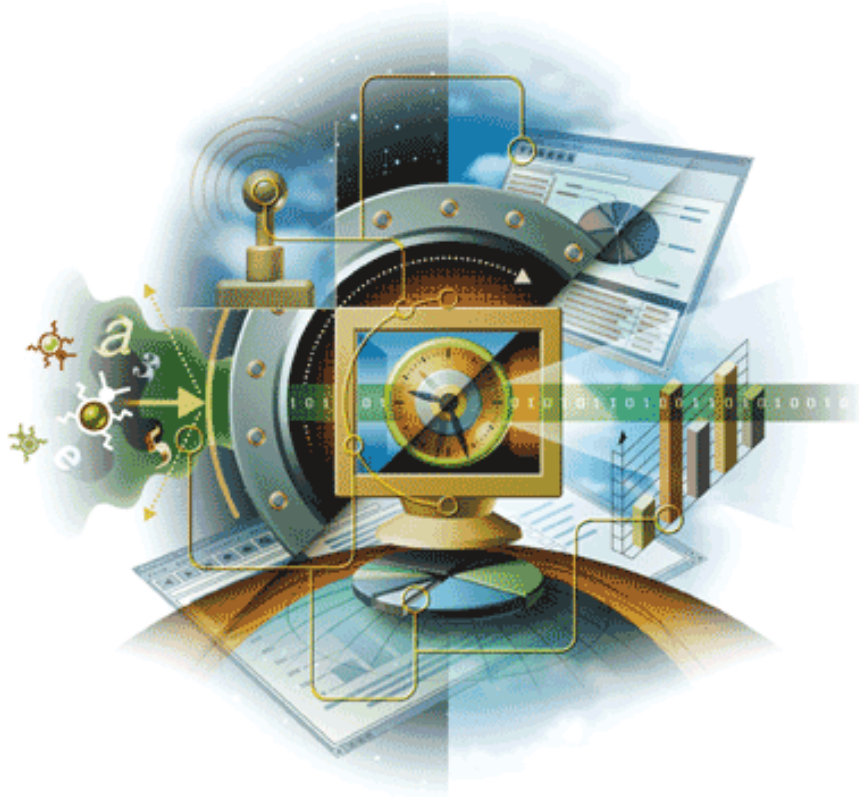


Virex®

versione 7.6

per l'uso con ePolicy Orchestrator



McAfee®
System Protection

Soluzioni leader di prevenzione delle intrusioni

COPYRIGHT

Copyright © 2004-2005 McAfee, Inc. Tutti i diritti riservati.

È vietato riprodurre, trasmettere, trascrivere, archiviare in un sistema di recupero dei dati o tradurre in altra lingua completamente o in parte questo documento con qualsiasi mezzo senza previa autorizzazione scritta di McAfee, Inc. o di un suo fornitore o di una sua consociata. Per ottenere l'autorizzazione, mettersi in contatto con l'ufficio legale di McAfee presso: 5000 Headquarters Drive, Plano, Texas 75024, USA, oppure chiamare il numero +1-972-963-8000.

ATTRIBUZIONI DEI MARCHI

Active Firewall, Active Security, ActiveSecurity (e in Katakana), ActiveShield, AntiVirus Anyware e design, Clean-Up, Design (E stilizzata), Design (N stilizzata), Entercept, Enterprise SecureCast, Enterprise SecureCast (e in Katakana), ePolicy Orchestrator, First Aid, ForceField, GMT, GroupShield, GroupShield (e in Katakana), Guard Dog, HomeGuard, Hunter, IntruShield, Intrusion Prevention Through Innovation, M e Design, McAfee, McAfee (e in Katakana), McAfee e Design, McAfee.com, McAfee VirusScan, NA Network Associates, Net Tools, Net Tools (e in Katakana), NetCrypto, NetOctopus, NetScan, NetShield, Network Associates, Network Associates Colliseum, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PrimeSupport, RingFence, Router PM, SecureCast, SecureSelect, SpamKiller, Stalker, ThreatScan, TIS, TMEG, Total Virus Defense, Trusted Mail, Uninstall, Virex, Virus Forum, Viruscan, Virusscan, Virusscan (e in Katakana), Webscan, Webshield, Webshield (e in Katakana), Webstalker, WebWall, What's The State Of Your IDS?, Who's Watching Your Network, Your E-Business Defender, Your Network. Our Business. sono marchi o marchi registrati di McAfee, Inc. e/o sue consociate negli USA e/o in altri paesi. Il rosso utilizzato con riferimento alla protezione è una caratteristica distintiva dei prodotti con marchio McAfee®. Tutti i marchi registrati e non registrati citati nel presente documento sono di proprietà esclusiva dei rispettivi titolari.

INFORMAZIONI SULLA LICENZA

Contratto di licenza

AVVISO AGLI UTENTI: LEGGERE ATTENTAMENTE IL TESTO DEL CONTRATTO RELATIVO ALLA LICENZA ACQUISTATO, CHE STABILISCE LE CONDIZIONI GENERALI DI FORNITURA PER L'UTILIZZO DEL SOFTWARE CONCESSO IN LICENZA. NEL CASO NON SI SAPPIA CON ESATTEZZA CHE TIPO DI LICENZA È STATA ACQUISTATO, CONSULTARE I DOCUMENTI DI VENDITA E ALTRE AUTORIZZAZIONI CONNESSE O LA DOCUMENTAZIONE RELATIVA ALL'ORDINE DI ACQUISTO CHE ACCOMPAGNA IL PACCHETTO O CHE È STATA RICEVUTA SEPARATAMENTE IN RELAZIONE ALL'ACQUISTO MEDESIMO (SOTTO FORMA DI OPUSCOLO, FILE CONTENUTO NEL CD ILLUSTRATIVO DEL PRODOTTO O FILE DISPONIBILE SUL SITO WEB DAL QUALE È STATO SCARICATO IL SOFTWARE). SE NON SI ACCETTANO ALCUNI O TUTTI I TERMINI DEL CONTRATTO, ASTENERSI DALL'INSTALLARE IL SOFTWARE. SE PREVISTO DAL CONTRATTO, L'UTENTE POTRÀ RESTITUIRE IL PRODOTTO A MCAFEE O AL PUNTO VENDITA DA CUI È STATO ACQUISTATO ED ESSERE INTERAMENTE RIMBORSATO.

Attribuzioni

Questo prodotto include o potrebbe includere:

- Software sviluppato da OpenSSL Project per l'utilizzo nell'OpenSSL Toolkit (<http://www.openssl.org/>).
- Software crittografico scritto da Eric A. Young e software scritto da Tim J. Hudson.
- Software concesso in licenza o in sublicenza all'utente in base a licenze GNU GPL (General Public License) o a licenze Free Software analoghe che autorizzano l'utente, tra l'altro, a copiare, modificare e ridistribuire alcuni programmi o parte di essi e ad accedere al codice sorgente. La convenzione GPL prevede che, per qualsiasi software coperto da licenza GPL e distribuito ad altri utenti in formato binario eseguibile, debba essere reso disponibile anche il relativo codice sorgente. Il codice sorgente di tali programmi software coperti da GPL è disponibile su questo CD. Qualora, in base a licenze Free Software, i diritti di utilizzo, copia o modifica di un programma che McAfee è tenuta a concedere siano più ampi dei diritti concessi in base al presente contratto, i suddetti diritti avranno la precedenza sui diritti e le restrizioni qui previste.
- Software originariamente scritto da Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer.
- Software originariamente scritto da Robert Nordier, Copyright © 1996-7 Robert Nordier.
- Software scritto da Douglas W. Sauder.
- Software sviluppato da Apache Software Foundation (<http://www.apache.org/>). Per ottenere una copia del contratto di licenza di questo software, visitare la pagina www.apache.org/licenses/LICENSE-2.0.txt.
- International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation e altri.
- Software sviluppato da CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc.
- Tecnologia FEAD® Optimizer®, Copyright Netopsystems AG, Berlino, Germania.
- Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc. e/o Outside In® HTML Export, © 2001 Stellent Chicago, Inc.
- Software protetto da copyright di Thai Open Source Software Center Ltd. e Clark Cooper, © 1998, 1999, 2000.
- Software protetto da copyright dei manutentori di software Expat.
- Software protetto da copyright di The Regents of the University of California, © 1989.
- Software protetto da copyright di Gunnar Ritter.
- Software protetto da copyright di Sun Microsystems®, Inc. © 2003.
- Software protetto da copyright di Gisle Aas. © 1995-2003.
- Software protetto da copyright di Michael A. Chase, © 1999-2000.
- Software protetto da copyright di Neil Winton, © 1995-1996.
- Software protetto da copyright di RSA Data Security, Inc., © 1990-1992.
- Software protetto da copyright di Sean M. Burke, © 1999, 2000.
- Software protetto da copyright di Martijn Koster, © 1995.
- Software protetto da copyright di Brad Appleton, © 1996-1999.
- Software protetto da copyright di Michael G. Schwern, © 2001.
- Software protetto da copyright di Graham Barr, © 1998.
- Software protetto da copyright di Larry Wall e Clark Cooper, © 1998-2000.
- Software protetto da copyright di Frodo Looijgaard, © 1997.
- Software protetto da copyright di Python Software Foundation, Copyright © 2001, 2002, 2003. Per ottenere una copia del contratto di licenza di questo software, visitare il sito www.python.org.
- Software protetto da copyright di Beman Dawes, © 1994-1999, 2002.
- Software scritto da Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame.
- Software protetto da copyright di Simone Bordet e Marco Cravero, © 2002.
- Software protetto da copyright di Stephen Purcell, © 2001.
- Software sviluppato da Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>).
- Software protetto da copyright di International Business Machines Corporation e altri, © 1995-2003.
- Software sviluppato da University of California, Berkeley e suoi contributori.
- Software sviluppato da Ralf S. Engelschall <rse@engelschall.com> per l'uso nel progetto mod_ssl project (<http://www.modssl.org/>).
- Software protetto da copyright di Kevlin Henney, © 2000-2002.
- Software protetto da copyright di Peter Dimov e Multi Media Ltd. © 2001, 2002.
- Software protetto da copyright di David Abrahams, © 2001, 2002. Per la relativa documentazione vedere <http://www.boost.org/libs/bind/bind.html>.
- Software protetto da copyright di Steve Cleary, Beman Dawes, Howard Hinnant e John Maddock, © 2000.
- Software protetto da copyright di Boost.org, © 1999-2002.
- Software protetto da copyright di Nicolai M. Josuttis, © 1999.
- Software protetto da copyright di Jeremy Siek, © 1999-2001.
- Software protetto da copyright di Daryle Walker, © 2001.
- Software protetto da copyright di Chuck Allison e Jeremy Siek, © 2001, 2002.
- Software protetto da copyright di Samuel Kremp, © 2001. Per aggiornamenti, documentazione e riepilogo delle revisioni, vedere <http://www.boost.org>.
- Software protetto da copyright di Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002.
- Software protetto da copyright di Cadenza New Zealand Ltd., © 2000.
- Software protetto da copyright di Jens Maurer, © 2000, 2001.
- Software protetto da copyright di Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000.
- Software protetto da copyright di Ronald Garcia, © 2002.
- Software protetto da copyright di David Abrahams, Jeremy Siek, e Daryle Walker, © 1999-2001.
- Software protetto da copyright di Stephen Cleary (shammah@voyager.net), © 2000.
- Software protetto da copyright di Housemarque Oy <<http://www.housemarque.com>>, © 2001.
- Software protetto da copyright di Paul Moore, © 1999.
- Software protetto da copyright di Dr. John Maddock, © 1998-2002.
- Software protetto da copyright di Greg Colvin e Beman Dawes, © 1998, 1999.
- Software protetto da copyright di Peter Dimov, © 2001, 2002.
- Software protetto da copyright di Jeremy Siek e John R. Bandela, © 2001.
- Software protetto da copyright di Joerg Walter e Mathias Koch, © 2000-2002.

Sommario

1	Introduzione	5
	Contenuto della guida	5
	Prerequisiti per l'uso di ePolicy Orchestrator per la gestione di Virex	6
	Introduzione alla console di ePolicy Orchestrator	6
	Destinatari della guida	7
	Convenzioni	7
	Risorse	8
	Come ottenere informazioni sui prodotti	8
	Collegamenti all'interno del prodotto	9
	Servizi relativi al prodotto	10
	Informazioni per contattare McAfee	11
2	Installazione	13
	Introduzione	13
	Requisiti di sistema	13
	Configurazione della console ePolicy Orchestrator per la gestione di Virex 7.6	13
	Archiviazione dei file NAP per la gestione di Virex 7.6	14
	Installazione dell'agente per i sistemi Macintosh	18
	Directory di installazione dell'agente	18
	Installazione dell'agente	18
	Installazione di Virex 7.6	24
	Disinstallazione	24
	Rimozione del file NAP di Virex dal server ePolicy Orchestrator	24
	Rimozione dell'Agente ePolicy Orchestrator dal server ePolicy Orchestrator	25
	Rimozione dell'Agente ePolicy Orchestrator per Mac OS X	25
3	Impostazione dei criteri di ePolicy Orchestrator per Virex 7.6	27
	Impostazione dei criteri in ePolicy Orchestrator	27
	Generale	29
	eUpdate	30
	Scanner attivo	32
	Scanner in background	33
	Scanner dei volumi montati	34
	Scanner su richiesta	35
	Pianificazione delle scansioni e di eUpdate	36
	Informazioni sulle attività pianificate	36
	eUpdate	40
	Visualizzazione delle proprietà del server ePolicy Orchestrator	42
4	Controllo remoto dell'agente	43
	Visualizzazione delle proprietà raccolte dall'agente	43
	Imposizione dei criteri per l'Agente ePolicy Orchestrator	44
	Opzioni dell'agente	44
	Eventi	45
	Visualizzazione degli eventi dei server	48
	Registrazione	49

5	Rapporti	51
	Rapporti.	51
	Configurazione dei rapporti.	52
	Glossario	53
	Indice	57

Contenuto della guida

Questa guida spiega come configurare Virex 7.6 tramite il programma di gestione McAfee ePolicy Orchestrator versione 3.0.2 e successive. Per utilizzare la guida in maniera efficiente è necessario conoscere ePolicy Orchestrator. Per ulteriori informazioni, vedere la *Guida del prodotto ePolicy Orchestrator*. Il programma ePolicy Orchestrator offre un unico centro di controllo per i prodotti antivirus McAfee, da cui gestire i criteri antivirus e visualizzare i rapporti di eventi antivirus e l'attività virale nell'ambiente aziendale. Con ePolicy Orchestrator è possibile configurare Virex nei computer di destinazione in rete; non è necessario configurarli singolarmente dalla finestra di dialogo **Preferenze** di Virex.

In questa guida vengono fornite le seguenti informazioni:

- Aggiunta della configurazione dell'Agente ePolicy Orchestrator al server ePolicy Orchestrator.
- Impostazione dei criteri antivirus sui sistemi di destinazione per configurare le seguenti funzioni di Virex:
 - Criteri generali per il controllo delle funzioni di Virex.
 - Criteri per il server eUpdate.
 - Criteri per lo Scanner attivo.
 - Criteri per lo Scanner in background.
 - Criteri per lo Scanner dei volumi montati.
 - Criteri per lo Scanner su richiesta.
- Configurazione dell'Agente ePolicy Orchestrator per Mac OS X.
 - Intervallo di comunicazione dell'agente.
 - Intervallo di imposizione dei criteri.
 - Inoltro dell'evento.
 - Registrazione..



Questa guida non fornisce informazioni dettagliate sull'installazione o l'uso del programma ePolicy Orchestrator. Tali informazioni sono disponibili nella *Guida del prodotto ePolicy Orchestrator*.

Prerequisiti per l'uso di ePolicy Orchestrator per la gestione di Virex

Perché il programma ePolicy Orchestrator possa configurare Virex occorre prima:

- Archiviare il file NAP di Virex 7.6 nell'archivio del programma ePolicy Orchestrator.
- Archiviare il file Non Windows Agent¹ in ePolicy Orchestrator.
- Installare Virex 7.6 nel sistema Macintosh.
- Installare l'Agente ePolicy Orchestrator nel sistema Macintosh.

Introduzione alla console di ePolicy Orchestrator

La console di gestione Microsoft (MMC) è l'interfaccia per il prodotto ePolicy Orchestrator e per le sue funzioni. Tramite questa si registrano e si configurano i prodotti antivirus Virex che saranno gestiti da ePolicy Orchestrator.

Quando si accede per la prima volta al server, la console viene visualizzata con la directory principale della console evidenziata nel riquadro sinistro. L'aspetto della console varia in base agli elementi selezionati nella struttura della console o nel riquadro dei dettagli. La console usa le funzioni standard della MMC.

Sotto i menu nella parte superiore della finestra, la console è divisa in due parti o riquadri.

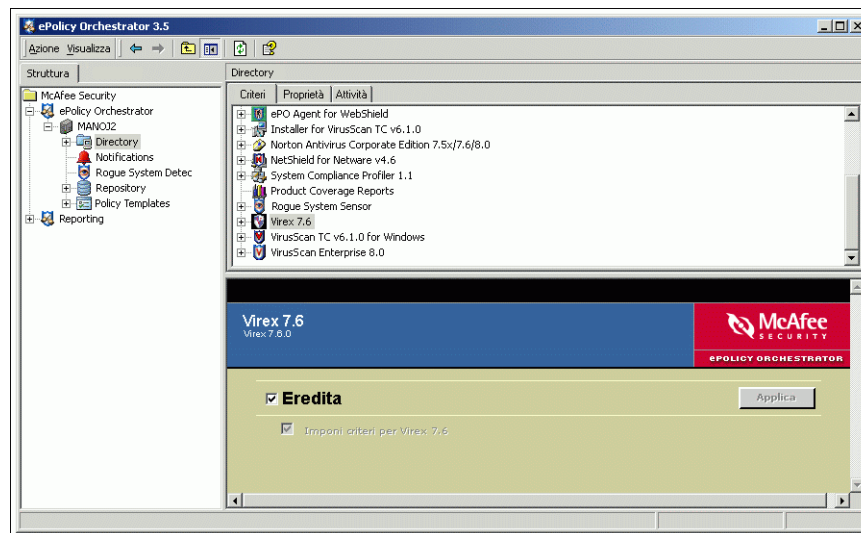


Figura 1-1 Console di ePolicy Orchestrator

- A sinistra è visualizzata la **struttura della console**. Mostra i server, le workstation e le periferiche che è possibile amministrare.
- A destra è visualizzato il **riquadro dei dettagli**. In base all'elemento selezionato nella struttura della console, il riquadro dei dettagli può essere diviso in **riquadro superiore dei dettagli** e **riquadro inferiore dei dettagli**.






¹ Non Windows Agent (NWA) è anche noto come Agente ePolicy Orchestrator per Mac OS X.

Destinatari della guida

Questa guida è destinata agli amministratori di rete e di sistema responsabili dei programmi antivirus per l'azienda.

Convenzioni

In questa guida vengono utilizzate le seguenti convenzioni:

Serif, grassetto	Tutti i termini di interfaccia utente, tra cui i nomi di opzioni, menu, pulsanti e finestre di dialogo. Esempio: Inserire il Nome utente e la Password dell'account desiderato.
Courier	Il percorso di una cartella o di un programma; un indirizzo Web (URL); testo che l'utente deve digitare esattamente come indicato, ad esempio un comando al prompt del sistema. Esempi: Il percorso predefinito del programma è: C:\Programmi\McAfee\EPO\3.5.0 Visitare il sito Web di McAfee all'indirizzo: http://www.mcafee.com Eseguire questo comando sul computer client: C:\SETUP.EXE
Corsivo	Per enfatizzare o introdurre un nuovo termine; per nomi di documentazione di prodotti e argomenti (intestazioni) all'interno della documentazione. Esempio: Per ulteriori informazioni, fare riferimento alla <i>Guida del prodotto Virex 7.6</i> .
<TERMINE>	Le parentesi ad angolo racchiudono termini generici. Esempio: Nella struttura della console in ePolicy Orchestrator , fare clic con il pulsante destro del mouse su <SERVER>.
	Nota: Informazioni supplementari; ad esempio, un metodo alternativo per eseguire lo stesso comando.
	Suggerimento: Suggerimenti per le procedure migliori e consigli di McAfee per la prevenzione delle minacce, le prestazioni e l'efficienza.
	Attenzione: Un'avvertenza importante per proteggere un sistema, un'azienda, un'installazione software o dei dati.
	Avviso: Avviso importante per proteggere l'utente da lesioni fisiche durante l'interazione con un prodotto hardware.
	Nuovo: Funzione o opzione nuova o riprogettata di questa versione del prodotto.

Risorse

I prodotti McAfee® si contraddistinguono per gli anni di esperienza e l'impegno dedicati a realizzare la soddisfazione dei clienti. Il team McAfee PrimeSupport® di cui fanno parte tecnici di supporto dotati di grande esperienza e professionalità, offre soluzioni su misura, che mettono a disposizione un'assistenza tecnica precisa e tempestiva per portare al successo progetti mission critical, tutti con livelli di servizio che soddisfano le esigenze di ogni organizzazione. McAfee Research, leader mondiale nella ricerca sui sistemi informativi e la sicurezza, continua a offrire innovazioni nello sviluppo e perfezionamento di tutte le nostre tecnologie.

Per ulteriori risorse, fare riferimento alle seguenti sezioni:

- Come ottenere informazioni sui prodotti.
- Collegamenti all'interno del prodotto.
- Servizi relativi al prodotto.
- Informazioni per contattare McAfee.

Come ottenere informazioni sui prodotti

Salvo diversa indicazione, la documentazione dei prodotti viene fornita in file Adobe Acrobat .PDF disponibili sul CD del prodotto o scaricabili dal sito di download di McAfee.

Guida del prodotto: presentazione e funzioni del prodotto, istruzioni dettagliate per la configurazione del software, informazioni sulla distribuzione, l'esecuzione delle attività ricorrenti e le procedure operative.

- *Virex 7.6 Guida del prodotto*

Guida in linea Virex 7.6: informazioni avanzate e dettagliate alle quali si accede dall'interno dell'applicazione software.

Guida alla configurazione: per l'uso con *ePolicy Orchestrator*®. Procedure per la distribuzione e la gestione di Virex tramite il programma di gestione ePolicy Orchestrator.

Note di rilascio^: *Leggimi*. Informazioni sul prodotto, sui problemi già risolti, su tutti i problemi insoliti conosciuti e sulle ultime aggiunte o modifiche apportate al prodotto o alla documentazione.

Contatti^: informazioni per contattare i servizi e le risorse McAfee: supporto tecnico, assistenza clienti, quartier generale della sicurezza (AVERT, Anti-Virus & Vulnerability Emergency Response Team), programma beta e formazione. In questo file sono inoltre inclusi numeri telefonici, indirizzi stradali, indirizzi Web e numeri di fax delle sedi della società negli USA e nel resto del mondo.

Licenza: opuscolo del contratto di licenza McAfee che include tutti i tipi di licenza che è possibile acquistare per il prodotto. Il contratto di licenza definisce le condizioni generali per l'uso del prodotto su licenza.

* Un manuale stampato che accompagna il CD del prodotto. Nota: alcuni manuali tradotti potrebbero essere disponibili solo in formato di file .PDF.

^ File di testo inclusi nel software e nel CD del prodotto.

Collegamenti all'interno del prodotto

Il prodotto fornisce collegamenti che consentono di accedere ad alcune informazioni utili:

- Guida in linea.
- Libreria di informazioni sui virus.
- Assistenza tecnica per ePolicy Orchestrator.
- Strumento delle risorse di escalation minima.
- AVERT Web Immune.
- Pagina iniziale di McAfee Security.

Guida in linea

Utilizzare questo collegamento per accedere agli argomenti della Guida in linea del prodotto.



Se il sistema di Guida in linea integrato del prodotto (al quale si accede dal software facendo clic sul menu **Aiuto**) viene visualizzato in modo errato nel sistema, è possibile che la versione di Microsoft® Internet Explorer in uso non stia utilizzando correttamente i controlli ActiveX. Tali controlli sono necessari per visualizzare il file della guida. Assicurarsi che sia installata la versione più recente di Internet Explorer.

Libreria di informazioni sui virus

Utilizzare il collegamento **Informazioni sui virus** per accedere alla Libreria di informazioni sui virus di Anti-Virus & Vulnerability Emergency Response Team (AVERT) di McAfee. Questo sito Web contiene informazioni dettagliate sulla provenienza dei virus, le modalità di infezione del sistema e le procedure di rimozione.

Oltre ai virus veri e propri, la Libreria di informazioni sui virus contiene informazioni utili sui virus fasulli (hoax), come gli avvisi di virus che si ricevono via e-mail. *Virtual Card For You* e *SULFNBK* sono due dei più noti avvisi di virus fasulli, ma ne esistono molti altri. Quando si ricevono avvisi di virus apparentemente legittimi, consultare sempre la nostra pagina con l'elenco dei virus fasulli prima di inoltrare il messaggio ai propri conoscenti.

Per accedere alla Libreria di informazioni sui virus:

- 1 Aprire ePolicy Orchestrator.
- 2 Selezionare il collegamento **Virus Information Library** (Libreria di informazioni sui virus) nella **Start Page** (Pagina di avvio).

Assistenza tecnica per ePolicy Orchestrator

Utilizzare il collegamento **Technical Support** (Assistenza tecnica) per accedere al portale dei servizi McAfee PrimeSupport KnowledgeCenter. Navigare nel sito per visualizzare le domande frequenti (FAQ), la documentazione ed eseguire una ricerca guidata.

- 1 Aprire ePolicy Orchestrator.
- 2 Fare clic sul collegamento **Technical Support for ePolicy Orchestrator** (Assistenza tecnica per ePolicy Orchestrator) nella **Start Page** (Pagina di avvio).

Strumento delle risorse di escalation minima

Utilizzare il collegamento dello strumento delle risorse di escalation minima per accedere al portale dei servizi McAfee PrimeSupport KnowledgeCenter. Accedere al sito dell'assistenza per registrare le escalation.

- 1 Aprire ePolicy Orchestrator.
- 2 Fare clic sul collegamento **Minimum Escalation Resource Tool** (Strumento delle risorse di escalation minima) nella **Start Page** (Pagina di avvio).

AVERT Web Immune

Utilizzare il collegamento AVERT Web Immune per accedere al portale di Avert Web Immune.

- 1 Aprire ePolicy Orchestrator.
- 2 Selezionare il collegamento **AVERT Web Immune** nella **Start Page** (Pagina di avvio).

Pagina iniziale di McAfee Security

Utilizzare il collegamento McAfee Security Home Page per accedere alla pagina iniziale del sito McAfee Security.

- 1 Aprire ePolicy Orchestrator.
- 2 Fare clic sul collegamento **McAfee Security Home Page** (Pagina iniziale di McAfee Security) nella **Start Page** (Pagina di avvio).

Servizi relativi al prodotto

Per permettere di trarre il massimo vantaggio dai prodotti McAfee, sono disponibili i seguenti servizi:

- Programma beta.
- HotFix e patch.
- Assistenza per i prodotti non più validi.

Programma beta

Il programma beta di McAfee consente di provare i prodotti prima che la versione completa venga distribuita al pubblico; è quindi possibile apprendere e provare le nuove funzioni dei prodotti esistenti, nonché sperimentare i prodotti totalmente nuovi. Questo programma può essere utile per provare e implementare in anticipo le funzioni nuove e aggiornate, in un ambiente protetto. Gli utenti hanno la possibilità di suggerire nuove funzioni del prodotto, nonché di interagire direttamente con il personale tecnico di McAfee.

Per ulteriori informazioni, visitare:

<http://www.mcafeesecurity.com/us/downloads/beta/mcafeebetahome.htm>

HotFix e patch

Gli HotFix e le patch sono rilasciati con i file di aggiornamento, i driver, gli eseguibili e così via, nell'intervallo che intercorre tra le principali release di un prodotto. Per accedere agli HotFix e alle patch più recenti, visitare:

<http://www.mcafeesecurity.com/us/downloads/updates/hotfixes.asp>

Assistenza per i prodotti non più validi

Il software antivirus utilizzato deve essere sempre aggiornato per conservare l'efficacia contro i virus e altri software potenzialmente dannosi. È importante aggiornare regolarmente i file di definizione dei virus (DAT). Per consentire al software di garantire una protezione dalle costanti minacce, spesso vengono apportate modifiche architetturali al modo in cui i file DAT interagiscono con il motore di scansione dei virus. È quindi importante aggiornare il motore quando viene rilasciata una nuova versione. Un motore meno recente non riuscirà a rilevare molte delle nuove minacce emergenti.

Al momento del rilascio di un nuovo motore, viene annunciata la data limite oltre la quale cesserà il supporto offerto per il motore esistente. Per informazioni sulla nostra politica relativa ai prodotti non più validi e per un elenco completo dei prodotti e dei motori supportati, visitare la pagina:

http://www.mcafeesecurity.com/us/products/mcafee/end_of_life.htm

Informazioni per contattare McAfee**Assistenza tecnica**

Pagina iniziale	http://www.mcafeesecurity.com/us/support/technical_support
Ricerca nella KnowledgeBase	https://knowledgemap.nai.com/phpclient/homepage.aspx
Portale servizi PrimeSupport *	https://mysupport.nai.com

Programma beta di McAfee

<http://www.mcafeesecurity.com/us/downloads/beta/mcafeebetahome.htm>

Quartier generale della sicurezza: AVERT: Anti-virus & Vulnerability Emergency Response Team

Pagina iniziale	http://www.mcafeesecurity.com/us/security/home.asp
Libreria di informazioni sui virus	http://vil.nai.com
AVERT WebImmune, *	https://www.webimmune.net/default.asp
Invio di un esempio	
Servizio di notifica AVERT DAT	http://vil.mcafeesecurity.com/vil/join-DAT-list.asp

Sito di download

Pagina iniziale	http://www.mcafeesecurity.com/us/downloads/
Aggiornamenti file DAT e motore	http://www.mcafeesecurity.com/us/downloads/updates/default.asp
	ftp://ftp.mcafeesecurity.com/pub/antivirus/datfiles/4.x
Aggiornamenti dei prodotti *	https://secure.nai.com/us/forms/downloads/upgrades/login.asp

Formazione

Formazione in sede	http://www.mcafeesecurity.com/us/services/security/home.htm
McAfee University	http://www.mcafeesecurity.com/us/services/education/mcafee/university.htm

Assistenza clienti

E-mail https://secure.nai.com/us/forms/support/request_form.asp

Web <http://www.mcafeesecurity.com/us/index.asp>

<http://www.mcafeesecurity.com/us/support/default.asp>

Numeri verdi per Stati Uniti,
Canada e America Latina:

+1-888-VIRUS NO oppure **+1-888-847-8766**

Dal lunedì al venerdì, dalle 8:00 alle 20:00, fuso orario centrale (USA e Canada)

Per ulteriori informazioni su come contattare McAfee, compresi i numeri verdi delle altre aree geografiche, consultare il file Contatti fornito con questa versione del prodotto.

* Sono necessarie le credenziali di accesso.

2 Installazione

Introduzione

L'agente è il componente distribuito di ePolicy Orchestrator che viene installato su ogni computer Macintosh della rete. L'agente raccoglie e invia le informazioni tra il server ePolicy Orchestrator e gli archivi e gestisce le installazioni di Virex 7.6 in rete. Le modalità di configurazione dell'agente e le sue impostazioni dei criteri determinano il livello di facilità di comunicazione e aggiornamento nell'ambiente.

Requisiti di sistema

L'agente può essere installato in sistemi operativi Macintosh quali:

- MAC OS 10.2.6
- MAC OS 10.2.8
- MAC OS 10.3.x

e una qualsiasi delle seguenti piattaforme Macintosh:

- G3
- G4
- G5

Configurazione della console ePolicy Orchestrator per la gestione di Virex 7.6

Il computer sul quale è stata eseguita un'installazione completa dell'Agente ePolicy Orchestrator consente di rendere facilmente disponibili i rapporti. Per impostare i rapporti per i propri computer è necessario attenersi alla seguente procedura:

- Accertarsi di aver configurato l'indirizzo IP e la porta del server ePolicy Orchestrator dall'interfaccia utente del Programma di configurazione di ePolicy Orchestrator del computer client.

Archiviazione dei file NAP per la gestione di Virex 7.6

File Network Associate Package (file NAP). Questa estensione di file viene usata per designare i file di programma del software McAfee che vengono installati nell'archivio del software per la gestione di ePolicy Orchestrator. Il server ePolicy Orchestrator viene installato con una serie di pagine dei criteri per i principali prodotti supportati, disponibili al momento del rilascio della versione di ePolicy Orchestrator in uso. Per gestire Virex 7.6 è necessario innanzitutto aggiungere i file NAP appropriati del prodotto all'archivio del software.

Dove si trovano i file *.NAP per Virex 7.6 che desidero aggiungere all'archivio?

McAfee rilascia i file NAP per tutti i prodotti antivirus e di protezione supportati da ePolicy Orchestrator. Il file NAP per un determinato prodotto è disponibile insieme agli altri file di installazione di quel prodotto, che si trovano sul CD del prodotto o nel file ZIP del prodotto se i file di installazione sono stati scaricati dal sito Web di McAfee. I file NAP per Virex 7.6 sono disponibili nella sottocartella Server Components (Componenti server) di **ePolicy Orchestrator** nel CD del prodotto o nel file ZIP del prodotto. Il file NAP ha sempre un'estensione .NAP e viene denominato con un codice di nome di prodotto e numero di versione, ad esempio NWA-MAC300.NAP.

Le pagine dei criteri non vengono aggiunte all'archivio master ma vengono archiviate nel server ePolicy Orchestrator. Pertanto, i file NAP non vengono replicati negli archivi distribuiti o aggiornati sui computer Macintosh.

Aggiunta le file .NAP per Non Windows Agent (NWA) per Macintosh

Per archiviare un file NAP di Non-Windows Agent per Macintosh nel server ePolicy Orchestrator:

- 1 Individuare il file NAP, sul CD del prodotto o nel file ZIP di installazione scaricato dal sito Web di McAfee, e salvarlo in una cartella temporanea accessibile dal server ePolicy Orchestrator.
- 2 Effettuare l'accesso al server ePolicy Orchestrator con diritti di amministratore.
- 3 Nella struttura della console in ePolicy Orchestrator, fare clic con il pulsante destro del mouse su **Repository** (Archivio) e selezionare **Configure Repository** (Configura archivio). Viene visualizzata la procedura guidata **Configure Software Repository** (Configurazione dell'archivio del software).

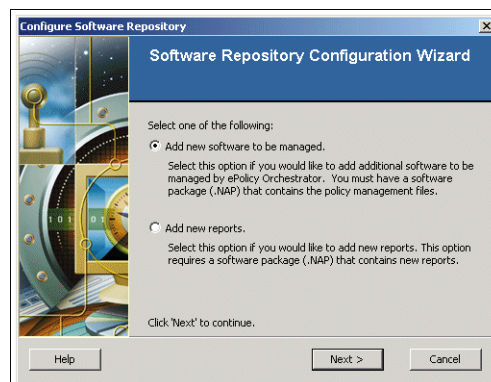


Figura 2-1 Procedura guidata Configure Software Repository (Configurazione dell'archivio del software)



Facendo doppio clic su **Repository** (Archivio) nella struttura della console in ePolicy Orchestrator e selezionando il collegamento **Check in NAP** (Archivia NAP) nel riquadro destro dei dettagli, viene visualizzata la procedura guidata **Configure Software Repository** (Configurazione dell'archivio del software).

- 4 Nella procedura guidata **Configure Software Repository** (Configurazione dell'archivio del software), selezionare **Add new software to be managed** (Aggiungi nuovo software da gestire) e fare clic su **Next** (Avanti).

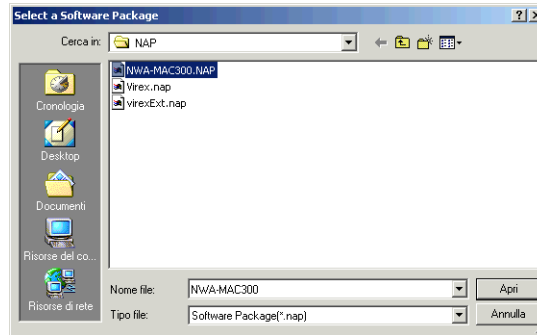


Figura 2-2 Finestra di dialogo Select a Software Package (Seleziona un pacchetto software)

- 5 Nella finestra di dialogo **Select a Software Package** (Seleziona un pacchetto software), sfogliare e selezionare il file **NWA-MAC300.NAP** salvato in una cartella temporanea nella **Fase 1**.
- 6 Fare clic su **Open** (Apri) per consentire a ePolicy Orchestrator di caricare il file NAP.

Aggiunta di un file .NAP di Virex

Per aggiungere un file .NAP di Virex al server ePolicy Orchestrator:

- 1 Individuare il file NAP, sul CD del prodotto o nel file ZIP di installazione scaricato dal sito Web di McAfee, e salvarlo in una cartella temporanea accessibile dal server ePolicy Orchestrator.
- 2 Effettuare l'accesso al server ePolicy Orchestrator con diritti di amministratore.
- 3 Nella struttura della console in ePolicy Orchestrator, fare clic con il pulsante destro del mouse su **Repository** (Archivio) e selezionare **Configure Repository** (Configura archivio). Viene visualizzata la procedura guidata **Configure Software Repository** (Configurazione dell'archivio del software).

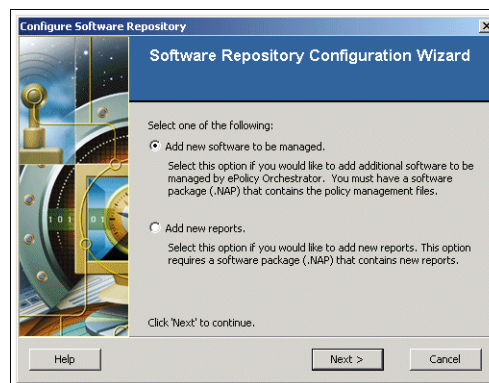


Figura 2-3 Procedura guidata Configure Software Repository (Configurazione dell'archivio del software)



Facendo doppio clic su **Repository** (Archivio) nella struttura della console in ePolicy Orchestrator e selezionando il collegamento **Check in NAP** (Archivia NAP) nel riquadro destro dei dettagli, viene visualizzata la procedura guidata **Configure Software Repository** (Configurazione dell'archivio del software).

- 4 Nella procedura guidata **Configure Software Repository** (Configurazione dell'archivio del software), selezionare **Add new software to be managed** (Aggiungi nuovo software da gestire) e fare clic su **Next** (Avanti).

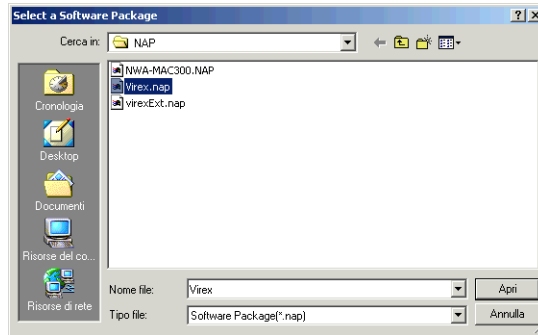


Figura 2-4 Finestra di dialogo Select a Software Package (Seleziona un pacchetto software)

- 5 Nella finestra di dialogo **Select a Software Package** (Seleziona un pacchetto software), sfogliare e selezionare il file **Virex.NAP** salvato in una cartella temporanea nella **Fase 1**.
- 6 Fare clic su **Open** (Apri) per consentire a ePolicy Orchestrator di caricare il file NAP.

Aggiunta di un file .NAP di rapporto

Per aggiungere un file NAP di rapporto al server ePolicy Orchestrator:

- 1 Individuare il file NAP, sul CD del prodotto o nel file ZIP di installazione scaricato dal sito Web di McAfee, e salvarlo in una cartella temporanea accessibile dal server ePolicy Orchestrator.
- 2 Effettuare l'accesso al server ePolicy Orchestrator con diritti di amministratore.

- 3 Nella struttura della console in ePolicy Orchestrator, fare clic con il pulsante destro del mouse su **Repository** (Archivio) e selezionare **Configure Repository** (Configura archivio). Viene visualizzata la procedura guidata **Configure Software Repository** (Configurazione dell'archivio del software).

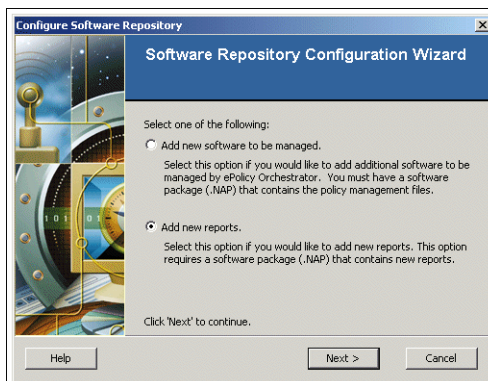


Figura 2-5 Procedura guidata Configure Software Repository (Configurazione dell'archivio del software)



Facendo doppio clic su **Repository** (Archivio) nella struttura della console in ePolicy Orchestrator e selezionando il collegamento **Check in NAP** (Archivia NAP) nel riquadro destro dei dettagli, viene visualizzata la procedura guidata **Configure Software Repository** (Configurazione dell'archivio del software).

- 4 Nella procedura guidata **Configure Software Repository** (Configurazione dell'archivio del software), selezionare **Add new reports** (Aggiungi nuovi rapporti) e fare clic su **Next** (Avanti).

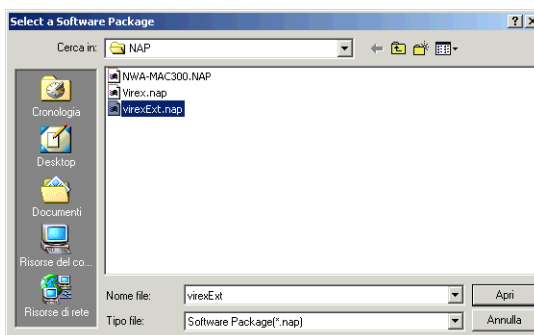


Figura 2-6 Finestra di dialogo Select a Software Package (Seleziona un pacchetto software)

- 5 Nella finestra di dialogo **Select a Software Package** (Seleziona un pacchetto software), sfogliare e selezionare il file **VirexExt.NAP** salvato in una cartella temporanea nella **Fase 1** e fare clic su **Open** (Apri) per consentire a ePolicy Orchestrator di caricare il file NAP di rapporto nell'archivio.

Una volta che ePolicy Orchestrator ha completato il caricamento dei file NAP, l'agente viene visualizzato nell'elenco dei criteri nel riquadro superiore dei dettagli.

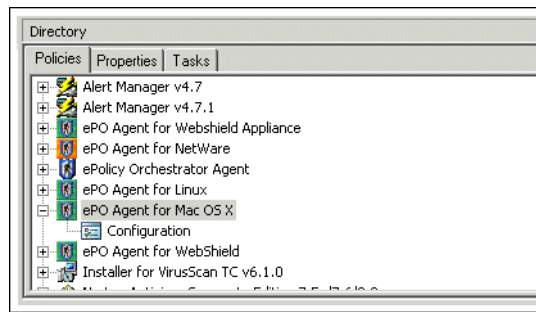


Figura 2-7 Scheda dei criteri

Installazione dell'agente per i sistemi Macintosh

Directory di installazione dell'agente

L'agente viene installato in /Library/NETAepoagt e utilizza anche /Library/NETASSOC per i dati correlati alla configurazione.



Non è possibile modificare la directory di installazione dell'Agente ePolicy Orchestrator per Macintosh OS X.

Installazione dell'agente

L'Agente ePolicy Orchestrator per Macintosh può essere installato tramite un'installazione standard (interfaccia grafica) o dalla linea di comando (in modalità invisibile).

Installazione standard

- 1 Individuare il file **nwa.dmg**, sul CD del prodotto o nel file ZIP di installazione scaricato dal sito Web di McAfee e salvarlo in una cartella temporanea.



nwa.dmg si trova nella cartella **ePO Agent** del file **ePO Components.ZIP** nel CD del prodotto.

- 2 Fare doppio clic su **nwa.dmg**. Vengono estratti i seguenti file:
 - NWA.pkg
 - cmdinstall

- 3 Fare doppio clic su **NWA.pkg**. Viene visualizzata la finestra **Benvenuto a: Agente ePO per Mac OS X**.

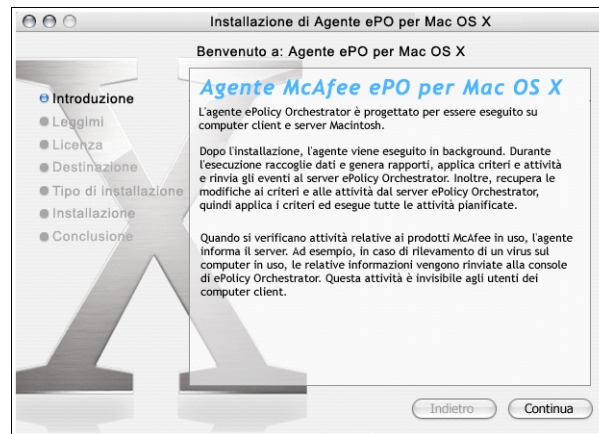


Figura 2-8 Finestra di installazione dell'Agente ePO - Introduzione

- 4 Fare clic su **Continua**. Viene visualizzata la finestra **Leggimi**. Il file Leggimi descrive le funzioni dell'agente, elenca i comportamenti o altri problemi noti relativi alla versione dell'agente.

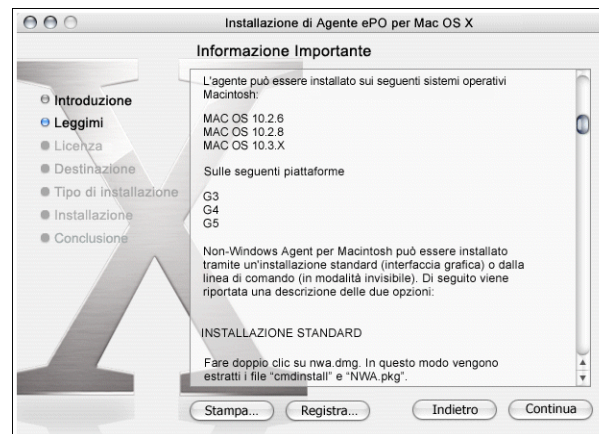


Figura 2-9 Finestra di installazione dell'Agente ePO - Leggimi

- 5 Fare clic su **Continua**. Viene visualizzata la finestra **Licenza d'uso**.

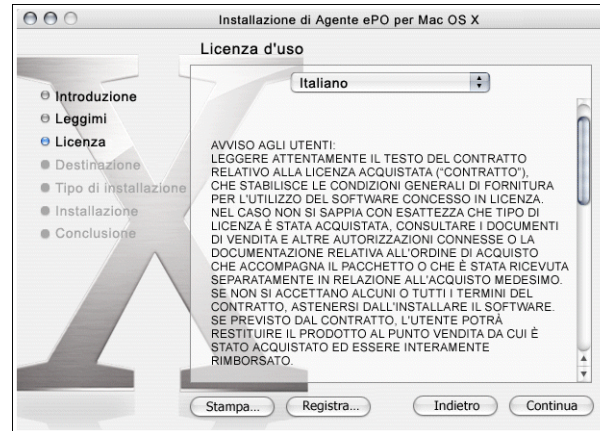


Figura 2-10 Finestra di installazione dell'Agente ePO - Licenza



Leggere e accettare la licenza d'uso. Se non si accettano i termini della licenza d'uso non è possibile continuare l'installazione.

- 6 Fare clic su **Continua**. Viene visualizzata la finestra **Seleziona Destinazione**.

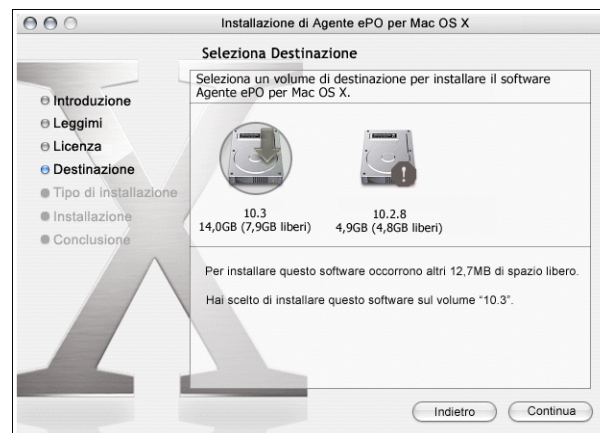


Figura 2-11 Finestra di installazione dell'Agente ePO - Seleziona Destinazione

Selezionare il volume nel quale si desidera installare l'Agente ePolicy Orchestrator e fare clic su **Continua**. Viene visualizzata la finestra **Installazione Standard**.

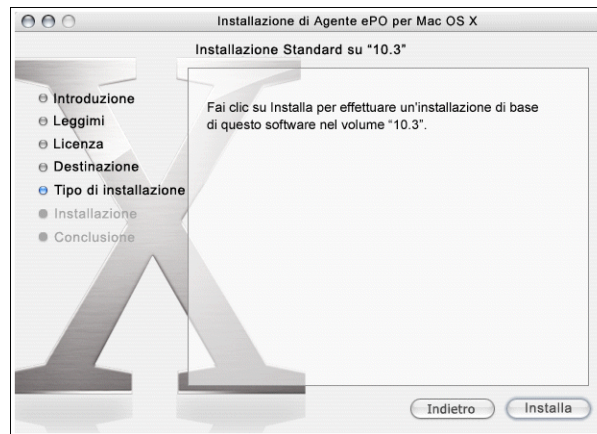


Figura 2-12 Procedura guidata di installazione dell'Agente ePO - Nuova installazione



La finestra **Installazione Standard** con il pulsante **Installa** viene visualizzato quando:

- Si installa l'agente per la prima volta.
- Si reinstalla l'agente dopo aver disinstallato la versione precedente dell'Agente ePolicy Orchestrator.

Se si esegue l'aggiornamento all'Agente ePolicy Orchestrator viene visualizzata la seguente finestra.



Figura 2-13 Finestra di installazione dell'Agente ePO - Installazione di aggiornamento

- 7 Fare clic su **Installa/Aggiorna** per continuare. Il programma di installazione richiede l'autenticazione prima di continuare. Immettere la password e fare clic su **OK**. Viene visualizzata la finestra **Installazione software**.

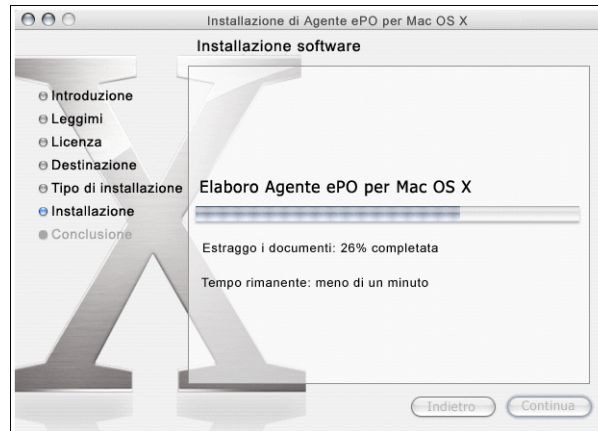


Figura 2-14 Finestra di installazione dell'Agente ePO - Installazione software

Durante questo processo il programma di installazione richiede di autenticare il **Programma di configurazione dell'Agente ePO**. Immettere la password e fare clic su **OK**. Viene visualizzata la finestra di dialogo **Programma di configurazione dell'Agente ePO**.

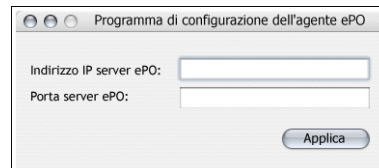


Figura 2-15 Finestra di dialogo Programma di configurazione dell'Agente ePO

- 8 Immettere l'**Indirizzo IP server ePO**: e il numero di **Porta server ePO**. Fare clic su **Applica**. Viene visualizzata la finestra **Installazione software**.



Figura 2-16 Finestra di installazione dell'Agente ePO - Installazione software

- 9 Fare clic su **Riavvia** per completare il processo di installazione.

Installazione in background (linea di comando)

- 1 Individuare il file **nwa.dmg**, sul CD del prodotto o nel file ZIP di installazione scaricato dal sito Web di McAfee e salvarlo in una cartella temporanea.



nwa.dmg si trova nella cartella **ePO Agent** del file **ePO Components.ZIP** nel CD del prodotto.

- 2 Fare doppio clic su **nwa.dmg**. Vengono estratti i seguenti file:

- NWA.pkg
- cmdinstall

- 3 Aprire la finestra **Terminale** e modificare la directory di lavoro su NAINWA.



Per eseguire questo comando sono necessari i diritti di amministratore.

- 4 Nella finestra **Terminale**, eseguire `sudo ./cmdinstall <Indirizzo IP server ePO>:<Porta server ePO>`

```

Terminal - bash - 85x41
Manoj-Ts-Computer:/Volumes/NAINWA manojt$ sudo ./cmdinstall 172.16.197.94:79
Password:
The working directory is /Volumes/NAINWA
Creating temporary folder /tmp/NAINWA.rESFqHq3
Dumping the server.inf file
172.16.197.94
79
installer[2428]: Installer Language: English
installer[2428]: Requirement: requires "certain InstallationCheck criteria" PASS for root=(none), domain=0
installer[2428]: Requirement: requires "certain file content criteria" PASS for root=(none), domain=0
installer[2428]: Requirement: requires "certain InstallationCheck criteria" PASS for root=/, domain=0
installer[2428]: == Starting check on volume /
installer[2428]: Requirement: requires "certain file content criteria" PASS for root=/, domain=0
installer[2428]: Requirement: requires "certain InstallationCheck criteria" PASS for root=/, domain=0
installer[2428]: == Starting check on volume /
installer[2428]: Requirement: requires "certain file content criteria" PASS for root=/, domain=0
installer: Package name is ePO Agent for Mac OS X
installer: Upgrading volume mounted at /.
installer: Preparing the Disk.....
  
```

Figura 2-17 Finestra Terminale - Avvio

- 5 Al termine dell'installazione in background, la finestra **Terminale** indica:

```

Terminal - bash - 85x24
#
installer: Processing ePO Agent for Mac OS X.....
#
installer: Finishing Installation
###installer[789]: Registered /Library/NETAepoagt/bin/ePO Agent Configurator.app.
###
installer:
##
installer: Optimizing System Performance.....
#installer[789]: Running task: /usr/bin/update_prebinding
installer[789]: 1978-02-15 10:56:34.539 update_prebinding[829] Start of update_prebinding
installer: Optimizing volume "10.3 ": 0% complete
installer: Optimizing volume "10.3 ": 5% complete
installer: Optimizing volume "10.3 ": 38% complete
installer: Optimizing volume "10.3 ": 100% complete
installer[789]: 1978-02-15 10:56:41.284 update_prebinding[829] Update_prebinding done
.
installer[789]: 1978-02-15 10:56:41.293 update_prebinding[829] 1 files successfully prebound, 0 files unsuccessfully prebound.
#installer[789]: Finished task: /usr/bin/update_prebinding
installer: The upgrade was successful.
Cleaning /tmp/NAINWA.NXT800VY
  
```

Figura 2-18 Finestra terminale - Installazione/Aggiornamento completato

- 6 In questo modo si completa l'installazione/l'aggiornamento dell'Agente ePolicy Orchestrator per Mac OS X.

Installazione di Virex 7.6



Per l'installazione del software Virex 7.6 nei sistemi Macintosh, vedere la *Guida del prodotto Virex 7.6*.

Disinstallazione

Rimozione del file NAP di Virex dal server ePolicy Orchestrator

È possibile disinstallare il file NAP di Virex dal server ePolicy Orchestrator.

Per rimuovere il file NAP di Virex:

- 1 Effettuare l'accesso al server database ePolicy Orchestrator.
- 2 Selezionare **Virex** in **Repository | Managed Products | MAC OS X |** (Archivio | Prodotti gestiti | MAC OS X) nella struttura della console.

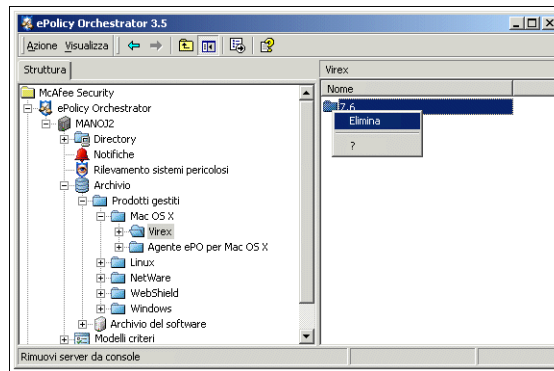


Figura 2-19 Fila NAP di Virex - Rimozione

- 3 Fare clic con il pulsante destro del mouse su **Virex** e selezionare **Remove** (Elimina) per disinstallare il file NAP di Virex dal server ePolicy Orchestrator.

Rimozione dell'Agente ePolicy Orchestrator dal server ePolicy Orchestrator



Non è possibile rimuovere l'**Agente ePolicy Orchestrator per MAC OS X** dal server ePolicy Orchestrator dopo averlo archiviato.

Rimozione dell'Agente ePolicy Orchestrator per Mac OS X

L'Agente ePolicy Orchestrator può essere disinstallato da un computer Macintosh tramite la linea di comando.

Dalla linea di comando

- 1 Effettuare l'accesso come Utente Root.



L'Utente Root nel sistema Macintosh è disattivato per impostazione predefinita; se disattivato, attivare l'Utente Root. Se si è effettuato l'accesso come utente, aprire la finestra **Terminale**, immettere il testo **"su"** e inserire la password di root per accedere come Utente Root.

- 2 Andare a /Library/NETAepoagt
- 3 Eseguire cmduninst

3

Impostazione dei criteri di ePolicy Orchestrator per Virex 7.6

In questo capitolo vengono illustrate le due procedure principali per l'imposizione dei criteri Virex da ePolicy Orchestrator:

- In ePolicy Orchestrator, vengono selezionati i nomi dei computer e dei criteri Virex ad essi applicabili. Ad esempio, se si desidera effettuare la scansione virus con i computer A e B, è possibile impostare molti criteri diversi applicabili a singoli computer a gruppi di computer.
- Si richiede a ePolicy Orchestrator di imporre questi criteri sui computer e l'agente comunica con il server per verificare la disponibilità di nuovi criteri. Il computer lo rispetta e ignora eventuali criteri precedentemente configurati nella finestra di dialogo **Preferenze** di Virex.

Impostazione dei criteri in ePolicy Orchestrator

La console di ePolicy Orchestrator consente di imporre i criteri a gruppi di computer o ad un singolo computer. Tali criteri prevalgono sulle configurazioni effettuate sui singoli computer. Per informazioni relative ai criteri e alle modalità di imposizione, consultare la *Guida del prodotto ePolicy Orchestrator*.

Prima di configurare un criterio, selezionare nella struttura della console il gruppo di computer per cui si desidera modificare i criteri Virex. Per farlo, è possibile utilizzare le pagine e le schede Virex disponibili nel riquadro dei dettagli della console di ePolicy Orchestrator. Queste pagine sono quasi identiche alle pagine e alle finestre di dialogo accessibili direttamente dall'interfaccia utente di Virex. Per informazioni complete sulle opzioni di configurazione in Virex 7.6, consultare la *Guida del prodotto Virex*.

Una volta modificato il criterio e salvate le modifiche per il computer o il gruppo di computer desiderati, si è pronti a distribuire le nuove impostazioni tramite l'Agente ePolicy Orchestrator. [Vedere Imposizione dei criteri a pagina 29.](#)

Per modificare i criteri per Virex 7.6 in ePolicy Orchestrator:

- 1 Effettuare l'accesso al server ePolicy Orchestrator.
- 2 Nella struttura della console in ePolicy Orchestrator | <SERVER> | Directory, selezionare il sito, il gruppo, il singolo computer oppure l'intera directory. Nel riquadro superiore dei dettagli vengono visualizzate le schede **Policies** (Criteri), **Properties** (Proprietà) e **Tasks** (Attività).

- 3** Selezionare la scheda **Policies** (Criteri) nel riquadro superiore dei dettagli, quindi espandere Virex. Sotto la voce Virex viene visualizzata un'unica voce.

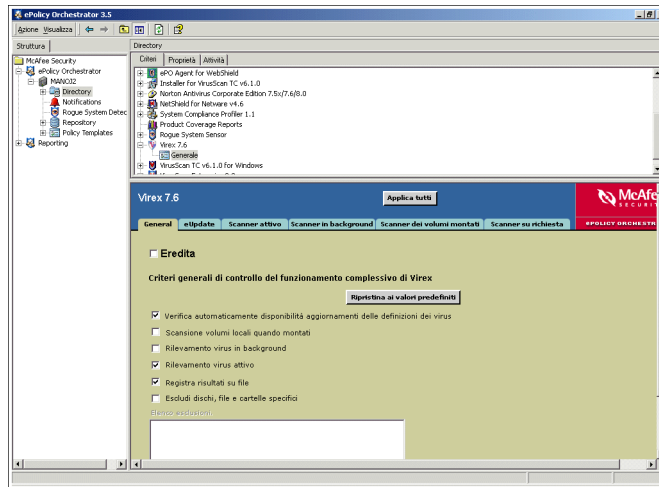


Figura 3-1 Console di ePolicy Orchestrator - Virex

Nel riquadro inferiore sono visualizzate le opzioni di configurazione disponibili nell'interfaccia di Virex.

- Generale
 - eUpdate
 - Scanner attivo
 - Scanner in background
 - Scanner dei volumi montati
 - Scanner su richiesta
- 4** Nel riquadro inferiore dei dettagli selezionare un'opzione dal riquadro sinistro, ad esempio **Generale**.
- 5** Nella pagina **Generale** deselezionare **Eredita**.
- 6** Configurare le opzioni desiderate.



Queste pagine sono identiche alle pagine di Virex. Per ulteriori informazioni, consultare la *Guida del prodotto Virex 7.6*.

- 7** Fare clic su **Applica** per salvare le impostazioni. È possibile continuare a configurare i criteri, quindi fare clic su **Applica tutti** per imporre tutti i criteri configurati.

Imposizione dei criteri

Una volta configurati i criteri, è necessario imporli sui computer su cui è installato Virex.

- 1 Nella struttura della console in Directory, selezionare il sito, il gruppo, il singolo computer oppure l'intera directory.
- 2 Nel riquadro superiore dei dettagli della scheda **Policies** (Criteri) selezionare **Virex**. La pagina **Virex** viene visualizzata nel riquadro inferiore dei dettagli.
- 3 Deselezionare **Inherit** (Eredita).
- 4 Selezionare **Imponi criteri per Virex 7.6**.
- 5 Fare clic su **Applica** per salvare le impostazioni.

Il software ePolicy Orchestrator renderà disponibili i criteri configurati all'Agente ePolicy Orchestrator presente sui computer Virex.

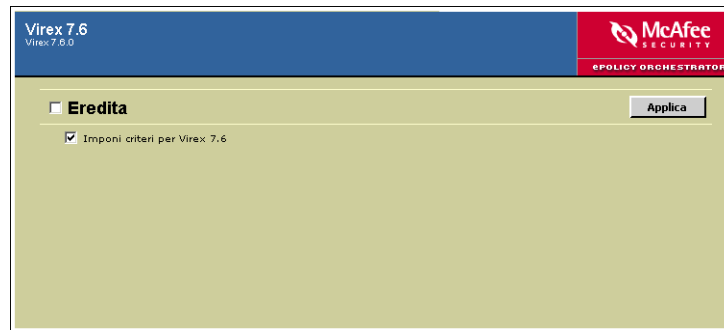


Figura 3-2 Imponi criteri per Virex 7.6

Generale

La scheda **Generale** consente di imporre criteri generali che controllano il funzionamento di Virex 7.6, quali ad esempio la verifica automatica della disponibilità degli aggiornamenti delle definizioni dei virus, la scansione dei volumi locali quando montati, la registrazione dei risultati della scansione, il rilevamento dei virus in background e la creazione di liste di esclusione per dischi, file e cartelle specifici.

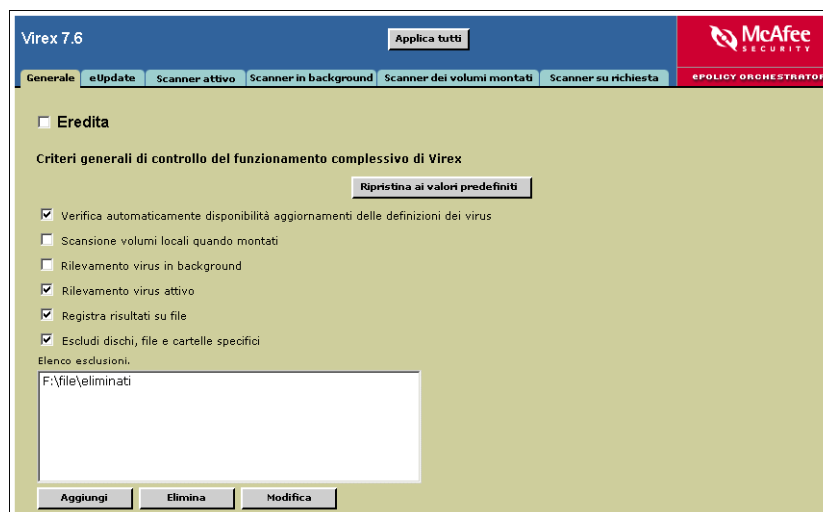


Figura 3-3 Scheda Generale

È possibile imporre i criteri generali seguenti::

Verifica automaticamente disponibilità aggiornamenti delle definizioni dei virus	Attiva/disattiva gli eUpdate automatici.
Scansione volumi locali quando montati	Attiva/disattiva lo Scanner dei volumi montati.
Rilevamento virus in background	Attiva/disattiva lo Scanner in background.
Rilevamento virus attivo	Attiva/disattiva lo Scanner attivo.
Registra risultati su file	Attiva/disattiva la registrazione dei risultati in un file.
Escludi dischi, file e cartelle specifici	<p>Configura le esclusioni di scansione. Le esclusioni vengono memorizzate sotto forma di elenco in un file di testo chiamato VShieldExclude.txt. Se questo file non è selezionato, le esclusioni non sono impostate.</p> <p>Per aggiungere un'esclusione:</p> <ul style="list-style-type: none"> Fare clic su Aggiungi; verrà visualizzato Aggiungi elemento da esaminare -- Finestra di dialogo pagina Web. Digitare il percorso completo di ogni file, directory e volume che si desidera escludere e fare clic su OK. Le esclusioni verranno elencate nell'elenco di esclusione. <p>Per rimuovere un'esclusione:</p> <ul style="list-style-type: none"> Selezionare l'esclusione nell'elenco di esclusione e fare clic su Rimuovi. <p>Per modificare un'esclusione:</p> <ul style="list-style-type: none"> Selezionare l'esclusione nell'elenco di esclusione e fare clic su Modifica per modificarla.

eUpdate

La scheda **eUpdate** consente di personalizzare le impostazioni di aggiornamento dei file DAT e del motore di scansione antivirus. eUpdate mantiene il software antivirus costantemente aggiornato con nuove informazioni sui virus e le possibilità di scansione. È possibile aggiornare i file DAT e del motore di scansione tramite FTP o HTTP.

Figura 3-4 Scheda eUpdate

Personalizzazione delle impostazioni di eUpdate

È possibile imporre le seguenti impostazioni di eUpdate per Virex:

FTP

FTP (File Transfer Protocol) è un protocollo che consente di inviare e ricevere i file su Internet. È necessario specificare i dettagli del server da cui si desidera trasferire i file sul computer per aggiornare i file DAT e del motore di scansione.

URL del server	Specificare l'URL del server utilizzato per il download degli aggiornamenti dei file DAT e del motore di scansione.
Porta	Specificare il numero di porta che si desidera utilizzare per FTP.
Nome utente	Digitare il nome utente.
Password	Digitare la password.
Account	Digitare l'account FTP.
Directory	Specificare il percorso in cui si trovano i file DAT e del motore di ricerca.

HTTP

Il protocollo HTTP (Hypertext Transfer Protocol) è un insieme di regole per il trasferimento di file (testo, immagini, audio, video e altri file multimediali) sul World Wide Web. È necessario specificare l'URL del server da cui si desidera trasferire i file sul computer per aggiornare i file DAT e del motore di scansione.

URL del server	Specificare l'URL del server utilizzato per il download degli aggiornamenti dei file DAT e del motore di scansione.
Nome utente	Digitare il nome utente.
Password	Digitare la password.

Scanner attivo

La funzione Scanner attivo protegge costantemente il disco rigido da virus diffusi tramite connessioni di rete e Internet. Poiché lo Scanner attivo è costantemente in funzione sul computer, il sistema non resta esposto al rischio di infezioni.

Lo Scanner attivo esegue la scansione dei file durante la loro scrittura sul disco rigido (tutte le partizioni) e su tutte le unità rimovibili. Si attiva all'avvio del computer e resta in esecuzione fino all'arresto del computer. Lo scanner viene eseguito per impostazione predefinita. L'utente può configurare gli elementi che lo scanner deve cercare e le modalità di risposta al rilevamento di file infetti.

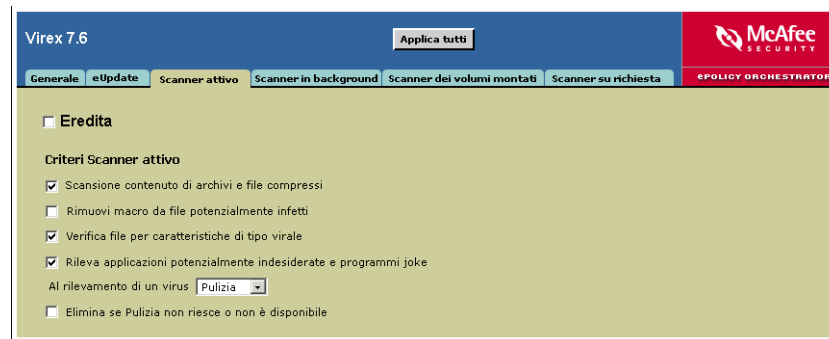


Figura 3-5 Scheda Scanner attivo

È possibile imporre i criteri di Scanner attivo seguenti:

Scansione contenuto di archivi e file compressi	Imposta lo scanner selezionato per la scansione di archivi e altri file compressi. Opzione attiva per impostazione predefinita per lo Scanner in background e lo Scanner su richiesta.
Rimuovi macro da file potenzialmente infetti	Se viene rilevato un file infetto, tutte le macro del file verranno rimosse quale parte dell'azione di pulizia.
Verifica file per caratteristiche di tipo virale	Attiva/disattiva la funzione euristica che esegue la scansione di file che presentano caratteristiche di tipo virale o worm e che potrebbero contenere infezioni sconosciute. Opzione attiva per impostazione predefinita per lo Scanner in background.
Rileva applicazioni potenzialmente indesiderate e programmi joke	Attiva/disattiva lo scanner per cercare programmi indesiderati o programmi joke.
Al rilevamento di un virus:	Seleziona l'azione primaria dello scanner.
<ul style="list-style-type: none"> ■ Pulizia ■ Elimina ■ Avvisa 	
Elimina se Pulizia non riesce o non è disponibile	Seleziona l'azione secondaria per lo scanner prescelto. Questa opzione è disponibile solo quando l'azione primaria è Pulizia.

Scanner in background

Lo Scanner in background è una funzione che esegue continuamente la scansione di tutti i file sul sistema. Lo scanner protegge il computer esaminandolo costantemente alla ricerca di eventuali file infetti. Questa scansione è un'operazione che fa ricorso a un numero ridotto di risorse, pertanto non vi sono cali di prestazioni del sistema. L'utente può configurare gli elementi che lo scanner deve cercare e le modalità di risposta al rilevamento di file infetti.

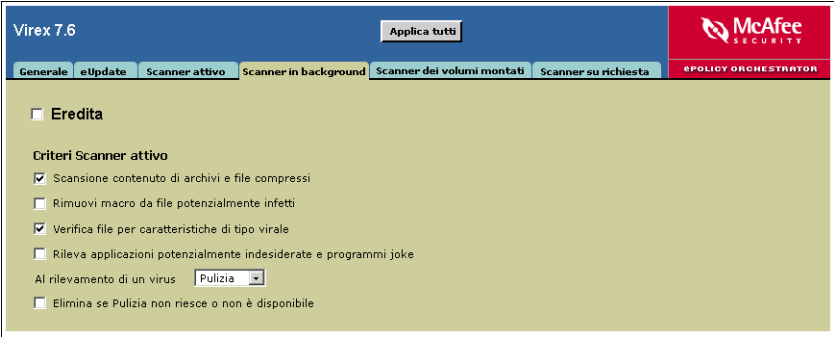


Figura 3-6 Scheda Scanner in background

È possibile imporre i criteri di Scanner in background seguenti:

Scansione contenuto di archivi e file compressi	Imposta lo scanner selezionato per la scansione di archivi e altri file compressi. Opzione attiva per impostazione predefinita per lo Scanner in background e lo Scanner su richiesta.
Rimuovi macro da file potenzialmente infetti	Se viene rilevato un file infetto, tutte le macro del file verranno rimosse quale parte dell'azione di pulizia.
Verifica file per caratteristiche di tipo virale	Attiva/disattiva la funzione euristica che esegue la scansione di file che presentano caratteristiche di tipo virale o worm e che potrebbero contenere infezioni sconosciute. Opzione attiva per impostazione predefinita per lo Scanner in background.
Rileva applicazioni potenzialmente indesiderate e programmi joke	Attiva/disattiva lo scanner per cercare programmi indesiderati o programmi joke.
Al rilevamento di un virus: <ul style="list-style-type: none">■ Pulizia■ Elimina■ Avvisa	Seleziona l'azione primaria dello scanner.
Elimina se Pulizia non riesce o non è disponibile	Seleziona l'azione secondaria per lo scanner prescelto. Questa opzione è disponibile solo quando l'azione primaria è Pulizia.

Scanner dei volumi montati

Lo Scanner dei volumi montati avvia la scansione di un volume come un CD o una fotocamera quando tale volume viene montato localmente. Grazie a questo scanner è possibile eseguire la scansione di un volume di grandi dimensioni o di una periferica alla ricerca di eventuali infezioni prima di interfacciarli con il proprio sistema. In tal modo si limita l'esposizione del sistema a virus dannosi. Questa funzione si attiva solo con supporti inseriti localmente o supporti rimovibili, come unità Zip, CD, DVD o file .DMG di OS X. Inoltre, esegue la scansione di periferiche USB come pen drive e fotocamere, e di periferiche Firewire come iPod. Non esegue la scansione di volumi su computer remoti collegati tramite la rete. Lo scanner viene eseguito in background e interagisce con l'utente.

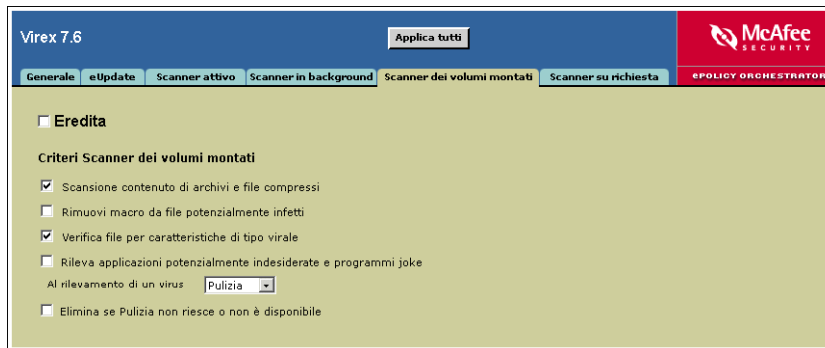


Figura 3-7 Scanner dei volumi montati

È possibile imporre i criteri di Scanner dei volumi montati seguenti:

Scansione contenuto di archivi e file compressi	Imposta lo scanner selezionato per la scansione di archivi e altri file compressi.
Rimuovi macro da file potenzialmente infetti	Se viene rilevato un file infetto, tutte le macro del file verranno rimosse quale parte dell'azione di pulizia.
Verifica file per caratteristiche di tipo virale	Attiva/disattiva la funzione euristica che esegue la scansione di file che presentano caratteristiche di tipo virale o worm e che potrebbero contenere infezioni sconosciute.
Rileva applicazioni potenzialmente indesiderate e programmi joke	Attiva/disattiva lo scanner per cercare programmi indesiderati o programmi joke.
Al rilevamento di un virus:	Seleziona l'azione primaria dello scanner.
<ul style="list-style-type: none"> ■ Pulizia ■ Elimina ■ Avvisa 	
Elimina se Pulizia non riesce o non è disponibile	Seleziona l'azione secondaria per lo scanner prescelto. Questa opzione è disponibile solo quando l'azione primaria è Pulizia.



Lo Scanner dei volumi montati non viene eseguito per impostazione predefinita.

Scanner su richiesta

Lo Scanner su richiesta consente di avviare una scansione in qualsiasi momento trascinando i file selezionati nella Console o attraverso una finestra di dialogo di apertura dei file. Con lo Scanner su richiesta è possibile selezionare più file, directory o volumi. I risultati della scansione vengono riepilogati in un rapporto che può essere salvato o stampato. L'utente può configurare gli elementi che lo scanner deve cercare e le modalità di risposta al rilevamento di file infetti. Inoltre, è possibile configurare un elenco di esclusioni che viene condiviso con lo Scanner attivo, lo Scanner in background e lo Scanner dei volumi montati. Lo scanner genera un avviso quando rileva un virus e quindi un registro che riporta le azioni intraprese.

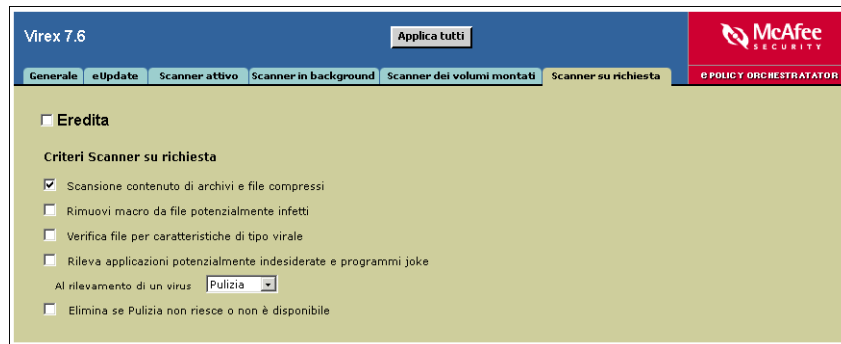


Figura 3-8 Scheda Scanner su richiesta

È possibile imporre i criteri di Scanner su richiesta seguenti:

Scansione contenuto di archivi e file compressi	Imposta lo scanner selezionato per la scansione di archivi e altri file compressi. Opzione attiva per impostazione predefinita per lo Scanner su richiesta.
Rimuovi macro da file potenzialmente infetti	Se viene rilevato un file infetto, tutte le macro del file verranno rimosse quale parte dell'azione di pulizia.
Verifica file per caratteristiche di tipo virale	Attiva/disattiva la funzione euristica che esegue la scansione di file che presentano caratteristiche di tipo virale o worm e che potrebbero contenere infezioni sconosciute.
Rileva applicazioni potenzialmente indesiderate e programmi joke	Attiva/disattiva lo scanner per cercare programmi indesiderati o programmi joke.
Al rilevamento di un virus:	Seleziona l'azione primaria dello scanner.
<ul style="list-style-type: none"> ■ Pulizia ■ Elimina ■ Avvisa 	
Elimina se Pulizia non riesce o non è disponibile	Seleziona l'azione secondaria per lo scanner prescelto. Questa opzione è disponibile solo quando l'azione primaria è Pulizia.

Pianificazione delle scansioni e di eUpdate

Quando viene eseguita la scansione con Virex, vengono utilizzate le informazioni contenute nel "file di definizione dei virus (DAT)" per cercare e rimuovere i virus. Ogni giorno vengono scoperti molti nuovi virus e regolarmente vengono creati nuovi file DAT per fornire la protezione da questi virus. Per garantire la migliore protezione antivirus, è possibile utilizzare ePolicy Orchestrator per indicare a Virex dove accedere ai file DAT più recenti, creare delle pianificazioni per sostituire i file DAT precedenti ed eseguire scansioni su richiesta.

Informazioni sulle attività pianificate

Con ePolicy Orchestrator è possibile creare i seguenti tipi di attività pianificate per il software Virex:

- Scansione su richiesta
- eUpdate

È possibile impostare l'esecuzione delle attività pianificate di un computer in base all'ora locale a all'ora di Greenwich (GMT). Tuttavia, dato che con ePolicy Orchestrator non è possibile monitorare l'avanzamento dell'attività, si consiglia di visualizzare periodicamente il registro sul server.

Scansione su richiesta

Con Virex è possibile eseguire la scansione su richiesta dei file per verificare che in tutti i file dei database non vi sia contenuto ambiguo. È possibile creare un numero qualsiasi di pianificazioni di scansioni su richiesta, configurate per essere eseguite a intervalli predefiniti o in qualsiasi momento dall'utente. È inoltre possibile disattivare le pianificazioni che non si desidera eseguire automaticamente.

Creazione di una nuova attività

Per creare una nuova attività:

- Fare clic sulla scheda **Tasks** (Attività) nel riquadro superiore dei dettagli. Fare clic con il pulsante destro del mouse nel riquadro e selezionare **Schedule Tasks** (Pianifica attività).

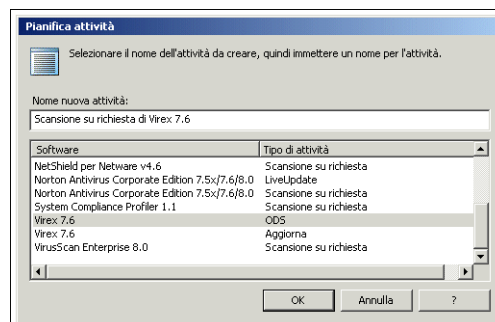


Figura 3-9 Schedule Tasks (Pianifica attività)

- Digitare il nome dell'attività nel campo **New Task Name** (Nome nuova attività) e selezionare l'attività che si desidera creare. Nell'elenco a discesa **Task Type** (Tipo di task) selezionare **On-Demand Scan** (Scansione su richiesta). Fare clic su **OK**.
- L'attività creata viene elencata nel riquadro **Tasks** (Attività).

Directory							
Criteri	Proprietà	Attività					
Nome attività	Ultima modifica	Creato in	Attivato	Tipo pianificazione	Data di inizio	Ora di inizio	
Distribuzione	Directory	Directory	Falso	Ogni giorno	9/20/2004	12:00:00 AM	
Aggiorna Virex 7.6	Directory	Directory	Falso	Ogni giorno	10/11/2004	11:24:00 AM	
Scansione su richiesta di...	Directory	Directory	Falso	Ogni giorno	10/11/2004	11:41:00 AM	

Figura 3-10 Scheda Tasks (Attività)

Modifica di un'attività

Per modificare un'attività:

- Fare clic con il pulsante destro del mouse sull'attività e selezionare **Edit Task** (Modifica attività).

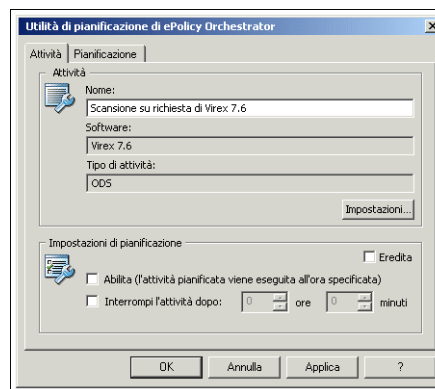


Figura 3-11 ePolicy Orchestrator Scheduler - scheda Task (Attività)

- Fare clic su **Settings** (Impostazioni) per includere i file e la directory nella scansione pianificata. [Vedere Scanner su richiesta a pagina 35](#).

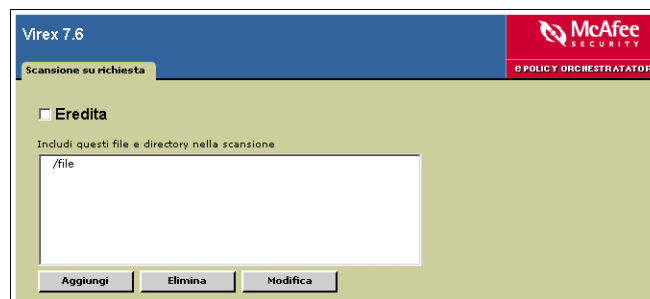


Figura 3-12 Scansione su richiesta - Includi file e directory



Deselezionare **Inherit** (Eredita) e selezionare **Enable (schedule task runs at specified time)** (Abilita - l'attività pianificata viene eseguita all'ora specificata) per attivare le impostazioni delle attività nel riquadro **Schedule Settings** (Impostazioni di pianificazione).

Includi questi file e directory nella scansione	<p>Configura le inclusioni di scansione.</p> <p>Per aggiungere un'inclusione:</p> <ul style="list-style-type: none"> Fare clic su Aggiungi; verrà visualizzato Aggiungi elemento da esaminare -- Finestra di dialogo pagina Web. Digitare il percorso completo di ogni file, directory e volume che si desidera includere e fare clic su OK. L'inclusione verrà elencata nell'elenco di inclusione. <p>Per rimuovere un'inclusione:</p> <ul style="list-style-type: none"> Selezionare l'inclusione nell'elenco di inclusione e fare clic su Rimuovi. <p>Per modificare un'inclusione:</p> <ul style="list-style-type: none"> Selezionare l'inclusione nell'elenco di inclusione e fare clic su Modifica. Verrà visualizzato Aggiungi elemento da esaminare -- Finestra di dialogo pagina Web, quindi modificare il percorso completo del file o directory che si desidera includere nella scansione e fare clic su OK.
---	--

Schedule Settings (Impostazioni di pianificazione)

Abilita (l'attività pianificata viene eseguita all'ora specificata)	Selezionare questa opzione per attivare l'esecuzione dell'attività in un momento specificato.
Stop the task if it runs for (Interrompi l'attività dopo):	Specificare le ore e minuti di interruzione per limitare la durata dell'esecuzione dell'attività prima che venga annullata.

Scheda Schedule (Pianificazione)

Sono disponibili numerose opzioni per pianificare un'attività.

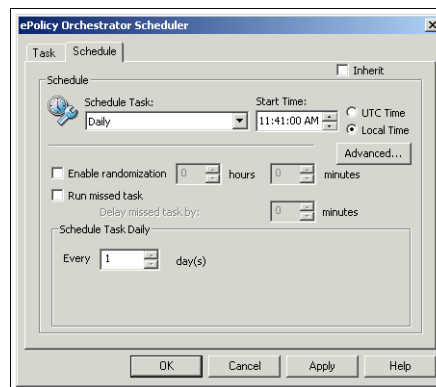


Figura 3-13 ePolicy Orchestrator Scheduler - scheda Schedule (Pianificazione)

Schedule Task (Pianifica attività)	<p>Selezionare il tipo di attività dall'elenco. È possibile selezionare una qualsiasi delle opzioni seguenti:</p> <ul style="list-style-type: none"> ■ Daily (Ogni giorno) ■ Weekly (Ogni settimana) ■ Monthly (Ogni mese) ■ Once (Una volta) ■ At System Startup (All'avvio del sistema) ■ Run Immediately (Esegui immediatamente)
Start Time (Ora di inizio) <ul style="list-style-type: none"> ■ UTC Time (Ora TUC) ■ Local Time (Ora locale) 	<p>Specificare l'ora di inizio della pianificazione. Selezionare l'ora locale per eseguire l'attività a intervalli pianificati in base all'ora di sistema del computer client. È utile pianificare l'esecuzione delle attività che richiedono un uso intensivo del processore, ad esempio le scansioni su richiesta, al di fuori dell'orario di lavoro.</p> <p>Se si seleziona UTC, l'attività verrà eseguita quando l'ora di inizio corrisponde all'ora TUC (Tempo universale coordinato), nota anche come ore di Greenwich (GMT). Se si utilizza questa opzione, l'attività verrà eseguita alla stessa ora su tutti i clienti Macintosh indipendentemente dall'ora locale sui sistemi Macintosh.</p>
Enable randomization (Abilita esecuzione casuale)	L'attività non viene eseguita esattamente all'ora specificata ma ad intervalli casuali specificati. Per attivare l'esecuzione casuale, selezionare le ore e i minuti.
Run missed task (Esegui attività non eseguita)	Garantisce l'esecuzione dell'attività nel caso in cui il computer Macintosh sia spento o altrimenti non disponibile al momento dell'ora di inizio pianificata. Se si seleziona questa opzione, l'attività verrà eseguita non appena il computer Macintosh sarà nuovamente disponibile.
Delay missed task by (Ritarda attività non eseguita di)	Fare clic su Advanced (Avanzate) nella finestra di dialogo Advanced Schedule Options (Opzioni di pianificazione avanzate). Se si seleziona questa opzione, viene ritardata l'esecuzione delle attività non eseguite dopo che il computer Macintosh è nuovamente disponibile.
Start Date / End Date (Data di inizio / Data di fine)	Fare clic su Advanced (Avanzate) nella finestra di dialogo Advanced Schedule Options (Opzioni di pianificazione avanzate). Digitare la data di inizio e la data di fine se si desidera eseguire l'attività soltanto in un determinato periodo di tempo, per alcuni giorni o settimane o temporaneamente.
Repeat Task (Ripeti l'attività)	<p>Fare clic su Advanced (Avanzate) nella finestra di dialogo Advanced Scheduled Options (Opzioni di pianificazione avanzate). Selezionare questa opzione per eseguire un'attività più volte al giorno. A tal fine selezionare Repeat Task (Ripeti attività) e impostare l'intervallo di ripetizione in modo appropriato.</p> <p>In genere viene consigliata per eseguire più volte al giorno un'attività di aggiornamento su client, in particolare se ci sono molti nuovi virus. È inoltre possibile pianificare la frequenza dell'attività con altri intervalli, ad esempio settimanali o mensili.</p>
Schedule Task Daily (Pianifica attività giornaliera)	Specificare l'intervallo per l'esecuzione dell'attività pianificata; tale intervallo dovrebbe essere di 1 giorno o di più giorni. Se si seleziona 1, l'attività pianificata viene eseguita a giorni alterni.

Eliminazione di un'attività

Per eliminare un'attività:

- Fare clic con il pulsante destro del mouse sull'attività nel riquadro **Tasks** (Attività) e selezionare **Delete** (Elimina).

eUpdate

Quando viene eseguita una scansione con Virex in base alle impostazioni specificate, per trovare e rimuovere i virus viene utilizzato il motore di scansione antivirus di Virex e i file di definizione dei virus (DAT) correnti. Ogni giorno vengono scoperti molti nuovi virus e regolarmente vengono creati nuovi file di definizione dei virus per fornire la protezione da questi virus. Il software antivirus in uso fornisce una protezione completa solo se è aggiornato con il file DAT e il motore di scansione antivirus più recenti. Si consiglia di aggiornare i file DAT di Virex almeno una volta alla settimana e di controllare regolarmente sul sito Web di McAfee AVERT (Anti-Virus Emergency Response Team) se sono disponibili nuovi file DAT. Se nel dominio corrente vi sono più server che eseguono tutti Virex, è possibile utilizzare un server per scaricare il file DAT più recente, quindi configurare gli altri per copiare i file da quel server. Il server può scaricare i file per più sistemi operativi, indipendentemente dai sistemi operativi in uso.

Definizione del percorso dei file DAT

Con la pagina eUpdate è possibile specificare l'origine dei file DAT.

vedere Personalizzazione delle impostazioni di eUpdate a pagina 31.

Creazione di un'attività di eUpdate

- 1 Nella struttura della console in **ePolicy Orchestrator** fare clic con il pulsante destro del mouse sulla directory oppure sul sito, sul gruppo o sull'host, quindi selezionare **Schedule Task** (Pianifica attività). Viene visualizzata la finestra di dialogo **Schedule Task** (Pianifica attività).

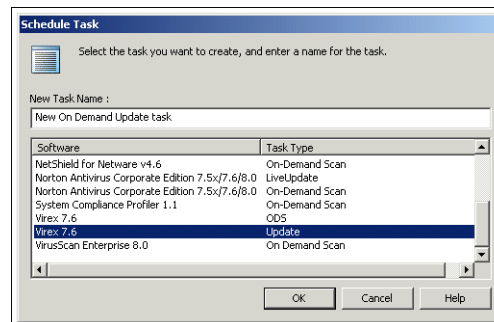


Figura 3-14 Nuova attività di aggiornamento

- 2 Nella finestra di dialogo **Schedule Task** (Pianifica attività) digitare un nome in **New Task Name** (Nome nuova attività).
- 3 Selezionare **Virex 7.6 - Update** (Virex 7.6 - Aggiornamento) dall'elenco **Software/Task Type** (Software/Tipo attività).
- 4 Fare clic su **OK** per creare l'attività.

Configurazione di un'attività di eUpdate

Dopo aver creato una nuova attività di eUpdate, è possibile configurarla in base alle proprie esigenze.

- 1 Nella scheda **Tasks** (Attività) del riquadro superiore dei dettagli fare clic con il pulsante destro del mouse, quindi selezionare **Edit Task** (Modifica attività). Viene visualizzata la finestra di dialogo **ePolicy Orchestrator Scheduler** (Utilità di pianificazione di ePolicy Orchestrator).
- 2 Deselezionare **Inherit** (Eredita). [vedere Modifica di un'attività a pagina 37](#).
- 3 Fare clic su **OK** per tornare alla finestra di dialogo **ePolicy Orchestrator Scheduler** (Utilità di pianificazione di ePolicy Orchestrator).
- 4 Per eliminare un'attività di eUpdate per Virex, [vedere Eliminazione di un'attività a pagina 39](#).

Disattivazione di un'attività di eUpdate

- 1 Nella scheda **Tasks** (Attività) del riquadro superiore dei dettagli fare clic con il pulsante destro del mouse, quindi selezionare **Edit Task** (Modifica attività). Viene visualizzata la finestra di dialogo **ePolicy Orchestrator Scheduler** (Utilità di pianificazione di ePolicy Orchestrator).
- 2 Dopo aver modificato le opzioni desiderate nella scheda **Task** (Attività) e nella scheda **Schedule** (Pianificazione) della finestra di dialogo **ePolicy Orchestrator Scheduler** (Utilità di pianificazione di ePolicy Orchestrator), fare clic sul pulsante **Settings** (Impostazioni). Viene visualizzata la pagina **Impostazioni attività di eUpdate per Virex**.

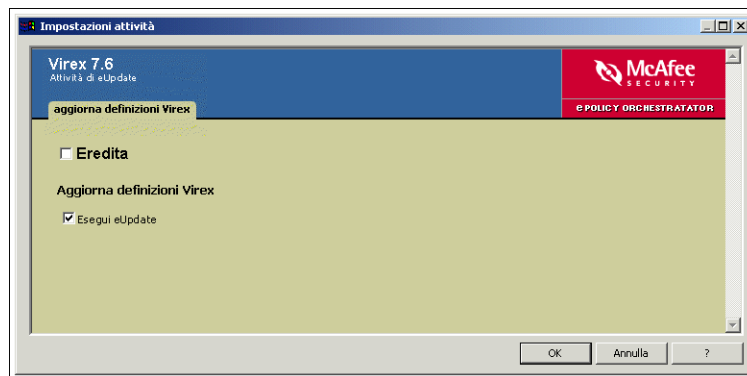


Figura 3-15 Aggiorna definizioni Virex - Esegui eUpdate

- 3 Deselezionare **Eredita** nella pagina **Impostazioni attività di eUpdate per Virex**.
- 4 Deselezionare **Esegui eUpdate**, quindi selezionare **Eredita**.
- 5 Fare clic su **OK** per tornare alla finestra di dialogo **ePolicy Orchestrator Scheduler** (Utilità di pianificazione di ePolicy Orchestrator).
- 6 Per eliminare un'attività di eUpdate per Virex, [vedere Eliminazione di un'attività a pagina 39](#).

Visualizzazione delle proprietà del server ePolicy Orchestrator

Dal server ePolicy Orchestrator è possibile visualizzare varie proprietà di sistema.

Per visualizzare le proprietà del server:

- 1 Selezionare il server nella directory della struttura della console per cui si desidera visualizzare le impostazioni.

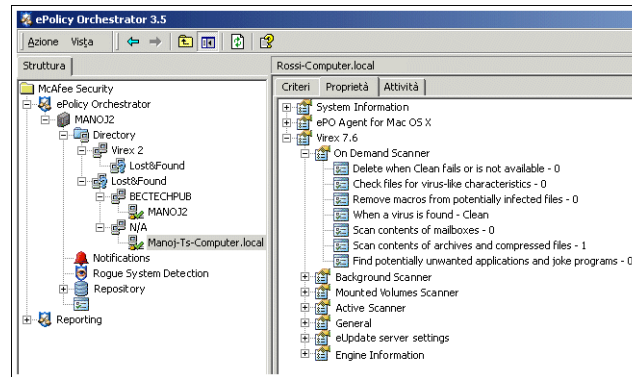


Figura 3-16 Directory della struttura della console

- 2 Fare clic sulla scheda **Properties** (Proprietà) nel riquadro superiore dei dettagli.
- 3 Nel riquadro **Properties** (Proprietà) espandere la struttura di **Virex 7.6** per visualizzare l'elenco delle proprietà.
- 4 Fare clic su + accanto a una proprietà per visualizzarne i dettagli.

4

Controllo remoto dell'agente

Visualizzazione delle proprietà raccolte dall'agente

È possibile utilizzare la console di ePolicy Orchestrator per visualizzare le proprietà correnti di un determinato computer. Tali proprietà includono informazioni di sistema di base, quali sistema operativo, indirizzo IP di rete, RAM e velocità del processore, nonché proprietà relative all'agente e ai prodotti antivirus o di protezione McAfee installati sul computer.

In particolare in caso di risoluzione di problemi, è buona norma verificare i criteri del computer per assicurarsi che le modifiche apportate ai criteri sulla console siano stati imposti al client Macintosh. L'agente rinvia le proprietà al server a ogni intervallo di comunicazione agente-server (ASCI) consentendo all'utente di visualizzare le proprietà di sistema impostate sui computer client Macintosh direttamente dalla console di ePolicy Orchestrator.

Distinzione tra proprietà e criteri

I criteri sono le regole configurate per l'agente o per prodotti specifici nelle pagine dei criteri sul server ePolicy Orchestrator. Quando l'agente impone questi criteri sul computer client Macintosh, essi diventano proprietà. Le proprietà sono dunque le impostazioni effettivamente in uso sul computer client Macintosh.

Visualizzazione delle proprietà raccolte dall'agente

Per visualizzare le proprietà raccolte dall'agente relative ai computer selezionati nella Directory:

- 1 Nella struttura della console, selezionare il computer in cui è installato Virex.
- 2 Nel riquadro superiore destro dei dettagli, fare clic sulla scheda **Properties** (Proprietà) per visualizzare le proprietà del computer selezionato.

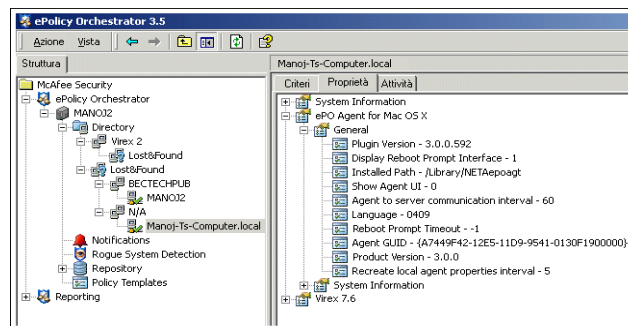


Figura 4-1 Visualizzazione delle proprietà raccolte dall'agente

- 3 Espandere i tipi di proprietà per visualizzare i dettagli relativi a proprietà specifiche. Le proprietà raccolte dall'agente sono elencate in ePolicy Orchestrator (Agente ePolicy Orchestrator).

Imposizione dei criteri per l'Agente ePolicy Orchestrator

Una volta terminata la configurazione dei criteri, è necessario imporli per renderli disponibili all'Agente ePolicy Orchestrator sugli host Virex.

Nella struttura della console di ePolicy Orchestrator, selezionare gli host per i quali si desidera imporre i criteri.

- 1 Nel riquadro superiore dei dettagli, selezionare **ePO agent for Mac OS X** (Agente ePO per Mac OS X).

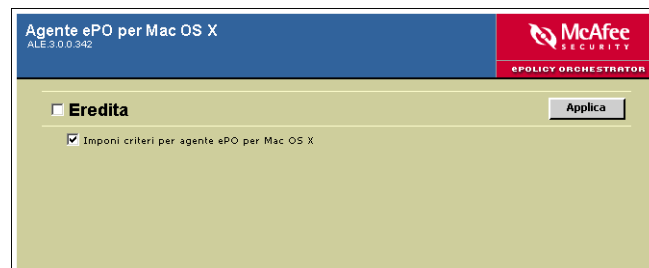


Figura 4-2 Imposizione dei criteri per l'Agente ePolicy Orchestrator per Mac OS X

- 2 Deselezionare **Inherit** (Eredita).
- 3 Selezionare **Enforce policies** (Imponi criteri) per l'Agente ePolicy Orchestrator per Mac OS X.
- 4 Fare clic su **Apply** (Applica) per salvare le impostazioni. ePolicy Orchestrator renderà i criteri configurati disponibili all'agente sugli host Virex.

Opzioni dell'agente

L'agente è il componente distribuito di ePolicy Orchestrator che viene installato su ogni computer Macintosh della rete. L'agente raccoglie le informazioni e ne gestisce lo scambio tra il server ePolicy Orchestrator, archivi e computer client e prodotti gestiti. La modalità di configurazione dell'agente e dei relativi criteri ne influenza il funzionamento e facilita la comunicazione e l'aggiornamento all'interno dell'ambiente di rete.

Per configurare i criteri dell'agente per un computer

- 1 Nella struttura della console di ePolicy Orchestrator, selezionare il computer aggiunto per Virex.
- 2 Nella scheda **Policies** (Criteri) nel riquadro superiore dei dettagli, selezionare **Configuration** (Configurazione) sotto alla voce **Agente ePO per Mac OS X**. Nel riquadro inferiore dei dettagli, viene visualizzata la pagina **Policy** (Criterio).

- 3 Nella scheda **Opzioni agente**, deselezionare **Eredita**.

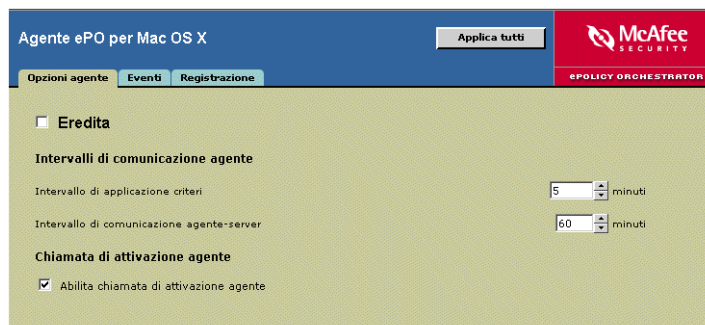


Figura 4-3 ePolicy Orchestrator - scheda Opzioni agente

- 4 In **Intervallo di applicazione dei criteri**, scegliere un intervallo in minuti conforme alle esigenze dell'organizzazione. Il valore predefinito è 5 minuti. È possibile specificare un valore compreso tra 5 e 10080 minuti (1 settimana).
- 5 In **Comunicazione agente-server**, scegliere un intervallo in minuti conforme alle esigenze dell'organizzazione. Il valore predefinito è 60 minuti. È possibile specificare un valore compreso tra 5 e 2880 minuti (2 giorni).
- 6 Per consentire al server ePolicy Orchestrator di inviare chiamate di attivazione all'agente, selezionare **Abilita chiamata di attivazione agente**.

Eventi

Il server ePolicy Orchestrator riceve notifiche da Non Windows Agent. È necessario configurare le pagine dei criteri per inoltrare immediatamente gli eventi al server ePolicy Orchestrator oppure agli intervalli di comunicazione agente-server stabiliti.

Se si sceglie di inviare gli eventi immediatamente, tutti gli eventi con un valore di gravità pari o superiore al valore configurato per l'agente vengono inviati immediatamente.

In caso contrario, l'agente inoltra gli eventi indipendentemente dalla gravità solo durante l'intervallo di comunicazione agente-server stabilito.

Per impostare i criteri dell'Agente ePolicy Orchestrator:

- 1 Effettuare l'accesso al server ePolicy Orchestrator.
- 2 Selezionare la Directory o il sito, il gruppo o il computer desiderato, quindi selezionare la scheda **Policies** (Criteri) nel riquadro superiore dei dettagli.
- 3 Selezionare **ePolicy Orchestrator Agent for Mac OS X | Configuration** (Agente ePolicy Orchestrator for Mac OS X | Configurazione) nel riquadro superiore dei dettagli.

- 4 Nel riquadro inferiore dei dettagli selezionare la scheda **Eventi**.

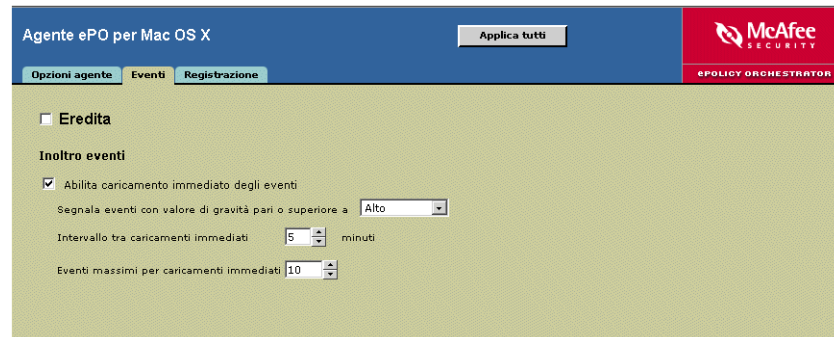


Figura 4-4 Scheda Eventi

- 5 Deselezionare **Eredita**.

Configurare le seguenti opzioni dei criteri:

Inoltro eventi

Selezionare **Abilita caricamento immediato degli eventi** per consentire all'agente di inoltrare immediatamente gli eventi al server.

Deselezionare questa opzione se si desidera che l'agente inoltri gli eventi solo al successivo intervallo di comunicazione agente-server stabilito. Se si seleziona questa opzione, è necessario specificare:

- La gravità minima degli eventi che si desidera inviare al server in Segnala eventi con valore di gravità pari o superiore a. È possibile specificare i valori di gravità Critico, Alto, Basso, Avviso, Informativo. Ad esempio, se si seleziona Basso, vengono inoltrati al server tutti gli eventi con una gravità pari o superiore a Minor.
 - L'intervallo di inoltro degli eventi in Intervallo tra caricamenti immediati. I minuti selezionati in questo campo determinano la frequenza massima con la quale vengono inoltrati gli eventi. Ad esempio, se si seleziona 5 minuti, l'agente inoltrerà gli eventi al server al massimo ogni cinque minuti.
 - Il numero massimo di eventi da inviare contemporaneamente in Eventi massimi per caricamenti immediati. Se il numero di eventi supera il limite indicato, i restanti eventi vengono inviati durante l'intervallo di inoltro eventi successivo.
- 6 Fare clic su **Apply All** (Applica tutti) per salvare le impostazioni. Le modifiche avranno effetto a partire dalla successiva comunicazione agente-server.

Eliminazione periodica di eventi meno recenti dal database

È possibile che si desideri eliminare periodicamente eventi dal database per controllarne le dimensioni e migliorare le prestazioni del sistema. L'utilità di molti eventi, in particolare quelli minori e informativi, diminuisce col passare del tempo. Inoltre, prima di eliminare eventi di qualsiasi tipo, è possibile ed è consigliabile eseguire un backup del database. È inoltre possibile archiviare questo database e utilizzarlo in un momento successivo per eventuali esigenze di rapporti cronologici.

Per eliminare eventi in modo permanente dal database di ePolicy Orchestrator, attenersi alla seguente procedura.

- 1 Effettuare l'accesso al server database ePolicy Orchestrator desiderato.
- 2 Nella struttura della console in **Reporting | ePO Databases | <server database>** (Creazione rapporti | Database ePO | server database), selezionare **Events** (Eventi). Nel riquadro dei dettagli vengono visualizzate le schede **Filtering**, **Import**, **Repair** e **Removal** (Filtraggio, Importazione, Riparazione e Rimozione).

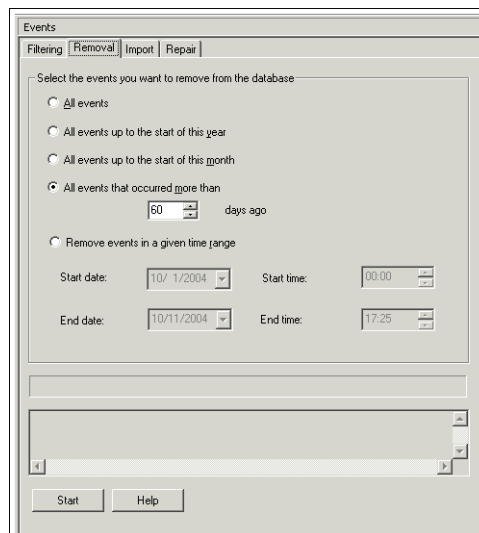


Figura 4-5 Eventi - scheda Removal (Rimozione)

- 3 Fare clic sulla scheda **Removal** (Rimozione).
- 4 Selezionare gli eventi che si desidera rimuovere dal database.
 - **All events** (Tutti gli eventi) — Selezionare questa opzione per rimuovere tutti gli eventi dal database.
 - **All events up to the start of the year** (Tutti gli eventi fino all'inizio dell'anno) — Selezionare questa opzione per rimuovere tutti gli eventi antecedenti all'inizio dell'anno di calendario corrente.

- **All events up to the start of the month** (Tutti gli eventi fino all'inizio del mese) — Selezionare questa opzione per rimuovere tutti gli eventi antecedenti all'inizio del mese corrente.
 - **All events that occurred more than X days ago** (Tutti gli eventi verificatisi più di X giorni fa) — Selezionare questa opzione per rimuovere tutti gli eventi antecedenti al numero di giorni specificato.
 - **Remove events in a given time range** (Rimuovi eventi in un determinato intervallo di tempo) — Selezionare questa opzione per specificare un intervallo di date. Verranno rimossi tutti gli eventi verificatisi nell'intervallo di date specificato.
- 5 Fare clic su **Start** (Avvia) per eliminare dal database gli eventi specificati.

Visualizzazione degli eventi dei server

Nella console di ePolicy Orchestrator, è possibile visualizzare, salvare e stampare tutti gli eventi informativi, di avviso e di errore relativi a ogni server ePolicy Orchestrator. Verificando la finestra degli eventi di un server è possibile sapere se le azioni iniziate dal server sono andate o meno a buon fine, ad esempio se un agente ha distribuito o estratto file DAT aggiornati da un archivio di origine.

Inoltre, è possibile specificare quali eventi vengono salvati nel database di ePolicy Orchestrator. Per informazioni sulla gestione dei database di ePolicy Orchestrator e degli eventi salvati nel database, consultare la *Guida del prodotto ePolicy Orchestrator*.

Per visualizzare, salvare o stampare eventi dei server dalla console di ePolicy Orchestrator:

- 1 Effettuare l'accesso al server ePolicy Orchestrator.
- 2 Nella struttura della console in ePolicy Orchestrator, selezionare il nodo del server, quindi fare clic sulla scheda **General** (Generale) nel riquadro dei dettagli.
- 3 Fare clic su **Server Events** (Eventi server) per aprire la finestra di dialogo **Server Event Viewer** (Visualizzatore eventi server).

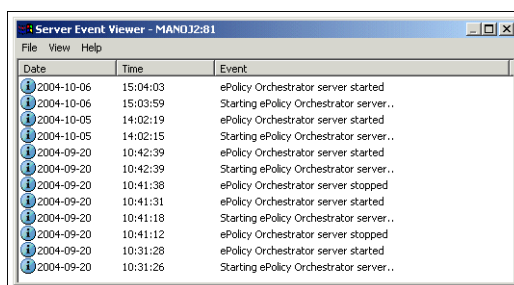


Figura 4-6 Server Event Viewer (Visualizzatore eventi server)

- 4 Selezionare **View | Refresh** (Visualizza | Aggiorna) per assicurarsi che l'elenco degli eventi sia aggiornato.

Visualizzazione dei dettagli di un determinato evento

Per visualizzare una descrizione dettagliata di un evento del server, selezionare e fare doppio clic sull'evento desiderato. Viene visualizzata la finestra di dialogo **Server Event Detail** (Dettaglio evento server).

Salvataggio degli eventi in un file di registro

Per salvare tutti gli eventi del server in un file di registro del server (.log), selezionare **File | Save As** (File | Salva con nome). Per salvare nel file di registro del server solo eventi selezionati, selezionare gli eventi desiderati, quindi selezionare **File | Save As** (File | Salva con nome). Nella finestra **Save As** (Salva con nome), selezionare **Selected Items** (Elementi selezionati).

Stampa degli eventi del server

Per stampare tutti gli eventi del server sulla stampante selezionata, fare clic su **Print** (Stampa) nel menu **File**. Per stampare solo eventi selezionati sulla stampante predefinita, selezionare gli eventi desiderati, quindi selezionare **File | Print** (File | Stampa).

Registrazione

Durante il suo normale funzionamento, l'agente sul computer Macintosh genera costantemente eventi software, inclusi eventi informativi sul normale funzionamento, ad esempio quando l'agente impone criteri localmente o quando avvia una scansione a richiesta. Tali eventi vengono registrati dall'agente, inviati al server a ogni intervallo di comunicazione agente-server specificato e archiviati nel database. Una tipica implementazione di ePolicy Orchestrator in una rete di grandi dimensioni può generare migliaia di eventi di questo tipo ogni ora.

Per impostare i criteri relativi alla registrazione di ePolicy Orchestrator:

- 1 Effettuare l'accesso al server ePolicy Orchestrator.
- 2 Selezionare la Directory o il sito, il gruppo o il computer desiderato, quindi selezionare la scheda **Policies** (Criteri) nel riquadro superiore dei dettagli.
- 3 Selezionare **ePolicy Orchestrator Agent for Mac OS X | Configuration** (Agente ePolicy Orchestrator for Mac OS X | Configurazione) nel riquadro superiore dei dettagli.

4 Nel riquadro inferiore dei dettagli, selezionare la scheda **Registrazione**.

Le opzioni di questa scheda consentono di configurare criteri relativi alla modalità di registrazione delle attività dell'agente.



Figura 4-7 Scheda Registrazione

Criteri di registrazione agente	Descrizione della proprietà
Abilita registrazione agente	Consente di abilitare la registrazione delle attività dell'agente. Se si seleziona questa casella di controllo, viene abilitata la registrazione in /Library/NETAepoagt/Scratch/etc/log.
Abilita registrazione dettagliata	Abilita la registrazione dettagliata delle attività dell'agente nel file di registro agent_<computer>.log. Il file di registro può assumere grandi dimensioni. Si consiglia di abilitare la registrazione dettagliata, in caso contrario la sola registrazione degli errori critici potrebbe essere insufficiente per risolvere problemi di comunicazione specifici.

5

Rapporti

Rapporti

Dalla console di ePolicy Orchestrator è possibile visualizzare dei rapporti che mostrano in che modo vengono gestite le infezioni dagli host Virex. Da qui si può verificare anche la configurazione impostata sugli host. È inoltre possibile creare rapporti utilizzando i dati inviati da Non Window Agent al database di ePolicy Orchestrator selezionato. È infine possibile salvare le selezioni effettuate nelle finestre di dialogo **Enter Report Inputs** (Immetti input rapporto) e **Report Data Filter** (Filtro dati rapporto) per l'eventuale utilizzo futuro.

I rapporti di ePolicy Orchestrator consentono di:

- Impostare un filtro di directory per raccogliere solo le informazioni che si desidera visualizzare. Quando si imposta questo filtro, è possibile scegliere quale parte della struttura della console di ePolicy Orchestrator includere nel rapporto.
- Impostare un filtro di dati, utilizzando operatori logici, per definire filtri precisi per i dati restituiti dal rapporto.
- Generare rapporti grafici dalle informazioni del database e filtrare i rapporti in base alle proprie necessità. È possibile stampare i rapporti ed esportarli per utilizzarli in altri prodotti software.
- Effettuare query su computer, eventi e installazioni.

Per eseguire un rapporto:

- 1 Effettuare l'accesso al server database ePolicy Orchestrator.
- 2 Selezionare il rapporto Virex desiderato in **Reporting | ePO Databases** | <server database> | **Reports** | <gruppo rapporti> (Creazione rapporti | Database ePO | server database | Rapporti | gruppo rapporti) nella struttura della console.
 - Se viene visualizzata la finestra di dialogo **Current Protection Standards** (Standard di protezione correnti), specificare i numeri di versione dei file di definizione dei virus oppure il motore di scansione dei virus per il quale si desidera eseguire il rapporto.
 - Se viene visualizzata la finestra di dialogo **Enter Report Inputs** (Immetti input rapporto), effettuare le selezioni desiderate nelle schede visualizzate: **Rules**, **Layout**, **Data Grouping**, **Within**, **Saved Settings** (Regole, Layout, Raggruppamento dati, Entro, Impostazioni salvate).



Le schede possono variare in base al rapporto selezionato. Per ulteriori dettagli sulle schede Rules, Layout, Grouping, Within e Saved settings, consultare la *Guida del prodotto ePolicy Orchestrator*.

- 3 Selezionare il rapporto (**Agent Versions**/Versioni agenti) che si desidera generare e impostare il filtro dati nella finestra di dialogo **Report Data Filter** (Filtro dati rapporto). Fare clic su **OK**.
- 4 Viene generato il rapporto **Agent Versions** (Versioni agenti).

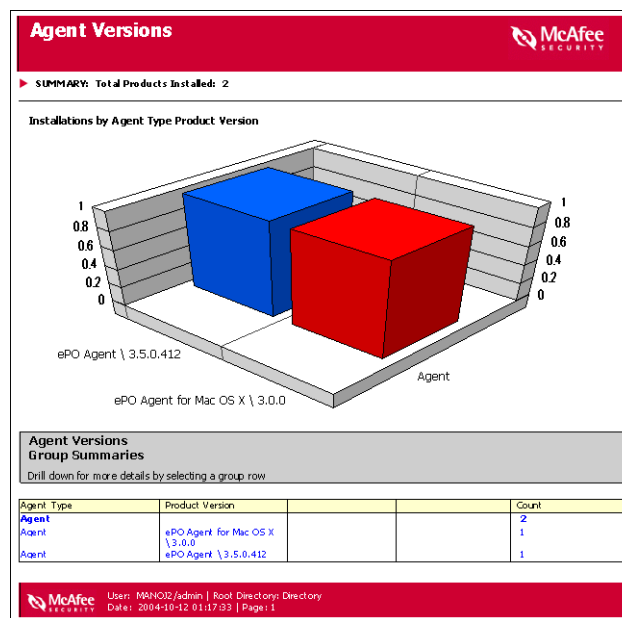


Figura 5-1 Rapporto di esempio - Agent Versions (Versioni agenti)

Configurazione dei rapporti

Esistono molti modi per controllare quali dati vengono visualizzati nei rapporti. È possibile definire il numero di versione dei file di definizione dei virus, i motori di scansione dei virus e i prodotti supportati che devono essere installati su computer client Macintosh affinché questi possano essere considerati conformi al programma di protezione e antivirus dell'azienda. È inoltre possibile limitare i risultati dei rapporti selezionando criteri di prodotto, quali nome del computer, sistema operativo, nome del virus, azione intrapresa su file infetti.

Dopo che i risultati del rapporto sono stati visualizzati, è possibile eseguire una serie di operazioni sui dati. È possibile visualizzare i dettagli sui dati del rapporto desiderati, ad esempio per verificare quali computer client Macintosh non dispongono di una versione di Virex compatibile installata. Alcuni rapporti possono addirittura includere collegamenti ad altri rapporti, denominati sottorapporti, che forniscono dati correlati al rapporto corrente. È inoltre possibile stampare o esportare i dati del rapporto in numerosi formati di file, inclusi HTML e Microsoft Excel.



Per ulteriori informazioni sulla configurazione dei rapporti, consultare la *Guida del prodotto ePolicy Orchestrator*.

Glossario

Agent Monitor, monitoraggio agente

Interfaccia utente dell'agente che può essere visualizzata sui computer gestiti. Consente di eseguire immediatamente quelle attività che normalmente vengono avviate dall'agente a intervalli predefiniti.

Agente ePolicy Orchestrator

Programma che esegue attività in background sui computer gestiti, funge da mediatore di tutte le richieste tra il server ePolicy Orchestrator e i prodotti antivirus e di protezione su questi computer e rinvia rapporti al server per indicare lo stato di queste attività.

agente inattivo

Agente che non ha comunicato con il server ePolicy Orchestrator nell'arco di un intervallo di tempo specificato.

archivi software distribuiti

Raccolta di siti Web o computer dislocati in rete in modo da fornire un accesso efficiente in termini di larghezza di banda ai computer client. Negli archivi distribuiti vengono memorizzati i file necessari ai computer client per installare i prodotti supportati e gli aggiornamenti di tali prodotti.

archiviare, archiviazione

Processo di aggiunta dei file all'archivio principale.

archivio

Percorso che memorizza le pagine dei criteri utilizzate per gestire i prodotti.

ASCI

Vedere *intervallo di comunicazione agente-server*.

attività di scansione

Evento di scansione singolo.

attività

Attività eseguita sia una sola volta come la *scansione su richiesta* sia di routine come l'*aggiornamento*, un'attività pianificata affinché abbia luogo in un orario specificato o a intervalli specificati.

Confrontare con *criterio*.

AutoUpgrade agente

Azione di aggiornamento automatico dell'agente ogni volta che è disponibile una nuova versione sul server ePolicy Orchestrator.

avviso

Messaggio o notifica relativi all'attività del computer quale il rilevamento di un virus. Può essere inviato automaticamente in base a una configurazione predefinita ad amministratori di sistema e utenti tramite e-mail, cercapersone o telefono.

Vedere anche *Alert Manager*.

chiamata di attivazione agente

Capacità di attivare la comunicazione agente-server dal lato server.

Vedere anche *chiamata di attivazione superagente*.

comunicazione agente-server

Qualsiasi comunicazione che si verifica tra l'Agente ePolicy Orchestrator e il server ePolicy Orchestrator in cui l'agente e il server si scambiano dati. In genere, l'agente avvia tutte le comunicazioni con il server.

console di ePolicy Orchestrator

Interfaccia utente del software ePolicy Orchestrator utilizzata per il controllo e il monitoraggio remoto dei computer gestiti.

Vedere anche *console remota di ePolicy Orchestrator*.

console remota di ePolicy Orchestrator

L'interfaccia utente di ePolicy Orchestrator quando è installata su un computer diverso dal server ePolicy Orchestrator.

Vedere anche *console di ePolicy Orchestrator*.

criterio

Le impostazioni di configurazione del prodotto gestito che sono definite e gestite da ePolicy Orchestrator.

database di ePolicy Orchestrator

Database che memorizza tutti i dati che il server ePolicy Orchestrator riceve dall'Agente ePolicy Orchestrator e tutte le impostazioni eseguite sul server.

Vedere anche *server database ePolicy Orchestrator*.

directory

Nella struttura della console, l'elenco di tutti i computer da gestire tramite ePolicy Orchestrator; il collegamento alle interfacce primarie per la gestione di questi computer.

distribuire, distribuzione

Azione di distribuzione e installazione dei programmi di installazione sui computer client da una postazione centrale.

elemento della struttura della console

Singole icone nella struttura della console di ePolicy Orchestrator.

ereditare, eredità

Azione di applicazione delle impostazioni definite per un elemento all'interno di una gerarchia dall'elemento precedente.

eseguire una scansione, scansione

Analisi dei file per determinare se è presente un virus o altro codice potenzialmente indesiderato.

Vedere *scansione all'accesso* e *scansione su richiesta*.

eventi del server

Attività sul server ePolicy Orchestrator che viene registrata dal Visualizzatore eventi di Windows. Queste informazioni non vengono memorizzate nel database di ePolicy Orchestrator, pertanto non sono disponibili ai fini della creazione dei rapporti.

eventi

Dati scambiati durante la comunicazione agente-server, che comprendono informazioni su ogni computer gestito (ad esempio, a livello di hardware e software) e sui relativi prodotti gestiti (ad esempio, impostazioni specifiche dei criteri e numero di versione del prodotto).

file binari (Installazione)

Il programma di installazione e tutti gli altri file necessari per installare i prodotti.

File DAT

File di definizione dei virus, a volte denominati file delle firme, che consentono al software antivirus di rilevare e gestire i virus e il codice correlato potenzialmente indesiderato incorporato nei file.

Vedere anche *file EXTRA.DAT*, *file DAT incrementali* e *SuperDAT*.

file di registro

Registrazione delle attività di un componente del software antivirus di McAfee. I file di registro prendono nota delle azioni intraprese durante un'installazione o durante le attività di scansione o di aggiornamento.

Vedere anche *eventi*.

gruppo Lost&Found

Gruppo utilizzato per memorizzare temporaneamente i computer dei quali non è possibile determinare la relativa posizione nella **Directory**.

gruppo

Nella struttura della console, una raccolta logica di entità riunite per semplificare la gestione. I gruppi possono contenere altri gruppi o computer; inoltre, è possibile assegnare ai gruppi intervalli di indirizzi IP o maschere di sottorete IP per consentire di ordinare i computer in base all'indirizzo IP. Se si crea un gruppo importando un dominio Windows NT, è possibile inviare automaticamente il pacchetto di installazione dell'agente a tutti i computer importati del dominio.

imporre, imposizione

Azione di applicazione delle impostazioni predefinite sui computer client a intervalli predefiniti.

inoltro immediato degli eventi

Azione di invio immediato degli eventi di gravità pari o superiore a un valore specifico al server ePolicy Orchestrator, una volta che è disponibile un numero predefinito di eventi. Questa comunicazione avviene al di fuori di altre comunicazioni agente-server.

installazione in background

Metodo di installazione che installa automaticamente un pacchetto software nel computer, senza intervento dell'utente.

intervallo di comunicazione agente-server (Asci)

Intervallo di tempo tra le comunicazioni agente-server predefinite.

intervallo di imposizione dei criteri

Intervallo di tempo durante il quale l'agente applica le impostazioni che ha ricevuto dal server ePolicy Orchestrator. Poiché queste impostazioni vengono applicate localmente, tale intervallo non richiede una larghezza di banda.

Ora TUC

Tempo universale coordinato (TUC). Fa riferimento all'ora sullo zero o sul meridiano di Greenwich.

pacchetti delle lingue dell'agente

Insieme di file che devono essere distribuiti ai computer client per visualizzare l'interfaccia utente dell'agente in lingue diverse dall'inglese.

pacchetto di installazione dell'agente

Il programma di installazione e tutti gli altri file necessari per installare l'agente.

priorità di avviso

Valore che si assegna a ogni messaggio di avviso a fini informativi. È possibile assegnare un livello di priorità ai messaggi di avviso. Tali livelli si distinguono in **Critico**, **Alto**, **Basso**, **Avviso** o **Informativo**.

proprietà

Dati scambiati durante la comunicazione agente-server, che comprendono informazioni su ogni computer gestito (ad esempio, a livello di hardware e software) e sui relativi prodotti gestiti (ad esempio, impostazioni specifiche dei criteri e numero di versione del prodotto).

pulire, pulizia

Azione intrapresa dallo scanner quando rileva un *virus*, un *cavallo di Troia* o un *worm*. L'azione di pulizia può consistere nel rimuovere il virus da un file per ripristinarne l'uso, rimuovere i riferimenti al virus dai file di sistema, dai file .INI del sistema e dal registro per terminare il processo generato dal virus, eliminare una macro o uno script di Microsoft Visual Basic che infetta un file, eliminare un file che è un cavallo di Troia o un worm oppure rinominare un file che non può essere pulito.

ramo

Posizioni nell'archivio principale che consentono di memorizzare e distribuire diverse versioni degli aggiornamenti selezionati.

Vedere anche *aggiornamento selettivo*.

riquadro dei dettagli

Il riquadro destro della console di ePolicy Orchestrator, che mostra i dettagli dell'elemento selezionato della struttura della console. A seconda dell'elemento della struttura della console selezionato, il riquadro dei dettagli può essere suddiviso in riquadri superiori e inferiori.

Vedere anche *riquadro superiore dei dettagli* e *riquadro inferiore dei dettagli*.

riquadro inferiore dei dettagli

Nella console, il riquadro inferiore destro che visualizza le impostazioni di configurazione dei prodotti elencati nella scheda **Policies** (Criteri) nel riquadro superiore dei dettagli.

Vedere anche *riquadro dei dettagli* e *riquadro superiore dei dettagli*.

riquadro superiore dei dettagli

Nella console, il riquadro superiore destro, che contiene le schede **Policies** (Criteri), **Properties** (Proprietà) e **Tasks** (Attività).

Vedere anche *riquadro dei dettagli* e *riquadro inferiore dei dettagli*.

scansione su richiesta

Analisi pianificata di file selezionati per determinare se è presente un virus o altro codice potenzialmente indesiderato. Può essere effettuata immediatamente, pianificata per un orario successivo o a intervalli regolari in base a una pianificazione.

Confrontare con *scansione all'accesso*.

server database ePolicy Orchestrator

Il computer che ospita il database di ePolicy Orchestrator. Può trattarsi dello stesso computer sul quale è installato il server ePolicy Orchestrator oppure di un altro computer.

server ePolicy Orchestrator

Il componente back-end del software ePolicy Orchestrator.

Vedere anche *Agente ePolicy Orchestrator* e *console di ePolicy Orchestrator*.

sito

Nella struttura della console, una raccolta logica di entità riunite per semplificare la gestione. I siti possono contenere gruppi o computer e possono essere organizzati in base all'intervallo di indirizzi IP, alla maschera di sottorete IP, alla posizione, al reparto e ad altre informazioni.

struttura della console

Contenuto della scheda **Tree** (Struttura) nel riquadro sinistro della console di ePolicy Orchestrator, che mostra gli elementi disponibili nella console.

utilità di segnalazione errori

Utilità progettata specificatamente per identificare e registrare sul sistema gli errori del software McAfee. Le informazioni ottenute possono essere utilizzate per diagnosticare e risolvere i problemi.

virus

Programma in grado di replicarsi con intervento minimo o senza alcun intervento dell'utente. Anche i programmi replicati si replicano ulteriormente.

worm

Virus che si diffonde creando copie di se stesso su altre unità, sistemi o reti.

Indice

A

- agente
 - directory, 18
 - imposizione dei criteri, 44
 - installazione, 18
 - installazione in background, 23
 - Installazione standard, 18
 - linea di comando, 23
 - opzioni, 44
 - requisiti di sistema, 13
 - visualizzazione delle proprietà, 43
- aggiornamento del software antivirus, 50
- assistenza clienti, informazioni per contattare, 12
- assistenza tecnica
 - accesso dal prodotto, 9
 - informazioni per contattare McAfee, 11
- attività
 - eliminazione, 39
 - modifica, 37
- AVERT
 - Anti-virus & Vulnerability Emergency Response Team, come contattare, 11
 - servizio di notifica DAT, 11
 - Weblmmune, 11

C

- collegamenti alle risorse nel prodotto, 9
- come contattare McAfee, 11
- come ottenere informazioni, 8
 - all'interno del prodotto, 9
 - elenco dei contatti, 11
- componenti server, 14

D

- definizione dei termini (*vedere* Glossario)
- destinatari di questa guida, 7

disinstallazione

- Agente ePO dal server ePO, 25
- Agente ePO per Mac OS X, 25
- file NAP di Virex dal server ePO, 24
- documentazione del prodotto, 8
- documentazione per il prodotto, 8

E

- ePolicy Orchestrator
 - proprietà del server, 42
- eUpdate, 30
 - configurazione, 41
 - creazione, 40
 - disattivazione, 41
 - FTP, 31
 - HTTP, 31
- eventi, 45
 - eliminazione degli eventi, 47
 - visualizzazione degli eventi dei server, 48

F

- file DAT
 - aggiornamenti tramite il servizio di notifica di AVERT, 11
 - aggiornamenti, sito Web, 11
 - definizione del percorso, 40
- file NAP
 - aggiunta di Non Windows Agent, 14
 - aggiunta di un file NAP di rapporto, 16
 - aggiunta di un file NAP di Virex, 15
 - archiviazione, 14
 - dove trovare i file NAP, 14

formazione in sede, 11

formazione sul prodotto, in sede, 11

formazione, in sede, 11

G

- glossario, 53

I

- impostazione dei criteri
 - ePolicy Orchestrator, 27
 - Generale, 29
 - scanner attivo, 32
 - Scanner dei volumi montati, 34
 - scanner in background, 33
 - Scanner su richiesta, 35
- informazioni sui prodotti, risorse, 8
- invio di un esempio di virus, 11

L

- Libreria di informazioni sui virus, 9, 11

M

- manuali, 8
- McAfee University, come contattare, 11

P

- pianificazione delle scansioni e di eUpdate, 36
- portale servizi, PrimeSupport, 11
- PrimeSupport, 11
- programma beta, come contattare, 11

Q

- quartier generale della sicurezza, come contattare AVERT, 11 a 12

R

- rapporti, 51
 - configurazione, 52
- registrazione, 49
- risorse per informazioni, 8

S

- servizi di consulenza, 11
- servizio di notifica, aggiornamenti DAT, 11
- sito Web di aggiornamento, 11
- sito Web di download, 11 a 12
- sito Web di formazione, 11

U

utilizzo della guida

convenzioni tipografiche
e simboli, [7](#)

V

virus, invio di un esempio

sito Web, [11](#)

W

WebImmune, [11](#)