AUTHORIZED DOCUMENTATION

Guida dell'utente di Endpoint Security Client 3.5

December 22, 2008

Novell®
ZENworks® Endpoint Security Management

3.5

www.novell.com

Note legali

Novell, Inc. non rilascia alcuna dichiarazione e non fornisce alcuna garanzia in merito al contenuto o all'uso di questa documentazione e in particolare non riconosce alcuna garanzia, espressa o implicita, di commerciabilità o idoneità per uno scopo specifico. Novell, Inc. si riserva inoltre il diritto di aggiornare la presente pubblicazione e di modificarne il contenuto in qualsiasi momento, senza alcun obbligo di notificare tali modifiche a qualsiasi persona fisica o giuridica.

Inoltre, Novell, Inc. non rilascia alcuna dichiarazione e non fornisce alcuna garanzia in merito a qualsiasi software e in particolare non riconosce alcuna garanzia, espressa o implicita, di commerciabilità o idoneità per uno scopo specifico. Novell, Inc. si riserva inoltre il diritto di modificare qualsiasi parte del software Novell in qualsiasi momento, senza alcun obbligo di notificare tali modifiche a qualsiasi persona fisica o giuridica.

Qualsiasi informazione tecnica o prodotto fornito in base a questo Contratto può essere soggetto ai controlli statunitensi relativi alle esportazioni e alla normativa sui marchi di fabbrica in vigore in altri paesi. L'utente si impegna a rispettare la normativa relativa al controllo delle esportazioni e a ottenere qualsiasi licenza o autorizzazione necessaria per esportare, riesportare o importare prodotti finali. L'utente si impegna inoltre a non esportare o riesportare verso entità incluse negli elenchi di esclusione delle esportazioni statunitensi o a qualsiasi paese sottoposto a embargo o che sostiene movimenti terroristici, come specificato nella legislazione statunitense in materia di esportazioni. L'utente accetta infine di non utilizzare i prodotti finali per utilizzi correlati ad armi nucleari, missilistiche o biochimiche. Per ulteriori informazioni sull'esportazione di software Novell, vedere la pagina Web sui servizi commerciali internazionali di Novell (http://www.novell.com/info/exports/). Novell non si assume alcuna responsabilità relativa al mancato ottenimento, da parte dell'utente, delle autorizzazioni di esportazione necessarie.

Novell, Inc. possiede i diritti di proprietà intellettuale relativa alla tecnologia incorporata nel prodotto descritto nel presente documento. In particolare, senza limitazioni, questi diritti di proprietà intellettuale possono comprendere uno o più brevetti USA elencati nella pagina Web relativa ai brevetti Novell (http://www.novell.com/company/legal/patents/) e uno o più brevetti aggiuntivi o in corso di registrazione negli Stati Uniti e in altri paesi.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
USA
www.novell.com

Documentazione online: per accedere alle ultime versioni della documentazione online di questo e altri prodotti Novell, visitare la pagina Web relativa alla documentazione di Novell (http://www.novell.com/documentation).

Marchi di fabbrica di Novell

Per informazioni sui marchi di fabbrica di Novell, vedere l'elenco di marchi di fabbrica e di servizio di Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiali di terze parti

Tutti i marchi di fabbrica di terze parti appartengono ai rispettivi proprietari.

Sommario

Informazioni sulla Guida

La presente *Guida dell'utente di Novell® ZENworks® Endpoint Security Client 3.5* è destinata all'utente finale e fornisce istruzioni sul funzionamento di Endpoint Security Client 3.5 per Windows* XP* e Windows 2000*.

Le informazioni della guida sono organizzate come segue:

Destinatari

È possibile inviarla a tutti i dipendenti dell'azienda per aiutarli a comprendere le modalità di utilizzo di Endpoint Security Client 3.5.

Feedback

È possibile inviare i propri commenti e suggerimenti relativi a questa guida e agli altri documenti forniti con questo prodotto. Utilizzare la funzionalità Commenti utente in fondo a ciascuna pagina della documentazione online oppure visitare la pagina Web per i commenti sulla documentazione di Novell (http://www.novell.com/documentation/feedback.html) e inserire i propri commenti.

Documentazione aggiuntiva

È disponibile ulteriore documentazione (nei formati PDF e HTML) relativa a ZENworks Endpoint Security Management e alla sua modalità di implementazione. Per ulteriore documentazione, visitare il sito Web relativo alla documentazione di ZENworks Endpoint Security Management 3.5 (http://www.novell.com/documentation/zesm35).

Convenzioni della documentazione

Nella documentazione di Novell, il simbolo maggiore di (>) viene utilizzato per separare le azioni di uno stesso passo di procedura e gli elementi in un percorso di riferimenti incrociati.

Un simbolo di marchio di fabbrica (®, ™, ecc.) denota un marchio di fabbrica Novell. L'asterisco * indica un marchio di fabbrica di terze parti.

Quando un nome di percorso può essere scritto con una barra rovesciata (\) per alcune piattaforme o con una barra (/) per altre piattaforme, verrà riportato con una barra rovesciata. Gli utenti di piattaforme che richiedono l'uso di barre (/) nei percorsi, ad esempio Linux*, dovranno utilizzare questo carattere e non la barra rovesciata.

Introduzione

1

Novell® ZENworks® Endpoint Security Management (ESM) è progettato per proteggere i dati aziendali attraverso uno strumento gestito a livello centrale denominato Endpoint Security Client. L'installazione di Endpoint Security Client 3.5 viene effettuata in computer aziendali in cui è presente Windows XP e Windows 2000 e consente la gestione di norme di sicurezza scritte e inviate attraverso il sistema di distribuzione e di gestione ESM. Ciò consente alle grosse imprese e alle aziende di piccole dimensioni di creare, distribuire, applicare e monitorare le norme di sicurezza sui computer all'interno e all'esterno del perimetro di sicurezza aziendale.

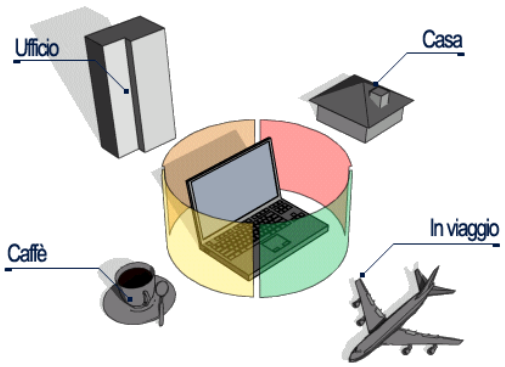
Per i computer in cui è installato Windows Vista e Windows 2008, consultare la *Guida dell'utente di ZENworks Endpoint Security Client 4.0*.

Le seguenti sezioni contengono informazioni aggiuntive:

1.1 Applicazione della sicurezza per i computer portatili

La sicurezza viene applicata sia a livello globale che a livello di ubicazione della rete. Ciascuna ubicazione elencata in una norma di sicurezza determina le autorizzazioni dell'utente in tale ambiente di rete e le impostazioni del firewall attivate. Le impostazioni del firewall determinano le porte, gli indirizzi e le applicazioni di rete autorizzati ad accedere alla rete, nonché la modalità di concessione di tale accesso.

Figura 1-1 *ESM regola le impostazioni di sicurezza in base all'ambiente di rete rilevato.*

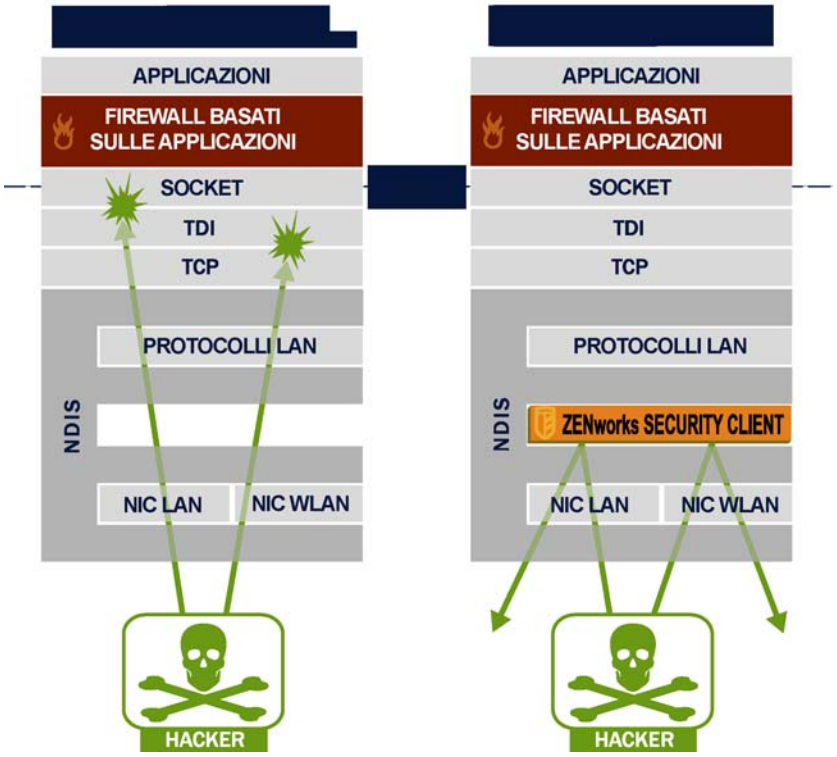


Una volta definiti gli ambienti di rete, le normali operazioni di Endpoint Security Client 3.5 vengono eseguite in modo invisibile all'utente. Talvolta è possibile che le misure di protezione di Endpoint Security Client 3.5 interrompano il normale funzionamento delle operazioni. In tali casi, vengono visualizzati messaggi e collegamenti ipertestuali che notificano all'utente le norme di sicurezza e le azioni intraprese per garantire la protezione, e che rimandano a ulteriori informazioni relative alla risoluzione del problema.

1.2 Protezione del firewall a livello di NDIS

Nell'ambito della sicurezza dei dispositivi mobili, ESM offre funzionalità avanzate rispetto alle tecnologie firewall tradizionali, che funzionano solo a livello applicativo oppure come driver firewall-hook. La sicurezza del client ESM è integrata nel driver Network Driver Interface Specification (NDIS) di ogni scheda di interfaccia di rete (NIC, Network Interface Card) e fornisce protezione immediata dal momento in cui il traffico entra nel computer. La Figura 1-2, “Efficienza del firewall a livello di NDIS”, a pagina 10 illustra le differenze tra ESM e i firewall a livello applicativo e i driver filtro.

Figura 1-2 *Efficienza del firewall a livello di NDIS*



Le decisioni relative alla sicurezza e le prestazioni di sistema sono ottimizzate quando le implementazioni di sicurezza funzionano al livello appropriato più basso dello stack di protocollo. Con Endpoint Security Client 3.5, il traffico non richiesto viene bloccato ai livelli inferiori dello stack del driver NDIS attraverso la tecnologia Adaptive Port Blocking (funzione SPI, Stateful Packet Inspection). Questo approccio protegge dagli attacchi basati su protocollo, inclusi le scansioni di porte non autorizzate e gli attacchi SYN Flood.

Per garantire la protezione dell'ambiente di sicurezza degli endpoint, si consiglia di eseguire tutte le procedure operative e di manutenzione illustrate nel presente documento.

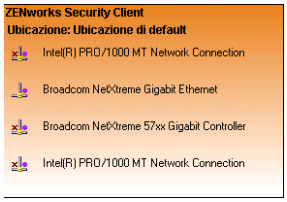
Panoramica di Endpoint Security Client 3.5

2

ZENworks® Security Client protegge i computer dagli attacchi ai dati a casa, in ufficio e in viaggio mediante l'applicazione delle norme di sicurezza create dall'amministratore aziendale di Endpoint Security Management (ESM). Le impostazioni del firewall assegnate alle ubicazioni individuali vengono automaticamente regolate in base al luogo in cui si trova l'utente: all'interno della rete aziendale, della rete domestica o di una rete pubblica o aperta se l'utente è in viaggio.

I livelli di sicurezza vengono applicati a diverse ubicazioni dell'utente e non richiedono esperienza o conoscenze in materia di sicurezza della rete, di configurazione delle porte, di file condivisi nascosti o di altri dettagli tecnici. Informazioni immediate sull'ubicazione e sull'impostazione del firewall in cui si trova Endpoint Security Client 3.5, nonché gli adattatori attivi o consentiti, sono disponibili semplicemente spostando il puntatore del mouse sull'icona della barra delle applicazioni per visualizzare le tecniche d'uso di Endpoint Security Client (vedere Figura 2-1).

Figura 2-1 *Tecniche d'uso di Endpoint Security Client*



Le seguenti sezioni contengono informazioni aggiuntive:

- Sezione 2.1, “Terminologia ESM”, a pagina 11
- Sezione 2.2, “Login a Endpoint Security Client 3.5”, a pagina 12

2.1 Terminologia ESM

Termini utilizzati di frequente in questa guida:

Ubicazioni: Le ubicazioni sono semplici definizioni che permettono agli utenti di identificare l'ambiente di rete in cui si trovano, forniscono impostazioni di sicurezza immediate (definite dall'amministratore) e possono consentire all'utente di salvare l'ambiente di rete e modificare le impostazioni del firewall applicate.

Ciascuna ubicazione è dotata di impostazioni di sicurezza univoche che impediscono l'accesso a determinati hardware e funzionalità di rete negli ambienti di rete più pericolosi, mentre concedono un accesso più ampio nel caso di ambienti affidabili. Le ubicazioni definiscono le seguenti informazioni:

- La frequenza con cui Endpoint Security Client 3.5 verifica la disponibilità di un aggiornamento delle norme in tale ubicazione
- Le autorizzazioni di gestione delle ubicazioni concesse a un utente
- Le impostazioni del firewall utilizzate in tale ubicazione

- L'hardware di comunicazione autorizzato alla connessione
- La modalità di gestione della connettività e della sicurezza Wi-Fi in tale ubicazione
- Il livello a cui all'utente è consentito utilizzare i dispositivi di memorizzazione estraibili (unità USB e schede di memoria) e le unità CD/DVD-RW
- Eventuali ambienti di rete che possono contribuire a definire l'ubicazione

Impostazioni del firewall: Le impostazioni del firewall controllano la connettività di tutte le porte di rete (1-65535), dei pacchetti di rete (ICMP, ARP e così via), degli indirizzi di rete (IP o MAC), nonché le applicazioni di rete (condivisione file, messaggistica istantanea e così via) autorizzate a connettersi alla rete quando è applicata l'impostazione. ESM comprende tre impostazioni di default per il firewall, che possono essere implementate in un'ubicazione. L'amministratore ESM può anche creare impostazioni firewall specifiche che non possono essere qui elencate.

- **Tutte adattive:** imposta tutte le porte di rete come Stateful (viene bloccato tutto il traffico di rete in entrata non richiesto e viene consentito tutto il traffico di rete in uscita). I pacchetti ARP e 802.1x sono autorizzati ed è consentita la connessione di tutte le applicazioni di rete.
- **Tutte aperte:** imposta tutte le porte di rete come aperte (viene consentito tutto il traffico di rete) e consente tutti i tipi di pacchetti. A tutte le applicazioni di rete è consentita la connessione di rete.
- **Tutte chiuse:** chiude tutte le porte di rete e limita tutti i tipi di pacchetti.

Adattatori: si riferisce ai tre adattatori di comunicazione che si trovano in genere in un endpoint:

- Adattatori per connessioni cablate (connessioni LAN)
- Adattatori per connessioni Wi-Fi (schede Wi-Fi PCMCIA e radio Wi-Fi incorporate).
- Adattatori per connessioni telefoniche (sia modem interni sia esterni)

Inoltre, si riferisce ad altro eventuale hardware per la comunicazione presente in un computer, ad esempio porte a infrarossi, Bluetooth*, FireWire*, seriali e parallele.

Dispositivi di memorizzazione: si riferisce ai dispositivi di memorizzazione esterni che si trovano in un endpoint e che possono comportare una minaccia alla sicurezza quando i dati vengono copiati su di essi o sono da essi introdotti. Le unità USB, le schede di memoria flash e SCSI PCMCIA, oltre alle unità Zip*, floppy, CDR esterne tradizionali e alle unità CD/DVD installate (incluse le unità CD-ROM, CD-R/RW, DVD e DVD R/RW) possono essere completamente bloccate, autorizzate oppure impostate sulla modalità di sola lettura in una singola ubicazione.

Ambienti di rete: un ambiente di rete è la raccolta dei servizi di rete e dei relativi indirizzi necessari per identificare un'ubicazione di rete (vedere Sezione 3.2.1, “Salvataggio di un ambiente di rete”, a pagina 16).

2.2 Login a Endpoint Security Client 3.5

Se si è membri del dominio aziendale, in Endpoint Security Client 3.5 vengono utilizzati nome utente e password di Windows* per eseguire il login al servizio di distribuzione norme (non viene visualizzata alcuna finestra popup). Se non si è membri del dominio in cui è ospitato il servizio di distribuzione delle norme, viene richiesto di immettere il nome utente e la password per tale dominio (vedere Figura 2-2).

Figura 2-2 *Login di Endpoint Security Client 3.5*

Immettere il nome utente e la password per il dominio, quindi fare clic su *OK*.

Nota: non è necessario eseguire il login quando Endpoint Security Client 3.5 è in esecuzione come applicazione non gestita. L'amministratore ESM utilizza un metodo diverso per distribuire le norme agli utenti non gestiti.

Utilizzo di Endpoint Security Client 3.5

3

Nelle seguenti sezioni vengono riportate ulteriori informazioni sulle azioni che è possibile eseguire con Endpoint Security Client 3.5, l'applicazione per l'utente finale di Novell® ZENworks® Endpoint Security:

Nota: Le azioni riportate sopra possono essere limitate dall'amministratore in qualsiasi ubicazione.

3.1 Alternanza tra ambienti di rete

È possibile che ciascuna rete utilizzata da un utente finale necessiti di misure di sicurezza diverse. Endpoint Security Client 3.5 fornisce sicurezza e protezione nelle ubicazioni identificate dalle connessioni di rete disponibili. Endpoint Security Client 3.5 rileva i parametri dell'ambiente di rete e passa all'ubicazione appropriata, applicando i livelli di protezione necessari in base alle norme di sicurezza correnti.

Le informazioni sull'ambiente di rete sono memorizzate o preimpostate all'interno di un'ubicazione. Ciò consente il passaggio automatico di Endpoint Security Client 3.5 a un'ubicazione nel momento in cui vengono rilevati i parametri relativi all'ambiente di rete.

- **Ambienti memorizzati:** definiti dall'utente (vedere Sezione 3.2.1, “Salvataggio di un ambiente di rete”, a pagina 16).
- **Ambiente preimpostato:** definito dall'amministratore ESM aziendale attraverso una norma di sicurezza pubblicata.

Quando l'utente si trova in un nuovo ambiente di rete, il client esegue il confronto dell'ambiente di rete rilevato con qualsiasi valore memorizzato e preimpostato nelle norme di sicurezza. Se viene trovata una corrispondenza, viene attivata l'ubicazione assegnata. Se l'ambiente rilevato non è identificabile come memorizzato o preimpostato, il client attiva l'ubicazione Sconosciuta di default.

L'ubicazione Sconosciuta comprende le seguenti preimpostazioni:

- Modifica ubicazioni = Consentito
- Modifica impostazioni firewall = Non consentito
- Salva ubicazione = Non consentito

- Aggiorna norme = Consentito
- Impostazioni firewall di default = Tutte adattive

I tre tipi di adattatori, per connessioni Wi-Fi, cablate e telefoniche, sono consentiti nell'ubicazione Sconosciuta. Ciò consente al computer di interfacciarsi al proprio ambiente di rete attraverso una periferica e di tentare l'associazione a una norma di ubicazione come descritto sopra.

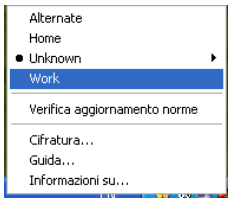
3.2 Modifica delle ubicazioni

All'avvio, Endpoint Security Client 3.5 attiva l'ubicazione Sconosciuta. Quindi, cerca di rilevare l'ambiente di rete corrente e di modificare l'ubicazione automaticamente. Se l'ambiente di rete non viene riconosciuto o se non è stato preimpostato o salvato (vedere Sezione 3.2.1, “Salvataggio di un ambiente di rete”, a pagina 16), è necessario modificare manualmente l'ubicazione.

Se non è possibile eseguire i seguenti passaggi, è possibile che la modifica manuale delle ubicazioni non sia autorizzata dall'amministratore di ZENworks Endpoint Security.

Per modificare un'ubicazione:

1. Fare clic con il pulsante destro del mouse sull'icona di *Endpoint Security Client* sulla barra delle applicazioni per visualizzare un menu di opzioni.



2. Scegliere l'ubicazione appropriata.

3.2.1 Salvataggio di un ambiente di rete

Per consentire la modifica automatica delle ubicazioni in Endpoint Security Client 3.5, è necessario che un ambiente di rete venga preimpostato nelle norme di sicurezza oppure salvato dall'utente finale. Quando si salva un ambiente di rete, i parametri della rete vengono salvati nell'ubicazione corrente e il passaggio all'ubicazione avviene in modo automatico la volta successiva in cui l'utente viene a trovarsi in tale ambiente. In un ambiente di rete Wi-Fi, Endpoint Security Client 3.5 stabilisce la connessione al singolo punto di accesso selezionato tramite la tecnologia LockOn™.

Per salvare un ambiente:

1. Fare clic con il pulsante destro del mouse sull'icona di *Endpoint Security Client* sulla barra delle applicazioni per visualizzare il menu.
2. Scegliere l'ubicazione a cui si desidera passare.
3. Fare clic con il pulsante destro del mouse sull'icona di *Endpoint Security Client*, passare il mouse sopra l'ubicazione corrente per visualizzare il sottomenu, quindi scegliere Salva ambiente di rete per salvare l'ambiente.

Se l'ambiente di rete selezionato è stato salvato in un'ubicazione precedente, viene richiesto se si desidera salvare la nuova ubicazione. Scegliere *Sì* per salvare l'ambiente nell'ubicazione corrente ed eliminarlo dall'ubicazione precedente, oppure scegliere *No* per lasciare l'ambiente nell'ubicazione precedente.

Nota: La funzione *Salva ambiente di rete* può essere limitata dall'amministratore ESM in qualsiasi ubicazione.

È possibile salvare ambienti di rete aggiuntivi in un'ubicazione. Ad esempio, se una norma corrente include un'ubicazione denominata Aeroporto, ogni aeroporto visitato dall'utente mobile può essere salvato come ambiente di rete per questa ubicazione. In questo modo, ogni volta che l'utente ritorna in un ambiente salvato di tipo "Aeroporto", viene automaticamente impostata l'ubicazione Aeroporto.

3.2.2 Salvataggio di un ambiente Wi-Fi

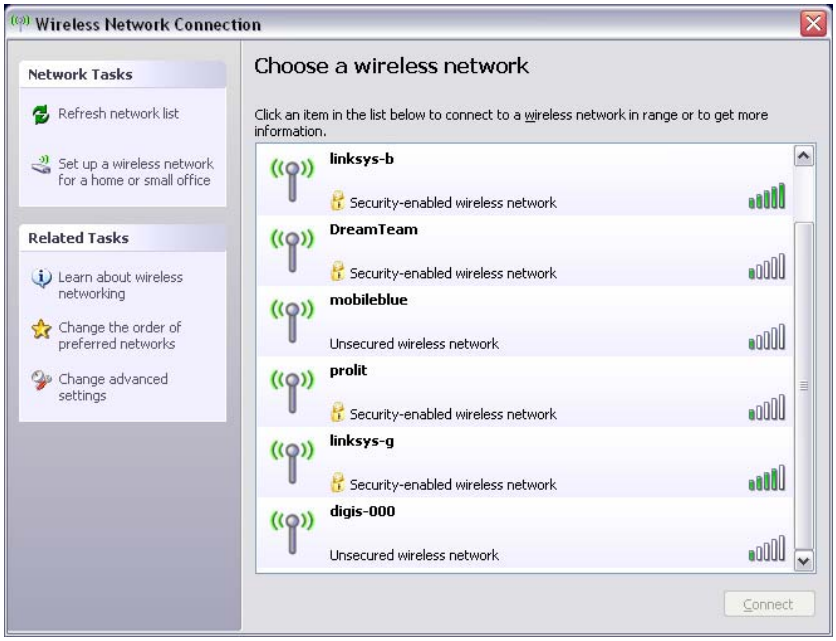
Quando si attiva un adattatore Wi-Fi, è possibile che risultino disponibili dozzine di punti di accesso. L'adattatore Wi-Fi può connettersi dapprima a un singolo punto di accesso; tuttavia, se in sua prossimità sono disponibili troppi punti di accesso, è possibile che la connessione al punto di accesso associato venga interrotta e che il gestore della connessione wireless richieda all'adattatore di passare al punto di accesso con il segnale più forte. In questo caso, l'attività di rete corrente viene interrotta, obbligando spesso l'utente a inviare nuovamente determinati pacchetti e a rieseguire la connessione della VPN alla rete aziendale.

Quando si salva un punto di accesso come parametro di ambiente di rete in un'ubicazione, viene stabilita la connessione a tale punto di accesso e la connettività non viene persa fino a quando non ci si allontana fisicamente dal punto di accesso. Quando ci si trova nuovamente in sua prossimità, l'adattatore viene automaticamente associato a tale punto, l'ubicazione viene modificata e tutti gli altri punti di accesso non sono più visibili attraverso il software di gestione delle connessioni wireless.

Per salvare un ambiente Wi-Fi:

1 Avviare il software per la gestione delle connessioni e selezionare il punto di accesso desiderato.

Nota: È possibile che l'ubicazione abbia priorità rispetto al software per la gestione delle connessioni se le norme di sicurezza di ESM sono impostate per la gestione della connettività wireless.



2 Immettere eventuali informazioni sulla sicurezza necessarie (WEP o un'altra chiave di sicurezza), quindi fare clic su *Connetti*.

3 Per salvare l'ambiente, completare le operazioni descritte al passaggio Sezione 3.2.1, “Salvataggio di un ambiente di rete”, a pagina 16.

3.2.3 Rimozione di un ambiente salvato

Per rimuovere un ambiente di rete salvato da un'ubicazione:

1 Fare clic con il pulsante destro del mouse sull'icona *Endpoint Security Client* sulla barra delle applicazioni per visualizzare il menu.

2 Selezionare l'ubicazione appropriata.

3 Fare clic con il pulsante destro del mouse sull'icona *Endpoint Security Client*, quindi selezionare l'ubicazione corrente per visualizzare il sottomenu.

4 Fare clic su *Azzera ambienti di rete* per eliminare l'ambiente.

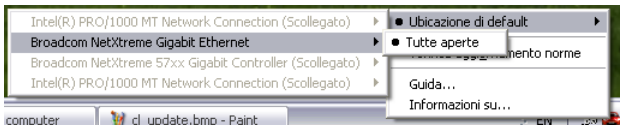
Nota: Verranno rimossi tutti gli ambienti di rete salvati per questa ubicazione.

3.3 Modifica delle impostazioni del firewall

A ogni ubicazione è possibile assegnare più impostazioni del firewall. Modificando le impostazioni del firewall si possono chiudere o aprire porte di rete e consentire o impedire certi tipi di connessioni di rete in una determinata ubicazione.

Per modificare le impostazioni del firewall:

1. Fare clic con il pulsante destro del mouse sull'icona *Endpoint Security Client* sulla barra delle applicazioni per visualizzare il menu.
2. Passare il mouse sopra l'ubicazione corrente per visualizzare il sottomenu, quindi fare clic sulla selezione per modificare l'impostazione del firewall.



Nota: Il numero di impostazioni del firewall disponibili in un'ubicazione è determinato dalle norme.

3.4 Cifratura dei dati

Se l'attivazione è determinata dalle norme, Endpoint Security Client 3.5 gestisce la cifratura dei file collocati in una directory specifica nell'endpoint e in dispositivi di memorizzazione estraibili.

Di seguito vengono riportate le istruzioni per l'utilizzo di ZENworks Security Client nell'endpoint.

- Sezione 3.4.1, “Gestione dei file su dischi fissi”, a pagina 19
- Sezione 3.4.2, “Gestione dei file nei dispositivi di memorizzazione estraibili”, a pagina 19

3.4.1 Gestione dei file su dischi fissi

Per dischi fissi si intendono tutte le unità disco rigido installate sul computer e le loro eventuali partizioni. Ogni disco fisso nell'endpoint dispone di una cartella `File cifrati` collocata nella directory radice. Tutti i file collocati in questa cartella vengono cifrati utilizzando la chiave di cifratura corrente. Solo gli utenti autorizzati possono decifrare questi file.

Quando si salva un file, selezionare la cartella `File cifrati` dalle cartelle disponibili nell'unità desiderata.

3.4.2 Gestione dei file nei dispositivi di memorizzazione estraibili

Per dispositivi di memorizzazione estraibili si intendono tutti i dispositivi di memorizzazione "connessi" a un computer. Essi includono, in via esemplificativa, le unità USB, le schede di memoria flash e PCMCIA, le unità Zip, floppy e CDR esterne tradizionali, le fotocamere digitali con capacità di memorizzazione e i lettori MP3.

Quando si esegue ZENworks Endpoint Security, i file memorizzati in questi dispositivi vengono cifrati nel momento in cui il sistema operativo o l'utente vi accede. I file copiati sul dispositivo vengono immediatamente cifrati. Se il dispositivo di memorizzazione estraibile è connesso a un computer non gestito dal sistema ZENworks Endpoint Security, i file rimangono cifrati e non possono essere decifrati.

La cifratura dei file viene eseguita quando si inserisce il dispositivo estraibile (vedere “Procedura per non eseguire la cifratura del dispositivo” a pagina 21). Tuttavia, i file aggiunti a un dispositivo di memorizzazione estraibile cifrato su un altro computer devono essere cifrati manualmente.

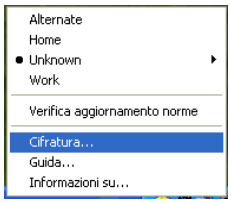
Le seguenti sezioni contengono informazioni aggiuntive:

- “Cifratura dei file” a pagina 20
- “Procedura per non eseguire la cifratura del dispositivo” a pagina 21
- “Utilizzo della cartella dei file condivisi” a pagina 21
- “Modifica della password dei file nella cartella File condivisi” a pagina 21

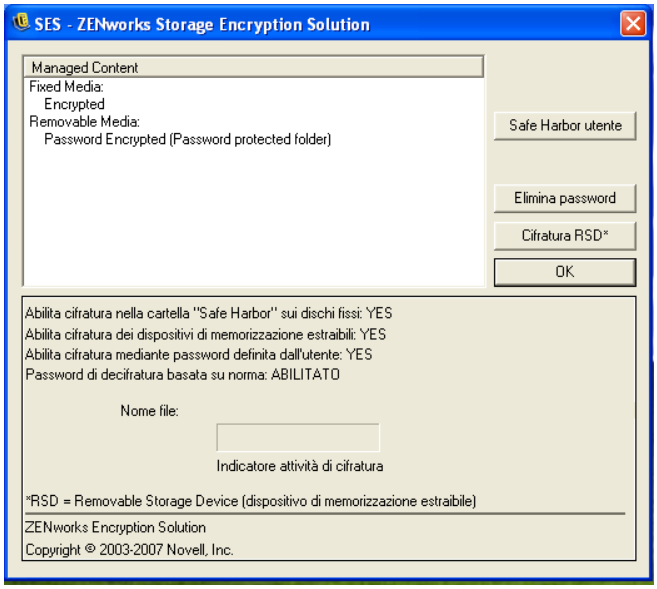
Cifratura dei file

Per cifrare i file aggiunti su un dispositivo di memorizzazione estraibile:

1. Inserire il dispositivo di memorizzazione nella porta appropriata del computer in uso.
2. Fare clic con il pulsante destro del mouse sull'icona *Endpoint Security Client* sulla barra delle applicazioni.
3. Scegliere·*Cifratura* dal menu.



4. Fare clic su *Cifratura RSD*. Verranno cifrati tutti i file sul dispositivo di memorizzazione estraibile con la chiave di cifratura corrente.

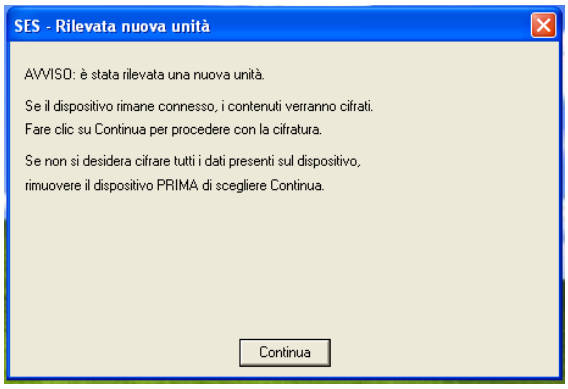


Il tempo necessario per l'esecuzione della cifratura dei file dipende dalla quantità di dati memorizzati sul dispositivo.

Procedura per non eseguire la cifratura del dispositivo

Quando si inserisce un dispositivo di memorizzazione estraibile, viene richiesto di scegliere se cifrare l'unità o se procedere alla sua rimozione senza cifrarne tutti i file.

Figura 3-1 *Avviso relativo alla cifratura all'inserimento di un nuovo dispositivo*



Per impedire la cifratura, rimuovere l'unità prima di fare clic su *Continua* . Fare clic su *Continua* per cifrare l'unità o per chiudere la finestra dopo aver rimosso il dispositivo.

Utilizzo della cartella dei file condivisi

Se previsto dalle norme, viene creata una cartella `File condivisi` su qualsiasi dispositivo di memorizzazione estraibile collegato al computer che esegue ZENworks Endpoint Security. I file di questa cartella sono accessibili dagli utenti all'interno di altri gruppi di norme mediante l'utilizzo di una password creata dall'utente. Gli utenti che utilizzano computer su cui non viene eseguito ZENworks Endpoint Security possono accedere a questi file utilizzando l'utility di decifratura dei file di ZENworks e immettendo la password.

Nota: Le password vengono eliminate ad ogni riavvio del computer. Dopo ogni riavvio, viene richiesta la password per accedere ai file aggiunti alla cartella `File condivisi`.

Per utilizzare la cartella `File condivisi`:

1. Spostare o salvare un file nella cartella `File condivisi`.
2. Quando richiesto, immettere una password e confermarla.
3. Immettere un suggerimento per la password.

Gli utenti di ZENworks Endpoint Security non gestiti dalle norme in uso possono accedere a questi file immettendo le password. Per accedere ai file, gli utenti non gestiti da ZENworks Endpoint Security avranno bisogno dell'utility di decifratura dei file di ZENworks e della password.

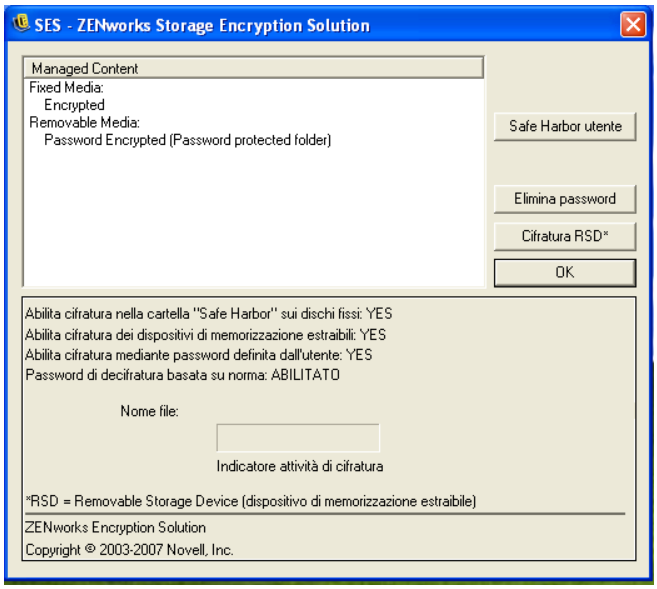
Modifica della password dei file nella cartella File condivisi

Per modificare le password dei file aggiunti alla cartella `File condivisi` è possibile utilizzare il comando Cifratura.

Nota: L'utilizzo di questo comando non modifica le password esistenti, ma solo la password dei file futuri.

Per modificare la password:

1. Inserire il dispositivo di memorizzazione nella porta appropriata del computer in uso.
2. Fare clic con il pulsante destro del mouse sull'icona *Endpoint Security Client* sulla barra delle applicazioni.
3. Scegliere *Cifratura* dal menu.
4. Fare clic su *Elimina password*.



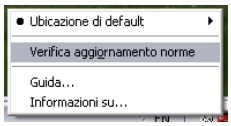
5. Trascinare un file nella cartella `File condivisi`, quindi immettere la nuova password e il relativo suggerimento.

Per accedere a tutti i nuovi file aggiunti alla cartella sarà necessario utilizzare la nuova password.

3.5 Aggiornamento delle norme

Agli utenti gestiti vengono rilasciate le nuove norme di sicurezza man mano che vengono pubblicate. In Endpoint Security Client gli aggiornamenti vengono automaticamente ricevuti a intervalli definiti dall'amministratore ESM. Tuttavia, l'utente gestito può verificare la disponibilità degli aggiornamenti delle norme al momento dell'utilizzo di una nuova ubicazione.

1. Fare clic con il pulsante destro del mouse sull'icona *Endpoint Security Client* sulla barra delle applicazioni per visualizzare il menu.
2. Scegliere *Controllo disponibilità aggiornamenti norma*.



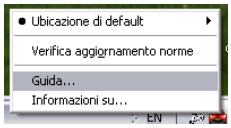
Nota: gli aggiornamenti automatici e la verifica degli aggiornamenti delle norme non sono funzioni disponibili quando Endpoint Security Client 3.5 è in esecuzione come applicazione non gestita. L'amministratore ESM utilizza un metodo diverso per distribuire gli aggiornamenti delle norme a tali utenti.

In Endpoint Security Client 3.5 viene visualizzato un messaggio di notifica se le norme sono state aggiornate.

Nota: In alcuni casi, quando si alternano le schede di accesso wireless, viene visualizzato il messaggio di `avvenuto aggiornamento delle norme`. In realtà, le norme non sono state aggiornate. Il messaggio indica che Endpoint Security Client 3.5 sta semplicemente confrontando il dispositivo con le eventuali limitazioni previste dalle norme correnti.

3.6 Visualizzazione della Guida

1. Fare clic con il pulsante destro del mouse sull'icona *Endpoint Security Client* sulla barra delle applicazioni per visualizzare il menu.
2. Scegliere *?*.



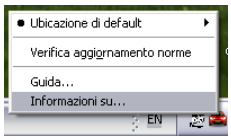
3.7 Password prioritaria

Le interruzioni di produttività che si possono verificare per le restrizioni associate alla connessione, al software o alle pen drive sono presumibilmente causate dalle norme di sicurezza applicate da Endpoint Security Client 3.5. Il cambiamento di ubicazione o delle impostazioni firewall in genere rimuove tali restrizioni e ripristina la funzionalità interrotta. Tuttavia, in alcuni casi è possibile che le restrizioni siano implementate in modo da interessare tutte le ubicazioni e tutte le impostazioni del firewall. In tal caso, è necessario annullare temporaneamente le restrizioni per poter consentire l'esecuzione delle operazioni.

Endpoint Security Client 3.5 dispone della funzione Password prioritaria, che consente di disattivare temporaneamente le norme di sicurezza correnti e di eseguire l'attività necessaria. L'amministratore della sicurezza distribuisce una chiave password monouso solo quando necessario e deve essere informato di qualsiasi problema relativo alle norme di sicurezza. Una volta scaduto il limite di tempo della chiave password, vengono ripristinate le norme di sicurezza che proteggono l'endpoint Anche il riavvio dell'endpoint consente il ripristino delle impostazioni di sicurezza.

Per attivare la password prioritaria:

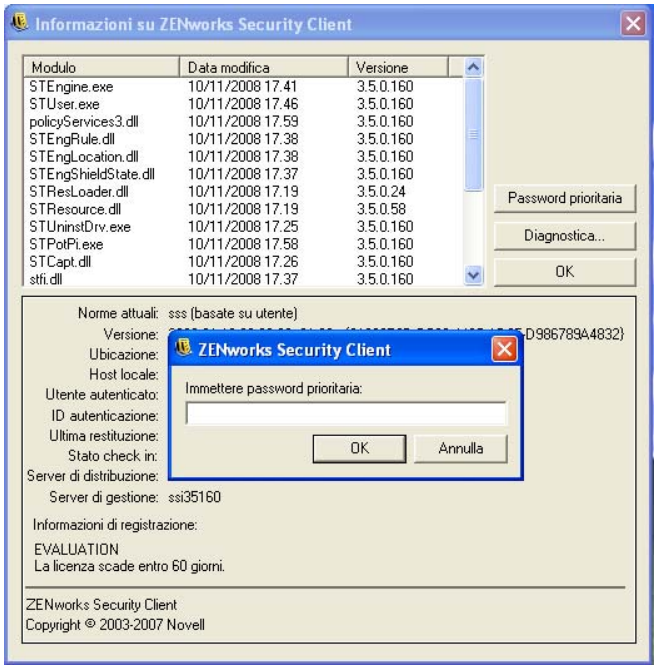
1. Rivolgersi all'amministratore ESM dell'azienda per ottenere la chiave password.
2. Fare clic con il pulsante destro del mouse sull'icona *Endpoint Security Client* sulla barra delle applicazioni per visualizzare il menu, quindi fare clic su *Informazioni su*.



3 Fare clic su *Password prioritaria* per visualizzare la finestra della password.

Nota: Se il pulsante *Password prioritaria* non viene visualizzato in questa schermata, le norme di sicurezza correnti non dispongono di una password prioritaria.

Figura 3-2 *Finestra Password*



4 Digitare la chiave password fornita dall'amministratore di ZENworks Endpoint Security.

5 Fare clic su *OK*. Le norme correnti verranno sostituite con le norme di default Tutte aperte per il periodo di tempo designato.

Facendo clic su *Carica norme* (che sostituisce il pulsante *Password prioritaria*) nella finestra *Informazioni su* vengono ripristinate le norme precedenti. Se l'amministratore ha aggiornato le norme per risolvere eventuali problemi esistenti, occorre invece utilizzare *Verifica aggiornamento norme* per scaricare immediatamente le nuove norme.

3.8 Diagnostica

Novell fornisce strumenti di diagnostica che consentono all'amministratore di risolvere i problemi relativi a Endpoint Security Client 3.5. L'amministratore ZENworks Endpoint Security assisterà gli utenti in tutte le fasi del processo di diagnostica.