare il testo del messaggio email, fare clic sul pulsante **Format Email Message... (Formatta messaggio email...)**.
6. Se necessario, fare clic sulle schede **Network (Rete)** o **SMS** per configurare i rispettivi parametri.
7. Fare clic su **OK** per completare le impostazioni.

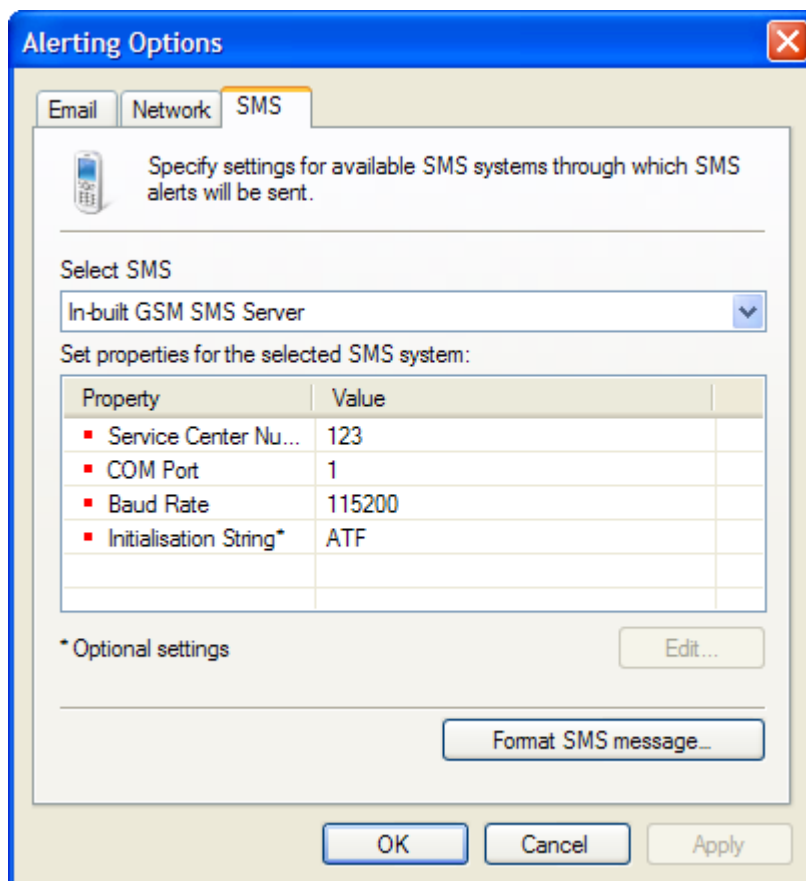
Avvisi mediante messaggi di rete

In questa finestra di dialogo non sono richieste impostazioni di configurazione per avvisi di rete. Tuttavia, è possibile personalizzare il messaggio di rete facendo clic sul pulsante **Format network message... (Formatta messaggio di rete)**.

Avvisi SMS

Gli avvisi SMS possono essere inviati in vari modi. Tra i metodi supportati figurano il gateway SMS di GFI FAXmaker e il gateway del servizio email verso SMS di Clickatell. Per configurare le opzioni di avviso SMS, seguire questa procedura:

1. Nella finestra di dialogo delle Opzioni di avviso, fare clic sulla scheda **SMS**.



Schermata 88 – Opzioni di avviso SMS

2. Selezionare il sistema SMS con cui inviare le notifiche SMS, nell'apposito elenco a discesa.
3. Nell'apposito elenco fornito, selezionare la proprietà da configurare e fare clic su **Edit... (Modifica)**.

4. Ripetere l'operazione finché non si sono configurate tutte le proprietà desiderate.
5. Per personalizzare il messaggio dell'avviso SMS, fare clic sul pulsante **Format SMS Message... (Formatta messaggio SMS...)**.
6. Fare clic su **OK** per completare le impostazioni.

Configurazione utenti da avvisare

Creazione utenti

Per creare un nuovo utente, seguire questa procedura:

1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Options (Opzioni)** ed espandere il nodo **Alerting Options (Opzioni di avviso)**.
3. Fare clic con il pulsante destro del mouse sul sub-nodo **Users (Utenti)** e selezionare **Create user... (Crea utenti)**.
4. Indicare i parametri desiderati nelle schede **General, Working Hours, Alerts e Member of**.

NOTA: per maggiori informazioni sulle modalità per compilare queste schede, si rinvia alla sezione "Configurazione dell'account amministratore di GFI EndPointSecurity" di questo capitolo.

Modifica proprietà dell'utente

Per modificare le proprietà dell'utente, seguire questa procedura:

1. nel pannello di sinistra, fare clic sul sub-nodo **Users (Utenti)**
2. nel pannello di destra, fare clic con il pulsante destro del mouse sull'utente da modificare e selezionare **Properties (Proprietà)**
3. apportare le modifiche desiderate e fare clic su **OK** per completare le impostazioni.

Rimozione di utenti

Per rimuovere un utente, seguire questa procedura:

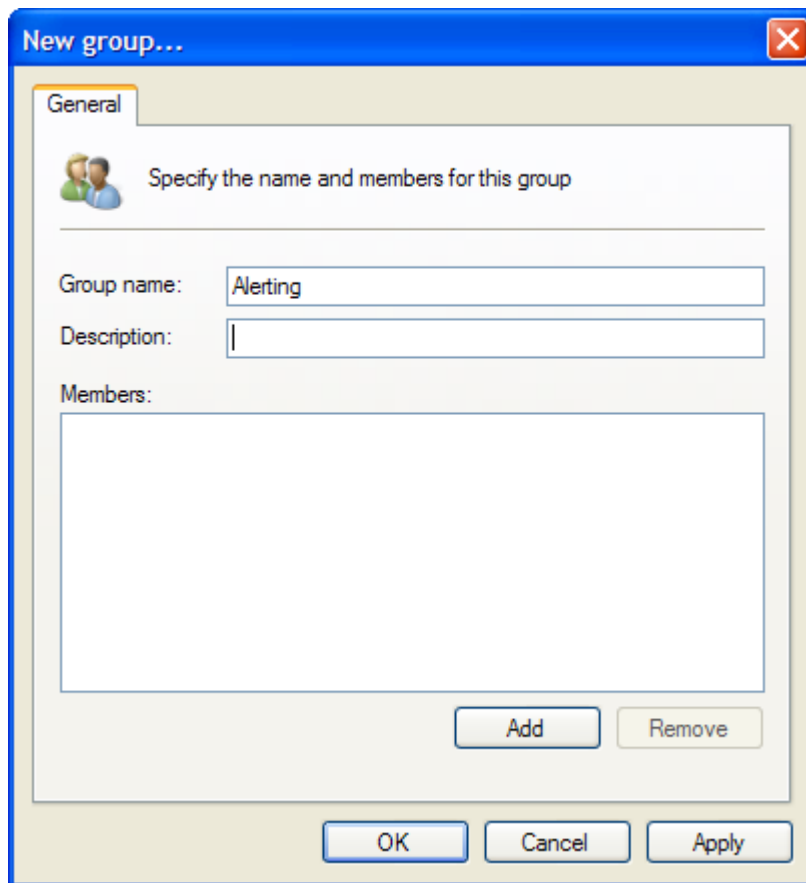
1. nel pannello sinistro, fare clic sul nodo **Users (Utenti)**
2. nel pannello di destra, fare clic con il pulsante destro del mouse sull'utente da eliminare e selezionare **Delete (Elimina)**.

Configurazione gruppi da avvisare

Creazione di gruppi

Per creare un nuovo gruppo, seguire questa procedura:

1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Options (Opzioni)** ed espandere il nodo **Alerting Options (Opzioni di avviso)**.



Schermata 89 – Creazione un nuovo gruppo di utenti

3. Fare clic con il pulsante destro del mouse sul sub-nodo **Group (Gruppo)** e selezionare **Create group... (Crea gruppo)**.
4. Indicare il nome e la descrizione del nuovo gruppo.
5. Fare clic su **Add (Aggiungi)** per cominciare ad aggiungere utenti al gruppo.
6. Fare clic su **OK** per completare le impostazioni.

Modifica delle proprietà di gruppo

Per modificare le proprietà del gruppo, seguire questa procedura:

1. nel pannello sinistro, fare clic sul sub-nodo **Groups (Gruppi)**
2. nel pannello di destra, fare clic con il pulsante destro del mouse sul gruppo da modificare e selezionare **Properties (Proprietà)**
3. apportare le modifiche desiderate e fare clic su **OK** per completare le impostazioni.

Rimozione di gruppi

Per rimuovere un gruppo, seguire questa procedura:

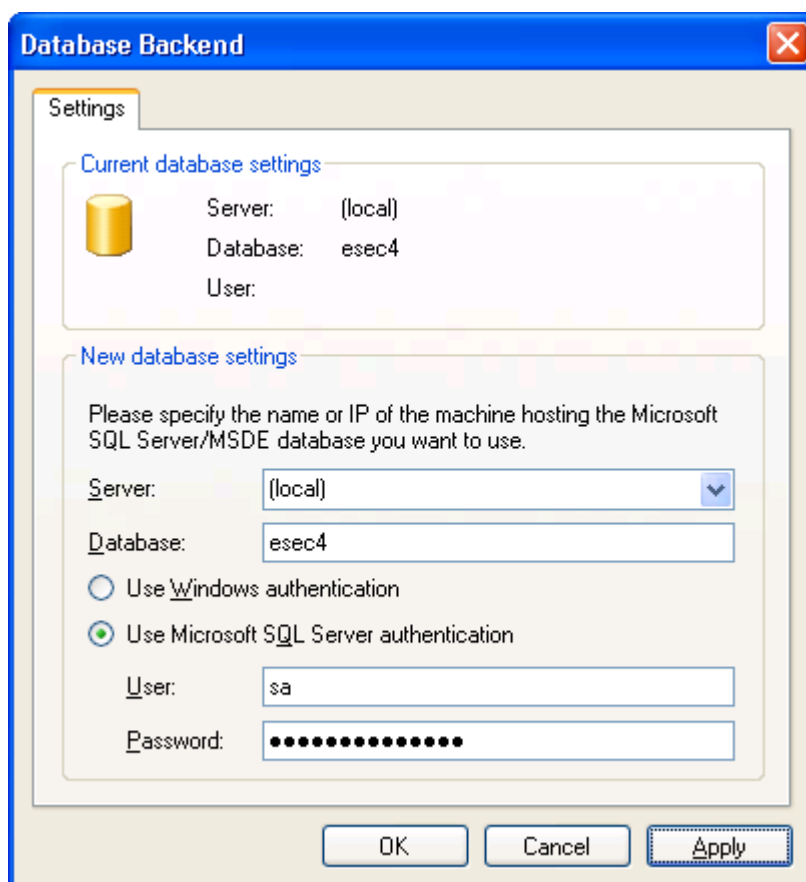
1. nel pannello di sinistra, fare clic sul nodo **Groups (Gruppi)**
2. nel pannello di destra, fare clic con il pulsante destro del mouse sul gruppo da eliminare e selezionare **Delete (Elimina)**.

Configurazione del database terminale

Adoperare la presente sezione per configurare il database Microsoft SQL Server. Il database sarà adoperato da GFI EndPointSecurity per tenere un audit trail di tutti gli eventi generati dagli agenti GFI EndPointSecurity distribuiti sui computer di rete.

Creazione del nuovo database

Per configurare il terminale database la prima volta, fare clic sul collegamento **Configure Backend Database (Configura terminale database)** fornito nella finestra di dialogo dell'Avvio rapido.



Schermata 90 – Finestra di dialogo delle impostazioni del database

Viene visualizzata la finestra di dialogo “Change Database (Modifica database)”. Per configurare Microsoft SQL Server e i dati del terminale database, procedere come segue:

1. Indicare il nome o l'IP del proprio Microsoft SQL Server.
2. Indicare un nome per il terminale database (ad esempio, EndPointSecurity4DB).
3. Selezionare il metodo di autenticazione da adoperare per il collegamento al terminale database. Se si seleziona l'autenticazione Microsoft SQL Server, specificare il nome utente e la password di login.
4. Fare clic su **OK** per completare le impostazioni.

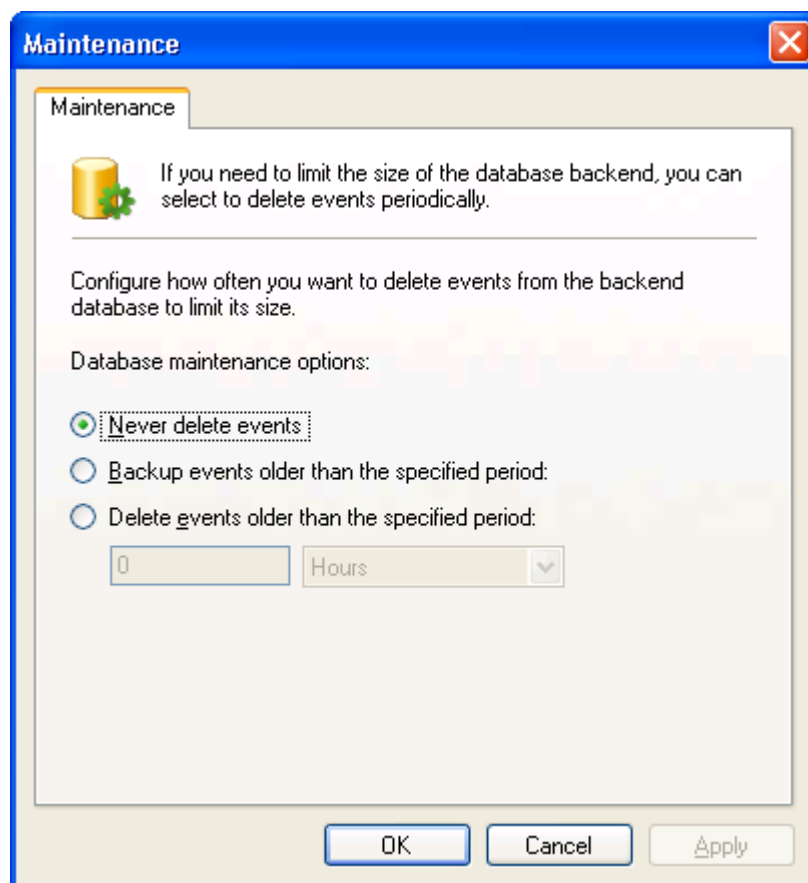
Modifica del terminale database

Per modificare le impostazioni del terminale database, seguire questa procedura:

1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Options (Opzioni)**.
3. Nel pannello di sinistra, selezionare **Database Backend (Terminale database)**.
4. Nel pannello di destra, fare clic su **Change database backend (Modifica terminale database)**.
5. Apportare le modifiche desiderate e fare clic su **OK** per completare le impostazioni.

Manutenzione database

La manutenzione periodica del database è essenziale per impedire la crescita eccessiva del database stesso. GFI EndPointSecurity consente di configurare quei parametri che provvederanno automaticamente alla manutenzione del terminale database.



Schermata 91 – Finestra di dialogo della manutenzione del database

I parametri di manutenzione del database comprendono:

- la frequenza, espressa in ore o giorni, con cui effettuare il salvataggio in backup
- la frequenza, espressa in ore o giorni, con cui gli eventi verranno eliminati dal terminale database.

La frequenza di eliminazione e quella di salvataggio in backup degli eventi vengono specificate in una casella di immissione e nell'elenco a discesa presenti nella finestra di dialogo.

NOTA 1: gli eventi sono eliminati automaticamente dal terminale database ogni volta che viene eseguita un'operazione di backup.

NOTA 2: i record eliminati NON SONO ripristinabili.

Per configurare la manutenzione del database, seguire questa procedura:

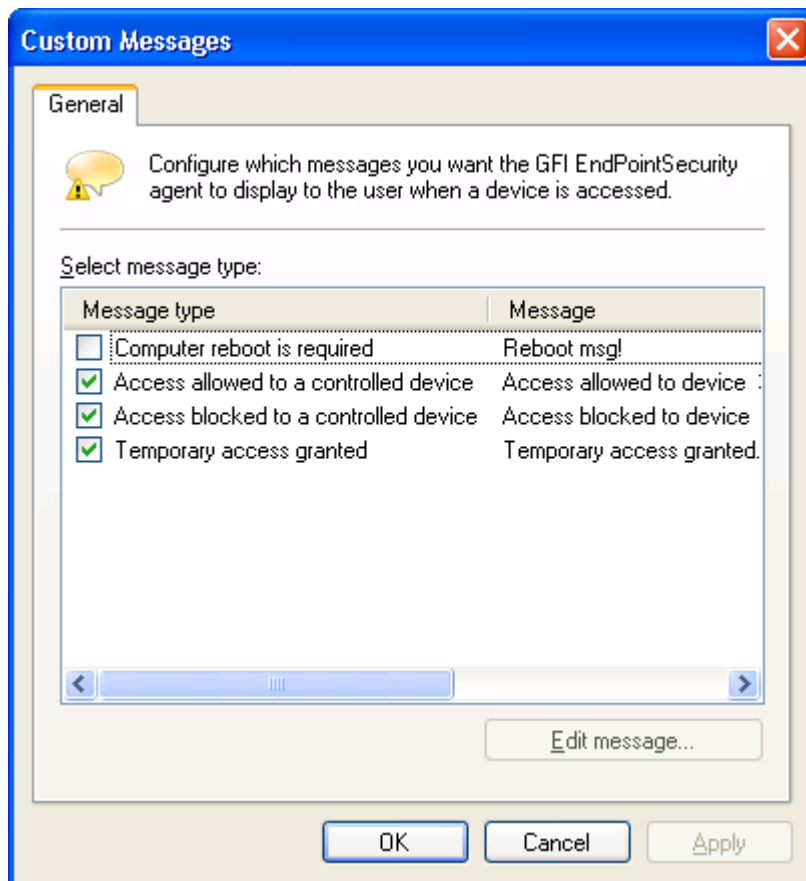
1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Options (Opzioni)**.
3. Nel pannello di sinistra, selezionare **Database Backend (Terminale database)**.
4. Nel pannello di destra, fare clic su **Database maintenance (Manutenzione database)**.
5. Configurare la manutenzione desiderata e fare clic su **OK** per completare le impostazioni.

Personalizzazione messaggi utenti

Adoperare la sezione **Custom Messages (Messaggi personalizzati)** che gli utenti visualizzeranno nel momento in cui viene bloccato l'utilizzo di un dispositivo.

Per personalizzare i messaggi, seguire questa procedura:

1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Options (Opzioni)**.
3. Nel pannello di sinistra, selezionare **Custom Messages (Messaggi personalizzati)**.



Schermata 92 – Personalizzazione dei messaggi utenti

4. Nel pannello di destra, fare clic su **Customize user messages (Personalizza messaggi utenti)**.
5. Selezionare il messaggio da personalizzare e fare clic su **Edit message (Modifica messaggio)** per personalizzare il testo.
6. Fare clic su **OK** per completare le impostazioni.

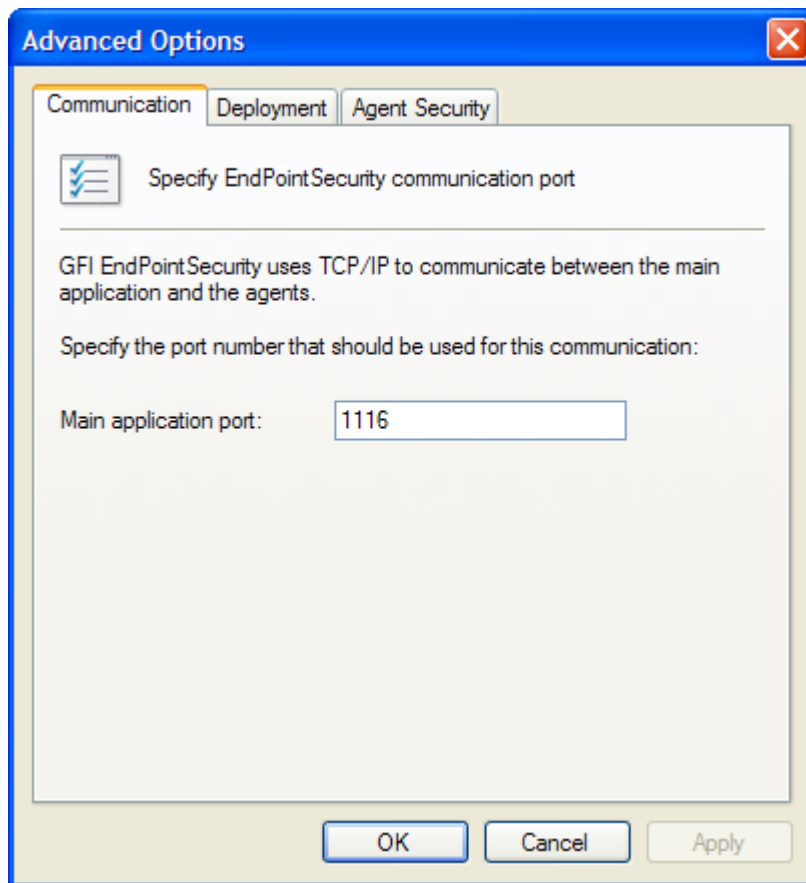
Opzioni avanzate

Adoperare la sezione **Advanced Options (Opzioni avanzate)** per configurare le seguenti opzioni:

- la porta di comunicazione TCP adoperata da GFI EndPointSecurity per le comunicazioni tra l'applicazione principale e gli agenti
- le conversazioni (*thread*) e i timeout di distribuzione
- la password di controllo degli agenti, con cui sarà possibile controllare solo gli agenti che utilizzano detta password.

Per personalizzare le opzioni avanzate, seguire questa procedura:

1. Selezionare la scheda **Configuration (Configurazione)**.
2. Fare clic su **Options (Opzioni)**.
3. Nel pannello di sinistra, selezionare **Advanced Options (Opzioni avanzate)**.



Schermata 93 – Impostazione Opzioni avanzate

4. Nel pannello di destra, fare clic su **Modify advanced options (Modifica opzioni avanzate)**.
5. Fare clic sulla scheda dell'opzione da personalizzare e apportare le modifiche desiderate.
6. Fare clic su **OK** per completare le impostazioni.

Opzioni varie

Introduzione

In questa sezione sono disponibili informazioni:

- sull'aggiornamento della licenza di GFI EndPointSecurity
- sull'aggiornamento a build più nuove di GFI EndPointSecurity.

Inserimento del codice di licenza dopo l'installazione

Dopo aver installato GFI EndPointSecurity è possibile inserire il codice di licenza senza dover installare o configurare di nuovo il prodotto. A questo scopo, seguire questa procedura:

1. Fare clic sulla scheda **General (Generale)**.
2. Nel pannello di sinistra, selezionare **Licensing (Gestione licenza)**.



Schermata 94 – Modifica del codice di licenza

3. Nel pannello di destra, fare clic sull'opzione **Edit license key... (Modificare codice di licenza)**

Ricerca di build più recenti

GFI rilascia periodicamente aggiornamenti del prodotto che possono essere scaricati in modalità automatica dal sito web di GFI. Per controllare l'eventuale disponibilità di una build più nuova di GFI EndPointSecurity da scaricare, seguire questa procedura:

1. Fare clic sulla scheda **General (Generale)**.
2. Nel pannello di sinistra, selezionare **Version Information (Informazioni sulla versione)**.
3. Nel pannello di destra, fare clic sull'opzione **Check for newer builds... (Ricerca build più nuove)**.

Risoluzione dei problemi

Introduzione

Questo capitolo descrive le modalità per risolvere eventuali problemi riscontrati nell'utilizzo del prodotto. Le fonti principali di informazioni disponibili per gli utenti sono le seguenti:

- il presente manuale: la maggior parte dei problemi può essere risolta leggendo il manuale
- la knowledgebase di GFI, accessibile dal sito web di GFI
- il sito di assistenza tecnica di GFI
- rivolgendosi al reparto assistenza tecnica di GFI all'indirizzo email supporto@gfi-italia.com
- rivolgendosi al reparto assistenza tecnica di GFI attraverso il servizio LiveSupport, alla pagina <http://support.gfi.com/livesupport.asp>
- contattando telefonicamente il nostro reparto assistenza tecnica.

Knowledgebase

GFI cura la gestione di una knowledgebase contenente le risposte ai problemi più comuni. In caso di problemi, consultare innanzi tutto la knowledgebase. La knowledge base riporta sempre le domande di assistenza e le patch più aggiornate.

La knowledgebase (in lingua inglese) è disponibile alla pagina <http://kbase.gfi.com/>.

Richiesta di assistenza tecnica via email

Se il problema non può essere risolto neanche dopo aver consultato la knowledgebase e il presente manuale, è possibile contattare il reparto assistenza tecnica di GFI. Il metodo migliore per contattarlo è tramite email, perché in questo modo è possibile inserire quelle informazioni di cruciale importanza, ad esempio un allegato, in grado di consentire una risoluzione più rapida del problema.

Il **Troubleshooter (Esperto nella risoluzione dei problemi)**, compreso nel gruppo di programmi, genera automaticamente una serie di file necessari a GFI per fornire l'assistenza tecnica desiderata. I file contengono le impostazioni di configurazione, i file di debugging e così via. Per generare tali file, avviare il programma guidato del *troubleshooter* e seguire le istruzioni dell'applicazione.

Oltre alla raccolta di tutte le possibili informazioni necessarie, saranno anche poste delle domande. Si è pregati di rispondere a tali domande in modo accurato: in assenza di informazioni adeguate, non sarà possibile diagnosticare in modo corretto il problema.

Fare quindi clic sulla cartella *troubleshooter\support*, localizzata nella directory del programma principale, comprimere i file in formato ZIP e inviare il file ZIP appena generato all'indirizzo email: supporto@gfi-italia.com.

Accertarsi innanzitutto di avere registrato i dati relativi alla propria azienda sul nostro sito web: <http://customers.gfi.com>.

La richiesta sarà evasa entro 24 ore, in base al fuso orario.

Richiesta di assistenza tecnica telefonica

Per richiedere assistenza tecnica, è possibile contattare GFI anche telefonicamente. A tale proposito, consultare il nostro sito web per i recapiti telefonici e orari di ufficio corretti, in base alla propria sede.

Sito web di assistenza tecnica:

<http://support.gfi.com>.

Accertarsi innanzitutto di avere registrato i dati relativi alla propria azienda sul nostro sito web: <http://customers.gfi.com>.

Forum su internet

È disponibile un servizio di supporto tecnico tra utenti tramite il forum su internet. Si può accedere al forum dal sito:

<http://forums.gfi.com/>.

Notifiche relative alle build

Si consiglia fortemente di iscriversi al nostro elenco di notifiche relative alle build. In questo modo, si verrà immediatamente informati in merito alle nuove build del prodotto. Per sottoscrivere tale servizio, andare sul sito:

<http://support.gfi.com>.

Indice analitico

A

accesso al dispositivo 11
Accesso temporaneo 12, 76
Active Directory 5, 7, 31, 58,
59, 62, 65, 80
agente 8, 28
archiviazione eventi 20
Autorizzazioni 59
Autorizzazioni di accesso alla
categoria di dispositivi
59
Autorizzazioni di utilizzo della
porta di connessione 62
Autorizzazioni per un
determinato dispositivo
65
Avvio rapido 19, 20, 21, 22,
88, 91, 96
Avvisi 44
avvisi di rete 88, 93
avvisi SMS 87, 93
avvisi via email 87, 92
Avviso 21

B

Blacklist 70
Browser dei log 42
Builds 101

C

Codice di licenza 13, 101
consolle di gestione 23
Consolle di gestione 8
consolle di gestione di GFI
EndPointSecurity 23
**Consolle di gestione di GFI
EndPointSecurity 8**
criterio di protezione 8, 28,
55
criterio di protezione
predefinito 25

D

Database di dispositivi 41
Distribuzione 9

E

EndPointSecurityAdministrat
or 87, 88

F

Finestra di dialogo Avvio
rapido 19
Firewire 6

G

GFI EndPointSecurity vers. 3
17
GFI LANguard Portable
Storage Control 17
Gruppi 94

I

impostazioni di avviso
predefinite 92
impostazioni di
configurazione 102

L

licenza 13
licenze 15, 23

M

Manutenzione database 97
Messaggi utenti 98
Monitoraggio 9
monitoraggio dello stato 45
MSI 7, 31

O

orario di lavoro 87, 90
orario lavorativo 89

P

Pianificazione della
distribuzione 30
privilegi 5, 59, 62, 65
programma guidato 102

Q

Query 43
query builder degli eventi 43

R

Rapporti 44
Requisiti di sistema 14
Risoluzione dei problemi 102

S

scansione dispositivi 36

Secure Digital 6
SQL Server 96
Statistiche 33
Stato degli agenti 32
Stato della distribuzione 31
Supporto database 20

T

terminale database 98
Terminale database 21, 47,
96, 97

U

USB 6
Utenti 94
Utenti autorizzati 58

V

Valutazione 17
Visualizzazione di stato
Generale 46

W

Whitelist 73