AUTHORIZED DOCUMENTATION

Endpoint Security Client 4.0-Benutzerhandbuch

December 22, 2008

Novell®
ZENworks® Endpoint Security Management

4.0

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 Client 4.0-Benutzerhandbuch* unterstützt den Endbenutzer bei der Verwendung des Endpoint Security Client 4.0 für Microsoft Windows* Vista* und Windows Server 2008*.

Die Informationen in diesem Handbuch gliedern sich wie folgt:

Zielgruppe

Dieses Handbuch sollte allen Mitarbeitern des Unternehmens zur Verfügung gestellt werden, um das Verständnis des Endpoint Security Client zu erleichtern.

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).

Konventionen in der Dokumentation

In dieser Novell-Dokumentation wird ein „Größer als“-Zeichen (>) verwendet, um verschiedene Aktionen innerhalb eines Schritts und Meldungen in einem Querverweispfad voneinander zu trennen.

Ein Markensymbol (®, ™ usw.) kennzeichnet eine Novell-Marke. Ein Sternchen (*) kennzeichnet eine Drittanbieter-Marke.

Wenn ein Pfadname für bestimmte Plattformen mit einem umgekehrten Schrägstrich und für andere Plattformen mit einem Schrägstrich geschrieben werden kann, wird der Pfadname in diesem Handbuch mit einem umgekehrten Schrägstrich dargestellt. Benutzer von Plattformen wie Linux*, die einen Schrägstrich erfordern, sollten wie von der Software gefordert Schrägstriche verwenden.

Einführung

1

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.

Novell ZENworks Endpoint Security Management (ESM) wurde für den Schutz der Datenbestände in Unternehmen konzipiert. Es bedient sich hierzu des zentral verwalteten Tools ZENworks Security Client. Der ZENworks Endpoint Security Client 4.0 wird auf Windows Vista- und Windows Server 2008-Computern des Unternehmens installiert und setzt Sicherheitsrichtlinien durch, die durch das ESM-Verwaltungs- und Verteilungssystem geschrieben und verteilt wurden. Damit können Großunternehmen und kleine Firmen Richtlinien zur Computersicherheit auf Computern innerhalb und außerhalb des gesicherten Firmenbereichs erstellen, bereitstellen, durchsetzen und überwachen.

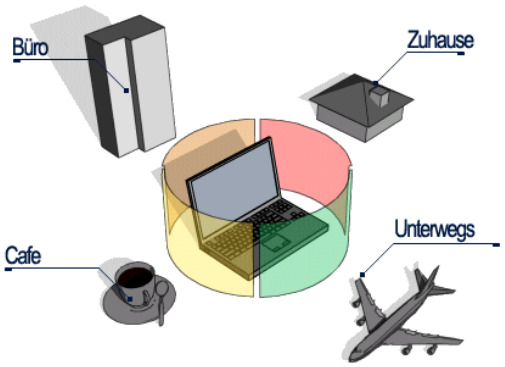
Folgende Abschnitte enthalten zusätzliche Informationen:

- Abschnitt 1.1, „Erzwungene Sicherheit für mobile Computer“, auf Seite 9
- Abschnitt 1.2, „Firewall-Schutz der NDIS-Schicht“, auf Seite 10

1.1 Erzwungene Sicherheit für mobile Computer

Sicherheit wird sowohl global als auch nach Netzwerkstandort durchgesetzt. Jeder Standort, der in einer Sicherheitsrichtlinie aufgeführt ist, bestimmt die Berechtigungen des Benutzers in dieser Netzwerkumgebung sowie die aktivierten Firewall-Einstellungen. Die Firewall-Einstellungen legen fest, welche Netzwerkports, Netzwerkadressen und Anwendungen Zugriff auf das Netzwerk erhalten und wie der Zugriff erteilt wird.

Abbildung 1-1 *ESM passt Sicherheitseinstellungen auf der Basis der erkannten Netzwerkumgebung an.*

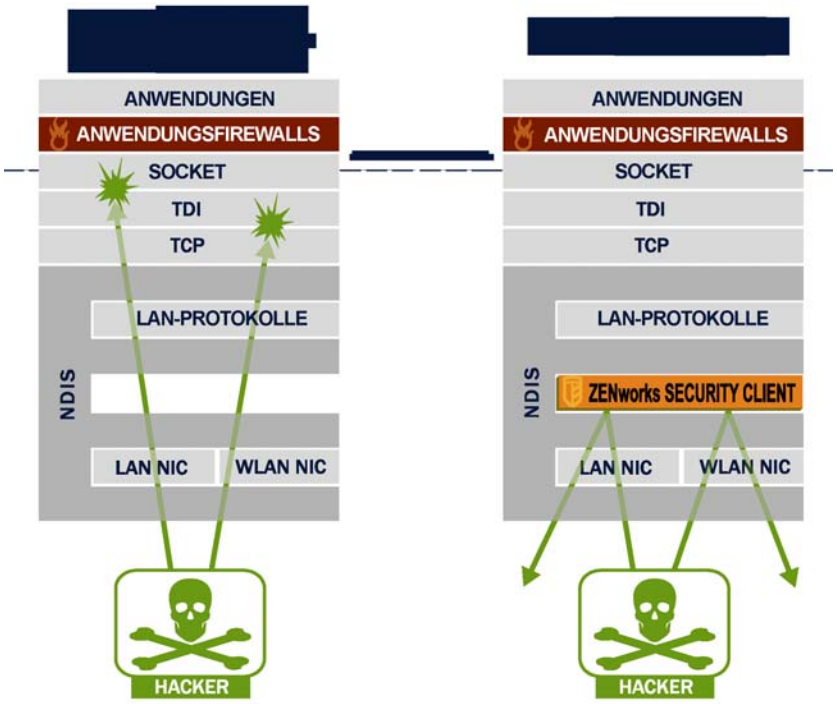


Der Normalbetrieb des Endpoint Security Client 4.0 ist für den Benutzer nicht sichtbar, nachdem die Netzwerkumgebungen definiert wurden. Gelegentlich können Schutzmaßnahmen des Endpoint Security Client 4.0 den normalen Betrieb unterbrechen. In diesem Fall informieren Meldungen und Hyperlinks die Benutzer über die Sicherheitsrichtlinie, welche Schutzmaßnahmen ergriffen wurden, und verweisen sie auf zusätzliche Informationen, die ihnen beim Beheben des Problems helfen.

1.2 Firewall-Schutz der NDIS-Schicht

Beim Sichern mobiler Geräte ist ESM typischen Technologien persönlicher Firewalls, die nur in der Anwendungsschicht oder als Firewall-Hook-Treiber arbeiten, überlegen. ESM-Client-Sicherheit ist in den NDIS-Treiber (NDIS - Network Driver Interface Specification) für jede Netzwerkschnittstellenkarte (NIC) integriert und bietet sicheren Schutz ab dem Augenblick, in dem Datenverkehr den Computer erreicht. Unterschiede zwischen ESM, der Anwendungsschicht-Firewalls und Filtertreibern werden in Abbildung 1-2, „Wirksamkeit einer·Firewall auf NDIS-Ebene“, auf Seite 10 verdeutlicht.

Abbildung 1-2 *Wirksamkeit einer·Firewall auf NDIS-Ebene*



Sicherheitsentscheidungen und Systemleistung werden optimiert, wenn Sicherheitsimplementierungen auf der niedrigsten geeigneten Schicht des Protokollstapels arbeiten. Mit dem Endpoint Security Client 4.0 wird unerwünschter Datenverkehr mithilfe der Technik "Adaptive Port Blocking" (zustandsabhängige Paketprüfung) auf die untersten Ebenen des NDIS-Treibers gebracht. Diese Methode schützt vor protokollbasierten Angriffen, einschließlich unzulässigen Portscans, SYN Flood- und anderen Angriffen.

Sie sollten unbedingt allen Betriebs- und Wartungsempfehlungen in diesem Dokument folgen, um zu gewährleisten, dass die Endgerät-Sicherheitsumgebung sicher ist.

Überblick über den Endpoint Security Client 4.0

2

Der ZENworks® Security Client schützt Computer·vor Dateninvasionsangriffen zu Hause, am Arbeitsplatz und unterwegs durch die Einhaltung von Sicherheitsrichtlinien, die vom Endpoint Secuirty Management-(ESM-)Administrator des Unternehmens festgelegt wurden. Die Firewall-Einstellungen, die für bestimmte Standorte definiert sind, werden automatisch angepasst, sobald Laptop-Benutzer vom Unternehmensnetzwerk in ihr Heimnetzwerk wechseln oder unterwegs sind und sich bei einem öffentlichen oder offenen Netzwerk anmelden.

Sicherheitsebenen werden auf verschiedene Benutzerstandorte angewendet, ohne dass der Benutzer über Expertenwissen oder Grundkenntnisse hinsichtlich Netzwerksicherheit, Portkonfiguration, versteckter gemeinsamer Dateien oder anderer technischer Details verfügen muss. Sie können die Endpoint Security Client-QuickInfos anzeigen, indem Sie mit der Maus über die Taskleiste fahren. Die QuickInfos enthalten Informationen zu den verfügbaren Standorten und Richtlinien (siehe Abbildung 2-1).

Abbildung 2-1 *Endpoint Security Client-QuickInfo*

Folgende Abschnitte enthalten zusätzliche Informationen:

- Abschnitt 2.1, „ESM-Terminologie“, auf Seite 11
- Abschnitt 2.2, „Anmelden beim Endpoint Security Client 4.0“, auf Seite 12

2.1 ESM-Terminologie

Die folgenden Begriffe werden in dieser Dokumentation häufig verwendet:

Standorte: Standorte sind einfache Definitionen, mit deren Hilfe Benutzer die Netzwerkumgebung erkennen können, in der sie sich befinden. Sie bieten sofortige Sicherheitseinstellungen (vom Administrator definiert) und gestatten es·dem Benutzer, die Einstellungen der Netzwerkumgebung zu speichern und die angewendeten Firewall-Einstellungen zu ändern.

Jeder Standort erhält eindeutige Sicherheitseinstellungen, die den Zugriff auf bestimmte Netzwerkefunktionen und bestimmte Hardware in Netzwerkumgebungen mit höherem Sicherheitsrisiko verhindern und breiteren Zugriff in verbürgten Umgebungen gewähren. Standorte definieren die folgenden Informationen:

- Die Häufigkeit, mit der der Endpoint Security Client diesen Standort auf aktualisierte Richtlinien überprüft.
- Die Berechtigungen zur Standortverwaltung, die einem Benutzer gewährt werden

- Die Firewall-Einstellungen, die an diesem Standort benutzt werden.
- Welcher Kommunikationshardware Verbindungen erlaubt sind.
- Auf welcher Ebene der Benutzer Wechseldatenträger (z. B. Thumbdrives und Speicherkarten) und/oder CD/DVD-RW-Laufwerke verwenden darf.
- Sämtliche Netzwerkumgebungen, die zur Definition des Standorts beitragen können.

Firewall-Einstellungen: Firewall-Einstellungen steuern die Konnektivität aller Netzwerkports (1-65535), Netzwerkpakete (ICMP, ARP usw.) und Netzwerkadressen (IP oder MAC) sowie, welche Netzwerkanwendungen (Dateifreigabe, Instant Messenger-Software usw.) eine Netzwerkverbindung erhalten dürfen, wenn die Einstellung angewendet wird. Drei Firewall-Einstellungen sind als Standards für ESM enthalten und können an einem Standort implementiert werden. Der ESM-Administrator kann auch spezifische Firewall-Einstellungen definieren, die hier nicht aufgeführt werden können.

- **Alle adaptiv:** Diese Firewall-Einstellung stellt alle Netzwerkports als "Stateful" ein (sämtlicher unerwünscht eingehender Netzwerkverkehr wird blockiert; sämtlicher ausgehender Netzwerkverkehr ist erlaubt). ARP und 802.1x-Pakete sind erlaubt und allen Netzwerkanwendungen ist eine Netzwerkverbindung erlaubt.
- **Alle geöffnet:** Diese Firewall-Einstellung stellt alle Netzwerkports als geöffnet ein (sämtlicher Netzwerkverkehr ist erlaubt). Alle Pakettypen sind zulässig. Sämtliche Netzwerkanwendungen dürfen eine Netzwerkverbindung aufbauen.
- **Alle geschlossen:** Diese Firewall-Einstellung schließt alle Netzwerkports und beschränkt alle Pakettypen.

Adapter: Bezieht sich auf drei Kommunikationsadapter, die sich gewöhnlich an einem Endgerät befinden:

- verbundene Adapter (LAN-Verbindungen)
- Wi-Fi-Adapter (PCMCIA Wi-Fi-Karten und integrierte Wi-Fi-Radios)

Bezieht sich auch auf Kommunikationshardware, die in einem Computer·enthalten sein kann, z. B. Infrarot-, Bluetooth*-, Firewire*- sowie serielle und parallele Anschlüsse.

Speichergeräte: Bezeichnet externe Speichergeräte, die eine Sicherheitsbedrohung darstellen können, wenn Daten auf diese Geräte an einem Endgerät kopiert oder davon übernommen werden. USB-Thumbdrives, Flash-Speicherkarten und SCSI PCMCIA-Speicherkarten mit herkömmlichen Zip*-, Disketten- und CDR-Laufwerken und die installierten CD/DVD-Laufwerke (einschließlich CD-ROM, CD-R/RW, DVD, DVD R/RW) können alle an einem einzelnen Standort blockiert, zugelassen oder schreibgeschützt bereitgestellt werden.

Netzwerkumgebungen: Eine Netzwerkumgebung ist die Kombination von Netzwerkdiensten und Service-Adressen, die zur Identifizierung eines Netzwerkstandorts erforderlich sind.

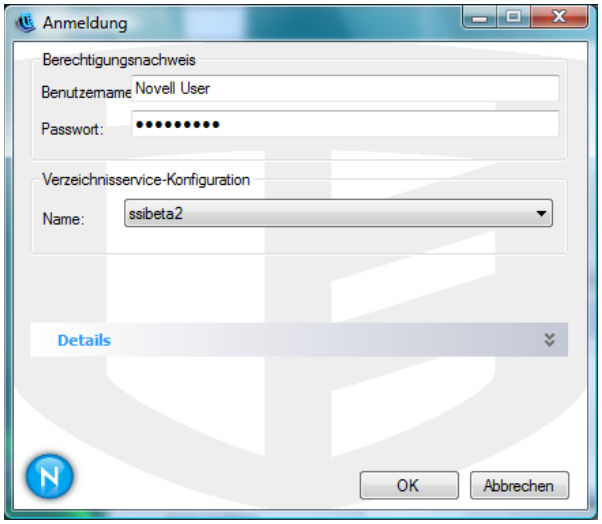
2.2 Anmelden beim Endpoint Security Client 4.0

Wenn Sie Mitglied der Active Directory-Domäne des Unternehmens sind, verwendet der Endpoint Security Client 4.0 Ihren Windows*-Benutzernamen und Ihr Passwort, um Sie beim Richtlinienverteilungsservice anzumelden. Dabei wird kein Popup-Fenster angezeigt. Wenn Sie Mitglied eines Novell eDirectory-Baums sind, werden Sie vom Endpoint Security Client 4.0 aufgefordert, Ihren Benutzernamen und Ihr Passwort einzugeben (siehe Abbildung 2-2).

Hinweis: Bei Novell eDirectory öffnet sich einmalig ein Popup-Fenster für die Anmeldung nachdem der Endpoint Security Client 4.0 installiert ist. Hier können Sie Ihren Benutzernamen und Ihr Passwort für den Baum eingeben.

Wenn Sie nicht der Domäne angehören, in welcher der Richtlinienverteilungsservice bereitgestellt wird, werden Sie vom Endpoint Security Client 4.0 zur Eingabe Ihres Benutzernamens und Passworts für diese Domäne aufgefordert (siehe Abbildung 2-2).

Abbildung 2-2 *Anmelden beim Endpoint Security Client 4.0*



Geben Sie Ihren Benutzernamen und Ihr Passwort für die Domäne oder den eDirectory-Baum ein und klicken Sie auf *OK*.

Der Konfigurationsname für den Verzeichnisdienst muss mit den Verzeichnisdiensten, bei denen Sie sich authentifizieren möchten, übereinstimmen. Verwenden Sie das Drop-Down-Menü, um zu sehen, ob mehr als ein Dienst zur Verfügung steht.

Hinweis: Eine Anmeldung beim Endpoint Security Client ist nicht nötig, wenn der Endpoint Security Client als Einzelplatzrechner ausgeführt wird. Der ESM-Administrator verfügt über eine andere Methode, um Benutzern mit Einzelplatzrechnern Richtlinien zuzustellen.

Verwendung des Endpoint Security Client 4.0

3

Die folgenden Abschnitte bieten zusätzliche Informationen über Aktionen, die Sie mit dem Endpoint Security Client 4.0, der Endnutzeranwendung von ZENworks® Endpoint Security, ausführen können:

Hinweis: Die oben aufgelisteten Aktionen können durch den Administrator an jedem beliebigen Standort eingeschränkt werden.

3.1 Wechsel zwischen Netzwerkumgebungen

Jedes Netzwerk, auf das ein Endbenutzer zugreift, kann·unterschiedliche Sicherheitsmaßnahmen erfordern. Der Endpoint Security Client 4.0 bietet Sicherheit und Schutz an Standorten, die von verfügbaren Netzwerkverbindungen identifiziert werden. Der Endpoint Security Client 4.0 erkennt die Netzwerk-Umgebungsparameter, wechselt zum geeigneten Standort und wendet die erforderlichen Schutzebenen gemäß der aktuellen Sicherheitsrichtlinie an.

Netzwerk-Umgebungsinformationen sind innerhalb eines Standorts gespeichert oder vorgegeben. Dadurch kann der Endpoint Security Client 4.0 automatisch zu einem Standort wechseln, wenn die Umgebungsparameter erkannt werden.

- **Gespeicherte Umgebungen:** Benutzerdefiniert (siehe Abschnitt 3.2.1, „Speichern einer Netzwerkumgebung“, auf Seite 16).
- **Vorgegebene Umgebung:** Vom ESM-Administrator des Unternehmens durch eine veröffentlichte Sicherheitsrichtlinie definiert.

Wenn der Benutzer eine neue Netzwerkumgebung betritt, vergleicht der Client die erkannte Netzwerkumgebung mit allen gespeicherten und vorgegebenen Werten in der Sicherheitsrichtlinie. Wird eine Entsprechung gefunden, aktiviert der Endpoint Security Client 4.0 den zugewiesenen Standort. Wenn die erkannte Umgebung nicht als gespeicherte oder vorgegebene Umgebung identifiziert werden kann, aktiviert der Client den Standardstandort "Unbekannt".

Der Standort "Unbekannt" besitzt die folgenden Vorgaben:

- Standort wechseln = Erlaubt
- Firewall-Einstellungen ändern = Erlaubt

- Standort speichern = Erlaubt
- Richtlinie aktualisieren = Erlaubt
- Standard-Firewall-Einstellungen - Alle offen

Standarmäßig sind alle Adaptertypen (verbunden, Wi-Fi und Modem) im Standort "Unbekannt" zulässig. Damit kann der Computer sich extern mit seiner Netzwerkumgebung verbinden und wie oben beschrieben versuchen, eine Standortrichtlinie zuzuordnen.

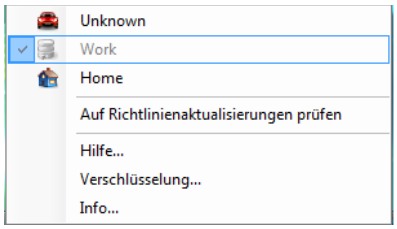
3.2 Wechseln des Standorts

Beim Start wechselt der Endpoint Security Client 4.0 zum Standort "Unbekannt". Er versucht dann, die aktuelle Netzwerkumgebung zu erkennen und automatisch den Standort zu wechseln. Wird·die Netzwerkumgebung nicht erkannt bzw.·wurde diese nicht vorgegeben, so muss der Standort manuell geändert werden.

Wenn Sie die folgenden Schritte nicht ausführen können, wurden Sie möglicherweise vom ZENworks Endpoint Security-Administrator daran gehindert, die Standorte manuell zu ändern.

So ändern Sie den Standort:

1 Klicken Sie in der Taskleiste mit der rechten Maustaste auf das Symbol für den *Endpoint Security Client 4.0*, um ein Auswahlmenü anzuzeigen.



2 Klicken Sie auf den gewünschten Standort.

3.2.1 Speichern einer Netzwerkumgebung

Eine Netzwerkumgebung muss entweder in der Sicherheitsrichtlinie vorgegeben oder vom Endbenutzer gespeichert sein, bevor der Endpoint Security Client 4.0 automatisch den Standort wechseln kann. Beim Speichern einer Netzwerkumgebung werden die Netzwerkparameter für den aktuellen Standort gespeichert, und der Endpoint Security Client 4.0 kann automatisch zu diesem Standort wechseln, wenn der Benutzer das nächste Mal die Netzwerkumgebung verwendet. Beim Anwenden in einer Wi-Fi-Netzwerkumgebung führt der Endpoint Security Client 4.0 ein LockOn™ auf den einzelnen ausgewählten Zugriffspunkt aus.

So speichern Sie eine Netzwerkumgebung:

1 Klicken Sie in der Taskleiste mit der rechten Maustaste auf das Symbol für den *Endpoint Security Client 4.0*, um das Menü anzuzeigen.

2 Klicken Sie auf den Standort, für den Sie Änderungen vornehmen möchten.

3 Klicken Sie mit der rechten Maustaste auf das Symbol für den *Endpoint Security Client 4.0*, bewegen Sie die Maus über den aktuellen Standort, um das Untermenü anzuzeigen, und klicken Sie auf "Netzwerkumgebung speichern", um die Umgebung zu speichern.

Wenn diese Netzwerkumgebung an einem vorherigen Standort gespeichert war, fragt der Endpoint Security Client 4.0, ob der Benutzer den neuen Standort speichern möchte. Wählen Sie *Ja*, um die Umgebung am aktuellen Standort zu speichern und sie von ihrem vorherigen Standort zu löschen. Oder wählen Sie *Nein*, um die Umgebung an ihrem vorherigen Standort zu belassen.

Hinweis: Die Funktion *Netzwerkumgebung speichern* kann an jedem Standort vom ESM-Administrator eingeschränkt werden.

Zusätzliche Netzwerkumgebungen können weiterhin für einen Standort gespeichert werden. Wenn beispielsweise ein Standort, der als "Flughafen" definiert ist, Teil der aktuellen Richtlinie ist, kann jeder Flughafen, den der mobile Benutzer besucht, als Netzwerkumgebung für diesen Standort gespeichert werden. Auf diese Weise wechselt der Endpoint Security Client 4.0 jedes Mal, wenn ein mobiler Benutzer zu einer gespeicherten Flughafenumgebung zurückkehrt, automatisch zum Standort "Flughafen".

3.2.2 Speichern einer Wi-Fi-Umgebung

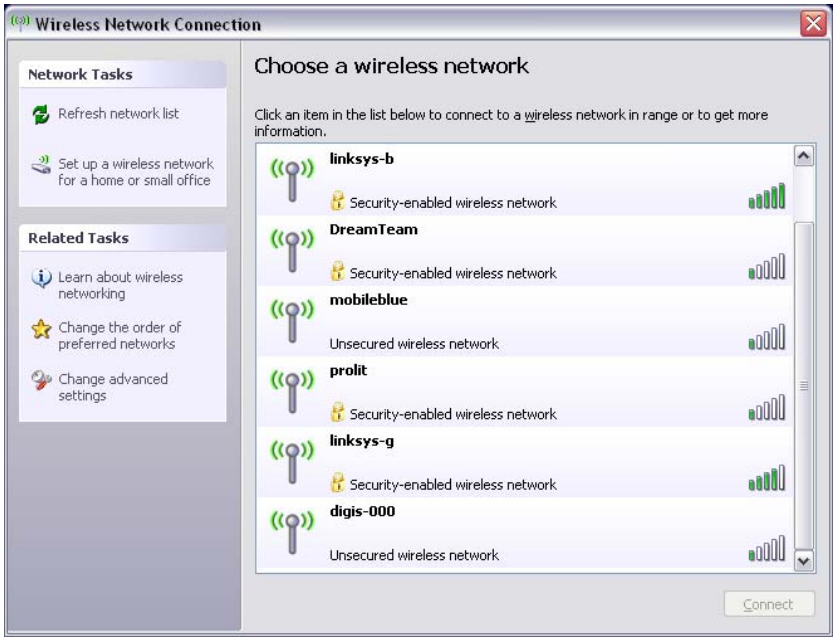
Wenn ein Benutzer seinen Wi-Fi-Adapter aktiviert, werden ihm unter Umständen dutzende verfügbare Zugriffspunkte angezeigt. Ein Wi-Fi-Adapter kann zuerst eine Verbindung zu einem einzelnen Zugriffspunkt herstellen, aber wenn sich zu viele Zugriffspunkte in der Nähe des Adapters befinden, kann die Verbindung zum verknüpften Zugriffspunkt aufgehoben werden und der Wireless Connection Manager kann den Adapter auffordern, zu dem Zugriffspunkt mit dem stärksten Signal zu wechseln. Wenn dies geschieht, wird die aktuelle Netzwerkaktivität angehalten. Häufig wird dabei ein Benutzer gezwungen, bestimmte Pakete erneut zu senden und das·VPN erneut mit dem Unternehmensnetzwerk zu verbinden.

Wenn ein Zugriffspunkt als Netzwerk-Umgebungsparameter an einem Standort gespeichert wird, verbindet sich der Adapter·mit diesem Zugriffspunkt und verliert erst dann die Verbindung, wenn sich der Benutzer physisch vom Zugriffspunkt entfernt. Bei der Rückkehr zum Zugriffspunkt verbindet sich der Adapter automatisch mit dem Zugriffspunkt, der Standort wird gewechselt und alle anderen Zugriffspunkte sind nicht mehr durch die Funkverbindungssoftware sichtbar.

So speichern Sie eine Wi-Fi-Umgebung:

1 Öffnen Sie die Verbindungsverwaltungssoftware und wählen Sie den gewünschten Zugriffspunkt aus.

Hinweis: Die Verbindungsverwaltungssoftware kann durch den Standort überschrieben werden, wenn die ESM-Sicherheitsrichtlinie auf·die Verwaltung Ihrer Wireless-Verbindungsmöglichkeit eingestellt ist.



2 Geben Sie sämtliche erforderlichen Sicherheitsinformationen (WEP oder einen anderen Sicherheitsschlüssel) ein und klicken Sie auf *Verbinden*.

3 Führen Sie die unter Abschnitt 3.2.1, „Speichern einer Netzwerkumgebung“, auf Seite 16 aufgelisteten Schritte aus, um diese Umgebung zu speichern.

3.2.3 Entfernen einer gespeicherten Umgebung

So entfernen Sie eine für einen Standort gespeicherte Netzwerkumgebung:

1 Klicken Sie in der Taskleiste mit der rechten Maustaste auf das Symbol für den *Endpoint Security Client*, um das Menü anzuzeigen.

2 Wechseln Sie zum passenden Standort.

3 Klicken Sie mit der rechten Maustaste auf das Symbol für den *Endpoint Security Client*, und wählen Sie den entsprechenden Standort aus, um das Untermenü anzuzeigen.

4 Klicken Sie auf *Netzwerkumgebung löschen*, um die Umgebung zu löschen.

Hinweis: Damit werden alle·gespeicherten Netzwerkumgebungen für diesen Standort gelöscht.

3.3 Datenverschlüsselung

Wenn dies per Richtlinie aktiviert wurde, verwaltet der Endpoint Security Client 4.0 die Verschlüsselung von Dateien, die in ein bestimmtes Verzeichnis am Endgerät und in Wechseldatenträgern platziert wurden.

Die folgenden Anleitungen helfen Ihnen bei der Verwendung von ZENworks Endpoint Security am Endgerät.

- Abschnitt 3.3.1, „Verwalten von Dateien auf Nichtsystemlaufwerken“, auf Seite 19
- Abschnitt 3.3.2, „Verwalten von Dateien auf Wechseldatenträgern“, auf Seite 19

3.3.1 Verwalten von Dateien auf Nichtsystemlaufwerken

Als Festplatten sind alle Nichtsystemlaufwerke definiert, die am Computer installiert sind, sowie alle Partitionen auf einem Festplattenlaufwerk. Jede Festplatte eines Endgeräts hat einen Safe Harbor-Ordner (standardmäßig ist der Name des Ordners `Encrypted Files`). Sie finden Ihn auf jedem Nichtsystemlaufwerk im Stammverzeichnis. Alle Dateien, die in diesem Ordner abgelegt werden, werden mit dem aktuellen Verschlüsselungsschlüssel verschlüsselt. Nur authorisierte Benutzer des Computers können diese Dateien entschlüsseln.

Wählen Sie beim Speichern einer Datei den Safe Harbor-Ordner aus den verfügbaren Ordnern auf dem gewünschten Laufwerk.

3.3.2 Verwalten von Dateien auf Wechseldatenträgern

Wechseldatenträger sind sämtliche Speichergeräte, die an einen Computer angeschlossen werden. Diese umfassen (sind aber nicht beschränkt auf) USB-Thumbdrives, Flash-Speicherkarten und PCMCIA-Speicherkarten sowie herkömmliche Zip-, Disketten- und externe CDR-Laufwerke, digitale Kameras mit Speicherkapazität und MP3-Player.

Wenn Sie ZENworks Endpoint Security ausführen, werden auf diesen Geräten gespeicherte Dateien verschlüsselt, sobald das Betriebssystem oder der Benutzer darauf zugreift. Dateien, die auf das Gerät kopiert werden, werden sofort verschlüsselt. Wenn der Wechseldatenträger an einen Computer angeschlossen wird, der nicht vom ZENworks Endpoint Security-System verwaltet wird, bleiben die Dateien verschlüsselt und können nicht entschlüsselt werden.

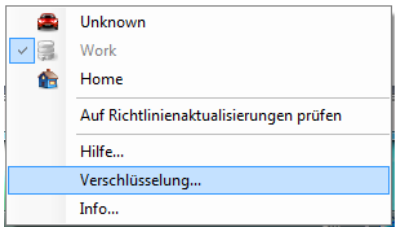
Die Verschlüsselung von Wechseldatenträgern erfolgt beim Einlegen des Datenträgers (siehe „Was muss ich tun, wenn ich den Datenträger nicht verschlüsseln möchte?“ auf Seite 20). Jedoch werden Dateien, die einem verschlüsselten Wechseldatenträger auf einem anderen Rechner hinzugefügt werden, nicht verschlüsselt und müssen manuell verschlüsselt werden.

Die folgenden Abschnitte enthalten weitere Informationen:

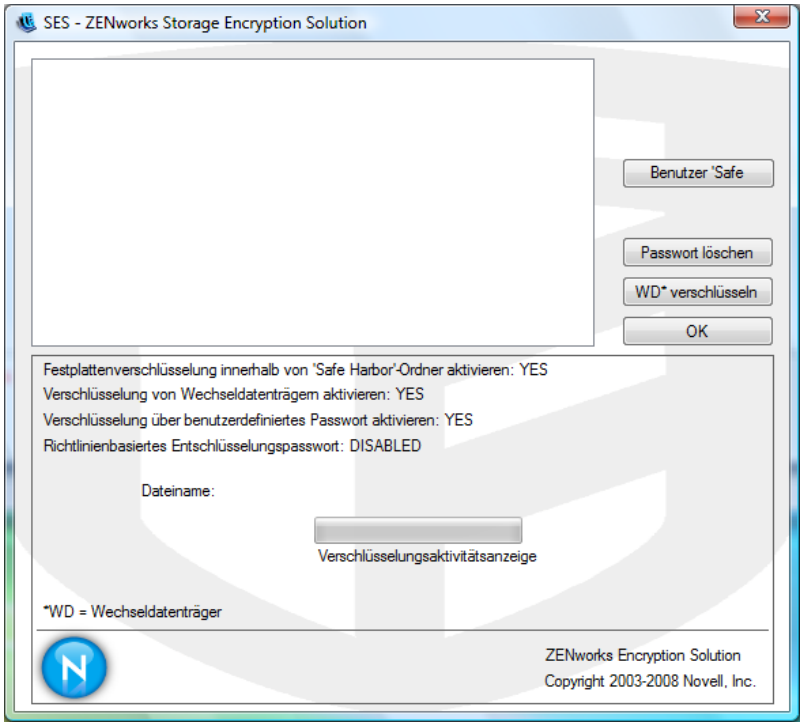
Verschlüsseln von Dateien

So verschlüsseln Sie hinzugefügte Dateien auf einem Wechseldatenträger:

1. Verbinden Sie den Wechseldatenträger mit dem entsprechenden Anschluss an Ihrem Computer.
2. Klicken Sie in der Taskleiste mit der rechten Maustaste auf das Symbol für den *Endpoint Security Client*.
3. Wählen Sie *Verschlüsselung* im Menü aus.



4 Klicken Sie auf *WD verschlüsseln*. Damit werden alle Dateien auf dem Wechseldatenträger mit dem aktuellen Verschlüsselungsschlüssel verschlüsselt.

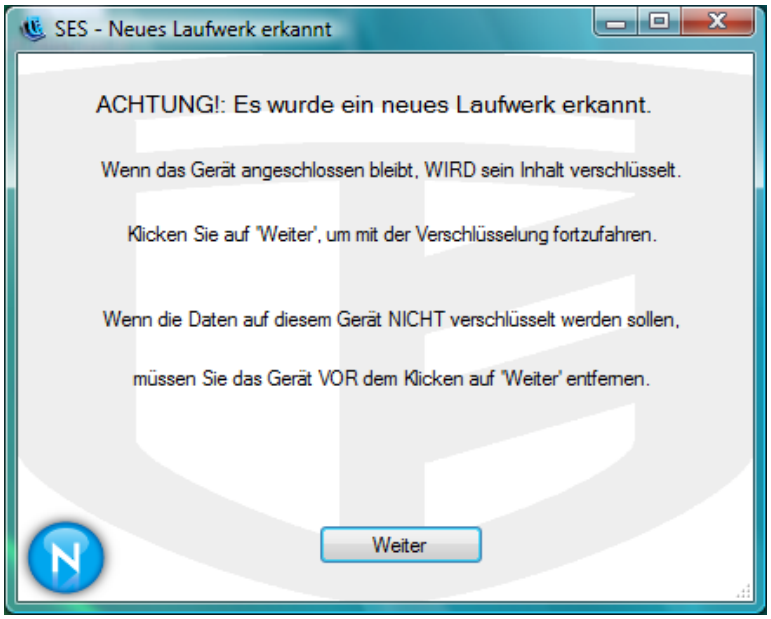


Die Zeitdauer für die Verschlüsselung der Dateien hängt von der Datenmenge ab, die auf dem Datenträger gespeichert ist.

Was muss ich tun, wenn ich den Datenträger nicht verschlüsseln möchte?

Beim Einlegen eines Wechseldatenträgers fragt der Endpoint Security Client ab, ob der Datenträger verschlüsselt werden soll oder ob Sie ihn stattdessen entfernen und nicht alle Dateien verschlüsseln möchten.

Abbildung 3-1 *Verschlüsselungswarnung, wenn ein neuer Datenträger eingelegt wird*



Warnung: Wenn Sie keine Verschlüsselung durchführen möchten, entfernen Sie den Datenträger und klicken Sie erst dann auf *Weiter*. Klicken Sie auf *Weiter*, um den Datenträger zu verschlüsseln bzw. um das Fenster zu schließen, nachdem das Laufwerk entnommen wurde.

Verwenden des Ordners "Freigegebene Dateien"

Wenn er per Richtlinie zur Verfügung gestellt wird, wird der Ordner `Freigegebene Dateien` auf einem beliebigen Wechseldatenträger erstellt, der an den Computer angeschlossen ist, auf dem ZENworks Endpoint Security ausgeführt wird. Auf Dateien in diesem Ordner können Benutzer in anderen Richtliniengruppen über ein vom Benutzer erstelltes Passwort zugreifen. Benutzer, auf deren Computer ZENworks Endpoint Security nicht ausgeführt wird, können auf diese Dateien mithilfe des ZENworks File Decryption-Dienstprogramms und durch Eingabe des Passworts zugreifen. Wenden Sie sich an den Novell-Support für Informationen über das ZENworks File Decryption-Dienstprogramm.

Hinweis: Die Passwörter werden bei jedem Neustart gelöscht. Für Dateien, die dem Ordner `Freigegebene Dateien` nach dem Neustart hinzugefügt werden, wird ein Passwort verlangt.

So verwenden Sie den Ordner `Freigegebene Dateien`:

1. Verschieben oder speichern Sie eine Datei im Ordner `Freigegebene Dateien`.
2. Geben Sie an der entsprechenden Aufforderung ein Passwort ein und wiederholen Sie es zur Bestätigung.
3. Geben Sie einen Hinweis für das Passwort ein.

Benutzer von ZENworks Endpoint Security, die nicht durch Ihre Richtlinie verwaltet werden, können auf diese Dateien zugreifen, indem sie ihre Passwörter eingeben. Benutzer, die nicht durch ZENworks Endpoint Security·verwaltet werden, benötigen das ZENworks File Decryption-Dienstprogramm und das Passwort, um auf die Dateien zuzugreifen.

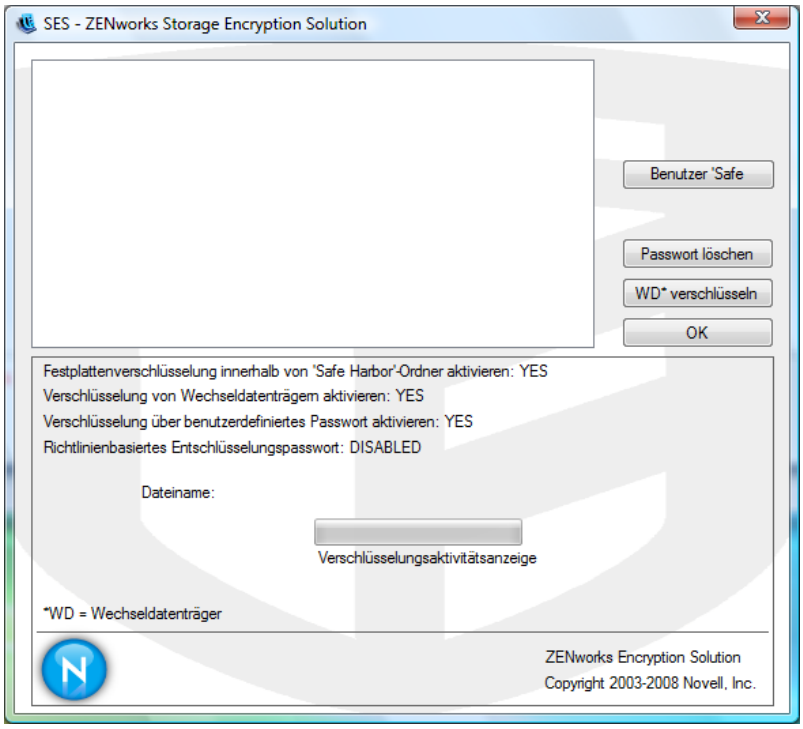
Ändern des Passworts für Dateien im Ordner "Freigegebene Dateien"

Mithilfe der Verschlüsselungssteuerung können Sie die Passwörter für Dateien ändern, die dem Ornder `Freigegebene Dateien` hinzugefügt wurden.

Hinweis: Damit werden keine bestehenden Passwörter geändert, sondern nur das Passwort für zukünftige Dateien.

So ändern Sie das Passwort:

1. Verbinden Sie den Wechseldatenträger mit dem entsprechenden Port an Ihrem Computer.
2. Klicken Sie in der Taskleiste mit der rechten Maustaste auf das Symbol für den *Endpoint Security Client*.
3. Wählen Sie *Verschlüsselung* im Menü aus.
4. Klicken Sie auf *Passwort löschen*.



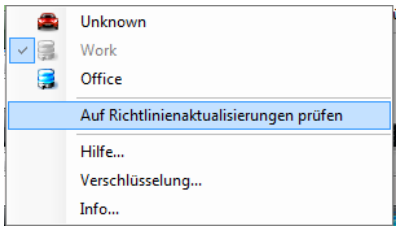
5. Ziehen Sie eine Datei in den Ordner `Freigegebene Dateien` und geben Sie das neue Passwort samt Hinweis ein.

Alle neuen Dateien, die dem Ordner hinzugefügt werden, erfordern·nun das neue Passwort für den Zugriff.

3.4 Aktualisieren von Richtlinien

Neue Sicherheitsrichtlinien werden an verwaltete Benutzer freigegeben, sobald sie veröffentlicht sind. Der Endpoint Security Client empfängt Aktualisierungen automatisch in Zeitintervallen, die der ESM-Administrator festgelegt hat. Verwaltete Benutzer können jedoch jederzeit Prüfungen nach Richtlinienaktualisierungen durchführen, wenn die Richtlinie dies zulässt.

1. Klicken Sie in der Taskleiste mit der rechten Maustaste auf das Symbol für den *Endpoint Security Client*, um das Menü anzuzeigen.
2. Klicken Sie auf *Auf Richtlinienaktualisierungen prüfen*.

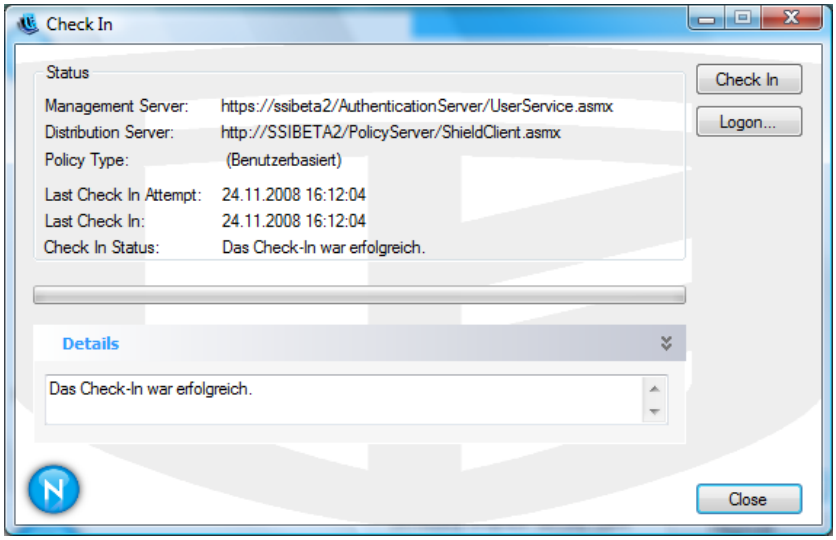


Hinweis: Automatische Aktualisierungen und Prüfungen auf Richtlinienaktualisierungen sind nicht möglich, wenn der Endpoint Security Client als Einzelplatzrechner ausgeführt wird. Der ESM-Administrator nutzt eine andere Methode, um diesen Benutzern Richtlinienaktualisierungen bereitzustellen.

Der Endpoint Security Client benachrichtigt Sie, wenn die Richtlinie aktualisiert wurde.

Sie können auch manuell eine Einlagerung vornehmen, wenn Ihr ZENworks Endpoint Security-Administrator diese Funktion zulässt.

1. Klicken Sie mit der rechten Maustaste auf das *Endpoint Security Client*-Symbol in der Taskleiste, um das Menü aufzurufen. Klicken Sie dann auf *Info*oder doppelklicken Sie auf das *Endpoint Security Client*-Symbol.
2. Klicken Sie auf *Einlagern*.



Wenn Sie nicht die Rechte haben, um eine Einlagerung durchzuführen, wird die Schaltfläche *Einlagern* grau dargestellt.

Das Einlagerungsfenster zeigt den aktuellen Status des Einlagerungsprozesses an. Handelt es sich um einen verwalteten Client werden die Verwaltungs- und Distributionsserver, der Richtlinientyp, der letzte Einlagerungsversuch, die letzte abgeschlossene Einlagerung sowie der Einlagerungsstatus angezeigt.

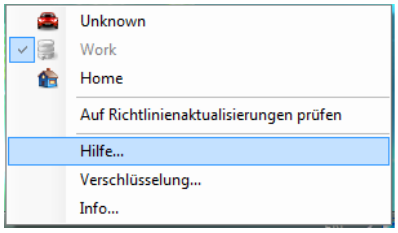
3 Um eine manuelle Einlagerung durchzuführen, klicken Sie auf *Manuelle Einlagerung*. Die Informationen im Einlagerungsfenster werden entsprechen aktualisiert.

Über die Schaltfläche *Anmeldung* können Sie sich im Richtlinienverteilungsdienst anmelden. Weitere Informationen finden Sie unter Abschnitt 2.2, „Anmelden beim Endpoint Security Client 4.0“, auf Seite 12.

3.5 Anzeigen der Hilfe

1 Klicken Sie in der Taskleiste mit der rechten Maustaste auf das Symbol für den *Endpoint Security Client*, um das Menü anzuzeigen.

2 Klicken Sie auf *Hilfe*.



3.6 Überschreiben eines Passworts

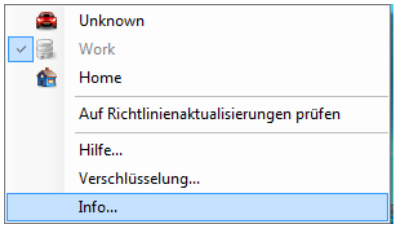
Produktivitätsunterbrechungen, mit denen ein Benutzer wegen Einschränkungen von Verbindungsmöglichkeiten, Software oder Thumbdrives möglicherweise konfrontiert wird, werden wahrscheinlich durch die Sicherheitsrichtlinie verursacht, die vom Endpoint Security Client durchgesetzt wird. Das Ändern von Standorten oder Firewall-Einstellungen hebt diese Einschränkungen im Normalfall auf und stellt die unterbrochene Funktionalität wieder her. In einigen Fällen kann die Einschränkung jedoch so implementiert sein, dass sie alle Standorte und Firewall-Einstellungen betrifft. In diesem Fall können die Einschränkungen in der aktuellen Richtlinie durch ein Überschreiben des Passworts vorübergehend aufgehoben werden, um Produktivität zu ermöglichen.

Der Endpoint Security Client 4.0 verfügt über die Funktion "Passwort überschreiben", mit deren Hilfe die aktuelle Sicherheitsrichtlinie vorübergehend deaktiviert wird, um die erforderliche Aktivität zuzulassen. Der Sicherheitsadministrator verteilt einen Passwortschlüssel zur einmaligen Verwendung nur bei Bedarf und muss bei Problemen mit einer Sicherheitsrichtlinie informiert werden. Nachdem die Zeitbeschränkung des Passwortschlüssels abgelaufen ist (wird durch den Administrator festgelegt), wird die Sicherheitsrichtlinie, die das Endgerät schützt wieder hergestellt. Ein Neustart des Endgeräts stellt ebenfalls die Sicherheitseinstellungen wieder her.

So aktivieren Sie die Überschreibung des Passworts:

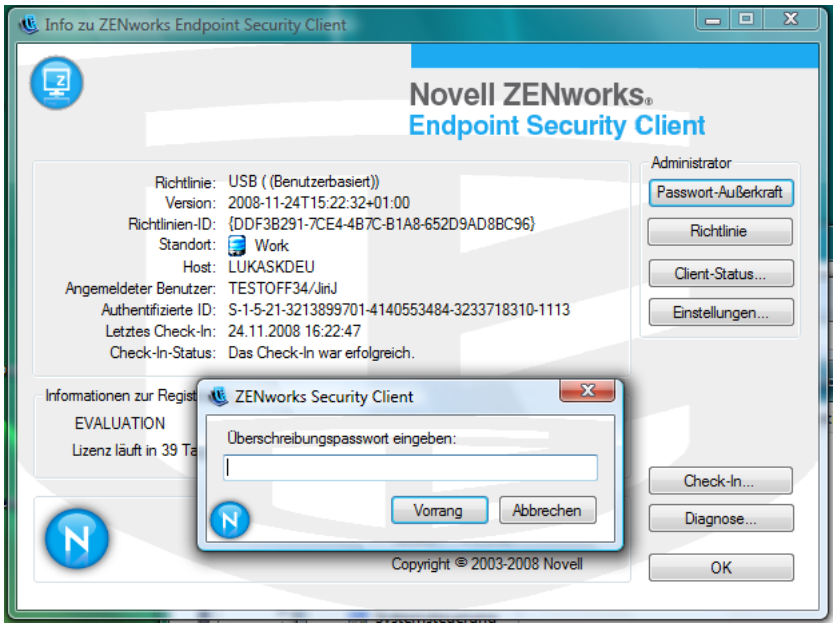
1 Bitten Sie den ESM-Administrator Ihres Unternehmens um den Passwortschlüssel.

2 Klicken Sie mit der rechten Maustaste auf das *Endpoint Security Client*-Symbol in der Taskleiste, um das Menü aufzurufen. Klicken Sie dann auf *Info*oder doppelklicken Sie auf das *Endpoint Security Client*-Symbol.



3 Klicken Sie auf *Passwort überschreiben*, um das Passwortfenster zu öffnen.

Hinweis: Wenn die Schaltfläche *Passwort überschreiben* in diesem Fenster nicht angezeigt wird, enthält Ihre aktuelle Richtlinie keine·Passwortüberschreibung.



4 Geben Sie den Passwortschlüssel ein, den Sie von Ihrem ZENworks Endpoint Security-Administrator erhalten haben.

5 Klicken Sie auf *OK*. Die aktuelle Richtlinie wird für die festgelegte Dauer durch einen Standard, die Richtlinie "Alle geöffnet", ersetzt.

Wenn Sie im Fenster *Info* auf *Richtlinien laden* klicken (das die Schaltfläche *Passwort überschreiben* ersetzt), wird die vorherige Richtlinie wiederhergestellt. Wenn Ihr Administrator Ihre Richtlinie aktualisiert hat, um bestehende Probleme zu lösen, verwenden Sie stattdessen *Auf Richtlinienaktualisierungen prüfen*, um sofort die neue Richtlinie herunterzuladen.

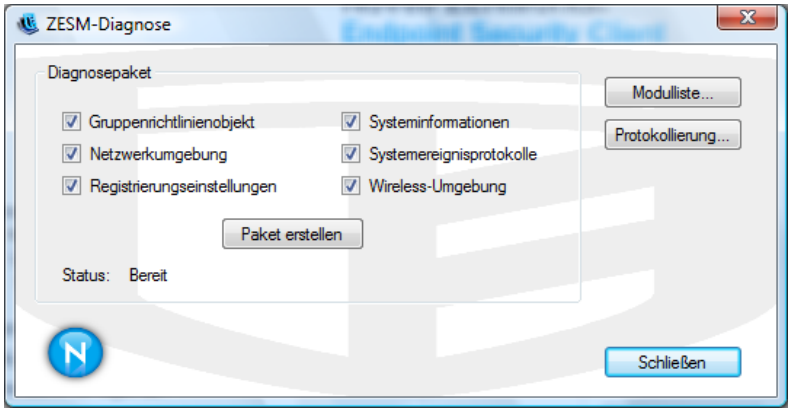
Warnung: Verschlüsselungsdienste werden niemals außer Kraft gesetzt.

3.7 Diagnose

Novell bietet Diagnosetools, damit der Administrator Fehler im Endpoint Security Client beheben kann. Ihr ZENworks Endpoint Security-Administrator führt Sie durch den Diagnosevorgang. Weitere Informationen erhalten Sie vom Novell Support.

Sie werden möglicherweise nach einen Diagnosepaket gefragt. Informationen zu dem erforderlichen Inhalten dieses Pakets, erhalten Sie von Ihrem ZENworks Endpoint Security-Administrator. So erstellen Sie ein Diagnosepaket:

1. Klicken Sie mit der rechten Maustaste auf das *Endpoint Security Client*-Symbol in der Taskleiste, um das Menü aufzurufen. Klicken Sie dann auf *Info*oder doppelklicken Sie auf das *Endpoint Security Client*-Symbol.
2. Klicken Sie auf *Diagnose*.



3. Sie können sämtliche Elemente im Bereich "Diagnosepaket" markieren oder nur die Elemente, die von Ihrem ZENworks Endpoint Security-Administrator gefordert wurden. Klicken Sie dann auf *Paket erstellen*.

   Der ZENworks Endpoint Security Client erstellt eine `zesmdiagnostics*.enc` -Datei auf Ihrem Computer, die Sie dann an den ZENworks Endpoint Security-Administrator senden können.