AUTHORIZED DOCUMENTATION

Guida della console di gestione

August 1, 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

Utilizzo della console di ZENworks Endpoint Security Management

1

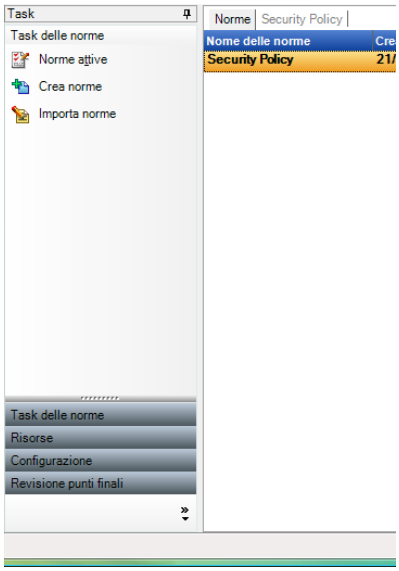
La console di gestione è il punto di accesso e di controllo centrale del servizio Novell® ZENworks® Endpoint Security Management.

Per avviare la finestra di login della console di gestione, fare clic su > Start*Programmi* > *Novell* > *Console di gestione ESM* > *Console di gestione*. Eseguire il login alla console specificando il nome e la password dell'amministratore. Il nome utente immesso deve corrispondere a un utente autorizzato nel servizio di gestione (vedere Sezione 1.3, “Utilizzo Impostazioni autorizzazioni”, a pagina 10).

Nota: Si consiglia di chiudere o ridurre a icona la console quando non è in uso.

1.1 Utilizzo della barra delle applicazioni

La barra presente sul lato sinistro consente l'accesso ai task della console di gestione. Qualora la barra non sia visibile, fare clic sul pulsante *Task* sul lato sinistro della console.



Le sezioni seguenti contengono ulteriori informazioni sui task che è possibile eseguire utilizzando la barra delle applicazioni:

- Sezione 1.1.1, “Task norme”, a pagina 8
- Sezione 1.1.2, “Risorse”, a pagina 8
- Sezione 1.1.3, “Configurazione”, a pagina 8
- Sezione 1.1.4, “Revisione dei punti finali”, a pagina 8

1.1.1 Task norme

La funzione principale della console di gestione consiste nel creare e applicare norme di sicurezza ai dispositivi dei punti finali gestiti. I task delle norme guidano l'amministratore nella creazione e la modifica delle norme di sicurezza utilizzate da ZENworks® Security Client per applicare la sicurezza gestita centralmente a ciascun dispositivo di punto finale.

I task delle norme includono quanto segue:

- **Norme attive:** Consente di visualizzare un elenco di norme correnti che è possibile rivedere e modificare. Fare clic sulle norme per aprirle.
- **Crea norme:** Consente di avviare la procedura guidata per le nuove norme con cui è possibile creare nuove norme di sicurezza
- **Importa norme:** Consente di visualizzare la finestra di dialogo Importa norme da cui è possibile importare le norme create con altri servizi di gestione. Per ulteriori informazioni, consultare Sezione 2.3.1, “Importazione delle norme”, a pagina 106.

Facendo clic su un qualsiasi task delle norme, la barra delle applicazioni viene ridotta a icona. Per riaprirla, fare clic sul pulsante *Task* a sinistra.

Vedere Capitolo 2, “Creazione e distribuzione delle norme di sicurezza”, a pagina 43 per ulteriori informazioni sui task delle norme e sulle modalità di creazione e di gestione delle norme di sicurezza.

1.1.2 Risorse

Nell'elenco dei task Risorse è possibile visualizzare il supporto tecnico e le risorse della Guida disponibili:

- **Rivolgersi al supporto tecnico:** Consente di avviare un browser e di visualizzare la pagina relativa ai contatti e agli uffici Novell®.
- **Supporto tecnico online:** Consente di avviare un browser e di visualizzare la pagina relativa alla formazione e al supporto Novell.
- **Guida della console di gestione:** Consente di avviare la guida online di ZENworks® Endpoint Security Management.

1.1.3 Configurazione

La finestra di configurazione del servizio di gestione fornisce i controlli sia per l'infrastruttura del server ZENworks® Endpoint Security Management che per il monitoraggio dei servizi di directory aziendali aggiuntivi. Per ulteriori informazioni, vedere Sezione 1.4, “Utilizzo della finestra Configurazione”, a pagina 14. Questo controllo non è disponibile quando è in esecuzione la console di gestione autonoma. Per ulteriori informazioni, consultare la *Guida all'installazione di ZENworks Endpoint Security Management*.

1.1.4 Revisione dei punti finali

La finestra Revisione punti finali consente di accedere alle funzioni di generazione rapporti e avvisi di ZENworks® Endpoint Security Management.

Generazione di rapporti: La generazione dei rapporti è un'attività critica nell'ambito della valutazione e dell'implementazione di norme di sicurezza avanzate. È possibile accedere ai rapporti attraverso la console di gestione facendo clic su *Rapporti* Le informazioni sulla sicurezza dei punti finali richiamate e segnalate, sono anche completamente configurabili e richiamabili per dominio, gruppo o singolo utente. Per ulteriori informazioni, consultare Sezione 1.6, “Utilizzo di Generazione rapporti”, a pagina 27.

Avvisi: Il monitoraggio degli avvisi·garantisce la segnalazione nella console di gestione di qualsiasi tentativo di compromissione delle norme di sicurezza aziendali. Gli avvisi informano l'amministratore di ZENworks Endpoint Security Management di eventuali problemi e gli consentono di intraprendere azioni correttive appropriate. È possibile configurare per intero il dashboard degli avvisi, in modo da poter controllare quando e con quale frequenza vengano attivati. Per ulteriori informazioni, consultare Sezione 1.5, “Utilizzo del monitoraggio degli avvisi”, a pagina 24.

1.2 Utilizzo della barra dei menu

La barra dei menu di ZENworks® Endpoint Security Management consente di accedere a tutte le funzioni della console di gestione

Sono disponibili le seguenti opzioni:

- **File:** Utilizzare il menu File per creare e gestire le norme di sicurezza.
  - **Crea nuove norme:** Consente di avviare la procedura guidata per le nuove norme con cui creare nuove norme di sicurezza.
  - **Aggiorna elenco norme:** Consente di aggiornare l'elenco delle norme per visualizzare tutte le norme attive.
  - **Norme di cancellazione:** Consente di cancellare le norme selezionate.
  - **Importa norme:** Consente di importare le norme nella console di gestione.
  - **Esporta norme:** Consente di esportare le norme e il file `setup.sen` richiesto in una posizione specificata all'esterno del database del servizio di gestione.
  - **Esci:** Consente di chiudere il software della console di gestione e di eseguire il logout dell'utente.
- **Strumenti:** Utilizzare il menu Strumenti per controllare la configurazione del servizio di gestione, chiavi di cifratura e autorizzazioni.
  - **Configurazione:** Consente di aprire la finestra Configurazione.
  - **Esportazione delle chiavi di cifratura:** Consente di aprire la finestra di dialogo Esporta chiavi di cifratura, in cui vengono specificate le chiavi che si desidera esportare e la password.
  - **Importazione delle chiavi di cifratura:** Consente di aprire la finestra di dialogo Importa chiavi di cifratura, in cui vengono specificate le chiavi che si desidera importare e la password.
  - **Genera nuova chiave:** Consente di generare la chiave di cifratura da utilizzare per applicare la protezione dei dati.
  - **Autorizzazioni:** Consente di aprire la finestra Autorizzazioni.

- **Visualizza:** Utilizzare il menu Visualizza per eseguire i task delle norme principali senza utilizzare la barra delle applicazioni.
  - **Norme:** Consente di passare alla visualizzazione delle norme quando queste sono aperte.
  - **Norme attive:** Consente di visualizzare l'elenco delle norme.
  - **Avvisi:** Consente di visualizzare il dashboard Avvisi.
  - **Generazione di rapporti:** Consente di visualizzare il dashboard Generazione rapporti.
- **Guida:** Consente di visualizzare lo strumento Guida alla console di gestione e la finestra di dialogo Informazioni:
  - **Guida:** Consente di avviare la Guida online della console di gestione che assiste nella creazione di norme e in tutti i task della console di gestione. È anche possibile accedere alla Guida premendo il tasto F1sul pannello.
  - **Informazioni sulla console di gestione:** Avvia la finestra Informazioni su, in cui è possibile visualizzare il tipo di installazione (ZENworks Endpoint Security Management o UWS) e il numero di versione corrente della console di gestione. Inoltre, in questa finestra viene immessa la chiave di licenza se l'acquisto è stato effettuato dopo l'installazione.

1.3 Utilizzo Impostazioni autorizzazioni

Impostazioni autorizzazioni si trova nel menu Strumenti e possono accedervi solo l'amministratore principale del servizio di gestione o altri amministratori da questi espressamente autorizzati. Il controllo non è disponibile quando è in esecuzione la console di gestione autonoma.

Le impostazioni di autorizzazione definiscono gli utenti o gruppi di utenti autorizzati ad accedere alle impostazioni di Console di gestione, Autorizzazioni amministrative o Destinatari pubblicazione.

Durante l'installazione del server di gestione, nel modulo di configurazione viene immesso un nome di amministratore o di conto risorsa per l'utente risorsa (consultare la *Guida all'installazione di ZENworks Endpoint Security Management*). Una volta superato il test e dopo aver salvato le informazioni dell'utente, a quest'ultimo vengono automaticamente concesse tutte le autorizzazioni.

Al termine dell'installazione della console di gestione, l'utente risorsa sarà l'unico a disporre di autorizzazioni complete, sebbene tutti i gruppi di utenti inseriti nel dominio siano autorizzati ad accedere alla console di gestione. È opportuno che l'utente risorsa impedisca l'accesso a tutti i gruppi o utenti che non hanno necessità di tale privilegio. L'utente risorsa può impostare autorizzazioni aggiuntive per gli utenti designati.

Le autorizzazioni vengono recuperate dalla tabella Autorizzazione all'avvio della console di gestione. Tali autorizzazioni indicano alla console se l'utente dispone dei diritti per eseguire il login alla console, creare o cancellare norme, modificare le impostazioni delle autorizzazioni, nonché se può pubblicare le norme e per quali destinatari.

Sono disponibili le seguenti impostazioni di accesso:

- **Accesso alla console di gestione:** L'utente può visualizzare norme e componenti, nonché modificare norme esistenti. Gli utenti che godono solo di questo privilegio non possono aggiungere o cancellare norme; le opzioni di pubblicazione e di autorizzazioni non sono disponibili.
- **Pubblica norme:** L'utente può pubblicare norme solo per utenti o gruppi assegnati.
- **Modifica autorizzazioni:** L'utente può accedere alle impostazioni delle autorizzazioni e modificarle per altri utenti già definiti, oppure concedere autorizzazioni a nuovi utenti.

- **Crea norme:** l'utente può creare nuove norme nella console di gestione.
- **Cancellare le norme:** L'utente può cancellare le norme nella console di gestione.

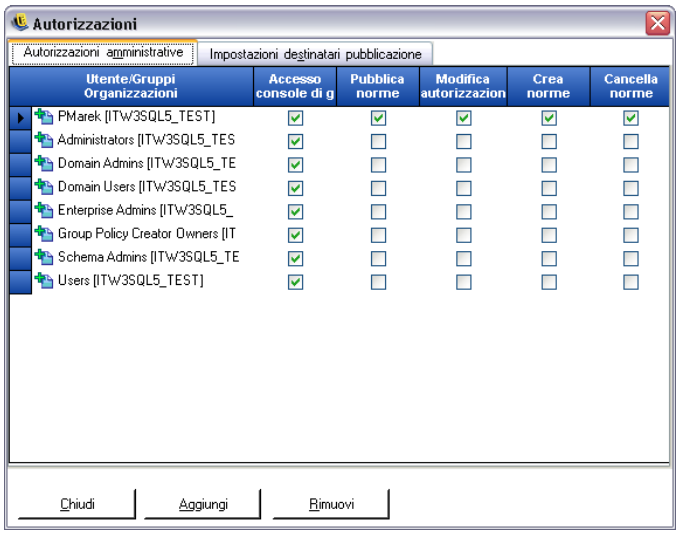
Nota: Per motivi di sicurezza, si consiglia di concedere le autorizzazioni di modifica e di cancellazione delle norme solo all'utente risorsa o a un numero limitato di amministratori.

1.3.1 Autorizzazioni amministrative

Per configurare le autorizzazioni amministrative:

1 Fare clic su *Strumenti* > *Autorizzazioni*.

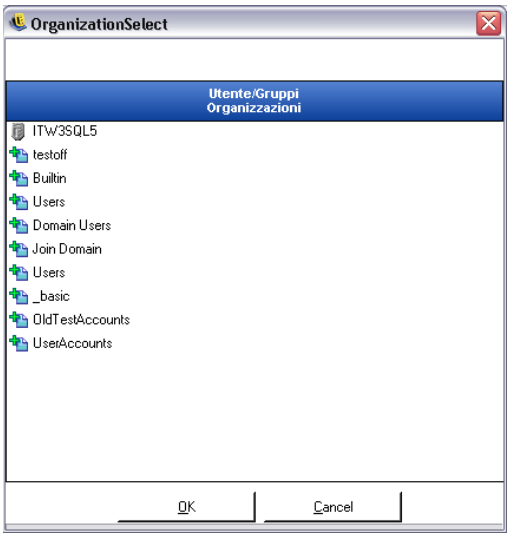
Vengono visualizzati i gruppi associati a questo dominio.



Nota: Per default, tutti i gruppi sono autorizzati ad accedere alla console di gestione, ma non sono in grado di eseguire i task delle norme. L'accesso alla console può essere rimosso deselezionando l'autorizzazione.

2 Per caricare utenti o gruppi in questo elenco:

2a Fare clic sul pulsante *Aggiungi* nella parte inferiore della schermata.



2b Selezionare gli utenti o i gruppi appropriati dall'elenco. Per selezionare più utenti, sceglierli individualmente tenendo premuto il tasto CTRL; per selezionarli in serie, scegliere il primo utente, tenere premuto il tasto Maiusc, quindi selezionare l'ultimo utente.

2c Al termine, scegliere *OK*.

3 Assegnare una (o tutte) le autorizzazioni agli utenti o gruppi disponibili.

Per rimuovere un utente o un gruppo selezionato, selezionarne il nome, quindi fare clic su *Rimuovi*. Il nome selezionato verrà riportato indietro nella Tabella organizzazione.

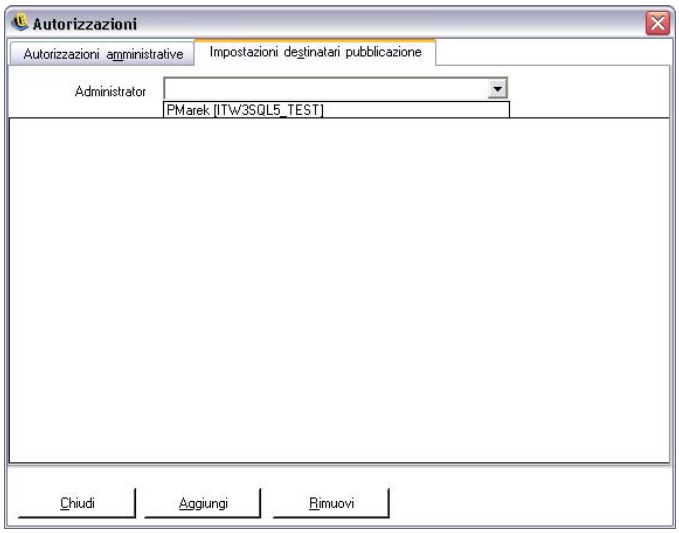
1.3.2 Impostazioni destinatari pubblicazione

Agli utenti o ai gruppi autorizzati per i quali è selezionata l'opzione *Pubblica norme* devono essere assegnati utenti o gruppi destinatari della pubblicazione.

Per impostare Impostazioni destinatari pubblicazione:

1 Fare clic sulla scheda *Impostazioni destinatari pubblicazione*.

2 Selezionare dall'elenco a discesa gli utenti o i gruppi cui è stata concessa l'autorizzazione di pubblicazione.



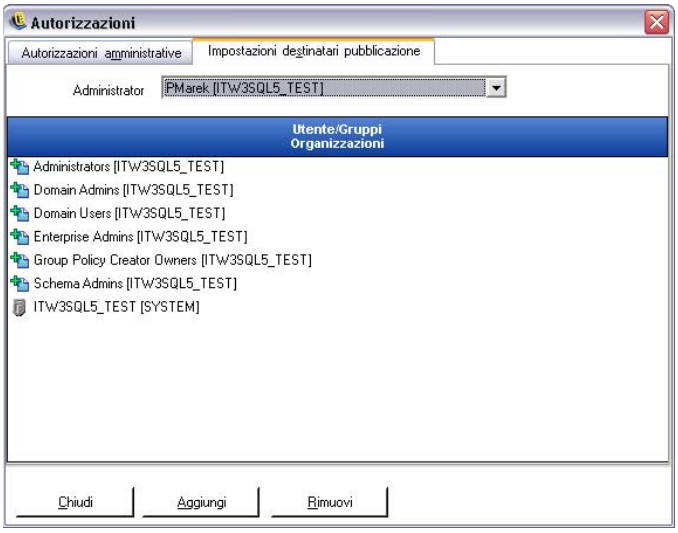
3 Assegnare utenti o gruppi a questo utente/gruppo procedendo come segue:

3a Per visualizzare la Tabella organizzazione, fare clic sul pulsante *Aggiungi* nella parte inferiore della schermata.

3b Selezionare gli utenti o i gruppi appropriati dall'elenco. Per selezionare più utenti, è possibile utilizzare i tasti CTRL e Maiusc.

3c Dopo aver selezionato tutti gli utenti o gruppi, fare clic sul pulsante *OK* per aggiungere utenti e gruppi all'elenco di pubblicazione

del nome selezionato.



I gruppi di autorizzazioni vengono implementati immediatamente.

4 Per rimuovere un utente o un gruppo selezionato, selezionare il nome nell'elenco, quindi fare clic su *Rimuovi*.

5 Fare clic su *Chiudi* per accettare le modifiche e ritornare all'editor.

Il nome selezionato è riportato indietro nella Tabella organizzazione.

Quando si aggiunge un nuovo servizio di directory (vedere “Autenticazione directory” a pagina 16), al conto risorsa inserito vengono concesse impostazioni di autorizzazioni complete, come descritto in precedenza.

1.4 Utilizzo della finestra Configurazione

La finestra Configurazione consente all'amministratore di ZENworks® Endpoint Security Management di accedere ai controlli *Infrastruttura e pianificazione*, *Autenticazione directory* e *Sincronizzazione server*. Fare clic sul collegamento *Configurazione* nella pagina principale oppure sul menu *Strumenti*, quindi su *Configurazione*. Viene visualizzata la finestra Configurazione.

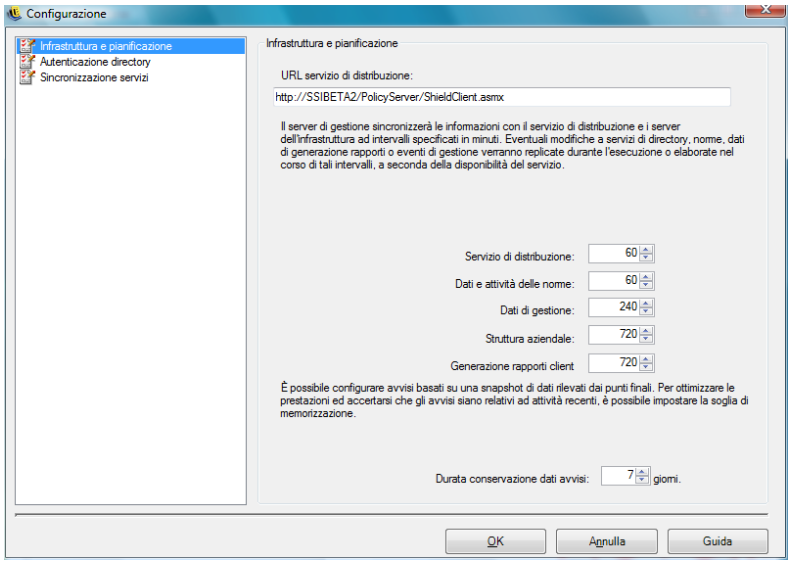
Nota: La funzione non è disponibile con una console di gestione autonoma.

Le seguenti sezioni contengono informazioni aggiuntive:

- Sezione 1.4.1, “Infrastruttura e pianificazione”, a pagina 14
- Sezione 1.4.2, “Autenticazione directory”, a pagina 16
- Sezione 1.4.3, “Sincronizzazione servizi”, a pagina 23

1.4.1 Infrastruttura e pianificazione

Il modulo di infrastruttura e pianificazione consente all'amministratore di ZENworks Endpoint Security Management di designare e modificare l'URL del servizio di distribuzione delle norme e di controllare gli intervalli di sincronizzazione dei componenti di ZENworks Endpoint Security Management.



Le seguenti sezioni contengono informazioni aggiuntive:

- “URL servizio di distribuzione” a pagina 15
- “Pianificazione” a pagina 15

URL servizio di distribuzione

L'impostazione *URL servizio di distribuzione* consente di aggiornare l'ubicazione del servizio di distribuzione norme sia per il servizio di gestione che per tutti gli ZENworks Security Client (senza necessità di reinstallarli) nel caso in cui il suddetto servizio venga spostato in un nuovo server. L'URL del server corrente viene elencato nel campo di testo.

Se è necessario cambiare il server, modificare soltanto il nome per puntare al nuovo server. Non modificare alcuna informazione dopo il nome del server.

Ad esempio, se l'URL corrente è `http:\\ACME\PolicyServer\ShieldClient.asmx` e il servizio di distribuzione norme viene installato su un nuovo server denominato ACME 43, l'URL dovrà essere aggiornato come segue:
`http:\\ACME43\PolicyServer\ShieldClient.asmx`

Dopo aver aggiornato l'URL, fare clic su *OK* per aggiornare tutte le norme e inviare un aggiornamento automatico del servizio di distribuzione norme. In questo modo viene aggiornato anche il servizio di gestione.

Quando si modifica l'URL del server, il precedente servizio di distribuzione norme non deve essere terminato finché le norme aggiornate non raggiungono un livello di conformità del 100% (vedere Sezione 1.6, “Utilizzo di Generazione rapporti”, a pagina 27).

Pianificazione

I componenti di pianificazione consentono all'amministratore di ZENworks Endpoint Security Management di designare il momento in cui il servizio di gestione eseguirà la sincronizzazione con gli altri componenti ZenWorks ESM, di assicurare che tutti i dati e i processi in coda corrispondano ad attività recenti e di pianificare le operazioni di manutenzione SQL. Tutti gli incrementi temporali sono espressi in minuti.

La pianificazione è suddivisa nel modo seguente:

- **Servizio di distribuzione :** pianificazione della sincronizzazione con il servizio di distribuzione norme.
- **Dati e attività delle norme:** pianificazione della sincronizzazione con aggiornamenti delle norme.
- **Dati di gestione** Sincronizzazione delle norme con il servizio di gestione.
- **Struttura aziendale:** Pianificazione della sincronizzazione con il servizio di directory aziendale (eDirectory™, Active Directory*, NT Domain* e/o LDAP). Le modifiche apportate al servizio di directory aziendale vengono·monitorate per consentire il rilevamento delle modifiche corrispondenti nelle assegnazioni delle norme utente nonché il relativo invio al servizio di distribuzione norme per l'autenticazione del client.
- **Generazione rapporti client:** Frequenza con cui il servizio di gestione interroga e scarica i dati relativi alla generazione di rapporti dal servizio di distribuzione norme.
- **Durata conservazione dati avvisi:** è possibile configurare gli avvisi in base a una snapshot di dati segnalata dai punti finali. Per ottimizzare le prestazioni e garantire che gli avvisi siano relativi ad attività recenti, è possibile impostare la soglia di memorizzazione in base al numero di giorni.

1.4.2 Autenticazione directory

Dopo aver installato ZENworks® Endpoint Security Management, è necessario creare e configurare un servizio di directory per poter iniziare a gestire i dispositivi nel sistema.

La Procedura guidata per la configurazione di un nuovo servizio directory consente di creare la configurazione di un servizio di directory che definisce l'ambito delle installazioni client di ZENworks Endpoint Security Management. La nuova configurazione utilizza il servizio di directory esistente per definire il limite logico per le installazioni client basate sull'utente e per quelle basate sul computer.

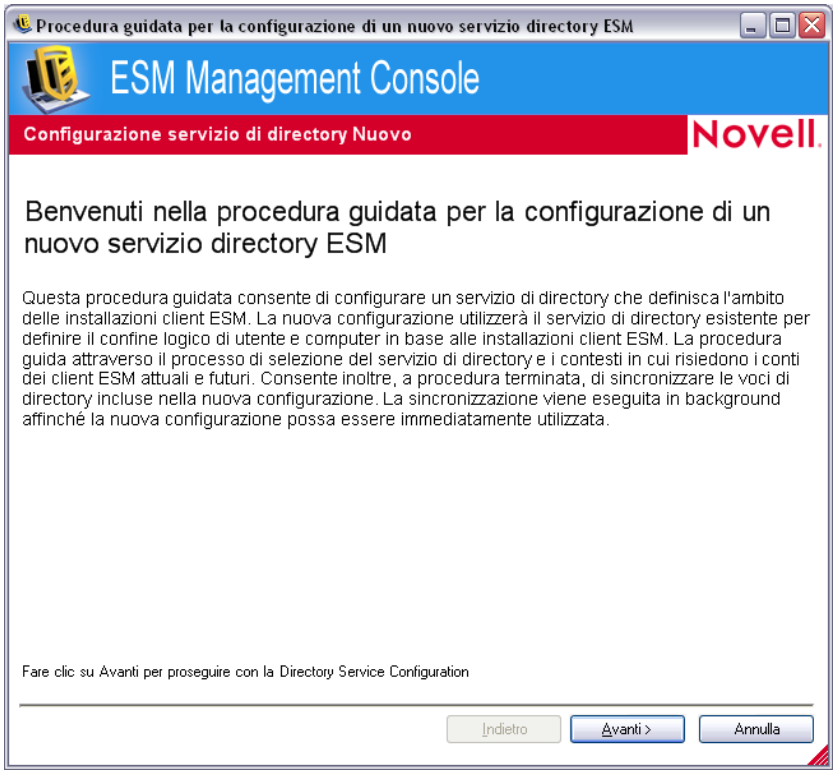
La procedura guidata assiste nel processo di selezione del servizio di directory e dei contesti in cui risiedono gli account client correnti e futuri.

La procedura consente inoltre di sincronizzare le voci di directory incluse nella nuova configurazione. La sincronizzazione viene eseguita in background, consentendo quindi all'utente di iniziare immediatamente a utilizzare la nuova configurazione.

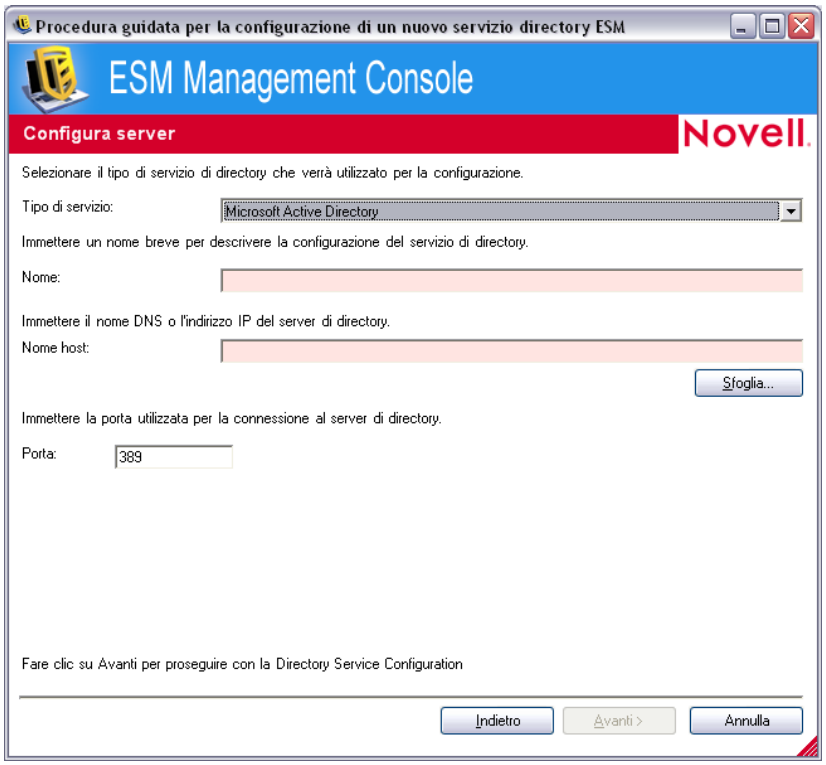
Al termine dell'installazione di ZENworks Endpoint Security Management, viene automaticamente visualizzata la Procedura guidata per la configurazione di un nuovo servizio directory. Se si è appena installato il prodotto ed è visualizzata la pagina di benvenuto, andare direttamente al passaggio Passo 4 della seguente procedura.

Per configurare il servizio di directory:

1. Nella console di gestione fare clic su *Strumenti* > *Configurazione*.
2. Fare clic su *Autenticazione directory*.
3. Fare clic su *Nuovo* per avviare la Procedura guidata per la configurazione di un nuovo servizio directory.



4 Fare clic su *Avanti* per visualizzare la pagina Configura server.

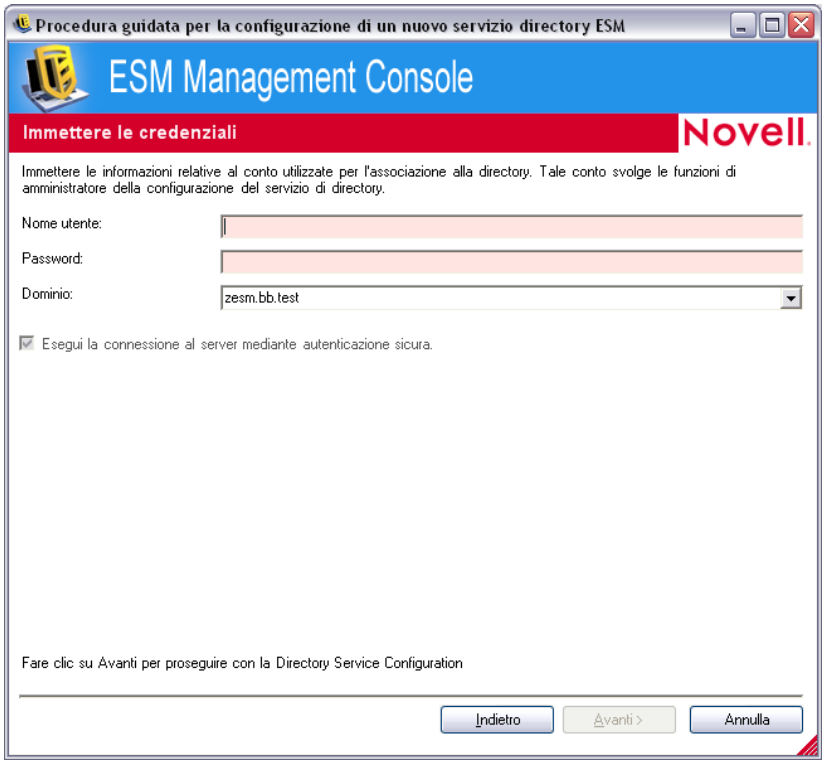


5 Immettere le informazioni richieste nei seguenti campi:

- **Tipo di servizio:** Selezionare un tipo di servizio dall'elenco a discesa *Tipo di servizio*:
  - Microsoft Active Directory
  - Novell eDirectory
- **Nome:** Specificare un nome breve per descrivere la configurazione del servizio di directory.
- **Nome host:** Specificare o cercare il nome DNS o l'indirizzo IP del server di directory.
- **Port:** Specificare la porta utilizzata per eseguire la connessione al server di directory.

  La porta di default è la 389. Se per eseguire la connessione al server di directory si utilizza una porta diversa, è possibile specificare tale porta.

6 Fare clic su *Avanti* per visualizzare la pagina Credenziali.



7 Immettere le informazioni richieste nei seguenti campi:

- **Nome utente:** Specificare l'amministratore del conto da associare alla directory.

  Tale conto svolge le funzioni di amministratore della configurazione del servizio di directory. Il nome di login deve corrispondere a un utente autorizzato a visualizzare tutto l'albero della directory. È consigliabile che questo utente sia l'amministratore del dominio o un amministratore dell'unità organizzativa. Utilizzare un formato LDAP se si esegue la configurazione per eDirectory, ad esempio: `cn=admin,o=acmeserver` dove `cn` rappresenta l'utente mentre `o` è l'oggetto in cui viene memorizzato il conto utente.

- **Password:** Specificare la password dell'amministratore del conto.

  Tale conto svolge le funzioni di amministratore della configurazione del servizio di directory.

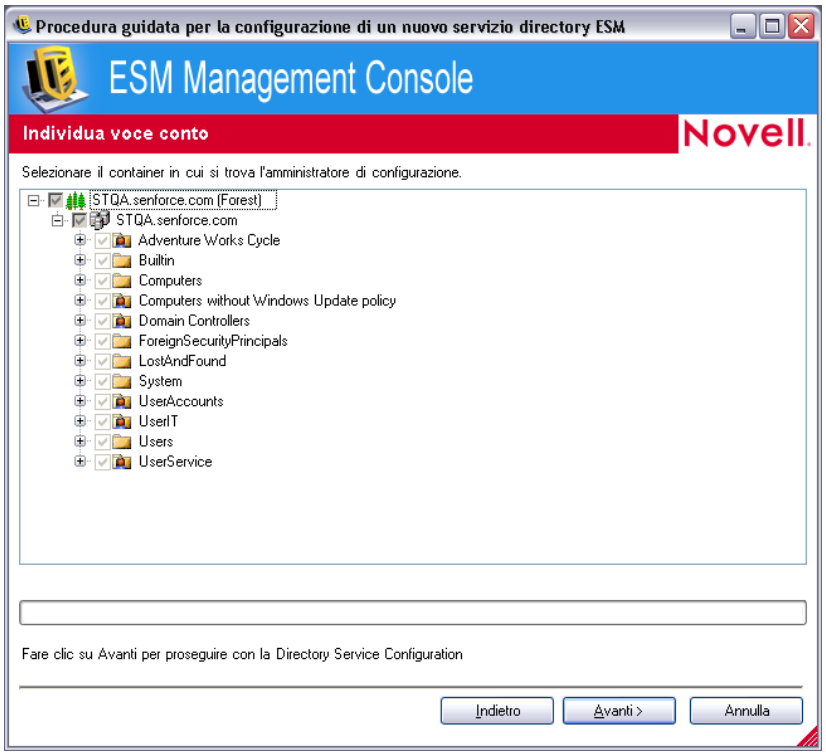
  La password non deve essere impostata con una scadenza e il conto non deve mai essere disattivato.

- **Dominio:** Specificare il dominio di cui è membro l'amministratore del conto.

- **Esegui la connessione al server mediante autenticazione sicura:** Deselezionare questa opzione se non si desidera utilizzare l'autenticazione sicura. Questa opzione è abilitata per default.

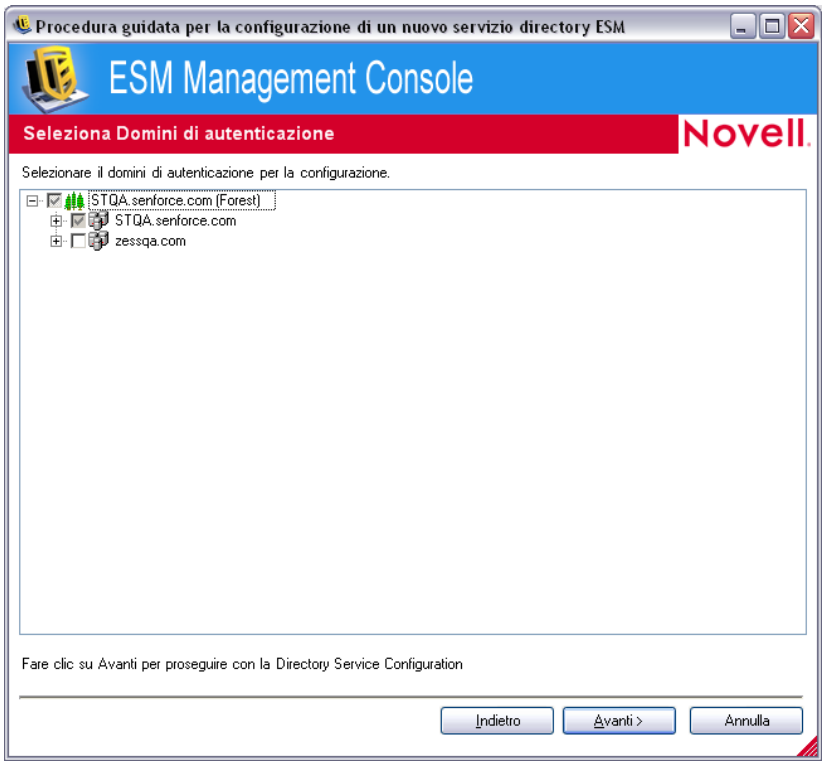
8 Fare clic su *Avanti* per continuare.

9 Se non è possibile trovare l'utente amministratore della configurazione specificato in Passo 7 nel dominio, viene visualizzata la pagina Individua voce conto.



Specificare il container in cui è incluso l'amministratore, quindi fare clic su *Avanti*.

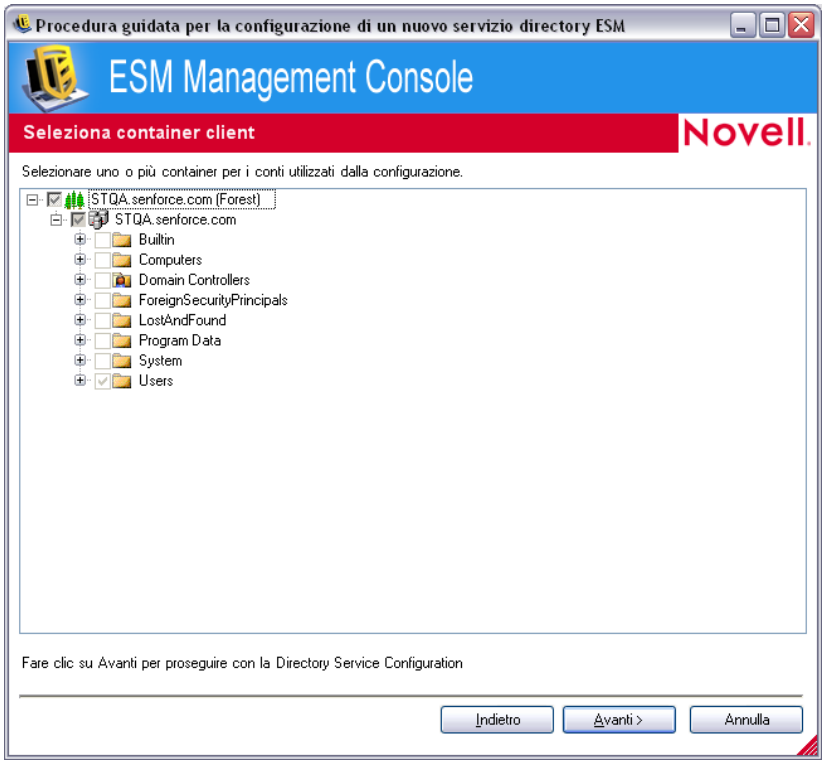
10 Nella pagina Seleziona domini di autenticazione sfogliare, l'albero per selezionare i domini utilizzati per autenticare gli utenti e i computer della configurazione corrente.



Il dominio contenente l'utente amministrativo specificato in Passo 7 è selezionato e non può essere deselezionato.

Le installazioni client che tentano di effettuare il check-in sul server di gestione non riusciranno se i client non sono membri di uno dei domini selezionati nella configurazione.

11 Fare clic su *Avanti* per visualizzare la pagina Seleziona container client, quindi selezionare i container per i conti utilizzati dalla configurazione.

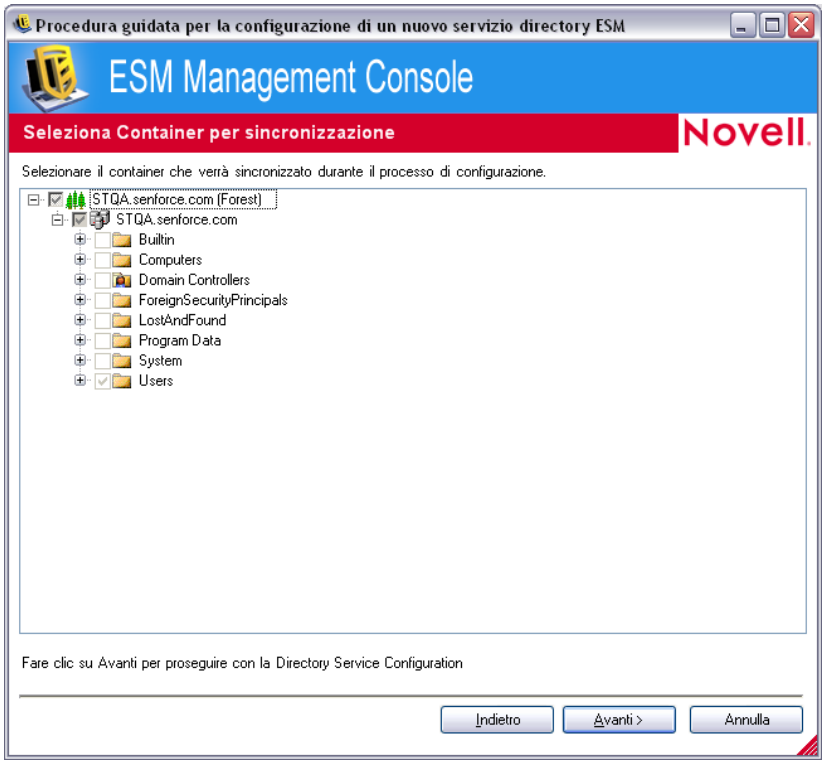


Il container che include l'utente amministrativo specificato in Passo 7 è selezionato e non può essere deselezionato.

La pagina Seleziona container client consente di restringere la ricerca ai soli container che includono utenti e computer gestiti, migliorando le prestazioni.

Le installazioni client che tentano di effettuare il check-in sul server di gestione non riusciranno se i conti corrispondenti non risiedono in uno dei container selezionati nella configurazione.

12 Fare clic su *Avanti* per visualizzare la pagina Container per sincronizzazione.



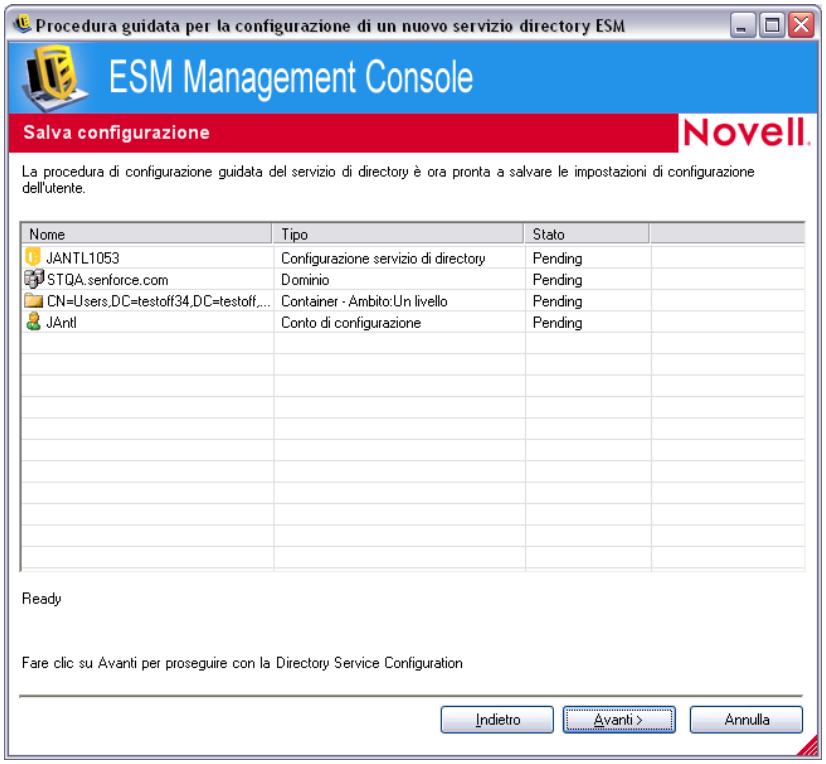
13 (Facoltativo) Selezionare i container da sincronizzare durante il processo di configurazione.

La sincronizzazione viene eseguita in background, consentendo quindi all'utente di iniziare immediatamente a utilizzare la nuova configurazione. Se il numero di utenti e computer da sincronizzare è elevato, questa operazione potrebbe richiedere alcune ore.

Se non si specificano container da sincronizzare, gli utenti e i computer di tali container vengono aggiunti alla console di gestione al momento del check-in.

La sincronizzazione dei container esegue il popolamento preliminare della console di gestione utilizzando tali utenti e computer, consentendo all'utente di iniziare immediatamente a eseguire azioni quali la creazione di norme di·sicurezza. Quando gli utenti o i computer effettuano il check-in nel sistema, queste norme vengono propagate e applicate. Il popolamento preliminare della console di gestione consente di iniziare immediatamente a creare norme specifiche per i singoli utenti o computer, anziché creare una norma da·applicare a tutti gli utenti e i computer del container. Se non si sincronizza il container, è necessario attendere fino a quando gli utenti e i computer non avranno effettuato il check-in nel sistema per poter creare norme univoche per i diversi utenti o computer.

14 Fare clic su *Avanti* per visualizzare la pagina Salva configurazione.

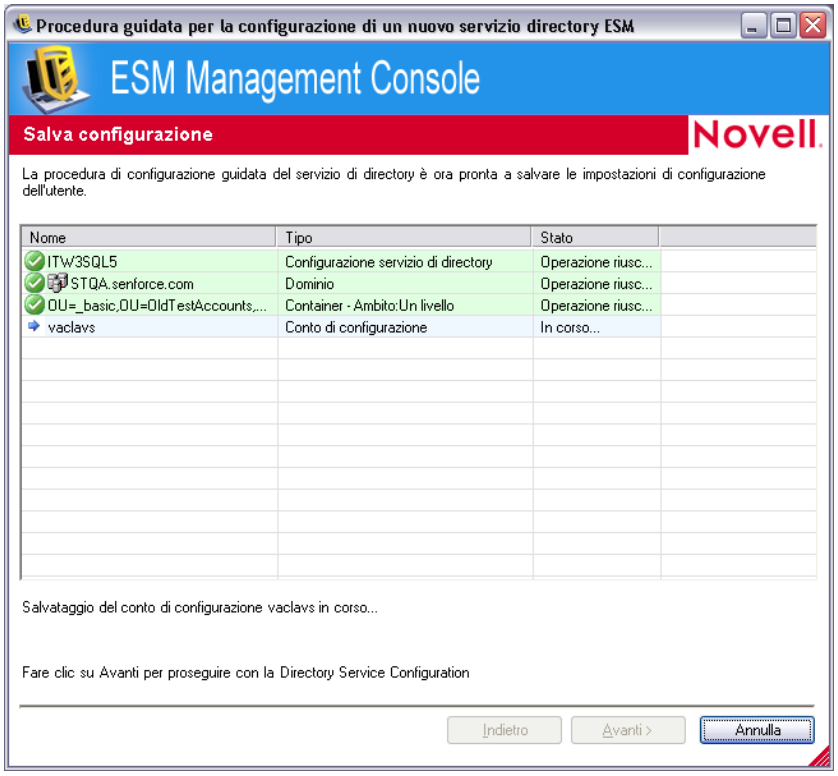


15 Rivedere le informazioni, quindi fare clic su *Avanti* per salvare la configurazione.

È possibile fare clic su *Indietro* per modificare qualsiasi impostazione, se necessario.

16 Fare clic su *Fine*.

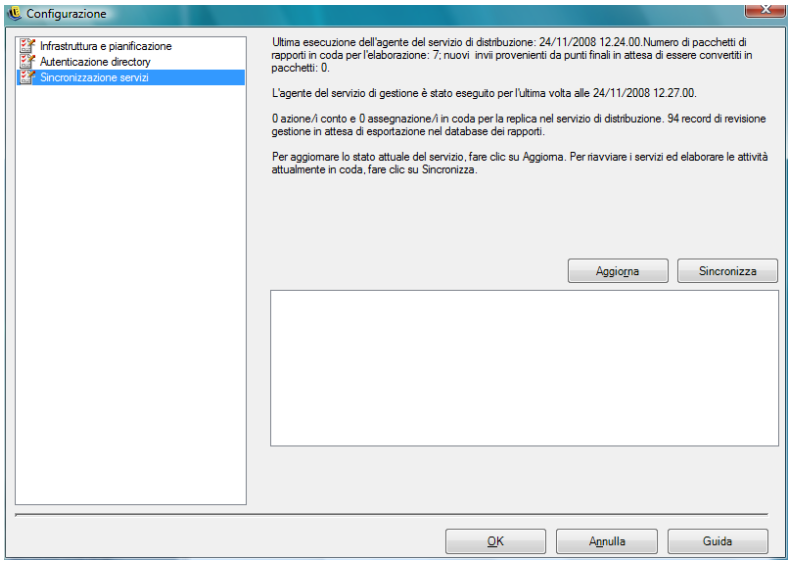
Quando si fa clic su *Fine*, viene visualizzata l'icona nell'area di notifica di Windows e ha inizio la sincronizzazione. È possibile fare doppio clic sull'icona per visualizzare la finestra di dialogo di sincronizzazione dei servizi di directory.



La sincronizzazione avviene in background. Se si esce dalla console di gestione, la sincronizzazione viene interrotta. Alla riapertura della console di gestione, la sincronizzazione riprende dal punto in cui era stata interrotta.

1.4.3 Sincronizzazione servizi

Questo controllo consente di forzare una sincronizzazione dei servizi di gestione e di distribuzione delle norme. In questo modo vengono completamente aggiornati gli avvisi, la generazione di rapporti e la distribuzione delle norme.

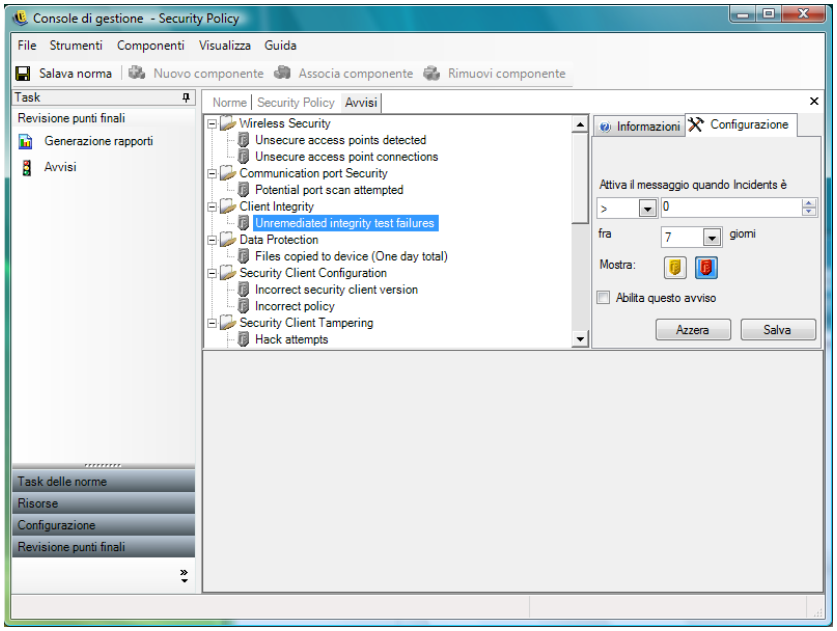


1. Per aggiornare lo stato dei servizi corrente, fare clic su *Aggiorna*.
2. Per riavviare i servizi ed elaborare le attività attualmente in coda, fare clic su *Sincronizza*.

1.5 Utilizzo del monitoraggio degli avvisi

Il monitoraggio degli avvisi consente all'amministratore di ZENworks® Endpoint Security Management di valutare lo stato di sicurezza di tutti i punti finali gestiti di ZENworks Endpoint Security Management in tutta l'azienda. I trigger degli avvisi sono completamente configurabili e possono segnalare avvertenze o avvisi di emergenza totale. Lo strumento è accessibile da *Revisione punti finali* nella barra delle applicazioni o dal menu *Visualizza*.

1 Per accedere agli avvisi, fare clic sull''icona Avvisi (Avvisi).



Il monitoraggio degli avvisi è disponibile per le aree seguenti:

- **Integrità client:** Notifica i risultati dei test di integrità non corretti.
- **Sicurezza porte di comunicazione:** Notifica i potenziali tentativi di scansione delle porte.
- **Protezione dati:** Notifica i file copiati su dispositivi di memorizzazione estraibili nell'arco di un giorno.
- **Configurazione client di sicurezza:** Notifica le versioni del client di sicurezza e le norme non corrette.
- **Manomissione client di sicurezza:** Notifica i tentativi di attacco da parte di utenti non autorizzati, i tentativi di disinstallazione e l'utilizzo della password prioritaria.
- **Sicurezza wireless:** Notifica i punti di accesso non sicuri, rilevati dall'utente e a cui l'utente è connesso.

1.5.1 Configurazione di avvisi in ZENworks Endpoint Security Management

Il monitoraggio degli avvisi richiede la raccolta e il caricamento periodici dei dati di generazione rapporti, al fine di ottenere il quadro più accurato possibile dell'ambiente di sicurezza corrente dei punti finali. Gli ZENworks® Security Client non gestiti non forniscono i dati di generazione rapporti, pertanto non sono inclusi nel monitoraggio degli avvisi.

Le seguenti sezioni contengono informazioni aggiuntive:

- “Attivazione della generazione dei rapporti” a pagina 25
- “Ottimizzazione della sincronizzazione” a pagina 25

Attivazione della generazione dei rapporti

La generazione dei rapporti deve essere attivata in tutte le norme di sicurezza. Vedere Sezione 2.2.4, “Rapporti di conformità”, a pagina 101 per ulteriori informazioni sull'impostazione della generazione dei rapporti per le norme di sicurezza. Impostare gli orari di invio dei rapporti su un intervallo che sia in grado di fornire aggiornamenti regolari sullo stato dei punti finali. Inoltre, un avviso non viene attivato senza un rapporto. Per ricevere gli avvisi relativi a una determinata attività, è necessario assegnare ad essa il rapporto appropriato nelle norme di sicurezza.

Ottimizzazione della sincronizzazione

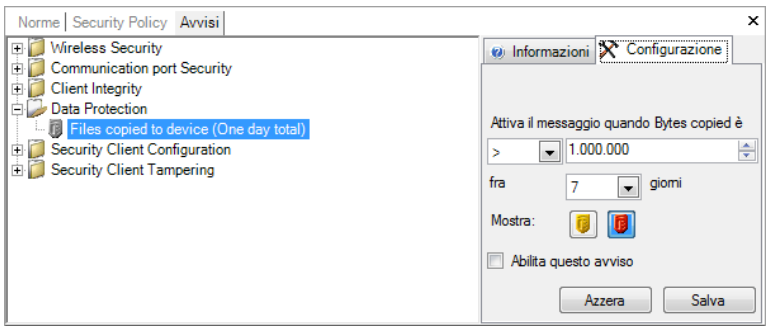
Per default, la sincronizzazione del servizio di generazione rapporti di ZENworks Endpoint Security Management avviene ogni 12 ore. Ciò indica che i dati di generazione rapporti e degli avvisi non saranno pronti se non sono trascorse 12 ore dall'installazione di ZENworks Endpoint Security Management. Per regolare questo intervallo di tempo, accedere allo strumento Configurazione (vedere “Pianificazione” a pagina 15), quindi impostare la durata di *Generazione rapporti client* sul numero di minuti appropriato alle proprie esigenze e al proprio ambiente.

Se i dati occorrono immediatamente, l'opzione *Sincronizzazione servizi* nello strumento Configurazione consente di avviare immediatamente il servizio di distribuzione norme, che raccoglie i dati dei rapporti dai punti finali, e il servizio di generazione rapporti, che aggiorna tutti gli avvisi in base ai dati appena raccolti). Per ulteriori informazioni, vedere Sezione 1.4.3, “Sincronizzazione servizi”, a pagina 23.

1.5.2 Configurazione dei trigger degli avvisi

I trigger degli avvisi possono essere impostati sulle soglie corrispondenti alle esigenze di sicurezza aziendali.

1 Selezionare un avviso dall'elenco, quindi fare clic sulla scheda *Configurazione* sul lato destro della console di gestione.



2 Regolare la soglia del trigger selezionando la condizione dall'elenco a discesa. La condizione indica se il numero di trigger è:

- uguale a (=)
- maggiore di (<)
- maggiore o uguale a (<=)
- minore di (>)
- minore o uguale a (>=)

3 Regolare il numero di trigger. Il numero varia in base al tipo di avviso.

4 Selezionare l'intervallo appropriato per tale numero.

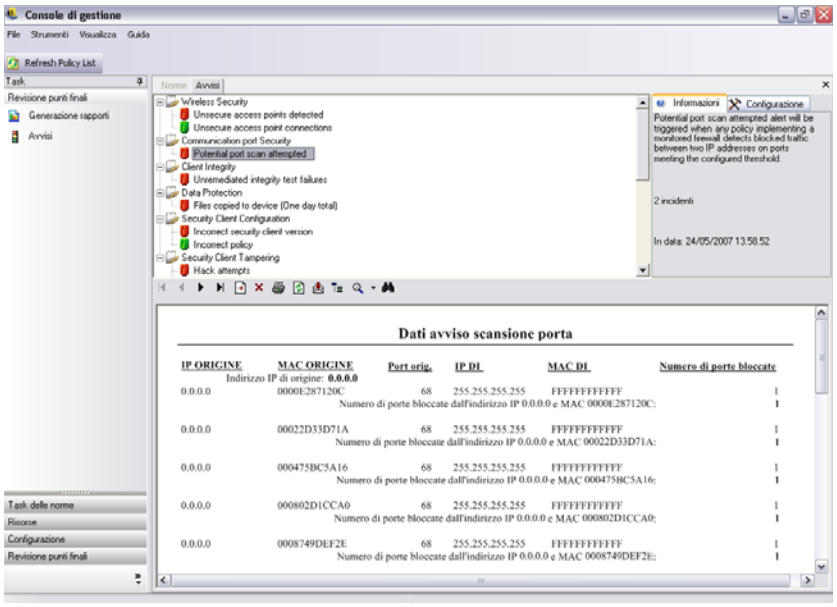
5 Selezionare il tipo di trigger. Può trattarsi di un'icona di avviso ( ) o di emergenza ( ).

6 Accertarsi che sia selezionata la casella *Abilita questo avviso*.

7 Fare clic su *Salva* per salvare l'avviso.

1.5.3 Gestione degli avvisi

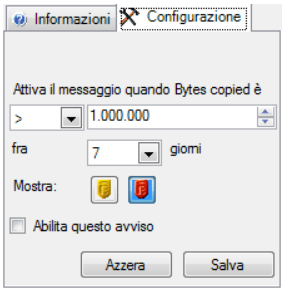
Gli avvisi notificano all'utente eventuali problemi da risolvere nell'ambiente di sicurezza dei punti finali. La soluzione generalmente viene gestita su base individuale o di gruppo. Per consentire l'identificazione dei problemi, quando si selezionano gli avvisi vengono visualizzati i relativi rapporti.



Questo rapporto indica i risultati dei trigger correnti visualizzando le informazioni relative all'utente o al dispositivo interessato. I dati in esso contenuti forniscono le informazioni necessarie per intraprendere le azioni correttive per qualsiasi eventuale problema di sicurezza aziendale. Per ulteriori informazioni, visualizzare la finestra Generazione di rapporti.

Dopo aver intrapreso le azioni correttive, l'avviso rimane inattivo fino al successivo aggiornamento di generazione rapporti. Per eliminare un avviso prima di un aggiornamento pianificato:

1 Selezionare un avviso dall'elenco, quindi fare clic sulla scheda *Configurazione* sul lato destro della console di gestione.



2 Fare clic su *Elimina*.

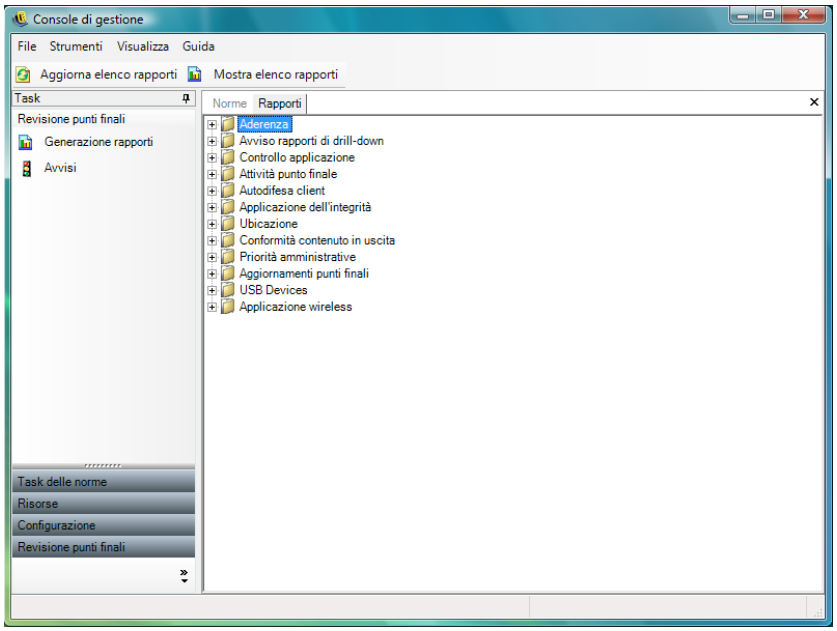
Questa operazione consente di eliminare i dati di generazione rapporti da Avvisi (ancora disponibili nel database dei rapporti). Non riattivare fino a quando non si ricevono nuovi dati.

1.6 Utilizzo di Generazione rapporti

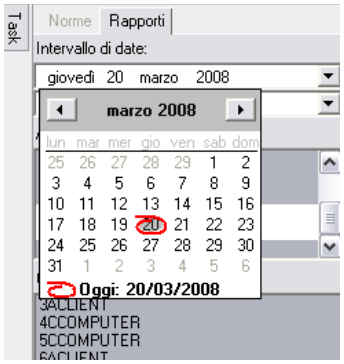
Il servizio di generazione rapporti fornisce i rapporti sulla conformità e sullo stato per l'azienda. I dati disponibili riguardano le directory e i gruppi utente all'interno di una directory. I rapporti Novell forniscono un feedback sugli effetti prodotti dai singoli componenti delle norme sui punti finali

dell'azienda. Le richieste relative a questi rapporti vengono impostate in Norme di sicurezza (vedere Sezione 2.2.4, “Rapporti di conformità”, a pagina 101) e possono fornire dati utili per determinare gli aggiornamenti delle norme.

Selezionare *Generazione rapporti* dalla barra degli strumenti *Revisione punti finali* oppure dal menu *Visualizza*. Verrà visualizzato l'elenco dei rapporti disponibili; per espandere l'elenco, fare clic sulle icone con segno più, poste accanto a ciascun tipo di rapporto.



I rapporti vengono configurati identificando l'intervallo di date e altri parametri, ad esempio utente o ubicazione. Per impostare i dati, espandere la vista calendario, quindi selezionare mese e giorno. Accertarsi di aver fatto clic sul giorno per modificare il parametro della data.



Fare clic su *Visualizza* per generare il rapporto.

Dopo aver generato un rapporto, è possibile utilizzare la relativa barra degli strumenti per visualizzarlo attraverso la console di gestione, stamparlo e inviarlo per posta elettronica, oppure per esportarlo come file `.pdf`.

Durante la revisione dei rapporti, i pulsanti freccia consentono di spostarsi all'interno di ciascuna pagina del rapporto. La prima pagina dei rapporti contiene in genere grafici e diagrammi, mentre le pagine restanti includono i dati richiamati, ordinati per data e tipo.

Il pulsante *Stampante* consente di stampare tutto il rapporto utilizzando la stampante di default del computer in uso.

Il pulsante *Esporta* consente di salvare il rapporto come file PDF, foglio di calcolo Excel*, documento Word o file RTF.

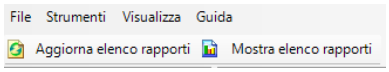
Il pulsante *Albero·gruppi* consente di mostrare o nascondere un elenco di parametri accanto al rapporto. Selezionare uno di questi parametri per eseguire il drill-down del rapporto. Fare clic sul pulsante *Albero gruppi* per chiudere la barra laterale.

Il pulsante *Lente di ingrandimento* consente di visualizzare un menu a discesa per regolare la dimensione di visualizzazione corrente.

Il pulsante *Binocoli* apre una finestra di ricerca.

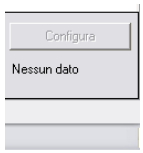
Quando si passa il mouse sopra un determinato parametro, ad esempio un nome utente o un nome dispositivo, il cursore·assume la forma di una lente di ingrandimento. È possibile fare doppio clic su un particolare elemento e visualizzare un nuovo rapporto soltanto per quell'oggetto. Fare clic sul pulsante *Chiudi* per chiudere la visualizzazione corrente e ritornare al rapporto originale.

Per ritornare all'elenco dei rapporti, fare clic sull'icona *Elenco rapporti* sopra la finestra dei rapporti.



I rapporti non sono disponibili fino a quando i dati non sono stati caricati dagli ZENworks® Security Client. Per default, la sincronizzazione del servizio di generazione rapporti di ZENworks Endpoint Security Management avviene ogni 12 ore. Ciò indica che i dati di generazione rapporti e degli avvisi non saranno pronti se non sono trascorse 12 ore dall'installazione di ZENworks Endpoint Security Management. Per regolare questo intervallo di tempo, accedere allo strumento Configurazione (vedere “Pianificazione” a pagina 15), quindi impostare la durata di *Generazione rapporti client* sul numero di minuti appropriato alle proprie esigenze e al proprio ambiente.

I pulsanti *Configura* o *Anteprima* dei rapporti che non dispongono di dati non risulteranno disponibili e sotto di essi verrà riportata l'indicazione "Nessun dato".



Sono disponibili i seguenti rapporti

- Sezione 1.6.1, “Rapporti di conformità”, a pagina 30
- Sezione 1.6.2, “Rapporti di drill-down degli avvisi”, a pagina 31
- Sezione 1.6.3, “Rapporti Controllo applicazioni”, a pagina 31
- Sezione 1.6.4, “Rapporti Soluzioni cifratura”, a pagina 32
- Sezione 1.6.5, “Rapporti attività punti finali”, a pagina 32

1.6.1 Rapporti di conformità

I rapporti di conformità forniscono le informazioni sulla conformità della distribuzione delle norme di sicurezza agli utenti gestiti. Un livello di conformità del 100% indica che tutti gli utenti gestiti hanno effettuato il check-in e ricevuto le norme correnti.

Sono disponibili i seguenti rapporti

- **Conformità check-in punti finali:** Fornisce un riepilogo dei giorni dall'esecuzione del check-in dei punti finali aziendali e la durata delle norme correnti. Per riepilogare il rapporto viene fatta una media dei numeri. Il rapporto non richiede l'immissione di variabili. Nel rapporto vengono visualizzati gli utenti per nome, le norme ad essi assegnate, i giorni trascorsi dall'ultimo check-in e la durata delle norme.
- **Versioni client punti finali:** Mostra la versione più recente riportata del client in ciascun punto finale. Per generare questo rapporto è necessario impostare i parametri della data.
- **Punti finali che non hanno mai effettuato il Check-in:** Elenca i conti utente che hanno eseguito la registrazione al servizio di gestione, ma che non hanno mai verificato la disponibilità degli aggiornamenti delle norme nel servizio di distribuzione. Per generare il rapporto è necessario selezionare uno o più gruppi.

  È possibile si tratti di utenti della console di gestione che non dispongono di un client di sicurezza installato a loro nome.
- **Non conformità norme di gruppo:** Mostra i gruppi nei quali alcuni utenti non dispongono delle norme corrette. Per generare il rapporto, è possibile effettuare le selezioni per uno o più gruppi.
- **Cronologia stato punti finali per computer:** Consente di visualizzare lo stato più recente (in un determinato intervallo di date) dei punti finali protetti da ZENworks Endpoint Security Management, raggruppati per nome di computer. Viene visualizzato il nome utente che ha eseguito il login, le norme correnti, la versione client di ZENworks Endpoint Security Management e l'ubicazione di rete. Questo rapporto richiede l'immissione di un intervallo di date. L'amministratore può eseguire il drill down facendo doppio clic su una qualsiasi voce per visualizzare un elenco completo dei rapporti sullo stato per un determinato computer.
- **Assegnazione norme:** Mostra utenti e gruppi (conti) che hanno ricevuto le norme specificate. Selezionare le norme desiderate dall'elenco e fare clic su *Visualizza* per eseguire il rapporto.
- **Cronologia stato punti finali per utente:** Consente di visualizzare lo stato più recente (in un determinato intervallo di date) dei punti finali protetti da ZENworks Endpoint Security Management, raggruppati per nome utente. Vengono visualizzati il nome del computer, le

norme correnti, la versione client di ZENworks Endpoint Security Management e l'ubicazione di rete. Questo rapporto richiede l'immissione di un intervallo di date. L'amministratore può eseguire il drill down facendo doppio clic su una qualsiasi voce per visualizzare un elenco completo dei rapporti sullo stato per un determinato utente.

1.6.2 Rapporti di drill-down degli avvisi

Forniscono ulteriori informazioni sugli avvisi. Tali rapporti consentono la visualizzazione dei dati solo quando viene attivato un avviso. L'annullamento di un avviso, comporta anche quello del relativo rapporto, tuttavia i dati continuano a essere disponibili in un rapporto standard.

Sono disponibili i seguenti rapporti

- **Dati avvisi manomissioni client:** Visualizza le istanze in cui un utente ha eseguito un tentativo non autorizzato di modificare o disabilitare ZENworks Security Client.
- **Dati avvisi file copiati:** Mostra i conti che presentano dati copiati in dispositivi di memorizzazione estraibili.
- **Dati avvisi versione client non corretta:** Mostra la cronologia dello stato del processo di aggiornamento di ZENworks Security Client.
- **Dati avvisi norme client non corrette:** Mostra gli utenti che non dispongono delle norme corrette.
- **Dati avvisi errori d'integrità:** Genera un rapporto relativo alla cronologia dei risultati positivi e negativi delle verifiche di integrità del client.
- **Dati avvisi tentativi di avvio priorità amministrativa:** Mostra istanze in cui i meccanismi di autodifesa del client sono stati ignorati a livello amministrativo, concedendo il controllo privilegiato su ZENworks Security Client.
- **Dati avvisi scansione porte:** Mostra il numero di pacchetti bloccati sul numero di porte diverse (la presenza di un numero eccessivo di porte può indicare la scansione di una porta).
- **Dati avvisi tentativi disinstallazione:** Elenca gli utenti che hanno tentato di disinstallare ZENworks Security Client.
- **Dati avvisi punti di accesso non sicuri:** Elenca i punti di accesso non sicuri rilevati da ZENworks Security Client.
- **Dati avvisi connessione a punti di accesso non sicuri:** Elenca i punti di accesso non sicuri del collegamento effettuato tramite ZENworks Security Client.

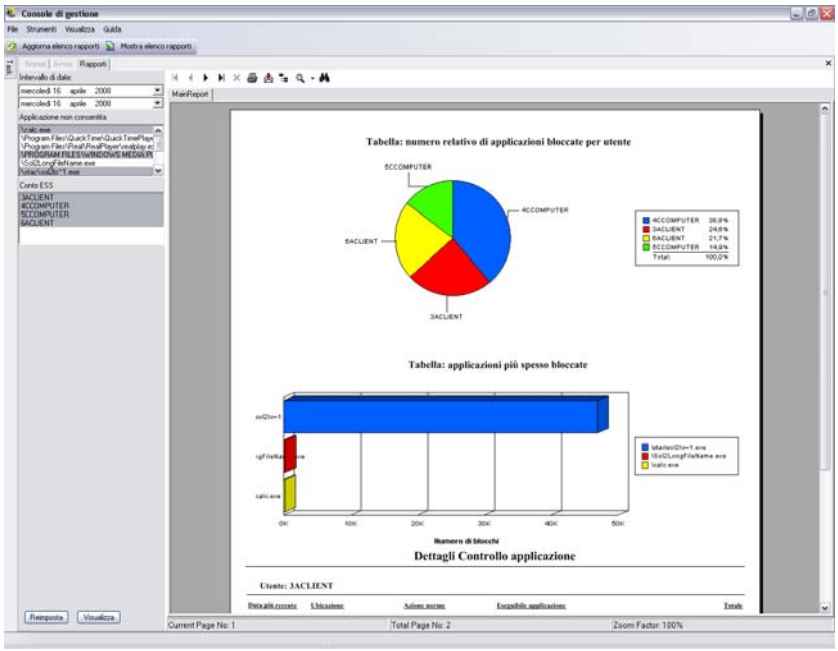
1.6.3 Rapporti Controllo applicazioni

Questi rapporti consentono di visualizzare tutti i tentativi di accesso alla rete o di esecuzione delle applicazioni bloccate non autorizzati dalle norme.

È disponibile il seguente rapporto:

- **Dettagli Controllo applicazioni:** Consente di visualizzare data, ubicazione, azione intrapresa da ZENworks® Security Client, applicazione che ha tentato l'esecuzione e numero di volte in cui è stata avviata l'applicazione. Le date sono visualizzate in formato UTC.

Specificare i parametri della data, selezionare i nomi delle applicazioni dall'elenco e i conti utente, quindi fare clic su *Visualizza* per eseguire il rapporto.



1.6.4 Rapporti Soluzioni cifratura

Se la cifratura dei punti finali è attivata, questi rapporti visualizzano il trasferimento dei file nelle e dalle cartelle cifrate.

Sono disponibili i seguenti rapporti

- **Attività cifratura file:** Mostra i file a cui è stata applicata la cifratura.
- **Eccezioni cifratura:** Mostra gli errori del sottosistema di cifratura (ad esempio, non è stato possibile decifrare un file protetto perché l'utente non disponeva delle chiavi corrette).
- **Volumi cifratura file:** Mostra i volumi (ad esempio, le unità estraibili o le partizioni di disco fisso) gestiti da Novell Encryption Solution.

1.6.5 Rapporti attività punti finali

Questi rapporti forniscono il feedback sui singoli componenti delle norme e sull'effetto prodotto nel funzionamento del punto finale.

Sono disponibili i seguenti rapporti

- **Pacchetti bloccati per indirizzo IP:** Consente di visualizzare i pacchetti bloccati filtrati dall'IP di destinazione. Le date sono visualizzate in formato UTC.

  Selezionare l'IP di destinazione dall'elenco e impostare i parametri della data. Il rapporto visualizza le date, le ubicazioni, le porte interessate e il nome dei pacchetti bloccati.
- **Pacchetti bloccati per utente:** Consente di visualizzare i pacchetti bloccati filtrati per utente. Le date sono visualizzate in formato UTC. I dati forniti sono fondamentalmente gli stessi dei pacchetti bloccati dall'IP di destinazione, ma sono suddivisi per utente.

- **Statistiche utilizzo rete per utente:** elenca i pacchetti inviati, ricevuti o bloccati e gli errori di rete filtrati da utenti. Questo rapporto richiede un intervallo di date. Le date sono visualizzate in formato UTC.
- **Statistiche utilizzo rete per tipo di adattatore:** Elenca i pacchetti inviati, ricevuti o bloccati e gli errori di rete filtrati per tipo di adattatore. Il rapporto richiede un intervallo di date e l'ubicazione. Le date sono visualizzate in formato UTC.

1.6.6 Rapporti Aggiornamenti punti finali

Questi rapporti consentono di visualizzare lo stato del processo di aggiornamento di ZENworks Security Client (vedere"Aggiornamento ZSC" a pagina 62). Le date sono visualizzate in formato UTC.

Sono disponibili i seguenti rapporti

- **Tabella percentuale di aggiornamenti del client di sicurezza non riusciti:** Riporta la percentuale di aggiornamenti di ZENworks Security Client non riusciti e non corretti. Per la generazione di questo rapporto non è richiesto alcun parametro.
- **Cronologia dello stato di aggiornamento dei client di sicurezza:** Mostra la cronologia dello stato del processo di aggiornamento di ZENworks Security Client. Selezionare l'intervallo di date e fare clic su *Visualizza* per eseguire il rapporto. Il rapporto visualizza gli utenti che hanno effettuato il check-in e ricevuto l'aggiornamento.
- **Tabella tipi di aggiornamenti dei client di sicurezza non riusciti:** Mostra gli aggiornamenti di ZENworks Security Client non riusciti e non corretti. Selezionare l'intervallo di date e fare clic su Visualizza per eseguire il rapporto. Il rapporto mostra gli utenti che hanno effettuato il check-in, ma che non sono riusciti a eseguire l'installazione dell'aggiornamento.

1.6.7 Rapporti Autodifesa client

I rapporti Autodifesa client notificano i tentativi degli utenti di modificare o disabilitare ZENworks® Security Client.

È disponibile il seguente rapporto:

- **Tentativi di utilizzo non autorizzato di ZENworks Security Client:** Questi rapporti segnalano le istanze in cui un utente ha eseguito un tentativo non autorizzato di modificare o disabilitare ZENworks Security Client. Le date sono visualizzate in formato UTC (Coordinated Universal Time).

  Immettere i parametri della data e fare clic su *Visualizza* per eseguire il rapporto.

1.6.8 Rapporti Applicazione integrità

Questi rapporti forniscono i risultati relativi all'integrità di antivirus/antispyware.

Sono disponibili i seguenti rapporti

- **Cronologia integrità client:** Genera un rapporto sull'esito positivo o negativo dei controlli di integrità del client. Le date sono visualizzate in formato UTC.

  Selezionare l'intervallo di date per il rapporto, regole di integrità e nomi utente.

- **Errori di integrità non corretti per regola:** Genera un rapporto relativo alle regole e ai test di integrità non riusciti e non ancora corretti.

  Selezionare le regole di integrità e fare clic su *Visualizza* per eseguire il rapporto.

- **Errori di integrità non corretti per utente:** Genera un rapporto relativo agli utenti le cui verifiche di integrità non riuscite non sono state ancora corrette.

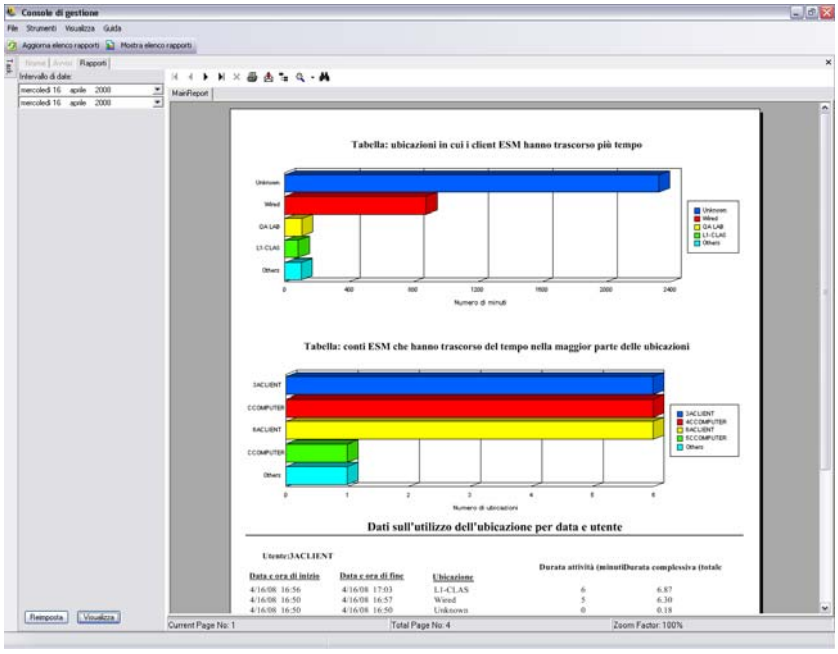
  Selezionare i nomi utente e fare clic su *Visualizza* per eseguire il rapporto.

1.6.9 Rapporti Ubicazioni

Il rapporto Ubicazione fornisce i dati relativi all'uso di ubicazioni comuni, ad esempio quelle più comunemente utilizzate dagli utenti.

È disponibile il seguente rapporto:

Dati sull'utilizzo dell'ubicazione per data e utente: Fornisce informazioni richiamate dai singoli client concernenti le ubicazioni utilizzate e la data di utilizzo. Le date sono visualizzate in formato UTC. Vengono visualizzate solo le ubicazioni effettivamente utilizzate dall'utente. Selezionare l'intervallo di date per generare il rapporto.



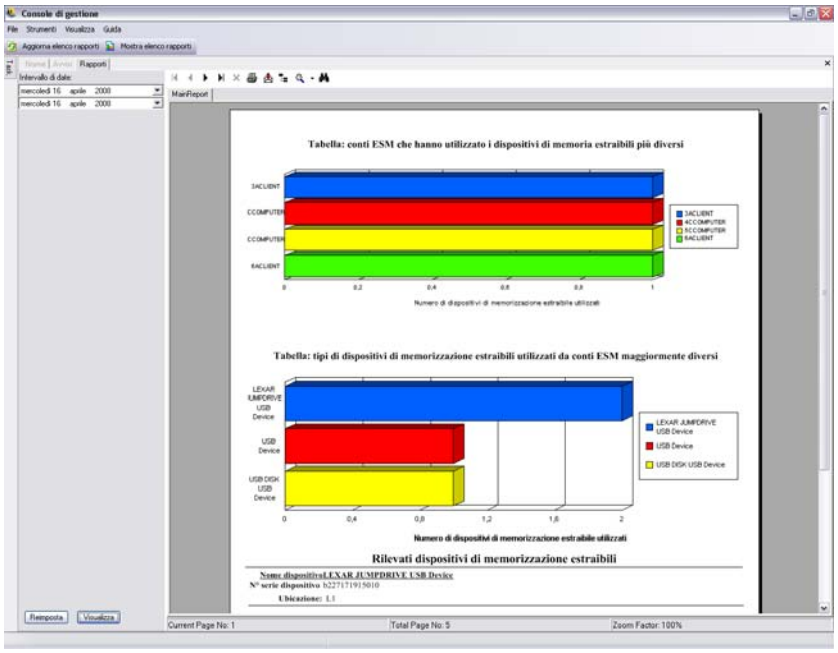
1.6.10 Rapporti Conformità contenuti in uscita

Questi rapporti forniscono informazioni sull'utilizzo delle unità estraibili e identificano i file che sono stati caricati su tali unità.

Sono disponibili i seguenti rapporti

- **Attività dispositivi di memorizzazione estraibili per conto:** Mostra i conti che hanno copiato i dati in un dispositivo di memorizzazione estraibile. Per la generazione di questo rapporto non è richiesto alcun parametro.

- **Attività dispositivi di memorizzazione estraibili per dispositivo:** Mostra i dispositivi di memorizzazione estraibili sui quali sono stati copiati i file. Per generare il rapporto, selezionare intervallo di date, nomi utente e ubicazioni.
- **Copie da dispositivo di memorizzazione estraibile per conto:** Mostra i file copiati da dispositivi di memorizzazione estraibili in dispositivi gestiti.
- **Dispositivi di memorizzazione estraibili rilevati:** Mostra i dispositivi di memorizzazione estraibili che sono stati rilevati nel punto finale. Per generare il rapporto, selezionare intervallo di date, nomi utente e ubicazioni.



- **Grafico di 7 giorni sull'attività dei dispositivi di memorizzazione estraibili per conto:**

  Consente di visualizzare una tabella dei conti in cui sono presenti dati recentemente copiati in un dispositivo di memorizzazione estraibile. Immettere i parametri della data per generare questo rapporto.

1.6.11 Rapporto Avvio priorità amministrativa

Mostra le istanze in cui i meccanismi di autodifesa del client sono stati ignorati dal punto di vista amministrativo, concedendo un controllo privilegiato su ZENworks® Security Client.

È disponibile il seguente rapporto:

- **Priorità ZENworks Security Client:** Mostra i tentativi di utilizzo della priorità riusciti per utente e data. Le date sono visualizzate in formato UTC.

  Selezionare l'utente e l'intervallo di date, quindi fare clic su *Visualizza* per eseguire il rapporto.

1.6.12 Rapporti Aggiornamenti punti finali

Questi rapporti mostrano lo stato del processo di aggiornamento di ZENworks® Security Client (vedere"Aggiornamento ZSC" a pagina 62). Le date sono visualizzate in formato UTC.

Sono disponibili i seguenti rapporti

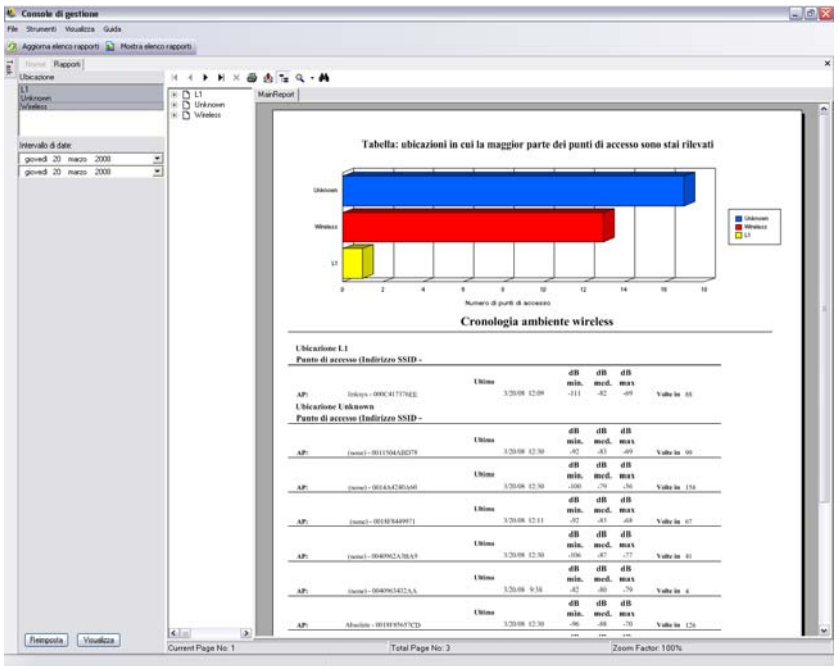
- **Tabella percentuale di aggiornamenti del client di sicurezza non riusciti:** Riporta la percentuale di aggiornamenti di ZENworks Security Client non riusciti e non corretti. Per la generazione di questo rapporto non è richiesto alcun parametro.
- **Cronologia dello stato di aggiornamento dei client di sicurezza:** Mostra la cronologia dello stato del processo di aggiornamento di ZENworks Security Client. Selezionare l'intervallo di date e fare clic su *Visualizza* per eseguire il rapporto. Il rapporto consente di visualizzare gli utenti che hanno effettuato il check-in e ricevuto l'aggiornamento.
- **Tabella tipi di aggiornamenti dei client di sicurezza non riusciti:** Mostra gli aggiornamenti di ZENworks Security Client non riusciti e non corretti. Selezionare l'intervallo di date e fare clic su *Visualizza* per eseguire il rapporto. Il rapporto mostra gli utenti che hanno effettuato il check-in, ma che non sono riusciti a eseguire l'installazione dell'aggiornamento.

1.6.13 Rapporti Applicazione wireless

Forniscono rapporti relativi agli ambienti Wi-Fi a cui è esposto il punto finale.

Sono disponibili i seguenti rapporti

- **Disponibilità connessione wireless:** Visualizza i punti di accesso disponibili per la connessione in base alle norme e all'ubicazione. Include canale, SSID, indirizzo MAC e indica se il punto di accesso è cifrato o meno.
- **Tentativi connessione wireless:** Fornisce un elenco di punti di accesso a cui i dispositivi tentano di connettersi, per ubicazione e conto.
- **Cronologia ambiente wireless:** Fornisce una panoramica su tutti i punti di accesso rilevati, a prescindere dalla proprietà. Include frequenza, potenza del segnale e indica se il punto di accesso è cifrato o meno. Le date sono visualizzate in formato UTC. Selezionare le ubicazioni e l'intervallo di date desiderati per generare il rapporto.



1.7 Utilizzo di ZENworks Storage Encryption Solution

ZENworks® Storage Encryption Solution consente di gestisce centralmente la sicurezza di tutti i dati dei dispositivi portatili applicando attivamente norme di cifratura aziendali al punto finale stesso.

ZENworks Storage Encryption Solution consente di eseguire le seguenti attività:

- Creare, distribuire, applicare e verificare centralmente le norme di cifratura in tutti i punti finali e dispositivi di memorizzazione estraibili.
- Proteggere con cifratura tutti i file salvati o copiati in una directory specifica su tutte le partizioni di disco fisso dell'unità disco.
- Proteggere con cifratura tutti i file copiati sui dispositivi di memorizzazione estraibili.
- Condividere i file liberamente all'interno di un'organizzazione bloccando l'accesso non autorizzato ai file.
- Condividere i file cifrati e protetti da password con gli utenti esterni all'organizzazione attraverso un'utility di decifratura.
- Eseguire con facilità l'aggiornamento, il backup e il recupero delle chiavi attraverso le norme, senza perdita di dati.

1.7.1 Caratteristiche di ZENworks Storage Encryption Solution

La cifratura dei dati viene applicata attraverso la creazione e la distribuzione delle norme di sicurezza di cifratura dei dati. I dati riservati presenti sul punto finale vengono memorizzati in una cartella cifrata. L'utente può accedere a questi dati, copiarli all'esterno della cartella cifrata e condividere i file, tuttavia i dati presenti in tale cartella continuano a essere cifrati. Solo gli utenti autorizzati per quel computer saranno in grado di leggere i dati. Quando le norme sono attivate, una cartella cifrata `Safe Harbor` viene aggiunta alla directory radice dei volumi non di sistema nel punto finale.

I dati riservati collocati su un'unità USB o su un altro dispositivo estraibile vengono immediatamente cifrati e possono essere letti solo sui computer dello stesso gruppo di norme. È possibile facoltativamente attivare una cartella di condivisione, che consente agli utenti di condividere i file con utenti esterni al gruppo di norme mediante una password (vedere “Cifratura dei dati” a pagina 59).

1.7.2 Condivisione di file cifrati

Gli utenti all'interno dello stesso gruppo di norme (ovvero, gli utenti che hanno ricevuto le stesse norme di sicurezza) dispongono delle chiavi per accedere ai dati memorizzati nel punto finale, nonché ai dati spostati su unità USB e altri dispositivi estraibili.

Gli utenti all'interno di un gruppo di norme separato (con cifratura attivata) sono in grado di accedere ai dati cifrati che si trovano nella cartella `File condivisi` utilizzando una password di accesso. Questi utenti non sono in grado di leggere i file cifrati all'esterno della cartella `File condivisi`.

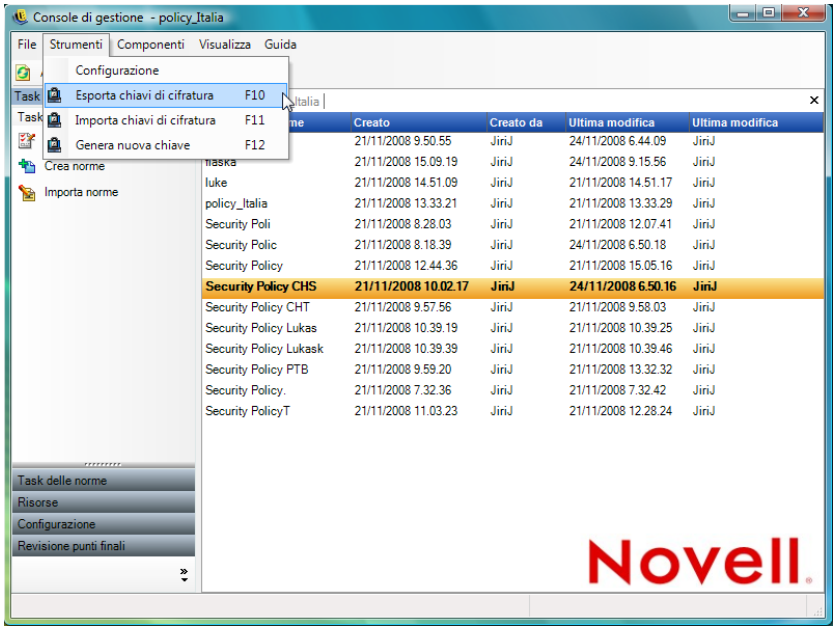
Gli utenti che non dispongono di norme abilitate alla cifratura e quelli che non hanno installato sui computer ZENworks Security Client (ad esempio i fornitori esterni) non sono in grado di leggere i file esterni alla cartella `File condivisi`. Per leggere i file con accesso tramite password necessiteranno della utility di decifratura file ZENworks®. Per ulteriori informazioni, consultare Sezione 1.9, “Utilizzo dell'utility di decifratura file ZENworks”, a pagina 39.

1.8 Utilizzo della gestione chiavi

La gestione delle chiavi consente di eseguire il backup, l'importazione e l'aggiornamento di una chiave di cifratura. Si consiglia di esportare e salvare le chiavi di cifratura al fine di garantire la decifratura dei dati in caso si verifichi un errore di sistema o una modifica accidentale delle norme.

La chiave comune è la chiave di cifratura di default utilizzata per tutti gli agenti di cifratura dei dati. È possibile aggiornare una chiave di cifratura qualora sia stata compromessa o per precauzione di sicurezza. Quando si genera una nuova chiave comune, la riesecuzione della cifratura dei contenuti gestiti influisce temporaneamente sulle prestazioni.

I comandi delle chiavi di cifratura sono accessibili dal menu *Strumenti* della console di gestione.



1.8.1 Esportazione delle chiavi di cifratura

Per scopi di backup o per inviare la chiave a un'altra istanza del servizio di gestione, l'insieme di chiavi di cifratura corrente può essere esportato in una ubicazione file designata.

1. Fare clic su *Strumenti* > *Esporta chiavi di cifratura*.
2. Specificare il percorso con un nome file oppure fare clic su *Sfoglia* per individuare e selezionare un'ubicazione file.
3. Specificare una password. Non è possibile importare la chiave senza questa password.
4. Fare clic su *OK*.

Tutti i file delle chiavi presenti nel database vengono inclusi nel file esportato.

1.8.2 Importazione delle chiavi di cifratura

È possibile importare le chiavi da un backup o da un'altra istanza del servizio di gestione. Ciò consente ai punti finali gestiti dal servizio di gestione di leggere i file protetti da altre installazioni ZENworks Endpoint Security Management. Durante l'importazione delle chiavi i duplicati vengono ignorati. Le chiavi importate diventano parte dell'insieme di chiavi e non sostituiscono la chiave comune corrente. Tutte le chiavi vengono trasmesse con la pubblicazione di nuove norme.

1. Fare clic su *Strumenti* > *Importa chiavi di cifratura*.
2. Specificare il nome file, con l'ubicazione del file, oppure fare clic su *Sfoglia* per individuare e selezionare il file di chiave.
3. Specificare la password per la chiave di cifratura.
4. Fare clic su *OK* per importare la chiave nel database.

1.8.3 Generazione di una nuova chiave

1. Fare clic su *Strumenti* > *Genera nuova chiave*.

Tutte le chiavi precedenti vengono memorizzate nelle norme.

1.9 Utilizzo dell'utility di decifratura file ZENworks

L'utility di decifratura file ZENworks® è utilizzata per estrarre i dati protetti dalla cartella `File condivisi` su dispositivi di memorizzazione estraibili cifrati. Questo semplice strumento può essere fornito a terze parti affinché possano accedere ai file della cartella `File condivisi` anche se non è collocabile su dispositivo di memorizzazione estraibile.

- Sezione 1.9.1, “Utilizzo dell'utility di decifratura file”, a pagina 39
- Sezione 1.9.2, “Configurazione dell'utility di decifratura file”, a pagina 40

Le seguenti sezioni contengono informazioni aggiuntive:

1.9.1 Utilizzo dell'utility di decifratura file

Per utilizzare l'utility di decifratura file:

1. Inserire il dispositivo di memorizzazione nella porta appropriata del computer in uso.
2. Aprire l'utility di decifratura file.
3. Individuare la directory `File condivisi` del dispositivo di memorizzazione e selezionare il file desiderato.
4. Per estrarre le directory (cartelle) anziché i file, fare clic sul pulsante *Avanzate* e selezionare *Directory*, quindi individuare la directory appropriata (fare clic su *Base* per tornare alla visualizzazione di default).
5. Individuare e selezionare la destinazione sul computer locale in cui verranno memorizzati questi file.
6. Fare clic su *Estrai*.

La transazione può essere monitorata facendo clic sul pulsante *Mostra avanzamento*.

1.9.2 Configurazione dell'utility di decifratura file

L'utility di decifratura file può essere configurata in "modalità amministratore" con l'insieme di chiavi corrente e consente di estrarre tutti i dati da un dispositivo di memorizzazione cifrato. Questa configurazione non è consigliabile perché potenziamente in grado di compromettere tutte le chiavi correnti utilizzate da ZENworks Storage Encryption Solution; tuttavia nei casi in cui sia impossibile recuperare i dati in altro modo, potrebbe rendersi necessaria.

Per configurare lo strumento:

1. Creare un collegamento all'utility di decifratura file all'interno della relativa directory corrente.
2. Fare clic con il pulsante destro del mouse sul collegamento, quindi su *Proprietà*.
3. Alla fine del nome di destinazione e dopo le virgolette, immettere -k (ad esempio: `C:\Admin Tools\stdecrypt.exe" -k`).
4. Fare clic su *Applica* > *OK*.
5. Aprire lo strumento utilizzando il collegamento e fare clic su *Avanzate*.
6. Fare clic sul pulsante *Carica chiavi* per aprire la finestra di dialogo Importa chiave.
7. Cercare il file delle chiavi, quindi specificare la password per le chiavi.

A questo punto è possibile estrarre tutti i file cifrati con queste chiavi.

1.10 Utilizzo del generatore della chiave della password prioritaria

Le interruzioni di operatività a cui è talvolta soggetto l'utente dovute a restrizioni di connettività, esecuzione software disattivata o accesso a dispositivi di memorizzazione estraibili sono presumibilmente causate dalle norme di sicurezza applicate da ZENworks® Security Client. 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 a livello di tutte le ubicazioni e di tutte le impostazioni del firewall, oppure che l'utente non sia in grado di cambiare ubicazione o impostazione.

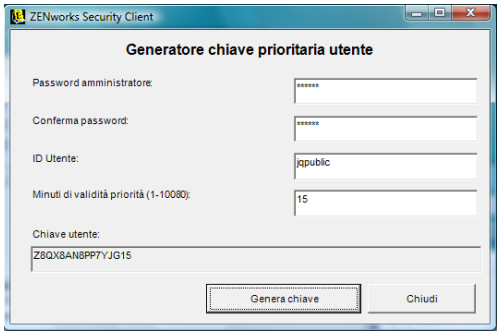
In questi casi, le restrizioni·delle norme correnti possono essere annullate attraverso una password prioritaria, la quale consente l'esecuzione delle attività fino a quando non è possibile modificare le norme. Questa funzione consente all'amministratore di impostare una password prioritaria protetta per utenti e funzionalità specifici, grazie alla quale sarà possibile eseguire le attività necessarie in via temporanea.

La password prioritaria disabilita le norme di sicurezza correnti e ripristina la norme di default Tutte aperte per un periodo di tempo predefinito. Scaduto il limite di tempo, le norme correnti o aggiornate vengono ripristinate. La password delle norme viene definita·nelle impostazioni Regole globali delle norme di sicurezza.

La password prioritaria:

- Ignora il blocco delle applicazioni.
- Consente agli utenti di cambiare ubicazioni
- Consente agli utenti di modificare le impostazioni del firewall
- Ignora il controllo hardware (unità USB, CD-ROM e così via)

La password immessa nelle norme non deve mai essere rilasciata a un utente. È necessario utilizzare il generatore della chiave della password prioritaria per generare una chiave da usare a breve termine.



Per generare una chiave prioritaria:

1. Aprire il generatore della chiave della password prioritaria (*Start* > *Programmi* > *Novell* > *ESM Management Console* > *Generatore password prioritaria*.
2. Specificare la password delle norme nel campo *Password amministratore*, quindi confermarla nel campo successivo.
3. Specificare il nome utente con cui l'utente finale ha eseguito il login.
4. Specificare la durata di disattivazione delle norme.
5. Fare clic sul pulsante *Genera chiave* per generare una chiave prioritaria.

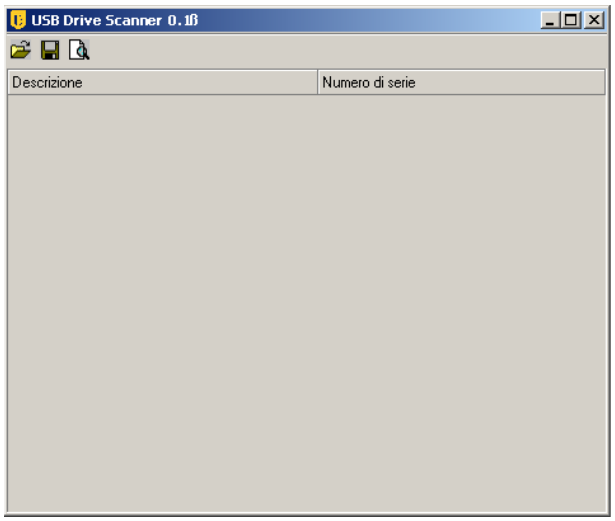
Questa chiave può essere comunicata all'utente finale durante una chiamata all'Help Desk, oppure copiata e incollata in un messaggio e-mail. L'utente a questo punto immette la chiave nella finestra Amministrazione di ZENworks Security Client (consultare la Guida dell'utente di *ZENworks Endpoint Security Management*). La chiave è valida solo per le norme di tale utente e solo per la durata specificata e può essere utilizzata solo una volta.

Nota: Se l'utente esegue il logoff o riavvia il computer durante l'utilizzo della password prioritaria, la password scadrà e sarà necessario emetterne una nuova.

Se sono state scritte delle nuove norme prima della scadenza del tempo limite, l'utente finale deve essere istruito affinché cerchi un aggiornamento norme e non faccia clic sul pulsante *Carica norme* nella finestra di dialogo Informazioni su ZENworks Security Client.

1.11 USB Drive Scanner

È possibile generare un elenco di dispositivi USB autorizzati e importarlo nelle norme utilizzando lo strumento USB Drive Scanner (incluso nel pacchetto di installazione).



Per generare un elenco di dispositivi autorizzati:

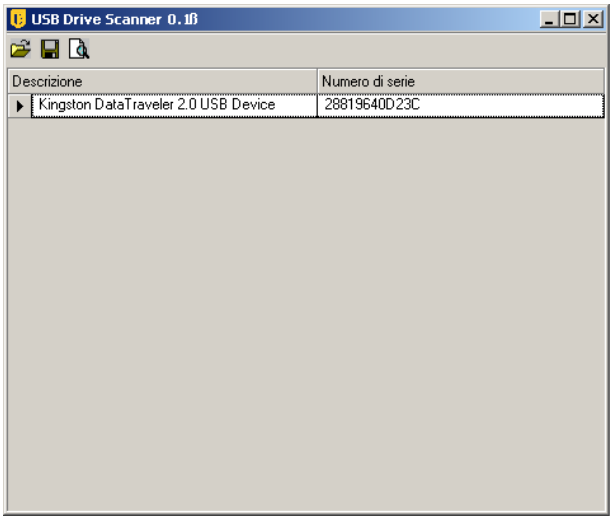
1 Aprire l'applicazione USB Drive Scanner.

Nota: Si tratta di un'installazione distinta dal servizio di gestione e dalla console di gestione. Sul desktop viene visualizzato un collegamento allo strumento.

---

2 Inserire un dispositivo USB nella porta USB del computer. Sul dispositivo deve essere presente un numero di serie.

3 Fare clic sull'icona *Effettua scansione*( ). Il nome del dispositivo e il numero di serie vengono visualizzati nei campi appropriati.



4 Ripetere Passo 2e Passo 3 fino a quando tutti i dispositivi non sono stati immessi nell'elenco.

5 Fare clic sull'icona `Salva` ( ).

Vedere Sezione , “Dispositivi preferiti”, a pagina 52 per istruzioni relative all'importazione dell'elenco nelle norme.

Per modificare un file salvato, fare clic sull'icona *Sfoglia*( ) per aprire il file.

Creazione e distribuzione delle norme di sicurezza

2

ZENworks® Security Client utilizza norme di sicurezza per garantire sicurezza di ubicazione agli utenti mobili. Le decisioni sulla disponibilità delle porte e delle applicazioni di rete, sull'accesso ai dispositivi di memorizzazione dei file e sulla connettività cablata o Wi-Fi vengono prese dall'amministratore per ciascuna ubicazione.

Le norme di sicurezza possono essere create in modo personalizzato per l'azienda, per i singoli gruppi utente o utenti/computer. Le norme di sicurezza possono consentire la completa produttività dei dipendenti proteggendo i punti finali, oppure imporre delle restrizioni relative alle applicazioni e ai componenti hardware che i dipendenti possono utilizzare.

Le seguenti sezioni contengono informazioni aggiuntive:

- Sezione 2.1, “Spostamento nella console di gestione”, a pagina 43
- Sezione 2.2, “Creazione delle norme di sicurezza”, a pagina 45
- Sezione 2.3, “Importazione ed esportazione di norme”, a pagina 105

2.1 Spostamento nella console di gestione

Per iniziare la creazione di norme di sicurezza:

1. Nella console di gestione, fare clic su *File* > *Crea nuove norme*.
2. Specificare il nome delle nuove norme, quindi fare clic su *Crea* per visualizzare la console di gestione in cui sono presenti la barra degli strumenti e le schede delle norme.

Le sezioni riportate di seguito descrivono l'interfaccia utente della console di gestione in quanto correlata alla creazione e alla distribuzione di norme di sicurezza tramite ZENworks® Endpoint Security Management:

- Sezione 2.1.1, “Utilizzo Schede Norme e Albero”, a pagina 43
- Sezione 2.1.2, “Utilizzo della barra degli strumenti Norme.”, a pagina 44

2.1.1 Utilizzo Schede Norme e Albero

Le norme di sicurezza vengono scritte o modificate spostandosi tra le schede disponibili nella parte superiore della console di gestione e utilizzando l'opzione nell'albero*Impostazioni globali* del riquadro sinistro.

Tra le schede disponibili sono incluse:

- **Impostazioni globali norme:** Le Impostazioni globali norme vengono applicate per default in tutte le norme e non sono specifiche dell'ubicazione.

  Le Impostazioni globali norme consentono di configurare le seguenti impostazioni:

  - Impostazioni norme
  - Controllo wireless

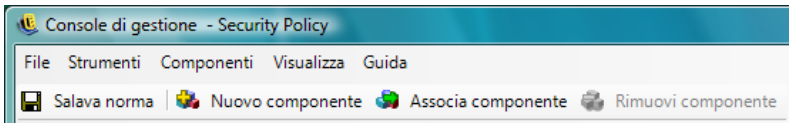
- Hardware di comunicazione
- Controllo periferiche di memorizzazione
- Connettività USB
- Cifratura dei dati
- ZENworks Security Client
- Applicazione VPN

- **Ubicazioni:** Le regole delle norme vengono applicate all'interno di un tipo di ubicazione specifico, sia definito come rete singola che come tipo di rete, ad esempio un bar o aeroporto.
- **Regole di integrità e correzione:** Tali regole assicurano che il software necessario (ad esempio antivirus e antispyware) sia in esecuzione e aggiornato nel dispositivo.
- **Rapporti di conformità:** Indica se i dati dei rapporti (incluso il tipo di dati) vengono richiamati per queste norme specifiche.
- **Pubblicano:** Consente di pubblicare le norme completate a singoli utenti, gruppi utente del servizio di directory e singoli computer.

L'albero delle norme visualizza i componenti dei sottoinsiemi disponibili per le categorie a schede. Ad esempio, *Impostazioni norme globali* include sottoinsiemi di *Impostazioni norme*, *Controllo wireless*, *Hardware com* e *Controllo periferiche di memorizzazione*. Solo gli elementi contenuti nella pagina dei sottoinsiemi principali sono necessari per definire una categoria. I sottoinsiemi restanti sono componenti facoltativi.

2.1.2 Utilizzo della barra degli strumenti Norme.

La barra degli strumenti Norme fornisce sei controlli. Il controllo *Salva norme* è disponibile in tutta la procedura di creazione delle norme, mentre i controlli dei componenti sono disponibili solo nelle schede *Ubicazioni* e *Integrità e correzione*.

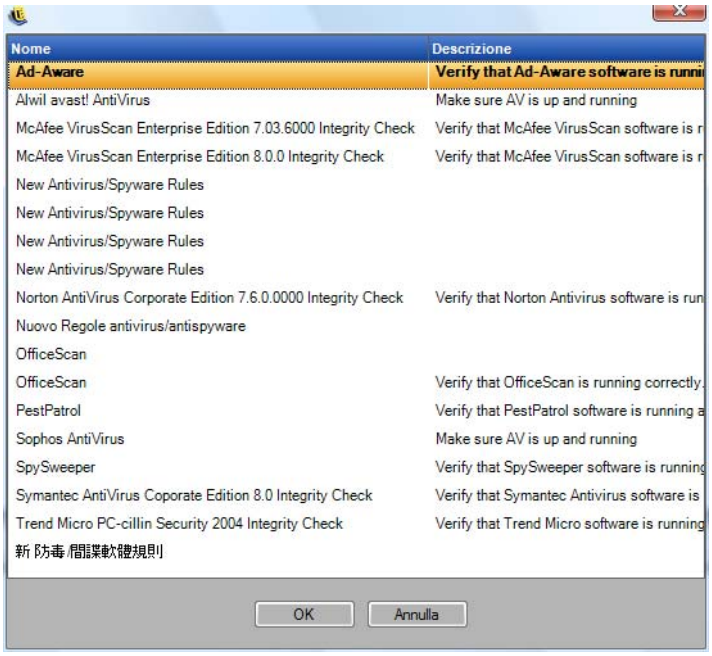


Di seguito vengono riportate le descrizioni degli strumenti:

- **Salva Norme:** Consente di salvare le norme nello stato corrente.

  Importante: Una volta completato ciascun sottoinsieme di componenti, si consiglia di fare clic sull'icona *Salva* nella barra degli strumenti *Norme*. Se i dati immessi in un componente sono incompleti o errati, viene visualizzata la schermata di notifica di errore (vedere Sezione 2.2.6, “Notifica di errore”, a pagina 105 per ulteriori informazioni).

- **Nuovo componente:** crea un nuovo componente in un sottoinsieme Ubicazione o Integrità. Dopo aver salvato le norme, viene reso disponibile un nuovo componente da associare ad altre norme.
- **Associa componente:** Consente di aprire la schermata Seleziona componente per il sottoinsieme corrente. I componenti disponibili includono eventuali componenti predefiniti compresi nell'installazione nonché tutti i componenti creati in altre norme.



Importante: Le modifiche apportate ai componenti associati interessano tutte le altre istanze di quel componente.

Ad esempio, è possibile creare un singolo componente Ubicazione denominato Ufficio che definisca l'ambiente di rete aziendale e le impostazioni di sicurezza da applicare ogni volta che un punto finale si trova in tale ambiente. Il componente può quindi essere applicato a tutte le norme di sicurezza. Gli aggiornamenti apportati alle impostazioni di ambiente o di sicurezza possono essere modificati nel componente delle norme e comporteranno l'aggiornamento dello stesso componente in tutte le altre norme a cui è associato.

Utilizzare il comando *Mostra utilizzo* per visualizzare tutte le altre norme associate al componente corrente.

- **Rimuovi componente:** Consente di rimuovere un componente dalle norme. Il componente rimane disponibile per l'associazione alle norme correnti e alle altre norme.
- **Aggiorna elenco norme:** Consente di aggiornare l'elenco delle norme.
- **Elenco rapporti:** Consente di visualizzare l'elenco dei rapporti.

2.2 Creazione delle norme di sicurezza

1. Nella console di gestione, fare clic su *File* > *Crea nuove norme*.
2. Specificare il nome delle nuove norme, quindi fare clic su *Crea* per visualizzare la console di gestione in cui sono presenti la barra degli strumenti e le schede delle norme.
3. Configurare le impostazioni delle norme utilizzando le informazioni reperibili nelle seguenti sezioni:

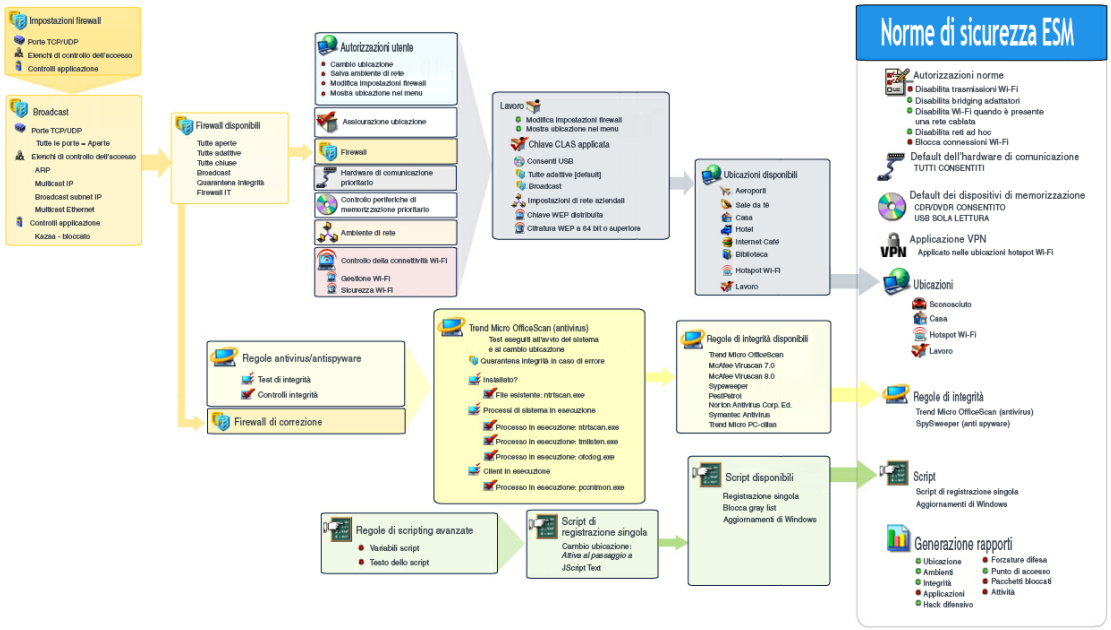
- Sezione 2.2.1, “Impostazioni globali norme”, a pagina 46
- Sezione 2.2.2, “Ubicazioni”, a pagina 68
- Sezione 2.2.3, “Regole di integrità e correzione”, a pagina 93

- Sezione 2.2.4, “Rapporti di conformità”, a pagina 101
- Sezione 2.2.5, “Pubblica”, a pagina 103
- Sezione 2.2.6, “Notifica di errore”, a pagina 105
- Sezione 2.2.7, “Mostra utilizzo”, a pagina 105

Le norme di sicurezza vengono create definendo tutte le impostazioni globali (comportamenti di default), quindi creando e associando i componenti esistenti per tali norme, ad esempio ubicazioni, firewall e regole di integrità, e infine stabilendo per esse la generazione di rapporti di conformità.

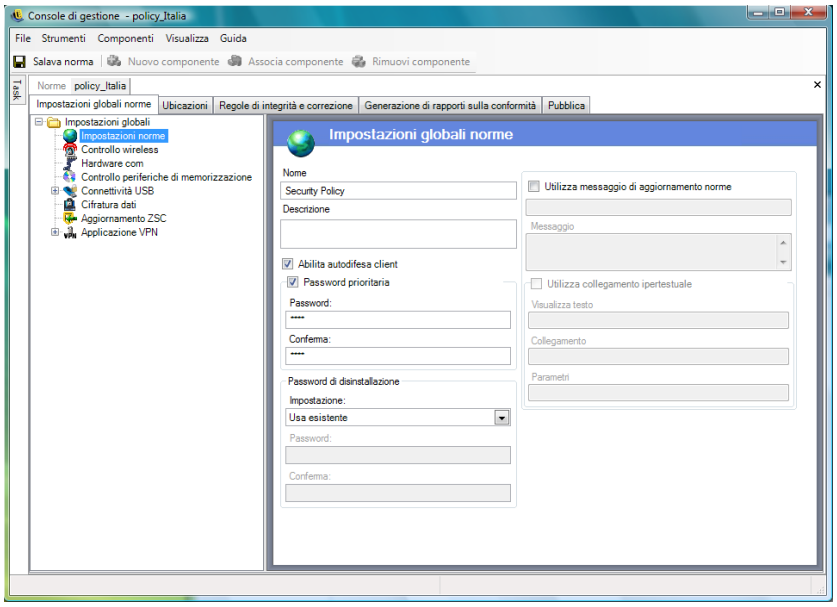
I componenti vengono creati all'interno di norme fittizie oppure associati ad altre norme. Si presume che per le prime norme vengano create tutte ubicazioni, impostazioni di firewall e regole di integrità univoche per l'azienda. Questi componenti vengono memorizzati nel database del servizio di gestione per l'eventuale utilizzo in altre norme in un secondo momento.

Il diagramma riportato di seguito mostra i componenti di ciascun livello e le norme risultanti provenienti dalle selezioni.



2.2.1 Impostazioni globali norme

Le impostazioni globali vengono applicate alle norme come impostazione di default. Per accedere a questo controllo, andare alla console di gestione e fare clic sulla scheda *Impostazioni globali norme*.



Le sezioni seguenti contengono ulteriori informazioni sulle impostazioni che è possibile configurare su base globale:

- “Impostazioni norme” a pagina 47
- “Controllo wireless” a pagina 48
- “Hardware di comunicazione” a pagina 49
- “Controllo periferiche di memorizzazione” a pagina 50
- “Connettività USB” a pagina 53
- “Cifratura dei dati” a pagina 59
- “Aggiornamento ZSC” a pagina 62
- “Applicazione VPN” a pagina 63
- “Messaggio utente personalizzato” a pagina 66
- “Collegamenti ipertestuali” a pagina 67

Impostazioni norme

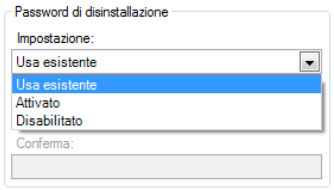
Tali impostazioni includono:

- **Nome e descrizione:** Il nome delle norme viene specificato all'inizio del processo di creazione delle norme stesse. È possibile modificare il nome o fornire una descrizione delle norme.
- **Abilita autodifesa client:** L'autodifesa del client può essere abilitata o disabilitata dalle norme. Quando la casella è selezionata, l'autodifesa del client è attiva. Deselezionando la casella l'autodifesa viene disattivata per tutti i punti finali che utilizzano quelle norme.
- **Password prioritaria:** Questa funzione consente all'amministratore di impostare una password prioritaria in grado di disabilitare temporaneamente le norme per un periodo di tempo specifico. Selezionare la casella *Password prioritaria* e specificare la password nell'apposito campo. Immettere di nuovo la password nel campo di conferma. Utilizzare questa password nel

Generatore password prioritaria per generare la chiave della password per queste norme. Per ulteriori informazioni, consultare Sezione 1.10, “Utilizzo del generatore della chiave della password prioritaria”, a pagina 40.

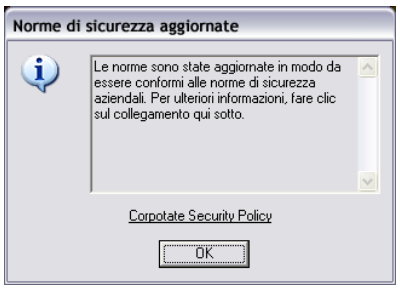
Avviso: È consigliabile non fornire questa password agli utenti. Il Generatore password prioritaria deve essere utilizzato per generare una chiave in via temporanea.

- **Password di disinstallazione:** Si consiglia di installare tutti gli ZENworks*Security Client con una password di disinstallazione per impedire agli utenti di disinstallare il software. La password in genere viene configurata al momento dell'installazione, tuttavia è possibile aggiornarla, abilitarla o disabilitarla mediante le norme.



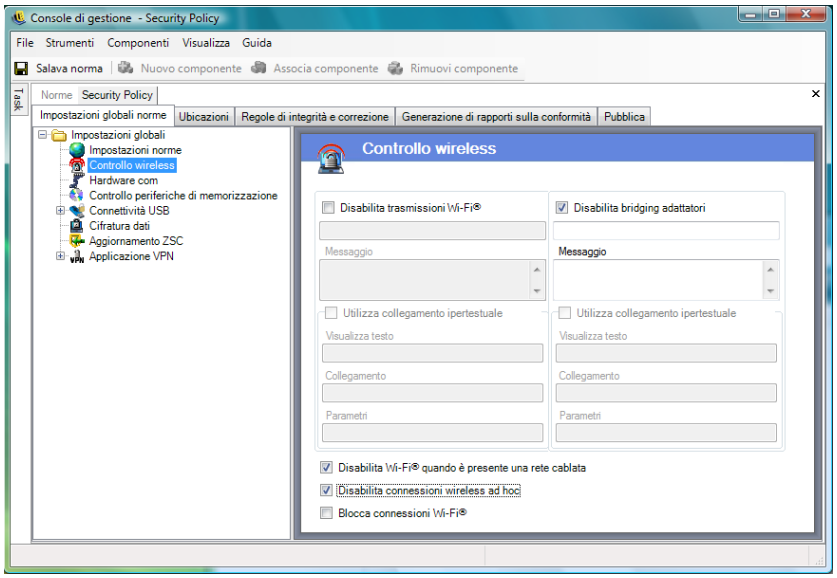
È possibile selezionare una delle seguenti impostazioni dall'elenco a discesa:

  - **Usa esistente:** È l'impostazione di default. Consente di lasciare invariata la password corrente.
  - **Abilitato:** Consente di attivare una password di disinstallazione o di modificarla. Specificare la nuova password e confermarla.
  - **Disabilitato:** Consente di disattivare il requisito della password di disinstallazione.
- **Utilizza messaggio di aggiornamento norme:** È possibile visualizzare un messaggio utente personalizzato a ogni aggiornamento delle norme. Fare clic sulla casella di controllo, quindi specificare le informazioni sul messaggio nei campi appositi.
- **Utilizza collegamento ipertestuale:** È possibile includere un collegamento ipertestuale a informazioni aggiuntive, norme aziendali e così via (vedere “Collegamenti ipertestuali” a pagina 67 per ulteriori informazioni).



Controllo wireless

Controllo wireless imposta i parametri di connessione dell'adattatore a livello globale per garantire la sicurezza sia dei punti finali che della rete. Per accedere a questo controllo, fare clic sulla scheda *Impostazioni globali norme*, quindi sull'icona *Controllo wireless* nell'albero delle norme a sinistra.



Tra le impostazioni di controllo wireless sono incluse le seguenti:

- **Disabilita trasmissioni Wi-Fi:** Consente di disabilitare a livello globale tutti gli adattatori Wi-Fi incluso il dispositivo per la disattivazione completa dell'audio della radio Wi-Fi incorporata.

  È possibile scegliere di visualizzare un messaggio utente personalizzato e un collegamento ipertestuale quando l'utente tenta di attivare una connessione Wi-Fi. Per ulteriori informazioni, vedere la sezione “Messaggio utente personalizzato” a pagina 66.
- **Disabilita bridging adattatori:** Consente di disabilitare la funzionalità di bridging della rete inclusa in Windows *XP, in questo modo l'utente può eseguire il bridging di più adattatori, con funzione di hub nella rete.

  È possibile scegliere di visualizzare un messaggio utente personalizzato e un collegamento ipertestuale quando l'utente tenta una connessione Wi-Fi. Per ulteriori informazioni, vedere la sezione “Messaggio utente personalizzato” a pagina 66.
- **Disabilita Wi-Fi quando è presente una rete cablata:** Consente di disabilitare a livello globale tutti gli adattatori Wi-Fi quando l'utente dispone di una connessione cablata (LAN attraverso la scheda NIC).
- **Disabilita reti ad hoc:** Consente di disabilitare a livello globale tutta le connessioni ad hoc, il che applica la connettività Wi-Fi su una rete (ad esempio tramite un punto di accesso) e limita l'intera rete peer-to-peer di questo tipo.
- **Blocca connessioni Wi-Fi:** Consente di bloccare a livello globale le connessioni Wi-Fi senza disattivare l'audio della radio Wi-Fi. Utilizzare questa impostazione quando si desidera disattivare le connessioni Wi-Fi, continuando a utilizzare i punti di accesso per il rilevamento delle ubicazioni. Per ulteriori informazioni, vedere la sezione Sezione 2.2.2, “Ubicazioni”, a pagina 68.

Hardware di comunicazione

Le impostazioni relative all'hardware di comunicazione controllano, per ogni ubicazione, i tipi di hardware autorizzati ad accedere all'ambiente di rete.

Nota: È possibile impostare i controlli dell'hardware di comunicazione a livello globale nella scheda *Impostazioni globali norme* oppure per singole ubicazioni nella scheda *Ubicazioni*.

Per impostare i controlli hardware di comunicazione a livello globale, fare clic sulla scheda *Impostazioni globali norme*, espandere *Impostazioni globali* nell'albero, quindi fare clic su *Hardware com*.

Per impostare i controlli hardware di comunicazione per un'ubicazione, fare clic sulla scheda *Ubicazioni*, espandere l'ubicazione desiderata nell'albero, quindi scegliere *Hardware com*. Per ulteriori informazioni sulle impostazioni hardware di comunicazione per un'ubicazione, vedere "Hardware di comunicazione" a pagina 71.

Scegliere se abilitare o disabilitare l'impostazione globale per ciascun dispositivo hardware di comunicazione elencato:

- **1394 (FireWire):** * accedere portare
- **IrDA:** Controlla la porta di accesso a infrarossi sul punto finale.
- **Bluetooth:** Controlla la porta di accesso Bluetooth* sul punto finale.
- **Seriale/Parallela:** Controlla la porta di accesso seriale e parallela sul punto finale.

Controllo periferiche di memorizzazione

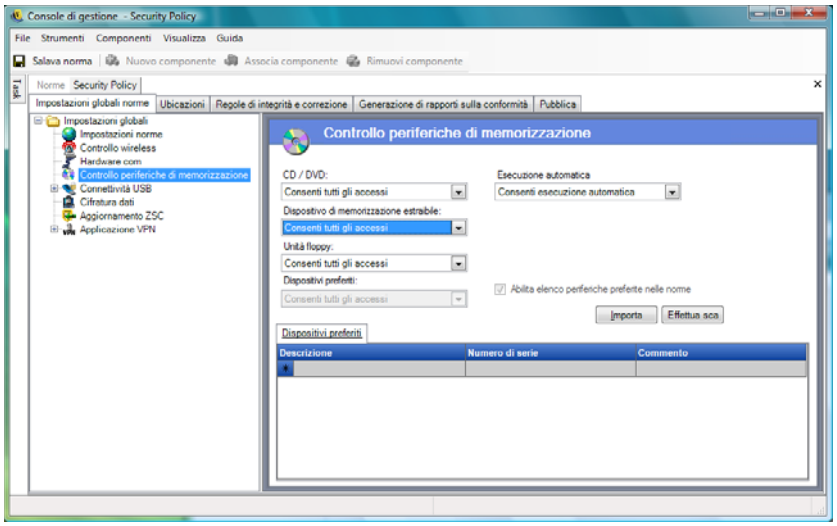
I controlli del dispositivo di memorizzazione configurano le impostazione del dispositivo di default per le norme. Questo prevede che venga indicato se al dispositivo di memorizzazione esterno sia concesso leggere o scrivere file, funzionare nello stato di sola lettura oppure essere totalmente disabilitato. Se disattivati, tali dispositivi non sono in grado di recuperare i dati dal punto finale. Tuttavia il disco rigido e tutte le unità di rete continuano a essere accessibili e funzionanti.

Controllo periferiche di memorizzazione di ZENworks Endpoint Security Management non è consentito quando viene attivato ZENworks Storage Encryption Solution.

Nota: È possibile impostare i controlli del dispositivo di memorizzazione a livello globale nella scheda *Impostazioni globali norme* oppure per singole ubicazioni nella scheda *Ubicazioni*.

Per impostare i controlli del dispositivo di memorizzazione a livello globale, fare clic sulla scheda *Impostazioni globali norme*, espandere *Impostazioni globali* nell'albero, quindi fare clic su *Controllo periferiche di memorizzazione*.

Per impostare i controlli del dispositivo di memorizzazione per un'ubicazione, fare clic sulla scheda *Ubicazioni*, espandere l'ubicazione desiderata nell'albero, quindi scegliere *Controllo periferiche di memorizzazione*. Per ulteriori informazioni, consultare "Hardware di comunicazione" a pagina 71.



Controllo periferiche di memorizzazione è suddiviso nelle seguenti categorie:

- **CD/DVD:** Controlla tutti i dispositivi elencati in *Unità DVD/CD-ROM* in Gestione periferiche di Windows.
- **Dispositivi di memorizzazione estraibili:** Controlla tutte le periferiche segnalate come dispositivi di memorizzazione estraibili in *Unità disco* in Gestione periferiche di Windows.
- **Unità floppy:** Controlla tutti i dispositivi elencati in *Unità Floppy* in Gestione periferiche di Windows.
- **Dispositivi preferiti:** Consente solo i dispositivi di memorizzazione estraibili elencati nella finestra Controllo periferiche di memorizzazione. Tutte le altre periferiche segnalate come estraibili non sono consentite.

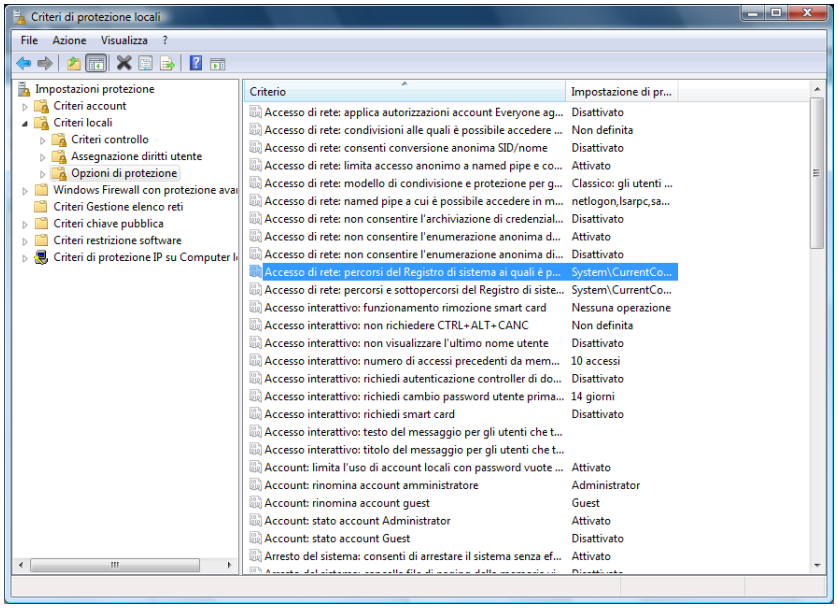
Le periferiche di memorizzazione fisse (unità disco rigido) e le unità di rete (se disponibili) non sono consentite.

Per impostare i valori di default delle norme per i dispositivi di memorizzazione, selezionare l'impostazione globale per entrambi i tipi dagli elenchi a discesa:

- **Abilita:** Il tipo di dispositivo è consentito per default.
- **Disattiva:** l'accesso al tipo di dispositivo non è consentito. Quando un utente cerca di accedere ai file salvati su un determinato dispositivo di memorizzazione, riceve un messaggio di errore, dal sistema operativo o dall'applicazione che sta cercando di accedere al dispositivo di memorizzazione locale, indicante che l'azione non è riuscita.
- **Sola lettura:** Il tipo di dispositivo è impostato su Sola lettura. Quando un utente cerca di scrivere sul dispositivo, riceve un messaggio di errore dal sistema operativo o dall'applicazione che sta cercando di accedere al dispositivo di memorizzazione locale, indicante che l'azione non è riuscita.

Nota: Se si desidera disattivare le unità CD-ROM o le unità floppy su un gruppo di punti finali oppure impostarle su Sola lettura, le impostazioni di sicurezza locale (trasmesse attraverso un oggetto norme di gruppo del servizio di directory) devono aver impostato sia *Periferiche: limita accesso al CD-ROM agli utenti che hanno effettuato l'accesso locale* che *Periferiche: limita accesso al disco floppy agli utenti che hanno effettuato l'accesso locale su Disabilitato*. Per verificare questa

condizione, aprire l'oggetto norme di gruppo o gli Strumenti di amministrazione del computer. Cercare Impostazioni sicurezza locale - Opzioni di sicurezza e verificare che entrambi i dispositivi siano disattivati. L'impostazione di default è Disabilitato.



Le seguenti sezioni contengono informazioni aggiuntive:

- “Dispositivi preferiti” a pagina 52
- “Importazione degli elenchi dei dispositivi” a pagina 53

Dispositivi preferiti

Facoltativamente è possibile aggiungere i dispositivi di memorizzazione estraibili preferiti a un elenco, consentendo l'accesso solo ai dispositivi autorizzati quando l'impostazione locale è utilizzata in un'ubicazione. I dispositivi aggiunti all'elenco devono avere un numero di serie.

Per inserire nell'elenco un dispositivo preferito:

1. Inserire il dispositivo nella porta USB del computer sul quale è installata la console di gestione.
2. Quando il dispositivo è pronto, fare clic sul pulsante *Effettua scansione*. Se il dispositivo ha un numero di serie, nell'elenco verranno visualizzati la descrizione e il numero di serie.
3. Selezionare un'impostazione dall'elenco a discesa (l'impostazione *Dispositivo estraibile globale* non si applica a queste norme):
   - **Abilitato:** Ai dispositivi inseriti nell'elenco dei preferiti sono consentite funzionalità di lettura/scrittura complete; tutti gli altri dispositivi di memorizzazione esterni e le unità USB sono disattivati.
   - **Sola lettura:** Ai dispositivi inseriti nell'elenco dei preferiti sono consentite funzionalità di sola lettura; tutti gli altri dispositivi di memorizzazione esterni e le unità USB sono disattivati.

Ripetere la procedura per ciascun dispositivo autorizzato in queste norme. A tutti i dispositivi verranno applicate le stesse impostazioni.

Nota: Le impostazioni di Controllo periferiche di memorizzazione basate sull'ubicazione hanno la priorità sulle impostazioni globali. Ad esempio, è possibile impostare tutti i dispositivi di memorizzazione esterni come dispositivi autorizzati nell'ubicazione di lavoro, mentre in tutte le altre ubicazioni sono consentiti solo quelli globali di default, limitando in questo modo gli utenti all'uso di quelli inseriti nell'elenco dei preferiti.

Importazione degli elenchi dei dispositivi

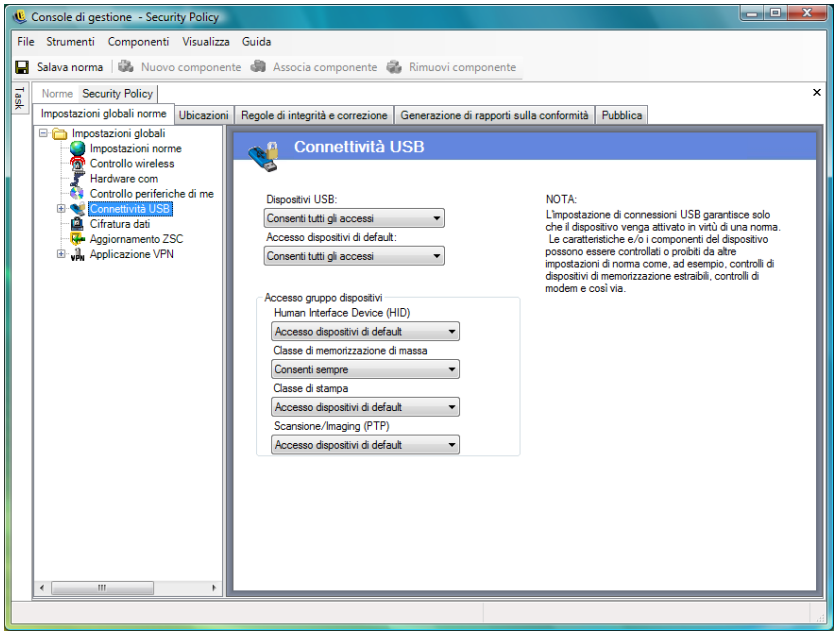
L'applicazione Novell USB Drive Scanner genera un elenco di dispositivi e relativi numeri di serie (vedere Sezione 1.11, “USB Drive Scanner”, a pagina 41). Per importare l'elenco, fare clic su *Importa* e selezionare l'elenco. Nell'elenco verranno popolati i campi *Descrizione* e *Numero di serie*.

Connettività USB

Per tutti i dispositivi che effettuano la connessione tramite il BUS USB, è possibile consentire o non consentire la connessione in base alle norme. I dispositivi possono essere sottoposti a scansione nelle norme dal rapporto Inventario periferiche USB oppure la scansione può essere effettuata su tutti i dispositivi attualmente connessi a un computer. È possibile filtrare i dispositivi in base a produttore, nome prodotto, numeri di serie, tipo e così via. A scopo di supporto, l'amministratore può configurare le norme perché accettino una serie di dispositivi, in base al tipo di produttore (ad esempio, sono consentiti tutti i dispositivi HP) o in base al tipo di prodotto (sono consentiti tutti i dispositivi USB HID, ad esempio mouse e tastiera). Inoltre, è possibile autorizzare singoli dispositivi per evitare l'introduzione nella rete di periferiche non supportate (ad esempio, non sono consentite stampanti fatta eccezione per quella corrente).

Per accedere a questo controllo, fare clic sulla scheda *Impostazioni globali norme*, quindi su *Connettività USB* nell'albero delle norme a sinistra.

Figura 2-1 *Pagina Connettività USB*



Per valutare se l'accesso può essere consentito, si considera innanzitutto se il bus è attivato o disattivato. L'attivazione è definita dall'impostazione *Dispositivi USB*. Se tale impostazione è *Disabilita tutti gli accessi*, il dispositivo viene disattivato e la valutazione viene terminata. Se tale impostazione è *Consenti tutti gli accessi*, il client prosegue la valutazione e continua a cercare corrispondenze a livello di filtro. Come per molti altri campi della Console di gestione ZENworks, quando viene impostato su un'ubicazione, il valore *Dispositivi USB* può anche essere impostato su *Applica impostazioni globali* e al suo posto verrà utilizzato il valore globale di questo campo.

Il client raccoglie i filtri applicati dalle norme, in base all'ubicazione e alle impostazioni globali. Il client raggrupperà quindi i filtri in base all'accesso nei gruppi seguenti:

- **Blocca sempre:** Bloccare sempre il dispositivo. Questa impostazione non può essere ignorata.
- **Consenti sempre:** Consentire sempre l'accesso tranne nel caso in cui per il dispositivo esista una corrispondenza a un filtro *Blocca sempre*.
- **Blocca:** Bloccare l'accesso tranne nel caso in cui per il dispositivo esista una corrispondenza a un filtro *Consenti sempre*.
- **Consenti:** Consentire l'accesso tranne nel caso in cui per il dispositivo esista una corrispondenza a un filtro *Blocca sempre* o *Blocca*.
- **Accesso dispositivi di default:** Se non sono state trovate altre corrispondenze, attribuire al dispositivo lo stesso livello di accesso dell'*Accesso dispositivi di default*.

La valutazione di un dispositivo viene eseguita per ciascun gruppo nell'ordine sopra indicato (prima il gruppo *Blocca sempre*, seguito da *Consenti sempre* e così via). Quando per un dispositivo viene trovata almeno una corrispondenza di un filtro in un gruppo, l'accesso del dispositivo viene impostato su quel livello e la valutazione viene terminata. Se il dispositivo viene valutato per tutti i filtri e non viene trovata alcuna corrispondenza, viene applicato il livello *Accesso dispositivi di default*.

L'accesso dispositivi impostato nell'area *Accesso gruppo dispositivi* viene considerato insieme a tutti gli altri filtri utilizzati in quella determinata ubicazione. Tale operazione viene eseguita generando filtri corrispondenti per ciascuno dei gruppi quando le norme vengono pubblicate nel client. I filtri sono i seguenti:

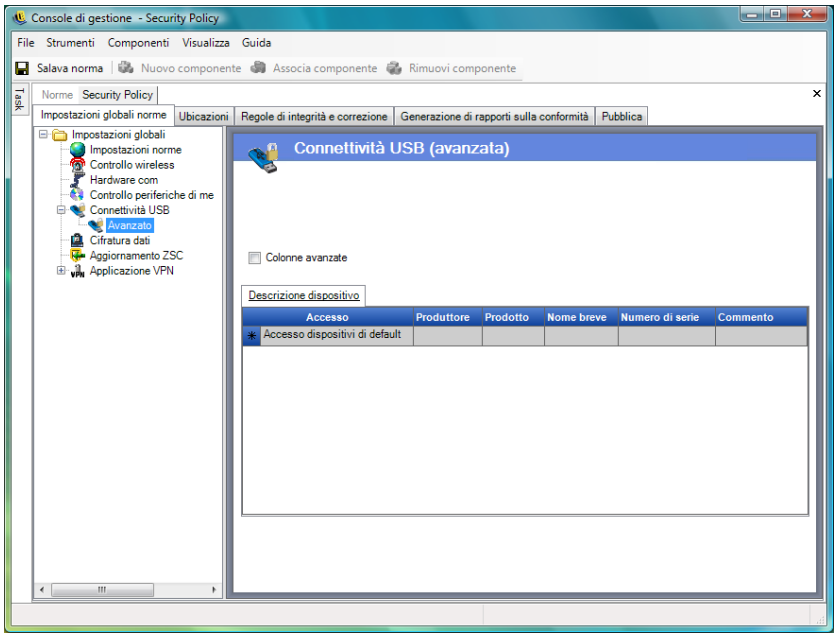
Accesso gruppo dispositivi:	Filtro:
Human Interface Device (HID)	"Classe dispositivo" è pari a 3.
Classe di memorizzazione di massa	"Classe dispositivo" è pari a 8.
Classe di stampa	"Classe dispositivo" è pari a 7.
Scansione/Imaging (PTP)	"Classe dispositivo" è pari a 6.

Avanzata

Nella gran parte dei casi, i quattro gruppi di dispositivi elencati nella pagina Connettività USB (Human Interface Device, Classe di memorizzazione di massa, Classe di stampa e Scansione/Imaging) sono sufficienti per consentire o negare l'accesso alla maggior parte dei dispositivi. Se si dispone di dispositivi che non rientrano in nessuno di questi gruppi, è possibile configurare le impostazioni nella pagina Connettività USB (avanzate). È inoltre possibile utilizzare questa impostazione nella pagina Avanzate per fornire un accesso White List a determinati dispositivi, anche se a questi ultimi può essere negato l'accesso in base alle impostazioni specificate nella pagina Connettività USB.

Per accedere alla pagina delle opzioni avanzate di connettività USB, fare clic sul segno più accanto a *Connettività USB* nell'albero *Impostazioni globali*, quindi fare clic su *Avanzate*. È possibile utilizzare il rapporto di verifica dei dispositivi USB per ottenere tutte le informazioni potenzialmente utilizzabili nella pagina Connettività USB (avanzate).

Figura 2-2 *Pagina Connettività USB (avanzate).*



Tra le colonne disponibili sono incluse:

- **Accesso:** Spostare il mouse su *Accesso dispositivi di default*, quindi specificare un livello di accesso:
  - **Blocca sempre:** Bloccare sempre il dispositivo. Questa impostazione non può essere ignorata.
  - **Consenti sempre:** Consentire sempre l'accesso tranne nel caso in cui per il dispositivo esista una corrispondenza a un filtro *Blocca sempre*.
  - **Blocca:** Bloccare l'accesso tranne nel caso in cui per il dispositivo esista una corrispondenza a un filtro *Consenti sempre*.
  - **Consenti:** Consentire l'accesso tranne nel caso in cui per il dispositivo esista una corrispondenza a un filtro *Blocca sempre* o *Blocca*.
  - **Accesso dispositivi di default:** Se non sono state trovate altre corrispondenze, attribuire al dispositivo lo stesso livello di accesso dell'*Accesso dispositivi di default*.
- **Produttore:** Fare clic sulla colonna *Produttore*, quindi digitare il nome del produttore che si desidera includere nel filtro (ad esempio, Canon).
- **Prodotto:** Fare clic sulla colonna *Prodotto*, quindi digitare il nome del prodotto che si desidera includere nel filtro.
- **Nome breve:** Fare clic sulla colonna *Nome breve*, quindi digitare il nome breve del dispositivo che si desidera includere nel filtro.

- **Numero di serie:** Fare clic sulla colonna *Numero di serie*, quindi digitare il numero di serie del dispositivo che si desidera includere nel filtro.
- **Commento:** Fare clic sulla colonna *Commento*, quindi digitare il commento che si desidera includere nel filtro (ad esempio, Canon).

È possibile fare clic sulla casella *Colonne avanzate* per aggiungere le seguenti colonne: *Versione USB*, *Classe dispositivo, Sottoclasse dispositivo, Protocollo del dispositivo, ID fornitore, ID prodotto, Dispositivo BCD, ID dispositivo O/S* e *Classe dispositivo O/S*.

Un dispositivo rende disponibile un set di attributi per il sistema operativo. Tali attributi trovano corrispondenza da parte del client nei campi richiesti da un filtro. Tutti i campi nel filtro devono corrispondere a un attributo fornito dal dispositivo per poter avere una corrispondenza. Se il dispositivo non fornisce un attributo o un campo richiesto dal filtro, non viene trovata alcuna corrispondenza per il filtro.

Si supponga, ad esempio, che un dispositivo fornisca i seguenti attributi: Produttore: Acme Classe: 8, Numero di serie: "1234".

Il filtro Classe == 8 riuscirebbe a trovare una corrispondenza per il dispositivo. Il filtro Prodotto == "Acme" non riuscirebbe a trovare alcuna corrispondenza perché il dispositivo non ha fornito al sistema operativo un attributo denominato Prodotto.

I campi riportati di seguito sono sottostringhe per le quali è stata trovata una corrispondenza: Produttore, Prodotto e Nome breve. Per tutti gli altri campi esistono corrispondenze esatte.

In realtà, il campo relativo al numero di serie USB è univoco solo se oltre ad esso vengono specificati i seguenti campi: Versione USB, ID fornitore, ID prodotto, Dispositivo BCD.

I valori validi correnti per la versione USB in formato decimale sono: 512 - USB 2.0, 272 - USB 1.1, 256 - USB 1.0.

Le seguenti sezioni contengono informazioni aggiuntive:

- “Aggiunta manuale di dispositivi” a pagina 56
- “Inserimento nella white list/black list di un dispositivo in base al tipo di prodotto” a pagina 57

Aggiunta manuale di dispositivi

Il seguente metodo consente di popolare l'elenco in modo tale da consentire o non consentire la connettività USB per i dispositivi:

Per aggiungere manualmente un dispositivo:

1. Inserire il dispositivo nella porta USB del computer sul quale è installata la console di gestione.

2. Quando il dispositivo è pronto, scegliere il pulsante *Effettua scansione*. Se il dispositivo ha un numero di serie, nell'elenco verranno visualizzati la Descrizione e il Numero di serie.
3. Selezionare un'impostazione dall'elenco a discesa (l'impostazione *Dispositivo estraibile globale* non viene applicata per queste norme):
   - **Abilita:** I dispositivi inseriti nell'elenco dei preferiti dispongono di funzionalità di lettura e scrittura; tutti gli altri dispositivi di memorizzazione esterni e le unità USB sono disattivati.
   - **Sola lettura:** I dispositivi inseriti nell'elenco dei preferiti dispongono di funzionalità di sola lettura; tutti gli altri dispositivi di memorizzazione esterni e le unità USB sono disattivati.

Ripetere questi passaggi per ciascun dispositivo che si desidera autorizzare con le presenti norme. A tutti i dispositivi verranno applicate le stesse impostazioni.

Inserimento nella white list/black list di un dispositivo in base al tipo di prodotto

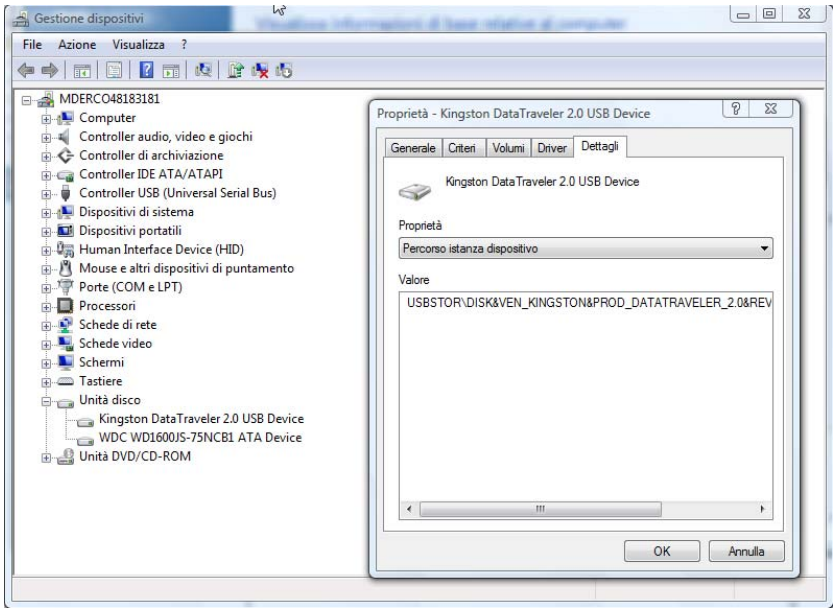
Nella sezione riportata di seguito viene descritta la modalità di inserimento nella white list/black list di un dispositivo USB in base al tipo di prodotto.

Nota: Di seguito viene riportata una procedura di esempio relativa alla modalità di individuazione del tipo di prodotto del dispositivo di memorizzazione estraibile USB in uso. La riuscita della procedura dipende dalle informazioni sul dispositivo rese disponibili dal relativo produttore. È possibile utilizzare il rapporto di verifica dei dispositivi USB per ottenere tutte le informazioni potenzialmente utilizzabili nella pagina Connettività USB (avanzate).

Per determinare il tipo di prodotto del dispositivo di memorizzazione estraibile USB:

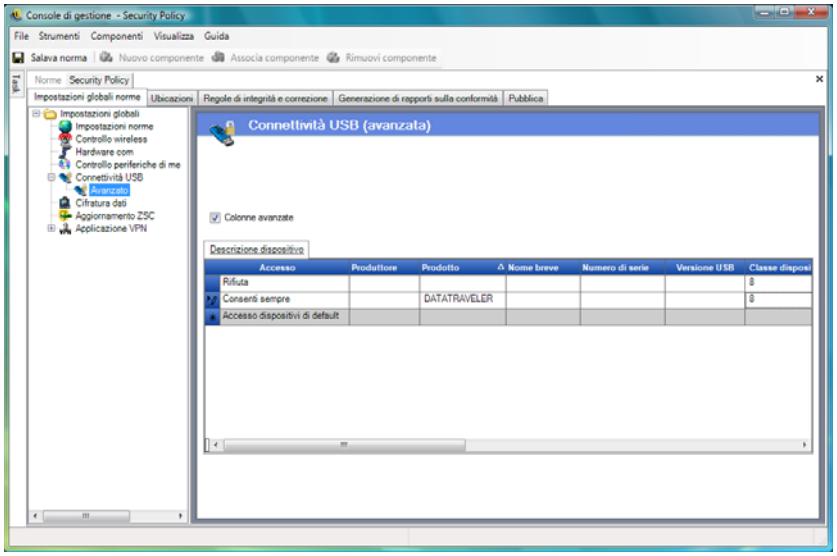
1. Nella console di Gestione computer di Microsoft Windows fare clic su *Gestione periferiche*.
2. Fare clic sul segno più accanto a *Unità disco* per espandere l'albero.
3. Fare clic con il pulsante destro del mouse sul dispositivo USB, quindi scegliere *Proprietà* per visualizzare la finestra di dialogo Proprietà del dispositivo.
4. Fare clic sulla scheda *Dettagli*, quindi selezionare *ID istanza periferica* dall'elenco discesa.

   Il tipo di prodotto viene visualizzato dopo &PROD nell'ID istanza periferica. Nell'esempio riportato di seguito, DATATRAVELER è il tipo di prodotto.



Inserimento di un dispositivo USB nella white list: Non modificare le impostazioni di default nella pagina Connettività USB . Nella pagina Avanzate, creare due righe. Nella prima riga, specificare *Rifiuta* nella colonna *Accesso* e 8 nella colonna *Classe dispositivo* (se *Classe dispositivo* non è disponibile, selezionare la casella di controllo *Colonne avanzate*). Nella seconda riga, specificare *Consenti sempre* nella colonna *Accesso*, il tipo di prodotto (ad esempio, DATATRAVELER) nella colonna *Prodotto* e 8 nella colonna *Classe dispositivo*.

La pagina Connettività USB (avanzate) avrà il seguente aspetto:

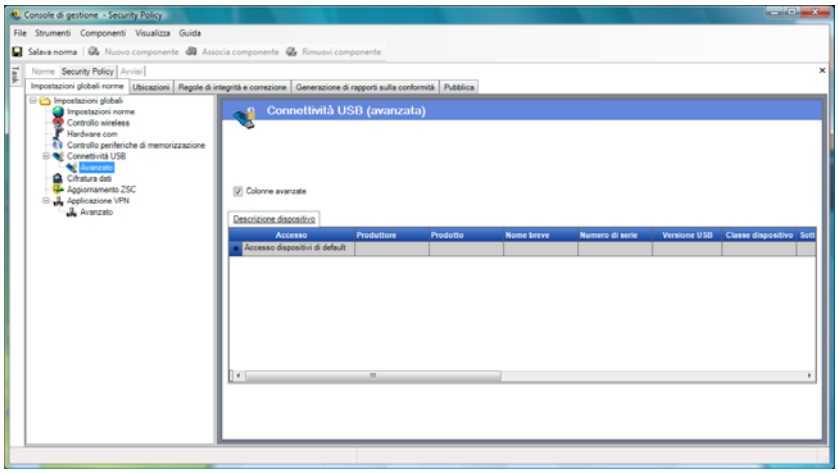


USB DATATRAVELER è ora incluso nella white list, il che significa che è autorizzato a eseguire l'accesso, mentre a tutti gli altri dispositivi di memorizzazione estraibili USB tale accesso è negato.

Inserimento di un dispositivo USB nella black list: Non modificare le impostazioni di default nella pagina Connettività USB. Nella pagina Avanzate, creare due righe. Nella prima riga, specificare *Consenti sempre* nella colonna *Accesso* e 8 nella colonna *Classe dispositivo* (se *Classe*

dispositivo non è disponibile, selezionare la casella di controllo *Colonne avanzate*). Nella seconda riga, specificare *Blocca sempre* nella colonna *Accesso*, il tipo di prodotto (ad esempio, DATATRAVELER) nella colonna *Prodotto* e 8 nella colonna *Classe dispositivo*.

La pagina Connettività USB (avanzate) avrà il seguente aspetto:



USB DATATRAVELER è ora incluso nella black list, il che significa che non è autorizzato a eseguire l'accesso, mentre a tutti gli altri dispositivi di memorizzazione estraibili USB tale accesso è consentito.

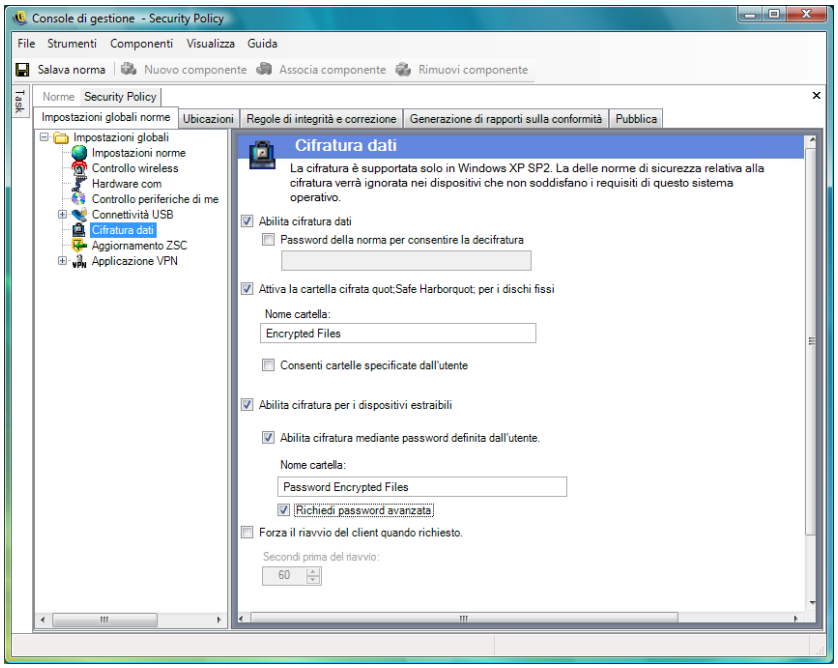
Cifratura dei dati

La cifratura dei dati stabilisce se la cifratura dei file è applicata sul punto finale e quale tipo di cifratura è disponibile. È possibile cifrare i dati per permettere la condivisione dei file (con protezione basata su password) o consentirne l'accesso in sola lettura sui computer che eseguono ZENworks Storage Encryption Solution.

Nota: La cifratura è supportata solo in Windows XP SP2. La porzione di cifratura delle norme di sicurezza viene ignorata nei dispositivi che non soddisfano questo requisito di sistema operativo.

Controllo periferiche di memorizzazione di ZENworks Endpoint Security Management non è consentito quando viene attivata ZENworks Storage Encryption Solution.

Per accedere a questo controllo, fare clic sulla scheda *Impostazioni globali norme*, quindi su *Cifratura dati* nell'albero delle norme a sinistra.



Per attivare i singoli controlli, fare clic sulla casella di controllo *Abilita cifratura dati*.

Nota: Le chiavi di cifratura vengono distribuite a tutti i computer che ricevono norme dal servizio di distribuzione, indipendentemente dall'attivazione o meno della cifratura dei dati. Questo controllo tuttavia istruisce ZENworks Security Client ad attivare le unità di cifratura affinché gli utenti siano in grado di leggere i file che sono stati loro inviati senza richiedere l'utility di decifratura file. Per ulteriori informazioni, vedere Sezione 1.9, “Utilizzo dell'utility di decifratura file ZENworks”, a pagina 39.

Stabilire i livelli di cifratura consentiti dalle presenti norme:

- **Password della norma per consentire la decifratura:** Specificare una password che tutti gli utenti che utilizzano queste norme devono immettere prima di decifrare eventuali file cifrati presenti nelle cartelle `Safe Harbor`.

  Questa impostazione è facoltativa. Lasciarla vuota per non richiedere la password.

- **Attiva la cartella cifrata "Safe Harbor" per i dischi fissi (volume non di sistema):**

  consente di generare una cartella nella radice dei volumi non di sistema nel punto finale denominata `File protetti da cifratura`. Tutti i file collocati in questa cartella vengono cifrati e gestiti da ZENworks Security Client. I dati collocati in questa cartella vengono automaticamente cifrati e sono accessibili solo da parte di utenti autorizzati.

È possibile modificare il nome della cartella facendo clic sul campo Nome cartella, evidenziando il testo corrente e inserendo il nome desiderato.

- **Cifra la cartella "Documenti personali" dell'utente:** Selezionare questa casella per impostare la cartella `Documenti personali` dell'utente come cartella cifrata (che va ad aggiungersi alla cartella `Safe Harbor`). Ciò vale solo per la cartella locale `Documenti personali`.
- **Allow user specified folders (volume non di sistema):** selezionare questa casella per consentire agli utenti di selezionare le cartelle cifrate del computer in uso. Ciò vale solo per le cartelle locali. Non è possibile cifrare i dispositivi di memorizzazione estraibili o le unità di rete.

Avviso: Prima di disabilitare la cifratura dei dati, assicurarsi che tutti i dati memorizzati in queste cartelle siano stati estratti dall'utente e salvati in un'altra ubicazione.

- **Abilita cifratura dei dispositivi di memorizzazione estraibili:** Tutti i dati scritti su dispositivi di memorizzazione estraibili proveniente da un punto finale protetto da queste norme vengono cifrati. Gli utenti che utilizzano queste norme sui propri computer sono in grado di leggere i dati, pertanto è possibile la condivisione dei file tramite dispositivo di memorizzazione estraibile all'interno di un gruppo di norme. Gli utenti esterni a questo gruppo di norme non sono in grado di leggere i file cifrati presenti sull'unità e possono solo accedere ai file presenti nella cartella `File condivisi` (se attivata) mediante apposita password.
  - **Abilita cifratura mediante password definita dall'utente:** Questa impostazione offre all'utente la possibilità di memorizzare i file in una cartella `File condivisi` sul dispositivo di memorizzazione estraibile (la cartella viene generata automaticamente al momento dell'applicazione di questa impostazione). Quando i file vengono aggiunti alla cartella, l'utente può specificare una password che verrà utilizzata per estrarre i file dagli utenti che non fanno parte del gruppo di norme corrente .

    È possibile modificare il nome della cartella facendo clic sul campo *Nome cartella*, evidenziando il testo corrente e inserendo il nome desiderato.
  - **Richiedi password avanzata:** Questa impostazione obbliga l'utente a impostare una password complessa per la cartella File condivisi. Una password complessa richiede quanto riportato di seguito:
    - sette o più caratteri
    - almeno uno di ciascuno dei quattro tipi di caratteri elencati:
      - lettere maiuscole dalla A alla Z
      - lettere minuscole dalla a alla z
      - numeri da 0 a 9
      - almeno un carattere speciale ~!@#$%^&*()+{}[]:;<>?,./

    Ad esempio: y9G@wb?

Avviso: Prima di disabilitare la cifratura dei dati, assicurarsi che tutti i dati memorizzati nei dispositivi di memorizzazione estraibili siano stati estratti e salvati in un'altra ubicazione.

- **Forza il riavvio del client quando richiesto:** Quando si aggiunge la cifratura alle norme, queste non diventeranno attive fino a quando il punto finale non viene riavviato. Questa impostazione impone il riavvio del sistema, visualizzando un conto alla rovescia e un

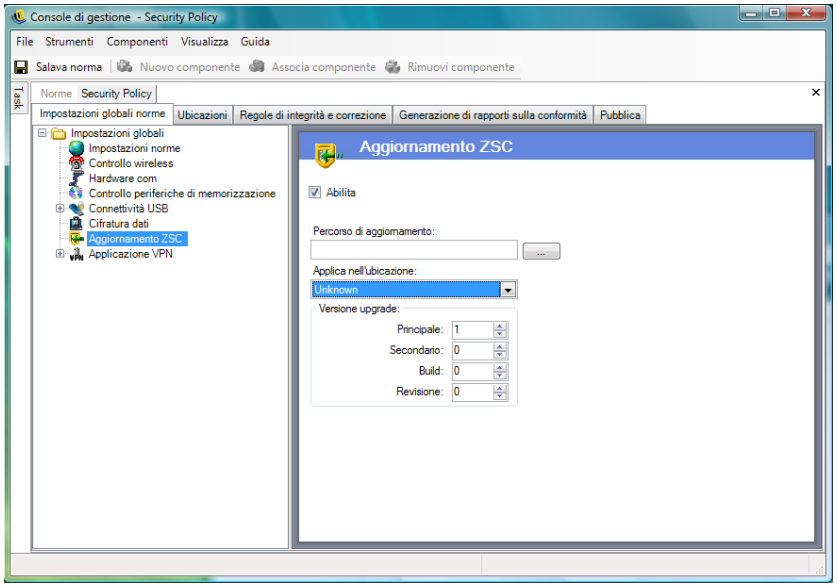
messaggio che avvisa l'utente che il computer verrà riavviato entro un determinato numero di secondi. L'utente ha a disposizione il tempo indicato per salvare il lavoro prima del riavvio del computer.

I riavvii sono necessari quando la cifratura viene attivata per la prima volta nelle norme e quando viene attivata la cifratura “Safe Harbor” o la cifratura di un dispositivo di memorizzazione estraibile (se attivato separatamente dall'attivazione della cifratura). Ad esempio, quando le norme di cifratura vengono applicate per la prima volta, sono necessari due riavvii, uno per inizializzare i driver e l'altro per cifrare eventuali Safe Harbor. Se vengono selezionati Safe Harbor aggiuntivi dopo che le norme sono state applicate, è necessario un solo riavvio per inserire il Safe Harbor nelle norme.

Aggiornamento ZSC

A riparazione ZENworks sicurezza client ZENworks Endpoint Security Management Anziché fornire un nuovo programma di installazione da distribuire a tutti i punti finali tramite MSI, la funzione di aggiornamento di ZENworks Security Client consente all'amministratore di dedicare un'area delle rete alla distribuzione delle patch di aggiornamento agli utenti finali, quando si collegano a quell'ambiente di rete.

Per accedere a questo controllo, fare clic sulla scheda *Impostazioni globali norme*, quindi su *Aggiornamento ZSC* nell'albero delle norme a sinistra.



Per semplificare e proteggere la distribuzione delle patch a tutti gli utenti di ZENworks Security Client:

1. Selezionare *Abilita* per attivare la schermata e la regola.
2. Specificare l'ubicazione in cui ZENworks Security Client cerca gli aggiornamenti.

   In base a quanto consigliato al punto successivo, è preferibile selezionare l'ubicazione associata all'ambiente aziendale (ad esempio l'ubicazione di lavoro).
3. Specificare l'URI in cui è stata salvata la patch.

È necessario che punti al file della patch, che può essere il file setup.exe per ZENworks Security Client o un file MSI creato dal file .exe. Per motivi di sicurezza, si consiglia di memorizzare questi file in un server sicuro, dietro il firewall aziendale.

4 Specificare le informazioni sulla versione del file negli appositi campi.

Le informazioni sulla versione sono reperibili con l'installazione di ZENworks Security Client e aprendo la finestra Informazioni su (per i dettagli, consultare la *Guida all'installazione di ZENworks Endpoint Security Management*). Il numero di versione del file `STEngine.exe` è quello da utilizzare nei suddetti campi.

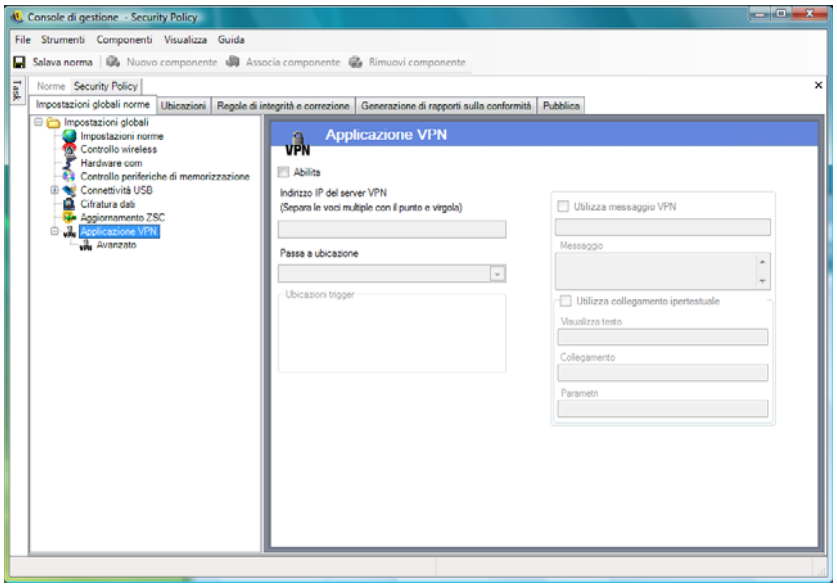
Ogni volta che l'utente immette l'ubicazione assegnata, ZENworks Security Client verifica che nell'URI sia presente un aggiornamento corrispondente al numero di versione. Se è disponibile un aggiornamento, ZENworks Security Client lo scarica e lo installa.

Applicazione VPN

Questa regola impone l'utilizzo di una VPN (Virtual Private Network) basata su SSL o basata su client. Di solito questa regola viene applicata agli hotspot wireless, consentendo all'utente di associarsi e connettersi alla rete pubblica. Nel momento in cui ciò avviene, la regola tenta di stabilire la connessione VPN, dopodiché passa l'utente a un'ubicazione e un'impostazione firewall definita. Tutti i parametri sono a discrezione dell'amministratore. Tutti i parametri hanno la priorità sulle impostazioni esistenti relative alle norme. Il componente Applicazione VPN richiede che l'utente sia collegato a una rete per poter essere avviato.

Nota: La funzione è disponibile solo nell'installazione di ZENworks Endpoint Security Management e non può essere utilizzata per le norme di sicurezza di UWS.

Per accedere a questo controllo, fare clic sulla scheda *Impostazioni globali norme*, quindi su *Applicazione VPN* nell'albero delle norme a sinistra.



Per utilizzare la regola di applicazione VPN, è necessario esistano almeno due ubicazioni.

Per aggiungere l'applicazione VPN a norme di sicurezza nuove o esistenti:

1. Selezionare *Abilita* per attivare la schermata e la regola.
2. Specificare gli indirizzi IP del server VPN nell'apposito campo. Se vengono specificati più indirizzi, separare ciascun indirizzo con un punto e virgola (ad esempio: 10.64.123.5;66.744.82.36).
3. Selezionare *Passa a ubicazione* dall'elenco a discesa.

   Si tratta dell'ubicazione in cui passa ZENworks Security Client nel momento in cui viene attivata la VPN. Tale ubicazione implica alcune limitazioni e per default deve utilizzare un'unica impostazione firewall restrittiva.

   L'impostazione del firewall *Tutte chiuse*, che consente di chiudere tutte le porte TCP/UDP, è consigliata per un'applicazione VPN rigorosa. Questa impostazione impedisce qualunque attività di networking non autorizzata, mentre l'indirizzo IP della VPN funziona come elenco di controllo dell'accesso per il server VPN, consentendo la connettività di rete.
4. Selezionare le ubicazioni del trigger in cui viene utilizzata la regola di applicazione VPN. Per un'applicazione VPN rigorosa, si consiglia di utilizzare per queste norme l'ubicazione sconosciuta di default. Dopo che l'autenticazione della rete, la regola VPN viene attivata e trasmessa all'ubicazione di destinazione assegnata.

   Nota: Il passaggio di ubicazione si verifica prima della connessione VPN e dopo l'autenticazione della rete.

   ---
5. Immettere un messaggio utente personalizzato da visualizzare al momento dell'autenticazione della VPN sulla rete. Per le VPN non basate su client, non è necessario eseguire altre operazioni.

   Per le VPN basate su client, includere un collegamento ipertestuale che punti al client VPN.

   Ad esempio: `C:\Programmi\Cisco Systems\VPN Client\ipsecdialer.exe`

   Questo collegamento avvia l'applicazione, tuttavia l'utente dovrà comunque eseguire il login. È possibile specificare uno switch nel campo *Parametri* oppure creare un file batch a cui puntare, anziché utilizzare l'eseguibile del client.

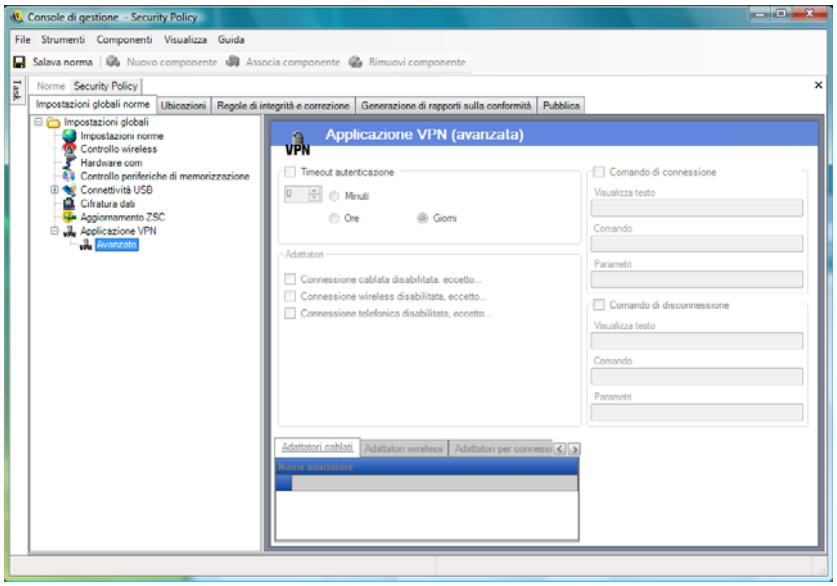
Nota: I client VPN che generano adattatori virtuali (ad esempio, Cisco Systems *VPN Client 4.0) visualizzano il messaggio `Le norme sono state aggiornate`. Le norme non sono state aggiornate, ZENworks Security Client sta semplicemente confrontando l'adattatore virtuale con le eventuali limitazioni previste dalle norme correnti.

Le impostazioni standard di applicazione VPN descritte sopra rendono la connettività VPN facoltativa. Agli utenti viene concessa la connettività alla rete corrente, a prescindere dall'avvio della VPN. Per un'applicazione più precisa, vedere Impostazioni VPN avanzate.

Impostazioni VPN avanzate

I controlli VPN avanzati consentono di impostare i timeout di autenticazione per impedire errori VPN, collegare i comandi per VPN basate su client e utilizzare i controlli degli adattatori per controllare gli adattatori autorizzati ad accedere alla VPN.

Per accedere a questo controllo, fare clic sulla scheda *Impostazioni globali norme*, quindi sul simbolo "+" accanto ad *Applicazione VPN* e infine su *Avanzate* nell'albero delle norme a sinistra.



È possibile configurare le seguenti impostazioni di applicazione VPN avanzate:

Timeout autenticazione: Per proteggere da eventuali errori di connettività della VPN, gli amministratori possono impostare il punto finale sull'impostazione del firewall protetta *Passa a ubicazione*. Il *timeout di autenticazione* indica la quantità di tempo in cui ZENworks Security Client rimane in attesa per ottenere l'autenticazione per il server VPN. Si consiglia di impostare un valore superiore a 1 minuto per questo parametro, per consentire l'autenticazione con connessioni più lente.

Comandi di connessione/disconnessione: Quando si utilizza il timer di autenticazione, i comandi di *connessione* e di *disconnessione* controllano l'attivazione della VPN basata su client. Inserire l'ubicazione del client VPN e gli switch necessari nei campi*Parametri* Il comando di disconnessione è opzionale e interessa i client VPN che richiedono la disconnessione dell'utente prima di eseguire il logout della rete.

Nota: I client VPN che generano adattatori virtuali (ad esempio, Cisco Systems VPN Client 4.0) visualizzano il messaggio: `Le norme sono state aggiornate` e potrebbero spostarsi temporaneamente dall'ubicazione corrente. Le norme non sono state aggiornate. ZENworks Security Client sta semplicemente confrontando l'adattatore virtuale con le eventuali limitazioni previste dalle norme correnti. Quando si eseguono client VPN di questo tipo, non deve essere utilizzato il collegamento ipertestuale del comando di disconnessione.

Adattatori: Si tratta sostanzialmente di mini norme sugli adattatori specifiche per l'applicazione VPN.

Se si seleziona un adattatore (trasformandone lo stato in Abilitato, eccetto), se ne autorizza la connessione alla VPN (la connessione wireless è specifica per il tipo di scheda).

Gli adattatori presenti negli elenchi di eccezioni non sono autorizzati a connettersi alla VPN, mentre tutti gli altri adattatori di quel tipo possono connettersi alla VPN.

Se un adattatore non è selezionato (Disabilitato, eccetto), solo gli adattatori inseriti nell'elenco di eccezione sono autorizzati a connettersi alla VPN. Per tutti gli altri adattatori la connessione non è consentita.

Questo controllo può essere utilizzato, ad esempio, per gli adattatori non compatibili con la VPN o per gli adattatori non supportati dal reparto IT.

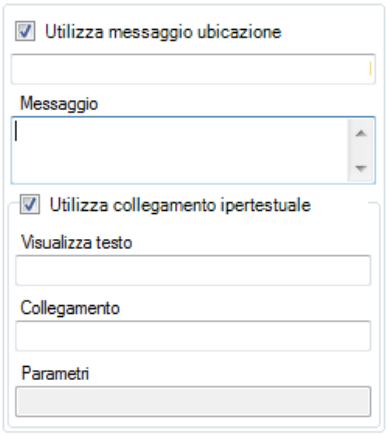
Questa regola ha la priorità sulle norme relative agli adattatori impostate per l'ubicazione di destinazione.

Messaggio utente personalizzato

I messaggi utente personalizzati consentono all'amministratore di ZENworks Endpoint Security Management di creare messaggi che rispondono direttamente alla domande sulle norme di sicurezza quando l'utente incontra restrizioni relative alla sicurezza applicate dalle norme. I messaggi utente personalizzati forniscono inoltre istruzioni specifiche all'utente. I controlli dei messaggi utente sono disponibili in diversi componenti delle norme.

Per creare un messaggio utente personalizzato:

1. Specificare un titolo per il messaggio. Quescasella per il testo del messaggioto viene visualizzato nella barra del titolo della casella per il testo del messaggio.
2. Specificare il messaggio. La lunghezza massima del messaggio è 1.000 caratteri.
3. Se è richiesto un collegamento ipertestuale, selezionare la casella *Mostra collegamenti ipertestuali* e specificare le informazioni necessarie.



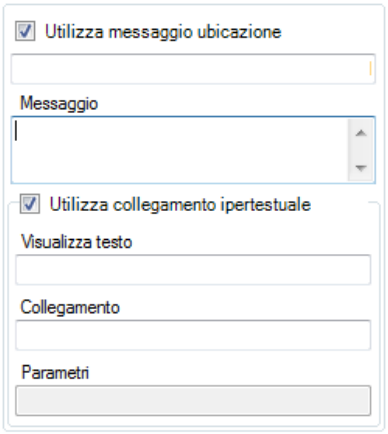
Nota: La modifica del messaggio o del collegamento ipertestuale in un componente condiviso si riflette in tutte le altre istanze del componente. Utilizzare il comando *Mostra utilizzo* per visualizzare tutte le altre norme associate al componente.

Collegamenti ipertestuali

Un amministratore può incorporare i collegamenti ipertestuali nei messaggi personalizzati per fornire spiegazioni sulle norme di sicurezza o collegamenti agli aggiornamenti del software che consentono di mantenere la conformità all'integrità. I collegamenti ipertestuali sono disponibili in diversi componenti delle norme. È possibile creare un collegamento ipertestuale VPN che punta al file eseguibile del client VPN o a un file batch che può essere eseguito per consentire all'utente di accedere direttamente alla VPN (vedere "Applicazione VPN" a pagina 63 per ulteriori informazioni).

Per creare un collegamento ipertestuale:

1. Specificare un nome per il collegamento. Si tratta del nome visualizzato sotto il messaggio. Viene richiesto anche per i collegamenti ipertestuali VPN avanzati.
2. Specificare il collegamento ipertestuale.
3. Specificare eventuali switch o altri parametri per il collegamento.

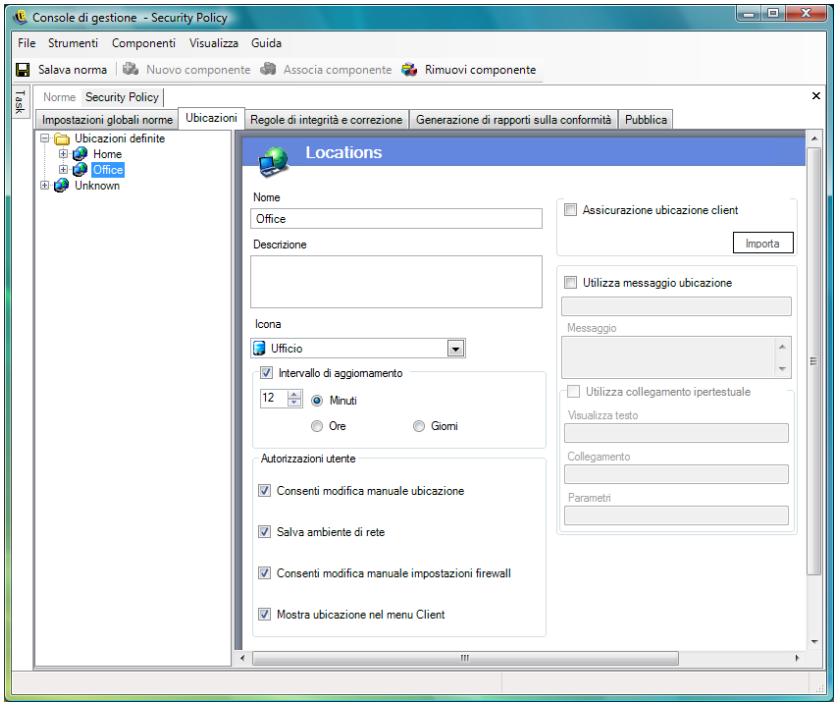


Nota: La modifica del messaggio o del collegamento ipertestuale in un componente condiviso si riflette in tutte le altre istanze del componente. Utilizzare il comando *Mostra utilizzo* per visualizzare tutte le altre norme associate al componente.

2.2.2 Ubicazioni

Le ubicazioni sono gruppi di regole assegnate ad ambienti di rete. Tali ambienti possono essere impostati nelle norme (vedere "Ambienti di rete" a pagina 85) o dall'utente, se dispone dell'autorizzazione. Ad ogni ubicazione è possibile assegnare impostazioni di sicurezza univoche, negando l'accesso a determinati tipi di networking e di hardware in ambienti di rete più pericolosi e concedendo un accesso più ampio nell'ambito degli ambienti affidabili.

Per accedere ai controlli delle ubicazioni, fare clic sulla scheda *Ubicazioni*.



Le seguenti sezioni contengono informazioni aggiuntive:

- "Informazioni sulle ubicazioni" a pagina 69
- "Hardware di comunicazione" a pagina 71
- "Controllo periferiche di memorizzazione" a pagina 73
- "Impostazioni firewall" a pagina 74
- "Ambienti di rete" a pagina 85
- "Connettività USB" a pagina 86
- "Gestione Wi-Fi" a pagina 88
- "Sicurezza Wi-Fi" a pagina 92

Informazioni sulle ubicazioni

È possibile configurare i seguenti tipi di ubicazione:

Ubicazione sconosciuta: Tutte le norme hanno un'ubicazione di default sconosciuta. Si tratta dell'ubicazione alla quale vengono trasferiti gli utenti quando abbandonano un ambiente di rete conosciuto. Questa ubicazione sconosciuta è univoca per tutte le norme e non è disponibile come componente condiviso. Non è possibile impostare o salvare ambienti di rete per questa ubicazione.

Per accedere ai controlli relativi all'ubicazione sconosciuta, aprire la scheda *Ubicazioni* e fare clic sull'ubicazione *Sconosciuta* nell'albero delle norme a sinistra.

Ubicazioni definite: È possibile creare ubicazioni definite per le norme o associare ubicazioni esistenti (quelle create per altre norme).

Per creare una nuova ubicazione:

1. Fare clic su *Ubicazioni definite*, quindi sul pulsante *Nuovo componente* della barra degli strumenti.
2. Assegnare un nome all'ubicazione e fornire una descrizione.
3. Definire le impostazioni dell'ubicazione:

   Icona: selezionare un'icona di ubicazione per fornire all'utente un suggerimento visivo che consenta di identificare l'ubicazione corrente. Questa icona viene visualizzata nella barra delle applicazioni dell'area di notifica. Utilizzare l'elenco a discesa per visualizzare e selezionare una delle icone di ubicazione disponibili.

   Intervallo di aggiornamento: specificare l'impostazione che consente di determinare la frequenza con cui viene verificata la disponibilità di un aggiornamento delle norme quando si accede all'ubicazione. La frequenza viene impostata in minuti, ore o giorni. La deselezione di questo parametro significa che ZENworks Security Client non verifica la presenza di un aggiornamento per questa ubicazione.

   Autorizzazioni utente: Specificare le autorizzazioni utente:

   - **Consenti modifica manuale ubicazione:** consente all'utente di modificare l'origine e la destinazione per l'ubicazione. Nel caso di ubicazioni non gestite (hotspot, aeroporti e così via) questa autorizzazione deve essere concessa. Negli ambienti controllati, in cui si conoscono i parametri di rete, l'autorizzazione può essere disabilitata. L'utente non può passare da un'ubicazione all'altra se questa autorizzazione è disabilitata; al contrario, ZENworks Security Client si basa sui parametri dell'ambiente di rete specificati per questa ubicazione.
   - **Salva ambiente di rete:** consente all'utente di salvare l'ambiente di rete per questa ubicazione per passare automaticamente all'ubicazione quando l'utente ritorna. Questa impostazione è consigliata per tutte le ubicazioni verso le quali l'utente deve passare. È possibile salvare più ambienti di rete per una singola ubicazione. Ad esempio, se una norma corrente include un'ubicazione denominata Aeroporto, ciascun aeroporto visitato dall'utente può essere salvato come ambiente di rete per questa ubicazione. In questo modo, quando l'utente torna in un ambiente Aeroporto salvato, ZENworks Security Client passa automaticamente all'ubicazione Aeroporto e applica le impostazioni di sicurezza definite. Naturalmente l'utente può cambiare ubicazione e non salvare l'ambiente.

- **Consenti modifica manuale impostazioni firewall:** consente all'utente di modificare le impostazioni del firewall.
- **Mostra ubicazione nel menu Client:** consente la visualizzazione dell'ubicazione nel menu Client. Se questa opzione non è selezionata, l'ubicazione non viene mai visualizzata.

Garanzia ubicazioni client: dal momento che le informazioni relative agli ambienti di rete utilizzate per stabilire un'ubicazione possono essere facilmente contraffatte, esponendo il punto finale a possibili intrusioni, il servizio garanzia ubicazioni client (CLAS, Client Location Assurance Service) rende disponibile l'opzione di verifica cifrata di un'ubicazione. Questo servizio è affidabile solo in ambienti di rete che si trovano completamente ed esclusivamente sotto il controllo dell'azienda. Se si aggiunge il servizio garanzia ubicazioni client a un'ubicazione, è possibile definire impostazioni e autorizzazioni del firewall meno restrittive per tale ubicazione, presupponendo che il punto finale si trovi dietro il firewall di rete.

ZENworks Security Client utilizza una porta fissa configurabile a livello aziendale per inviare una domanda di autenticazione al servizio garanzia ubicazioni client. Il servizio garanzia ubicazioni client decifra il pacchetto e risponde alla domanda di autenticazione, dimostrando di avere la chiave privata corrispondente alla chiave pubblica. L'icona della barra delle applicazioni include un segno di spunta, che indica che l'utente si trova nell'ubicazione corretta.

ZENworks Security Client non è in grado di passare all'ubicazione a meno che non rilevi il server CLAS. Se il server CLAS non viene rilevato, anche se tutti gli altri parametri di rete corrispondono, ZENworks Security Client rimane nell'ubicazione sconosciuta per proteggere il punto finale.

Per attivare CLAS per un'ubicazione, selezionare la casella di controllo *Garanzia ubicazioni client*, fare clic su *Importa*, quindi individuare e selezionare il file. Quando la chiave è stata importata correttamente, viene visualizzata la dicitura Configurato.

Questa opzione non è disponibile per l'ubicazione sconosciuta.

Utilizza messaggio ubicazione: Consente di visualizzare un messaggio utente personalizzato opzionale quando ZENworks Security Client passa a questa ubicazione. Questo messaggio può fornire istruzioni per l'utente finale, dettagli su restrizioni delle norme per l'ubicazione corrente o includere un collegamento ipertestuale a ulteriori informazioni.

4. Fare clic su *Salva norme*. Se le norme in uso presentano errori, vedere Sezione 2.2.6, “Notifica di errore”, a pagina 105.

Per associare un'ubicazione esistente:

1. Fare clic su *Ubicazioni definite*, quindi sul pulsante *Associa componente* della barra degli strumenti.
2. Selezionare le ubicazioni desiderate dall'elenco.
3. Modificare le impostazioni, se necessario.

Nota: La modifica delle impostazioni di un componente condiviso ha effetto su tutte le altre istanze dello stesso componente. Utilizzare il comando *Mostra utilizzo* per visualizzare tutte le altre norme associate al componente.

---

4. Fare clic su *Salva norme*. Se le norme in uso presentano errori, vedere Sezione 2.2.6, “Notifica di errore”, a pagina 105.

È necessario definire nelle norme ubicazioni con definizioni multiple (oltre alle ubicazioni semplici Lavoro e Sconosciuta) per fornire all'utente diverse opzioni di autorizzazioni di sicurezza quando si connette al di fuori del firewall aziendale. L'utilizzo di nomi semplici per le ubicazioni (ad esempio,

Bar, Aeroporti, Casa) e di suggerimenti visivi, mediante l'icona dell'ubicazione nella barra delle applicazioni, consente all'utente di passare facilmente alle impostazioni di sicurezza appropriate per ciascun ambiente di rete.

Hardware di comunicazione

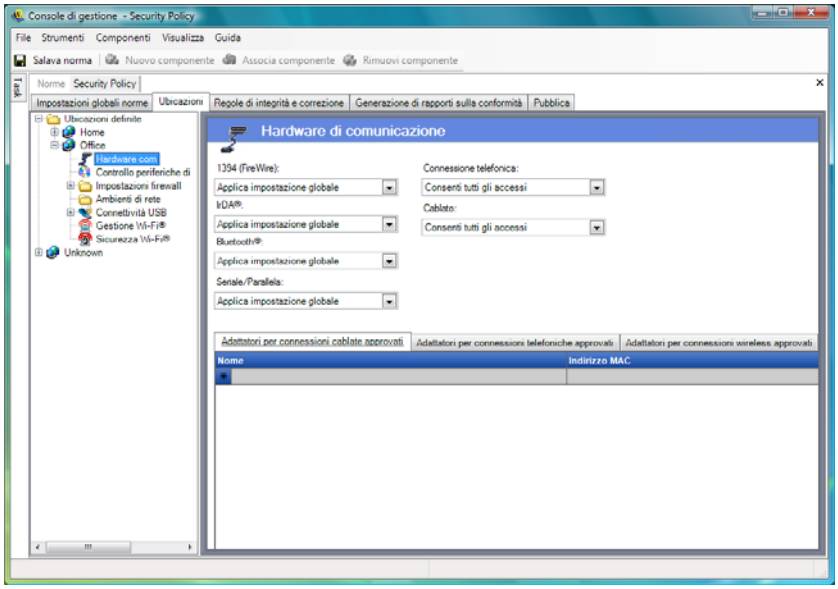
Le impostazioni relative all'hardware di comunicazione controllano, per ogni ubicazione, i tipi di hardware autorizzati ad accedere all'ambiente di rete.

Nota: I controlli dell'hardware di comunicazione possono essere impostati globalmente nella scheda *Impostazioni globali norme* o per le singole ubicazioni nella scheda *Ubicazioni*.

Per impostare i controlli dell'hardware di comunicazione per un'ubicazione, fare clic sulla scheda *Ubicazioni*, espandere l'ubicazione desiderata nell'albero, quindi fare clic su *Hardware com*.

oppure

Per impostare globalmente i controlli dell'hardware di comunicazione, fare clic sulla scheda *Impostazioni globali norme*, espandere *Impostazioni globali* nell'albero, quindi fare clic su *Hardware com*. Per ulteriori informazioni, consultare “Hardware di comunicazione” a pagina 49.



Scegliere se abilitare, disabilitare o applicare l'impostazione globale per ciascun dispositivo hardware di comunicazione elencato:

- **1394 (FireWire):** * accedere portare
- **IrDA:** Controlla la porta di accesso a infrarossi sul punto finale.
- **Bluetooth:** Controlla la porta di accesso Bluetooth* sul punto finale.
- **Seriale/Parallela:** controlla la porta di accesso seriale e parallela sul punto finale.

- **Connessione telefonica:** controlla la connettività via modem per ogni ubicazione. Questa opzione non è disponibile quando si configurano le impostazioni di comunicazione in modo globale mediante la scheda *Impostazioni globali norme*.
- **Cablato:** controlla la connettività con scheda LAN per ogni ubicazione. Questa opzione non è disponibile quando si configurano le impostazioni di comunicazione in modo globale mediante la scheda *Impostazioni globali norme*.

L'opzione Abilita consente l'accesso completo alla porta di comunicazione.

L'opzione Disabilita impedisce ogni accesso alla porta di comunicazione.

Nota: Gli adattatori wireless sono controllati globalmente o disabilitati localmente tramite i controlli della Sicurezza Wi-Fi. È possibile specificare gli adattatori per marca utilizzando l'elenco Adattatori wireless approvati.

Elenco adattatori per connessioni telefoniche approvati: ZENworks Security Client è in grado di bloccare la connessione di tutti gli adattatori per connessioni telefoniche (modem) approvati tranne quelli specificati. Ad esempio, un amministratore può implementare norme che consentono l'impiego di una sola marca o un tipo specifico di scheda modem. Ciò consente di ridurre i costi associati all'utilizzo di hardware non supportato da parte dei dipendenti.

Elenco Adattatori wireless approvati: ZENworks Security Client è in grado di bloccare la connessione di tutti gli adattatori wireless approvati tranne quelli specificati. Ad esempio, un amministratore può implementare norme che consentano l'impiego di una sola marca o un tipo specifico di scheda wireless. Ciò consente di ridurre i costi di supporto derivanti dall'utilizzo di hardware non supportato da parte dei dipendenti, e soprattutto consente di supportare e applicare iniziative di sicurezza basate su standard IEEE, oltre che protocolli di sicurezza quali LEAP, PEAP, WPA, TKIP e altri.

Utilizzo della funzione AdapterAware:

ZENworks Security Client riceve una notifica ogni volta che un dispositivo di rete viene installato nel sistema e determina se il dispositivo è autorizzato o non autorizzato. Se non è autorizzato, il driver del dispositivo viene disabilitato, rendendo inutilizzabile il nuovo dispositivo, e l'utente riceve una notifica relativa al problema.

Nota: Quando un nuovo adattatore non autorizzato (sia per la connessione telefonica sia wireless) installa per la prima volta i propri driver nel punto finale (tramite PCMCIA o USB), l'adattatore risulta abilitato in Gestione dispositivi di Windows finché il sistema non viene riavviato, anche se tutta la connettività di rete è bloccata.

Specificare il nome di ciascun adattatore consentito. Sono ammessi nomi parziali. I nomi degli adattatori hanno una lunghezza massima di 50 caratteri e distinguono tra maiuscole e minuscole. Il nome del dispositivo è obbligatorio nel sistema operativo Windows 2000 per l'utilizzo di questa funzionalità. Se non vengono immessi adattatori, saranno consentiti tutti gli adattatori del tipo specificato. Se viene immesso un solo adattatore, sarà consentito solo quell'adattatore per l'ubicazione.

Nota: Se il punto finale si trova in un'ubicazione per cui viene definito un solo SSID del punto di accesso come identificazione della rete, ZENworks Security Client passa a quella ubicazione prima di disabilitare l'adattatore non autorizzato. Se si verifica questa condizione, è necessario utilizzare una password prioritaria per fornire uno switch di ubicazione manuale.

Controllo periferiche di memorizzazione

Questi controlli consentono di definire le impostazioni di default dei dispositivi di memorizzazione per le norme. È possibile consentire a tutti i dispositivi di memorizzazione esterni di leggere e scrivere file, funzionare in modalità di sola lettura o essere completamente disattivati. Se disattivati, tali dispositivi non sono in grado di richiamare i dati dal punto finale. Tuttavia, il disco fisso e tutte le unità di rete continuano a essere accessibili e funzionanti.

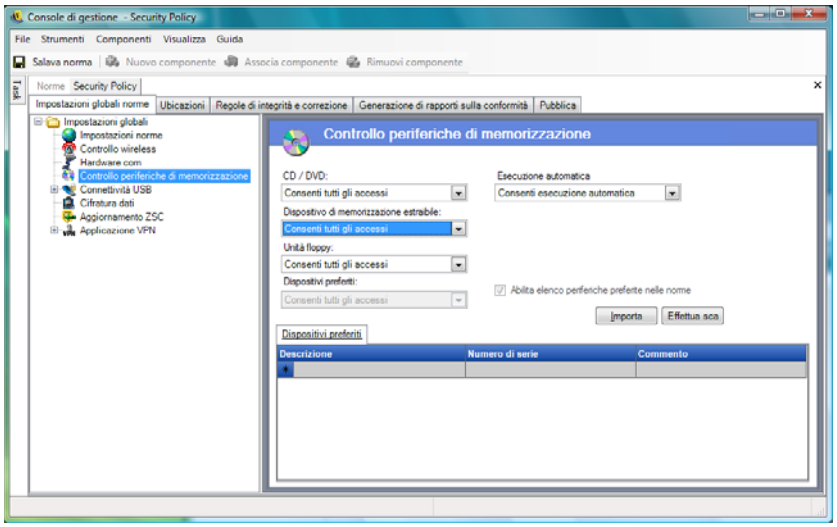
Non è consentito il controllo delle periferiche di memorizzazione di ZENworks Endpoint Security Management se è attivato ZENworks Storage Encryption Solution.

Nota: I controlli delle periferiche di memorizzazione possono essere impostati globalmente nella scheda *Impostazioni globali norme* o per singole ubicazioni nella scheda *Ubicazioni*.

Per impostare i controlli delle periferiche di memorizzazione per un'ubicazione, fare clic sulla scheda *Ubicazioni*, espandere l'ubicazione desiderata nell'albero, quindi fare clic su *Controllo periferiche di memorizzazione*.

oppure

Per impostare globalmente i controlli delle periferiche di memorizzazione, fare clic sulla scheda *Impostazioni globali norme*, espandere *Impostazioni globali* nell'albero, quindi fare clic su *Controllo periferiche di memorizzazione*. Per ulteriori informazioni, consultare "Controllo periferiche di memorizzazione" a pagina 50.



Controllo periferiche di memorizzazione è suddiviso nelle seguenti categorie:

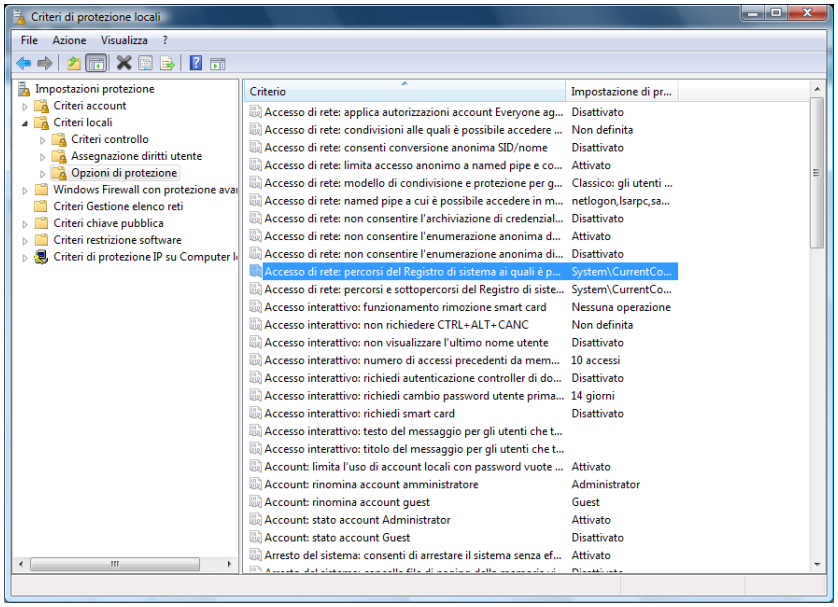
- **CD/DVD:** Controlla tutti i dispositivi elencati in *Unità DVD/CD-ROM* in Gestione periferiche di Windows.
- **Dispositivi di memorizzazione estraibili:** Controlla tutte le periferiche segnalate come dispositivi di memorizzazione estraibili in *Unità disco* in Gestione periferiche di Windows.
- **Unità floppy:** Controlla tutti i dispositivi riportati nell'elenco *Unità disco floppy* in Gestione periferiche di Windows.

i dispositivi di memorizzazione fissi (unità a disco fisso) e le unità di rete (se disponibili) sono sempre consentiti.

Per impostare i valori di default delle norme per i dispositivi di memorizzazione, selezionare l'impostazione globale per entrambi i tipi dagli elenchi a discesa:

- **Abilita:** Il tipo di dispositivo è consentito per default.
- **Disattiva:** l'accesso al tipo di dispositivo non è consentito. Quando un utente cerca di accedere ai file salvati su un determinato dispositivo di memorizzazione, riceve un messaggio di errore, dal sistema operativo o dall'applicazione che sta cercando di accedere al dispositivo di memorizzazione locale, indicante che l'azione non è riuscita.
- **Sola lettura:** Il tipo di dispositivo è impostato su Sola lettura. Quando un utente cerca di scrivere sul dispositivo, riceve un messaggio di errore dal sistema operativo o dall'applicazione che sta cercando di accedere al dispositivo di memorizzazione locale, indicante che l'azione non è riuscita.

Nota: Se si desidera disattivare le unità CD-ROM o le unità floppy su un gruppo di punti finali oppure impostarle su Sola lettura, le impostazioni di sicurezza locale (trasmesse attraverso un oggetto norme di gruppo del servizio di directory) devono aver impostato sia *Periferiche: limita accesso al CD-ROM agli utenti che hanno effettuato l'accesso locale* che *Periferiche: limita accesso al disco floppy agli utenti che hanno effettuato l'accesso locale su Disabilitato*. Per verificare questa condizione, aprire l'oggetto norme di gruppo o gli Strumenti di amministrazione del computer. Cercare Impostazioni sicurezza locale - Opzioni di sicurezza e verificare che entrambi i dispositivi siano disattivati. L'impostazione di default è Disabilitato.



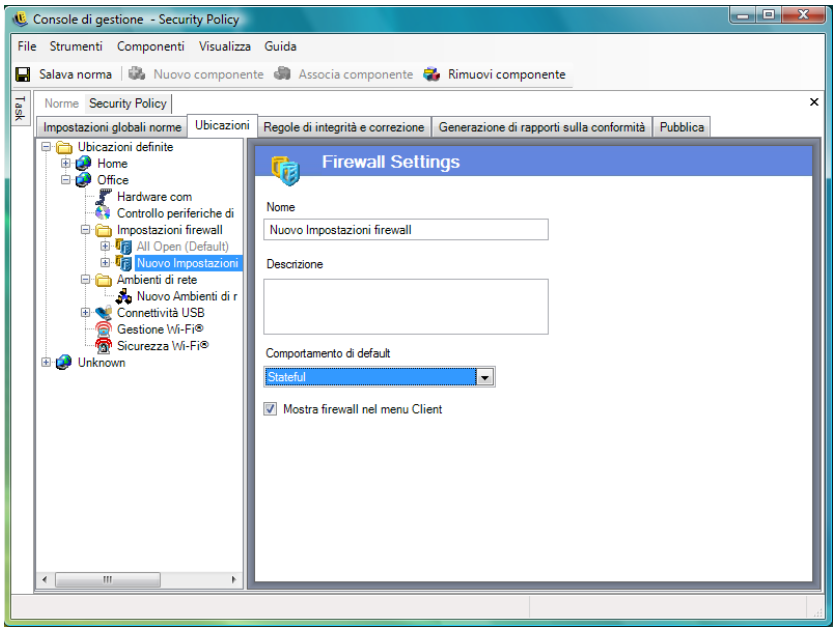
Impostazioni firewall

Le impostazioni del firewall controllano la connettività di tutte le porte di rete, degli elenchi di controllo dell'accesso, dei pacchetti di rete (ICMP, ARP e così via) e stabiliscono quali applicazioni sono autorizzate a utilizzare un socket o funzionare quando le impostazioni vengono applicate.

Nota: Questa funzione è disponibile solo nell'installazione di ZENworks Endpoint Security Management e non può essere utilizzata per le norme di sicurezza di UWS.

Per accedere a questo controllo, fare clic sulla scheda *Ubicazioni*, quindi sull'icona *Impostazioni firewall* nell'albero delle norme visualizzato a sinistra.

Ciascun componente delle impostazioni del firewall viene configurato separatamente. Soltanto il comportamento di default delle porte TCP/UDP deve essere impostato. Questa impostazione interessa tutte le porte TCP/UDP quando è abilitata. È possibile creare porte individuali o gruppi di porte con un'impostazione diversa.



Per creare una nuova impostazione del firewall:

1. Selezionare *Impostazioni firewall* nell'albero dei componenti e fare clic sul pulsante *Nuovo componente*.
2. Assegnare un nome all'impostazione del firewall e immettere una descrizione.
3. Fare clic con il pulsante destro del mouse su *Porte TCP/UDP* nell'albero dei componenti, quindi fare clic su *Aggiungi nuovo - Porte TCP/UDP* per selezionare il comportamento di default per tutte le porte TCP/UDP.

   È possibile aggiungere ulteriori porte ed elenchi alle impostazioni del firewall e assegnare ad essi comportamenti univoci che hanno la priorità sull'impostazione di default.

   Ad esempio, il comportamento di default di tutte le porte è impostato su Tutti Stateful. Ciò significa che alle impostazioni del firewall vengono aggiunti gli elenchi di porte per i flussi multimediali e l'esplorazione del Web. Il comportamento della porta per i flussi multimediali è impostato su Chiuso, mentre il comportamento della porta per l'esplorazione del Web è impostato su Aperto. Il traffico di rete attraverso le porte TCP 7070, 554, 1755 e 8000 viene bloccato. Il traffico di rete attraverso le porte 80 e 443 è aperto e visibile sulla rete. Tutte le altre porte funzionano in modalità Stateful e richiedono l'autorizzazione del traffico in transito.

   Per ulteriori informazioni, consultare “Porte TCP/UDP” a pagina 76.
4. Fare clic con il pulsante destro del mouse su *Elenchi di controllo dell'accesso*, quindi fare clic su *Aggiungi nuovo - Elenchi di controllo dell'accesso* per aggiungere indirizzi per i quali è necessario il transito di traffico non richiesto, indipendentemente dal comportamento della porta corrente.

Per ulteriori informazioni, consultare “Elenchi di controllo dell'accesso” a pagina 80.

5 Fare clic con il pulsante destro del mouse su *Controllo applicazione*, quindi fare clic su *Aggiungi nuovo - Controllo applicazione* per bloccare le applicazioni in modo che non possano ottenere l'accesso alla rete o semplicemente essere eseguite.

   Per ulteriori informazioni, consultare “Controllo applicazione” a pagina 83.

6 Indicare se il firewall verrà visualizzato nel menu di ZENworks Security Client (se questa opzione non è selezionata, l'utente non vede questa impostazione del firewall).

7 Fare clic su *Salva norme*. Se le norme in uso presentano errori, vedere Sezione 2.2.6, “Notifica di errore”, a pagina 105.

Per associare un'impostazione del firewall esistente:

1 Selezionare *Impostazioni firewall* nell'albero dei componenti e fare clic sul pulsante *Associa componente*.

2 Selezionare le impostazioni del firewall desiderate dall'elenco,

3 Modificare l'impostazione di default del comportamento, se necessario.

Nota: La modifica delle impostazioni di un componente condiviso ha effetto su tutte le altre istanze del componente. Utilizzare il comando *Mostra utilizzo* per visualizzare tutte le altre norme associate al componente.

---

4 Fare clic su *Salva norme*. Se le norme in uso presentano errori, vedere Sezione 2.2.6, “Notifica di errore”, a pagina 105.

All'interno di una singola ubicazione è possibile includere più impostazioni del firewall. Una viene definita come impostazione di default, mentre le impostazioni rimanenti restano a disposizione dell'utente come opzioni a cui passare. Poter disporre di più impostazioni risulta particolarmente utile per un utente che normalmente ha bisogno di determinate restrizioni di sicurezza in un ambiente di rete e occasionalmente desidera che tali restrizioni vengano rimosse o potenziate per un breve periodo di tempo, ad esempio per le trasmissioni ICMP.

Al momento dell'installazione vengono incluse le seguenti impostazioni del firewall:

- **Tutte adattive:** Consente di impostare tutte le porte di rete su Stateful (tutto il traffico di rete in entrata non richiesto viene bloccato, tutto il traffico di rete in uscita è consentito). I pacchetti ARP e 802.1x sono autorizzati ed è consentita la connessione di tutte le applicazioni di rete.
- **Tutte aperte:** Consente di impostare tutte le porte di rete come aperte (viene consentito tutto il traffico di rete) e autorizzare 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.

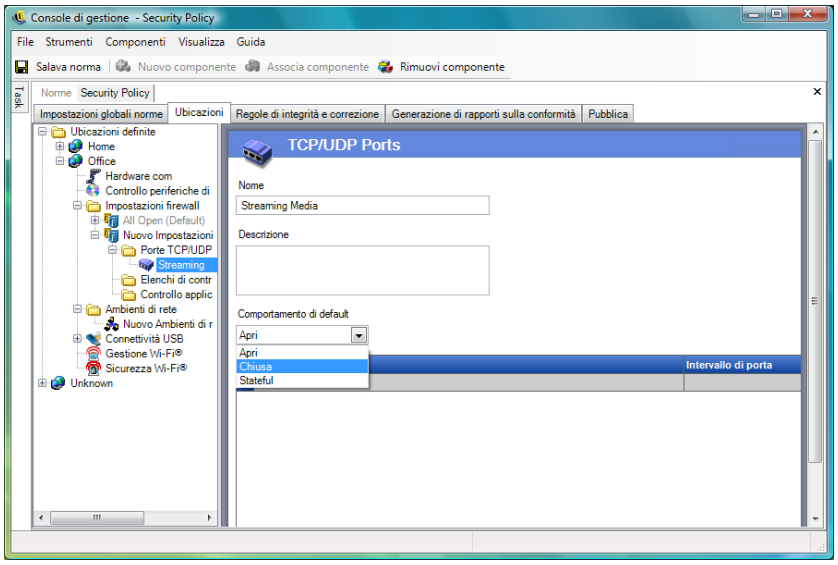
Per le nuove ubicazioni, l'impostazione di default del firewall è Tutte aperte. Per definire una diversa impostazione del firewall come valore di default, fare clic con il pulsante destro del mouse sull'impostazione desiderata e selezionare *Imposta come default*.

Porte TCP/UDP

Il metodo principale utilizzato per la protezione dei dati dei punti finali è il controllo dell'attività delle porte TCP/UDP. Tale funzione consente di creare un elenco di porte TCP/UDP che verranno gestite in modo univoco mediante questa impostazione del firewall. Gli elenchi contengono un insieme di porte e intervalli di porte con il relativo tipo di trasporto, che ne definisce la funzione.

Nota: Tale funzione è disponibile solo nell'installazione di ZENworks Endpoint Security Management e non può essere utilizzata per le norme di sicurezza di UWS.

Per accedere al controllo, fare clic sulla scheda *Ubicazioni*, quindi fare clic sul simbolo + accanto a *Impostazioni firewall* e scegliere il simbolo + accanto al firewall desiderato. Quindi, fare clic sull'icona *Porte TCP/UDP* nell'albero delle norme visualizzato a sinistra.



È possibile definire elenchi di porte TCP/UDP con singole porte o sotto forma di intervallo (1-100) per ciascuna riga dell'elenco.

Per creare una nuova impostazione della porta TCP/UDP:

1. Fare clic con il pulsante destro del mouse su *Porte TCP/UDP*nell'albero dei componenti, quindi fare clic su *Aggiungi nuovo - Porte TCP/UDP*.
2. Assegnare un nome all'elenco di porte e immettere una descrizione.
3. Selezionare un valore per il comportamento della porta dall'elenco a discesa:
   - **Aperto:** è consentito tutto il traffico di rete in entrata e in uscita. Poiché tutto il traffico di rete è consentito, le informazioni di identificazione del computer sono visibili per la porta o l'intervallo di porte.
   - **Chiuso:** tutto il traffico di rete in entrata e in uscita viene bloccato. Poiché tutte le richieste di identificazione di rete sono bloccate, le informazioni di identificazione del computer non sono visibili per la porta o l'intervallo di porte.
   - **Stateful:** tutto il traffico di rete non richiesto in entrata viene bloccato. Tutto il traffico di rete in uscita è consentito tramite la porta o l'intervallo di porte.
4. Specificare il tipo di trasporto facendo clic sulla freccia in basso nella colonna *Tipo di porta*:
   - TCP/UDP
   - Ether
   - IP
   - TCP
   - UDP

5 Immettere porte e intervalli di porte in base ai criteri che seguono:

- Porte singole
- Un intervallo di porte con il primo numero di porta seguito da un trattino e l'ultimo numero di porta

  Ad esempio, immettere 1-100 per aggiungere tutte le porte da 1 a 100

  Visitare il sito Web dell'Internet Assigned Numbers Authority (http://www.iana.org) (ente per l'assegnazione degli indirizzi IP) per un elenco completo di porte e tipi di trasporto.

6 Fare clic su *Salva norme*.

Per associare una porta TCP/UDP esistente all'impostazione del firewall:

1 Selezionare *Porte TCP/UDP* dall'albero dei componenti e fare clic sul pulsante *Associa componente*.

2 Selezionare le porte desiderate dall'elenco.

3 Configurare le impostazioni di default del comportamento.

  La modifica delle impostazioni di un componente condiviso ha effetto su tutte le altre istanze dello stesso componente. Utilizzare il comando *Mostra utilizzo* per visualizzare tutte le altre norme associate al componente.

4 Fare clic su *Salva norme*.

Diversi gruppi di porte TCP/UDP sono stati abbinati e sono disponibili al momento dell'installazione:

Nome	Descrizione	Trasporto	Valore
Tutte le porte	Tutte le porte	Tutti	1-65535
BlueRidge VPN	Porte utilizzate dal client Blue Ridge VPN	UDP	820
Cisco VPN	Porte utilizzate dal client Cisco * VPN	IP	50,51
		UDP	500,4500
		UDP	1000-1200
		UDP	62514,62515,62517
		UDP	62519-62521
		UDP	62532,62524
Networking comune	Porte di rete normalmente richieste per la creazione di firewall	TCP	53
		UDP	53
		UDP	67,68
		TCP	546, 547
		UDP	546, 547
		TCP	647, 847
		UDP	647, 847

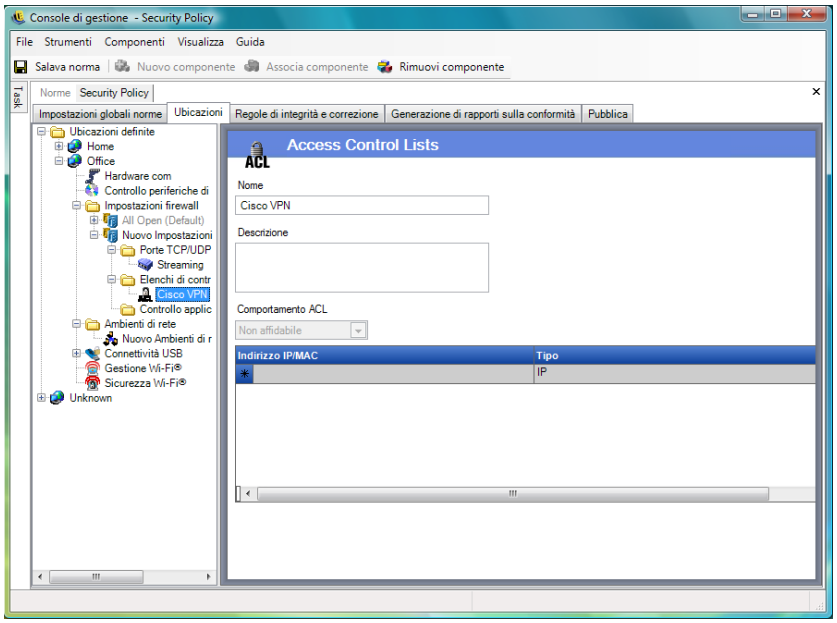
Nome	Descrizione	Trasporto	Valore
Comunicazione database	Porte per database Microsoft*, Oracle*, Siebel*, Sybase* e SAP*	TCP	4100
		TCP	1521
		TCP	1433
		UDP	1444
		TCP	2320
		TCP	49998
		TCP	3200
		TCP	3600
File Transfer Protocol (FTP)	Porta FTP	TCP/UDP	21
Messaggistica in tempo reale	Porte per i sistemi di messaggistica in tempo reale Microsoft, AOL* e Yahoo*	TCP	6891-6900
		TCP	1863,443
		UDP	1863,443
		UDP	5190
		TCP	6901
		UDP	6901
		TCP	5000-5001
		UDP	5055
		TCP	20000-20059
		UDP	4000
		TCP	4099
		TCP	5190
VPN compatibili con Internet Key Exchange	Porte utilizzate dai client VPN compatibili con il protocollo Internet Key Exchange	UDP	500
Servizi di rete Microsoft	Porte comunemente usate per la condivisione di file / Active Directory*	TCP/UDP	135-139, 445
Porte aperte	Porte aperte per il firewall	TCP/UDP	80
Flussi multimediali	Porte comunemente usate per i flussi multimediali Microsoft e Real	TCP	7070, 554, 1755, 8000
Esplorazione del Web	Porte comunemente usate per l'esplorazione del Web, incluso il protocollo SSL	Tutti	80, 443

Elenchi di controllo dell'accesso

Per alcuni indirizzi può essere necessario consentire il transito di traffico non richiesto indipendentemente dal comportamento corrente delle porte (ad esempio, server di backup aziendali, server di Exchange e così via). Nei casi in cui il traffico non richiesto debba essere consentito da e verso server sicuri, è possibile risolvere il problema mediante un elenco di controllo dell'accesso (ACL, Access Control List).

Nota: Questa funzione è disponibile solo nell'installazione di ZENworks Endpoint Security Management e non può essere utilizzata per le norme di sicurezza di UWS.

Per accedere al controllo, fare clic sulla scheda *Ubicazioni*, scegliere il simbolo + accanto a *Impostazioni firewall*e fare clic sul simbolo + accanto al firewall desiderato. Quindi, fare clic con il pulsante destro del mouse su *Elenchi di controllo dell'accesso* nell'albero delle norme visualizzato a sinistra e scegliere *Aggiungi nuovo - Elenchi di controllo dell'accesso*.



Per creare una nuova impostazione degli elenchi di controllo dell'accesso:

1. Fare clic con il pulsante destro del mouse su *Elenchi di controllo dell'accesso* dall'albero dei componenti, quindi scegliere *Aggiungi nuovo - Elenchi di controllo dell'accesso*.
2. Assegnare un nome all'elenco di controllo dell'accesso e immettere una descrizione.
3. Specificare l'indirizzo o la macro dell'elenco di controllo dell'accesso.
4. Specificare il tipo di elenco di controllo dell'accesso:
   - **IP:** L'indirizzo può essere lungo al massimo 15 caratteri e contenere solo i numeri da 0 a 9 e punti, ad esempio 123.45.6.189. L'indirizzo IP può inoltre essere immesso come intervallo, ad esempio 123.0.0.0 - 123.0.0.255.
   - **MAC:** L'indirizzo può essere lungo al massimo 12 caratteri e contenere solo i numeri da 0 a 9 e le lettere da A a F (maiuscole e minuscole), separati da due punti, ad esempio 00:01:02:34:05:B6).

5. Selezionare un valore dall'elenco a discesa Comportamento ACL per stabilire se gli elenchi di controllo dell'accesso sono impostati su *Attendibile* (sempre consentiti anche se tutte le porte TCP/UDP sono chiuse) o *Non attendibile* (accesso bloccato).
6. Se si seleziona *Attendibile*, selezionare le *Porte attendibili facoltative (TCP/UDP)* utilizzate dall'elenco di controllo dell'accesso. Queste porte consentono tutto il traffico ACL, mentre le altre porte TCP/UDP mantengono le impostazioni correnti. Se si seleziona *Nessuno*, l'elenco di controllo dell'accesso potrà utilizzare qualsiasi porta.
7. Fare clic su *Salva norme*.

Per associare un elenco di controllo dell'accesso o una macro esistente all'impostazione del firewall:

1. Selezionare *Elenco di controllo dell'accesso* dall'albero dei componenti e fare clic sul pulsante *Associa componente*.
2. Selezionare gli elenchi di controllo dell'accesso o le macro dall'elenco.
3. Configurare le impostazioni del comportamento dell'elenco di controllo dell'accesso secondo le proprie esigenze.

   Nota: La modifica delle impostazioni di un componente condiviso ha effetto su tutte le altre istanze dello stesso componente. Utilizzare il comando *Mostra utilizzo* per visualizzare tutte le altre norme associate al componente.

4. Fare clic su *Salva norme*.

Elenco delle macro degli indirizzi di rete

Di seguito viene riportato un elenco delle macro speciali per il controllo dell'accesso. È possibile associare tali macro individualmente come parte di un elenco di controllo dell'accesso a un'impostazione del firewall.

Tabella 2-1 *Macro degli indirizzi di rete*

Macro	Descrizione
[Arp]	Consente i pacchetti ARP (Address Resolution Protocol). Il termine *address resolution* (risoluzione di indirizzi) indica il processo di rilevamento di un indirizzo di un computer in una rete. L'indirizzo viene risolto utilizzando un protocollo in cui un'informazione viene inviata da un processo client in esecuzione sul computer locale a un processo server in esecuzione su un computer remoto. L'informazione ricevuta consente al server di identificare in modo univoco il sistema di rete per il quale è stato richiesto l'indirizzo e di fornire l'indirizzo desiderato. La procedura di risoluzione dell'indirizzo viene completata quando il client riceve una risposta dal server contenente l'indirizzo richiesto.
[Icmp]	Consente i pacchetti ICMP (Internet Control Message Protocol). I pacchetti ICMP sono utilizzati dai router, dai dispositivi intermedi o dagli host per comunicare aggiornamenti o informazioni sugli errori ad altri router, dispositivi intermedi o host. I messaggi ICMP vengono inviati in diverse situazioni, ad esempio quando un datagramma non è in grado di raggiungere la propria destinazione, quando il gateway non ha la capacità di buffering per inoltrare un datagramma e quando il gateway indica all'host di inviare il traffico su un instradamento più breve.

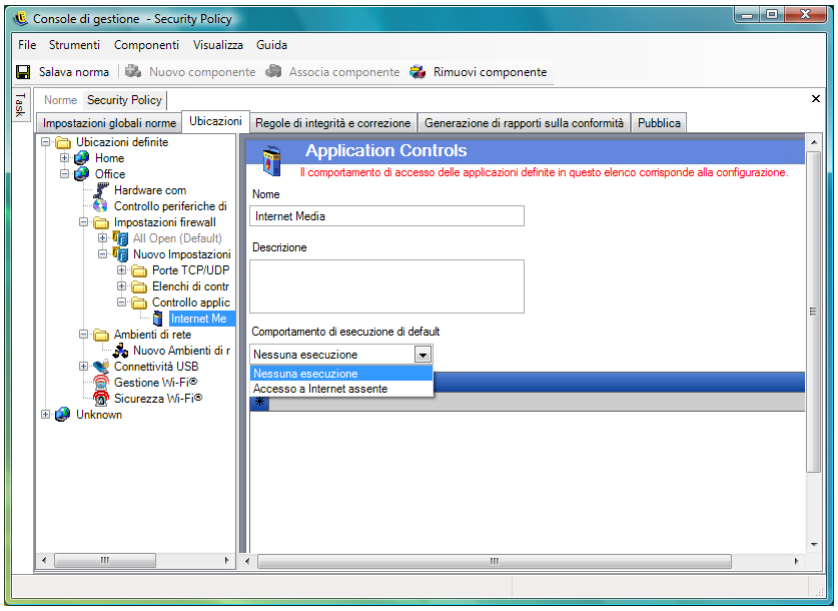
Macro	Descrizione
[IpMulticast]	Consente i pacchetti IP multicast. Multicast è una tecnologia di mantenimento della larghezza di banda che consente di ridurre il traffico attraverso la distribuzione simultanea di un singolo flusso di informazioni a migliaia di destinatari aziendali e abitazioni private. La tecnologia multicast viene utilizzata per applicazioni quali la videoconferenza, le comunicazioni aziendali, la formazione a distanza e la distribuzione di software, quotazioni di titoli e notizie. I pacchetti multicast possono essere distribuiti utilizzando indirizzi IP o Ethernet.
[EthernetMulticast]	Consente i pacchetti Ethernet multicast.
[IpSubnetBrdcast]	Consente i pacchetti broadcast subnet. I broadcast subnet vengono utilizzati per inviare pacchetti a tutti gli host di una rete con sottoreti o super-reti o agli host di una rete non classful. Tutti gli host di una rete non classful sono in ascolto ed elaborano i pacchetti indirizzati all'indirizzo di broadcast subnet.
[Snap]	Consente i pacchetti con codifica SNAP.
[LLC]	Consente i pacchetti con codifica LLC.
[Allow8021X]	Consente i pacchetti 802.1x. Per superare alcuni difetti delle chiavi WEP (Wired Equivalent Policy), Microsoft e altre società utilizzano lo standard 802.1x come metodo di autenticazione alternativo. 802.1x è uno standard basato sul controllo delle porte di accesso alla rete, che utilizza il protocollo EAP (Extensible Authentication Protocol) o i certificati. Attualmente i maggiori fornitori di schede wireless e molti fornitori di punti di accesso supportano lo standard 802.1x. Questa impostazione consente, inoltre, l'utilizzo di pacchetti di autenticazione LEAP (Light Extensible Authentication Protocol) e WPA (WiFi Protected Access).
[Gateway]	Rappresenta l'indirizzo gateway di default della configurazione IP corrente. Quando si immette questo valore, ZENworks Security Client consente tutto il traffico di rete proveniente dal gateway di default della configurazione IP corrente come elenco di controllo dell'accesso attendibile.
[GatewayAll]	Uguale all'impostazione [Gateway] ma per tutti i gateway definiti.
[Wins]	Rappresenta l'indirizzo del server WINS di default nella configurazione IP client corrente. Quando si immette questo valore, ZENworks Security Client consente tutto il traffico di rete proveniente dal server WINS di default della configurazione IP corrente come elenco di controllo dell'accesso attendibile.
[WinsAll]	Uguale all'impostazione [Wins], ma per tutti i server WINS definiti.
[Dns]	Rappresenta l'indirizzo del server DNS di default nella configurazione IP client corrente. Quando si immette questo valore, ZENworks Security Client consente tutto il traffico di rete proveniente dal server DNS di default della configurazione IP corrente come elenco di controllo dell'accesso attendibile.
[DnsAll]	Uguale all'impostazione [Dns], ma per tutti i server DNS definiti.
[Dhcp]	Rappresenta l'indirizzo del server DHCP di default nella configurazione IP client corrente. Quando si immette questo valore, ZENworks Security Client consente tutto il traffico di rete proveniente dal server DHCP di default della configurazione IP corrente come elenco di controllo dell'accesso attendibile.
[DhcpAll]	Uguale all'impostazione [Dhcp], ma per tutti i server DHCP definiti.

Controllo applicazione

Questa funzione consente all'amministratore di bloccare le applicazioni, impedendo loro di accedere alla rete o semplicemente di funzionare.

Nota: Questa funzione è disponibile solo nell'installazione di ZENworks Endpoint Security Management e non può essere utilizzata per le norme di sicurezza di UWS.

Per accedere a questo controllo, aprire la scheda *Ubicazioni*, fare clic sul simbolo + accanto a *Impostazioni firewall*, quindi scegliere il simbolo + accanto al firewall desiderato e fare clic sull'icona *Controllo applicazione* nell'albero delle norme visualizzato a sinistra.



Per creare una nuova impostazione dei controlli delle applicazioni:

1. Fare clic con il pulsante destro del mouse su *Controllo applicazione* nell'albero dei componenti, quindi scegliere *Aggiungi nuovo - Controllo applicazione*.
2. Assegnare un nome all'elenco di controllo dell'applicazione e fornire una descrizione.
3. Selezionare un comportamento di esecuzione. Questo comportamento viene applicato a tutte le applicazioni elencate. Se si desidera specificare più comportamenti (ad esempio si desidera impedire l'accesso alla rete ad alcune applicazioni e impedire l'esecuzione di tutte le applicazioni di condivisione dei file), è necessario definire più controlli delle applicazioni. Selezionare una delle opzioni seguenti:
   - **Tutti consentiti:** Per tutte le applicazioni elencate sono consentiti l'esecuzione e l'accesso alla rete.
   - **Nessuna esecuzione:** Per tutte le applicazioni elencate non è consentita l'esecuzione.
   - **Nessun accesso di rete:** Per tutte le applicazioni elencate non è consentito l'accesso alla rete. Le applicazioni avviate da un'altra applicazione (ad esempio i browser Web) non sono autorizzate ad accedere alla rete.

Nota: Il blocco dell'accesso alla rete per un'applicazione non impedisce il salvataggio dei file su unità di rete mappate. Gli utenti possono salvare i propri dati su tutte le unità di rete disponibili.

4 Specificare tutte le applicazioni da bloccare. Immettere un'applicazione per riga.

Importante: Il blocco dell'esecuzione di applicazioni critiche potrebbe avere effetti negativi sul funzionamento del sistema. Le applicazioni Microsoft Office bloccate tentano di eseguire il proprio programma di installazione.

5 Fare clic su *Salva norme*.

Per associare un elenco di controllo delle applicazioni esistente all'impostazione del firewall:

1 Selezionare Controllo applicazione nell'albero dei componenti e fare clic sul pulsante *Associa componente*.
2 Selezionare un'applicazione dall'elenco.
3 Configurare le applicazioni e il livello di restrizione secondo le proprie esigenze.

Nota: La modifica delle impostazioni di un componente condiviso ha effetto su tutte le altre istanze dello stesso componente. Utilizzare il comando *Mostra utilizzo* per visualizzare tutte le altre norme associate al componente.

4 Fare clic su *Salva norme*.

I controlli delle applicazioni disponibili sono elencati di seguito. Il comportamento dell'esecuzione di default è Nessun accesso di rete.

Tabella 2-2 *Controlli applicazione*

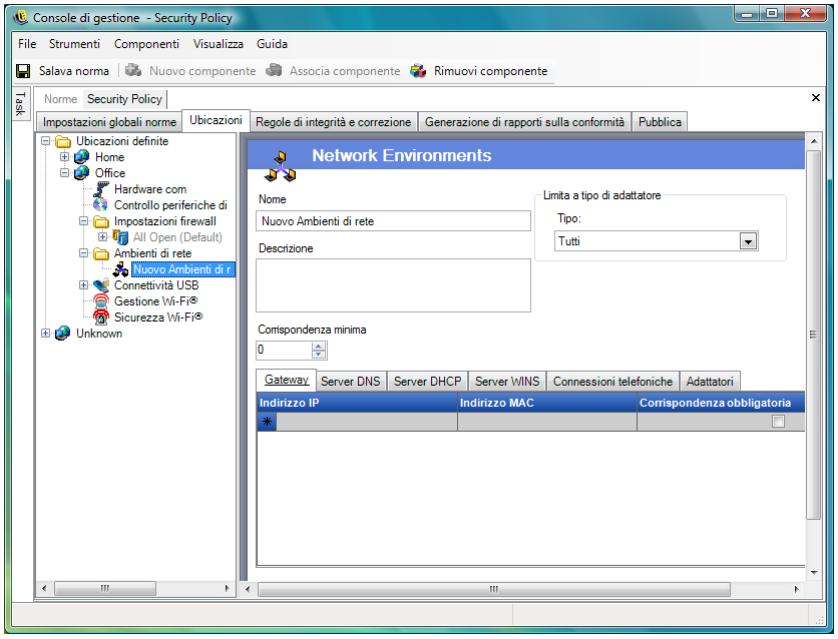
Nome	Applicazioni
Browser Web	explore.exe, netscape.exe e netscp.exe
Messaggistica in tempo reale	aim.exe, icq.exe, msmsgs.exe, msnmsgr.exe, trillian.exe e ypager.exe
Condivisione file	blubster.exe, grokster.exe, imesh.exe, kazaa.exe, morpheus.exe, napster.exe e winmx.exe
Supporti multimediali Internet	mplayer2.exe, wmplayer.exe, naplayer.exe, realplay.exe, spinner.exe e QuickTimePlayer.exe

Se si aggiunge la stessa applicazione a due diversi controlli delle applicazioni nella stessa impostazione del firewall (ad esempio, in un controllo si imposta il blocco dell'esecuzione dell'applicazione `kazaa.exe` e in un altro controllo il blocco dell'accesso alla rete con la stessa impostazione del firewall), per il file eseguibile verrà applicato il controllo più restrittivo (vale a dire che verrà bloccata l'esecuzione dell'applicazione).

Ambienti di rete

Se per un'ubicazione si conoscono i parametri di rete (server gateway, server DNS, server WINS, punti di accesso disponibili e specifiche connessioni con adattatore), è possibile immettere nelle norme i dettagli del servizio (IP e MAC) che identificano la rete. In tal modo si consentirà il passaggio immediato fra ubicazioni senza necessità di salvataggio dell'ambiente da parte dell'utente.

Per accedere a questo controllo, fare clic sulla scheda *Ubicazioni*. quindi scegliere la cartella *Ambienti di rete* nell'albero delle norme visualizzato a sinistra.



Gli elenchi consentono all'amministratore di definire quali servizi di rete sono presenti nell'ambiente. Ogni servizio di rete può contenere più indirizzi. L'amministratore stabilisce la corrispondenza minima di indirizzi nell'ambiente per l'attivazione del passaggio di ubicazione.

È necessario utilizzare due o più parametri di ubicazione in ciascuna definizione di ambiente di rete.

Per definire un ambiente di rete:

1. selezionare *Ambienti di rete* nell'albero dei componenti, quindi fare clic sul pulsante *Nuovo componente*.
2. Assegnare un nome all'ambiente di rete e immettere una descrizione.
3. Selezionare dall'elenco a discesa *Limita a tipo di adattatore* il tipo di adattatore autorizzato ad accedere all'ambiente di rete:
   - Wireless
   - Tutti
   - Modem
   - Cablato
   - Wireless
4. Specificare il numero minimo di servizi di rete richiesti per identificare questo ambiente di rete.

Ciascun ambiente di rete ha un numero minimo di indirizzi, che ZENworks Security Client utilizza per l'identificazione. Il numero impostato in *Corrispondenza minima* non deve essere superiore al numero totale di indirizzi di rete identificati come obbligatori negli elenchi a schede. Specificare il numero minimo di servizi di rete richiesti per identificare questo ambiente di rete.

5 Specificare le seguenti informazioni per ciascun servizio:

- **Indirizzo IP:** Specificare al massimo 15 caratteri contenenti solo i numeri da 0 a 9 e punti. Ad esempio, 123.45.6.789
- **Indirizzo MAC:** Se necessario, specificare al massimo 12 caratteri contenenti solo i numeri da 0 a 9 e le lettere da A a F (maiuscole e minuscole) separati da due punti. Ad esempio, 00:01:02:34:05:B6
- Selezionare la casella di controllo *Corrispondenza obbligatoria* se è necessaria l'identificazione di questo servizio per definire l'ambiente di rete.

6 Per le schede *Connessioni telefoniche* e *Adattatori*, specificare i seguenti requisiti:

- Per *Connessioni telefoniche*, specificare il nome della voce RAS della rubrica telefonica o il numero composto.

  Nota: Le voci della rubrica telefonica devono contenere caratteri alfanumerici e non possono contenere solo caratteri speciali (@, #, $, % e così via). o caratteri numerici (da 1 a 9). Le voci che contengono solo caratteri speciali e caratteri numerici vengono interpretate come numeri composti.

- Per Adattatori, specificare il numero SSID per ciascun adattatore consentito. È possibile specificare gli adattatori per indicare esattamente quali adattatori sono autorizzati ad accedere a questo ambiente di rete. Se non si immette alcun SSID, l'accesso sarà consentito a tutti gli adattatori del tipo autorizzato.

Per associare un ambiente di rete esistente all'ubicazione:

Nota: l'associazione di un singolo ambiente di rete a due o più ubicazioni all'interno delle stesse norme di sicurezza può provocare risultati imprevisti. Tale operazione non è consigliata.

1 Selezionare *Ambienti di rete* nell'albero dei componenti, quindi fare clic sul pulsante *Associa componente*.

2 Selezionare gli ambienti di rete dall'elenco.

3 Configurare i parametri di ambiente secondo le proprie esigenze.

Nota: La modifica delle impostazioni di un componente condiviso ha effetto su tutte le altre istanze dello stesso componente. Utilizzare il comando *Mostra utilizzo* per visualizzare tutte le altre norme associate al componente.

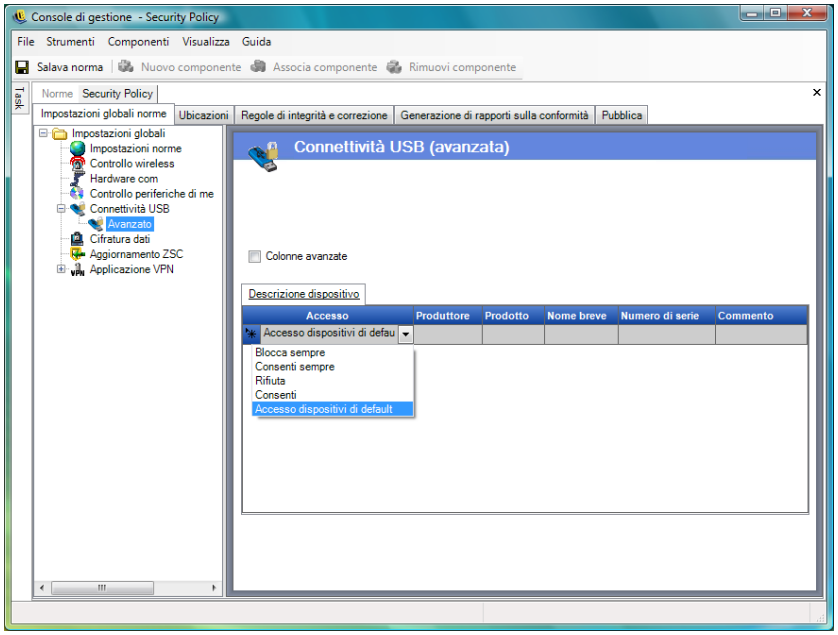
4 Fare clic su *Salva norme*.

Connettività USB

Tutti i dispositivi che si connettono tramite il BUS USB possono essere consentiti o negati dalle norme. Tali dispositivi possono essere analizzati nelle norme utilizzando il rapporto sull'inventario dei dispositivi USB oppure esaminando tutti i dispositivi attualmente collegati a un computer. I dispositivi possono essere filtrati in base al produttore, al nome del prodotto, ai numeri di serie, al tipo e così via. Ai fini del supporto, l'amministratore può configurare le norme in modo tale da

accettare un gruppo di dispositivi in base al tipo di produttore (ad esempio, sono consentiti tutti i dispositivi HP) o in base al tipo di prodotto (ad esempio, sono consentiti tutti i dispositivi HID, come il mouse e la tastiera). Inoltre, è possibile consentire singoli dispositivi per impedire che dispositivi non supportati vengano introdotti nella rete (ad esempio, non sono consentite stampanti tranne quella indicata nelle norme).

Per accedere a questo controllo, fare clic sulla scheda *Impostazioni globali norme*, quindi su *Connettività USB* nell'albero delle norme a sinistra.



Specificare se consentire o negare l'accesso ai dispositivi non presenti nell'elenco.

L'elenco viene popolato con i seguenti metodi, affinché sia possibile consentire o negare la connettività USB ai dispositivi:

- “Aggiunta manuale di dispositivi” a pagina 87
- “Importazione degli elenchi dei dispositivi” a pagina 88

Aggiunta manuale di dispositivi

1. Inserire il dispositivo nella porta USB del computer sul quale è installata la console di gestione.
2. Quando il dispositivo è pronto, fare clic sul pulsante *Effettua scansione*. Se il dispositivo ha un numero di serie, nell'elenco verranno visualizzati la descrizione e il numero di serie.
3. Selezionare un'impostazione dall'elenco a discesa (l'impostazione *Dispositivo estraibile globale* non viene applicata per queste norme):
   - **Abilita:** I dispositivi inseriti nell'elenco dei preferiti dispongono di funzionalità di lettura e scrittura; tutti gli altri dispositivi di memorizzazione esterni e le unità USB sono disattivati.
   - **Sola lettura:** I dispositivi inseriti nell'elenco dei preferiti dispongono di funzionalità di sola lettura; tutti gli altri dispositivi di memorizzazione esterni e le unità USB sono disattivati.

Ripetere questi passaggi per ciascun dispositivo consentito in queste norme. A tutti i dispositivi verranno applicate le stesse impostazioni.

Importazione degli elenchi dei dispositivi

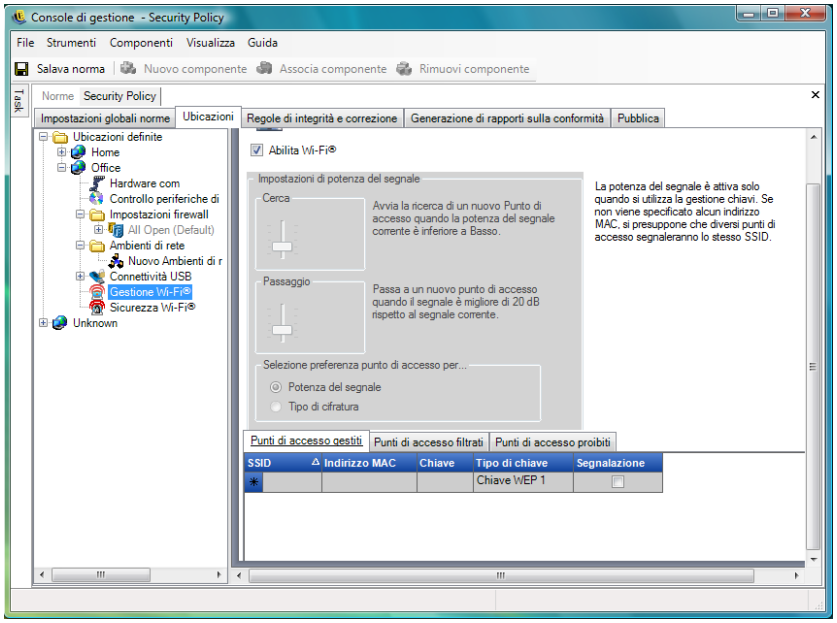
L'applicazione Novell USB Drive Scanner genera un elenco di dispositivi e relativi numeri di serie (vedere Sezione 1.11, “USB Drive Scanner”, a pagina 41). Per importare l'elenco, fare clic su *Importa* e selezionare l'elenco. Nell'elenco vengono popolati i campi *Descrizione* e *Numero di serie*.

Gestione Wi-Fi

Consente all'amministratore di creare elenchi di punti di accesso. I punti di accesso wireless immessi in questi elenchi rappresentano i punti di accesso ai quali il punto finale è autorizzato a connettersi all'interno dell'ubicazione. Si tratta, inoltre, dei punti di accesso che il punto finale è autorizzato a visualizzare in Zero Configuration Manager di Microsoft. I servizi di gestione della configurazione wireless di terze parti non sono supportati da questa funzionalità. Se non vengono specificati punti di accesso, saranno tutti disponibili per il punto finale.

Per accedere a questo controllo, fare clic sulla scheda *Ubicazioni*, quindi su *Gestione Wi-Fi* nell'albero delle norme visualizzato a sinistra.

Nota: In Sicurezza Wi-Fi o Gestione Wi-Fi la deselezione di *Abilita* comporta la disabilitazione di tutte le connessioni Wi-Fi nell'ubicazione.



L'immissione di punti di accesso nell'elenco *Punti di accesso gestiti* comporta la disattivazione di Zero Configuration e forza la connessione del punto finale solo ai punti di accesso indicati quando questi sono disponibili. Se i punti di accesso gestiti non sono disponibili, ZENworks Security Client ritorna all'elenco dei punti accesso filtrati. I punti di accesso immessi nell'elenco Punti di accesso proibiti non vengono mai visualizzati in Zero Configuration.

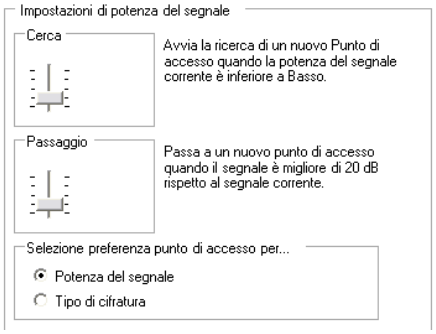
Nota: L'elenco dei punti di accesso è supportato solo dal sistema operativo Windows * XP. Prima di distribuire un elenco di punti di accesso, è consigliabile che tutti i punti finali eliminino l'elenco delle reti preferite di Zero Configuration.

Le seguenti sezioni contengono informazioni aggiuntive:

- “Impostazioni della potenza del segnale Wi-Fi” a pagina 89
- “Punti di accesso gestiti” a pagina 90
- “Punti di accesso filtrati” a pagina 91
- “Punti di accesso proibiti” a pagina 91

Impostazioni della potenza del segnale Wi-Fi

Quando nell'elenco vengono definiti uno o più punti di accesso gestiti tramite WEP, è possibile impostare la potenza del segnale dell'adattatore Wi-Fi. È possibile regolare le soglie di potenza del segnale per ubicazione, al fine di stabilire quando ZENworks Security Client deve cercare o scartare un nuovo punto di accesso o passare a un altro punto di accesso dell'elenco.



Le seguenti informazioni possono essere modificate:

- **Cerca:** Quando viene raggiunto questo livello di forza del segnale, ZENworks Security Client inizia la ricerca di un nuovo punto di accesso a cui connettersi. L'impostazione di default è Basso [-70 dB].
- **Switch:** Perché ZENworks Security Client possa connettersi a un nuovo punto di accesso, tale punto di accesso deve trasmettere al livello di potenza del segnale indicato, superiore a quello della connessione corrente. L'impostazione di default è +20 dB.

Le soglie di potenza del segnale sono determinate dalla quantità di potenza (in dB) rilevata attraverso il driver miniport del computer. Dato che ogni scheda e radio Wi-Fi potrebbe considerare i segnali dB in modo differente per l'indicazione della potenza del segnale ricevuto (RSSI), i numeri variano in base all'adattatore.

È possibile impostare preferenze per la selezione del punto di accesso in base a quanto segue:

- Potenza del segnale
- Tipo di cifratura

I numeri di default associati alle soglie definite nella console di gestione sono generici per la maggior parte degli adattatori Wi-Fi. È opportuno cercare i valori RSSI degli adattatori Wi-Fi in uso per impostare un livello corretto. I valori utilizzati da Novell sono i seguenti:

Nome	Valore di default
Eccellente	-40 dB
Ottimo	-50 dB
Buono	-60 dB
Basso	-70 dB
Bassissimo	-80 dB

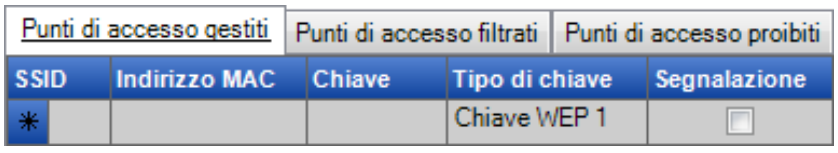
Nota: Sebbene i nomi delle potenze di segnale elencati sopra corrispondano a quelli utilizzati dal servizio Zero Configuration di Microsoft, i valori di soglia non sono corrispondenti. Il servizio Zero Configuration stabilisce i propri valori in base al rapporto segnale/rumore (SNR, Signal to Noise Ratio) e non soltanto in base al valore in dB rilevato dalla RSSI. Ad esempio, se un adattatore Wi-Fi ricevesse un segnale di -54 dB e avesse un livello di rumore di -22 DB, il rapporto segnale/rumore sarebbe pari a 32 dB (-54 - -22=32), che sulla scala di Zero Configuration corrisponderebbe a una potenza di segnale Eccellente. Tuttavia, sulla scala Novell il segnale di -54 dB (ammesso che fosse rilevato di tale intensità dal driver miniport, ma probabilmente sarebbe inferiore) corrisponderebbe a una potenza di segnale di tipo Ottimo.

Si noti che l'utente finale non vede mai le soglie di potenza del segnale di Novell. Queste informazioni vengono fornite al solo scopo di mostrare la differenza tra quanto visualizzato dall'utente in Zero Configuration e quanto avviene nella realtà.

Punti di accesso gestiti

ZENworks Endpoint Security Management fornisce un semplice processo che consente di distribuire e applicare automaticamente le chiavi WEP (Wired Equivalent Privacy) senza l'intervento dell'utente, (ignorando e chiudendo il servizio Zero Configuration di Microsoft). In questo modo si protegge l'integrità delle chiavi poiché non vengono riportate in chiaro in messaggi e-mail o promemoria scritti. L'utente finale non avrà mai la necessità di conoscere la chiave per connettersi automaticamente al punto di accesso. Ciò consente di prevenire una possibile redistribuzione delle chiavi a utenti non autorizzati.

A causa dei rischi per la sicurezza correlati all'utilizzo dell'autenticazione a chiave WEP condivisa, Novell supporta esclusivamente l'autenticazione a chiave WEP aperta. Con l'autenticazione condivisa, il processo di convalida della chiave per il client/punto di accesso invia una versione con testo non cifrato e una versione con testo cifrato di una stringa di autenticazione che può essere facilmente intercettata tramite connessione wireless. In questo modo un pirata informatico ha la possibilità di impossessarsi della stringa in versione cifrata e non cifrata. Una volta ottenute queste informazioni, violare la chiave diventa una banalità.



Immettere le seguenti informazioni per ciascun punto di accesso:

- **SSID:** Identificare il numero SSID. Il numero SSID distingue tra maiuscole e minuscole.

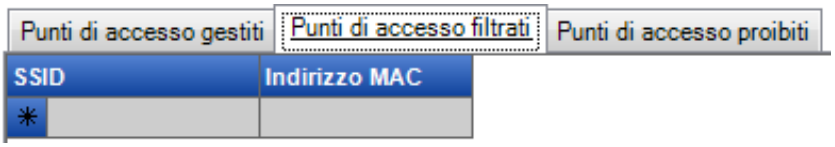
- **Indirizzo MAC:** Identificare l'indirizzo MAC (consigliato per distinguere tra SSID simili). Se non viene specificato un punto di accesso, si suppone che più punti di accesso segnalino lo stesso numero SSID.
- **Chiave:** Specificare la chiave WEP per il punto di accesso (10 o 26 caratteri esadecimali).
- **Tipo chiave:** Identificare il tipo di chiave di cifratura, selezionando il livello appropriato dall'elenco a discesa.
- **Segnalazione:** Selezionare questa casella di controllo se il punto di accesso definito sta trasmettendo il proprio SSID. Lasciare questa opzione deselezionata se il punto di accesso non emette la segnalazione.

Nota: ZENworks Security Client tenta prima di connettersi a ciascun punto di accesso che emette la segnalazione indicato nelle norme. Se non viene individuato un accesso con segnalazione, ZENworks Security Client tenta di connettersi a uno dei punti di accesso senza segnalazione (identificati da SSID) elencati nelle norme.

Quando si definiscono uno o più punti di accesso nell'elenco *Punti di accesso gestiti*, è possibile impostare la potenza del segnale dell'adattatore Wi-Fi.

Punti di accesso filtrati

I punti di accesso immessi nell'elenco *Punti di accesso filtrati* sono gli unici punti di accesso visualizzati in Zero Configuration. Ciò impedisce che un punto finale si connetta a punti di accesso non autorizzati.

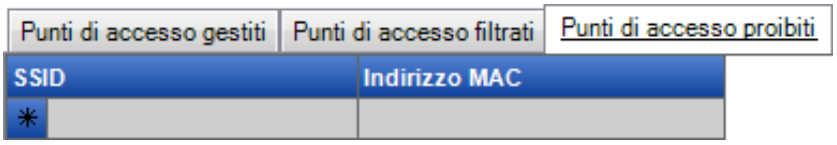


Immettere le seguenti informazioni per ciascun punto di accesso:

- **SSID:** Identificare il numero SSID. Il numero SSID distingue tra maiuscole e minuscole.
- **Indirizzo MAC:** Identificare l'indirizzo MAC (consigliato per distinguere tra SSID simili). Se non viene specificato un punto di accesso, si suppone che più punti di accesso segnalino lo stesso SSID.

Punti di accesso proibiti

I punti di accesso immessi nell'elenco Punti di accesso proibiti non vengono visualizzati in Zero Configuration e i punti finali non sono autorizzati a connettersi ad essi.



Immettere le seguenti informazioni per ciascun punto di accesso:

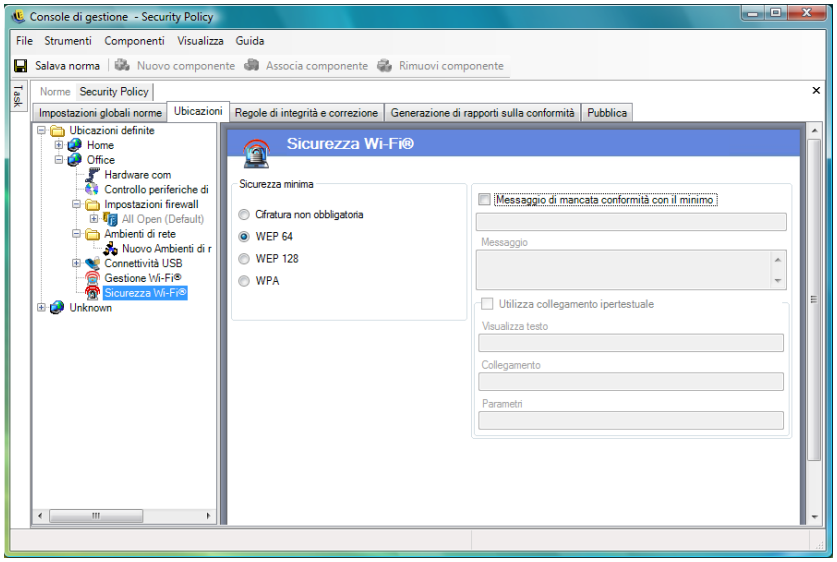
- **SSID:** Identificare il numero SSID. Il numero SSID distingue tra maiuscole e minuscole.
- **Indirizzo MAC:** Identificare l'indirizzo MAC (consigliato per distinguere tra SSID simili). Se non viene specificato un punto di accesso, si suppone che più punti di accesso segnalino lo stesso SSID.

Sicurezza Wi-Fi

Se l'hardware di comunicazione Wi-Fi (scheda PCMCIA adattatore Wi-Fi o altre schede e/o radio Wi-Fi integrate) è autorizzato a livello globale (vedere "Controllo wireless" a pagina 48), è possibile applicare impostazioni aggiuntive all'adattatore per l'ubicazione corrente.

Per accedere a questo controllo, fare clic sulla scheda *Ubicazioni*, quindi su *Sicurezza Wi-Fi* nell'albero delle norme visualizzato a sinistra.

Nota: In Sicurezza Wi-Fi o Gestione Wi-Fi la deselezione di *Abilita* comporta la disabilitazione di tutte le connessioni Wi-Fi nell'ubicazione.



È possibile impostare l'adattatore Wi-Fi in modo che comunichi solo con i punti di accesso che hanno un livello di cifratura uguale o superiore a un determinato livello in una data ubicazione.

Ad esempio, se in una succursale di un ufficio viene utilizzata una configurazione WPA di punti di accesso, è possibile impostare l'adattatore in modo che comunichi solo con i punti di accesso che hanno un livello di cifratura superiore o uguale a WEP 128. In questo modo si impedisce all'adattatore di collegarsi accidentalmente a punti di accesso inaffidabili o non sicuri.

Si consiglia di immettere un messaggio utente personalizzato quando si seleziona l'impostazione *Cifratura non obbligatoria*.

Quando si immettono due o più punti di accesso negli elenchi *Punti di accesso gestiti* e *Punti di accesso filtrati*, è possibile impostare una preferenza per effettuare la connessione ai punti di accesso in base al livello di cifratura o alla potenza del segnale. Il livello selezionato impone la connettività con i punti di accesso che soddisfano i requisiti di cifratura minimi.

Ad esempio, se il requisito di cifratura è WEP 64 e la preferenza è basata sulla cifratura, i punti di accesso con il livello di cifratura più elevato avranno la preferenza su tutti gli altri. Se la preferenza è basata sulla potenza di segnale, i punti di accesso con il segnale più potente avranno la preferenza durante la connessione.

2.2.3 Regole di integrità e correzione

ZENworks Endpoint Security Management è dotato di una funzionalità in grado di verificare l'esecuzione delle applicazioni software sui punti finali e fornisce procedure correttive immediate qualora la verifica abbia esito negativo.

Le seguenti sezioni contengono informazioni aggiuntive:

- “Regole antivirus e antispyware” a pagina 93
- “Test di integrità” a pagina 95
- “Controlli di integrità” a pagina 96
- “Regole di scripting avanzate” a pagina 97

Regole antivirus e antispyware

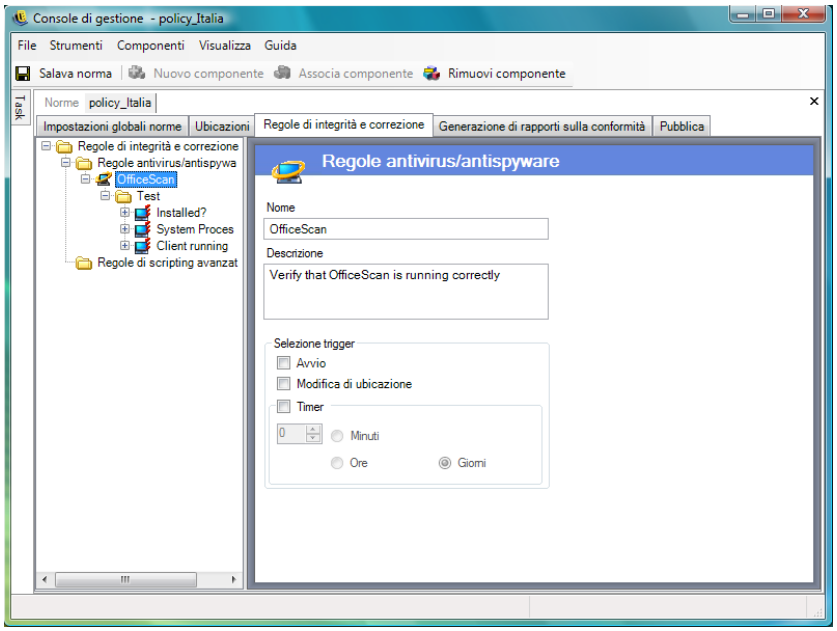
Le regole antivirus e antispyware verificano che il software antivirus o antispyware presente nel punto finale sia in esecuzione e aggiornato. Vengono eseguiti dei test per stabilire se il software è aggiornato e in esecuzione. Se entrambi i controlli hanno esito positivo, è possibile passare a qualsiasi ubicazione definita. L'esito negativo di uno dei test può determinare le seguenti azioni (definite dall'amministratore):

- Viene inviato un rapporto al servizio di generazione rapporti.
- Viene visualizzato un messaggio utente personalizzato con un collegamento facoltativo che fornisce informazioni sulle modalità di correzione della violazione della regola.
- L'utente viene messo in stato di quarantena: l'accesso alla rete viene limitato e viene bloccato l'accesso per determinati programmi per impedire l'ulteriore infezione della rete.

Una volta stabilita la conformità dei punti finali mediante un test successivo, le impostazioni di sicurezza ritornano automaticamente al loro stato originario.

Nota: Questa funzione è disponibile solo nell'installazione di ZENworks Endpoint Security Management e non può essere utilizzata per le norme di sicurezza di UWS.

Per accedere a questo controllo, fare clic sulla scheda *Regole di integrità e correzione* e fare clic su *Regole antivirus/antispyware* nell'albero delle norme visualizzato a sinistra.



È possibile creare test personalizzati per le applicazioni software non presenti nell'elenco di default. È possibile creare un singolo test che esegua controlli su una o più applicazioni software con la stessa regola. Ciascun controllo di file esistenti e processi in esecuzione ha il proprio risultato con esito positivo o negativo.

Per creare una nuova regola antivirus o antispyware:

1. Selezionare *Regole antivirus/antispyware* dall'albero dei componenti e fare clic su *Nuovo - Antivirus/antispyware*.
2. Fare clic su *Nuovo componente*.
3. Assegnare un nome alla regola e immettere una descrizione.
4. Selezionare il trigger per la regola:
   - **Avvio:** Consente di eseguire i test all'avvio del sistema.
   - **Cambio ubicazione:** Consente di eseguire i test ogni volta che ZENworks Security Client passa a una nuova ubicazione.
   - **Timer:** Consente di eseguire test di integrità secondo una pianificazione basata su minuti, ore o giorni.
5. Fare clic su *Salva norme*. Se le norme in uso presentano errori, vedere Sezione 2.2.6, “Notifica di errore”, a pagina 105.
6. Definire i test di integrità.

Per associare regole antivirus o antispyware esistenti:

1. Selezionare *Regole antivirus/antispyware* e fare clic su *Associa componente*.
2. Selezionare le regole desiderate dall'elenco.
3. (Facoltativo) Ridefinire i test, i controlli e i risultati.

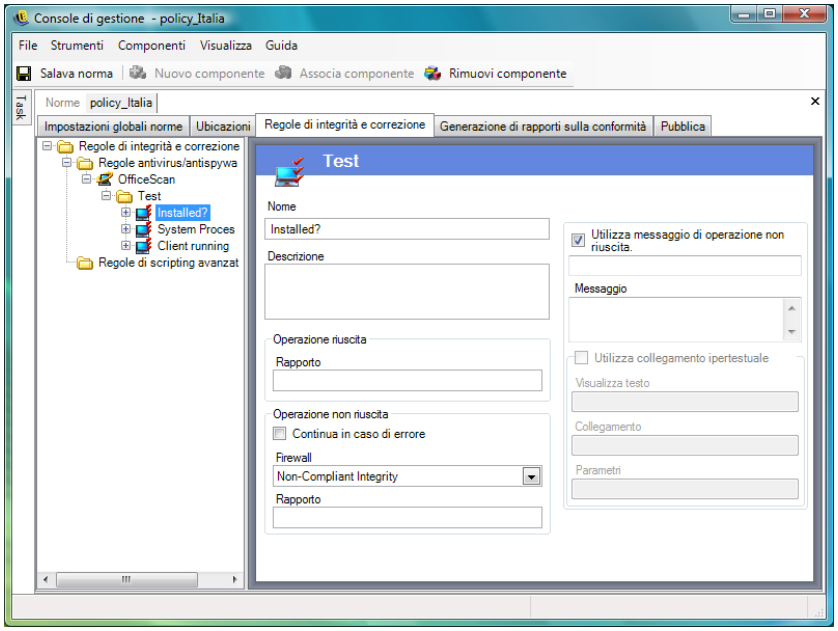
Nota: La modifica delle impostazioni di un componente condiviso ha effetto su tutte le altre istanze dello stesso componente. Utilizzare il comando *Mostra utilizzo* per visualizzare tutte le altre norme associate al componente.

4 Fare clic su *Salva norme*. Se le norme in uso presentano errori, vedere Sezione 2.2.6, "Notifica di errore", a pagina 105.

I test e i controlli di integrità vengono inclusi automaticamente e possono essere modificati in base alle necessità.

Test di integrità

Per ogni test di integrità possono essere eseguiti due controlli, *File esistenti* e *Processi in esecuzione*. Ogni test ha il proprio risultato, con esito positivo o negativo.



Tutte le regole antivirus e antispyware definite hanno test e controlli standard prestabiliti. È possibile aggiungere test supplementari alla regola di integrità.

L'esecuzione di più test avviene nell'ordine specificato. Il primo test deve essere completato correttamente per poter eseguire il test successivo.

Per creare un test di integrità:

1 Selezionare *Test integrità* dall'albero dei componenti, fare clic sull'icona con il segno + accanto al rapporto desiderato per espandere l'elenco, fare clic con il pulsante destro del mouse su *Test* e fare clic su *Aggiungi nuovo - Test*.

2 Assegnare un nome al test e immettere una descrizione.

3 Specificare il testo del rapporto di operazione riuscita per il test.

4 Definire le seguenti opzioni in caso di operazione non riuscita:

- **Continua in caso di errore:** Selezionare questa opzione per consentire all'utente di continuare a utilizzare la connettività di rete in caso di esito negativo del test o qualora fosse necessario ripetere il test.
- **Firewall:** Questa impostazione viene applicata in caso di esito negativo del test. Le opzioni Tutte chiuse, Integrità non conforme o un'impostazione personalizzata della quarantena consentono di impedire la connessione alla rete da parte dell'utente.
- **Messaggio:** Selezionare un messaggio utente personalizzato da visualizzare in caso di esito negativo del test. Il messaggio può includere istruzioni di correzione per l'utente finale.
- **Rapporto:** Indicare il rapporto di operazione non riuscita inviato al servizio di generazione rapporti.

5 Immettere un messaggio di operazione non riuscita. Questo messaggio viene visualizzato solo quando uno o più controlli hanno esito negativo. Fare clic sulla casella di controllo e specificare le informazioni del messaggio nelle caselle visualizzate.

6 È possibile aggiungere un collegamento ipertestuale per fornire operazioni di correzione. Può trattarsi di un collegamento a ulteriori informazioni o un collegamento che consente di scaricare una patch o un aggiornamento per il test con esito negativo (vedere Sezione , “Collegamenti ipertestuali”, a pagina 67).

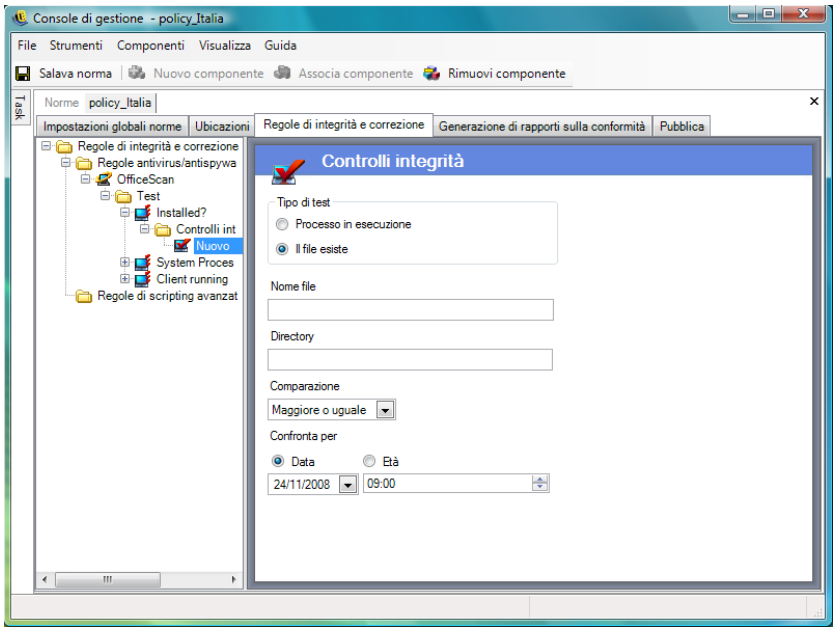
7 Fare clic su *Salva norme*. Se le norme in uso presentano errori, vedere Sezione 2.2.6, “Notifica di errore”, a pagina 105.

8 Definire i test di integrità.

9 Ripetere i passaggi descritti sopra per creare un nuovo test antivirus o antispyware.

Controlli di integrità

I controlli previsti per ciascun test consentono di determinare se uno o più processi antivirus/antispyware sono in esecuzione o se esistono dei file essenziali. Per l'esecuzione di un test di integrità è necessario definire almeno un controllo.



Per creare un nuovo controllo, fare clic con il pulsante destro del mouse su *Controlli integrità* dall'albero delle norme visualizzato a sinistra, quindi scegliere *Aggiungi nuovo - Controlli integrità*. Selezionare uno dei due tipi di controllo e immettere le seguenti informazioni:

Processo in esecuzione: Determinare se il software è in esecuzione al momento dell'evento trigger (ad esempio, il client AV). Per eseguire questo controllo, è sufficiente immettere il nome del file eseguibile.

File esistenti: Questo controllo consente di stabilire se il software è aggiornato al momento dell'attivazione dell'evento.

Immettere le seguenti informazioni negli appositi campi:

- **Nome file:** Specificare il nome del file che si desidera controllare.
- **Directory file:** Specificare la directory in cui il file risiede.
- **Confronto file:** Selezionare un confronto di date dall'elenco a discesa:
  - Nessuno
  - Uguale
  - Maggiore o uguale
  - Minore o uguale
- **Confronta per:** Specificare *Età* o *Data*.
  - *Data* assicura che il file non sia precedente alla data e all'ora specificate (ad esempio, la data dell'ultimo aggiornamento).
  - *Età* assicura che il file non sia precedente a un periodo di tempo specifico, espresso in giorni.

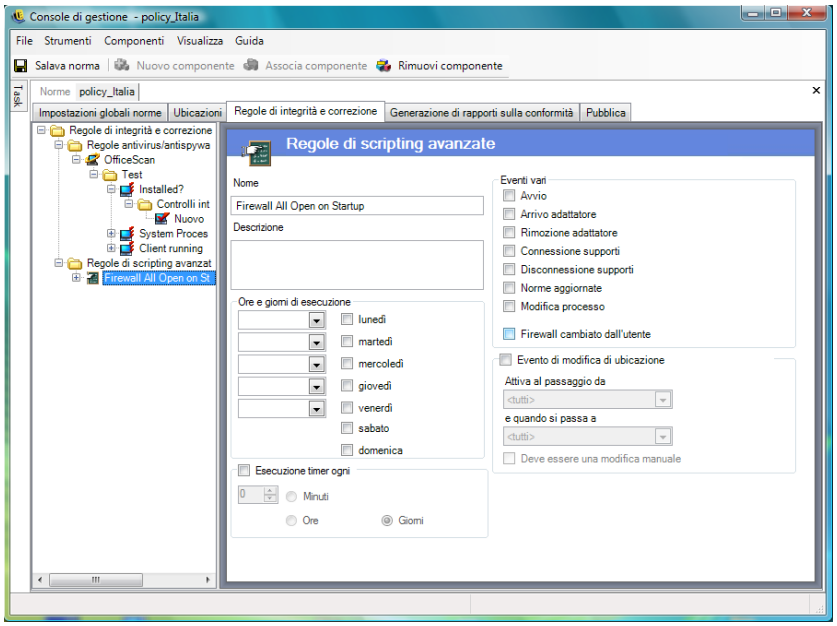
Nota: Se si seleziona l'opzione *Età*, il metodo di confronto Uguale viene considerato equivalente al metodo Minore o uguale.

I controlli vengono eseguiti nell'ordine in cui vengono immessi.

Regole di scripting avanzate

ZENworks Endpoint Security Management include uno strumento di scripting per le regole che consente agli amministratori di creare regole e azioni correttive estremamente flessibili e complesse.

Per accedere a questo controllo, fare clic sulla scheda *Regole di integrità e correzione* e scegliere l'icona *Regole di scripting avanzate* nell'albero delle norme visualizzato a sinistra.



Lo strumento di scripting utilizza i comuni linguaggi di scripting VBScript o JScript per creare regole che contengono un trigger (che definisce quando la regola va eseguita) e lo script vero e proprio (la logica della regola). La scelta del tipo di script da eseguire da parte dell'amministratore non è sottoposta a restrizioni.

Lo scripting avanzato viene implementato in sequenza insieme ad altre regole di integrità. Di conseguenza, uno script con un lungo tempo di esecuzione impedisce l'esecuzione di altre regole (comprese le regole a tempo) finché non viene completato.

Per creare una nuova regola di scripting avanzata:

1. Fare clic con il pulsante destro del mouse su *Regole di scripting avanzate* nell'albero dei componenti, quindi scegliere *Aggiungi nuovo - Regole di scripting*.
2. Assegnare un nome alla regola e immettere una descrizione.
3. Specificare gli eventi trigger.
   - **Ore e giorni di esecuzione:** Specificare fino a cinque ore diverse per l'esecuzione dello script. Lo script viene eseguito una volta alla settimana, nei giorni selezionati.
   - **Esecuzione timer ogni:** Specificare la frequenza di esecuzione del timer.
   - **Eventi vari:** Specificare gli eventi sul punto finale che attivano lo script.
   - **Evento di modifica di ubicazione:** Specificare l'evento di modifica di ubicazione che attiva lo script. Tali eventi non sono indipendenti, ma si aggiungono all'evento precedente.
     - **Evento modifica ubicazione:** Lo script viene eseguito ogni volta che l'ubicazione cambia.
     - **Attiva quando si passa da:** Lo script viene eseguito solo quando l'utente lascia l'ubicazione specificata per qualsiasi altra ubicazione.

- **Attiva quando si passa a:** Lo script viene eseguito quando l'utente accede all'ubicazione specificata da qualsiasi altra ubicazione. Se per l'opzione *Attiva quando si passa a* viene fornito un parametro di ubicazione, ad esempio Ufficio, lo script viene eseguito solo quando l'ubicazione passa dall'ufficio all'ubicazione specificata).
- **Modifica manuale obbligatoria:** Lo script viene eseguito solo quando l'utente passa manualmente a o da un'ubicazione.

4 Creare delle variabili script. Per ulteriori informazioni, vedere "Variabili script" a pagina 99.

5 Scrivere il testo dello script. Per ulteriori informazioni, consultare "Testo dello script" a pagina 101.

6 Fare clic su *Salva norme*. Se le norme in uso presentano errori, vedere Sezione 2.2.6, "Notifica di errore", a pagina 105.

Per associare una regola di scripting avanzata esistente:

1 Selezionare *Regole di scripting avanzate* nell'albero dei componenti e fare clic su *Associa nuovo*.

2 Selezionare le regole desiderate dall'elenco.

3 Ridefinire l'evento trigger, le variabili o lo script, secondo le proprie esigenze.

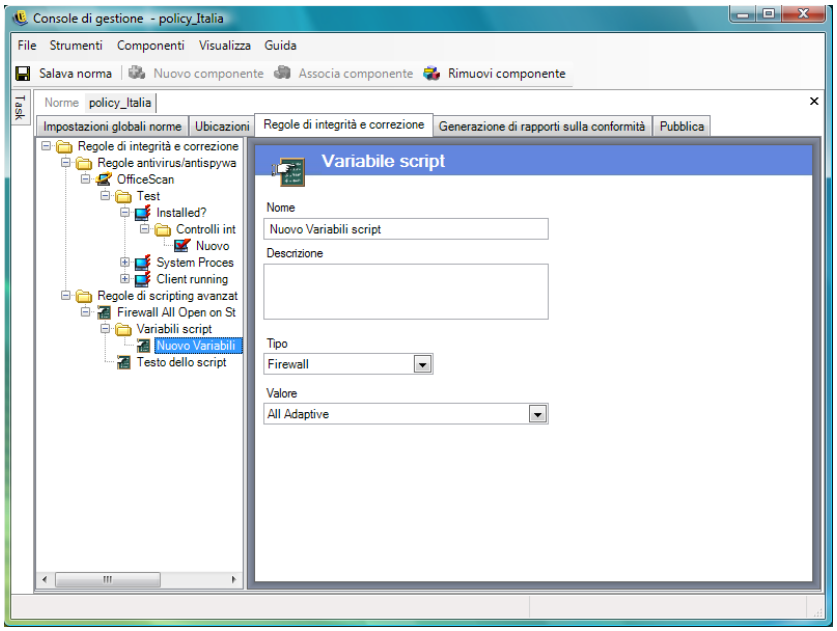
Nota: La modifica delle impostazioni di un componente condiviso ha effetto su tutte le altre istanze dello stesso componente. Utilizzare il comando *Mostra utilizzo* per visualizzare tutte le altre norme associate al componente.

---

4 Fare clic su *Salva norme*. Se le norme in uso presentano errori, vedere Sezione 2.2.6, "Notifica di errore", a pagina 105.

Variabili script

Si tratta di un'impostazione facoltativa che consente all'amministratore di definire una variabile (var) per lo script e di utilizzare una funzionalità diZENworks Endpoint Security Management (ad esempio, visualizzare messaggi utente personalizzati o collegamenti ipertestuali definiti, passare a un'ubicazione o a un'impostazione del firewall definita), oppure di modificare il valore della variabile senza modificare lo script stesso.



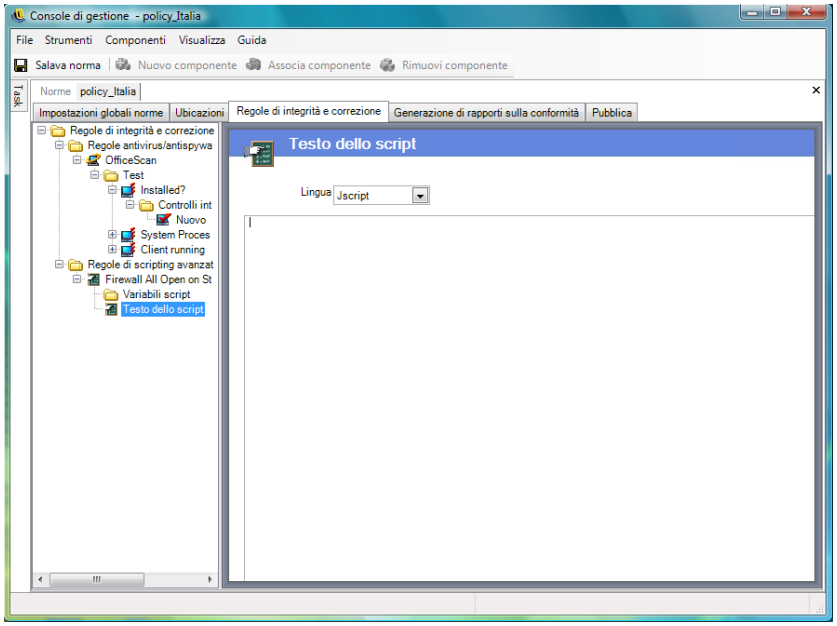
Per creare una nuova variabile per lo script:

1. Fare clic con il pulsante destro del mouse su *Variabili script* dall'albero dei componenti e fare clic su *Aggiungi nuovo - Variabili*.
2. Assegnare un nome alla variabile e immettere una descrizione.
3. Selezionare il tipo di variabile:
   - **Messaggi utente personalizzati:** Definisce un messaggio utente personalizzato che può essere avviato come un'azione.
   - **Firewall:** Definisce un'impostazione del firewall che può essere applicata come un'azione.
   - **Collegamenti ipertestuali:** Definisce un collegamento ipertestuale che può essere avviato come un'azione.
   - **Ubicazione:** Definisce un'ubicazione che può essere applicata come un'azione.
   - **Numero:** Definisce un valore numerico.
   - **Stringa:** Definisce un valore stringa.
4. Specificare il valore della variabile:
   - Tutte adattive
   - Tutte chiuse
   - Tutte aperte
   - Nuove impostazioni firewall
   - Integrità non conforme
5. Fare clic su *Salva norme*. Se le norme in uso presentano errori, vedere Sezione 2.2.6, “Notifica di errore”, a pagina 105.

Testo dello script

L'amministratore di ZENworks Endpoint Security Management non si limita a decidere il tipo di script che verrà eseguito da ZENworks Security Client. Tutti gli script devono essere testati prima della distribuzione delle norme.

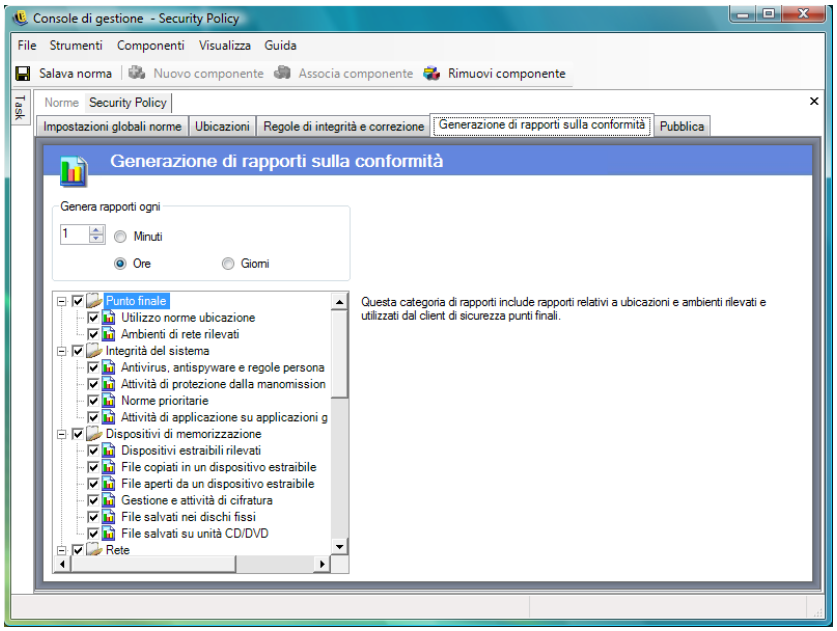
Selezionare il tipo di script (Jscript o VBscript) e immettere il testo nel relativo campo. Lo script può essere copiato da un'altra origine e incollato nel campo.



2.2.4 Rapporti di conformità

Grazie al livello e all'accesso dei driver di ZENworks Security Client, è possibile creare rapporti per qualsiasi transazione eseguita dal punto finale. Il punto finale può eseguire ciascun inventario di sistema facoltativo ai fini della soluzione dei problemi o della creazione di norme. Per accedere ai rapporti, fare clic sulla scheda *Rapporti di conformità*.

Nota: La generazione di rapporti non è disponibile quando si esegue la console di gestione autonoma.



Per eseguire i rapporti di conformità per queste norme:

1. Specificare la frequenza di generazione dei rapporti. Indica la frequenza con cui i dati vengono trasferiti da ZENworks Security Client al servizio di distribuzione norme.
2. Selezionare ciascuna categoria o tipo di rapporto che si desidera acquisire.

Sono disponibili i seguenti rapporti:

Punto finale

- **Utilizzo norme ubicazione:** ZENworks Security Client genera rapporti relativi a tutte le norme sulle ubicazioni applicate e sulla loro durata.
- **Ambienti di rete rilevati:** ZENworks Security Client genera rapporti relativi alle impostazioni di tutti gli ambienti di rete rilevati.

Integrità del sistema

- **Antivirus, antispyware e regole personalizzate:** ZENworks Security Client genera rapporti relativi ai messaggi di integrità configurati, in base ai risultati dei test.
- **Attività di protezione dalla manomissione dei punti finali:** ZENworks Security Client genera rapporti relativi a eventuali tentativi di manomissione del client di sicurezza.
- **Norme prioritarie:** ZENworks Security Client genera rapporti relativi a tutti i tentativi di avvio della priorità amministrativa sul client di sicurezza.
- **Attività di applicazione su applicazioni gestite:** ZENworks Security Client genera rapporti relativi a tutte le attività di applicazione su applicazioni gestite.

Dispositivi di memorizzazione

- **Dispositivi estraibili rilevati:** ZENworks Security Client genera rapporti relativi a tutte le attività di applicazione su applicazioni gestite.

- **File copiati in un dispositivo estraibile:** ZENworks Security Client genera rapporti relativi ai file copiati su un dispositivo di memorizzazione estraibile.
- **File aperti da un dispositivo estraibile:** ZENworks Security Client genera rapporti relativi ai file aperti da un dispositivo di memorizzazione estraibile.
- **Gestione e attività di cifratura:** ZENworks Security Client genera rapporti sull'attività di cifratura/decifratura mediante ZENworks Storage Encryption Solution.
- **File salvati nei dischi fissi:** ZENworks Security Client genera rapporti sul numero di file scritti nelle unità a disco fisso del sistema.
- **File salvati su unità CD/DVD:** ZENworks Security Client genera rapporti sul numero di file scritti sulle unità CD/DVD del sistema.

Networking

- **Attività firewall:** ZENworks Security Client genera rapporti relativi a tutto il traffico bloccato dal firewall configurato per le norme di ubicazione applicate.

  Importante: L'abilitazione di questo rapporto potrebbe causare il richiamo di grandi quantità di dati. I dati possono creare rapidamente un sovraccarico del database. Il test di un solo client di sicurezza ha riportato 1.115 caricamenti di dati di pacchetti bloccati in un intervallo di 20 ore. È opportuno eseguire un periodo di monitoraggio e ottimizzazione con un client di prova nell'ambiente interessato prima della distribuzione su larga scala.

- **Attività adattatore di rete:** ZENworks Security Client genera rapporti relativi a tutte le attività associate al traffico su un dispositivo di rete gestito.

Wi-Fi

- **Punti di accesso wireless rilevati:** ZENworks Security Client genera rapporti relativi a tutti i punti di accesso rilevati.
- **Connessioni a punti di accesso wireless:** ZENworks Security Client genera rapporti relativi a tutte le connessioni ai punti di accesso effettuate dal punto finale.

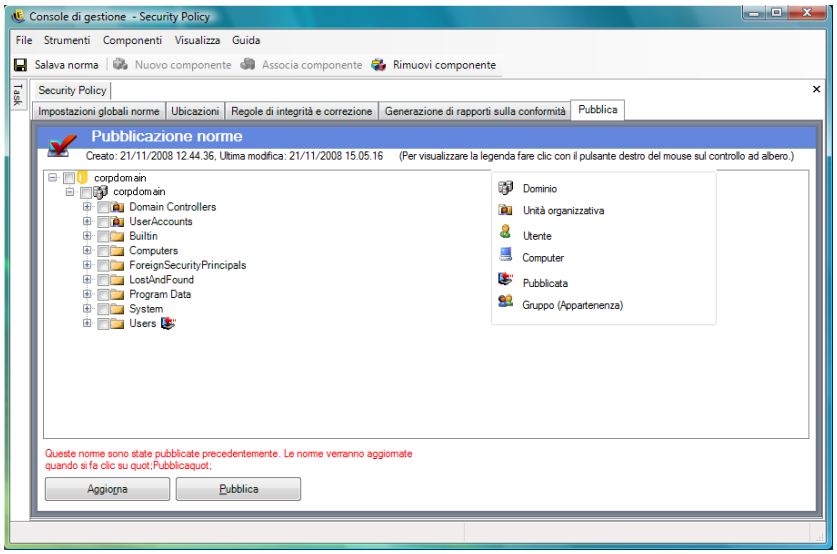
Inventario del dispositivo

- **Dispositivi USB:** ZENworks Security Client genera report su tutti i dispositivi USB rilevati nel sistema.

2.2.5 Pubblica

Le norme di sicurezza completate vengono inviate agli utenti mediante il meccanismo di pubblicazione. Dopo la pubblicazione è possibile aggiornare ulteriormente le norme con gli aggiornamenti che l'utente finale riceve quando effettua i check-in pianificati. Per pubblicare le norme, fare clic sulla scheda *Pubblica*. Vengono visualizzate le seguenti informazioni:

- L'albero della directory corrente.
- Le date di creazione e modifica delle norme.
- I pulsanti *Aggiorna* e *Pubblica*.



In base alle autorizzazioni di pubblicazione dell'utente corrente, è possibile che una o più selezioni vengano visualizzate in rosso nell'albero della directory. Gli utenti non sono autorizzati a pubblicare agli utenti/gruppi visualizzati in rosso.

Gli utenti e i relativi gruppi associati non vengono visualizzati finché non effettuano l'autenticazione al servizio di gestione. Le modifiche apportate al servizio di directory aziendale potrebbero non essere visualizzate immediatamente nella console di gestione. Fare clic su *Aggiorna* per aggiornare l'albero della directory per il servizio di gestione.

Le seguenti sezioni contengono informazioni aggiuntive:

- “Pubblicazione di norme” a pagina 104
- “Aggiornamento di norme pubblicate” a pagina 104

Pubblicazione di norme

1. Selezionare un gruppo di utenti (o singoli utenti) dall'albero della directory visualizzato a sinistra. Fare doppio clic sugli utenti per selezionarli (se viene selezionato un gruppo di utenti, sono inclusi tutti gli utenti).

   Accanto agli utenti che non hanno ricevuto le norme viene visualizzata l'icona . L'icona viene visualizzata nell'albero della directory accanto al nome dell'utente o del gruppo che ha già ricevuto le norme.

   Per annullare la selezione di un utente o gruppo ed eliminare l'icona , fare doppio clic sul nome.

2. Fare clic su *Pubblica* per inviare le norme al servizio di distribuzione norme.

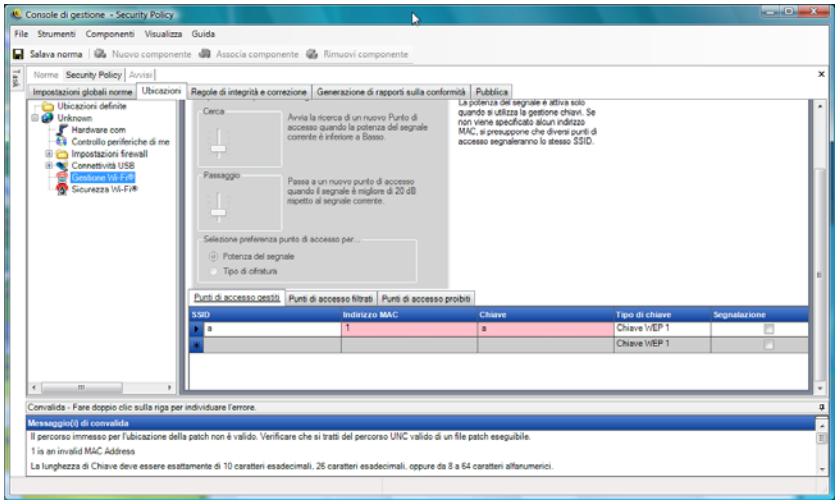
Aggiornamento di norme pubblicate

Una volta pubblicate le norme per gli utenti, è possibile mantenerle aggiornate semplicemente modificandone i componenti e ripubblicandole. Se ad esempio l'amministratore di ZENworks Endpoint Security Management deve cambiare la chiave WEP per un punto di accesso, sarà sufficiente modificare la chiave, salvare le norme e fare clic su *Pubblica*. L'utente finale interessato riceve le norme aggiornate (con la nuova chiave) al check-in successivo.

2.2.6 Notifica di errore

Quando l'amministratore tenta di salvare le·norme in un componente con dati incompleti o errati, nella parte inferiore della console di gestione viene visualizzato il riquadro Convalida, nel quale viene evidenziato ciascun errore. Ogni errore deve essere corretto prima di poter salvare le norme.

Fare doppio clic su ciascuna riga di convalida per visualizzare la schermata con l'errore. Gli errori vengono evidenziati come indicato nella figura riportata di seguito.

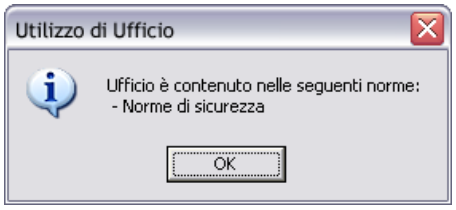


2.2.7 Mostra utilizzo

Le modifiche apportate ai componenti delle norme condivisi interesseranno tutte le norme cui sono associati. Prima di aggiornare o modificare un componente delle·norme, si consiglia di eseguire il comando *Mostra utilizzo* per determinare le norme che verranno interessate dalla modifica.

1 Fare clic con il pulsante destro del mouse sul componente e fare clic su *Mostra utilizzo*.

Viene visualizzata una finestra popup nella quale viene mostrata ciascuna istanza del componente in altre norme.



2.3 Importazione ed esportazione di norme

Le seguenti sezioni contengono informazioni aggiuntive:

- Sezione 2.3.1, “Importazione delle norme”, a pagina 106
- Sezione 2.3.2, “Esportazione delle norme”, a pagina 106
- Sezione 2.3.3, “Esportazione delle norme per utenti non gestiti”, a pagina 106

2.3.1 Importazione delle norme

È possibile importare le norme da qualsiasi ubicazione file sulla rete disponibile.

1. Nella console di gestione fare clic su *File* > *Importa norme*.

   Se si stanno modificando o progettando delle norme, prima di aprire la finestra di importazione le norme vengono chiuse dall'editor (e viene richiesto di salvarle).

2. Individuare il percorso del file e specificare il nome del file nel campo.

Una volta importate le norme, è possibile modificarle ulteriormente o pubblicarle subito.

2.3.2 Esportazione delle norme

Le norme possono essere esportate dalla console di gestione e distribuite via e-mail o mediante una condivisione di rete. Questa funzionalità consente di distribuire norme aziendali in ambienti in cui vengono utilizzati più servizi di gestione ed editor delle norme.

Per esportare le norme di sicurezza:

1. Nella console di gestione fare clic su *File* > *Esporta*.
2. Specificare una destinazione e assegnare alle norme un nome con estensione `.sen` (ad esempio, `C:\Desktop\normevendita.sen`). Per selezionare un percorso, fare clic sul pulsante Sfoglia.
3. Fare clic su *Esporta*.

Vengono esportati due file. Il primo è il file delle norme (`*.file`). Il secondo file è il file `setup.sen`, necessario per la decifratura delle norme durante l'importazione.

Le norme esportate devono essere importate in una console di gestione prima di essere pubblicate agli utenti gestiti.

2.3.3 Esportazione delle norme per utenti non gestiti

In caso di distribuzione di un'installazione non gestita di ZENworks Security Client nell'azienda, è necessario installare una console di gestione autonoma per creare le norme. Per ulteriori informazioni, vedere la "Guida all'installazione di ZENworks Endpoint Security Management".

Per distribuire le norme non gestite:

1. Individuare e copiare il file `setup.sen` della console di gestione in una cartella separata.

   Il file `setup.sen` viene generato all'installazione della console di gestione e viene collocato nella directory `\Programmi\Novell\ESM Management Console\`.

2. Creare le norme nella console di gestione. Per ulteriori informazioni, consultare Sezione 2.2, "Creazione delle norme di sicurezza", a pagina 45.
3. Utilizzare il comando *Esporta* per esportare le norme nella stessa cartella contenente il file `setup.sen`.

   A tutte le norme distribuite deve essere assegnato il nome `policy.sen` affinché ZENworks Security Client le accetti.

4. Distribuire i file `norme.sen` e `setup.sen`. I file devono essere copiati nella directory `\Programmi\Novell\ZENworks Security Client\` per tutti i client non gestiti.

Il file `setup.sen` deve essere copiato nelle copie di ZENworks Security Client non gestite solo una volta con le prime norme. In seguito sarà necessario distribuire solo le nuove norme.