AUTHORIZED DOCUMENTATION

# Guida all'installazione

January 5, 2009

# Novell®
# ZENworks® Endpoint Security Management

**3.5**

www.novell.com

## Note legali

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

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

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



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

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

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

## Marchi di fabbrica di Novell

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

## Materiali di terze parti

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

# Sommario

# Informazioni sulla Guida

La presente *Guida all'installazione di Novell® ZENworks® Endpoint Security Management* fornisce istruzioni complete sull'installazione dei componenti di ZENworks Endpoint Security Management e assiste gli amministratori durante la gestione e l'esecuzione degli stessi.

Le informazioni della guida sono organizzate come segue:



### Destinatari

Questa guida è destinata agli amministratori di ZENworks Endpoint Security Management.

### Feedback

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

### Documentazione aggiuntiva

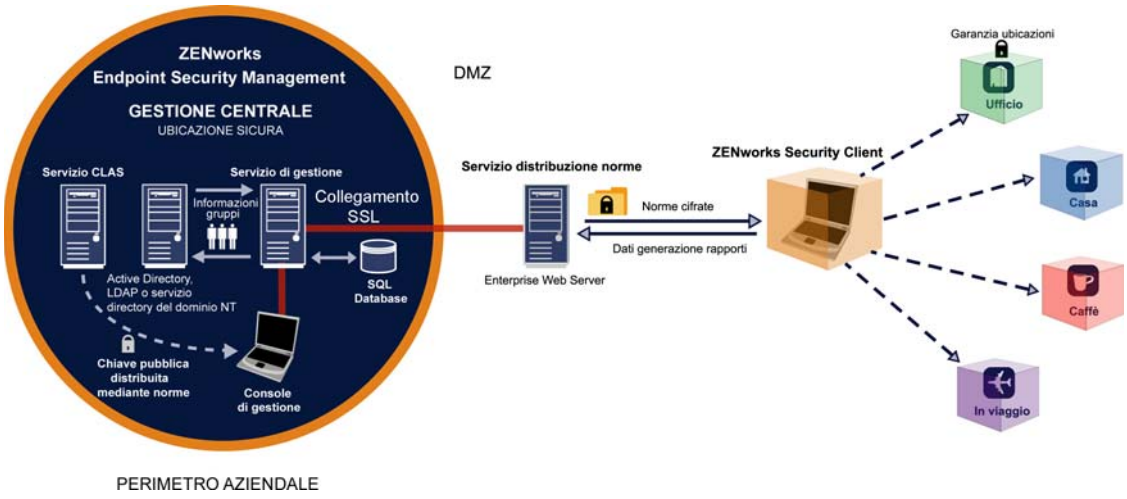
È disponibile ulteriore documentazione (nei formati PDF e HTML) relativa a ZENworks Endpoint Security Management e alla sua modalità di implementazione. Per ulteriore documentazione, visitare il sito Web relativo alla documentazione di ZENworks Endpoint Security Management 3.5 (http://www.novell.com/documentation/zesm35).

# ZENworks Endpoint Security Management Panoramica

# 1

Novell® ZENworks® Endpoint Security Management è costituito da cinque componenti funzionali di livello elevato: il servizio di distribuzione norme, il servizio di gestione, la console di gestione, il servizio garanzia ubicazioni client e l'Endpoint Security Client. L'illustrazione che segue mostra tali componenti nell'architettura:

***Figura 1-1*** *Architettura di ZENworks Endpoint Security Management*




Endpoint Security Client è responsabile dell'applicazione delle norme di sicurezza distribuite al sistema di endpoint. L'installazione di Endpoint Security Client in tutti i computer aziendali consente agli endpoint di spostarsi all'esterno del perimetro aziendale e di rimanere protetti e agli endpoint rimasti all'interno del perimetro di ricevere controlli di sicurezza aggiuntivi all'interno del firewall del perimetro.

Ciascun componente di gestione centrale viene installato separatamente, eccetto per un'installazione su server singolo. Per ulteriori informazioni, vedere Capitolo 3, “Installazione su server singolo”, a pagina 17.

I componenti riportati di seguito sono installati su server protetti all'interno del perimetro aziendale:

- **Servizio di distribuzione delle norme:** Responsabile della distribuzione delle norme di sicurezza a Endpoint Security Client e del recupero dei dati sui rapporti da Endpoint Security Client. È possibile distribuire il servizio di distribuzione norme nella DMZ, all'esterno del firewall aziendale, per garantire aggiornamenti regolari delle norme per punti finali mobili.
- **Servizio di gestione:** Responsabile dell'assegnazione delle norme utente e dell'autenticazione dei componenti, del recupero dei dati sui rapporti, della creazione e divulgazione di rapporti ZENworks Endpoint Security Management, nonché della creazione e memorizzazione delle norme di sicurezza.
- **Console di gestione:** Interfaccia utente visibile, che si esegue direttamente sui server che ospitano il servizio di gestione o su una workstation che risiede all'interno del firewall aziendale con connessione al server del servizio di gestione. La console di gestione è utilizzata

sia per configurare il servizio di gestione sia per creare e gestire le norme di sicurezza degli utenti e dei gruppi. Le norme vengono create, copiate, modificate, divulgate e cancellate tramite la console di gestione.

- **Servizio garanzia ubicazioni client:** Fornisce una garanzia crittografica che i dispositivi sui quali è installato Endpoint Security Client si trovino effettivamente in un'ubicazione definita, come indicato da altri parametri dell'ambiente di rete esistente.

# 1.1 Requisiti di sistema

| Requisiti di sistema dei server | Requisiti di sistema di Endpoint (client) |
|---|---|
| **Sistemi operativi:**<br>Microsoft&thrdmrk; Windows&thrdmrk; 2000 Server SP4<br>Microsoft Windows 2000 Advanced Server SP4<br>Windows 2003 Server<br>**Processore:**<br>Pentium&thrdmrk; 4 HT 3,0 GHz (o superiore)<br>Almeno 756 MB di RAM (consigliato oltre 1 GB)<br>**Spazio su disco:**<br>500 MB: senza database Microsoft SQL locale<br>5 GB: con database MS SQL locale (SCSI consigliata)<br>**Software necessario:**<br>RDBMS supportato (SQL Server Standard, SQL Server Enterprise, Microsoft SQL Server 2000 SP4, SQL 2005)<br>Microsoft Internet Information Services (configurato per l'SSL)<br>Servizi di directory supportati (eDirectory™ o Active Directory&thrdmrk;)<br>.NET Framework 3.5 (solo per server e console di gestione)<br>**Console di gestione autonoma:**<br>RDBMS supportato (SQL Server Standard, SQL Server Enterprise, Microsoft SQL Server 2000 SP4, SQL 2005, SQL Express) | **Sistemi operativi:**<br>Windows XP SP1<br>Windows XP SP2<br>Windows 2000 SP4<br>Windows Vista SP1 (32 bit)<br>Windows Server 2008 (32 bit)<br>**Processore:**<br>Pentium 3 600 MHz (o superiore)<br>Minimo 128 MB di RAM (consigliati 256 MB o più)<br>**Spazio su disco:**<br>5 MB richiesti, 5 MB aggiuntivi consigliati per la generazione dei rapporti<br>**Software necessario:**<br>Windows 3.1 Installer<br>Tutti gli aggiornamenti di Windows devono essere i più recenti |

Il servizio di distribuzione norme, il servizio di gestione e il servizio garanzia ubicazioni client richiedono l'attivazione di un account locale di ASP.NET 2.0. Un account disabilitato non consentirebbe infatti il corretto funzionamento dei servizi.

## 1.2 Informazioni sulle guide di ZENworks Endpoint Security Management

Le guide di ZENworks Endpoint Security Management forniscono tre livelli di informazioni per gli utenti del prodotto.

- *Guida all'installazione di ESM:* fornisce istruzioni complete per l'installazione dei componenti di ZENworks Endpoint Security Management e assiste gli amministratori durante la gestione e l'esecuzione degli stessi. La guida in questione è quella che state leggendo in questo momento.
- *Guida dell'amministratore di ZENworks Endpoint Security Management*: questa guida è destinata agli amministratori di ZENworks Endpoint Security Management che si occupano della gestione dei servizi, della creazione delle norme di sicurezza per l'azienda, della generazione e analisi dei dati sui rapporti e dell'assistenza agli utenti per la risoluzione dei problemi. Questa guida contiene le istruzioni per l'esecuzione di queste attività.
- *Guida dell'utente di ZENworks Endpoint Security Client 3.5*: lo scopo di questa guida è fornire istruzioni all'utente relative al funzionamento di Endpoint Security Client. È possibile inviarla a tutti i dipendenti dell'azienda per aiutarli a comprendere le modalità di utilizzo di Endpoint Security Client.

# Installazione di ZENworks Endpoint Security Management

# 2

Le sezioni riportate di seguito contengono ulteriori informazioni sull'installazione di Novell® ZENworks® Endpoint Security Management:



## 2.1 Informazioni sulla preinstallazione

Il software di installazione di ZENworks Endpoint Security Management deve essere messo al sicuro per impedire eventuali manomissioni o uso non autorizzato. Analogamente, è necessario che gli amministratori rivedano le istruzioni relative alla preinstallazione e installazione per garantire il funzionamento senza interruzioni del sistema ZENworks Endpoint Security Management ed evitare che risulti vulnerabile a causa di inadeguata protezione dell'hardware.

L'amministratore che installa questo software deve essere l'amministratore principale per i server e il dominio. Se si utilizzano certificati SSL aziendali, per creare il certificato di protezione della radice SSL dovrà essere utilizzato anche lo stesso nome utente.

## 2.2 Pacchetti di installazione

Quando l'installazione viene eseguita dal DVD, si avvia un programma di installazione principale che utilizza una semplice interfaccia utente con cui l'amministratore di ZENworks Endpoint Security Management viene guidato attraverso il processo di installazione. Caricare il DVD di installazione su ciascun computer per accedere al programma principale e installare i componenti desiderati.

### 2.2.1 Informazioni sul programma di installazione principale

All'avvio, il programma di installazione principale consente di visualizzare due opzioni di menu: *Prodotti* e *Documentazione*.

Il collegamento *Prodotti* consente di aprire il menu di installazione. Gli elementi del menu presenti su questa schermata avviano il programma di installazione designato per ciascun componente. Nel caso di Endpoint Security Client 3.5 o Endpoint Security Client 4.0, è disponibile un'opzione aggiuntiva per avviare l'installazione in modalità Amministratore che aiuta l'amministratore di ZENworks Endpoint Security Management nella creazione di un pacchetto MSI per una distribuzione semplificata (vedere Capitolo 9.2, “Installazione MSI”, a pagina 61).

Per informazioni sul funzionamento completo dei componenti di ZENworks Endpoint Security Management, consultare la *Guida dell'amministratore di ZENworks Endpoint Security Management*, disponibile mediante il collegamento *Documentazione*.

## 2.3 Opzioni di installazione

Le installazioni dei componenti di back end di ZENworks Endpoint Security Management possono essere eseguite su un server singolo o su più server. Le installazioni su server singolo sono ideali per distribuzioni limitate che non richiedono aggiornamenti regolari delle norme. Le installazioni su più server sono ideali per distribuzioni più ampie che richiedono aggiornamenti regolari delle norme. Rivolgersi ai servizi professionali di Novell per individuare il tipo di installazione adatto alle proprie esigenze.

Endpoint Security Client è in grado di funzionare, in caso di necessità, senza connettersi al servizio di distribuzione norme. Analogamente, una console di gestione autonoma può essere eventualmente installata a scopo di valutazione. L'installazione relativa alla modalità di funzionamento Non gestita viene descritta in Capitolo 11, “Installazione non gestita di ZENworks Endpoint Security Management”, a pagina 79.

## 2.4 Ordine di installazione

ZENworks Endpoint Security Management deve essere installato nel seguente ordine:

1. Installazione su server singolo o installazione su più server
   - Servizio di distribuzione norme
   - Servizio di gestione
2. Console di gestione
3. Servizio garanzia ubicazioni client
4. Endpoint Security Client 3.5 o Endpoint Security Client 4.0

## 2.5 Prima di installare ZENworks Endpoint Security Management

Prima di avviare l'installazione, è necessario che l'amministratore di ZENworks Endpoint Security Management valuti quanto segue:

### In che modo gli utenti riceveranno le norme di sicurezza di ZENworks Endpoint Security Management?

Le opzioni per la distribuzione delle norme consentono di stabilire se gli utenti possono ricevere aggiornamenti ovunque, ossia anche all'esterno della rete centrale, oppure solo quando sono inseriti in una rete protetta (o comunque connessi tramite VPN). Alle organizzazioni che prevedono di aggiornare con frequenza le norme di sicurezza di ZENworks Endpoint Security Management, si consiglia di utilizzare un'installazione su più server che collochi il servizio di distribuzione norme in un server Web esterno alla DMZ.

### Tipi di distribuzioni server disponibili

Se l'azienda dispone solo di alcuni server, potrebbe essere necessario distribuire un'installazione su server singolo. Se invece la disponibilità di server non rappresenta un problema, è opportuno prendere in considerazione le dimensioni della distribuzione client e il numero di utenti che operano all'esterno del firewall.

### Distribuzione di SQL Server disponibile

Al momento dell'installazione ZENworks Endpoint Security Management crea tre database SQL. Se la distribuzione è ridotta, potrà essere installato un solo database SQL o un database lato server sui server del servizio di gestione e di distribuzione norme. Nel caso di distribuzioni più estese, dovrà invece essere impiegato un server di database SQL separato per ricevere i dati dai servizi di gestione e di distribuzione norme. Sono consentiti solo i tipi RDBMS riportati di seguito:

- SQL Server Standard
- SQL Server Enterprise
- Microsoft SQL Server 2000 SP4

Se l'istanza è denominata, la configurazione dei server sarà la seguente:

Provider=sqloledb

Origine dati=Nome server\Nome istanza (questo tipo di definizione è obbligatorio per l'installazione di ZENworks Endpoint Security Management)

Catalogo iniziale=Nome database

ID utente=Nome utente

Password=Password

Impostare SQL sulla modalità mista.

Il nome utente e la password utilizzati durante l'installazione non possono essere di un utente del dominio ma devono essere di un utente SQL con diritti SysAdmin.

### Per stabilire comunicazioni SSL si utilizzeranno certificati esistenti oppure certificati Novell firmati da se stessi?

Per progettazioni relative a recupero di emergenza e failover, devono essere utilizzati certificati SSL di un'Autorità di certificazione (VeriSign, GeoTrust, Thawte e così via) rilasciati dall'azienda o emessi in altro modo per distribuzioni complete di ZENworks Endpoint Security Management. Quando si utilizzano certificati propri, il certificato del servizio Web e la CA radice vengono creati sul computer designato come servizio di distribuzione norme e quindi distribuiti ai computer appropriati. Per creare un'Autorità di certificazione aziendale, vedere le istruzioni passo per passo su come impostare in modo sicuro una CA, disponibili sul sito Web di Microsoft.

Per valutazioni o distribuzioni ridotte (meno di 100 utenti), è possibile utilizzare i certificati firmati da se stessi di ZENworks Endpoint Security Management. I certificati SSL di Novell vengono installati sui server durante l'esecuzione dell'installazione tipica.

### Modalità di distribuzione dei client Endpoint Security Client

Il software di Endpoint Security Client può essere distribuito singolarmente su ciascun endpoint o attraverso una tecnologia Push MSI. Le istruzioni sulla creazione di pacchetti MSI sono reperibili in Capitolo 9.2, “Installazione MSI”, a pagina 61.

### Se le norme dovranno essere basate sul computer o sull'utente.

È possibile distribuire le norme in un solo computer, dove ciascun utente che esegue il login riceverà le stesse norme oppure impostarle per utenti singoli o gruppi.

Ogni installazione prevede diversi prerequisiti. Prima di eseguire l'installazione di qualsiasi componente, è consigliabile che tutti gli elenchi di controllo dei prerequisiti siano completi. Rivedere gli elenchi alle pagine riportate di seguito:


- Capitolo 3, “Installazione su server singolo”, a pagina 17
- Capitolo 5, “Installazione del servizio di distribuzione norme”, a pagina 23
- Capitolo 6, “Installazione del servizio di gestione”, a pagina 31
- Capitolo 7, “Installazione della console di gestione”, a pagina 43
- Capitolo 8, “Installazione del servizio garanzia ubicazioni client”, a pagina 55
- Capitolo 9, “Installazione di Endpoint Security Client 3.5”, a pagina 59

# Installazione su server singolo

# 3

L'installazione su server singolo (SSI) di ZENworks® Endpoint Security Management consente la coesistenza sullo stesso server del servizio di distribuzione norme e del servizio di gestione (impossibile se non si utilizza questa opzione di installazione). Questo server deve essere distribuito all'interno del firewall per motivi di sicurezza e prevede che gli utenti ricevano gli aggiornamenti delle norme solo quando si trovano all'interno dell'infrastruttura aziendale oppure sono connessi mediante VPN.

La distribuzione dell'installazione su server singolo in un PDC (Controller di dominio primario) non è supportata sia per motivi di sicurezza che di funzionalità.

---

**Nota:** È consigliabile che il server SSI venga configurato (consolidato) in modo da disattivare tutte le applicazioni, i servizi, gli account e le altre opzioni non necessarie alla funzionalità designata del server. La procedura utilizzata dipende dalle specifiche dell'ambiente locale, pertanto non è possibile descriverla in anticipo. Si consiglia agli amministratori di consultare la sezione appropriata della pagina Web sulla sicurezza di Microsoft Technet (http://www.microsoft.com/technet/security/default.mspx). Ulteriori raccomandazioni relative al controllo dell'accesso sono disponibili nella *Guida dell'amministratore di ZENworks Endpoint Security Management*.

Per garantire un accesso protetto esclusivamente a computer attendibili, è possibile impostare la directory virtuale e IIS in modo da includere elenchi ACL. Fare riferimento agli articoli riportati di seguito:

- Granting and Denying Access to Computers (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- Restrict Site Access by IP Address or Domain Name (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- IIS FAQ: 2000 IP address and domain name restrictions (http://www.iisfaq.com/default.aspx?View=A136&P=109)
- Working With IIS Packet Filtering (http://www.15seconds.com/issue/011227.htm)

Per motivi di sicurezza, si raccomanda di rimuovere da qualsiasi installazione IIS le seguenti cartelle di default:

- `IISHelp`
- `IISAdmin`
- `Script`
- `Stampanti`

Si consiglia inoltre di utilizzare IIS Lockdown Tool 2.1, disponibile sul sito microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx).

La versione 2.1 è controllata da modelli forniti per i principali prodotti Microsoft dipendenti da IIS. Selezionare il modello maggiormente corrispondente al ruolo di questo server. In caso di dubbi, si consiglia il modello di server Web dinamico.

---

Prima di iniziare l'installazione verificare la conformità ai seguenti prerequisiti:

- Garantire l'accesso a un servizio di directory supportato (eDirectory™, Active Directory o domini di NT*). I domini di NT vengono supportati solo quando il servizio server singolo è installato su Microsoft Windows 2000 Advanced Server (SP4).
- Se la distribuzione viene eseguita con un servizio eDirectory, accertarsi che Novell Client™ sia installato sul server e sia in grado di eseguire l'autenticazione in modo corretto in eDirectory. Creare una password dell'account non modificabile da utilizzare per l'autenticazione della console di gestione (vedere Sezione 7.2.1, “Aggiunta dei servizi eDirectory”, a pagina 47).
- Per la risoluzione di nomi server da Endpoint Security Client a server singolo, verificare che i computer di destinazione in cui viene installato Endpoint Security Client siano in grado di eseguire il ping del nome server SSI. Se l'operazione non riesce, sarà necessario risolvere il problema prima di proseguire con l'installazione (cambiare il nome del server SSI in FQDN/NETBIOS, cambiare AD per utilizzare FQDN/NETBIOS, cambiare le configurazioni DNS, modificando il file host locale sui computer di destinazione per includere le informazioni MS corrette e così via.).
- Abilitare o installare i servizi IIS (Internet Information Services) di Microsoft ed eseguire la configurazione per accettare i certificati SSL (Secure Socket Layer).

  ---

  **Importante:** Non selezionare la casella di controllo *Richiedi un canale protetto (SSL)* nella pagina Comunicazioni protette (nell'utility Gestione computer di Microsoft espandere *Servizi e applicazioni* > espandere *Gestione Internet Information Services (IIS)* > espandere *Siti Web* > fare clic con il pulsante destro del mouse su *Sito Web predefinito* > fare clic su *Proprietà* > fare clic sulla scheda *Protezione directory* > fare clic sul pulsante *Modifica* nella casella di gruppo Comunicazioni protette). La selezione di questa opzione interrompe la comunicazione tra il server e il client ZENworks Endpoint Security Management sull'endpoint.

  ---

- Se si utilizzano certificati SSL propri, accertarsi che il certificato del servizio Web e la CA radice siano caricati sul computer e che il nome server convalidato nella procedura precedente (NETBIOS o FQDN) corrisponda al valore *Rilasciato a* relativo al certificato configurato in IIS.
- Se si utilizzano certificati propri o se è già stato installato il certificato firmato da se stessi di Novell, è anche possibile convalidare l'SSL verificando il seguente URL da un computer in cui è installato Endpoint Security Client: `https://NOME_SERVER_SSI/AuthenticationServer/UserService.asmx` (dove *NOME_SERVER_SSI* è il nome server). Dovrebbe restituire dati validi (una pagina html) e non avvisi di certificato. Tutti gli avvisi di certificato devono essere risolti prima dell'installazione, a meno che non si decida di utilizzare i certificati Novell firmati da se stessi.
- Assicurare l'accesso a un RDBMS supportato (Microsoft SQL Server 2000 SP4, SQL Server Standard, SQL Server Enterprise). Impostare il database sulla modalità mista.

# 3.1 Procedura di installazione

Dal menu del programma di installazione principale selezionare *Installazione su server singolo*. Questa installazione ne unisce due, ovvero quella del servizio di distribuzione norme e quella del servizio di gestione. Per ulteriori informazioni, vedere Capitolo 5, “Installazione del servizio di distribuzione norme”, a pagina 23 e Capitolo 6, “Installazione del servizio di gestione”, a pagina 31.

Come accade per le installazioni individuali, con l'impostazione *Tipica* verranno installate le impostazioni di default dei servizi e i certificati SSL Novell firmati da se stessi. L'*Installazione personalizzata* consente agli amministratori di stabilire i percorsi della directory e permette l'utilizzo di un'autorità di certificazione di proprietà dell'azienda.

## 3.2 Avvio del servizio

Il servizio combinato (distribuzione norme e gestione) si avvia immediatamente dopo l'installazione, senza che sia necessario riavviare il server. La console di gestione viene utilizzata per gestire i servizi di distribuzione norme e di gestione tramite la funzione Configurazione. Per ulteriori informazioni, consultare la *Guida dell'amministratore di ZENworks Endpoint Security Management*.

Una volta completata l'installazione, sarà possibile installare su questo server sia la console di gestione che il servizio garanzia ubicazioni client. Se si desidera installare la console di gestione su un computer separato, copiare la cartella dei file di installazione di ZENworks Endpoint Security Management nel computer della console di gestione designata per completare l'installazione.

Continuare con Capitolo 5, “Installazione del servizio di distribuzione norme”, a pagina 23.

# Installazione su più server

# 4

L'installazione su più server è consigliata per distribuzioni estese o nel caso in cui il servizio di distribuzione norme debba essere collocato all'esterno del firewall aziendale per garantire agli utenti la regolare ricezione di aggiornamenti delle norme quando si trovano fuori dal perimetro. È necessario eseguire l'installazione su più server in almeno due server distinti. Se si tenta di installare il servizio di distribuzione norme e il servizio di gestione sullo stesso server, l'installazione non riuscirà. Per ulteriori informazioni relative all'installazione su server singolo, vedere Capitolo 3, “Installazione su server singolo”, a pagina 17.

L'installazione su più server deve avere inizio con l'installazione del servizio di distribuzione norme su un server protetto, interno o esterno al firewall aziendale. Per ulteriori informazioni, consultare Capitolo 5, “Installazione del servizio di distribuzione norme”, a pagina 23.

All'installazione del servizio di distribuzione norme, deve fare seguito quella del servizio di gestione. Per ulteriori informazioni, consultare Capitolo 6, “Installazione del servizio di gestione”, a pagina 31.

Si consiglia di installare su questo server anche la console di gestione. Per ulteriori informazioni, consultare Capitolo 7, “Installazione della console di gestione”, a pagina 43.

Continuare con Capitolo 5, “Installazione del servizio di distribuzione norme”, a pagina 23.

# Installazione del servizio di distribuzione norme

# 5

Il server che ospita il servizio di distribuzione norme di ZENworks® Endpoint Security Management deve essere sempre raggiungibile dagli utenti, sia all'interno della rete che all'esterno nella DMZ. Prima dell'installazione (vedere "Requisiti di sistema" a pagina 10), accertarsi che il software necessario sia installato sul server. Dopo aver selezionato il server, annotarne il nome, sia il nome NETBIOS che FQDN (Nome di dominio completo).

Per motivi di sicurezza e di funzionalità, la distribuzione del servizio di distribuzione norme su un controller PDC (controller di dominio primario) non è supportata.

---

**Nota:** È consigliabile che il server SSI venga configurato (consolidato) in modo da disattivare tutte le applicazioni, i servizi, gli account e le altre opzioni non necessarie alla funzionalità designata del server. La procedura utilizzata dipende dalle specifiche dell'ambiente locale, pertanto non è possibile descriverla in anticipo. Si consiglia agli amministratori di consultare la sezione appropriata della pagina Web sulla sicurezza di Microsoft Technet (http://www.microsoft.com/technet/security/default.mspx). Ulteriori raccomandazioni relative al controllo dell'accesso sono disponibili nella *Guida dell'amministratore di ZENworks Endpoint Security Management*.

Per garantire un accesso protetto esclusivamente a computer attendibili, è possibile impostare la directory virtuale e IIS in modo da includere elenchi ACL. Fare riferimento agli articoli riportati di seguito:

- Granting and Denying Access to Computers (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- Restrict Site Access by IP Address or Domain Name (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- IIS FAQ: 2000 IP address and domain name restrictions (http://www.iisfaq.com/default.aspx?View=A136&P=109)
- Working With IIS Packet Filtering (http://www.15seconds.com/issue/011227.htm)

Per motivi di sicurezza, si raccomanda di rimuovere da qualsiasi installazione IIS le seguenti cartelle di default:

- `IISHelp`
- `IISAdmin`
- `Script`
- `Stampanti`

Si consiglia inoltre di utilizzare IIS Lockdown Tool 2.1, disponibile sul sito microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx).

La versione 2.1 è controllata da modelli forniti per i principali prodotti Microsoft dipendenti da IIS. Selezionare il modello maggiormente corrispondente al ruolo di questo server. In caso di dubbi, si consiglia il modello di server Web dinamico.

---

Verificare i prerequisiti riportati di seguito prima di iniziare l'installazione:

- Garantire la risoluzione dei nomi server dal servizio di gestione (MS) al servizio di distribuzione norme (DS): accertarsi che il computer di destinazione in cui viene installato MS sia in grado di eseguire il "ping" del nome server DS (NETBIOS se il servizio di distribuzione è configurato nel firewall di rete, FQDN se invece è installato all'esterno, nella DMZ).
- Se l'operazione riesce, questo sarà il nome server da immettere durante l'installazione. Se l'operazione non riesce, sarà necessario risolvere il problema prima di proseguire con l'installazione.
- Assicurarsi che avvenga la risoluzione dei nomi server da Endpoint Security Client a DS: verificare che i client degli endpoint (in cui è installato Endpoint Security Client) siano in grado di eseguire il ping dello stesso nome server DS utilizzato in precedenza. Se l'operazione non riesce, sarà necessario risolvere il problema prima di proseguire con l'installazione.
- Abilitare o installare i servizi IIS (Internet Information Services) di Microsoft, accertarsi che ASP.NET sia abilitato e configurarlo per accettare i certificati SSL (Secure Socket Layer).

  ---

  **Importante:** Non selezionare la casella di controllo *Richiedi un canale protetto (SSL)* nella pagina Comunicazioni protette (nell'utility Gestione computer Microsoft espandere *Servizi e applicazioni* > espandere *Gestione Internet Information Services (IIS)* > espandere *Siti Web* > fare clic con il pulsante destro del mouse su *Sito Web predefinito* > fare clic su *Proprietà* > fare clic sulla scheda *Protezione directory* > fare clic sul pulsante *Modifica* nella casella di gruppo Comunicazioni protette). La selezione di questa opzione interrompe la comunicazione tra il server e il client ZENworks Endpoint Security Management sull'endpoint.

  ---

- Se si utilizzano certificati SSL propri, accertarsi che il certificato del servizio Web sia caricato sul computer e che il nome server convalidato nella procedura precedente (NETBIOS o FQDN) corrisponda al valore *Rilasciato a* relativo al certificato configurato in IIS.
- Se vengono utilizzati certificati SSL propri, convalidare l'SSL dal server MS al server DS: aprire un browser Web sul servizio di gestione e immettere il seguente URL: `https://NOMEDS` (dove *NOMEDS* è il nome server del DS). Questa operazione dovrebbe restituire dati validi e non avvisi di certificati (ad esempio, "Pagina in costruzione" può essere considerato valido). Tutti gli avvisi di certificato devono essere risolti prima dell'installazione, a meno che non si decida di utilizzare i certificati Novell firmati da se stessi.
- Assicurare l'accesso a un RDBMS supportato (Microsoft SQL Server 2000 SP4, SQL Server Standard, SQL Server Enterprise e SQL Server 2005). Impostare il database sulla modalità mista. Questo database deve essere ospitato sul server del servizio gestione oppure su un server condiviso posizionato dietro il firewall aziendale.

# 5.1 Procedura di installazione

Fare clic su *Installazione servizio di distribuzione norme* dal menu Interfaccia di installazione. Ha inizio l'installazione del servizio di distribuzione norme.

All'avvio, il programma di installazione verifica che tutto il software necessario sia presente sul server. Eventuali componenti mancanti vengono installati automaticamente prima che l'installazione prosegua fino alla schermata iniziale (potrebbe essere necessario accettare contratti di licenza per software aggiuntivo). Se i componenti MDAC (Microsoft Data Access Components) 2.8 non sono installati, sarà necessario installarli e riavviare il server prima di proseguire con l'installazione di ZENworks Endpoint Security Management. Se si utilizza Windows 2003 Server, ASP.NET 2.0 verrà configurato per essere eseguito dal programma di installazione.

Una volta iniziata l'installazione del servizio di distribuzione norme, eseguire la seguente procedura:

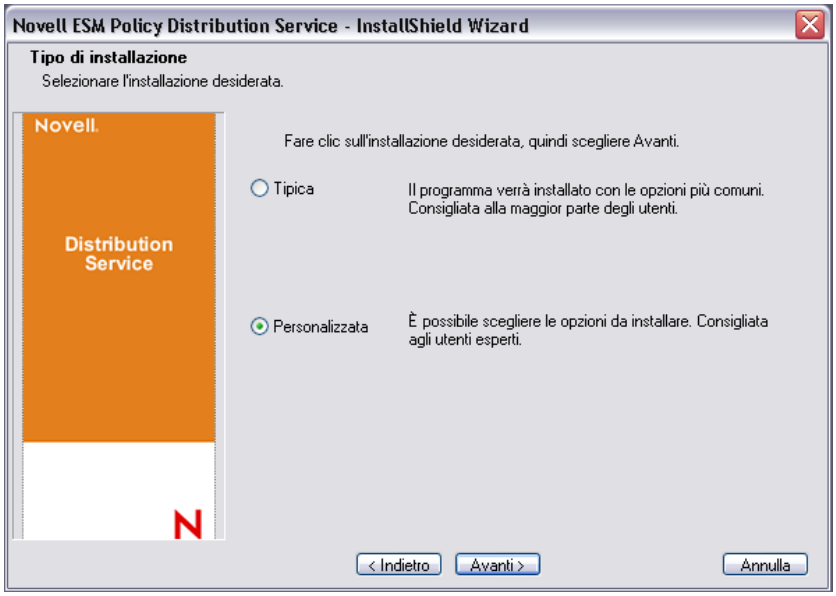
---

**Nota:** la procedura riportata di seguito indica quali operazioni dovranno essere eseguite dall'amministratore per completare il processo di installazione. I processi interni vengono visualizzati durante tutta l'installazione e non sono qui documentati, a meno che non si tratti di azioni o informazioni specifiche utili per la riuscita dell'installazione.

---

1. Fare clic su *Avanti* nella schermata iniziale per continuare.
2. Accettare il contratto di licenza, quindi fare clic su *Avanti*.
3. Selezionare l'installazione *Tipica* o quella *Personalizzata*.

***Figura 5-1*** *Selezione dell'installazione tipica o personalizzata*




Di seguito vengono presentati entrambi i percorsi di installazione:

- Sezione 5.1.1, “Installazione tipica”, a pagina 25
- Sezione 5.1.2, “Installazione personalizzata”, a pagina 27

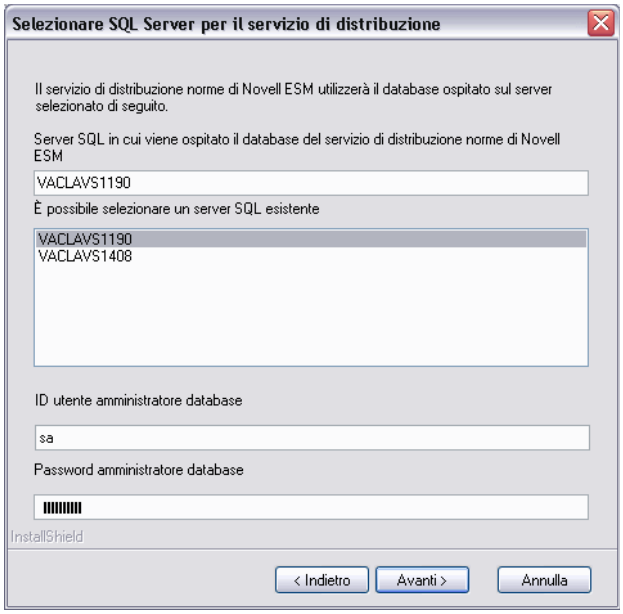
## 5.1.1 Installazione tipica

Con l'installazione tipica i file del software del servizio di distribuzione norme vengono collocati nella directory di default: `\Programmi\Novell\ESM Policy Distribution Service`. Il nome del database SQL assegnato è STDSDB. I tre file del database SQL (dati, indice e log) sono ubicati in: `\Programmi\Microsoft SQL Server\mssql\Data`.

1. I certificati SSL di Novell vengono creati per l'installazione. Se si desidera utilizzare certificati SSL propri, eseguire Installazione personalizzata. Questi certificati devono essere distribuiti a tutti gli utenti.
2. Il programma di installazione rileva i database SQL disponibili su computer e rete. Selezionare un database SQL protetto per il servizio di distribuzione norme e immettere il nome e la password dell'amministratore del database (se la password non contiene caratteri, il programma

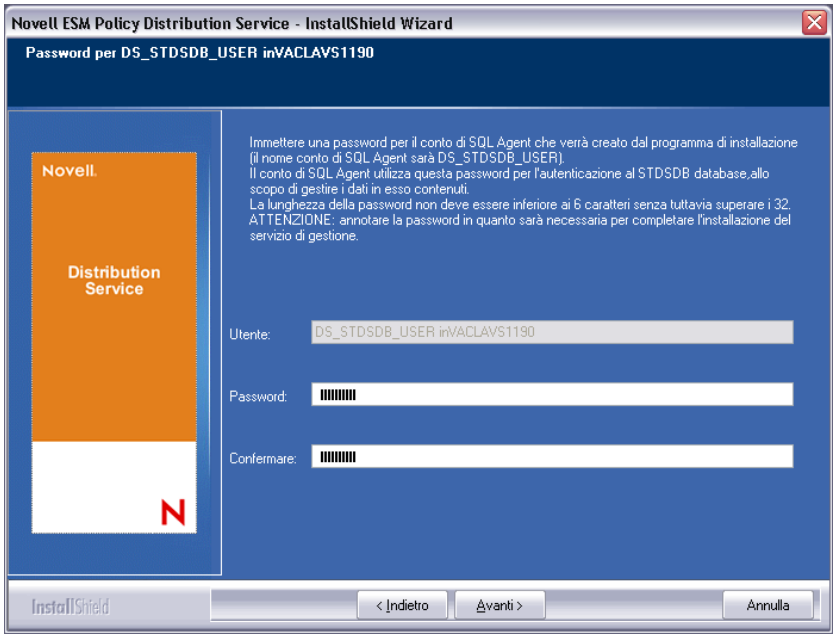
di installazione avviserà del potenziale problema di sicurezza). Il nome utente e la password non possono essere di un utente del dominio ma devono essere di un utente SQL con diritti SysAdmin.

***Figura 5-2*** *Selezione di SQL Server*



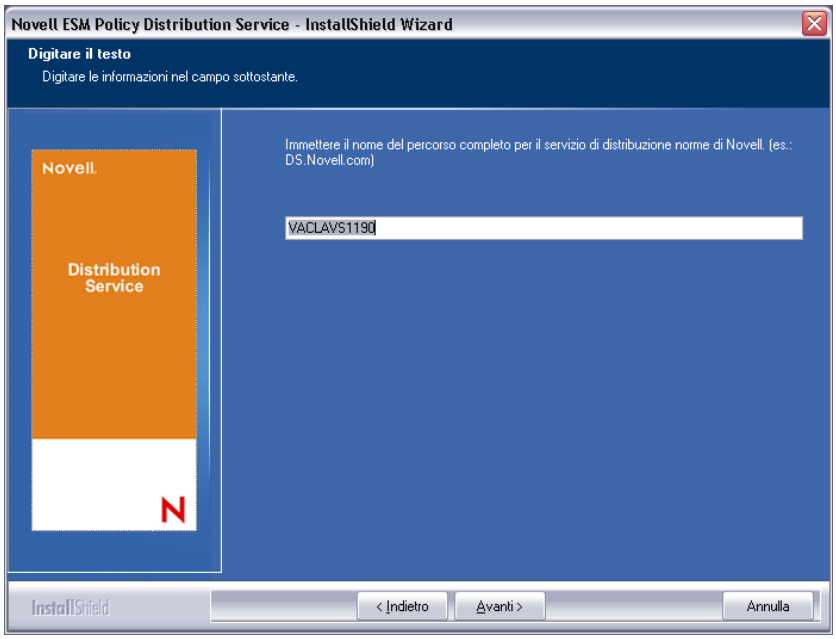

3 Specificare la password per l'agente del servizio di distribuzione norme. Si tratta del nome utente e della password che vengono utilizzati dal servizio per eseguire il login al relativo database SQL.

***Figura 5-3*** *Password SQL del servizio di distribuzione*



4 Specificare il nome di dominio del servizio di distribuzione norme. Se il server risiede all'esterno del firewall aziendale, dovrà essere un nome di dominio completo. Diversamente, è richiesto solo il nome NETBIOS per il server.

***Figura 5-4*** *Immettere il nome di dominio del servizio di distribuzione norme*




5 Nella schermata Copia file, fare clic su *Avanti* per iniziare l'installazione.

6 Nella directory di installazione viene generata una cartella `File di installazione ESM`. Tale cartella contiene un file `ID installazione` e un file `ESM-DS.cer (` (certificato SSL firmato da se stessi di Novell) richiesti dal servizio di gestione. Copiare questo file direttamente sul computer designato come host per il servizio di gestione, tramite condivisione di rete oppure salvandolo su disco o su unità USB e caricandolo manualmente sulla directory di installazione del server.

7 Il servizio di distribuzione norme risulta ora installato. Fare clic su *Fine* per chiudere il programma di installazione e avviare il monitoraggio delle prestazioni.

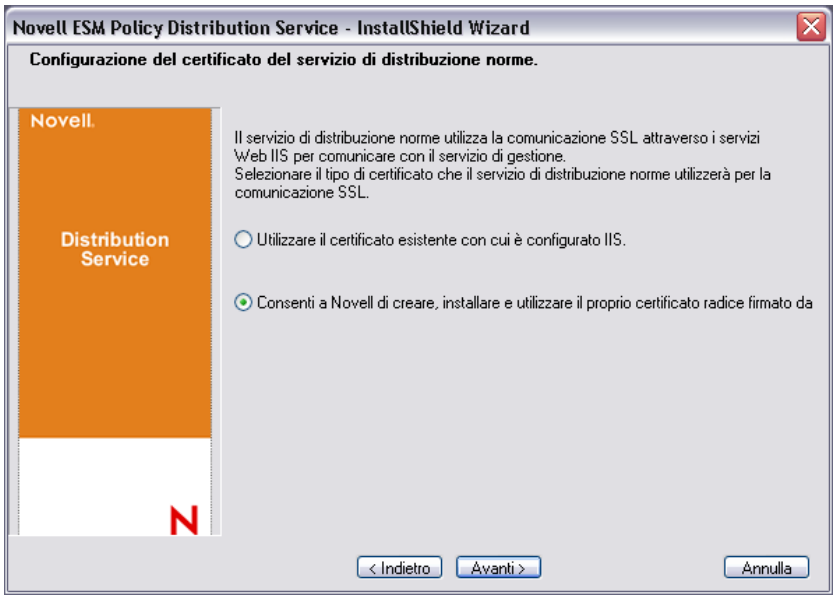
## 5.1.2 Installazione personalizzata

Con l'installazione personalizzata vengono visualizzate le impostazioni di default utilizzate nell'installazione tipica e all'amministratore è consentito specificare o selezionare una directory diversa per posizionare i file del software.

L'amministratore può selezionare o installare un certificato SSL Novell firmato da se stessi oppure usarne uno proprio.

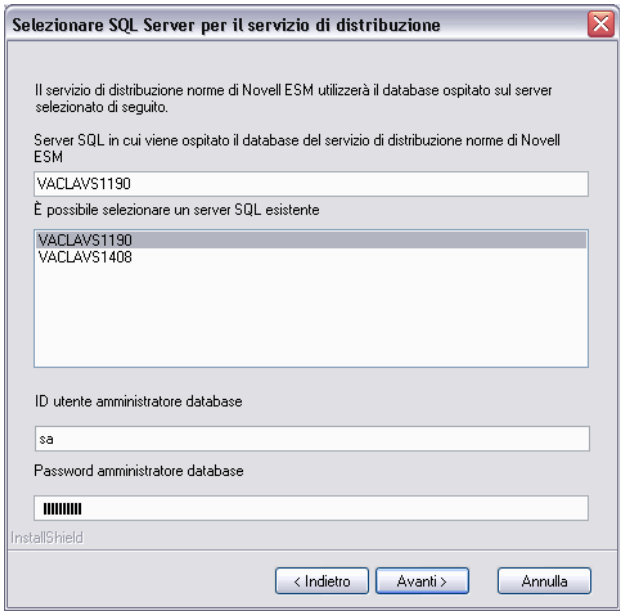
1 Il certificato SSL è necessario per una comunicazione protetta tra il servizio di distribuzione norme e il servizio di gestione, nonché tra il DS e tutti i client di sicurezza di Novell. Se si dispone già di un'autorità di certificazione, fare clic su *Utilizza il certificato esistente per il quale è configurato IIS*. Se invece occorre un certificato, fare clic su *Consenti a Novell di creare, installare e utilizzare il proprio certificato radice firmato da se stessi*. Il programma di installazione crea i certificati e l'autorità di firma. Indipendentemente dal tipo, questi certificati devono essere distribuiti a tutti gli utenti.

***Figura 5-5*** *Impostazione della radice di fiducia*




**2** Il programma di installazione rileva i database SQL disponibili su computer e rete. Selezionare il database SQL protetto per il servizio di distribuzione norme, quindi immettere il nome e la password dell'amministratore del database (se la password non contiene caratteri, il programma di installazione avvisa del potenziale problema di sicurezza). Il nome utente e la password non possono essere di un utente del dominio ma devono essere di un utente SQL con diritti SysAdmin.

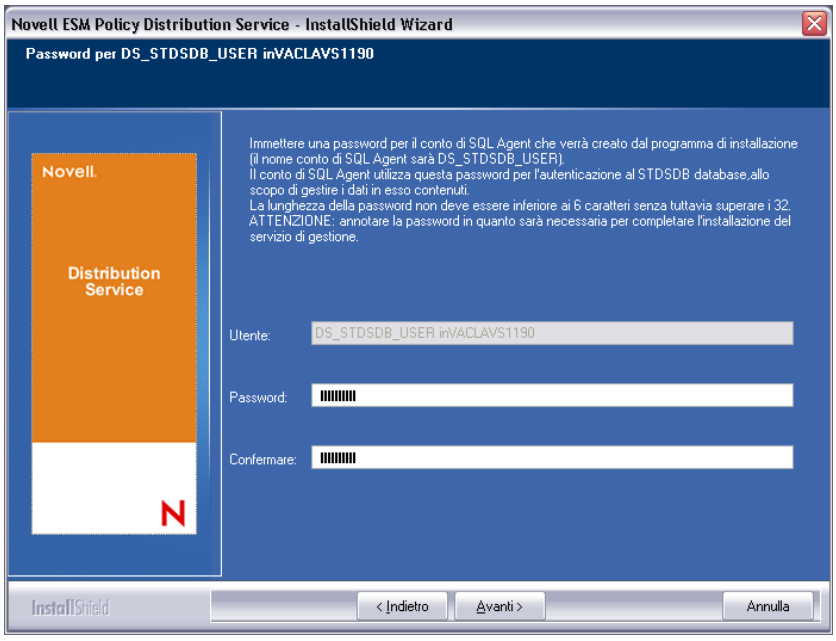
***Figura 5-6*** *Selezione di SQL Server*




**3** Impostare il nome del database (il nome di default è STDSDB).

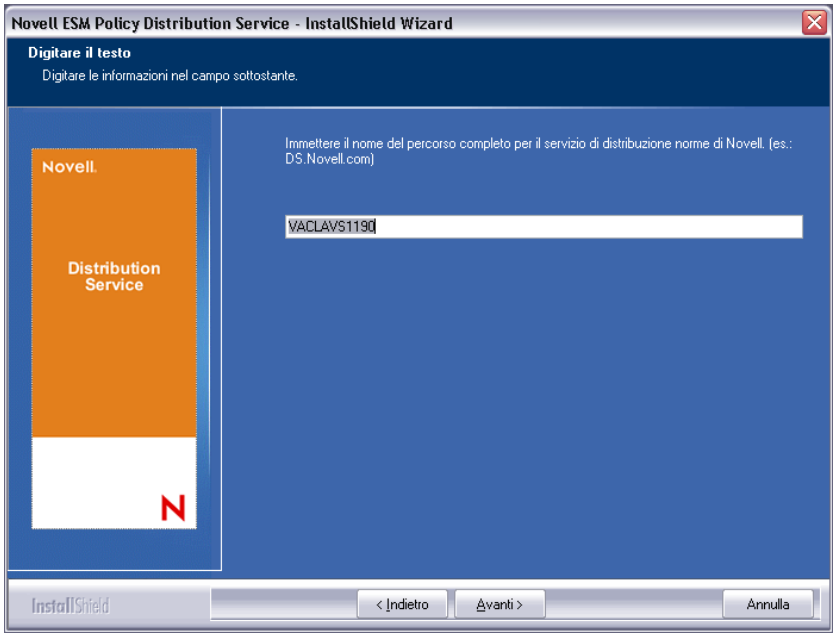
4 Specificare la password per l'agente del servizio di distribuzione norme. Si tratta del nome utente e della password che vengono utilizzati dal servizio per eseguire il login al relativo database SQL.

***Figura 5-7*** *Password SQL del servizio di distribuzione*




5 Specificare il nome di dominio del servizio di distribuzione norme. Se il server risiede all'esterno del firewall aziendale, dovrà essere un nome di dominio completo. Diversamente, è richiesto solo il nome NETBIOS per il server.

***Figura 5-8*** *Immettere il nome di dominio del servizio di distribuzione norme*




6 Nella schermata Copia file, fare clic su *Avanti* per iniziare l'installazione.

7 Specificare i percorsi file per dati, indice e file di log.

8 Nella directory di installazione viene generata una cartella `File di installazione ESM`. Tale cartella contiene un file `ID installazione` e un file `ESM-DS.cer` (certificato SSL firmato da se stessi di Novell, se selezionato) richiesti dal servizio di gestione. Utilizzare Sfoglia per designare la posizione in cui deve essere salvato il file sul server (impostazione di default = directory di installazione).

***Figura 5-9*** *Salvataggio dei file di installazione*


9 Se si sceglie di utilizzare un certificato SSL aziendale, posizionare una copia di questo file nella cartella `File di installazione ESM`.

10 Copiare l'intero contenuto della cartella `File di installazione ESM` direttamente sul computer designato come host per il servizio di gestione, tramite condivisione di rete oppure salvando i file su disco o su un'unità USB e caricandoli manualmente nella directory di installazione del server.

11 Il servizio di distribuzione norme risulta ora installato. Fare clic su *Fine* per chiudere il programma di installazione e avviare il monitoraggio delle prestazioni.

## 5.2 Avvio del servizio

Il servizio di distribuzione norme viene avviato immediatamente dopo l'installazione, senza che sia necessario riavviare il server. Lo strumento Configurazione della console di gestione consente di regolare i tempi di caricamento del servizio di distribuzione. Per ulteriori informazioni, consultare la *Guida dell'amministratore di ZENworks Endpoint Security Management*.

Continuare con Capitolo 6, “Installazione del servizio di gestione”, a pagina 31.

# Installazione del servizio di gestione

6

Il servizio di gestione deve essere installato su un server protetto dietro un firewall e non può condividere lo stesso server del servizio di distribuzione norme (fatta eccezione per l'installazione su server singolo, vedere Capitolo 3, “Installazione su server singolo”, a pagina 17). Per motivi di sicurezza, il servizio di gestione non deve essere installato all'esterno del firewall di rete. Dopo aver selezionato il server, annotarne il nome, ovvero i nomi NETBIOS e FQDN (Nome di dominio completo). La distribuzione del servizio di gestione su un PDC (controller di dominio primario) non è supportata sia per motivi di sicurezza che di funzionalità.

---

**Nota:** È consigliabile che il server SSI venga configurato (consolidato) in modo da disattivare tutte le applicazioni, i servizi, gli account e le altre opzioni non necessarie alla funzionalità designata del server. La procedura utilizzata dipende dalle specifiche dell'ambiente locale, pertanto non è possibile descriverla in anticipo. Si consiglia agli amministratori di consultare la sezione appropriata della pagina Web sulla sicurezza di Microsoft Technet (http://www.microsoft.com/technet/security/default.mspx). Ulteriori raccomandazioni relative al controllo dell'accesso sono disponibili nella *Guida dell'amministratore di ZENworks Endpoint Security Management*.

Per garantire un accesso protetto esclusivamente a computer attendibili, è possibile impostare la directory virtuale e IIS in modo da includere elenchi ACL. Fare riferimento agli articoli riportati di seguito:

- Granting and Denying Access to Computers (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- Restrict Site Access by IP Address or Domain Name (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- IIS FAQ: 2000 IP address and domain name restrictions (http://www.iisfaq.com/default.aspx?View=A136&P=109)
- Working With IIS Packet Filtering (http://www.15seconds.com/issue/011227.htm)

Per motivi di sicurezza, si raccomanda di rimuovere da qualsiasi installazione IIS le seguenti cartelle di default:

- `IISHelp`
- `IISAdmin`
- `Script`
- `Stampanti`

Si consiglia inoltre di utilizzare IIS Lockdown Tool 2.1, disponibile sul sito microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx).

La versione 2.1 è controllata da modelli forniti per i principali prodotti Microsoft dipendenti da IIS. Selezionare il modello maggiormente corrispondente al ruolo di questo server. In caso di dubbi, si consiglia il modello di server Web dinamico.

---

Prima di iniziare l'installazione verificare la conformità ai seguenti prerequisiti:

- Garantire l'accesso a un servizio di directory supportato (eDirectory, Active Directory o domini di NT*). *= Supportato solo quando il servizio di gestione è installato su Microsoft Windows 2000 Advanced Server (SP4).
- Se la distribuzione viene eseguita con un servizio eDirectory™, accertarsi che Novell Client™ sia installato sul server e sia in grado di eseguire l'autenticazione in modo corretto in eDirectory. Creare una password dell'account non modificabile da utilizzare per l'autenticazione della console di gestione (vedere Sezione 7.2.1, “Aggiunta dei servizi eDirectory”, a pagina 47).
- Assicurarsi che avvenga la risoluzione di nomi server da Endpoint Security Client a MS: verificare che i computer di destinazione (in cui è installato Endpoint Security Client) siano in grado di eseguire il ping del nome server MS. Se l'operazione riesce, questo è il valore immesso durante l'installazione. Se l'operazione non riesce, sarà necessario risolvere il problema prima di proseguire con l'installazione
- Abilitare o installare IIS (Microsoft Internet Information Services), assicurarsi che ASP.NET sia abilitato e configurarlo per accettare i certificati SSL (Secure Socket Layer).

  ---

  **Importante:** Non selezionare la casella di controllo *Richiedi un canale protetto (SSL)* nella pagina Comunicazioni protette (nell'utility Gestione computer di Microsoft espandere *Servizi e applicazioni* > espandere *Gestione Internet Information Services (IIS)* > espandere *Siti Web* > fare clic con il pulsante destro del mouse su *Sito Web predefinito* > fare clic su *Proprietà* > fare clic sulla scheda *Protezione directory* > fare clic sul pulsante *Modifica* nella casella di gruppo Comunicazioni protette). La selezione di questa opzione interrompe la comunicazione tra il server e il client ZENworks Endpoint Security Management sull'endpoint.

  ---

- Se si utilizzano certificati SSL propri, accertarsi che la CA radice sia caricata sul computer e che il nome server convalidato nella procedura precedente (NETBIOS o FQDN) corrisponda al valore *Rilasciato a* relativo al certificato configurato in IIS.
- Se si utilizzano certificati propri o se è già stato installato il certificato firmato da se stessi di Novell, è anche possibile convalidare l'SSL verificando il seguente URL da un computer in cui è installato Endpoint Security Client: `https://NOME_SERVER_MS/AuthenticationServer/UserService.asmx` (dove *NOME_SERVER_MS* è il nome server). Dovrebbe restituire dati validi (una pagina html) e non avvisi di certificato. Prima dell'installazione devono essere risolti tutti gli avvisi di certificato.
- Assicurare l'accesso a un RDBMS supportato (Microsoft SQL Server 2000 SP4, SQL Server Standard, SQL Server Enterprise, SQL 2005). Impostare il database sulla modalità mista.
- Copiare la directory `File di installazione ESM`, contenente l'ID di installazione del servizio di distribuzione norme e il certificato SSL radice per tale servizio, all'interno della directory di installazione di questo server.

# 6.1 Procedura di installazione

Fare clic su *Installazione del servizio di gestione* dal menu Interfaccia di installazione. Ha inizio l'installazione del servizio di gestione.

All'avvio, il programma di installazione verifica che tutto il software necessario sia presente sul server. Eventuali componenti mancanti vengono installati automaticamente prima che l'installazione prosegua fino alla schermata iniziale (potrebbe essere necessario accettare contratti di licenza per software aggiuntivo). Se i componenti MDAC (Microsoft Data Access Components) 2.8 non sono

installati, sarà necessario installarli e riavviare il server prima di proseguire con l'installazione di ZENworks Endpoint Security Management. Se si utilizza Windows 2003 Server, ASP.NET 2.0 deve essere configurato per essere eseguito dal programma di installazione.

Una volta iniziata l'installazione del servizio di gestione, eseguire la seguente procedura:

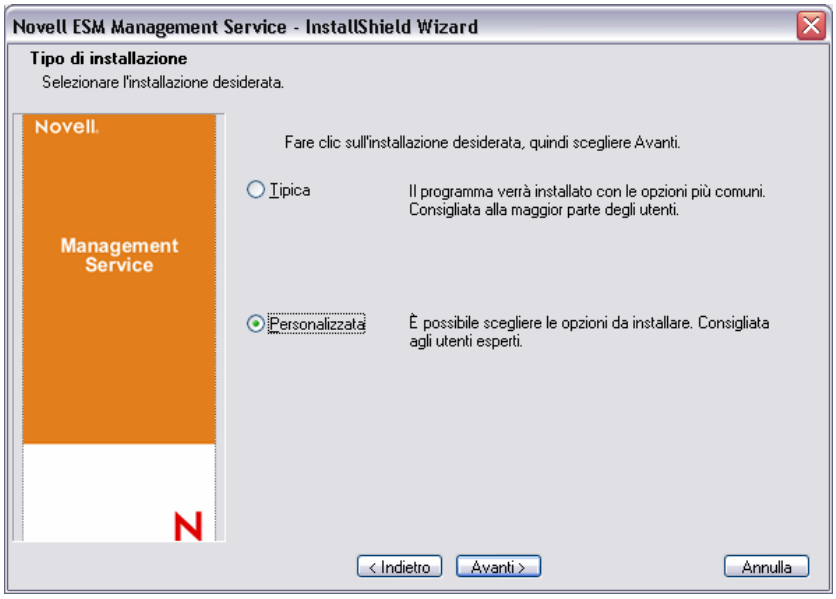
---

**Nota:** la procedura riportata di seguito indica quali operazioni dovranno essere eseguite dall'amministratore per completare il processo di installazione. I processi interni vengono visualizzati durante tutta l'installazione e non sono qui documentati, a meno che non si tratti di azioni o informazioni specifiche utili per la riuscita dell'installazione.

---

1. Fare clic su *Avanti* nella schermata iniziale per continuare.
2. Accettare il contratto di licenza, quindi fare clic su *Avanti*.
3. Selezionare l'installazione *Tipica* o quella *Personalizzata*.

***Figura 6-1*** *Selezionare l'installazione Tipica o Personalizzata*




Di seguito vengono presentati entrambi i percorsi di installazione:

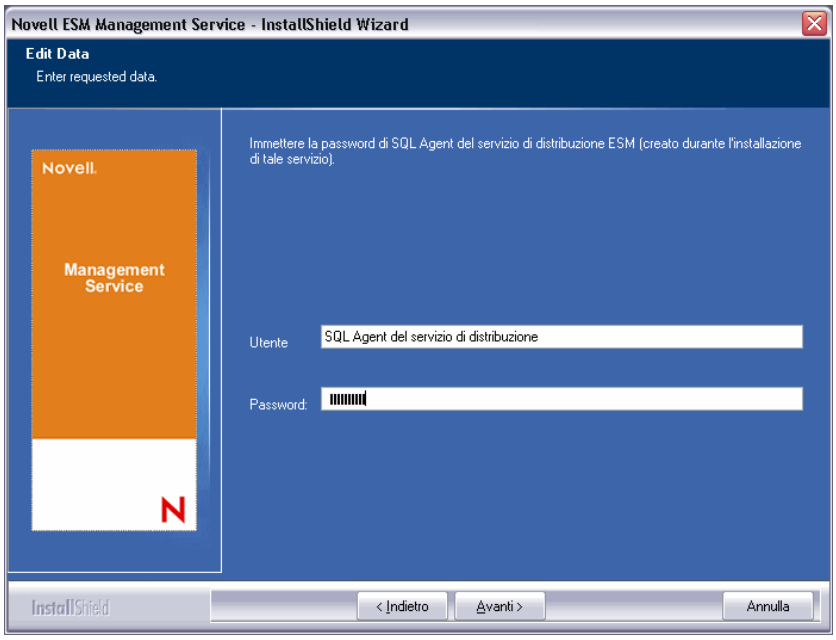
- Sezione 6.1.1, “Installazione tipica”, a pagina 33
- Sezione 6.1.2, “Installazione personalizzata”, a pagina 37

## 6.1.1 Installazione tipica

Con l'installazione tipica i file del software del servizio di gestione vengono collocati nella directory di default: `\Programmi\Novell\ESM Management Service`. Il nome del database SQL assegnato è STDSDB. I tre file del database SQL (dati, indice e log) sono ubicati in: `\Programmi\Microsoft SQL Server\mssql\Data`.

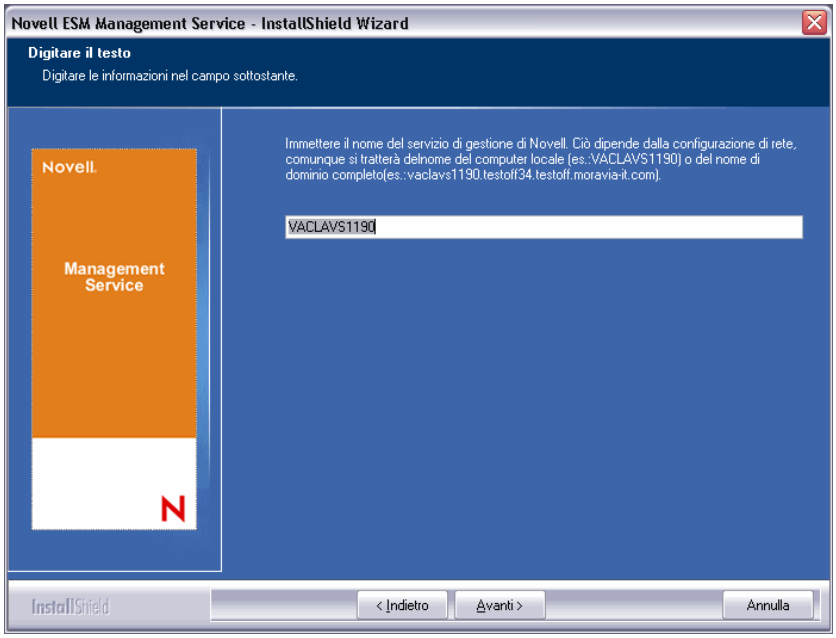
1. Specificare la password dell'agente del servizio di distribuzione norme, creata durante l'installazione di tale servizio.

***Figura 6-2*** *Immettere la password SQL*




**2** Specificare il nome del server che ospita il servizio di gestione.

***Figura 6-3*** *Immettere il nome del server MS*




**3** I certificati SSL di Novell vengono creati per l'installazione. Se si desidera utilizzare certificati SSL propri, eseguire una Installazione personalizzata. Questi certificati devono essere distribuiti a tutti gli utenti.

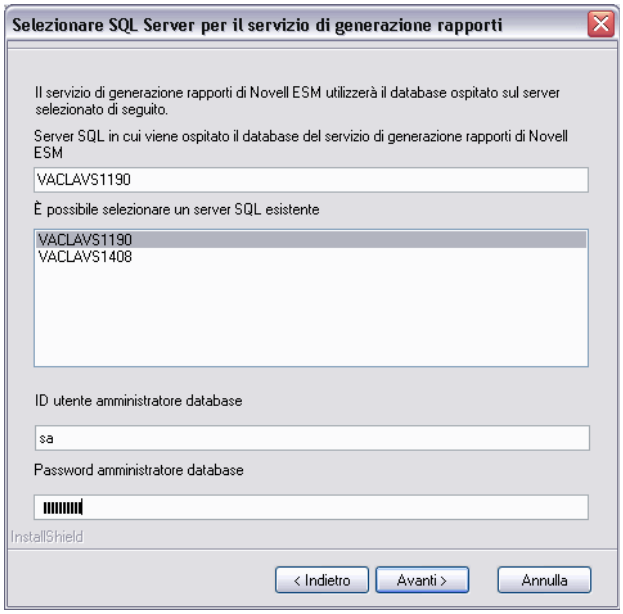
**4** Il programma di installazione rileva i database SQL disponibili su computer e rete. Selezionare il database SQL per il servizio di gestione e specificare il nome e la password dell'amministratore del database (se la password non contiene caratteri, il programma di

installazione avvisa del potenziale problema di sicurezza). Il nome utente e la password non possono essere di un utente del dominio ma devono essere di un utente SQL con diritti SysAdmin.

***Figura 6-4*** *Selezionare il database SQL MS*

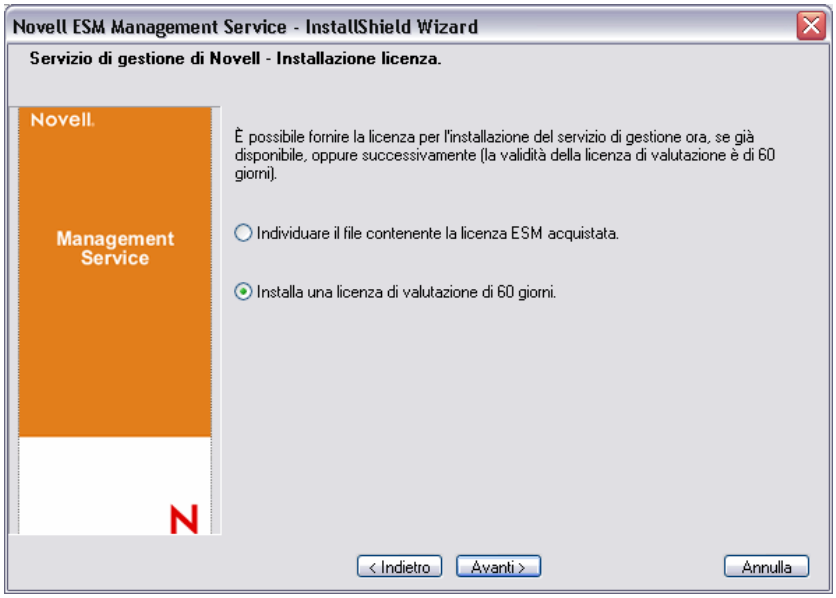

5 Selezionare il database SQL per il servizio di generazione rapporti e specificare la password dell'amministratore del database relativa a quel database. Se si desidera acquisire e memorizzare un numero elevato di rapporti, è consigliabile che il database del servizio di generazione rapporti sia dotato di un server SQL proprio.

***Figura 6-5*** *Selezionare il database del servizio di generazione rapporti*



6 Se ZENworks Endpoint Security Management è già stato acquistato, verrà fornito un file di licenza separato. Copiare il file di licenza su questo server e individuarlo (per ulteriori dettagli vedere la pagina delle istruzioni inclusa nel file di licenza). Se non è stata ancora acquistata una licenza di ZENworks Endpoint Security Management, selezionare *Licenza di valutazione di 60 giorni* per continuare.

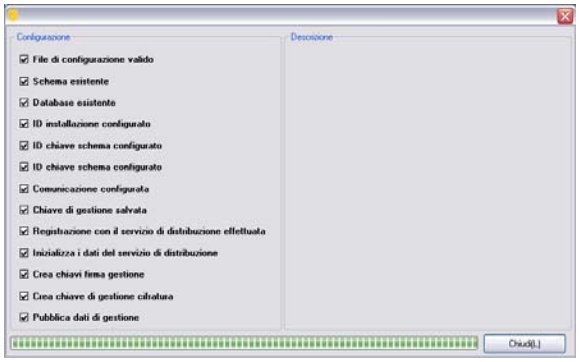
***Figura 6-6*** *Ricerca del file di licenza Novell*




7 Nella schermata Copia file, fare clic su *Avanti* per iniziare l'installazione.

8 Il servizio di gestione esegue un controllo della comunicazione su entrambi i database SQL e sul servizio di distribuzione norme. Se non è possibile verificare la comunicazione, il programma di installazione notifica il problema all'utente. Affinché l'installazione riesca è necessario selezionare tutte le caselle.

***Figura 6-7*** *Verifica della comunicazione*




9 Se per l'installazione viene utilizzato il servizio eDirectory, ignorare i passaggi Passo 10 e Passo 11.

10 Se l'installazione viene eseguita su un server membro di un dominio che include un servizio Active Directory o un servizio di directory dei domini di NT, il programma rileva e aggiunge automaticamente nell'installazione i seguenti dati, utilizzando una connessione protetta e di sola lettura:

- Nome dominio radice o nome computer
- Nome dell'amministratore del dominio o account risorsa con autorizzazioni di lettura appropriate

11 Specificare la password dell'amministratore nello spazio fornito e fare clic su *Test per verificare la connessione da stabilire*. Se il test riesce, fare clic su *Salva*. Se invece non riesce oppure il dominio corretto non viene rilevato, sarà necessario aggiungerla manualmente utilizzando la console di gestione (vedere Sezione 7.2.1, “Aggiunta dei servizi eDirectory”, a pagina 47).

---

**Nota:** la password immessa non deve avere alcuna scadenza e l'account non deve mai essere disabilitato.

---

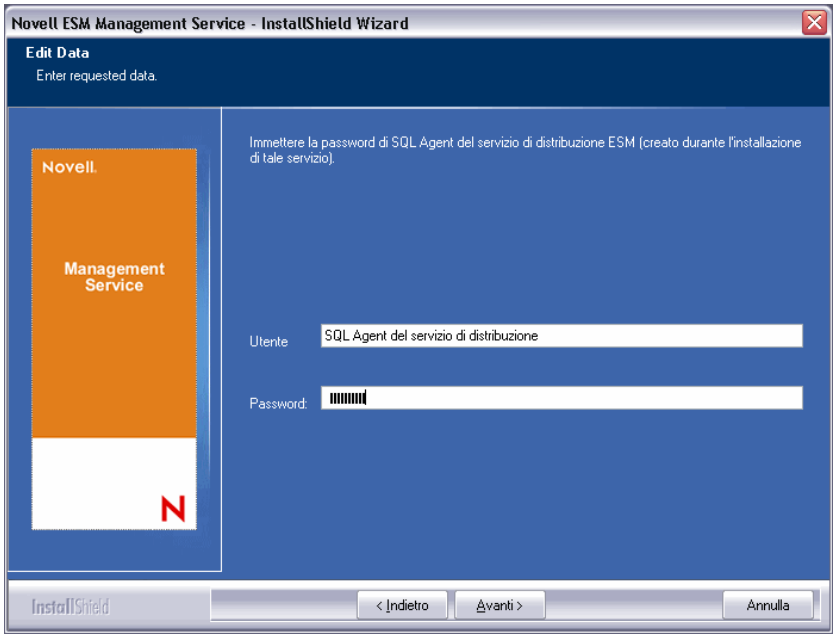
12 Il servizio di gestione è ora installato, fare clic su *Chiudi* per chiudere le verifiche di comunicazione, quindi su *Fine* per chiudere il programma di installazione.

## 6.1.2 Installazione personalizzata

Con l'installazione personalizzata vengono visualizzate le impostazioni di default utilizzate nell'installazione tipica e all'amministratore è consentito specificare o selezionare un'ubicazione diversa.

1 Specificare la password dell'agente del servizio di distribuzione norme, creata durante l'installazione di tale servizio.

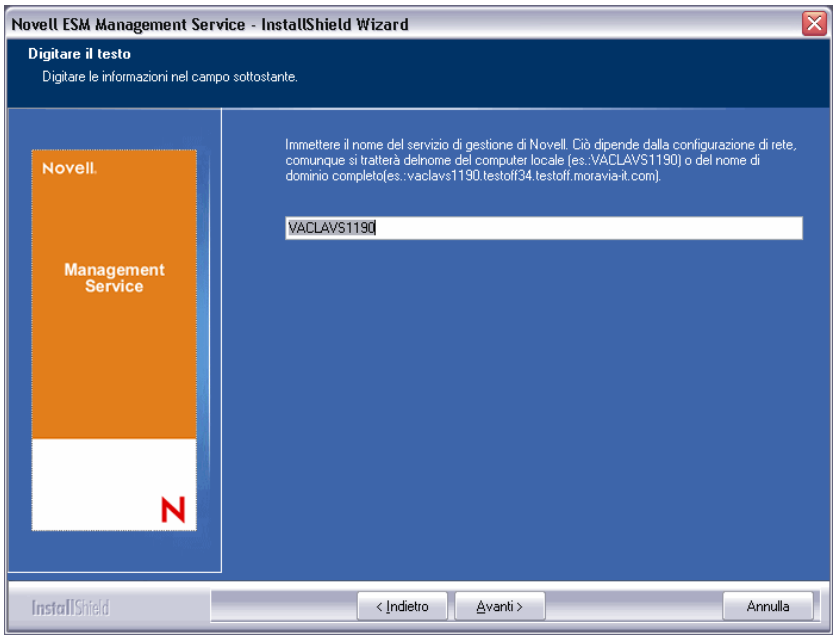
***Figura 6-8*** *Immettere la password SQL*



2 Selezionare il tipo di certificato SSL utilizzato per l'installazione del servizio di distribuzione norme. Se è stata utilizzata l'autorità di certificazione (aziendale) esistente, fare clic su *Il servizio di distribuzione di Novell ha utilizzato un certificato con cui IIS era già configurato*. Se il programma di installazione del servizio di distribuzione ha creato un certificato Novell, fare clic su *Il servizio di distribuzione di Novell ha installato un proprio certificato radice firmato da se stessi*.

3 Specificare il nome del server che ospita il servizio di gestione.

***Figura 6-9*** *Immettere il nome del server MS*

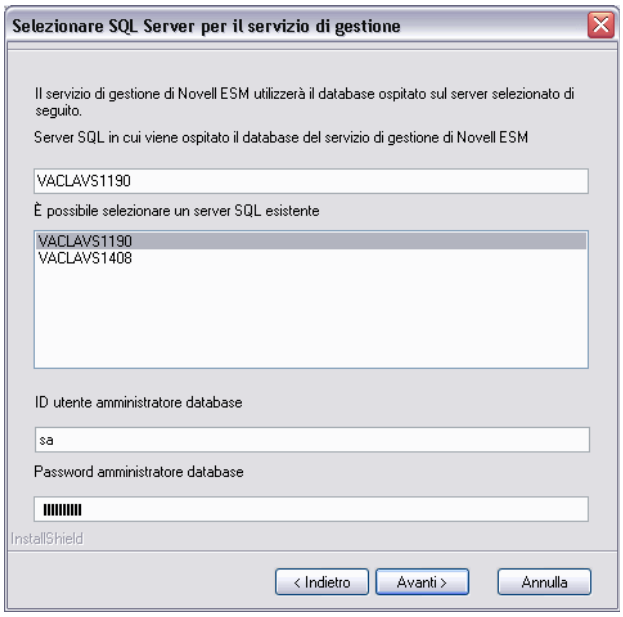



4 Per una comunicazione protetta tra il servizio di gestione e tutti i client Endpoint Security Client è necessario un certificato SSL. Se si dispone già di un'autorità di certificazione, fare clic su *Utilizza il certificato esistente per il quale è configurato IIS*. Se invece occorre un certificato, fare clic su *Consenti a Novell di creare, installare e utilizzare il proprio certificato radice firmato da se stessi*. Il programma di installazione crea i certificati e l'autorità di firma. Indipendentemente dal tipo, questi certificati devono essere distribuiti a tutti gli utenti.

5 Quando vengono selezionati certificati Novell, selezionare l'ubicazione in cui è possibile salvare il certificato per semplificare la distribuzione (l'impostazione di default è la directory di installazione).

6 Il programma di installazione rileva i database SQL disponibili su computer e rete. Selezionare il database SQL per il servizio di gestione e specificare il nome e la password dell'amministratore del database (se la password non contiene caratteri, il programma di installazione avvisa del potenziale problema di sicurezza). Il nome utente e la password non possono essere di un utente del dominio ma devono essere di un utente SQL con diritti SysAdmin.

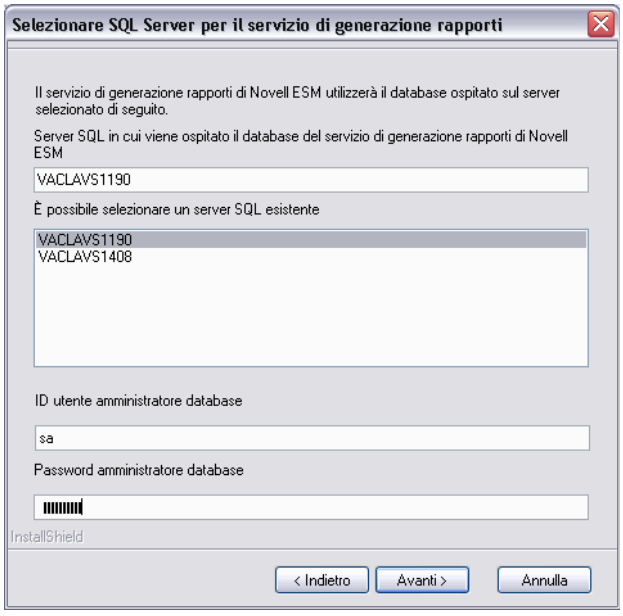
***Figura 6-10*** *Selezionare il database SQL MS*




**7** Impostare il nome del database (quello di default è STDSDB).

**8** Selezionare il database SQL per il servizio di generazione rapporti e specificare la password dell'amministratore del database relativa a quel database.

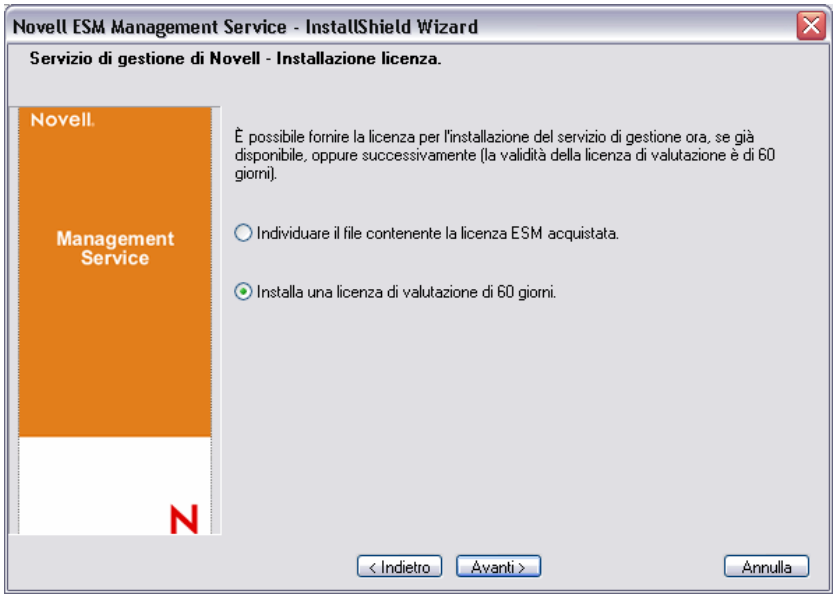
***Figura 6-11*** *Selezionare il database del servizio di generazione rapporti*




**9** Impostare il nome del database (quello di default è STDSDB)

10 Se ZENworks Endpoint Security Management è già stato acquistato, verrà fornito un file di licenza separato. Copiare il file di licenza su questo server e individuarlo (per ulteriori dettagli vedere la pagina delle istruzioni inclusa nel file di licenza). Se non è stata ancora acquistata una licenza di ZENworks Endpoint Security Management, selezionare *Licenza di valutazione di 60 giorni* per continuare.

***Figura 6-12*** *Ricerca del file di licenza Novell*



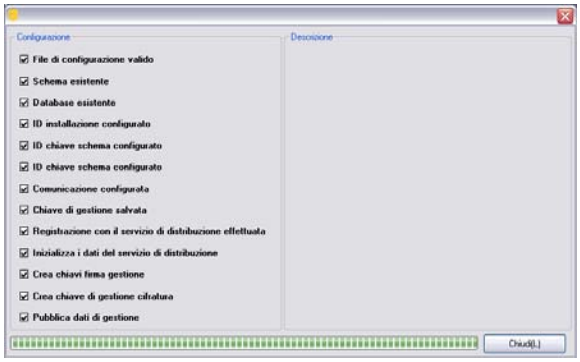

11 Nella schermata Copia file, fare clic su *Avanti* per iniziare l'installazione.

12 Selezionare i percorsi file per dati, indice e file di log del database del servizio di gestione.

13 Selezionare i percorsi file per dati, indice e file di log del database del servizio di generazione rapporti.

14 Il servizio di gestione esegue una verifica della comunicazione su entrambi i database SQL e sul servizio di distribuzione norme. Se non è possibile verificare la comunicazione, il programma di installazione notifica il problema all'utente. Affinché l'installazione riesca è necessario selezionare tutte le caselle.

***Figura 6-13*** *Verifica della comunicazione*




15 Se per l'installazione viene utilizzato il servizio eDirectory, ignorare i passaggi Passo 16 e Passo 17.

16 Se l'installazione viene eseguita su un server membro di un dominio che include un servizio Active Directory o un servizio di directory dei domini di NT, il programma rileva e aggiunge automaticamente nell'installazione i seguenti dati, utilizzando una connessione protetta e di sola lettura:

- Nome dominio radice o nome computer
- Nome dell'amministratore del dominio o account risorsa con autorizzazioni di lettura appropriate

17 Specificare la password dell'amministratore nello spazio fornito e fare clic su *Test per verificare la connessione da stabilire*. Se il test riesce, fare clic su *Salva*. Se invece non riesce oppure il dominio corretto non viene rilevato, sarà necessario aggiungerla manualmente utilizzando la console di gestione (vedere Sezione 7.2.1, “Aggiunta dei servizi eDirectory”, a pagina 47).

---

**Nota:** la password specificata non deve avere alcuna scadenza e l'account non deve mai essere disabilitato.

---

18 Il servizio di gestione è ora installato, fare clic su *Chiudi* per chiudere le verifiche di comunicazione, quindi su *Fine* per chiudere il programma di installazione.

## 6.2 Avvio del servizio

Il servizio di gestione viene avviato immediatamente dopo l'installazione, senza che sia necessario riavviare il server. La console di gestione viene utilizzata per gestire i dati relativi al servizio di gestione (vedere la *Guida dell'amministratore di ZENworks Endpoint Security Management*).

Novell consiglia di installare la console di gestione su questo server. Se si installa la console di gestione su un computer separato, copiare la directory `File di installazione ESM`, mediante condivisione di rete o salvando il file su disco o su unità USB, nel computer che ospita la console di gestione.

Continuare con Capitolo 7, “Installazione della console di gestione”, a pagina 43.

# Installazione della console di gestione

# 7

La console di gestione può essere installata sul server del servizio di gestione o su un PC protetto che disponga di comunicazione diretta con il server del servizio di gestione. È possibile configurare più console di gestione per comunicare con un solo servizio di gestione, tuttavia, è consigliabile limitare l'accesso alla console di gestione a utenti selezionati.

Per motivi di sicurezza, si consiglia di installare la console di gestione direttamente sul server del servizio di gestione.

Se si desidera installare la console di gestione su una workstation separata, prima di iniziare l'installazione, accertarsi che esistano i seguenti prerequisiti:

- Accertarsi che il dispositivo su cui si desidera installare la console di gestione soddisfi i requisiti riportati di seguito:
  - Windows XP SP1, Windows XP SP2 o Windows 2000 SP4.
  - Si consiglia un processore a 1,0 GHz con un minimo di 256 MB di RAM e 100 MB di spazio disponibile su disco.
- Copiare sul PC la cartella `File di installazione ESM` contenente i certificati SSL radice per il servizio di distribuzione norme e il servizio di gestione, unitamente al file `STInstParam.id`.
- Se la console di gestione viene installata sul server del servizio di gestione, verificare che la versione di Microsoft Internet Explorer sia 5.5 o successiva.

## 7.1 Procedura di installazione

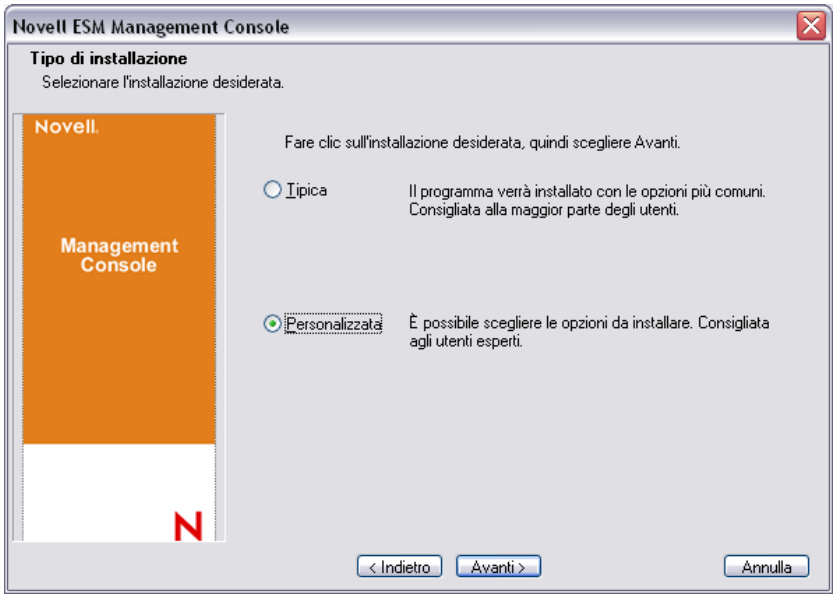
Fare clic su *Installazione della console di gestione* dal menu dell'interfaccia di installazione.

All'avvio, il programma di installazione verifica se sul computer sono presenti sia .NET Framework 3.5 che WSE 2.0 SP2, entrambi richiesti. Se uno o entrambi risultano assenti, verranno installati automaticamente prima che l'installazione prosegua nella schermata iniziale (sarà necessario accettare il contratto di licenza per .NET 3.5).

Per installare la console di gestione:

1. Fare clic su *Avanti* per continuare.
2. Accettare il contratto di licenza, quindi fare clic su *Avanti*.
3. Selezionare l'installazione *Tipica* o quella *Personalizzata*.

***Figura 7-1*** *Selezionare l'installazione Tipica o Personalizzata*




Di seguito vengono presentati entrambi i percorsi di installazione:

- Sezione 7.1.1, “Installazione tipica”, a pagina 44
- Sezione 7.1.2, “Installazione personalizzata”, a pagina 44

## 7.1.1 Installazione tipica

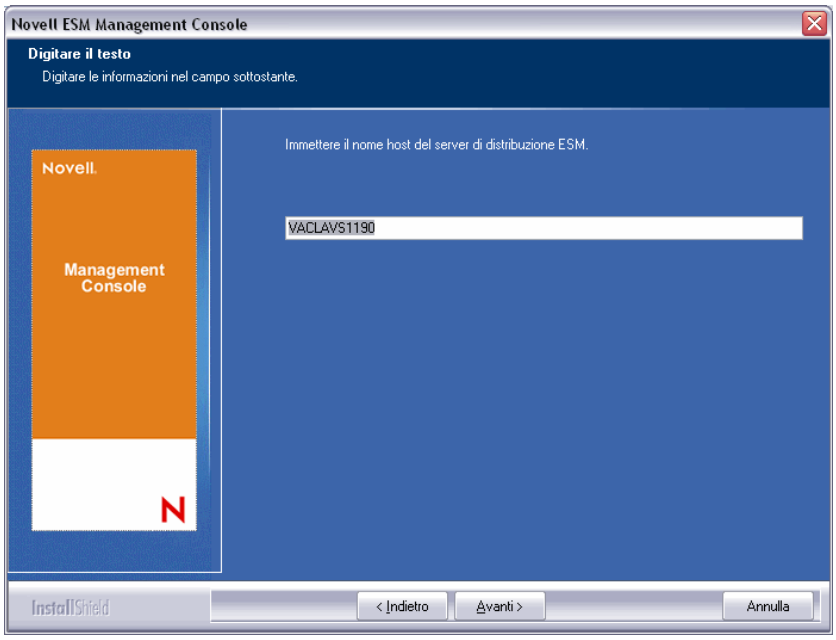
L'installazione tipica prevede l'utilizzo di tutte le informazioni su SSL e sul server di default contenute nel file `STInstParam.id` e utilizza la directory di default:`\Programmi\Novell\ESM Management Console`. Non è necessario eseguire alcuna selezione aggiuntiva per l'installazione della console di gestione, purché la directory `File di installazione ESM` si trovi sul computer.

## 7.1.2 Installazione personalizzata

L'installazione personalizzata consente di visualizzare le impostazioni di default `STInstParam.id` utilizzate nell'installazione tipica e permette all'amministratore di modificare tali informazioni.

1 Specificare il nome host del servizio di distribuzione norme (dovrà essere il nome di dominio completo se il server di distribuzione viene distribuito all'esterno del firewall aziendale).

***Figura 7-2*** *Immettere il nome host del servizio di distribuzione*

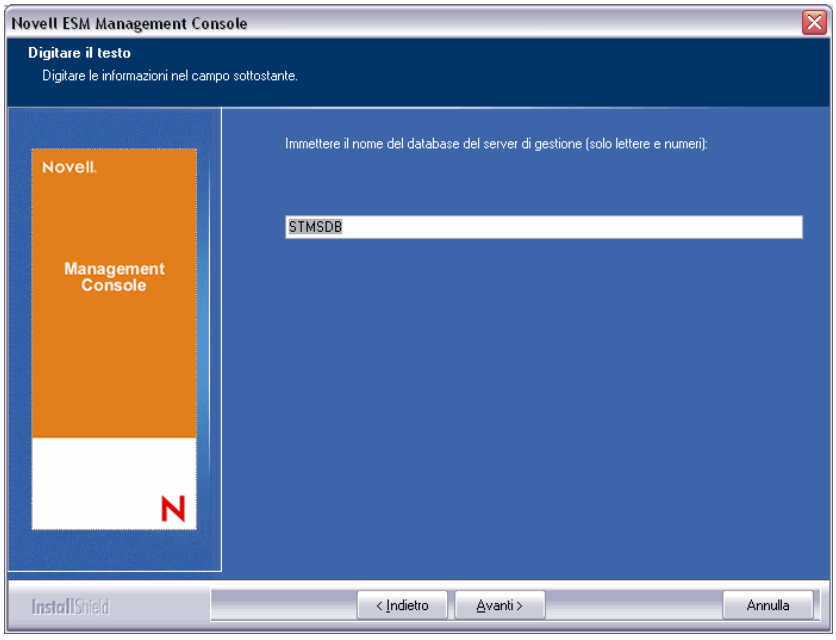



2 Specificare il nome host del servizio di gestione.

3 Specificare il nome host del database SQL del servizio di gestione.

4 Specificare il nome del database SQL del servizio di gestione.

***Figura 7-3*** *Immettere il nome del database SQL MS*




5 Specificare il nome utente e la password SA SQL identificati durante l'installazione del servizio di gestione.

6 Selezionare il tipo di certificato SSL installato sul servizio di distribuzione norme e sul servizio di gestione.

***Figura 7-4*** *Selezione dei certificati del server*


7 Selezionare la directory in cui è installata la console di gestione. L'ubicazione di default è `\Programmi\Novell\ESM Management Console`.

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 configurazione guidata del nuovo servizio di directory consente di creare la configurazione di un servizio di directory che definisce l'ambito delle installazioni di Endpoint Security Client. 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.

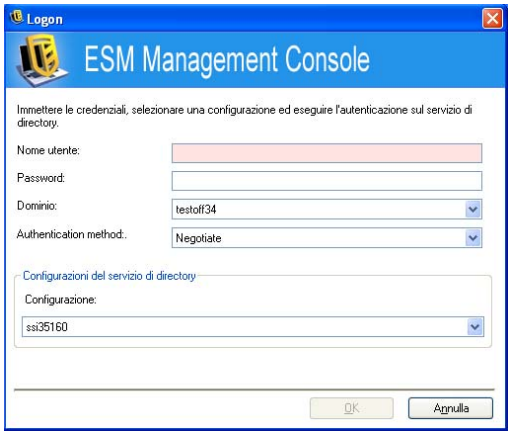
Al termine dell'installazione di ZENworks Endpoint Security Management, viene automaticamente visualizzata la Procedura guidata per la configurazione di un nuovo servizio directory. Per ulteriori informazioni sulla creazione e sulla configurazione del servizio di directory, consultare "Configurazione del servizio di directory" nella *Guida dell'amministratore di ZENworks Endpoint Security Management*.

# 7.2 Avvio della console

Per avviare la finestra di login della console di gestione, fare clic su *Start* > *Tutti i programmi* > *Novell* > *Console di gestione ESM* > *Console di gestione*.

Eseguire il login alla console di gestione immettendo il nome e la password dell'amministratore. Prima di poter immettere il nome utente e la password, è necessario essere connessi al dominio del servizio di directory (vedere Sezione 7.2.1, "Aggiunta dei servizi eDirectory", a pagina 47). Il nome utente deve essere di un utente del dominio del servizio di gestione.

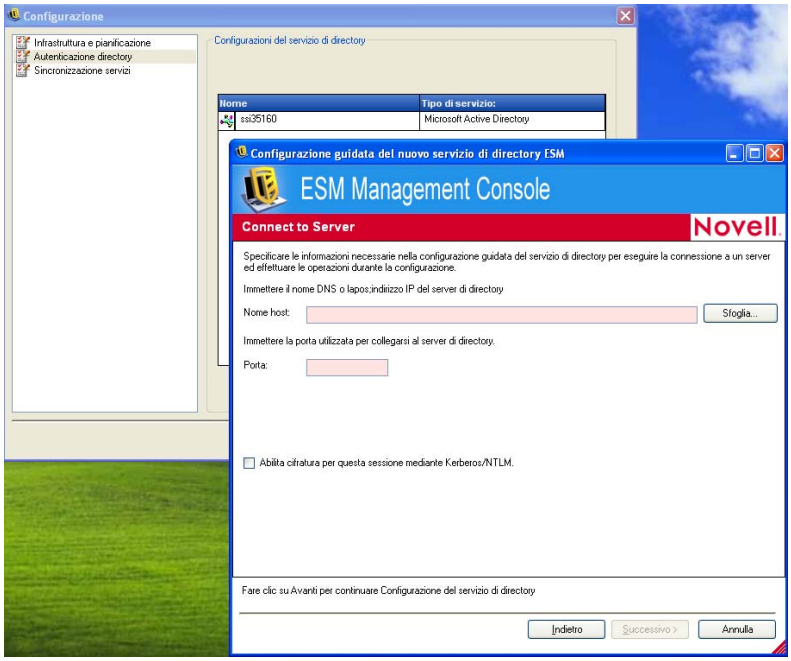
***Figura 7-5*** *Eseguire il login alla console di gestione di ZENworks Endpoint Security Management*




## 7.2.1 Aggiunta dei servizi eDirectory

**1** Fare clic sul pulsante *Opzioni* sulla schermata di login per visualizzare la finestra Configurazione.

***Figura 7-6*** *Autenticazione directory*




**2** Immettere un nome breve per il servizio di directory e selezionare eDirectory dall'elenco a discesa *Tipo di servizio*.

**3** Nel campo *Nome server host/dominio*, specificare l'indirizzo IP del server eDirectory e il nome dell'albero in *Dominio/Albero*.

**4** Selezionare *Disponibile per autenticazione utente* per visualizzare il dominio nel menu a discesa di login.

**5** Deselezionare *Autenticazione protetta* in *Opzioni connessioni servizio*.

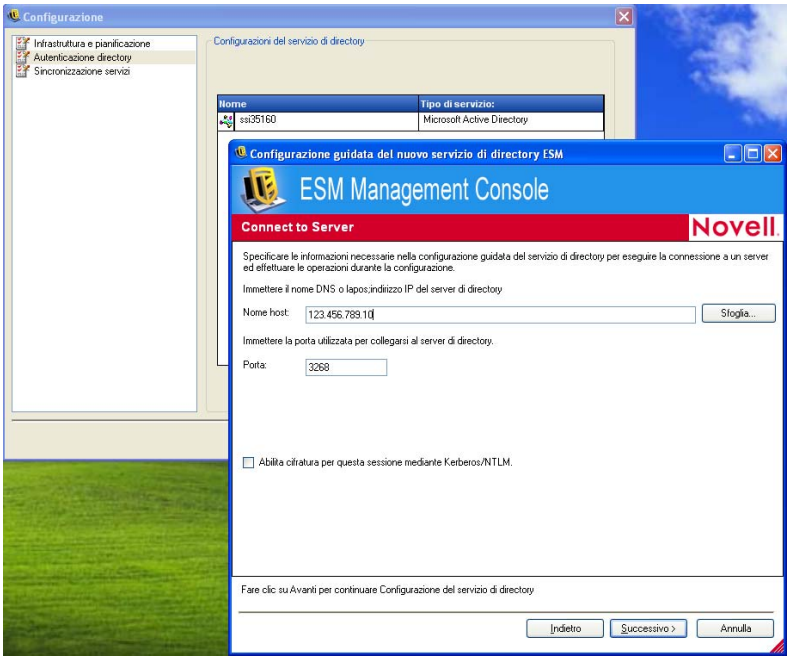
6 Specificare il nome dell'account utilizzando il formato LDAP. Ad esempio in "cn=admin,o=acmeserver" "cn" è l'utente mentre "o" è l'oggetto in cui viene memorizzato l'account utente.

7 Specificare la password dell'account.

**Nota:** la password non deve avere alcuna scadenza e l'account non deve mai essere disabilitato.

8 Fare clic su *Test* per verificare la comunicazione al servizio di directory. Se non è possibile stabilire una comunicazione, l'utente viene notificato dell'errore. Eventuali informazioni inesatte verranno corrette, se possibile, dall'interfaccia durante il test.

***Figura 7-7*** *Schermata directory completata*




9 Fare clic su *Salva* per aggiungere questo servizio di directory al database, quindi scegliere *Nuovo* per includervi un ulteriore servizio.

10 Fare clic su *OK* o su *Annulla* per uscire dalla finestra Configurazione e ritornare alla schermata di login.

Consultare la *Guida dell'amministratore di ZENworks Endpoint Security Management* per informazioni sulla configurazione dell'ascolto per i servizi di directory aggiuntivi, tra cui Active Directory e i servizi dei domini di NT.

## 7.2.2 Configurazione di Impostazioni autorizzazioni della console di gestione

*Autorizzazioni* è incluso nel menu *Strumenti* della console di gestione e consente l'accesso solo all'amministratore principale del servizio di gestione e ad eventuali altri utenti autorizzati da tale amministratore. Questo controllo non è disponibile quando viene eseguita la console di gestione autonoma. Per ulteriori dettagli vedere Capitolo 11, “Installazione non gestita di ZENworks Endpoint Security Management”, a pagina 79.

Le impostazioni delle autorizzazioni definiscono l'utente o il gruppo di utenti autorizzato ad accedere alla console di gestione, pubblicare norme e modificare le impostazioni suddette.

Durante l'installazione del server di gestione, nel modulo di configurazione viene immesso il nome dell'account di un amministratore o di una risorsa. Dopo aver superato il test e salvato le informazioni dell'utente, a quest'ultimo vengono automaticamente concesse le autorizzazioni.

Una volta installata la console di gestione, a tutti i gruppi di utenti interni al dominio vengono concesse autorizzazioni complete. È necessario che l'utente della risorsa rimuova le autorizzazioni per tutti i gruppi, ad eccezione dei gruppi e degli utenti che devono accedere. L'utente risorsa può impostare autorizzazioni aggiuntive per gli utenti designati. Di seguito vengono illustrate le caratteristiche delle autorizzazioni concesse.

- **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, né disporre delle opzioni di pubblicazione e di autorizzazione.
- **Pubblica norme:** l'utente può pubblicare norme solo per utenti e gruppi assegnati.
- **Modifica autorizzazione:** 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, è consigliabile che solo all'utente risorsa o a un numero limitato di amministratori venga concesso di modificare autorizzazioni e cancellare norme.

---

Le seguenti sezioni contengono informazioni aggiuntive:

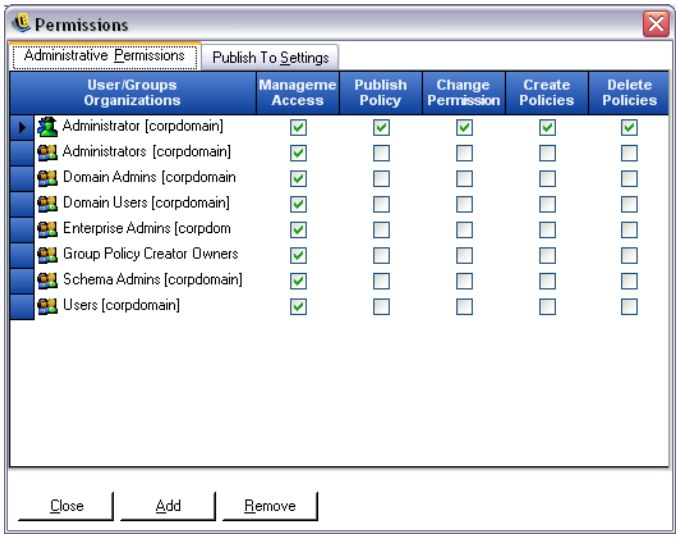

- “Configurazione di Autorizzazioni amministrative” a pagina 49
- “Configurazione di Impostazioni destinatari pubblicazione” a pagina 51


### Configurazione di Autorizzazioni amministrative

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

Vengono visualizzati i gruppi associati a questo dominio.

***Figura 7-8*** *Finestra delle impostazioni relative alle autorizzazioni della console di gestione*




---

**Nota:** Per default, a tutti i gruppi vengono concesse autorizzazioni complete nella console di gestione. Gli amministratori devono immediatamente deselezionare dai gruppi non autorizzati tutti i task relativi alle norme. È possibile rimuovere l'accesso alla console deselezionando la relativa autorizzazione.

---

**2** (Facoltativo) Per caricare utenti e nuovi gruppi in questo elenco:

**2a** Per visualizzare la Tabella organizzazione, fare clic sul pulsante *Aggiungi* nella parte inferiore della schermata.

***Figura 7-9*** *Impostazioni autorizzazioni - Tabella organizzazione.*

**2b** Selezionare gli utenti e i gruppi appropriati dall'elenco. Per selezionare più utenti, utilizzare i tasti Ctrl o Maiusc.

**2c** Quando tutti gli utenti e i gruppi sono stati selezionati, fare clic su*OK* per aggiungerli alla griglia del modulo Autorizzazioni.

**3** Assegnare autorizzazioni a utenti e gruppi disponibili.

Per rimuovere un utente o un gruppo selezionato, selezionarne il nome, quindi fare clic su *Rimuovi*.

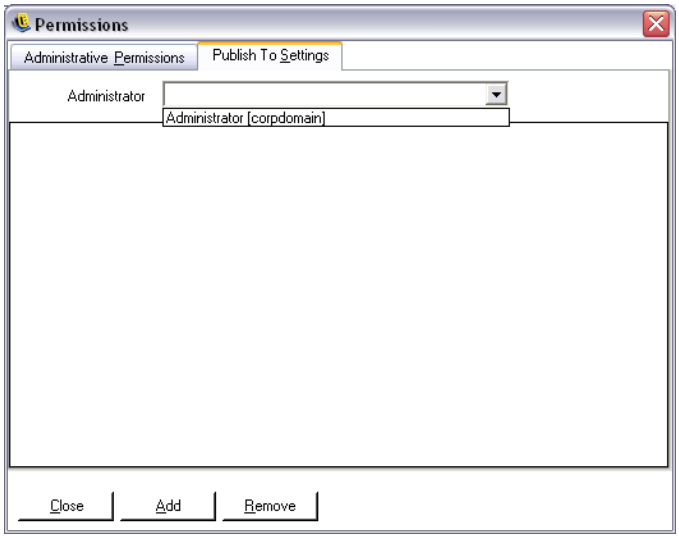
### Configurazione di Impostazioni destinatari pubblicazione

A utenti e gruppi che hanno *Pubblica norme* selezionato devono essere assegnati utenti o gruppi destinatari della pubblicazione. Per impostare Impostazioni destinatari pubblicazione:

**1** Fare clic sulla scheda *Impostazioni destinatari pubblicazione*.

**2** Dall'elenco a discesa, selezionare utenti e gruppi cui è stata concessa l'autorizzazione di pubblicazione.

***Figura 7-10*** *Impostazioni destinatari pubblicazione*



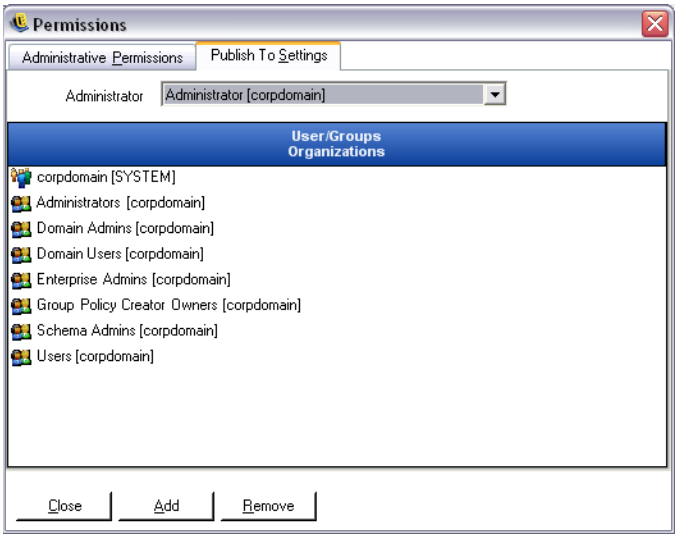

**3** Per assegnare utenti e gruppi a questo utente o gruppo:

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

**3b** Selezionare gli utenti e i gruppi appropriati dall'elenco. Per selezionare più utenti, utilizzare i tasti Ctrl e Maiusc.

**3c** Una volta selezionati tutti gli utenti/gruppi, fare clic sul pulsante *OK*.

***Figura 7-11*** *Elenco destinatari pubblicazione*




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

Poiché i set di autorizzazioni vengono immediatamente implementati, è sufficiente che l'amministratore faccia clic su *Chiudi* e accetti le modifiche per ritornare all'editor.

Quando si aggiunge un nuovo servizio di directory, all'account risorsa vengono concesse autorizzazioni complete, come descritto in precedenza.

## 7.2.3 Pubblicazione di norme

Per pubblicare norme di sicurezza con impostazioni di default:

1. Fare clic su *Crea nuove norme*.
2. Specificare un nome per le norme, quindi fare clic su *Crea*.
3. Salvare le norme e fare clic sulla scheda *Pubblica*.
4. Dal momento che gli utenti di Endpoint Security Client devono effettuare la restituzione per la visualizzazione nell'albero, selezionare la parte superiore dell'albero sulla sinistra, quindi fare doppio clic per popolare il campo di pubblicazione con tutti i gruppi e gli utenti correnti.
5. Fare clic su *Pubblica* per inviare le norme al servizio di distribuzione norme.

Le norme generate in questo modo presentano le seguenti caratteristiche:

- Creazione di un'unica ubicazione (Sconosciuto)
- Unità CD/DVD ROM consentite.
- Dispositivi di memorizzazione estraibili consentiti.
- Tutte le porte di comunicazione (Wi-Fi inclusa) consentite.
- Impostazione firewall, Tutte adattive (è consentito tutto il traffico in uscita sulle porte di rete mentre non è consentito il traffico in ingresso non richiesto sulle stesse porte) inclusa.

Per informazioni sulla creazione di norme di sicurezza più affidabili, consultare la *Guida dell'amministratore di ZENworks Endpoint Security Management*.

Continuare con Capitolo 8, “Installazione del servizio garanzia ubicazioni client”, a pagina 55.

## 7.3 Installazione del lettore USB

Il lettore USB di Novell è incluso nel pacchetto di installazione, utile all'amministratore per la creazione di elenchi di dispositivi USB consentiti.

Per installare il lettore:

1. Fare clic su *Installazione* per avviare il processo di installazione
2. Nella schermata iniziale, fare clic su *Avanti* per continuare.
3. Accettare la licenza, quindi fare clic su *Avanti*.
4. Nella schermata di informazioni per il cliente, specificare il nome utente appropriato e le informazioni sull'organizzazione, quindi scegliere se tutti gli utenti del computer potranno accedere a questo software oppure solo l'utente specificato.
5. Fare clic su *Installa*.
6. Fare clic su *Fine*.

Per ulteriori informazioni sull'utilizzo del lettore USB, consultare la *Guida dell'amministratore di Endpoint Security Management*.

# Installazione del servizio garanzia ubicazioni client

8

Gli utenti dovrebbero poter accedere a questo server solo quando entrano in un ambiente di rete controllato, per avere la certezza di trovarsi effettivamente nell'ambiente identificato da ZENworks® Security Client. Di seguito sono riportate istruzioni sulle configurazioni per failover e ridondanze. Se lo si desidera, è possibile distribuire il servizio garanzia ubicazioni client (CLAS) nello stesso server che ospita l'installazione del servizio di gestione su server singolo o su più server.

Installare il servizio CLAS su un server rilevabile dai punti finali solo in un ambiente di rete che richieda verifica crittografica.

La distribuzione del servizio CLAS su un PDC (controller di dominio primario) non è supportata sia per motivi di sicurezza che di funzionalità.

---

**Nota:** È consigliabile che il server SSI venga configurato (consolidato) in modo da disattivare tutte le applicazioni, i servizi, gli account e le altre opzioni non necessarie alla funzionalità designata del server. La procedura utilizzata dipende dalle specifiche dell'ambiente locale, pertanto non è possibile descriverla in anticipo. Si consiglia agli amministratori di consultare la sezione appropriata della pagina Web sulla sicurezza di Microsoft Technet (http://www.microsoft.com/technet/security/default.mspx). Ulteriori raccomandazioni relative al controllo dell'accesso sono disponibili nella *Guida dell'amministratore di ZENworks Endpoint Security Management*.

Per garantire un accesso protetto esclusivamente a computer attendibili, è possibile impostare la directory virtuale e IIS in modo da includere elenchi ACL. Fare riferimento agli articoli riportati di seguito:

- Granting and Denying Access to Computers (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- Restrict Site Access by IP Address or Domain Name (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- IIS FAQ: 2000 IP address and domain name restrictions (http://www.iisfaq.com/default.aspx?View=A136&P=109)
- Working With IIS Packet Filtering (http://www.15seconds.com/issue/011227.htm)

Per motivi di sicurezza, si raccomanda di rimuovere da qualsiasi installazione IIS le seguenti cartelle di default:

- `IISHelp`
- `IISAdmin`
- `Script`
- `Stampanti`

Si consiglia inoltre di utilizzare IIS Lockdown Tool 2.1, disponibile sul sito microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx).

La versione 2.1 è controllata da modelli forniti per i principali prodotti Microsoft dipendenti da IIS. Selezionare il modello maggiormente corrispondente al ruolo di questo server. In caso di dubbi, si consiglia il modello di server Web dinamico.

---

Prima di iniziare l'installazione, accertarsi che esistano i seguenti prerequisiti:

- ❑ Garantire la risoluzione dei nomi server dal servizio di gestione (MS) al servizio di distribuzione norme (DS): accertarsi che il computer di destinazione in cui viene installato MS sia in grado di eseguire il "ping" del nome server DS (NETBIOS se il servizio di distribuzione è configurato nel firewall di rete, FQDN se invece è installato all'esterno, nella DMZ).
- ❑ Abilitare o installare i servizi Microsoft IIS (Internet Information Services) ed accertarsi che ASP.NET sia attivo.

  ---

  **Importante:** Non selezionare la casella di controllo *Richiedi un canale protetto (SSL)* nella pagina Comunicazioni protette (nell'utility Gestione computer di Microsoft espandere *Servizi e applicazioni* > espandere *Gestione Internet Information Services (IIS)* > espandere *Siti Web* > fare clic con il pulsante destro del mouse su *Sito Web predefinito* > fare clic su *Proprietà* > fare clic sulla scheda *Protezione directory* > fare clic sul pulsante *Modifica* nella casella di gruppo Comunicazioni protette). La selezione di questa opzione interrompe la comunicazione tra il server e il client ZENworks Endpoint Security Management sull'endpoint.

  ---

Fare clic su *Installazione servizio garanzia ubicazioni client* dal menu Interfaccia di installazione. Ha inizio l'installazione del servizio CLAS.

All'avvio, il programma di installazione verifica che tutto il software necessario sia presente sul server. Eventuali componenti mancanti vengono installati automaticamente prima che l'installazione prosegua fino alla schermata iniziale (potrebbe essere necessario accettare contratti di licenza per software aggiuntivo). Se i componenti MDAC (Microsoft Data Access Components) 2.8 non sono installati, sarà necessario installarli e riavviare il server prima di proseguire con l'installazione di ZENworks Endpoint Security Management. Se si utilizza Windows 2003 Server, ASP.NET 2.0 verrà configurato per essere eseguito dal programma di installazione.

# 8.1 Procedura di installazione

Per installare il servizio CLAS e generare una chiave di licenza:

1. Fare clic su *Avanti* nella schermata iniziale per continuare.
2. Accettare il contratto di licenza, quindi fare clic su *Avanti*.
3. I file vengono copiati nella directory di default: `\Programmi\Novell\ESM CLAS`.
4. Durante l'installazione del servizio garanzia ubicazioni client vengono generate due chiavi, una privata e una pubblica. È possibile memorizzare il file publickey sul desktop o in un'altra directory. Se si desidera memorizzare il file publickey in una directory diversa, fare clic su *Sì*, quindi scegliere la cartella desiderata. Fare clic su *No* per accettare l'impostazione di default e memorizzare il file publickey con il file privatekey.
5. Fare clic su *Fine* per chiudere il programma di installazione.

È necessario che il servizio di gestione possa accedere alla chiave pubblica.

## 8.2 Installazioni del failover CLAS

È possibile installare sui server di tutta l'azienda più iterazioni CLAS, per garantire tramite cifratura più ubicazioni aziendali o per assicurare che, nel caso in cui il server CLAS principale dovesse smettere di funzionare, venga comunque garantita l'ubicazione.

Nel secondo scenario, la chiave privata viene individuata in base all'URL anziché all'indirizzo IP. Pertanto, è possibile configurare un blocco di server per condividere un singolo URL. È possibile installare CLAS su un solo server, la cui immagine viene poi copiata su ciascun server aggiuntivo; in alternativa, è possibile installare il servizio su ciascun server separatamente, copiando le chiavi pubblica e privata sugli altri server. Tutti i server presenti in un blocco URL devono avere a disposizione le stesse chiavi pubblica e privata.

## 8.3 Trasferimento della chiave pubblica al servizio di gestione

Al termine dell'installazione la chiave pubblica generata, che viene trasferita a Endpoint Security Client tramite le norme di sicurezza, si trova nella directory `\Programmi\Novell\Novell ESM CLAS` del server. La chiave pubblica viene identificata dal nome file `publickey`. Tale nome file può essere modificato nel modo desiderato.

Il file publickey deve essere copiato e trasferito al servizio di gestione (in un qualunque punto), consentendo in tal modo alla console di gestione di accedere alla chiave e distribuirla a tutti i client Endpoint Security Client tramite una norma di sicurezza. Il file `publickey` è anche caricabile su un PC che esegue la console di gestione di ZENworks Endpoint Security Management.

Continuare con Capitolo 9, “Installazione di Endpoint Security Client 3.5”, a pagina 59.

# Installazione di Endpoint Security Client 3.5

9

Utilizzare Novell ZENworks Endpoint Security Client 3.5 per i client Windows XP (SP1 e SP2) e Windows 2000 SP4. Fare clic sul programma di installazione *ZENworks Security Client* appropriato dal menu Interfaccia di installazione. Ha inizio l'installazione di Endpoint Security Client. Nelle pagine che seguono viene delineato il processo di installazione sia per l'installazione di base che per l'installazione MSI.

- L'installazione di base consente di installare Endpoint Security Client 3.5 solo sul computer corrente.
- L'installazione MSI prevede l'avvio del programma in modalità amministrativa (`/a`) e la creazione di un pacchetto MSI del software. È possibile eseguire il push down di tale pacchetto oppure renderlo disponibile in un'ubicazione di rete specifica con gli input dell'utente richiesti preconfigurati. In questo modo i singoli utenti saranno in grado di installare il software con i valori predefiniti del server.

## 9.1 Installazione di base di Endpoint Security Client 3.5

Questa procedura consente di installare Endpoint Security Client 3.5 solo sul computer corrente.

Verificare che tutte le patch di sicurezza di Microsoft e il software antivirus siano installati e aggiornati.

Installare i certificati radice del servizio di gestione sul computer locale (`ESM-MS.cer` o il certificato aziendale)

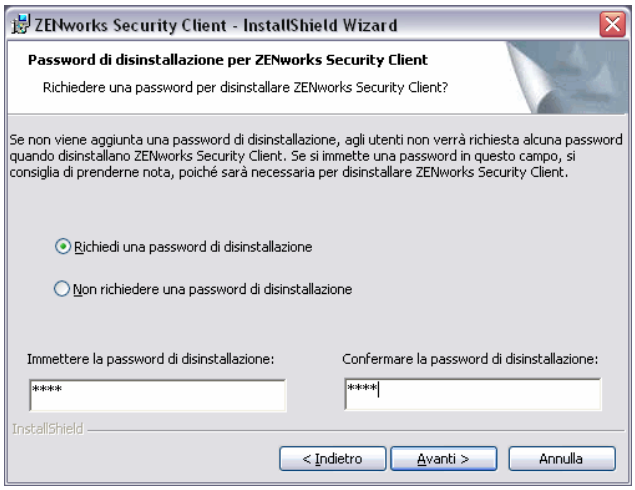
---

**Nota:** durante l'installazione di Endpoint Security Client 3.5 si consiglia di disattivare il software antivirus/antispyware che interagisce con funzioni di registro valide.

---

1. Fare clic su *Avanti* nella schermata iniziale per continuare.
2. Accettare il contratto di licenza, quindi fare clic su *Avanti*.
3. Immettere una password di installazione. Questa operazione impedisce all'utente di disinstallare Endpoint Security Client 3.5 attraverso *Installazione applicazioni* (consigliato).

***Figura 9-1*** *Password di disinstallazione*



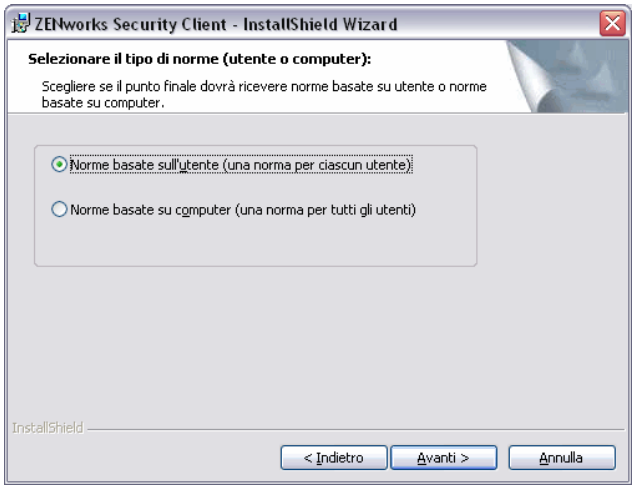

4 Selezionare la modalità di ricezione delle norme (dal servizio di distribuzione per client gestiti o recuperate localmente in caso di configurazione non gestita [vedere Capitolo 11, “Installazione non gestita di ZENworks Endpoint Security Management”, a pagina 79 per i dettagli relativi all'argomento]).

***Figura 9-2*** *Impostazioni di gestione*


5 Specificare le informazioni sul servizio di gestione.

6 Scegliere se le norme devono essere ricevute per gli utenti o per il computer (norme basate sul computer).

***Figura 9-3*** *Norme basate sull'utente o sul computer*




7 Fare clic su *Installa*.

Completata l'installazione del software, all'utente viene richiesto di riavviare il computer.

---

**Nota:** è possibile scegliere di copiare il certificato per il servizio di gestione in una cartella con la stessa ubicazione di `setup.exe`, prima di eseguire l'installazione. Con questa operazione l'installazione del certificato nel computer è automatica (ad esempio, per tutti gli utenti). Tale processo può essere eseguito anche con il file `.dat` della licenza Novell.

---

# 9.2 Installazione MSI

Questa procedura consente di creare un pacchetto MSI per Endpoint Security Client 3.5. Questo pacchetto viene utilizzato da un amministratore di sistema per pubblicare l'installazione in un gruppo di utenti tramite una norma di Active Directory o attraverso altri metodi di distribuzione del software.

Per creare il pacchetto MSI:

Se si esegue l'operazione dal CD o dal programma di installazione principale ISO e non si intende eseguire nessuna variabile della riga di comando (vedere Sezione 9.2.1, “Variabili della riga di comando”, a pagina 64):

1 Inserire il CD e attendere l'avvio del programma di installazione principale.
2 Fare clic su *Installazione prodotto*.
3 Fare clic su *Client di sicurezza*.
4 Fare clic su *Crea pacchetto MSI ZSC*.

Se per l'installazione si utilizza solo `setup.exe` (l'eseguibile si trova nel CD in: `D:\ESM32\ZSC`), iniziare procedendo come segue:

1 Fare clic con il pulsante destro del mouse su `setup.exe`.
2 Selezionare *Crea collegamento*.
3 Fare clic con il pulsante destro del mouse sul collegamento, quindi su *Proprietà*.

4 Alla fine del campo Destinazione, dopo le virgolette, immettere uno spazio utilizzando la barra spaziatrice, quindi digitare `/a`.

   Ad esempio: `"C:\Documents and Settings\\euser\Desktop\\CL-Release-3.2.455\setup.exe" /a`

   Per l'installazione MSI, sono disponibili diverse variabili della riga di comando; per ulteriori informazioni, vedere Sezione 9.2.1, “Variabili della riga di comando”, a pagina 64.

5 Fare clic su *OK*.

6 Fare doppio clic sul collegamento per avviare il programma di installazione MSI.

Quando l'installazione ha inizio:

1 Fare clic su *AVANTI* nella schermata iniziale per continuare.

2 Accettare il contratto di licenza, quindi fare clic su *Avanti*.

3 Indicare se è richiesta una password di disinstallazione (consigliato) e immettere la password.

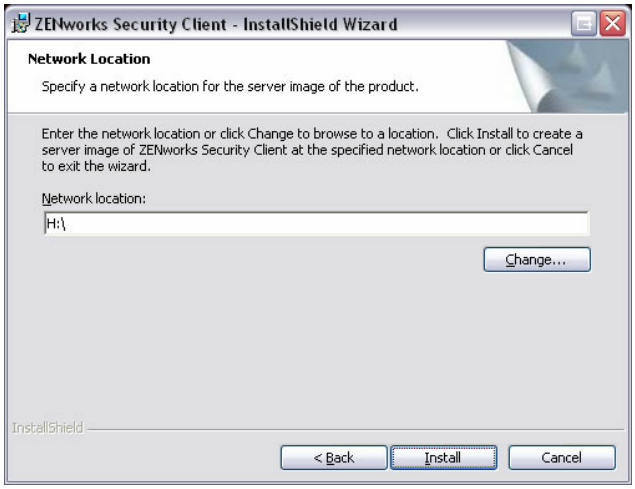
4 Selezionare la modalità di ricezione delle norme (dal servizio di distribuzione per client gestiti, recuperate localmente per una configurazione non gestita). Se è selezionata la modalità Gestita:

- Specificare le informazioni sul servizio di gestione (il nome, FQDN o NETBIOS, dipende dalla modalità di inserimento adottata durante l'installazione del servizio di gestione).
- Scegliere se le norme saranno basate sull'utente o sul computer.

5 (Facoltativo) Specificare un indirizzo di e-mail nel campo fornito per essere informati nel caso l'installazione non riesca.

6 Specificare l'ubicazione di rete in cui viene creata l'immagine MSI o individuare tale ubicazione facendo clic sul pulsante *Modifica*.

***Figura 9-4*** *Selezione dell'ubicazione di rete per l'immagine MSI*



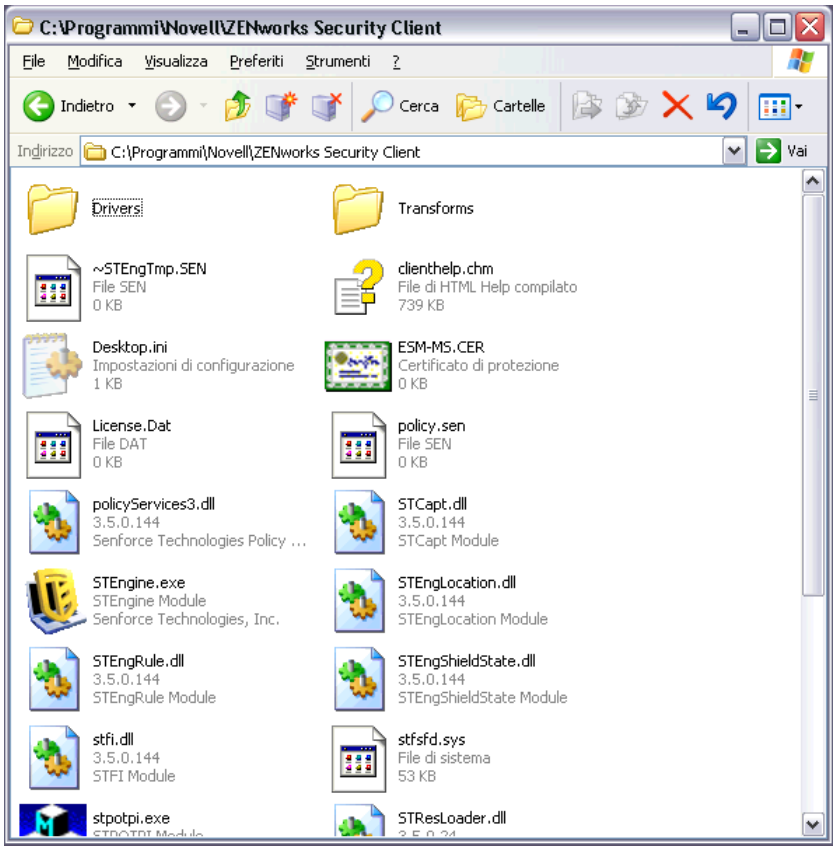

7 Fare clic su *Installa* per creare un'immagine MSI.

8 Individuare l'immagine MSI creata e aprire la cartella `"\Programmi\Novell\ZENworks Security Client\"`

9 Copiare il certificato SSL del servizio di gestione (`ESM-MS.cer` o il certificato aziendale) e la chiave di licenza Novell in questa cartella, sostituendo i file da 0 KB di default attualmente presenti nella cartella. Il certificato SSL ESM-MS è disponibile nella cartella `File di`

`installazione di ZENworks Endpoint Security Management`. La chiave di licenza viene spedita separatamente via e-mail (non è tuttavia necessaria qualora la valutazione sia di 30 giorni).

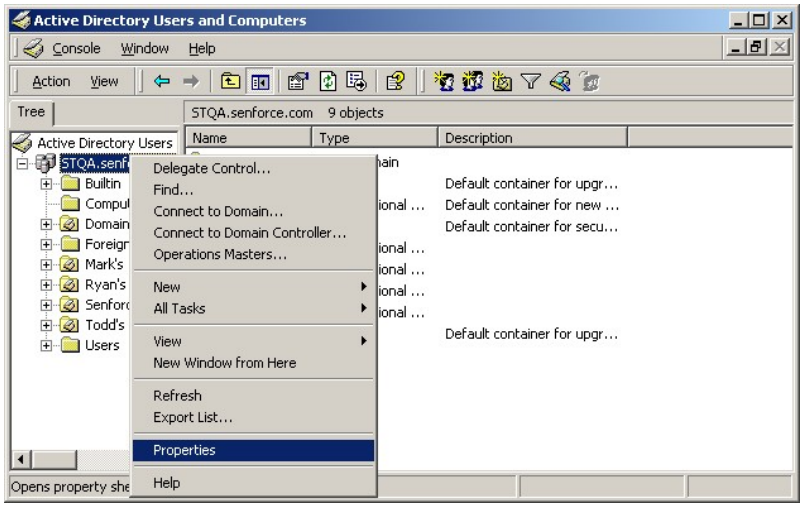
***Figura 9-5*** *Sostituzione dei file di default nel pacchetto MSI*




Per impostare il pacchetto MSI per il push down ai gruppi di utenti, come norme di gruppo:

1 Aprire *Strumenti di amministrazione - Utenti e computer di Active Directory*, quindi aprire *Dominio radice* o *Proprietà OU*.

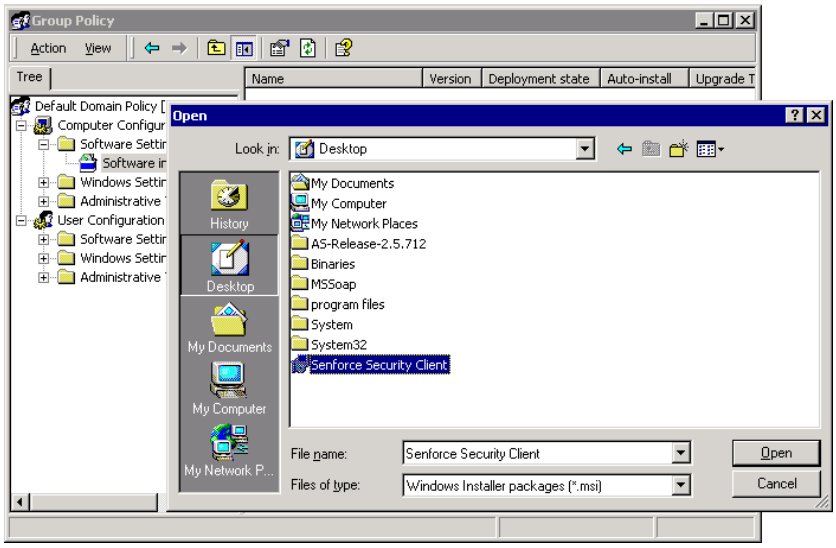
***Figura 9-6*** *Apertura di Proprietà in Dominio radice o OU*




**2** Fare clic sulla scheda *Norme di gruppo* e quindi su *Modifica*.

**3** Aggiungere il pacchetto MSI alla configurazione del computer.

***Figura 9-7*** *Selezione del pacchetto MSI da aggiungere*




## 9.2.1 Variabili della riga di comando

Le opzioni relative alle variabili della riga di comando sono disponibili per l'installazione MSI. Queste variabili devono essere impostate nel collegamento eseguibile configurato per l'esecuzione in modalità amministrativa. Per utilizzare una variabile, è necessario immettere nel collegamento MSI la seguente riga di comando:

`"...\setup.exe" /a /V"variabili"`. Immettere uno dei comandi riportati di seguito tra virgolette. Separare le diverse variabili con un singolo spazio.

Esempio: `setup.exe /a /V"STDRV=stateful STBGL=1"` consente di creare un pacchetto MSI in cui Endpoint Security Client 3.5 verrà avviato con l'opzione Tutti Stateful e rigida applicazione della White List.

**Nota:** l'avvio in modalità Stateful potrebbe causare problemi di interoperabilità (ritardi indirizzo DHCP, problemi di interoperabilità di rete Novell e così via).

Sono disponibili le seguenti righe di comando:

***Tabella 9-1*** *Variabili della riga di comando*

| Variabile della riga di comando | Descrizione | Note |
|---|---|---|
| STDRV=stateful | Driver NDIS tutti stateful durante l'avvio. | Modifica lo stato di default del driver NDIS da Tutte aperte a Tutte Stateful permettendo la totalità del traffico di rete durante l'avvio, finché Endpoint Security Client 3.5 non ha stabilito l'ubicazione. |
| /qn | Installazione non interattiva. | Utilizzare per non visualizzare il processo di installazione MSI tipica. Endpoint Security Client 3.5 si attiverà al successivo riavvio dell'utente. |
| STRBR=ReallySuppress | Nessun riavvio dopo il completamento dell'installazione. | L'applicazione della sicurezza e l'autodifesa del client non funzionano completamente fino a dopo il primo riavvio. |
| STBGL=1 | Rigida applicazione della White List sul controllo delle applicazioni. | Le norme DEVONO essere create per l'identificazione dell'applicazione sulla White List e distribuite con queste norme. |
| STUPGRADE=1 | Upgrade di Endpoint Security Client 3.5. | Utilizzare durante l'upgrade di Endpoint Security Client 3.5. |
| STUNINSTALL=1 | Disinstallazione di Endpoint Security Client 3.5. | Utilizzare durante la disinstallazione di Endpoint Security Client 3.5. |
| STUIP="la password" | Disinstallazione con password | Utilizzare quando una password di disinstallazione è attiva. |
| STNMS="Nome MS" | Modifica del nome del servizio di gestione. | Modifica il nome del servizio di gestione per Endpoint Security Client 3.5. |
| POLICYTYPE=1 | Modifica di Endpoint Security Client 3.5 in norme basate sul computer. | Utilizzare per modificare i client Endpoint Security Client installati con MSI affinché accettino le norme basate sul computer invece di quelle basate sull'utente. |

| Variabile della riga di comando | Descrizione | Note |
|---|---|---|
| POLICYTYPE=2 | Modifica di Endpoint Security Client 3.5 in norme basate sull'utente. | Utilizzare per modificare i client Endpoint Security Client installati con MSI affinché accettino le norme basate sull'utente invece di quelle basate sul computer. |
| STVA="Nome adattatore" | Aggiunta di adattatore virtuale. | Utilizzare per attivare il controllo delle norme su un adattatore virtuale |
| /L*v c:\log.txt | Attivazione della registrazione. | Utilizzare per attivare la registrazione al momento dell'installazione. In caso contrario, sarà necessario eseguire l'operazione attraverso gli strumenti di diagnostica di Endpoint Security Client (consultare la Guida dell'amministratore). |

## 9.2.2 Distribuzione di norme con il pacchetto MSI

Le norme di default prevedevano la possibilità di sostituzione con norme configurate dall'azienda al momento dell'installazione MSI. Per eseguire il push down di norme specifiche con l'immagine MSI:

1. Creare una norma da distribuire a tutti gli utenti attraverso la console di gestione (consultare la *Guida dell'amministratore di ZENworks Endpoint Security Management* per informazioni sulla creazione di norme).
2. Esportare la norma e salvarla come `policy.sen`.

   **Nota:** tutte le norme distribuite con questa modalità (non gestita) devono essere denominate `policy.sen` affinché Endpoint Security Client 3.5 le accetti. Le norme non denominate `policy.sen` non verranno implementate da Endpoint Security Client 3.5.
3. Aprire la cartella in cui erano state esportate le norme e copiare i file `policy.sen` e `setup.sen`.
4. Individuare l'immagine MSI creata e aprire la cartella "`\Programmi\Novell\ZENworks Security Client\`".
5. Incollare i file `policy.sen` e `setup.sen` nella cartella. In questo modo i file `policy.sen` e `setup.sen` di default verranno sostituiti.

## 9.2.3 Installazione utente di Endpoint Security Client 3.5 da MSI

Quando l'utente esegue nuovamente l'autenticazione nel dominio (mediante riavvio del computer), l'esecuzione del pacchetto di installazione MSI avviene prima del login. Al termine dell'installazione, il computer si riavvia e l'utente può effettuare il login al computer. Endpoint Security Client 3.5 è installato e in esecuzione nel computer.

## 9.3 Esecuzione di Endpoint Security Client 3.5

Endpoint Security Client 3.5 viene eseguito automaticamente all'avvio del sistema. Per ulteriori informazioni su Endpoint Security Client 3.5, consultare la *Guida dell'amministratore di ZENworks Endpoint Security Client 3.5*.

È possibile distribuire la Guida dell'utente a tutti gli utenti per aiutarli a comprendere meglio il funzionamento del nuovo software di sicurezza degli endpoint.

# Installazione di ZENworks Endpoint Security Client 4.0

# 10

Novell® ZENworks® Endpoint Security Client 4.0 è una versione client per il supporto di Microsoft Windows Vista con Support Pack 1 in esecuzione in modalità a 32 bit e di Windows Server 2008 in esecuzione in modalità a 32 bit. Endpoint Security Client 4.0 utilizza il server e la console di gestione di ZENworks Endpoint Security Management 3.5. È possibile gestire Windows XP con il client 3.5 e Windows Vista con il client 4.0.

Nelle pagine che seguono viene delineato il processo di installazione sia per l'installazione di base che per l'installazione MSI.

L'installazione di base consente di installare Endpoint Security Client 4.0 solo sul computer corrente.

L'installazione MSI prevede l'avvio del programma in modalità amministrativa (`/a`) e la creazione di un pacchetto MSI del software. È possibile eseguire il push down di tale pacchetto oppure renderlo disponibile in un'ubicazione di rete specifica con gli input dell'utente richiesti preconfigurati. In questo modo i singoli utenti saranno in grado di installare il software con i valori predefiniti del server.



## 10.1 Installazione di base di Endpoint Security Client 4.0

Questa procedura consente di installare ZENworks Endpoint Security Client 4.0 solo sul computer corrente.

**Istruzioni preliminari:**

- Verificare che tutte le patch di sicurezza di Microsoft e il software antivirus siano installati e aggiornati. Il software di Endpoint Security Client 4.0 può essere installato in Windows Vista con Support Pack 1 e in Windows Server 2008, entrambi in esecuzione in modalità a 32 bit.
- Durante l'installazione di Endpoint Security Client 4.0 si consiglia di disattivare il software antivirus/antispyware che interagisce con funzioni di registro valide.
- Il client Endpoint Security Client gestito richiede la comunicazione SSL per il componente del servizio di ZENworks Endpoint Security Management. Se sono stati selezionati i certificati firmati da se stessi durante l'installazione del servizio di gestione o del server singolo, l'endpoint in cui è in esecuzione il client di sicurezza deve avere il certificato installato nel contesto appropriato (preferibilmente nel contesto del computer locale).

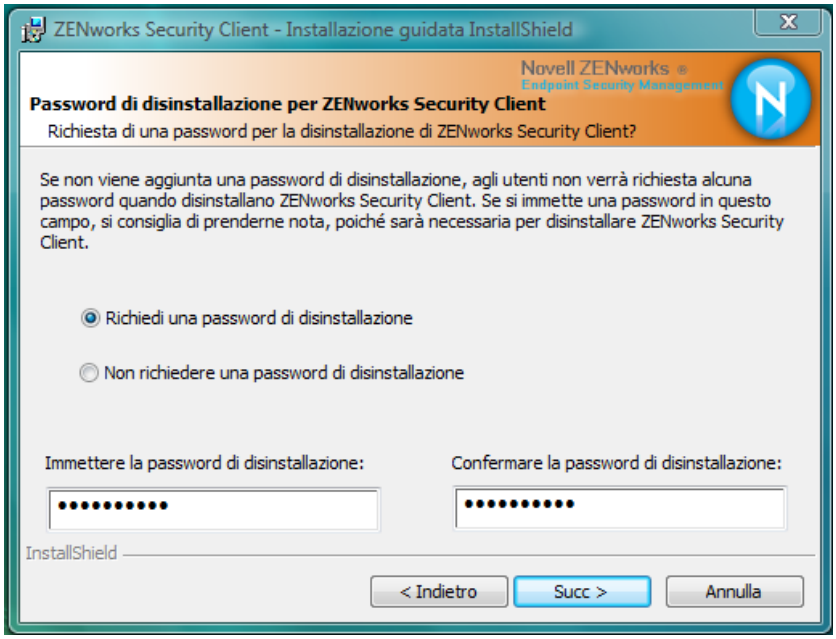
Per effettuare questa operazione automaticamente, collocare il file `ESM-MS.cer` nella cartella con il file `Setup.exe` del programma di installazione di Endpoint Security Client. Facoltativamente è possibile copiare l'intera cartella `File di installazione ESM` dall'installazione del servizio di gestione (o dall'installazione del server singolo) nella cartella con il programma di installazione di Endpoint Security Client `Setup.exe` (assicurarsi che il file `ESM-MS.cert` si trovi nella cartella `File di installazione ESM` e che la cartella sia denominata `File di installazione ESM`. Con questa operazione l'installazione del certificato nel computer è automatica (ad esempio, per tutti gli utenti). Tale processo può essere eseguito anche con il file `.dat` della licenza Novell.

Selezionare la directory del programma di installazione di *ZENworks Security Client* appropriata dal menu Interfaccia di installazione.

1. Fare doppio clic su `Setup.exe` per iniziare il processo di installazione.
2. Selezionare la lingua desiderata per l'installazione, quindi fare clic su *OK*.

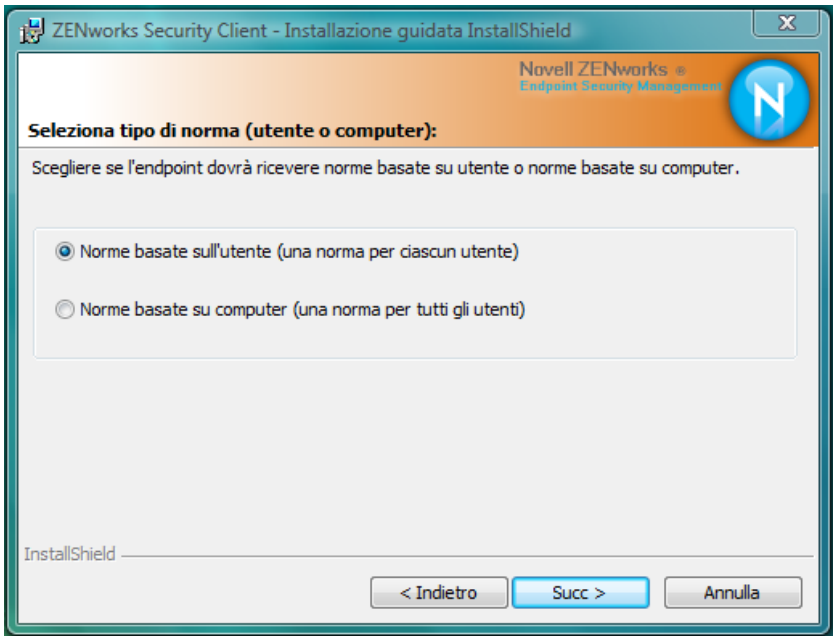
   Tra le lingue disponibili sono incluse:

   - Cinese semplificato
   - Cinese tradizionale
   - Inglese (lingua di default)
   - Francese
   - Tedesco
   - Italiano
   - Giapponese
   - Portoghese
   - Spagnolo tradizionale
3. Endpoint Security Client 4.0 richiede che, prima dell'installazione del client, nel computer sia installato Microsoft Web Services Enhancements (WSE) 2.0 con Service Pack 3 e Microsoft Visual C++ 2008. Se il processo di installazione non rileva questi componenti, verrà visualizzata questa schermata. Fare clic su *Installa* per installare questi requisiti.
4. Disattivare il software antivirus e antispyware, se ancora non è stato fatto, prima di premere *Avanti* nella schermata iniziale.
5. Accettare il contratto di licenza, quindi fare clic su *Avanti*.




6 Selezionare *Richiedi una password di disinstallazione*. In questo modo si impedisce all'utente di disinstallare Endpoint Security Client 4.0 (consigliato).

7 Aggiungere una password di disinstallazione e confermarla, quindi fare clic su *Avanti*.

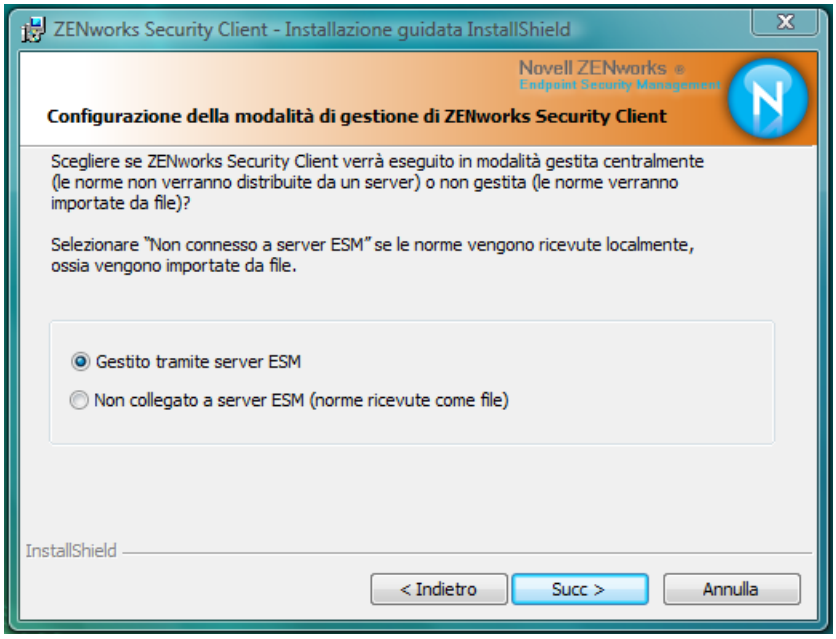



8 Selezionare un tipo di norma (basata sull'utente, per cui ogni utente dispone di una singola norma, o basata sul computer, per cui una norma viene utilizzata per tutti gli utenti). Fare clic su *Avanti*.

---

**Nota:** Selezionare la norma basata sull'utente se la rete utilizza eDirectory come servizio di directory. eDirectory non supporta le norme basate sui computer.

---




9 Selezionare la modalità di ricezione delle norme (gestite attraverso i server ESM per i client gestiti o recuperate localmente per una configurazione non gestita) (autonoma). Fare clic su *Avanti*.

Per informazioni su un'installazione non gestita, consultare Capitolo 11, “Installazione non gestita di ZENworks Endpoint Security Management”, a pagina 79.

10 (Facoltativo) Se è stato selezionato *Gestito mediante server ESM* nel Passo 9, digitare il nome del server che supporta il servizio di gestione.

Il nome del server immesso deve corrispondere al nome “Rilasciato a” fornito nel certificato radice attendibile utilizzato nel server in cui è installato il servizio ZENworks Endpoint Management o il server singolo. Si tratterà del nome NETBIOS o del nome FQDN (Fully Qualified Domain Name) del server in cui è in esecuzione il componente del servizio ZENworks Endpoint Management. Dopo l'immissione, fare clic su *Avanti*.

11 Fare clic su *Installa* per avviare l'installazione.

12 Al termine dell'installazione del software, riavviare il computer quando richiesto.

Per un elenco di funzioni non disponibili per il client 4.0 per Vista, consultare Sezione 10.4, “Funzioni non supportate in Endpoint Security Client 4.0”, a pagina 76.

## 10.2 Installazione MSI

Questa procedura consente di creare un pacchetto MSI per Endpoint Security Client 4.0. Questo pacchetto viene utilizzato da un amministratore di sistema per pubblicare l'installazione in un gruppo di utenti tramite una norma di Active Directory o attraverso altri metodi di distribuzione del software.

- Sezione 10.2.4, “Variabili della riga di comando”, a pagina 75
- Sezione 10.2.5, “Distribuzione di norme con il pacchetto MSI”, a pagina 76

### 10.2.1 Utilizzo del programma di installazione principale

Se si esegue l'installazione dal CD o dal programma di installazione principale ISO e non si intende eseguire nessuna variabile della riga di comando:

1. Inserire il CD e attendere l'avvio del programma di installazione principale.
2. Fare clic su *Installazione prodotto*.
3. Fare clic su *Client di sicurezza*.
4. Fare clic su *Crea pacchetto MSI ZSC*.
5. Continuare con Sezione 10.2.3, “Completamento dell'installazione”, a pagina 73.

### 10.2.2 Utilizzo del file Setup.exe

Se si utilizza solo il file `setup.exe` per l'installazione:

1. Fare clic con il pulsante destro del mouse su `setup.exe`.

   Il file eseguibile è disponibile sul CD in `D:\ESM32\ZSC`.
2. Selezionare *Crea collegamento*.
3. Fare clic con il pulsante destro del mouse sul collegamento, quindi su *Proprietà*.
4. Alla fine del campo *Destinazione*, dopo le virgolette, premere una volta la barra spaziatrice per inserire uno spazio, quindi digitare `/a`.

   Ad esempio: `"C:\Documents and Settings\\euser\Desktop\\CL-Release-3.2.455\setup.exe" /a`

   Per l'installazione MSI sono disponibili numerose variabili della riga di comando. Per ulteriori informazioni, vedere Sezione 9.2.1, “Variabili della riga di comando”, a pagina 64.
5. Fare clic su *OK*.
6. Fare doppio clic sul collegamento per avviare il programma di installazione MSI.
7. Continuare con Sezione 10.2.3, “Completamento dell'installazione”, a pagina 73.

### 10.2.3 Completamento dell'installazione

Completare Utilizzo del programma di installazione principale o Utilizzo del file Setup.exe, quindi utilizzare questa procedura per terminare l'installazione del client.

1. Fare clic su *AVANTI* nella schermata iniziale per continuare.
2. Selezionare *Richiedi una password di disinstallazione* (consigliato) e immettere la password. Fare clic su *Avanti*.

---

**Nota:** Se si disinstalla Endpoint Security Client attraverso un pacchetto MSI, è necessario specificare la password di disinstallazione tramite le proprietà MSI (consultare Tabella 10-1 a pagina 75).

---

3 Selezionare un tipo di norma (basata sull'utente, per cui ogni utente dispone di una singola norma, o basata sul computer, per cui una norma viene utilizzata per tutti gli utenti). Fare clic su *Avanti*.

---

**Nota:** Selezionare la norma basata sull'utente se la rete utilizza eDirectory come servizio di directory. eDirectory non supporta le norme basate sui computer.

---

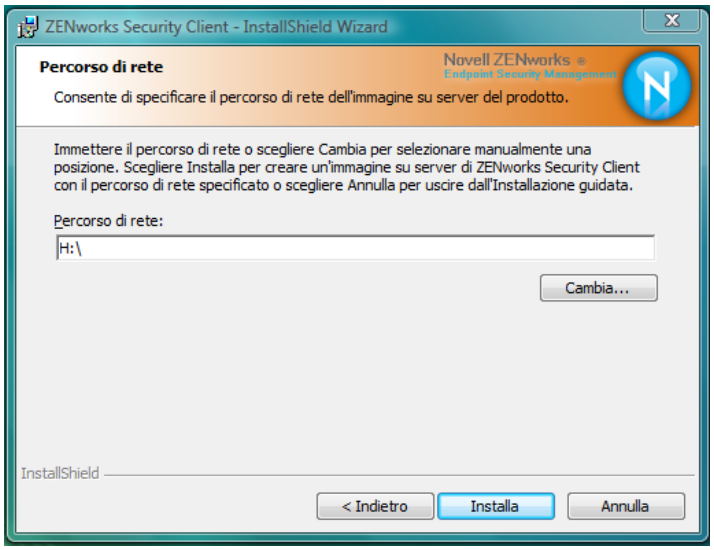
4 Selezionare la modalità di ricezione delle norme (gestite attraverso i server ESM per i client gestiti o recuperate localmente per una configurazione non gestita) (autonoma).

5 Se è stato selezionato *Gestito mediante server ESM* in Passo 4:

- Il nome del server immesso deve corrispondere al nome "Rilasciato a" fornito nel certificato radice attendibile utilizzato nel server in cui è installato il servizio ZENworks Endpoint Management o il server singolo. Si tratterà del nome NETBIOS o del nome FQDN (Fully Qualified Domain Name) del server in cui è in esecuzione il componente del servizio ZENworks Endpoint Management.

6 (Facoltativo) Specificare un indirizzo di e-mail nel campo fornito per essere informati nel caso l'installazione non riesca.

7 Specificare l'ubicazione di rete in cui creare l'immagine MSI o individuare e selezionare l'ubicazione facendo clic sul pulsante *Cambia*.




8 Fare clic su *Installa* per creare un'immagine MSI. Fare clic su *Fine* per chiudere il programma di installazione.

9 Individuare l'ubicazione in cui è stata creata l'immagine MSI e aprire la cartella `\Programmi\Novell ZENworks\Endpoint Security Client\`.

10 Copiare il certificato SSL del servizio di gestione (`ESM-MS.cer` o il certificato aziendale) e la chiave di licenza Novell in questa cartella, sostituendo i file da 0 KB di default attualmente presenti nella cartella.

Il certificato SSL ESM-MS è disponibile nella cartella `File di installazione di ZENworks Endpoint Security Management`. La chiave di licenza viene inviata separatamente per posta elettronica. Nel caso del periodo di valutazione di 60 giorni, non è necessaria alcuna chiave di licenza.

## 10.2.4 Variabili della riga di comando

Sono disponibili opzioni delle variabili della riga di comando per un'installazione MSI. Queste variabili devono essere impostate nel collegamento eseguibile configurato per l'esecuzione in modalità amministrativa. Per utilizzare una variabile, è necessario immettere la seguente riga di comando nel collegamento MSI:

`"...\setup.exe" /a /V"variabili"`. Immettere uno dei comandi riportati di seguito tra virgolette. Separare le diverse variabili con un singolo spazio.

Sono disponibili le seguenti righe di comando:

***Tabella 10-1*** *Variabili della riga di comando*

| Variabile della riga di comando | Descrizione | Note |
|---|---|---|
| /qn | Installazione non interattiva. | Sopprime il processo di installazione MSI tipico. Endpoint Security Client si attiverà al successivo riavvio da parte dell'utente. |
| SESMSG=1 | Mostra un messaggio che indica che per i file presenti nelle cartelle “Safe Harbor” non è possibile rimuovere automaticamente la cifratura se viene distribuita una norma di cifratura. | Il valore di default è 0 (che indica che i messaggi non vengono visualizzati) per rendere la disinstallazione automatica. |
| STRBR=ReallySuppress | Nessun riavvio al termine dell'installazione. | L'applicazione della sicurezza e l'autodifesa del client non funzionano completamente fino a dopo il primo riavvio. |
| STUPGRADE=1 | Upgrade di Endpoint Security Client 4.0. | Esegue l'upgrade di Endpoint Security Client 4.0. |
| STUNINSTALL=1 | Disinstallazione di Endpoint Security Client 4.0. | Disinstalla Endpoint Security Client 4.0. |
| STUIP="la password" | Disinstallazione con password | Utilizzare questa variabile quando è attiva una password di disinstallazione. |
| STNMS="Nome MS" | Modifica del nome del servizio di gestione. | Modifica il nome del servizio di gestione per Endpoint Security Client 4.0. |
| POLICYTYPE=1 | Modifica di Endpoint Security Client 4.0. in norme basate sul computer. | Modifica i client Endpoint Security Client installati con MSI affinché accettino le norme basate sul computer anziché quelle basate sull'utente. |
| POLICYTYPE=2 | Modifica di Endpoint Security Client 4.0 in norme basate sull'utente. | Modifica i client ZENworks Security 4.0 per Vista installati con MSI affinché accettino le norme basate sull'utente anziché quelle basate sul computer. |

| Variabile della riga di comando | Descrizione | Note |
|---|---|---|
| STVA="Nome adattatore" | Aggiunta di un adattatore virtuale. | Attiva il controllo delle norme in relazione a un adattatore virtuale. |
| /L*v c:\log.txt | Attivazione della registrazione. | Attiva il login al momento dell'installazione. Se non si utilizza questa variabile, il login deve essere eseguito attraverso gli strumenti di diagnostica di Endpoint Security Client. |

### 10.2.5 Distribuzione di norme con il pacchetto MSI

Le norme di default prevedevano la possibilità di sostituzione con norme configurate dall'azienda al momento dell'installazione MSI. Per eseguire il push down di norme specifiche con l'immagine MSI:

1. Creare una norma da distribuire a tutti gli utenti attraverso la console di gestione (consultare la *Guida dell'amministratore di ZENworks Endpoint Security Management* per informazioni sulla creazione di norme).
2. Esportare la norma, quindi rinominarla in `policy.sen`.

   Tutte le norme distribuite con questa modalità (non gestita) devono essere denominate `policy.sen` affinché Endpoint Security Client 4.0 le accetti. Le norme non denominate `policy.sen` non vengono implementate da Endpoint Security Client 4.0.
3. Aprire la cartella in cui erano state esportate le norme e copiare i file `policy.sen` e `setup.sen`.
4. Individuare l'immagine MSI creata e aprire la cartella `\Programmi\Novell ZENworks\Endpoint Security Client\`.
5. Incollare i file `policy.sen` e `setup.sen` nella cartella. In questo modo i file `policy.sen` e `setup.sen` di default verranno sostituiti.

## 10.3 Esecuzione di Endpoint Security Client 4.0

Endpoint Security Client 4.0 viene eseguito automaticamente all'avvio del sistema. Per ulteriori informazioni su Endpoint Security Client 4.0, consultare la *Guida dell'utente di ZENworks Endpoint Security Client 4.0*.

È possibile distribuire la Guida dell'utente a tutti gli utenti per aiutarli a comprendere meglio il funzionamento del nuovo software di sicurezza degli endpoint.

## 10.4 Funzioni non supportate in Endpoint Security Client 4.0

Tra le funzioni non supportate o supportate parzialmente in Endpoint Security Client 4.0 sono comprese:

- Autodifesa del client.
- Supporto del modem.

- Scripting.
- Modifica manuale dei firewall in un'ubicazione.
- Visibilità di più firewall in un'ubicazione. È disponibile solo il firewall di default.
- Regole di integrità.
- Blocco delle applicazioni.
- Le informazioni relative all'icona dell'area di notifica al passaggio del mouse sono cambiate. L'icona mostra solo informazioni sulle norme e sull'ubicazione.
- Connettività USB.
- Gestione delle chiavi Wi-Fi.
- Alle connessioni cablate non viene data maggiore importanza delle connessioni wireless.
- Aggiornamenti di Endpoint Security Client (in base alle norme).
- Timeout di autenticazione VPN.
- Riproduzione automatica per il controllo di dispositivi di memorizzazione.
- Voci della rubrica telefonica nell'ambiente di rete.

# Installazione non gestita di ZENworks Endpoint Security Management

# 11

Un'azienda può eseguire ZENworks® Security Client e la console di gestione anche in modalità non gestita (senza collegarsi al servizio di distribuzione norme o al servizio di gestione). Questa modalità è disponibile come opzione di installazione, ed è principalmente destinata all'impostazione di valutazioni semplici. Tale opzione inoltre è ideale per le aziende che dispongono di poco spazio per il server o ne sono totalmente prive oppure hanno esigenze di protezione di base. Tuttavia con questo tipo di configurazione non sono disponibili aggiornamenti rapidi delle norme e generazione di rapporti sulla conformità.

## 11.1 Installazione non gestita di Endpoint Security Client.

Per installare un Endpoint Security Client non gestito, seguire le istruzioni in Capitolo 9, “Installazione di Endpoint Security Client 3.5”, a pagina 59 e selezionare l'opzione *Non connesso a server ESM (norme ricevute come file*. L'installazione ignora le domande relative ai nomi dei server e installa Endpoint Security Client sul computer (è anche possibile creare un pacchetto MSI per un Endpoint Security Client non gestito).

***Figura 11-1*** *Selezionare "Non connesso a server ESM"*


## 11.2 Console di gestione autonoma

Questa configurazione consente l'installazione della console di gestione di ZENworks Endpoint Security Management e la creazione di norme senza connettersi a un servizio di gestione esterno o distribuire norme attraverso il relativo servizio. Selezionare *Installazione console di gestione autonoma* dal menu del programma di installazione principale e seguire le istruzioni in Capitolo 7, “Installazione della console di gestione”, a pagina 43 per l'installazione.

All'avvio dell'installazione, viene installato un database SQL (se il computer ne contiene già uno, il programma di installazione configurerà i database appropriati). Una volta installato il database, l'installazione si interrompe. Per attivare il database SQL è necessario riavviare il computer. Dopo il riavvio, attivare nuovamente l'installazione per continuare.

La funzionalità di gran parte delle norme è disponibile per la distribuzione, fatta eccezione per Generazione rapporti. Tutti i file delle norme esportati devono essere distribuiti alla directory `\Programmi\Novell\ZENworks Security Client\` di Endpoint Security Client.

## 11.3 Distribuzione delle norme non gestite

Per distribuire 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 collocato nella directory `\Programmi\Novell\ESM Management Console\`.
2. Creare una norma nella console di gestione (per ulteriori informazioni, consultare la *Guida dell'amministratore di ZENworks Endpoint Security Client*).
3. Utilizzare il comando *Esporta* per esportare le norme nella stessa cartella contenente il file `setup.sen`. Tutte le norme distribuite devono essere denominate `policy.sen` affinché Endpoint Security Client le accetti.
4. Distribuire i file `policy.sen` e `setup.sen`. È necessario copiare i file nella directory `\Programmi\Novell\ZENworks Security Client\` per tutti i client non gestiti.

   Solo il file `setup.sen` deve essere copiato una volta nei dispositivi non gestiti con le prime norme. Successivamente, occorre distribuire solo le nuove norme.

Se un Endpoint Security Client non gestito viene installato nello stesso computer della console di gestione autonoma, anche il file `setup.sen` deve essere copiato nella directory `\Programmi\Novell\ZENworks Security Client\`. Se Endpoint Security Client non gestito viene installato sul computer dopo l'editor autonomo, il file dovrà essere trasferito manualmente come descritto in precedenza.

Facendo clic sul pulsante *Pubblica* le norme vengono immediatamente pubblicate nell'Endpoint Security Client non gestito di tale computer. Per fornire norme a più utenti non gestiti, utilizzare la funzione Esporta come descritto in precedenza.

# Aggiornamenti della documentazione

A

Questa sezione contiene le informazioni sulle modifiche al contenuto della documentazione effettuate in questa *Guida all'installazione di ZENworks Endpoint Security Management* dopo il rilascio iniziale per la versione 3.5. Le modifiche vengono elencate in base alla data di pubblicazione.

La documentazione relativa a questo prodotto è disponibile sul Web in due formati: HTML e PDF. I documenti HTML e PDF sono entrambi aggiornati con le modifiche elencate nella presente sezione.

Per sapere se la copia della documentazione PDF in uso è la più recente, consultare la data di pubblicazione sul titolo della pagina del documento PDF.

La documentazione è stata aggiornata nelle seguenti date:

- Sezione A.1, “5 gennaio 2009”, a pagina 81

## A.1 5 gennaio 2009

Sono state aggiornate le sezioni seguenti:

| Ubicazione | Aggiornamento |
|---|---|
| Tutte le sezioni | Il nome del client è stato modificato in tutta la guida. Ora è formalmente denominato Novell ZENworks Endpoint Security Client. Nei capitoli corrispondenti, i client vengono denominati Endpoint Security Client 3.5 (per Windows XP) ed Endpoint Security Client 4.0 (per Windows Vista). |
| Sezione 1.1, “Requisiti di sistema”, a pagina 10 | Sono stati aggiunti requisiti di sistema per il nuovo client Vista e la console di gestione autonoma. |
| Capitolo 9, “Installazione di Endpoint Security Client 3.5”, a pagina 59 | Sono state aggiunte informazioni e la modifica del nome che indica che Endpoint Security Client 3.5 riguarda Windows XP. |
| Capitolo 10, “Installazione di ZENworks Endpoint Security Client 4.0”, a pagina 69 | È stato aggiunto un capitolo relativo a Endpoint Security Client 4.0 (per Windows Vista). |