AUTHORIZED DOCUMENTATION

Installationshandbuch

January 5, 2009

Novell®
ZENworks® Endpoint Security Management

3.5

www.novell.com

Rechtliche Hinweise

Novell, Inc. leistet keinerlei Gewähr bezüglich des Inhalts oder Gebrauchs dieses Handbuchs. Insbesondere werden keine ausdrücklichen oder stillschweigenden Gewährleistungen hinsichtlich der handelsüblichen Qualität oder Eignung für einen bestimmten Zweck übernommen. Novell, Inc. behält sich weiterhin das Recht vor, diese Dokumentation zu revidieren und ihren Inhalt jederzeit und ohne vorherige Ankündigung zu ändern.

Des Weiteren übernimmt Novell, Inc. für Software keinerlei Haftung und schließt insbesondere jegliche ausdrücklichen oder impliziten Gewährleistungsansprüche bezüglich der Marktfähigkeit oder der Eignung für einen bestimmten Zweck aus. Außerdem behält sich Novell, Inc. das Recht vor, Novell-Software ganz oder teilweise jederzeit inhaltlich zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen von diesen Überarbeitungen oder Änderungen in Kenntnis zu setzen.

Alle im Zusammenhang mit dieser Vereinbarung zur Verfügung gestellten Produkte oder technischen Informationen unterliegen möglicherweise den US-Gesetzen zur Exportkontrolle sowie den Handelsgesetzen anderer Länder. Sie erkennen alle Ausfuhrkontrollbestimmungen an und erklären sich damit einverstanden, alle für ausstehende Exporte, Re-Exporte oder Importe erforderlichen Lizenzen bzw. Klassifizierungen einzuholen. Sie erklären sich damit einverstanden, nicht an juristische Personen, die in der aktuellen US-Exportausschlussliste enthalten sind, oder an in den US-Exportgesetzen aufgeführte terroristische Länder oder Länder, die einem Embargo unterliegen, zu exportieren oder zu reexportieren. Sie stimmen zu, keine Lieferungen für verbotene nukleare oder chemisch-biologische Waffen oder Waffen im Zusammenhang mit Flugkörpern zu verwenden. Weitere Informationen zum Export von Novell-Software finden Sie auf der Webseite "Novell International Trade Services" (http://www.novell.com/info/exports/). Novell übernimmt keine Verantwortung für das Nichteinholen notwendiger Exportgenehmigungen.

Novell, Inc. besitzt Anrechte auf geistiges Eigentum für Technologie, die in das in dieser Dokumentation beschriebene Produkt integriert ist. Diese Rechte auf geistiges Eigentum umfassen möglicherweise insbesondere ein oder mehrere Patente in den USA, die auf der Webseite "Legal Patents" von Novell (http://www.novell.com/company/legal/patents/) aufgeführt sind, sowie ein oder mehrere andere Patente oder laufende Patentanträge in den USA und in anderen Ländern.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online-Dokumentation: Die neueste Online-Dokumentation für dieses und andere Novell-Produkte finden Sie auf der Dokumentations-Webseite von Novell (http://www.novell.com/documentation).

Novell-Marken

Hinweise zu Novell-Marken finden Sie in der Novell Trademark and Service Mark-Liste (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materialien von Drittanbietern

Die Rechte für alle Marken von Drittanbietern liegen bei den jeweiligen Eigentümern.

Inhalt

Informationen zu diesem Handbuch

Dieses *Novell® ZENworks® Endpoint Security Management-Installationshandbuch* liefert eine umfassende Anleitung zur Installation der ZENworks Endpoint Security Management-Komponenten und hilft Administratoren beim Einrichten und Ausführen dieser Komponenten.

Die Informationen in diesem Handbuch gliedern sich wie folgt:

Zielgruppe

Dieses Handbuch wurde für die Administratoren von ZENworks Endpoint Security Management konzipiert.

Rückmeldungen

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation zu diesem Produkt. Sie können uns über die Funktion "Kommentare von Benutzern" im unteren Bereich jeder Seite der Online-Dokumentation oder auf der Website für Feedback zur Novell-Dokumentation (http://www.novell.com/documentation/feedback.html) Ihre Meinung mitteilen.

Zusätzliche Dokumentation

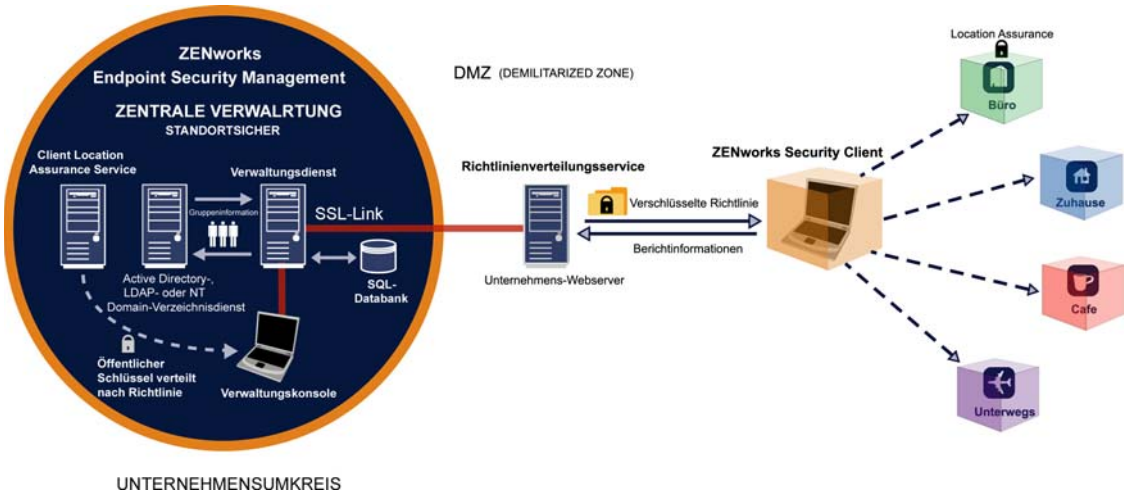
Im Lieferumfang von ZENworks Endpoint Security Management finden Sie weitere Dokumentationen (im PDF- und HTML-Format), die Informationen zum Produkt und zu dessen Installation beinhalten. Weitere Dokumentation finden Sie auf der Dokumentations-Website zu ZENworks Endpoint Security Management 3.5 (http://www.novell.com/documentation/zesm35).

ZENworks Endpoint Security Management Überblick

1

Novell® ZENworks® Endpoint Security Management besteht im Wesentlichen aus fünf funktionalen Komponenten: dem Richtlinienverteilungsservice, dem Verwaltungsdienst, der Verwaltungskonsole, dem Client Location Assurance Service und dem Endpoint Security Client. Die nachstehende Abbildung zeigt diese Komponenten innerhalb der Architektur:

Abbildung 1-1 *ZENworks Endpoint Security Management-Architektur*



Der Endpoint Security Client ist für die Einhaltung der verteilten Sicherheitsrichtlinien im Endgerätsystem verantwortlich. Wenn der Endpoint Security Client auf allen firmeninternen PCs installiert ist, können die Endgeräte den Firmenumkreis verlassen und sind dabei weiterhin gesichert. Für Endgeräte innerhalb der Firewall des Umkreises werden zusätzliche Sicherheitsprüfungen durchgeführt.

Jede Komponente der zentralen Verwaltung wird einzeln installiert (mit Ausnahme der Einzelserverinstallation). Weitere Informationen finden Sie in Kapitel 3, „Durchführen einer Einzelserverinstallation“, auf Seite 17.

Folgende Komponenten werden auf Servern installiert, die innerhalb des Firmenumkreises gesichert werden:

- **Richtlinienverteilungsservice:** Der Richtlinienverteilungsservice ist für die Verteilung von Sicherheitsrichtlinien an den Endpoint Security Client und den Abruf von Berichterstellungsdaten vom Endpoint Security Client zuständig. Der Richtlinienverteilungsservice kann außerhalb der firmeninternen Firewall in der DMZ bereitgestellt werden, um regelmäßige Richtlinienaktualisierungen für mobile Endgeräte zu gewährleisten.
- **Verwaltungsdienst:** Der Verwaltungsdienst ist für die Zuweisung von Benutzerrichtlinien und die Authentifizierung von Komponenten, den Abruf von Berichterstellungsdaten, die Erstellung und Verbreitung von ZENworks Endpoint Security Management-Berichten sowie die Erstellung und Speicherung von Sicherheitsrichtlinien zuständig.

- **Verwaltungskonsole:** Diese sichtbare Benutzeroberfläche wird direkt auf dem Server, der als Host für den Verwaltungsdienst festgelegt ist, oder auf einer Arbeitsstation ausgeführt, die sich innerhalb der firmeninternen Firewall befindet und mit dem Verwaltungsdienst-Server verbunden ist. Die Verwaltungskonsole dient der Konfiguration des Verwaltungsdiensts sowie der Verwaltung von Benutzer- und Gruppensicherheitsrichtlinien. Richtlinien werden mit der Verwaltungskonsole erstellt, kopiert, bearbeitet, verbreitet oder gelöscht.
- **Client Location Assurance Service:** Bietet eine kryptografische Garantie dafür, dass sich ein Endpoint Security Client an einem definierten Standort befindet, so wie es andere Parameter der Netzwerkumgebung anzeigen.

1.1 Systemvoraussetzungen

Server-Systemanforderungen	Systemanforderungen für Endpoint (Client)
Betriebssysteme: Microsoft&thrdmrk; Windows&thrdmrk; 2000 Server SP4 Microsoft Windows 2000 Advanced Server SP4 Windows 2003 Server **Prozessor:** Pentium&thrdmrk;3,0 GHz 4 HT (oder höher) mindestens 756 MB RAM (1 GB oder höher empfohlen) **Festplattenspeicher:** 500 MB: ohne lokale Microsoft SQL-Datenbank 5 GB: mit lokaler MS SQL-Datenbank (SCSI empfohlen) **Erforderliche Software:** Unterstütztes RDBMS (SQL Server Standard, SQL Server Enterprise, Microsoft SQL Server 2000 SP4, SQL 2005) Microsoft Internet Information Services (konfiguriert für SSL) Unterstützte Verzeichnisdienste (eDirectory™ oder Active Directory&thrdmrk;) .NET Framework 3.5 (nur für Server und Verwaltungskonsole) **Einzelplatz-Verwaltungskonsole:** Unterstütztes RDBMS (SQL Server Standard, SQL Server Enterprise, Microsoft SQL Server 2000 SP4, SQL 2005, SQL Express)	**Betriebssysteme:** Windows XP SP1 Windows XP SP2 Windows 2000 SP4 Windows Vista SP1 (32-Bit) Windows Server 2008 (32-Bit) **Prozessor:** 600 MHz Pentium 3 (oder höher) Minimum 128 MB RAM (256 MB oder mehr empfohlen **Festplattenspeicher:** 5 MB erforderlich, 5 zusätzliche MB für Berichterstellung erforderlich **Erforderliche Software:** Windows 3.1 Installationsprogramm Alle Windows-Updates müssen auf dem neuesten Stand sein.

Der Richtlinienverteilungsservice, die Verwaltungsdienste und der Client Location Assurance Service setzen die Aktivierung eines lokalen ASP.NET-Kontos (Version 2.0) voraus. Wenn dieses Konto deaktiviert ist, funktionieren die Dienste nicht richtig.

1.2 Info zu den ZENworks Endpoint Security Management-Handbüchern

Die Handbücher zu ZENworks Endpoint Security Management bieten drei Anleitungsebenen für die Benutzer des Produkts.

- *ESM-Installationshandbuch:* Dieses Handbuch stellt die vollständigen Installationsanweisungen für die ZENworks Endpoint Security Management-Komponenten zur Verfügung und bietet dem Administrator Hilfe für die Installation und Ausführung dieser Komponenten. Dieses Handbuch lesen Sie gerade.
- *ZENworks Endpoint Security Management-Administratorenhandbuch*: Dieses Handbuch richtet sich an die ZENworks Endpoint Security Management-Administratoren, die die Dienste verwalten, Sicherheitsrichtlinien für das Unternehmen erstellen, Berichterstellungsdaten generieren und analysieren und Endbenutzern bei der Fehlerbehebung behilflich sind. Anleitungen zu den genannten Aufgaben erhalten Sie in diesem Handbuch.
- *ZENworks Endpoint Security Client 3.5-Benutzerhandbuch*: Dieses Handbuch richtet sich an den Endbenutzer des Endpoint Security Client. Dieses Handbuch kann allen Mitarbeitern des Unternehmens zur Verfügung gestellt werden, um das Verständnis des Endpoint Security Client zu erleichtern.

Installation von ZENworks Endpoint Security Management

2

In den folgenden Abschnitten finden Sie weitere Informationen zur Installation von Novell® ZENworks® Endpoint Security Management:

2.1 Informationen vor der Installation

Die Installationssoftware für ZENworks Endpoint Security Management sollte zur Vermeidung unzulässigen oder unautorisierten Gebrauchs physikalisch geschützt sein. Administratoren sollten zudem die Richtlinien für Vorinstallation und Installation berücksichtigen, damit gewährleistet wird, dass das ZENworks Endpoint Security Management-System ohne Unterbrechungen arbeitet und nicht durch unzureichenden Hardwareschutz anfällig wird.

Der Administrator, der diese Software installiert, muss der primäre Administrator für die Server und die Domäne sein. Bei Verwendung von firmeninternen SSL-Zertifikaten muss derselbe Benutzername wie bei der Erstellung des SSL-Herkunftsverbürgungszertifikats verwendet werden.

2.2 Installationspakete

Wenn von der DVD aus installiert wird, wird ein Hauptinstallationsprogramm gestartet. Dafür wird eine einfache Benutzeroberfläche verwendet, die den ZENworks Endpoint Security Management-Administrator durch den Installationsvorgang leitet. Laden Sie einfach die Installations-DVD auf jedem Computer, um auf das Hauptinstallationsprogramm zuzugreifen und die gewünschten Komponenten zu installieren.

2.2.1 Info zum Hauptinstallationsprogramm

Beim Starten zeigt das Hauptinstallationsprogramm zwei Menüoptionen an: *Produkte* und *Dokumentation*

Über den Link *Produkte* wird das Installationsprogramm geöffnet. Mithilfe der Menüelemente in diesem Bildschirm starten Sie das für die einzelnen Komponenten festgelegte Installationsprogramm. Beim Endpoint Security Client 3.5 oder Endpoint Security Client 4.0 ist eine Zusatzoption verfügbar, mit der die Installation im Administrator-Modus gestartet werden kann. Diese hilft dem ZENworks Endpoint Security Management-Administrator beim Erstellen eines MSI-Pakets zur einfacheren Verteilung (siehe Kapitel 9.2, „MSI-Installation“, auf Seite 63).

Umfassende Informationen zur Verwendung der ZENworks Endpoint Security Management-Komponenten finden Sie im *ZENworks Endpoint Security Management-Administratorenhandbuch*, das über den Link *Dokumentation* erhältlich ist.

2.3 Installationsoptionen

ZENworks Endpoint Security Management-Backend-Komponenten können auf einem einzelnen oder auf mehreren Servern installiert werden. Einzelserverinstallationen eignen sich gut für kleinere Bereitstellungen, bei denen keine regelmäßigen Richtlinienaktualisierungen erforderlich sind. Eine Installation auf mehreren Servern wird für große Bereitstellungen empfohlen, bei denen regelmäßige Richtlinienaktualisierungen erforderlich sind. Wenden Sie sich an Novell Professional Services, um festzustellen, welcher Installationstyp für Sie am besten geeignet ist.

Der Endpoint Security Client kann (falls erforderlich) ohne Konnektivität zum Richtlinienverteilungsservice verwendet werden. Zu Evaluierungszwecken kann optional eine Einzelplatz-Verwaltungskonsole installiert werden. Die Installation für diesen unverwalteten Betriebsmodus wird unter Kapitel 11, „Installation von ZENworks Endpoint Security Management im unverwalteten Modus“, auf Seite 81 beschrieben.

2.4 Installationsreihenfolge

ZENworks Endpoint Security Management sollte in der nachstehend angegebenen Reihenfolge installiert werden:

1. Installation auf einem einzelnen oder auf mehreren Servern
   - Richtlinienverteilungsservice
   - Verwaltungsdienst
2. Verwaltungskonsole
3. Client Location Assurance Service
4. Endpoint Security Client 3.5 oder Endpoint Security Client 4.0

2.5 Vor der Installation von ZENworks Endpoint Security Management

Vor Beginn der Installation muss sich der ZENworks Endpoint Security Management-Administrator einige Fragen stellen:

Wie sollen die Benutzer die ZENworks Endpoint Security Management-Sicherheitsrichtlinien empfangen?

Die Optionen für die Richtlinienverteilung hängen davon ab, ob die Benutzer Richtlinienaktualisierungen überall empfangen können sollen, auch außerhalb des zentralen Netzwerks, oder ob sie diese nur empfangen können sollen, wenn sie sich in einem gesicherten Netzwerk befinden (oder mit einem solchen über VPN verbunden sind). Organisationen, die eine häufige Aktualisierung der ZENworks Endpoint Security Management-Sicherheitsrichtlinien planen, wird empfohlen, eine Installation auf mehreren Servern zu verwenden, die den Richtlinienverteilungsservice auf einem Webserver außerhalb der DMZ platziert.

Welche Serverbereitstellungen sind verfügbar?

Wenn Ihre Organisation nur über einige Server verfügt, müssen Sie·die·Installation möglicherweise auf einem Einzelserver bereitstellen. Wenn die Verfügbarkeit von Servern kein Problem darstellt, dann sollten Sie die Größe der Client-Bereitstellung und die Anzahl der Benutzer außerhalb der Firewall in Betracht ziehen.

Welche SQL Server-Bereitstellung ist für Sie verfügbar?

ZENworks Endpoint Security Management erstellt bei der Installation drei SQL-Datenbanken. Bei einer kleinen Bereitstellung kann eine einzelne SQL-Datenbank oder eine serverseitige Datenbank auf den Servern für die Richtlinienverteilung und den Verwaltungsdienst installiert werden. Bei größeren Bereitstellungen sollte ein eigener SQL-Datenbankserver für den Datenempfang vom Richtlinienverteilungsservice und dem Verwaltungsdienst eingesetzt werden. Zulässig sind nur folgende RDBMS-Typen:

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

Wenn es sich um eine benannte Instanz handelt, müssen die Server wie folgt konfiguriert werden:

Provider=sqloledb

Data Source=Servername\Instanzenname (dieser Definitionstyp ist für die Installation von ZENworks Endpoint Security Management erforderlich)

Initial Catalog=Datenbankname

User Id=Benutzername

Password=Passwort

Legen Sie SQL auf den gemischten Modus fest.

Bei der Installation darf als Benutzername und Passwort kein Domänenbenutzer verwendet werden. Es muss sich um einen SQL-Benutzer mit Systemadministratorrechten handeln.

Werden für die SSL-Kommunikation vorhandene Zertifikate oder eigensignierte Zertifikate von Novell verwendet?

Für Fälle von Disaster Recovery und/oder Failover-Designs wird empfohlen, eine firmeninterne oder eine andere Zertifizierungsstelle (VeriSign, GeoTrust, Thawte usw.) für die vollständige Bereitstellung von ZENworks Endpoint Security Management zu verwenden. Wenn Sie eigene Zertifikate verwenden, sollten das Webservice-Zertifikat und die Herkunftsverbürgungs-Zertifizierungsstelle auf dem Computer erstellt werden, der als Richtlinienverteilungsservice festgelegt ist, und anschließend an die entsprechenden Computer verteilt werden. Informationen zum Erstellen einer firmeninternen Zertifizierungsstelle finden Sie in den Schritt-für-Schritt-Anweisungen zum sicheren Einrichten einer Zertifizierungsstelle, die unter microsoft.com verfügbar sind.

Zu Evaluierungszwecken oder für kleine Bereitstellungen (unter 100 Benutzern) verfügt ZENworks Endpoint Security Management über eigensignierte Zertifikate. Wenn die Standardinstallation ausgeführt wird, werden SSL-Zertifikate von Novell auf den Servern installiert.

Wie sollen die Endpoint Security-Clients bereitgestellt werden?

Die Endpoint Security Client-Software kann für jedes Endgerät einzeln oder durch einen MSI-Push bereitgestellt werden. Anweisungen für die Erstellung eines MSI-Pakets finden Sie in Kapitel 9.2, „MSI-Installation“, auf Seite 63.

Sollen die Richtlinien computer- oder benutzerbasiert sein?

Richtlinien können an einen Einzelcomputer verteilt werden, sodass jeder angemeldete Benutzer dieselbe Richtlinie empfängt. Richtlinien können auch für einzelne Benutzer oder Gruppen festgelegt werden.

Für jede Installation gelten eine Reihe von Voraussetzungen. Es wird empfohlen, für jede Komponente die Checkliste mit den Voraussetzungen vor der Ausführung der Installation vollständig abzuarbeiten. Schlagen Sie diese Listen auf den folgenden Seiten nach:

- Kapitel 3, „Durchführen einer Einzelserverinstallation“, auf Seite 17
- Kapitel 5, „Durchführen der Installation des Richtlinienverteilungsservices“, auf Seite 23
- Kapitel 6, „Durchführen der Installation des Verwaltungsdienstes“, auf Seite 33
- Kapitel 7, „Durchführen der Installation der Verwaltungskonsole“, auf Seite 45
- Kapitel 8, „Installation des Client Location Assurance Services“, auf Seite 57
- Kapitel 9, „Installation von Endpoint Security Client 3.5“, auf Seite 61

Durchführen einer Einzelserverinstallation

3

Eine Einzelserverinstallation (SSI) von ZENworks® Endpoint Security Management ermöglicht die Koexistenz des Richtlinienverteilungsservices und des Verwaltungsdienstes auf demselben Server. (Dies ist ohne Verwendung dieser Installationsoption nicht möglich.) Aus Sicherheitsgründen muss der Server innerhalb der Firewall bereitgestellt werden. In diesem Fall dürfen Benutzer Richtlinienaktualisierungen nur zu empfangen, wenn sie sich innerhalb der Firmeninfrastruktur befinden oder per VPN verbunden sind.

Die Bereitstellung der Einzelserverinstallation auf einem PDC (Primärdomänencontroller) wird aus Gründen der Sicherheit und der Funktionalität nicht unterstützt.

Hinweis: Es wird empfohlen, den SSI-Server so zu konfigurieren (härten), dass alle Anwendungen, Dienste, Konten und andere Optionen, die für die vorgesehene Serverfunktionalität nicht benötigt werden, deaktiviert sind. Die dafür erforderlichen Schritte hängen von den Einzelheiten der lokalen Umgebung ab und lassen sich deshalb nicht vorausgreifend beschreiben. Administratoren sollten den entsprechenden Abschnitt der Microsoft Technet Sicherheitswebseite (http://www.microsoft.com/technet/security/default.mspx) nachschlagen. Weitere Empfehlungen für die Zugriffssteuerung finden Sie im *ZENworks Endpoint Security Management-Administratorenhandbuch*.

Wenn Sie den Zugriff auf verbürgte Computer begrenzen möchten, können das virtuelle Verzeichnis und IIS mit ACLs eingerichtet werden. Schlagen Sie folgende Artikel nach:

- Gewähren oder Verweigern des Zugriffs auf Computer (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- Site-Zugriff anhand von IP-Adresse oder Domänennamen beschränken (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- IIS-FAQ: Beschränkungen für 2000-IP-Adresse und Domänenname (http://www.iisfaq.com/default.aspx?View=A136&P=109)
- Arbeiten mit IIS-Paketfilterung (http://www.15seconds.com/issue/011227.htm)

Aus Sicherheitsgründen empfiehlt es sich, folgende Standardordner aus allen IIS-Installationen zu entfernen:

- `IISHelp`
- `IISAdmin`
- `Skripts`
- `Drucker`

Novell empfiehlt außerdem, das IIS-Lockdown-Werkzeug zu verwenden, das auf microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx) zur Verfügung steht.

Die Version 2.1 wird von den für die wichtigsten IIS-abhängigen Microsoft-Produkte bereitgestellten Schablonen gesteuert. Wählen Sie die Schablone, die der Funktion dieses Servers am besten entspricht. Im Zweifelsfall wird die Schablone "Dynamischer Webserver" empfohlen.

Vergewissern Sie sich bitte, dass folgende Voraussetzungen gegeben sind, bevor Sie mit der Installation beginnen:

- ❑ Stellen Sie sicher, dass Zugriff auf einen unterstützten Verzeichnisdienst besteht (eDirectory™, Active Directory oder NT Domänen). NT Domänen werden nur unterstützt, wenn der Einzelserverdienst auf einem Microsoft Windows 2000 Advanced Server (SP4) installiert ist.
- ❑ Vergewissern Sie sich, dass der Novell-Client™ auf dem Server installiert ist und sich korrekt bei eDirectory authentifizieren kann, wenn für die Bereitstellung ein eDirectory-Service verwendet wird. Erstellen Sie für die Verwaltungskonsolen-Authentifizierung ein Kontopasswort, das nicht geändert wird (siehe Abschnitt 7.2.1, „eDirectory Services hinzufügen“, auf Seite 49).
- ❑ Überprüfen Sie für die Servernamenauflösung vom Endpoint Security Client zu SSI, ob die Zielcomputer (auf denen der Endpoint Security Client installiert ist) Pings für den SSI-Servernamen senden können. Wenn dieser Vorgang nicht erfolgreich verläuft, müssen Sie das Problem lösen, bevor Sie mit der Installation fortfahren. (Ändern Sie den SSI-Servernamen in FQDN/NetBIOS, ändern Sie AD, damit FQDN/NetBIOS verwendet wird, ändern Sie die DNS-Konfigurationen, indem Sie die lokale Hostdatei auf den Zielcomputern so ändern, dass die richtigen MS-Informationen enthalten sind etc.)
- ❑ Aktivieren oder installieren Sie Microsoft Internetinformationsdienste (IIS) und konfigurieren Sie IIS so, dass SSL- (Secure Socket Layer) Zertifikate akzeptiert werden.

  Wichtig: Deaktivieren Sie auf der Seite "Sichere Kommunikation" das Kontrollkästchen *Sicherer Kanal (SSL) erforderlich*. Erweitern Sie dazu im Microsoft-Dienstprogramm "Computerverwaltung" den Knoten *Dienste und Anwendungen* > erweitern Sie *Internetinformationsdienste-Manager* > erweitern Sie *Websites* > klicken Sie mit der rechten Maustaste auf *Standardwebsite* > klicken Sie auf *Eigenschaften* > klicken Sie auf die Registerkarte *Verzeichnissicherheit* > und klicken Sie im Gruppenfeld "Sichere Kommunikation" auf die Schaltfläche *Bearbeiten*. Durch das Aktivieren dieser Option bricht die Kommunikation zwischen dem ZENworks Endpoint Security Management-Server und dem ZENworks Endpoint Security-Client auf dem Endgerät ab.

- ❑ Wenn Sie eigene SSL-Zertifikate verwenden, vergewissern Sie sich, dass das Webservice-Zertifikat und die Herkunftsverbürgungs-Zertifizierungsstelle auf dem Computer geladen sind und dass der in den vorhergehenden Schritten überprüfte Servername (NetBIOS oder FQDN) dem Wert *Ausgestellt für* für das in IIS konfigurierte Zertifikat entspricht.
- ❑ Wenn Sie eigene Zertifikate verwenden oder bereits ein eigensigniertes Zertifikat von Novell installiert haben, können Sie SSL auch überprüfen, indem Sie folgende URL von einem Computer aus eingeben, auf dem der Endpoint Security Client installiert ist: `https://SSI_SERVER_NAME/AuthenticationServer/UserService.asmx` (wobei *SSI_SERVER_NAME* der Servername ist). Es müssen gültige Daten (eine HTML-Seite) zurückgegeben werden, nicht Zertifikatswarnungen. Zertifikatswarnungen müssen vor der Installation gelöst werden (es sei denn, Sie entscheiden sich dafür, Novell Self Signed Certificates zu verwenden).
- ❑ Stellen Sie sicher, dass Zugriff auf ein unterstütztes RDBMS besteht (Microsoft SQL Server 2000 SP4, SQL Server Standard, SQL Server Enterprise). Legen Sie die Datenbank auf "Gemischter Modus" fest.

3.1 Installationsschritte

Klicken Sie im Hauptinstallationsprogramm auf *Einzelserverinstallation*. Diese Installation kombiniert die Installationen des Richtlinienverteilungsservices und des Verwaltungsdienstes. Weitere Informationen hierzu finden Sie unter Kapitel 5, „Durchführen der Installation des Richtlinienverteilungsservices“, auf Seite 23 und Kapitel 6, „Durchführen der Installation des Verwaltungsdienstes“, auf Seite 33.

Wie bei deren Einzelinstallation werden mit der *Standardeinstellung* die Standardwerte der Dienste und die eigensignierten SSL-Zertifikate von Novell installiert. Die *benutzerdefinierte Installation* ermöglicht es dem Administrator, Verzeichnispfade festzulegen und erlaubt die Verwendung von firmeneigenen Zertifizierungsstellen.

3.2 Starten des Service

Der kombinierte Verteilungsservice und Verwaltungsdienst startet direkt nach der Installation, ohne dass der Server neu gebootet werden muss. Mit der Konfigurationsfunktion der Verwaltungskonsole werden sowohl der Verteilungsservice als auch der Verwaltungsdienst verwaltet. Weitere Details finden Sie im *ZENworks Endpoint Security Management-Administratorenhandbuch*.

Wenn die Installation abgeschlossen ist, können auch die Verwaltungskonsole und der Client Location Assurance Service auf diesem Server installiert werden. Wenn Sie die Verwaltungskonsole auf einem gesonderten Computer installieren, kopieren Sie das gesamte Verzeichnis der ZENworks Endpoint Security Management-Setupdateien auf den Computer, der als Host für die Verwaltungskonsole festgelegt wurde.

Fahren Sie mit Kapitel 5, „Durchführen der Installation des Richtlinienverteilungsservices“, auf Seite 23 fort.

Durchführen einer Installation auf mehreren Servern

4

Eine Installation auf mehreren Servern wird für große Bereitstellungen empfohlen. Sie wird auch empfohlen, wenn der Richtlinienverteilungsservice außerhalb der firmeninternen Firewall platziert werden soll, damit die Benutzer regelmäßige Richtlinienaktualisierungen empfangen können, wenn sie sich außerhalb des Netzwerkperimeters befinden. Eine Installation auf mehreren Servern muss auf mindestens zwei Servern durchgeführt werden. Der Richtlinienverteilungsservice und der Verwaltungsdienst lassen sich nicht getrennt voneinander auf demselben Server installieren. Weitere Details finden Sie unter Kapitel 3, „Durchführen einer Einzelserverinstallation“, auf Seite 17 für die Option einer Einzelserverinstallation.

Die Installation auf mehreren Servern sollte mit der Installation des Richtlinienverteilungsservices auf einem gesicherten Server innerhalb oder außerhalb der firmeninternen Firewall beginnen. Weitere Informationen finden Sie unter Kapitel 5, „Durchführen der Installation des Richtlinienverteilungsservices“, auf Seite 23.

Nach der Installation des Richtlinienverteilungsservices sollte der Verwaltungsdienst installiert werden. Weitere Informationen finden Sie unter Kapitel 6, „Durchführen der Installation des Verwaltungsdienstes“, auf Seite 33.

Es wird empfohlen, die Verwaltungskonsole auch auf diesem Server zu installieren. Weitere Informationen finden Sie unter Kapitel 7, „Durchführen der Installation der Verwaltungskonsole“, auf Seite 45.

Fahren Sie mit Kapitel 5, „Durchführen der Installation des Richtlinienverteilungsservices“, auf Seite 23 fort.

Durchführen der Installation des Richtlinienverteilungsservices

5

Der Server, der als Host für den Richtlinienverteilungsservice von ZENworks® Endpoint Security Management festgelegt ist sollte für Ihre Benutzer immer erreichbar sein, ob im Netzwerk oder außen in der DMZ. Vergewissern Sie sich, dass die erforderliche Software vor der Installation auf dem Server installiert ist (siehe „Systemvoraussetzungen“ auf Seite 10). Notieren Sie sich den Servernamen, nachdem Sie den Server ausgewählt haben, und zwar sowohl den NetBIOS-Namen als auch den Fully Qualified Domain Name (FQDN).

Die Implementierung des Richtlinienverteilungsservices auf einem PDC (Primärdomänencontroller) wird aus Gründen der Sicherheit und der Funktionalität nicht unterstützt.

Hinweis: Es wird empfohlen, den SSI-Server so zu konfigurieren (härten), dass alle Anwendungen, Dienste, Konten und andere Optionen, die für die vorgesehene Serverfunktionalität nicht benötigt werden, deaktiviert sind. Die dafür erforderlichen Schritte hängen von den Einzelheiten der lokalen Umgebung ab und lassen sich deshalb nicht vorausgreifend beschreiben. Administratoren sollten den entsprechenden Abschnitt der Microsoft Technet Sicherheitswebseite (http://www.microsoft.com/technet/security/default.mspx) nachschlagen. Weitere Empfehlungen für die Zugriffssteuerung finden Sie im *ZENworks Endpoint Security Management-Administratorenhandbuch*.

Wenn Sie den Zugriff auf verbürgte Computer begrenzen möchten, können das virtuelle Verzeichnis und IIS mit ACLs eingerichtet werden. Schlagen Sie folgende Artikel nach:

- Gewähren oder Verweigern des Zugriffs auf Computer (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- Site-Zugriff anhand von IP-Adresse oder Domänennamen beschränken (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- IIS-FAQ: Beschränkungen für 2000-IP-Adresse und Domänenname (http://www.iisfaq.com/default.aspx?View=A136&P=109)
- Arbeiten mit IIS-Paketfilterung (http://www.15seconds.com/issue/011227.htm)

Aus Sicherheitsgründen empfiehlt es sich, folgende Standardordner aus allen IIS-Installationen zu entfernen:

- `IISHelp`
- `IISAdmin`
- `Skripts`
- `Drucker`

Novell empfiehlt außerdem, das IIS-Lockdown-Werkzeug zu verwenden, das auf microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx) zur Verfügung steht.

Die Version 2.1 wird von den für die wichtigsten IIS-abhängigen Microsoft-Produkte bereitgestellten Schablonen gesteuert. Wählen Sie die Schablone, die der Funktion dieses Servers am besten entspricht. Im Zweifelsfall wird die Schablone "Dynamischer Webserver" empfohlen.

Vergewissern Sie sich, dass folgende Voraussetzungen erfüllt sind, bevor Sie mit der Installation beginnen:

- Servernamenauflösung vom Verwaltungsdienst (MS) zu Richtlinienverteilungsservice (DS): Vergewissern Sie sich, dass der Zielcomputer, auf dem MS installiert werden soll, Pings für den DS-Servernamen senden kann (NetBIOS, wenn der DS innerhalb der Netzwerk-Firewall konfiguriert wird, FQDN bei Installation außerhalb in der DMZ).
- Bei Erfolg wird dieser Servername bei der Installation eingegeben. Wenn dieser Vorgang nicht erfolgreich verläuft, müssen Sie das Problem lösen, bevor Sie mit der Installation fortfahren.
- Servernamenauflösung vom Endpoint Security Client an DS: Überprüfen Sie, ob die Endgerät-Clients (auf denen der Endpoint Security Client installiert ist) Pings für den DS-Servernamen senden können. Wenn dieser Vorgang nicht erfolgreich verläuft, müssen Sie das Problem lösen, bevor Sie mit der Installation fortfahren.
- Aktivieren oder installieren Sie Microsoft Internetinformationsdienste (IIS), stellen Sie sicher, dass ASP.NET aktiviert ist, und konfigurieren Sie es so, dass SSL- (Secure Socket Layer) Zertifikate akzeptiert werden.

  Wichtig: Deaktivieren Sie auf der Seite "Sichere Kommunikation" das Kontrollkästchen *Sicherer Kanal (SSL) erforderlich*. Erweitern Sie dazu im Dienstprogramm "Microsoft Computer Management" *Dienste und Anwendungen* > erweitern Sie *Internetinformationsdienste-Manager* > erweitern Sie *Websites* > klicken Sie mit der rechten Maustaste auf *Standardwebsite* > klicken Sie auf *Eigenschaften* > klicken Sie auf die Registerkarte *Verzeichnissicherheit* > und klicken Sie im Gruppenfeld "Sichere Kommunikation" auf die Schaltfläche *Bearbeiten*. Durch das Aktivieren dieser Option bricht die Kommunikation zwischen dem ZENworks Endpoint Security Management-Server und dem ZENworks Endpoint Security-Client auf dem Endgerät ab.

- Wenn Sie eigene SSL-Zertifikate verwenden, vergewissern Sie sich, dass das Webservice-Zertifikat auf dem Computer geladen ist und dass der in den vorhergehenden Schritten überprüfte Servername (NetBIOS oder FQDN) dem Wert *Ausgestellt für* für das in IIS konfigurierte Zertifikat entspricht.
- Wenn Sie eigene SSL-Zertifikate verwenden, überprüfen Sie die SSL vom MS-Server zum DS-Server: Öffnen Sie einen Webbrowser im Verwaltungsdienst und geben Sie folgende URL ein: `https://`*`DSNAME`* (wobei *DSNAME* der Servername des DS ist). Es müssen gültige Daten zurückgegeben werden, nicht Zertifikatswarnungen ("Diese Seite befindet sich im Aufbau" zählt zu den gültigen Daten). Zertifikatswarnungen müssen vor der Installation gelöst werden (es sei denn, Sie entscheiden sich dafür, Novell Self Signed Certificates zu verwenden).
- Stellen Sie sicher, dass Zugriff auf ein unterstütztes RDBMS besteht (Microsoft SQL Server 2000 SP4, SQL Server Standard, SQL Server Enterprise, SQL Server 2005). Legen Sie die Datenbank auf "Gemischter Modus" fest. Der Host für diese Datenbank sollte der Verwaltungsdienst-Server oder ein gemeinsam genutzter Server sein, der hinter der firmeninternen Firewall gesichert ist.

5.1 Installationsschritte

Klicken Sie im Installationsmenü auf *Richtlinienverteilungsservice*. Die Installation des Richtlinienverteilungsservices wird gestartet.

Beim Start überprüft das Installationsprogramm, ob die erforderliche Software auf dem Server vorhanden ist. Wenn Programme fehlen, werden diese automatisch installiert, bevor die Installation mit dem Begrüßungsbildschirm fortgesetzt wird (möglicherweise müssen Lizenzvereinbarungen für die Zusatzsoftware akzeptiert werden). Falls Microsoft Data Access Components (MDAC) 2.8 installiert werden muss, muss der Server nach dessen Installation neu booten, bevor die Installation von ZENworks Endpoint Security Management fortgesetzt werden kann. Wenn Windows 2003 Server verwendet wird, wird ASP.NET 2.0 vom Installationsprogramm so konfiguriert, dass es ausgeführt wird.

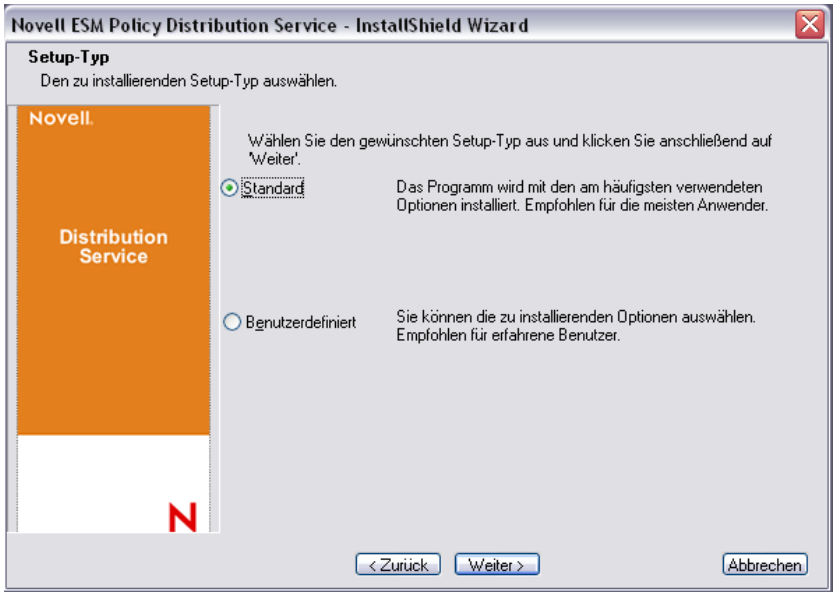
Führen Sie zu Beginn der Installation des Richtlinienverteilungsservices folgende Schritte aus:

Hinweis: Die folgenden Schritte umreißen, was sie als Benutzer tun müssen, um den Installationsvorgang abzuschließen. Interne Prozesse werden während des gesamten Installationsvorgangs angezeigt und hier nicht dokumentiert, solange keine bestimmten Aktionen oder Informationen vorliegen, die für eine erfolgreiche Installation erforderlich sind.

---

1. Klicken Sie zum Fortfahren im Begrüßungsbildschirm auf *Weiter*.
2. Akzeptieren Sie den Lizenzvertrag und klicken Sie dann auf *Weiter*.
3. Wählen Sie die Installationsoption *Standard* oder *Benutzerdefiniert*.

Abbildung 5-1 *Wählen Sie die Installationsoption "Standard" oder "Benutzerdefiniert".*



Beide Installationspfade werden unten beschrieben:

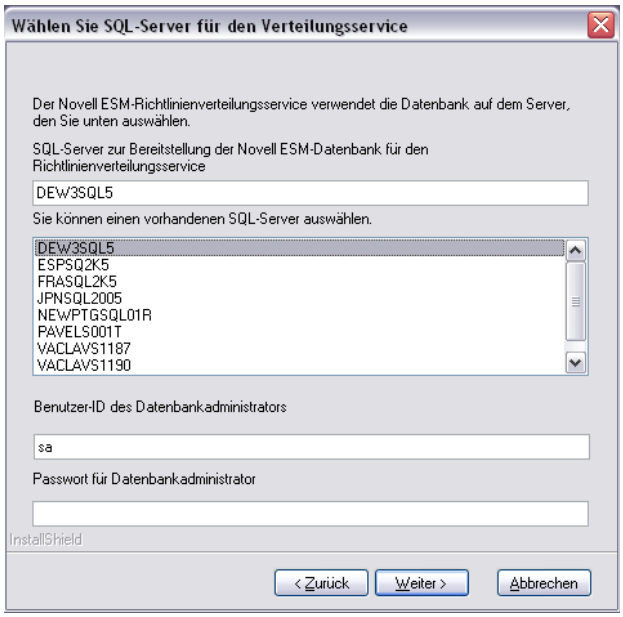
- Abschnitt 5.1.1, „Standardinstallation“, auf Seite 26
- Abschnitt 5.1.2, „Benutzerdefinierte Installation“, auf Seite 28

5.1.1 Standardinstallation

Die Standardinstallation platziert die Softwaredateien des Richtlinienverteilungsservices im Standardverzeichnis: `\Programme\Novell\ESM Policy Distribution Service`. Der SQL-Datenbankname STDSDB wird zugewiesen. Die drei SQL-Datenbankdateien (Daten, Index und Protokoll) werden in folgendem Verzeichnis platziert: `\Programme\Microsoft SQL Server\mssql\Data`.

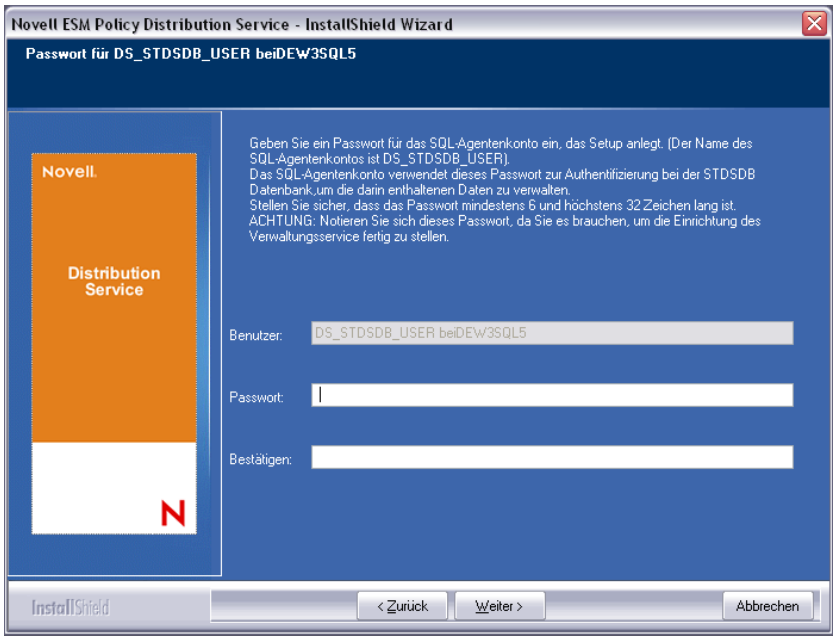
1. Für die Installation werden Novell SSL-Zertifikate erstellt. Verwenden Sie die benutzerdefinierte Installation, wenn Sie eigene SSL-Zertifikate verwenden möchten. Diese Zertifikate müssen an alle Endbenutzer verteilt werden.
2. Das Installationsprogramm erkennt die auf dem Computer und im Netzwerk verfügbaren SQL-Datenbanken. Wählen Sie eine gesicherte SQL-Datenbank für den Richtlinienverteilungsservice und geben Sie den Namen und das Passwort des Datenbank-Administrators ein (wenn das Passwort aus null Zeichen besteht, warnt das Installationsprogramm vor einem möglichen Sicherheitsproblem). Benutzername und Passwort dürfen kein Domänenbenutzer sein. Es muss sich um einen SQL-Benutzer mit Systemadministratorrechten handeln.

Abbildung 5-2 *SQL Server auswählen*



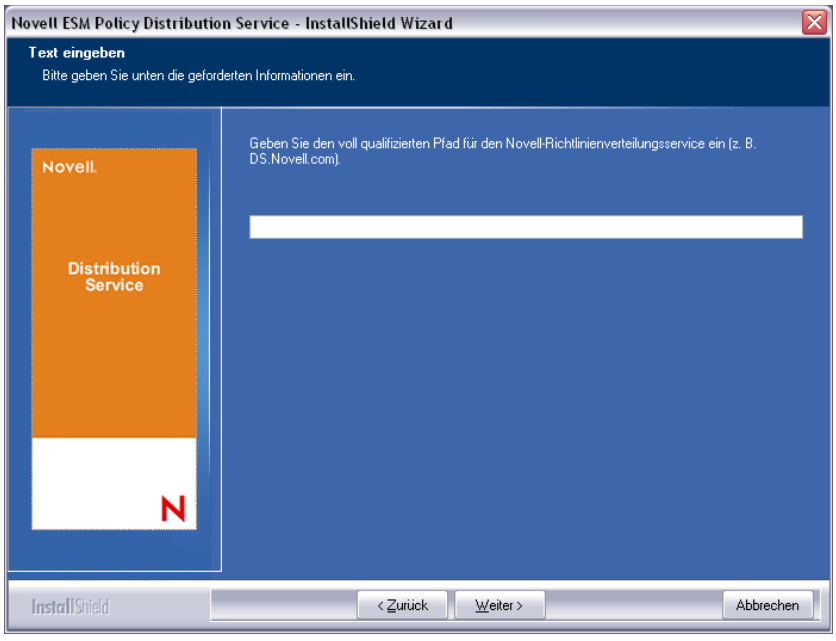
3. Geben Sie das Passwort für den Richtlinienverteilungsservice-Agenten ein. Dieser Benutzername und das Passwort werden vom Service für die Anmeldung bei der SQL-Datenbank verwendet.

Abbildung 5-3 *SQL-Passwort des Richtlinienverteilungsservices*



4 Geben Sie den Domänennamen des Richtlinienverteilungsservices ein. Dabei muss es sich um den FQDN handeln, wenn der Server sich außerhalb der Firmenfirewall befindet. Andernfalls ist nur der NetBIOS-Name für den Server erforderlich.

Abbildung 5-4 *Geben Sie den Domänennamen des Richtlinienverteilungsservices ein.*



5 Klicken Sie im Bildschirm "Dateien kopieren" auf *Weiter*, um mit der Installation zu beginnen.

6 Im Installationsverzeichnis wird ein Ordner für die `ESM-Setupdateien` erstellt. Dieser Ordner enthält eine `Setup-ID-Datei` sowie die Datei `ESM-DS.cer` (eigensigniertes SSL-Zertifikat von Novell), die für den Verwaltungsdienst erforderlich ist. Kopieren Sie diese Datei

direkt auf den Computer, der als Host für den Verwaltungsdienst festgelegt ist, per Netzwerkfreigabe oder indem Sie die Datei auf einer Festplatte oder einem Thumb-Laufwerk speichern und es manuell in das Installationsverzeichnis des Servers laden.

7 Der Richtlinienverteilungsservice ist jetzt installiert. Klicken Sie auf *Fertig stellen*, um das Installationsprogramm zu schließen und die Leistungsüberwachung zu starten.

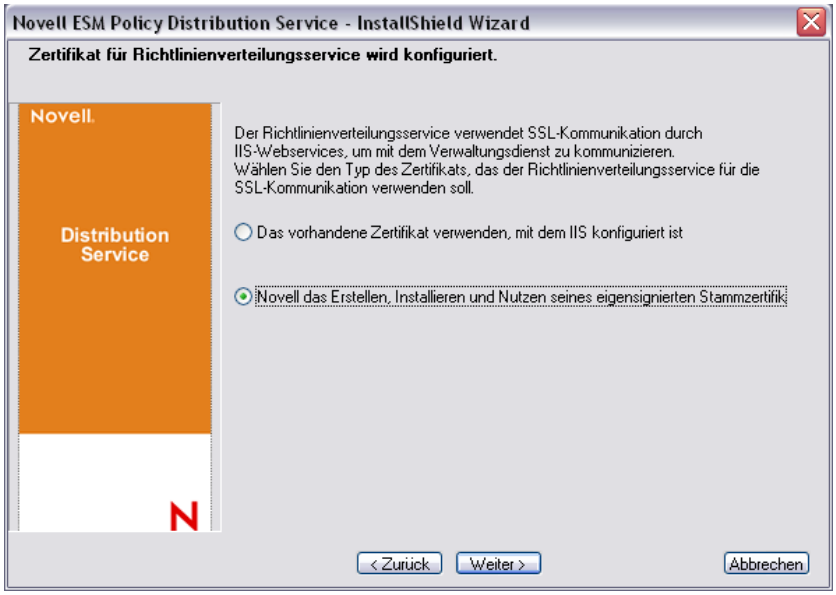
5.1.2 Benutzerdefinierte Installation

Die benutzerdefinierte Installation zeigt die für die Standardinstallation verwendeten Standardwerte an und erlaubt es dem Administrator, ein anderes Verzeichnis einzugeben oder zu suchen, um die Softwaredateien zu platzieren.

Der Administrator kann zwischen der Installation eines eigenen oder eines eigensignierten SSL-Zertifikats von Novell wählen.

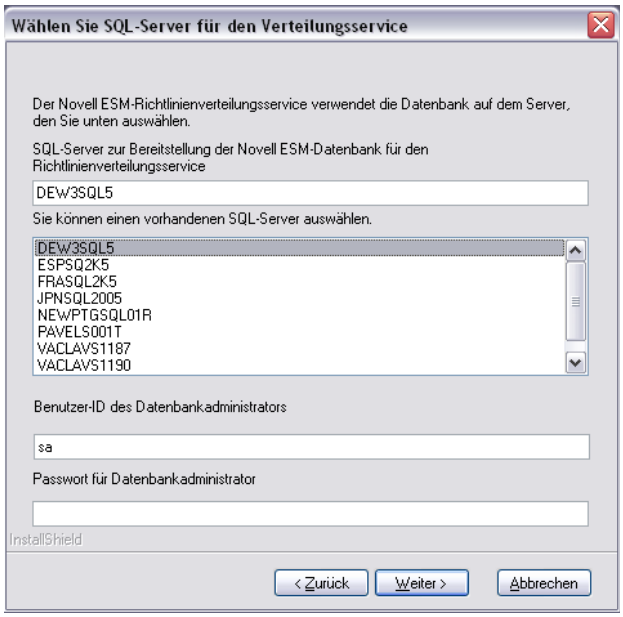
1 Ein SSL-Zertifikat ist für die sichere Kommunikation zwischen dem Richtlinienverteilungsservice und dem·Verwaltungsdienst sowie dem Verteilungsservice (DS) und allen Novell Security Clients erforderlich. Wenn Sie bereits über eine Zertifizierungsstelle verfügen, klicken Sie auf *Das vorhandene Zertifikat verwenden, für das IIS konfiguriert ist*. Wenn Sie ein Zertifikat benötigen, klicken Sie auf *Novell die Erstellung, Installation und Verwendung eines eigenen eigensignierten Herkunftsverbürgungszertifikats erlauben*. Das Installationsprogramm erstellt die Zertifikate und die signierende Zertifizierungsstelle. Unabhängig vom Zertifikatstyp müssen diese Zertifikate an alle Endbenutzer verteilt werden.

Abbildung 5-5 *Herkunftsverbürgungen einrichten*



2 Das Installationsprogramm erkennt die auf dem Computer und im Netzwerk verfügbaren SQL-Datenbanken. Wählen Sie die gesicherte SQL-Datenbank für den Richtlinienverteilungsservice und geben Sie den Namen und das Passwort des Datenbank-Administrators ein (wenn das Passwort aus null Zeichen besteht, warnt das Installationsprogramm vor einem möglichen Sicherheitsproblem). Benutzername und Passwort dürfen kein Domänenbenutzer sein. Es muss sich um einen SQL-Benutzer mit Systemadministratorrechten handeln.

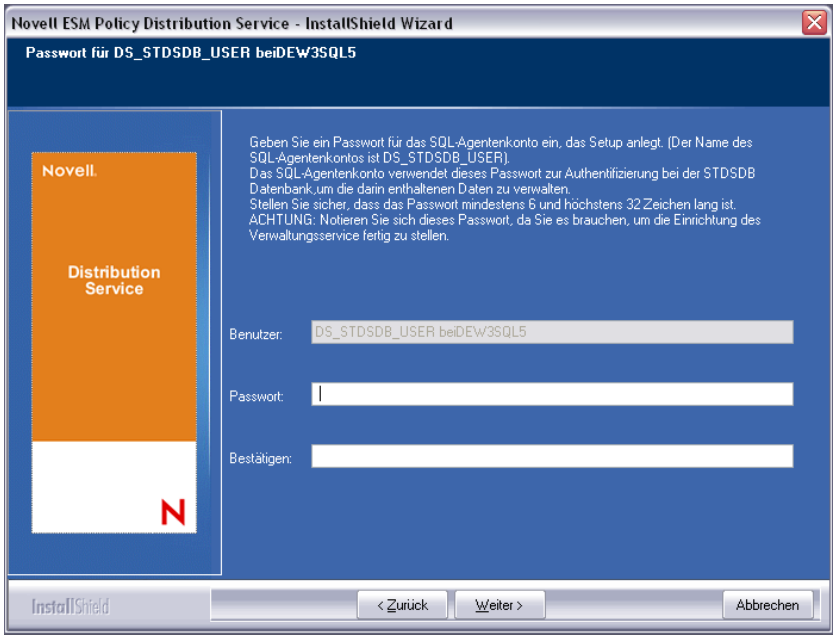
Abbildung 5-6 *SQL Server auswählen*



3 Legen Sie den Namen für die Datenbank fest·(standardmäßig ist STDSDB eingegeben).

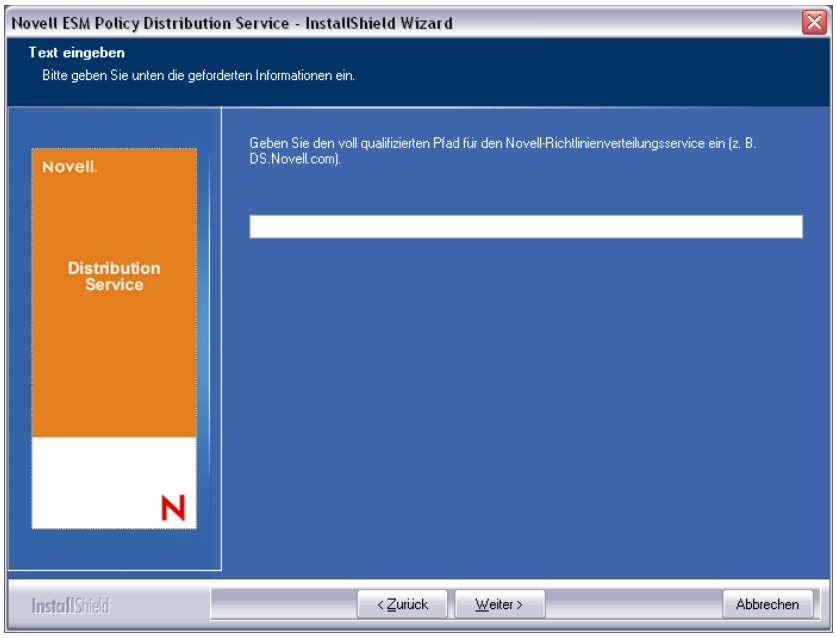
4 Geben Sie das Passwort für den Richtlinienverteilungsservice-Agenten ein. Dieser Benutzername und das Passwort werden vom Service für die Anmeldung bei der SQL-Datenbank verwendet.

Abbildung 5-7 *SQL-Passwort des Richtlinienverteilungsservices*



5 Geben Sie den Domänennamen des Richtlinienverteilungsservices ein. Dabei muss es sich um den FQDN handeln, wenn der Server sich außerhalb der Firmenfirewall befindet. Andernfalls ist nur der NetBIOS-Name für den Server erforderlich.

Abbildung 5-8 *Geben Sie den Domänennamen des Richtlinienverteilungsservices ein.*



6 Klicken Sie im Bildschirm "Dateien kopieren" auf *Weiter*, um mit der Installation zu beginnen.

7 Wählen Sie die Dateipfade für die Daten-, Index- und Protokolldateien aus.

8 Im Installationsverzeichnis wird ein Ordner für die `ESM-Setupdateien` erstellt. Dieser Ordner enthält eine `Setup-ID-Datei` sowie die Datei `ESM-DS.cer` (eigensigniertes SSL-Zertifikat von Novell), die für den Verwaltungsdienst erforderlich ist. Verwenden Sie "Durchsuchen", um den Speicherort dieser Datei auf dem Server zu bestimmen·(Standardverzeichnis = Installationsverzeichnis).

Abbildung 5-9 *Setupdateien speichern*

9 Wenn Sie sich für die Verwendung eines firmeninternen SSL-Zertifikats entscheiden, platzieren Sie eine Kopie dieser Datei im Ordner der `ESM-Setupdateien`.

10 Kopieren Sie den kompletten Ordner der `ESM-Setupdateien` direkt auf den Computer, der als Host für den Verwaltungsdienst festgelegt ist, über Netzwerkfreigabe oder indem Sie die Datei auf einer Festplatte oder einem Thumb-Laufwerk speichern und es manuell in das Installationsverzeichnis des Servers laden.

11 Der Richtlinienverteilungsservice ist jetzt installiert. Klicken Sie auf *Fertig stellen*, um das Installationsprogramm zu schließen und die Leistungsüberwachung zu starten.

5.2 Starten des Service

Der Richtlinienverteilungsservice startet direkt nach der Installation, ohne dass der Server neu gebootet werden muss. Mit der Verwaltungskonsole werden die Heraufladezeiten für den Richtlinienverteilungsservice angepasst. Dafür wird das Konfigurationswerkzeug verwendet. Weitere Details finden Sie im *ZENworks Endpoint Security Management-Administratorenhandbuch*.

Fahren Sie mit Kapitel 6, „Durchführen der Installation des Verwaltungsdienstes“, auf Seite 33 fort.

Durchführen der Installation des Verwaltungsdienstes

6

Der Verwaltungsdienst sollte auf einem sicheren Server hinter der Firewall installiert werden und kann nicht auf demselben Server wie der Richtlinienverteilungsservice installiert werden. (mit Ausnahme der Einzelserverinstallation, siehe Kapitel 3, „Durchführen einer Einzelserverinstallation“, auf Seite 17). Der Verwaltungsdienst sollte aus Sicherheitsgründen nicht außerhalb der Netzwerkfirewall installiert werden. Notieren Sie sich den Servernamen, nachdem Sie den Server ausgewählt haben, und zwar sowohl den NetBIOS-Namen als auch den Fully Qualified Domain Name (FQDN). Die Bereitstellung des·Verwaltungsdienst auf einem PDC (Primärdomänencontroller) wird aus Gründen der Sicherheit und der Funktionalität nicht unterstützt.

Hinweis: Es wird empfohlen, den SSI-Server so zu konfigurieren (härten), dass alle Anwendungen, Dienste, Konten und andere Optionen, die für die vorgesehene Serverfunktionalität nicht benötigt werden, deaktiviert sind. Die dafür erforderlichen Schritte hängen von den Einzelheiten der lokalen Umgebung ab und lassen sich deshalb nicht vorausgreifend beschreiben. Administratoren sollten den entsprechenden Abschnitt der Microsoft Technet Sicherheitswebseite (http://www.microsoft.com/technet/security/default.mspx) nachschlagen. Weitere Empfehlungen für die Zugriffssteuerung finden Sie im *ZENworks Endpoint Security Management-Administratorenhandbuch*.

Wenn Sie den Zugriff auf verbürgte Computer begrenzen möchten, können das virtuelle Verzeichnis und IIS mit ACLs eingerichtet werden. Schlagen Sie folgende Artikel nach:

- Gewähren oder Verweigern des Zugriffs auf Computer (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- Site-Zugriff anhand von IP-Adresse oder Domänennamen beschränken (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- IIS-FAQ: Beschränkungen für 2000-IP-Adresse und Domänenname (http://www.iisfaq.com/default.aspx?View=A136&P=109)
- Arbeiten mit IIS-Paketfilterung (http://www.15seconds.com/issue/011227.htm)

Aus Sicherheitsgründen empfiehlt es sich, folgende Standardordner aus allen IIS-Installationen zu entfernen:

- `IISHelp`
- `IISAdmin`
- `Skripts`
- `Drucker`

Novell empfiehlt außerdem, das IIS-Lockdown-Werkzeug zu verwenden, das auf microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx) zur Verfügung steht.

Die Version 2.1 wird von den für die wichtigsten IIS-abhängigen Microsoft-Produkte bereitgestellten Schablonen gesteuert. Wählen Sie die Schablone, die der Funktion dieses Servers am besten entspricht. Im Zweifelsfall wird die Schablone "Dynamischer Webserver" empfohlen.

Vergewissern Sie sich bitte, dass folgende Voraussetzungen gegeben sind, bevor Sie mit der Installation beginnen:

- ❑ Stellen Sie sicher, dass Zugriff auf einen unterstützten Verzeichnisdienst besteht (eDirectory, Active Directory oder NT Domänen*). * = Wird nur unterstützt, wenn der Verwaltungsdienst auf einem Windows 2000 Advanced Server (SP4) installiert ist.
- ❑ Vergewissern Sie sich, dass der Novell-Client™ auf dem Server installiert ist und sich korrekt bei eDirectory authentifizieren kann, wenn für die Bereitstellung ein eDirectory™-Service verwendet wird. Erstellen Sie für die Verwaltungskonsolen-Authentifizierung ein Kontopasswort, das nicht geändert wird (siehe Abschnitt 7.2.1, „eDirectory Services hinzufügen“, auf Seite 49).
- ❑ Überprüfen Sie für die Servernamenauflösung vom Endpoint Security Client zum Verwaltungsdienst (MS), ob die Zielcomputer (auf denen der Endpoint Security Client installiert werden soll) Pings für den MS-Servernamen senden können. Bei Erfolg wird dieser Wert bei der Installation eingegeben. Wenn dieser Vorgang nicht erfolgreich verläuft, müssen Sie das Problem lösen, bevor Sie mit der Installation fortfahren.
- ❑ Aktivieren oder installieren Sie Microsoft Internetinformationsdienste (IIS), stellen Sie sicher, dass ASP.NET aktiviert ist, und konfigurieren Sie es so, dass SSL-Zertifikate (Secure Socket Layer) akzeptiert werden.

  Wichtig: Deaktivieren Sie auf der Seite "Sichere Kommunikation" das Kontrollkästchen *Sicherer Kanal (SSL) erforderlich*. Erweitern Sie dazu im Dienstprogramm "Microsoft Computer Management" *Dienste und Anwendungen* > erweitern Sie *Internetinformationsdienste-Manager* > erweitern Sie *Websites* > klicken Sie mit der rechten Maustaste auf *Standardwebsite* > klicken Sie auf *Eigenschaften* > klicken Sie auf die Registerkarte *Verzeichnissicherheit* > und klicken Sie im Gruppenfeld "Sichere Kommunikation" auf die Schaltfläche *Bearbeiten*. Durch das Aktivieren dieser Option bricht die Kommunikation zwischen dem ZENworks Endpoint Security Management-Server und dem ZENworks Endpoint Security-Client auf dem Endgerät ab.

- ❑ Wenn Sie eigene SSL-Zertifikate verwenden, vergewissern Sie sich, dass die Herkunftsverbürgungs-Zertifizierungsstelle auf dem Computer geladen ist und dass der in den vorhergehenden Schritten überprüfte Servername (NetBIOS oder FQDN) dem Wert *Ausgestellt für* für das in IIS konfigurierte Zertifikat entspricht.
- ❑ Wenn Sie eigene Zertifikate verwenden oder bereits ein eigensigniertes Zertifikat von Novell installiert haben, können Sie die SSL auch überprüfen, indem Sie folgende URL von einem Computer aus eingeben, auf dem der Endpoint Security Client installiert ist: `https://MS_SERVER_NAME/AuthenticationServer/UserService.asmx` (wobei *MS_SERVER_NAME* der Servername ist). Es müssen gültige Daten (eine HTML-Seite) zurückgegeben werden, nicht Zertifikatswarnungen. Alle Zertifikatswarnungen müssen vor der Installation gelöst werden.
- ❑ Stellen Sie sicher, dass Zugriff auf ein unterstütztes RDBMS besteht (Microsoft SQL Server 2000 SP4, SQL Server Standard, SQL Server Enterprise, SQL 2005). Legen Sie die Datenbank·auf "Gemischter Modus" fest.
- ❑ Kopieren Sie das Verzeichnis `ESM Setupdateien` in das Installationsverzeichnis dieses Servers. Dieser Ordner enthält die Richtlinienverteilungsservice-Setup-ID und das SSL-Herkunftsverbürgungszertifikat für den Richtlinienverteilungsservice.

6.1 Installationsschritte

Klicken Sie im Installationsmenü auf *Installation des Verwaltungsdienstes*. Die Installation des Verwaltungsdienstes beginnt.

Beim Start überprüft das Installationsprogramm, ob die erforderliche Software auf dem Server vorhanden ist. Wenn Programme fehlen, werden diese automatisch installiert, bevor die Installation mit dem Begrüßungsbildschirm fortgesetzt wird (möglicherweise müssen Lizenzvereinbarungen für die Zusatzsoftware akzeptiert werden). Falls Microsoft Data Access Components (MDAC) 2.8 installiert werden muss, muss der Server nach dessen Installation neu booten, bevor die Installation von ZENworks Endpoint Security Management fortgesetzt werden kann. Wenn Windows 2003 Server verwendet wird, wird ASP.NET 2.0 vom Installationsprogramm so konfiguriert, dass es ausgeführt wird.

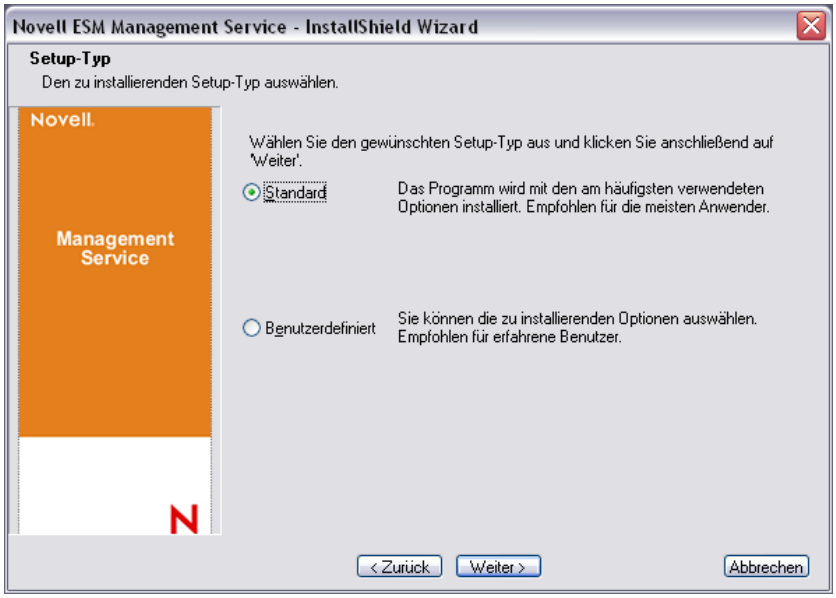
Führen Sie folgende Schritte aus, wenn die Installation des Verwaltungsdienstes beginnt:

Hinweis: Die folgenden Schritte umreißen, was sie als Benutzer tun müssen, um den Installationsvorgang abzuschließen. Interne Prozesse werden während des gesamten Installationsvorgangs angezeigt und hier nicht dokumentiert, solange keine bestimmten Aktionen oder Informationen vorliegen, die für eine erfolgreiche Installation erforderlich sind.

---

1. Klicken Sie zum Fortfahren im Begrüßungsbildschirm auf *Weiter*.
2. Akzeptieren Sie den Lizenzvertrag und klicken Sie dann auf *Weiter*.
3. Wählen Sie die Installationsoption *Standard* oder *Benutzerdefiniert*.

Abbildung 6-1 *"Standard" oder "Benutzerdefiniert" wählen*



Beide Installationspfade werden unten beschrieben:

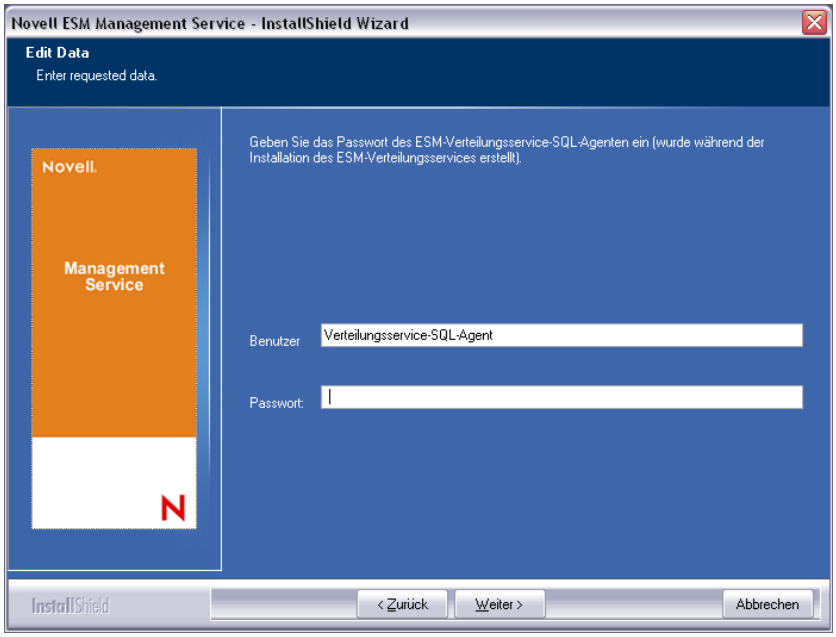
- Abschnitt 6.1.1, „Standardinstallation“, auf Seite 36
- Abschnitt 6.1.2, „Benutzerdefinierte Installation“, auf Seite 39

6.1.1 Standardinstallation

Die Standardinstallation platziert die Softwaredateien des Verwaltungsdienstes im Standardverzeichnis: `\Programme\Novell\ESM Management Service`. Der SQL-Datenbankname STMSDB wird zugewiesen. Die drei SQL-Datenbankdateien (Daten, Index und Protokoll) werden in folgendem Verzeichnis platziert: `\Programme\Microsoft SQL Server\mssql\Data`.

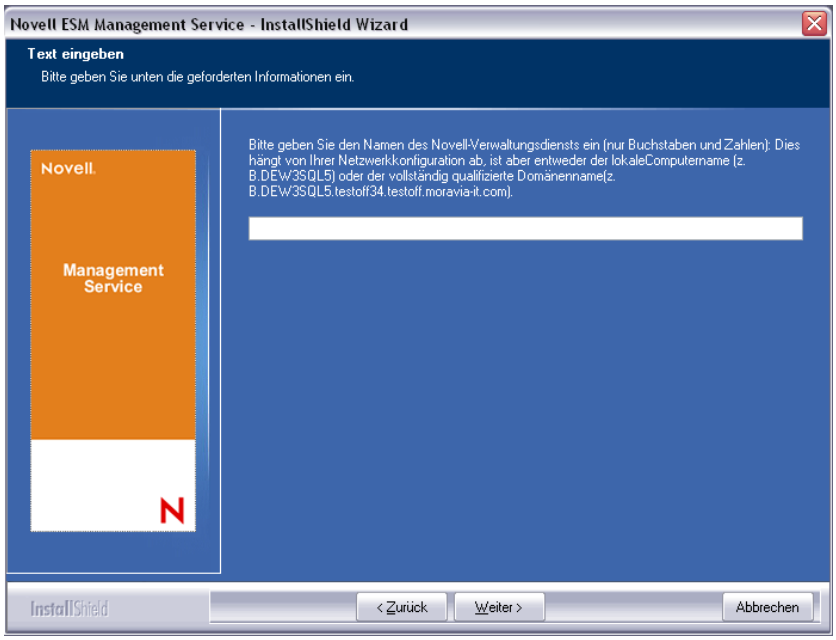
1 Geben Sie das Passwort für den Richtlinienverteilungsservice-Agenten ein, das bei der Installation des Richtlinienverteilungsservices erstellt wurde.

Abbildung 6-2 *SQL-Passwort eingeben*



2 Geben Sie den Namen des Servers ein, der als Host für den Verwaltungsdienst festgelegt werden soll.

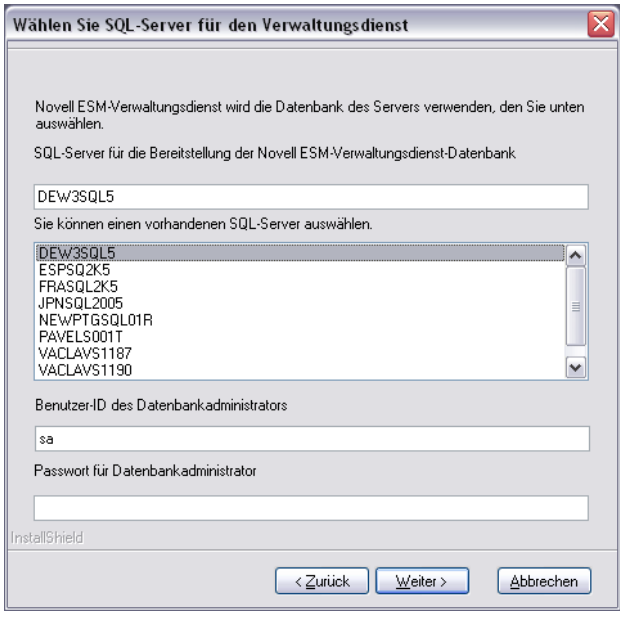
Abbildung 6-3 *MS-Servernamen eingeben*



3 Für die Installation werden Novell SSL-Zertifikate erstellt. Verwenden Sie die benutzerdefinierte Installation, wenn Sie eigene SSL-Zertifikate verwenden möchten. Diese Zertifikate müssen an alle Endbenutzer verteilt werden.

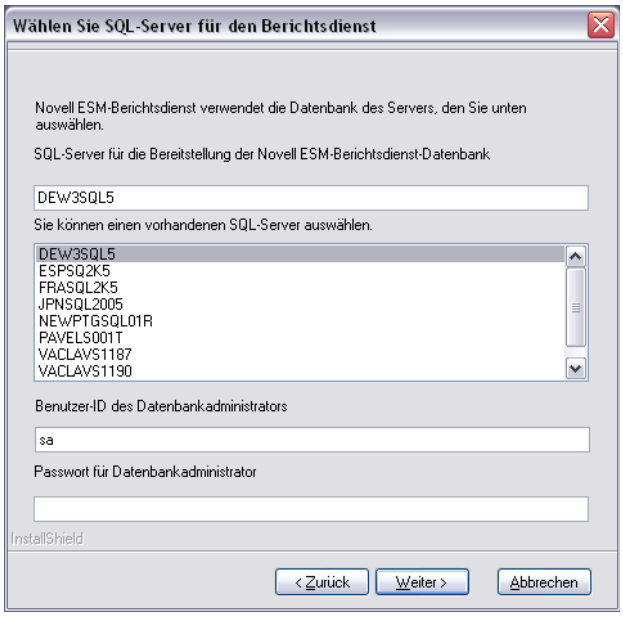
4 Das Installationsprogramm erkennt die auf dem Computer und im Netzwerk verfügbaren SQL-Datenbanken. Wählen Sie die SQL-Datenbank für den Richtlinienverteilungsservice und geben Sie den Benutzernamen und das Passwort des Datenbank-Administrators ein (wenn das Passwort aus null Zeichen besteht, warnt das Installationsprogramm vor einem möglichen Sicherheitsproblem). Benutzername und Passwort dürfen kein Domänenbenutzer sein. Es muss sich um einen SQL-Benutzer mit Systemadministratorrechten handeln.

Abbildung 6-4 *MS SQL-Datenbank auswählen*



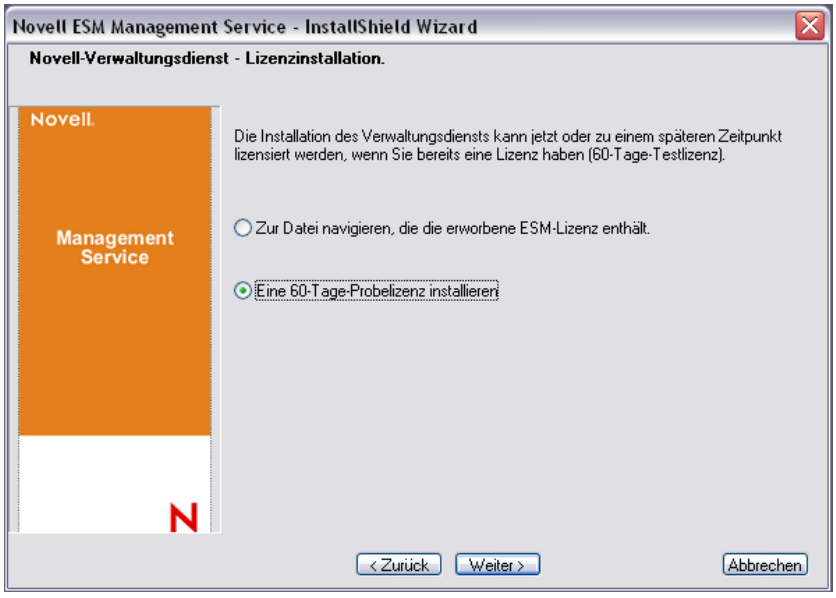
5 Wählen Sie die SQL-Datenbank für den Berichterstellungsservice aus und geben Sie den Benutzernamen und das Passwort des Administrators dieser Datenbank ein. Wenn Sie eine große Anzahl an Berichten umleiten und speichern möchten, wird empfohlen, der Datenbank für den Berichterstellungsservice einen eigenen SQL-Server zuzuordnen.

Abbildung 6-5 *Datenbank für den Berichterstellungsservice auswählen*



6 Wenn ZENworks Endpoint Security Management bereits erworben wurde, wird eine gesonderte Lizenzdatei geliefert. Kopieren Sie die Lizenzdatei auf diesen Server und durchsuchen Sie diesen nach der Datei (weitere Details finden sie auf der Ihrer Lizenzdatei zugehörigen Anweisungsseite). Wenn Sie noch keine ZENworks Endpoint Security Management-Lizenz erworben haben, wählen Sie *Evaluierungslizenz für 60 Tage*, um fortzufahren.

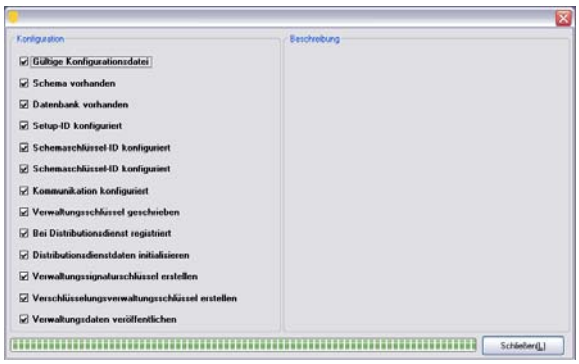
Abbildung 6-6 *Novell-Lizenzdatei suchen*



7 Klicken Sie im Bildschirm "Dateien kopieren" auf *Weiter*, um mit der Installation zu beginnen.

8 Der Verwaltungsdienst führt eine Kommunikationsprüfung für beide SQL-Datenbanken und den Richtlinienverteilungsservice aus. Wenn keine Kommunikation bestätigt wird, erhalten Sie eine Fehlermeldung. Für eine erfolgreiche Installation müssen alle Kontrollkästchen markiert sein.

Abbildung 6-7 *Kommunikationsprüfung*



9 Überspringen Sie die Schritte Schritt 10 und Schritt 11, wenn Sie eDirectory als Verzeichnisdienst verwenden.

10 Wenn die Installation auf einem Mitgliedserver für eine Domäne mit einem Active Directory- oder NT Domänen-Verzeichnisdienst durchgeführt wird, erkennt das Installationsprogramm automatisch folgende Daten und fügt diese unter Verwendung einer sicheren Nur-Lesen-Verbindung hinzu:

- Name der Stammdomäne oder des Computers
- Name des Domänen-Administrators oder ein Ressourcenkonto mit geeigneten Leseberechtigungen

11 Geben Sie das Administrator-Passwort in das vorgesehene Feld ein und klicken Sie auf *Testen*, um zu überprüfen, ob eine Verbindung hergestellt wird. Klicken Sie auf *Speichern*, wenn der Test erfolgreich verlaufen ist. Wenn bei dem Test ein Fehler auftritt oder nicht die richtige Domäne erkannt wird, muss diese manuell über die Verwaltungskonsole hinzugefügt werden (siehe Abschnitt 7.2.1, „eDirectory Services hinzufügen“, auf Seite 49).

Hinweis: Das eingegebene Passwort muss so eingestellt werden, dass es nicht abläuft, und dieses Konto darf nie deaktiviert werden.

---

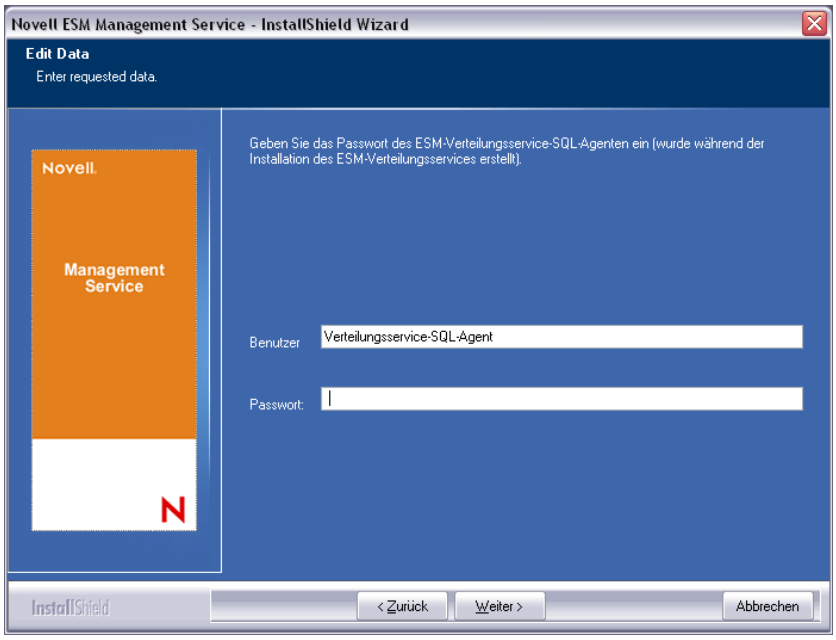
12 Der Verwaltungsdienst ist jetzt installiert. Klicken Sie auf *Fertig*, um die Kommunikationsprüfung zu schließen. Klicken Sie anschließend auf *Fertig stellen*, um das Installationsprogramm zu schließen.

6.1.2 Benutzerdefinierte Installation

Die benutzerdefinierte Installation zeigt die für die Standardinstallation verwendeten Standardwerte an und erlaubt es dem Administrator, einen anderen Speicherort einzugeben oder zu suchen.

1 Geben Sie das Passwort für den Richtlinienverteilungsservice-Agenten ein, das bei der Installation des Richtlinienverteilungsservices erstellt wurde.

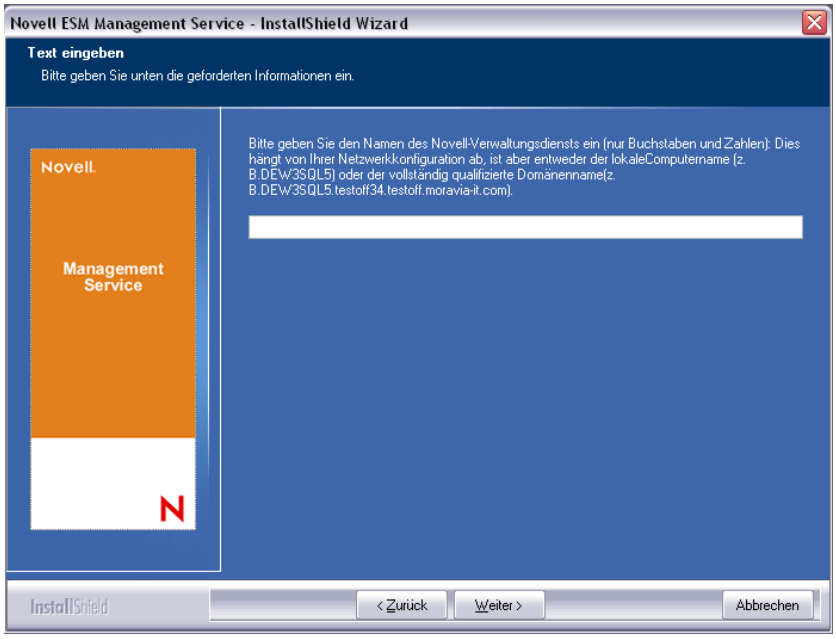
Abbildung 6-8 *SQL-Passwort eingeben*



2 Geben Sie den SSL-Zertifikatstyp ein, der für die Installation des Richtlinienverteilungsservices verwendet·wurde. Wenn Sie eine eigene (firmeninterne) Zertifizierungsstelle verwendet haben, klicken Sie auf: *Der Novell-Verteilungsservice hat ein Zertifikat verwendet, mit dem IIS bereits konfiguriert war*. Wenn das Installationsprogramm des Verteilungsservices ein Novell-Zertifikat erstellt hat, klicken Sie auf: *Der Novell-Verteilungsservice hat ein eigensigniertes Herkunftsverbürgungszertifikat installiert*.

3 Geben Sie den Namen des Servers ein, der als Host für den Verwaltungsdienst festgelegt werden soll.

Abbildung 6-9 *MS-Servernamen eingeben*



4 Ein SSL-Zertifikat ist für die sichere Kommunikation zwischen dem Verwaltungsdienst und allen Endpoint Security-Clients erforderlich. Wenn Sie bereits über eine Zertifizierungsstelle verfügen, klicken Sie auf *Das vorhandene Zertifikat verwenden, für das IIS konfiguriert ist.* Wenn Sie ein Zertifikat benötigen, klicken Sie auf *Novell das Erstellen, Installieren und Nutzen seines eigensignierten Herkunftsverbürgungszertifikats gestatten*. Das Installationsprogramm erstellt die Zertifikate und die signierende Zertifizierungsstelle. Unabhängig vom Zertifikatstyp müssen diese Zertifikate an alle Endbenutzer verteilt werden.

5 Wählen Sie bei Verwendung von Novell-Zertifikaten einen Speicherort, der die Verteilung vereinfacht (Standard ist das Installationsverzeichnis).

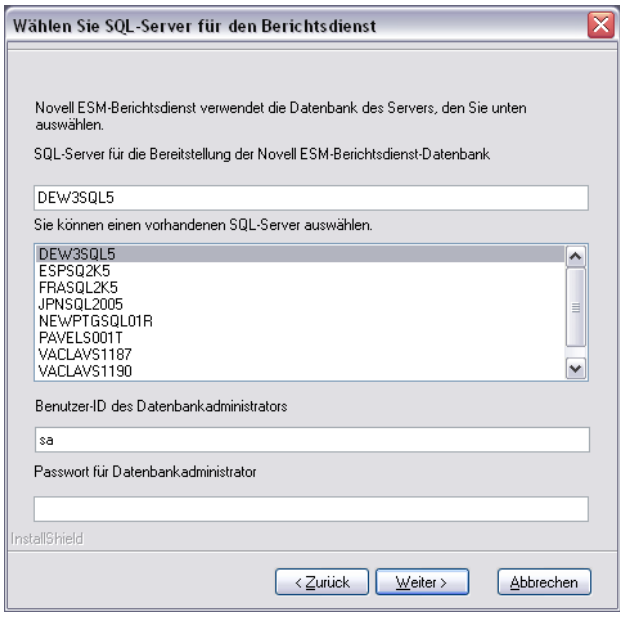
6 Das Installationsprogramm erkennt die auf dem Computer und im Netzwerk verfügbaren SQL-Datenbanken. Wählen Sie die SQL-Datenbank für den Richtlinienverteilungsservice und geben Sie den Benutzernamen und das Passwort des Datenbank-Administrators ein (wenn das Passwort aus null Zeichen besteht, warnt das Installationsprogramm vor einem möglichen Sicherheitsproblem). Benutzername und Passwort dürfen kein Domänenbenutzer sein. Es muss sich um einen SQL-Benutzer mit Systemadministratorrechten handeln.

Abbildung 6-10 *MS SQL-Datenbank auswählen*

7 Legen Sie den Namen für die Datenbank fest·(standardmäßig ist STMSDB eingegeben).

8 Wählen Sie die SQL-Datenbank für den Berichterstellungsservice aus und geben Sie den Benutzernamen und das Passwort des Administrators dieser Datenbank ein.

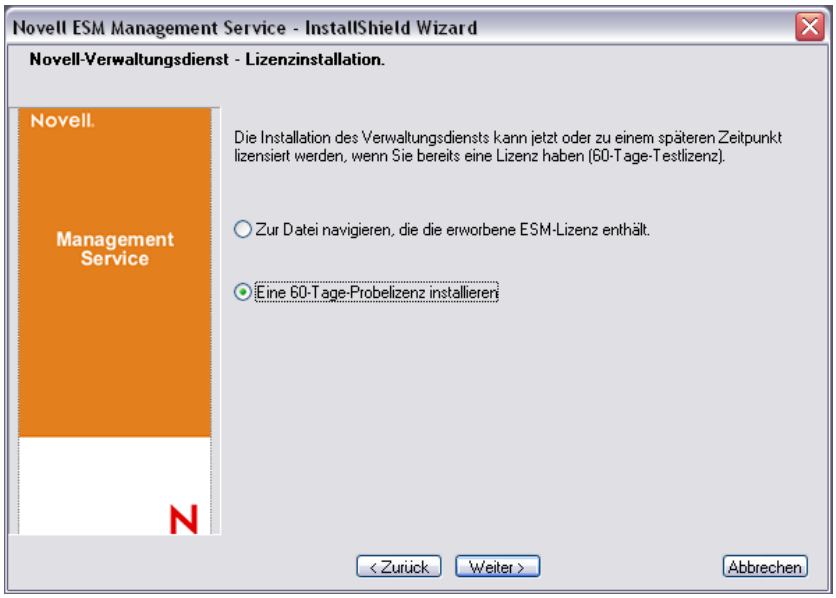
Abbildung 6-11 *Datenbank für den Berichterstellungsservice auswählen*



9 Legen Sie den Namen für die Datenbank fest·(standardmäßig ist STRSDB eingegeben).

10 Wenn ZENworks Endpoint Security Management bereits erworben wurde, wird eine gesonderte Lizenzdatei geliefert. Kopieren Sie die Lizenzdatei auf diesen Server und durchsuchen Sie diesen nach der Datei (weitere Details finden sie auf der Ihrer Lizenzdatei zugehörigen Anweisungsseite). Wenn Sie noch keine ZENworks Endpoint Security Management-Lizenz erworben haben, wählen Sie *Evaluierungslizenz für 60 Tage*, um fortzufahren.

Abbildung 6-12 *Novell-Lizenzdatei suchen*



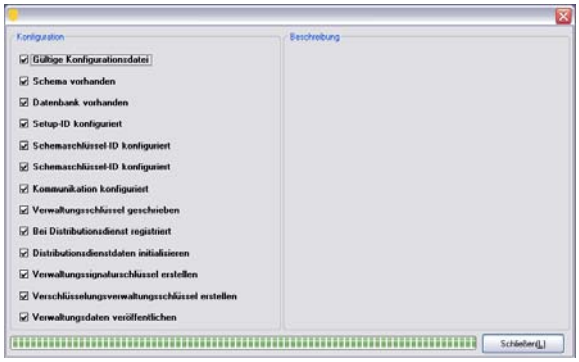
11 Klicken Sie im Bildschirm "Dateien kopieren" auf *Weiter*, um mit der Installation zu beginnen.

12 Wählen Sie die Dateipfade für die Daten-, Index- und Protokolldateien der Verwaltungsdienst-Datenbank aus.

13 Wählen Sie die Dateipfade für die Daten-, Index- und Protokolldateien der Berichterstellungsservice-Datenbank aus.

14 Der Verwaltungsdienst führt eine Kommunikationsprüfung für beide SQL-Datenbanken und den Richtlinienverteilungsservice aus. Wenn keine Kommunikation bestätigt wird, erhalten Sie eine Fehlermeldung. Für eine erfolgreiche Installation müssen alle Kontrollkästchen markiert sein.

Abbildung 6-13 *Kommunikationsprüfung*



15 Überspringen Sie die Schritte Schritt 16 und Schritt 17, wenn Sie eDirectory als Verzeichnisdienst verwenden.

16 Wenn die Installation auf einem Mitgliedserver für eine Domäne mit einem Active Directory- oder NT Domänen-Verzeichnisdienst durchgeführt wird, erkennt das Installationsprogramm automatisch folgende Daten und fügt diese unter Verwendung einer sicheren Nur-Lesen-Verbindung hinzu:

- Name der Stammdomäne oder des Computers
- Name des Domänen-Administrators oder ein Ressourcenkonto mit geeigneten Leseberechtigungen

17 Geben Sie das Administrator-Passwort in das vorgesehene Feld ein und klicken Sie auf *Testen*, um zu überprüfen, ob eine Verbindung hergestellt wird. Klicken Sie auf *Speichern*, wenn der Test erfolgreich verlaufen ist. Wenn bei dem Test ein Fehler auftritt oder nicht die richtige Domäne erkannt wird, muss diese manuell über die Verwaltungskonsole hinzugefügt werden (siehe Abschnitt 7.2.1, „eDirectory Services hinzufügen“, auf Seite 49).

Hinweis: Das eingegebene Passwort muss so eingestellt sein, dass es nicht abläuft. Außerdem darf dieses Konto nicht deaktiviert werden.

---

18 Der Verwaltungsdienst ist jetzt installiert. Klicken Sie auf *Fertig*, um die Kommunikationsprüfung zu schließen. Klicken Sie anschließend auf *Fertig stellen*, um das Installationsprogramm zu schließen.

6.2 Starten des Service

Der Verwaltungsdienst startet direkt nach der Installation, ohne dass der Server neu gebootet werden muss. Mit der Verwaltungskonsole werden die Daten des Verwaltungsdienstes verwaltet. (Weitere Details finden Sie im *ZENworks Endpoint Security Management-Administratorenhandbuch*.)

Novell empfiehlt, die Verwaltungskonsole auf diesem Server zu installieren. Wenn Sie die Verwaltungskonsole auf einem gesonderten Computer installieren, kopieren Sie das gesamte Verzeichnis der `ESM-Setupdateien` auf den Computer, der als Host für die Verwaltungskonsole festgelegt wurde, über Netzwerkfreigabe oder indem Sie die Datei auf einer Festplatte oder einem Thumb-Laufwerk speichern.

Fahren Sie mit Kapitel 7, „Durchführen der Installation der Verwaltungskonsole“, auf Seite 45 fort.

Durchführen der Installation der Verwaltungskonsole

7

Die Verwaltungskonsole kann auf dem Server des Verwaltungsdienstes oder auf einem sicheren PC, der über eine direkte Verbindung mit dem Server des Verwaltungsdienstes verfügt, installiert werden. Es ist möglich, mehrere Installationen von Verwaltungskonsolen zu konfigurieren, die mit einem einzelnen Verwaltungsdienst verbunden sind. Es wird jedoch empfohlen, den Zugriff auf die Verwaltungskonsole auf bestimmte Benutzer zu begrenzen.

Aus Sicherheitsgründen wird empfohlen, die Verwaltungskonsole direkt auf dem Verwaltungsdienst-Server zu installieren.

Vergewissern Sie sich, dass vor Beginn der Installation folgende Voraussetzungen erfüllt sind, sofern die Verwaltungskonsole auf einer eigenen Arbeitsstation installiert werden soll:

- ❑ Stellen Sie sicher, dass der Computer, auf dem die Verwaltungskonsole installiert werden soll, die folgenden Voraussetzungen erfüllt:
  - Windows XP SP1, Windows XP SP2 oder Windows 2000 SP4.
  - Ein Prozessor mit 1,0 GHz wird empfohlen mit mindestens 256 MB RAM und 100 MB freiem Festplattenspeicherplatz.
- ❑ Kopieren Sie den Ordner der `ESM-Setupdateien` auf den PC. Dieser Ordner enthält die SSL-Herkunftsverbürgungszertifikate für den Richtlinienverteilungsservice und den Verwaltungsdienst sowie die Datei `STInstParam.id`.
- ❑ Vergewissern Sie sich, dass Microsoft Internet Explorer 5.5 oder eine höhere Version installiert ist, wenn Sie die Verwaltungskonsole auf dem Server des Verwaltungsdienstes installieren.

7.1 Installationsschritte

Klicken Sie im Installationsmenü auf *Installation des Verwaltungsdienstes*.

Beim Start überprüft das Installationsprogramm, ob .NET Framework 3.5 und WSE 2.0 SP2 (beide erforderlich) auf dem Computer vorhanden sind. Wenn eines oder beide Programme fehlen, werden diese automatisch installiert, bevor die Installation mit dem Begrüßungsbildschirm fortgesetzt wird (sie müssen die Lizenzvereinbarung für .NET 3.5 akzeptieren).

So installieren Sie die Verwaltungskonsolen:

1. Klicken Sie zum Fortfahren auf *Weiter*.
2. Akzeptieren Sie den Lizenzvertrag und klicken Sie dann auf *Weiter*.
3. Wählen Sie die Installationsoption *Standard* oder *Benutzerdefiniert*.

Abbildung 7-1 *"Standard" oder "Benutzerdefiniert" wählen*

Beide Installationspfade werden unten beschrieben:

- Abschnitt 7.1.1, „Standardinstallation“, auf Seite 46
- Abschnitt 7.1.2, „Benutzerdefinierte Installation“, auf Seite 46

7.1.1 Standardinstallation

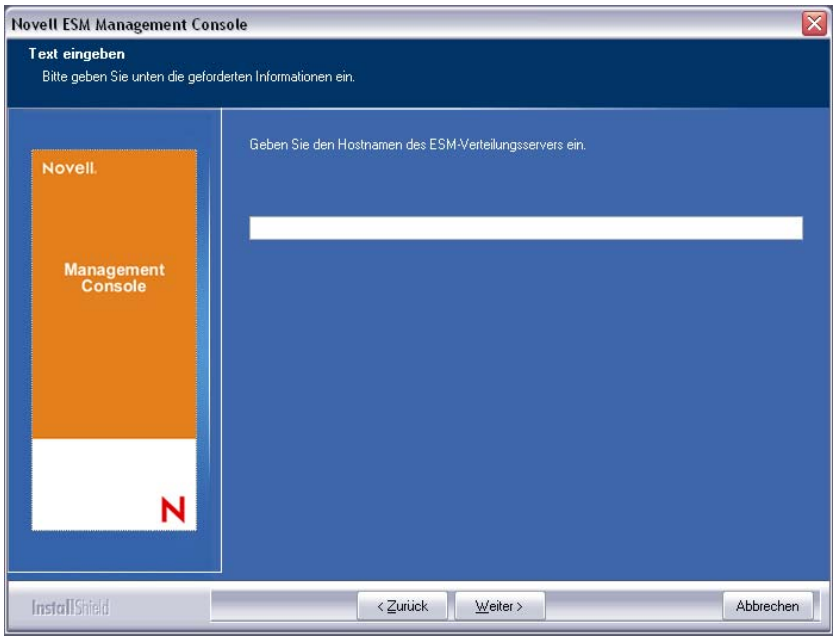
Bei der Standardinstallation werden die Server- und SSL-Standardinformationen verwendet, die in der Datei `STInstParam.id` enthalten sind, und `\Programme\Novell\ESM Management Console` als Standardverzeichnis eingerichtet. Wenn das Verzeichnis der `ESM-Setupdateien` auf dem Computer vorhanden ist, müssen für die Installation der Verwaltungskonsole keine weiteren Optionen ausgewählt werden.

7.1.2 Benutzerdefinierte Installation

Bei einer benutzerdefinierten Installation werden die in `STInstParam.id` enthaltenen und für die Standardinstallation verwendeten Standardwerte angezeigt. Der Administrator kann diese Werte ändern.

1 Geben Sie den Hostnamen des Richtlinienverteilungsservices ein. (Dabei muss es sich um den FQDN handeln, wenn der Server außerhalb der firmeninternen Firewall bereitgestellt wird.)

Abbildung 7-2 *Hostnamen des Richtlinienverteilungsservice eingeben*

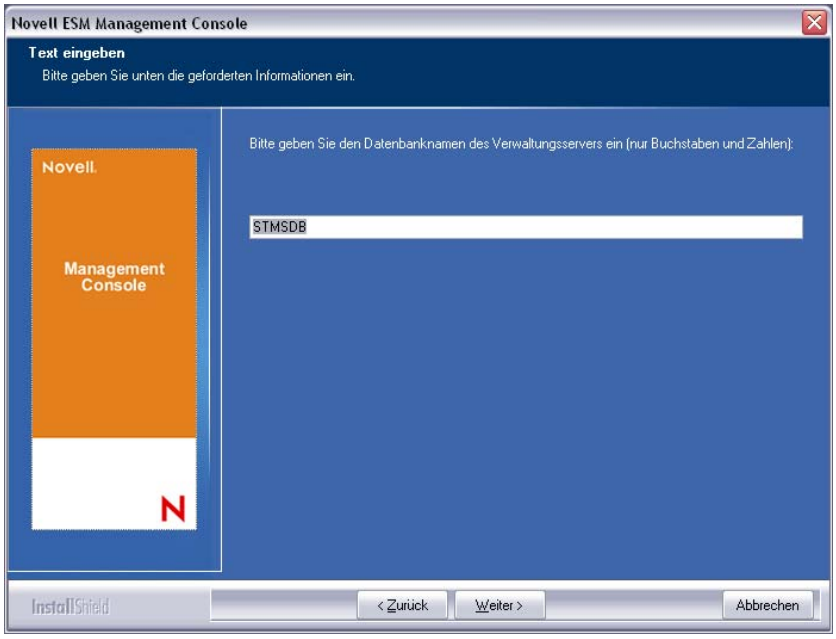


2 Geben Sie den Hostnamen für den Verwaltungsdienst ein.

3 Geben Sie den Hostnamen der SQL-Datenbank des Verwaltungsdienstes ein.

4 Geben Sie den Namen der SQL-Datenbank des Verwaltungsdienstes ein.

Abbildung 7-3 *Namen der SQL-Datenbank des MS eingeben*



5 Geben Sie den SQL-SA-Benutzernamen und das dazugehörige Passwort ein, die bei der Installation des Verwaltungsdienstes festgelegt wurden.

6 Wählen Sie den Typ des für den Richtlinienverteilungsservice und den Verwaltungsdienst installierten SSL-Zertifikats aus.

Abbildung 7-4 *Serverzertifikate auswählen*

7 Wählen Sie das Installationsverzeichnis der Verwaltungskonsole aus. Das Standardverzeichnis lautet `\Programme\Novell\ESM Management Console`.

Nach der Installation von ZENworks Endpoint Security Management müssen Sie einen Verzeichnisdienst erstellen und konfigurieren, bevor Sie mit der Verwaltung von Geräten in Ihrem System beginnen können.

Mit dem Assistenten zur Neukonfiguration von Verzeichnisdiensten können Sie eine Verzeichnisdienstkonfiguration erstellen, die den Umfang Ihrer Endpoint Security Client-Installationen definiert. Die neue Konfiguration verwendet Ihren vorhandenen Verzeichnisdienst, um die logische Begrenzng für Ihre benutzer- und computerbasierten Client-Installationen zu definieren.

Der Assistent führt Sie durch den Prozess der Auswahl eines Verzeichnisdiensts und der Kontexte, in denen sich die aktuellen und zukünftigen Client-Konten befinden.

Mithilfe des Assistenten können Sie außerdem die in der neuen Konfiguration enthaltenen Verzeichniseinträge synchronisieren. Diese Synchronisierung wird im Hintergrund ausgeführt, sodass Sie sofort beginnen können, Ihre neue Konfiguration zu verwenden.

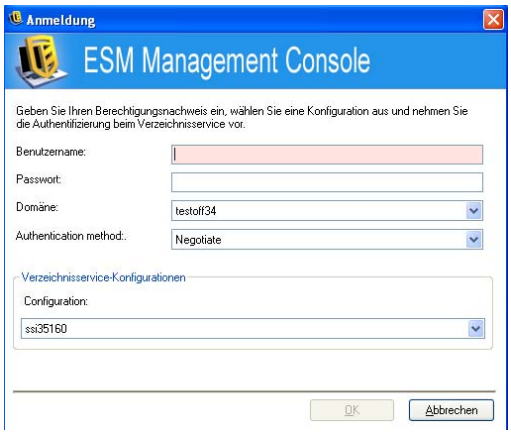
Nach der Installation von ZENworks Endpoint Security Management wird der Assistent zur Neukonfiguration von Verzeichnisdiensten automatisch angezeigt. Weitere Informationen zum Erstellen und Konfigurieren des Verzeichnisdienstes erhalten Sie unter “Konfigurieren des Verzeichnisdiensts” im *ZENworks Endpoint Security Management-Administratorenhandbuch*.

7.2 Die Konsole starten

Um das Anmeldefenster der Verwaltungskonsole zu starten klicken Sie auf *Start > Alle Programme > Novell > ESM Management Console > Management Console*.

Melden Sie sich bei der Verwaltungskonsole an, indem Sie Namen und Passwort des Administrators eingeben. Bevor Sie den Benutzernamen und das Passwort eingeben, müssen Sie eine Verbindung zur Domäne des Verzeichnisdienstes herstellen (siehe Abschnitt 7.2.1, „eDirectory Services hinzufügen“, auf Seite 49). Der eingegebene Benutzername muss zur Verwaltungsdienst-Domäne gehören.

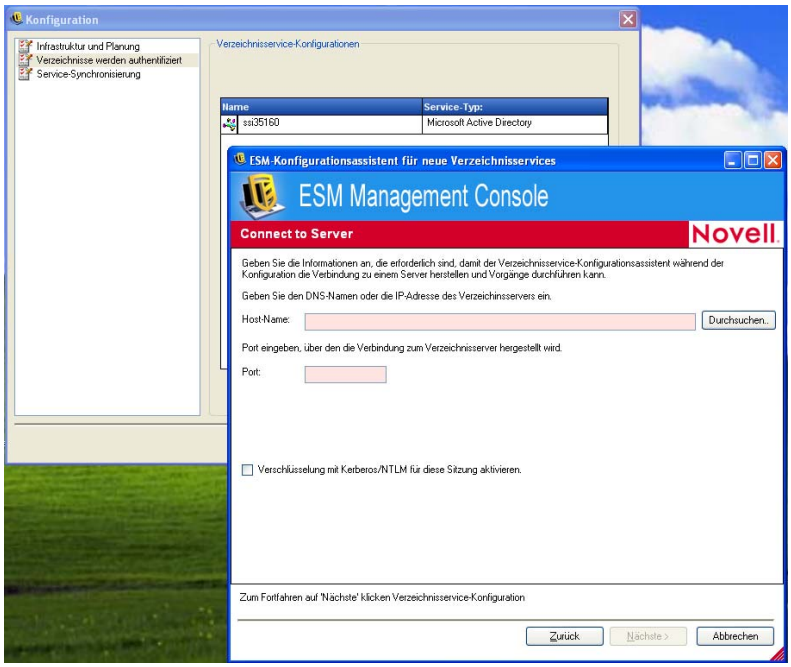
Abbildung 7-5 *Melden Sie sich bei der ZENworks Endpoint Security Management-Verwaltungskonsole an.*



7.2.1 eDirectory Services hinzufügen

1 Klicken Sie im Anmeldebildschirm auf die Schaltfläche *Optionen*. Das Konfigurationsfenster wird angezeigt

Abbildung 7-6 *Authentifizierungsverzeichnisse*



2 Geben Sie einen Anzeigenamen (Friendly Name) für den Verzeichnisdienst ein und wählen Sie in der Pulldown-Liste für die Servicetypen den Eintrag *eDirectory* aus.

3 Geben Sie im Feld *Host/DN* die IP-Adresse des eDirectory-Servers und im Feld *Domänenbaum* den Baumnamen ein.

4 Markieren Sie *Für Benutzerauthentifizierung verfügbar*, um die Domäne im Pulldown-Menü für die Anmeldung anzuzeigen.

5 Deaktivieren Sie *Sichere Authentifizierung* in den *Service-Verbindungsoptionen*.

6 Geben Sie den Kontonamen im LDAP-Format ein. Beispiel: In "cn=admin,o=acmeserver" ist cn der Benutzer und o ist das Objekt, in dem der Benutzername gespeichert ist.

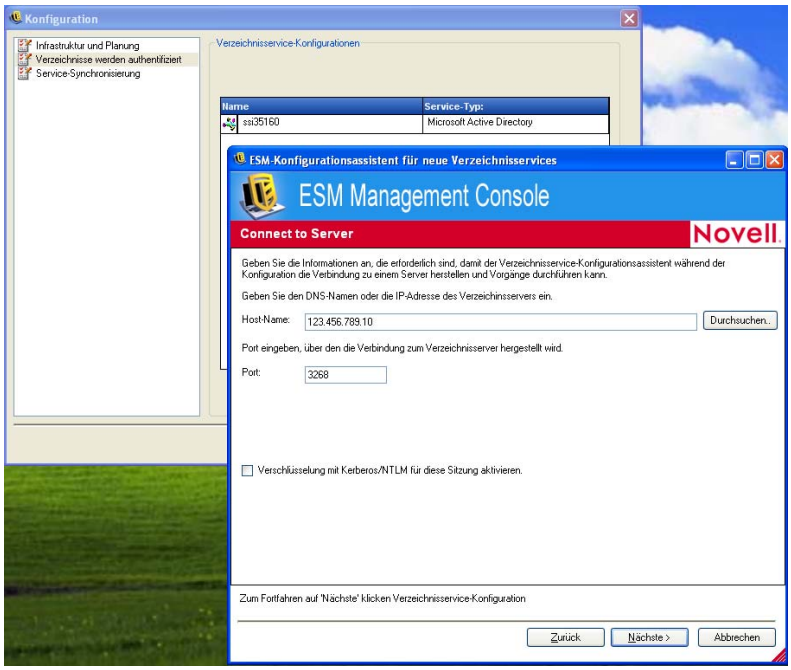
7 Geben Sie das Passwort für das Konto ein.

Hinweis: Das eingegebene Passwort muss so eingestellt sein, dass es nicht abläuft. Außerdem darf dieses Konto nicht deaktiviert werden.

---

8 Klicken Sie zur Überprüfung der Kommunikation mit diesem Verzeichnisdienst auf *Testen*. Wenn keine Kommunikation möglich ist, wird der Benutzer über den Fehler informiert. Unzureichende Informationen werden durch die Schnittstelle während des Tests nach Möglichkeit korrigiert.

Abbildung 7-7 *Fertig ausgefüllter Verzeichnisbildschirm*



9 Klicken Sie auf *Speichern*, um diesen Verzeichnisdienst zur Datenbank hinzuzufügen. Dann klicken Sie auf *Neu*, um der Datenbank weitere Verzeichnisdienste hinzuzufügen.

10 Klicken Sie auf *OK* oder *Abbrechen*, um das Konfigurationsfenster zu schließen und in das Anmeldefenster zurückzukehren.

Im *ZENworks Endpoint Security Management-Administratorenhandbuch* finden Sie Informationen zur Konfiguration der Überwachung für zusätzliche Verzeichnisdienste, einschließlich der unterstützten Dienste Active Directory und NT Domänen.

7.2.2 Konfigurieren der Berechtigungseinstellungen für die Verwaltungskonsole

Diese *Berechtigungen* befinden sich im Menü *Tools* der Verwaltungskonsole. Zugriff ist nur für den primären Administrator des Verwaltungsdienstes und/oder Personen möglich, denen Zugriffsberechtigungen von diesem Administrator gewährt wurden. Diese Steuerung ist für die Einzelplatz-Verwaltungskonsole nicht verfügbar (siehe Kapitel 11, „Installation von ZENworks Endpoint Security Management im unverwalteten Modus“, auf Seite 81 für weitere Details).

Die Berechtigungseinstellungen legen fest, welcher Benutzer oder welche Gruppe auf die Verwaltungskonsole, die Richtlinienveröffentlichung und die Einstellungen für Berechtigungsänderungen zugreifen können.

Während der Installation des Management Servers wird ein Administratoren- oder Ressourcenkonto-Name in das Konfigurationsformular eingegeben. Wenn der Test erfolgreich verlaufen ist und die Benutzerinformationen gespeichert wurden, werden diesem Benutzer automatisch fünf Berechtigungen gewährt.

Wenn die Verwaltungskonsole installiert ist, werden allen Benutzergruppen innerhalb der Domäne vollständige Berechtigungen gewährt. Der Benutzer der Ressource sollte allen die Berechtigungen entziehen, mit Ausnahme der Gruppen und Benutzer, denen der Zugriff gewährt werden soll. Der Benutzer der Ressource hat die Möglichkeit, weitere Berechtigungen für die festgelegten Benutzer zu einzurichten. Die gewährten Berechtigungen haben folgendes Resultat:

- **Zugriff auf die Verwaltungskonsole:** Der Benutzer kann Richtlinien und Komponenten anzeigen und vorhandene Richtlinien bearbeiten. Benutzer, denen nur diese Berechtigung erteilt wurde, können Richtlinien weder hinzufügen noch löschen, da die Veröffentlichungs- und Berechtigungsoptionen nicht verfügbar sind.
- **Richtlinie veröffentlichen:** Der Benutzer kann in der Verwaltungskonsole neue Richtlinien erstellen.
- **Berechtigung ändern:** Der Benutzer hat die Möglichkeit, auf die Berechtigungseinstellungen für andere, bereits erstellte Benutzer zuzugreifen und diese zu ändern sowie neuen Benutzern Berechtigungen zu gewähren.
- **Richtlinien erstellen:** Der Benutzer kann in der Verwaltungskonsole neue Richtlinien erstellen.
- **Richtlinien löschen:** Der Benutzer kann in der Verwaltungskonsole alle Richtlinien löschen.

Hinweis: Aus Sicherheitsgründen wird empfohlen, dass nur dem Benutzer der Ressource oder sehr wenigen Administratoren die Berechtigungen zum Ändern von Berechtigungen und zum Löschen von Richtlinien gewährt werden.

Die folgenden Abschnitte enthalten weitere Informationen:

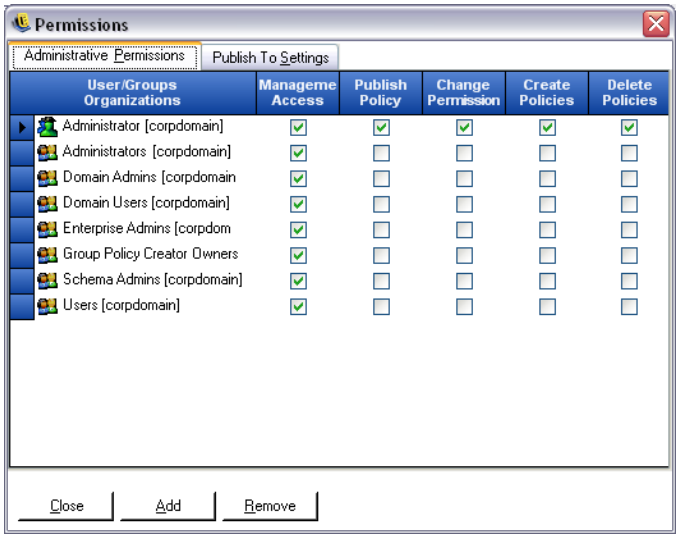
- „Verwaltungsberechtigungen konfigurieren“ auf Seite 51
- „Veröffentlichungseinstellungen konfigurieren“ auf Seite 53

Verwaltungsberechtigungen konfigurieren

1 Klicken Sie auf *Tools* > *Berechtigungen*.

Die dieser Domäne zugeordneten Gruppen werden angezeigt.

Abbildung 7-8 *Verwaltungskonsolenfenster für Berechtigungseinstellungen*



Hinweis: Standardmäßig werden allen Gruppen vollständige Berechtigungen für die Verwaltungskonsole gewährt. Administratoren sollten alle Richtlinienaufgaben von nicht autorisierten Gruppen sofort deaktivieren. Der Zugriff auf die Konsole kann durch Deaktivieren dieser Berechtigung entfernt werden.

---

2 (Optional) So laden Sie Benutzer und neue Gruppen in diese Liste:

2a Klicken Sie im unteren Bildschirmbereich auf die Schaltfläche *Hinzufügen*, damit die Organisationstabelle angezeigt wird.

Abbildung 7-9 *Organisationstabelle für Berechtigungseinstellungen*

2b Wählen Sie die geeigneten Benutzer und Gruppen aus der Liste aus. Wählen Sie mit der Steuerungs- oder Umschalttaste mehrere Benutzer aus.

2c Klicken Sie auf die Schaltfläche *OK*, wenn alle Benutzer und Gruppen ausgewählt sind. Damit werden die sie der Tabelle im Berechtigungsformular hinzugefügt.

3 Weisen Sie den verfügbaren Benutzern und Gruppen Berechtigungen zu.

Wenn Sie bestimmte Benutzer oder Gruppen entfernen möchten, heben Sie deren Namen hervor und klicken Sie auf *Entfernen*.

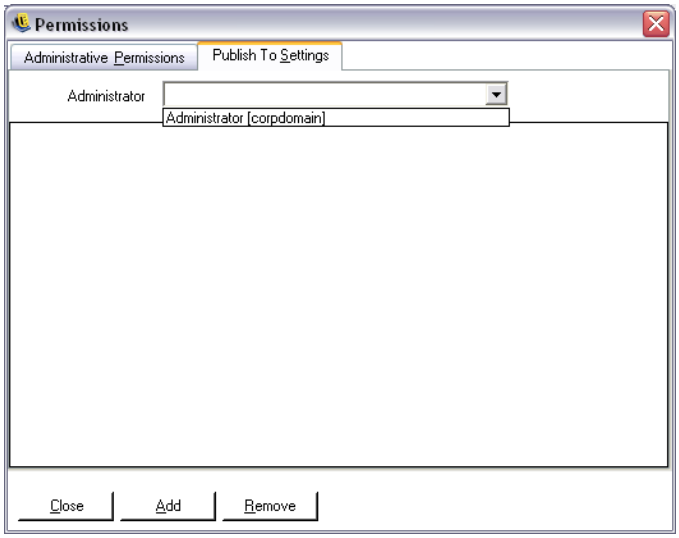
Veröffentlichungseinstellungen konfigurieren

Benutzern/Gruppen, für die *Richtlinien veröffentlichen* markiert ist, müssen Benutzer oder Gruppen zugewiesen werden, für die Richtlinien veröffentlicht werden. So legen Sie die Veröffentlichungseinstellungen fest:

1 Klicken Sie auf die Registerkarte *Veröffentlichungseinstellungen*.

2 Wählen Sie die Benutzer und Gruppen, denen die Veröffentlichungsberechtigung gewährt wurde, aus der Drop-Down-Liste aus.

Abbildung 7-10 *Einstellungen für "Veröffentlichen an"*



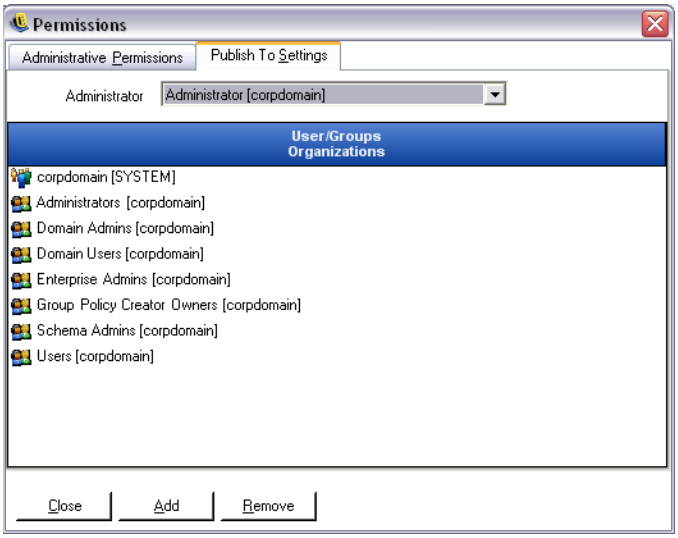
3 So weisen Sie diesem Benutzer oder dieser Gruppe weitere Benutzer und Gruppen zu:

3a Klicken Sie im unteren Bildschirmbereich auf die Schaltfläche *Hinzufügen*, damit die Organisationstabelle angezeigt wird.

3b Wählen Sie die geeigneten Benutzer und Gruppen aus der Liste aus. Mit der Steuerungs- und der Umschalttaste wählen Sie mehrere Benutzer aus.

3c Sobald alle Benutzer/Gruppen ausgewählt wurden, klicken Sie auf *OK*.

Abbildung 7-11 *Liste "Veröffentlichen an"*



Wenn Sie bestimmte Benutzer oder Gruppen entfernen möchten, heben Sie deren Namen in der Liste hervor und klicken Sie auf *Entfernen*.

Die Berechtigungseinstellungen werden sofort implementiert, sodass der Administrator nur auf *Schließen* klicken und die Änderungen akzeptieren muss, um zum Editor zurückzukehren.

Wenn ein neuer Verzeichnisdienst hinzugefügt wird, werden dem Ressourcenkonto wie oben beschrieben vollständige Berechtigungseinstellungen gewährt.

7.2.3 Richtlinien veröffentlichen

So veröffentlichen Sie eine Sicherheitsrichtlinie mit den Standardeinstellungen:

1. Klicken Sie auf *Neue Richtlinie erstellen*.
2. Geben Sie einen Namen für die Richtlinie ein und klicken Sie auf *Erstellen*.
3. Speichern Sie die Richtlinie und klicken Sie auf die Registerkarte *Veröffentlichen*.
4. Da sich Endpoint Security Client-Benutzer anmelden müssen, um Elemente im Baum anzeigen zu können, wählen Sie den oberen Teil des Baums auf der linken Seite. Doppelklicken Sie, um das Veröffentlichungsfeld mit den aktuellen Gruppen und Benutzern auszufüllen.
5. Klicken Sie auf *Veröffentlichen*, um die Richtlinie an den Richtlinienverteilungsservice zu senden.

Die auf diese Weise generierte Richtlinie hat folgende Eigenschaften:

- Es wird ein (unbekannter) Einzelstandort erstellt.
- CD/DVD ROM-Laufwerke sind zulässig.
- Wechselspeichergeräte sind zulässig.
- Alle Kommunikationsports (einschließlich Wi-Fi) sind zulässig.
- Die Richtlinie beinhaltet die Firewalleinstellung "Alle adaptiv" (Ausgangsverkehr über Networking-Ports ist zulässig, nicht angeforderter Eingangsverkehr über Networking-Ports ist unzulässig).

Informationen zum Erstellen einer besseren Sicherheitsrichtlinie und alle Details zu Richtlinienkomponenten finden Sie im *ZENworks Endpoint Security Management-Administratorenhandbuch*.

Fahren Sie mit Kapitel 8, „Installation des Client Location Assurance Services“, auf Seite 57 fort.

7.3 USB-Reader installieren

Im Installationspaket ist der USB-Reader von Novell enthalten, der dem Administrator Hilfe beim Erstellen der Liste der zulässigen USB-Geräte bietet.

So installieren Sie den Reader:

1. Klicken Sie auf *Setup*, um mit der Installation zu beginnen.
2. Klicken Sie zum Fortfahren im Begrüßungsbildschirm auf *Weiter*.
3. Akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf *Weiter*.
4. Geben Sie im Kundeninformationsbildschirm den entsprechenden Benutzernamen und Informationen zur Organisation ein und wählen Sie, ob jeder Benutzer des Computers oder nur der oben eingegebene Benutzer auf diese Software zugreifen kann.
5. Klicken Sie auf *Installieren*.
6. Klicken Sie auf *Fertig stellen*.

Weitere Informationen zur Verwendung des USB-Readers finden Sie im *ZENworks Endpoint Security Management-Administratorenhandbuch*.

Installation des Client Location Assurance Services

8

Zugriff auf den Server sollte nur in einer gesteuerten Netzwerkumgebung bestehen. Nur so wird sichergestellt, dass der Benutzer sich in der von dem ZENworks® Security Client identifizierten Umgebung befindet. Anweisungen für Failover- und Redundanzkonfigurationen finden Sie weiter unten. Der Client Location Assurance Service (CLAS) kann, wenn gewünscht, auf demselben Server bereitgestellt werden, der als Host für die Einzelserverinstallation oder bei mehreren Servern für die Installation des Verwaltungsdienstes festgelegt wurde.

Installieren Sie CLAS auf einem Server, der von Endgeräten nur erkannt werden kann, wenn diese sich in der Netzwerkumgebung befinden, die eine kryptografische Überprüfung erfordert.

Die Bereitstellung von CLAS auf einem PDC (Primärdomänencontroller) wird aus Gründen der Sicherheit und der Funktionalität nicht unterstützt.

Hinweis: Es wird empfohlen, den SSI-Server so zu konfigurieren (härten), dass alle Anwendungen, Dienste, Konten und andere Optionen, die für die vorgesehene Serverfunktionalität nicht benötigt werden, deaktiviert sind. Die dafür erforderlichen Schritte hängen von den Einzelheiten der lokalen Umgebung ab und lassen sich deshalb nicht vorausgreifend beschreiben. Administratoren sollten den entsprechenden Abschnitt der Microsoft Technet Sicherheitswebseite (http://www.microsoft.com/technet/security/default.mspx) nachschlagen. Weitere Empfehlungen für die Zugriffssteuerung finden Sie im *ZENworks Endpoint Security Management-Administratorenhandbuch*.

Wenn Sie den Zugriff auf verbürgte Computer begrenzen möchten, können das virtuelle Verzeichnis und IIS mit ACLs eingerichtet werden. Schlagen Sie folgende Artikel nach:

- Gewähren oder Verweigern des Zugriffs auf Computer (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- Site-Zugriff anhand von IP-Adresse oder Domänennamen beschränken (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- IIS-FAQ: Beschränkungen für 2000-IP-Adresse und Domänenname (http://www.iisfaq.com/default.aspx?View=A136&P=109)
- Arbeiten mit IIS-Paketfilterung (http://www.15seconds.com/issue/011227.htm)

Aus Sicherheitsgründen empfiehlt es sich, folgende Standardordner aus allen IIS-Installationen zu entfernen:

- `IISHelp`
- `IISAdmin`
- `Skripts`
- `Drucker`

Novell empfiehlt außerdem, das IIS-Lockdown-Werkzeug zu verwenden, das auf microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx) zur Verfügung steht.

Die Version 2.1 wird von den für die wichtigsten IIS-abhängigen Microsoft-Produkte bereitgestellten Schablonen gesteuert. Wählen Sie die Schablone, die der Funktion dieses Servers am besten entspricht. Im Zweifelsfall wird die Schablone "Dynamischer Webserver" empfohlen.

Vergewissern Sie sich bitte, dass folgende Voraussetzungen gegeben sind, bevor Sie mit der Installation beginnen:

- Servernamenauflösung vom Verwaltungsdienst (MS) zu Richtlinienverteilungsservice (DS): Vergewissern Sie sich, dass der Zielcomputer, auf dem MS installiert werden soll, Pings für den DS-Servernamen senden kann (NetBIOS, wenn der DS innerhalb der Netzwerk-Firewall konfiguriert wird, FQDN bei Installation außerhalb in der DMZ).
- Aktivieren oder installieren Sie Microsoft Internetinformationsdienste (IIS) und stellen Sie sicher, dass ASP.NET aktiviert ist.

  Wichtig: Deaktivieren Sie auf der Seite "Sichere Kommunikation" das Kontrollkästchen *Sicherer Kanal (SSL) erforderlich*. Erweitern Sie dazu im Dienstprogramm "Microsoft Computer Management" *Dienste und Anwendungen* > erweitern Sie *Internetinformationsdienste-Manager* > erweitern Sie *Websites* > klicken Sie mit der rechten Maustaste auf *Standardwebsite* > klicken Sie auf *Eigenschaften* > klicken Sie auf die Registerkarte *Verzeichnissicherheit* > und klicken Sie im Gruppenfeld "Sichere Kommunikation" auf die Schaltfläche *Bearbeiten*. Durch das Aktivieren dieser Option bricht die Kommunikation zwischen dem ZENworks Endpoint Security Management-Server und dem ZENworks Endpoint Security-Client auf dem Endgerät ab.

Klicken Sie im Installationsmenü auf *Client Location Assurance Service*. Die Installation von CLAS beginnt.

Beim Start überprüft das Installationsprogramm, ob die erforderliche Software auf dem Server vorhanden ist. Beim Start überprüft das Installationsprogramm, ob die erforderliche Software auf dem Server vorhanden ist. Wenn Programme fehlen, werden diese automatisch installiert, bevor die Installation mit dem Begrüßungsbildschirm fortgesetzt wird (möglicherweise müssen Lizenzvereinbarungen für die Zusatzsoftware akzeptiert werden). Falls Microsoft Data Access Components (MDAC) 2.8 installiert werden muss, muss der Server nach dessen Installation neu booten, bevor die Installation von ZENworks Endpoint Security Management fortgesetzt werden kann. Wenn Windows 2003 Server verwendet wird, wird ASP.NET 2.0 vom Installationsprogramm so konfiguriert, dass es ausgeführt wird.

8.1 Installationsschritte

So installieren Sie den CLAS und erstellen einen Lizenzschlüssel:

1. Klicken Sie zum Fortfahren im Begrüßungsbildschirm auf *Weiter*.
2. Akzeptieren Sie den Lizenzvertrag und klicken Sie dann auf *Weiter*.
3. Während der Installation werden Dateien in das Standardverzeichnis kopiert: `\Programme\Novell\ESM CLAS`.
4. Während der Installation von Client Location Assurance Service werden zwei Schlüssel generiert, der private Schlüssel und der öffentliche Schlüssel. Die publickey-Datei kann auf dem Desktop oder in einem anderen Verzeichnis gespeichert werden. Wenn Sie die publickey-Datei in einem anderen Verzeichnis speichern möchten, klicken Sie auf *Ja* und durchsuchen Sie

die Festplatte nach dem gewünschten Ordner. Klicken Sie auf *Nein*, um die Standardeinstellung zu akzeptieren. In diesem Fall wird die publickey-Datei zusammen mit der privatekey-Datei gespeichert.

5 Klicken Sie auf *Fertig stellen*, um das Installationsprogramm abzuschließen.

Der Verwaltungsdienst muss auf den öffentlichen Schlüssel zugreifen können.

8.2 Failover-Installationen von CLAS

Auf den Servern im gesamten Unternehmen sind möglicherweise mehrere CLAS-Iterationen installiert, entweder, um mehrere Standorte kryptografisch zu sichern, oder um zu gewährleisten, dass bei Ausfall des primären CLAS-Servers die Überprüfung des Standorts durch den ZENworks Security Client weiterhin möglich ist.

Beim zweiten Szenario wird der private Schlüssel anhand der URL (Uniform Resource Locator), nicht anhand der IP-(Internet Protocol-)Adresse ausfindig gemacht. Folglich kann ein Block von Servern zur gemeinsamen Nutzung einer einzigen URL eingerichtet werden. CLAS kann entweder auf einem einzigen Server (in diesem Fall kann das Image dieses Servers auf jeden weiteren Server kopiert werden) oder auf jedem der Server installiert werden. Die privaten und öffentlichen Schlüssel können dann auf die anderen Server kopiert werden. Alle Server in einem URL-Block müssen dieselben privaten und öffentlichen Schlüssel verwenden.

8.3 Übertragen des öffentlichen Schlüssels an den Verwaltungsservice

Nachdem die Installation abgeschlossen ist, wird der generierte öffentliche Schlüssel gemäß Sicherheitsrichtlinie an den Endpoint Security Client übertragen und befindet sich dann auf dem Server im Verzeichnis `\Programme\Novell\Novell ESM CLAS`. Der öffentliche Schlüssel trägt den Dateinamen `publickey`. Dieser Dateiname kann in einen beliebigen Namen geändert werden.

Die publickey-Datei muss anschließend kopiert und an den Verwaltungsdienst übertragen werden (an beliebiger Stelle des Dienstes). Dann kann die Verwaltungskonsole auf den Schlüssel zugreifen und diesen gemäß einer Sicherheitsrichtlinie an alle Endpoint Security-Clients verteilen. Es ist auch möglich, die `publickey`-Datei auf einen PC zu laden, auf dem eine ZENworks Endpoint Security Management-Verwaltungskonsole ausgeführt wird.

Fahren Sie mit Kapitel 9, „Installation von Endpoint Security Client 3.5“, auf Seite 61 fort.

Installation von Endpoint Security Client 3.5

9

Verwenden Sie Novell ZENworks Endpoint Security Client 3.5 für Windows XP (SP1 und SP2) und Windows 2000 SP4-Clients. Klicken Sie im Installationsmenü auf das entsprechende *ZENworks Security Client*-Installationsprogramm. Die Installation des Endpoint Security Client wird gestartet. Auf den folgenden Seiten wird der Installationsvorgang für die Standard- und die MSI-Installation beschrieben.

- Bei der Standardinstallation wird der Endpoint Security Client 3.5 nur auf dem aktuellen Computer installiert.
- Bei der MSI-Installation wird das Installationsprogramm im Administrator-Modus (`/a`) gestartet, und es wird ein MSI-Softwarepaket erstellt. Dieses Paket kann anschließend verteilt oder an einem bestimmten Ort im Netzwerk verfügbar gemacht werden. Die erforderlichen Benutzereingaben sind dabei vorkonfiguriert. So können die einzelnen Benutzer die Software mit vordefinierten Serverwerten installieren.

9.1 Standardinstallation von Endpoint Security Client 3.5

Bei diesem Vorgang wird der Endpoint Security Client 3.5 nur auf dem aktuellen Computer installiert.

Überprüfen Sie, ob alle Sicherheitspatches für Microsoft* sowie die Antivirussoftware installiert und aktuell sind.

Installieren Sie die SSL-Herkunftsverbürgungszertifikate für den Verwaltungsdienst auf dem lokalen Computer (`ESM-MS.cer` oder das firmeninterne Zertifikat).

Hinweis: Es wird empfohlen, während der Installation des Endpoint Security Client 3.5 Antivirus-/Spyware-Software zu schließen, die sich möglicherweise auf gültige Registrierungsfunktionen auswirkt.

---

1. Klicken Sie zum Fortfahren im Begrüßungsbildschirm auf *Weiter*.
2. Akzeptieren Sie den Lizenzvertrag und klicken Sie dann auf *Weiter*.
3. Geben Sie ein Installationspasswort ein. Dies verhindert, dass der Benutzer den Endpoint Security Client 3.5 über *Software* in der Windows-Systemsteuerung deinstallieren kann (empfohlen).

Abbildung 9-1 *Deinstallationspasswort*

4 Wählen Sie aus, wie Richtlinien empfangen werden sollen (vom Distributionsdienst für verwaltete Clients oder lokal für eine unverwaltete Konfiguration abgerufen [Details zur unverwalteten Konfiguration finden Sie unter Kapitel 11, „Installation von ZENworks Endpoint Security Management im unverwalteten Modus“, auf Seite 81]).

Abbildung 9-2 *Verwaltungseinstellungen*

5 Geben Sie die Informationen für den Verwaltungsdienst ein.

6 Wählen Sie aus, ob Richtlinien für Benutzer oder für den Computer (computerbasierte Richtlinien) empfangen werden sollen.

Abbildung 9-3 *Benutzer- oder computerbasierte Richtlinien*

7 Klicken Sie auf *Installieren*.

Wenn die Software installiert ist, wird der Benutzer aufgefordert, den Computer neu zu starten.

Hinweis: Optional können Sie das Zertifikat für den Verwaltungsdienst vor Ausführung der Installation in einen Ordner neben `setup.exe` kopieren. Dadurch wird das Zertifikat automatisch auf dem Computer (das heißt für alle Benutzer) installiert. Dieser Vorgang kann auch mit der von Novell ausgegebenen Datei `license.dat` durchgeführt werden.

9.2 MSI-Installation

Bei diesem Vorgang wird ein MSI-Paket für den Endpoint Security Client 3.5 erstellt. Mit diesem Paket kann ein Systemadministrator die Installation über eine Active Directory-Richtlinie oder über andere Software-Verteilungsmethoden an eine Gruppe von Benutzern veröffentlichen.

So erstellen Sie das MSI-Paket:

Wenn Sie die Installation von der CD oder über das ISO-Hauptinstallationsprogramm ausführen und keine Befehlszeilenvariablen ausführen möchten (siehe Abschnitt 9.2.1, „Befehlszeilenvariablen“, auf Seite 66):

1 Legen Sie die CD ein und warten Sie, bis das Hauptinstallationsprogramm startet.
2 Klicken Sie auf *Produktinstallation*.
3 Klicken Sie auf *Security Client*.
4 Klicken Sie auf *ZSC-MSCI-Paket erstellen*.

Beginnen Sie wie folgt, wenn Sie für die Installation nur die Datei `setup.exe` verwenden (die ausführbare Datei befindet sich auf der CD unter: `D:\ESM32\ZSC`):

1 Klicken Sie mit der rechten Maustaste auf `setup.exe`.
2 Wählen Sie *Verknüpfung erstellen*.
3 Klicken Sie mit der rechten Maustaste auf die Verknüpfung und klicken Sie dann auf *Eigenschaften*.

4 Betätigen Sie am Ende des Zielfelds, hinter den Anführungszeichen, einmal die Leertaste, um einen Leerschritt einzugeben, und geben Sie dann `/a` ein.

   Beispiel: `C:\Dokumente und Einstellungen\euser\Desktop\CL-Release-3.2.455\setup.exe`

   Für die MSI-Installation sind mehrere Befehlszeilenvariablen verfügbar (siehe Abschnitt 9.2.1, „Befehlszeilenvariablen“, auf Seite 66).

5 Klicken Sie auf *OK*.

6 Doppelklicken Sie zum Starten des MSI-Installationsprogramms auf die Verknüpfung.

Sobald die Installation startet, führen Sie folgende Schritte aus:

1 Klicken Sie zum Fortfahren im Begrüßungsbildschirm auf *Weiter*.

2 Akzeptieren Sie den Lizenzvertrag und klicken Sie dann auf *Weiter*.

3 Wählen Sie aus, ob ein Deinstallationspasswort erforderlich ist (empfohlen), und geben sie dieses ein.

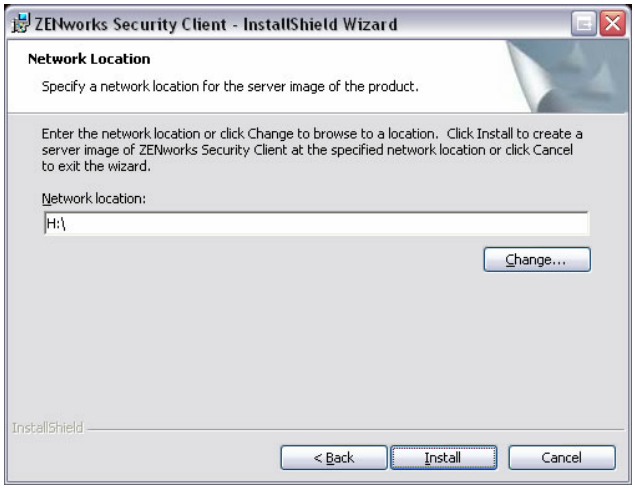
4 Wählen Sie aus, wie Richtlinien empfangen werden sollen (für verwaltete Clients vom Verteilungsservice, für eine unverwaltete Konfiguration lokal abgerufen). Wenn die verwaltete Option ausgewählt wurde:

   - Geben Sie die Informationen zum Verwaltungsdienst ein (ein FQDN oder NetBIOS-Name, je nach Eingabe bei der Installation des Verwaltungsdienstes).
   - Wählen Sie aus, ob benutzerbasierte oder computerbasierte Richtlinien verwendet werden sollen.

5 (Optional) Geben Sie im dafür vorgesehenen Feld eine E-Mail-Adresse ein, damit Sie bei einer fehlerhaften Installation benachrichtigt werden.

6 Geben Sie den Netzwerkstandort ein, an dem das MSI-Image erstellt werden soll, oder suchen Sie nach diesem Standort, indem Sie auf die Schaltfläche *Ändern* klicken.

Abbildung 9-4 *Netzwerkstandort für das MSI-Image auswählen*

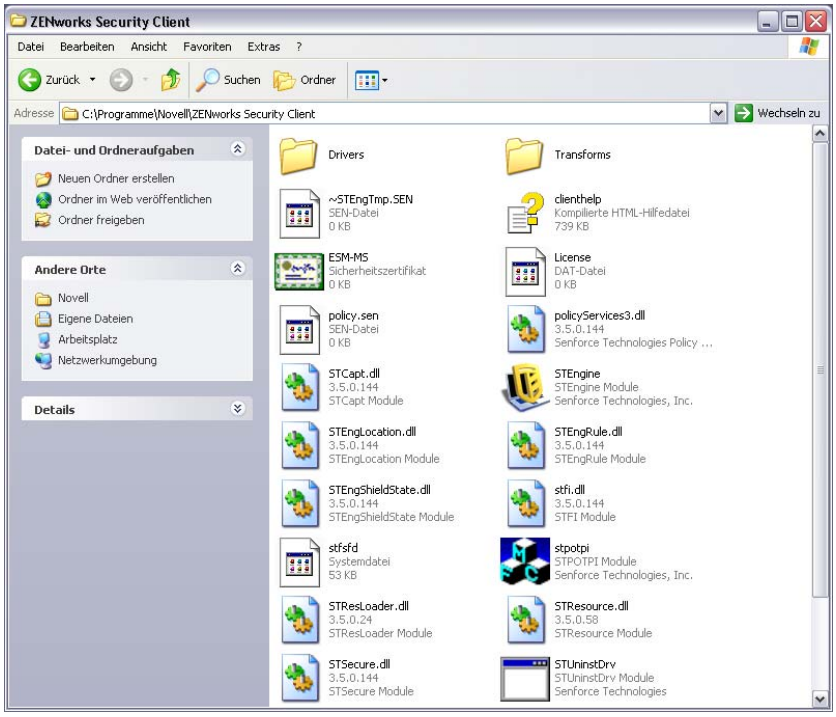


7 Klicken Sie zum Erstellen des MSI-Image auf *Installieren*.

8 Wechseln Sie zu dem erstellten MSI-Image und öffnen Sie den Ordner `\Programme\Novell\ZENworks Security Client\`.

9 Kopieren Sie das SSL-Zertifikat für den Verwaltungsdienst (`ESM-MS.cer` oder das firmeninterne Zertifikat) und den Novell-Lizenzschlüssel in diesen Ordner. Ersetzen Sie dabei die aktuell im Ordner befindlichen Standarddateien von 0 KB. Das SSL-Zertifikat für ESM-MS ist im Ordner der `ZENworks Endpoint Security Management-Setupdateien` verfügbar. Der Lizenzschlüssel wird separat per E-Mail versendet (wenn Sie den 30-tägigen Evaluierungszeitraum in Anspruch nehmen, ist in diesem Moment kein Lizenzschlüssel erforderlich).

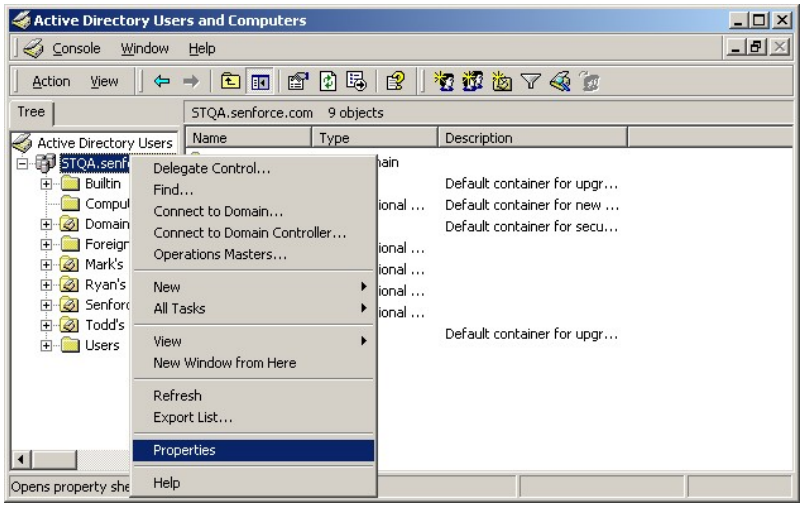
Abbildung 9-5 *Ersetzen Sie die Standarddateien im MSI-Paket.*



Führen Sie folgende Schritte aus, wenn Sie festlegen möchten, dass das MSI-Paket wie eine Gruppenrichtlinie an die Benutzergruppen verteilt werden soll:

1 Öffnen Sie unter *Verwaltung* die Option *Active Directory-Benutzer und -Computer* und öffnen Sie die Eigenschaften der *Stammdomäne* oder der OU.

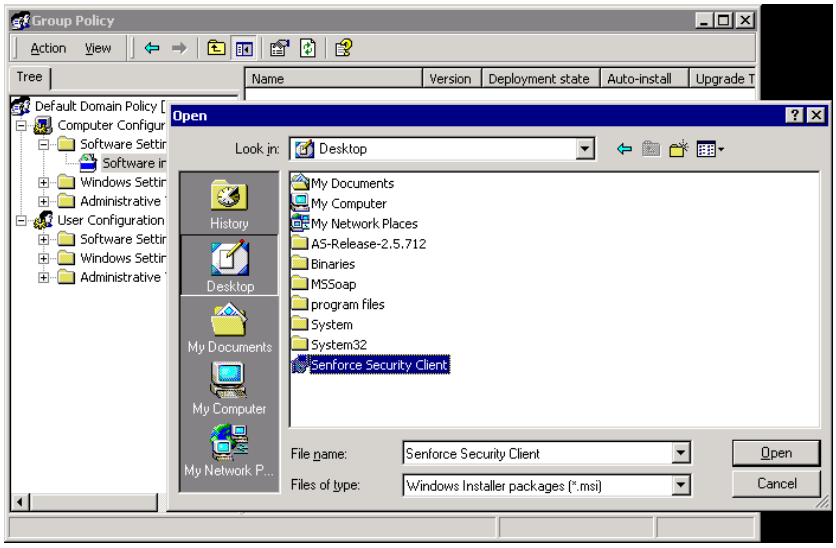
Abbildung 9-6 *Öffnen Sie die Eigenschaften der Stammdomäne oder der OU.*



2 Klicken Sie auf die Registerkarte *Gruppenrichtlinie* und anschließend auf *Bearbeiten*.

3 Fügen Sie der Computerkonfiguration das MSI-Paket hinzu.

Abbildung 9-7 *Wählen Sie das hinzuzufügende MSI-Paket aus.*



9.2.1 Befehlszeilenvariablen

Für die MSI-Installation sind Optionen über Befehlszeilenvariablen verfügbar. Diese müssen in der Verknüpfung mit der ausführbaren Datei festgelegt sein, die für die Ausführung im Administrator-Modus festgelegt ist. Wenn Sie eine Variable verwenden möchten, muss folgende Befehlszeile in der MSI-Verknüpfung eingegeben werden:

`"...\setup.exe" /a /V"variables"`. Geben Sie zwischen den Anführungszeichen einen beliebigen der unten angegebenen Befehle ein. Trennen Sie mehrere Variablen durch ein einfaches Leerzeichen.

Beispiel: Mit `setup.exe /a /V"STDRV=stateful STBGL=1"` wird ein MSI-Paket erstellt, bei dem der Endpoint Security Client 3.5 im "Alle Stateful"-Modus unter strikter Beachtung einer weißen Liste gebootet wird.

Hinweis: Das Booten im Stateful-Modus kann zu Interoperabilitätsproblemen führen (DHCP-Adressverzögerungen, Novell-Netzwerk-Interoperabilitätsprobleme usw.).

Es stehen folgende Befehlszeilenvariablen zur Verfügung:

Tabelle 9-1 *Befehlszeilenvariablen*

Befehlszeilenvariable	Beschreibung	Hinweise
STDRV=stateful	NDIS-Treiber zur Bootzeit "Alle Stateful".	Ändert den Standardstatus des NDIS-Treibers von "Alle geöffnet" in "Alle Stateful". Dadurch wird der gesamte Netzwerkverkehr beim Booten so lange zugelassen, bis der Endpoint Security Client 3.5 sein Verzeichnis bestimmt hat.
/qn	Stille Installation.	Verwenden Sie diese Variable, um den Standard-MSI-Installationsvorgang zu unterdrücken. Der Endpoint Security Client 3.5 wird beim nächsten Neustart durch den Benutzer aktiviert.
STRBR=ReallySuppress	Kein Neustart bei Abschluss der Installation.	Die Sicherheitsbeschränkungen und der Client-Selbstschutz sind erst nach dem ersten Neustart voll funktionsfähig.
STBGL=1	Strikte Beachtung einer weißen Liste bei der Anwendungssteuerung.	Es MUSS eine Richtlinie erstellt werden, die die Anwendung auf der weißen Liste identifiziert, die mit dieser Richtlinie verteilt wird.
STUPGRADE=1	Aufrüsten des Endpoint Security Client 3.5	Verwenden Sie diese Variable zum Aufrüsten des Endpoint Security Client 3.5.
STUNINSTALL=1	Deinstallieren des Endpoint Security Client 3.5	Verwenden Sie diese Variable zum Deinstallieren des Endpoint Security Client 3.5.
STUIP="Passwort"	Deinstallation mit Passwort	Verwenden Sie diese Variable, wenn ein Deinstallationspasswort aktiviert ist.
STNMS="MS-Name"	Ändern des Verwaltungsdienst-Namens.	Ändert den Verwaltungsdienst-Namen für den Endpoint Security Client 3.5.

Befehlszeilenvariable	Beschreibung	Hinweise
POLICYTYPE=1	Ändern des Endpoint Security Client 3.5 in computerbasierte Richtlinien.	Mit dieser Variable ändern Sie mit dem MSI installierte Endpoint Security Clients so, dass computerbasierte statt benutzerbasierte Richtlinien akzeptiert werden.
POLICYTYPE=2	Ändern des Endpoint Security Client 3.5 in benutzerbasierte Richtlinien.	Mit dieser Variable ändern Sie mit dem MSI installierte Endpoint Security Clients so, dass benutzerbasierte statt computerbasierte Richtlinien akzeptiert werden.
STVA="Adaptername"	Hinzufügen eines virtuellen Adapters.	Mit dieser Variable aktivieren Sie die Richtliniensteuerung eines virtuellen Adapters.
/L*v c:\log.txt	Einschalten·der Protokollierung.	Mit dieser Variable schalten Sie die Protokollierung bei der Installation ein. Andernfalls muss dies über die Endpoint Security Client-Diagnosetools vorgenommen werden (siehe Administratoren-Handbuch).

9.2.2 Verteilen einer Richtlinie mit dem MSI-Paket

Die in der MSI-Installation enthaltene Standardrichtlinie kann durch eine firmenintern konfigurierte Richtlinie ersetzt werden. So verteilen Sie eine bestimmte Richtlinie mit dem MSI-Image:

1. Erstellen Sie eine Richtlinie, die per Verwaltungskonsole an alle Benutzer verteilt werden soll. Details zur Richtlinienerstellung finden Sie im *ZENworks Endpoint Security Management-Administratorenhandbuch*.
2. Exportieren Sie die Richtlinie und speichern Sie diese als `policy.sen`.

   Hinweis: Alle auf diese Weise (unverwaltet) verteilten Richtlinien müssen `policy.sen` genannt werden, damit sie vom Endpoint Security Client 3.5 akzeptiert werden. Nicht `policy.sen` genannte Richtlinien werden vom Endpoint Security Client 3.5 nicht implementiert.
3. Öffnen Sie den Ordner, in den die Richtlinie exportiert wurde, und kopieren Sie die Dateien `policy.sen` und `setup.sen`.
4. Wechseln Sie zu dem erstellten MSI-Image und öffnen Sie den Ordner `\Programme\Novell\ZENworks Security Client\`.
5. Fügen Sie die Dateien `policy.sen` und `setup.sen` in den Ordner ein. Dadurch werden die Standarddateien `policy.sen` und `setup.sen` ersetzt.

9.2.3 Benutzerinstallation des Endpoint Security Client 3.5 per MSI

Wenn sich der Endbenutzer bei der Domäne erneut authentifiziert (durch Neubooten des Computers), wird das MSI-Installationspaket vor dessen Anmeldung ausgeführt. Nach Abschluss wird der Computer neu gebootet und die Anmeldung des Benutzers am Computer wird zugelassen. Der Endpoint Security Client 3.5 wird installiert und auf dem Computer ausgeführt.

9.3 Ausführen des Endpoint Security Client 3.5

Der Endpoint Security Client 3.5 wird automatisch beim Systemstart ausgeführt. Informationen zum Ausführen des Endpoint Security Client 3.5 finden Sie im *ZENworks Endpoint Security Client-Benutzerhandbuch*.

Das Benutzerhandbuch kann an alle Benutzer verteilt werden, damit diese die Funktionsweise ihrer neuen Endgerät-Sicherheitssoftware besser verstehen.

Installation von ZENworks Endpoint Security Client 4.0

10

Der Novell® ZENworks® Endpoint Security Client 4.0 ist ein Client zur Unterstützung von Microsoft Windows Vista mit Support Pack 1 im 32-Bit-Modus und Windows Server 2008 im 32-Bit-Modus. Der Endpoint Security Client 4.0 nutzt sowohl den ZENworks Endpoint Security Management 3.5-Server als auch die zugehörige Verwaltungskonsole. Sie haben nun die Möglichkeit, Windows XP mit der 3.5 Client-Instanz und Windows Vista mit der 4.0 Client-Instanz zu verwalten.

Auf den folgenden Seiten wird der Installationsvorgang für die Standard- und die MSI-Installation beschrieben.

Bei der Standardinstallation wird der Endpoint Security Client 4.0 nur auf dem aktuellen Computer installiert.

Bei der MSI-Installation wird das Installationsprogramm im Administrator-Modus (`/a`) gestartet und ein MSI-Paket der Software erstellt. Dieses Paket kann anschließend verteilt oder an einem bestimmten Ort im Netzwerk verfügbar gemacht werden. Die erforderlichen Benutzereingaben sind dabei vorkonfiguriert. So können die einzelnen Benutzer die Software mit vordefinierten Serverwerten installieren.

10.1 Standardinstallation von Endpoint Security Client 4.0

Bei diesem Vorgang wird der ZENworks Endpoint Security Client 4.0 nur auf dem aktuellen Computer installiert.

Vor dem Beginn:

- Überprüfen Sie, ob alle Sicherheitspatches für Microsoft* sowie die Antivirussoftware installiert und aktuell sind. Die Endpoint Security Client 4.0-Software kann unter Windows Vista mit Support Pack 1 und auf Windows Server 2008 installiert werden. Beide müssen im 32-Bit-Modus ausgeführt werden.
- Novell empfiehlt, während der Installation des Endpoint Security Client 4.0 Antivirus-/Spyware-Software zu schließen, die sich möglicherweise auf gültige Registrierungsfunktionen auswirkt.
- Für den verwalteten Endpoint Security Client ist eine SSL-Kommunikation zur ZENworks Endpoint Security Management Service-Komponente erforderlich. Wenn Sie bei der Installation des Verwaltungsdienstes oder der Einzelserverinstallation die Option

"eigensignierte Zertifikate" ausgewählt haben, muss auf dem Endgerät, auf dem der Security Client ausgeführt wird, das Zertifikat im ordnungsgemäßen Kontext (vorzugsweise im lokalen Computer-Kontext) installiert sein.

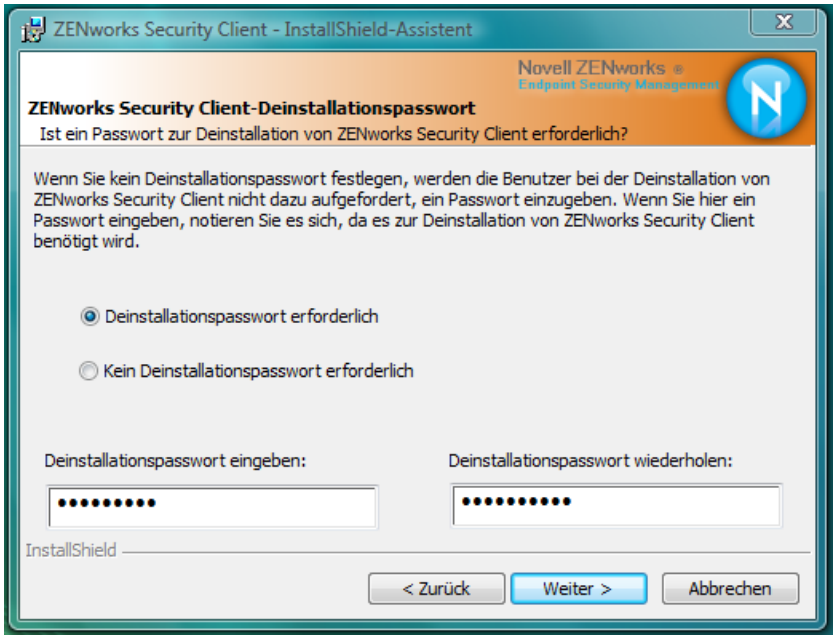
Sie können diesen Vorgang automatisch durchführen, indem Sie die Datei `ESM-MS.cer` in den gleichen Ordner legen, der auch die Installationsdatei des Endpoint Security Client `Setup.exe` enthält. Alternativerweise können Sie den gesamten `ESM Setup Files`-Ordner aus der Verwaltungsdienstinstallation (oder der Einzelserverinstallation) in den Ordner mit der Installationsdatei von Endpoint Security Client `Setup.exe` kopieren. Stellen Sie sicher, dass die Datei `ESM-MS.cert` im Ordner `ESM Setup Files` liegt und dass der Ordner `ESM Setup Files` heißt. Dadurch wird das Zertifikat automatisch auf dem Computer (das heißt für alle Benutzer) installiert. Dieser Vorgang kann auch mit der von Novell ausgegebenen Datei `license.dat` durchgeführt werden.

Wählen Sie im Installationsmenü das entsprechende *ZENworks Security Client*-Installationsverzeichnis aus.

1. Doppelklicken Sie auf `Setup.exe`, um den Installationsvorgang zu starten.
2. Wählen Sie für diese Installation die gewünschte Sprache aus und klicken Sie auf *OK*.

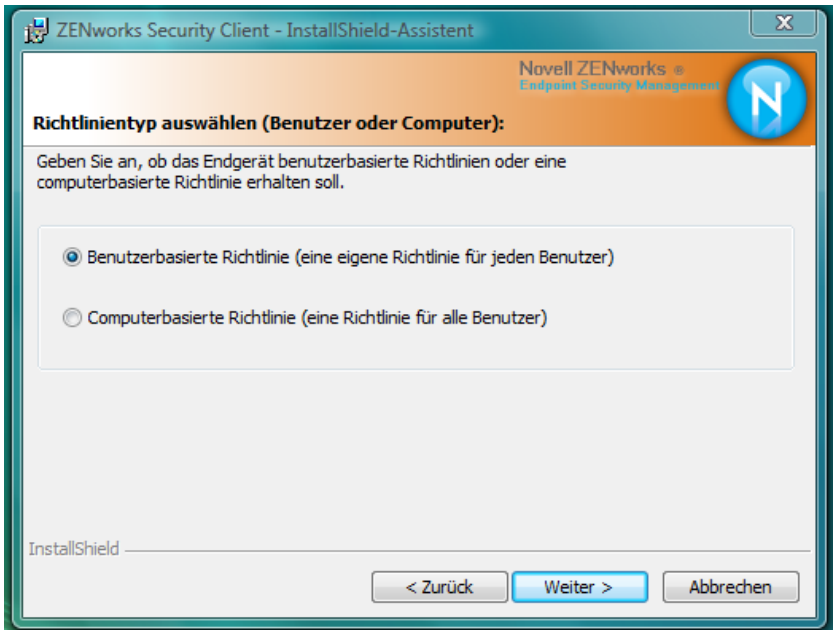
   Unter anderem stehen folgende Sprachen zur Auswahl:

   - Chinesisch-vereinfacht
   - Chinesisch-traditionell
   - Englisch (Standardsprache)
   - Französisch
   - Deutsch
   - Italienisch
   - Japanisch
   - Portugiesisch
   - Spanisch-traditionell
3. Für den Endpoint Security Client 4.0 müssen Sie Microsoft Web Services Enhancements (WSE) 2.0 mit Service Pack 3 und Microsoft Visual C++ 2008 auf Ihrem Computer installiert haben, bevor Sie mit der Installation des Client beginnen können. Wenn diese Komponenten während des Installationsprozesses nicht gefunden werden, wird der folgende Bildschirm angezeigt. Klicken Sie auf *Installieren*, um diese erforderlichen Komponenten zu installieren.
4. Falls noch nicht geschehen, schalten Sie Antivirus- und Anti-Spyware-Software aus, bevor Sie im Begrüßungsbildschirm auf *Weiter* klicken.
5. Akzeptieren Sie den Lizenzvertrag und klicken Sie dann auf *Weiter*.



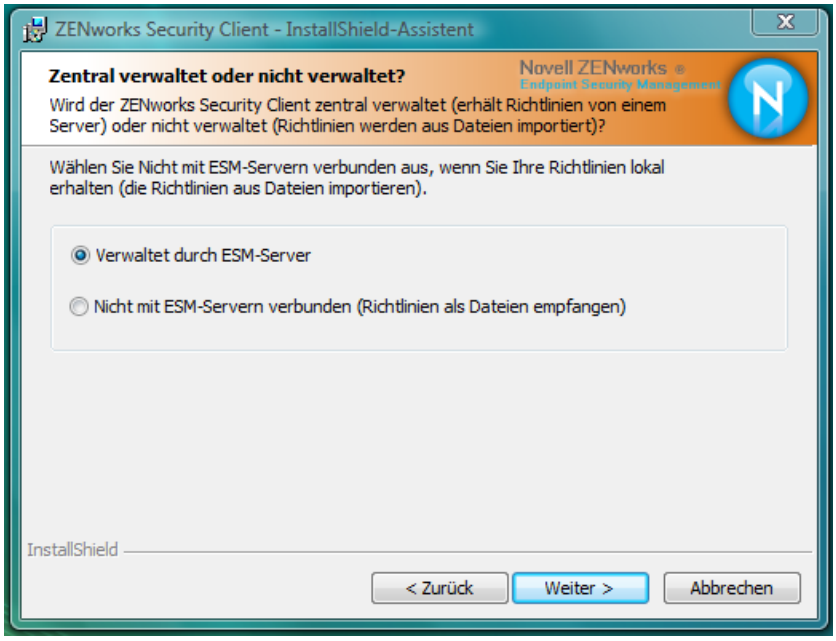
6 Wählen Sie *Erfordert ein Deinstallationspasswort*. Auf diese Weise kann der Benutzer den Endpoint Security Client 4.0 nicht deinstallieren (empfohlen).

7 Fügen Sie ein Passwort zur Deinstallation hinzu, bestätigen Sie das Passwort und klicken Sie auf *Weiter*.



8 Wählen Sie einen Richtlinientyp aus. Sie können entweder eine benutzerbasierte Richtlinie wählen, bei der jeder Benutzer über eine eigene Richtlinie verfügt, oder eine computerbasierte Richtlinie, bei der eine Richtlinie für alle Benutzer verwendet wird. Klicken Sie auf *Weiter*.

Hinweis: Wählen Sie "Benutzerbasierte Richtlinie", falls Sie in Ihrem Netzwerk eDirectory als Verzeichnisdienst verwenden. eDirectory unterstützt keine computerbasierten Richtlinien.



9 Wählen Sie, wie die Richtlinien empfangen werden sollen (verwaltet durch ESM-Server für verwaltete Clients oder lokal für eine unverwaltete (Einzelplatz-) Konfiguration abgerufen). Klicken Sie auf *Weiter*.

Ausführliche Informationen zu einer unverwalteten Installation erhalten Sie unter Kapitel 11, „Installation von ZENworks Endpoint Security Management im unverwalteten Modus“, auf Seite 81.

10 (Optional) Wenn Sie unter Schritt 9 die Option *Verwaltet durch ESM-Server* gewählt haben, geben Sie den Namen des Servers ein, der den Verwaltungsdienst unterstützt.

Der von Ihnen eingegebene Servername muss dem Namen unter "Ausgestellt für" entsprechen, der auf dem Server, auf dem ZENworks Endpoint Management Service oder Single Server installiert wurden, im Zertifikat der Herkunftsverbürgung angegeben wurde. Dies ist entweder der Name des NETBIOS oder der Fully Qualified Domain Name (FQDN, vollqualifizierter Domänenname) des Servers, auf dem die ZENworks Endpoint Management Service-Komponente ausgeführt wird. Klicken Sie nach dem Eingeben auf *Weiter*.

11 Klicken Sie auf *Installieren*, um mit der Installation zu beginnen.

12 Starten Sie nach dem Installieren der Software auf Aufforderung den Computer neu.

Eine Liste mit Funktionen, die für den 4.0 Client für Vista nicht verfügbar sind, erhalten Sie unter Abschnitt 10.4, „Im Endpoint Security Client 4.0 nicht unterstützte Funktionen“, auf Seite 79.

10.2 MSI-Installation

Bei diesem Vorgang wird ein MSI-Paket für den Endpoint Security Client 4.0 erstellt. Mit diesem Paket kann ein Systemadministrator die Installation über eine Active Directory-Richtlinie oder über andere Software-Verteilungsmethoden an eine Gruppe von Benutzern veröffentlichen.

- Abschnitt 10.2.3, „Abschließen der Installation“, auf Seite 75
- Abschnitt 10.2.4, „Befehlszeilenvariablen“, auf Seite 77
- Abschnitt 10.2.5, „Verteilen einer Richtlinie mit dem MSI-Paket“, auf Seite 78

10.2.1 Verwenden des Hauptinstallationsprogramms

Wenn Sie die Installation von der CD oder über das ISO-Hauptinstallationsprogramm ausführen und keine Befehlszeilenvariablen ausführen möchten:

1. Legen Sie die CD ein und warten Sie, bis das Hauptinstallationsprogramm startet.
2. Klicken Sie auf *Produktinstallation*.
3. Klicken Sie auf *Security Client*.
4. Klicken Sie auf *ZSC-MSCI-Paket erstellen*.
5. Fahren Sie mit Abschnitt 10.2.3, „Abschließen der Installation“, auf Seite 75 fort.

10.2.2 Verwenden der Datei Setup.exe

Wenn Sie nur die Datei `setup.exe` für die Installation verwenden:

1. Klicken Sie mit der rechten Maustaste auf `setup.exe`.

   Sie finden die ausführbare Datei auf der CD im Verzeichnis `D:\ESM32\ZSC`.
2. Wählen Sie *Verknüpfung erstellen*.
3. Klicken Sie mit der rechten Maustaste auf die Verknüpfung und klicken Sie dann auf *Eigenschaften*.
4. Geben Sie am Ende des Feldes *Ziel* nach den Anführungszeichen ein Leerzeichen ein, und geben Sie danach den Befehl `/a` ein.

   Beispiel: `C:\Dokumente und Einstellungen\euser\Desktop\CL-Release-3.2.455\setup.exe`

   Für die MSI-Installation stehen mehrere Befehlszeilenvariablen zur Verfügung. Weitere Einzelheiten finden Sie unter Abschnitt 9.2.1, „Befehlszeilenvariablen“, auf Seite 66.
5. Klicken Sie auf *OK*.
6. Doppelklicken Sie zum Starten des MSI-Installationsprogramms auf die Verknüpfung.
7. Fahren Sie mit Abschnitt 10.2.3, „Abschließen der Installation“, auf Seite 75 fort.

10.2.3 Abschließen der Installation

Führen Sie entweder Verwenden des Hauptinstallationsprogramms oder Verwenden der Datei Setup.exe aus, und verwenden Sie diesen Vorgang dann, um die Installation des Client abzuschließen.

1. Klicken Sie zum Fortfahren im Begrüßungsbildschirm auf *Weiter*.
2. Wählen Sie *Erfordert ein Deinstallationspasswort* (empfohlen) und geben Sie das Passwort ein. Klicken Sie auf *Weiter*.

Hinweis: Wenn Sie den Endpoint Security Client über ein MSI-Paket deinstallieren, müssen Sie das Deinstallationspasswort über die MSI-Eigenschaften angeben (siehe Tabelle 10-1 auf Seite 77).

3 Wählen Sie einen Richtlinientyp aus. Sie können entweder eine benutzerbasierte Richtlinie wählen, bei der jeder Benutzer über eine eigene Richtlinie verfügt, oder eine computerbasierte Richtlinie, bei der eine Richtlinie für alle Benutzer verwendet wird. Klicken Sie auf *Weiter*.

Hinweis: Wählen Sie "Benutzerbasierte Richtlinie", falls Sie in Ihrem Netzwerk eDirectory als Verzeichnisdienst verwenden. eDirectory unterstützt keine computerbasierten Richtlinien.

4 Wählen Sie, wie die Richtlinien empfangen werden sollen (verwaltet durch ESM-Server für verwaltete Clients oder lokal für eine unverwaltete (Einzelplatz-) Konfiguration abrufen).

5 (Optional) Wenn Sie unter Schritt 4 die Option *Verwaltet durch ESM-Server* ausgewählt haben:

- Der von Ihnen eingegebene Servername muss dem Namen unter "Ausgestellt für" entsprechen, der auf dem Server, auf dem ZENworks Endpoint Management Service oder Single Server installiert wurden, im Zertifikat der Herkunftsverbürgung angegeben wurde. Dies ist entweder der Name des NETBIOS oder der Fully Qualified Domain Name (FQDN, vollqualifizierter Domänenname) des Servers, auf dem die ZENworks Endpoint Management Service-Komponente ausgeführt wird.

6 (Optional) Geben Sie im dafür vorgesehenen Feld eine E-Mail-Adresse ein, damit Sie bei einer fehlerhaften Installation benachrichtigt werden.

7 Geben Sie den Netzwerkstandort an, an dem Sie das MSI-Image erstellen möchten, oder navigieren Sie in das gewünschte Verzeichnis, indem Sie auf die Schaltfläche *Ändern* klicken.

8 Klicken Sie zum Erstellen des MSI-Image auf *Installieren*. Klicken Sie auf *Fertig stellen*, um das Installationsprogramm abzuschließen.

9 Navigieren Sie in das Verzeichnis, in das Sie das MSI-Image erstellt haben, und öffnen Sie den Ordner `\Programme\\Novell ZENworks\Endpoint Security Client\`.

10 Kopieren Sie das SSL-Zertifikat für den Verwaltungsdienst (`ESM-MS.cer` oder das firmeninterne Zertifikat) und den Novell-Lizenzschlüssel in diesen Ordner. Ersetzen Sie dabei die aktuell im Ordner befindlichen Standarddateien von 0 KB.

Das SSL-Zertifikat für ESM-MS ist im Ordner der `ZENworks Endpoint Security Management-Setupdateien` verfügbar. Der Lizenzschlüssel wird separat per E-Mail versendet. Wenn Sie den 60-tägigen Evaluierungszeitraum in Anspruch nehmen, ist zu diesem Zeitpunkt kein Lizenzschlüssel erforderlich.

10.2.4 Befehlszeilenvariablen

Für eine MSI-Installation sind Optionen für Befehlszeilenvariablen verfügbar. Diese müssen in der Verknüpfung mit der ausführbaren Datei festgelegt sein, die für die Ausführung im Administrator-Modus festgelegt ist. Wenn Sie eine Variable verwenden möchten, muss folgende Befehlszeile in der MSI-Verknüpfung eingegeben werden:

`"...\setup.exe" /a /V"variables"`. Geben Sie zwischen den Anführungszeichen einen beliebigen der unten angegebenen Befehle ein. Trennen Sie mehrere Variablen durch ein einfaches Leerzeichen.

Es stehen folgende Befehlszeilenvariablen zur Verfügung:

Tabelle 10-1 *Befehlszeilenvariablen*

Befehlszeilenvariable	Beschreibung	Hinweise
/qn	Stille Installation.	Unterdrückt den Standard-MSI-Installationsvorgang. Der Endpoint Security Client wird beim nächsten Neustart durch den Benutzer aktiviert.
SESMSG=1	Zeigt dem Endbenutzer eine Meldung an, dass für geschützte Dateien bei Verwendung einer Verschlüsselungsrichtlinie die Verschlüsselung nicht automatisch entfernt werden kann.	Standardwert ist 0 (Meldungen nicht anzeigen), um die Deinstallation "still" durchzuführen.
STRBR=ReallySuppress	Kein Neustart bei Abschluss der Installation.	Die Sicherheitsbeschränkungen und der Client-Selbstschutz sind erst nach dem ersten Neustart voll funktionsfähig.
STUPGRADE=1	Aufrüsten des Endpoint Security Client 4.0	Rüstet den Endpoint Security Client 4.0 auf.
STUNINSTALL=1	Deinstallieren des Endpoint Security Client 4.0	Deinstalliert den Endpoint Security Client 4.0.
STUIP="Passwort"	Deinstallation mit Passwort	Verwenden Sie diese Variable, wenn ein Deinstallationspasswort aktiviert ist.
STNMS="MS-Name"	Ändern des Verwaltungsdienst-Namens.	Ändert den Verwaltungsdienst-Namen für den Endpoint Security Client 4.0.

Befehlszeilenvariable	Beschreibung	Hinweise
POLICYTYPE=1	Ändern des Endpoint Security Client 4.0 in computerbasierte Richtlinien.	Ändert über MSI installierte Endpoint Security Clients, damit diese computerbasierte Richtlinien anstelle von benutzerbasierten Richtlinien akzeptieren.
POLICYTYPE=2	Ändern des Endpoint Security Client 4.0 in benutzerbasierte Richtlinien.	Ändert über MSI installierte ZENworks Security 4.0 Clients für Vista, damit diese benutzerbasierte Richtlinien anstelle von computerbasierten Richtlinien akzeptieren.
STVA="Adaptername"	Virtuellen Adapter hinzufügen	Aktiviert die Richtliniensteuerung über einen virtuellen Adapter.
/L*v c:\log.txt	Einschalten·der Protokollierung.	Aktiviert die Protokollierung bei der Installation. Falls Sie diese Variable nicht verwenden, müssen Sie die Protokollierung über die Endpoint Security Client-Diagnosetools vornehmen.

10.2.5 Verteilen einer Richtlinie mit dem MSI-Paket

Die in der MSI-Installation enthaltene Standardrichtlinie kann durch eine firmenintern konfigurierte Richtlinie ersetzt werden. So verteilen Sie eine bestimmte Richtlinie mit dem MSI-Image:

1. Erstellen Sie eine Richtlinie, die per Verwaltungskonsole an alle Benutzer verteilt werden soll. Details zur Richtlinienerstellung finden Sie im *ZENworks Endpoint Security Management-Administratorenhandbuch*.
2. Exportieren Sie die Richtlinie und benennen Sie sie in `policy.sen` um.

   Alle auf diese Weise (unverwaltet) verteilten Richtlinien müssen `policy.sen` genannt werden, damit sie vom Endpoint Security Client 4.0 akzeptiert werden. Nicht `policy.sen` genannte Richtlinien werden vom Endpoint Security Client 4.0 nicht implementiert.
3. Öffnen Sie den Ordner, in den die Richtlinie exportiert wurde, und kopieren Sie die Dateien `policy.sen` und `setup.sen`.
4. Wechseln Sie zu dem erstellten MSI-Image und öffnen Sie den Ordner `\Programme\Novell ZENworks\Endpoint Security Client\`.
5. Fügen Sie die Dateien `policy.sen` und `setup.sen` in den Ordner ein. Dadurch werden die Standarddateien `policy.sen` und `setup.sen` ersetzt.

10.3 Ausführen des Endpoint Security Client 4.0

Der Endpoint Security Client 4.0 wird automatisch beim Systemstart ausgeführt. Informationen zum Ausführen des Endpoint Security Client 4.0 finden Sie im *ZENworks Endpoint Security Client 4.0-Benutzerhandbuch*.

Das Benutzerhandbuch kann an alle Benutzer verteilt werden, damit diese die Funktionsweise ihrer neuen Endgerät-Sicherheitssoftware besser verstehen.

10.4 Im Endpoint Security Client 4.0 nicht unterstützte Funktionen

Zu den Funktionen, die von Endpoint Security Client 4.0 nicht bzw. nur teilweise unterstützt werden, zählen:

- Client Self Defense.
- Modemunterstützung.
- Skripts.
- Manuelles Ändern von Firewalls an einem Standort.
- Mehrere sichtbare Firewalls an einem Standort. Nur die standardmäßige Firewall steht zur Verfügung.
- Integritätsregeln.
- Anwendungsblockierung.
- Die angezeigten Informationen beim Platzieren der Maus auf das Symbol haben sich geändert. Das Symbol zeigt lediglich Informationen über Richtlinie und Standort an.
- USB-Konnektivität.
- Wi-Fi-Schlüsselverwaltung.
- Kabelgebundene Verbindungen haben keinen höheren Stellenwert als Wireless-Verbindungen.
- Endpoint Security Client-Updates (nach Richtlinie).
- Zeitüberschreitung bei der VPN-Authentifizierung.
- Automatische Wiedergabe für die Speichergerätesteuerung.
- Telefonbucheinträge in der Netzwerkumgebung.

Installation von ZENworks Endpoint Security Management im unverwalteten Modus

11

Der ZENworks® Security Client und die Verwaltungskonsole können von einem Unternehmen auch im unverwalteten Modus ausgeführt werden (ohne Verbindung zum Richtlinienverteilungsservice oder dem Verwaltungsdienst). Diese Installationsoption ist in erster Linie für die Einrichtung einfacher Evaluierungen vorgesehen. Diese Option ist außerdem besonders für Unternehmen mit wenig oder keinem Speicherplatz auf dem Server oder einfachen Sicherheitsansprüchen geeignet. Mit dieser Konfiguration sind jedoch keine schnellen Richtlinienaktualisierungen oder Compliance-Berichterstellungen verfügbar.

11.1 Installation von Endpoint Security Client im unverwalteten Modus

Befolgen Sie für die Installation eines unverwalteten Endpoint Security Client die Anweisungen in Kapitel 9, „Installation von Endpoint Security Client 3.5“, auf Seite 61 und wählen Sie die Option *Nicht an ESM-Server angeschlossen (Richtlinien als Dateien empfangen)*. Die Installation überspringt dann Fragen zu den Servernamen und installiert den Endpoint Security Client auf diesem Computer (ein MSI-Paket kann auch für einen unverwalteten Endpoint Security Client erstellt werden).

Abbildung 11-1 *Wählen Sie "Keine Verbindung zu ZENworks Endpoint Security Management-Servern".*

11.2 Einzelplatz-Verwaltungskonsole

Diese Konfiguration erlaubt die Installation einer ZENworks Endpoint Security Management-Verwaltungskonsole und die Erstellung von Richtlinien ohne Verbindung zu einem außerhalb befindlichen Verwaltungsdienst oder die Verteilung von Richtlinien mit dem

Richtlinienverteilungsservice. Wählen Sie im Hauptinstallationsmenü *Einzelplatz-Verwaltungskonsole installieren* und befolgen Sie für die Installation die Anweisungen in Kapitel 7, „Durchführen der Installation der Verwaltungskonsole“, auf Seite 45.

Zu Beginn der Installation wird zunächst eine SQL-Datenbank installiert (wenn eine Datenbank auf dem Computer vorhanden ist, werden vom Installationsprogramm stattdessen die geeigneten Datenbanken eingerichtet). Die Installation stoppt, sobald die Datenbank installiert ist. Der Computer muss neu gestartet werden, um die SQL-Datenbank zu aktivieren. Aktivieren Sie zum Fortfahren die Installation erneut, nachdem der Computer neu gebootet wurde.

Mit Ausnahme der Berichterstellung sind die meisten Richtlinienfunktionen verfügbar. Alle exportierten Richtliniendateien müssen an ein Endpoint Security Client-Verzeichnis `\Programme\Novell\ZENworks Security Client\` verteilt werden.

11.3 Verteilen unverwalteter Richtlinien

So verteilen Sie unverwaltete Richtlinien:

1. Suchen Sie die `setup.sen`-Datei der Verwaltungskonsole und kopieren Sie sie in einen separaten Ordner.

   Die `setup.sen`-Datei wird bei der Installation der Verwaltungskonsole generiert und im Verzeichnis `\Programme\Novell\ESM Management Console\` abgelegt.
2. Erstellen Sie eine Richtlinie in der Verwaltungskonsole. (Weitere Informationen finden Sie im *ZENworks Endpoint Security Management-Administratorenhandbuch*.)
3. Verwenden Sie den Befehl *Exportieren*, um die Richtlinie in den Ordner zu exportieren, der auch die Datei `setup.sen` enthält. Alle Richtlinien müssen den Namen `policy.sen` erhalten, damit der Endpoint Security Client sie akzeptiert.
4. Verteilen Sie die Dateien `policy.sen` und `setup.sen`. Diese Dateien müssen für alle unverwalteten Clients in das Verzeichnis `\Programme\Novell\ZENworks Security Client\` kopiert werden.

   Die Datei `setup.sen` muss nur einmal mit der ersten Richtlinie auf die unverwalteten Geräte kopiert werden. Danach müssen nur neue Richtlinien verteilt werden.

Wenn ein unverwalteter Endpoint Security Client auf demselben Computer wie die Einzelplatz-Verwaltungskonsole installiert wird, muss die Datei `setup.sen` ebenfalls in das Verzeichnis `\Programme\Novell\ZENworks Security Client\` kopiert werden. Wenn ein unverwalteter Endpoint Security Client nach dem Einzelplatz-Editor auf dem Computer installiert wird, muss die Datei wie oben beschrieben manuell übertragen werden.

Mit einem Klick auf die Schaltfläche *Veröffentlichen* wird die Richtlinie sofort an den unverwalteten Endpoint Security-Client dieses Computers veröffentlicht. Verwenden Sie die oben beschriebene Exportfunktion, wenn Sie Richtlinien für mehrere unverwaltete Benutzer verfügbar machen möchten.

Aktualisierungen für Dokumentationen

A

Dieser Abschnitt enthält Informationen zu Änderungen der Dokumentation, die nach der ursprünglichen Veröffentlichung für Version 3.5 in diesem *Novell ZENworks Endpoint Security Management-Installationshandbuch* vorgenommen wurden. Die Änderungen sind nach Veröffentlichungsdatum sortiert.

Die Dokumentationen für dieses Produkt stehen im Web im HTML-Format und als PDF-Datei zur Verfügung. Sowohl die HTML- als auch die PDF-Dokumentationen wurden im Hinblick auf die in diesem Abschnitt aufgeführten Änderungen auf den neuesten Stand gebracht.

Ob es sich bei der von Ihnen verwendeten PDF-Dokumentation um die neueste Ausgabe handelt, sehen Sie am Veröffentlichungsdatum auf der Titelseite des Dokuments.

Die Dokumentation wurde an folgenden Terminen aktualisiert:

- Abschnitt A.1, „5. Januar 2009“, auf Seite 83

A.1 5. Januar 2009

Die folgenden Abschnitte wurden aktualisiert:

Standort	Aktualisierung
Alle Abschnitte	Der Name des Client wurde im ganzen Handbuch geändert. Korrekterweise heißt der Client jetzt Novell ZENworks Endpoint Security Client. In den jeweiligen Kapiteln werden die Clients Endpoint Security Client 3.5 (für Windows XP) und Endpoint Security Client 4.0 (für Windows Vista) genannt.
Abschnitt 1.1, „Systemvoraussetzungen“, auf Seite 10	Systemanforderungen für den neuen Vista-Client und die Einzelplatz-Verwaltungskonsole wurden hinzugefügt.
Kapitel 9, „Installation von Endpoint Security Client 3.5“, auf Seite 61	Informationen, dass der Endpoint Security Client 3.5 für Windows XP entwickelt wurde, sowie die Namensänderung wurden hinzugefügt.
Kapitel 10, „Installation von ZENworks Endpoint Security Client 4.0“, auf Seite 71	Ein Kapitel über Endpoint Security Client 4.0 (für Windows Vista) wurde hinzugefügt.