AUTHORIZED DOCUMENTATION

Hilfe zur Verwaltungskonsole

August 1, 2008

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.

Copyright © 2007-2008 Novell, Inc. Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Herausgebers darf kein Teil dieser Veröffentlichung reproduziert, fotokopiert, übertragen oder in einem Speichersystem verarbeitet werden.

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

1 Verwenden der ZENworks Endpoint Security Management-Konsole

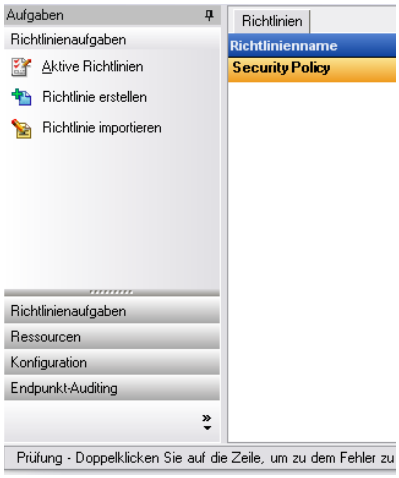
Die Verwaltungskonsole dient dem zentralen Zugriff und der Steuerung des Novell® ZENworks® Endpoint Security Management-Service.

Wenn Sie das Anmeldefenster der Verwaltungskonsole aufrufen möchten, wählen Sie die Optionsfolge *Start* > *Alle Programme* > *Novell* > *ESM Management Console* > *Verwaltungskonsole*. Melden Sie sich bei der Konsole an, indem Sie Namen und Passwort des Administrators angeben. Der eingegebene Benutzername muss einem autorisierten Benutzer im Verwaltungsdienst entsprechen (siehe Abschnitt 1.3, „Wenn Sie Berechtigungseinstellungen“, auf Seite 10).

Hinweis: Es empfiehlt sich, die Konsole zu schließen bzw. zu minimieren, wenn sie nicht verwendet wird.

1.1 Verwenden der Taskleiste

Die Taskleiste auf der linken Seite ermöglicht den Zugriff auf die Aufgaben der Verwaltungskonsole. Wird die Taskleiste nicht angezeigt, klicken Sie links in der Konsole auf die Schaltfläche *Aufgaben*.



In den nachfolgenden Abschnitten finden Sie weitere Informationen zu den Aufgaben, die Sie über die Taskleiste durchführen können.

- Abschnitt 1.1.1, „Richtlinienaufgaben“, auf Seite 8
- Abschnitt 1.1.2, „Ressourcen“, auf Seite 8
- Abschnitt 1.1.3, „Konfiguration“, auf Seite 8
- Abschnitt 1.1.4, „Endpunktüberwachung“, auf Seite 8

1.1.1 Richtlinienaufgaben

Die Verwaltungskonsole dient hauptsächlich der Erstellung von Sicherheitsrichtlinien und deren Anwendung auf verwaltete Endgeräte. Die Richtlinienaufgaben dienen dem Administrator als Schritt-für-Schritt-Anleitungen für das Erstellen und Bearbeiten von Sicherheitsrichtlinien, mit deren Hilfe der ZENworks® Security Client zentral verwaltete Sicherheitsaspekte auf die einzelnen Endgeräte anwendet.

Die Richtlinienaufgaben umfassen Folgendes:

- **Aktive Richtlinien:** Zeigt eine Liste mit aktuellen Richtlinien an, die überprüft und bearbeitet werden können. Klicken Sie auf eine Richtlinie, um sie zu öffnen.
- **Richtlinie erstellen:** Startet den Assistenten für neue Richtlinien, mit dem Sie eine neue Sicherheitsrichtlinie erstellen können.
- **Richtlinie importieren:** Zeigt das Dialogfeld "Richtlinie importieren" an, über das Richtlinien erstellt werden können, die mit anderen Verwaltungsdiensts erstellt wurden. Weitere Informationen finden Sie unter Abschnitt 2.3.1, „Importieren von Richtlinien“, auf Seite 113.

Wenn Sie auf eine der Richtlinienaufgaben klicken, wird die Taskleiste minimiert. Klicken Sie links auf die Schaltfläche *Aufgaben*, um sie wieder anzuzeigen.

In Kapitel 2, „Erstellen und Verteilen von Sicherheitsrichtlinien“, auf Seite 47 erhalten Sie Informationen über die Richtlinienaufgaben und die Erstellung und Verwaltung von Sicherheitsrichtlinien.

1.1.2 Ressourcen

In der Aufgabenliste "Ressourcen" werden die Ressourcen für technischen Support und Hilfe angezeigt, die zur Verfügung stehen:

- **Wenden Sie sich an den Support:** Startet einen Browser und zeigt die Seite mit den Kontaktinformationen und Niederlassungen von Novell® an.
- **Online Technical Support:** Startet einen Browser und zeigt die Seite mit dem Schulungs- und Supportangebot von Novell an.
- **Hilfe zur Verwaltungskonsole:** Ruft die Online-Hilfe zu ZENworks® Endpoint Security Management auf.

1.1.3 Konfiguration

Das Konfigurationsfenster des Verwaltungsdiensts enthält sowohl Steuerelemente für die ZENworks® Endpoint Security Management-Serverinfrastruktur als auch Steuerelemente für die Überwachung zusätzlicher Verzeichnisdienste für Unternehmen. Weitere Informationen finden Sie unter Abschnitt 1.4, „Verwenden des Fensters "Konfiguration"“, auf Seite 14. Dieses Steuerelement ist nicht verfügbar, wenn die Standalone-Verwaltungskonsole ausgeführt wird. Weitere Informationen finden Sie in der *ZENworks Endpoint Security Management-Installationsanleitung*.

1.1.4 Endpunktüberwachung

Über das Fenster "Endpunktüberwachung" können Sie auf ZENworks® Endpoint Security Management-Funktionen für Berichte und Warnmeldungen zugreifen.

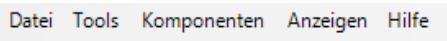
Berichterstellung: Berichte sind für die Anlayse und Implementierung starker Sicherheitsrichtlinien von entscheidender Bedeutung. Wenn Sie auf Berichte zugreifen möchten, klicken Sie in der Verwaltungskonsole auf *Berichte*. Die erfassten und gemeldeten Endpunktsicherheitsdaten können ebenfalls uneingeschränkt konfiguriert sowie nach Domäne, Gruppe oder einzelnem Benutzer zusammengestellt werden. Weitere Informationen finden Sie unter Abschnitt 1.6, „Verwenden von Berichten“, auf Seite 29.

Warnmeldungen: Die Überwachung von Warnmeldungen stellt sicher, dass jegliche Verstöße gegen Sicherheitsrichtlinien des Unternehmens in der Verwaltungskonsole gemeldet werden. Mit Warnmeldungen wird der ZENworks Endpoint Security Management-Administrator auf potenzielle Probleme hingewiesen und kann die entsprechenden Maßnahmen zur Behebung ergreifen. Das Dashboard "Warnmeldungen" kann uneingeschränkt konfiguriert werden. Auf diese Weise können Sie steuern, wann und wie oft Warnmeldungen ausgegeben werden. Weitere Informationen finden Sie unter Abschnitt 1.5, „Verwenden der Warnmeldungsüberwachung“, auf Seite 25.

1.2 Verwenden der Menüleiste

Über die ZENworks® Endpoint Security Management-Menüleiste können Sie auf sämtliche Funktionen der Verwaltungskonsole zugreifen.

Mit den zur Verfügung stehenden Optionen können Sie



- **Datei:** Über das Menü "Datei" werden Sicherheitsrichtlinien erstellt und verwaltet.
  - **Neue Richtlinie erstellen:** Startet den Assistenten für neue Richtlinien, mit dem Sie eine neue Sicherheitsrichtlinie erstellen können.
  - **Richtlinienliste aktualisieren:** Aktualisiert die Liste der Richtlinien; es werden alle aktiven Richtlinien angezeigt.
  - **Löschrichtlinie:** Löscht die ausgewählte Richtlinie.
  - **Richtlinie importieren:** Ermöglicht Ihnen das Importieren einer Richtlinie in die Verwaltungskonsole.
  - **Richtlinie exportieren:** Hiermit können Sie eine Richtlinie und die erforderliche `setup.sen`-Datei an einem angegebenen Speicherort außerhalb der Verwaltungsdienstdatenbank speichern.
  - **Beenden:** Schließt die Verwaltungskonsole und meldet den Benutzer ab.
- **Werkzeuge:** Über das Menü "Werkzeuge" können Sie Konfiguration, Verschlüsselungsschlüssel und Berechtigungen des Verwaltungsdiensts steuern.
  - **Konfiguration:** Öffnet das Fenster "Konfiguration".
  - **Exportieren von Verschlüsselungsschlüsseln:** Öffnet das Dialogfeld "Verschlüsselungsschlüssel exportieren", in dem Sie die zu exportierenden Schlüssel sowie das Passwort angeben können.
  - **Importieren von Verschlüsselungsschlüsseln:** Öffnet das Dialogfeld "Verschlüsselungsschlüssel importieren", in dem Sie die zu importierenden Schlüssel sowie das Passwort angeben können.

- **Neuen Schlüssel generieren:** Generiert einen neuen Verschlüsselungsschlüssel, der der Erzwingung des Schutzes von Daten dient.
- **Berechtigungen:** Öffnet das Fenster "Berechtigungen".

- **Anzeigen:** Über das Menü "Anzeigen" können Sie häufige Richtlinienaufgaben ausführen, ohne die Taskleiste verwenden zu müssen.
  - **Richtlinie:** Ist eine Richtlinie geöffnet, wird zu ihr gewechselt.
  - **Aktive Richtlinien:** Zeigt die Richtlinienliste an.
  - **Warnmeldungen:** Zeigt das Dashboard "Warnmeldungen" an.
  - **Berichterstellung:** Zeigt das Dashboard "Bericht" an.
- **Hilfe:** Zeigt die Hilfe sowie das Dialogfeld "Info" der Verwaltungskonsole an:
  - **Hilfe:** Ruft die Online-Hilfe der Verwaltungskonsole auf, in der Sie schrittweise Anleitungen zur Erstellung von Richtlinien sowie zur Durchführung von Verwaltungskonsolenaufgaben finden. Die Hilfe kann auch über die Taste F1 auf der Tastatur aufgerufen werden.
  - **Info zur Verwaltungskonsole:** Öffnet das Fenster "Info", in dem der Installationstyp (ZENworks Endpoint Security Management oder UWS) sowie die aktuelle Versionsnummer der Verwaltungskonsole angezeigt werden. In diesem Fenster wird auch der Lizenzschlüssel eingegeben, falls er nach der Installation erworben wurde.

1.3 Wenn Sie Berechtigungseinstellungen

"Berechtigungseinstellungen" befindet sich im Menü "Werkzeuge". Nur der primäre Administrator des Verwaltungsdiensts sowie sämtliche Administratoren, denen dieser Administrator den Zugriff gewährt hat, können hierauf zugreifen. Dieses Steuerelement ist nicht verfügbar, wenn die Standalone-Verwaltungskonsole ausgeführt wird.

Durch die Berechtigungseinstellungen wird definiert, welcher Benutzer bzw. welche Benutzergruppe Zugriff auf die Verwaltungskonsole bzw. die Einstellungen für "Administrative Berechtigungen" bzw. "Veröffentlichen an" hat.

Während der Installation des Verwaltungsservers wird ein Administrator- bzw. Ressourcenkontoname in das Konfigurationsformular eingegeben (siehe *ZENworks Endpoint Security Management-Installationsanleitung*). Wenn der Test erfolgreich verlaufen ist und die Benutzerinformationen gespeichert wurden, werden diesem Benutzer automatisch alle Berechtigungen erteilt.

Nach der Installation der Verwaltungskonsole ist der Ressourcenbenutzer der einzige Benutzer mit uneingeschränkten Berechtigungen, obwohl allen Benutzergruppen innerhalb der Domäne der Zugriff auf die Verwaltungskonsole gewährt wird. Der Ressourcenbenutzer sollte sämtlichen Gruppen oder Benutzern, die sie nicht benötigen, die Zugriffsberechtigung entziehen. Der Ressourcenbenutzer kann zusätzliche Berechtigungen für bestimmte Benutzer festlegen.

Wenn die Verwaltungskonsole gestartet wird, werden die Berechtigungen aus der Berechtigungstabelle abgerufen. Diese Berechtigungen teilen der Konsole mit, ob der Benutzer berechtigt ist, sich bei der Konsole anzumelden, Richtlinien zu erstellen oder zu löschen, Berechtigungseinstellungen zu ändern, und ob und an wen der Benutzer Richtlinien veröffentlichen darf.

Folgende Zugriffseinstellungen stehen zur Verfügung:

- **Zugriff auf die Verwaltungskonsole:** Der Benutzer kann Richtlinien und Komponenten anzeigen und bestehende Richtlinien bearbeiten. Benutzer, denen nur diese Berechtigung erteilt wurde, können Richtlinien weder hinzufügen noch löschen, da die Veröffentlichungs- und Berechtigungsoptionen nicht verfügbar sind.
- **Richtlinie herausgeben:** Der Benutzer kann Richtlinien nur für zugewiesene Benutzer oder Gruppen herausgeben.
- **Berechtigungen ändern:** Der Benutzer hat die Möglichkeit, auf die Berechtigungseinstellungen für andere, bereits definierte·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 sämtliche Richtlinien in der Verwaltungskonsole löschen.

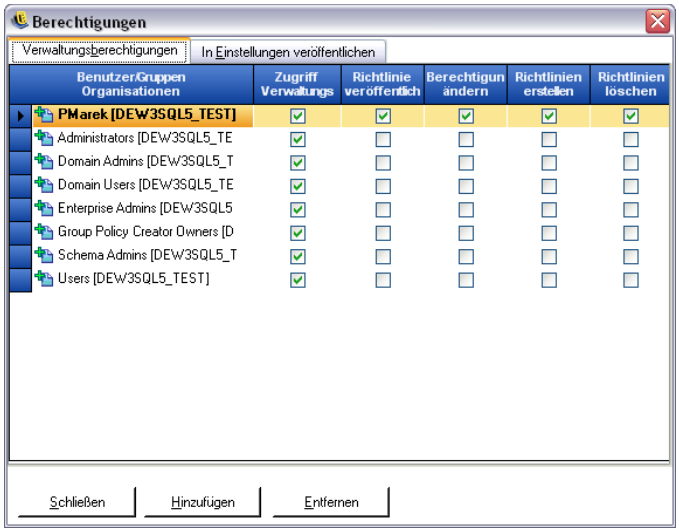
Hinweis: Aus Sicherheitsgründen wird empfohlen, dass nur der Ressourcenbenutzer oder sehr wenige Administratoren die Berechtigung "Berechtigungen ändern" und "Richtlinien löschen" erhalten.

1.3.1 Administrative Berechtigungen

So legen Sie die administrativen Berechtigungen fest:

1 Wählen Sie die Optionsfolge *Werkzeuge* > *Berechtigungen*.

Die dieser Domäne zugeordneten Gruppen werden angezeigt.

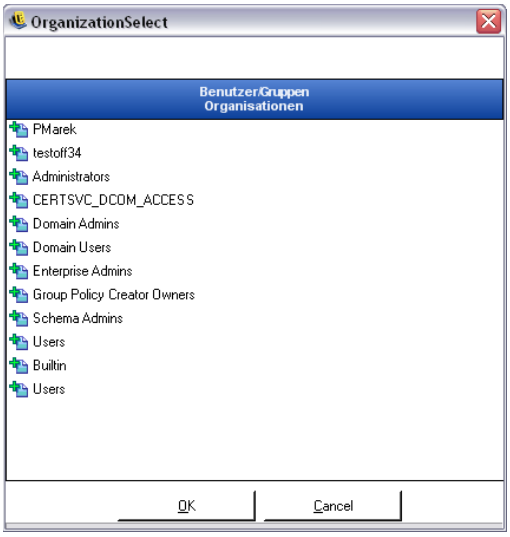


Hinweis: Alle Gruppen erhalten standardmäßig Zugriff auf die Verwaltungskonsole, jedoch können sie keine Richtlinienaufgaben ausführen. Der Zugriff auf die Konsole kann durch das Aufheben der Berechtigungsauswahl entzogen werden.

---

2 So laden Sie Benutzer oder Gruppen in diese Liste:

2a Klicken Sie am unteren Bildschirmrand auf die Schaltfläche *Hinzufügen*.



2b Wählen Sie die entsprechenden Benutzer oder Gruppen in der Liste aus. Wenn Sie mehrere Benutzer auswählen möchten, können Sie diese bei gedrückt gehaltener Steuerungstaste einzeln auswählen. Sie können auch eine Reihe von Benutzern auswählen, indem Sie den oberen Eintrag auswählen, die Umschalttaste gedrückt halten und dann den unteren Eintrag auswählen.

2c Sind alle Benutzer oder Gruppen ausgewählt, klicken Sie auf *OK*.

3 Weisen Sie den verfügbaren Benutzern bzw. Gruppen einige (oder alle) Berechtigungen zu.

Wenn Sie einen ausgewählten Benutzer/eine ausgewählte Gruppe entfernen möchten, wählen Sie den Namen aus und klicken Sie dann auf *Entfernen*. Der ausgewählte Name wird wieder in die Organisationstabelle verschoben.

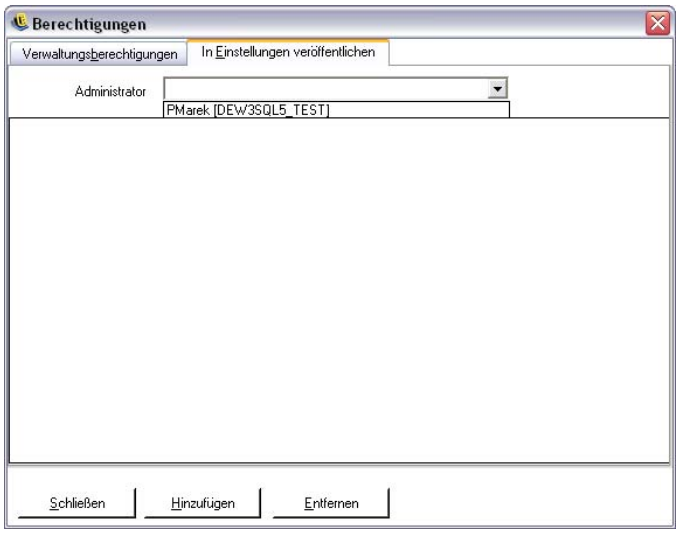
1.3.2 Einstellungen für "Veröffentlichen an"

Benutzer bzw. Gruppen, für die *Richtlinie herausgeben* aktiviert ist, müssen Benutzern oder Gruppen zugewiesen werden, an die sie veröffentlichen können.

So legen Sie die Einstellungen für "Veröffentlichen an" fest:

1 Klicken Sie auf die Registerkarte *Einstellungen für "Veröffentlichen an"*.

2 Wählen Sie in der Dropdown-Liste die Benutzer bzw. Gruppen mit der Berechtigung "Veröffentlichen" aus.



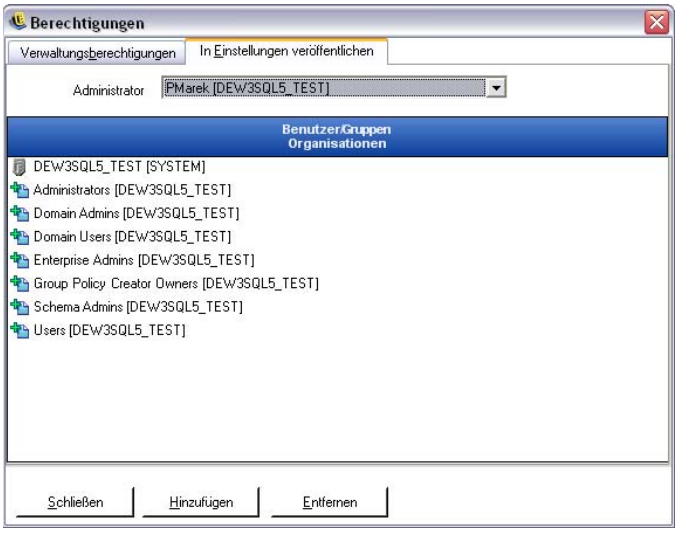
3 Weisen Sie diesem Benutzer/dieser Gruppe Benutzer bzw. Gruppen zu:

3a Klicken Sie am unteren Bildschirmrand auf *Hinzufügen*. Daraufhin wird die Organisationstabelle angezeigt.

3b Wählen Sie die entsprechenden Benutzer oder Gruppen in der Liste aus. Mit Steuerungstaste bzw. der Umschalttaste lassen sich mehrere Benutzer·auswählen.

3c Sind alle Benutzer bzw. Gruppen ausgewählt, klicken Sie auf die Schaltfläche *OK*, um die Benutzer und Gruppen der Veröffentlichungsliste

des ausgewählten Namens hinzuzufügen.



Die Berechtigungssätze werden umgehend implementiert.

4 Wenn Sie einen ausgewählten Benutzer bzw. eine ausgewählte Gruppe entfernen möchten, wählen Sie den Namen in der Liste aus und klicken Sie dann auf *Entfernen*.

5 Mit *Schließen* übernehmen Sie die Änderungen und kehren zum Editor zurück.

Der ausgewählte Name wird wieder in die Organisationstabelle verschoben.

Wenn ein neuer Verzeichnisdienst hinzugefügt wird (siehe „Authentifizierungsverzeichnisse“ auf Seite 16), werden dem eingegebenen Ressourcenkonto wie oben beschrieben uneingeschränkte Berechtigungseinstellungen gewährt.

1.4 Verwenden des Fensters "Konfiguration"

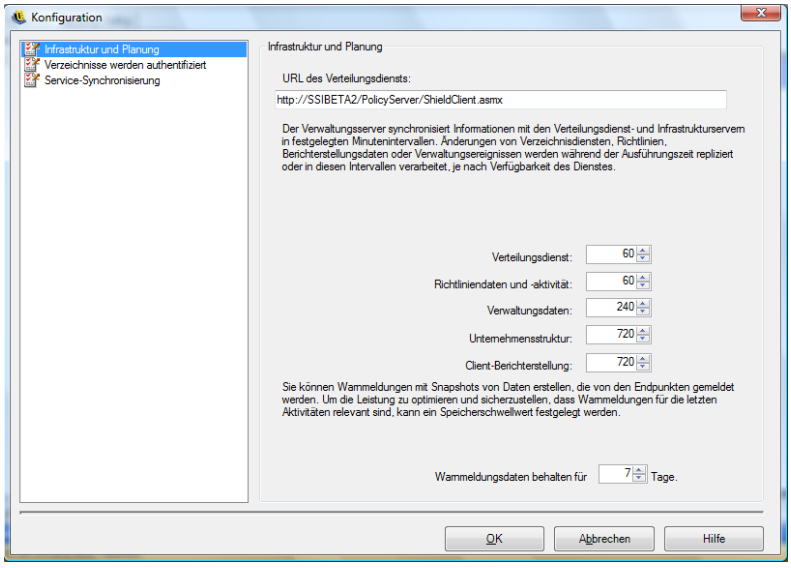
Über das Fenster "Konfiguration" kann der ZENworks® Endpoint Security Management-Administrator auf die Steuerelemente für *Infrastruktur und Planung*, *Authentifizierungsverzeichnisse* sowie *Serversynchronisierung* zugreifen. Klicken Sie auf der Hauptseite auf den Link *Konfiguration* oder öffnen Sie das Menü *Werkzeuge* und klicken Sie dann auf *Konfiguration*. Daraufhin wird das Fenster "Konfiguration" angezeigt.

Hinweis: Diese Funktion ist bei einer Standalone-Verwaltungskonsole nicht verfügbar.

Die folgenden Abschnitte enthalten weitere Informationen:

1.4.1 Infrastruktur und Planung

Mithilfe des Moduls für Infrastruktur und Planung kann der ZENworks Endpoint Security Management-Administrator die URL für den Richtlinienverteilungsservice festlegen und ändern sowie die Synchronisierungsintervalle für die ZENworks Endpoint Security Management-Komponenten steuern.



Die folgenden Abschnitte enthalten weitere Informationen:

Verteilungsservice-URL

Über die Einstellung *Verteilungsservice-URL* wird der Speicherort des Richtlinienverteilungsservice sowohl für den Verwaltungsdiensts als auch für sämtliche ZENworks Security Client-Instanzen aktualisiert (ohne dass sie neu installiert werden müssen), wenn der Richtlinienverteilungsservice auf einen neuen Server verlagert wird. Die URL des aktuellen Servers ist im Textfeld angegeben.

Wenn Sie den Server ändern müssen, ändern Sie lediglich den Servernamen, um auf den neuen Server zu verweisen. Ändern Sie keine der Informationen, die auf den Servernamen folgen.

Wird die aktuelle URL beispielsweise als `http:\\ACME\PolicyServer\ShieldClient.asmx` angegeben und der Richtlinienverteilungsservice ist auf einem neuen Server namens ACME 43 installiert, sollte die URL folgendermaßen aktualisiert werden: `http:\\ACME43\PolicyServer\ShieldClient.asmx`.

Klicken Sie nach der Aktualisierung der URL auf *OK*, um alle Richtlinien zu aktualisieren und eine automatische Aktualisierung des Richtlinienverteilungsservice zu übermitteln. Auf diese Weise wird auch der Verwaltungsdienst aktualisiert.

Beim Ändern der Server-URL sollte der alte Richtlinienverteilungsservice erst beendet werden, wenn die aktualisierten Richtlinien eine Einhaltungsstufe von 100 % aufweisen (siehe Abschnitt 1.6, „Verwenden von Berichten“, auf Seite 29).

Planung

Mithilfe der Komponenten für die Planung kann der ZENworks Endpoint Security Management-Administrator festlegen, wann der Verwaltungsdienst mit anderen ZENworks Endpoint Security Management-Komponenten synchronisiert wird, um sicherzustellen, dass alle Daten und Aufträge in der Warteschlange den vorangegangenen Aktivitäten entsprechen, und um die SQL-Wartungsaufträge zu planen. Alle Zeitangaben erfolgen in Minuten.

Die Planung wird wie folgt gegliedert:

- **Verteilungsservice** Synchronisierungsplan mit dem Richtlinienverteilungsservice.
- **Richtliniendaten und -aktivität** Synchronisierungsplan mit Richtlinienaktualisierungen.
- **Verwaltungsdaten:** Richtliniensynchronisierung mit dem Verwaltungsdienst.
- **Unternehmensstruktur:** Synchronisierungsplan mit dem Verzeichnisdienst des Unternehmens (eDirectory™, Active Directory*, NT-Domäne* und/oder LDAP). Änderungen im Verzeichnisdienst des Unternehmens werden überwacht, damit entsprechende Änderungen in Zuweisungen von Benutzerrichtlinien erkannt und zur Client-Authentifizierung an den Richtlinienverteilungsservice gesendet werden.
- **Client-Berichterstellung:** Häufigkeit, mit der der Verwaltungsdienst Berichtsdaten vom Richtlinienverteilungsservice anfordert und herunterlädt.
- **Warnmeldungsdaten behalten für:** Sie können Warnmeldungen auf der Basis eines von den Endpunkten gemeldeten Datensnapshots konfigurieren. Um die Leistung zu optimieren und sicherzustellen, dass die Warnmeldungen für kürzlich erfolgte Aktivitäten relevant sind, können Sie den Speicherschwellenwert in Tagen festlegen.

1.4.2 Authentifizierungsverzeichnisse

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 Client-Installationen in ZENworks Endpoint Security Managment definiert. Die neue Konfiguration verwendet Ihren vorhandenen Verzeichnisdienst, um die logische Begrenzng für Ihre benutzer- und computerbasierten Client-Installationen zu definieren.

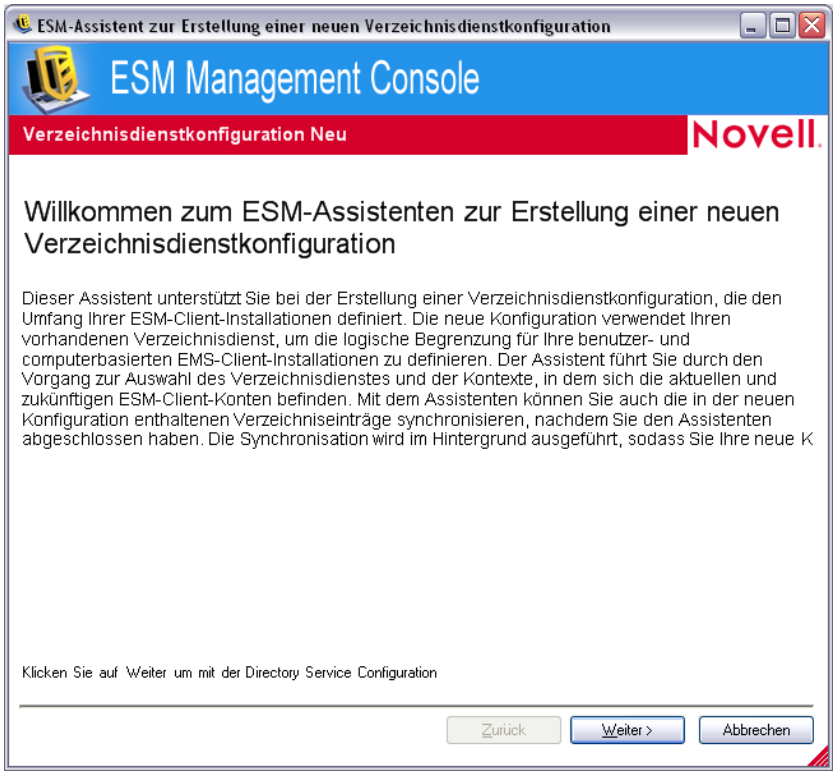
Der Assistent führt Sie durch den Prozess der Auswahl eines Verzeichnisdiensts und der Kontexte, in denen sich die aktuellen und zukünftigen Client-Konten befinden.

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.

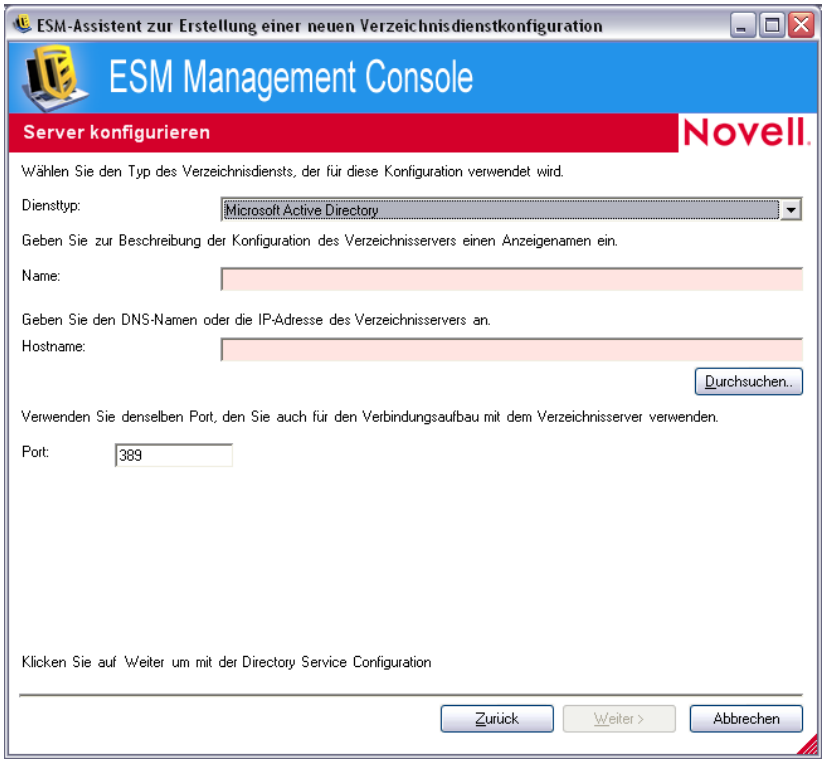
Nach der Installation von ZENworks Endpoint Security Management wird der Assistent zur Neukonfiguration von Verzeichnisdiensten automatisch angezeigt. Nach der Installation des Produkts und der Anzeige der Seite "Willkommen", springen Sie zu Schritt 4 in der folgenden Prozedur.

So konfigurieren Sie den Verzeichnisdienst:

1. Klicken Sie in der Verwaltungskonsole auf *Werkzeuge* > *Konfiguration*.
2. Klicken Sie auf *Authentifizierungsverzeichnisse*.
3. Klicken Sie auf *Neu*, um den Assistenten zur Neukonfiguration von Verzeichnisdiensten aufzurufen.



4 Klicken Sie auf *Weiter*, um die Seite "Server konfigurieren" anzuzeigen.

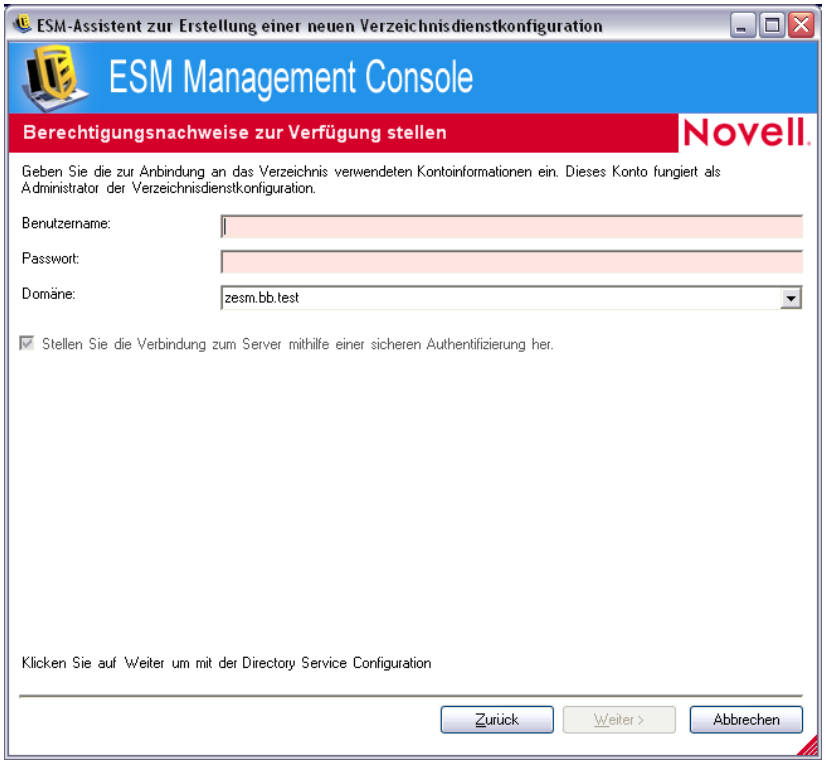


5 Füllen Sie die Felder aus:

- **Service-Typ:** Wählen Sie eine Dienstart aus der Dropdown-Liste *Dienstart* aus:
  - Microsoft Active Directory
  - Novell eDirectory
- **Name:** Geben Sie zur Beschreibung der Verzeichnisdienstkonfiguration einen Anzeigenamen ein.
- **Hostname:** Geben Sie den DNS-Namen oder die IP-Adresse des Verzeichnisservers ein oder suchen Sie ihn.
- **Port:** Geben Sie den Port an, über den die Verbindung mit dem Verzeichnisserver hergestellt werden soll.

  Port 389 ist voreingestellt. Wenn Sie einen anderen Port verwenden, um eine Verbindung zum Verzeichnisserver herzustellen, können Sie auch diesen Port angeben.

6 Klicken Sie auf *Weiter*, um die Seite "Berechtigungsnachweis angeben" anzuzeigen:



7 Füllen Sie die Felder aus:

- **Benutzername:** Geben Sie den Kontoadministrator an, der mit dem Verzeichnis verbunden werden soll.

  Dieses Konto fungiert bei der Verzeichnisdienst-Konfiguration als Administratorkonto. Bei dem Anmeldenamen muss es sich um einen Benutzer handeln, der berechtigt ist, den gesamten Verzeichnisbaum einzusehen. Es wird empfohlen, dass dieser Benutzer entweder der Domänen-Administrator oder ein OU-Administrator ist. Verwenden Sie bei der Konfiguration für eDirectory das LDAP-Format, beispielsweise `cn=admin,o=acmeserver`; hierbei steht `cn` für den Benutzer und `o` für das Objekt, in dem das Benutzerkonto gespeichert ist.

- **Passwort:** Geben Sie das Passwort für den Kontoadministrator an.

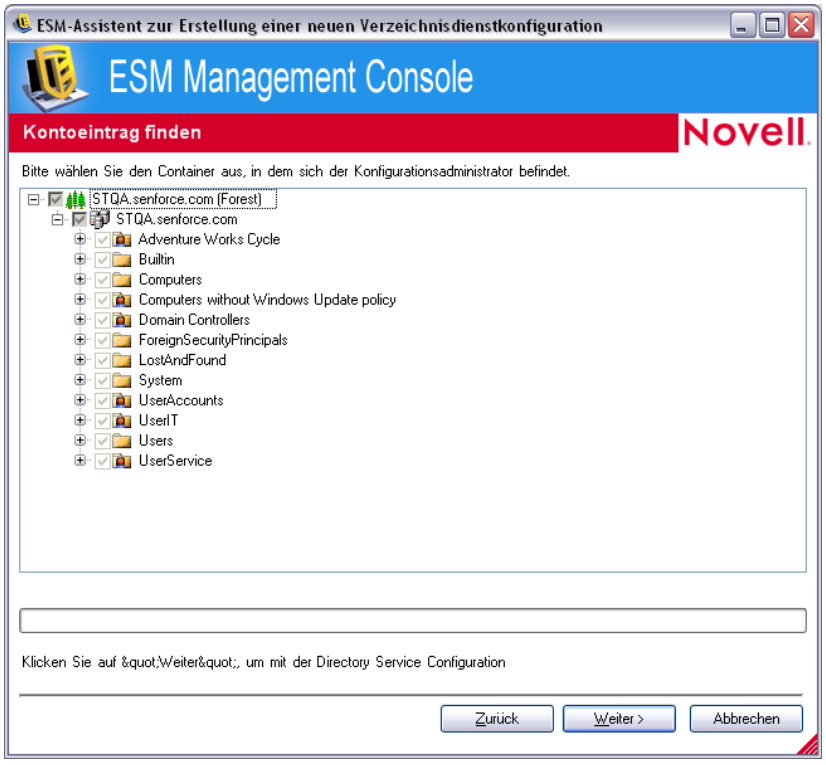
  Dieses Konto fungiert bei dieser Verzeichnisdienstkonfiguration als Administratorkonto.

  Für das Passwort sollte keine Ablauffrist festgelegt werden und dieses Konto sollte unter keinen Umständen deaktiviert werden.
- **Domäne:** Geben Sie die Domäne an, bei der der Kontoadministrator Mitglied ist.
- **Stellen Sie mithilfe der sicheren Authentifizierung eine Verbindung zum Server her.**

  Heben Sie die Auswahl für diese Option auf, wenn keine sichere Authentifizierung verwendet werden soll. Diese Option ist standardmäßig aktiviert.

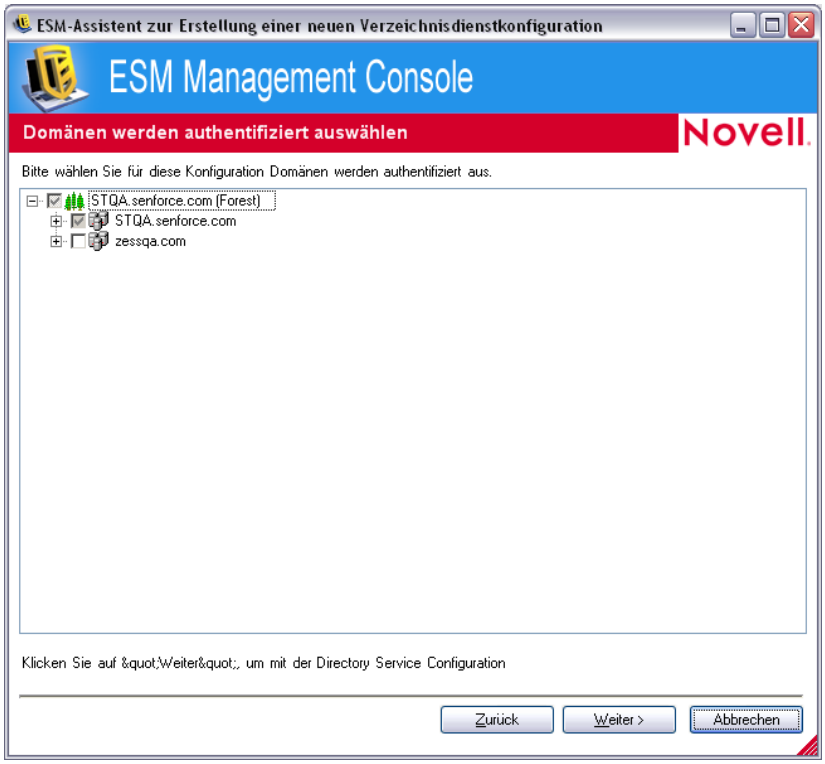
8 Klicken Sie zum Fortfahren auf *Weiter*.

9 Wenn der in Schritt 7 angegebene Konfigurations-Administratorbenutzer in der Domäne nicht gefunden werden kann, wird die Seite "Kontoeintrag suchen" angezeigt.



Geben Sie den Container an, in dem sich der Administrator befindet und klicken Sie anschließend auf *Weiter*.

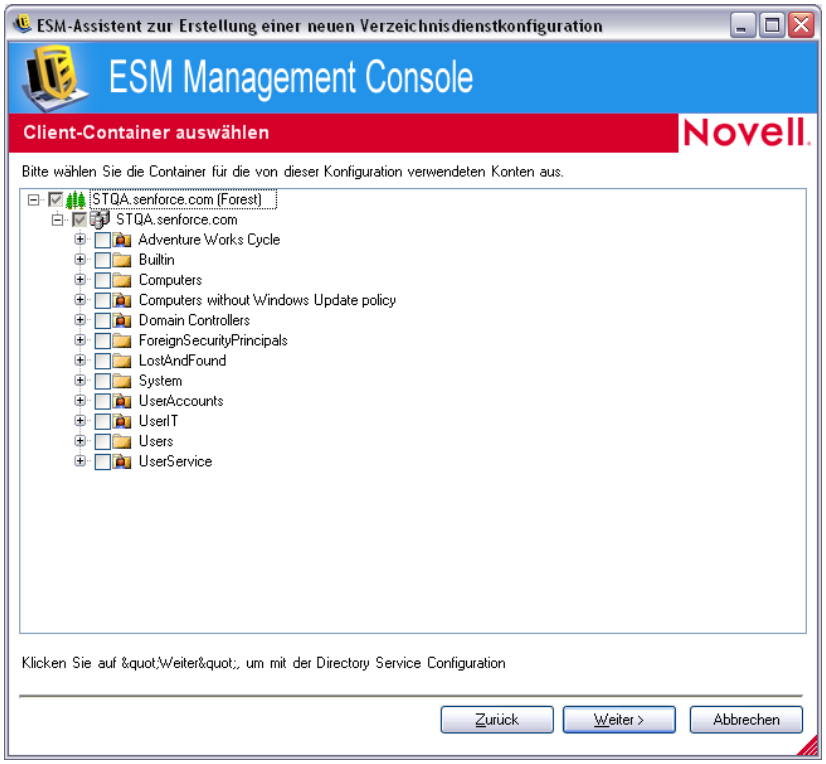
10 Durchsuchen Sie auf der Seite "Authentifizierungsdomäne(n) auswählen" den Baum, um die Domänen auszuwählen, die zur Authentifizierung der Benutzer und Computer dieser Konfiguration verwendet werden.



Die Domäne, die den in Schritt 7 angegebenen verwaltungsbefugten Benutzer enthält, wird ausgewählt; diese Auswahl kann nicht wieder aufgehoben werden.

Die Installation eines Client schlägt beim Versuch der Anmeldung am Verwaltungsserver fehl, wenn der Client kein Mitglied der Domänen ist, die in der Konfiguration ausgewählt wurden.

11 Klicken Sie auf *Weiter*, um die Seite "Client-Container auswählen" anzuzeigen und wählen Sie anschließend die Container für die von dieser Konfiguration verwendeten Konten aus.

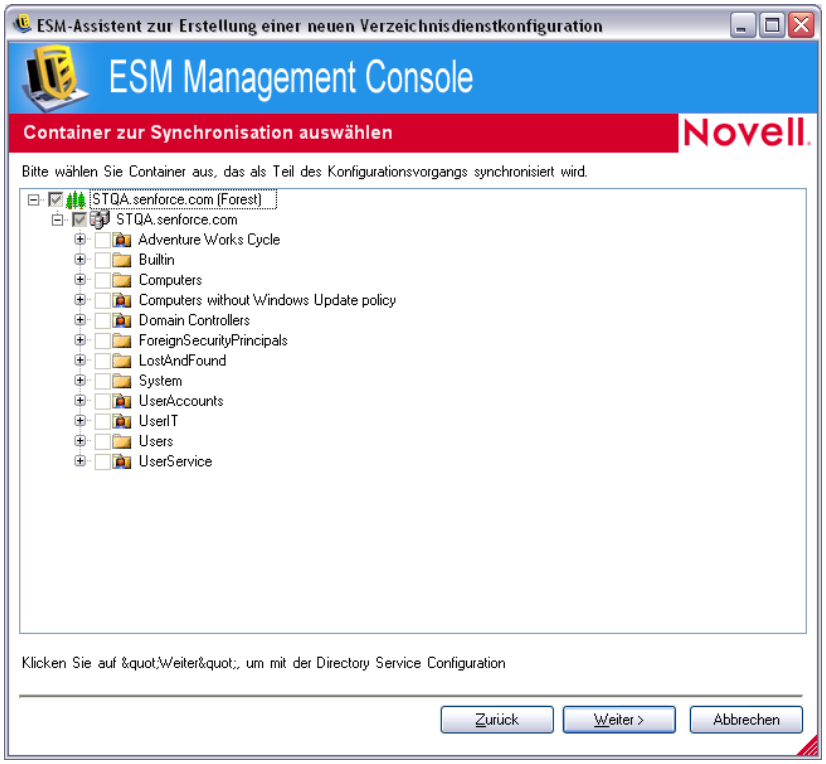


Der Container, der den in Schritt 7 angegebenen verwaltungsbefugten Benutzer enthält, wird ausgewählt; diese Auswahl kann nicht wieder aufgehoben werden.

Auf der Seite "Client-Container auswählen" können Sie die Suche auf jene Container eingrenzen, die die verwalteten Benutzer und Computer enthält. Dadurch wird die Leistung verbessert.

Die Installation eines Client schlägt beim Versuch der Anmeldung am Verwaltungsserver fehl, wenn dessen Konto sich nicht in einem der in der Konfiguration ausgewählten Container befindet.

12 Klicken Sie auf *Weiter*, um die Seite "Zu synchronisierende(r) Container" anzuzeigen.



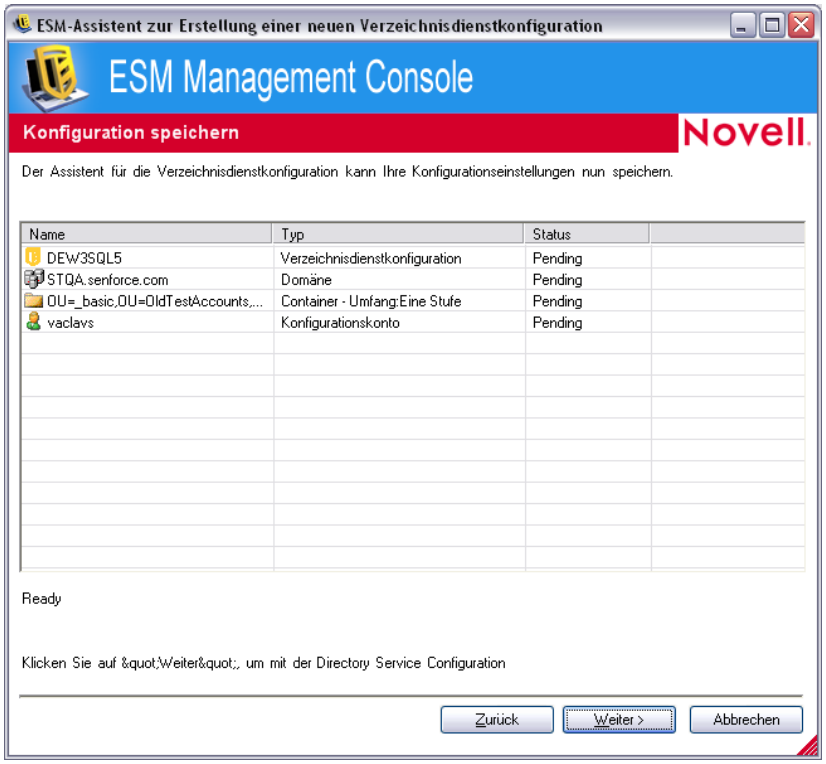
13 (Optional) Wählen Sie die Container aus, die als Teil des Konfigurationsvorgangs synchronisiert werden sollen.

Die Synchronisierung wird im Hintergrund ausgeführt, weshalb Sie sofort damit beginnen können, Ihre neue Konfiguration zu verwenden. Die Synchronisierung vieler Benutzer und Computer kann einige Stunden in Anspruch nehmen.

Wenn Sie keine Container zur Synchronisierung angeben, werden die Benutzer und Computer in diesen Containern in der Verwaltungskonsole ausgefüllt, sobald sie sich anmelden.

Bei der Synchronisierung von Containern wird die Verwaltungskonsole vorab mit diesen Benutzern und Computern ausgefüllt, sodass Sie sofort Aktionen wie die Erstellung von Sicherheitsrichtlinien durchführen können. Wenn sich die Benutzer und Computer dann am System anmelden, werden diese Richtlinien aktiviert und angewendet. Wenn die Verwaltungskonsole vorab ausgefüllt wird, können Sie sofort damit beginnen, für Einzelbenutzer oder Computer spezifische Richtlinien zu erstellen, statt Richtlinien zu erstellen, die für alle Benutzer und Computer im Container zutreffen. Wenn Sie den Container nicht synchronisieren, müssen Sie warten, bis sich diese Benutzer und Computer am System anmelden, bevor Sie eindeutige Richtlinien für verschiedene Benutzer und Computer erstellen können.

14 Klicken Sie auf *Weiter*, um die Seite "Konfiguration speichern" anzuzeigen.

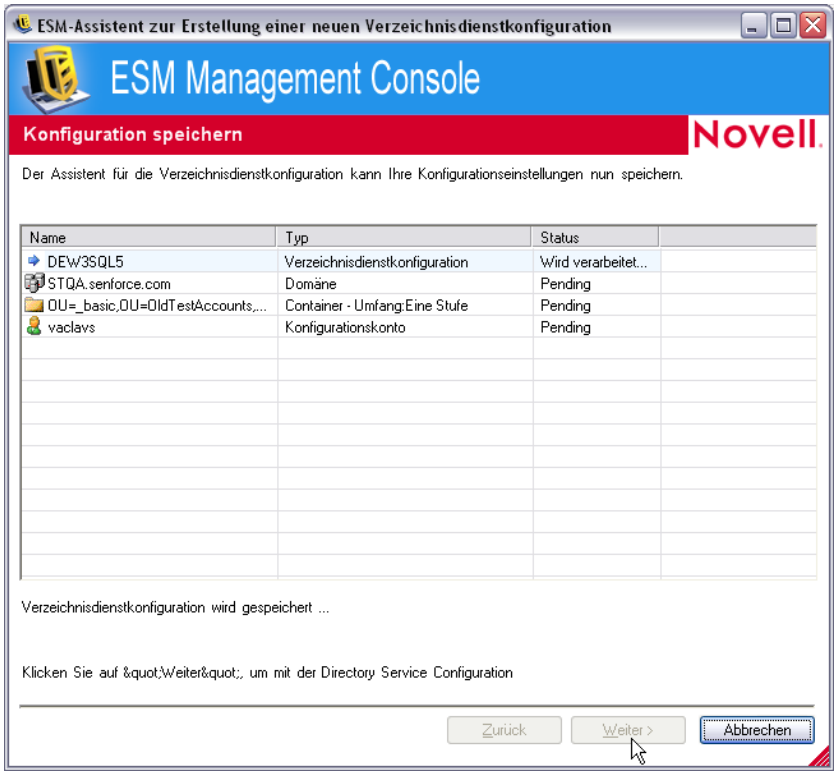


15 Überprüfen Sie die Informationen und klicken Sie anschließend auf *Weiter*, um die Konfiguration zu speichern.

   Sie können gegebenenfalls zur Änderung der Einstellungen auf *Zurück* klicken.

16 Klicken Sie auf *Fertig stellen*.

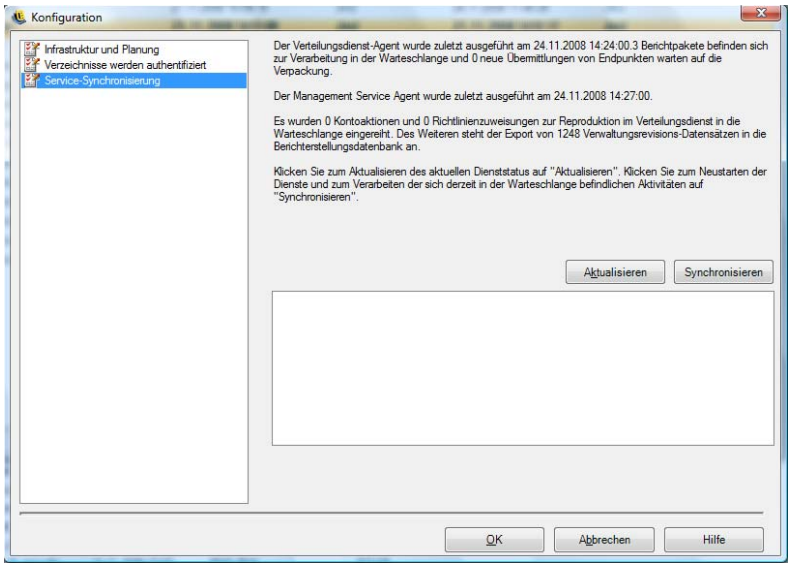
Wenn Sie auf *Fertig stellen* klicken, wird das Symbol im Benachrichtigungsbereich von Windows angezeigt und die Synchronisierung startet. Sie können auf das Symbol doppelklicken, um das Dialogfeld "Synchronisierung von Verzeichnisdiensten" anzuzeigen.



Die Synchronisierung wird im Hintergrund ausgeführt. Wenn Sie die Verwaltungskonsole beenden, wird die Synchronisierung angehalten. Beim erneuten Öffnen der Verwaltungskonsole wird die Synchronisierung dort fortgesetzt, wo sie angehalten wurde.

1.4.3 Service-Synchronisierung

Mit diesem Steuerelement können Sie die Synchronisierung des Verwaltungsdienst und des Richtlinienverteilungsservice erzwingen. Dabei werden sämtliche Warnmeldungen, Berichte und Richtlinienverteilungen aktualisiert.

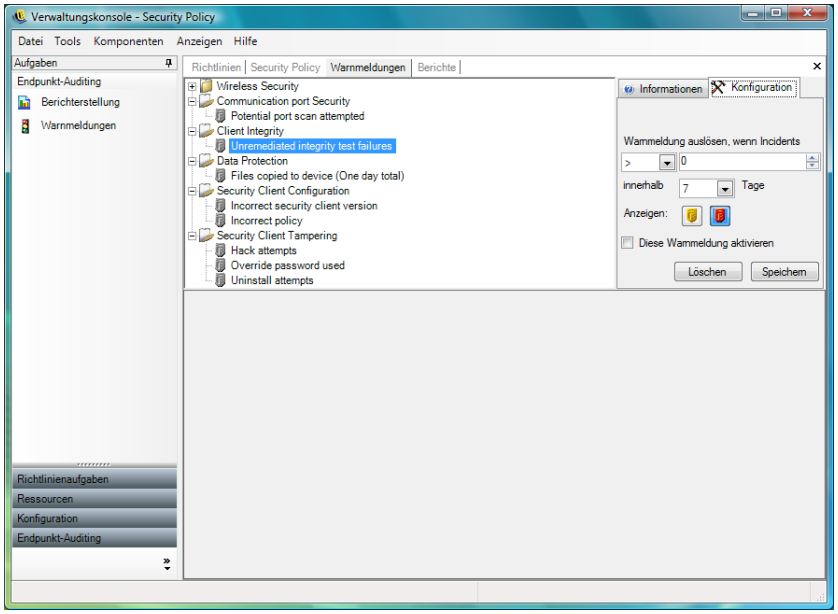


1. Um den aktuellen Service-Status zu aktualisieren, klicken Sie auf *Aktualisieren*.
2. Um die Services neu zu starten und die aktuell in der Warteschlange befindlichen Aktivitäten zu verarbeiten, klicken Sie auf *Synchronisieren*.

1.5 Verwenden der Warnmeldungsüberwachung

Mithilfe der Warnmeldungsüberwachung kann der ZENworks® Endpoint Security Management-Administrator den Sicherheitsstatus sämtlicher mit ZENworks Endpoint Security Management verwalteten Endpunkte im gesamten Unternehmen beurteilen. Warnungsauslöser sind uneingeschränkt·konfigurierbar und können entweder eine Warnung ausgeben oder als Notfallwarnung dienen. Der Zugriff auf dieses Werkzeug erfolgt entweder über *Endpunktüberwachung* in der Taskleiste oder über das Menü *Anzeigen*.

1 Wenn Sie auf Warnmeldungen zugreifen möchten, klicken Sie auf das Symbol "Warnmeldungen" (Warnmeldungen).



Warnungsüberwachung ist für die folgenden Bereiche verfügbar:

- **Client-Integrität:** Benachrichtigt über nicht korrigierte Ergebnisse eines Integritätstests.
- **Sicherheit des Kommunikationsports:** Benachrichtigt über potenzielle Portscan-Versuche.
- **Datenschutz:** Benachrichtigt über Dateien, die innerhalb eines Tages auf Wechselspeichergeräte kopiert wurden.
- **Security Client-Konfiguration:** Benachrichtigt über falsche Security Client-Versionen und fehlerhafte Richtlinien.
- **Security Client Tampering:** Benachrichtigt über Hackversuche, Deinstallationsversuche und Nutzung des Override-Passworts durch Benutzer.
- **Drahtlose Sicherheit:** Benachrichtigt über nicht sichere Zugriffspunkte, die erkannt wurden und zu denen der Benutzer eine Verbindung aufgebaut hat.

1.5.1 Konfigurieren von ZENworks Endpoint Security Management für Warnmeldungen

Für Warnmeldungen müssen Berichtsdaten regelmäßig erfasst und heraufgeladen werden, um ein möglichst präzises Bild der aktuellen Endpunkt-Sicherheitsumgebung zu vermitteln. Nicht verwaltete ZENworks® Security Client-Instanzen stellen keine Berichtsdaten bereit und werden daher bei der Warnmeldungsüberwachung nicht berücksichtigt.

Die folgenden Abschnitte enthalten weitere Informationen:

- „Aktivieren der Berichterstellung“ auf Seite 27
- „Optimieren der Synchronisierung“ auf Seite 27

Aktivieren der Berichterstellung

Berichterstellung sollte in jeder Sicherheitsrichtlinie aktiviert sein. Weitere Informationen über das Einrichten der Berichterstellung für eine Sicherheitsrichtlinie erhalten Sie in Abschnitt 2.2.4, „Einhaltungsberichterstellung“, auf Seite 108. Passen Sie die Sendezeiten für Berichte an ein Intervall an, das konsistente Aktualisierungen zum Endpunktstatus gewährleistet. Darüber hinaus wird eine Warnmeldung nicht ohne einen Bericht aktiviert. Einer Aktivität, über die Sie informiert werden möchten, muss in der Sicherheitsrichtlinie ein entsprechender Bericht zugewiesen sein.

Optimieren der Synchronisierung

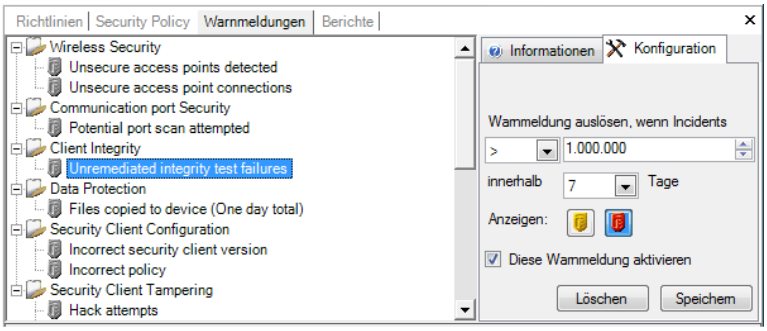
Standardmäßig erfolgt die Synchronisierung des Berichtsservice von ZENworks Endpoint Security Management alle 12 Stunden. Das bedeutet, dass die ersten Berichts- und Warnmeldungsdaten erst 12 Stunden nach der Installation von ZENworks Endpoint Security Management zur Verfügung stehen. Um diesen Zeitrahmen anzupassen, öffnen Sie das Werkzeug "Konfiguration" (siehe „Planung“ auf Seite 15) und passen Sie das Intervall für *Client-Berichte* an die Anzahl der Minuten an, die für Ihre Anforderungen und Ihre Umgebung geeignet sind.

Wenn Daten sofort benötigt werden, können über die Option *Service-Synchronisierung* im Werkzeug "Konfiguration" sofort der Richtlinienverteilungsservice (der Berichtsdaten von den Endpunkten erfasst) und der Berichtsservice (der alle Warnmeldungen auf der Basis der neu erfassten Daten aktualisiert) gestartet werden. Weitere Informationen finden Sie in Abschnitt 1.4.3, „Service-Synchronisierung“, auf Seite 24.

1.5.2 Warnmeldungsauslöser konfigurieren

Warnmeldungsauslöser können an Schwellenwerte angepasst werden, die den Sicherheitsanforderungen Ihres Unternehmens genügen.

1 Wählen Sie eine Warnmeldung in der Liste aus und klicken Sie dann rechts in der Verwaltungskonsole auf die Registerkarte *Konfiguration*.



2 Passen Sie den Schwellenwert für den Auslöser an, indem Sie in der Dropdown-Liste eine Bedingung auswählen. Damit legen Sie das Verhältnis zur Auslöseranzahl fest:

- Gleich (=)
- Größer als (<)
- Größer gleich (<=)
- Kleiner als (>)
- Kleiner gleich (>=)

3 Stellen Sie die Auslöseranzahl ein. Diese Zahl variiert abhängig vom Typ der Warnmeldung.

4 Wählen Sie das Intervall aus, innerhalb dessen diese Zahl erreicht werden muss.

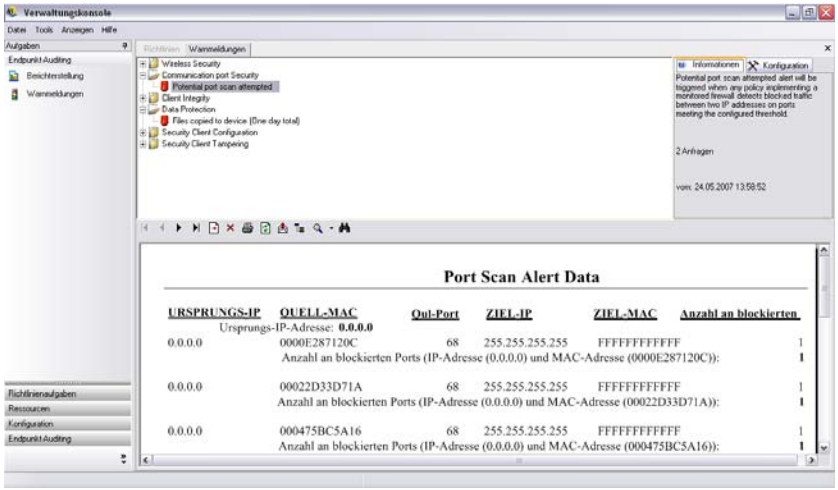
5 Wählen Sie den Auslösertyp aus. Hierbei kann es sich um ein Warnsymbol ( ) oder ein Notfallsymbol ( ) handeln.

6 Vergewissern Sie sich, dass das Kontrollkästchen *Diese Warnmeldung aktivieren* aktiviert ist.

7 Klicken Sie auf *Speichern*, um die Warnmeldung zu speichern.

1.5.3 Verwalten von Warnmeldungen

Warnmeldungen informieren Sie über Probleme, die innerhalb der Endpunkt-Sicherheitsumgebung behoben werden müssen. Abhilfe wird normalerweise individuell oder auf Gruppenbasis geschaffen. Als Hilfe bei der Problemsuche werden Warnmeldungsberichte angezeigt, wenn die Warnmeldung ausgewählt wird.



Dieser Bericht zeigt die aktuellen Auslöserergebnisse mit Informationen zu·dem betroffenen Benutzer oder Gerät. Mithilfe der hier bereitgestellten Daten können hinsichtlich potenzieller Bedrohungen der Unternehmenssicherheit die entsprechenden Gegenmaßnahmen ergriffen werden. Zusätzliche Informationen finden Sie, indem Sie "Berichterstellung" öffnen.

Nachdem Abhilfemaßnahmen ergriffen wurden, bleibt die Warnmeldung bis zur nächsten Berichtaktualisierung aktiv. So löschen Sie eine Warnmeldung vor der geplanten Aktualisierung:

1 Wählen Sie eine Warnmeldung in der Liste aus und klicken Sie dann rechts in der Verwaltungskonsole auf die Registerkarte *Konfiguration*.

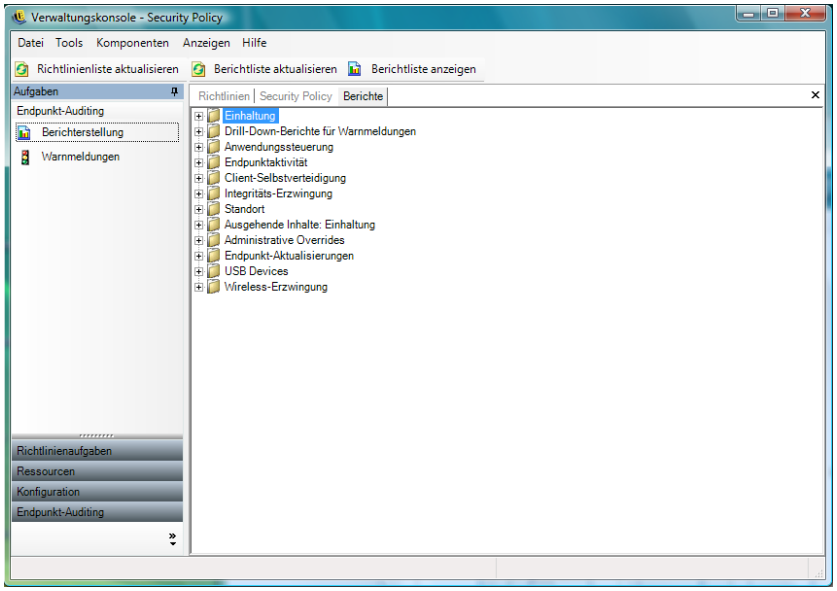
2 Klicken Sie auf *Löschen*.

Hiermit werden die Berichtsdaten unter "Warnmeldungen" gelöscht (diese Daten stehen in der Berichtsdatenbank weiterhin zur Verfügung). Die erneute Aktivierung erfolgt erst beim Eingang neuer Daten.

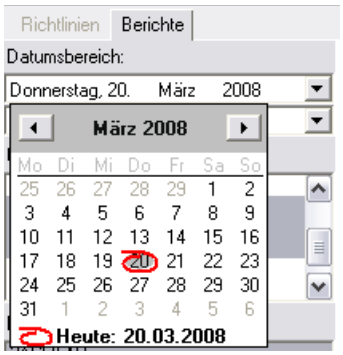
1.6 Verwenden von Berichten

Der Berichtsservice stellt Einhaltungs- und Statusberichte für das Unternehmen bereit. Die verfügbaren Daten werden für Verzeichnisse und Benutzergruppen in einem Verzeichnis geliefert. Novell®-Berichte geben Feedback zu den Auswirkungen, die einzelne Richtlinienkomponenten auf Unternehmensendpunkte haben. Anforderungen dieser Berichte werden in der Sicherheitsrichtlinie festgelegt (siehe Abschnitt 2.2.4, „Einhaltungsberichterstellung“, auf Seite 108) und können hilfreiche Daten für Richtlinienaktualisierungen bereitstellen.

Wählen Sie die Option *Bericht* entweder in der Taskleiste *Endpunktüberwachung* oder im Menü *Anzeigen* aus. Die Liste der verfügbaren Berichte wird angezeigt (klicken Sie auf das Pluszeichen neben den einzelnen Berichtstypen, um die Liste zu erweitern).



Berichte werden durch Angabe des Datumsbereichs und anderer Parameter, beispielsweise Benutzer oder Standort, konfiguriert. Wenn Sie die Daten festlegen möchten, erweitern Sie die Ansicht so, dass der Kalender angezeigt wird, und wählen Sie dann Monat und Tag aus. Klicken Sie in jedem Fall auf den Tag, um den Datumsparameter zu ändern.



Mit *Anzeigen* wird der Bericht generiert.

Nachdem ein Bericht generiert wurde, können Sie die Symbolleiste für Berichte nutzen, um den Bericht in der Verwaltungskonsole anzuzeigen, den Bericht zu drucken, den Bericht als E-Mail zu senden oder ihn als `.pdf`-Datei zu exportieren.

Beim Ansehen von Berichten navigieren Sie mithilfe der Pfeiltasten durch die Seiten des Berichts. Berichte enthalten in der Regel auf der ersten Seite Diagramme und auf den übrigen Seiten die gesammelten Daten nach Datum und Zeit geordnet.

Über die Schaltfläche *Drucker* wird der vollständige Bericht auf dem Standarddrucker für diesen Computer ausgegeben.

Mit der Schaltfläche *Exportieren* speichern Sie den Bericht als PDF-Datei, Excel*-Arbeitsblatt, Word-Dokument oder RTF-Datei.

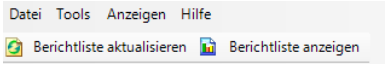
Die Schaltfläche *Gruppenhierarchie* blendet eine Liste von Parametern als Seitenleiste neben dem Bericht ein und aus. Wählen Sie einen dieser Parameter aus, um tiefere Ebenen des Berichts anzuzeigen. Klicken Sie auf die Schaltfläche *Gruppenhierarchie*, um die Seitenleiste zu schließen.

Durch Klicken auf das Symbol mit der Lupe wird ein Dropdown-Menü zur Anpassung der aktuellen Anzeigegröße eingeblendet.

Durch Klicken auf das Symbol mit dem Fernglas wird ein Suchfenster geöffnet.

Wenn Sie die Maus auf einen bestimmten Parameter, beispielsweise einen Benutzer- oder Gerätenamen, bewegen, wird der Mauszeiger zur Lupe. Sie können auf das entsprechende Element doppelklicken und einen neuen Bericht ausschließlich zu diesem Objekt anzeigen. Klicken Sie auf die Schaltfläche *Schließen*, um die aktuelle Ansicht zu schließen und zum ursprünglichen Bericht zurückzukehren.

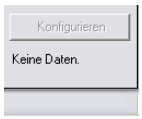
Wenn Sie wieder zur Berichtliste wechseln möchten, klicken Sie auf das Symbol *Berichtliste* oberhalb des Berichtfensters.



Berichte stehen erst zur Verfügung, wenn Daten von den ZENworks® Security Clients heraufgeladen wurden. Standardmäßig erfolgt die Synchronisierung des Berichtsservice von ZENworks Endpoint Security Management alle 12 Stunden. Das bedeutet, dass die ersten Berichts-

und Warnmeldungsdaten erst 12 Stunden nach der Installation von ZENworks Endpoint Security Management zur Verfügung stehen. Um diesen Zeitrahmen anzupassen, öffnen Sie das Werkzeug "Konfiguration" (siehe „Planung“ auf Seite 15) und passen Sie das Intervall für *Client-Berichte* an die Anzahl der Minuten an, die für Ihre Anforderungen und Ihre Umgebung geeignet sind.

Bei Berichten ohne Daten ist die Schaltfläche *Konfigurieren* bzw. *Vorschau* abgeblendet; darunter ist "0 Daten" zu lesen.



Folgende Berichte stehen zur Verfügung:

1.6.1 Adherence Reports

Adherence Reports enthalten Informationen über die Einhaltung bei der Verteilung von Sicherheitsrichtlinien an verwaltete Benutzer. Eine Einhaltung von 100 % gibt an, dass alle verwalteten Benutzer das Check-in vorgenommen und die aktuelle Richtlinie erhalten haben.

Folgende Berichte stehen zur Verfügung:

- **Endpunkt-Check-In-Einhaltung:** Stellt eine Übersicht über die Tage seit dem Check-in (nach Unternehmensendpunkten geordnet) bereit und gibt das Alter der jeweiligen aktuellen Richtlinie an. Zur Übersicht im Bericht wird der Durchschnittswert dieser Angaben ermittelt.

Für diesen Bericht müssen keine Variablen eingegeben werden. Der Bericht zeigt die Benutzer nach Namen an und gibt Aufschluss darüber, welche Richtlinien ihnen zugewiesen wurden, wie viele Tage seit ihrem letzten Check-in verstrichen sind und wie alt ihre Richtlinie ist.

- **Endpunkt-Clientversionen:** Zeigt die zuletzt gemeldete Version des Clients an jedem Endpunkt. Stellen Sie die Datumsparameter ein, um diesen Bericht zu generieren.
- **Endpunkte, die nie eingecheckt haben:** Listet die Benutzerkonten auf, die sich beim Verwaltungsdienst registriert haben, aber sich nie beim Verteilungsservice für eine Richtlinienaktualisierung angemeldet haben. Wählen Sie eine oder mehrere Gruppen aus, um den Bericht zu generieren.

  Das können Benutzer der Verwaltungskonsole sein, in deren Namen kein Security Client installiert ist.
- **Nichteinhaltung der Gruppenrichtlinie:** Zeigt Gruppen, in denen einige Benutzer nicht über die richtige·Richtlinie verfügen. Für die Generierung des Berichts können für eine oder mehrere Gruppen Auswahlen getroffen werden.
- **Endpunkt-Statusverlauf nach Rechner:** Zeigt den aktuellsten Status (innerhalb eines bestimmten Datumsbereichs) von Endpunkten an, die durch ZENworks Endpoint Security Management geschützt werden. Die Ansicht erfolgt nach Computernamen geordnet. Er zeigt den Namen des angemeldeten Benutzers, die aktuelle Richtlinie, die Version des ZENworks Endpoint Security Management-Client sowie den Netzwerkstandort an. Für diesen Bericht muss ein Datumsbereich eingegeben werden. Der Administrator kann einen Drill-Down-Vorgang ausführen, indem er auf einen Eintrag doppelklickt, um eine vollständige Liste von Statusberichten für einen bestimmten Computer zu sehen.
- **Richtlinienzuweisung:** Zeigt, welche Benutzer und Gruppen (Konten) die angegebene Richtlinie erhalten haben. Wählen Sie die gewünschte Richtlinie in der Liste aus und klicken Sie dann auf *Anzeigen*, um den Bericht auszuführen.
- **Endpunkt-Statusverlauf nach Benutzer:** Zeigt den aktuellsten Status (innerhalb eines bestimmten Datumsbereichs) von Endpunkten an, die durch ZENworks Endpoint Security Management geschützt werden. Die Ansicht erfolgt nach Benutzernamen geordnet. Er zeigt den Computernamen, die aktuelle Richtlinie, die Version des ZENworks Endpoint Security Management-Client sowie den Netzwerkstandort an. Für diesen Bericht muss ein Datumsbereich eingegeben werden. Der Administrator kann einen Drill-Down-Vorgang ausführen, indem er auf einen Eintrag doppelklickt, um eine vollständige Liste von Statusberichten für einen bestimmten Benutzer·zu sehen.

1.6.2 Drill-Down-Berichte für Warnmeldungen

Drill-Down-Berichte für Warnmeldungen stellen zusätzliche warnmeldungsbezogene Informationen zur Verfügung. Diese Berichte zeigen Daten nur dann an, wenn eine Warnmeldung ausgelöst wird. Das Löschen einer Warnmeldung zieht das Löschen des Warnmeldungsberichts nach sich, jedoch stehen die Daten weiterhin in einem Standardbericht zur Verfügung.

Folgende Berichte stehen zur Verfügung:

- **Client Tampering Alert Data:** Zeigt Instanzen an, in denen ein unbefugter Benutzer versucht hat, den ZENworks Security Client zu ändern oder zu deaktivieren.
- **Files Copied Alert Data:** Zeigt Konten, die Daten auf Wechselspeichergeräte kopiert haben.

- **Incorrect Client Version Alert Data:** Zeigt den Statusverlauf des ZENworks Security Client-Aktualisierungsvorgangs.
- **Incorrect Client Policy Alert Data:** Zeigt Benutzer, die nicht über die korrekte Richtlinie verfügen.
- **Integrity Failures Alert Data:** Berichtet über den Verlauf von bestandenen und nicht bestandenen Client-Integritätsprüfungen.
- **Override Attempts Alert Data:** Zeigt Instanzen, in denen Selbstverteidigungsmechanismen des Client administrativ außer Kraft gesetzt wurden, um privilegierte Kontrolle über den ZENworks Security Client zu erhalten.
- **Port Scan Alert Data:** Zeigt die Anzahl blockierter Pakete bei der angegebenen Anzahl verschiedener Ports an. (Eine große Anzahl an Ports kann darauf hinweisen, dass ein Portscan erfolgt ist).
- **Uninstall Attempt Alert Data:** Listet Benutzer auf, die versucht haben, den ZENworks Security Client zu deinstallieren.
- **Unsecure Access Point Alert Data:** Listet nicht sichere Zugriffspunkte auf, die vom ZENworks Security Client erkannt wurden.
- **Unsecure Access Point Connection Alert Data:** Listet nicht sichere Zugriffspunkte auf, mit denen der ZENworks Security Client eine Verbindung hergestellt hat.

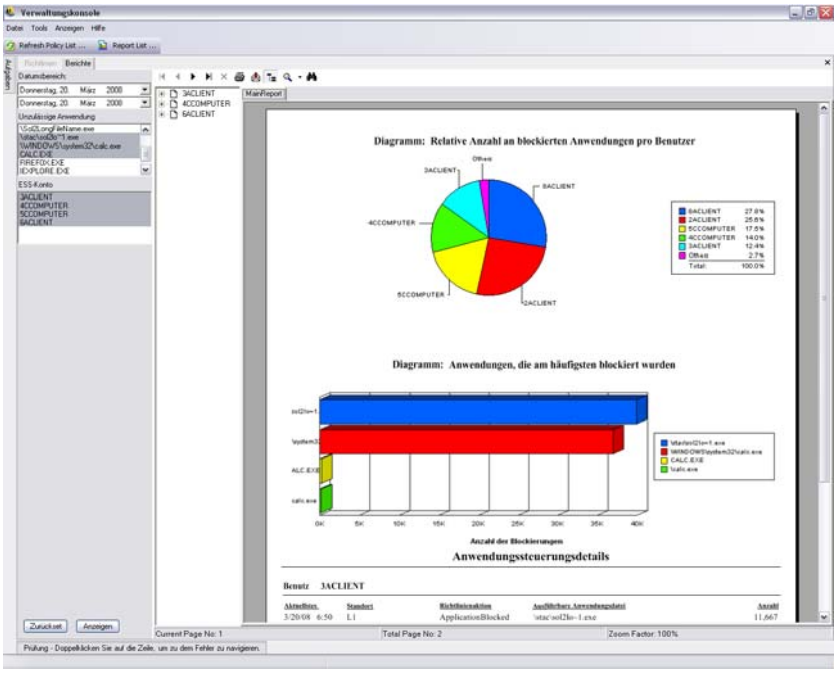
1.6.3 Berichte über Anwendungssteuerung

In Berichten über Anwendungssteuerung werden sämtliche unbefugten Versuche blockierter Anwendungen, auf das Netzwerk zuzugreifen bzw. zur Ausführung zu gelangen, obwohl dies durch die Richtlinie untersagt ist, angezeigt.

Folgender Bericht steht zur Verfügung:

- **Application Control Details:** Zeigt das Datum, den Standort, die vom ZENworks® Security Client ergriffene Maßnahme, die Anwendung, die versucht hat, zur Ausführung zu gelangen, sowie die Häufigkeit an, mit der die Anwendung gestartet wurde. Datumsangaben werden in UTC (Universal Coordinated Time) angezeigt.

Geben Sie die Datumsparameter an, wählen Sie die Anwendungsnamen in der Liste aus, wählen Sie die Benutzerkonten aus und klicken Sie dann auf *Anzeigen*, um den Bericht auszuführen.



1.6.4 Encryption Solution Reports

Ist die Endpunktverschlüsselung aktiviert, geben Encryption Solutions Reports Aufschluss über die Übermittlung von Dateien an verschlüsselte Ordner/von verschlüsselten Ordnern.

Folgende Berichte stehen zur Verfügung:

- **File Encryption Activity:** Zeigt Dateien, auf die Verschlüsselung angewendet wurde.
- **Encryption Exceptions:** Zeigt Fehler aus dem Verschlüsselungs-Subsystem (Beispiel: eine geschützte Datei konnte nicht entschlüsselt werden, da der Benutzer nicht über die richtigen Schlüssel verfügte).
- **File Encryption Volumes:** Zeigt Volumes (z. B. Wechsellaufwerke oder Festplattenpartitionen), die von Novell Encryption Solution verwaltet werden.

1.6.5 Berichte über Endpunktaktivitäten

Berichte über Endpunktaktivitäten bieten Feedback zu einzelnen Richtlinienkomponenten und deren Auswirkung auf den Betrieb des Endpunkts.

Folgende Berichte stehen zur Verfügung:

- **Blockierte Pakete nach IP-Adresse:** Zeigt blockierte Pakete an, nach Ziel-IP gefiltert. Die Datumsangaben werden in UTC (Universal Coordinated Time) angezeigt.

  Wählen Sie die Ziel-IP in der Liste aus und stellen Sie die Datumsparameter ein. Der Bericht zeigt Datumsangaben, Standorte, betroffene Ports und die Namen der blockierten Pakete.
- **Blockierte Pakete nach Benutzer:** Zeigt blockierte Pakete an, nach Benutzer gefiltert. Datumsangaben werden in UTC (Universal Coordinated Time) angezeigt. Die Daten sind im Prinzip dieselben wie für "Blockierte Pakete nach Ziel-IP", jedoch nach Benutzer gegliedert.

- **Network Usage Statistics by User:** Listet gesendete, empfangene oder blockierte Pakete sowie Netzwerkfehler auf, gefiltert nach Benutzern. Für diesen Bericht muss ein Datumsbereich eingegeben werden. Datumsangaben werden in UTC (Universal Coordinated Time) angezeigt.
- **Network Usage Statistics by Adapter Type:** Listet gesendete, empfangene oder blockierte Pakete sowie Netzwerkfehler auf, gefiltert nach Adaptertyp. Für diesen Bericht müssen ein Datumsbereich sowie der Standort eingegeben werden. Datumsangaben werden in UTC (Universal Coordinated Time) angezeigt.

1.6.6 Berichte über Endpunktaktualisierungen

In Berichten über Endpunktaktualisierungen wird der Status des ZENworks Security Client-Aktualisierungsvorgangs angezeigt (siehe „ZSC-Aktualisierung“ auf Seite 67). Datumsangaben werden in UTC (Universal Coordinated Time) angezeigt.

Folgende Berichte stehen zur Verfügung:

- **Diagramm: Prozentsatz der Security Client-Aktualisierungen, bei denen ein Fehler aufgetreten ist:** Stellt den prozentualen Anteil von fehlgeschlagenen ZENworks Security Client-Aktualisierungen (die nicht korrigiert wurden) in einem Diagramm dar. Für die Generierung dieses Berichts sind keine Parameter erforderlich.
- **Verlauf des Security Client-Aktualisierungsstatus:** Zeigt den Statusverlauf des ZENworks Security Client-Aktualisierungsvorgangs. Wählen Sie den Datumsbereich aus und klicken Sie auf *Anzeigen*, um den Bericht auszuführen. Der Bericht zeigt, welche Benutzer sich angemeldet und die Aktualisierung erhalten haben.
- **Diagramm: Art der Security Client-Aktualisierungen, bei denen ein Fehler aufgetreten ist:** Zeigt die ZENworks Security Client-Aktualisierungen an, bei denen ein Fehler aufgetreten ist und keine Korrektur erfolgte. Wählen Sie den Datumsbereich aus und klicken Sie auf "Anzeigen", um den Bericht auszuführen. Der Bericht zeigt, welche Benutzer sich angemeldet haben, bei denen aber die Installation des Updates misslang.

1.6.7 Client Self Defense Reports

Mit Client Self Defense Reports werden Sie informiert, wenn Benutzer versuchen, den ZENworks® Security Client zu ändern oder zu deaktivieren.

Folgender Bericht steht zur Verfügung:

- **ZENworks Security Client Hack Attempts:** Meldet Instanzen, in denen ein unbefugter Benutzer versuchte, den ZENworks Security Client zu ändern oder zu deaktivieren. In UTC angezeigte Datumswerte.

  Geben Sie die Datumsparameter ein und klicken Sie auf *Anzeigen*, um den Bericht auszuführen.

1.6.8 Integrity Enforcement Reports

Integrity Enforcement Reports geben Aufschluss über Antivirus-/Anti-Spyware-Integritätsergebnisse.

Folgende Berichte stehen zur Verfügung:

- **Client Integrity History:** Berichtet über Erfolg bzw. Misserfolg von Client-Integritätsprüfungen. Datumsangaben werden in UTC (Universal Coordinated Time) angezeigt.

  Wählen Sie den Datumsbereich für den Bericht, Integritätsregeln sowie Benutzernamen aus.

- **Unremediated Integrity Failures by Rule:** Berichtet über Integritätsregeln und Tests, bei denen Fehler aufgetreten sind (nicht bestanden) und die noch nicht korrigiert wurden.

  Wählen Sie die Integritätsregeln aus und klicken Sie dann auf *Anzeigen*, um den Bericht auszuführen.

- **Unremediated Integrity Failures by User:** Berichtet über Benutzer, die Integritätstests nicht bestanden haben und bei denen noch keine Korrektur vorgenommen wurde.

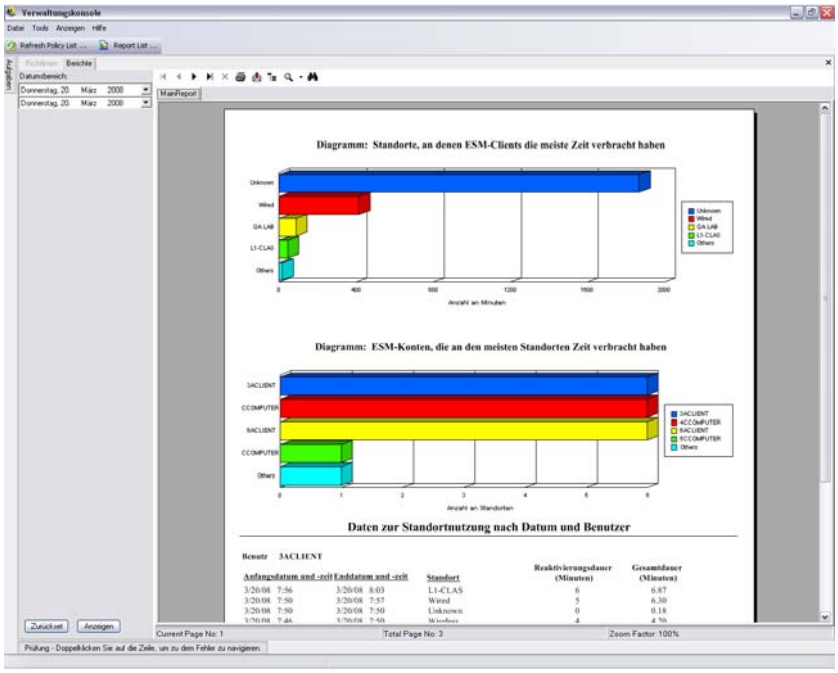
  Wählen Sie die Benutzernamen aus und klicken Sie dann auf *Anzeigen*, um den Bericht auszuführen.

1.6.9 Standortberichte

Der Standortbericht gibt Aufschluss über die allgemeine Standortnutzung, also beispielsweise darüber. welche Standorte von den Benutzern am häufigsten genutzt werden.

Folgender Bericht steht zur Verfügung:

Daten zur Standortnutzung nach Datum und Benutzer: Stellt von individuellen Clients erfasste Daten über die verwendeten Standorte und den jeweiligen Zeitpunkt der Verwendung bereit. Datumsangaben werden in UTC (Universal Coordinated Time) angezeigt. Bei den angezeigten Standorten handelt es sich um von dem Benutzer genutzte Standorte; nicht genutzte Standorte werden nicht angezeigt. Wählen Sie einen Datumsbereich aus, um den Bericht zu generieren.

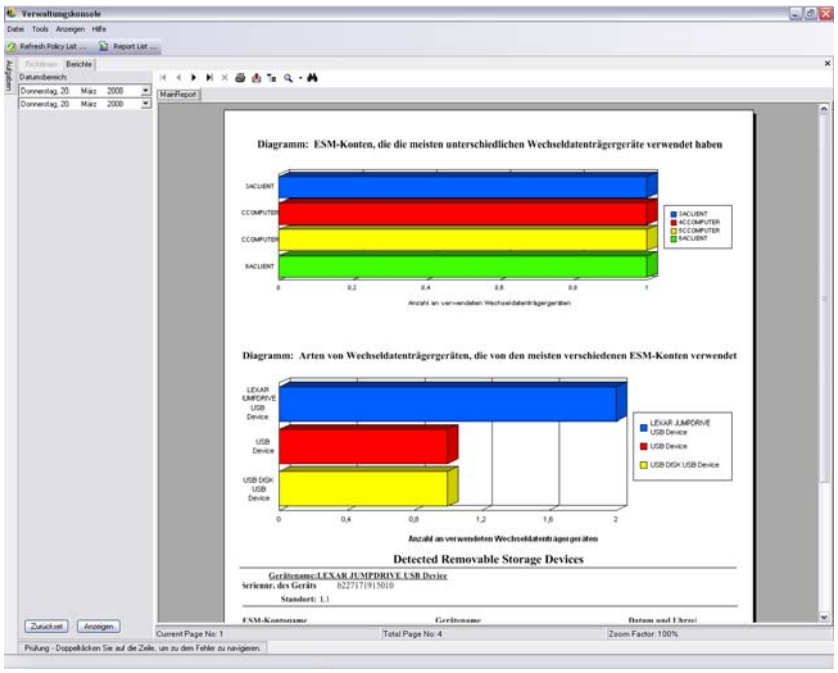


1.6.10 Outbound Content Compliance Reports

Outbound Content Compliance Reports stellen Informationen zur Nutzung von Wechsellaufwerken bereit und geben Aufschluss darüber, welche Dateien auf diese Laufwerke heraufgeladen wurden.

Folgende Berichte stehen zur Verfügung:

- **Removable Storage Activity by Account:** Zeigt Konten, die Daten auf Wechselspeichermedien kopiert haben. Für die Generierung dieses Berichts sind keine Parameter erforderlich.
- **Removable Storage Activity by Device:** Zeigt Wechseldatenträger, auf die Dateien kopiert wurden. Wählen Sie Datumsbereich, Benutzernamen sowie Standorte aus, um diesen Bericht zu generieren.
- **Kopiervorgänge von Wechseldatenträger nach Konto:** Zeigt Dateien an, die von Wechselspeichergeräten auf verwaltete Geräte kopiert wurden.
- **Detected Removable Storage Devices:** Zeigt Wechseldatenträger, die am Endpunkt erkannt wurden. Wählen Sie Datumsbereich, Benutzernamen und Standorte aus, um diesen Bericht zu generieren.



- **Diagramm über 7 Tage Wechselspeicheraktivitäten nach Konto:** Zeigt ein Diagramm mit Konten, die kürzlich Daten auf ein Wechselmedium kopiert haben. Geben Sie den Datumsbereich an, um diesen Bericht zu generieren.

1.6.11 Administrative Overrides Report

Der Administrative Overrides Report gibt Aufschluss über Instanzen, in denen Selbstverteidigungsmechanismen des Client administrativ außer Kraft gesetzt wurden, um privilegierte Kontrolle über den ZENworks® Security Client zu erhalten.

Folgender Bericht steht zur Verfügung:

- **ZENworks Security Client Overrides:** Zeigt erfolgreiche Versuche der Außerkraftsetzung, nach Benutzer und Datum geordnet. Datumsangaben werden in UTC (Universal Coordinated Time) angezeigt.

  Wählen Sie den Benutzer und den Datumsbereich aus und klicken Sie dann auf *Anzeigen*, um den Bericht auszuführen.

1.6.12 Berichte über Endpunktaktualisierungen

In Berichten über Endpunktaktualisierungen wird der Status des ZENworks® Security Client-Aktualisierungsvorgangs angezeigt (siehe „ZSC-Aktualisierung“ auf Seite 67). Datumsangaben werden in UTC (Universal Coordinated Time) angezeigt.

Folgende Berichte stehen zur Verfügung:

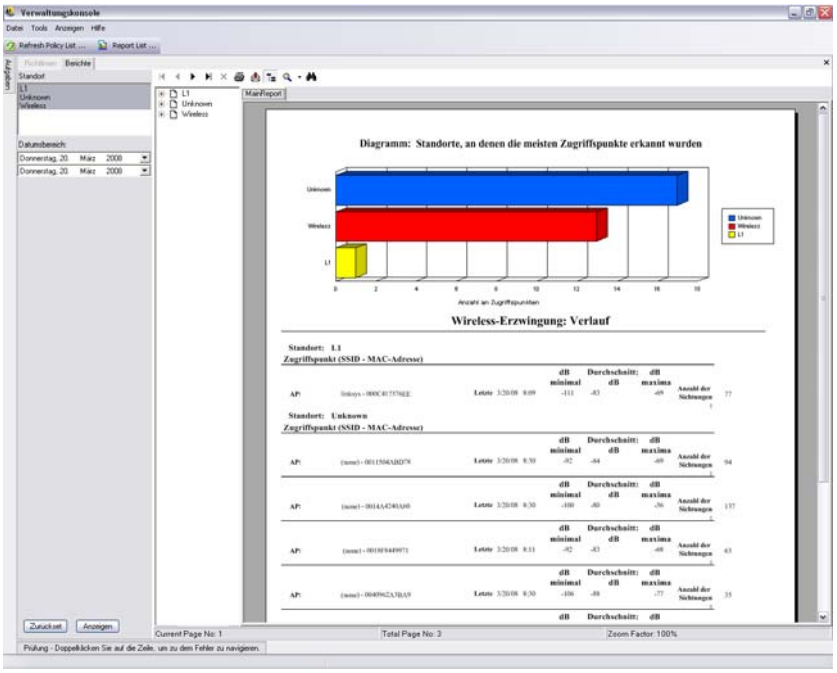
- **Diagramm: Prozentsatz der Security Client-Aktualisierungen, bei denen ein Fehler aufgetreten ist:** Stellt den prozentualen Anteil der ZENworks Security Client-Aktualisierungen, bei denen ein Fehler aufgetreten ist und keine Korrektur erfolgte, in einem Diagramm dar. Für die Generierung dieses Berichts sind keine Parameter erforderlich.
- **Verlauf des Security Client-Aktualisierungsstatus:** Zeigt den Statusverlauf des ZENworks Security Client-Aktualisierungsvorgangs. Wählen Sie den Datumsbereich aus und klicken Sie dann auf *Anzeigen*, um den Bericht auszuführen. Aus dem Bericht geht hervor, welche Benutzer das Check-in vorgenommen und die Aktualisierung erhalten haben.
- **Diagramm: Art der Security Client-Aktualisierungen, bei denen ein Fehler aufgetreten ist:** Zeigt die ZENworks Security Client-Aktualisierungen an, bei denen ein Fehler aufgetreten ist und keine Korrektur erfolgte. Wählen Sie den Datumsbereich aus und klicken Sie dann auf *Anzeigen*, um den Bericht auszuführen. Aus dem Bericht geht hervor, welche Benutzer das Check-in vorgenommen haben, bei denen die Aktualisierung jedoch nicht installiert werden konnte.

1.6.13 Wireless Enforcement Reports

Wireless Enforcement Reports geben Aufschluss über Wi-Fi-Umgebungen, denen der Endpunkt ausgesetzt ist.

Folgende Berichte stehen zur Verfügung:

- **Wireless Connection Availability:** Zeigt die Zugriffspunkte, die für Verbindungen zur Verfügung stehen, nach Richtlinie und Standort. Umfasst Kanal, SSID, MAC-Adresse sowie Angaben dazu, ob der Zugriffspunkt verschlüsselt ist.
- **Wireless-Verbindungsversuche:** Stellt eine Liste mit Zugriffspunkten bereit, mit denen Geräte versucht haben, eine Verbindung herzustellen (nach Standort und Konto geordnet).
- **Wireless-Umgebung: Verlauf:** Stellt eine Übersicht über alle ermittelten Zugriffspunkte bereit, ungeachtet des Eigentümers. Gibt Aufschluss über Frequenz, Signalstärke sowie darüber, ob der Zugriffspunkt verschlüsselt ist. Datumsangaben werden in UTC (Universal Coordinated Time) angezeigt. Wählen Sie die gewünschten Standorte und den Datumsbereich aus, um diesen Bericht zu generieren.



1.7 Verwenden von ZENworks Storage Encryption Solution

ZENworks® Storage Encryption Solution ermöglicht die vollständige und zentrale Sicherheitsverwaltung aller mobilen Daten durch aktive Durchsetzung einer unternehmensspezifischen Verschlüsselungsrichtlinie am Endpunkt selbst.

Mit ZENworks Storage Encryption Solution haben Sie folgende Möglichkeiten:

- Zentrale Erstellung, Verteilung, Durchsetzung und Überwachung von Verschlüsselungsrichtlinien an allen Endpunkten und Wechseldatenträgern.
- Verschlüsselung aller Dateien, die in ein bestimmtes Verzeichnis auf allen Partitionen des Festplattenlaufwerks gespeichert oder kopiert werden.
- Verschlüsselung aller Dateien, die auf Wechseldatenträger kopiert werden.
- Beliebige Freigabe von Dateien in einem Unternehmen, während unbefugter Zugriff auf Dateien blockiert wird.
- Freigabe von passwortgeschützten, verschlüsselten Dateien für Mitarbeiter außerhalb des Unternehmens durch ein verfügbares Verschlüsselungsdienstprogramm.
- Bequeme Aktualisierung, Sicherung und Wiederherstellung von Schlüsseln über die Richtlinie, ganz ohne Datenverlust.

1.7.1 Erläuterung: ZENworks Storage Encryption Solution

Datenverschlüsselung wird durch die Erstellung und Verteilung von Sicherheitsrichtlinien zur Datenverschlüsselung durchgesetzt. Vertrauliche Daten am Endpunkt werden in einem verschlüsselten Ordner gespeichert. Der Benutzer kann auf diese Daten außerhalb des verschlüsselten Ordners zugreifen und sie kopieren und die Dateien freigeben, jedoch bleiben die Daten innerhalb des Ordners verschlüsselt. Versuche, die Daten zu lesen, sind für unbefugte

Benutzer an diesem Computer nicht erfolgreich. Wenn die Richtlinie aktiviert ist, wird ein verschlüsselter `Safe Harbor`-Ordner dem Stammverzeichnis aller Nichtsystemlaufwerke am Endgerät hinzugefügt.

Vertrauliche Daten, die auf einem Thumbdrive oder einem anderen Wechselspeichergerät gespeichert·werden, werden sofort verschlüsselt und können nur auf Computern derselben Richtliniengruppe gelesen werden. Ein Freigabeordner kann optional aktiviert werden, wodurch Benutzer die Dateien mit Personen außerhalb ihrer Richtliniengruppe über ein Passwort gemeinsam nutzen können (siehe „Datenverschlüsselung“ auf Seite 64).

1.7.2 Freigabe verschlüsselter Dateien

Benutzer in derselben Richtliniengruppe (Benutzer, die dieselbe Sicherheitsrichtlinie erhalten haben) besitzen die Schlüssel für den Zugriff auf Daten, die auf dem Endpunkt gespeichert sind, sowie auf Daten, die auf Thumbdrives und andere Wechselspeichergeräte verschoben wurden.

Benutzer in einer separaten Richtliniengruppe (mit aktivierter Verschlüsselung) können mithilfe eines Zugriffspassworts auf verschlüsselte Daten zugreifen, die sich im Ordner `Freigegebene Dateien` befinden. Diese Benutzer können keine verschlüsselten Dateien außerhalb des Ordners `Freigegebene Dateien` lesen.

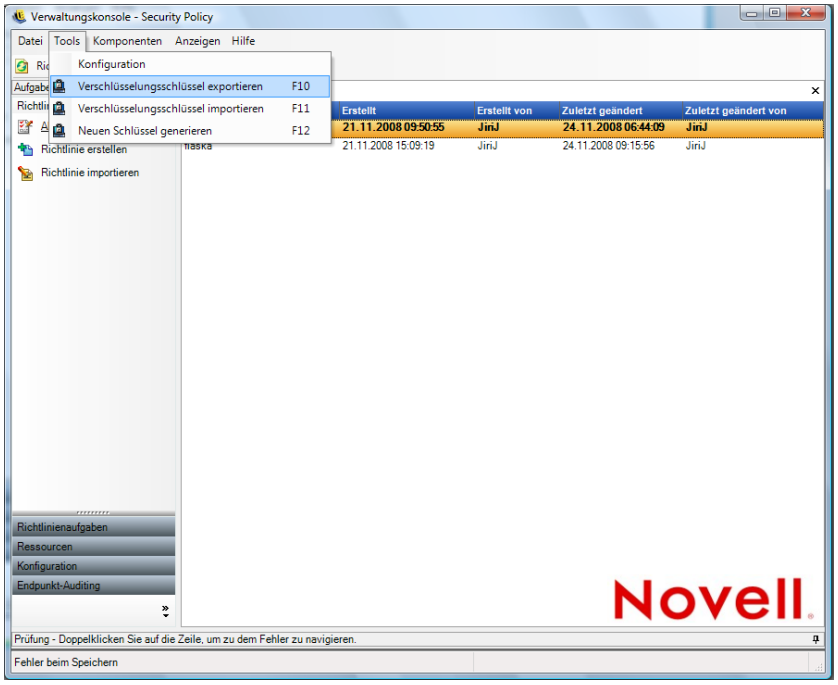
Benutzer, in deren Richtlinie die Verschlüsselung nicht aktiviert ist, und Benutzer, auf deren Computer der ZENworks Security Client nicht installiert ist (z. B. unternehmensfremde Auftragnehmer), können keine Dateien lesen, die sich außerhalb des Ordners `Freigegebene Dateien` befinden. Sie benötigen das ZENworks® File Decryption, um mit einem Passwort auf die Dateien zuzugreifen und sie lesen zu können. Weitere Informationen finden Sie unter Abschnitt 1.9, „Verwenden des ZENworks File Decryption Utility“, auf Seite 42.

1.8 Verwenden der Schlüsselverwaltung

Mithilfe der Schlüsselverwaltung können Sie einen Verschlüsselungsschlüssel sichern, importieren und aktualisieren. Es wird empfohlen, Verschlüsselungsschlüssel zu exportieren und zu speichern, um sicherzustellen, dass Daten nach einen Systemausfall oder versehentlicher Richtlinienänderung entschlüsselt werden können.

Der gemeinsame Schlüssel ist der Standard-Verschlüsselungsschlüssel, der für alle Datenverschlüsselungsagenten verwendet wird. Der Verschlüsselungsschlüssel kann im Manipulationsfall bzw. als Sicherheitsmaßnahme aktualisiert werden. Das Generieren eines neuen gemeinsamen Schlüssels führt zu einem temporären Leistungsabfall, während der verwaltete Inhalt neu verschlüsselt wird.

Der Zugriff auf Steuerelemente für Verschlüsselungsschlüssel erfolgt über das Menü *Werkzeuge* der Verwaltungskonsole.



1.8.1 Exportieren von Verschlüsselungsschlüsseln

Für Sicherungszwecke und zum Übertragen des Schlüssels an eine andere Instanz des Verwaltungsdiensts kann der aktuelle Verschlüsselungsschlüsselsatz an einen angegeben Dateispeicherort exportiert werden.

1. Wählen Sie die Optionsfolge *Werkzeuge* > *Verschlüsselungsschlüssel exportieren*.
2. Geben Sie einen Pfad sowie einen·Dateinamen an oder klicken Sie auf *Durchsuchen*, um einen Dateispeicherort auszuwählen.
3. Stellt das Passwort bereit. Der Schlüssel kann nicht ohne Passwort exportiert werden.
4. Klicken Sie auf *OK*.

Alle Schlüsseldateien in der Datenbank sind Bestandteil der exportierten Datei.

1.8.2 Importieren von Verschlüsselungsschlüsseln

Sie können Schlüssel aus einer Sicherungskopie oder aus einer anderen Instanz des Verwaltungsdiensts importieren. So können Endpunkte, die von diesem Verwaltungsdienst verwaltet werden, Dateien lesen, die durch andere ZENworks Endpoint Security Management-Installationen geschützt sind. Duplikate werden beim Importieren von Schlüsseln ignoriert. Importierte Schlüssel werden Teil Ihres Schlüsselsatzes und ersetzen nicht den aktuellen gemeinsamen Schlüssel. Alle Schlüssel werden mitgegeben, wenn eine neue Richtlinie veröffentlicht wird.

1. Wählen Sie die Optionsfolge *Werkzeuge* > *Verschlüsselungsschlüssel importieren*.
2. Geben Sie den Dateinamen (und den Dateispeicherort) an oder klicken Sie auf *Durchsuchen*, um die Schlüsseldatei auszuwählen.
3. Geben Sie das Passwort für den Verschlüsselungsschlüssel an.
4. Mit *OK* wird der Schlüssel in die Datenbank importiert.

1.8.3 Generieren eines neuen Schlüssels

1 Wählen Sie die Optionsfolge *Werkzeuge* > *Neuen Schlüssel generieren*.

Alle vorherigen Schlüssel sind in der Richtlinie gespeichert.

1.9 Verwenden des ZENworks File Decryption Utility

Das ZENworks® File Decryption Utility extrahiert geschützte Daten aus dem Ordner `Freigegebene Dateien` auf verschlüsselte Wechselspeichergeräte. Dieses einfache Werkzeug kann Dritten zur Verfügung gestellt werden, um ihnen den Zugriff auf die Dateien im Ordner `Freigegebene Dateien` zu ermöglichen; es kann jedoch nicht auf dem Wechselspeichergerät gespeichert werden.

- Abschnitt 1.9.1, „Verwenden des File Decryption Utility“, auf Seite 42
- Abschnitt 1.9.2, „Konfigurieren des File Decryption Utility“, auf Seite 42

Die folgenden Abschnitte enthalten weitere Informationen:

1.9.1 Verwenden des File Decryption Utility

So verwenden Sie das Dienstprogramm zur Dateientschlüsselung (File Decryption Utility):

1 Schließen Sie den Wechseldatenträger an den passenden Anschluss an Ihrem Computer an.

2 Öffnen Sie das File Decryption Utility.

3 Navigieren Sie zum Verzeichnis `Freigegebene Dateien` des Speichergeräts und wählen Sie die gewünschte Datei aus.

4 Wenn Sie Verzeichnisse (Ordner) anstelle von Dateien extrahieren möchten, klicken Sie auf die Schaltfläche *Erweitert*, wählen Sie *Verzeichnisse* aus und navigieren Sie dann zum entsprechenden Verzeichnis. (Klicken Sie auf *Standard*, um zur Standardanzeige zurückzukehren.)

5 Wählen Sie auf dem lokalen Computer das Verzeichnis aus, in dem diese Dateien gespeichert werden sollen.

6 Klicken Sie auf *Extrahieren*.

Die Transaktion kann überwacht werden, indem Sie auf *Status anzeigen* klicken.

1.9.2 Konfigurieren des File Decryption Utility

Das File Decryption Utility kann mit dem aktuellen Schlüsselsatz im Administrator-Modus konfiguriert werden, um alle Daten von einem verschlüsselten Speichergerät zu extrahieren. Von dieser Konfiguration wird abgeraten, da hierbei die Gefahr besteht, dass alle aktuellen Schlüssel, die von ZENworks Storage Encryption Solution verwendet werden, beeinträchtigt werden. In Fällen, in denen sich die Daten auf andere Weise nicht wiederherstellen lassen, ist diese Konfiguration jedoch möglicherweise die einzige Lösung.

So konfigurieren Sie das Tool:

1. Erstellen Sie eine Verknüpfung mit dem File Decryption Utility in seinem aktuellen Verzeichnis.
2. Klicken Sie mit der rechten Maustaste auf die Verknüpfung und klicken Sie dann auf *Eigenschaften*.
3. Geben Sie am Ende des Zielnamens und nach den Anführungszeichen -k ein (Beispiel: `"C:\Admin Tools\stdecrypt.exe" -k`).
4. Klicken Sie auf *Anwenden* > *OK*.
5. Rufen Sie das Werkzeug über die Verknüpfung auf und klicken Sie dann auf *Erweitert*.
6. Klicken Sie auf die Schaltfläche *Schlüssel laden*, um das Dialogfeld "Schlüssel importieren" zu öffnen.
7. Suchen Sie die Schlüsseldatei und geben Sie dann das Passwort für die Schlüssel an.

Alle Dateien, die mit diesen Schlüsseln verschlüsselt sind, können nun extrahiert werden.

1.10 Verwenden des Benutzeraußerkraftsetzung Schlüsselgenerators

Unterbrechungen des produktiven Ablaufs, die unter Umständen·aufgrund eingeschränkter Konnektivität, Unterbindung der Ausführung bestimmter Software bzw. eingeschränkten Zugriffs auf Wechselspeichergeräte auftreten, sind höchstwahrscheinlich auf die Sicherheitsrichtlinie zurückzuführen, die vom ZENworks® Security Client erzwungen wird. Durch einen Standortwechsel oder das Ändern der Firewall-Einstellungen lassen sich diese Einschränkungen in der Regel umgehen, und es stehen wieder sämtliche Funktionen zur Verfügung. In einigen Fällen kann die Einschränkung jedoch so implementiert sein, dass sie für alle Standorte und Firewall-Einstellungen gilt oder dass der Benutzer nicht in der Lage ist, den Standort oder eine Firewall-Einstellung zu ändern.

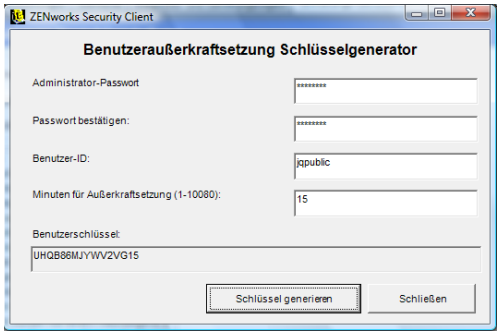
In diesem Fall können die Einschränkungen in der aktuellen Richtlinie durch ein Überschreiben des Passworts aufgehoben werden, um Produktivität zu ermöglichen, bis die Richtlinie geändert werden kann. Mithilfe dieser Funktion kann ein Administrator ein passwortgeschütztes Überschreiben für angegebene Benutzer und Funktionen einrichten, um die erforderlichen Aktivitäten temporär zu erlauben.

Durch die Passwort-Außerkraftsetzung wird·die aktuelle Sicherheitsrichtlinie deaktiviert und die standardmäßige Richtlinie "Alle geöffnet" für einen vordefinierten Zeitraum wiederhergestellt. Am Ende dieses Zeitraums wird die aktuelle bzw. aktualisierte Richtlinie wiederhergestellt. Das Passwort für eine Richtlinie wird in den Einstellungen "Globale Regeln" der Sicherheitsrichtlinie festgelegt.

Die Passwort-Außerkraftsetzung hat folgende Funktionen:

- Setzt eine Anwendungsblockierung außer Kraft
- Ermöglicht den Benutzern, den Standort zu ändern
- Ermöglicht den Benutzern, Firewall-Einstellungen zu ändern
- Setzt die Hardwaresteuerung (Thumbdrives, CD-ROM usw.) außer Kraft

Das in die Richtlinie eingegebene Passwort sollte unter keinen Umständen an einen Benutzer weitergegeben werden. Der Benutzeraußerkraftsetzung Schlüsselgenerator sollte zur Generierung eines Schlüssels für die kurzfristige Verwendung verwendet werden.



So generieren Sie einen Überschreibungsschlüssel:

1. Rufen Sie den Benutzeraußerkraftsetzung Schlüsselgenerator auf (*Start > Alle Programme > Novell > ESM Management Console > Benutzeraußerkraftsetzung Schlüsselgenerator*).
2. Geben Sie das Richtlinienpasswort im Feld für das Administratorpasswort an und bestätigen Sie es im darauffolgenden Feld.
3. Geben Sie den Benutzernamen an, unter dem sich der Endbenutzer angemeldet hat.
4. Geben Sie den Zeitraum an, für den die Richtlinie deaktiviert werden soll.
5. Klicken Sie auf *Schlüssel generieren*, um einen Überschreibungsschlüssel zu generieren.

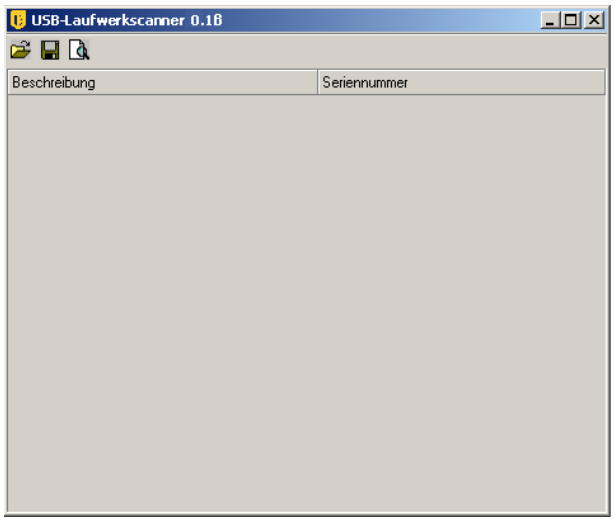
Dieser Schlüssel kann dem Benutzer entweder während eines Anrufs beim Helpdesk vorgelesen werden oder er kann kopiert und in eine E-Mail eingefügt werden. Der Benutzer gibt dann den Schlüssel in das ZENworks Security Client-Verwaltungsfenster ein (ziehen Sie das *Endpoint Security Management-Handbuch zu ZENworks Security Client zurate*). Dieser Schlüssel hat nur für die Richtlinie dieses Benutzers und nur für den angegebenen Zeitraum Gültigkeit. Der Schlüssel kann nur ein einziges Mal verwendet werden.

Hinweis: Wenn sich der Benutzer während der Passwort-Außerkraftsetzung abmeldet oder den Computer neu bootet, läuft das Passwort ab und es muss ein neues ausgegeben werden.

Wird vor Ablauf der Frist eine neue Richtlinie geschrieben, sollte der Benutzer angewiesen werden, auf Richtlinienaktualisierung zu prüfen, anstatt im Dialogfeld "Info" des ZENworks Security Client auf die Schaltfläche *Richtlinie laden* zu klicken.

1.11 USB-Laufwerkscanner

Eine Liste mit zugelassenen USB-Geräten kann mit dem optionalen USB-Laufwerkscanner (im Installationspaket enthalten) generiert und in eine Richtlinie importiert werden.



So generieren Sie eine Liste mit zugelassenen Geräten:

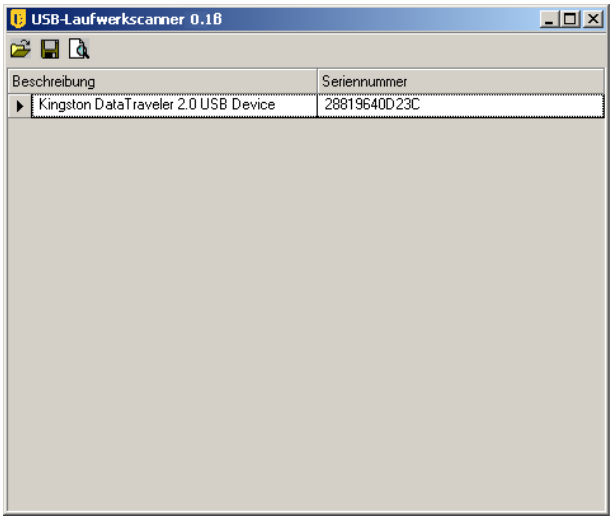
1 Öffnen Sie den USB-Laufwerkscanner.

Hinweis: Es handelt sich hierbei um eine separate Installation, die nicht im Zusammenhang mit dem Verwaltungsdienst und der Verwaltungskonsole steht. Auf dem Desktop befindet sich eine Verknüpfung zu diesem Werkzeug.

---

2 Verbinden Sie ein USB-(Universal Serial Bus-)Gerät mit dem USB-Anschluss des Computers. Das Gerät muss·eine Seriennummer aufweisen.

3 Klicken Sie auf das Symbol für die Absuche (). Der Name des Geräts sowie seine Seriennummer werden in den entsprechenden Feldern angezeigt.



4 Wiederholen Sie Schritt 2 und Schritt 3, bis sämtliche Geräte in die Liste aufgenommen wurden.

5 Klicken Sie auf das Symbol zum `Speichern` ().

Anweisungen zum Importieren der Liste in eine Richtlinie finden Sie unter Abschnitt , „Bevorzugte Geräte“, auf Seite 57.

Wenn Sie eine gespeicherte Datei bearbeiten möchten, klicken Sie auf das Symbol zum *Durchsuchen* (), um die Datei zu öffnen.

Erstellen und Verteilen von Sicherheitsrichtlinien

2

Mithilfe von Sicherheitsrichtlinien gewährleistet der ZENworks® Security Client die Standortsicherung für mobile Benutzer. Die Entscheidung hinsichtlich der Verfügbarkeit von Ports, der Verfügbarkeit von Netzwerkanwendungen, dem Zugriff auf Speichergeräte sowie darüber, ob die Konnektivität verkabelt oder kabellos (Wi-Fi) erfolgt, trifft der Administrator für die einzelnen Standorte.

Sicherheitsrichtlinien können ganz individuell für das Unternehmen, einzelne Benutzergruppen oder einzelne Benutzer/Computer erstellt werden. Sicherheitsrichtlinien können für 100%ige Mitarbeiterproduktivität bei gleichzeitigem Schutz des Endpunkts sorgen; Mitarbeiter können jedoch auch auf die Ausführung bestimmter Anwendungen und die ausschließliche Nutzung autorisierter Hardware beschränkt werden.

Die folgenden Abschnitte enthalten weitere Informationen:

- Abschnitt 2.1, „Navigieren in der Verwaltungskonsole“, auf Seite 47
- Abschnitt 2.2, „Erstellen von Sicherheitsrichtlinien“, auf Seite 50
- Abschnitt 2.3, „Importieren und Exportieren von Richtlinien“, auf Seite 113

2.1 Navigieren in der Verwaltungskonsole

So erstellen Sie eine Sicherheitsrichtlinie:

1. Wählen Sie in der Verwaltungskonsole die Optionsfolge *Datei* > *Neue Richtlinie erstellen*.
2. Geben Sie den Namen für die neue Richtlinie an und klicken Sie dann auf *Erstellen*. Daraufhin wird die Verwaltungskonsole mit der Symbolleiste und den Registerkarten für Richtlinien angezeigt.

In den nachfolgenden Abschnitten wird die Benutzeroberfläche der Verwaltungskonsole erläutert, und zwar im Hinblick auf das Erstellen und Verteilen von Sicherheitsrichtlinien über ZENworks® Endpoint Security Management:

- Abschnitt 2.1.1, „Verwenden der Registerkarten und des Baums für Richtlinien“, auf Seite 47
- Abschnitt 2.1.2, „Verwenden der Richtliniensymbolleiste“, auf Seite 48

2.1.1 Verwenden der Registerkarten und des Baums für Richtlinien

Wenn Sie eine Sicherheitsrichtlinie erstellen oder bearbeiten möchten, nutzen Sie die verfügbaren Registerkarten am oberen Rand der Verwaltungskonsole sowie die Optionen im Baum *Globale Einstellungen* im linken Bereich.

Es stehen u. a. folgende Registerkarten zur Verfügung:

- **Allgemeine Richtlinieneinstellungen:** Die allgemeinen Richtlinieneinstellungen werden in der gesamten Richtlinie als Standard angewendet und sind nicht standortspezifisch.

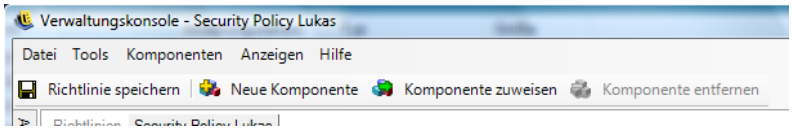
  Über die allgemeinen Richtlinieneinstellungen lassen sich folgende Einstellungen konfigurieren:

  - Richtlinieneinstellungen
  - Wireless-Steuerung
  - Kommunikationshardware
  - Steuerelement für Speichergerätsteuerung
  - USB-Konnektivität
  - Datenverschlüsselung
  - ZENworks Security Client
  - VPN-Erzwingung
- **Standorte:** Diese Richtlinienregeln werden für einen spezifischen Standorttyp angewendet, egal, ob als einzelnes Netzwerk oder eine Art von Netzwerk (Café, Flughafen) angegeben.
- **Integritäts- und Behebungsregeln:** Diese Regeln gewährleisten, dass essenzielle Software (z. B. Antivirus- und Spyware-Programme) auf dem Gerät ausgeführt wird und auf dem neuesten Stand ist
- **Einhaltungsberichterstellung:** Informiert die Richtlinie darüber, ob Berichtsdaten (einschließlich des Datentyps) für diese spezielle Richtlinie erfasst werden.
- **Herausgeben:** Veröffentlicht die vollständige Richtlinie für einzelne Benutzer, Verzeichnisdienst-Benutzergruppen und einzelne Computer.

Im Richtlinienbaum werden die verfügbaren Teilmengenkomponenten für die Registerkartenkategorien angezeigt. Unter *Allgemeine Richtlinieneinstellungen* sind beispielsweise *Richtlinieneinstellungen*, *Wireless-Steuerung*, *Komm-Hardware* und *Speichergerätsteuerung* zu finden. Für die Definition einer Kategorie sind nur die in der primären Teilmenge enthaltenen Elemente erforderlich; bei den restlichen Teilmengen handelt es sich um optionale Komponenten.

2.1.2 Verwenden der Richtliniensymbolleiste

Die Richtliniensymbolleiste enthält sechs Steuerelemente. Das Steuerelement *Richtlinie speichern* steht während der gesamten Richtlinienerstellung zur Verfügung, die Komponentensteuerelemente hingegen nur auf den Registerkarten für Standorte und *Integrität und Sanierung*.

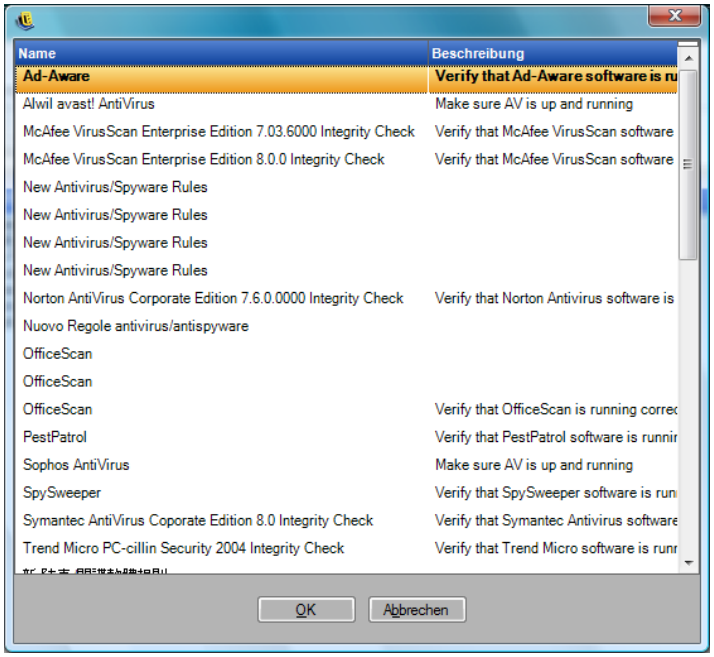


Nachfolgend finden Sie eine Erläuterung der Tools.

- **Speichern Richtlinie:** Speichert die Richtlinie in ihrem aktuellen Zustand.

Wichtig: Bei der Durcharbeitung der einzelnen Komponententeilmengen wird dringend empfohlen, regelmäßig auf das Symbol *Speichern* in der Richtliniensymbolleiste zu klicken. Wenn in einer Komponente unvollständige oder falsche Daten eingegeben werden, wird der Bildschirm mit der Fehlerbenachrichtigung angezeigt (weitere Details finden Sie unter Abschnitt 2.2.6, „Fehlerbenachrichtigung“, auf Seite 112).

- **Neue Komponente:** Erstellt in einer Teilmenge für Standort oder Integrität eine neue Komponente. Nach dem Speichern der Richtlinie steht eine neue Komponente zur Verfügung, die mit anderen Richtlinien verknüpft werden kann.
- **Komponente verknüpfen:** Öffnet den Bildschirm für die Komponentenauswahl für die aktuelle Teilmenge. Zu den verfügbaren Komponenten zählen sämtliche vordefinierten Komponenten, die zum Installationszeitpunkt zur Verfügung standen, sowie alle Komponenten, die in anderen Richtlinien erstellt wurden.



Wichtig: Änderungen, die an verknüpften Komponenten vorgenommen wurden, wirken sich auf alle anderen Instanzen der jeweiligen Komponente aus.

Sie können beispielsweise eine einzelne Standortkomponente namens "Arbeit" erstellen, die die Unternehmens-Netzwerkumgebung und die Sicherheitseinstellungen definiert, die jedes Mal angewendet werden sollen, wenn sich ein Endpunkt in dieser Umgebung befindet. Diese Komponente kann nun auf alle Sicherheitsrichtlinien angewendet werden. Wenn Aktualisierungen der Umgebung oder Sicherheitseinstellungen in der Komponente in einer Richtlinie geändert werden, wird die Aktualisierung derselben Komponente in allen anderen Richtlinien vorgenommen, mit denen sie verknüpft ist.

Mithilfe des Befehls *Auslastung anzeigen* können alle anderen mit dieser Komponente verknüpften Richtlinien angezeigt werden.

- **Komponente entfernen:** Entfernt eine Komponente aus der Richtlinie. Die Komponente kann weiterhin in dieser und anderen Richtlinien verknüpft werden.
- **Richtlinienliste aktualisieren:** Aktualisiert die Richtlinienliste.
- **Berichtsliste:** Zeigt die Liste der Berichte an.

2.2 Erstellen von Sicherheitsrichtlinien

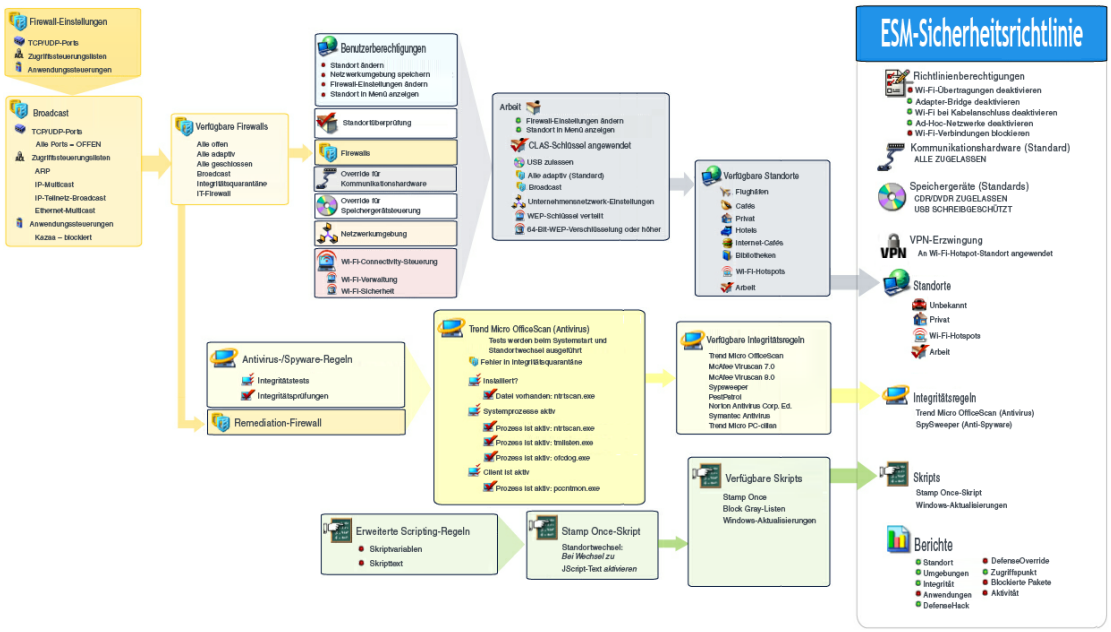
1. Wählen Sie in der Verwaltungskonsole die Optionsfolge *Datei* > *Neue Richtlinie erstellen*.
2. Geben Sie den Namen für die neue Richtlinie an und klicken Sie dann auf *Erstellen*. Daraufhin wird die Verwaltungskonsole mit der Symbolleiste und den Registerkarten für Richtlinien angezeigt.
3. Konfigurieren Sie die Richtlinieneinstellungen anhand der Informationen in folgenden Abschnitten:

- Abschnitt 2.2.1, „Allgemeine Richtlinieneinstellungen“, auf Seite 51
- Abschnitt 2.2.2, „Standorte“, auf Seite 73
- Abschnitt 2.2.3, „Integritäts- und Behebungsregeln“, auf Seite 100
- Abschnitt 2.2.4, „Einhaltungsberichterstellung“, auf Seite 108
- Abschnitt 2.2.5, „Herausgeben“, auf Seite 110
- Abschnitt 2.2.6, „Fehlerbenachrichtigung“, auf Seite 112
- Abschnitt 2.2.7, „Auslastung anzeigen“, auf Seite 113

Zum Erstellen von Sicherheitsrichtlinien werden sämtliche allgemeinen Einstellungen (Standardverhalten) definiert, dann Komponenten für diese Richtlinie erstellt und vorhandene Komponenten verknüpft (z. B. Standorte, Firewalls und Integritätsregeln) und abschließend die Einhaltungs-Berichterstellungsfunktion für die Richtlinie eingerichtet.

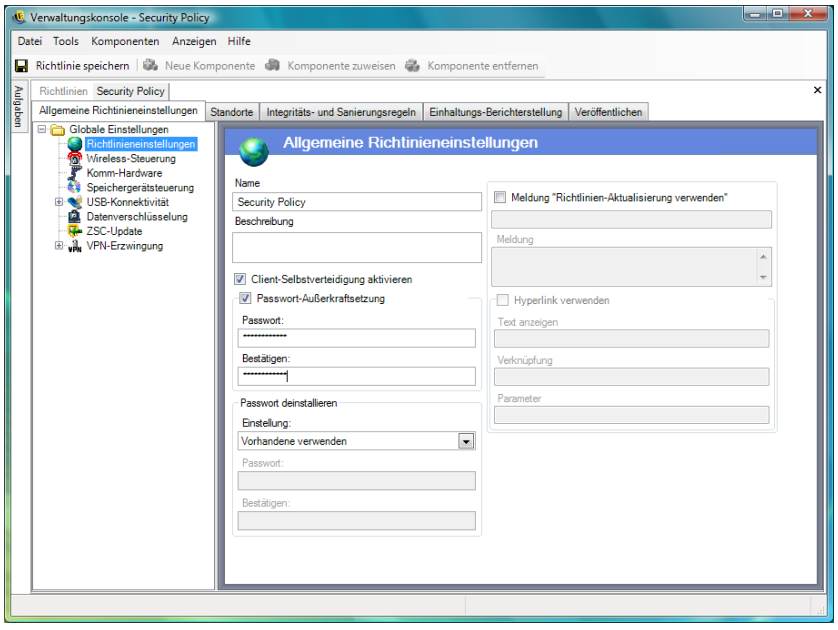
Die Komponenten werden entweder in einer "Dummy"-Richtlinie erstellt, oder es werden von anderen Komponenten aus Verknüpfungsvorgänge durchgeführt. Bei den ersten paar Richtlinien wird davon ausgegangen, dass Sie sämtliche eindeutigen Standorte, Firewall-Einstellungen und Integritätsregeln für das Unternehmen definieren. Diese Komponenten werden für die etwaige spätere Verwendung in anderen Richtlinien in der Datenbank des Verwaltungsdienst gespeichert.

Im nachfolgenden Diagramm sind die Komponenten der einzelnen Ebenen sowie eine Richtlinie zu sehen, die auf der jeweiligen Auswahl basiert.



2.2.1 Allgemeine Richtlinieneinstellungen

Die allgemeinen Richtlinieneinstellungen werden als grundlegende Standardwerte für die Richtlinie angewendet. Wenn Sie auf dieses Steuerelement zugreifen möchten, wechseln Sie zur Verwaltungskonsole und klicken Sie dann auf die Registerkarte *Allgemeine Richtlinieneinstellungen*.



In den nachfolgenden Abschnitten finden Sie weitere Informationen zu den Einstellungen, die auf allgemeiner (globaler) Basis konfiguriert werden können:

- „Richtlinieneinstellungen“ auf Seite 52

- „Wireless-Steuerung“ auf Seite 53
- „Kommunikationshardware“ auf Seite 54
- „Steuerelement für Speichergerätsteuerung“ auf Seite 55
- „USB-Konnektivität“ auf Seite 58
- „Datenverschlüsselung“ auf Seite 64
- „ZSC-Aktualisierung“ auf Seite 67
- „VPN-Erzwingung“ auf Seite 68
- „Benutzerdefinierte Meldung“ auf Seite 71
- „Hyperlinks“ auf Seite 72

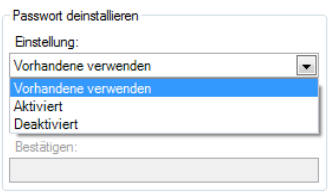
Richtlinieneinstellungen

Zu den primären allgemeinen Einstellungen zählen:

- **Name und Beschreibung:** Der Richtlinienname wird zu Beginn des Richtlinienerstellungsvorgangs angegeben. Sie können den Namen bearbeiten oder eine Beschreibung·der Richtlinie eingeben.
- **Client-Selbstverteidigung aktivieren:** Die Client-Selbstverteidigung kann nach Richtlinie aktiviert bzw. deaktiviert werden. Bleibt dieses Kästchen aktiviert (mit einem Häkchen versehen), wird sichergestellt, dass die Client-Selbstverteidigung aktiv ist. Durch Deaktivieren (Entfernen des Häkchens) wird die Client-Selbstverteidigung für alle Endpunkte deaktiviert, die diese Richtlinie verwenden.
- **Passwort-Außerkraftsetzung:** Mit dieser Funktion kann ein Administrator eine Passwort-Außerkraftsetzung festlegen, durch die die Richtlinie für einen festgelegten Zeitraum vorübergehend deaktiviert werden kann. Aktivieren Sie das Kontrollkästchen *Passwort-Außerkraftsetzung* und geben Sie das Passwort im entsprechenden Feld an. Geben Sie im Bestätigungsfeld das Passwort erneut ein. Verwenden Sie dieses Passwort im Generator für die Passwort-Außerkraftsetzung, um den Passwortschlüssel für diese Richtlinie zu generieren. Weitere Informationen finden Sie unter Abschnitt 1.10, „Verwenden des Benutzeraußerkraftsetzung Schlüsselgenerators“, auf Seite 43.

  Warnung: Es wird dringend davon abgeraten, Benutzern dieses Passwort zu nennen. Der Override Password Generator sollte verwendet werden, um einen temporären Schlüssel für sie zu generieren.

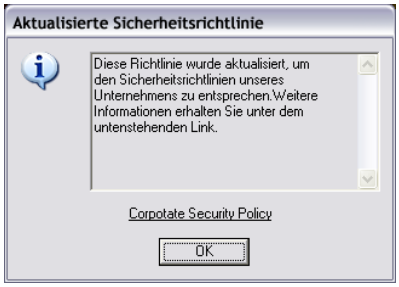
- **Passwort deinstallieren:** Es empfiehlt sich, jede ZENworks* Security Client-Instanz mit einem Deinstallationspasswort zu installieren, um Benutzer daran zu hindern, die Software zu deinstallieren. Dieses Passwort wird normalerweise zum Installationszeitpunkt konfiguriert, das Passwort kann jedoch per Richtlinie aktualisiert, aktiviert bzw. deaktiviert werden.



In der Dropdown-Liste können Sie eine der folgenden Einstellungen auswählen:

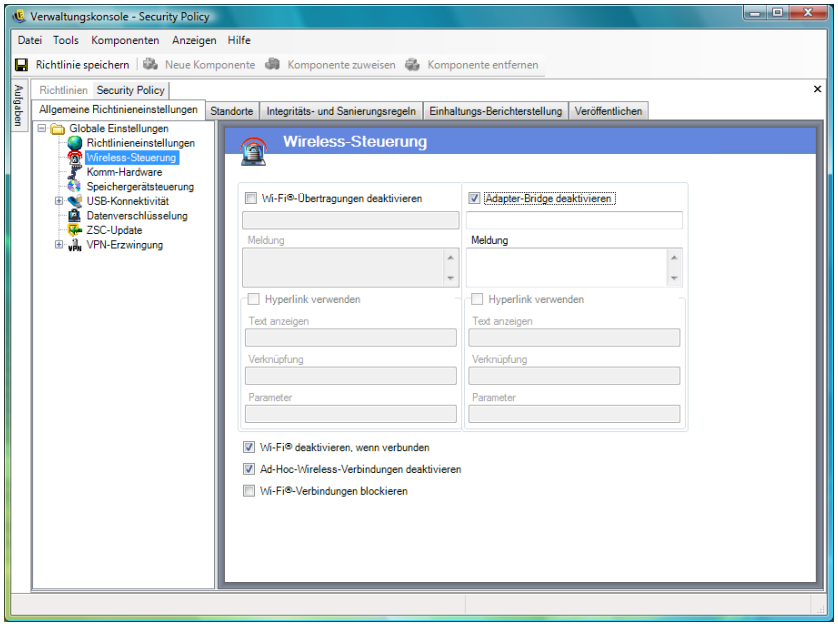
- **Vorhandene verwenden:** Das ist die Standardeinstellung. Hiermit bleibt das aktuelle Passwort unverändert.
- **Aktiviert:** Aktiviert bzw. ändert ein Deinstallationspasswort. Geben Sie das neue Passwort an und bestätigen Sie es anschließend.
- **Deaktiviert:** Sorgt dafür, dass kein Deinstallationspasswort erforderlich ist.

- **Meldung bei Richtlinienaktualisierung verwenden:** Sie können festlegen, dass bei jeder Aktualisierung der Richtlinie eine benutzerdefinierte Meldung angezeigt wird. Klicken Sie in das Kontrollkästchen und geben Sie dann in den dafür vorgesehenen Feldern die Informationen zur Meldung an.
- **Hyperlink verwenden:** Sie können einen Hyperlink hinzufügen, über den weitere Informationen, die Unternehmensrichtlinie o. ä. aufgerufen werden (weitere Informationen finden Sie unter „Hyperlinks“ auf Seite 72).



Wireless-Steuerung

Mit "Wireless-Steuerung" werden Parameter für die Adapterkonnektivität global festgelegt, um sowohl den Endpunkt als auch das Netzwerk zu schützen. Für den Zugriff auf dieses Steuerelement wechseln Sie zur Registerkarte *Allgemeine Richtlinieneinstellungen* und klicken Sie im Richtlinienbaum auf der linken Seite auf das Symbol *Wireless-Steuerung*.



Zu den Einstellungen für die Wireless-Steuerung zählen u. a.:

- **Wi-Fi-Übertragungen deaktivieren:** Deaktiviert global alle Wi-Fi-Adapter; dies schließt die vollständige Stummschaltung eines integrierten Wi-Fi-Radios ein.

  Sie können festlegen, dass eine benutzerdefinierte Meldung und ein Hyperlink angezeigt werden, wenn der Benutzer versucht, eine Wi-Fi-Verbindung zu aktivieren. Weitere Informationen finden Sie unter „Benutzerdefinierte Meldung“ auf Seite 71.
- **Adapter-Bridge deaktivieren:** Deaktiviert global die Netzwerk-Bridge-Funktionalität von Windows* XP, mit deren Hilfe der Benutzer mehrere Adapter zu einer Bridge zusammenschließen kann (Funktion als Hub im Netzwerk).

  Sie können festlegen, dass eine benutzerdefinierte Meldung und ein Hyperlink angezeigt werden, wenn der Benutzer versucht, eine Wi-Fi-Verbindung herzustellen. Weitere Informationen finden Sie unter „Benutzerdefinierte Meldung“ auf Seite 71.
- **Wi-Fi deaktivieren, wenn verbunden:** Deaktiviert global alle Wi-Fi-Adapter, wenn der Benutzer mit einer verkabelten Verbindung (LAN über NIC) arbeitet.
- **Adhoc-Netzwerke deaktivieren:** Deaktiviert global sämtliche Adhoc-Konnektivitätsfunktionen; so werden die Wi-Fi-Konnektivität über ein Netzwerk (z. B. über einen Zugriffspunkt) erzwungen sowie sämtliche Peer-to-Peer-Netzwerkfunktionen dieser Art beschränkt.
- **Wi-Fi-Verbindungen blockieren:** Blockiert Wi-Fi-Verbindungen global, ohne das Wi-Fi-Radio stummzuschalten. Verwenden Sie diese Einstellung, wenn Sie Wi-Fi-Verbindungen deaktivieren, jedoch Zugriffspunkte für die Standorterkennung verwenden möchten. Weitere Informationen finden Sie unter Abschnitt 2.2.2, „Standorte“, auf Seite 73.

Kommunikationshardware

Mithilfe der Einstellungen für die Kommunikationshardware wird nach Standort gesteuert, welche Hardwaretypen in dieser Netzwerkumgebung eine Verbindung herstellen dürfen.

Hinweis: Sie können die Steuerelemente für Kommunikationshardware auf der Registerkarte *Allgemeine Richtlinieneinstellungen* global bzw. auf der Registerkarte *Standorte* für einzelne Standorte festlegen.

Wenn Sie die Steuerelemente für Kommunikationshardware global festlegen möchten, klicken Sie auf die Registerkarte *Allgemeine Richtlinieneinstellungen*, erweitern Sie den Eintrag *Globale Einstellungen* im Baum und klicken Sie dann auf *Komm-Hardware*.

Wenn Sie die Steuerelemente für Kommunikationshardware für einen Standort festlegen möchten, klicken Sie auf die Registerkarte *Standorte*, erweitern Sie den gewünschten Standort im Baum und klicken Sie dann auf *Komm-Hardware*. Weitere Informationen zum Festlegen der Einstellungen für Kommunikationshardware für einen Standort finden Sie unter „Kommunikationshardware“ auf Seite 76.

Legen Sie fest, ob die allgemeine Einstellung für die einzelnen aufgelisteten Kommunikationshardware-Geräte zugelassen oder deaktiviert werden soll:

- **1394 (FireWire):** Steuert den Zugriff auf den FireWire*-Anschluss des Endpunkts.
- **IrDA:** Steuert den Zugriff auf den Infrarotanschluss des Endpunkts.

- **Bluetooth:** Steuert den Zugriff auf den Bluetooth*-Anschluss des Endpunkts.
- **Seriell/Parallel:** Steuert den Zugriff auf den seriellen/parallelen Anschluss des Endpunkts.

Steuerelement für Speichergerätsteuerung

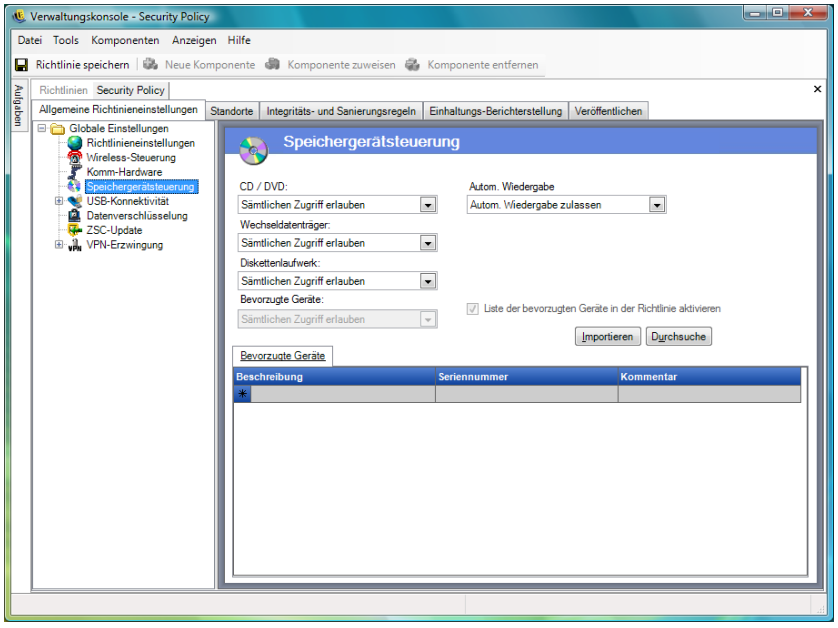
Mithilfe von Steuerelementen für Speichergeräte werden die Speichergerät-Standardeinstellungen für die Richtlinie festgelegt. Hierbei wird u. a. festgelegt, ob externe Dateispeichergeräte über Lese- oder Schreibrechte für Dateien verfügen, im schreibgeschützten Modus betrieben oder vollständig deaktiviert werden. Bei Deaktivierung sind diese Geräte nicht in der Lage, Daten vom Endpunkt abzurufen. Der Zugriff auf die Festplatte und alle Netzlaufwerke sowie deren Verwendung sind weiterhin möglich.

Die Speichergerätsteuerung von ZENworks Endpoint Security darf nicht verwendet werden, wenn Storage Encryption Solution aktiviert ist.

Hinweis: Sie können die Steuerelemente für Speichergeräte auf der Registerkarte *Allgemeine Richtlinieneinstellungen* global bzw. auf der Registerkarte *Standorte* für einzelne Standorte festlegen.

Wenn Sie die Steuerelemente für Speichergeräte global festlegen möchten, klicken Sie auf die Registerkarte *Allgemeine Richtlinieneinstellungen*, erweitern Sie den Eintrag *Globale Einstellungen* im Baum und klicken Sie dann auf *Speichergerätsteuerung*.

Wenn Sie die Steuerelemente für Speichergeräte für einen Standort festlegen möchten, klicken Sie auf die Registerkarte *Standorte*, erweitern Sie den gewünschten Standort im Baum und klicken Sie dann auf *Speichergerätsteuerung*. Weitere Informationen finden Sie unter „Kommunikationshardware“ auf Seite 76.



Die Speichergerätsteuerung ist in folgende Kategorien unterteilt:

- **CD/DVD:** Steuert sämtliche Geräte, die im Windows-Geräte-Manager unter *DVD/CD-ROM-Laufwerke* aufgeführt sind.

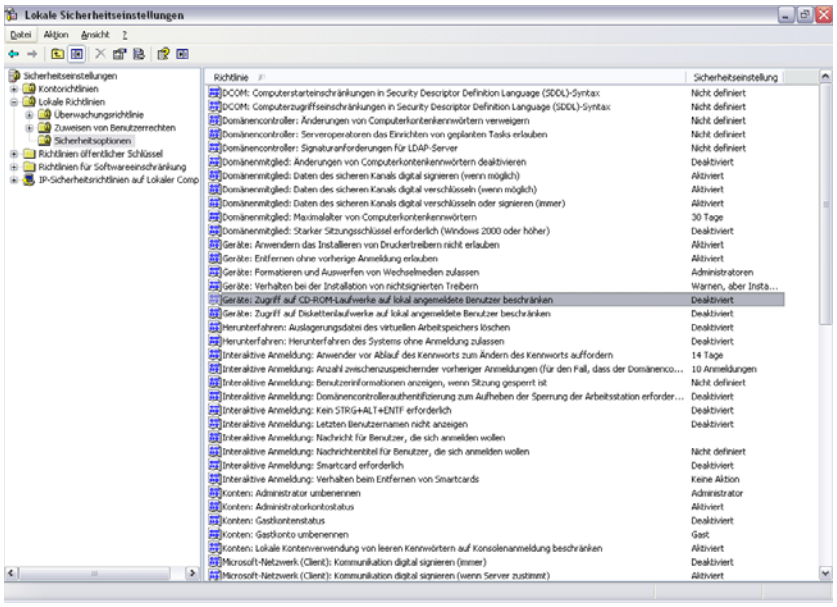
- **Wechseldatenträger:** Steuert sämtliche Geräte, die im Windows-Geräte-Manager unter *Laufwerke* aufgeführt sind.
- **Diskettenlaufwerk:** Steuert sämtliche Geräte, die im Windows-Geräte-Manager unter *Diskettenlaufwerke* aufgeführt sind.
- **Bevorzugte Geräte:** Lässt nur die Wechselspeichergeräte zu, die im Fenster "Speichergerätsteuerung" aufgeführt sind. Alle anderen Geräte, die als Wechseldatenträger gemeldet werden, sind nicht zulässig.

Feste Speicher (Festplatten) und Netzlaufwerke (falls verfügbar) sind immer zulässig.

Wenn Sie den Richtlinienstandard für Speichergeräte festlegen möchten, wählen Sie in den Dropdown-Listen die globale Einstellung für beide Typen aus:

- **Aktivieren:** Der Gerätetyp ist standardmäßig zulässig.
- **Deaktivieren:** Der Gerätetyp ist nicht zulässig. Wenn Benutzer versuchen, auf einem definierten Speichergerät auf Dateien zuzugreifen, wird eine Fehlermeldung des Betriebssystems bzw. der Anwendung, die auf das lokale Speichergerät zuzugreifen versucht, ausgegeben, die besagt, dass bei dem Vorgang ein Fehler aufgetreten ist.
- **Nur Lesen:** Für den Gerätetyp ist "Nur Lesen" festgelegt. Wenn Benutzer versuchen, auf das Gerät zu schreiben, wird eine Fehlermeldung des Betriebssystems bzw. der Anwendung, die auf das lokale Speichergerät zuzugreifen versucht, ausgegeben, die besagt, dass bei dem Vorgang ein Fehler aufgetreten ist.

Hinweis: Wenn Sie CD-ROM-Laufwerke bzw. Diskettenlaufwerke für eine Gruppe von Endpunkten auf "Nur Lesen" einstellen möchten, muss in den lokalen Sicherheitseinstellungen (die durch ein Verzeichnisdienst-Gruppenrichtlinienobjekt übergeben wurden) sowohl für *Geräte: Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken* als auch für *Geräte: Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken* die Option "Deaktiviert" festgelegt sein. Um dies sicherzustellen, öffnen Sie entweder das Gruppenrichtlinienobjekt oder sehen in der Systemsteuerung unter "Verwaltung" nach. Wählen Sie die Optionsfolge "Lokale Sicherheitseinstellungen" - "Sicherheitsoptionen" und vergewissern Sie sich, dass beide Geräte deaktiviert sind. "Deaktiviert" ist der Standardwert.



Die folgenden Abschnitte enthalten weitere Informationen:

- „Bevorzugte Geräte“ auf Seite 57
- „Importieren von Gerätelisten“ auf Seite 58

Bevorzugte Geräte

Bevorzugte Wechselspeichergeräte können optional in eine Liste aufgenommen werden, um nur autorisierten Geräten den Zugriff zu erlauben, wenn die globale Einstellung an einem Standort verwendet wird. In diese Liste aufgenommene Geräte müssen eine Seriennummer aufweisen.

So nehmen Sie ein bevorzugtes Gerät in die Liste auf:

1. Verbinden Sie das Gerät mit dem USB-Anschluss des Computers, auf dem die Verwaltungskonsole installiert ist.
2. Wenn das Gerät bereit ist, klicken Sie auf die Schaltfläche für die Absuche. Verfügt das Gerät über eine Seriennummer, werden die zugehörige Beschreibung und Seriennummer in der Liste aufgeführt.
3. Wählen Sie in der Dropdown-Liste eine Einstellung aus (die Einstellung für das globale Wechselspeichergerät findet bei dieser Richtlinie keine Anwendung):
   - **Aktiviert:** Den Geräten in der Bevorzugt-Liste werden uneingeschränkte Lese-/Schreibrechte erteilt, alle anderen USB-Geräte und alle anderen externen Speichergeräte werden deaktiviert.
   - **Nur Lesen:** Den Geräten in der Bevorzugt-Liste wird das Recht "Nur Lesen" erteilt, alle anderen USB-Geräte und externen Speichergeräte werden deaktiviert.

Wiederholen Sie diese Schritte für sämtliche Geräte, die gemäß dieser Richtlinie zulässig sind. Auf sämtliche Geräte wird dieselbe Einstellung angewendet.

Hinweis: Standortbasierte Einstellungen hinsichtlich der Speichergerätsteuerung setzen die globalen Einstellungen außer Kraft. Sie können beispielsweise konfigurieren, dass am Standort "Arbeit" alle externen Speichergeräte zulässig sind, während an allen anderen Standorten der globale Standardwert Gültigkeit hat (die Benutzer werden auf die Geräte in der Bevorzugt-Liste beschränkt).

Importieren von Gerätelisten

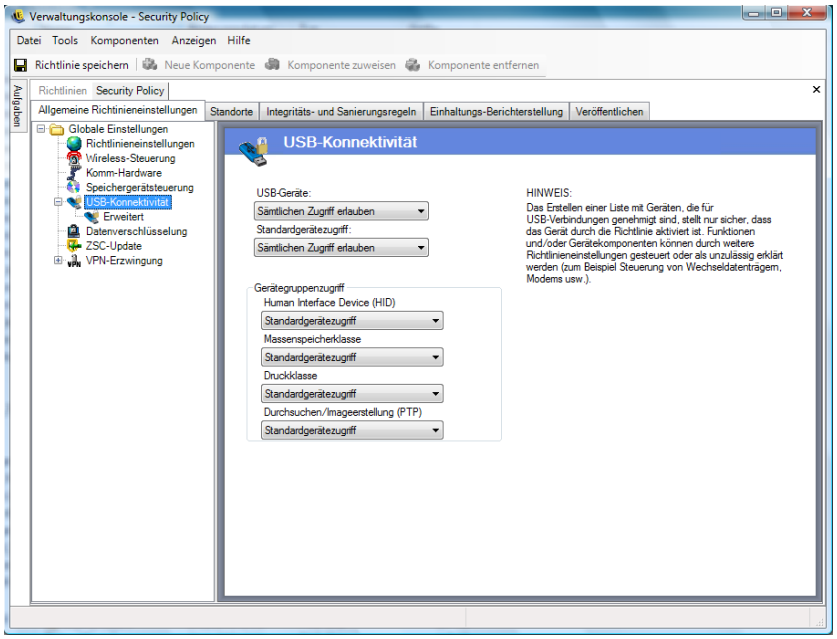
Der Novell-USB-Laufwerkscanner generiert eine Liste mit Geräten und deren Seriennummer (Abschnitt 1.11, „USB-Laufwerkscanner“, auf Seite 44). Wenn Sie diese Liste importieren möchten, klicken Sie auf *Importieren* und begeben Sie sich zu der Liste. Daraufhin werden die Felder *Beschreibung* und *Seriennummer* ausgefüllt.

USB-Konnektivität

Sämtliche Geräte, die über den USB-BUS eine Verbindung aufbauen, können nach der Richtlinie zugelassen oder verweigert werden. Diese Geräte können aus dem USB-Gerätinventarbericht per Absuche in die Richtlinie übernommen werden; eine weitere Möglichkeit ist die Absuche aller Geräte, die derzeit mit einem Computer verbunden sind. Diese Geräte können, basierend auf Hersteller, Produktname, Seriennummer, Typ usw., gefiltert werden. Zu Supportzwecken kann der Administrator die Richtlinie so konfigurieren, dass ein Satz Geräte akzeptiert wird, entweder nach Herstellertyp (Beispiel: alle HP-Geräte sind zulässig) oder nach Produkttyp (alle USB-Eingabegeräte (Maus und Tastatur) sind zulässig). Zudem können einzelne Geräte erlaubt werden, um zu verhindern, dass nicht unterstützte Geräte Bestandteil des Netzwerks werden (Beispiel: mit Ausnahme dieses Druckers sind keine Drucker zulässig).

Für den Zugriff auf dieses Steuerelement wechseln Sie zur Registerkarte *Allgemeine Richtlinieneinstellungen* und klicken Sie dann im Richtlinienbaum auf der linken Seite auf *USB-Konnektivität*.

Abbildung 2-1 *Seite "USB-Konnektivität".*



Zugriff wird zunächst danach evaluiert, ob der Bus aktiv ist. Dies hängt von der Einstellung unter *USB-Geräte* ab. Wenn hier *Zugriff generell deaktivieren* festgelegt ist, wird das Gerät deaktiviert und die Evaluierung wird gestoppt. Wenn hier *Zugriff generell zulassen* festgelegt ist, setzt der Client die Evaluierung und den Gerätesatz fort und sucht nach Übereinstimmungen im Filter. Wie bei den anderen Feldern in der ZENworks-Verwaltungszone, wenn diese auf einen Standort festgelegt ist, kann der Wert für *USB-Geräte* auch auf *Globale Einstellungen anwenden* festgelegt werden, wodurch in diesem Feld dann der globale Wert verwendet wird.

Der Client sammelt die Filter, die von der Richtlinie angewendet werden, basierend auf Standort und globale Einstellungen. Der Client gruppiert dann die Filter, basierend auf dem Zugriff in den folgenden Gruppen:

- **Immer blockieren:** Das Gerät immer blockieren. Diese Einstellung kann nicht überschrieben werden.
- **Immer zulassen:** Zugriff immer erlauben, es sei denn, für das Gerät trifft der Filter *Immer blockieren* zu.
- **Blockieren:** Zugriff immer blockieren, es sei denn, das Gerät stimmt mit Filter *Immer zulassen* überein.
- **Zulassen:** Zugriff erlauben, es sei denn, das Gerät stimmt mit Filter *Immer blockieren* oder *Blockieren* überein.
- **Standardgerätezugriff:** Für das Gerät die gleiche Zugriffsstufe anwenden wie unter *Standardgerätezugriff*, wenn keine andere Übereinstimmung gefunden wird.

Ein Gerät wird für jede Gruppe in der oben genannten Reihenfolge evaluiert (zuerst die Gruppe *Immer blockieren*, dann *Immer zulassen* etc.). Wenn ein Gerät mit mindestens einem Filter in einer Gruppe übereinstimmt, wird der Zugriff für dieses Gerät auf diese Stufe festgelegt und die Evaluierung wird gestoppt. Wenn das Gerät hinsichtlich aller Filter evaluiert und keine Übereinstimmung gefunden wird, wird die Stufe *Standardgerätezugriff* angewendet.

Der im Bereich *Gerätegruppenzugriff* festgelegte Gerätezugriff wird berücksichtigt, einschließlich aller anderen auf diesem Standort verwendeten Filter. Dies erfolgt durch Generieren übereinstimmender Filter für jede Gruppierung, wenn die Richtlinie für den Client veröffentlicht wird. Diese Filter sind:

Gerätegruppenzugriff:	**Filter:**
Ein- und Ausgabegeräte (Human Interface Device – HID)	"Geräteklasse" entspricht 3.
Massenspeicherklasse	"Geräteklasse" entspricht 8.
Druckklasse	"Geräteklasse" entspricht 7.
Scanning/Imaging (PTP)	"Geräteklasse" entspricht 6.

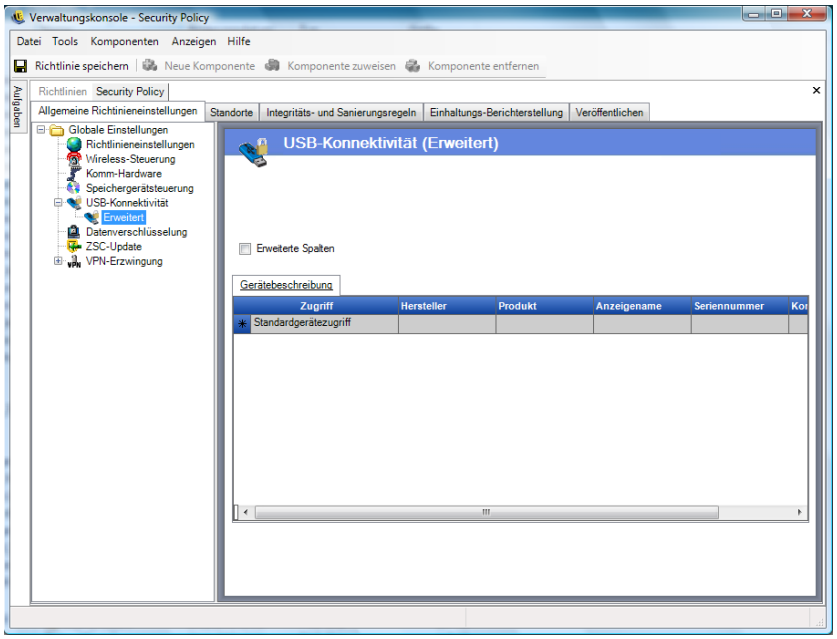
Speziell

In den meisten Situationen reichen die vier auf der Seite "USB-Konnektivität" aufgelisteten Gerätegrupen (HID, Massenspeicherklasse, Druckklasse und Scanning/Imaging), um den meisten USB-Geräten den Zugriff zu erlauben oder zu verweigern. Bei Geräten, die nicht in einer dieser Gruppen registriert sind, können Sie die Einstellungen auf der Seite "USB-Konnektivität –

Erweitert" konfigurieren. Sie können auch die Einstellungen auf der Seite "Erweitert" verwenden, um Whitelist-Zugriff auf bestimmte Geräte zu erlauben, auch wenn ihnen bereits aufgrund der Einstellungen auf der Seite "USB-Konnektivität" der Zugriff verweigert wurde.

Zum Zugriff auf die erweiterten Optionen für USB-Konnektivität klicken Sie auf das Pluszeichen neben *USB-Konnektivität* im Baum *Globale Einstellungen* und anschließend auf *Erweitert*. Sie können den USB-Geräteauditbericht dazu verwenden, alle Informationen abzurufen, die Sie potenziell auf der Seite "USB-Konnektivitätssteuerung – Erweitert" verwenden können.

Abbildung 2-2 *Seite "USB-Konnektivitätssteuerung – Erweitert"*



Die Standardspalten enthalten folgende Einträge:

- **Zugriff:** Ziehen Sie die Maus über *Standardgerätezugriff* und geben Sie eine Zugriffsstufe an:
  - **Immer blockieren:** Das Gerät immer blockieren. Diese Einstellung kann nicht überschrieben werden.
  - **Immer zulassen:** Zugriff immer erlauben, es sei denn, für das Gerät trifft der Filter *Immer blockieren* zu.
  - **Blockieren:** Zugriff immer blockieren, es sei denn, das Gerät stimmt mit Filter *Immer zulassen* überein.
  - **Zulassen:** Zugriff erlauben, es sei denn, das Gerät stimmt mit Filter *Immer blockieren* oder *Blockieren* überein.
  - **Standardgerätezugriff:** Für das Gerät die gleiche Zugriffsstufe anwenden wie unter *Standardgerätezugriff*, wenn keine andere Übereinstimmung gefunden wird.
- **Hersteller:** Klicken Sie auf die Spalte *Hersteller* und geben Sie den Namen des Herstellers ein, den Sie zum Filter hinzufügen möchten (zum Beispiel Canon).
- **Produkt:** Klicken Sie auf die Spalte *Produkt* und geben Sie den Namen des Produkts ein, das Sie zum Filter hinzufügen möchten.
- **Anzeigename:** Klicken Sie auf die Spalte *Anzeigename* und geben Sie den Anzeigenamen für das Gerät ein, das Sie zum Filter hinzufügen möchten.

- **Seriennummer:** Klicken Sie auf die Spalte *Seriennummer* und geben Sie die Seriennummer des Geräts ein, das Sie zum Filter hinzufügen möchten.
- **Kommentar:** Klicken Sie auf die Spalte *Kommentar* und geben Sie den Kommentar ein, den Sie zum Filter hinzufügen möchten (zum Beispiel Canon).

Sie können auf das Feld *Erweiterte Spalten* klicken, um die folgenden Spalten hinzuzufügen: *USB-Version*, *Geräteklasse, Geräteunterklasse, Geräteprotokoll, Händler-ID, Produkt-ID, BCD-Gerät, BS-Geräte-ID* sowie *BS-Geräteklasse*.

Ein Gerät stellt dem BS einen Satz Attribute zur Verfügung. Der Client gleicht diese Attribute mit den Feldern ab, die von einem Filter benötigt werden. Alle Felder im Filter müssen einem vom Gerät zur Verfügung gestellten Attribut entsprechen, um eine Übereinstimmung zu finden. Wenn das Gerät kein Attribut oder Feld zur Verfügung stellt, das für den Filter erforderlich ist, kann dieser Filter keine Übereinstimmung finden.

Angenommen, ein Gerät stellt beispielsweise die folgenden Attribute zur Verfügung: Hersteller: Acme, Klasse: 8, Seriennummer: "1234".

Der Filter: Klasse = 8 würde eine Übereinstimmung für dieses Gerät finden. Der Filter: Produkt = "Acme" würden keine Übereinstimmung finden, da das Gerät dem BS kein Produkt-Attribut zur Verfügung gestellt hat.

Die folgenden Felder bieten Übereinstimmungen in Teilzeichenketten: Hersteller, Produkt und Anzeigename. Alle anderen Felder sind exakte Übereinstimmungen.

Es ist interessant, dass das Feld der USB-Seriennummern (SN) nach Spez. nur eindeutig ist, wenn es bei der Angabe der folgenden Felder zusammen mit der SN berücksichtigt wird: USB-Version, Händler-ID, Produktions-ID und BCD-Gerät.

Zurzeit gültige Werte für USB-Version in Dezimalschreibweise sind: 512 – USB 2.0, 272 – USB 1.1, 256 – USB 1.0.

Die folgenden Abschnitte enthalten weitere Informationen:

- „Manuelles Hinzufügen von Geräten“ auf Seite 61
- „Aufnehmen eines Geräts in die "weiße" bzw. "schwarze" Liste (nach Produkttyp)“ auf Seite 62

Manuelles Hinzufügen von Geräten

Mithilfe der folgenden Methoden können Sie die Liste ausfüllen und dann angeben, ob Sie die USB-Konnektivität für Geräte zulassen oder verweigern.

So fügen Sie ein Gerät manuell hinzu:

1. Verbinden Sie das Gerät mit dem USB-Anschluss des Computers, auf dem die Verwaltungskonsole installiert ist.

2 Wenn das Gerät bereit ist, klicken Sie auf die Schaltfläche *Scan*. Verfügt das Gerät über eine Seriennummer, werden die zugehörige Beschreibung und Seriennummer in der Liste aufgeführt.

3 Wählen Sie in der Dropdown-Liste eine Einstellung aus (die Einstellung für das globale Wechselspeichergerät findet bei dieser Richtlinie keine Anwendung):

- **Aktivieren:** Den Geräten in der Bevorzugt-Liste werden uneingeschränkte Lese-/Schreibrechte erteilt, alle anderen USB-Geräte und alle anderen externen Speichergeräte werden deaktiviert
- **Nur Lesen:** Den Geräten in der Bevorzugt-Liste wird das Recht "Nur Lesen" erteilt, alle anderen USB-Geräte und anderen externen Speichergeräte werden deaktiviert

Wiederholen Sie diese Schritte für jedes Gerät, das in dieser Richtlinie zulässig sein soll. Auf sämtliche Geräte wird dieselbe Einstellung angewendet.

Aufnehmen eines Geräts in die "weiße" bzw. "schwarze" Liste (nach Produkttyp)

Im folgenden Abschnitt wird beschrieben, wie ein USB-Gerät entsprechend seines Produkttyps in die "weiße" bzw. "schwarze" Liste aufgenommen wird.

Hinweis: Nachfolgendes Verfahren dient lediglich als Beispiel, das Ihnen zeigen soll, wie Sie den Produkttyp Ihres USB-Wechselspeichergeräts ermitteln. Je nachdem, welche Informationen der Hersteller Ihres Geräts bereitstellt, funktioniert dieses Verfahren eventuell nicht. Sie können den USB-Geräteauditbericht dazu verwenden, alle Informationen abzurufen, die Sie potenziell auf der Seite "USB-Konnektivitätssteuerung – Erweitert" verwenden können.

So ermitteln Sie den Produkttyp eines USB-Wechselspeichergeräts:

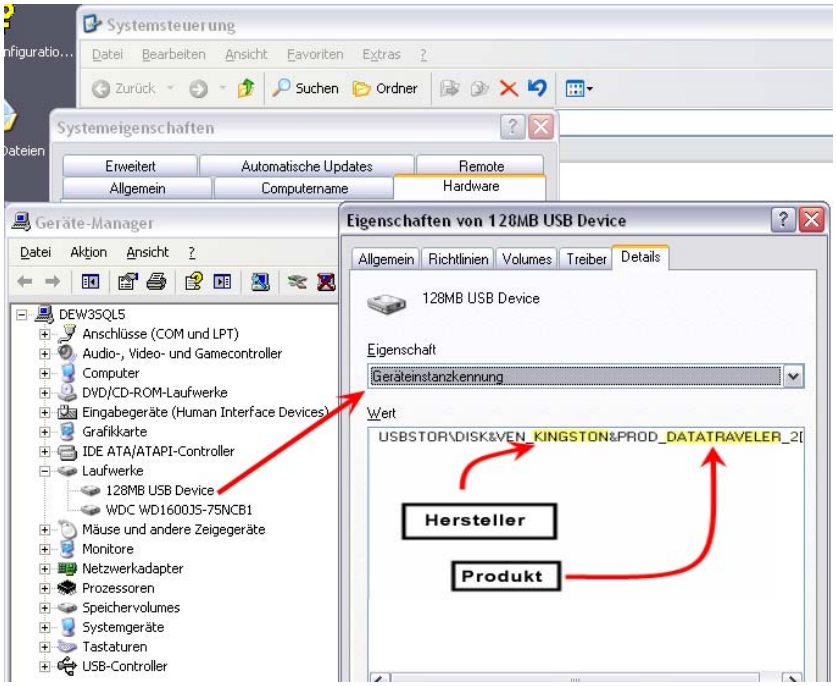
1 Öffnen Sie den *Geräte-Manager* von Microsoft Windows.

2 Klicken Sie auf das Pluszeichen neben *Laufwerke*, um den Baum zu erweitern.

3 Klicken Sie mit der rechten Maustaste auf das USB-Gerät und klicken Sie dann auf *Eigenschaften*, um das Dialogfeld "Eigenschaften" des Geräts anzuzeigen.

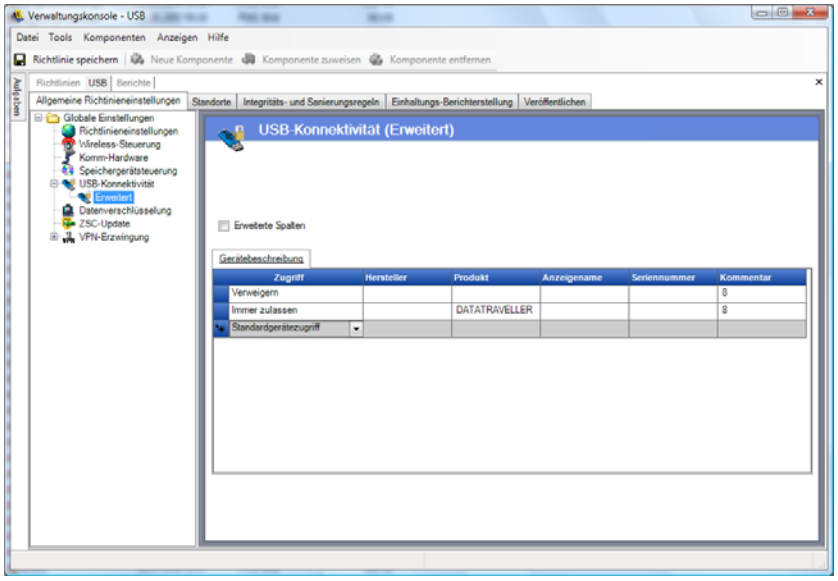
4 Klicken Sie auf die Registerkarte *Details* und wählen Sie in der Dropdown-Liste *Geräteinstanzkennung* aus.

Der Produkttyp wird in der Geräteinstanzkennung nach der Zeichenfolge &PROD angezeigt. Im folgenden Beispiel ist DATATRAVELER der Produkttyp.



So nehmen Sie ein USB-Gerät in die "weiße" Liste auf: Behalten Sie auf der Seite "USB-Konnektivität" die Standardeinstellungen bei. Erstellen Sie auf der Seite "Erweitert" zwei Zeilen: Geben Sie in der ersten Zeile in der Spalte *Zugriff* die Einstellung *Verweigern* an und in der Spalte *Geräteklasse* die Zahl 8 (wenn *Geräteklasse* nicht angezeigt wird, aktivieren Sie das Kontrollkästchen *Erweiterte Spalten*). Geben Sie in der zweiten Zeile in der Spalte *Zugriff* die Einstellung *Immer zulassen* an, in der Spalte *Produkt* den Produkttyp (im Beispiel DATATRAVELER) und in der Spalte *Geräteklasse* die Zahl 8.

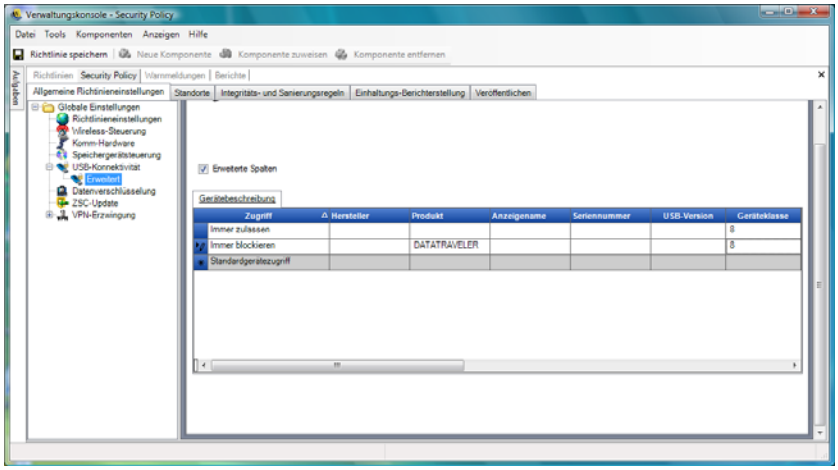
Die Seite "USB-Konnektivität (Erweitert)" sollte wie folgendes Beispiel aussehen:



Das USB-Gerät mit dem Produkttyp DATATRAVELER ist nun in die "weiße" Liste aufgenommen. Ihm wird von ZENworks Endpoint Security Management Zugriff gewährt, während allen anderen USB-Geräten der Zugriff verweigert wird.

So nehmen Sie ein USB-Gerät in die "schwarze" Liste auf: Behalten Sie auf der Seite "USB-Konnektivität" die Standardeinstellungen bei. Erstellen Sie auf der Seite "Erweitert" zwei Zeilen: Geben Sie in der ersten Zeile in der Spalte *Zugriff* die Einstellung *Immer zulassen* an und in der Spalte *Geräteklasse* die Zahl 8 (wenn *Geräteklasse* nicht angezeigt wird, aktivieren Sie das Kontrollkästchen *Erweiterte Spalten*). Geben Sie in der zweiten Zeile in der Spalte *Zugriff* die Einstellung *Immer blockieren* an, in der Spalte *Produkt* den Produkttyp (im Beispiel DATATRAVELER) und in der Spalte *Geräteklasse* die Zahl 8.

Die Seite "USB-Konnektivität (Erweitert)" sollte wie folgendes Beispiel aussehen:



Das USB-Gerät mit dem Produkttyp DATATRAVELER ist nun in die "schwarze" Liste aufgenommen. Ihm wird der Zugriff von ZENworks Endpoint Security Management verweigert, während allen anderen USB-Geräten Zugriff gewährt wird.

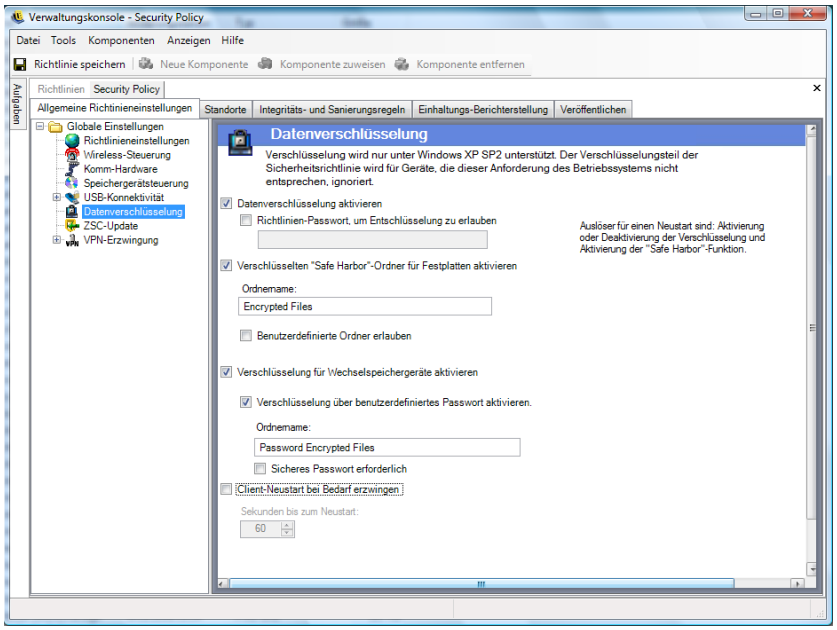
Datenverschlüsselung

Mit "Datenverschlüsselung" wird bestimmt, ob die Dateiverschlüsselung am Endpunkt erzwungen wird und welche Art der Verschlüsselung zur Verfügung steht. Daten können verschlüsselt werden, um die Dateifreigabe (mit Passwortschutz) zu ermöglichen; außerdem kann auf Computern, auf denen ZENworks Storage Encryption Solution ausgeführt wird, festgelegt werden, dass Daten schreibgeschützt sind.

Hinweis: Verschlüsselung wird nur unter Windows XP SP2 unterstützt. Auf Geräten mit anderen Betriebssystemen wird der Verschlüsselungsteil der Sicherheitsrichtlinie ignoriert.

Die Speichergerätsteuerung von ZENworks Endpoint Security darf nicht verwendet werden, wenn ZENworks Storage Encryption Solution aktiviert ist.

Für den Zugriff auf dieses Steuerelement wechseln Sie zur Registerkarte *Allgemeine Richtlinieneinstellungen* und klicken Sie dann im Richtlinienbaum auf der linken Seite auf *Datenverschlüsselung*.



Zur Aktivierung der einzelnen Steuerelemente aktivieren Sie das Kontrollkästchen *Datenverschlüsselung aktivieren*.

Hinweis: Verschlüsselungsschlüssel werden an alle Computer verteilt, die Richtlinien vom Richtlinienverteilungsservice erhalten, unabhängig davon, ob die Datenverschlüsselung aktiviert ist oder nicht. Mit diesem Steuerelement wird der ZENworks Security Client jedoch angewiesen, die eigenen Verschlüsselungstreiber zu aktivieren, wodurch ein Benutzer die an ihn gesendeten Dateien lesen kann, ohne dass hierfür das File Decryption Utility erforderlich ist. Weitere Einzelheiten finden Sie unter Abschnitt 1.9, „Verwenden des ZENworks File Decryption Utility“, auf Seite 42.

Legen Sie fest, welche Verschlüsselungsgrade diese Richtlinie erlaubt:

- **Richtlinienpasswort für Entschlüsselung:** Geben Sie ein Passwort an, damit alle Benutzer, die diese Richtlinie verwenden, dieses Passwort eingeben müssen, bevor sie verschlüsselte Dateien entschlüsseln können, die in ihren `Safe Harbor`-Ordnern gespeichert sind.

  Hierbei handelt es sich um eine optionale Einstellung. Wenn hier keine Angabe erfolgt, ist das Passwort nicht erforderlich.

- **Festplattenverschlüsselung innerhalb von "Safe Harbor"-Ordner aktivieren (Nichtsystemlaufwerke):** Generiert im Stammverzeichnis sämtlicher Nichtsystemlaufwerke am Endgerät einen Ordner, dessen Name Aufschluss darüber gibt, dass er `durch Verschlüsselung geschützte Dateien` enthält. Alle Dateien, die in diesem Ordner gespeichert werden, werden verschlüsselt und durch den ZENworks Security Client verwaltet. Daten, die in diesem Ordner gespeichert werden, werden automatisch verschlüsselt und nur autorisierte Benutzer dieses Computers können darauf zugreifen.

Wenn Sie den Ordnernamen ändern möchten, klicken Sie in das Feld *Ordnername*, markieren Sie den dort enthaltenen Text und geben Sie den von Ihnen gewünschten Namen ein.

- **Benutzerordner "Eigene Dateien" verschlüsseln:** Aktivieren Sie dieses Kontrollkästchen, um den Ordner `Eigene Dateien` der Benutzer als verschlüsselten Ordner zu definieren (zusätzlich zum `Safe Harbor`-Ordner). Dies bezieht sich nur auf den lokalen Ordner mit der Bezeichnung `Eigene Dateien`.
- **Benutzerdefinierte Ordner zulassen (Nichtsystemlaufwerk):** Aktivieren Sie dieses Kontrollkästchen, damit Benutzer auswählen können, welche Ordner auf ihrem Computer verschlüsselt sein sollen. Dies bezieht sich nur auf lokale Ordner. Wechselspeichergeräte oder Netzlaufwerke können nicht verschlüsselt werden.

Warnung: Vergewissern Sie sich vor der Deaktivierung der Datenverschlüsselung, dass sämtliche in diesen Ordnern gespeicherten Daten vom Benutzer extrahiert und an einem anderen Ort gespeichert wurden.

- **Verschlüsselung für Wechselspeichergeräte aktivieren:** Sämtliche Daten, die an einem durch diese Richtlinie geschützten Endpunkt auf Wechselspeichergeräte geschrieben werden, werden verschlüsselt. Benutzer, für deren Computer diese Richtlinie gilt, können die Daten lesen, folglich ist die Dateifreigabe über ein Wechselspeichergerät innerhalb einer Richtliniengruppe möglich. Benutzer, die dieser Richtliniengruppe nicht angehören, können die auf dem Laufwerk verschlüsselten Dateien nicht lesen. Sie können lediglich unter Angabe des entsprechenden Passworts auf Dateien im Ordner `Freigegebene Dateien` (falls aktiviert) zugreifen.
  - **Verschlüsselung mit benutzerdefiniertem Passwort aktivieren:** Diese Einstellung ermöglicht es dem Benutzer, Dateien in einem Ordner mit freigegebenen Dateien auf dem Wechselspeichergerät zu speichern (dieser Ordner wird bei Anwendung dieser Einstellung automatisch generiert). Der Benutzer kann beim Hinzufügen von Dateien zu diesem Ordner ein Passwort angeben, dass dann von Benutzern, die nicht Mitglied der aktuellen Richtliniengruppe sind, zum Extrahieren der Dateien verwendet wird.

    Wenn Sie den Ordnernamen ändern möchten, klicken Sie in das Feld *Ordnername*, markieren Sie den dort enthaltenen Text und geben Sie dann den von Ihnen gewünschten Namen ein.
  - **Sicheres Passwort erforderlich:** Durch diese Einstellung wird der Benutzer gezwungen, ein sicheres Passwort für den Ordner "Freigegebene Dateien" festzulegen. Ein starkes Passwort enthält folgende Merkmale:
    - Sieben oder mehr Zeichen
    - Mindestens ein Zeichen von jedem der vier folgenden Zeichenklassen:
      - Großbuchstaben A-Z
      - Kleinbuchstaben a-z
      - Zahlen von 0-9
      - Mindestens ein Sonderzeichen ~!@#$%^&*()+{}[]:;<>?,./

    Beispiel: y9G@wb?

Warnung: Vergewissern Sie sich vor der Deaktivierung der Datenverschlüsselung, dass sämtliche auf Wechseldatenträgern (Wechselspeichergeräten) gespeicherten Daten vom Benutzer extrahiert und an einem anderen Ort gespeichert wurden.

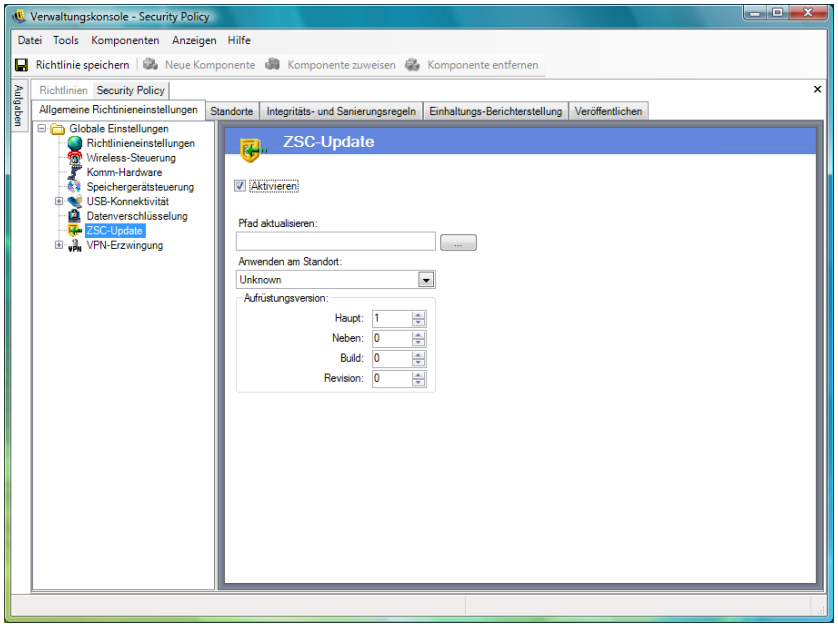
- **Client-Neustart bei Bedarf erzwingen:** Wenn eine Richtlinie um Verschlüsselung ergänzt wird, erfolgt die Aktivierung erst, nachdem der Endpunkt neu gebootet wurde. Mit dieser Einstellung wird das erforderliche Neubooten erzwungen. Es wird ein Countdown angezeigt und der Benutzer wird gewarnt, dass der Computer nach der angegebenen Anzahl an Sekunden neu gebootet wird. So lange hat der Benutzer Zeit, seine Arbeit zu speichern, bevor der·Computer neu gebootet wird.

  Erneutes Booten ist erforderlich, wenn die Verschlüsselung in einer Richtlinie erstmals aktiviert wird und wenn die Safe Harbor-Verschlüsselung oder die Verschlüsselung für Wechseldatenträger aktiviert wird (wenn die Aktivierung getrennt von der Verschlüsselungsaktivierung erfolgt). Beispielsweise ist zweimaliges erneutes Booten erforderlich, wenn eine Verschlüsselungsrichtlinie erstmals angewendet wird: Beim ersten erneuten Booten werden die Treiber initialisiert und beim zweiten werden etwaige Safe Harbor-Bereiche in die Verschlüsselung einbezogen. Wenn nach der Anwendung der Richtlinie weitere Safe Harbor-Bereiche ausgewählt werden, ist nur ein einmaliges erneutes Booten erforderlich, um den betreffenden Safe Harbor-Bereich in die Richtlinie aufzunehmen.

ZSC-Aktualisierung

Patches zur Beseitigung geringfügiger Probleme mit dem ZENworks Security Client werden im Rahmen regelmäßiger ZENworks Endpoint Security Management-Aktualisierungen zur Verfügung gestellt. Anstatt ein neues Installationsprogramm zur Verfügung zu stellen, das über MSI an alle Endpunkte verteilt werden muss, kann der Administrator dank der ZENworks Security Client-Aktualisierungsfunktion eine Zone im Netzwerk bestimmen, von der aus Aktualisierungspatches an Endbenutzer verteilt werden, wenn diese eine Verbindung mit dieser Netzwerkumgebung herstellen.

Für den Zugriff auf dieses Steuerelement wechseln Sie zur Registerkarte *Allgemeine Richtlinieneinstellungen* und klicken Sie dann im Richtlinienbaum auf der linken Seite auf *ZSC-Aktualisierung*.



Führen Sie folgende Schritte durch, um die einfache und sichere Verteilung dieser Patches an sämtliche ZENworks Security Client-Benutzer zu ermöglichen:

1. Wählen Sie die Option *Aktivieren*, um den Bildschirm und die Regel zu aktivieren.
2. Geben Sie den Ort an, an dem der ZENworks Security Client nach den Aktualisierungen suchen soll.

   Basierend auf den Empfehlungen im nachfolgenden Schritt empfiehlt sich hierfür der mit der Unternehmensumgebung verknüpfte Standort (Standort "Arbeit").
3. Geben Sie den URI (Uniform Resource Identifier) an, unter dem der Patch gespeichert wurde.

   Hier muss der Verweis auf die Patchdatei erfolgen, entweder die Datei "setup.exe" für den ZENworks Security Client oder eine MSI-Datei, die anhand der .exe-Datei erstellt wurde. Aus Sicherheitsgründen empfiehlt es sich, diese Dateien auf einem sicheren Server hinter der Firewall des Unternehmens zu speichern.
4. Geben Sie die Versionsinformationen zu dieser Datei in den dafür vorgesehenen Feldern an.

   Die Versionsinformationen können Sie anzeigen, indem Sie den ZENworks Security Client installieren und das Dialogfeld "Info" öffnen (Details finden Sie in der *ZENworks Endpoint Security Management-Installationsanleitung*). In den Feldern muss die Versionsnummer von `STEngine.exe` eingegeben werden.

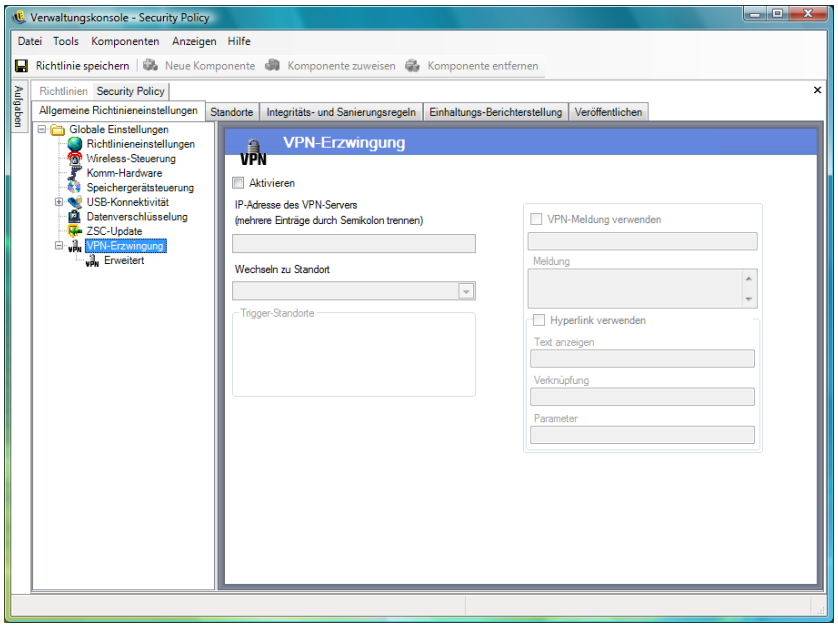
Jedes Mal, wenn sich der Benutzer an den zugewiesenen Standort begibt, sucht·der ZENworks Security Client unter dem URI nach·einer Aktualisierung, die dieser Versionsnummer entspricht. Ist eine Aktualisierung verfügbar, wird sie vom ZENworks Security Client heruntergeladen und installiert.

VPN-Erzwingung

Mit dieser Regel wird die Nutzung eines SSL-(Secure Sockets Layer-)VPN oder eines clientbasierten VPN (Virtual Private Network) erzwungen. Diese Regel wird im Normalfall an Wireless-Hotspots angewendet. Es wird dem Benutzer ermöglicht, eine Verknüpfung mit dem/eine Verbindung zum öffentlichen Netzwerk herzustellen; dann versucht die Regel, die VPN-Verbindung aufzubauen und dafür zu sorgen, dass der Benutzer einen definierten Standort und eine definierte Firewall-Einstellung verwendet. Alle·Parameter werden vom Administrator festgelegt. Alle Parameter setzen vorhandene Richtlinieneinstellungen außer Kraft. Um die Komponente für die VPN-Erzwingung verwenden zu können, muss der Benutzer vor dem Starten mit einem Netzwerk verbunden sein.

Hinweis: Diese Funktion steht nur bei der ZENworks Endpoint Security-Installation zur Verfügung und kann für UWS-(Unlimited Web Solutions-)Sicherheitsrichtlinien nicht verwendet werden.

Für den Zugriff auf dieses Steuerelement wechseln Sie zur Registerkarte *Allgemeine Richtlinieneinstellungen* und klicken Sie dann im Richtlinienbaum auf der linken Seite auf *VPN-Erzwingung*.



Um die Regel für die VPN-Erzwingung verwenden zu können, müssen mindestens zwei Standorte vorhanden sein.

So ergänzen Sie eine neue oder vorhandene Sicherheitsrichtlinie um die VPN-Erzwingung:

1. Wählen Sie *Aktivieren*, um den Bildschirm und die Regel zu aktivieren.
2. Geben Sie die IP-Adressen für den VPN-Server in dem dafür vorgesehenen Feld an. Wenn Sie mehrere Adressen angeben, trennen Sie die einzelnen Einträge durch einen Strichpunkt voneinander ab (Beispiel: 10.64.123.5;66.744.82.36).
3. Wählen Sie in der Dropdown-Liste den Standort aus, zu dem gewechselt werden soll.

   Dies ist der Standort, zu dem der ZENworks Security Client wechselt, wenn das VPN aktiviert wird. Für diesen Standort sollten bestimmte Einschränkungen gelten und es sollte nur eine einzige restriktive·Firewall-Einstellung als Standard verwendet werden.

   Die Firewall-Einstellung *Alle geschlossen*, gemäß der sämtliche TCP-/UDP-Ports geschlossen werden, wird für die strikte VPN-Erzwingung empfohlen. Mit dieser Einstellung werden sämtliche nicht autorisierten Netzwerkvorgänge unterbunden, und die VPN-IP-Adresse dient als ACL (Access Control List, Zugriffssteuerungsliste) für den VPN-Server. Zudem wird hiermit die Netzwerkkonnektivität ermöglicht.
4. Wählen Sie die Auslöserstandorte aus, an denen die Regel für die VPN-Erzwingung angewendet werden soll. Zur strikten VPN-Erzwingung sollte der standardmäßige Standort "Unbekannt" für diese Richtlinie verwendet werden. Nach der Netzwerkauthentifizierung wird die VPN-Regel aktiviert und bewirkt den Wechsel zu dem zugewiesenen Wechselstandort.

   Hinweis: Der Wechsel zum Standort erfolgt vor der VPN-Verbindung, nachdem die Netzwerkauthentifizierung vorgenommen wurde.

   ---
5. Geben Sie eine benutzerdefinierte Meldung ein, die nach der Authentifizierung des VPN beim Netzwerk angezeigt wird. Für VPN ohne Client sollte dies ausreichend sein.

   Nehmen Sie für VPN mit einem Client einen Hyperlink mit auf, der auf den VPN-Client verweist.

Beispiel: `C:\Programme\Cisco Systems\VPN Client\ipsecdialer.exe`

Über diesen Link wird die Anwendung aufgerufen, der Benutzer muss sich aber dennoch anmelden. In das Parameterfeld kann ein Schalter eingegeben werden (es kann auch eine Stapeldatei erstellt werden, auf die anstelle der ausführbaren Client-Datei verwiesen wird).

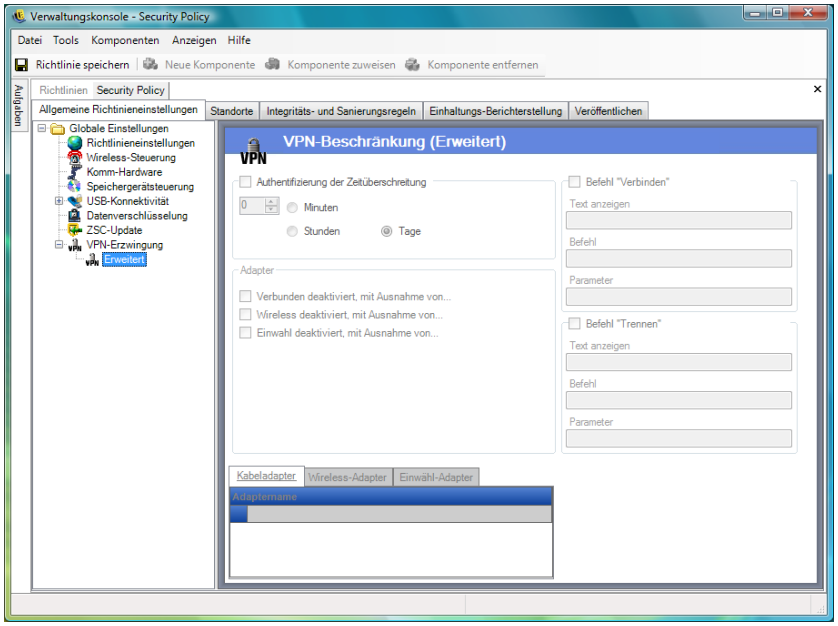
Hinweis: Bei VPN-Clients, die virtuelle Adapter generieren (z. B. Cisco Systems* VPN Client 4.0), wird eine Meldung ausgegeben, die besagt, dass die Richtlinie aktualisiert wurde. Die Richtlinie wurde nicht aktualisiert, der ZENworks Security Client gleicht lediglich den virtuellen Adapter mit sämtlichen Adapterbeschränkungen in der aktuellen Richtlinie ab.

Bei den oben erwähnten Standardeinstellungen für die VPN-Erzwingung ist VPN-Konnektivität eine Option. Benutzer verfügen über Konnektivität zum aktuellen Netzwerk, egal ob sie·das VPN starten oder nicht. Ziehen Sie hinsichtlich der strikteren Erzwingung den nachfolgenden Abschnitt zu erweiterten VPN-Einstellungen zurate.

Erweiterte VPN-Einstellungen

Mit Steuerelementen für erweitertes VPN werden Authentifizierungs-Zeitüberschreitungen zum Schutz vor VPN-Fehlern und Verbindungsbefehle für clientbasierte VPN festgelegt sowie Adaptersteuerelemente zur Steuerung der Adapter mit VPN-Zugriffsrecht verwendet.

Für den Zugriff auf dieses Steuerelement klicken Sie auf die Registerkarte *Allgemeine Richtlinieneinstellungen*, klicken Sie auf das "+"-Symbol neben *VPN-Erzwingung* und klicken Sie dann im Richtlinienbaum auf der linken Seite auf *Erweitert*.



Es können folgende erweiterte Einstellungen für die VPN-Erzwingung konfiguriert werden:

Zeitüberschreitung bei der Authentifizierung: Administratoren können den Endpunkt in eine gesicherte Firewall-Einstellung aufnehmen (die oben erwähnte Einstellung für den Standort, zu dem gewechselt wird), zum Schutz vor Ausfall der VPN-Konnektivität. Bei der Authentifizierungs-Zeitüberschreitung handelt es sich um den Wert, der angibt, wie lange der ZENworks Security

Client auf die Authentifizierung beim VPN-Server wartet. Dieser Parameter sollte auf länger als 1 Minute eingestellt werden, um die Authentifizierung auch bei langsameren Verbindungen zu ermöglichen.

Verbindungs-/Trennbefehle: Bei Einsatz des Authentifizierungszeitgebers werden die Befehle *Verbinden* und *Trennen* zur Steuerung der clientbasierten VPN-Aktivierung verwendet. Geben Sie den Standort des VPN-Client und die erforderlichen Schalter in den Parameterfeldern an. Der Trennbefehl ist optional und wird für VPN-Clients zur Verfügung gestellt, bei denen der Benutzer die Verbindung trennen muss, bevor die Abmeldung beim Netzwerk erfolgt.

Hinweis: Bei VPN-Clients, die virtuelle Adapter generieren (z. B. Cisco Systems* VPN Client 4.0), wird eine Meldung ausgegeben, die besagt, dass die Richtlinie aktualisiert wurde, und möglicherweise erfolgt der vorübergehende Wechsel an einen anderen Standort. Die Richtlinie wurde nicht aktualisiert; der ZENworks Security Client gleicht lediglich den virtuellen Adapter mit sämtlichen Adapterbeschränkungen in der aktuellen Richtlinie ab. Bei der Ausführung von VPN-Clients dieses Typs wird von der Verwendung des Hyperlinks für den Trennbefehl abgeraten.

Adapter: Hierbei handelt es sich um eine Mini-Adapterrichtlinie, die sich speziell auf die VPN-Erzwingung bezieht.

Wenn ein Adapter ausgewählt·ist (Änderung in eine Option mit dem Ausdruck "...deaktiviert, mit Ausnahme von..."), kann der jeweilige Adapter ("Wireless" bezieht sich hierbei spezifisch auf den Kartentyp) die Konnektivität zum VPN nutzen.

Adapter, die in die nachfolgenden Ausnahmelisten aufgenommen werden, können die VPN-Konnektivität nicht nutzen, alle anderen Adapter des jeweiligen Typs hingegen schon.

Wenn ein Adapter nicht ausgewählt ist (mit dem Ausdruck "...deaktiviert, mit Ausnahme von..."), dürfen nur·die in die Ausnahmeliste aufgenommenen Adapter eine Verbindung zum VPN herstellen, alle anderen hingegen nicht.

Dieses Steuerelement kann beispielsweise für Adapter verwendet werden, die mit dem VPN nicht kompatibel sind, oder für Adapter, die von der IT-Abteilung nicht unterstützt werden.

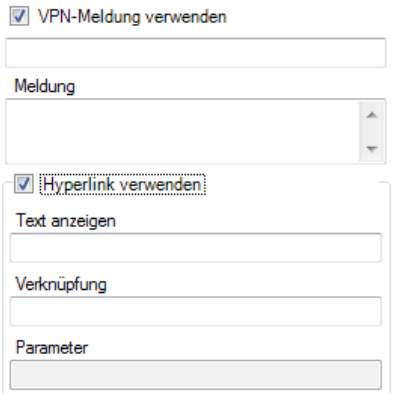
Diese Regel setzt die Adapterrichtlinie außer Kraft, welche für den Standort festgelegt wurde, zu dem gewechselt wird.

Benutzerdefinierte Meldung

Mithilfe der Funktion für benutzerdefinierte Meldungen kann der ZENworks Endpoint Security Management-Administrator Meldungen als direkte Antwort auf Fragen zu Sicherheitsrichtlinien erstellen. Dies ist hilfreich, um Benutzern, die auf richtlinienerzwungene Sicherheitsbeschränkungen stoßen, Unterstützung zukommen zu lassen. Auf diese Weise können auch spezifische Anweisungen für die Benutzer bereitgestellt werden. Steuerelemente für Benutzermeldungen stehen in mehreren Komponenten der Richtlinie zur Verfügung.

So erstellen Sie eine benutzerdefinierte Meldung:

1. Geben Sie einen Titel für die Meldung ein. Dieser Titel wird in der oberen Leiste des Meldungsfelds angezeigt.
2. Geben Sie die Meldung ein. Die Meldung darf maximal 1000 Zeichen umfassen.
3. Ist ein Hyperlink erforderlich, aktivieren Sie das Kontrollkästchen für die Anzeige von Hyperlinks und machen Sie die erforderlichen Angaben.



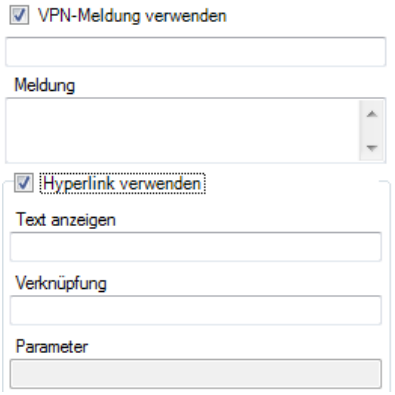
Hinweis: Wird die Meldung bzw. der Hyperlink in einer freigegebenen Komponente geändert, bewirkt dies die Änderung in allen anderen Instanzen dieser Komponente. Mithilfe des Befehls *Auslastung anzeigen* können alle anderen mit dieser Komponente verknüpften Richtlinien angezeigt werden.

Hyperlinks

Ein Administrator kann Hyperlinks in benutzerdefinierte Meldungen aufnehmen, um Sicherheitsrichtlinien weiter zu erläutern oder Links zu Software-Aktualisierungen bereitzustellen (zur Gewährleistung der Integritätseinhaltung). Hyperlinks stehen in mehreren Richtlinienkomponenten zur Verfügung. Es kann ein VPN-Hyperlink erstellt werden, der entweder auf die ausführbare Datei des VPN-Client oder auf eine Stapeldatei verweist, die ausgeführt wird und so den Benutzer vollständig beim VPN anmeldet (weitere Details finden Sie unter „VPN-Erzwingung“ auf Seite 68).

So erstellen Sie einen Hyperlink:

1. Geben Sie einen Namen für den Link an. Dieser Name wird unterhalb der Meldung angezeigt. Er ist auch für Hyperlinks für erweitertes VPN erforderlich.
2. Geben Sie den Hyperlink an.
3. Geben Sie sämtliche Schalter oder anderen Parameter für den Link an.

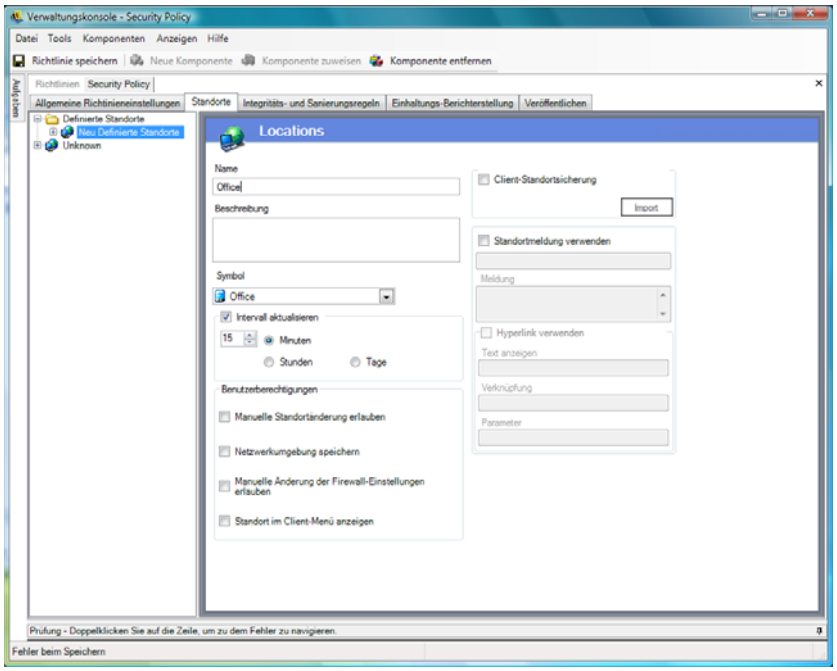


Hinweis: Wird die Meldung bzw. der Hyperlink in einer freigegebenen Komponente geändert, bewirkt dies die Änderung in allen anderen Instanzen dieser Komponente. Mithilfe des Befehls *Auslastung anzeigen* können alle anderen mit dieser Komponente verknüpften Richtlinien angezeigt werden.

2.2.2 Standorte

Unter Standorten versteht man Regelgruppen, die Netzwerkumgebungen zugewiesen sind. Diese Umgebungen können in der Richtlinie (siehe „Netzwerkumgebungen“ auf Seite 91) oder vom Benutzer festgelegt werden, falls erlaubt. Für jeden Standort können individuelle Sicherheitseinstellungen definiert werden. So kann beispielsweise in feindlicheren Netzwerkumgebungen der Zugriff auf bestimmte Netzwerkfunktionen und Hardware untersagt werden, während in vertrauenswürdigen Umgebungen weniger Einschränkungen gelten.

Für den Zugriff auf die standortbezogenen Steuerelemente klicken Sie auf die Registerkarte *Standorte*.



Die folgenden Abschnitte enthalten weitere Informationen:

- „Info zu Standorten“ auf Seite 74
- „Kommunikationshardware“ auf Seite 76
- „Steuerelement für Speichergerätsteuerung“ auf Seite 79
- „Firewall-Einstellungen“ auf Seite 81
- „Netzwerkumgebungen“ auf Seite 91
- „USB-Konnektivität“ auf Seite 93
- „Wi-Fi-Verwaltung“ auf Seite 95
- „Wi-Fi-Sicherheit“ auf Seite 99

Info zu Standorten

Folgende Standorttypen können konfiguriert werden:

Standort "Unbekannt": Sämtliche Richtlinien verfügen über einen standardmäßigen Standort mit der Bezeichnung "Unbekannt". Dies ist der Standort, an den der ZENworks Security Client Benutzer versetzt, wenn sie·eine bekannte Netzwerkumgebung verlassen. Der Standort "Unbekannt" ist für jede Richtlinie eindeutig und steht nicht als freigegebene Komponente zur Verfügung. Das Festlegen und Speichern von Netzwerkumgebungen ist für diesen Standort nicht möglich.

Für den Zugriff auf die Steuerelemente für den Standort "Unbekannt" klicken Sie auf die Registerkarte *Standorte* und dann im Richtlinienbaum auf der linken Seite auf den Standort *Unbekannt*.

Definierte Standorte: Für die Richtlinie können definierte Standorte erstellt oder bestehende (für andere Richtlinien erstellte) Standorte verknüpft werden.

So erstellen Sie einen neuen Standort:

1. Klicken Sie auf *Definierte Standorte* und dann in der Symbolleiste auf die Schaltfläche *Neue Komponente*.
2. Benennen Sie den Standort und geben Sie eine Beschreibung ein.
3. Definieren Sie die Standorteinstellungen:

   Symbol: Wählen Sie ein Standortsymbol als optische Hilfestellung aus, um dem Benutzer die Identifizierung des aktuellen Standorts zu erleichtern. Das Standortsymbol wird im Benachrichtigungsbereich der Taskleiste angezeigt. Zeigen Sie die verfügbaren Standortsymbole in der Dropdown-Liste an und treffen Sie eine Auswahl.

   Aktualisierungsintervall: Legen Sie fest, wie oft der ZENworks Security Client an diesem Standort auf·Richtlinienaktualisierungen prüft. Der Häufigkeitswert wird in Minuten, Stunden oder Tagen angegeben. Wenn die Auswahl dieses Parameters aufgehoben wird, prüft der ZENworks Security Client an diesem Standort nicht auf Aktualisierungen.

   Benutzerberechtigungen: Geben Sie die Benutzerberechtigungen an:

   - **Manuellen Standortwechsel zulassen:** Ermöglicht dem Benutzer den Wechsel zu/von diesem Standort. Für nicht verwaltete Standorte (Hotspots, Flughäfen, Hotels usw.) sollte diese Berechtigung erteilt werden. In gesteuerten und kontrollierten Umgebungen, in denen die Netzwerkparameter bekannt sind, kann diese Berechtigung deaktiviert werden. Wenn diese Berechtigung deaktiviert ist, kann der Benutzer nicht·von/zu Standorten wechseln, stattdessen verwendet der ZENworks Security Client die Netzwerkumgebungsparameter, die für diesen Standort angegeben wurden.
   - **Netzwerkumgebung speichern:** Hiermit kann der Benutzer die Netzwerkumgebung an diesem Standort speichern und so bei seiner Rückkehr den automatischen Wechsel zu dem Standort ermöglichen. Diese Einstellung empfiehlt sich für sämtliche Standorte, zu denen der Benutzer wechseln muss. Es können mehrere Netzwerkumgebungen für einen einzelnen Standort gespeichert werden. Wenn beispielsweise ein Standort, der als "Flughafen" definiert ist, Teil der aktuellen Richtlinie ist, kann jeder Flughafen, den der Benutzer besucht, als Netzwerkumgebung für diesen Standort gespeichert werden. Auf diese Weise kann ein mobiler Benutzer zu einer gespeicherten Flughafen-Umgebung zurückkehren, und der ZENworks Security Client wechselt automatisch zum Standort "Flughafen" und wendet die definierten Sicherheitseinstellungen an. Ein Benutzer hat selbstverständlich die Möglichkeit, einen Standortwechsel vorzunehmen, ohne die Umgebung zu speichern.
   - **Manuelle Änderung von Firewall-Einstellungen zulassen:** Ermöglicht dem Benutzer, die Firewall-Einstellungen zu ändern.
   - **Standort in Client-Menü anzeigen:** Hiermit kann der Standort im Client-Menü angezeigt werden. Ist diese Option nicht ausgewählt, wird der Standort unter keinen Umständen angezeigt.

   Client Location Assurance: Da die Netzwerk-Umgebungsinformationen zur Ermittlung eines Standorts leicht gefälscht werden können und so der Endpunkt potenzielles Angriffsziel für Eindringlinge werden kann, stellt Client Location Assurance Service (CLAS) eine Option zur kryptographischen Überprüfung·des Standorts bereit. Dieser Service ist nur in Netzwerkumgebungen zuverlässig, die vollständig und ausschließlich der Kontrolle des Unternehmens unterstehen. Wenn ein Standort um Client Location Assurance ergänzt wird, können die Firewall-Einstellungen und Berechtigungen für diesen Standort weniger strikt festgelegt werden, da davon ausgegangen wird, dass der Endpunkt nun hinter der Netzwerk-Firewall geschützt ist.

Der ZENworks Security Client verwendet einen festen, von Unternehmen konfigurierbaren Port, um eine Herausforderung an Client Location Assurance Service zu senden. Client Location Assurance Service entschlüsselt das Paket, antwortet auf die Herausforderung und beweist so, dass er über den privaten Schlüssel verfügt, der dem öffentlichen Schlüssel entspricht. Im Symbol in der Taskleiste ist ein Häkchen zu sehen; so wird angegeben, dass sich der Benutzer am richtigen Standort befindet.

Der ZENworks Security Client kann nur zu dem Standort wechseln, wenn der CLAS-Server erkannt wird. Wird der CLAS-Server nicht erkannt, verbleibt der ZENworks Security Client am Standort "Unbekannt", um den Endpunkt zu sichern, selbst wenn alle anderen Netzwerkparameter übereinstimmen.

Wenn Sie CLAS für einen Standort aktivieren möchten, aktivieren Sie das Kontrollkästchen für Client Location Assurance, klicken Sie auf *Importieren* und wählen Sie dann die Datei aus. Nach erfolgreichem Import des Schlüssels wird das Wort "Konfiguriert" angezeigt.

Diese Option steht für den Standort "Unbekannt" nicht zur Verfügung.

Standortmeldung verwenden: Hiermit kann eine optionale benutzerdefinierte Meldung angezeigt werden, wenn der ZENworks Security Client zu diesem Standort wechselt. Diese Meldung kann Anweisungen für den Endbenutzer, Details zu Richtlinienbeschränkungen an diesem Standort oder einen Hyperlink für weitere Informationen enthalten.

4 Klicken Sie auf *Richtlinie speichern*. Wenn Ihre Richtlinie Fehler aufweist, ziehen Sie Abschnitt 2.2.6, „Fehlerbenachrichtigung“, auf Seite 112 zurate.

So verknüpfen Sie einen bestehenden Standort:

1 Klicken Sie auf *Definierte Standorte* und dann in der Symbolleiste auf die Schaltfläche *Komponente verknüpfen*.

2 Wählen Sie die gewünschten Standorte in der Liste aus.

3 Bearbeiten Sie die Einstellungen gegebenenfalls.

Hinweis: Wenn Sie die Einstellungen in einer freigegebenen Komponente ändern, beeinflusst dies alle Instanzen dieser Komponente. Mithilfe des Befehls *Auslastung anzeigen* können alle anderen mit dieser Komponente verknüpften Richtlinien angezeigt werden.

---

4 Klicken Sie auf *Richtlinie speichern*. Wenn Ihre Richtlinie Fehler aufweist, ziehen Sie Abschnitt 2.2.6, „Fehlerbenachrichtigung“, auf Seite 112 zurate.

Es sollten mehrere definierte Standorte (über einfache Standorte vom Typ "Arbeit" und "Unbekannt" hinaus) in die Richtlinie aufgenommen werden, um den Benutzern beim Verbindungsaufbau außerhalb der Firewall des Unternehmens unterschiedliche Sicherheitsberechtigungen zur Verfügung zu stellen. Wenn die Standortnamen einfach gehalten werden (z. B. Cafés, Flughäfen, Zuhause) und das Standortsymbol in der Taskleiste optische Hilfestellung gibt, können Benutzer ganz einfach zu den entsprechenden Sicherheitseinstellungen wechseln, die für die jeweilige Netzwerkumgebung erforderlich sind.

Kommunikationshardware

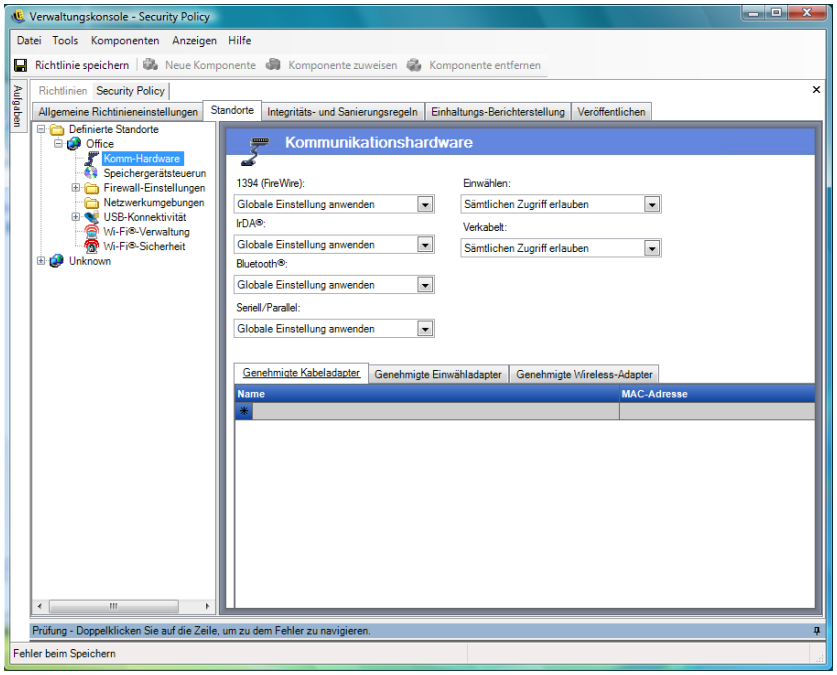
Mithilfe der Einstellungen für die Kommunikationshardware wird nach Standort gesteuert, welche Hardwaretypen in dieser Netzwerkumgebung eine Verbindung herstellen dürfen.

Hinweis: Sie können die Steuerelemente für Kommunikationshardware auf der Registerkarte *Allgemeine Richtlinieneinstellungen* global bzw. auf der Registerkarte *Standorte* für einzelne Standorte festlegen.

Wenn Sie die Steuerelemente für Kommunikationshardware für einen Standort festlegen möchten, klicken Sie auf die Registerkarte *Standorte*, erweitern Sie den gewünschten Standort im Baum und klicken Sie dann auf *Komm-Hardware*.

oder

Wenn Sie die Steuerelemente für Kommunikationshardware global festlegen möchten, klicken Sie auf die Registerkarte *Allgemeine Richtlinieneinstellungen*, erweitern Sie den Eintrag *Globale Einstellungen* im Baum und klicken Sie dann auf *Komm-Hardware*. Weitere Informationen finden Sie unter „Kommunikationshardware“ auf Seite 54.



Treffen Sie eine Auswahl, um zu aktivieren, zu deaktivieren oder um die globale Einstellung für die einzelnen, aufgeführten Kommunikationshardware-Geräte anzuwenden:

- **1394 (FireWire):** Steuert den Zugriff auf den FireWire*-Anschluss des Endpunkts.
- **IrDA:** Steuert den Zugriff auf den Infrarotanschluss des Endpunkts.
- **Bluetooth:** Steuert den Zugriff auf den Bluetooth*-Anschluss des Endpunkts.
- **Seriell/Parallel:** Steuert den Zugriff auf den seriellen/parallelen Anschluss des Endpunkts.
- **Einwählen:** Steuert die Modemkonnektivität nach Standort. Diese Option steht bei der globalen Konfiguration von Einstellungen für Kommunikationshardware über die Registerkarte *Allgemeine Richtlinieneinstellungen* nicht zur Verfügung.
- **Wired:** Steuert die LAN-Kartenkonnektivität nach Standort. Diese Option steht bei der globalen Konfiguration von Einstellungen für Kommunikationshardware über die Registerkarte *Allgemeine Richtlinieneinstellungen* nicht zur Verfügung.

Lautet die Einstellung "Aktivieren", ist der uneingeschränkte Zugriff auf den Kommunikationsanschluss möglich.

Lautet die Einstellung "Deaktivieren", wird jeglicher Zugriff auf den Kommunikationsanschluss unterbunden.

Hinweis: Wi-Fi-Adapter werden entweder global gesteuert oder mithilfe der Steuerelemente für die Wi-Fi-Sicherheit lokal deaktiviert. Adapter können nach Marke angegeben werden, und zwar anhand der Liste der genehmigten Wireless-Adapter.

Liste der genehmigten Einwähladapter: Der ZENworks Security Client kann dafür sorgen, dass nur die angegebenen, genehmigten Einwähladapter (Modems) eine Verbindung herstellen können. So kann ein Administrator beispielsweise eine Richtlinie implementieren, gemäß der nur eine bestimmte Marke oder Art von Modemkarte zulässig ist. Hierdurch werden die Kosten verringert, die entstehen, wenn Mitarbeiter nicht unterstützte Hardware verwenden.

Liste der genehmigten Wireless-Adapter: Der ZENworks Security Client kann dafür sorgen, dass nur die angegebenen, genehmigten Wireless-Adapter eine Verbindung herstellen können. So kann ein Administrator beispielsweise eine Richtlinie implementieren, gemäß der nur eine bestimmte Marke oder Art von Wireless-Karte zulässig ist. Hierdurch werden die Supportkosten verringert, die entstehen, wenn Mitarbeiter nicht unterstützte Hardware verwenden. Zudem werden so die Unterstützung und die Umsetzung von auf IEEE-(Institute of Electrical & Electronics Engineers-)Standards aufbauenden Sicherheitsinitiativen vereinfacht. Dies gilt u. a. auch für LEAP (Lightweight Extensible Authentication Protocol), PEAP (Protected Extensible Authentication Protocol), WPA (Wireless Protected Access) und TKIP (Temporal Key Integrity Protocol).

Verwenden der AdapterAware-Funktion:

Der ZENworks Security Client wird bei jeder Installation eines Netzwerkgeräts im System benachrichtigt und ermittelt, ob das Gerät autorisiert oder nicht autorisiert ist. Ist es nicht autorisiert, wird der Gerätetreiber deaktiviert, das neue Gerät kann also nicht verwendet werden. Der Benutzer wird entsprechend benachrichtigt.

Hinweis: Wenn ein neuer, nicht autorisierter Adapter (gilt sowohl für Einwähl- als auch für Wireless-Adapter) erstmals seine Treiber am Endpunkt installiert (über PCMCIA oder USB), wird der Adapter im Windows-Geräte-Manager bis zum Neubooten des Systems als aktiviert angezeigt, obwohl jegliche Netzwerkkonnektivität blockiert ist.

Geben Sie den Namen jedes zulässigen Adapters an. Es ist zulässig, nur Teile von Adapternamen einzugeben. Adapternamen sind auf 50 Zeichen beschränkt und die Groß-/Kleinschreibung wird beachtet. Das Betriebssystem Windows 2000 benötigt den Gerätenamen, um diese Funktionalität bereitstellen zu können. Werden keine Adapter eingegeben, sind alle Adapter des Typs zulässig. Wird nur ein Adapter eingegeben, ist nur dieser eine Adapter an diesem Standort zulässig.

Hinweis: Befindet sich der Endpunkt an einem Standort, an dem als Netzwerkidentifikation lediglich eine Zugriffspunkt-SSID (Service Set Identification) angegeben wird, wechselt der ZENworks Security Client zu diesem Standort, bevor der nicht autorisierte Adapter deaktiviert wird. Die Passwort-Außerkraftsetzung sollte ermöglicht werden, um für diesen Fall einen manuellen Standortwechsel bereitzustellen.

Steuerelement für Speichergerätsteuerung

Mit Steuerelementen für die Speichergerätsteuerung werden die Speichergerät-Standardeinstellungen für die Richtlinie festgelegt, in denen sämtliche externen Dateispeichergeräte über Lese- oder Schreibrechte für Dateien verfügen, im schreibgeschützten Modus betrieben werden oder vollständig deaktiviert sind. Bei Deaktivierung können·diese Geräte keine Daten vom Endpunkt abrufen. Der Zugriff auf die Festplatte und alle Netzlaufwerke sowie deren Verwendung sind weiterhin möglich.

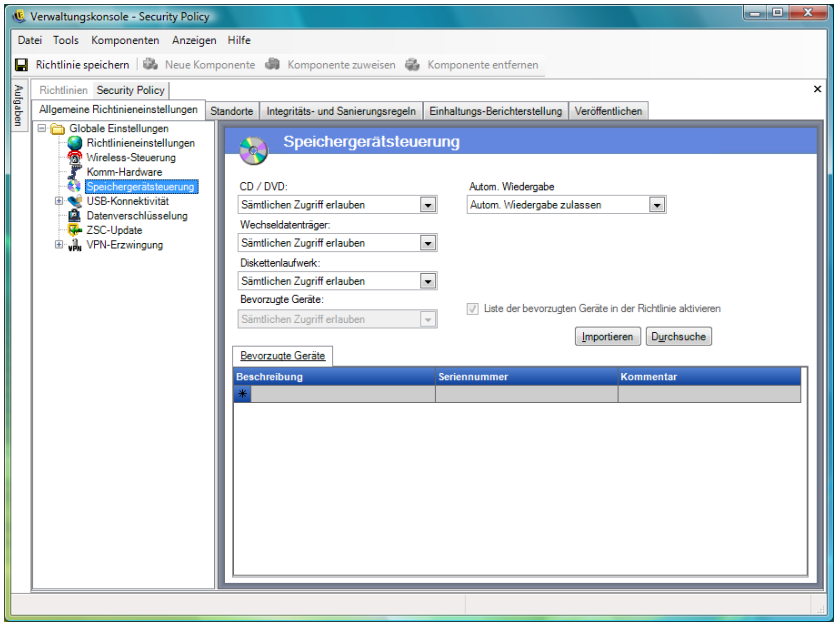
Die Speichergerätsteuerung von ZENworks Endpoint Security darf nicht verwendet werden, wenn ZENworks Storage Encryption Solution aktiviert ist.

Hinweis: Sie können die Steuerelemente für Speichergeräte auf der Registerkarte *Allgemeine Richtlinieneinstellungen* global bzw. auf der Registerkarte *Standorte* für einzelne Standorte festlegen.

Wenn Sie die Steuerelemente für Speichergeräte für einen Standort festlegen möchten, klicken Sie auf die Registerkarte *Standorte*, erweitern Sie den gewünschten Standort im Baum und klicken Sie dann auf *Speichergerätsteuerung*.

oder

Wenn Sie die Steuerelemente für Speichergeräte global festlegen möchten, klicken Sie auf die Registerkarte *Allgemeine Richtlinieneinstellungen*, erweitern Sie den Eintrag *Globale Einstellungen* im Baum und klicken Sie dann auf *Speichergerätsteuerung*. Weitere Informationen finden Sie unter „Steuerelement für Speichergerätsteuerung“ auf Seite 55.



Die Speichergerätsteuerung ist in folgende Kategorien unterteilt:

- **CD/DVD:** Steuert sämtliche Geräte, die im Windows-Geräte-Manager unter *DVD/CD-ROM-Laufwerke* aufgeführt sind.

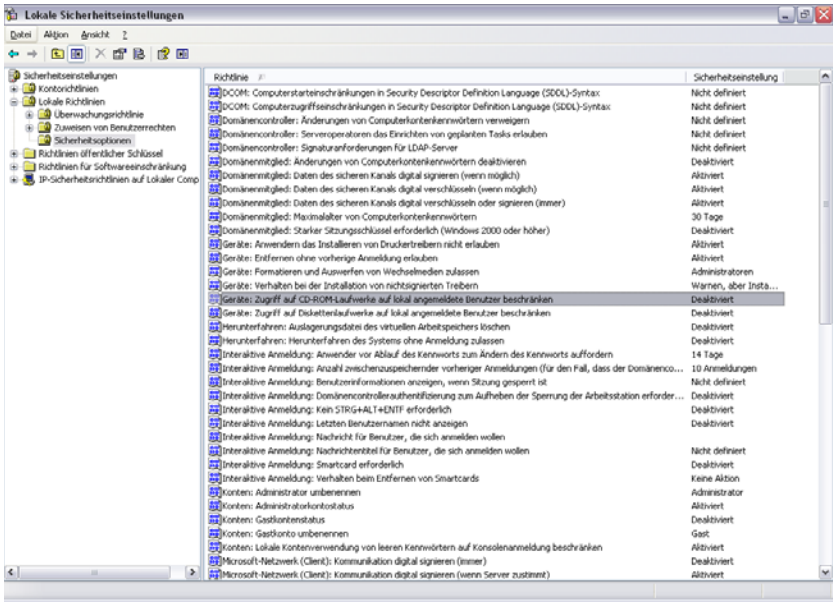
- **Wechseldatenträger:** Steuert sämtliche Geräte, die im Windows-Geräte-Manager unter *Laufwerke* aufgeführt sind.
- **Diskettenlaufwerk:** Steuert sämtliche Geräte, die im Windows-Geräte-Manager unter *Diskettenlaufwerke* aufgeführt sind.

Feste Speicher (Festplatten) und Netzlaufwerke (falls verfügbar) sind immer zulässig.

Wenn Sie den Richtliniestandard für Speichergeräte festlegen möchten, wählen Sie in den Dropdown-Listen die globale Einstellung für beide Typen aus:

- **Aktivieren:** Der Gerätetyp ist standardmäßig zulässig.
- **Deaktivieren:** Der Gerätetyp ist nicht zulässig. Wenn Benutzer versuchen, auf einem definierten Speichergerät auf Dateien zuzugreifen, wird eine Fehlermeldung des Betriebssystems bzw. der Anwendung, die auf das lokale Speichergerät zuzugreifen versucht, ausgegeben, die besagt, dass bei dem Vorgang ein Fehler aufgetreten ist.
- **Nur Lesen:** Für den Gerätetyp ist "Nur Lesen" festgelegt. Wenn Benutzer versuchen, auf das Gerät zu schreiben, wird eine Fehlermeldung des Betriebssystems bzw. der Anwendung, die auf das lokale Speichergerät zuzugreifen versucht, ausgegeben, die besagt, dass bei dem Vorgang ein Fehler aufgetreten ist.

Hinweis: Wenn Sie CD-ROM-Laufwerke bzw. Diskettenlaufwerke für eine Gruppe von Endpunkten auf "Nur Lesen" einstellen möchten, muss in den lokalen Sicherheitseinstellungen (die durch ein Verzeichnisdienst-Gruppenrichtlinienobjekt übergeben wurden) sowohl für *Geräte: Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken* als auch für *Geräte: Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken* die Option "Deaktiviert" festgelegt sein. Um dies sicherzustellen, öffnen Sie entweder das Gruppenrichtlinienobjekt oder sehen in der Systemsteuerung unter "Verwaltung" nach. Wählen Sie die Optionsfolge "Lokale Sicherheitseinstellungen" - "Sicherheitsoptionen" und vergewissern Sie sich, dass beide Geräte deaktiviert sind. "Deaktiviert" ist der Standardwert.



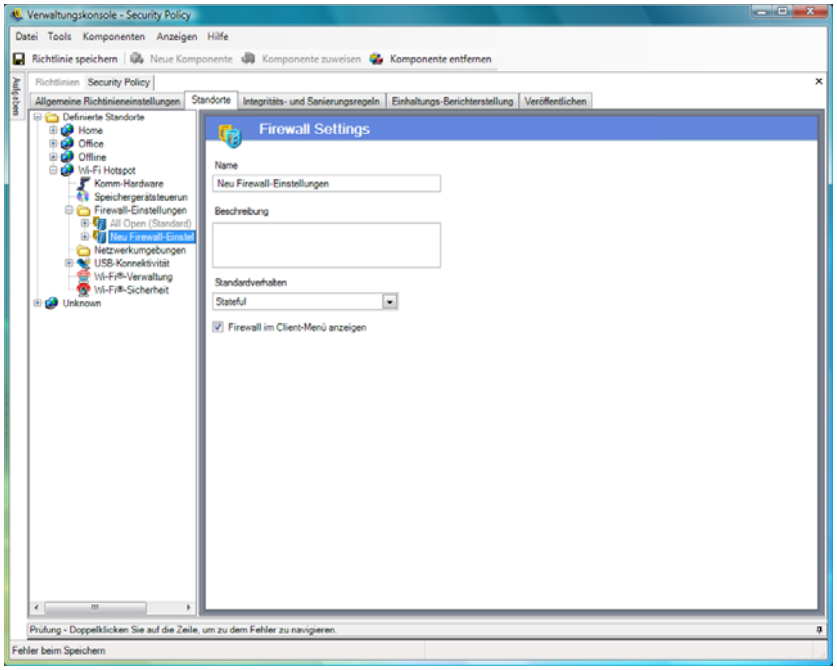
Firewall-Einstellungen

Mit Firewall-Einstellungen wird die Konnektivität sämtlicher Netzwerkports, Zugriffssteuerungslisten, Netzwerkpakete (ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol) usw.) gesteuert. Zudem wird gesteuert, welche Anwendungen über ein ausgehendes Socket verfügen bzw. verwendet werden können, wenn die Firewall-Einstellung angewandt wird.

Hinweis: Diese Funktion steht nur bei der ZENworks Endpoint Security-Installation zur Verfügung und kann für UWS-(Unlimited Web Solutions-)Sicherheitsrichtlinien nicht verwendet werden.

Für den Zugriff auf dieses Steuerelement klicken Sie auf die Registerkarte *Standorte* und klicken Sie dann im Richtlinienbaum auf der linken Seite auf das Symbol für *Firewall-Einstellungen*.

Die einzelnen Komponenten einer Firewall-Einstellung werden separat konfiguriert, hierbei muss lediglich das Standardverhalten der TCP-/UDP-Ports festgelegt werden. Ist diese Einstellung aktiviert, wirkt sie sich auf sämtliche TCP-/UDP-Ports aus. Individuelle oder zu Gruppen zusammengefasste Ports können mit einer anderen Einstellung erstellt werden.



So erstellen Sie eine neue Firewall-Einstellung:

1. Wählen Sie im Komponentenbaum den Eintrag *Firewall-Einstellungen* aus und klicken Sie dann auf die Schaltfläche *Neue Komponente*.
2. Benennen Sie die Firewall-Einstellung und geben Sie eine Beschreibung ein.
3. Klicken Sie im Komponentenbaum mit der rechten Maustaste auf *TCP-/UDP-Anschlüsse* und wählen Sie dann die Option zum Hinzufügen neuer TCP-/UDP-Ports, um das Standardverhalten für sämtliche TCP-/UDP-Ports festzulegen.

   Die Firewall-Einstellungen können um weitere Ports und Listen ergänzt werden und ihnen können individuelle und eindeutige Verhaltensweisen zugewiesen werden, die die Standardeinstellungen außer Kraft setzen.

Die Standardeinstellung für sämtliche Ports lautet beispielsweise "Alle Stateful". Das bedeutet, dass die Portlisten für Streaming-Medien und Webbrowsing der Firewall-Einstellung hinzugefügt werden. Das Verhalten des Ports für Streaming-Medien ist auf "Geschlossen" eingestellt, das Verhalten des Ports für Webbrowsing auf "Geöffnet". Der Netzwerkverkehr über die TCP-Ports 7070, 554, 1755 und 8000 wird blockiert. Der Netzwerkverkehr über die Ports 80 und 443 ist·möglich (Port offen) und kann·im Netzwerk nachvollzogen werden. Alle anderen Ports befinden·sich im Stateful-Modus; der Datenverkehr, der über sie abgewickelt wird, muss·also erst angefordert werden.

Weitere Informationen finden Sie unter „TCP-/UDP-Ports“ auf Seite 83.

4. Klicken Sie mit der rechten Maustaste auf *Zugriffssteuerungslisten* und wählen Sie dann die Option zum Hinzufügen neuer Zugriffssteuerungslisten, um Adressen hinzuzufügen, bei denen unerwünschter Datenverkehr möglicherweise passieren können muss, ungeachtet des aktuellen Portverhaltens.

   Weitere Informationen finden Sie unter „Zugriffssteuerungslisten“ auf Seite 86.

5. Klicken Sie mit der rechten Maustaste auf *Anwendungssteuerung* und wählen Sie dann die Option zum Hinzufügen neuer Anwendungssteuerungen, um Anwendungen entweder am Netzwerkzugriff zu hindern oder einfach ihre Ausführung zu unterbinden.

   Weitere Informationen finden Sie unter „Anwendungssteuerungselemente“ auf Seite 89.

6. Legen Sie fest, ob diese Firewall im ZENworks Security Client-Menü angezeigt werden soll (bei Deaktivierung dieser Option wird diese Firewall-Einstellung für den Benutzer nicht angezeigt).

7. Klicken Sie auf *Richtlinie speichern*. Wenn Ihre Richtlinie Fehler aufweist, ziehen Sie Abschnitt 2.2.6, „Fehlerbenachrichtigung“, auf Seite 112 zurate.

So verknüpfen Sie eine bestehende Firewall-Einstellung:

1. Wählen Sie im Komponentenbaum den Eintrag *Firewall-Einstellungen* aus und klicken Sie dann auf die Schaltfläche *Komponente verknüpfen*.

2. Wählen Sie die gewünschten Firewall-Einstellungen in der Liste aus.

3. Ändern Sie im Bedarfsfall die Einstellung für das Standardverhalten.

   Hinweis: Wenn Sie die Einstellungen in einer freigegebenen Komponente ändern, beeinflusst dies alle Instanzen dieser Komponente. Mithilfe des Befehls *Auslastung anzeigen* können alle anderen mit dieser Komponente verknüpften Richtlinien angezeigt werden.

   ---

4. Klicken Sie auf *Richtlinie speichern*. Wenn Ihre Richtlinie Fehler aufweist, ziehen Sie Abschnitt 2.2.6, „Fehlerbenachrichtigung“, auf Seite 112 zurate.

An einem einzigen Standort kann es mehrere Firewall-Einstellungen geben. Eine Einstellung ist als Standardeinstellung definiert, die restlichen Einstellungen stehen dem Benutzer als Optionen zur Verfügung, die er im Bedarfsfall nutzen kann. Mehrere Einstellungen sind hilfreich, wenn für einen Benutzer im Regelfall bestimmte Sicherheitseinschränkungen innerhalb einer Netzwerkumgebung erforderlich sind und diese Einschränkungen beispielsweise für ICMP-Rundsendungen für kurze Zeit entweder aufgehoben oder verstärkt werden müssen.

Nach der Installation stehen folgende Firewall-Einstellungen zur Verfügung:

- **Alle adaptiv:** Legt sämtliche Netzwerkports als "Stateful" fest (jeglicher unerwünscht eingehender Netzwerkverkehr wird blockiert, jeglicher ausgehender Netzwerkverkehr ist zulässig), ARP- und 802.1x-Pakete sind zulässig und sämtliche Netzwerkanwendungen dürfen eine Netzwerkverbindung aufbauen.
- **Alle geöffnet:** Legt sämtliche Netzwerkports als geöffnet fest (jeglicher Netzwerkverkehr ist zulässig), und alle Pakettypen sind zulässig. Sämtliche Netzwerkanwendungen dürfen eine Netzwerkverbindung aufbauen.
- **Alle geschlossen:** Hiermit werden sämtliche Netzwerkports geschlossen und sämtliche Pakettypen beschränkt.

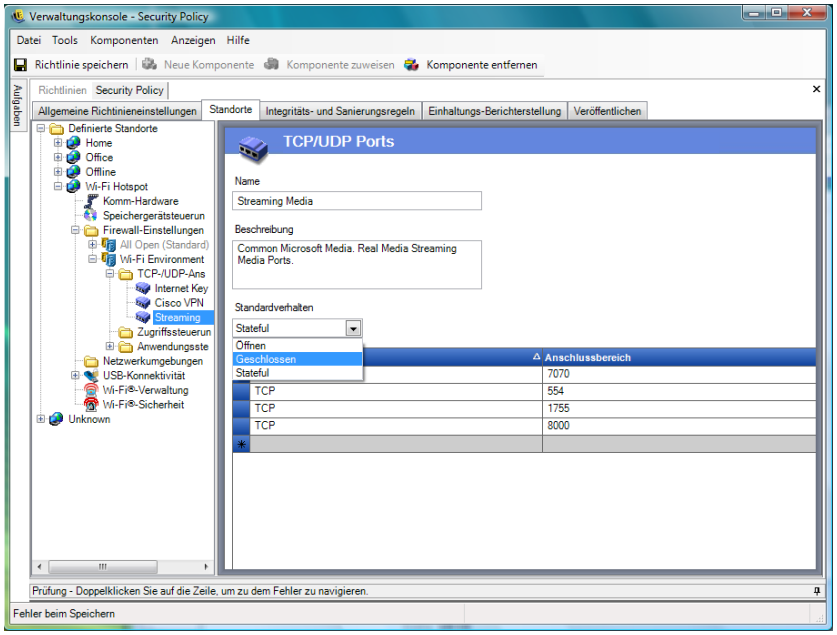
Bei einem neuen Standort ist eine einzige Firewall-Einstellung, "Alle geöffnet", als Standard eingestellt. Wenn Sie eine andere Firewall-Einstellung als Standard festlegen möchten, klicken Sie mit der rechten Maustaste auf die gewünschte Firewall-Einstellung und wählen Sie dann *Als Standard einrichten*.

TCP-/UDP-Ports

Endpunktdaten werden hauptsächlich durch Steuerung der TCP-/UDP-Port-Aktivität gesichert. Mit dieser Funktion können Sie eine Liste der TCP-/UDP-Ports erstellen, die nur in dieser Firewall-Einstellung behandelt werden. Die Listen enthalten eine Sammlung an Ports und Portbereichen zusammen mit ihren Transporttypen, die die Funktion des Bereichs definieren.

Hinweis: Diese Funktion steht nur bei der ZENworks Endpoint Security-Installation zur Verfügung und kann für UWS-(Unlimited Web Solutions-)Sicherheitsrichtlinien nicht verwendet werden.

Für den Zugriff auf dieses Steuerelement klicken Sie auf die Registerkarte *Standorte*, klicken Sie auf das "+"-Symbol neben *Firewall-Einstellungen*, klicken Sie auf das "+"-Symbol neben der gewünschten Firewall und klicken Sie dann im Richtlinienbaum auf der linken Seite auf das Symbol für *TCP-/UDP-Anschlüsse*.



Neue Listen mit TCP-/UDP-Ports können mit einzelnen Ports oder als Bereich (1-100) definiert werden (pro Listenzeile).

So erstellen Sie eine neue TCP-/UDP-Port-Einstellung:

1. Klicken Sie im Komponentenbaum mit der rechten Maustaste auf *TCP-/UDP-Anschlüsse* und wählen Sie dann die Option zum Hinzufügen neuer TCP-/UDP-Ports .
2. Benennen Sie die Portliste und geben Sie eine Beschreibung ein.
3. Wählen Sie das Portverhalten in der Dropdown-Liste aus:
   - **Geöffnet:** Sämtlicher ein- und ausgehender Netzwerkverkehr ist zulässig. Da sämtlicher Netzwerkverkehr zulässig ist, kann die Identität Ihres Computers für diesen Port bzw. Portbereich eingesehen werden.
   - **Geschlossen:** Sämtlicher ein- und ausgehender Netzwerkverkehr ist blockiert. Da sämtliche Netzwerk-Identifikationsanforderungen blockiert werden, ist Ihre Computeridentität für diesen Port oder Portbereich verborgen.
   - **Stateful:** Sämtlicher unerwünscht eingehender Netzwerkverkehr wird blockiert. Sämtlicher ausgehende Netzwerkverkehr ist über diesen Port oder Portbereich erlaubt.
4. Geben Sie den Transporttyp an, indem Sie in der Spalte *Anschlusstyp* auf den Abwärtspfeil klicken:
   - TCP/UDP
   - Ether
   - IP
   - TCP
   - UDP
5. Geben Sie Ports und Portbereiche wie folgt ein:
   - Einzelne Ports
   - Einen Portbereich mit der ersten Portnummer, gefolgt von einem Bindestrich und der letzten Portnummer.

     Mit 1-100 werden·beispielsweise alle Ports von 1 bis 100 hinzugefügt.

     Eine vollständige Liste von Ports und Transporttypen finden Sie auf der Webseite Assigned Numbers Authority (http://www.iana.org).
6. Klicken Sie auf *Richtlinie speichern*.

So verknüpfen Sie einen bestehenden TCP/UDP-Port mit dieser Firewall-Einstellung:

1. Wählen Sie *TCP-/UDP-Anschlüsse* im Komponentenbaum aus und klicken Sie dann auf die Schaltfläche *Komponente verknüpfen*.
2. Wählen Sie die gewünschten Ports·in der Liste aus.
3. Konfigurieren Sie die Einstellungen für das Standardverhalten.

   Wenn Sie die Einstellungen in einer freigegebenen Komponente ändern, beeinflusst dies alle Instanzen dieser Komponente. Mithilfe des Befehls *Auslastung anzeigen* können alle anderen mit dieser Komponente verknüpften Richtlinien angezeigt werden.
4. Klicken Sie auf *Richtlinie speichern*.

Mehrere TCP/UDP-Portgruppen wurden gebündelt und stehen bei der Installation zur Verfügung:

Name	Beschreibung	Transport	Wert
Alle Ports	Alle Ports	Alle	1-65535
BlueRidge VPN	Ports, die vom BlueRidge VPN-Client genutzt werden	UDP	820
Cisco VPN	Ports, die vom Cisco* VPN-Client genutzt werden	IP	50,51
		UDP	500,4500
		UDP	1000-1200
		UDP	62514,62515,62517
		UDP	62519-62521
		UDP	62532,62524
Allgemeines Networking	Allgemein verwendete Netzwerkports für die Erstellung von Firewalls	TCP	53
		UDP	53
		UDP	67,68
		TCP	546, 547
		UDP	546, 547
		TCP	647, 847
		UDP	647, 847
Datenbankkommunikation	Microsoft*-, Oracle*-, Siebel*-, Sybase*-, SAP*-Datenbankports	TCP	4100
		TCP	1521
		TCP	1433
		UDP	1444
		TCP	2320
		TCP	49998
		TCP	3200
		TCP	3600
File Transfer Protocol (FTP)	Port für das File Transfer Protocol	TCP/UDP	21

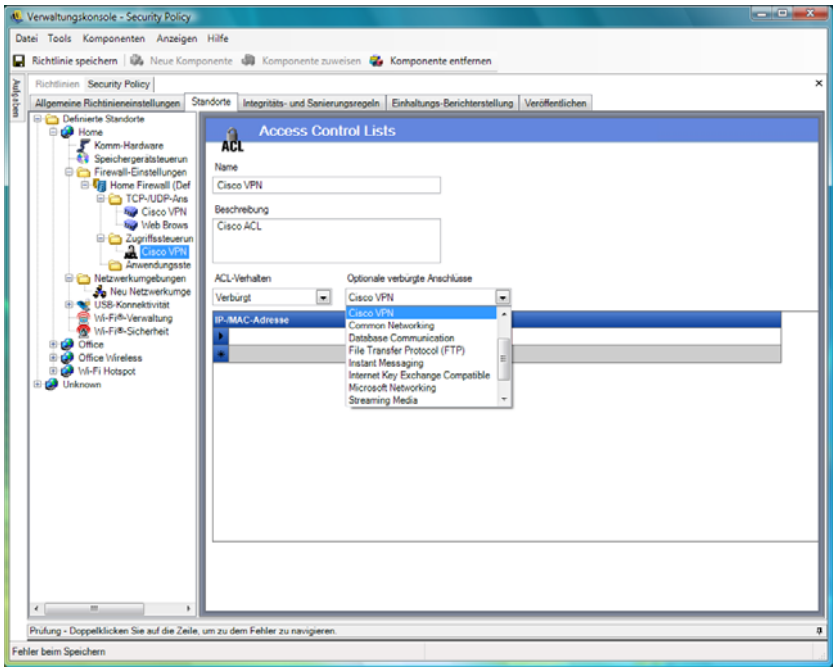
Name	Beschreibung	Transport	Wert
Instant Messaging	Microsoft-, AOL*- und Yahoo* Instant Messaging-Ports	TCP	6891-6900
		TCP	1863,443
		UDP	1863,443
		UDP	5190
		TCP	6901
		UDP	6901
		TCP	5000-5001
		UDP	5055
		TCP	20000-20059
		UDP	4000
		TCP	4099
		TCP	5190
Internet Key Exchange-kompatibles VPN	Ports, die von Internet Key Exchange-kompatiblen VPN-Clients genutzt·werden	UDP	500
Microsoft Networking	Übliche Dateifreigabe-/Active Directory*-Ports	TCP/UDP	135-139, 445
Offene Ports	Ports, die für diese Firewall offen sind	TCP/UDP	80
Streaming-Medien	Übliche Ports für Microsoft- und Real-Streaming-Media	TCP	7070, 554, 1755, 8000
Webbrowser	Übliche Webbrowser-Ports, einschließlich SSL	Alle	80, 443

Zugriffssteuerungslisten

Es gibt Adressen, bei denen unerwünschter Datenverkehr möglicherweise passieren können muss, ungeachtet des aktuellen Portverhaltens (z. B. Sicherungsserver oder Exchange Server-Instanz des Unternehmens). In Instanzen, in denen unerwünschter Datenverkehr an und von verbürgte(n) Server(n) geleitet werden muss, kann zur Lösung dieses Problems eine Zugriffssteuerungsliste (ACL) definiert werden.

Hinweis: Diese Funktion steht nur bei der ZENworks Endpoint Security-Installation zur Verfügung und kann für UWS-(Unlimited Web Solutions-)Sicherheitsrichtlinien nicht verwendet werden.

Für den Zugriff auf dieses Steuerelement klicken Sie auf die Registerkarte *Standorte*, klicken Sie auf das "+"-Symbol neben *Firewall-Einstellungen*, klicken Sie auf das "+"-Symbol neben der gewünschten Firewall, klicken Sie im Richtlinienbaum auf der linken Seite mit der rechten Maustaste auf *Zugriffssteuerungslisten* und wählen Sie dann die Option zum Hinzufügen neuer Zugriffssteuerungslisten.



So erstellen Sie eine neue ACL-Einstellung:

1. Klicken Sie im Komponentenbaum mit der rechten Maustaste auf *Zugriffssteuerungslisten* und wählen Sie dann die Option zum Hinzufügen neuer Zugriffssteuerungslisten.
2. Geben Sie einen Namen und eine Beschreibung für die Zugriffssteuerungsliste ein.
3. Geben Sie Adresse oder Makro für die Zugriffssteuerungsliste an.
4. Geben Sie den ACL-Typ an:
   - **IP:** Bei diesem Typ ist die Adresse auf 15 Zeichen beschränkt und enthält lediglich die Zahlen 0–9 sowie Punkte (Beispiel: 123.45.6.189). IP-Adressen können auch als Bereich eingegeben werden, beispielsweise 123.0.0.0–123.0.0.255.
   - **MAC:** Bei diesem Typ ist die Adresse auf 12 Zeichen beschränkt und enthält lediglich die Zahlen 0–9 sowie die Buchstaben A–F (Groß- und Kleinbuchstaben), durch Doppelpunkte voneinander getrennt (Beispiel: 00:01:02:34:05:B6).
5. Klicken Sie in die Dropdown-Liste für das ACL-Verhalten und legen Sie fest, ob die aufgelisteten ACL *Verbürgt* (immer erlauben, auch wenn sämtliche TCP-/UDP-Ports geschlossen sind) oder *Nicht verbürgt* (Zugriff blockieren) sein sollen.
6. Wenn Sie *Verbürgt* ausgewählt haben, wählen Sie optionale verbürgte Ports (TCP/UDP) aus, die diese ACL verwenden soll. Diese Ports erlauben sämtlichen ACL-Verkehr, während andere TCP-/UDP-Ports ihre aktuellen Einstellungen beibehalten. Die Auswahl von *Keine* bedeutet, dass diese ACL jeden Port verwenden kann.
7. Klicken Sie auf *Richtlinie speichern*.

So verknüpfen Sie eine vorhandene ACL bzw. ein vorhandenes Makro mit dieser Firewall-Einstellung:

1. Wählen Sie *Zugriffssteuerungsliste* im Komponentenbaum aus und klicken Sie dann auf die Schaltfläche *Komponente verknüpfen*.
2. Wählen Sie die ACL bzw. Makros in der Liste aus.

3 Konfigurieren Sie die Einstellungen für das ACL-Verhalten nach Bedarf.

Hinweis: Wenn Sie die Einstellungen in einer freigegebenen Komponente ändern, beeinflusst dies alle Instanzen dieser Komponente. Mithilfe des Befehls *Auslastung anzeigen* können alle anderen mit dieser Komponente verknüpften Richtlinien angezeigt werden.

4 Klicken Sie auf *Richtlinie speichern*.

Liste mit Netzwerkadressmakros

Nachfolgend finden Sie eine Liste mit speziellen Zugriffssteuerungsmakros. Diese können individuell als Teil einer ACL in einer Firewall-Einstellung verknüpft werden.

Tabelle 2-1 *Netzwerkadressmakros*

Makro	Beschreibung
[Arp]	Erlaubt ARP-(Address Resolution Protocol-)Pakete. Der Begriff *Address Resolution* (Adressauflösung) bezeichnet den Suchvorgang nach einer Adresse eines Computers in einem Netzwerk. Die Adresse wird mithilfe eines Protokolls aufgelöst, in dem eine Information durch einen auf dem lokalen Computer ausgeführten Clientprozess an einen Serverprozess gesendet wird, der auf einem Remote-Computer ausgeführt wird. Die vom Server empfangenen Informationen ermöglichen es dem Server, eindeutig das Netzwerksystem zu identifizieren, für das die Adresse angefordert wurde, um so die gewünschte Adresse bereitzustellen. Der Adressauflösungsvorgang wird abgeschlossen, wenn der Client vom Server eine Antwort mit der angeforderten Adresse erhält.
[Icmp]	Erlaubt ICMP-(Internet Control Message Protocol-)Pakete. ICMPs werden von Routern, zwischengeschalteten Geräten oder Hosts verwendet, um Aktualisierungen oder Fehlerinformationen an andere Router, zwischengeschaltete Geräte oder Hosts zu übermitteln. ICMP-Meldungen werden in mehreren Situationen gesendet: etwa, wenn ein Datagramm sein Ziel nicht erreichen kann, das Gateway nicht über die Pufferkapazität zur Weiterleitung eines Datagramms verfügt und wenn das Gateway den Host anweisen kann, Datenverkehr auf einer kürzeren Route zu senden.
[IpMulticast]	Erlaubt IP-Multicast-Pakete. Multicast ist eine Bandbreiten-konservierende Technologie, die den Verkehr reduziert, indem sie gleichzeitig einen einzelnen Informationsstrom an Tausende von Empfängern im Unternehmen und daheim liefert. Anwendungen, die Multicast nutzen, sind Videokonferenzen, Unternehmenskommunikation, Fernkurse sowie Verteilung von Software, Börsenkursen und Nachrichten. Multicast-Pakete können mit IP- oder Ethernet-Adressen verteilt werden.
[EthernetMulticast]	Erlaubt Ethernet-Multicast-Pakete.
[IpSubnetBrdcast]	Erlaubt Subnet-Broadcast-Pakete. Subnet-Broadcasts werden verwendet, um Pakete an alle Hosts eines Netzwerks zu senden, das Subnetze oder Supernetze besitzt oder auf andere Weise außerhalb der normalen Klasseneinteilung liegt. Alle Hosts eines Netzwerks außerhalb der normalen Klasseneinteilung, die den Eingang von Paketen überwachen und Pakete verarbeiten, die an die Subnet-Broadcast-Adresse gesendet werden.
[Snap]	Erlaubt Snap-kodierte Pakete.
[LLC]	Erlaubt LLC-kodierte Pakete.

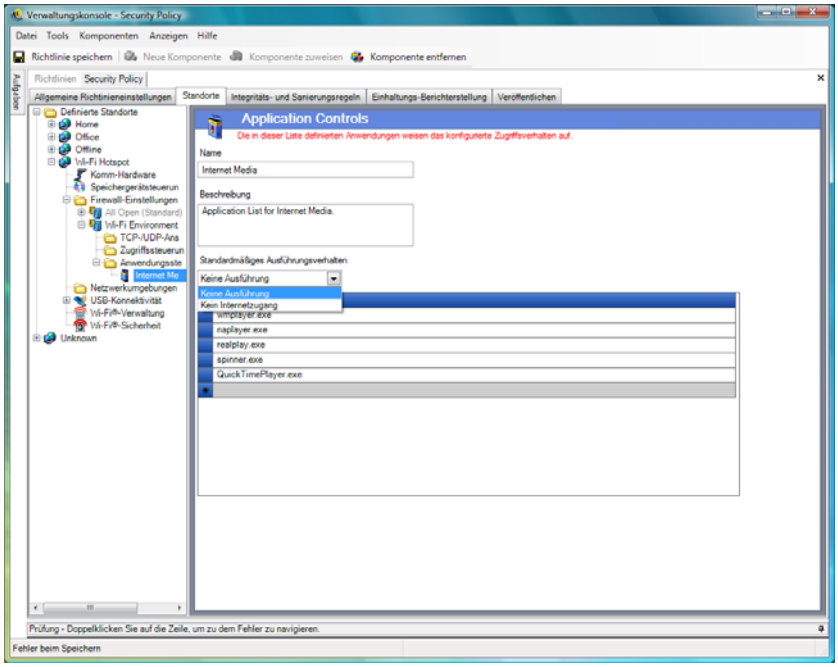
Makro	Beschreibung
[Allow8021X]	Erlaubt 802.1x-Pakete. Um Defizite in Wired Equivalent Privacy (WEP) - Schlüsseln zu überwinden, nutzen Microsoft und andere Unternehmen 802.1x als alternative Authentifizierungsmethode. 802.1x ist eine portbasierte Netzwerk-Zugriffsteuerung, bei der Extensible Authentication Protocol (EAP) oder Zertifikate zum Einsatz kommen. Derzeit unterstützen die meisten Hersteller von Wireless-Karten und viele Hersteller von Zugriffspunkten 802.1x. Diese Einstellung erlaubt auch Light Extensible Authentication Protocol- (LEAP) und WiFi Protected Access- (WPA) Authentifizierungspakete.
[Gateway]	Repräsentiert die Standard-Gateway-Adresse der aktuellen IP-Konfiguration. Wenn dieser Wert eingegeben wird, erlaubt der ZENworks Security Client sämtlichen Netzwerkverkehr vom Standard-Gateway der aktuellen IP-Konfiguration als verbürgte ACL.
[GatewayAll]	Wie [Gateway], jedoch für alle definierten Gateways.
[Wins]	Repräsentiert die Standard-WINS-Server-Adresse der aktuellen Client-IP-Konfiguration. Wenn dieser Wert eingegeben wird, erlaubt der ZENworks Security Client sämtlichen Netzwerkverkehr vom Standard-WINS-Server der aktuellen IP-Konfiguration als verbürgte ACL.
[WinsAll]	Wie [Wins], jedoch für alle definierten WINS-Server.
[Dns]	Repräsentiert die Standard-DNS-Server-Adresse der aktuellen Client-IP-Konfiguration. Wenn dieser Wert eingegeben wird, erlaubt der ZENworks Security Client sämtlichen Netzwerkverkehr vom Standard-DNS-Server der aktuellen IP-Konfiguration als verbürgte ACL.
[DnsAll]	Wie [Dns], jedoch für alle definierten DNS-Server.
[Dhcp]	Repräsentiert die Standard-DHCP-Server-Adresse der aktuellen Client-IP-Konfiguration. Wenn dieser Wert eingegeben wird, erlaubt der ZENworks Security Client sämtlichen Netzwerkverkehr vom Standard-DHCP-Server der aktuellen IP-Konfiguration als verbürgte ACL.
[DhcpAll]	Wie [Dhcp], jedoch für alle definierten DHCP-Server.

Anwendungssteuerungselemente

Diese Funktion ermöglicht es dem Administrator, für Anwendungen den Netzwerkzugriff zu blockieren oder einfach ihre Ausführung ganz zu verhindern.

Hinweis: Diese Funktion steht nur bei der ZENworks Endpoint Security-Installation zur Verfügung und kann für UWS-(Unlimited Web Solutions-)Sicherheitsrichtlinien nicht verwendet werden.

Für den Zugriff auf dieses Steuerelement klicken Sie auf die Registerkarte *Standorte*, klicken Sie auf das "+"-Symbol neben *Firewall-Einstellungen*, klicken Sie auf das "+"-Symbol neben der gewünschten Firewall und klicken Sie dann im Richtlinienbaum auf der linken Seite auf das Symbol für *Anwendungssteuerelemente*.



So legen Sie eine neue Einstellung für Anwendungssteuerungselemente fest:

1. Klicken Sie im Komponentenbaum mit der rechten Maustaste auf *Anwendungssteuerelemente* und wählen Sie dann die Option zum Hinzufügen neuer Anwendungssteuerelemente.
2. Geben Sie einen Namen und eine Beschreibung für die Liste der Anwendungssteuerelemente ein.
3. Wählen Sie ein Ausführungsverhalten aus. Dieses Verhalten wird auf alle aufgelisteten Anwendungen angewendet. Wenn mehrere Verhaltensweisen erforderlich sind (Beispiel: Einigen Netzwerkanwendungen wird der Netzwerkzugriff verweigert, allen Anwendungen für die Dateifreigabe hingegen die Ausführung), müssen mehrere Anwendungssteuerelemente definiert werden. Aktivieren Sie einen der folgenden Parameter:
   - **Alle erlaubt:** Alle aufgelisteten Anwendungen dürfen ausgeführt werden und auf das Netzwerk zugreifen.
   - **Keine Ausführung:** Keine der aufgelisteten Anwendungen darf ausgeführt werden.
   - **Kein Netzwerkzugriff:** Keine der aufgelisteten Anwendungen darf auf das Netzwerk zugreifen. Anwendungen (z. B. Webbrowser), die von einer anderen Anwendung aus aufgerufen werden, dürfen ebenfalls nicht auf das Netzwerk zugreifen.

   Hinweis: Das Blockieren des Netzwerkzugriffs hat keinen Einfluss auf das Speichern von Dateien auf zugeordnete Netzwerklaufwerke. Benutzer dürfen auf allen Netzlaufwerken speichern, die ihnen zur Verfügung stehen.

   ---
4. Geben Sie jede zu blockierende Anwendung an. Es muss eine Anwendung pro Zeile eingegeben werden.

   Wichtig: Das Blockieren der Ausführung von wichtigen Anwendungen kann sich negativ auf den Systembetrieb auswirken. Blockierte Microsoft Office-Anwendungen versuchen, ihre Installationsprogramme auszuführen.

   ---
5. Klicken Sie auf *Richtlinie speichern*.

So verknüpfen Sie eine vorhandene Anwendungssteuerungselementliste mit dieser Firewall-Einstellung:

1. Wählen Sie "Anwendungssteuerelemente" im Komponentenbaum aus und klicken Sie dann auf die Schaltfläche *Komponente verknüpfen*.
2. Wählen Sie einen·Anwendungssatz in der Liste aus.
3. Konfigurieren Sie die Anwendungen und den Beschränkungsgrad nach Bedarf.

   Hinweis: Wenn Sie die Einstellungen in einer freigegebenen Komponente ändern, beeinflusst dies alle Instanzen dieser Komponente. Mithilfe des Befehls *Auslastung anzeigen* können alle anderen mit dieser Komponente verknüpften Richtlinien angezeigt werden.

4. Klicken Sie auf *Richtlinie speichern*.

Die verfügbaren Anwendungssteuerelemente sind·nachfolgend aufgeführt. Das Standardverhalten bei der Ausführung ist "Kein Netzwerkzugriff".

Tabelle 2-2 *Anwendungssteuerungselemente*

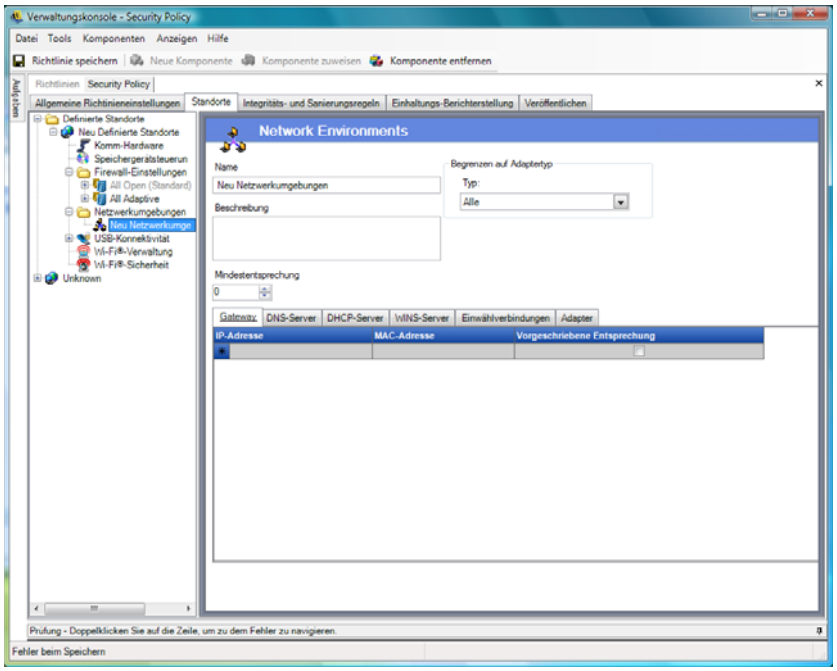
Name	Anwendungen
Webbrowser	explore.exe; netscape.exe; netscp.exe
Instant Messaging	aim.exe; icq.exe; msmsgs.exe; msnmsgr.exe; trillian.exe; ypager.exe
Dateifreigabe	blubster.exe; grokster.exe; imesh.exe; kazaa.exe; morpheus.exe; napster.exe; winmx.exe
Internet-Medien	mplayer2.exe; wmplayer.exe; naplayer.exe; realplay.exe; spinner.exe; QuickTimePlayer.exe

Wenn dieselbe Anwendung zu zwei unterschiedlichen Anwendungssteuerelementen in derselben Firewall-Einstellung hinzugefügt wird (Beispiel: Die Ausführung von `kazaa.exe` wird in einem Anwendungssteuerelement blockiert, und in einem anderen definierten Anwendungssteuerelement unter derselben Firewall-Einstellung wird der Netzwerkzugriff für kazaa.exe blockiert.), wird die strikteste·Steuerung für die entsprechende ausführbare Datei (Anwendung) angewendet (in diesem Beispiel würde die Ausführung von kazaa blockiert).

Netzwerkumgebungen

Wenn die Netzwerkparameter (Gateway-Server, DNS-Server, DHCP-Server, WINS-(Windows Internet Naming Service-)Server, verfügbare Zugriffspunkte und spezifische Adapterverbindungen) für einen Standort bekannt sind, können die Servicedetails (IP und MAC), die der Identifizierung des Netzwerks dienen, in die Richtlinie eingegeben werden, um den sofortigen Standortwechsel zu ermöglichen, ohne dass der Benutzer die Umgebung als Standort speichern muss.

Für den Zugriff auf dieses Steuerelement klicken Sie auf die Registerkarte *Standorte* und klicken Sie im Richtlinienbaum auf der linken Seite auf den Ordner *Netzwerkumgebungen*.



Anhand der Listen kann der Administrator definieren, welche Netzwerkservices in der Umgebung vorhanden sind. Jeder Netzwerkservice kann mehrere Adressen umfassen. Der Administrator bestimmt, wie viele der Adressen in der Umgebung übereinstimmen müssen, damit der Standortwechsel aktiviert wird.

In jeder Netzwerkumgebungsdefinition müssen mindestens zwei Standortparameter angegeben werden.

So definieren Sie eine Netzwerkumgebung:

1. Wählen Sie im Komponentenbaum den Eintrag *Netzwerkumgebungen* aus und klicken Sie dann auf die Schaltfläche *Neue Komponente*.
2. Benennen Sie die Netzwerkumgebung und geben Sie eine Beschreibung ein.
3. Wählen Sie in der Dropdown-Liste zur Einschränkung auf den Adaptertyp den Adaptertyp aus, der auf diese Netzwerkumgebung zugreifen darf:
   - Wireless
   - Alle
   - Modem
   - Wired
   - Wireless
4. Geben Sie an, wie viele Netzwerkservices zur Identifizierung dieser Netzwerkumgebung mindestens erforderlich sind.

   Jede Netzwerkumgebung weist eine Mindestanzahl an Adressen auf, anhand derer die Identifizierung durch den ZENworks Security Client erfolgt. Die unter *Mindestentsprechung* angegebene Anzahl darf die Gesamtzahl der Netzwerkadressen nicht überschreiten, die in den Registerkartenlisten als erforderlich angegeben werden. Geben Sie an, wie viele Netzwerkservices zur Identifizierung dieser Netzwerkumgebung mindestens erforderlich sind.

5 Geben Sie für jeden Service folgende Informationen an:

- **IP-Adresse:** Geben Sie bis zu 15 Zeichen an, die sich nur aus den Zahlen 0–9 und Punkten zusammensetzen. Zum Beispiel 123.45.6.789
- **MAC-Adresse:** Sie können auch bis zu 12 Zeichen angeben, die sich nur aus den Zahlen 0–9 und den Buchstaben A–F (Groß- und Kleinbuchstaben) zusammensetzen und durch Doppelpunkte getrennt sind. Beispiel: 00:01:02:34:05:B6
- Aktivieren Sie das Kontrollkästchen *Muss entsprechen*, wenn die Identifizierung dieses Service für die Definition der Netzwerkumgebung erforderlich ist.

6 Machen Sie für die Registerkarten *Einwählverbindungen* und *Karten* folgende Angaben:

- Geben Sie bei *Einwählverbindungen* den Namen des RAS-(Remote Access Services-)Eintrags aus dem Telefonbuch bzw. die gewählte Nummer an.

  Hinweis: Telefonbucheinträge müssen alphanumerische Zeichen enthalten und dürfen nicht nur aus Sonderzeichen (@, #, $, -, % usw.) bestehen. oder Ziffern (1-9) bestehen. Einträge, die nur aus Sonderzeichen und Ziffern bestehen, werden als gewählte Nummern angesehen.

- Geben Sie bei "Karten" die SSID für die einzelnen zulässigen Karten an. Karten können angegeben werden, um ganz genau zu beschränken, welche Karten auf diese Netzwerkumgebung zugreifen können. Werden keine SSIDs eingegeben, wird allen Adaptern des zulässigen Typs Zugriff gewährt.

So verknüpfen Sie eine bestehende Netzwerkumgebung mit diesem Standort:

Hinweis: Das Verknüpfen einer einzelnen Netzwerkumgebung mit zwei oder mehr Standorten in derselben Sicherheitsrichtlinie führt zu unvorhergesehenen Ergebnissen und wird nicht empfohlen.

1 Wählen Sie im Komponentenbaum den Eintrag *Netzwerkumgebungen* aus und klicken Sie dann auf die Schaltfläche *Komponente verknüpfen*.

2 Wählen Sie die Netzwerkumgebungen in der Liste aus.

3 Konfigurieren Sie die Umgebungsparameter nach Bedarf.

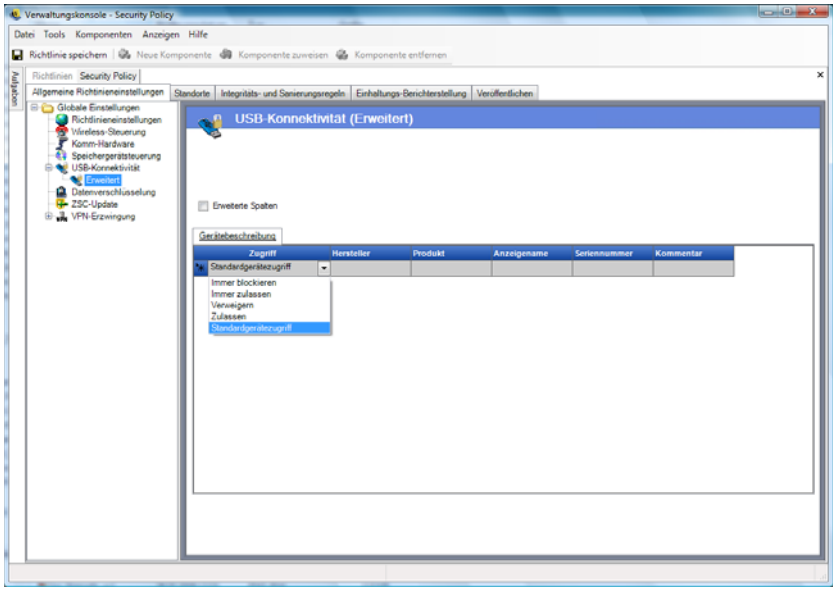
Hinweis: Wenn Sie die Einstellungen in einer freigegebenen Komponente ändern, beeinflusst dies alle Instanzen dieser Komponente. Mithilfe des Befehls *Auslastung anzeigen* können alle anderen mit dieser Komponente verknüpften Richtlinien angezeigt werden.

4 Klicken Sie auf *Richtlinie speichern*.

USB-Konnektivität

Sämtliche Geräte, die über den USB-BUS eine Verbindung aufbauen, können nach Richtlinie erlaubt oder verweigert werden. Diese Geräte können aus dem USB-Gerätinventarbericht per Absuche in die Richtlinie übernommen werden; eine weitere Möglichkeit ist die Absuche aller Geräte, die derzeit mit einem Computer verbunden sind. Diese Geräte können basierend auf Hersteller, Produktname, Seriennummer, Typ usw. gefiltert werden. Zu Supportzwecken kann der Administrator die Richtlinie so konfigurieren, dass ein Satz Geräte akzeptiert wird, entweder nach Herstellertyp (Beispiel: alle HP-Geräte sind zulässig) oder nach Produkttyp (alle USB-Eingabegeräte, etwa Maus und Tastatur, sind zulässig). Zudem können einzelne Geräte erlaubt werden, um zu verhindern, dass nicht unterstützte Geräte Bestandteil des Netzwerks werden (Beispiel: mit Ausnahme des Druckers in der Richtlinie sind keine Drucker zulässig).

Für den Zugriff auf dieses Steuerelement wechseln Sie zur Registerkarte *Allgemeine Richtlinieneinstellungen* und klicken Sie dann im Richtlinienbaum auf der linken Seite auf *USB-Konnektivität*.



Geben Sie an, ob der Zugriff auf nicht in der Liste enthaltene Geräte erlaubt oder verweigert werden soll.

Mithilfe der folgenden Methoden können Sie die Liste ausfüllen und dann angeben, ob Sie die USB-Konnektivität für Geräte zulassen oder verweigern.

- „Manuelles Hinzufügen von Geräten“ auf Seite 94
- „Importieren von Gerätelisten“ auf Seite 95

Manuelles Hinzufügen von Geräten

1. Verbinden Sie das Gerät mit dem USB-Anschluss des Computers, auf dem die Verwaltungskonsole installiert ist.
2. Wenn das Gerät bereit ist, klicken Sie auf die Schaltfläche für die Absuche. Verfügt das Gerät über eine Seriennummer, werden die zugehörige Beschreibung und Seriennummer in der Liste aufgeführt.
3. Wählen Sie in der Dropdown-Liste eine Einstellung aus (die Einstellung für das globale Wechselspeichergerät findet bei dieser Richtlinie keine Anwendung):
   - **Aktivieren:** Den Geräten in der Bevorzugt-Liste werden uneingeschränkte Lese-/Schreibrechte erteilt, alle anderen USB-Geräte und alle anderen externen Speichergeräte werden deaktiviert.
   - **Nur Lesen:** Den Geräten in der Bevorzugt-Liste wird das Recht "Nur Lesen" erteilt, alle anderen USB-Geräte und anderen externen Speichergeräte werden deaktiviert.

Wiederholen Sie diese Schritte für sämtliche Geräte, die gemäß dieser Richtlinie zulässig sind. Auf sämtliche Geräte wird dieselbe Einstellung angewendet.

Importieren von Gerätelisten

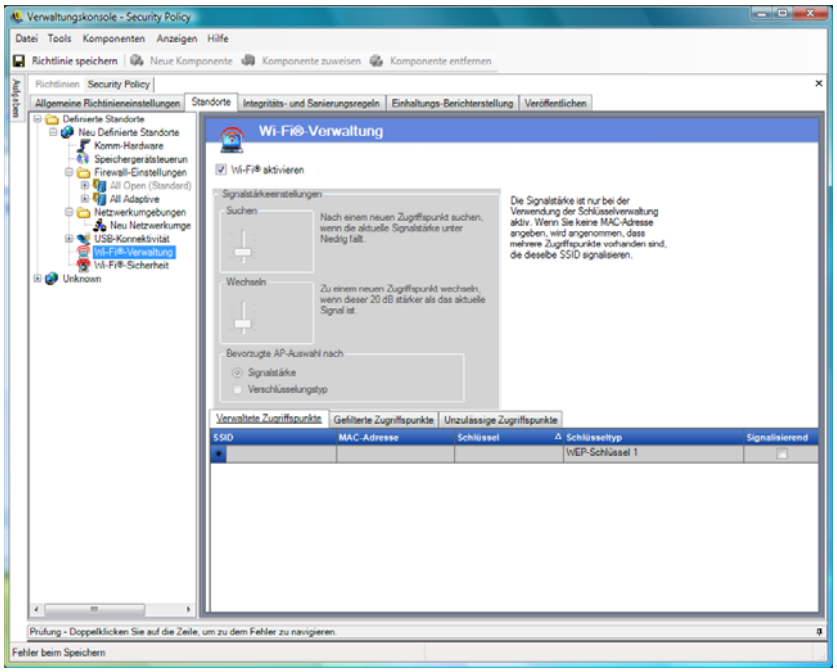
Der Novell-USB-Laufwerkscanner generiert eine Liste mit Geräten und deren Seriennummer (Abschnitt 1.11, „USB-Laufwerkscanner“, auf Seite 44). Wenn Sie diese Liste importieren möchten, klicken Sie auf *Importieren* und begeben Sie sich zu der Liste. Daraufhin werden die Felder *Beschreibung* und *Seriennummer* ausgefüllt.

Wi-Fi-Verwaltung

Im Rahmen der Wi-Fi-Verwaltung kann der Administrator Listen mit Zugriffspunkten erstellen. Durch die in diese Listen aufgenommenen Wireless-Zugriffspunkte wird bestimmt, mit welchen Zugriffspunkten der Endpunkt am Standort eine Verbindung herstellen darf. Zudem wird hiermit festgelegt, welche Zugriffspunkte für den Endpunkt in Zero Configuration Manager (Zero Config) von Microsoft angezeigt werden. Drittanbieter-Manager für die Wireless-Konfiguration werden für diese Funktionalität nicht unterstützt. Wenn keine Zugriffspunkte eingegeben werden, stehen dem Endpunkt alle Zugriffspunkte zur Verfügung.

Für den Zugriff auf dieses Steuerelement klicken Sie auf die Registerkarte *Standorte* und klicken Sie dann im Richtlinienbaum auf der linken Seite auf *Wi-Fi-Verwaltung*.

Hinweis: Wird im Bereich für die Wi-Fi-Sicherheit oder die Wi-Fi-Verwaltung die Auswahl der Option *Aktivieren* aufgehoben, wird jegliche Wi-Fi-Konnektivität an diesem Standort deaktiviert.



Durch die Eingabe von Zugriffspunkten in die Liste *Verwaltete Zugriffspunkte* wird Zero Config deaktiviert und der Endpunkt wird gezwungen, nur eine Verbindung mit den Zugriffspunkten herzustellen, wenn sie verfügbar sind. Wenn die verwalteten Zugriffspunkte nicht zur Verfügung stehen, nutzt der ZENworks Security Client wieder die Liste der gefilterten Zugriffspunkte (Fallback). Zugriffspunkte, die in die Liste der unzulässigen·Zugriffspunkte eingegeben wurden, werden in Zero Config unter keinen Umständen angezeigt.

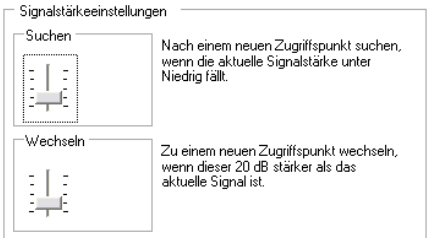
Hinweis: Die Liste mit den Zugriffspunkten wird nur unter dem Betriebssystem Windows* XP unterstützt. Vor der Bereitstellung einer Liste mit Zugriffspunkten wird empfohlen, dass an sämtlichen Endpunkten die Liste der bevorzugten Netzwerke aus Zero Config gelöscht wird.

Die folgenden Abschnitte enthalten weitere Informationen:

- „Einstellungen für die Wi-Fi-Signalstärke“ auf Seite 96
- „Verwaltete Zugriffspunkte“ auf Seite 97
- „Gefilterte Zugriffspunkte“ auf Seite 98
- „Unzulässige Zugriffspunkte“ auf Seite 98

Einstellungen für die Wi-Fi-Signalstärke

Wenn in der Liste mehr als ein WEP-verwalteter Zugriffspunkt definiert ist, kann die Signalstärken-Umschaltung für den Wi-Fi-Adapter festgelegt werden. Die Schwellenwerte für die Signalstärke können nach Standort angepasst werden, um zu bestimmen, wann der ZENworks Security Client nach einem anderen in der Liste definierten Zugriffspunkt sucht, ihn verwirft bzw. zu ihm wechselt.



Folgende Informationen können angepasst werden:

- **Search:** Wenn die Signalstärke diesen Grad erreicht, beginnt der ZENworks Security Client mit der Suche nach einem neuen Zugriffspunkt, mit dem eine Verbindung hergestellt werden kann. "Niedrig" [-70 dB] ist die Standardeinstellung.
- **Switch:** Damit der ZENworks Security Client die Verbindung mit einem neuen Verbindungspunkt herstellen kann, muss die Rundsendung dieses Zugriffspunkts mit der angegebenen Signalstärke erfolgen (oberhalb der aktuellen Verbindung). Die Standardeinstellung ist +20 dB.

Die Schwellenwerte für die Signalstärke werden anhand der Leistung (in dB) bestimmt, die vom Miniport-Treiber des Computers gemeldet wird. Da die dB-Signale hinsichtlich der Received Signal Strength Indication (RSSI, Angabe der Funksignalstärke) von jeder Wi-Fi-Karte und jedem Radio anders verarbeitet werden, können die Werte von Adapter zu Adapter unterschiedlich sein.

Sie können basierend auf folgenden Kriterien die von Ihnen bevorzugte Zugriffspunktauswahl festlegen:

- Signalstärke
- Verschlüsselungstyp

Die Standardwerte, die den definierten Schwellenwerten in der Verwaltungskonsole zugeordnet sind, sind für die meisten Wi-Fi-Adapter zutreffend. Es empfiehlt sich, die RSSI-Werte Ihrer Wi-Fi-Karte zu ermitteln, um den genauen Grad eingeben zu können. Die Novell-Werte lauten:

Name	Standardwert
Ausgezeichnet	-40 dB
Sehr gut	-50 dB
Gut	-60 dB
Niedrig	-70 dB
Sehr niedrig	-80 dB

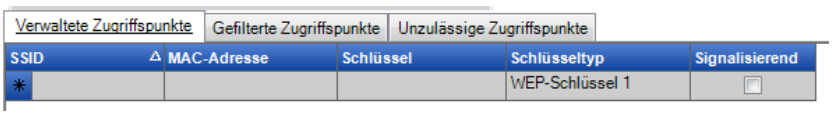
Hinweis: Obwohl die oben angegebenen Signalstärkenbezeichnungen denen entsprechen, die vom Zero Configuration Service von Microsoft verwendet werden, ist dies bei den Schwellenwerten möglicherweise nicht der Fall. Zero Config ermittelt die Werte basierend auf dem Störabstand (Signal to Noise Ratio, SNR), nicht nur auf dem von RSSI gemeldeten dB-Wert. Angenommen, ein Wi-Fi-Adapter empfängt ein Signal mit -54 dB und weist einen Störpegel von -22 dB auf, dann wird der Störabstand als 32 dB (-54 - -22 = 32) gemeldet, was laut der Zero Configuration-Skala einer ausgezeichneten Signalstärke entspricht. Auf der Novell-Skala jedoch entspricht das Signal mit -54 dB (falls so vom Miniport-Treiber gemeldet) einer sehr guten Signalstärke.

Wichtiger Hinweis: Für den Endbenutzer werden die Novell-Schwellenwerte für die Signalstärke unter keinen Umständen angezeigt; diese Angaben sollen lediglich verdeutlichen, was für den Benutzer von Zero Config angezeigt wird und was sich hinter den Kulissen tatsächlich abspielt.

Verwaltete Zugriffspunkte

In ZENworks Endpoint Security Management gibt es einen einfachen Prozess für die automatische Verteilung und Anwendung von Wired Equivalent Privacy-(WEP-)Schlüsseln ohne Benutzereingriff (hierbei wird Zero Configuration Manager von Microsoft umgangen und beendet). Die Integrität der Schlüssel bleibt hierbei gewahrt, da sie nicht in Klartext per E-Mail oder Memo weitergegeben werden. Dem Endbenutzer muss der Schlüssel nicht bekannt sein, um die automatische Verbindung zum Zugriffspunkt herzustellen. Hierdurch wird die potenzielle erneute Verteilung der Schlüssel an nicht autorisierte Benutzer verhindert.

Aufgrund der Sicherheitslücken, die die Shared WEP Key Authentication mit sich bringt, wird von Novell nur die Open WEP Key Authentication unterstützt. Bei der Shared Authentication sendet der Bestätigungsprozess für den Client-/Zugriffspunkt-Schlüssel sowohl eine unverschlüsselte als auch eine verschlüsselte Version eines Herausforderungssatzes, der ohne Mühe drahtlos ausspioniert werden kann. Auf diese Weise kann ein Hacker sowohl in den Besitz der unverschlüsselten Version (Klartextversion) als auch der verschlüsselten Version eines Satzes gelangen. Sobald ihm diese Information zur Verfügung steht, ist das Knacken des Schlüssels ein Kinderspiel.



Geben Sie für jeden Zugriffspunkt·folgende Informationen an:

- **SSID:** Geben Sie die SSID-Nummer an. Bei der SSID-Nummer muss die Groß-/Kleinschreibung beachtet werden.

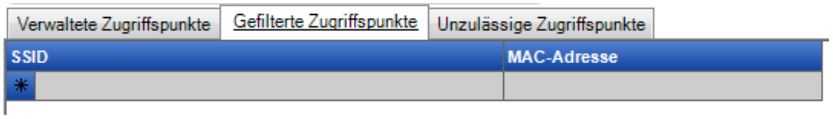
- **MAC-Adresse:** Geben Sie die MAC-Adresse an (wird aufgrund der Häufigkeit unter SSID empfohlen). Erfolgt keine Angabe, wird angenommen, dass es mehrere Zugriffspunkte gibt, die bei Störmeldungen dieselbe SSID verwenden.
- **Tasten:** Geben Sie den WEP-Schlüssel für den Zugriffspunkt an (10 oder 26 Hexadezimalzeichen).
- **Schlüsseltyp:** Geben Sie den Verschlüsselungsschlüsselindex an, indem Sie in der Dropdown-Liste die entsprechende Ebene auswählen.
- **Störungsmeldung:** Aktivieren Sie diese Option, wenn der definierte Zugriffspunkt zurzeit seine SSID per Rundsendung bekannt gibt. Wenn es sich um einen Zugriffspunkt handelt, auf den dies nicht zutrifft, belassen Sie diese Option deaktiviert.

Hinweis: Der ZENworks Security Client versucht zunächst, die Verbindung zu den einzelnen störungsmeldenden Zugriffspunkten herzustellen, die in der Richtlinie aufgelistet sind. Wenn kein störungsmeldender Zugriffspunkt gefunden werden kann, versucht der ZENworks Security Client, die Verbindung zu einem nicht störungsmeldenden Zugriffspunkt (Identifizierung anhand der SSID) herzustellen, der in der Richtlinie aufgelistet ist.

Wenn in der Liste *Verwaltete Zugriffspunkte* ein oder mehrere Zugriffspunkte definiert sind, kann die Signalstärken-Umschaltung für den Wi-Fi-Adapter festgelegt werden.

Gefilterte Zugriffspunkte

Die in die Liste *Gefilterte Zugriffspunkte* eingegebenen Zugriffspunkte sind die einzigen, die in Zero Config angezeigt werden. Dadurch wird ein Endpunkt daran gehindert, eine Verbindung zu nicht autorisierten Zugriffspunkten herzustellen.

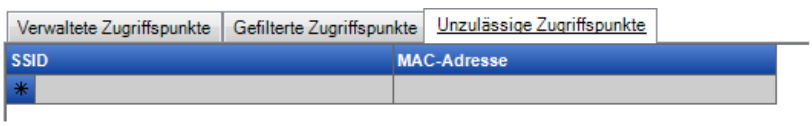


Geben Sie für jeden Zugriffspunkt folgende Informationen ein:

- **SSID:** Geben Sie die SSID-Nummer an. Bei der SSID-Nummer muss die Groß-/Kleinschreibung beachtet werden.
- **MAC-Adresse:** Geben Sie die MAC-Adresse an (wird aufgrund der Häufigkeit unter SSID empfohlen). Erfolgt keine Angabe, wird angenommen, dass es mehrere Zugriffspunkte gibt, die bei Störmeldungen dieselbe SSID verwenden.

Unzulässige Zugriffspunkte

In die Liste *Unzulässige Zugriffspunkte* eingegebene Zugriffspunkte werden in Zero Config nicht angezeigt, und der Endpunkt darf keine Verbindung zu ihnen herstellen.



Geben Sie für jeden Zugriffspunkt·folgende Informationen ein:

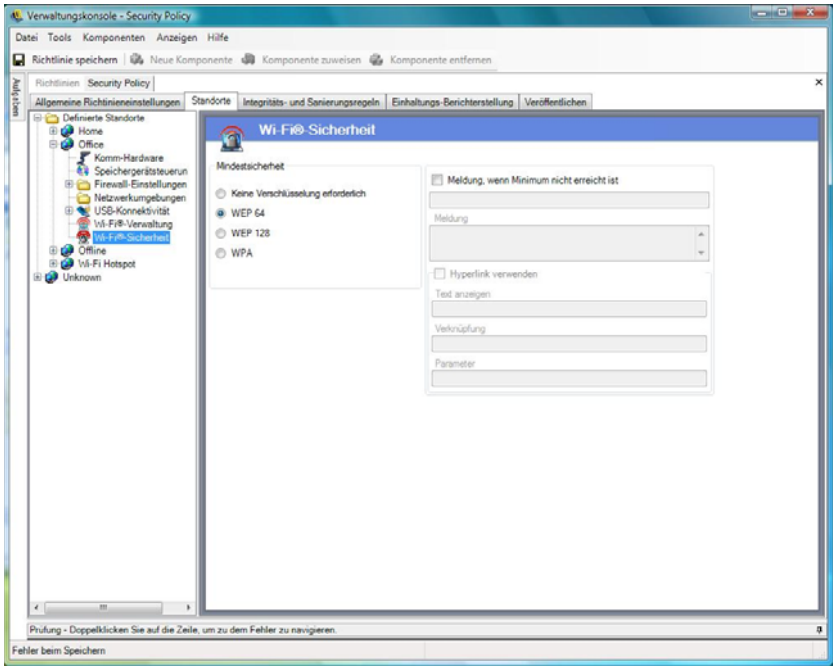
- **SSID:** Geben Sie die SSID-Nummer an. Bei der SSID-Nummer muss die Groß-/Kleinschreibung beachtet werden.
- **MAC-Adresse:** Geben Sie die MAC-Adresse an (wird aufgrund der Häufigkeit unter SSID empfohlen). Erfolgt keine Angabe, wird angenommen, dass es mehrere Zugriffspunkte gibt, die bei Störmeldungen dieselbe SSID verwenden.

Wi-Fi-Sicherheit

Wenn Wi-Fi-Kommunikationshardware (Wi-Fi-Adapter, PCMCIA-Karten oder andere Karten und integrierte Wi-Fi-Radios) global zulässig ist (siehe „Wireless-Steuerung“ auf Seite 53), können zusätzliche Einstellungen auf den Adapter an diesem Standort angewendet werden.

Für den Zugriff auf dieses Steuerelement klicken Sie auf die Registerkarte *Standorte* und klicken Sie dann im Richtlinienbaum auf der linken Seite auf *Wi-Fi-Sicherheit*.

Hinweis: Wird im Bereich für die Wi-Fi-Sicherheit oder die Wi-Fi-Verwaltung die Auswahl der Option *Aktivieren* aufgehoben, wird jegliche Wi-Fi-Konnektivität an diesem Standort deaktiviert.



Der Wi-Fi-Adapter kann so konfiguriert werden, dass er an einem bestimmten Standort nur mit Zugriffspunkten mit einem bestimmten Verschlüsselungsgrad kommuniziert.

Wird beispielsweise eine WPA-Konfiguration von Zugriffspunkten in einer Zweigstelle bereitgestellt, kann der Adapter darauf beschränkt werden, nur mit Zugriffspunkten mit dem Verschlüsselungsgrad WEP 128 (oder einem höheren Grad) zu kommunizieren. So wird verhindert, dass unbeabsichtigt mit fremden Zugriffspunkten kommuniziert wird, die nicht sicher sind.

Es empfiehlt sich, eine benutzerdefinierte Meldung zu verfassen, wenn eine andere (sicherere) Einstellung als die verwendet wird, die besagt, dass keine Verschlüsselung erforderlich ist.

Es kann eine Voreinstellung für den Verbindungsaufbau mit Zugriffspunkten festgelegt werden (nach Verschlüsselungsstufe oder Signalstärke), wenn zwei oder mehr Zugriffspunkte in die Liste der verwalteten und gefilterten Zugriffspunkte aufgenommen werden. Durch die ausgewählte Stufe wird die Konnektivität mit Zugriffspunkten erzwungen, die mindestens die Mindestverschlüsselungsanforderung erfüllen.

Wenn beispielsweise WEP 64 die Verschlüsselungsanforderung ist und die Verschlüsselung ausschlaggebend ist, haben Zugriffspunkte mit dem höchsten Verschlüsselungsgrad Vorrang vor allen anderen. Wenn die Signalstärke ausschlaggebend ist, hat beim Verbindungsaufbau das stärkste Signal Vorrang.

2.2.3 Integritäts- und Behebungsregeln

ZENworks Endpoint Security Management bietet die Möglichkeit, zu überprüfen, ob erforderliche Software am Endpunkt ausgeführt wird, und stellt bei einem negativen Ergebnis sofortige Abhilfeprozeduren zur Verfügung.

Die folgenden Abschnitte enthalten weitere Informationen:

- „Antivirus- und Spyware-Regeln“ auf Seite 100
- „Integritätstests“ auf Seite 102
- „Integritätsprüfungen“ auf Seite 103
- „Erweiterte Skriptregeln“ auf Seite 105

Antivirus- und Spyware-Regeln

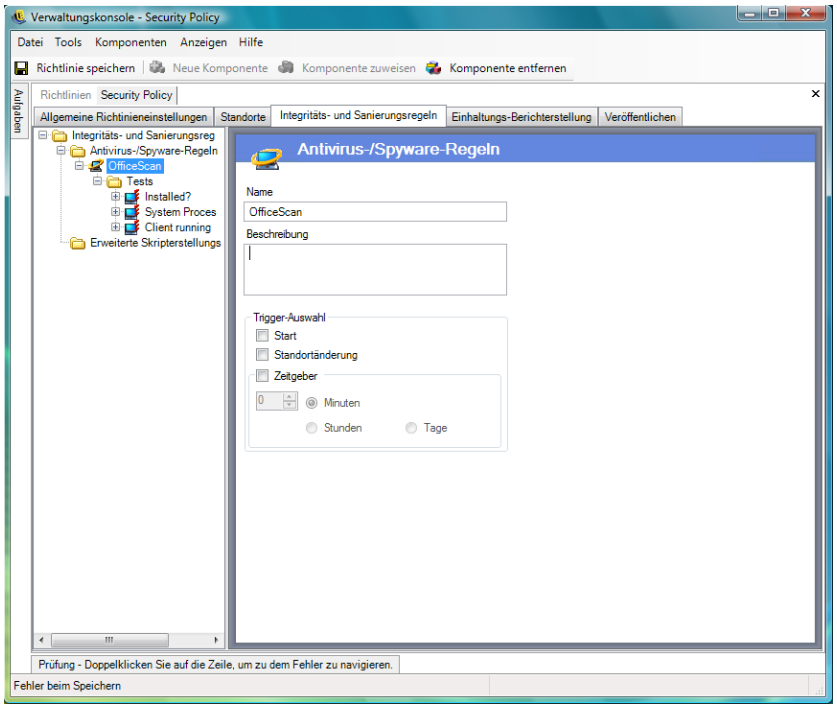
Antivirus- und Spyware-Regeln prüfen, ob vorgesehene Antivirus- oder Spyware-Software am Endpunkt ausgeführt wird und auf dem neuesten Stand ist. Mithilfe von Tests wird ermittelt, ob die Software läuft und die Version aktuell ist. Ein positives Ergebnis beider Prüfungen erlaubt den Wechsel zu einem beliebigen der definierten Standorte. Wenn einer der Tests nicht bestanden wird, kann dies folgende Vorgänge nach sich ziehen (vom Administrator definiert):

- Ein Bericht wird an den Berichtsservice gesendet.
- Eine benutzerdefinierte Meldung wird angezeigt mit einer optionalen Verknüpfung, die Informationen über die Behebung der Regelverletzung bietet.
- Der Benutzer wird in einen Quarantänezustand geschaltet, der seinen Netzwerkzugriff begrenzt und für bestimmte Anwendungen den Zugriff auf das Netzwerk unterbindet; so wird verhindert, dass der Benutzer das Netzwerk weiter infiziert.

Sobald in einem Folgetest festgestellt wird, dass die Endpunkte die Regeln einhalten, gelten für·die Sicherheitseinstellungen automatisch wieder die ursprünglichen Werte.

Hinweis: Diese Funktion steht nur bei der ZENworks Endpoint Security-Installation zur Verfügung und kann für UWS-(Unlimited Web Solutions-)Sicherheitsrichtlinien nicht verwendet werden.

Für den Zugriff auf dieses Steuerelement klicken Sie auf die Registerkarte *Integritäts- und Sanierungsregeln* und klicken Sie dann im Richtlinienbaum auf der linken Seite auf *Antivirus-/Spyware-Regeln*.



Für Software, die sich nicht in der Standardliste befindet, können spezielle Tests definiert werden. Ein einzelner Test kann erstellt werden, der Prüfungen für einen oder mehrere Softwareteile in derselben Regel ausführt. Jede Vornahme der Prüfungen "Prozess läuft" und "Datei vorhanden" hat ihre eigenen Erfolgs- und Fehler-Ergebnisse.

So erstellen Sie eine neue Antivirus- oder Spyware-Regel:

1. Wählen Sie im Komponentenbaum den Eintrag *Antivirus-/Spyware-Regeln* und klicken Sie dann auf die Option zum Erstellen einer neuen Antivirus-/Spyware-Regel.
2. Klicken Sie auf *Neue Komponente*.
3. Geben Sie einen Namen und eine Beschreibung für die Regel ein.
4. Wählen Sie den Auslöser für die Regel aus:
   - **Programmstart:** Führt Tests beim Systemstart aus.
   - **Standortwechsel:** Führt Tests aus, wenn der ZENworks Security Client zu einem anderen Standort wechselt.
   - **Zeitgeber:** Führt Integritätstests gemäß einem definierten Zeitplan (auf Basis von Minute, Stunde oder Tag) aus.
5. Klicken Sie auf *Richtlinie speichern*. Wenn Ihre Richtlinie Fehler aufweist, ziehen Sie Abschnitt 2.2.6, „Fehlerbenachrichtigung“, auf Seite 112 zurate.
6. Definieren Sie die Integritätstests.

So verknüpfen Sie bestehende Antivirus- oder Spyware-Regeln:

1. Wählen Sie *Antivirus-/Spyware-Regeln* aus und klicken Sie dann auf *Komponente verknüpfen*.
2. Wählen Sie die gewünschten Regeln·in der Liste aus.
3. (Optional) Definieren Sie Tests, Überprüfungen und Ergebnisse neu.

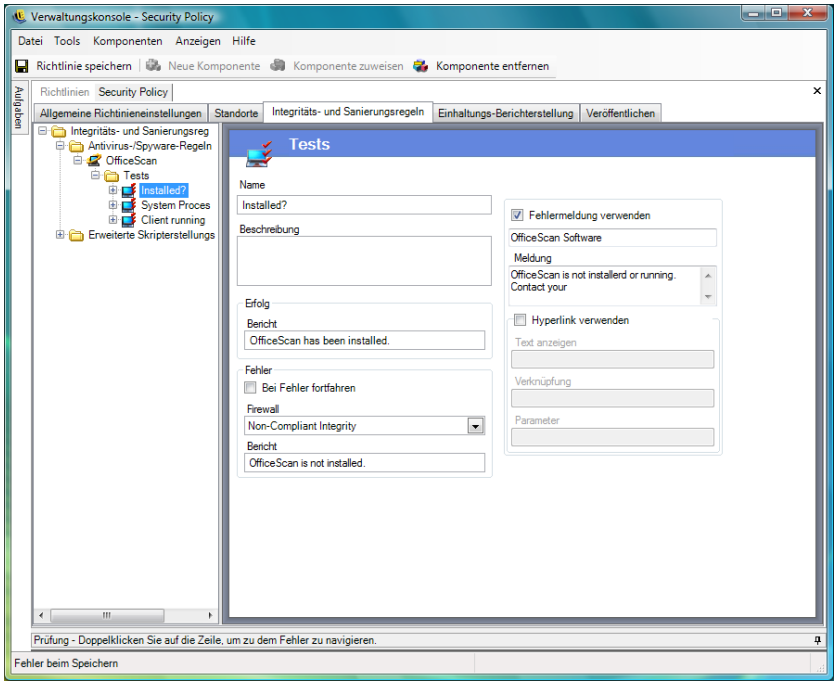
Hinweis: Wenn Sie die Einstellungen in einer freigegebenen Komponente ändern, beeinflusst dies alle Instanzen dieser Komponente. Mithilfe des Befehls *Auslastung anzeigen* können alle anderen mit dieser Komponente verknüpften Richtlinien angezeigt werden.

4 Klicken Sie auf *Richtlinie speichern*. Wenn Ihre Richtlinie Fehler aufweist, ziehen Sie Abschnitt 2.2.6, „Fehlerbenachrichtigung“, auf Seite 112 zurate.

Integritätstests und -prüfungen sind automatisch inbegriffen und können nach Bedarf bearbeitet werden.

Integritätstests

Bei jedem Integritätstest können zwei Überprüfungen vorgenommen werden, *Datei vorhanden* und *Prozess läuft*. Jeder Test erhält seine eigenen Erfolgs- oder Fehlerergebnisse.



Für alle definierten Antivirus- und Spyware-Regeln wurden vorab Standardtests und -prüfungen geschrieben. Zusätzliche Tests können der Integritätsregel hinzugefügt werden.

Mehrere Tests werden in der hier angegebenen Reihenfolge ausgeführt. Der erste Test muss·erfolgreich abgeschlossen sein, bevor der nächste Test ausgeführt wird.

So erstellen Sie einen Integritätstest:

1 Wählen Sie im Komponentenbaum den Eintrag *Integritätstests*, klicken Sie zum Erweitern der Liste neben dem gewünschten Bericht auf das "+"-Symbol, klicken Sie mit der rechten Maustaste auf *Tests* und wählen Sie dann die Option zum Hinzufügen neuer Tests.

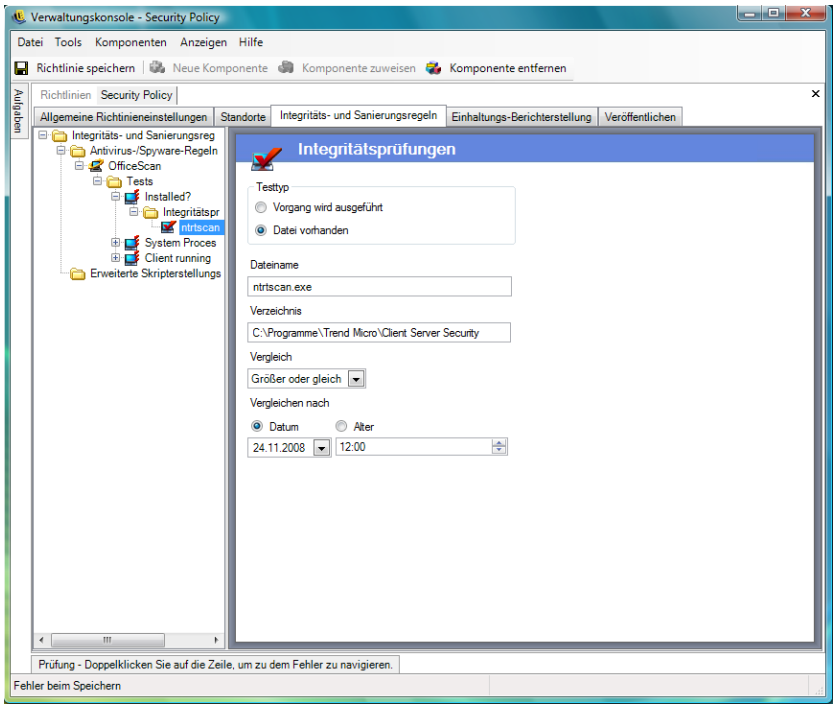
2 Geben Sie einen Namen und eine Beschreibung für den Test ein.

3 Geben Sie den Text für den Erfolgsbericht des Tests ein.

4. Definieren Sie Folgendes für einen Testfehler:
   - **Bei Fehler fortfahren:** Wählen Sie diese Option, wenn die Netzwerkkonnektivität bei Fehlschlag des Tests weiterhin für den Benutzer gegeben sein soll; Sie können auch festlegen, dass der Test wiederholt werden soll.
   - **Firewall:** Diese Einstellung wird angewendet, wenn der Test fehlschlägt. "Alle geschlossen", "Non-compliant Integrity" oder eine benutzerdefinierte Quarantäne-Firewall-Einstellung verhindert, dass der Benutzer eine Verbindung zum Netzwerk herstellen kann.
   - **Nachricht:** Wählen Sie eine benutzerdefinierte Meldung, die bei Fehlschlag des Tests angezeigt werden soll. Diese kann Schritte zur Problembehebung durch den Endbenutzer enthalten.
   - **Bericht:** Geben Sie den Fehlschlag-Bericht an, der an den Berichtsservice gesendet werden soll.
5. Geben Sie eine Fehlschlag-Meldung an. Diese Meldung wird nur angezeigt, wenn eine oder mehrere der Prüfungen nicht bestanden werden. Aktivieren Sie das Kontrollkästchen und geben Sie dann in den dafür vorgesehenen Feldern die Informationen zur Meldung an.
6. Ein Hyperlink kann hinzugefügt werden, über den Abhilfemaßnahmen bereitgestellt werden. Dabei kann es sich um einen Link zu weiteren Informationen oder zum Download eines Patches oder einer Aktualisierung für den nicht bestandenen Test handeln (siehe Abschnitt , „Hyperlinks“, auf Seite 72).
7. Klicken Sie auf *Richtlinie speichern*. Wenn Ihre Richtlinie Fehler aufweist, ziehen Sie Abschnitt 2.2.6, „Fehlerbenachrichtigung“, auf Seite 112 zurate.
8. Definieren Sie die Integritätsprüfungen.
9. Wiederholen Sie die obigen Schritte, um gegebenenfalls einen neuen Antivirus- oder Spyware-Test zu erstellen.

Integritätsprüfungen

Mithilfe der Prüfungen für die einzelnen Tests wird ermittelt, ob einer oder mehrere der Antivirus-/Spyware-Prozesse ausgeführt werden bzw. ob essenzielle Dateien vorhanden sind. Mindestens eine Prüfung muss definiert werden, damit ein Integritätstest ausgeführt werden kann.



Wenn Sie eine neue Prüfung erstellen möchten, klicken Sie im Richtlinienbaum auf der linken Seite mit der rechten Maustaste auf *Integritätsprüfungen* und wählen·Sie dann die Option zum Hinzufügen neuer Integritätsprüfungen. Wählen Sie einen der beiden Prüfungstypen und geben Sie die unten beschriebenen Informationen ein:

Prozess wird ausgeführt: Hiermit kann ermittelt werden, ob die Software (z. B. der AV-Client) zum Zeitpunkt der Ereignisauslösung ausgeführt wird. Die einzige erforderliche Information für diesen Test ist der Name der ausführbaren Datei.

Datei vorhanden: Anhand dieser Prüfung wird festgestellt, ob die Software zum Zeitpunkt des Auslöseereignisses auf dem aktuellen Stand war.

Geben Sie die folgenden Informationen in die entsprechenden Felder ein:

- **Dateiname:** Geben Sie den Namen der Datei an, die Sie überprüfen möchten.
- **Verzeichnis:** Geben Sie das Verzeichnis an, in dem sich die Datei befindet.
- **Vergleich:** Wählen Sie in der Dropdown-Liste einen Datumsvergleich aus:
  - None
  - Gleich
  - Größer oder gleich
  - Kleiner oder gleich
- **Vergleich nach:** Geben Sie *Alter* oder *Datum an*.
  - *Datum* stellt sicher, dass die Datei nicht älter als das angegebene Datum mit Uhrzeit ist (z. B. das Datum der letzten Aktualisierung).
  - *Alter* stellt sicher, dass die·Datei nicht älter als eine bestimmte Zeitspanne, gemessen in Tagen, ist.

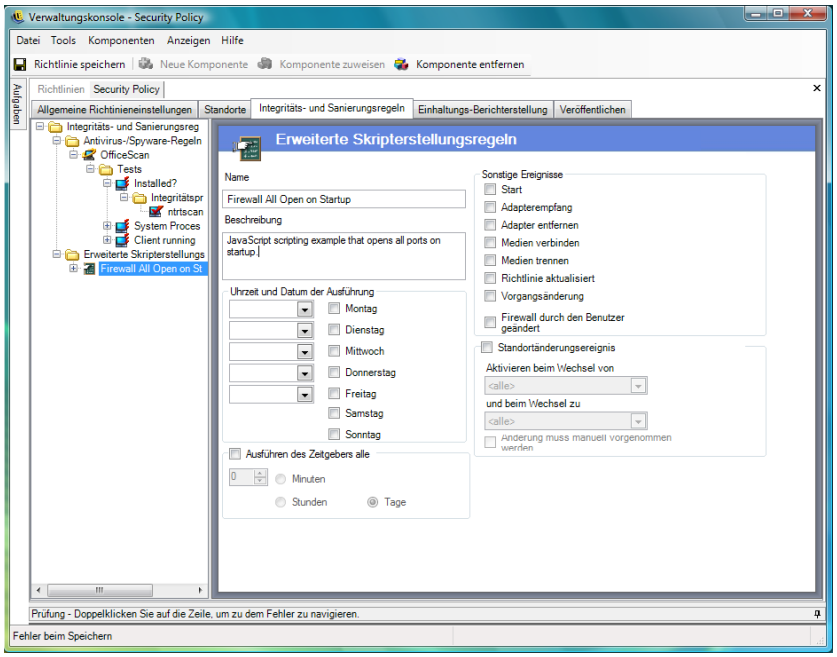
Hinweis: Der Dateivergleich "Gleich" wird bei Verwendung der Altersprüfung als "Kleiner oder gleich" behandelt.

Die Prüfungen werden in der Reihenfolge durchgeführt, in der sie eingegeben werden.

Erweiterte Skriptregeln

ZENworks Endpoint Security Management enthält ein Werkzeug zur erweiterten Regel-Skripterstellung, mit dem Administratoren ausgesprochen·flexible und komplexe Regeln und Abhilfemaßnahmen definieren können.

Für den Zugriff auf dieses Steuerelement klicken Sie auf die Registerkarte *Integritäts- und Sanierungsregeln* und klicken Sie dann im Richtlinienbaum auf der linken Seite auf das Symbol für *Erweiterte Skriptregeln*.



Das Skriptwerkzeug verwendet die gängigen Skriptsprachen VBScript oder JScript zur Erstellung von Regeln, die sowohl einen Auslöser (wann die Regel ausgeführt werden soll) als auch das eigentliche Skript (die Logik der Regel) enthalten. Der Administrator ist nicht auf einen Typ des auszuführenden Skripts eingeschränkt.

Die Implementierung der erweiterten Skripterstellung erfolgt sequenziell, gemeinsam mit anderen Integritätsregeln. Folglich unterbindet ein Skript, dessen Ausführung geraume Zeit in Anspruch nimmt, die Ausführung anderer Regeln (einschließlich zeitlich festgelegter Regeln) so lange, bis dieses Skript abgeschlossen ist.

So erstellen Sie eine neue erweiterte Skriptregel:

1. Klicken Sie im Komponentenbaum mit der rechten Maustaste auf *Erweiterte Skriptregeln* und wählen Sie dann die Option zum Hinzufügen neuer Skriptregeln.
2. Geben Sie einen Namen und eine Beschreibung für die Regel ein.

3 Geben Sie die Auslöse-Ereignisse an.

- **Zeitpunkte und Tage für die Ausführung:** Sie können bis zu fünf unterschiedliche Zeitpunkte für die Skriptausführung angeben. Das Skript wird wöchentlich ausgeführt, und zwar an den ausgewählten Tagen.
- **Zeitgeberausführung alle:** Geben Sie an, wie oft der Zeitgeber ausgeführt werden soll.
- **Sonstige Ereignisse:** Geben Sie die Ereignisse am Endpunkt an, die zur Auslösung des Skripts führen.
- **Ereignis: Standortwechsel:** Geben Sie das Standortwechselereignis an, das zur Auslösung des Skripts führt. Diese Ereignisse sind nicht unabhängig, sondern vielmehr als Ergänzung des vorangegangenen Ereignisses zu verstehen.
  - **Ereignis: Standortprüfung:** Das Skript wird bei jedem Standortwechsel ausgeführt.
  - **Aktivieren bei Wechsel von:** Das Skript wird nur ausgeführt, wenn der Benutzer diesen (angegebenen) Standort verlässt und an einen beliebigen anderen Standort wechselt.
  - **Aktivieren bei Wechsel zu:** Das Skript wird ausgeführt, wenn der Benutzer von einem beliebigen anderen Standort an diesen angegebenen Standort wechselt. Wenn bei *Aktivieren bei Wechsel von* ein Standortparameter angegeben wurde, beispielsweise "Büro", wird das Skript nur ausgeführt, wenn der Standortwechsel vom Büro zu dem angegebenen Standort erfolgt.
  - **Wechsel muss manuell erfolgen:** Das Skript wird nur ausgeführt, wenn der Benutzer den manuellen Standortwechsel vornimmt.

4 Erstellen Sie Skriptvariablen. Weitere Informationen hierzu finden Sie in „Skriptvariablen“ auf Seite 107.

5 Schreiben Sie den Skripttext. Weitere Informationen finden Sie unter „Skripttext“ auf Seite 108.

6 Klicken Sie auf *Richtlinie speichern*. Wenn Ihre Richtlinie Fehler aufweist, ziehen Sie Abschnitt 2.2.6, „Fehlerbenachrichtigung“, auf Seite 112 zurate.

So verknüpfen Sie eine vorhandene erweiterte Skriptregel:

1 Wählen Sie *Erweiterte Skriptregeln* im Komponentenbaum aus und klicken Sie auf *Neue verknüpfen*.

2 Wählen Sie die gewünschten Regeln·in der Liste aus.

3 Definieren Sie Auslöse-Ereignis, Variablen bzw. Skript nach Bedarf neu.

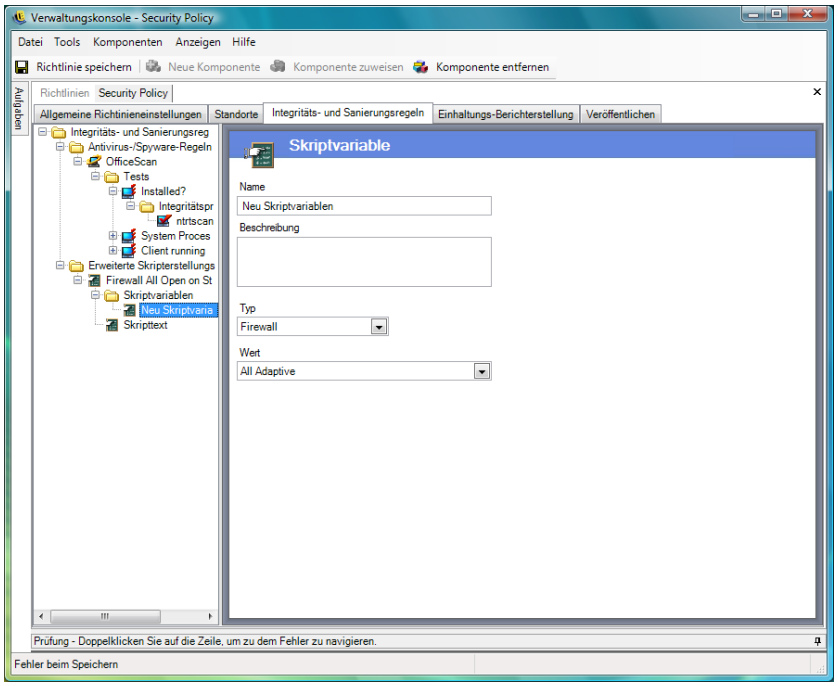
Hinweis: Wenn Sie die Einstellungen in einer freigegebenen Komponente ändern, beeinflusst dies alle Instanzen dieser Komponente. Mithilfe des Befehls *Auslastung anzeigen* können alle anderen mit dieser Komponente verknüpften Richtlinien angezeigt werden.

---

4 Klicken Sie auf *Richtlinie speichern*. Wenn Ihre Richtlinie Fehler aufweist, ziehen Sie Abschnitt 2.2.6, „Fehlerbenachrichtigung“, auf Seite 112 zurate.

Skriptvariablen

Dies ist eine optionale Einstellung, mit welcher der Administrator eine Variable (var) für das Skript definieren kann. Damit hat er die Möglichkeit, ZENworks Endpoint Security Management-Funktionalität zu verwenden (z. B. benutzerdefinierte Meldungen oder Hyperlinks starten, zu einem definierten Standort oder einer Firewall-Einstellung umschalten) oder den Wert einer Variablen zu ändern, ohne das eigentliche Skript zu ändern.



So erstellen Sie eine neue Skriptvariable:

1. Klicken Sie im Komponentenbaum mit der rechten Maustaste auf *Skriptvariablen* und wählen Sie dann die Option zum Hinzufügen neuer Variablen.
2. Geben Sie einen Namen und eine Beschreibung für die Variable ein.
3. Wählen Sie den Typ der Variablen:
   - **Benutzerdefinierte Meldungen:** Definiert eine benutzerdefinierte Meldung, die als Aktion gestartet werden kann.
   - **Firewall:** Definiert eine Firewall-Einstellung, die als Aktion angewendet werden kann.
   - **Hyperlinks:** Definiert einen Hyperlink, der als Aktion gestartet werden kann.
   - **Standort:** Definiert einen Standort, der als Aktion angewendet werden kann.
   - **Nummer:** Definiert einen Zahlenwert.
   - **String:** Definiert einen Zeichenkettenwert.
4. Geben Sie den Wert der Variablen an:
   - Alle adaptiv
   - Alle geschlossen
   - Alle geöffnet

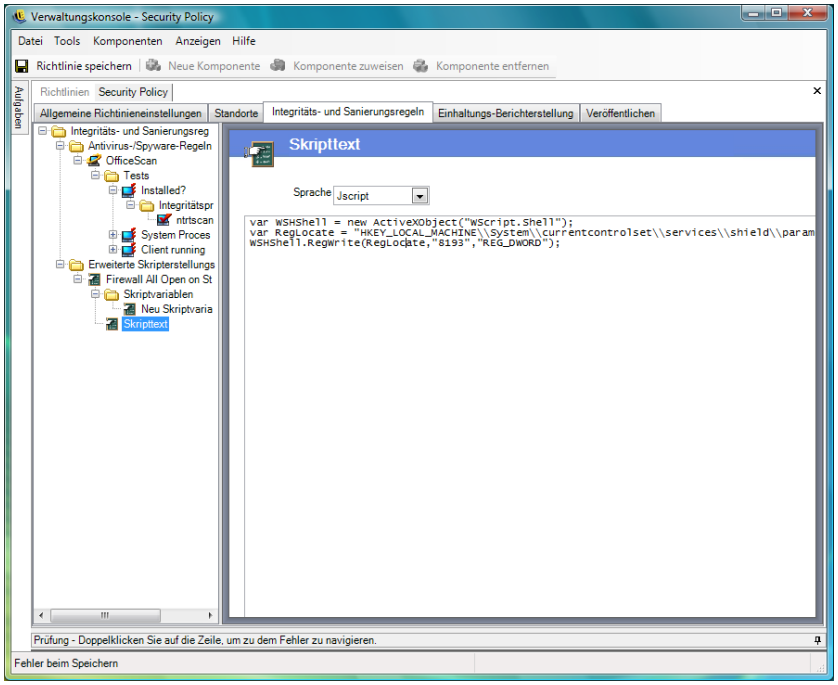
- Neue Firewall-Einstellungen
- Non-Compliant Integrity

5 Klicken Sie auf *Richtlinie speichern*. Wenn Ihre Richtlinie Fehler aufweist, ziehen Sie Abschnitt 2.2.6, „Fehlerbenachrichtigung“, auf Seite 112 zurate.

Skripttext

Der ZENworks Endpoint Security Management-Administrator ist nicht auf den Skripttyp beschränkt, den der ZENworks Security Client ausführen kann. Es empfiehlt sich, sämtliche Skripte zu testen, bevor die Richtlinie verteilt wird.

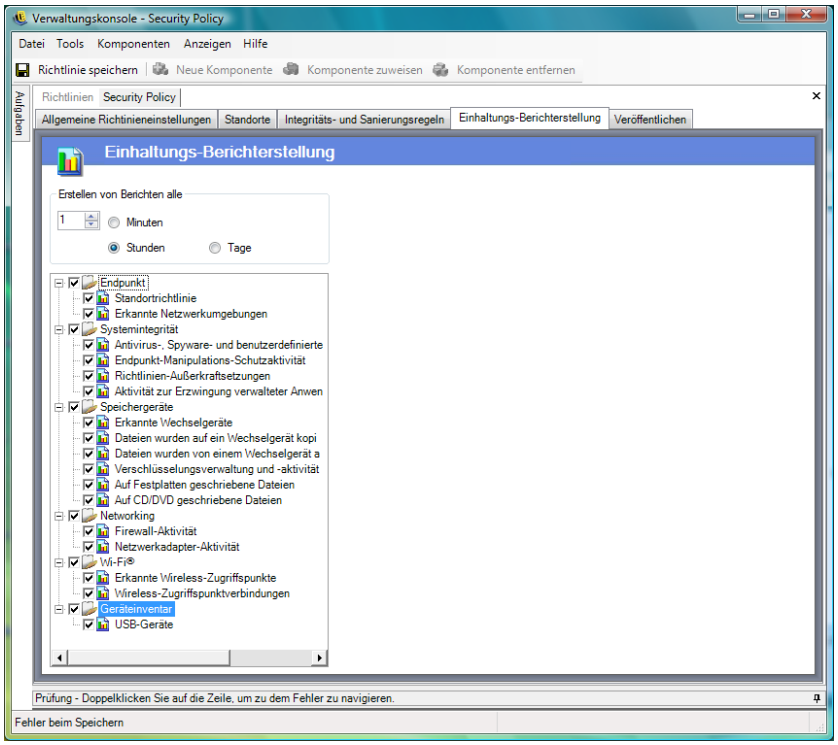
Wählen Sie den Skripttyp aus (Jscript oder VBscript) und geben Sie den Skripttext in das Feld ein. Das Skript kann aus einer anderen Quelle kopiert und in das Feld eingefügt werden.



2.2.4 Einhaltungsberichterstellung

Aufgrund von Ebene und Zugriff der ZENworks Security Client-Treiber kann praktisch jede Transaktion, die der Endpunkt ausführt, in einen Bericht aufgenommen werden. Der Endpunkt kann jedes optionale Systeminventar für Fehlerbehebung und Richtlinienerstellung ausführen. Der Zugriff auf diese Berichte erfolgt über die Registerkarte *Einhaltungs-Berichterstellung*.

Hinweis: Berichterstellung ist nicht verfügbar, wenn die Standalone-Verwaltungskonsole ausgeführt wird.



So führen Sie die Einhaltungs-Berichterstellung für diese Richtlinie durch:

1. Geben Sie an, wie oft Berichte generiert werden sollen. Dies ist die Häufigkeit, mit der das Heraufladen von Daten vom ZENworks Security Client zum Richtlinienverteilungsservice erfolgt.
2. Wählen Sie sämtliche Berichtskategorien bzw. Typen aus, die erfasst werden sollen.

Folgende Berichte stehen zur Verfügung:

Endpunkt

- **Nutzung der Standortrichtlinien:** Der ZENworks Security Client meldet alle erzwungenen Standortrichtlinien und die Dauer dieser Erzwingung.
- **Erkannte Netzwerkumgebungen:** Der ZENworks Security Client meldet alle erkannten Netzwerkumgebungs-Einstellungen.

Systemintegrität

- **Antivirus-, Spyware- und benutzerdefinierte Regeln:** Der ZENworks Security Client meldet die konfigurierten Integritätsmeldungen auf der Basis von Testergebnissen.
- **Schutzaktivität gegen unbefugten Endpunktzugriff:** Der ZENworks Security Client meldet alle Security Client-Manipulationsversuche.
- **Verwaltungsanweisung:** Der ZENworks Security Client meldet alle Versuche, die Verwaltungsanweisung in der Security Client-Instanz zu initiieren.
- **Erzwingungsaktivitäten für verwaltete Anwendungen:** Der ZENworks Security Client meldet alle Aktivitäten zur Erzwingung bei verwalteten Anwendungen.

Speichergeräte

- **Erkannte Wechseldatenträger:** Der ZENworks Security Client meldet alle Wechselspeichergeräte, die von der Security Client-Instanz erkannt wurden.
- **Auf einen Wechseldatenträger kopierte Dateien:** Der ZENworks Security Client meldet Dateien, die auf ein Wechselspeichergerät kopiert werden.
- **Von einem Wechseldatenträger geöffnete Dateien:** Der ZENworks Security Client meldet Dateien, die auf einem Wechselspeichergerät geöffnet werden.
- **Verschlüsselungsverwaltung und -aktivität:** Der ZENworks Security Client meldet Verschlüsselungs-/Entschlüsselungsaktivitäten mit ZENworks Storage Encryption Solution.
- **Auf Festplatten geschriebene Dateien:** Der ZENworks Security Client meldet, wie viele Dateien auf die Festplatten des Systems geschrieben werden.
- **Auf CD-/DVD-Laufwerke geschriebene Dateien:** Der ZENworks Security Client meldet, wie viele Dateien auf die CD-/DVD-Laufwerke des Systems geschrieben werden.

Netzwerke

- **Firewall-Aktivität:** Der ZENworks Security Client meldet sämtlichen Datenverkehr, der von der Firewall blockiert wurde, die für die angewendete Standortrichtlinie konfiguriert wurde.

  Wichtig: Das Aktivieren dieses Berichts kann dazu führen, dass große Datenmengen erfasst werden. Die Daten können sehr schnell zur Überlastung der Datenbank führen. Ein Test von einer·ZENworks Security Client-Instanz ergab 1.115 Daten-Uploads blockierter Pakete in einem Zeitraum von 20 Stunden. Vor der großangelegten Bereitstellung empfiehlt sich eine Überwachungs- und Anpassungsphase mit einem Test-Client in der jeweiligen Umgebung.

- **Netzwerkadapter-Aktivität:** Der ZENworks Security Client meldet alle Datenverkehrsaktivitäten für ein verwaltetes Netzwerkgerät.

Wi-Fi

- **Erkannte Wireless-Zugriffspunkte:** Der ZENworks Security Client meldet alle erkannten Zugriffspunkte.
- **Wireless-Zugriffspunktverbindungen:** Der ZENworks Security Client meldet alle Zugriffspunktverbindungen, die vom Endpunkt erfolgt sind.

Geräteinventar

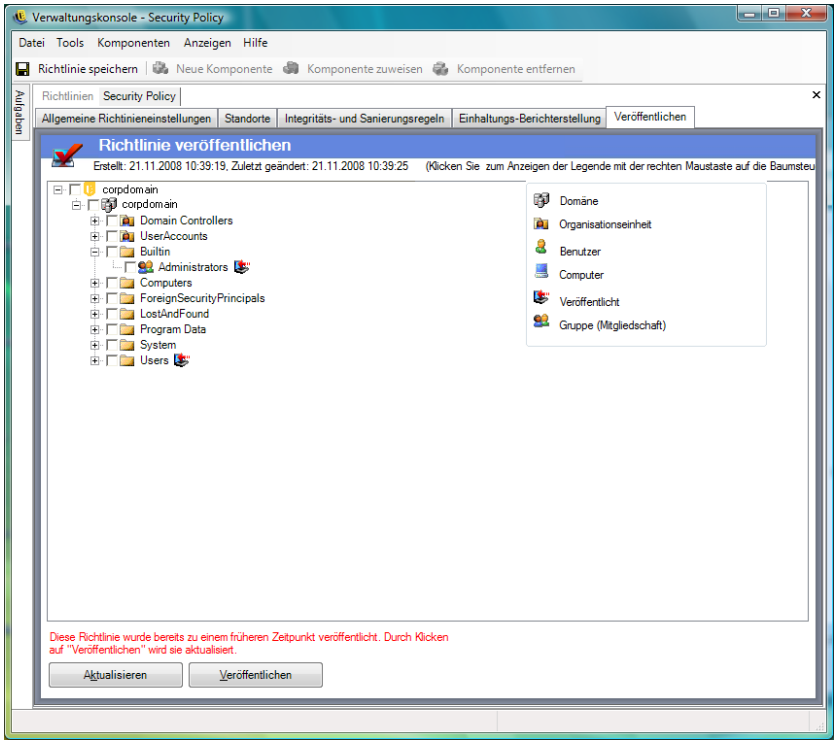
- **USB-Geräte:** Der ZENworks Security Client meldet alle erkannten USB-Geräte im System.

2.2.5 Herausgeben

Fertiggestellte Sicherheitsrichtlinien werden über den Veröffentlichungsmechanismus an Benutzer gesendet. Sobald eine Richtlinie veröffentlicht ist, kann sie weiter aktualisiert werden; die Benutzer erhalten zu diesem Zweck bei geplanten Check-ins Aktualisierungen. Wenn Sie eine Richtlinie veröffentlichen möchten, klicken Sie auf die Registerkarte *Veröffentlichen*. Die folgenden Informationen werden angezeigt:

- Der aktuelle Verzeichnisbaum

- Erstellungs- und Änderungsdatum für die Richtlinie
- Schaltflächen *Aktualisieren* und *Veröffentlichen*



Auf der Basis der aktuellen Veröffentlichungsberechtigungen des Benutzers kann der Verzeichnisbaum eine oder mehrere Auswahlen in Rot anzeigen. Benutzer dürfen keine·Benutzer/Gruppen veröffentlichen, die in Rot angezeigt sind.

Benutzer und ihre verknüpften Gruppen werden erst angezeigt, wenn sie sich beim Verwaltungsdienst authentifiziert haben. Änderungen im Verzeichnisdienst des Unternehmens werden eventuell nicht sofort in der Verwaltungskonsole angezeigt. Klicken Sie auf *Aktualisieren*, um den Verzeichnisbaum für den Verwaltungsdienst zu aktualisieren.

Die folgenden Abschnitte enthalten weitere Informationen:

- „Richtlinien veröffentlichen“ auf Seite 111
- „Aktualisieren einer veröffentlichten Richtlinie“ auf Seite 112

Richtlinien veröffentlichen

1 Wählen Sie eine Benutzergruppe (oder Einzelbenutzer) im Verzeichnisbaum links aus. Doppelklicken Sie auf Benutzer, um sie auszuwählen (ist eine Benutzergruppe ausgewählt, sind alle Benutzer eingeschlossen).

Neben den Namen von Benutzern, die die Richtlinie nicht erhalten haben, wird das Symbol angezeigt. Wenn ein Benutzer/eine Gruppe die Richtlinie bereits erhalten hat, wird neben den Einträgen im Verzeichnisbaum das Symbol angezeigt.

Wenn Sie die Auswahl eines Benutzers/einer Gruppe aufheben möchten, doppelklicken sie das jeweilige Element, um das Symbol zu entfernen.

2 Klicken Sie auf *Veröffentlichen*, um die Richtlinie an den Richtlinienverteilungsservice zu senden.

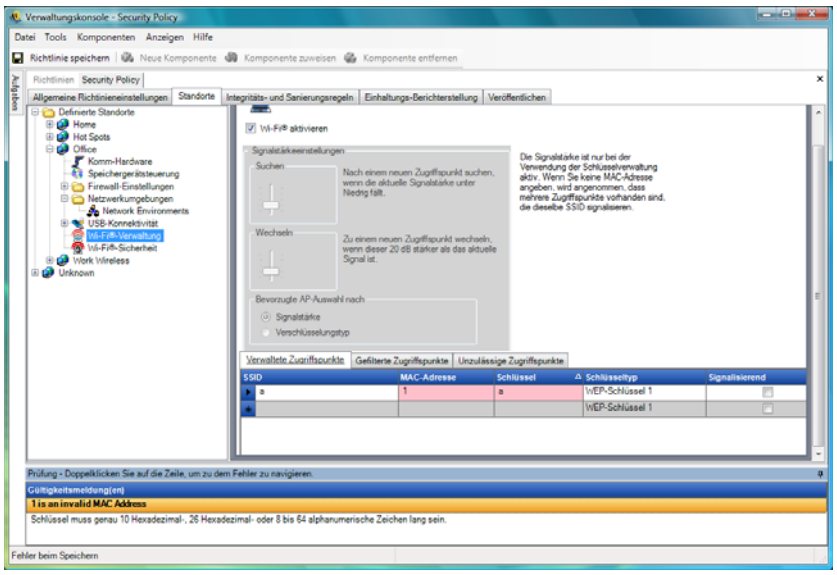
Aktualisieren einer veröffentlichten Richtlinie

Nachdem eine Richtlinie für Benutzer veröffentlicht wurde, können einfache Aktualisierungen verwaltet werden, indem die Komponenten in einer Richtlinie bearbeitet werden und die Richtlinie erneut veröffentlicht wird. Wenn der ZENworks Endpoint Security Management-Administrator beispielsweise den WEP-Schlüssel für einen Zugriffspunkt ändern muss, muss er lediglich den Schlüssel bearbeiten, die Richtlinie speichern und dann auf *Veröffentlichen* klicken. Die betroffenen Benutzer erhalten die aktualisierte Richtlinie (und den neuen Schlüssel) bei ihrem nächsten Check-in.

2.2.6 Fehlerbenachrichtigung

Wenn der Administrator versucht, eine Richtlinie mit unvollständigen oder falschen Daten in einer Komponente zu speichern, wird der Bestätigungsbereich am unteren Rand der Verwaltungskonsole angezeigt, in dem die einzelnen Fehler hervorgehoben sind. Sämtliche Fehler müssen·korrigiert werden, bevor die Richtlinie gespeichert werden kann.

Doppelklicken Sie auf die einzelnen Bestätigungszeilen, um zum Bildschirm mit dem jeweiligen Fehler zu gelangen. Fehler werden wie in der nachfolgenden Abbildung dargestellt hervorgehoben.

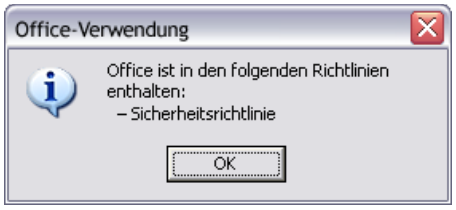


2.2.7 Auslastung anzeigen

Änderungen, die an freigegebenen Richtlinienkomponenten vorgenommen werden, wirken sich auf alle Richtlinien aus, die damit verknüpft sind. Bevor Sie eine Richtlinienkomponente aktualisieren oder anderweitig ändern, sollten Sie den Befehl *Auslastung anzeigen* ausführen, um zu ermitteln, welche Richtlinien von der Änderung betroffen sind.

1 Klicken Sie mit der rechten Maustaste auf die Komponente und klicken Sie dann auf *Auslastung anzeigen*.

Daraufhin wird ein Popup-Fenster mit sämtlichen Instanzen dieser Komponente in anderen Richtlinien angezeigt.



2.3 Importieren und Exportieren von Richtlinien

Die folgenden Abschnitte enthalten weitere Informationen:

- Abschnitt 2.3.1, „Importieren von Richtlinien“, auf Seite 113
- Abschnitt 2.3.2, „Exportieren einer Richtlinie“, auf Seite 113
- Abschnitt 2.3.3, „Exportieren von Richtlinien an nicht verwaltete Benutzer“, auf Seite 114

2.3.1 Importieren von Richtlinien

Eine Richtlinie kann von einem beliebigen Dateispeicherort im verfügbaren Netzwerk importiert werden.

1 Wählen Sie in der Verwaltungskonsole die Optionsfolge *Datei* > *Richtlinie importieren*.

Wenn Sie zurzeit eine Richtlinie bearbeiten oder entwerfen, schließt der Editor die Richtlinie (und fordert Sie auf, sie zu speichern), bevor das Importfenster geöffnet wird.

2 Klicken Sie auf "Durchsuchen", um den Dateispeicherort anzugeben, und geben Sie den Dateinamen im entsprechenden Feld an.

Nachdem die Richtlinie importiert wurde, kann sie weiter bearbeitet oder sofort veröffentlicht werden.

2.3.2 Exportieren einer Richtlinie

Richtlinien können über die Verwaltungskonsole exportiert und per E-Mail oder über eine Netzwerkfreigabe verteilt werden. Auf diese Weise können Richtlinien auf Unternehmensebene in Umgebungen verteilt werden, in denen mehrere Verwaltungsdienste und Richtlinieneditoren eingesetzt sind.

So exportieren Sie eine Sicherheitsrichtlinie:

1 Wählen Sie in der Verwaltungskonsole die Optionsfolge *Datei* > *Exportieren*.

2 Geben Sie ein Verzeichnis an und benennen Sie die Richtlinie; die Erweiterung muss hierbei `.sen` lauten (Beispiel: `C:\Desktop\salespolicy.sen`). Sie können auf "Durchsuchen" klicken und einen Speicherort angeben.

3 Klicken Sie auf *Exportieren*.

Daraufhin werden zwei Dateien exportiert. Bei der ersten Datei handelt es sich um die Richtlinie (`*.sen`-Datei). Bei der zweiten Datei handelt es sich um die Datei `setup.sen`, die erforderlich ist, um die Richtlinie beim Importieren zu entschlüsseln.

Exportierte Richtlinien müssen·in die Verwaltungskonsole importiert werden, bevor sie an·verwaltete Benutzer veröffentlicht werden können.

2.3.3 Exportieren von Richtlinien an nicht verwaltete Benutzer

Wurden im Unternehmen nicht verwaltete ZENworks Security Client-Instanzen bereitgestellt, muss zur Erstellung von Richtlinien eine Standalone-Verwaltungskonsole installiert werden. Weitere Informationen finden Sie in der "ZENworks Endpoint Security Management-Installationsanleitung".

So verteilen Sie nicht verwaltete Richtlinien:

1 Kopieren Sie die Datei `setup.sen` der Verwaltungskonsole in einen separaten Ordner.

Die Datei `setup.sen` wird bei der Installation der Verwaltungskonsole generiert und im Verzeichnis `\Programme\Novell\ESM Management Console\` gespeichert.

2 Erstellen Sie in der Verwaltungskonsole eine Richtlinie. Weitere Informationen finden Sie unter Abschnitt 2.2, „Erstellen von Sicherheitsrichtlinien“, auf Seite 50.

3 Exportieren Sie mit dem Befehl *Exportieren* die Richtlinie in den Ordner, der auch die Datei `setup.sen` enthält.

Sämtliche verteilten Richtlinien müssen nach dem Schema `policy.sen` benannt werden, damit der ZENworks Security Client sie akzeptiert.

4 Verteilen Sie die Dateien `policy.sen` und `setup.sen`. Diese Dateien müssen·für alle nicht verwalteten Client-Instanzen in das Verzeichnis `\Programme\Novell\ZENworks Security Client\` kopiert werden.

Die Datei `setup.sen` muss nur einmal (gemeinsam mit der ersten Richtlinie) auf die nicht verwalteten ZENworks Security Client-Instanzen kopiert werden. Im Anschluss müssen nur noch neue Richtlinien verteilt werden.