Hilfe für Websense Manager

Websense® Web Security
Websense Web Filter

Version 7

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published 2008
Printed in the United States and Ireland

Trademarks

Inhalt

1 Erste Schritte

Die Websense-Software ermöglicht es Netzwerkadministratoren aus allen Industriezweigen, vom Wirtschaftssektor über das Bildungswesen bis hin zum öffentlichen Sektor, Netzwerkdatenverkehr zum Internet zu steuern und zu überwachen.

- Minimieren Sie die Ausfallzeit der Mitarbeiter durch Zugriff auf unzulässige, unsachgemäße oder nicht arbeitsrelevante Daten im Internet.
- Minimieren Sie den Missbrauch von Netzwerkressourcen und das Risiko juristischer Maßnahmen aufgrund unsachgemäßen Zugriffs.
- Erweitern Sie die Sicherheit Ihres Netzwerks, und schützen Sie es vor potenziellen Bedrohungen wie z. B. Spyware, Malware und Hacking-Angriffen.

Hier finden Sie Informationen über folgende Themen:

Grundlegende Websense-Konfiguration	Implementieren der Filterung der Internetaktivitäten
• *Arbeiten in Websense Manager*, Seite 17	• *Filtern von Kategorien und Protokollen*, Seite 40
• *Ihre Subskription*, Seite 28	• *Hinzufügen eines Clients*, Seite 73
• *Die Websense Master Database*, Seite 32	• *Arbeiten mit Richtlinien*, Seite 79
• *Überprüfen der Konfiguration von Network Agent*, Seite 373	• *Zuweisen einer Richtlinie an Clients*, Seite 83

Darüber hinaus lernen Sie Folgendes:

Beurteilen der Konfiguration	Verfeinern der Filterrichtlinien
• *Heute: Zustand, Sicherheit und Nutzen seit Mitternacht*, Seite 22	• *Eine benutzerdefinierte Kategorie erstellen*, Seite 189
• *Verlauf: Letzte 30 Tage*, Seite 25	• *Filter für bestimmte Sites neu definieren*, Seite 193
• *Präsentationsberichte*, Seite 102	• *Benutzer auf eine festgelegte Liste von Internetsites einschränken*, Seite 178
• *Untersuchungsberichte*, Seite 123	• *Auf Schlüsselwort basierte Filterung*, Seite 191

Beurteilen der Konfiguration	Verfeinern der Filterrichtlinien
• *Filterverhalten mit der Toolbox überprüfen*, Seite 209	• *Datenverkehr basierend auf Dateitypen verwalten*, Seite 205 • *Bandbreite mit Bandwidth Optimizer verwalten*, Seite 203

Übersicht

Bei der Arbeit mit Integrationsprodukten wie z. B. Proxy-Servern, Firewalls, Routern und Caching Appliances bietet die Websense-Software das Modul und die Konfigurationstools für die Entwicklung, Überwachung und Durchsetzung von Richtlinien für den Zugriff auf das Internet.

Die Kombination einer Reihe von Websense-Komponenten (beschrieben unter *Websense-Produktkomponenten*, Seite 288) bietet Funktionalitäten für die Filterung der Internetaktivitäten, Benutzeridentifikation, Benachrichtigung, Berichterstellung und Fehler- und Problembehandlung.

Eine Übersicht über die in dieser Version der Websense-Software enthaltenen neuen Funktionen finden Sie in den Anmerkungen zu diesem Release, die auf dem Unterstützungsportal von Websense erhältlich sind.

Nach der Installation übernimmt die Websense-Software die Richtlinie **Standard**, mir der die Internetnutzung überwacht wird, ohne dabei Anforderungen zu blockieren. Diese Richtlinie regelt so lange den Zugriff aller Clients im Netzwerk auf das Internet, bis Sie Ihre eigenen Richtlinien definieren und den Clients zuweisen. Auch nachdem Sie Ihre benutzerdefinierten Filtereinstellungen erstellt haben, wird die Standardrichtlinie immer dann angewendet, wenn ein Client von keiner anderen Richtlinie erfasst wird. Weitere Informationen dazu finden Sie unter *Die Richtlinie "Standard"*, Seite 78.

Die Verfahren für das Erstellen von Filtern, Hinzufügen von Clients, Definieren von Richtlinien und Anwenden von Richtlinien auf Clients wird an folgenden Stellen beschrieben:

- *Filter für die Internetnutzung*, Seite 39
- *Clients*, Seite 63
- *Filterrichtlinien für die Internetnutzung*, Seite 77

Das browserbasierte Tool Websense Manager bietet mit einer zentralen Benutzeroberfläche Zugriff auf die allgemeine Konfiguration, Richtlinienverwaltung sowie auf Berichterstellungsfunktionen Ihrer Websense-Software. Weitere Informationen dazu finden Sie unter *Arbeiten in Websense Manager*, Seite 17.

Sie können verschiedene Ebenen für den Zugriff auf Websense Manager definieren, um bestimmten Administratoren das Verwalten einer definierten Gruppe von Clients oder einzelnen Personen das Generieren von Berichten ihrer eigenen Internetnutzung zu ermöglichen. Weitere Informationen dazu finden Sie unter *Delegierte Verwaltung*, Seite 251.

Arbeiten in Websense Manager

Verwandte Themen:

- *Anmelden bei Websense Manager*, Seite 18
- *Navigieren in Websense Manager*, Seite 19
- *Heute: Zustand, Sicherheit und Nutzen seit Mitternacht*, Seite 22
- *Verlauf: Letzte 30 Tage*, Seite 25

Websense Manager ist die zentrale Konfigurationsschnittstelle, mit der Sie das Filterverhalten anpassen, die Internetnutzung überwachen, Berichte über die Internetnutzung generieren und die Konfiguration und Einstellungen der Websense-Software verwalten. Dieses webbasierte Tool kann auf zwei unterstützten Browsern ausgeführt werden:

- Microsoft Internet Explorer 7
- Mozilla Firefox 2

Es ist zwar möglich, Websense Manager mit einigen anderen Browsern zu starten; den vollen Funktionsumfang und die korrekte Anzeige der Anwendung erhalten Sie jedoch nur mit den unterstützten Browsern.

Verwenden Sie zum Starten von Websense Manager eine der folgenden Vorgehensweisen:

- Unter Windows:
  - Wählen Sie **Start > Alle Programme > Websense**, und wählen Sie anschließend **Websense Manager**.
  - Doppelklicken Sie auf das Desktopsymbol von Websense Manager.
- Öffnen Sie einen der unterstützten Browser auf einem beliebigen Computer in Ihrem Netzwerk, und geben Sie Folgendes ein:

  ```
  https://<IP-Adresse>:9443/mng
  ```

  Ersetzen Sie *<IP-Adresse>* durch die IP-Adresse des Computers, auf dem Websense Manager ausgeführt wird.

Wenn eine Verbindung mit Websense Manager auf dem Standardport nicht möglich ist, überprüfen Sie anhand der Datei **tomcat.log** auf dem Computer mit Websense Manager die korrekte Eingabe des Ports (standardmäßig im Verzeichnis **C:\Program Files\Websense\tomcat\logs** oder **/opt/Websense/tomcat/logs/** gespeichert).

Wenn Sie den richtigen Port verwenden und trotzdem keine Verbindung mit Websense Manager von einem Remote-Computer herstellen können, stellen Sie sicher, dass Ihre Firewall die Kommunikation mit diesem Port zulässt.

Für eine sichere, browserbasierte Kommunikation mit Websense Manager wird eine SSL-Verbindung verwendet. Diese Verbindung verwendet ein von Websense, Inc., ausgestelltes Sicherheitszertifikat. Da die unterstützten Browser Websense, Inc., nicht als bekannte Certificate Authority anerkennen, wird beim ersten Starten von Websense Manager in einem neuen Browser ein Zertifikatfehler angezeigt. Damit dieser Fehler nicht mehr gemeldet wird, können Sie das Zertifikat in dem Browser installieren oder dauerhaft annehmen. Eine Anleitung dazu finden Sie in der Websense Knowledge Base.

Sobald das Sicherheitszertifikat angenommen wurde, wird die Anmeldeseite von Websense Manager im Browserfenster angezeigt (siehe *Anmelden bei Websense Manager*).

Anmelden bei Websense Manager

Verwandte Themen:

- *Arbeiten in Websense Manager*
- *Navigieren in Websense Manager*, Seite 19
- *Heute: Zustand, Sicherheit und Nutzen seit Mitternacht*, Seite 22
- *Verlauf: Letzte 30 Tage*, Seite 25

Nach der Installation erhält der erste Benutzer, der sich bei Websense Manager anmeldet, umfassenden Zugriff mit Administratorrechten. Der Benutzername lautet **WebsenseAdministrator** und kann nicht geändert werden. Das Passwort für den WebsenseAdministrator wird während der Installation konfiguriert.

Wenn Sie sich anmelden möchten, starten Sie zunächst Websense Manager (siehe *Arbeiten in Websense Manager*). Gehen Sie auf der Anmeldeseite folgendermaßen vor:

1. Wählen Sie einen **Policy Server**, der verwaltet werden soll.

   Wenn in Ihrer Umgebung nur ein Policy Server vorhanden ist, ist dieser standardmäßig ausgewählt.
2. Wählen Sie einen **Kontotyp**:
   - Wenn Sie sich mit einem Websense-Benutzerkonto wie WebsenseAdministrator anmelden möchten, klicken Sie auf **Websense-Konto** (Standard).
   - Wenn Sie sich mit Ihren Netzwerk-Anmeldeinformationen anmelden möchten, klicken Sie auf **Netzwerkkonto**.
3. Geben Sie einen **Benutzernamen** und ein **Passwort** ein, und klicken Sie anschließend auf **Anmelden**.

Sie sind nun bei Websense Manager angemeldet.

- Wenn dies Ihre erste Anmeldung bei Websense Manager ist, haben Sie die Möglichkeit, einen Lerntext für den Schnelleinstieg zu starten. Das Lesen des

Lerntextes für den Schnelleinstieg wird insbesondere solchen Benutzern dringend empfohlen, die die Websense-Software oder diese Version der Websense-Software zum ersten Mal verwenden.

- Wenn Sie die delegierte Verwaltung verwenden und Rollen mit Administratorrechten erstellt haben, werden Sie möglicherweise dazu aufgefordert, eine Rolle zum Verwalten auszuwählen. Weitere Informationen dazu finden Sie unter *Delegierte Verwaltung*, Seite 251.

Eine Websense Manager-Sitzung wird 30 Minuten nach der letzten Aktivität auf der Benutzeroberfläche, wie z. B. Wechseln der Seiten durch Klicken, Eingeben von Informationen, Zwischenspeichern von Änderungen im Cache oder Speichern von Änderungen, beendet. Der Benutzer wird 5 Minuten vor Sitzungsende durch eine Warnmeldung darauf hingewiesen.

- Wenn Änderungen auf der Seite noch nicht im Cache zwischengespeichert wurden, oder wenn im Cache zwischengespeicherte Änderungen anstehen, gehen die Änderungen beim Beenden der Sitzung verloren. Klicken Sie daher zum Zwischenspeichern der Änderungen im Cache auf **OK** und zum Speichern und Übernehmen der Änderungen auf **Alles speichern**.
- Wenn Websense Manager in mehreren Registerkarten desselben Browser-Fensters geöffnet ist, wird mit allen Instanzen auf dieselbe Sitzung zugegriffen. Wenn auf einer Registerkarte eine Zeitüberschreitung der Sitzung vorliegt, gilt dies für alle Registerkarten.
- Wenn Websense Manager in mehreren Browser-Fenstern auf demselben Computer geöffnet ist, wird **in folgenden Fällen** mit allen Instanzen auf dieselbe Sitzung zugegriffen:
  - Sie verwenden Microsoft Internet Explorer und verwenden das Tastaturkürzel Strg+N zum Öffnen einer neuen Instanz von Websense Manager.
  - Sie verwenden Mozilla Firefox.

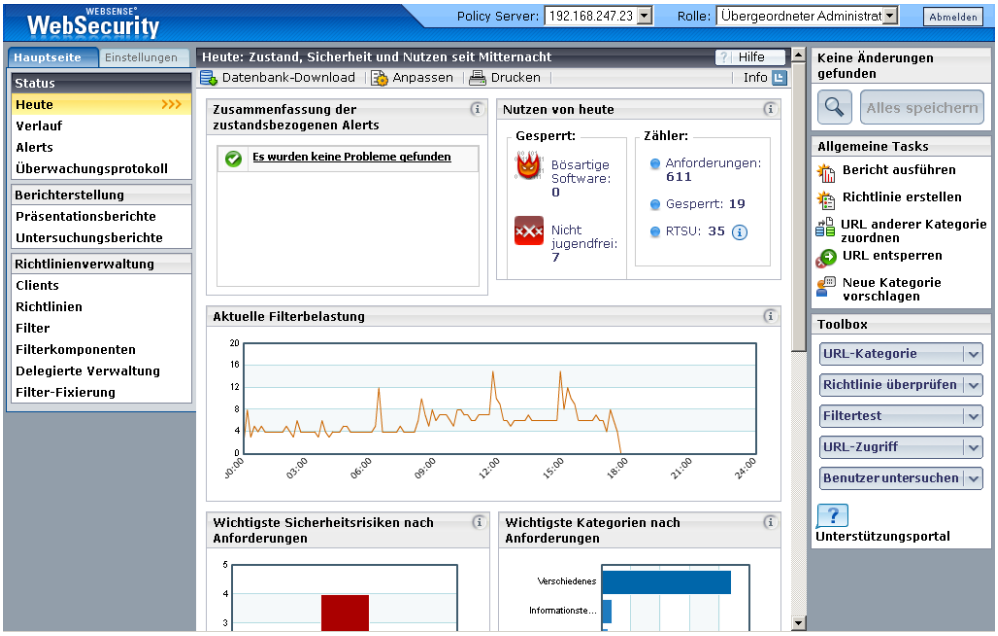
  Wenn in einem Fenster eine Zeitüberschreitung der Sitzung vorliegt, gilt dies für alle Fenster.
- Wenn Sie mehrere Internet Explorer-Fenster unabhängig voneinander starten und sich anschließend mit unterschiedlichen Administrator-Anmeldeinformationen bei Websense Manager anmelden, greifen die Fenster **nicht** auf dieselbe Sitzung zu. Wenn in einem Fenster das Zeitlimit überschritten wurde, sind die anderen Fenster davon nicht betroffen.

Wenn Sie den Browser schließen, ohne sich zuvor von Websense Manager abzumelden, oder wenn der Remote-Computer, mit dem Sie auf Websense Manager zugreifen, unerwartet heruntergefahren wird, wird Ihr Zugriff möglicherweise kurzfristig gesperrt. Die Websense-Software erkennt diesen Vorfall innerhalb von ca. 2 Minuten und beendet die unterbrochene Sitzung, sodass Sie sich erneut anmelden können.

Navigieren in Websense Manager

Die Benutzeroberfläche von Websense Manager kann in vier Hauptbereiche unterteilt werden:

1. Websense-Banner
2. Linkes Navigationsfenster
3. Rechtes Teilfenster mit Verknüpfungen
4. Inhaltsfenster



Das **Websense-Banner** enthält Folgendes:

- Bei welchem **Policy Server** Sie aktuell angemeldet sind (siehe *Arbeiten mit Policy Server*, Seite 294)
- Ihre aktuelle **Rolle** mit Administratorrechten (siehe *Einführung in die Administratorrollen*, Seite 252)
- Die Schaltfläche **Abmelden** zum Beenden der administrativen Sitzung

Der in Websense Manager angezeigte Inhalt hängt von den Berechtigungen ab, die dem angemeldeten Benutzer erteilt wurden. So werden z. B. einem Benutzer, der lediglich über die Berechtigung für die Berichterstellung verfügt, keine Konfigurationseinstellungen für den Server oder Richtlinienverwaltungstools angezeigt. Weitere Informationen dazu finden Sie unter *Delegierte Verwaltung*, Seite 251.

Dieser Abschnitt beschreibt die für WebsenseAdministrator und andere Benutzer mit Berechtigungen eines übergeordneten Administrators (Super Administrator) verfügbaren Optionen.

Das **linke Navigationsfenster** enthält zwei Registerkarten: **Hauptseite** und **Einstellungen**. Verwenden Sie die Registerkarte **Hauptseite**, um auf Funktionen für die Statusbestimmung, Berichterstellung und Richtlinienverwaltung zuzugreifen. Verwenden Sie die Registerkarte **Einstellungen**, um Ihr Websense-Konto zu verwalten und globale Systemverwaltungsaufgaben durchzuführen.

Das **rechte Teilfenster mit Verknüpfungen** enthält Links zu nützlichen Tools und allgemeinen Verwaltungsaufgaben. Hier können Sie außerdem in Websense Manager vorgenommene Änderungen überprüfen und speichern.

- Der obere Bereich des Navigationsfensters weist darauf hin, ob im Cache Änderungen zwischengespeichert wurden, die gespeichert werden müssen. Wenn Sie in Websense Manager arbeiten, zeigt die Informationszeile für Änderungen an, ob **Anstehende Änderungen** vorhanden sind.

  Im Allgemeinen werden Ihre Änderungen im Cache zwischengespeichert, wenn Sie eine Aufgabe in Websense Manager ausführen und anschließend auf "OK" klicken. (In einigen Fällen müssen Sie sowohl auf der untergeordneten Seite als auch auf der Hauptseite auf "OK" klicken, um die Änderungen im Cache zwischenzuspeichern.)

  Nachdem Sie die Änderungen im Cache zwischengespeichert haben, klicken Sie auf "**Alles speichern**", um die Änderungen zu speichern und zu übernehmen. Wenn Sie die im Cache zwischengespeicherten Änderungen vor dem Speichern anzeigen möchten (siehe *Überprüfen, Speichern und Verwerfen von Änderungen*, Seite 21), klicken Sie auf die Schaltfläche **Anstehende Änderungen anzeigen**. Dabei handelt es sich um die kleinere Schaltfläche links neben der Schaltfläche **Alles speichern**.
- Unter **Allgemeine Tasks** befinden sich Verknüpfungen zu häufig durchgeführten Verwaltungsaufgaben. Klicken Sie auf ein Element in der Liste, um zu der Seite zu wechseln, auf der die Aufgabe ausgeführt wird.
- Die **Toolbox** enthält Tools für die Schnellsuche, mit denen Sie Ihre Filterkonfiguration überprüfen können. Weitere Informationen dazu finden Sie unter *Filterverhalten mit der Toolbox überprüfen*, Seite 209.

Überprüfen, Speichern und Verwerfen von Änderungen

Wenn Sie eine Aufgabe in Websense Manager ausführen und anschließend auf **OK** klicken, werden Ihre Änderungen im Cache zwischengespeichert. Verwenden Sie die Seite **Anstehende Änderungen anzeigen**, um die im Cache zwischengespeicherten Änderungen zu überprüfen.

Wichtig

Vermeiden Sie mehrfaches Klicken auf die Schaltfläche "OK". Wiederholtes, schnelles Klicken auf dieselbe Schaltfläche kann in Mozilla Firefox zu Anzeigeproblemen führen, die nur durch Verlassen und erneutes Öffnen des Browsers behoben werden können.

Mehrere Änderungen an einem Funktionsbereich werden in der Regel in einem einzelnen Eintrag in der Cacheliste zusammengefasst. Wenn Sie z. B. 6 Clients hinzufügen und 2 Clients löschen, wird in der Cacheliste nur angezeigt, dass Änderungen an den Clients vorgenommen wurden. Änderungen an einer einzelnen Seite für Einstellungen hingegen führen möglicherweise zu mehreren Einträgen in der Cacheliste. Dies tritt dann auf, wenn eine einzelne Seite für Einstellungen für die Konfiguration mehrerer Funktionen der Websense-Software verwendet wird.

- Klicken Sie zum Speichern aller im Cache zwischengespeicherter Änderungen auf **Alle Änderungen speichern**.
- Klicken Sie zum Verwerfen aller im Cache zwischengespeicherter Änderungen auf **Alle Änderungen verwerfen**.

Nachdem Sie "Alle Änderungen speichern" oder "Alle Änderungen verwerfen" gewählt haben, wird die Informationsleiste für Änderungen im rechten Teilfenster für Verknüpfungen entsprechend aktualisiert, und Sie kehren zu der zuletzt ausgewählten Seite zurück. Die Funktionen "Alle Änderungen speichern" und "Alle Änderungen verwerfen" können nicht rückgängig gemacht werden.

Verwenden Sie das Überwachungsprotokoll, um die Details der in Websense Manager vorgenommenen Änderungen zu überprüfen. Weitere Informationen dazu finden Sie unter *Anzeigen und Exportieren des Überwachungsprotokolls*, Seite 300.

Heute: Zustand, Sicherheit und Nutzen seit Mitternacht

Verwandte Themen:

- *Navigieren in Websense Manager*, Seite 19
- *Verlauf: Letzte 30 Tage*, Seite 25
- *Anpassen der Seite "Heute"*, Seite 24
- *Alerts*, Seite 303

Die Seite **Status > Heute: Zustand, Sicherheit und Nutzen seit Mitternacht** wird als erste Seite nach der Anmeldung bei Websense Manager angezeigt. Sie gibt den aktuellen Status Ihrer Filtersoftware wieder und enthält eine grafische Darstellung der Filterung der Internetaktivitäten für einen Zeitraum von bis zu 24 Stunden, beginnend ab 0:01 Uhr (Systemzeit des Computers, auf dem die Protokolldatenbank ausgeführt wird).

Im oberen Bereich der Seite bieten zwei Abschnitte mit Zusammenfassungen eine schnelle Übersicht über den aktuellen Status:

- Die **Zusammenfassung der zustandsbezogenen Alerts** enthält den Status der Websense-Software. Wenn ein Fehler oder eine Warnung in der Zusammenfassung angezeigt wird, klicken Sie auf die Alert-Meldung, um die Seite Alerts mit weiteren Informationen zu öffnen (siehe *Überprüfen des aktuellen Systemstatus*, Seite 311).

  Die Daten in der Zusammenfassung der zustandsbezogenen Alerts werden alle 30 Sekunden aktualisiert.
- Unter **Nutzen von heute** werden Beispiele angezeigt, die darstellen, wie die Websense-Filterung Ihr Netzwerk heute geschützt hat. Darüber hinaus sind hier die Gesamtsumme der bearbeiteten Internetanforderungen sowie weitere Aktivitätssummen verzeichnet.

Unter der Zusammenfassung der Informationen befinden sich bis zu vier Diagramme mit Informationen über Filterungsaktivitäten. Diese Diagramme stehen übergeordneten Administratoren (Super Administrators) und delegierten Administratoren zur Verfügung, die über die Berechtigung verfügen, Berichte auf der Seite "Heute" anzuzeigen. Siehe *Rollen bearbeiten*, Seite 272.

Die Daten in diesen Diagrammen werden alle 2 Minuten aktualisiert. Sie müssen die Seite möglicherweise nach unten blättern, um alle Diagramme anzuzeigen.

Diagrammname	Beschreibung
Aktuelle Filterbelastung	Erfahren Sie, welches Volumen des gefilterten Internet-Datenverkehrs an die Protokolldatenbank übergeben wurde. Die Darstellung erfolgt in 10-Minuten-Intervallen.
Wichtigste Sicherheitsrisiken nach Anforderungen	Finden Sie heraus, welche Sicherheitsrisikokategorien heute am häufigsten angefordert wurden, und ermitteln Sie, ob die Filterrichtlinien angemessenen Schutz für Ihr Netzwerk gewährleisten.
Wichtigste Kategorien nach Anforderungen	Erfahren Sie, auf welche Kategorien heute am häufigsten zugegriffen wird. Erhalten Sie eine grobe Übersicht zu potenziellen Risiken in den Bereichen der Sicherheit, Bandbreite oder Produktivität.
Richtliniendurchsetzung nach Risikoklasse	Erfahren Sie, wie viele Anforderungen für jede Risikoklasse heute zugelassen und gesperrt wurden (siehe *Risikoklassen*, Seite 43). Beurteilen Sie, ob die aktuellen Richtlinien wirksam sind oder ob Änderungen erforderlich sind.
Wichtigste Protokolle nach Bandbreite	Erfahren Sie, welche Protokolle heute in Ihrem Netzwerk am meisten Bandbreite belegen. Beurteilen Sie anhand dieser Informationen den Bandbreitenbedarf und die potenzielle Notwendigkeit von Richtlinienänderungen.
Computer, von denen Sites mit Sicherheitsrisiko angefordert wurden	Finden Sie heraus, welche Computer heute auf Sites mit Sicherheitsrisiko zugegriffen haben. Unter Umständen ist es ratsam, diese Computer zu überprüfen, um sicherzustellen, dass sie nicht mit Viren oder Spyware infiziert sind.
Wichtigste gesperrte Benutzer	Prüfen Sie, welche Benutzer heute die meisten gesperrten Sites angefordert haben, und verschaffen Sie sich so einen Einblick in die tatsächliche Einhaltung der in der Organisation geltenden Standards zur Internetnutzung.
Wichtigste Sites ohne Kategoriezuordnung	Erfahren Sie, auf welche Sites, die in der Websense Master Database keiner Kategorie zugeordnet sind, heute am häufigsten zugegriffen wurde. Ordnen Sie unter **Allgemeine Tasks > URL anderer Kategorie zuordnen** eine Site einer Kategorie für die Filterung zu.

Klicken Sie auf ein beliebiges Balkendiagramm, um einen Untersuchungsbericht mit weiteren detaillierten Informationen zu starten.

Es werden drei Schaltflächen über der Seite angezeigt:

- **Datenbank-Download**: Diese Schaltfläche ist nur für übergeordnete Administratoren (Super Administrators) verfügbar und öffnet eine Seite, in der der Status von Downloads der Master Database angezeigt und gestartet werden (siehe *Überprüfen des Download-Status der Stammdatenbank (Master Database)*, Seite 299).

- **Anpassen**: Diese Schaltfläche steht nur übergeordneten Administratoren (Super Administrators) zur Verfügung und öffnet eine Seite, in der Sie festlegen können, welche Diagramme auf der Seite angezeigt werden (siehe *Anpassen der Seite "Heute"*, Seite 24).
- **Drucken**: Diese Schaltfläche steht allen Administratoren zur Verfügung. Hiermit wird ein zweites Fenster mit einer druckbaren Version der auf der Seite "Heute" angezeigten Diagramme geöffnet. Verwenden Sie die Optionen des Browsers zum Drucken dieser Seite. Die Navigationsoptionen auf der Hauptseite von Websense Manager werden beim Druck nicht berücksichtigt.

Unter den Diagrammen für Internetaktivitäten und Filterung befindet sich die **Zusammenfassung des Filtering Service**, die den Status jedes dem aktuellen Policy Server zugewiesenen Filtering Service enthält. Klicken Sie auf die IP-Adresse des Filtering Service, um weitere Informationen zu dieser Instanz des Filtering Service anzuzeigen.

Websense Manager-Sitzungen werden aus Sicherheitsgründen nach 30 Minuten Inaktivität beendet. Sie können die Filterungs- und Alert-Daten jedoch auch über diesen Zeitraum hinaus überwachen: Aktivieren Sie im unteren Bereich der Seite "Heute" die Option **Überwachung des Status für "Heute", "Verlauf" und "Alerts" ohne Zeitlimit fortsetzen**. Die auf diesen drei Seiten dargestellten Informationen werden weiterhin aktualisiert, bis Sie den Browser schließen oder zu einer anderen Websense Manager-Seite navigieren.

Wichtig

Wenn Sie die Überwachungsoption aktivieren und die Seiten "Heute", "Verlauf" und "Alerts" für mehr als 30 Minuten nicht verlassen, werden Sie beim Versuch, zu einer anderen Websense Manager-Seite zu navigieren, auf die Anmeldeseite weitergeleitet.

Wenn Sie diese Option aktivieren, müssen alle im Cache zwischengespeicherten Änderungen gespeichert werden, bevor das 30-minütige Limit der Zeitüberschreitung abgelaufen ist.

Anpassen der Seite "Heute"

Verwandte Themen:

- *Heute: Zustand, Sicherheit und Nutzen seit Mitternacht*, Seite 22
- *Anpassen der Seite "Verlauf"*, Seite 27

Auf der Seite **Heute > Anpassen** können bis zu vier Diagramme für die Seite Status > Heute ausgewählt werden. Nur übergeordnete Administratoren (Super Administrators) mit Richtlinienberechtigungen, für die keine Bedingungen gelten (einschließlich WebsenseAdministrator), können die Seite "Heute" anpassen.

Die ausgewählten Diagramme werden bei allen übergeordneten Administratoren (Super Administrators) und delegierten Administratoren, die zur Anzeige von Diagrammen auf der Seite "Heute" berechtigt sind, dort angezeigt. Siehe *Rollen bearbeiten*, Seite 272.

Einige Diagramme enthalten potenziell vertrauliche Informationen, wie Benutzernamen oder IP-Adressen. Stellen Sie sicher, dass die ausgewählten Diagramme für alle Administratoren geeignet sind, die zu einer Anzeige berechtigt sind.

Wenn Sie Diagramme auswählen möchten, aktivieren oder deaktivieren Sie das Kontrollkästchen neben dem Diagrammnamen. Wenn Sie die gewünschte Auswahl vorgenommen haben, klicken Sie auf **OK**, um zur Seite "Heute" zurückzukehren und die Diagramme anzuzeigen. Wenn Sie zur Seite "Heute" zurückkehren möchten, ohne dabei Änderungen zu übernehmen, klicken Sie auf **Abbrechen**.

Eine kurze Beschreibung der in den jeweiligen Diagrammen angezeigten Informationen finden Sie unter *Heute: Zustand, Sicherheit und Nutzen seit Mitternacht*, Seite 22.

Verlauf: Letzte 30 Tage

Verwandte Themen:

- *Heute: Zustand, Sicherheit und Nutzen seit Mitternacht*, Seite 22
- *Navigieren in Websense Manager*, Seite 19
- *Anpassen der Seite "Verlauf"*, Seite 27

Die Seite **Status > Verlauf: Letzte 30 Tage** bietet einen Überblick über das Filterverhalten während der letzten 30 Tage. Die Diagramme werden täglich um 0:01 Uhr aktualisiert (Systemzeit des Computers, auf dem die Protokolldatenbank ausgeführt wird), um die Daten des vergangenen Tages zu berücksichtigen.

Welcher Zeitraum von den Diagrammen und Übersichtstabellen genau erfasst wurde, hängt davon ab, wie lange die Websense-Software die Filterung durchgeführt hat. Während des ersten Monats der Installation der Websense-Software enthält die Seite Daten entsprechend der Anzahl Tage seit Beginn der Installation. Daraufhin erfasst der Bericht 30 Tage vor dem Tag der Anzeige.

Die **Schätzwerte** im oberen Bereich der Seite bieten eine Schätzung der durch die Websense-Software generierten Zeit- und Bandbreitenersparnisse sowie eine Zusammenfassung der gesperrten Anforderungen von Kategorien, die für viele Unternehmen von Bedeutung sind.

Bewegen Sie den Mauszeiger unter "Ersparnis" über das Element **Zeit** oder **Bandbreite**, um eine Erläuterung darüber anzuzeigen, wie der Schätzwert berechnet wurde (siehe *Eingesparte Zeit und Bandbreite*, Seite 27). Sie können die Berechnungsweise der Werte ändern, indem Sie auf **Anpassen** klicken.

Der Bereich **Gesperrte Anforderungen** bietet eine weitere Darstellung darüber, wie die Websense-Software Ihr Netzwerk geschützt hat. Hier werden verschiedene, für viele Unternehmen interessante Kategorien mit der Gesamtanzahl der in der jeweiligen Kategorie während des Zeitraums gesperrten Anforderungen aufgelistet.

Abhängig davon, über welche Berechtigungen für die Berichterstellungsfunktion die Rolle verfügt, können delegierte Administratoren die unten beschriebenen Diagramme möglicherweise nicht anzeigen. Siehe *Rollen bearbeiten*, Seite 272.

Die Seite enthält außerdem bis zu vier Diagramme mit Hervorhebungen der Filterung. Sie müssen die Seite möglicherweise nach unten blättern, um alle Diagramme anzuzeigen. Die Daten in den Diagrammen werden einmal pro Tag aktualisiert. Klicken Sie auf ein Diagramm, um einen Untersuchungsbericht mit weiteren Informationen zu starten.

Diagrammname	Beschreibung
Internetaktivität nach Anforderungen	Überprüfen Sie die Anzahl der täglich an die Protokolldatenbank übergebenen gefilterten Internetanforderungen.
Wichtigste Sicherheitsrisiken nach Anforderungen	Sehen Sie, welche Sicherheitsrisikokategorien in letzter Zeit angefordert wurden, und ermitteln Sie, ob die Filterrichtlinien angemessenen Schutz für Ihr Netzwerk gewährleisten.
Wichtigste Kategorien nach Anforderungen	Erfahren Sie, auf welche Kategorien am häufigsten zugegriffen wurde. Erhalten Sie eine grobe Übersicht zu potenziellen Risiken in den Bereichen der Sicherheit, Bandbreite oder Produktivität.
Wichtigste Sites ohne Kategoriezuordnung	Erfahren Sie, auf welche Sites, die in der Websense Master Database keiner Kategorie zugeordnet sind, am häufigsten zugegriffen wurde. Ordnen Sie unter **Allgemeine Tasks > URL anderer Kategorie zuordnen** eine Site einer Kategorie für die Filterung zu.
Wichtigste Protokolle nach Bandbreite	Erfahren Sie, welche Protokolle in Ihrem Netzwerk in letzter Zeit am meisten Bandbreite belegen. Beurteilen Sie anhand dieser Informationen den Bandbreitenbedarf und potenzielle Richtlinienänderungen.
Richtliniendurchsetzung nach Risikoklasse	Erfahren Sie, wie viele Anforderungen für jede Risikoklasse in letzter Zeit zugelassen und gesperrt wurden (siehe *Risikoklassen*, Seite 43). Beurteilen Sie, ob die aktuellen Richtlinien wirksam sind oder ob Änderungen erforderlich sind.
Wichtigste gesperrte Benutzer	Sehen Sie, für welche Benutzer die meisten Internetanforderungen gesperrt wurden. Verschaffen Sie sich einen Einblick in die tatsächliche Einhaltung der in der Organisation geltenden Standards zur Internetnutzung.
Zusammenfassung der Richtliniendurchsetzung	Erhalten Sie eine Übersicht der vor kurzem zugelassenen Anforderungen, der gesperrten Anforderungen in der Klasse "Sicherheitsrisiko" und der gesperrten Anforderungen für andere Sites. Überlegen Sie, welche Aspekte der Filterung eine detailliertere Auswertung benötigen.

Es werden zwei Schaltflächen über der Seite angezeigt:

- **Anpassen**: Diese Schaltfläche steht nur übergeordneten Administratoren (Super Administrators) zur Verfügung und öffnet eine Seite, in der Sie festlegen können, welche Diagramme auf der Seite angezeigt werden. Darüber hinaus haben Sie die Möglichkeit, die Berechnungsweise der geschätzten Ersparnisse zu ändern (siehe *Anpassen der Seite "Verlauf"*, Seite 27).
- **Drucken**: Diese Schaltfläche steht allen Administratoren zur Verfügung. Hiermit wird ein zweites Fenster mit einer druckbaren Version der auf der Seite "Verlauf" angezeigten Diagramme geöffnet. Verwenden Sie die Optionen des Browsers zum Drucken dieser Seite. Die Navigationsoptionen auf der Hauptseite von Websense Manager werden beim Druck nicht berücksichtigt.

Eingesparte Zeit und Bandbreite

Neben der verbesserten Sicherheit bietet die Filterung von Websense auch eine Minimierung des durch unproduktive Internetaktivitäten verursachten Verlusts von Zeit und Bandbreite.

Im Abschnitt "Ersparnis" des Bereichs "Schätzwerte" wird eine Schätzung dieser Zeit- und Bandbreitenersparnisse angezeigt. Diese Werte werden wie Folgt berechnet:

- Zeitersparnis: Multiplikation des Werts unter **Typische Dauer eines Besuchs** mit dem Wert unter **Gesperrte Sites**. In ihrer Ausgangskonfiguration verwendet die Websense-Software einen Standardwert für die durchschnittliche Anzahl Sekunden, die ein Benutzer einer angeforderte Website anzeigt. Der Wert für die gesperrten Sites stellt die Gesamtzahl der gesperrten Anforderungen während des auf der Seite "Verlauf" festgelegten Zeitraums dar.
- Bandbreitenersparnis: Multiplikation des Werts unter **Typische Bandbreite pro Besuch:** mit dem Wert unter **Gesperrte Sites**. In ihrer Ausgangskonfiguration verwendet die Websense-Software einen Standardwert für die durchschnittliche Anzahl Bytes, die von einer durchschnittlichen Website belegt werden. Der Wert für die gesperrten Sites stellt die Gesamtzahl der gesperrten Anforderungen während des auf der Seite Verlauf festgelegten Zeitraums dar.

Weitere Informationen darüber, wie die in diesen Berechnungen verwendeten Werte geändert werden, um die Verwendung in Ihrer Organisation wiederzugeben, finden Sie unter *Anpassen der Seite "Verlauf"*, Seite 27.

Anpassen der Seite "Verlauf"

Verwandte Themen:

- *Verlauf: Letzte 30 Tage*, Seite 25
- *Anpassen der Seite "Heute"*, Seite 24

Auf der Seite **Verlauf > Anpassen** können Sie bestimmen, welche Diagramme auf der Seite **Status > Verlauf** angezeigt werden und wie Zeit- und Bandbreitenersparnisse berechnet werden.

Aktivieren Sie das Kontrollkästchen neben den Namen von bis zu vier Diagrammen, die auf der Seite Verlauf angezeigt werden sollen. Eine kurze Beschreibung der Diagramme finden Sie unter *Verlauf: Letzte 30 Tage*, Seite 25. Nur übergeordnete Administratoren (Super Administrators) mit Richtlinienberechtigungen, für die keine Bedingungen gelten (einschließlich WebsenseAdministrator), können die Diagramme auf der Seite "Verlauf" anpassen.

Einige Diagramme enthalten potenziell vertrauliche Informationen, wie z. B. Benutzernamen. Stellen Sie sicher, dass die ausgewählten Diagramme für alle Administratoren geeignet sind, die zu einer Anzeige berechtigt sind.

Sowohl übergeordnete Administratoren (Super Administrators) als auch delegierte Administratoren können die Art und Weise anpassen, wie Zeit- und Bandbreitenersparnisse berechnet werden. Delegierte Administratoren können auf diese Felder zugreifen, indem sie in dem Popup-Fenster, das die Berechnung der Zeit- und Bandbreitenersparnis erläutert, auf den Link **Anpassen** klicken.

Geben Sie neue durchschnittliche Zeit- und Bandbreitenmesswerte ein, die als Basis für die Berechnung verwendet werden sollen:

Option	Beschreibung
Durchschnittliche Zeitersparnis pro gesperrte Seite in Sekunden:	Geben Sie eine durchschnittliche Anzahl Sekunden für die Dauer ein, die ein Benutzer nach Schätzung Ihrer Organisation mit der Anzeige einer Seite verbringt. Die Websense-Software multipliziert diesen Wert mit der Anzahl gesperrter Seiten, um die auf der Seite "Verlauf" angezeigten Zeitersparnisse zu bestimmen.
Durchschnittliche Ersparnis von Bandbreite [KB] pro gesperrte Seite	Geben Sie eine durchschnittliche Größe der angezeigten Seiten in Kilobyte (KB) an. Die Websense-Software multipliziert diesen Wert mit der Anzahl gesperrter Seiten, um die auf der Seite "Verlauf" angezeigten Bandbreitenersparnisse zu bestimmen.

Wenn Sie die gewünschten Änderungen vorgenommen haben, klicken Sie auf **OK**, um zur Seite "Verlauf" zurückzukehren und die neuen Diagramme oder Schätzungen der Zeit und Bandbreite anzuzeigen. Wenn Sie zur Seite Verlauf zurückkehren möchten, ohne dabei Änderungen zu übernehmen, klicken Sie auf **Abbrechen**.

Ihre Subskription

Websense-Subskriptionen werden per Client ausgestellt. Ein Client ist ein Benutzer oder Computer in Ihrem Netzwerk.

Wenn Sie eine Subskription erwerben, erhalten Sie per E-Mail einen Subskriptionsschlüssel. Jeder Schlüssel ist für eine Installation von Websense Policy Server gültig. Wenn Sie mehrere Policy Server installieren, benötigen Sie für jede Installation einen Schlüssel.

Bevor Sie die Filterung starten können, müssen Sie einen gültigen Subskriptionsschlüssel eingeben (siehe *Konfigurieren Ihrer Kontoinformationen*, Seite 31). Dies erlaubt Ihnen den Download der Master Database (siehe *Die Websense Master Database*, Seite 32), die von der Websense-Software zum Filtern von Clients benötigt wird.

Nach dem ersten erfolgreichen Datenbank-Download wird im Websense Manager die Anzahl der in Ihrer Subskription enthalten Clients angezeigt.

Die Websense-Software führt eine Subskriptionstabelle der pro Tag gefilterten Clients. Die Subskriptionstabelle wird jede Nacht gelöscht. Bei der ersten Internetanfrage eines Clients nach dem Löschen der Tabelle wird seine IP-Adresse in die Tabelle eingetragen.

Wenn die Anzahl der in der Tabelle aufgelisteten Clients die Subskriptionsebene erreicht, wird die Subskription mit jeder Internetanfrage eines bisher noch nicht aufgelisteten Clients überschritten. Ist dies der Fall, wird dem Client, der die Subskriptionsebene überschreitet, je nach konfigurierter Einstellung entweder der Zugriff auf das Internet komplett gesperrt, oder er erhält ungefilterten Zugriff auf das Internet. Gleichermaßen wird je nach Einstellung bei Ablauf der Subskription allen Clients entweder der Zugriff auf das Internet komplett gesperrt, oder es wird ihnen ungefilterter Zugriff auf das Internet gewährt.

Informationen über die Konfiguration des Filterverhaltens bei Ablauf der Subskription erhalten Sie unter *Konfigurieren Ihrer Kontoinformationen*, Seite 31.

Informationen über die Konfiguration der Websense-Software für das Senden einer E-Mail-Benachrichtigung bei Erreichen oder Überschreiten des Limits der Subskription erhalten Sie unter *Konfigurieren von System-Alerts*, Seite 307.

Die Anzahl der gefilterten Kategorien hängt von Ihrer Websense-Subskription ab. Die Websense-Software filtert alle Sites in allen Kategorien, die bei Ihrem Erwerb aktiviert wurden.

Verwalten Ihres Kontos über das MyWebsense-Portal

Websense, Inc., stellt unter www.mywebsense.com ein Kundenportal zur Verfügung, über das Sie Produkt-Updates, Patches, aktuelle Informationen über Produkte, Testversionen und technische Unterstützung für Ihre Websense-Software erhalten.

Wenn Sie ein Konto einrichten, werden Sie zur Eingabe aller Websense-Subskriptionsschlüssel aufgefordert. Damit wird sichergestellt, dass Sie auf die für Ihr Websense-Produkt und Ihre Websense-Version zugeschnittenen Informationen, Alerts und Patches Zugriff erhalten.

Wenn Sie über ein MyWebsense-Konto verfügen und einmal das Passwort für den WebsenseAdministrator vergessen haben und sich nicht bei Websense Manager

anmelden können, müssen Sie auf der Anmeldeseite von Websense Manager nur noch auf **Passwort vergessen** klicken. Sie werden daraufhin zur Anmeldung bei MyWebsense aufgefordert und erhalten dort Anweisungen für das Generieren und Aktivieren eines neuen Passworts.

> **Wichtig**
>
> Wenn Sie ein neues Passwort anfordern, muss der im MyWebsense-Portal ausgewählte Subskriptionsschlüssel dem in Websense Manager auf der Seite "Konto" eingegebenen Schlüssel entsprechen.

Es können sich mehrere Mitglieder Ihrer Organisation mit demselben Subskriptionsschlüssel bei MyWebsense anmelden.

Wenn Sie von Websense Manager aus auf das MyWebsense-Portal zugreifen möchten, wählen Sie **Hilfe > MyWebsense**.

Aktivieren von Websense Web Protection Services™

Websense Web Security-Subskriptionen beinhalten den Zugriff auf Websense Web Protection Services: SiteWatcher™, BrandWatcher™ und ThreatWatcher™. Sobald Sie diese Dienste aktiviert haben, schützen sie die Websites, Markennamen und Web-Server Ihrer Organisation.

Dienst	Beschreibung
SiteWatcher	Sendet einen Alert, wenn die Websites Ihrer Organisation von bösartigem Code befallen wurden und ermöglicht es Ihnen, sofort Maßnahmen zu ergreifen, um Kunden, potenzielle Neukunden und Partner zu schützen, die diese Seite besuchen.
BrandWatcher	• Sendet einen Alert, wenn die Websites oder Marken Ihrer Organisation Ziel eines Phishing- oder Keylogging-Angriffs sind. • Sie erhalten Informationen über Internet-Schutzmechanismen, erfolgte Angriffe und andere, sicherheitsrelevante Details, damit Sie entsprechende Maßnahmen ergreifen, Kunden benachrichtigen und negative PR minimieren können.
ThreatWatcher	• Informiert darüber, auf welche Daten der unternehmenseigenen Web-Server Hacker Zugriff erhalten, und sucht nach bekannten Sicherheitslücken und Gefahrenpotenzialen. • Stellt Berichte zur Risikoeinschätzung mit empfohlenen Abhilfemaßnahmen über ein Internet-Portal bereit. • Beugt bösartigen Angriffen auf Ihre Web-Server vor, bevor sie erfolgen.

Melden Sie sich beim MyWebsense-Portal an, um Websense Protection Services zu aktivieren. Sobald ThreatWatcher aktiviert ist, können Sie sich bei MyWebsense anmelden und Berichte über Bedrohungen für die registrierten Web-Server abrufen.

Konfigurieren Ihrer Kontoinformationen

Verwandte Themen:

- *Ihre Subskription*, Seite 28
- *Konfigurieren von Datenbank-Downloads*, Seite 34
- *Arbeiten mit Protokollen*, Seite 196

Öffnen Sie die Seite **Einstellungen > Konto**, um Subskriptionsinformationen einzugeben und anzuzeigen und das Passwort für WebsenseAdministrator zu ändern, mit dem auf Websense Manager zugegriffen wird. WebsenseAdministrator ist standardmäßig das Haupt-Administratorkonto für die Verwaltung der Websense-Software.

Hier können Sie außerdem einrichten, dass die Websense-Software anonyme Daten zur Protokollnutzung an Websense, Inc., sendet. Diese Informationen werden zur Aktualisierung der Websense Master Database herangezogen, die eine Sammlung von mehr als 36 Millionen Websites und mehr als 100 Protokolldefinitionen darstellt (weitere Informationen finden Sie unter *Die Websense Master Database*, Seite 32).

1. Geben Sie nach der Installation der Websense-Software, oder wenn Sie einen neuen Subskriptionsschlüssel erhalten haben, den Schlüssel in das Feld **Subskriptionsschlüssel** ein.

   Nachdem Sie einen neuen Subskriptionsschlüssel eingegeben haben und auf "OK" geklickt haben, wird der Download der Master Database automatisch gestartet.
2. Nach dem ersten Download der Master Database werden die folgenden Informationen angezeigt:

Ablaufdatum des Schlüssels	Ablaufdatum Ihrer aktuellen Subskription. Nach diesem Datum müssen Sie die Subskription erneuern, um weiterhin die Master Database herunterladen und Ihr Netzwerk filtern zu können.
Subskribierte Netzwerkbenutzer	Anzahl der Benutzer innerhalb eines Netzwerks, deren Anforderungen gefiltert werden können.
Subskribierte Remotebenutzer	Anzahl der Benutzer außerhalb des Netzwerks, deren Anforderungen gefiltert werden können (optionale Funktion "Remote Filtering" erforderlich).

3. Wählen Sie **Benutzer sperren, wenn die Subskription abgelaufen ist oder überschritten wurde**, um Folgendes zu erreichen:
   - Sperrung jeglichen Zugriffs auf das Internet für alle Benutzer, wenn die Subskription abgelaufen ist.
   - Sperrung jeglichen Zugriffs auf das Internet für Benutzer, durch die die Anzahl der subskribierten Benutzer überschritten wird.

   Wenn diese Option nicht aktiviert ist, haben Benutzer in diesen Situationen ungefilterten Zugriff auf das Internet.
4. Wenn Sie das Passwort für WebsenseAdministrator ändern möchten, geben Sie zunächst das aktuelle Passwort ein. Geben Sie dann das neue Passwort ein, und bestätigen Sie es anschließend.
   - Das Passwort muss aus mindestens 4 und maximal 25 Zeichen bestehen. Bei der Eingabe muss die Groß- und Kleinschreibung beachtet werden, und das Passwort darf Buchstaben, Zahlen, Sonderzeichen und Leerzeichen enthalten.
   - Für das WebsenseAdministrator-Konto wird die Benutzung eines starken Passworts empfohlen. Das Passwort sollte mindestens 8 Zeichen lang sein und mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Zahl und ein Sonderzeichen enthalten.
5. Aktivieren Sie die Option **Daten zur Kategorie- und Protokollnutzung an Websense Inc. senden**, damit Websense-Software Daten über die Nutzung von Websense definierter Kategorien und Protokolle sammelt und anonym an Websense, Inc., sendet.

   Mit diesen Nutzungsdaten kann Websense, Inc., die Filterleistung der Websense-Software ständig erweitern.

Die Websense Master Database

Verwandte Themen:

- *Datenbankaktualisierungen in Echtzeit*, Seite 33
- *Real-Time Security Updates™*, Seite 34
- *Filtern von Kategorien und Protokollen*, Seite 40
- *Arbeiten mit Filtering Service*, Seite 298
- *Überprüfen des Download-Status der Stammdatenbank (Master Database)*, Seite 299
- *Wieder aufnehmbare Downloads der Stammdatenbank (Master Database)*, Seite 300

Die Websense Master Database enthält die Kategorie- und Protokolldefinitionen, die die Basis für die Filterung von Internetinhalten darstellt (siehe *Filtern von Kategorien und Protokollen*, Seite 40).

- Mit **Kategorien** werden verschiedene Websites (identifiziert durch URL und IP-Adresse) gruppiert, die ähnliche Inhalte aufweisen.
- Mit **Protokolldefinitionen** werden Protokolle für die Kommunikation mit dem Internet gruppiert, die für ähnliche Aufgaben verwendet werden, wie z. B. das Übertragen von Dateien oder das Senden von Sofortnachrichten.

Während der Software-Installation wird eine eingeschränkte Version der Datenbank für Filteraktivitäten installiert. Es wird jedoch empfohlen, so bald wie möglich die komplette Master Database herunterzuladen, um eine größtmögliche Leistung bei der Filterung von Internetaktivitäten zu erreichen. Wenn Sie die Master Database zum ersten Mal herunterladen möchten, geben Sie Ihren Subskriptionsschlüssel auf der Seite **Einstellungen > Konto** ein (siehe *Konfigurieren Ihrer Kontoinformationen*, Seite 31).

Wenn die Websense-Software den Download über einen Proxy durchführen muss, konfigurieren Sie außerdem die Proxy-Einstellungen auf der Seite **Einstellungen > Datenbank-Download** (siehe *Konfigurieren von Datenbank-Downloads*, Seite 34).

Das Herunterladen der gesamten Datenbank kann einige Minuten oder aber über eine Stunde dauern. Hierbei hängt die Dauer unter anderem von Faktoren wie der Geschwindigkeit der Internetverbindung, der Bandbreite, dem verfügbaren Speicher und dem freien Speicherplatz ab.

Nach dem ersten Download führt die Websense-Software regelmäßige Downloads der Datenbankänderungen durch. Dabei wird einem von Ihnen eingerichteten Plan gefolgt (siehe *Konfigurieren von Datenbank-Downloads*, Seite 34). Da die Master Database häufig aktualisiert wird, werden die Downloads in der Standardeinstellung einmal täglich durchgeführt.

Wenn die Master Database älter als 14 Tage ist, stellt die Websense-Software die Filterung von Internetanforderungen ein.

Wenn Sie einen Datenbank-Download außerplanmäßig initiieren oder den Status oder das Datum des letzten Datenbank-Downloads oder die aktuelle Versionsnummer der Datenbank anzeigen möchten, öffnen Sie **Status > Heute**, und klicken Sie auf **Datenbank-Download**.

Datenbankaktualisierungen in Echtzeit

Neben den planmäßigen Downloads führt die Websense-Software je nach Bedarf Notfallupdates der Datenbank durch. Ein Update in Echtzeit kann z. B. durchgeführt werden, um eine Site neu zu kategorisieren, die kurzfristig falsch kategorisiert wurde. Diese Updates stellen sicher, dass Sites und Protokolle ordnungsgemäß gefiltert werden.

Die Websense-Software prüft einmal in der Stunde auf Datenbankaktualisierungen.

Die neuesten Updates werden auf der Seite **Status > Alerts** verzeichnet (siehe *Überprüfen des aktuellen Systemstatus*, Seite 311).

Real-Time Security Updates™

Benutzer von Websense Web Security haben nicht nur Zugriff auf die standardmäßigen Datenbankaktualisierungen in Echtzeit, sondern können darüber hinaus Real-Time Security Updates so einstellen, dass sicherheitsbezogene Updates der Master Database heruntergeladen werden, sobald sie von Websense, Inc., veröffentlicht werden.

Real-Time Security Updates bieten einen zusätzlichen Schutz gegen internetbasierte Sicherheitsbedrohungen. Werden diese Updates umgehend nach ihrer Veröffentlichung installiert, wird die Verwundbarkeit durch neues Phishing (Identitätsdiebstahl), falsche Anwendungen und bösartigen Code, die populäre Websites oder Anwendungen befallen können, gemindert.

Filtering Service prüft alle 5 Minuten auf neue Sicherheitsupdates. Da die Updates jedoch nur dann gesendet werden, wenn Sicherheitsbedrohungen auftreten, werden nur gelegentlich Änderungen vorgenommen, die die normale Netzwerkaktivität kaum beeinträchtigen.

Real-Time Security Updates aktivieren Sie auf der Seite **Einstellungen > Datenbank-Download** (siehe *Konfigurieren von Datenbank-Downloads*, Seite 34).

Konfigurieren von Datenbank-Downloads

Verwandte Themen:

- *Konfigurieren Ihrer Kontoinformationen*, Seite 31
- *Die Websense Master Database*, Seite 32
- *Überprüfen des Download-Status der Stammdatenbank (Master Database)*, Seite 299

Auf der Seite **Einstellungen > Datenbank-Download** legen Sie den Plan für automatische Datenbank-Downloads fest. Geben Sie dort außerdem wichtige Informationen zu Proxy-Server oder Firewalls an, die die Websense-Software beim Herunterladen der Datenbank passieren muss.

1. Wählen Sie unter **Tage für den Download** die Tage aus, an denen der automatische Download stattfinden soll.

Die Master Database muss mindestens einmal in 14 Tagen heruntergeladen werden, um eine kontinuierliche Filterung durch die Websense-Software zu gewährleisten. Wenn Sie keinen Tag für den Download auswählen, startet die Websense-Software automatisch einen Download, wenn die Datenbank 7 Tage alt ist.

> **Hinweis**
> Die Funktionalität der Tage für den Download wird deaktiviert, wenn Real-Time Security Updates aktiviert sind (siehe Schritt 3). Es werden täglich automatisch Downloads durchgeführt, um sicherzustellen, dass die neueste Standarddatenbank für die Sicherheitsupdates zur Verfügung steht.

2. Wählen Sie die Startzeit (**Von**) und die Endzeit (**Bis**) für den **Zeitrahmen für den Download**. Wenn keine Zeiten ausgewählt wurden, findet der Datenbank-Download zwischen 21:00 und 06:00 Uhr statt.

   Die Websense-Software kontaktiert den Server der Master Database zu einem zufälligen Zeitpunkt innerhalb dieses Zeitraums. Informationen über das Konfigurieren von Alerts bei fehlgeschlagenen Downloads finden Sie unter *Konfigurieren von System-Alerts*, Seite 307.

   > **Hinweis**
   > Nach dem Herunterladen der Master Database oder eines Updates kann der CPU durch das Laden der Datenbank in den lokalen Speicher zu 90 % ausgelastet werden.

3. (*Websense Web Security*) Wählen Sie **Sicherheitsupdates in Echtzeit aktivieren**, damit die Websense-Software alle 5 Minuten auf Sicherheitsupdates für die Master Database prüft. Wenn ein Sicherheitsupdate gefunden wird, wird es umgehend heruntergeladen.

   Real-Time Security Updates schützen Ihr Netzwerk schnell vor der Verwundbarkeit durch neues Phishing (Identitätsdiebstahl), falsche Anwendungen und bösartigen Code, die populäre Websites oder Anwendungen befallen können.

4. Wählen Sie **Proxy-Server oder Firewall verwenden**, wenn die Websense-Software über einen Proxy-Server oder eine Firewall mit Proxy-Funktion (im Gegensatz zum Integrationsprodukt, mit dem die Websense-Software kommuniziert) auf das Internet zugreift, um die Master Database herunterzuladen. Nehmen Sie anschließend die folgende Konfiguration vor.

IP oder Name des Servers	Geben Sie die IP-Adresse oder den Namen des Computers ein, auf dem der Proxy-Server oder die Firewall ausgeführt wird.
Port	Geben Sie die Nummer des Ports ein, den der Datenbank-Download passieren muss (Standard ist 8080).

5. Wenn bei dem in Schritt 4 konfigurierten Proxy-Server oder der entsprechenden Firewall eine Authentifizierung für den Zugriff auf das Internet erforderlich ist, wählen Sie **Authentifizierung verwenden**, und geben Sie anschließend **Benutzername** und **Passwort** ein, mit denen die Websense-Software Zugriff auf das Internet erhält.

   Hinweis
   Wenn die Option "Authentifizierung verwenden" ausgewählt wurde, muss der Proxy-Server oder die Firewall so konfiguriert werden, dass eine Klartext- oder Standardauthentifizierung zulässig ist, um das Herunterladen der Master Database zu ermöglichen.

   Standardmäßig sind der Benutzername und das Passwort so codiert, dass der Zeichensatz den Regions- und Spracheinstellung des Computers entspricht, auf dem der Policy Server ausgeführt wird. Diese Codierung kann über die Seite **Einstellungen > Verzeichnisdienste** manuell konfiguriert werden (siehe *Erweiterte Verzeichniseinstellungen*, Seite 70).

Testen der Netzwerkkonfiguration

Damit die Filterung von Internetanforderungen ausgeführt werden kann, muss die Websense-Software den Internet-Datenverkehr zu und von den Computern in Ihrem Netzwerk einsehen können. Verwenden Sie den Detektor für Netzwerkdatenverkehr, um sicherzustellen, dass diese Kommunikation mit dem Internet für die Filtersoftware sichtbar ist. Anweisungen dazu finden Sie unter *Überprüfen der Konfiguration von Network Agent*, Seite 373.

Wenn der Detektor für Datenverkehr nicht alle Bereiche Ihres Netzwerks einsehen kann, finden Sie Konfigurationsanweisungen unter *Netzwerkkonfiguration*, Seite 363.

Technische Unterstützung von Websense

Websense, Inc., legt großen Wert auf die Zufriedenheit seiner Kunden. Die Website für technischen Support von Websense steht zu jeder Zeit für die neuesten Release-Informationen, den Zugriff auf die Knowledge Base oder Produktdokumentationen bereit. Darüber hinaus haben Sie hier die Möglichkeit, Unterstützung anzufordern.

www.websense.com/SupportPortal/

Die Antwortzeit für Online-Anforderungen beträgt während der Geschäftszeiten ca. 4 Stunden. Anforderungen außerhalb der Geschäftszeiten werden am nächsten Geschäftstag beantwortet.

Sie können darüber hinaus telefonische Hilfe anfordern. Damit Ihre telefonischen Anforderungen schnell und effizient beantwortet werden können, sollten Sie Folgendes bereithalten:

- Websense-Subskriptionsschlüssel
- Zugriff auf Websense Manager
- Zugriff auf die Computer, auf denen Filtering Service, Log Server und der Datenbank-Server (Microsoft SQL Server oder MSDE) ausgeführt werden
- Berechtigung für den Zugriff auf die Websense-Protokolldatenbank
- Kenntnis der Architektur des Netzwerks, oder Kontakt mit einer Person, die über diese Kenntnis verfügt
- Technische Daten der Computer, auf denen Filtering Service und Websense Manager ausgeführt werden
- Eine Liste der weiteren Anwendungen, die auf dem Computer ausgeführt werden, auf dem auch Filtering Service ausgeführt wird

Bei schwerwiegenderen Problemen sind möglicherweise weitere Informationen erforderlich.

Die reguläre telefonische Unterstützung steht während der jeweiligen Geschäftszeiten von Montag bis Freitag unter den folgenden Telefonnummern zur Verfügung:

- San Diego, Kalifornien, USA: **+1 858.458.2940**
- London, Großbritannien: **+44 (0) 1932 796244**

Die Geschäftszeiten sowie andere Möglichkeiten der Unterstützung finden Sie auf der oben genannten Website für technische Unterstützung.

Kunden in Japan werden gebeten, Kontakt mit dem Vertriebshändler aufzunehmen. Er kann Ihnen mitteilen, wie Sie schnellstmöglich Unterstützung erhalten.

2 Filter für die Internetnutzung

Verwandte Themen:

- *Filtern von Kategorien und Protokollen*, Seite 40
- *Arbeiten mit Filtern*, Seite 51
- *Konfigurieren von Websense-Filtereinstellungen*, Seite 60
- *Filterrichtlinien für die Internetnutzung*, Seite 77
- *Filterrichtlinien verfeinern*, Seite 177

Richtlinien regeln den Zugriff von Benutzern auf das Internet. Eine Richtlinie ist ein Plan, der regelt, wie und wann die Websense-Software den Zugriff auf Websites und Internetanwendungen filtern soll. Eine einfach Richtlinie besteht aus folgenden Elementen:

- **Kategoriefilter**, die die an Website-Kategorien durchgeführten Aktionen (Zulassen oder Sperren) regeln
- **Protokollfilter**, die die an Internetanwendungen und Nicht-HTTP-Protokollen durchgeführten Aktionen regeln
- Ein Plan, der bestimmt, wann ein Filter eingesetzt wird

Die richtlinienbasierte Filterung ermöglicht es Ihnen, Clients (Benutzer, Gruppen und Computer in Ihrem Netzwerk) verschiedene Stufen des Zugriffs auf das Internet zu gewähren. Zunächst erstellen Sie Filter, mit denen Sie präzise Einschränkungen des Zugriffs auf das Internet definieren, und anschließend erstellen Sie mit den Filtern eine Richtlinie.

Bei der erstmaligen Installation erstellt die Websense-Software die Richtlinie **Standard**, um damit die erste Überwachung von Internetanfragen einzuleiten, sobald ein Subskriptionsschlüssel eingegeben wurde (siehe *Die Richtlinie "Standard"*, Seite 78). In der Ausgangskonfiguration der Standardrichtlinie sind alle Anfragen zulässig.

Hinweis

Wenn Sie ein Upgrade von einer früheren Version der Websense-Software vornehmen, werden vorhandene Richtlinieneinstellungen übernommen. Überprüfen Sie nach dem Upgrade Ihre Richtlinien, um sicherzustellen, dass sie weiterhin gültig sind.

Wenn Sie verschiedenen Clients unterschiedliche Filtereinschränkungen zuweisen möchten, definieren Sie zunächst Kategoriefilter. Sie können z. B. Folgendes definieren:

- Einen Kategoriefilter, der den Zugriff auf alle Websites sperrt, ausgenommen solcher Websites, die zu den Kategorien "Wirtschaft und Handel", "Bildung" und "Nachrichten & Medien" gehören
- Einen zweiten Kategoriefilter, der den Zugriff auf alle Websites zulässt, ausgenommen solcher, die ein Sicherheitsrisiko darstellen oder nicht jugendfreies Material enthalten
- Einen dritten Kategoriefilter, der den Zugriff auf Websites überwacht, ohne sie zu sperren (siehe *Erstellen von Kategoriefiltern*, Seite 52)

Zusätzlich zu diesen Kategoriefiltern können Sie Folgendes definieren:

- Einen Protokollfilter, der den Zugriff auf die Protokollgruppen für Instant Messaging, die gemeinsame Nutzung von Dateien über Peer-to-Peer-Datenaustausch (P2P), die Umgehung durch Proxy und Streaming Media sperrt
- Ein zweiter Protokollfilter, der alle Nicht-HTTP-Protokolle mit Ausnahme solcher zulässt, die mit der Umgehung durch Proxy verbunden sind
- Ein dritter Protokollfilter, der alle Nicht-HTTP-Protokolle zulässt (siehe *Erstellen von Protokollfiltern*, Seite 55)

Sobald Sie einen Filtersatz definiert haben, der den Vorschriften für den Internetzugriff Ihres Unternehmens entspricht, können Sie sie zu den Richtlinien hinzufügen und auf Clients anwenden (siehe *Filterrichtlinien für die Internetnutzung*, Seite 77).

Filtern von Kategorien und Protokollen

Die Websense Master Database organisiert Websites mit ähnlichem Inhalt (gekennzeichnet durch URLs und IP-Adressen) in **Kategorien**. Jede Kategorie hat einen beschreibenden Namen, wie "Nicht jugendfreies Material", "Glücksspiel" oder "Peer-to-Peer". Sie können auch Ihre eigenen, benutzerdefinierten Kategorien erstellen, mit denen Sie Websites gruppieren können, die für Ihr Unternehmen von besonderem Interesse sind (siehe *Eine benutzerdefinierte Kategorie erstellen*, Seite 189). Die Kategorien der Master Database stellen gemeinsam mit den benutzerdefinierten Kategorien die Basis der Filterung der Internetaktivitäten dar.

Websense, Inc., nimmt keine Bewertung der Kategorien oder Sites in der Master Database vor. Die Kategorien sollen eine hilfreiche Gruppierung der betreffenden Websites für die subskribierten Kunden darstellen. Sie wurden nicht dazu entwickelt, Websites oder Gruppen von Websites oder die Personen oder Interessen, die sie veröffentlichen, zu charakterisieren, und sollten nicht als solches ausgelegt werden. Gleichermaßen sind die Beschriftungen der Websense-Kategorien als zweckmäßige Kurzschrift gedacht und sollen keine Meinung oder Haltung wiedergeben oder als solche ausgelegt werden, weder zustimmender noch jedweder anderer Natur gegenüber dem behandelten Gegenstand oder den Websites, die damit klassifiziert werden.

Die aktuelle Liste der Master Database-Kategorien erhalten Sie unter:

www.websense.com/global/en/ProductsServices/MasterDatabase/URLCategories.php

Wenn Sie das Hinzufügen einer Website zur Master Database vorschlagen möchten, klicken Sie in Websense Manager im rechten Teilfenster für Verknüpfungen auf **Neue Kategorie vorschlagen**, oder navigieren Sie zu:

www.websense.com/SupportPortal/SiteLookup.aspx

Nachdem Sie sich auf dem MyWebsense-Portal angemeldet haben, werden Sie zum Tool "Site Lookup and Category Suggestion" (Site-Suche und Kategorievorschlag) weitergeleitet.

Wenn Sie einen **Kategoriefilter** in Websense Manager erstellen, wählen Sie aus, welche Kategorien gesperrt werden und welche zulässig sind.

Neben den URL-Kategorien enthält die Websense Master Database auch Protokollgruppen, mit denen der Internet-Datenverkehr über Nicht-HTTP-Protokolle verwaltet wird. Jede Protokollgruppe definiert ähnliche Internetprotokoll-Typen (wie FTP oder IRC) und Anwendungen (wie AOL Instant Messenger oder BitTorrent). Die Definitionen werden jede Nacht geprüft und aktualisiert.

Ähnlich wie bei den Kategorien können Sie benutzerdefinierte Protokolle für die Filterung der Internetaktivitäten definieren.

Die aktuelle Liste der Master Database-Protokolle erhalten Sie unter:

www.websense.com/global/en/ProductsServices/MasterDatabase/ProtocolCategories.php

Wenn Sie einen **Protokollfilter** erstellen, wählen Sie aus, welche Protokolle gesperrt werden und welche zulässig sind.

> **Hinweis**
> Network Agent muss installiert sein, um eine protokollbasierte Filterung zu ermöglichen.

Einige von Websense definierte Protokolle ermöglichen das Sperren des an einen externen Server ausgehenden Internet-Datenverkehrs, wie z. B. an einen bestimmten Instant Messaging-Server. Nur von Websense definierte Protokolle mit dynamisch zugewiesenen Portnummern können als ausgehenden Datenverkehr blockiert werden.

Neue Kategorien und Protokolle

Wenn der Master Database neue Kategorien und Protokolle hinzugefügt werden, wird jedem Element eine Standardfilteraktion wie z. B. **Zulassen** oder **Sperren** zugewiesen (siehe *Filteraktionen*, Seite 47).

- Die Standardaktion wird auf alle aktiven Kategorie- und Protokollfilter angewendet (siehe *Arbeiten mit Filtern*, Seite 51). Bearbeiten Sie die aktiven Filter, um die Filtermethode der Kategorie oder des Protokolls zu ändern.

- Die Standardaktion basiert auf dem Feedback, ob die jeweiligen Websites oder Protokolle im Allgemeinen als für Unternehmen geeignet betrachtet werden.

Sie können die Websense-Software so konfigurieren, dass Sie durch eine Systemmeldung darüber informiert werden, wenn neue Kategorien oder Protokolle zur Master Database hinzugefügt wurden. Weitere Informationen dazu finden Sie unter *Alerts*, Seite 303.

Spezialkategorien

Die Master Database enthält Spezialkategorien, mit denen Sie bestimmte Typen der Internetnutzung verwalten können. Die folgenden Kategorien stehen in allen Editionen der Websense-Software zur Verfügung:

- Mit der Kategorie **Besondere Ereignisse** werden Websites klassifiziert, die als häufig abgefragte Themen eingestuft werden, um Sie bei der Bewältigung eines plötzlich ansteigenden Internet-Datenverkehrs aufgrund besonderer Ereignisse zu unterstützen. Ein Beispiel: Die offizielle Website der Fußballweltmeisterschaft befindet sich normalerweise in der Kategorie "Sport"; kann jedoch für die Dauer der Endspielrunde der Fußballweltmeisterschaft in die Kategorie "Besondere Ereignisse" verschoben werden.

  Updates der Kategorie "Besondere Ereignisse" werden im Zuge der geplanten Downloads der Master Database hinzugefügt. Die Websites werden dieser Kategorie für einen kurzen Zeitraum hinzugefügt und anschließend entweder in eine andere Kategorie verschoben oder aus der Master Database gelöscht.
- Die Kategorie **Produktivität** konzentriert sich auf die Vermeidung von Aktivitäten, die eine Zeitverschwendung darstellen können.
  - Werbung
  - Download von Freeware und Software
  - Instant Messaging
  - Online-Brokerage und Handel
  - Pay-to-Surf
- Mit der Kategorie **Bandbreite** soll die eingesetzte Netzwerkbandbreite reduziert werden.
  - Internetradio & Internet-TV
  - Internet-Telefonie
  - Peer-to-Peer
  - Private Netzwerkspeicherung/-sicherung
  - Streaming Media

Websense Web Security enthält zusätzliche Sicherheitskategorien:

- **Websense Security Filtering** (auch einfach **Sicherheit** genannt) konzentriert sich auf Internetsites, die bösartigen Code enthalten und gegen Antivirenprogramme resistent sind. In dieser Kategorie enthaltende Websites werden standardmäßig gesperrt.

- Bot-Netzwerke
- Keylogger
- Bösartige Webseiten
- Phishing und sonstige Fälschungen
- Potentiell unerwünschte Software
- Spyware

- Die Kategorie **Erweiterter Schutz** konzentriert sich auf potentiell bösartige Websites. Websites in den Unterkategorien "Erhöhtes Risiko" und "Neue Schwachstellen" werden standardmäßig gesperrt.
  - **Erhöhtes Risiko** enthält Websites, die ihre wahre Natur oder Identität verschleiern oder Elemente enthalten, die eine latent bösartige Intention vermuten lassen.
  - **Neue Schwachstellen** enthält Websites, über die festgestellt wurde, dass sie bekannten und potentiellen Exploit-Code enthalten.
  - **Potentiell schädlicher Inhalt** enthält Websites, die wahrscheinlich wenig oder keinen nützlichen Inhalt enthalten.

Die Gruppe "Erweiterter Schutz" filtert potentiell bösartige Websites basierend auf ihrem *Ruf*. Der Ruf einer Site basiert auf den ersten Anzeichen potentiell bösartiger Aktivitäten. Ein Angreifer könnte sich z. B. eine URL zu Eigen machen, die einer rechtmäßigen URL ähnlich ist oder einen weit verbreiteten Schreibfehler enthält. Eine solche Website könnte für die Verbreitung von Malware an Benutzer eingesetzt werden, bevor traditionelle Filter aktualisiert und die Website als bösartig eingestuft werden können.

Wenn die Sicherheitsrecherche von Websense eine potentielle Bedrohung erkennt, wird sie der Kategorie "Erweiterter Schutz" hinzugefügt, bis Websense eine endgültige Kategorie für die Website gefunden hat.

Risikoklassen

Verwandte Themen:

- *Zuweisen von Risikoklassen an Kategorien*, Seite 324
- *Präsentationsberichte*, Seite 102
- *Untersuchungsberichte*, Seite 123

Die Websense Master Database gruppiert Kategorien in **Risikoklassen**. Risikoklassen deuten auf mögliche Ebenen der Verwundbarkeit durch Websites in der Gruppe der Kategorien hin.

Risikoklassen werden hauptsächlich für die Berichterstellung eingesetzt. Die Seiten "Heute" und "Verlauf" enthalten Diagramme, in denen die Internetaktivitäten nach Risikoklassen dargestellt sind. Außerdem können Sie nach Risikoklassen geordnete Präsentationen oder Untersuchungsberichte erstellen.

Risikoklassen können darüber hinaus die Erstellung von Kategoriefiltern vereinfachen. In der Ausgangskonfiguration des Kategoriefilters "Basissicherheit" werden alle Standardkategorien in der Sicherheitsrisikoklasse gesperrt. Sie können die Gruppierung der Risikoklasse als Richtlinie für die Erstellung Ihrer eigenen Kategoriefilter und die Entscheidung, ob eine Kategorie zugelassen, gesperrt oder auf sonstige Weise eingeschränkt werden soll, verwenden.

Die Websense-Software enthält 5 Risikoklassen, die weiter unten beschrieben werden. Die Websense-Software gruppiert die folgenden Kategorien standardmäßig in die jeweilige Risikoklasse.

- Eine Kategorie kann mehreren Risikoklassen oder auch gar keiner Risikoklasse zugewiesen werden.
- Die Gruppierungen können regelmäßig in der Master Database geändert werden.

Gesetzliche Haftung

Nicht jugendfreies Material (einschließlich Nicht jugendfreie Inhalte, Unterwäsche & Bademode, Nacktheit und Sex)

Bandbreite > Peer-to-Peer

Glücksspiel

Rechtswidrig oder Bedenklich

Informationstechnologie > Hacking und Umgehung durch Proxy

Militantes und Extremismus

Rassismus und Hass

Geschmackloses

Gewalt

Waffen

Minderung der Netzwerkbandbreite

Bandbreite (einschließlich Internetradio & Internet-TV, Internet-Telefonie, Peer-to-Peer, Private Netzwerkspeicherung/-sicherung und Streaming Media)

Unterhaltung > MP3 und Dienste zum Herunterladen von Audio-Dateien

Produktivität > Werbung *und* Freeware/Software-Download

Arbeitsbezogene Nutzung

Wirtschaft und Handel (einschließlich Finanzdaten und Finanzdienstleistungen)

Bildung > Bildungsunterlagen *und* Nachschlagewerke & Referenzmaterial

Staat & Regierung (einschließlich Militär)

Informationstechnologie (einschließlich Computersicherheit, Suchmaschinen und Portale und Webseiten zur URL-Übersetzung)

Reisen

Kraftfahrzeuge

Sicherheitsrisiko

Bandbreite > Peer-to-Peer

Erweiterter Schutz (einschließlich Erhöhtes Risiko, Neue Schwachstellen und Potentiell schädlicher Inhalt) [*Websense Web Security*]

Informationstechnologie > Hacking *und* Umgehung durch Proxy

Produktivität > Freeware/Software-Download

Sicherheit (einschließlich Bot-Netzwerke, Keylogger, Bösartige Webseiten, Phishing und sonstige Fälschungen, Potentiell unerwünschte Software und Spyware)

Produktivitätsverlust

Schwangerschaftsabbruch (einschließlich Abtreibungsbefürworter *und* Abtreibungsgegner)

Nicht jugendfreies Material > Aufklärung & Sexualerziehung

Meinungsgruppen

Bandbreite > Internetradio & Internet-TV, Peer-to-Peer und Streaming Media

Arzneimittel (einschließlich Drogen- und Arzneimittelmissbrauch, Marihuana, Verschreibungspflichtige Medikamente und Präparate und Substanzen ohne gesetzliche Regelung)

Bildung (einschließlich Kulturelle Einrichtungen *und* Bildungseinrichtungen)

Unterhaltung (einschließlich MP3 und Dienste zum Herunterladen von Audio-Dateien)

Glücksspiel

Spiele

Staat & Regierung > Politische Gruppen

Gesundheit

Informationstechnologie > Web Hosting

Internet-Kommunikation (einschließlich Allgemeine E-Mail, Organisationsspezifische E-Mail, Text- und Media-Messaging und Web Chat)

Jobsuche

Nachrichten & Medien (einschließlich Alternative Journale)

Produktivität (einschließlich Freeware/Software-Download, Instant Messaging, Nachrichten-Boards und Foren, Online-Brokerage und Handel und Pay-to-Surf)

Religion (einschließlich Nichttraditionelle Religionen, Okkultismus und volkstümliche Glaubensrichtungen *und* Traditionelle Religionen)

Online-Shopping (einschließlich Internet-Auktionen *und* Immobilien)

Soziale Organisationen (einschließlich Berufsverbände und Arbeiterorganisationen, Dienstleistungsorganisationen und wohltätige Organisationen und Soziale Organisationen und Zweckverbände)

Gesellschaft & Lifestyle (einschließlich Alkohol, Tabak, Schwule, Lesben und Bisexuelle, Hobbys, Partnersuche, Restaurants und Gastronomie und Persönliche Sites und Sites für webbasierte soziale Netzwerke)

Besondere Ereignisse

Produktivitätsverlust

Sport (einschließlich Jagdsport/Sportschießvereine)

Reisen

Kraftfahrzeuge

Übergeordnete Administratoren (Super Administrators) können die den Risikoklassen zugewiesenen Kategorien auf der Seite **Einstellungen > Risikoklasse** ändern (siehe *Zuweisen von Risikoklassen an Kategorien*, Seite 324).

Sicherheitsprotokollgruppen

Neben den Kategorien "Sicherheit" und "Erweiterter Schutz" enthält Websense Web Security zwei Protokolle für das Auffinden und den Schutz vor Spyware und bösartigem Code oder Inhalt, der über das Internet übertragen wird.

- Die Protokollgruppe **Malicious Traffic** (Bösartiger Datenverkehr) enthält das Protokoll **Bot-Netzwerke**, mit dem der von einem Bot generierte Command-and-Control-Datenverkehr gesperrt wird, mit dem versucht wird, zu bösartigen Zwecken eine Verbindung mit einem Bot-Netzwerk herzustellen.
- Die Protokollgruppe **Malicious Traffic - Monitor Only** (Bösartiger Datenverkehr – Nur Überwachung) wird für die Identifikation von Datenverkehr verwendet, der bösartiger Software zugeordnet werden kann.
  - **Email-Borne Worms** (E-Mail-Würmer) verfolgt ausgehenden SMTP-Datenverkehr, der durch einen e-mail-basierten Wurmangriff verursacht worden sein könnte.
  - **Other Malicious Traffic** (Anderer bösartiger Datenverkehr) verfolgt eingehenden und ausgehenden Datenverkehr, bei dem eine Verbindung mit bösartigen Anwendungen vermutet wird.

Die Protokollgruppe "Malicious Traffic" (Bösartiger Datenverkehr) ist standardmäßig gesperrt und kann innerhalb Ihrer Protokollfilter konfiguriert werden (siehe *Bearbeiten eines Protokollfilters*, Seite 56). Die Protokolle unter "Malicious Traffic - Monitor Only" (Bösartiger Datenverkehr – Nur Überwachung) können für die Berichterstellung protokolliert werden, es kann jedoch keine andere Filteraktion darauf angewendet werden.

Instant Messaging Attachment Manager

Bei dem Instant Messaging (IM) Attachment Manager handelt es sich um eine optionale Funktionalität. Wenn Sie diese Funktion subskribieren, können Sie das gemeinsame Nutzen von Dateien mit IM-Clients einschließlich AOL/ICQ, Microsoft (MSN) und Yahoo einschränken. So können Sie den Datenverkehr über IM zulassen und die Übertragung von Anhängen durch IM-Clients sperren.

Instant Messaging File Attachments (Instant Messaging-Dateianhänge) ist eine Protokollgruppe, die Definitionen für mehrere IM-Clients enthält. Wenn der IM Attachment Manager aktiviert ist, werden diese Protokolle in der Protokollliste in allen aktiven Protokollfiltern und auf der Seite "Protokolle bearbeiten" angezeigt.

Die Filterung von Anhängen bei Instant Messaging kann sowohl für internen als auch für externen Datenverkehr angewendet werden. Wenn Sie die Filterung des internen Datenverkehrs aktivieren möchten, definieren Sie den zu überwachenden Teil des Netzwerks auf der Seite **Einstellungen > Network Agent > Global** (siehe *Konfigurieren globaler Einstellungen*, Seite 366).

Filteraktionen

Kategorie- und Protokollfilter weisen jeder Kategorie und jedem Protokoll eine **Aktion** zu. Diese Aktion wird von der Websense-Filtersoftware als Reaktion auf die Internetanforderung eines Clients durchgeführt. Folgende Aktionen werden sowohl mit Kategorien als auch mit Protokollen durchgeführt:

- **Sperren** der Anforderung. Die Benutzer erhalten eine Seite oder Meldung, die Sie über die Sperrung informieren, und die entsprechende Website kann nicht angezeigt oder die Internetanwendung nicht verwendet werden.
- **Zulassen** der Anforderung. Die Benutzer können die Website anzeigen oder die Internetanwendung verwenden.
- Beurteilen der aktuellen Nutzung der **Bandbreite**, bevor die Anforderung gesperrt oder zugelassen wird. Wenn diese Aktion aktiviert ist, und die Nutzung der Bandbreite einen bestimmten Schwellenwert erreicht, werden weitere Internetanforderungen aus einer bestimmten Kategorie oder für ein bestimmtes Protokoll gesperrt. Siehe *Bandbreite mit Bandwidth Optimizer verwalten*, Seite 203.

Weitere Aktionen können nur auf Kategorien angewendet werden.

> **Hinweis**
>
> Die Optionen "Bestätigen" und "Quote" sollten nicht verwendet werden, wenn individuelle Clients (Benutzer, Gruppen und Computer) von mehreren Policy Servern verwaltet werden.
>
> Andere Policy Server haben keinen Zugriff auf die Zeitsteuerung dieser Funktionen, und den betroffenen Clients könnte ein breiterer oder geringerer Zugriff auf das Internet gewährt werden als beabsichtigt.

- **Bestätigen**: Die Benutzer erhalten eine Sperrseite, auf der Sie zur Bestätigung aufgefordert werden, dass diese Seite zu geschäftlichen Zwecken aufgerufen wird. Wenn der Benutzer auf **Weiter** klickt, kann er die Website anzeigen.

  Mit dem Klicken auf "Weiter" wird ein Zeitmesser gestartet. Während des eingestellten Zeitraums (standardmäßig 60 Sekunden) kann der Benutzer weitere Websites in Kategorien anzeigen, deren Anzeige bestätigt werden muss, ohne dass eine weitere Sperrseite angezeigt wird. Wenn das Ende des Zeitraums erreicht ist, wird bei der Anforderung einer weitere Website, die bestätigt werden muss, eine Sperrseite angezeigt.

Der Standardzeitraum kann auf der Seite **Einstellungen > Filterung (Filtering)** geändert werden.

- **Quote**: Die Benutzer werden über eine Sperrseite abgefragt, ob Quotenzeit für die Anzeige der Website verwendet werden soll. Wenn der Benutzer auf **Quotenzeit verwenden** klickt, kann er die Website anzeigen.

  Wenn auf die Schaltfläche "Quotenzeit verwenden" geklickt wird, werden Zeitmesser gestartet: ein Zeitmesser für die Sitzung, bei der Quotenzeit verwendet wird, und ein Zeitmesser für die Gesamtquotenzeit.

  - Wenn der Benutzer während des Standardzeitraums einer **Sitzung** (standardmäßig 10 Minuten) zusätzliche Websites anfordert, bei denen Quotenzeit verwendet wird, kann er diese Websites besuchen, ohne dass eine weitere Sperrseite angezeigt wird.
  - Die **Gesamtquotenzeit** wird auf Tagesbasis berechnet. Wenn die Gesamtquotenzeit aufgebraucht ist, können Clients erst am darauffolgenden Tag auf Websites dieser Kategorien zugreifen. Die standardmäßig pro Tag zugewiesene Quotenzeit (standardmäßig 60 Minuten) wird auf der Seite **Einstellungen > Filterung (Filtering)** festgelegt. Darüber hinaus können Clients eine individuelle tägliche Quotenzeit zugewiesen werden. Weitere Informationen dazu finden Sie unter *Verwenden von Quotenzeit für die Zugriffsbeschränkung für das Internet*, Seite 48.

- **Schlüsselworte sperren**: Wenn Sie Schlüsselworte definieren und die Sperrfunktion für Schlüsselworte aktivieren, kann auf Websites, deren URL einen ein gesperrtes Schlüsselwort enthält, nicht zugegriffen werden. Siehe *Auf Schlüsselwort basierte Filterung*, Seite 191.
- **Dateitypen sperren**: Wenn das Sperren von Dateitypen aktiviert ist, wird Benutzern, die eine Datei mit einem gesperrten Dateityp herunterladen möchten, eine Sperrseite angezeigt, und die Datei wird nicht heruntergeladen. Siehe *Datenverkehr basierend auf Dateitypen verwalten*, Seite 205.

Verwenden von Quotenzeit für die Zugriffsbeschränkung für das Internet

Wenn ein Benutzer auf "Quotenzeit verwenden" klickt, werden Websites der entsprechenden Kategorie angezeigt, bis die Sitzung, bei der Quotenzeit verwendet wird, beendet ist. Die standardmäßig verfügbare Quotenzeit pro Sitzung (entsprechende Konfiguration auf der Seite **Einstellungen > Filterung (Filtering)**) beträgt 10 Minuten.

Hinweis

Die Option "Quote" sollte nicht verwendet werden, wenn einzelne Clients von mehreren Policy Servern verwaltet werden.

Andere Policy Server haben keinen Zugriff auf die Zeitsteuerung dieser Funktion, und den betroffenen Clients könnte ein breiterer oder geringerer Zugriff auf das Internet gewährt werden als beabsichtigt.

Wenn eine Sitzung, bei der Quotenzeit verwendet wird, beendet ist, wird bei einer Anforderung für eine Website, die Quotenzeit erfordert, eine Sperrmeldung für Quotenzeit angezeigt. Benutzer, deren tägliche Quotenzeitzuweisung noch nicht aufgebraucht ist, können eine neue Sitzung unter Verwendung von Quotenzeit starten.

Sobald Quotenzeit konfiguriert wurde, greift die Websense-Software bei der Bestimmung, wie auf die Benutzeranforderung einer Website reagiert wird, die Quotenzeit erfordert, auf eine Prioritätsliste zurück. Die Software berücksichtigt die folgenden konfigurierten Quotenzeiten:

1. Für den Benutzer
2. Für den Computer oder den Netzwerk-Client
3. Für Gruppen, zu denen der Benutzer gehört

   Wenn ein Benutzer Mitglied mehrerer Gruppen ist, gewährt die Websense-Software die Quotenzeit entsprechend der Einstellung **Restriktivere Filterung verwenden** auf der Seite **Einstellungen > Filterung (Filtering)** (siehe *Konfigurieren von Websense-Filtereinstellungen*, Seite 60).
4. Standardquotenzeit

Internet-Applets, wie z. B. Java- oder Flash-Applets, reagieren möglicherweise nicht erwartungsgemäß auf die Einschränkung durch Quotenzeit. Ein in einem Browser ausgeführtes Applet kann, auch wenn darauf von einer Website zugegriffen wird, über die konfigurierte Quotenzeit für eine Sitzung hinaus laufen.

Der Grund dafür ist, dass solche Appletts vollständig auf den Client-Computer heruntergeladen und wie eine Anwendung ausgeführt wird, ohne dabei Daten an den ursprünglichen Host-Server zu senden. Wenn der Benutzer im Browser auf die Schaltfläche zum Aktualisieren klickt, erkennt die Websense-Software jedoch die Kommunikation mit dem Host-Server, und sperrt daraufhin die Anforderungen entsprechend der geltenden Einschränkungen der Quotenzeit.

Freigabe mit Passwort

Durch die Freigabe mit Passwort können Benutzer mit einem gültigen Passwort auf Websites zugreifen, die durch die Websense-Software gesperrt werden. Die Freigabe mit Passwort kann individuellen Clients (Benutzern, Gruppen, Computern oder Netzwerken) gewährt werden.

Wenn die Option für die Freigabe mit Passwort aktiviert ist, enthalten Sperrmeldungen von Websense ein Feld für die Eingabe eines Passworts. Nach der Eingabe eines gültigen Passworts können Clients für einen befristeten Zeitraum auf gesperrte Seiten zugreifen.

> **Hinweis**
>
> Die Option für die Freigabe mit Passwort sollte nicht verwendet werden, wenn einzelne Clients von mehreren Policy Servern verwaltet werden.
>
> Andere Policy Server haben keinen Zugriff auf die Zeitsteuerung dieser Funktion, und den betroffenen Clients könnte ein breiterer oder geringerer Zugriff auf das Internet gewährt werden als beabsichtigt.

Die Option für die Freigabe mit Passwort wird über die Seite **Einstellungen > Filterung (Filtering)** aktiviert (siehe *Konfigurieren von Websense-Filtereinstellungen*, Seite 60).

Gewähren Sie bestimmten Clients die Berechtigungen für die Freigabe mit Passwort über die Seite **Richtlinienverwaltung > Clients** (siehe *Hinzufügen eines Clients*, Seite 73, oder *Ändern von Clienteinstellungen*, Seite 75).

Suchfilterung

Bei der Suchfilterung handelt es sich um eine Funktionalität, die von einigen Suchmaschinen zur Reduzierung der Anzahl ungeeigneter Suchergebnisse verwendet wird.

Normalerweise enthalten Internet-Suchmaschinen auch Miniaturansichten von Websites, die den Suchkriterien entsprechen. Wenn diese Miniaturansichten auf gesperrte Websites verweisen, verhindert die Websense-Software den Zugriff des Benutzers auf die eigentliche Website, lässt jedoch die Anzeige des Bildes in der Suchmaschine zu.

Wenn die Suchfilterung aktiviert wird, verwendet die Websense-Software eine Funktion für Suchmaschinen, die die Anzeige von Miniaturansichten in den Suchergebnissen verhindert, die auf gesperrte Seiten verweisen. Das Suchfilterung gilt sowohl für Clients für lokales als auch für Clients für fernes Filtern.

Websense, Inc., führt eine Datenbank mit Suchmaschinen mit Suchfilterungsfunktion. Wenn der Datenbank eine Suchmaschine hinzugefügt oder eine Suchmaschine daraus entfernt wird, wird ein Alert generiert (siehe *Alerts*, Seite 303).

Die Suchfilterung wird über die Seite **Einstellungen > Filterung (Filtering)** aktiviert. Weitere Informationen dazu finden Sie unter *Konfigurieren von Websense-Filtereinstellungen*, Seite 60.

Arbeiten mit Filtern

Verwandte Themen:

- *Filtern von Kategorien und Protokollen*, Seite 40
- *Filterrichtlinien für die Internetnutzung*, Seite 77
- *Erstellen von Kategoriefiltern*, Seite 52
- *Erstellen von Protokollfiltern*, Seite 55
- *Einen Filter für die Zugriffsbeschränkung erstellen*, Seite 180

Im Websense Manager auf der Seite **Richtlinienverwaltung > Filter** können Sie Kategorie- und Protokollfilter anzeigen, erstellen und ändern. Darüber hinaus finden Sie hier weitere Filter-Tools.

Die Seite "Filter" ist in drei Hauptbereiche eingeteilt:

- **Kategoriefilter** bestimmen, welche Kategorien gesperrt oder zugelassen werden.
- **Protokollfilter** bestimmen, welche Nicht-HTTP-Protokolle gesperrt oder zugelassen werden.

  Network Agent muss installiert sein, um eine protokollbasierte Filterung zu ermöglichen.
- **Filter für die Zugriffsbeschränkung** definieren eine einschränkende Liste zulässiger Websites (siehe *Benutzer auf eine festgelegte Liste von Internetsites einschränken*, Seite 178).

Die Kategorie- und Protokollfilter sowie die Filter für die Zugriffsbeschränkung bilden die Grundelemente der **Richtlinien**. Jede Richtlinie besteht aus mindestens einem Kategoriefilter oder einem Filter für Zugriffsbeschränkung und einem Protokollfilter, die entsprechend eines speziellen Plans auf ausgewählte Clients angewendet werden.

- Klicken Sie zum Prüfen eines vorhandenen Kategorie- oder Protokollfilters oder eines Filters für die Zugriffsbeschränkung auf den Filternamen. Weitere Informationen finden Sie unter:
  - *Bearbeiten eines Kategoriefilters*, Seite 53
  - *Bearbeiten eines Protokollfilters*, Seite 56
  - *Einen Filter für die Zulassungsbeschränkung bearbeiten*, Seite 181
- Klicken Sie zum Erstellen eines neuen Kategorie- oder Protokollfilters oder eines Filters für die Zugriffsbeschränkung auf **Hinzufügen**. Weitere Informationen finden Sie unter:
  - *Erstellen von Kategoriefiltern*, Seite 52
  - *Erstellen von Protokollfiltern*, Seite 55
  - *Einen Filter für die Zugriffsbeschränkung erstellen*, Seite 180

Wenn Sie einen vorhandenen Filter duplizieren möchten, aktivieren Sie das Kontrollkästchen neben dem Filternamen, und klicken Sie anschließend auf **Kopieren**. Für die Kopie wird der Name des Originalfilters verwendet und durch eine angehängte Nummerierung eindeutig gemacht. Anschließend wird die Kopie zur Liste der Filter hinzugefügt. Sie können die Kopie wie jeden anderen Filter bearbeiten.

Wenn Sie Rollen für die delegierte Verwaltung erstellt haben (siehe *Delegierte Verwaltung*, Seite 251), können übergeordnete Administratoren (Super Administrators) von Ihnen erzeugte Filter in andere Rollen kopieren, um diese delegierten Administratoren zur Verfügung zu stellen.

Wenn Sie Filter in eine andere Rolle kopieren möchten, aktivieren Sie zunächst das Kontrollkästchen neben dem Filternamen, und klicken Sie anschließend auf **Kopieren zu Rolle**. Weitere Informationen dazu finden Sie unter *Filter und Richtlinien in Rollen kopieren*, Seite 183.

Erstellen von Kategoriefiltern

Verwandte Themen:

- *Arbeiten mit Filtern*, Seite 51
- *Bearbeiten eines Kategoriefilters*, Seite 53

Auf der Seite **Richtlinienverwaltung > Filter > Kategoriefilter hinzufügen** können Sie einen neuen Kategoriefilter erstellen. Sie können als Basis für den neuen Filter eine vordefinierte Vorlage oder eine Kopie eines vorhandenen Kategoriefilters verwenden.

1. Geben Sie unter **Name des Filters** einen eindeutigen Filternamen ein. Der Name muss zwischen 1 und 50 Zeichen lang sein und darf keines der folgenden Zeichen enthalten:

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Filternamen dürfen Leerzeichen, Bindestriche und Apostrophe enthalten.
2. Geben Sie eine kurze **Beschreibung** für den Filter ein. Diese Beschreibung wird auf der Seite "Filter" im Bereich "Kategoriefilter" neben dem Filternamen angezeigt und sollte den Zweck des Filters erläutern.

   Die Zeichenbeschränkungen für Filternamen gelten auch für Beschreibungen, mit den folgenden zwei Ausnahmen: Beschreibungen dürfen Punkte (.) und Kommas (,) enthalten.
3. Wählen Sie einen Eintrag in der Dropdown-Liste aus, und bestimmen Sie damit, ob eine Vorlage oder eine Kopie eines vorhandenen Filters verwendet wird. Weitere Informationen über Vorlagen finden Sie unter *Vorlagen für Kategorie- und Protokollfilter*, Seite 58.
4. Wenn Sie den neuen Filter anzeigen und bearbeiten möchten, klicken Sie auf **OK**. Der Filter wird auf der Seite "Filter" zur Liste **Kategoriefilter** hinzugefügt.

Wenn Sie den Filter anpassen möchten, klicken Sie auf den Filternamen. Fahren Sie anschließend mit *Bearbeiten eines Kategoriefilters* fort.

Bearbeiten eines Kategoriefilters

Verwandte Themen:

- *Filtern von Kategorien und Protokollen*, Seite 40
- *Filteraktionen*, Seite 47
- *Verwenden von Quotenzeit für die Zugriffsbeschränkung für das Internet*, Seite 48
- *Freigabe mit Passwort*, Seite 49
- *Arbeiten mit Filtern*, Seite 51
- *Arbeiten mit Kategorien*, Seite 186

Auf der Seite **Richtlinienverwaltung > Filter > Kategoriefilter bearbeiten** können Sie Änderungen an vorhandenen Kategoriefiltern vornehmen.

Wichtig

Wenn Sie einen Kategoriefilter bearbeiten, wirken sich die Änderungen auf jede Richtlinie aus, die diesen Filter einsetzt.

Richtlinien, die einen Kategoriefilter mit demselben Namen in einer anderen Rolle für die delegierte Verwaltung einsetzen, sind nicht betroffen.

Der Filtername und die Beschreibung werden im oberen Bereich der Seite angezeigt.

- Klicken Sie auf **Umbenennen**, um den Filternamen zu ändern.
- Geben Sie einfach Text in das Feld **Beschreibung** ein, um die Filterbeschreibung zu ändern.

Die Zahl neben der Option **Folgende Richtlinien verwenden diesen Filter** gibt an, wie viele Richtlinien derzeit den ausgewählten Filter verwenden. Wenn der Kategoriefilter aktiviert ist, klicken Sie auf **Richtlinien anzeigen**, um eine Liste der Richtlinien anzuzeigen, die diesen Filter verwenden.

Der untere Bereich der Seite enthält eine Liste der Kategorien sowie die jeweils aktuell angewendeten Aktionen.

1. Wählen Sie einen Eintrag in der Liste **Kategorien**, um Kategorieinformationen anzuzeigen oder die der gewählten Kategorie zugewiesenen Filteraktionen zu ändern.
2. Bevor Sie Änderungen an einer Aktion vornehmen, die einer Kategorie zugewiesen ist, prüfen Sie im Bereich **Kategoriedetails** alle Spezialattribute, die mit der Kategorie verbunden sind.
   - Wenn Sie (sofern vorhanden) einer Kategorie erneut zugeordnete oder ungefilterte URLs prüfen möchten, klicken Sie auf **Benutzerdefinierte URLs**

in dieser Kategorie anzeigen. Siehe *Filter für bestimmte Sites neu definieren*, Seite 193.

- Wenn Sie dieser Kategorie zugeordnete Schlüsselworte prüfen möchten, klicken Sie auf **Schlüsselworte in dieser Kategorie anzeigen**. Siehe *Auf Schlüsselwort basierte Filterung*, Seite 191.
- Wenn Sie reguläre Ausdrücke prüfen möchten, die für die Definition benutzerdefinierter URLs oder Schlüsselworte für die Kategorie verwendet wurden, klicken Sie auf **Reguläre Ausdrücke in dieser Kategorie anzeigen**.

3. Verwenden Sie die Schaltflächen im unteren Bereich der Kategorieliste, um die auf die gewählte Kategorie angewendete Aktion zu ändern. Weitere Informationen über die verfügbaren Aktionen finden Sie unter *Filteraktionen*, Seite 47.

   Delegierte Administratoren können nicht Aktionen in Kategorien ändern, die von einem übergeordneten Administrator (Super Administrator) gesperrt wurden. Weitere Informationen dazu finden Sie unter *Definieren von Filtereinschränkungen für alle Rollen*, Seite 282.

4. Verwenden Sie die Kontrollkästchen rechts neben der Liste "Kategorien", um erweiterte Filteraktionen auf die ausgewählte Kategorie anzuwenden:

   - Wenn Sie die Art und Weise ändern möchten, wie Schlüsselworte bei der Filterung der ausgewählten Kategorie verwendet werden, aktivieren oder deaktivieren Sie **Schlüsselworte sperren**. *Auf Schlüsselwort basierte Filterung*, Seite 191.
   - Wenn Sie bestimmen möchten, ob Benutzer auf bestimmte Dateitypen von Websites in der ausgewählten Kategorie zugreifen können, aktivieren oder deaktivieren Sie **Dateitypen sperren**. Siehe *Datenverkehr basierend auf Dateitypen verwalten*, Seite 205.

     Wenn Sie sich für das Sperren von Dateitypen entschieden haben, wählen Sie einen oder mehrere Dateitypen, die gesperrt werden sollen.
   - Wenn Sie festlegen möchten, ob der Zugriff auf Websites in der Kategorie basierend auf bestimmten Bandbreiten-Schwellenwerten eingeschränkt werden soll, aktivieren oder deaktivieren Sie **Sperrung durch Bandwidth Optimizer**. Siehe *Bandbreite mit Bandwidth Optimizer verwalten*, Seite 203.

     Wenn eine Sperrung basierend auf der Bandbreite vorgenommen werden soll, geben Sie an, welche Schwellenwerte verwendet werden sollen.

5. Wiederholen Sie die Schritte 1 bis 3, um Änderungen an den auf andere Kategorien angewendeten Filtern vorzunehmen.
6. Nachdem Sie den Filter bearbeitet haben, klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern und zur Seite "Filter" zurückzukehren. Die Änderungen werden erst übernommen, wenn Sie auf **Alles speichern** klicken.

Wenn Sie den neuen Kategoriefilter aktivieren möchten, fügen Sie ihn zu einer Richtlinie hinzu und ordnen die Richtlinie Clients zu. Siehe *Filterrichtlinien für die Internetnutzung*, Seite 77.

Erstellen von Protokollfiltern

Verwandte Themen:

- *Filtern von Kategorien und Protokollen*, Seite 40
- *Filteraktionen*, Seite 47
- *Bearbeiten eines Protokollfilters*, Seite 56
- *Arbeiten mit Protokollen*, Seite 196

Auf der Seite **Richtlinienverwaltung > Filter > Protokollfilter hinzufügen** können Sie einen neuen Protokollfilter definieren. Sie können als Basis für den neuen Filter eine vordefinierte Vorlage oder eine Kopie eines vorhandenen Protokollfilters verwenden.

1. Geben Sie unter **Name des Filters** einen eindeutigen Filternamen ein. Der Name muss zwischen 1 und 50 Zeichen lang sein und darf keines der folgenden Zeichen enthalten:

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Filternamen dürfen Leerzeichen, Bindestriche und Apostrophe enthalten.
2. Geben Sie eine kurze **Beschreibung** für den Filter ein. Diese Beschreibung wird auf der Seite "Filter" im Bereich "Protokollfilter" neben dem Filternamen angezeigt und sollte den Zweck des Filters erläutern.

   Die Zeichenbeschränkungen für Filternamen gelten auch für Beschreibungen, mit den folgenden zwei Ausnahmen: Beschreibungen dürfen Punkte (.) und Kommas (,) enthalten.
3. Wählen Sie einen Eintrag in der Dropdown-Liste aus, und bestimmen Sie damit, ob als Basis für den neuen Filter eine Vorlage (siehe *Vorlagen für Kategorie- und Protokollfilter*, Seite 58) oder eine Kopie eines vorhandenen Filters verwendet wird.
4. Wenn Sie den neuen Filter anzeigen und bearbeiten möchten, klicken Sie auf **OK**. Der Filter wird auf der Seite "Filter" zur Liste **Protokollfilter** hinzugefügt.

Schließen Sie das Anpassen eines neuen Filters mit *Bearbeiten eines Protokollfilters* ab.

Bearbeiten eines Protokollfilters

Verwandte Themen:

- *Filtern von Kategorien und Protokollen*, Seite 40
- *Erstellen von Protokollfiltern*, Seite 55
- *Filteraktionen*, Seite 47
- *Arbeiten mit Protokollen*, Seite 196
- *Bandbreite mit Bandwidth Optimizer verwalten*, Seite 203

Auf der Seite **Richtlinienverwaltung > Filter > Protokollfilter bearbeiten** können Sie Änderungen an vorhandenen Protokollfiltern vornehmen.

Wichtig

Die an dieser Stelle vorgenommenen Änderungen wirken sich auf alle Richtlinien aus, die diesen Filter umsetzen.

Richtlinien, die einen Protokollfilter mit demselben Namen in einer anderen Rolle für die delegierte Verwaltung einsetzen, sind nicht betroffen.

Der Filtername und die Beschreibung werden im oberen Bereich der Seite angezeigt.

- Klicken Sie auf **Umbenennen**, um den Filternamen zu ändern.
- Geben Sie einfach Text in das Feld **Beschreibung** ein, um die Filterbeschreibung zu ändern.

Die Zahl neben der Option **Folgende Richtlinien verwenden diesen Filter** gibt an, wie viele Richtlinien derzeit den ausgewählten Filter verwenden. Wenn der Protokollfilter aktiviert ist, klicken Sie auf **Richtlinien anzeigen**, um eine Liste der Richtlinien anzuzeigen, die diesen Filter verwenden.

Der untere Bereich der Seite enthält eine Liste der Protokolle sowie die jeweils aktuell angewendeten Aktionen.

So ändern Sie die Art und Weise, wie Protokolle gefiltert und protokolliert werden:

1. Wählen Sie ein Protokoll in der Liste **Protokolle** aus. Rechts in der Liste werden erweiterte Filteraktionen für das ausgewählte Protokoll angezeigt.

2. Verwenden Sie die Schaltflächen **Zulassen** und **Sperren** im unteren Bereich der Protokollliste, um die auf das gewählte Protokoll angewendete Aktion zu ändern.

   Hinweis

   Die Websense-Software kann Anfragen für TCP-basierte Protokolle sperren, jedoch nicht Anfragen für UDP-basierte Protokolle.

   Einige Anwendungen verwenden sowohl TCP- als auch UDP-basierte Nachrichten. Wenn eine Anfrage des ursprünglichen Netzwerks einer Anwendung per TCP erfolgt und darauf folgende Daten per UDP gesendet werden, sperrt die Websense-Software die ursprüngliche TCP-Anforderung und somit den folgenden UDP-Datenverkehr.

   UDP-Anforderungen werden möglicherweise als gesperrt protokolliert, auch wenn sie zulässig sind.

   Wenn Sie dieselbe Aktion auf andere Protokolle in der ausgewählten Protokollgruppe anwenden möchten, klicken Sie auf **Auf Gruppe anwenden**.

3. Wenn Sie Informationen über die Nutzung des ausgewählten Protokolls für eine Bearbeitung oder Berichterstellung benötigen, aktivieren Sie das Kontrollkästchen **Protokolldaten protokollieren**.
4. Wenn Sie einen Bandbreitengrenzwert für die Nutzung dieses Protokolls einrichten möchten, klicken Sie auf **Sperrung durch Bandwidth Optimizer**, und geben Sie anschließend die zu verwendenden Bandbreiten-Schwellenwerte ein. Weitere Informationen dazu finden Sie unter *Bandbreite mit Bandwidth Optimizer verwalten*, Seite 203.
5. Nachdem Sie den Filter bearbeitet haben, klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern und zur Seite "Filter" zurückzukehren. Die Änderungen werden erst übernommen, wenn Sie auf **Alles speichern** klicken.

Wenn Sie den neuen Protokollfilter aktivieren möchten, fügen Sie ihn zu einer Richtlinie hinzu und weisen die Richtlinie Clients zu (siehe *Filterrichtlinien für die Internetnutzung*, Seite 77).

Hinweis

Sie können Richtlinien erstellen, die die Umsetzung eines Protokollfilters zu einem bestimmten Zeitpunkt starten. Wenn Benutzer eine Protokollsitzung starten, bevor dieser Filter umgesetzt wird, können Sie weiterhin bis zum Ende der Sitzung auf das Protokoll zugreifen, auch wenn es durch das Protokoll gesperrt wird. Sobald ein Benutzer die Sitzung beendet, werden weitere Anforderungen für das Protokoll gesperrt.

Von Websense definierte Kategorie- und Protokollfilter

Die Websense-Software enthält mehrere Muster für Kategorie- und Protokollfilter. Sie können diese Filter unverändert verwenden oder gemäß Ihrer Anforderungen anpassen. Wenn Sie sie nicht benötigen, kann eine Vielzahl der vordefinierten Filter gelöscht werden.

Die vordefinierten Kategoriefilter sind:

- Basis
- Basissicherheit
- Alles sperren
- Standard
- Nur überwachen
- Alles zulassen

Die Kategoriefilter "Alles sperren" und "Alles zulassen" sind nicht auf der Seite "Filter" enthalten, obwohl Sie zu Richtlinien hinzugefügt werden können. Diese Filter haben eine besondere Funktion bei der Filterung und können nicht gelöscht oder bearbeitet werden. Wenn eine Internetanforderung gefiltert wird, prüft die Websense-Software zunächst, ob die Filter "Alles sperren" oder "Alles zulassen" greifen, bevor die Anwendung weiterer Filter geprüft wird (siehe *Filtern einer Site*, Seite 85).

Die vordefinierten Protokollfilter sind:

- Basissicherheit
- Standard
- Nur überwachen
- Alles zulassen

Der Protokollfilter "Alles zulassen" wird wie der entsprechende Kategoriefilter nicht auf der Seite "Filter" angezeigt und kann nicht bearbeitet oder gelöscht werden. Er wird ebenfalls bei der Filterung priorisiert.

Die Kategorie- und Protokollfilter "Standard" können bearbeitet, jedoch nicht gelöscht werden. In Upgrade-Umgebungen werden bei Lücken in der Standardrichtlinie die Standardfilter dazu verwendet, Anforderungen zu filtern, auf die keine Richtlinie zutrifft.

Vorlagen für Kategorie- und Protokollfilter

Wenn Sie einen neuen Kategorie- oder Protokollfilter erstellen, können Sie als Basis dafür auf der Seite "Filter" eine Kopie eines vorhandenen Filters machen, auf der Seite "Filter hinzufügen" einen vorhandenen Filter als Modell auswählen oder eine **Vorlage** für Filter verwenden.

Die Websense-Software enthält 5 Vorlagen für Kategoriefilter:

- Mit **Nur überwachen** und **Alles zulassen** werden alle Kategorien zugelassen.
- Mit **Alles sperren** werden alle Kategorien gesperrt.

- Mit **Basis** werden die am häufigsten gesperrten Kategorien gesperrt und alle weiteren Kategorien zugelassen.
- Mit **Standard** werden die Aktionen "Sperren", "Zulassen", "Weiter" und "Quote" auf Kategorien angewendet.
- Mit **Basissicherheit** werden nur Standardkategorien in der Sicherheitsrisikoklasse gesperrt (siehe *Risikoklassen*, Seite 43).

Die Websense-Software enthält außerdem 3 Vorlagen für Protokollfilter:

- Mit **Nur überwachen** und **Alles zulassen** werden alle Protokolle zugelassen.
- Mit **Basissicherheit** werden die Protokolle für die gemeinsame Nutzung von Dateien über Peer-to-Peer-Datenaustausch (P2P) und die Umgehung durch Proxy sowie für Dateianhänge beim Instant Messaging (sofern subskribiert) und bösartigen Datenverkehr (Websense Web Security) gesperrt.
- Mit **Standard** werden die Protokolle für Instant Messaging/Chat sowie die gemeinsame Nutzung von Dateien über Peer-to-Peer-Datenaustausch (P2P), die Umgehung durch Proxy, Dateianhänge beim Instant Messaging (sofern subskribiert) und bösartigen Datenverkehr (Websense Web Security) gesperrt.

Obwohl Sie die meisten von Websense definierten Kategorie- und Protokollfilter ändern oder löschen können, können Vorlagen nicht geändert oder entfernt werden. Gleichermaßen können Sie beliebig viele benutzerdefinierte Filter erstellen, jedoch keine neuen Vorlagen erstellen.

Da Vorlagennicht geändert werden können, wird damit kontinuierlich auf die ursprünglichen Filteraktionen der von Websense definierten Filter verwiesen. So werden mit den Vorlagen für Kategorie- und Protokollfilter "Standard" dieselben Aktionen wie bei den ursprünglichen Kartegorie- und Protokollfiltern "Standard" angewendet. Dies führt dazu, dass Sie die ursprüngliche Filterkonfiguration von Websense zu jeder Zeit wiederherstellen können, indem Sie Filter erstellen, die die Standardeinstellungen der Vorlage verwenden.

Anweisungen dazu, wie Vorlagen für das Erstellen eines neuen Filters verwendet werden, finden Sie unter *Erstellen von Kategoriefiltern*, Seite 52, or *Erstellen von Protokollfiltern*, Seite 55.

Konfigurieren von Websense-Filtereinstellungen

Verwandte Themen:

- *Filtern von Kategorien und Protokollen*, Seite 40
- *Clients*, Seite 63
- *Sperren von Seiten*, Seite 89
- *Filteraktionen*, Seite 47
- *Freigabe mit Passwort*, Seite 49
- *Filterreihenfolge*, Seite 84
- *Bandbreite mit Bandwidth Optimizer verwalten*, Seite 203
- *Auf Schlüsselwort basierte Filterung*, Seite 191

Auf der Seite **Einstellungen > Filterung (Filtering)** können Sie Basiseinstellungen für eine Reihe von Filterfunktionen vornehmen.

Geben Sie unter **Bandwidth Optimizer** die Daten ein, die für das Filtern der Internetnutzung basierend auf der verfügbaren Bandbreite erforderlich sind. Weitere Informationen über eine auf der Bandbreite basierende Filterung finden Sie unter *Bandbreite mit Bandwidth Optimizer verwalten*, Seite 203.

1. Wählen Sie zum Festlegen einer **Geschwindigkeit der Internetverbindung** eine der folgenden Vorgehensweisen:
   - Wählen Sie eine Standardgeschwindigkeit aus der Dropdown-Liste aus.
   - Geben Sie in das Textfeld eine Netzwerkgeschwindigkeit in Kilobit per Sekunde ein.
2. Geben Sie in das Feld **Standardbandbreite für Netzwerk** einen Standardgrenzwert (Prozentsatz des Gesamt-Netzwerkdatenverkehrs) ein, der verwendet wird, wenn die Filterung basierend auf der Netzwerkbandbreite aktiviert ist.
3. Geben Sie im Feld **Standardbandbreite pro Protokoll** einen Standardgrenzwert ein, der verwendet wird, wenn die Filterung auf Basis der Protokollbandbreite aktiviert ist.

Bestimmen Sie im Abschnitt **Allgemeine Filterfunktionen**, wie Benutzer gefiltert werden, wenn mehrere Gruppenrichtlinien greifen, wählen Sie Optionen für die Schlüsselwortsuche und legen Sie das Verhalten bei Sitzungen unter den Optionen "Freigabe mit Passwort", "Weiter" und "Quote" fest.

1. Wenn Sie bestimmen möchten, wie Benutzer gefiltert werden, wenn mehrere Gruppenrichtlinien zutreffen, aktivieren oder deaktivieren Sie **Gruppenrichtlinie mit stärkster Restriktion verwenden** (siehe *Filterreihenfolge*, Seite 84).
   - Wenn die Option aktiviert ist, wird die Richtlinie verwendet, die über die stärkste Restriktion verfügt. Mit anderen Worten, wenn eine zutreffende Gruppenrichtlinie den Zugriff auf eine Kategorie sperrt und eine andere den

Zugriff zulässt, wird die Benutzeranforderung für eine Website in dieser Kategorie gesperrt.

- Wenn die Option deaktiviert ist, wird die Einstellung mit den meisten Berechtigungen verwendet.

2. Wählen Sie eine der folgenden **Optionen für die Schlüsselwortsuche** (siehe *Auf Schlüsselwort basierte Filterung*, Seite 191).

nur CGI	Sperrt Websites, wenn Schlüsselworte in CGI-Abfragezeichenfolgen enthalten sind (nach dem "?" in einer Internetadresse). Beispiel: **search.yahoo.com/search?p=test** Wenn diese Option aktiviert ist, sucht die Websense-Software nicht vor dem "?" nach Schlüsselworten.
nur URL	Sperrt Websites, wenn in der URL Schlüsselworte enthalten sind. Wenn die angeforderte Adresse eine CGI-Abfragezeichenkette enthält, sucht die Websense-Software bis zum "?" nach Schlüsselworten.
URL und CGI	Sperrt Websites, wenn an einer beliebigen Position in der Adresse Schlüsselworte enthalten sind. Wenn eine CGI-Abfragezeichenkette enthalten ist, sucht die Websense-Software vor und nach dem "?" nach Schlüsselworten.
Sperrfunktion für Schlüsselworte deaktivieren	Gehen Sie bei der Verwendung vorsichtig vor. Mit **Sperrfunktion für Schlüsselworte deaktivieren** wird die gesamte Sperrfunktion für Schlüsselworte deaktiviert, auch wenn in einem Kategoriefilter die Option **Schlüsselworte sperren** ausgewählt wurde.

3. Geben Sie im Feld **Zeitlimit für die Freigabe mit Passwort** den maximalen Zeitraum in Sekunden ein (bis zu 3.600, standardmäßig 60), über den ein Benutzer auf Websites in allen Kategorien zugreifen kann, nachdem die Freigabe mit Passwort gewählt wurde (siehe *Freigabe mit Passwort*, Seite 49).
4. Geben Sie im Feld **Zeitlimit für 'Weiter'** den maximalen Zeitraum in Sekunden ein (bis zu 3.600, standardmäßig 60), den ein Benutzer, der auf die Schaltfläche "Weiter" klickt, auf Websites in Kategorien zugreifen kann, die von der Aktion "Bestätigen" geregelt werden (siehe *Filteraktionen*, Seite 47).
5. Geben Sie im Feld **Dauer von Sitzungen, bei denen Quotenzeit vom Zeitkonto verwendet wird** den Intervall ein (bis zu 60 Minuten, standardmäßig 10), während dessen Benutzer auf Websites in durch Quoten begrenzten Kategorien zugreifen können (siehe *Verwenden von Quotenzeit für die Zugriffsbeschränkung für das Internet*, Seite 48).

   Eine Sitzung beginnt, wenn der Benutzer auf die Schaltfläche "Quotenzeit verwenden" klickt.
6. Geben Sie die **Standardmäßig verfügbare Quotenzeit pro Tag** für alle Benutzer ein (bis zu 240 Minuten, standardmäßig 60).

   Wenn Sie die Quotenzeit für individuelle Benutzer ändern möchten, öffnen Sie die Seite **Richtlinien > Clients**.

Während Sie Änderungen an der Dauer von Sitzungen, bei denen Quotenzeit vom Zeitkonto verwendet wird, vornehmen, wird die **Standardanzahl von Sitzungen pro Tag, bei denen Quotenzeit verwendet wird** entsprechend berechnet und angezeigt.

Geben Sie im Bereich **Sperrmeldung** die URL oder den Pfad zu einer alternativen HTML-Sperrseite ein, die Sie für den oberen Frame browserbasierter Sperrmeldungen erstellt haben (siehe *Erstellen von alternativen Sperrmeldungen*, Seite 96).

- Für die verschiedenen Protokolle **FTP**, **HTTP** (einschließlich **HTTPS**) und **Gopher** können unterschiedliche Seiten verwendet werden.
- Lassen Sie diese Felder frei, wenn Sie die Standardsperrmeldung der Websense-Software oder eine angepasste Version dieser Meldung verwenden möchten (siehe *Anpassen der Sperrmeldung*, Seite 92).

Wählen Sie unter **Suchfilterung** die Option **Suchfilterung aktivieren**, wenn die Websense-Software eine in bestimmte Suchmaschinen integrierte Einstellung aktivieren soll, die die Anzeige eindeutiger Miniaturansichten und anderer expliziter Inhalte gesperrter Websites in den Suchergebnissen verhindert (siehe *Suchfilterung*, Seite 50).

Eine Liste der Suchmaschinen, für die diese Funktion unterstützt wird, befindet sich am Ende des Abschnitts.

Wenn Sie die Konfiguration der Filtereinstellungen abgeschlossen haben, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst übernommen, wenn Sie auf **Alles speichern** klicken.

3 Clients

Sie können die Art und Weise anpassen, wie Anforderungen von bestimmten Benutzern oder Computern in der Websense-Software behandelt werden, indem Sie sie in Websense Manager als **Clients** hinzufügen. Folgendes kann als Client hinzugefügt werden:

- **Computer**: Individuelle Rechner in Ihrem Netzwerk, definiert durch eine IP-Adresse.
- **Netzwerke**: Gruppen von Computern, kollektiv durch einen IP-Adressbereich definiert.
- **Benutzer**: Benutzer-, Gruppen- oder Domänenkonten in einem unterstützten Verzeichnisdienst.

In der Ausgangskonfiguration filtert die Websense-Software alle Clients auf dieselbe Weise. Dazu wird die Richtlinie **Standard** verwendet (siehe *Die Richtlinie "Standard"*, Seite 78). Nachdem Sie einen Client in Websense Manager zur Seite "Clients" hinzugefügt haben, können Sie diesen Client einer bestimmten Filterrichtlinie hinzufügen.

Wenn mehrere Richtlinien gelten, wenn z. B. eine Richtlinie für den Benutzer und eine weitere für den Computer gilt, bestimmt die Websense-Software, welche Richtlinie durchgesetzt wird. Dabei wird folgendermaßen vorgegangen:

1. Es wird die Richtlinie verwendet, die dem **Benutzer**, der die Anforderung stellt, zugewiesen wurde. Wenn diese Richtlinie zum Zeitpunkt der Anforderung über keine geplanten Filter verfügt, wird die nächste zutreffende Richtlinie verwendet.
2. Wenn keine benutzerspezifische Richtlinie vorhanden ist oder die Richtlinie zum Zeitpunkt der Anforderung über keine aktiven Filter verfügt, wird nach einer Richtlinie gesucht, die (erstens) dem **Computer** oder (zweitens) dem **Netzwerk** zugewiesen ist, von dem die Anforderung gestellt wurde.
3. Wenn keine Richtlinie für den Computer oder das Netzwerk vorhanden ist oder die Richtlinie zum Zeitpunkt der Anforderung über keine aktiven Filter verfügt, wird nach einer Richtlinie gesucht, die einer beliebigen **Gruppe** zugewiesen ist, der der Benutzer angehört. Wenn der Benutzer zu mehreren Gruppen gehört, berücksichtigt die Websense-Software alle Gruppenrichtlinien, die gelten können (siehe *Filterreihenfolge*, Seite 84).
4. Wenn keine Gruppenrichtlinie vorhanden ist, wird nach einer Richtlinie gesucht, die der **Domäne** (OU) des Benutzer zugewiesen wurde.

5. Wenn keine geltende Richtlinie gefunden wurde oder die Richtlinie zum Zeitpunkt der Anforderung keinen Kategoriefilter durchsetzt, wird die Richtlinie **Standard** für die Rolle verwendet, der der Client zugewiesen wurde.

Weitere Informationen darüber, wie die Websense-Software Filterrichtlinien auf Clients anwendet, finden Sie unter *Filtern einer Site*, Seite 85.

Arbeiten mit Clients

Verwandte Themen:

- *Clients*, Seite 63
- *Arbeiten mit Computern und Netzwerken*, Seite 65
- *Arbeiten mit Benutzern und Gruppen*, Seite 66
- *Hinzufügen eines Clients*, Seite 73
- *Ändern von Clienteinstellungen*, Seite 75

Auf der Seite **Richtlinienverwaltung > Clients** können Sie Informationen über vorhandene Clients anzeigen, Clients hinzufügen, bearbeiten oder löschen oder Clients zu einer Rolle für die delegierte Verwaltung verschieben.

Wenn Sie ein delegierter Administrator sind, müssen Sie Clients zu Ihrer Liste verwalteter Clients hinzufügen, damit diese auf der Seite "Clients" angezeigt werden. Anweisungen dazu finden Sie unter *Hinzufügen eines Clients*, Seite 73.

Clients werden in drei Gruppen aufgeteilt:

- **Verzeichnis**: Dazu gehören Benutzer, Gruppen und Domänen Ihres Verzeichnisdienstes (siehe *Arbeiten mit Benutzern und Gruppen*, Seite 66).
- **Netzwerke**: IP-Adressbereiche innerhalb des gefilterten Netzwerks, die mit einer einzigen Richtlinie geregelt werden können (siehe *Arbeiten mit Computern und Netzwerken*, Seite 65).
- **Computer**: individuelle Rechner in einem gefilterten Netzwerk, identifiziert durch IP-Adressen (siehe *Arbeiten mit Computern und Netzwerken*, Seite 65).

Klicken Sie auf das Pluszeichen (+) neben dem Clienttyp, um eine Liste der vorhandenen Clients des ausgewählten Typs anzuzeigen. Die aufgelisteten Clients enthalten zusätzlich folgende Informationen:

- Den Clientnamen, die IP-Adresse oder den IP-Adressbereich.
- Die dem Client aktuell zugewiesene **Richtlinie**. Die Richtlinie **Standard** wird so lange verwendet, bis Sie eine andere Richtlinie zuweisen (siehe *Filterrichtlinien für die Internetnutzung*, Seite 77).
- Ob der Client die Option **Mit Passwort freigeben** verwenden kann, um gesperrte Websites anzuzeigen (siehe *Freigabe mit Passwort*, Seite 49).

- Ob dem Client eine benutzerdefinierte **Quotenzeit** zugewiesen wurde (siehe *Verwenden von Quotenzeit für die Zugriffsbeschränkung für das Internet*, Seite 48).

Wenn Sie einen bestimmten Client suchen, wechseln Sie zum entsprechenden Knoten in der Verzeichnisstruktur.

Wenn Sie die Einstellungen einer Clientrichtlinie, der Freigabe mit Passwort, der Quotenzeit oder der Authentifizierung bearbeiten möchten, wählen Sie einen oder mehrere Clients in der Liste aus, und klicken Sie anschließend auf **Bearbeiten**. Weitere Informationen dazu finden Sie unter *Ändern von Clienteinstellungen*, Seite 75.

Wenn Sie einen Client hinzufügen oder eine Richtlinie auf einen verwalteten Client anwenden möchten, der derzeit nicht auf der Seite "Clients" angezeigt wird, klicken Sie auf **Hinzufügen**. Weitere Informationen für die dann folgende Vorgehensweise finden Sie unter *Hinzufügen eines Clients*, Seite 73.

Wenn Sie Rollen für die delegierte Verwaltung erstellt haben (siehe *Delegierte Verwaltung*, Seite 251), können übergeordnete Administratoren (Super Administrators) ihre Clients zu anderen Rollen verschieben. Aktivieren Sie zunächst das Kontrollkästchen neben dem Clienteintrag, und klicken Sie anschließend auf **Verschieben zu Rolle**. Wenn ein Client zu einer Rolle für die delegierte Verwaltung verschoben wird, werden die ihm zugewiesene Richtlinie und die Filter zur Rolle kopiert. Weitere Informationen dazu finden Sie unter *Verschieben von Clients zu Rollen*, Seite 75.

Wenn Sie die Websense-Software für die Kommunikation mit einem LDAP-basierten Verzeichnisdienst konfiguriert haben, wird die Schaltfläche **Benutzerdefinierte LDAP-Gruppen verwalten** in der Symbolleiste im oberen Bereich der Seite angezeigt. Klicken Sie auf diese Schaltfläche, um auf einem LDAP-Attribut basierende Gruppen zu bearbeiten (siehe *Arbeiten mit benutzerdefinierten LDAP-Gruppen*, Seite 71).

Wenn Sie einen Client aus dem Websense Manager entfernen möchten, wählen Sie den Client und klicken auf **Löschen**.

Arbeiten mit Computern und Netzwerken

Verwandte Themen:

- *Arbeiten mit Clients*, Seite 64
- *Arbeiten mit Benutzern und Gruppen*, Seite 66
- *Hinzufügen eines Clients*, Seite 73
- *Zuweisen einer Richtlinie an Clients*, Seite 83

In Websense Manager handelt es sich bei einem **Computer** um die IP-Adresse eines Rechners (z. B. 10.201.3.1), dessen Aktivitäten gefiltert werden. Ein **Netzwerk** ist der einer Gruppe von Rechnern, deren Aktivitäten gefiltert werden, zugewiesene IP-Adressbereich (z. B. 10.201.3.2 - 10.201.3.44).

Computer- und Netzwerkclients können auf dieselbe Weise wie Benutzer-, Gruppen- oder Domänenclients Richtlinien zugewiesen werden.

- Weisen Sie z. B. einem **Computer** eine Richtlinie zu, bei der sich die Benutzer nicht anmelden müssen oder bei der sich die Benutzer mit einem Gastkonto anmelden können.
- Weisen Sie einem **Netzwerk** eine Richtlinie zu, um dieselben Filterrichtlinien mehreren Computern gleichzeitig zuzuweisen.

Wenn Sie einem Computer oder einem Netzwerk eine Richtlinie zuweisen, wird diese Richtlinie unabhängig davon, wer am Computer angemeldet ist, dessen Aktivitäten gefiltert werden, durchgesetzt, **es sei denn** Sie haben dem angemeldeten Benutzer eine Richtlinie zugewiesen. Diese Computer- oder Netzwerkrichtlinie hat Vorrang vor jeglichen **Gruppenrichtlinien**, die für den Benutzer gelten könnten.

Arbeiten mit Benutzern und Gruppen

Verwandte Themen:

- *Arbeiten mit Clients*, Seite 64
- *Verzeichnisdienste*, Seite 67
- *Arbeiten mit benutzerdefinierten LDAP-Gruppen*, Seite 71
- *Arbeiten mit Computern und Netzwerken*, Seite 65
- *Hinzufügen eines Clients*, Seite 73
- *Zuweisen einer Richtlinie an Clients*, Seite 83

Um individuellen Benutzern und Gruppen in Ihrem Netzwerk Richtlinien zuzuweisen, konfigurieren Sie die Websense-Software so, dass sie auf Ihren Verzeichnisdienst zugreift, um Informationen über das Verzeichnisobjekt (Benutzer, Gruppe, Domäne und Organisationseinheit) abzurufen.

Die Websense-Software kann mit Windows NT Directory/Active Directory (Mixed Mode) kommunizieren. Auf Windows Active Directory, Novell eDirectory und Sun

Java System Directory wird über das Lightweight Directory Access Protocol (LDAP) zugegriffen.

> **Hinweis**
>
> LDAP-basierte Verzeichnisdienste unterstützen keine doppelten Benutzernamen. Stellen Sie sicher, dass ein Benutzername nicht in mehreren Domänen verwendet wird.
>
> Darüber hinaus werden keine Benutzernamen mit leerem Passwort unterstützt, wenn Sie Windows Active Directory oder Sun Java System Directory verwenden. Stellen Sie sicher, dass allen Benutzern Passwörter zugewiesen wurden.

Der Websense User Service übermittelt Informationen vom Verzeichnisdienst an Policy Server und Filtering Service, die bei der Anwendung von Filterrichtlinien verwendet werden.

Websense, Inc., empfiehlt die Installation von User Service auf einem Computer mit dem Betriebssystem Windows (obwohl auch eine Installation auf einem Computer mit Linux möglich ist). In der Regel handelt es sich dabei um den Computer, auf dem Policy Server installiert ist.

Informationen darüber, wie die Websense-Software für die Kommunikation mit dem Verzeichnisdienst konfiguriert wird, finden Sie unter *Verzeichnisdienste*.

Verzeichnisdienste

Ein Verzeichnisdienst ist ein Tool, in dem Informationen über die Benutzer und Ressourcen eines Netzwerks gespeichert werden. Bevor Sie Benutzer-Clients in Websense Manager hinzufügen können (Benutzer, Gruppen, Domänen oder Organisationseinheiten), müssen Sie die Websense-Software für das Abrufen von Informationen vom Verzeichnisdienst konfigurieren.

Auf der Seite **Einstellungen > Verzeichnisdienste** geben Sie die Verzeichnisdienste an, die in Ihrem Netzwerk verwendet werden. Sie können nur die Einstellungen für einen Verzeichnisdiensttyp pro Policy Server vornehmen.

Wählen Sie zunächst einen Verzeichnisdienst in der Liste "Verzeichnisse". Die Auswahl bestimmt, welche Einstellungen auf der Seite angezeigt werden.

Die Konfigurationsanweisungen finden Sie im entsprechenden Abschnitt:

- *Windows NT Directory/Active Directory (Mixed Mode)*, Seite 68
- *Windows Active Directory (Native Mode)*, Seite 68
- *Novell eDirectory und Sun Java System Directory*, Seite 69

Windows NT Directory/Active Directory (Mixed Mode)

Wenn es sich bei Ihrem Verzeichnisdienst um Windows NT Directory oder Active Directory im Mixed Mode handelt, ist keine weitere Konfiguration erforderlich.

In seltenen Fällen müssen Sie auf dieser Seite möglicherweise zusätzliche Informationen angeben, wenn Sie einen anderen Verzeichnisdienst verwenden. Dies ist nur unter folgenden Umständen der Fall:

- Der DC Agent wird für eine transparente Identifikation verwendet (siehe *DC Agent*, Seite 225)

  und

- User Service läuft auf einem Computer mit Linux.

Wenn dies Ihrer Konfiguration entspricht, geben Sie die unter Windows NT Directory/ Active Directory (Mixed Mode) angegebenen Administrator-Anmeldeinformationen an. Wenn Ihre Installation nicht diese Konfiguration verwendet, sind die Felder für die Administrator-Anmeldeinformationen deaktiviert.

Windows Active Directory (Native Mode)

Windows Active Directory speichert Benutzerinformationen in einem oder mehreren *globalen Katalogen*. Mit dem globalen Katalog können Personen und Anwendungen Objekte (Benutzer, Gruppen usw.) in einer Active Directory-Domäne suchen.

Damit die Websense-Software mit einem Active Directory im Native Mode kommunizieren kann, müssen sie Informationen über die globalen Katalogserver in Ihrem Netzwerk angeben.

1. Klicken Sie neben der Liste der globalen Katalogserver auf **Hinzufügen**. Die Seite "Globalen Katalogserver hinzufügen" wird angezeigt.
2. Geben Sie im Feld **IP oder Name des Servers** den globalen Katalogserver ein:
   - Wenn mehrere globale Katalogserver mit Failoverkonfiguration vorliegen, geben Sie den DNS-Domänennamen ein.
   - Wenn die globalen Katalogserver ohne Failoverkonfiguration vorliegen, geben Sie die IP-Adresse oder den Hostnamen (wenn in Ihrem Netzwerk die Namensauflösung aktiviert ist) des Servers ein, der hinzugefügt werden soll.
3. Geben Sie den **Port** ein, den die Websense-Software für die Kommunikation mit dem globalen Katalog verwenden soll (standardmäßig **3268**).
4. (Optional) Geben Sie den **Root-Kontext** ein, den die Websense-Software für die Suche nach Benutzerinformationen verwenden soll. Wenn Sie einen Wert angeben, muss es sich dabei um einen gültigen Kontext in Ihrer Domäne handeln.
   - Wenn Sie 3268 oder 3269 als Kommunikationsport angegeben haben, müssen Sie keinen Root-Kontext eingeben.
   - Wenn Sie den Port 389 oder 636 angegeben haben, müssen Sie einen Root-Kontext angeben.

- Wenn im Feld "Root-Kontext" kein Eintrag vorgenommen wird, beginnt die Websense-Software bei der Suche mit der obersten Ebene des Verzeichnisdienstes.

  Hinweis
  Vermeiden Sie dieselben Benutzernamen in mehreren Domänen. Wenn die Websense-Software doppelte Kontonamen für einen Benutzer findet, kann der Benutzer nicht transparent identifiziert werden.

5. Geben Sie an, welches Administratorkonto die Websense-Software für das Abrufen von Benutzername und Pfadinformationen vom Verzeichnisdienst verwenden soll. Dieses Konto muss über die Berechtigung verfügen, im Verzeichnisdienst zu lesen, benötigt jedoch keine Berechtigung für das Vornehmen von Änderungen im Verzeichnisdienst und muss kein Domänenadministrator sein.

   Wählen Sie **Definierter Name nach Komponenten** oder **Vollständig definierter Name**, um anzugeben, wie die Kontoinformationen eingegeben werden sollen.

   - Wenn Sie "Definierter Name nach Komponenten" gewählt haben, geben Sie den **Anzeigenamen**, das **Passwort** für das Konto, den **Ordner für das Konto** und den **DNS-Domänennamen** für das Administratorkonto an. Verwenden Sie für den Benutzernamen des Administratorkontos den allgemeinen Namen (cn) und nicht die Benutzer-ID (uid).

     Hinweis
     Das Feld **Ordner für das Konto** unterstützt keine Werte mit dem Tag für die Organisationseinheit (ou) (z. B. *ou=Finance*). Wenn der Name des Administratorkontos über ein ou-Tag verfügt, geben Sie den vollständig definierten Namen für das Administratorkonto ein.

   - Wenn Sie "Vollständig definierter Name" ausgewählt haben, geben Sie den definierten Namen als eine einzelne Zeichenfolge im Feld **Definierter Benutzername** ein (z. B. *cn=Admin, cn=Users, ou=InfoSystems, dc=company, dc=net*) und geben anschließend das **Passwort** für das Konto ein.

6. Klicken Sie auf **OK**.
7. Wiederholen Sie diese Vorgehensweise für alle globalen Katalogserver.
8. Klicken Sie auf **Erweiterte Verzeichniseinstellungen**, und fahren Sie mit *Erweiterte Verzeichniseinstellungen*, Seite 70 fort.

Novell eDirectory und Sun Java System Directory

Zum Abrufen von Informationen vom Verzeichnisdienst benötigt die Websense-Software den definierten Namen, den Root-Kontext und das Passwort für ein Benutzerkonto mit Administratorberechtigungen.

1. Geben Sie die IP-Adresse des Computers, auf dem der Verzeichnisserver ausgeführt wird, im Feld **IP-Adresse des Servers** ein.
2. Geben Sie unter **Port** die Portnummer ein, die die Websense-Software für die Kommunikation mit dem Verzeichnis verwenden soll. Der Standardwert ist 389.
3. Wenn das Verzeichnis Administratorrechte für den Lesezugriff erfordert, nehmen Sie die entsprechenden Angaben in den Feldern **Definierter Name des Administrators** und **Passwort**.
4. (Optional) Geben Sie den **Root-Kontext** ein, den die Websense-Software für die Suche nach Benutzerinformationen verwenden soll, wie z. B. *o=domain.com*.

   Das Einschränken des Kontextes führt zu einem schnelleren und effizienteren Auffinden von Benutzerinformationen.

   Hinweis

   Vermeiden Sie die Verwendung desselben Benutzernamens in mehreren Domänen. Wenn die Websense-Software doppelte Kontonamen für einen Benutzer findet, kann der Benutzer nicht transparent identifiziert werden.

5. Klicken Sie auf **Erweiterte Verzeichniseinstellungen**, und fahren Sie mit *Erweiterte Verzeichniseinstellungen*, Seite 70 fort.

Erweiterte Verzeichniseinstellungen

Verwandte Themen:

- *Windows Active Directory (Native Mode)*, Seite 68
- *Novell eDirectory und Sun Java System Directory*, Seite 69

Mit diesen Einstellungen können Sie Folgendes definieren:

- Wie die Websense-Software den Verzeichnisdienst durchsucht, um Informationen zu Benutzern, Gruppen und Domänen zu finden
- Ob die Websense-Software eine verschlüsselte Verbindung für die Kommunikation mit dem Verzeichnisserver verwendet
- Welchen Zeichensatz die Websense-Software für die Verschlüsselung der LDAP-Informationen verwendet

Konfigurieren Sie diese Einstellungen je nach Anforderungen des jeweiligen LDAP-basierten Verzeichnisdienstes.

1. Wenn Sie benutzerdefinierte Objektklassentypen (Attributnamen) im Verzeichnisdienst verwenden, aktivieren Sie die Option **Benutzerdefinierte Filter verwenden**. Die Standard-Filterzeichenfolgen werden in den Feldern für Filter angezeigt.

2. Bearbeiten Sie die vorhandenen Filterzeichenfolgen, indem Sie die für Ihr Verzeichnis gültigen Objektklassentypen ersetzen. Wenn Ihr Verzeichnis z. B. einen Objektklassentyp wie **dept** statt **ou** (Organisationseinheit) verwendet, geben Sie einen neuen Wert in das Feld "Filter für die Suche nach Domänen" ein.

   Attribute sind immer Zeichenketten, die für die Suche in den Inhalten des Verzeichnisdienstes verwendet werden. Benutzerdefinierte Filter stellen die hier beschriebene Funktionalität bereit.

   - **Filter für die Suche nach Benutzern** bestimmt, wie User Service nach Benutzern sucht.
   - **Filter für die Suche nach Gruppen** bestimmt, wie User Service nach Gruppen sucht.
   - **Filter für die Suche nach Domänen** bestimmt, wie User Service nach Domänen und Organisationseinheiten sucht.
   - **Filter für die Suche nach Benutzergruppen** bestimmt, wie User Service Benutzer mit Gruppen verbindet.

3. Wenn Sie eine sichere Verbindung für die Kommunikation zwischen der Websense-Software und dem Verzeichnisdienst verwenden möchten, aktivieren Sie **SSL verwenden**.
4. Bestimmen Sie mit den Optionen **UTF-8** oder **MBCS**, welchen Zeichensatz die Websense-Software für das Verschlüssen der LDAP-Informationen verwendet.

   MBCS (Multibyte-Zeichensatz) wird häufig für die Verschlüsselung von ostasiatischen Sprachen wie Chinesisch, Japanisch und Koreanisch verwendet.
5. Klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst übernommen, wenn Sie auf **Alles speichern** klicken.

Arbeiten mit benutzerdefinierten LDAP-Gruppen

Verwandte Themen:

- *Arbeiten mit Benutzern und Gruppen*, Seite 66
- *Verzeichnisdienste*, Seite 67
- *Hinzufügen oder Bearbeiten einer benutzerdefinierten LDAP-Gruppe*, Seite 72

Auf der Seite **Benutzerdefinierte LDAP-Gruppen verwalten** können Sie benutzerdefinierten Gruppen verwalten, die auf Attributen basieren, die im Verzeichnisdienst definiert wurden. Diese Option steht nur zur Verfügung, wenn Sie

in der Websense-Software die Kommunikation mit einem LDAP-basierten Verzeichnisdienst konfiguriert haben.

> **Wichtig**
>
> Wenn Sie benutzerdefinierte LDAP-Gruppen zu Websense Manager hinzufügen, werden die Gruppendefinitionen vom aktiven Policy Server gespeichert. Sie haben keine Auswirkung auf andere Policy Server-Instanzen. Wenn Sie benutzerdefinierte LDAP-Gruppen zu mehreren Policy Servers hinzufügen möchten, melden Sie sich mit dem Websense Manager bei jedem Policy Server an und geben die Informationen ein.
>
> Wenn Sie LDAP-Gruppen hinzufügen und anschließend entweder die Verzeichnisserver oder den Standort des Verzeichnisservers ändern, werden die vorhandenen Gruppen ungültig. Sie müssen die Gruppen erneut hinzufügen und anschließend jede Gruppe als Client definieren.

- Klicken Sie zum Hinzufügen einer Gruppe auf **Hinzufügen** (siehe *Hinzufügen oder Bearbeiten einer benutzerdefinierten LDAP-Gruppe*, Seite 72).
- Klicken Sie zum Ändern eines Eintrags in einer Liste auf seinen Gruppennamen (siehe *Hinzufügen oder Bearbeiten einer benutzerdefinierten LDAP-Gruppe*).
- Wenn Sie einen Einträg entfernen möchten, wählen Sie ihn zunächst aus, und klicken anschließend auf **Löschen**.

Wenn Sie alle Änderungen an benutzerdefinierten LDAP-Gruppen vorgenommen haben, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern und zur vorherigen Seite zurückzukehren. Die Änderungen werden erst übernommen, wenn Sie auf **Alles speichern** klicken.

Hinzufügen oder Bearbeiten einer benutzerdefinierten LDAP-Gruppe

Auf der Seite **Benutzerdefinierte LDAP-Gruppe hinzufügen** können Sie eine Gruppe basierend auf einem beliebigen im Verzeichnisdienst definierten Attribut in Websense Manager definieren. Auf der Seite **Benutzerdefinierte LDAP-Gruppe bearbeiten** können Sie Änderungen an vorhandenen Definitionen vornehmen.

> **Wichtig**
>
> Wenn Sie LDAP-Gruppen hinzufügen und anschließend entweder die Verzeichnisdienste oder den Standort des Verzeichnisservers ändern, werden die vorhandenen Gruppen ungültig. Sie müssen die Gruppen erneut hinzufügen und anschließend jede Gruppe als Client definieren.

1. Geben Sie den **Gruppennamen** ein, oder ändern Sie ihn. Verwenden Sie einen beschreibenden Namen, der den Zweck der LDAP-Gruppe verdeutlicht.

   Bei Gruppennamen muss die Groß- und Kleinschreibung beachtet werden, und sie müssen eindeutig sein.
2. Geben Sie die Beschreibung ein, die diese Gruppe in Ihrem Verzeichnisdienst definiert, oder ändern Sie sie. Beispiel:

   ```
   (WorkStatus=parttime)
   ```

   In diesem Beispiel ist **WorkStatus** ein Benutzerattribut, das den Beschäftigungsstatus beschreibt, und **parttime** der Wert, der angibt, dass der Benutzer in einer Teilzeitbeschäftigung angestellt ist.
3. Klicken Sie auf **OK**, um zur Seite "Benutzerdefinierte LDAP-Gruppen verwalten" zurückzukehren. Der neue oder geänderte Eintrag wird in der Liste angezeigt.
4. Fügen Sie einen weiteren Eintrag hinzu, oder bearbeiten Sie einen Eintrag, oder klicken Sie auf **OK**, um die Änderungen in den Cache zwischenzuspeichern und zur vorherigen Seite zurückzukehren. Die Änderungen werden erst übernommen, wenn Sie auf **Alles speichern** klicken.

Hinzufügen eines Clients

Verwandte Themen:

- *Arbeiten mit Clients*, Seite 64
- *Arbeiten mit Computern und Netzwerken*, Seite 65
- *Arbeiten mit Benutzern und Gruppen*, Seite 66
- *Durchsuchen des Verzeichnisdienstes*, Seite 74
- *Ändern von Clienteinstellungen*, Seite 75

Auf der Seite **Richtlinienverwaltung > Clients > Clients hinzufügen** können Sie Benutzer-, Gruppen-, Computer- und Netzwerkclients zu Websense Manager hinzufügen, um ihnen eine Richtlinie zuzuweisen.

Wenn Sie sich mit einer Rolle für delegierte Verwaltung angemeldet haben, können Sie nur Clients hinzufügen, die in der Liste der von Ihnen verwalteten Clients enthalten sind. Während Sie Clients zur Seite "Clients" hinzufügen, müssen Sie ihnen eine Richtlinie hinzufügen.

1. Geben Sie einen oder mehrere Clients an:
   - Navigieren Sie zum Hinzufügen eines Benutzer-, Gruppen- oder Domänenclients im Verzeichnisbaum **Verzeichnis**, um Einträge in Ihrem Verzeichnisdienst zu finden. Wenn Sie einen LDAP-basierten Verzeichnisdienst verwenden, können Sie darüber hinaus auf **Suchen** klicken, um ein Tool zum Durchsuchen des Verzeichnisses zu öffnen (siehe *Durchsuchen des Verzeichnisdienstes*, Seite 74).

- Wenn Sie einen Computer- oder Netzwerkclient hinzufügen möchten, geben Sie eine **IP-Adresse** oder einen **IP-Adressbereich** ein. Netzwerkdefinitionen dürfen sich zwar nicht überschneiden, ein Netzwerkclient kann jedoch eine separat angegebene IP-Adresse als Computerclient enthalten. Im Falle einer solchen Überschneidung hat die dem Computer zugewiesene Richtlinie Vorrang vor der Richtlinie, die dem Netzwerk zugewiesen wurde.

2. Klicken Sie auf die Schaltfläche mit dem Pfeil (>), um jeden Client zur Liste **Ausgewählte Clients** hinzuzufügen.

   Wenn Sie einen Eintrag aus der Liste "Ausgewählte Clients" entfernen möchten, wählen Sie den Client und klicken anschließend auf **Entfernen**.
3. Wählen Sie eine **Richtlinie**, die allen Clients in der Liste "Ausgewählte Clients" hinzugefügt werden soll.
4. Klicken Sie zum Schluss auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst übernommen, wenn Sie auf **Alles speichern** klicken.

Die Clients werden zur entsprechenden Liste auf der Seite **Richtlinienverwaltung > Clients** hinzugefügt. Wenn Sie die einem oder mehreren Clients zugewiesene Richtlinie ändern oder weitere Client-Einstellungen konfigurieren möchten, wählen Sie die jeweiligen Client-Einträge aus und klicken anschließend auf **Bearbeiten**. Weitere Informationen dazu finden Sie unter *Ändern von Clienteinstellungen*, Seite 75.

Durchsuchen des Verzeichnisdienstes

Wenn Sie in der Websense-Software die Kommunikation mit einem LDAP-basierten Verzeichnisdienst konfiguriert haben, können Sie eine Suchfunktion verwenden, um Benutzer auszuwählen, die als Clients in Websense Manager hinzugefügt werden sollen. Die Suchfunktion steht auch für das Hinzufügen verwalteter Clients und Administratoren zu Rollen für die delegierte Verwaltung zur Verfügung.

So durchsuchen Sie einen Verzeichnisdienst nach Informationen über Benutzer, Gruppen und Organisationseinheiten:

1. Klicken Sie auf **Suchen**.
2. Geben Sie unter **Name** den gesamten Namen oder Teile des Namens des Benutzers, der Gruppe oder Organisationseinheit ein.
3. Legen Sie in der Liste **Typ** den Typ des Verzeichniseintrags (Benutzer, Gruppe, OU oder alle) fest, den Sie suchen.

   Bei einem Verzeichnisdienst mit vielen Einträgen kann die Auswahl von **Alle** dazu führen, dass der Suchvorgang sehr lange dauert.
4. Durchsuchen Sie den Verzeichnisbaum **Suchkontext**, um festzulegen, welcher Bereich des Verzeichnisses durchsucht werden soll. Je präziser der Kontext ausgewählt wird, desto schneller verläuft der Suchvorgang.
5. Klicken Sie auf **Los**.

   Es wird eine Liste der Suchergebnisse angezeigt.

6. Wählen Sie einen oder mehrere Einträge im Suchergebnis aus, und klicken Sie anschließend auf die Schaltfläche mit dem nach rechts weisenden Pfeil (>), um die ausgewählten Elemente als Client oder Administrator hinzuzufügen.
7. Klicken Sie auf **Neue Suche**, oder geben Sie neue Suchkriterien ein.
8. Klicken Sie auf **Durchsuchen**, um erneut das Verzeichnis zu durchsuchen.
9. Wenn Sie alle Änderungen vorgenommen haben, klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst übernommen, wenn Sie auf **Alles speichern** klicken.

Ändern von Clienteinstellungen

Auf der Seite **Richtlinienverwaltung > Clients > Client bearbeiten** können Sie die Einstellungen der Richtlinie oder der Authentifizierung für einen oder mehrere Clients ändern. Wenn Sie vor dem Klicken auf "Bearbeiten" mehrere Clients ausgewählt haben, werden die auf der Seite "Clients bearbeiten" vorgenommenen Änderungen an der Konfiguration auf alle ausgewählten Clients angewendet.

1. Wählen Sie eine **Richtlinie** aus, die auf die ausgewählten Clients angewendet werden soll. Die Standardrichtlinie regelt alle Clients, bis eine andere Richtlinie zugewiesen wurde.
2. Wenn Sie Benutzern die Möglichkeit bieten möchten, eine Websense-Sperrseite durch die Eingabe eines Passworts zu umgehen, klicken Sie unter "Mit Passwort freigeben" auf **Ein**. Geben Sie dann ein Passwort ein, und bestätigen Sie es anschließend.

   Wenn Sie die Berechtigung zur Freigabe mit Passwort entfernen möchten, klicken Sie auf **Aus**.
3. Klicken Sie zum Hinzufügen einer **Quotenzeit** zu den ausgewählten Clients auf **Benutzerdefiniert**, und geben Sie anschließend die gewünschte Quotenzeit als Anzahl Minuten ein.

   Wenn Sie die Standardeinstellungen der Quote wiederherstellen möchten, klicken Sie auf **Standard**.
4. Klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern und zur Seite "Clients" zurückzukehren. Die Änderungen werden erst übernommen, wenn Sie auf **Alles speichern** klicken.

Die neuen Clienteinstellungen werden auf der Seite **Richtlinienverwaltung > Clients** in den Einträgen der Clients angezeigt.

Verschieben von Clients zu Rollen

Übergeordnete Administratoren (Super Administrators) können auf der Seite **Clients zu Rolle verschieben** einen oder mehrere Clients zu einer Rolle für die delegierte Verwaltung verschieben. Nachdem ein Client verschoben wurde, wird dieser Client

auf der Seite "Clients" der Rolle, in die verschoben wurde, in der Liste "Verwaltete Clients" angezeigt.

- Die Richtlinie, die dem Client in der Rolle des übergeordneten Administrators (Super Administrator) zugewiesen wurde, und die Filter, die diese Richtlinie durchsetzt, werden zur Rolle für die delegierte Verwaltung kopiert.
- Delegierte Administratoren können die Richtlinien ändern, die den von Ihnen verwalteten Clients zugewiesenen wurden.
- Die Einschränkungen durch die Filter-Fixierung betreffen nicht Clients, die durch übergeordnete Administratoren (Super Administrators) verwaltet werden. Verwaltete Clients in Rollen für die delegierte Verwaltung sind hingegen von der Filter-Fixierung betroffen.
- Wenn eine Gruppe, Domäne oder Organisationseinheit als verwalteter Client einer Rolle hinzugefügt wird, können delegierte Administratoren in dieser Rolle Benutzern in der Gruppe, Domäne oder Organisationseinheit Richtlinien zuweisen.
- Wenn ein Netzwerk (IP-Adressbereich) einer Rolle als verwalteter Client hinzugefügt wird, können delegierte Administratoren in dieser Gruppe individuellen Computern in diesem Netzwerk Richtlinien zuweisen.
- Ein Client kann nicht zu mehreren Rollen verschoben werden.

So verschieben Sie ausgewählte Clients zu einer Rolle für die delegierte Verwaltung:

1. Wählen Sie in der Dropdown-Liste **Rolle auswählen** eine Zielrolle aus.
2. Klicken Sie auf **OK**.

   Ein Dialogfenster weist darauf hin, dass die ausgewählten Clients verschoben werden. Das Verschieben kann eine Weile in Anspruch nehmen.
3. Die Änderungen werden erst übernommen, wenn Sie auf **Alles speichern** klicken.

Wenn delegierte Administratoren in der ausgewählten Rolle während des Vorgangs des Verschiebens mit Zugriffsberechtigung auf Richtlinien angemeldet sind, müssen sie sich von Websense Manager abmelden und erneut anmelden, um die neuen Clients in ihrer Liste "Verwaltete Clients" anzuzeigen.

4 Filterrichtlinien für die Internetnutzung

Verwandte Themen:

- *Filter für die Internetnutzung*, Seite 39
- *Clients*, Seite 63
- *Die Richtlinie "Standard"*, Seite 78
- *Arbeiten mit Richtlinien*, Seite 79
- *Filterreihenfolge*, Seite 84

Richtlinien steuern den Internetzugriff der Benutzer. Eine Richtlinie besteht aus folgenden Bestandteilen:

- Kategoriefilter, die auf jede Kategorie von Websites Filteraktionen (wie "Sperren" oder "Zulassen") anwenden (siehe *Filtern von Kategorien und Protokollen*, Seite 40)
- Filter für die Zugriffsbeschränkung, mit denen der Zugriff auf eine Liste mit bestimmten Websites beschränkt wird (siehe *Benutzer auf eine festgelegte Liste von Internetsites einschränken*, Seite 178)
- Protokollfilter, die dazu verwendet werden, Aktionen auf Internetprotokolle anzuwenden (siehe *Filtern von Kategorien und Protokollen*, Seite 40)
- Ein Zeitplan, in dem festgelegt ist, wann eine Kategorie oder ein Filter für die Zugriffsbeschränkung und ein Protokollfilter angewendet wird

Die neue Softwareinstallation von Websense enthält drei vordefinierte Richtlinien:

- Mit der Richtlinie **Standard** wird der Internetzugriff aller Clients gefiltert, die keiner anderen Richtlinie unterliegen. Die Websense-Software setzt diese Richtlinie um, sobald der Subskriptionsschlüssel eingegeben wird (siehe *Die Richtlinie "Standard"*, Seite 78).
- Die Richtlinie **Ohne Einschränkung** gewährt uneingeschränkten Zugriff auf das Internet. Diese Richtlinie wird nicht standardmäßig auf Clients angewendet.
- Die Richtlinie **Beispiel - Standardbenutzer** zeigt, wie mehrere Kategorie- und Protokollfilter in einer Richtlinie angewendet werden können, um so verschiedene Stufen der Filtereinschränkung zu unterschiedlichen Zeiten bereitzustellen. Anhand dieser Richtlinie wird im Lerntext für den Schnelleinstieg für neue Benutzer demonstriert, wie eine Richtlinie bearbeitet und auf Clients angewendet wird.

Verwenden Sie eine dieser Richtlinien im vorliegenden Zustand, bearbeiten Sie sie gemäß den Anforderungen Ihrer Organisation, oder erstellen Sie eigene Richtlinien.

Die Richtlinie "Standard"

Verwandte Themen:

- *Filterrichtlinien für die Internetnutzung*, Seite 77
- *Arbeiten mit Richtlinien*, Seite 79
- *Filterreihenfolge*, Seite 84

Die Richtlinie **Standard** beginnt mit der Überwachung der Internetnutzung, sobald Sie bei der Installation der Websense-Software den Subskriptionsschlüssel eingeben. Zu Beginn lässt die Richtlinie "Standard" alle Anforderungen zu.

Hinweis

Bei der Aktualisierung von einer früheren Version der Websense-Software bleiben die vorhandenen Richtlinieneinstellungen bestehen. Überprüfen Sie nach der Aktualisierung die Richtlinien, um sicherzustellen, dass sie noch immer richtig sind.

Bei der Erstellung und Anwendung Ihrer eigenen Filterrichtlinien dient die Richtlinie "Standard" auch weiterhin als Sicherheitsnetz und filtert den Internetzugriff der Clients, die keiner anderen Richtlinie unterliegen.

Bei einer Neuinstallation muss die Richtlinie "Standard" die Internetfilterung übernehmen und dazu 24 Stunden am Tag und 7 Tage die Woche eine Kombination aus Kategoriefiltern und Filtern für die Zugriffsbeschränkung sowie gegebenenfalls auch Protokollfilter anwenden.

Wichtig

Bei Benutzern, die eine Aktualisierung von einer früheren Version der Websense-Software durchführen, deckt die Richtlinie "Standard" möglicherweise nicht alle Zeiträume ab. Es ist nicht erforderlich, die Richtlinie "Standard" zu ändern. Wenn die Richtlinie jedoch zu einem zukünftigen Zeitpunkt bearbeitet wird, lässt die Websense-Software eine Speicherung der Änderungen erst dann zu, wenn alle Zeiträume abgedeckt sind.

Bearbeiten Sie die Richtlinie "Standard" nach Bedarf, um Sie an die Bedürfnisse Ihrer Organisation anzupassen. Die Richtlinie "Standard" kann nicht gelöscht werden.

Arbeiten mit Richtlinien

Verwandte Themen:

- *Filterrichtlinien für die Internetnutzung*, Seite 77
- *Erstellen einer Richtlinie*
- *Bearbeiten einer Richtlinie*
- *Filter für die Internetnutzung*
- *Filterrichtlinien verfeinern*

Auf der Seite **Richtlinienverwaltung > Richtlinien** können Sie die Informationen zu bestehenden Richtlinien überprüfen. Diese Seite dient auch als Ausgangspunkt zum Hinzufügen, Bearbeiten und Löschen von Richtlinien sowie zum Kopieren von Richtlinien zu Rollen für die delegierte Verwaltung (nur übergeordnete Administratoren) und zum Ausdrucken detaillierter Informationen zur Konfiguration Ihrer Richtlinie.

Die Seite "Richtlinien" umfasst eine Liste der bestehenden Richtlinien. In dieser Liste wird der Name und eine Beschreibung jeder einzelnen Richtlinie sowie die Anzahl der Benutzer-, Netzwerk- und Computer-Clients, denen die Richtlinie zugeordnet wurde, aufgeführt.

- Klicken Sie zum Hinzufügen einer Richtlinie auf **Hinzufügen**. Weitere Informationen finden Sie unter *Erstellen einer Richtlinie*, Seite 80.
- Klicken Sie zum Bearbeiten einer Richtlinie auf den Richtliniennamen in der Liste. Weitere Informationen finden Sie unter *Bearbeiten einer Richtlinie*, Seite 81.
- Klicken Sie auf eine Ziffer in der Spalte "Benutzer", "Netzwerke" oder "Computer", um zu sehen, welche Clients nach dieser Richtlinie gefiltert werden. Die Client-Informationen werden in einem Popup-Dialogfeld angezeigt.

Klicken Sie auf **Richtlinien in Datei ausgeben**, um eine Liste mit allen Richtlinien und den zugehörigen Komponenten einschließlich Filtern, benutzerdefinierten Kategorien und Protokollen, Schlüsselwörtern, benutzerdefinierten URLs und regulären Ausdrücken auszudrucken. Mit dieser Funktion wird ein detailliertes Arbeitsblatt mit Richtlinieninformationen im Format von Microsoft Excel erstellt. Dies soll es Personalbeauftragten, Führungskräften und anderen Personen mit leitender Funktion ermöglichen, Informationen zu Filterrichtlinien auf einfache Art und Weise überprüfen zu können.

Wenn Sie Rollen für die delegierte Verwaltung erstellt haben (siehe *Delegierte Verwaltung*, Seite 251), können übergeordnete Administratoren (Super Administrators) die von ihnen erstellten Richtlinien zu anderen Rollen zwecks ihrer

Nutzung von delegierten Administratoren kopieren. Die Filter, die von dieser Richtlinie durchgesetzt werden, werden ebenfalls kopiert.

> **Hinweis**
> Da delegierte Administratoren der Filter-Fixierung unterliegen, können die Filter und Richtlinien mit Einstellung "Alles zulassen", die die Fixierung anwenden, nicht zu Rollen kopiert werden.

Wenn Sie Richtlinien in eine andere Rolle verschieben möchten, aktivieren Sie zunächst das Kontrollkästchen neben dem Richtliniennamen, und klicken Sie anschließend auf **Kopieren zu Rolle**. Weitere Informationen dazu finden Sie unter *Filter und Richtlinien in Rollen kopieren*, Seite 183.

Erstellen einer Richtlinie

Verwandte Themen:

- *Filterrichtlinien für die Internetnutzung*, Seite 77
- *Arbeiten mit Richtlinien*, Seite 79
- *Bearbeiten einer Richtlinie*, Seite 81
- *Arbeiten mit Filtern*, Seite 51
- *Benutzer auf eine festgelegte Liste von Internetsites einschränken*, Seite 178

Auf der Seite **Richtlinienverwaltung > Richtlinien > Richtlinie hinzufügen** können Sie neue, benutzerdefinierte Richtlinien erstellen.

1. Geben Sie einen eindeutigen **Richtliniennamen** ein. Der Name der Richtlinie muss eine Länge zwischen 1 und 50 Zeichen aufweisen und darf keine der folgenden Zeichen enthalten:

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Richtliniennamen können Leerzeichen, Bindestriche und Apostrophe enthalten.
2. Geben Sie eine **Beschreibung** für die neue Richtlinie ein. Die Beschreibung sollte aussagekräftig und detailorientiert sein, damit sie auch im späteren Verlauf der Richtlinienverwaltung hilfreich ist.

   Die Einschränkungen für die Verwendung der Zeichen, die für Richtliniennamen verwendet werden können, gelten auch für Beschreibungen. Es gibt allerdings zwei Ausnahmen: Beschreibungen dürfen Punkte (.) und Kommas (,) enthalten.
3. Wenn eine bestehende Richtlinie als Grundlage der neuen Richtlinie verwendet werden soll, aktivieren Sie das Kontrollkästchen **Vorhandene Richtlinie als Basis verwenden**, und wählen Sie daraufhin eine Richtlinie aus der Dropdownliste aus.

   Aktivieren Sie das Kontrollkästchen nicht, um eine leere Richtlinie als Grundlage zu verwenden.

4. Klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Gehen Sie dann zur Seite "Richtlinie bearbeiten".

   Schließen Sie die Definition der Richtlinie auf der Seite "Richtlinie bearbeiten" ab. Siehe *Bearbeiten einer Richtlinie*, Seite 81.

Bearbeiten einer Richtlinie

Verwandte Themen:

- *Filterrichtlinien für die Internetnutzung*, Seite 77
- *Arbeiten mit Richtlinien*, Seite 79
- *Erstellen einer Richtlinie*, Seite 80
- *Arbeiten mit Filtern*, Seite 51
- *Benutzer auf eine festgelegte Liste von Internetsites einschränken*, Seite 178

Auf der Seite **Richtlinienverwaltung > Richtlinien > Richtlinie bearbeiten** können Sie Änderungen an einer bestehenden Richtlinie vornehmen oder die Definition einer neuen Richtlinie abschließen.

Bearbeiten Sie den Namen und die Beschreibung der Richtlinie im oberen Bereich der Seite:

- Klicken Sie auf **Umbenennen**, um den Richtliniennamen zu ändern.
- Geben Sie einfach ihren Text in das Feld **Beschreibung** ein, um die Filterbeschreibung zu ändern.

Unter der Richtlinienbeschreibung wird im Feld **Clients** aufgeführt, wie viele Clients eines Typs (Benutzer, Computer und Netzwerk) aktuell von dieser Richtlinie gefiltert werden. Klicken Sie auf den Link für den entsprechenden Clienttyp, um zu sehen, welche Clients der Richtlinie unterliegen.

Um die Richtlinie zusätzlichen Clients zuzuweisen, klicken Sie in der Symbolleiste im oberen Bereich der Seite auf **Auf Clients anwenden**, und lesen Sie die weiteren Informationen unter *Zuweisen einer Richtlinie an Clients*, Seite 83.

Im Bereich **Richtliniendefinition** können Sie die Filter definieren, die von der Richtlinie zu verschiedenen Zeiten angewendet werden sollen.

1. Klicken Sie auf **Hinzufügen**, um dem Plan eine Zeitsperre hinzuzufügen.
2. Mit den Spalten **Start** und **Ende** in der Tabelle "Planung" können sie den Zeitraum definieren, der von der Zeitsperre betroffen ist.

   Wenn Sie die Filterung für einen Zeitraum definieren möchten, der über Mitternacht hinausgeht (beispielsweise von 17:00 bis 8:00 Uhr), fügen Sie zwei Zeitsperren zum Plan hinzu: eine Zeitsperre für den Zeitraum von der Startzeit bis Mitternacht und eine für den Zeitraum von Mitternacht bis zum Ende der Sperre.

An der in der Websense-Software enthaltenen Richtlinie **Beispiel - Standardbenutzer** ist ersichtlich, wie ein Filterzeitraum definiert wird, der über Mitternacht hinausgeht.

3. Mit der Spalte **Tage** kann definiert werden, an welchen Tagen der Woche die Zeitsperre gilt. Klicken Sie auf den Nach-unten-Pfeil im rechten Bereich der Spalte, um die Tage aus einer Liste auszuwählen. Klicken Sie auf den Nach-oben-Pfeil, wenn sie die Tage ausgewählt haben.
4. Verwenden Sie die Spalte **Kategoriefilter/Filter für die Zugriffsbeschränkung**, um einen Filter auszuwählen, der während der Zeitsperre angewendet werden soll.

   Wählen Sie unter **Kategoriefilter erstellen** oder **filter für die Zugriffsbeschränkung erstellen** einen neuen Filter aus, wenn in der Richtlinie ein neuer Filter hinzugefügt und angewendet werden soll. Anleitungen hierzu finden Sie unter *Erstellen von Kategoriefiltern*, Seite 52, oder *Einen Filter für die Zugriffsbeschränkung erstellen*, Seite 180.
5. Verwenden Sie die Spalte **Protokollfilter**, um einen Filter auszuwählen, der während der Zeitsperre angewendet werden soll.

   Wählen Sie **Protokollfilter erstellen** aus, um einen neuen Filter hinzuzufügen, der in der Richtlinie angewendet werden soll. Anweisungen dazu finden Sie unter *Erstellen von Protokollfiltern*, Seite 55.
6. Wiederholen Sie die Schritte 1 bis 5, um zusätzliche Zeitsperren zum Plan hinzuzufügen.

Wenn eine Zeitsperre im Plan ausgewählt ist, werden im unteren Teil der Seite "Richtlinien bearbeiten" die Filter angezeigt, die während der Zeitsperre angewendet werden. Alle aufgeführten Filter enthalten folgende Informationen:

- Den Filtertyp (Kategoriefilter, Filter für die Zugriffsbeschränkung oder Protokollfilter)
- Den Filternamen und die Beschreibung
- Die Filterinhalte (Kategorien oder Protokolle mit den angewendeten Aktionen oder eine Liste der zulässigen Websites)
- Die Anzahl der Richtlinien, die den ausgewählten Filter anwenden
- Schaltflächen, mit denen der Filter bearbeitet werden kann

Wenn Sie einen Filter auf dieser Seite bearbeiten, wirken sich die Änderungen auf alle Richtlinien aus, die den Filter umsetzen. Klicken Sie vor dem Bearbeiten eines Filters, der von mehreren Richtlinien umgesetzt wird, auf den Link **Folgende Richtlinien verwenden diesen Filter**. Damit können Sie anzeigen, welche Richtlinien betroffen sind.

Die Schaltflächen im unteren Bereich der Filterauflistung sind je nach Filtertyp unterschiedlich:

Filtertyp	Schaltflächen
Kategoriefilter	• Mit der Schaltfläche **Zulassen**, **Sperren**, **Bestätigen** oder **Quote** können Sie die auf die ausgewählten Kategorien angewendete Aktion ändern (siehe *Filteraktionen*, Seite 47). • Um einer übergeordneten Kategorie (Hauptkategorie) und sämtlichen Unterkategorien dieselbe Aktion zuzuweisen, ändern Sie zuerst die auf die Hauptkategorie angewendete Aktion, und klicken Sie dann auf **Auf Unterkategorien anwenden**. • Klicken Sie auf **Erweitert**, um die Sperrfunktion für Schlüsselworte, die Sperrung nach Dateitypen oder die Sperrung aufgrund der Bandbreite zu aktivieren.
Filter für die Zugriffsbeschränkung	• Mit den Schaltflächen **Sites hinzufügen** und **Ausdrücke hinzufügen** können Sie zulässige URLs, IP-Adressen oder reguläre Ausdrücke dem Filter hinzufügen (siehe *Benutzer auf eine festgelegte Liste von Internetsites einschränken*, Seite 178). • Um eine Site aus dem Filter zu entfernen, wählen Sie die URL, die IP-Adresse oder den Ausdruck aus, und klicken Sie auf **Löschen**.
Protokollfilter	• Mit der Schaltfläche **Zulassen** oder **Sperren** können Sie die auf die ausgewählten Protokolle angewendete Aktion ändern (siehe *Filteraktionen*, Seite 47). • Um die auf alle Protokolle in einer Protokollgruppe angewendete Aktion zu ändern, ändern Sie die auf ein beliebiges Protokoll angewendete Aktion, und klicken Sie dann auf **Auf Gruppe anwenden**. • Klicken Sie auf **Erweitert**, um Daten für das ausgewählte Protokoll aufzuzeichnen oder die Sperrung aufgrund der Bandbreite zu aktivieren.

Wenn Sie die Bearbeitung der Richtlinie abgeschlossen haben, klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Zuweisen einer Richtlinie an Clients

Verwandte Themen:

- *Filterrichtlinien für die Internetnutzung*, Seite 77
- *Erstellen einer Richtlinie*, Seite 80
- *Bearbeiten einer Richtlinie*, Seite 81
- *Clients*, Seite 63
- *Hinzufügen eines Clients*, Seite 73

Auf der Seite **Richtlinien > Richtlinie bearbeiten > Richtlinie auf Clients anwenden** können Sie die ausgewählte Richtlinie den Clients zuweisen.

In der Liste "Clients" werden alle verfügbaren Benutzer, Computer und Netzwerk-Clients sowie die aktuell dem Client zugewiesene Richtlinie aufgeführt.

Wählen Sie das Kontrollkästchen neben den Clients, die durch die ausgewählte Richtlinie gefiltert werden sollen, und klicken Sie dann auf **OK**, um zur Seite "Richtlinien bearbeiten" zurückzukehren. Klicken Sie erneut auf **OK**, um die Änderungen im Cache zwischenzuspeichern.

Klicken Sie auf **Alles speichern**, damit die neue Richtlinie von der Websense-Software zum Filtern von Anforderungen des ausgewählten Clients verwendet wird.

Filterreihenfolge

Die Websense-Software arbeitet mit mehreren Filtern, die in einer bestimmten Reihenfolge angewendet werden, um zu bestimmen, ob die angeforderten Internetdaten zugelassen, gesperrt oder begrenzt werden sollen.

Für jede eingehende Anfrage geht die Websense-Software folgendermaßen vor:

1. Die Einhaltung der Subskription wird überprüft. Dabei wird sichergestellt, dass die Subskription aktuell ist und die Anzahl der subskribierten Clients nicht überschritten wird.
2. Es wird bestimmt, welche Richtlinie zur Anwendung kommt. Dabei gilt folgende Suchreihenfolge:
   a. Richtlinie, die dem **Benutzer** zugewiesen ist.
   b. Richtlinie, die der **IP-Adresse** (Computer oder Netzwerk) des verwendeten Computers zugewiesen ist.
   c. Richtlinien, die der **Gruppe** zugewiesen sind, zu der der Benutzer gehört.
   d. Richtlinien, die der **Domäne** des Benutzers zugewiesen sind.
   e. Die Richtlinie **Standard**.

   Es wird die erste Richtlinie angewendet, die als zutreffend erkannt wird.
3. Die Anforderung wird gemäß den Beschränkungen der Richtlinie gefiltert.

In einigen Fällen gehört ein Benutzer mehr als einer Gruppe oder Domäne an, und es trifft keine Benutzer-, Computer- oder Netzwerkrichtlinie zu. In einem solchen Fall werden von der Websense-Software die Richtlinien überprüft, die den einzelnen Benutzergruppen zugewiesen wurden.

- Wenn für alle Gruppen dieselbe Richtlinie gilt, filtert die Websense-Software die Anfrage gemäß dieser Richtlinie.
- Wenn für eine der Gruppen eine andere Richtlinie gilt, filtert die Websense-Software die Anfrage je nach der gewählten Einstellung für die Option **Restriktivere Filterung verwenden** auf der Seite **Einstellungen > Filterung**.

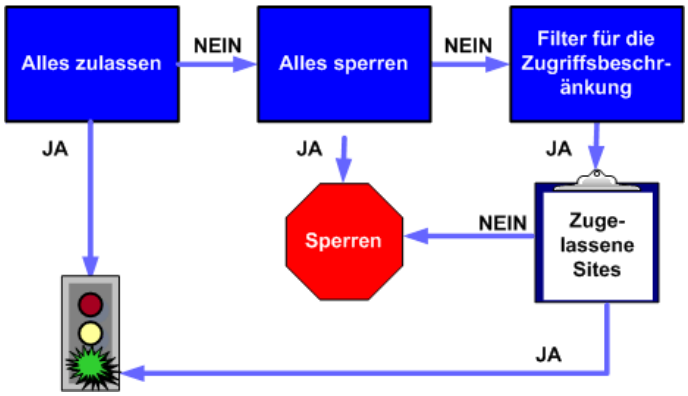
Wenn die Option **Restriktivere Filterung verwenden** aktiviert ist und eine der zutreffenden Richtlinien den Zugriff auf die angeforderte Kategorie sperrt, wird die Site von der Websense-Software gesperrt.

Wenn die Option nicht aktiviert ist und eine der zutreffenden Richtlinien den Zugriff auf die angeforderte Kategorie zulässt, wird der Zugriff auf die Site von der Websense-Software zugelassen.

Wenn eine der zutreffenden Richtlinien einen Filter für die Zugriffsbeschränkung anwendet, kann die Option **Restriktivere Filterung verwenden** unerwartete Auswirkungen haben. Siehe *Filter für die Zugriffsbeschränkung und Filterprioritäten*, Seite 179.

Filtern einer Site

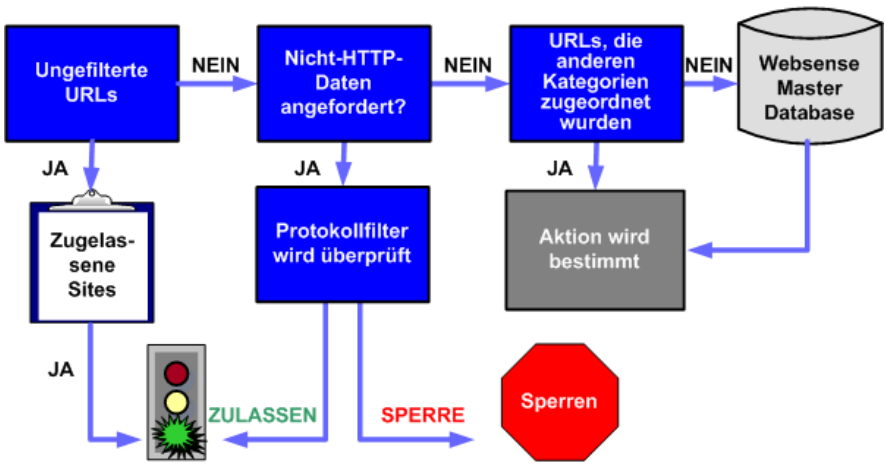
Richtlinienbeschränkungen werden von der Websense-Software wie im Folgenden dargestellt beurteilt, um zu bestimmen, ob die angeforderte Site zugelassen oder gesperrt werden sollte.



1. Es wird bestimmt, welcher **Kategoriefilter** oder **Filter für die Zugriffsbeschränkung** von der Richtlinie auf das aktuelle Datum und die aktuelle Uhrzeit angewendet wird.
   - Wenn für den aktiven Kategoriefilter **Alles zulassen** festgelegt ist, wird die Site zugelassen.
   - Wenn für den aktiven Kategoriefilter **Alles sperren** festgelegt ist, wird die Site gesperrt.
   - Wenn es sich um einen **Filter für die Zugriffsbeschränkung** handelt, wird überprüft, ob der Filter die URL oder IP-Adresse enthält. Die Site wird zugelassen, falls dies zutrifft. Andernfalls wird die Site gesperrt.

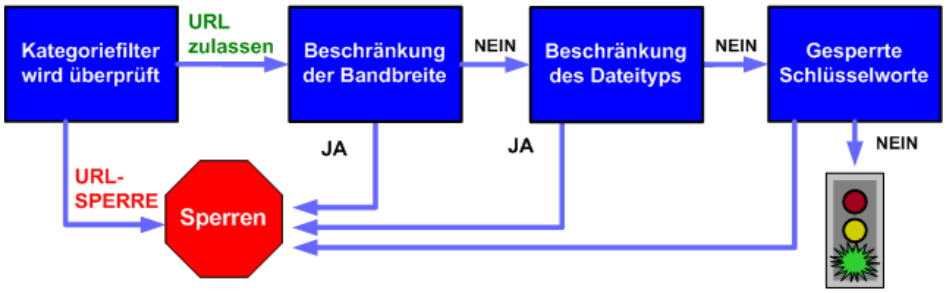
- Wenn ein anderer Kategoriefilter zutrifft, wird zu Schritt 2 übergegangen.

> **Hinweis**
> URLs, auf die über den Cache einer Internetsuchmaschine zugegriffen wird, werden von der Websense-Software nach demselben Prinzip wie andere URLs gefiltert. Auf diese Weise gespeicherte URLs werden gemäß den für die entsprechenden URL-Kategorien aktivierten Richtlinien gefiltert. In Protokolleinträgen für im Cache zwischengespeicherte URLs wird die gesamte zwischengespeicherte URL einschließlich eventuell zutreffender Suchmaschinenparameter angezeigt.



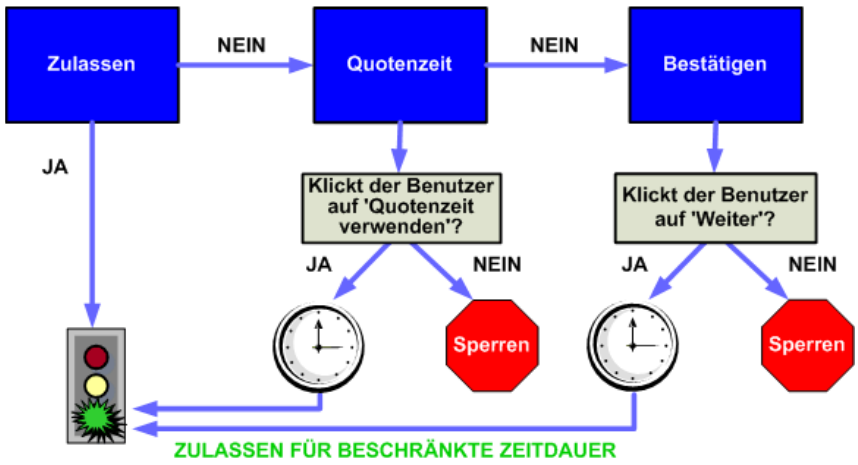
2. Es wird versucht, eine Übereinstimmung der Site mit einem Eintrag in der Liste **Ungefilterte URLs** zu finden.
   - Wenn die URL auf der Liste angezeigt wird, wird die Site zugelassen.
   - Wenn die URL nicht in der Liste angezeigt wird, wird zu Schritt 3 übergegangen.
3. Der aktive **Protokollfilter** wird überprüft, und es wird bestimmt, ob Nicht-HTTP-Protokolle mit der Anforderung in Zusammenhang stehen.
   - In diesem Fall werden Protokollfiltereinstellungen auf Daten angewendet, die übertragen werden können.
   - Andernfalls folgt Schritt 4.
4. Es wird versucht, eine Übereinstimmung der Site mit einem Eintrag in der Liste **URLs, die anderen Kategorien zugeordnet wurden** zu finden.
   - Wenn eine Übereinstimmung gefunden wird, wird die Kategorie der Site identifiziert, und es folgt Schritt 6.
   - Andernfalls folgt Schritt 5.

5. Es wird versucht, eine Übereinstimmung der Site mit einem Eintrag in der Liste **Stammdatenbank** zu finden.
   - Wenn die URL in der Stammdatenbank gefunden wird, wird die Kategorie der Site identifiziert, und es folgt Schritt 6.
   - Andernfalls wird die Site als "Verschiedenes/Ohne Kategoriezuordnung" kategorisiert, und es folgt Schritt 6.



6. Es erfolgt eine Überprüfung der aktiven Kategoriefilter und die Identifizierung der Aktion, die auf die Kategorie mit der angeforderten Site angewendet wird.
   - Wenn als Aktion **Gesperrt** festgelegt ist, wird die Site gesperrt.
   - Wenn eine andere Aktion angewendet wird, folgt Schritt 7.
7. Die Einstellungen für **Bandwidth Optimizer** werden im aktiven Kategoriefilter überprüft (siehe *Bandbreite mit Bandwidth Optimizer verwalten*, Seite 203).
   - Falls die aktuelle Bandbreitenauslastung die konfigurierten Einschränkungen überschreitet, wird die Site gesperrt.
   - Falls die aktuelle Bandbreitenauslastung die festgelegten Einschränkungen nicht überschreitet oder keine Aktionen auf Grundlage der Bandbreite angewendet werden, wird zu Schritt 8 übergegangen.
8. Die Einstellungen für die Beschränkung nach **Dateityp** werden für die aktive Kategorie überprüft (siehe *Datenverkehr basierend auf Dateitypen verwalten*, Seite 205).
   - Wenn die Site Dateien mit gesperrten Erweiterungen enthält, wird der Zugriff auf diese Dateien gesperrt. Wenn die Site selbst einem gesperrten Dateityp angehört, wird der Zugriff auf die Site gesperrt.
   - Wenn die Site keine Dateien mit gesperrten Erweiterungen enthält, wird zu Schritt 9 übergegangen.
9. Die URL und der CGI-Pfad werden auf gesperrte **Schlüsselworte** hin untersucht, falls die Sperrfunktion für Schlüsselwörter aktiviert ist (siehe *Auf Schlüsselwort basierte Filterung*, Seite 191).
   - Wenn ein gesperrtes Schlüsselwort gefunden wird, wird die Site gesperrt.

- Wenn kein gesperrtes Schlüsselwort gefunden wird, wird zu Schritt 10 übergegangen.



10. Die Site wird gemäß der auf die Kategorie angewendeten Aktion behandelt.
    - **Zulassen**: Die Site wird zugelassen.
    - **Gesperrt mit Quote**: Es wird eine Sperrmeldung angezeigt, die die Option enthält, die Site mit Quotenzeit anzuzeigen oder zur vorhergehenden Seite zurückzukehren.
    - **Bestätigen**: Es wird eine Sperrmeldung angezeigt, die die Option enthält, die Site für arbeitsrelevante Zwecke anzuzeigen.

Die Websense-Software fährt so lange fort, bis die angeforderte Site entweder gesperrt oder ausdrücklich zugelassen wird. An diesem Punkt werden von der Software keine weiteren Versuche zur Filterung unternommen. Wenn eine angeforderte Site beispielsweise zu einer gesperrten Kategorie gehört und ein gesperrtes Schlüsselwort enthält, wird die Site von der Software auf Kategorieebene gesperrt, ohne dass eine Überprüfung des Schlüsselwortfilters stattfindet. Log Server protokolliert die Anfrage daraufhin aufgrund einer gesperrten Kategorie anstelle eines Schlüsselworts als gesperrt.

Hinweis

Benutzer mit Berechtigung zur Freigabe mit Passwort können unabhängig vom Grund für die Sperrung der Site auf Internetsites zugreifen.

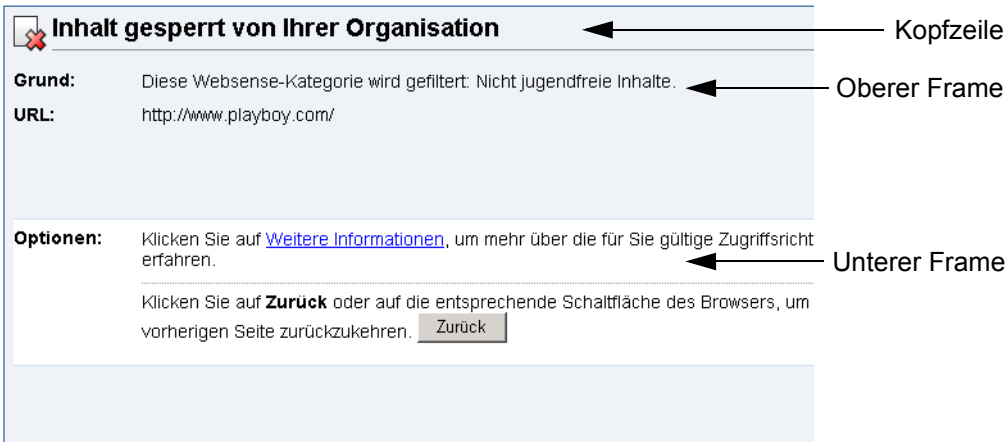
5 Sperren von Seiten

Verwandte Themen:

- *Protokollsperrmeldungen*, Seite 90
- *Arbeiten mit Sperrseiten*, Seite 91
- *Erstellen von alternativen Sperrmeldungen*, Seite 96
- *Verwenden einer alternativen Sperrseite auf einem anderen Computer*, Seite 97

Wenn eine Website durch die Websense-Software gesperrt ist, wird eine Sperrseite im Browser des Clients angezeigt. Wenn die Website gesperrt wird, weil sie zu einer Kategorie in der Klasse "Sicherheitsrisiko" gehört (siehe *Risikoklassen*, Seite 43), wird eine spezielle Version der Sperrseite angezeigt.

Eine Standardsperrseite besteht aus drei Hauptbereichen.



- Die **Kopfzeile** erklärt, dass die Site gesperrt ist.
- Im **oberen Frame** ist eine Sperrmeldung enthalten, die die gewünschte URL und den Grund für die Sperrung der URL angibt.
- Der **untere Frame** enthält alle für den Benutzer verfügbaren Funktionen, z. B. die Option, zur vorherigen Seite zurückzukehren, oder durch Klicken auf die Schaltflächen "Weiter" oder "Quotenzeit verwenden" die Site anzuzeigen.

Sperrseiten werden aus HTML-Dateien erstellt. Standard-Sperrseitendateien sind im Lieferumfang der Websense-Software enthalten. Sie können diese Standarddateien verwenden oder eigene benutzerdefinierte Versionen erstellen.

- Passen Sie die Standardseiten an, um die Sperrmeldung zu ändern (siehe *Arbeiten mit Sperrseiten*, Seite 91).
- Konfigurieren Sie die Websense-Software, um (Standard- oder benutzerdefinierte) Sperrseiten zu verwenden, die auf einem fernen Webserver gehostet werden (siehe *Verwenden einer alternativen Sperrseite auf einem anderen Computer*, Seite 97).

Protokollsperrmeldungen

Verwandte Themen:

- *Arbeiten mit Sperrseiten*, Seite 91
- *Erstellen von alternativen Sperrmeldungen*, Seite 96
- *Verwenden einer alternativen Sperrseite auf einem anderen Computer*, Seite 97

Die Websense-Software zeigt in der Regel eine Protokollsperrmeldung an, wenn ein Benutzer oder eine Anwendung ein gesperrtes Nicht-HTTP-Protokoll anfordert.

Wenn jedoch eine gesperrte FTP-, HTTPS- oder Gopher-Site in einem Browser angefordert wird und die Anforderung einen Proxy-Server passiert, wird die HTML-basierte Sperrseite stattdessen in einem Browser angezeigt.

Wenn eine Anwendung das gesperrte Protokoll anfordert, kann der Benutzer außerdem eine Fehlermeldung von der Anwendung erhalten, in der angegeben ist, dass sie nicht ausgeführt werden kann. Fehlermeldungen von Anwendungen werden nicht von der Websense-Software generiert.

Zur Anzeige von Protokollsperrmeldungen auf Windows-Computern ist es u. U. erforderlich, das System zu konfigurieren:

- Der Windows Messenger-Dienst muss aktiviert sein, um Protokollsperrmeldungen auf Clientcomputern anzuzeigen, auf denen Windows NT, XP oder 200x ausgeführt wird. In der Standardeinstellung ist dieser Dienst deaktiviert. Öffnen Sie das Dialogfeld "Windows Services", um herauszufinden, ob der Dienst auf einem bestimmten Computer ausgeführt wird (siehe *Das Dialogfeld für die Windows-Dienste*, Seite 422).
- Führen Sie die Datei **winpopup.exe** aus, die sich im Windows-Verzeichnis befindet, um Protokollsperrmeldungen auf einem Windows 98-Computer anzuzeigen. Führen Sie die Anwendung über die Eingabeaufforderung aus oder kopieren Sie sie in den Ordner "Autostart", um sie automatisch zu starten.

Protokollsperrmeldungen werden auf Linux-Computern nicht angezeigt. HTML-Sperrseiten werden unabhängig vom Betriebssystem angezeigt.

Bei aktivierter Protokollfilterung werden Protokollanforderungen von der Websense-Software unabhängig davon gefiltert, ob Protokollsperrmeldungen für die Anzeige auf Clientcomputern konfiguriert sind.

Arbeiten mit Sperrseiten

Verwandte Themen:

- *Protokollsperrmeldungen*, Seite 90
- *Anpassen der Sperrmeldung*, Seite 92
- *Erstellen von alternativen Sperrmeldungen*, Seite 96
- *Verwenden einer alternativen Sperrseite auf einem anderen Computer*, Seite 97

Die Dateien, die verwendet werden, um Websense-Sperrseiten zu erstellen, werden im Verzeichnis **Websense\BlockPages\en\Default** gespeichert:

- **master.html** erstellt den Informations-Frame für die Sperrseite und verwendet eine der folgenden Dateien, um die entsprechenden Optionen im unteren Frame anzuzeigen.

Dateiname	Inhalt
blockFrame.html	Text und Schaltflächen (Option "Zurück") für Sites in gesperrten Kategorien.
continueFrame.html	Text und Schaltflächen für Sites in Kategorien, auf die die Aktion **Bestätigen** angewendet wird.
quotaFrame.html	Text und Schaltflächen für Sites in Kategorien, auf die die Aktion **Quote** angewendet wird.
moreInfo.html	Inhalt für die Seite, die angezeigt wird, wenn ein Benutzer auf der Sperrseite auf den Link **Weitere Informationen** klickt.

- **block.html** enthält den Text für den oberen Frame der Sperrmeldung, in dem erklärt wird, dass der Zugriff eingeschränkt ist, die angeforderte Site aufgelistet und der Grund beschrieben wird, warum die Site eingeschränkt ist.

Anpassen der Sperrmeldung

Verwandte Themen:

- *Verändern der Größe des Meldungs-Frames*, Seite 93
- *Ändern des Logos, das auf der Sperrseite angezeigt wird*, Seite 93
- *Verwenden von Inhaltsvariablen der Sperrseite*, Seite 94
- *Wiederherstellen der Standardsperrseiten*, Seite 96

Sie können eine Kopie der Standard-Sperrseitendateien erstellen und anschließend in der Kopie den oberen Frame der Sperrseite anpassen, die die Benutzer erhalten.

- Fügen Sie Informationen über die Richtlinien Ihrer Organisation für die Internetnutzung ein.
- Geben Sie eine Methode an, wie mit der Personalabteilung oder einem Websense-Administrator bezüglich der Richtlinien für die Internetnutzung Kontakt aufgenommen werden kann.

1. Navigieren Sie zum Websense-Sperrseitenverzeichnis:

   `<Installationspfad>\BlockPages\en\Default`

2. Kopieren Sie die Sperrseitendateien in das benutzerdefinierte Sperrseitenverzeichnis.

   `<Installationspfad>\BlockPages\en\Custom`

   Hinweis
   Bearbeiten Sie die ursprünglichen Sperrmeldungsdateien **nicht** im Verzeichnis **BlockPages\en\Default**. Kopieren Sie die Dateien in das Verzeichnis **BlockPages\en\Custom** und bearbeiten Sie dann die Kopien.

3. Öffnen Sie die Datei in einem Texteditor, z. B. in Editor oder vi.

   Warnung
   Verwenden Sie einen einfachen Texteditor, um Sperrmeldungsdateien zu bearbeiten. Einige HTML-Editoren verändern den HTML-Code, wodurch die Dateien beschädigt und Probleme mit der Anzeige der Sperrmeldungen verursacht werden können.

4. Bearbeiten Sie den Text. Die in den Dateien enthaltenen Kommentare dienen als Anleitung für die Durchführung von Änderungen.

   Verändern Sie **nicht** die Token (von den Symbolen $* und *$ umgeben) oder die Struktur des HTML-Codes. Diese Token ermöglichen der Websense-Software die Anzeige von bestimmten Informationen in der Sperrmeldung.

5. Speichern Sie die Datei.

6. Starten Sie Filtering Service neu (Anweisungen finden Sie unter *Anhalten und Starten der Websense-Dienste*, Seite 302).

Verändern der Größe des Meldungs-Frames

Abhängig davon, welche Informationen in der Sperrmeldung enthalten sein sollen, ist es u. U. erforderlich, die standardmäßige Breite der Sperrmeldung und Höhe des oberen Frames anzupassen. So ändern Sie die Größenparameter in der Datei **master.html**:

1. Kopieren Sie **master.html** aus dem Verzeichnis **Websense\BlockPages\en\Default** in **Websense\BlockPages\en\Custom**.
2. Öffnen Sie die Datei in einem Texteditor, z. B. im Editor oder in vi (und nicht in einem HTML-Editor).
3. Ändern Sie die Breite des Meldungs-Frames, indem Sie die folgende Zeile bearbeiten:

   ```
   <div style="border: 1px solid #285EA6;width: 600px...">
   ```

   Ändern Sie den Wert für die **Breite** gemäß Ihren Anforderungen.
4. Bearbeiten Sie die folgende Zeile, um es zu ermöglichen, im oberen Frame der Meldung durch Blättern zusätzliche Informationen anzuzeigen.

   ```
   <iframe src="$*WS_BLOCKMESSAGE_PAGE*$*WS_SESSIONID*$" ...
   scrolling="no" style="width:100%; height: 6em;">
   ```

   Ändern Sie den Wert des Parameters für das **Blättern** in **auto**, damit eine Bildlaufleiste angezeigt wird, wenn die Höhe des Frames für den Meldungstext nicht ausreicht.

   Sie können auch die Höhe des Frames ändern, indem Sie den Parameterwert für die **Höhe** ändern.
5. Speichern und schließen Sie die Datei.
6. Starten Sie Filtering Service neu, um die Änderung zu übernehmen (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).

Ändern des Logos, das auf der Sperrseite angezeigt wird

In der Datei **master.html** ist u. a. auch der HTML-Code enthalten, der verwendet wird, um ein Websense-Logo auf der Sperrseite anzuzeigen. So zeigen Sie stattdessen das Logo Ihrer Organisation an:

1. Kopieren Sie die Sperrseitendateien aus dem Verzeichnis **Websense\BlockPages\en\Default** in **Websense\BlockPages\en\Custom**, falls sie noch nicht kopiert wurden.
2. Kopieren Sie eine Grafikdatei mit dem Logo Ihrer Organisation an denselben Speicherort.

3. Öffnen Sie **master.html** in einem Texteditor, z. B. im Editor oder in vi (aber nicht in einem HTML-Editor), und bearbeiten Sie die folgende Zeile, um das Websense-Logo durch das Logo Ihrer Organisation zu ersetzen:

   ```
   <img title="Websense" src="/en/Custom/wslogo_block_page.png"
   ...>
   ```

   - Ersetzen Sie **wslogo_block_page.png** durch den Namen der Grafikdatei, die das Logo Ihrer Organisation enthält.
   - Ersetzen Sie den Wert des Parameters für den **Titel**, damit der Name Ihrer Organisation angegeben wird.
4. Speichern und schließen Sie die Datei.
5. Starten Sie Filtering Service neu, um die Änderung zu übernehmen (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).

Verwenden von Inhaltsvariablen der Sperrseite

Inhaltsvariablen steuern, welche Informationen auf HTML-Sperrseiten angezeigt werden. Die folgenden Variablen sind im Code der Standardsperrmeldung enthalten.

Variablenname	Angezeigter Inhalt
WS_DATE	Aktuelles Datum
WS_USERNAME	Name des aktuellen Benutzers (ausschließlich Domänenname)
WS_USERDOMAIN	Domänenname für den aktuellen Benutzer
WS_IPADDR	IP-Adresse des Computers, von dem die Anforderung stammt
WS_WORKSTATION	Computername des gesperrten Computers (wenn kein Name verfügbar ist, wird die IP-Adresse angezeigt)

Fügen Sie den Variablennamen im entsprechenden HTML-Tag zwischen die Symbole $* *$ ein, um eine Variable zu verwenden:

```
<p id="UserName">$*WS_USERNAME*$</p>
```

In diesem Fall ist *WS_USERNAME* die Variable.

Der Code der Sperrmeldung enthält zusätzliche Variablen, die weiter unten beschrieben werden. Diese Variablen können nützlich sein, wenn Sie Ihre eigenen, benutzerdefinierten Sperrmeldungen erstellen. Wenn diese Variablen jedoch in von Websense definierten Sperrmeldungsdateien enthalten sind, ändern Sie diese **nicht**.

Filtering Service verwendet diese Variablen zum Bearbeiten der gesperrten Anforderungen. Aus diesem Grund dürfen sie nicht verändert werden.

Variablenname	Zweck
WS_URL	Zeigt die angeforderte URL an
WS_BLOCKREASON	Zeigt den Grund für die Sperrung der Site an (z. B. die angewendete Filteraktion)
WS_ISSECURITY	Gibt an, ob die angeforderte Site zu einer der Standardkategorien in der Klasse "Sicherheitsrisiko" gehört. Wenn TRUE, wird die Sicherheitssperrseite angezeigt.
WS_PWOVERRIDECGIDATA	Gibt Informationen über die Verwendung der Schaltfläche **Mit Passwort freigeben** in ein Eingabefeld des HTML-Codes der Sperrseite ein
WS_QUOTA_CGIDATA	Gibt Informationen über die Verwendung der Schaltfläche **Quotenzeit verwenden** in ein Eingabefeld des HTML-Codes der Sperrseite ein
WS_PASSWORDOVERRID_BEGIN, WS_PASSWORDOVERRID_END	Element zum Aktivieren der Funktion zur Freigabe mit Passwort
WS_MOREINFO	Zeigt (nach Klicken auf den Link **Weitere Informationen**) ausführliche Informationen darüber an, warum die angeforderte Site gesperrt wurde
WS_POLICYINFO	Zeigt an, welcher Richtlinie der anfordernde Client unterliegt
WS_MOREINFOCGIDATA	Sendet Daten über die Verwendung des Links **Weitere Informationen** an Filtering Service
WS_QUOTATIME	Zeigt die Menge der verbleibenden Quotenzeit für den anfordernden Client an
WS_QUOTAINTERVALTIME	Zeigt die Länge der Quotensitzung an, die für den anfordernden Client konfiguriert wurde
WS_QUOTABUTTONSTATE	Gibt an, ob die Schaltfläche **Quotenzeit verwenden** für eine bestimmte Anforderung aktiviert oder deaktiviert ist
WS_SESSIONID	Fungiert als interne Kennung, die mit einer Anforderung verknüpft ist

Variablenname	Zweck
WS_TOPFRAMESIZE	Gibt die Größe des oberen Bereichs einer Sperrseite (als prozentualen Anteil) an, die von einem benutzerdefinierten gesperrten Server gesendet wurde, wenn einer konfiguriert wurde
WS_BLOCKMESSAGE_PAGE	Gibt die Quelle an, die für den oberen Frame einer Sperrseite verwendet werden soll
WS_CATEGORY	Zeigt die Kategorie der gesperrten URL an
WS_CATEGORYID	Eindeutige Kennung für die Kategorie der angeforderten URL

Wiederherstellen der Standardsperrseiten

Wenn Benutzer Fehlermeldungen erhalten, nachdem Sie benutzerdefinierte Sperrmeldungen implementiert haben, können Sie die Standardsperrmeldungen wie folgt wiederherstellen:

1. Löschen Sie alle Dateien im Verzeichnis **Websense\BlockPages\en\Custom**. Daraufhin verwendet die Websense-Software automatisch wieder die Dateien im Standardverzeichnis.
2. Starten Sie Filtering Service neu (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).

Erstellen von alternativen Sperrmeldungen

Verwandte Themen:

- *Arbeiten mit Sperrseiten*, Seite 91
- *Anpassen der Sperrmeldung*, Seite 92

Sie können Ihre eigenen HTML-Dateien erstellen, die den Text bereitstellen, der im oberen Frame der Sperrseite angezeigt wird. Verwenden Sie vorhandene HTML-Dateien, erstellen Sie alternative Dateien von Grund auf oder erstellen Sie Kopien von **block.html**, um diese als Vorlage zu verwenden.

- Erstellen Sie für jedes der drei folgenden Protokolle unterschiedliche Sperrmeldungen: HTTP, FTP und Gopher.
- Hosten Sie die Dateien auf dem Websense-Computer oder auf Ihrem internen Webserver (siehe *Verwenden einer alternativen Sperrseite auf einem anderen Computer*, Seite 97).

Nachdem Sie die alternativen Sperrmeldungsdateien erstellt haben, müssen Sie die Websense-Software konfigurieren, um die neuen Meldungen anzeigen zu können (siehe *Konfigurieren von Websense-Filtereinstellungen*, Seite 60). Dabei können Sie angeben, welche Meldung für jedes der konfigurierbaren Protokolle verwendet wird.

Verwenden einer alternativen Sperrseite auf einem anderen Computer

Verwandte Themen:

- *Arbeiten mit Sperrseiten*, Seite 91
- *Anpassen der Sperrmeldung*, Seite 92
- *Erstellen von alternativen Sperrmeldungen*, Seite 96

Statt Sperrseiten von Websense zu verwenden und nur die Meldung im oberen Frame anzupassen, können Sie auch Ihre eigenen HTML-Sperrseiten erstellen und diese auf einem internen Webserver hosten.

Hinweis

Sperrseiten können auf einem externen Webserver gespeichert werden. Wenn dieser Server jedoch eine Site hostet, die in der Stammdatenbank (Master Database) aufgeführt ist und zu einer gesperrten Kategorie gehört, ist die Sperrseite auch gesperrt.

Einige Organisationen verwenden alternative, ferne Sperrseiten, um die Identität des Websense-Servercomputers zu verbergen.

Die ferne Sperrseite kann eine beliebige HTML-Datei sein, die nicht über dasselbe Format wie die standardmäßigen Websense-Sperrseiten verfügen muss. Wenn Sie Sperrseiten mit dieser Methode erstellen, können Sie die Funktionen "Weiter", "Quotenzeit verwenden" und "Mit Passwort freigeben" jedoch nicht verwenden, die mit den von Websense definierten Sperrseiten (Standard oder benutzerdefiniert) verfügbar sind.

Wenn sich die Dateien am richtigen Speicherort befinden, bearbeiten Sie die Datei **eimserver.ini**, damit sie auf die neue Sperrseite verweist.

1. Beenden Sie die Filtering Service- und Policy Server-Dienste von Websense in dieser Reihenfolge (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).
2. Navigieren Sie auf dem Filtering Service-Computer zum **bin**-Verzeichnis von Websense (in der Standardeinstellung: \Programme\Websense\bin oder /opt/websense/bin).
3. Erstellen Sie eine Sicherungskopie der Datei **eimserver.ini** und speichern Sie sie in einem anderen Verzeichnis.

4. Öffnen Sie die Datei **eimserver.ini** in einem Texteditor und suchen Sie den Bereich **[WebsenseServer]** (im oberen Bereich der Datei).
5. Geben Sie entweder den Hostnamen oder die IP-Adresse des Servers, der die Sperrseite hostet., im folgenden Format ein:

   ```
   UserDefinedBlockPage=http://<Hostname oder IP-Adresse>
   ```

   Der Protokollbereich der URL (http://) muss angegeben werden.
6. Speichern Sie die Datei und schließen Sie den Texteditor.
7. Starten Sie Policy Server und Filtering Service von Websense in dieser Reihenfolge neu.

Nachdem die Dienste gestartet wurden, erhalten die Benutzer die Sperrseite, die auf dem alternativen Computer gehostet werden.

6 Verwenden von Berichten für das Beurteilen der Filterrichtlinien

Verwandte Themen:

- *Berichterstellung – Übersicht*, Seite 100
- *Präsentationsberichte*, Seite 102
- *Untersuchungsberichte*, Seite 123
- *Zugreifen auf eigene Berichte*, Seite 151

Websense Manager stellt verschiedene Berichterstellungs-Tools zur Beurteilung der Effektivität Ihrer Filterrichtlinien bereit. (Websense Manager und die Reporting-Komponenten von Websense müssen auf Windows-Servern installiert sein.)

- Die Seite **Heute** wird als erste Seite nach dem Öffnen von Websense Manager angezeigt. Sie enthält den Betriebsstatus der Websense-Software und kann Diagramme der Filteraktivitäten im Netzwerk seit Mitternacht anzeigen. (Siehe *Heute: Zustand, Sicherheit und Nutzen seit Mitternacht*, Seite 22.)
- Die Seite **Verlauf** enthält Diagramme der Filteraktivitäten im Netzwerk für einen Zeitraum von bis zu 30 Tagen, je nach Informationsmenge in der Protokolldatenbank. Diese Diagramme enthalten nicht die Aktivitäten des aktuellen Tages. (Siehe *Verlauf: Letzte 30 Tage*, Seite 25.)
- **Präsentationsberichte** und **Untersuchungsberichte** bieten viele Optionen für das Generieren, Anpassen und Planen von Berichten. Weitere Informationen dazu finden Sie unter *Berichterstellung – Übersicht*, Seite 100.

Wenn Websense Manager in Ihrer Organisation auf einem Linux-Server installiert wurde oder Sie die Verwendung des Reporting-Programms Websense Explorer for Linux statt der Reporting-Komponenten für Windows vorziehen, werden die Berichterstellungsoptionen nicht in Websense Manager angezeigt. Auf den Seiten "Heute" und "Verlauf" werden keine Filterdiagramme angezeigt. Informationen über die Installation dieses Programms und das Generieren von Berichten finden Sie im *Explorer for Linux Administrator's Guide*.

Berichterstellung – Übersicht

Verwandte Themen:

- *Verwenden von Berichten für das Beurteilen der Filterrichtlinien*, Seite 99
- *Präsentationsberichte*, Seite 102
- *Untersuchungsberichte*, Seite 123
- *Zugreifen auf eigene Berichte*, Seite 151

Neben den auf den Seiten "Heute" und "Verlauf" angezeigten Diagrammen bietet die Websense-Software 2 Berichterstellungsoptionen: Präsentationsberichte und Untersuchungsberichte.

> **Hinweis**
> In Organisationen mit delegierter Verwaltung sind einige Administratoren möglicherweise nicht in der Lage, auf alle Berichterstellungsfunktionen zuzugreifen. Siehe *Delegierte Verwaltung*, Seite 251.

Präsentationsberichte bieten eine Liste von Berichtsdefinitionen. Einige Berichte sind Tabellenberichte, andere enthalten sowohl ein Balkendiagramm als auch eine Tabelle. So generieren Sie einen Präsentationsbericht:

1. Wählen Sie einen Bericht aus der Liste aus.
2. Klicken Sie auf **Ausführen**.
3. Wählen Sie einen Datumsbereich.
4. Klicken Sie auf **Jetzt ausführen**.

Neben dem Generieren vordefinierter Diagramme haben Sie die Möglichkeit, diese zu kopieren und einen benutzerdefinierten Berichtsfilter anzuwenden, der bestimmte Clients, Kategorien, Protokolle oder Aktivitäten ermittelt, die einbezogen werden müssen. Markieren Sie häufig verwendete Berichtsdefinitionen als Favoriten, um die Suche danach zu vereinfachen.

Sie können die Ausführung jedes beliebigen Präsentationsberichts für einen bestimmten Zeitpunkt oder in einer wiederkehrenden Zeitfolge planen. Detaillierte Informationen dazu finden Sie unter *Präsentationsberichte*, Seite 102.

Untersuchungsberichte ermöglichen das interaktive Durchsuchen von Protokolldaten. Die Hauptseite enthält ein Balkendiagramm als Zusammenfassung der Aktivität sortiert nach Risikoklasse. Klicken Sie auf die verschiedenen Elemente auf

der Seite, um das Diagramm zu aktualisieren oder eine andere Ansicht der Daten zu erzeugen.

- Klicken Sie auf den Namen der Risikoklasse, und wählen Sie anschließend eine detailliertere Ansicht der Informationen dieser Risikoklasse. Sie können z. B. die Aktivität sortiert nach Benutzern in der Risikoklasse "Gesetzliche Haftung" anzeigen.
- Klicken Sie auf einen Benutzernamen im resultierenden Diagramm, um diesen Benutzer detaillierter anzuzeigen.
- Wählen Sie eine andere Option aus der Liste **Internetnutzung nach**, um das zusammenfassende Balkendiagramm zu ändern.
- Füllen Sie die Felder direkt über dem Balkendiagramm aus, um zwei Informationsebenen gleichzeitig anzuzeigen. Ein Beispiel: Wenn Sie mit einem zusammenfassenden Diagramm der Kategorien beginnen, könnten Sie **10**, **Benutzer** und **5** auswählen, um die Aktivität der 5 wichtigsten Benutzer in den 10 wichtigsten Kategorien anzuzeigen.
- Klicken Sie auf einen Balken oder eine Zahl, um einen Detailbericht dieses Elements (Risikoklasse, Kategorie, Benutzer oder anderes) anzuzeigen.
- Klicken Sie auf **Als Favoriten definierte Berichte**, um ein besonders hilfreiches Berichtsformat für eine zukünftige Verwendung zu speichern, oder um einen zuvor gespeicherten Favoriten zu generieren.

Es stehen zahlreiche Möglichkeiten zur Verfügung. Detaillierte Informationen über die vielen Anzeigemöglichkeiten der Internetnutzungsdaten finden Sie unter *Untersuchungsberichte*, Seite 123.

Was ist die "Navigationsdauer im Internet"?

Verwandte Themen:

- *Datenbankjobs*, Seite 342
- *Konfigurieren der Optionen für die Navigationsdauer im Internet*, Seite 347

Sie können sowohl Präsentations- als auch Untersuchungsberichte auf Basis der Navigationsdauer im Internet (IBT), dem Zeitraum, den eine Person für den Zugriff auf Websites verwendet hat, generieren. Kein Software-Programm ist in der Lage, den genauen Zeitraum zu bestimmen, den eine Person mit dem tatsächlichen Betrachten einer bestimmten Website verbringt, nachdem diese geöffnet wurde. Die Person könnte möglicherweise die Website öffnen, sie für ein paar Sekunden betrachten, und dann einen geschäftlichen Anruf entgegennehmen, bevor sie eine weitere Website anfordert. Eine weitere Person verbringt möglicherweise mehrere Minuten mit dem detaillierten Lesen jeder Website, bevor sie zur nächsten wechselt.

Die Websense-Software stellt einen Protokolldatenbank-Job für das Berechnen der Navigationsdauer im Internet (IBT) bereit, der auf einer Formel bestimmter

konfigurierbarer Werte basiert. Dieser Job wird einmal am Tag ausgeführt, wodurch die Daten der Navigationsdauer die tatsächlichen Protokolldaten verzögern können.

Für die Berechnung der Navigationszeit beginnt eine Internetsitzung, wenn ein Benutzer einen Browser öffnet. Sie dauert an, so lange dieser Benutzer mindestens alle 3 Minuten weitere Websites anfordert. (Dieser Standardschwellenwert für die Lesezeit kann konfiguriert werden.)

Die Internetsitzung endet, wenn mehr als 3 Minuten vergehen, bevor der Benutzer eine andere Website anfordert. Die Websense-Software berechnet die Gesamtzeit der Sitzung, wobei mit dem Zeitpunkt der ersten Anforderung begonnen und 3 Minuten nach der letzten Anforderung geendet wird.

Eine neue Sitzung beginnt, wenn der Benutzer nach mehr als 3 Minuten weitere Anforderungen stellt. In der Regel besteht die Navigationsdauer eines Benutzers aus mehreren Sitzungen pro Tag.

Informationen über den Job für die Berechnung der Navigationsdauer im Internet und die entsprechenden Konfigurationsoptionen finden Sie unter *Datenbankjobs*, Seite 342, und *Konfigurieren der Optionen für die Navigationsdauer im Internet*, Seite 347.

Präsentationsberichte

Verwandte Themen:

- *Kopieren eines Präsentationsberichts*, Seite 105
- *Kopieren eines Präsentationsberichts*, Seite 105
- *Arbeiten mit Favoriten*, Seite 113
- *Generieren von Präsentationsberichten*, Seite 114
- *Planen von Präsentationsberichten*, Seite 116
- *Anzeigen der Liste der geplanten Jobs*, Seite 121

Die Seite **Berichterstellung > Präsentationsberichte** enthält eine Liste der vordefinierten Diagramme und Tabellenberichte, die jeweils bestimmte Informationen aus der Protokolldatenbank wiedergeben (siehe *Einführung in die Log Database*, Seite 341). Wählen Sie einen Bericht aus diesem Berichtskatalog aus, um eine kurze Beschreibung anzuzeigen.

Sie können einen vordefinierten Bericht kopieren und den Berichtsfilter anpassen, um festzulegen, welche Clients, Kategorien, Protokolle und Aktionen enthalten sein sollen. Häufig verwendete Berichte können als Favoriten markiert werden, sodass sie rasch gefunden werde können.

Sie können einen beliebigen Bericht sofort ausführen oder die Ausführung ausgewählter Berichte in einer verzögerten oder wiederkehrenden Zeitfolge planen. Wählen Sie das Ausgabeformat, und verteilen Sie die geplanten Berichte an eine ausgewählte Empfängergruppe.

Wenn Sie einen Bericht direkt von der Seite "Präsentationsberichte" im HTML-Format generieren, wird der Bericht nicht gespeichert, wenn Sie zu einer anderen Seite wechseln. Wenn Sie einen Bericht im PDF- oder XLS-Format generieren und sofort anzeigen, wird der Bericht nicht gespeichert, wenn Sie das Anzeigeprogramm (Adobe Reader oder Microsoft Excel) schließen.

Alternativ können Sie die PDF- oder XLS-Datei speichern, statt sie umgehend anzuzeigen, oder die Option "Speichern" im Anzeigeprogramm verwenden. Achten Sie in diesen Fällen darauf, Berichtsdateien regelmäßig zu löschen oder zu verschieben, um weiterhin über ausreichenden Speicherplatz zu verfügen.

Geplante Berichte werden automatisch im folgenden Verzeichnis gespeichert:

```
<Installationspfad>\ReportingOutput
```

Der Standardinstallationspfad lautet C:\Program Files\Websense.

Wenn ein geplanter Präsentationsbericht ausgeführt wird, wird die Berichtsdatei als E-Mail-Anhang mit dem Namen **presentationreport_0** an die Empfänger gesendet. Die Ziffernfolge wird je nach Anzahl der angehängten Berichte schrittweise erhöht. Beachten Sie, dass der Name des Anhangs nicht dem Namen der Datei entspricht, die im Verzeichnis ReportingOutput gespeichert wurde. Wenn Sie einen bestimmten Bericht in diesem Verzeichnis suchen, durchsuchen Sie die Dateien, die an dem Tag erstellt wurden, an dem der geplante Job ausgeführt wurde.

Berichte werden automatisch nach 15 Tagen aus dem Verzeichnis ReportingOutput gelöscht. Wenn Sie die Berichte für einen längeren Zeitraum aufbewahren möchten, können Sie sie in Ihre Backup-Routine aufnehmen, oder planen Sie sie, und speichern Sie die per E-Mail gesendeten Dateien an einem Speicherort, der eine langfristige Speicherung zulässt.

Je nach Anzahl der täglich generierten Berichte können Berichtsdateien erheblichen Speicherplatz beanspruchen. Stellen Sie sicher, dass auf der Festplatte auf dem Computer, auf dem Websense Manager ausgeführt wird, ausreichender Speicherplatz zur Verfügung steht. Wenn das Verzeichnis ReportingOutput zu viel Speicherplatz einnimmt, bevor die Dateien automatisch gelöscht werden, können Sie die Dateien manuell löschen.

Die Websense-Software generiert den Bericht in dem von Ihnen ausgewählten Format: PDF (Adobe Reader), XLS (Microsoft Excel) oder HTML. Wenn Sie das HTML-Format wählen, wird der Bericht im Inhaltsfenster von Websense Manager angezeigt. Diese Berichte können nicht gedruckt oder als Datei gespeichert werden. Wenn Sie einen Bericht drucken oder als Datei speichern möchten, wählen Sie die Ausgabeformate PDF oder XLS.

Wenn Sie das PDF- oder XLS-Format wählen, können Sie auswählen, ob die Berichtsdatei auf der Festplatte gespeichert oder in einem separaten Fenster angezeigt wird.

> **Wichtig**
>
> Zum Anzeigen von Präsentationsberichten im PDF-Format muss Adobe Reader Version 7.0 (oder höher) auf dem Computer installiert sein, von dem auf Websense Manager zugegriffen wird.
>
> Zum Anzeigen von Präsentationsberichten im XLS-Format muss Microsoft Excel 2003 (oder höher) auf dem Computer installiert sein, von dem auf Websense Manager zugegriffen wird.

Navigieren Sie auf der Seite "Präsentationsberichte" durch den Berichtskatalog, und wählen Sie einen Bericht. Verwenden Sie daraufhin die Steuerungen auf der Seite, um z. B. den Bericht auszuführen oder eine Kopie zu erstellen, bei der Sie den Berichtsfilter anpassen.

Schaltfläche	Aktion
Nur Favoriten anzeigen	Wählen Sie diese Option, wenn im Berichtskatalog nur die als Favoriten definierten Berichte angezeigt werden sollen. Deaktivieren Sie diese Option, um die vollständige Berichtsliste wiederherzustellen.
Berichtsfilter bearbeiten	Diese Option steht nur zur Verfügung, wenn eine Kopie eines vordefinierten Berichts ausgewählt wurde. Mit ihr können Sie bestimmte Kategorien, Protokolle, Benutzer und Aktionen auswählen, die im Bericht enthalten sein sollen. Siehe *Kopieren eines Präsentationsberichts*, Seite 105.
Kopieren	Erstellt eine Kopie des ausgewählten Berichts und fügt sie dem Berichtskatalog als benutzerdefinierten Bericht hinzu. Siehe *Kopieren eines Präsentationsberichts*, Seite 105. Wählen Sie den benutzerdefinierten Bericht, und legen Sie anschließend bestimmte Parameter dafür fest, indem Sie auf **Berichtsfilter bearbeiten** klicken.
Favorit	Definiert den ausgewählten Bericht als Favoriten oder entfernt die Kennzeichnung als Favorit. Siehe *Arbeiten mit Favoriten*, Seite 113. Als Favoriten definierte Berichte werden im Berichtskatalog mit einem Sternsymbol gekennzeichnet. Steuern Sie mit dem Kontrollkästchen **Nur Favoriten anzeigen**, welche Berichte im Berichtskatalog angezeigt werden.

Schaltfläche	Aktion
Löschen	Löscht die ausgewählte Berichtskopie aus dem Berichtskatalog. In der Installation der Software enthaltene vordefinierte Berichte können nicht gelöscht werden. Wenn der gelöschte Bericht in geplanten Jobs enthalten ist, wird er weiterhin mit diesem Job generiert.
Ausführen	Generiert den ausgewählten Bericht, nachdem Sie den Datumsbereich und das Ausgabeformat ausgewählt haben. Siehe *Generieren von Präsentationsberichten*, Seite 114. Informationen über das Steuern anderer Aspekte eines benutzerdefinierten Berichts (Kopie eines vordefinierten Berichts) finden Sie unter *Kopieren eines Präsentationsberichts*, Seite 105. Wenn Sie das Ausführen des Berichts für eine andere Uhrzeit oder in einer wiederkehrenden Zeitfolge planen möchten, klicken Sie auf "Scheduler".

Die Schaltflächen über der Seite bieten zusätzliche Optionen für Präsentationsberichte.

Schaltfläche	Aktion
Warteschlange für Jobs	Zeigt eine Seite mit der Liste aller geplanter Jobs, die erstellt wurden, mit ihrem jeweiligen Status an. Siehe *Anzeigen der Liste der geplanten Jobs*, Seite 121.
Scheduler	Ermöglicht das Definieren eines Jobs mit einem oder mehreren Berichte, die zu einem bestimmten Zeitpunkt oder in einer wiederkehrenden Zeitfolge ausgeführt werden sollen. Siehe *Planen von Präsentationsberichten*, Seite 116.

Kopieren eines Präsentationsberichts

Verwandte Themen:

- *Kopieren eines Präsentationsberichts*, Seite 105
- *Präsentationsberichte*, Seite 102

In seiner Ausgangskonfiguration enthält die Seite **Präsentationsberichte** einen Berichtskatalog mit allen vordefinierten Berichten, die mit der Software installiert wurden. Sie können einen dieser Berichte für einen bestimmten Zeitraum generieren, indem Sie den Bericht auswählen und anschließend auf "Ausführen" klicken.

Diese vordefinierten Berichte können auch als Vorlagen eingesetzt werden, indem sie kopiert und anschließend für einen benutzerdefinierten Berichtsfilter verwendet werden. Erstellen Sie einen Berichtsfilter, um z. B. zu steuern, welche Benutzer, Kategorien, Protokolle und Aktionen übernommen werden sollen, wenn Sie mit dieser Kopie einen Bericht generieren.

Nachdem Sie einen Bericht kopiert und den Berichtsfilter bearbeitet haben, können Sie den neuen Bericht kopieren, um Variationen dieser Kopie zu erstellen.

1. Wählen Sie einen Bericht im Berichtskatalog aus.
2. Klicken Sie auf **Kopieren**.

   Im Berichtskatalog wird ein Duplikat des Berichtsnamens mit einem Code angezeigt, der darauf hinweist, dass es sich um eine Kopie handelt.
3. Wählen Sie eine Kopie im Berichtskatalog aus, und klicken Sie anschließend auf **Berichtsfilter bearbeiten**, um die Elemente des Berichts zu ändern. Siehe *Kopieren eines Präsentationsberichts*, Seite 105.

Definieren des Berichtsfilters

Verwandte Themen:

- *Kopieren eines Präsentationsberichts*, Seite 105
- *Generieren von Präsentationsberichten*, Seite 114

Mit Berichtsfiltern können Sie steuern, welche Informationen in einen Bericht einbezogen werden. Sie haben z. B. die Möglichkeit, einen Bericht auf ausgewählte Clients, Kategorien, Risikoklassen oder Protokolle oder sogar ausgewählte Filteraktionen (Zulassen, Sperren usw.) einzuschränken. Darüber hinaus können Sie dem Eintrag im Berichtskatalog einen neuen Namen und eine neue Beschreibung geben, ein benutzerdefiniertes Logo dafür auswählen und andere allgemeine Optionen mit dem Berichtsfilter festlegen.

Hinweis

Für die Verwendung eines benutzerdefinierten Logos sind einige Vorbereitungen vor dem Definieren des Berichtsfilters erforderlich. Sie müssen die gewünschte Grafik in einem unterstützten Grafikformat erstellen und die Datei an dem dafür vorgesehenen Speicherort speichern. Siehe *Anpassen des Berichtslogos*, Seite 112.

Die für den Filter jeweils verfügbaren Optionen hängen vom ausgewählten Bericht ab. Wenn Sie z. B. einen Bericht für Gruppeninformationen wie "Wichtigste gesperrte Gruppen nach Anforderungen" ausgewählt haben, können Sie zwar steuern, welche Gruppen im Bericht angezeigt werden. Sie können jedoch nicht individuelle Benutzer auswählen.

Der Filter für vordefinierte Berichte kann nicht geändert werden. Sie können jedoch den Filter einer Kopie eines vordefinierten Berichts bearbeiten:

1. Wählen Sie einen Bericht im Berichtskatalog aus.

   Wenn die Schaltfläche "Berichtsfilter bearbeiten" deaktiviert ist, fahren Sie mit Schritt 2 fort.

Wenn die Schaltfläche "Berichtsfilter bearbeiten" aktiviert ist, fahren Sie mit Schritt 3 fort.

2. Klicken Sie auf **Kopieren**, um eine bearbeitbare Kopie zu erstellen.

   Im Berichtskatalog wird ein Duplikat des Berichtsnamens mit einem Code angezeigt, der darauf hinweist, dass es sich um eine Kopie handelt.

3. Klicken Sie auf die Schaltfläche **Berichtsfilter bearbeiten**.

   Die Seite "Berichtsfilter bearbeiten" wird geöffnet und enthält separate Registerkarten für die Verwaltung unterschiedlicher Berichtselemente. Wählen Sie auf den Registerkarten die gewünschten Elemente aus, und klicken Sie anschließend auf **Weiter**, um zur nächsten Registerkarte zu wechseln. Detaillierte Anweisungen finden Sie unter:

   - *Auswählen von Clients für einen Bericht*, Seite 107
   - *Auswählen von Kategorien für einen Bericht*, Seite 108
   - *Auswählen von Protokollen für einen Bericht*, Seite 109
   - *Auswählen von Aktionen für einen Bericht*, Seite 110
   - *Festlegen von Berichtsoptionen*, Seite 111

4. Wählen Sie auf der Registerkarte **Bestätigen** aus, ob der Bericht direkt ausgeführt oder für einen späteren Zeitpunkt geplant werden soll, und speichern Sie den Berichtsfilter. Siehe *Bestätigung der Berichtsfilterdefinition*, Seite 113.

Auswählen von Clients für einen Bericht

Verwandte Themen:

- *Auswählen von Kategorien für einen Bericht*, Seite 108
- *Auswählen von Protokollen für einen Bericht*, Seite 109
- *Auswählen von Aktionen für einen Bericht*, Seite 110
- *Festlegen von Berichtsoptionen*, Seite 111
- *Bestätigung der Berichtsfilterdefinition*, Seite 113

Auf der Registerkarte **Clients** der Seite "Präsentationsberichte" > "Berichtsfilter" können Sie steuern, welche Clients in den Bericht einbezogen werden. Sie können nur einen Clienttyp pro Bericht auswählen. Für denselben Bericht können Sie z. B. nicht Benutzer und gleichzeitig Gruppen auswählen.

Wenn in der Berichtsdefinition ein bestimmter Clienttyp festgelegt ist, können Sie Clients von diesem Typ oder Clients, die eine größere Gruppe darstellen, auswählen. Wenn Sie z. B. einen Filter für einen Bericht basierend auf "Wichtigste gesperrte Gruppen nach Anforderungen" definieren, können Sie Gruppen, Domänen oder Organisationseinheiten, jedoch keine individuellen Benutzer für den Bericht auswählen.

Wenn Sie einen Bericht über alle relevanten Clients ausführen möchten, müssen Sie auf dieser Registerkarte keine Auswahl treffen.

1. Wählen Sie einen Clienttypen aus der Dropdown-Liste aus.
2. Wählen Sie die maximale Anzahl Suchergebnisse in der Liste **Suche einschränken** aus.

   Je nach Datenverkehr in Ihrem Unternehmen sind möglicherweise eine große Anzahl Benutzer, Gruppen oder Domänen in der Protokolldatenbank enthalten. Diese Option regelt die Länge der Ergebnisliste und den Zeitraum, der für die Anzeige der Suchergebnisse erforderlich ist.
3. Geben Sie einen oder mehrere Zeichen ein, nach denen gesucht werden soll, und klicken sie anschließend auf **Suchen**.

   Verwenden Sie den Stern (*) als Platzhalterzeichen für fehlende Zeichen. So kann z. B. A*a die Ergebnisse Andrea, Anna, Annika, Anna-Lena, Alina usw. liefern.

   Definieren Sie die Zeichenfolge möglichst präzise, um sicherzustellen, dass alle gewünschten Ergebnisse in der für die eingeschränkte Suche angegebenen Höchstanzahl enthalten sind.
4. Markieren Sie einen oder mehrere Einträge in der Ergebnisliste, und klicken Sie auf die Schaltfläche mit dem nach rechts weisenden Pfeil (>), um Sie in die Liste **Ausgewählte Objekte** zu verschieben.
5. Wiederholen Sie sofern erforderlich die Schritte 2 bis 4, um weitere Suchaufträge zu starten und weitere Clients in die Liste "Ausgewählte Objekte" zu verschieben.
6. Nachdem Sie alle gewünschten Clients ausgewählt haben, klicken Sie auf **Weiter**, um die Registerkarte "Kategorien" zu öffnen. Siehe *Auswählen von Kategorien für einen Bericht*, Seite 108.

Auswählen von Kategorien für einen Bericht

Verwandte Themen:

- *Auswählen von Clients für einen Bericht*, Seite 107
- *Auswählen von Protokollen für einen Bericht*, Seite 109
- *Auswählen von Aktionen für einen Bericht*, Seite 110
- *Festlegen von Berichtsoptionen*, Seite 111
- *Bestätigung der Berichtsfilterdefinition*, Seite 113

Die Registerkarte **Kategorien** der Seite "Präsentationsbericht" > "Berichtsfilter" ermöglicht das Steuern der im Bericht enthaltenen Informationen auf der Basis von Kategorien oder Risikoklassen. Siehe *Risikoklassen*, Seite 43.

Wenn Sie einen Bericht über alle relevanten Kategorien oder Risikoklassen ausführen möchten, müssen Sie auf dieser Registerkarte keine Auswahl treffen.

1. Wählen Sie eine Klassifikation aus: **Kategorie** oder **Risikoklasse**.

   Erweitern Sie eine übergeordnete Kategorie, um ihre Unterkategorien anzuzeigen. Erweitern Sie eine Risikoklasse, um eine Liste der Kategorien anzuzeigen, die dieser Risikoklasse aktuell zugewiesen sind.

   Wenn sich der zugewiesene Bericht auf eine bestimmte Risikoklasse bezieht, stehen nur die entsprechende Risikoklasse und die Kategorien, die sie repräsentiert, zur Auswahl zur Verfügung.

   > **Hinweis**
   > Wenn Sie eine Gruppe mit Kategorien der im Bericht genannten Risikoklasse auswählen, sollten Sie auch den Berichttitel entsprechend anpassen.

2. Aktivieren Sie das Kontrollkästchen jeder Kategorie oder Risikoklasse, für die ein Bericht erstellt werden soll.

   Verwenden Sie die Schaltflächen **Alles auswählen** und **Auswahl aufheben** unter der Liste, um die Anzahl der erforderlichen Einzelauswahl von Elementen zu minimieren.

3. Klicken Sie auf die Schaltfläche mit dem nach rechts weisenden Pfeil (>), um Ihre Auswahl in die Liste **Ausgewählte Objekte** zu verschieben.

   Wenn Sie eine Risikoklasse markieren, werden durch Klicken der Schaltfläche mit dem nach rechts weisenden Pfeil alle damit verbundenen Kategorien in die Liste "Ausgewählte Objekte" verschoben.

4. Nachdem Sie alle gewünschten Elemente ausgewählt haben, klicken Sie auf **Weiter**, um die Registerkarte "Protokolle" zu öffnen. Siehe *Auswählen von Protokollen für einen Bericht*, Seite 109.

Auswählen von Protokollen für einen Bericht

Verwandte Themen:

- *Auswählen von Clients für einen Bericht*, Seite 107
- *Auswählen von Kategorien für einen Bericht*, Seite 108
- *Auswählen von Aktionen für einen Bericht*, Seite 110
- *Festlegen von Berichtsoptionen*, Seite 111
- *Bestätigung der Berichtsfilterdefinition*, Seite 113

Auf der Registerkarte **Protokolle** der Seite "Präsentationsberichte" > "Berichtsfilter" können Sie steuern, welche Protokolle in den Bericht einbezogen werden.

Wenn Sie einen Bericht über alle relevanten Protokolle ausführen möchten, müssen Sie auf dieser Registerkarte keine Auswahl treffen.

1. Erweitern und reduzieren Sie die Protokollgruppen mit dem Symbol neben dem Gruppennamen.
2. Aktivieren Sie das Kontrollkästchen jedes Protokolls, für das der Bericht ausgeführt werden soll.

   Verwenden Sie die Schaltflächen **Alles auswählen** und **Auswahl aufheben** unter der Liste, um die Anzahl der erforderlichen Einzelauswahl von Elementen zu minimieren.
3. Klicken Sie auf die Schaltfläche mit dem nach rechts weisenden Pfeil (>), um Ihre Auswahl in die Liste **Ausgewählte Objekte** zu verschieben.
4. Nachdem Sie alle gewünschten Elemente ausgewählt haben, klicken Sie auf **Weiter**, um die Registerkarte "Aktionen" zu öffnen. Siehe *Auswählen von Aktionen für einen Bericht*, Seite 110.

Auswählen von Aktionen für einen Bericht

Verwandte Themen:

- *Auswählen von Clients für einen Bericht*, Seite 107
- *Auswählen von Kategorien für einen Bericht*, Seite 108
- *Auswählen von Protokollen für einen Bericht*, Seite 109
- *Festlegen von Berichtsoptionen*, Seite 111
- *Bestätigung der Berichtsfilterdefinition*, Seite 113

Mit der Registerkarte **Aktionen** der Seite "Präsentationsberichte" > "Berichtsfilter" können Sie steuern, welche konkreten Filteraktionen, wie die Zulassung durch eingeschränkte Zugriffsfilter oder die Sperrung durch die Quote, in den Bericht übernommen werden. Wenn im Bericht ein bestimmter Aktionstyp festgelegt wurde, wie z. B. "Gesperrt", können Sie für den Bericht nur Aktionen von diesem Typ auswählen.

Wenn Sie einen Bericht über alle relevanten Aktionen ausführen möchten, müssen Sie auf dieser Registerkarte keine Auswahl treffen.

1. Erweitern und reduzieren Sie die Aktionsgruppen mit dem Symbol neben dem Gruppennamen.
2. Aktivieren Sie das Kontrollkästchen jeder Aktion, für die der Bericht ausgeführt werden soll.

   Verwenden Sie die Schaltflächen **Alles auswählen** und **Auswahl aufheben** unter der Liste, um nicht jedes Element einzeln auswählen zu müssen.
3. Klicken Sie auf die Schaltfläche mit dem nach rechts weisenden Pfeil (>), um Ihre Auswahl in die Liste **Ausgewählte Objekte** zu verschieben.

4. Nachdem Sie alle gewünschten Elemente ausgewählt haben, klicken Sie auf **Weiter**, um die Registerkarte "Optionen" zu öffnen. Siehe *Festlegen von Berichtsoptionen*, Seite 111.

Festlegen von Berichtsoptionen

Verwandte Themen:

- *Anpassen des Berichtslogos*, Seite 112
- *Auswählen von Clients für einen Bericht*, Seite 107
- *Auswählen von Kategorien für einen Bericht*, Seite 108
- *Auswählen von Protokollen für einen Bericht*, Seite 109
- *Auswählen von Aktionen für einen Bericht*, Seite 110
- *Festlegen von Berichtsoptionen*, Seite 111
- *Bestätigung der Berichtsfilterdefinition*, Seite 113

Verwenden Sie die Registerkarte **Optionen** der Seite "Präsentationsberichte" > "Berichtsfilter bearbeiten", um verschiedene Aspekte des Berichts zu konfigurieren.

1. Ändern Sie die Einstellungen von **Name des Berichtskatalogs** dahingehend, dass der Name des Berichtskatalogs im Berichtskatalog angezeigt wird. Der Name kann bis zu 85 Zeichen enthalten.

   Dieser Name wird nicht im eigentlichen Bericht angezeigt. Er wird nur im Berichtskatalog zur Identifikation der besonderen Kombination von Berichtsformat und -filter verwendet.
2. Ändern Sie den **Berichtstitel**, der auf dem Bericht angezeigt wird. Der Titel kann bis zu 85 Zeichen enthalten.
3. Ändern Sie die **Beschreibung**, die im Berichtskatalog angezeigt wird. Die Beschreibung kann bis zu 336 Zeichen enthalten.

   Die Beschreibung sollte bei der Kennzeichnung dieser besonderen Kombination von Berichtsformat und -filter im Berichtskatalog unterstützen.
4. Wählen Sie ein Logo, das neben dem Bericht angezeigt werden soll.

   Es werden alle unterstützten Bilddateien im dafür vorgesehenen Verzeichnis aufgelistet. Siehe *Anpassen des Berichtslogos*, Seite 112.
5. Aktivieren Sie das Kontrollkästchen **Als Favorit speichern**, wenn der Bericht als Favorit definiert werden soll.

   Im Berichtskatalog werden Favoriten mit einem Sternsymbol gekennzeichnet. Sie können auf der Seite "Berichtskatalog" die Option **Nur Favoriten anzeigen** auswählen, um die Anzahl angezeigter Berichte zu reduzieren und schneller zu einem bestimmten Bericht zu navigieren.
6. Aktivieren Sie das Kontrollkästchen **Nur Wichtigste anzeigen**, und geben Sie anschließend eine Zahl von 1 bis 20 ein, um die Anzahl wiedergegebener Elemente einzuschränken.

Diese Option steht nur zur Verfügung, wenn der ausgewählte Bericht als "Bericht für ‚Wichtigste N'" formatiert und für die Anzeige einer eingeschränkten Anzahl Elemente konfiguriert wurde. Das eingeschränkte Element hängt vom Bericht ab. Bei einem Bericht "Wichtigste besuchte Kategorien" bestimmt dieser Eintrag z. B., wie viele Kategorien im Bericht enthalten sind.

7. Nachdem Sie alle Eingaben vorgenommen und gewünschten Elemente ausgewählt haben, klicken Sie auf **Weiter**, um die Registerkarte "Bestätigen" zu öffnen. Siehe *Bestätigung der Berichtsfilterdefinition*, Seite 113.

Anpassen des Berichtslogos

Bei vordefinierten Präsentationsberichten wird in der oberen linken Ecke das Websense-Logo angezeigt. Wenn Sie einen vordefinierten Bericht kopieren und seinen Berichtsfilter definieren, können Sie ein anderes Logo auswählen.

1. Erstellen Sie eine Bilddatei in einem der folgenden Formate:

   - BMP
   - GIF
   - JFIF
   - JPE
   - JPG
   - JPEG
   - PNG
   - TTF

2. Der Dateiname des Bildes darf 25 Zeichen ohne Dateierweiterung enthalten.
3. Speichern Sie die Bilddatei im folgenden Verzeichnis:

   `<Installationspfad>\Manager\ReportingTemplates\images`

   Der Standardinstallationspfad lautet C:\Program Files\Websense.

Alle unterstützten Bilddateien in diesem Verzeichnis werden automatisch in der Dropdown-Liste angezeigt auf der Registerkarte "Optionen" der Seite "Berichtsfilter bearbeiten" angezeigt. Die Größe des Bildes wird automatisch auf die für das Logo bereitgestellte Feldgröße angepasst. (Siehe *Festlegen von Berichtsoptionen*, Seite 111.)

Hinweis

Entfernen Sie aus diesem Verzeichnis keine Bilder, die in Berichtsfiltern aktiv sind. Wenn die angegebene Logodatei fehlt, kann der Bericht nicht generiert werden.

Bestätigung der Berichtsfilterdefinition

Verwandte Themen:

- *Auswählen von Clients für einen Bericht*, Seite 107
- *Auswählen von Kategorien für einen Bericht*, Seite 108
- *Auswählen von Protokollen für einen Bericht*, Seite 109
- *Auswählen von Aktionen für einen Bericht*, Seite 110
- *Festlegen von Berichtsoptionen*, Seite 111

Die Registerkarte **Bestätigen** der Seite "Präsentationsbericht" > "Berichtsfilter" enthält den Namen und die Beschreibung, die im Berichtkatalog angezeigt werden, und ermöglicht eine Auswahl der weiteren Vorgehensweise.

1. Prüfen Sie die Angaben unter **Name** und **Beschreibung**.

   Wenn Änderungen erforderlich sind, klicken Sie auf **Zurück**, um zur Registerkarte "Optionen" zurückzukehren, auf der Sie die entsprechenden Änderungen vornehmen können. (Siehe *Festlegen von Berichtsoptionen*, Seite 111.)
2. Geben Sie an, wie Sie fortfahren möchten:

Option	Beschreibung
Speichern	Speichert den Berichtsfilter und kehrt zum Berichtskatalog zurück. Siehe *Präsentationsberichte*, Seite 102.
Speichern und ausführen	Speichert den Berichtsfilter und öffnet die Seite "Bericht ausführen". Siehe *Generieren von Präsentationsberichten*, Seite 114.
Speichern und planen	Speichert den Berichtsfilter und öffnet die Seite "Bericht planen". Siehe *Planen von Präsentationsberichten*, Seite 116.

3. Klicken Sie auf **Fertig stellen**, um die in Schritt 2 vorgenommene Auswahl zu übernehmen.

Arbeiten mit Favoriten

Verwandte Themen:

- *Präsentationsberichte*, Seite 102
- *Generieren von Präsentationsberichten*, Seite 114
- *Planen von Präsentationsberichten*, Seite 116

Sie können jeden beliebigen Präsentationsbericht, ob vordefiniert oder benutzerdefiniert, als Favoriten kennzeichnen. Verwenden Sie diese Option, um Berichte zu kennzeichnen, die Sie häufig generieren und schnell im Berichtskatalog finden möchten.

1. Markieren Sie auf der Seite **Präsentationsberichte** einen Bericht, den Sie häufig generieren oder schnell finden möchten.
2. Klicken Sie auf **Favorit**.

   In der Liste wird neben den als Favorit definierten Berichtsnamen ein Sternsymbol angezeigt, wodurch Sie diese schnell aufzufinden sind, wenn alle Berichte angezeigt werden.
3. Aktivieren Sie über dem Berichtskatalog das Kontrollkästchen **Nur Favoriten anzeigen**, um die Liste auf die als Favorit definierten Berichte zu reduzieren. Deaktivieren Sie dieses Kontrollkästchen, um die vollständige Berichtsliste wiederherzustellen.

Wenn sich Ihre Bedürfnisse ändern und ein als Favorit definierter Bericht nicht mehr so häufig verwendet wird wie zuvor, können Sie die entsprechende Kennzeichnung entfernen.

1. Markieren Sie einen Bericht, der das Sternsymbol für Favoriten enthält.
2. Klicken Sie auf **Favorit**.

   Das Sternsymbol wird von diesem Berichtsnamen im Berichtskatalog entfernt. Der Bericht wird jetzt nicht mehr in der Liste angezeigt, die beim Wählen von **Nur Favoriten anzeigen** angezeigt wird.

Generieren von Präsentationsberichten

Verwandte Themen:

- *Präsentationsberichte*, Seite 102
- *Planen von Präsentationsberichten*, Seite 116

Das Generieren eines einzelnen Berichts umfasst die im Folgenden beschriebenen Schritte.

> **Hinweis**
>
> Stellen Sie vor dem Generieren eines Berichts im PDF-Format sicher, dass Adobe Reader Version 7.0 (oder höher) auf dem Computer installiert ist, von dem auf Websense Manager zugegriffen wird.
>
> Stellen Sie vor dem Generieren eines Berichts im XLS-Format sicher, dass Microsoft Excel 2003 (oder höher) auf dem Computer installiert ist, von dem auf Websense Manager zugegriffen wird.
>
> Wenn die entsprechende Software nicht installiert ist, haben Sie die Möglichkeit, die Datei zu speichern.

Sie können auch Jobs mit einem oder mehreren Berichten erstellen und planen, dass diese einmalig oder in einer wiederkehrenden Zeitfolge ausgeführt werden sollen (siehe *Planen von Präsentationsberichten*, Seite 116).

1. Markieren Sie auf der Seite **Präsentationsberichte** einen Bericht im Verzeichnisbaum "Berichtskatalog", und klicken Sie anschließend auf **Ausführen**.
2. Wählen Sie das **Startdatum** und das **Enddatum** für die Berichtsdaten.
3. Wählen Sie ein **Ausgabeformat** für den Bericht.

Format	Beschreibung
PDF	Portable Document Format. PDF-Dateien werden im Adobe Reader angezeigt.
HTML	HyperText Markup Language. HTML-Dateien können direkt in den Browsern Internet Explorer oder Firefox angezeigt werden.
XLS	Excel-Tabelle. XLS-Dateien werden in Microsoft Excel angezeigt.

4. Wenn Sie einen Bericht als "**Wichtigste N**" ausgewählt haben, wählen Sie die Anzahl der Elemente, für die der Bericht erstellt wird.
5. Klicken Sie auf **Ausführen**.

   HTML-Berichte werden im Inhaltsfenster angezeigt. Wenn Sie das Ausgabeformat PDF oder XLS gewählt haben, können Sie den Bericht entweder in einem separaten Fenster anzeigen oder auf der Festplatte speichern.
6. Wenn Sie einen Bericht drucken möchten, verwenden Sie die Druckfunktion des Programms, mit dem der Bericht angezeigt wird.

   Beste Druckergebnisse erzielen Sie, wenn Sie eine PDF- oder XLS-Datei für den Druck generieren. Verwenden Sie dann die Druckoptionen in Adobe Reader oder Microsoft Excel.

Sie können einen Bericht speichern, der im PDF- oder XLS-Format ausgegeben wurde, indem Sie die Speicherfunktion in Adobe Reader oder Microsoft Excel verwenden.

Planen von Präsentationsberichten

Verwandte Themen:

- *Präsentationsberichte*, Seite 102
- *Generieren von Präsentationsberichten*, Seite 114
- *Anzeigen der Liste der geplanten Jobs*, Seite 121
- *Kopieren eines Präsentationsberichts*, Seite 105

Sie können Präsentationsberichte bei Bedarf ausführen oder auf der Seite **Präsentationsberichte > Scheduler** Jobs erstellen, die einen Zeitplan für das Ausführen von einem oder mehreren Berichten definieren.

Die durch geplante Jobs generierten Berichte werden an einen oder mehrere Empfänger per E-Mail gesendet. Berücksichtigen Sie bei der Erstellung geplanter Jobs, dass Ihr E-Mail-Server die Größe und Menge der angehängten Berichtsdateien verarbeiten können muss.

So greifen Sie auf den Scheduler zu:

- Klicken Sie im oberen Bereich der Seite "Präsentationsberichte" über dem Berichtskatalog auf die Schaltfläche **Scheduler**.
- Wenn Sie einen Berichtsfilter zum Bericht hinzufügen oder bearbeiten, wählen Sie auf der Registerkarte "Bestätigen" die Option **Speichern und planen**, und klicken Sie anschließend auf **Fertig stellen**. (Siehe *Kopieren eines Präsentationsberichts*, Seite 105.)
- Klicken Sie auf der Seite "Warteschlange für Jobs" auf den Link eines Jobnamens, um den Job zu bearbeiten.
- Klicken Sie auf der Seite "Warteschlange für Jobs" auf **Hinzufügen**, um einen neuen Job zu erstellen.

Die Seite "Scheduler" enthält mehrere Registerkarten für die Auswahl der Berichte, die ausgeführt werden, und des Zeitplans für deren Ausführung. Detaillierte Anweisungen finden Sie unter:

- *Festlegen des Zeitplans*, Seite 117
- *Auswählen zu planender Berichte*, Seite 118
- *Auswählen von Ausgabeoptionen*, Seite 120
- *Festlegen des Datumsbereichs*, Seite 119
- *Auswählen von Ausgabeoptionen*, Seite 120

Nach dem Erstellen von Jobs können Sie eine Liste der Jobs anzeigen, in der ihr Status sowie andere nützliche Informationen angezeigt werden. Siehe *Anzeigen der Liste der geplanten Jobs*, Seite 121.

Festlegen des Zeitplans

Verwandte Themen:

- *Planen von Präsentationsberichten*, Seite 116
- *Auswählen zu planender Berichte*, Seite 118
- *Auswählen von Ausgabeoptionen*, Seite 120
- *Festlegen des Datumsbereichs*, Seite 119

Definieren Sie auf der Seite "Präsentationsberichte" > "Scheduler" auf der Registerkarte **Schedule** einen Berichterstellungsjob, der einmal oder in einer wiederkehrenden Zeitfolge ausgeführt wird.

> **Hinweis**
> Es wird empfohlen, Berichterstellungsjobs für verschiedene Tage oder verschiedene Uhrzeiten zu planen, um eine Überlastung der Protokolldatenbank und eine herabgesetzte Leistung der Protokollierung und interaktiven Berichterstellung zu vermeiden.

1. Geben Sie unter **Jobname** einen Jobnamen an, der diesen geplanten Job eindeutig identifiziert.
2. Wählen Sie ein **Wiederholungsmuster** und **Wiederholungsoptionen** für den Job aus. Die jeweils verfügbaren Optionen hängen vom ausgewählten Muster ab.

Muster	Optionen
Nur einmal ausführen	Geben Sie das exakte Datum an, an dem der Job ausgeführt werden soll, oder klicken Sie auf das Symbol, um das Datum im Kalender auszuwählen.
Täglich wiederholen	Keine zusätzlichen Wiederholungsoptionen verfügbar.
Wöchentlich wiederholen	Aktivieren Sie die Kontrollkästchen der Wochentage, an denen der Job ausgeführt wird.
Monatlich wiederholen	Geben Sie die Daten des Monats an, in dem der Job ausgeführt werden soll. Die Daten müssen als Zahl zwischen 1 und 31 angegeben und durch Kommas getrennt werden (1,10,20). Wenn Sie den Job in jedem Monat an aufeinander folgenden Daten ausführen möchten, geben Sie ein Start- und ein Enddatum getrennt durch einen Bindestrich ein (3-5).

3. Legen Sie unter **Uhrzeit planen** die Startzeit für das Ausführen des Jobs fest.

Der Job wird entsprechend der Systemzeit des Computers gestartet, auf dem Websense Manager ausgeführt wird.

> **Hinweis**
> Wenn das Generieren der geplanten Berichte heute beginnen soll, wählen Sie einen Zeitpunkt, der spät genug ist, dass Sie die Jobdefinition vor der Startzeit vervollständigen können.

4. Wählen Sie unter **Intervall planen** ein Startdatum für den Job und eine Option für das Beenden des Jobs aus.

Option	Beschreibung
Unbefristet	Der Job wird für einen unendlichen Zeitraum entsprechend des erstellten Zeitplans ausgeführt. Das Beenden des Jobs kann nur durch Bearbeiten oder Löschen des Jobs erreicht werden. Siehe *Anzeigen der Liste der geplanten Jobs*, Seite 121.
Beenden nach	Wählen Sie die Häufigkeit der Ausführung des Jobs. Nach der angegebenen Anzahl Ausführungen wird der Job nicht erneut ausgeführt, verbleibt jedoch in der Warteschlange für Jobs, bis Sie ihn löschen. Siehe *Anzeigen der Liste der geplanten Jobs*, Seite 121.
Beenden am	Legt das Enddatum der Ausführung des Jobs fest. Er wird an oder nach diesem Datum nicht erneut ausgeführt.

5. Klicken Sie auf **Weiter**, um die Registerkarte "Berichte" zu öffnen. Siehe *Auswählen zu planender Berichte*, Seite 118.

Auswählen zu planender Berichte

Verwandte Themen:

- *Planen von Präsentationsberichten*, Seite 116
- *Festlegen des Zeitplans*, Seite 117
- *Auswählen von Ausgabeoptionen*, Seite 120
- *Festlegen des Datumsbereichs*, Seite 119

Verwenden Sie die Registerkarte **Bericht auswählen** der Seite "Präsentationsberichte" > "Scheduler", um Berichte für den Job auszuwählen.

1. Markieren Sie einen Bericht für diesen Job im Verzeichnisbaum "Berichtskatalog".
2. Klicken Sie auf die Schaltfläche mit dem nach rechts weisenden Pfeil (>), um den Bericht in die Liste **Ausgewählte Objekte** zu verschieben.

3. Wiederholen Sie die Schritte 1 und 2, bis alle Berichte für diesen Job in der Liste **Ausgewählte Objekte** angezeigt werden.
4. Klicken Sie auf **Weiter**, um die Registerkarte "Datumsbereich" zu öffnen. Siehe *Festlegen des Datumsbereichs*, Seite 119.

Festlegen des Datumsbereichs

Verwandte Themen:

- *Planen von Präsentationsberichten*, Seite 116
- *Festlegen des Zeitplans*, Seite 117
- *Auswählen zu planender Berichte*, Seite 118
- *Auswählen von Ausgabeoptionen*, Seite 120

Verwenden Sie die Registerkarte **Datumsbereich** der Seite "Präsentationsberichte" > "Scheduler", um den Datumsbereich für den Job auszuwählen. Welche Optionen verfügbar sind, ist von Ihrer Auswahl auf der Seite **Datumsbereich** abhängig.

Datumsbereich	Beschreibung
Alle Daten	Berichte enthalten alle Daten, die in der Protokolldatenbank zur Verfügung stehen. Es sind keine weiteren Einträge erforderlich. Wenn diese Option für sich wiederholende Jobs verwendet wird, kann es dazu kommen, dass dieselben Informationen in mehreren Berichtsausführungen enthalten sind.
Bestimmte Daten	Wählen Sie die exakten Start- (**Von**) und Enddaten (**Bis**) für die Berichte in diesem Job. Diese Option eignet sich für Jobs, die nur einmal ausgeführt werden. Wenn diese Option für eine Ausführung in einer wiederkehrenden Zeitfolge gewählt wird, führt dies zu doppelten Berichten.
Relative Daten	Verwenden Sie die Dropdown-Listen für die Auswahl der Anzahl der zu berichtenden Zeiträume ("Diese/r", "Letzte/r", "Letzte 2" usw.) und des Typs des Zeitraums ("Tage", "Wochen" oder "Monate"). Der Job könnte z. B. "Letzte 2" "Wochen" oder "Diese/r" "Monat" berücksichtigen. "Woche" stellt eine Kalenderwoche von Sonntag bis Samstag dar. "Monat" stellt einen Kalendermonat dar. Beispiele: "Diese/r" "Woche" erzeugt einen Bericht von Sonntag bis heute, "Diese/r" "Monat" erzeugt einen Bericht vom Ersten des Monats bis heute, "Letzte/r" "Woche" erzeugt einen Bericht für den vergangenen Sonntag bis Samstag usw. Diese Option eignet sich für Jobs, die in wiederkehrender Zeitfolge ausgeführt werden. Sie können festlegen, welche Datenmenge in jedem Bericht enthalten ist, und die Duplizierung von Daten in separaten Berichtsausführungen minimieren.

Nachdem Sie den Datumsbereich für den Job festgelegt haben, klicken Sie auf **Weiter**, um die Registerkarte "Ausgabe" zu öffnen. Siehe *Auswählen von Ausgabeoptionen*, Seite 120.

Auswählen von Ausgabeoptionen

Verwandte Themen:

- *Planen von Präsentationsberichten*, Seite 116
- *Festlegen des Zeitplans*, Seite 117
- *Auswählen zu planender Berichte*, Seite 118
- *Festlegen des Datumsbereichs*, Seite 119

Nachdem Sie die Berichte für einen Job ausgewählt haben, verwenden Sie die Registerkarte **Ausgabe**, um das Ausgabeformat und die Verteilungsoptionen auszuwählen.

1. Wählen Sie das Dateiformat für den fertiggestellten Bericht.

Format	Beschreibung
PDF	Portable Document Format. Auf den Computern der Empfänger muss Adobe Reader Version 7.0 (oder höher) installiert sein, um PDF-Berichte anzeigen zu können.
XLS	Excel-Tabelle. Auf den Computern der Empfänger muss Microsoft Excel 2003 (oder höher) installiert sein, um XLS-Berichte anzeigen zu können.

2. Geben Sie die E-Mail-Adressen ein, an die der Bericht weitergeleitet werden soll.

   Geben Sie jede Adresse in einer separaten Zeile ein.
3. Aktivieren Sie sofern erforderlich das Kontrollkästchen **Betreff und Textkörper der E-Mail anpassen**. Geben Sie anschließend den benutzerdefinierten Text für **Betreff** und **Text** der E-Mail ein, mit der die Berichte dieses Jobs gesendet werden.
4. Klicken Sie auf **Job speichern**, um die Jobdefinition zu speichern und zu implementieren und die Seite "Warteschlange für Jobs" anzuzeigen.
5. Prüfen Sie diesen und beliebige andere geplante Jobs. Siehe *Anzeigen der Liste der geplanten Jobs*, Seite 121.

Anzeigen der Liste der geplanten Jobs

Verwandte Themen:

- *Präsentationsberichte*, Seite 102
- *Planen von Präsentationsberichten*, Seite 116
- *Auswählen von Ausgabeoptionen*, Seite 120
- *Planen von Untersuchungsberichten*, Seite 145

Auf der Seite **Präsentationsberichte > Warteschlange für Jobs** werden die geplanten Jobs angezeigt, die für Präsentationsberichte erstellt wurden. Die Liste enthält den Status jedes Jobs sowie grundlegende Informationen über den Job, wie z. B. die Häufigkeit der Ausführung. Auf dieser Seite können Sie geplante Jobs hinzufügen und löschen, einen Job vorrübergehend aussetzen und vieles mehr.

(Informationen über das Prüfen geplanter Jobs für Untersuchungsberichte finden Sie unter *Verwalten geplanter Jobs für Untersuchungsberichte*, Seite 148.)

Die Liste enthält die folgenden Informationen zu den einzelnen Jobs.

Spalte	Beschreibung
Jobname	Der Name, der dem Job bei der Erstellung zugewiesen wurde.
Status	Folgende Status sind möglich: • AKTIVIERT kennzeichnet einen Job, der entsprechend eines festgelegten Wiederholungsmusters ausgeführt wird. • DEAKTIVIERT kennzeichnet einen Job, der inaktiv ist und nicht ausgeführt wird.
Wiederholungsintervall	Das für diesen Job festgelegte Wiederholungsmuster ("Nur einmal ausführen", "Täglich wiederholen", "Wöchentlich wiederholen", "Monatlich wiederholen").
Verlauf	Klicken Sie auf den Link **Details**, um die Seite "Verlauf von Jobs" für den ausgewählten Job anzuzeigen. Siehe *Anzeigen des Verlaufs von Jobs*, Seite 122.
Nächste geplante Ausführung	Datum und Uhrzeit der nächsten Ausführung.
Eigner	Der Benutzername des Administrators, der den Job geplant hat.

Verwenden Sie die Optionen auf der Seite, um die Jobs zu verwalten. Einige der Schaltflächen erfordern, dass Sie zunächst das Kontrollkästchen neben dem Namen des Jobs aktivieren, der enthalten sein soll.

Option	Beschreibung
Link eines Jobnamens	Öffnet die Seite "Scheduler", auf der Sie die Jobdefinition bearbeiten können. Siehe *Planen von Präsentationsberichten*, Seite 116.
Job hinzufügen	Öffnet die Seite "Scheduler", auf der Sie einen neuen Job definieren können. Siehe *Planen von Präsentationsberichten*, Seite 116.
Löschen	Löscht alle in der Liste ausgewählten Jobs aus der Warteschlange für Jobs. Nachdem ein Job gelöscht wurde, kann er nicht wiederhergestellt werden. Wenn Sie einen bestimmten Job vorübergehend anhalten möchten, verwenden Sie die Schaltfläche **Deaktivieren**.
Jetzt ausführen	Startet umgehend die Ausführung der in der Liste ausgewählten Jobs. Diese Ausführung findet zusätzlich zu den regulär geplanten Ausführungen statt.
Aktivieren	Aktiviert die in der Liste ausgewählten deaktivierten Jobs neu. Die Ausführung des Jobs beginnt entsprechend des festgelegten Zeitplans.
Deaktivieren	Hält die Ausführung in der Liste ausgewählter aktivierter Jobs an. Verwenden Sie diese Option, um Jobs anzuhalten, die Sie in der Zukunft möglicherweise erneut aktivieren möchten.

Anzeigen des Verlaufs von Jobs

Verwandte Themen:

- *Planen von Präsentationsberichten*, Seite 116
- *Anzeigen der Liste der geplanten Jobs*, Seite 121

Auf der Seite **Präsentationsberichte > Warteschlange für Jobs > Verlauf von Jobs** können Sie Informationen über die zuletzt stattgefundenen Versuche, den ausgewählten Job auszuführen, anzeigen. Die Seite enthält einen separaten Eintrag für jeden Bericht, der die folgenden Informationen enthält.

Spalte	Beschreibung
Name des Berichts	Der auf dem Bericht angegebene Titel.
Startdatum	Datum und Uhrzeit, zu der der Bericht gestartet wurde.
Enddatum	Datum und Uhrzeit, zu der der Bericht fertiggestellt wurde.

Spalte	Beschreibung
Status	Indikator, ob der Bericht erfolgreich ausgeführt wurde oder fehlgeschlagen ist.
Nachricht	Informationen zum Job, wie z. B. ob der Bericht erfolgreich per E-Mail gesendet wurde.

Untersuchungsberichte

Verwandte Themen:

- *Zusammenfassende Berichte*, Seite 125
- *Zusammenfassende Berichte mit mehreren Ebenen*, Seite 130
- *Flexible Detailberichte*, Seite 131
- *Detailberichte zu Benutzeraktivitäten*, Seite 136
- *Standardberichte*, Seite 141
- *Als Favoriten gekennzeichnete Untersuchungsberichte*, Seite 143
- *Planen von Untersuchungsberichten*, Seite 145
- *Berichte über Sonderfälle*, Seite 149
- *Ausgabe in Datei*, Seite 150
- *Standardeinstellungen für Datenbankverbindung und Berichte*, Seite 355

Verwenden Sie die Seite **Berichterstellung > Untersuchungsberichte**, um die Filterung der Internetaktivitäten interaktiv zu analysieren.

In der Ausgangskonfiguration enthält die Hauptseite für Untersuchungsberichte einen zusammenfassenden Bericht der Aktivitäten der einzelnen Risikoklassen. Arbeiten Sie in der Ansicht des zusammenfassenden Berichts, indem Sie auf die verfügbaren Links und Elemente klicken, um gewünschte Bereiche zu durchsuchen und einen allgemeinen Einblick in die Internetnutzung Ihres Unternehmens zu erhalten. Siehe *Zusammenfassende Berichte*, Seite 125.

Zusammenfassende Berichte mit mehreren Ebenen (siehe *Zusammenfassende Berichte mit mehreren Ebenen*, Seite 130) und Berichte mit flexiblen Details (siehe *Flexible Detailberichte*, Seite 131) ermöglichen die Analyse der Informationen aus verschiedenen Perspektiven.

Weitere Berichtsansichten und Funktionen für Untersuchungsberichte erreichen Sie über die Links im oberen Bereich der Seite. Die untenstehende Tabelle enthält eine

Liste der Links und der damit verbundenen Funktionen. (Nicht alle Links sind auf allen Seiten verfügbar.)

Option	Aktion
Benutzer nach Tag/ Monat	Zeigt ein Dialogfeld an, in dem Sie einen Bericht über die Aktivitäten eines bestimmten Benutzers definieren können, der entweder den Zeitraum eines Tages oder eines Monats wiedergibt. Weitere Informationen finden Sie unter *Detailberichte zu Benutzeraktivitäten*, Seite 136.
Standardberichte	Zeigt eine Liste vordefinierter Berichte an, über die Sie schnell eine bestimmte Kombination von Daten ablesen können. Siehe *Standardberichte*, Seite 141.
Als Favoriten definierte Berichte	Ermöglicht das Speichern des aktuellen Berichts als Favorit, und enthält eine Liste der vorhandenen Favoriten, die Sie generieren oder planen können. Siehe *Als Favoriten gekennzeichnete Untersuchungsberichte*, Seite 143.
Warteschlange für Jobs	Zeigt eine Liste der geplanten Berichterstellungsjobs für Untersuchungsberichte an. Siehe *Planen von Untersuchungsberichten*, Seite 145.
Sonderfälle anzeigen	Zeigt Berichte über Internetnutzung an, die erheblich vom Durchschnitt abweicht. Siehe *Berichte über Sonderfälle*, Seite 149.
Optionen	Zeigt eine Seite für die Auswahl einer anderen Protokolldatenbank an. Auf der Seite Optionen können Sie außerdem bestimmte Berichterstellungsfunktionen anpassen, wie die ursprünglich auf zusammenfassenden Berichten berücksichtigte Zeitdauer und die Standardspalten für Detailberichte. Siehe *Standardeinstellungen für Datenbankverbindung und Berichte*, Seite 355.
	Klicken Sie auf diese Schaltfläche rechts neben den Feldern der Suchfunktion, um den aktuellen Bericht in eine Tabellenkalkulationsdatei zu exportieren, die mit Microsoft Excel kompatibel ist. Sie werden dazu aufgefordert, die Datei entweder zu öffnen oder zu speichern. Um die Datei öffnen zu können, muss Microsoft Excel 2003 (oder höher) installiert sein. Siehe *Ausgabe in Datei*, Seite 150.
	Klicken Sie auf diese Schaltfläche rechts neben den Feldern der Suchfunktion, um den aktuellen Bericht in eine PDF-Datei zu exportieren, die mit Adobe Reader kompatibel ist. Sie werden dazu aufgefordert, die Datei entweder zu öffnen oder zu speichern. Um die Datei öffnen zu können, muss Adobe Reader Version 7.0 (oder höher) installiert sein. Siehe *Ausgabe in Datei*, Seite 150.

Beachten Sie, dass die Berichterstellung auf die Informationen beschränkt ist, die in der Protokolldatenbank aufgezeichnet wurden. Wenn Sie die Protokollierung für Benutzernamen, IP-Adressen oder ausgewählte Kategorien deaktivieren (siehe *Konfigurieren von Filtering Service für die Protokollierung*, Seite 326), können diese Informationen nicht in den Bericht übernommen werden. Gleichermaßen sind

Anforderungen für Protokolle, deren Protokollierung Sie deaktiviert haben (siehe *Bearbeiten eines Protokollfilters*, Seite 56), nicht verfügbar. Wenn Berichte sowohl den Domänennamen (www.domaene.com) als auch den Pfad zu einer bestimmten Seite auf der Domäne (/produkte/produktA) enthalten sollen, muss die Protokollierung der vollständigen URL aktiviert sein (siehe *Konfigurieren der Protokollierung der vollständigen URL*, Seite 346).

Untersuchungsberichte in Websense werden durch den Prozessor und den verfügbaren Speicher des Computers, auf dem Websense Manager ausgeführt wird, sowie durch einige Netzwerkressourcen eingeschränkt. Bei großen Berichten kann das Generieren einige Zeit in Anspruch nehmen. Die Fortschrittsmeldung enthält eine Option für das Speichern des Berichts als Favoriten, sodass seine Ausführung zu einem separaten Zeitpunkt geplant werden kann. Siehe *Planen von Untersuchungsberichten*, Seite 145.

Zusammenfassende Berichte

Verwandte Themen:

- *Zusammenfassende Berichte mit mehreren Ebenen*, Seite 130
- *Flexible Detailberichte*, Seite 131
- *Detailberichte zu Benutzeraktivitäten*, Seite 136
- *Standardberichte*, Seite 141
- *Als Favoriten gekennzeichnete Untersuchungsberichte*, Seite 143
- *Planen von Untersuchungsberichten*, Seite 145
- *Berichte über Sonderfälle*, Seite 149
- *Ausgabe in Datei*, Seite 150

In ihrer Ausgangskonfiguration enthält die Seite "Untersuchungsberichte" einen zusammenfassenden Bericht der Nutzung aller Benutzer sortiert nach Risikoklassen, der die in der Protokolldatenbank verzeichnete Aktivität des aktuellen Tages wiedergibt. Die Maßeinheit dieses ersten Balkendiagramms ist Hits (Anzahl Anforderungen der Website). Informationen über die Konfiguration des Zeitraums für diesen in der Ausgangskonfiguration definierten zusammenfassenden Bericht finden Sie unter *Standardeinstellungen für Datenbankverbindung und Berichte*, Seite 355.

Sie können schnell die im Bericht enthaltenen Informationen ändern oder einen höheren Detaillierungsgrad anzeigen, indem Sie auf die verschiedenen Links und Optionen auf der Seite klicken.

1. Wählen Sie eine der folgenden Optionen in der Liste **Maßeinheit** aus.

Option	Beschreibung
Hits	Die Anzahl der Anforderungen dieser URL. Je nachdem, wie der Log Server konfiguriert wurde, kann es sich dabei um tatsächliche Hits, bei denen ein separater Eintrag für jedes einzelne Element einer angeforderten Website protokolliert wird, oder um Besuche handeln, bei denen die verschiedenen Elemente der Website in einem einzelnen Protokolleintrag kombiniert werden. Siehe *Konfigurieren von Log-Cachedateien*, Seite 333.
Bandbreite [KB]	Die Summe der Datenmenge der ursprünglichen Anforderung des Benutzers und der Antwort der Website in Kilobyte. Dies ist die Summe der Gesamtwerte unter "Gesendet" und "Empfangen". Beachten Sie, dass einige Integrationsprodukte diese Informationen nicht an die Websense-Software senden. Beispiele dafür sind Check Point FireWall-1 und Cisco PIX Firewall. Wenn das von Ihnen verwendete Integrationsprodukt diese Informationen nicht sendet und der Websense Network Agent installiert ist, aktivieren Sie die Option **HTTP-Anforderungen protokollieren** für die entsprechende Netzwerkschnittstellenkarte, um einen Bericht der Bandbreitendaten zu ermöglichen. Siehe *Konfigurieren der Einstellungen für die Netzwerkschnittstellenkarte (NIC)*, Seite 369.
Gesendet [KB]	Die Anzahl der Kilobyte, die im Rahmen der Internetanforderung gesendet wurden. Dies stellt die übermittelte Datenmenge dar, bei der es sich sowohl um eine einfache Anforderung einer URL als auch um eine bedeutendere Übertragung handeln kann, bei der sich der Benutzer z. B. für eine Website registriert.
Empfangen [KB]	Die Anzahl Kilobyte, die als Antwort auf eine Anforderung empfangen wurde. Dies beinhaltet sämtlichen Text sowie alle Grafiken und Skripte, die in der Website enthalten sind. Bei gesperrten Websites variiert die Anzahl Kilobyte je nach Software, die den Protokolleintrag erstellt. Wenn die Einträge von Websense Network Agent protokolliert werden, stellt die Anzahl empfangener Kilobytes einer gesperrten Website die Größe der Sperrseite von Websense dar. Wenn der Protokolleintrag von Websense Security Gateway erstellt wird, stellt die Anzahl Kilobyte empfangener Daten aufgrund des Scannings in Echtzeit die Größe der gescannten Seite dar. Weitere Informationen über das Scanning in Echtzeit finden Sie unter *Analysieren des Inhalts mit den Echtzeit-Optionen*, Seite 153. Wenn ein anderes Integrationsprodukt die Protokolleinträge erstellt, können die für eine gesperrte Website empfangenen Kilobytes Null (0) lauten, die Größe der Sperrseite wiedergeben oder einen von der angeforderten Website erhaltenen Wert darstellen.

Option	Beschreibung
Navigationsdauer	Ein Schätzwert der Anzeigedauer einer Website. Siehe *Was ist die "Navigationsdauer im Internet"?*, Seite 101.

2. Ändern Sie die primäre Gruppierung des Berichts, indem Sie über dem Bericht eine Option in der Liste **Internetnutzung nach** auswählen.

   Die verfügbaren Optionen variieren je nach Inhalt der Protokolldatenbank und bestimmten Netzwerkaspekten. Wenn z. B. nur eine Gruppe oder Domäne in der Protokolldatenbank vorhanden ist, stehen Gruppen und Domänen in dieser Liste nicht zur Auswahl. Gleichermaßen werden bei einer zu hohen Anzahl Benutzer (mehr als 5.000) oder Gruppen (mehr als 3.000) die entsprechenden Optionen nicht angezeigt. (Einige dieser Grenzwerte können konfiguriert werden. Siehe *Anzeige- und Ausgabeoptionen*, Seite 357.)

3. Klicken Sie auf einen Namen in der linken Spalte (oder auf den Pfeil neben dem Namen), um eine Liste der Optionen anzuzeigen, wie z. B. die Anzeige sortiert nach Benutzer, Domäne oder Aktion.

   Die aufgeführten Optionen ähneln denen unter "Internetnutzung nach" und können so angepasst werden, dass sie eine aussagekräftige Untermenge des aktuell angezeigten Inhalts darstellen.

   Hinweis

   In einigen Fällen werden Optionen wie "Benutzer" oder "Gruppe" in roter Schrift angezeigt. Dies weist darauf hin, dass die Auswahl dieser Option zu einem sehr langen Bericht führen kann, dessen Generierung einen längeren Zeitraum in Anspruch nehmen könnte. Erwägen Sie einen höheren Detaillierungsgrad, bevor Sie diese Option wählen.

4. Wählen Sie eine dieser Optionen, um einen neuen zusammenfassenden Bericht zu generieren, der die ausgewählten Informationen zum entsprechenden Eintrag enthält.

   Wenn Sie z. B. bei einem zusammenfassenden Bericht der Risikoklasse unter der Risikoklasse "Gesetzliche Haftung" auf "durch Benutzer" klicken, wird ein Bericht der Aktivitäten jedes Benutzers in der Risikoklasse "Gesetzliche Haftung" erstellt.

5. Klicken Sie auf einen neuen Eintrag in der linken Spalte, und wählen Sie anschließend eine Option aus, um nähere Details über dieses Element anzuzeigen.

6. Verwenden Sie die Pfeile neben der Spaltenüberschrift, um die Sortierreihenfolge des Berichts zu ändern.

7. Steuern Sie den zusammenfassenden Bericht mit den folgenden Optionen über dem Diagramm. Zeigen Sie anschließend die damit verbundenen Details an, indem Sie auf die Elemente des neuen Berichts klicken.

Option	Aktion
Berichtspfad (Benutzer > Tag)	Neben der Liste **Internetnutzung nach** wird ein Pfad angezeigt, der die Auswahl wiedergibt, mit der der aktuelle Bericht erstellt wurde. Klicken Sie auf einen beliebigen Link in dem Pfad, um zu dieser Ansicht der Daten zurückzukehren.
Anzeigen	Wählen Sie einen Zeitraum für den Bericht: "Einen Tag", "Eine Woche", "Einen Monat" oder "Alle". Der Bericht wird aktualisiert und enthält die Daten des ausgewählten Zeitraums. Verwenden Sie die danebenliegenden Pfeilschaltflächen, um schrittweise (ein Tag, eine Woche, ein Monat) durch die verfügbaren Daten zu navigieren. Wenn Sie die Auswahl ändern, werden die Felder **Anzeigen von** aktualisiert, um den angezeigten Zeitraum wiederzugeben. Im Feld **Anzeigen** wird statt eines Zeitraums "Benutzerdefiniert" angezeigt, wenn Sie ein bestimmtes Datum in den Feldern "Anzeigen von" oder im Dialogfeld "Favoriten" auswählen.
Anzeigen von... bis...	Die Daten in diesen Feldern werden automatisch aktualisiert, um den angezeigten Zeitraum wiederzugeben, wenn Sie Änderungen am Feld **Anzeigen** vornehmen. Geben Sie alternativ genaue Start- und Enddaten für die Berichte ein, oder klicken Sie auf das Kalendersymbol, um die gewünschten Daten auszuwählen. Klicken Sie auf die danebenliegende Pfeilschaltfläche, um den Bericht nach der Auswahl von Daten zu aktualisieren.
Kreisdiagramm/ Balkendiagramm	Klicken Sie bei aktiviertem Balkendiagramm auf **Kreisdiagramm**, um den aktuellen zusammenfassenden Bericht als Kreisdiagramm anzuzeigen. Klicken Sie auf die Beschriftung des Teilstücks, um dieselben Optionen anzuzeigen, die auch zur Verfügung stehen, wenn Sie auf einen Eintrag in der linken Spalte des Balkendiagramms klicken. Klicken Sie bei aktiviertem Kreisdiagramm auf **Balkendiagramm**, um den aktuellen zusammenfassenden Bericht als Balkendiagramm anzuzeigen.
Vollbildanzeige	Wählen Sie diese Option, um den aktuellen Untersuchungsbericht in einem separaten Fenster ohne das linke und rechte Navigationsfenster anzuzeigen.

Option	Aktion
Anonym/Namen	Klicken Sie auf **Anonym**, wenn in Berichten statt des Benutzernamens eine intern zugewiesene Benutzeridentifikationsnummer angezeigt werden soll. Wenn Namen ausgeblendet sind, klicken Sie auf **Namen**, um an diesen Positionen stattdessen Benutzernamen anzuzeigen. Unter bestimmten Bedingungen können Benutzernamen nicht angezeigt werden. Weitere Informationen finden Sie unter *Konfigurieren von Filtering Service für die Protokollierung*, Seite 326. Wenn Sie auf "Anonym" klicken, und anschließend zu einer anderen Ansicht der Daten wechseln, wie z. B. der Detailansicht oder der Anzeige von Sonderfällen, werden die Benutzernamen im neuen Bericht weiterhin ausgeblendet. Wenn Sie jedoch mit ausgeblendeten Namen zur Übersichtsansicht wechseln möchten, müssen Sie die Links im oberen Bereich des Berichts verwenden, und nicht den Verzeichnispfad im Banner. Wenn bestimmte Administratoren nie Zugriff auf Benutzernamen in Berichten haben dürfen, weisen Sie sie einer Rolle zu, deren Berechtigungen für die Berichterstellungsfunktion die Anzeige von Benutzernamen in Untersuchungsberichten und den Zugriff auf Präsentationsberichte unterbinden.
Suchen nach	Wählen Sie ein Berichtselement aus der Liste, und geben Sie anschließend den gesamten Wert oder Teile eines Werts für die Suche im danebenliegenden Textfeld ein. Klicken Sie auf die angeschlossene Pfeilschaltfläche, um die Suche zu starten und Ergebnisse anzuzeigen. Wenn Sie einen Teil einer IP-Adresse eingeben, wie z. B. 10.5., wird nach allen Subnetzen gesucht (in diesem Beispiel von 10.5.0.0 bis 10.5.255.255).

8. Fügen Sie eine Informationsuntermenge für alle oder ausgewählte Einträge in der linken Spalte ein, indem Sie einen zusammenfassenden Bericht mit mehreren Ebenen erstellen. Siehe *Zusammenfassende Berichte mit mehreren Ebenen*, Seite 130.
9. Erstellen Sie einen Tabellenbericht für ein bestimmtes Element in der linken Spalte, indem Sie auf die nebenstehende Zahl oder den Messbalken klicken. Dieser detaillierte Bericht kann auf Ihre Bedürfnisse angepasst werden. Siehe *Flexible Detailberichte*, Seite 131.

Zusammenfassende Berichte mit mehreren Ebenen

Verwandte Themen:

- *Untersuchungsberichte*, Seite 123
- *Zusammenfassende Berichte*, Seite 125
- *Flexible Detailberichte*, Seite 131
- *Detailberichte zu Benutzeraktivitäten*, Seite 136
- *Standardberichte*, Seite 141
- *Als Favoriten gekennzeichnete Untersuchungsberichte*, Seite 143
- *Planen von Untersuchungsberichten*, Seite 145
- *Berichte über Sonderfälle*, Seite 149
- *Ausgabe in Datei*, Seite 150

Zusammenfassende Berichte mit mehreren Ebenen enthalten eine zweite Informationsebene, mit der die angezeigten primären Informationen ergänzt werden. Wenn z. B. die primäre Anzeige Risikoklassen enthält, können Sie eine zweite Ebene definieren, um herauszufinden, welche Kategorien innerhalb der jeweiligen Risikoklasse am häufigsten verwendet wurde. Oder wenn der primäre Bericht Anforderungen für jede Kategorie enthält, können Sie z. B. die 5 wichtigsten Kategorien und die 10 Benutzer anzeigen, die in den Kategorien jeweils die meisten Anforderungen gestellt haben.

Verwenden Sie die Einstellungen direkt über dem zusammenfassenden Bericht, um einen zusammenfassenden Bericht mit mehreren Ebenen zu erstellen.

1. Wählen Sie in der Liste **Wichtigste** eine Zahl für die Anzahl der primären Einträge (linke Spalte), über die berichtet wird. Der resultierende Bericht enthält die primären Einträge mit den höchsten Werten. (Dabei werden die frühesten Daten angezeigt, wenn es sich bei dem primären Eintrag um "Tag" handelt.)

   Alternativ aktivieren Sie das Kontrollkästchen neben einzelnen Einträgen in der linken Spalte, um einen Bericht nur über diese Einträge zu erstellen. Das Feld **Wichtigste** enthält den Eintrag **Benutzerdefiniert**.
2. Wählen Sie in der Liste **nach** die sekundären Informationen aus, die im Bericht enthalten sein sollen.
3. Wählen Sie im Feld **Anzeige** die Anzahl der sekundären Ergebnisse, die für jeden primären Eintrag im Bericht enthalten sein sollen.
4. Klicken Sie auf **Ergebnisse anzeigen**, um den zusammenfassenden Bericht mit mehreren Ebenen zu generieren.

   Der zusammenfassende Bericht wird aktualisiert und zeigt nur die ausgewählte Anzahl primärer Einträge an. Unter den Balken der primären Einträge wird eine Liste sekundärer Einträge angezeigt.

5. Verwenden Sie die Pfeile neben der Spaltenüberschrift, um die Sortierreihenfolge des Berichts zu ändern.

Wenn Sie zu einem zusammenfassenden Bericht mit einer Ebene zurückkehren möchten, wählen Sie unter **Internetnutzung nach** eine andere Option. Klicken Sie alternativ auf einen der primären oder sekundären Einträge, und wählen Sie eine Option, mit der ein neuer Untersuchungsbericht dieser Informationen erstellt wird.

Flexible Detailberichte

Verwandte Themen:

- *Untersuchungsberichte*, Seite 123
- *Zusammenfassende Berichte*, Seite 125
- *Zusammenfassende Berichte mit mehreren Ebenen*, Seite 130
- *Als Favoriten gekennzeichnete Untersuchungsberichte*, Seite 143
- *Planen von Untersuchungsberichten*, Seite 145
- *Berichte über Sonderfälle*, Seite 149
- *Ausgabe in Datei*, Seite 150
- *Standardeinstellungen für Datenbankverbindung und Berichte*, Seite 355
- *Spalten für flexible Detailberichte*, Seite 134

Detailberichte bieten eine tabellarische Ansicht der Informationen in der Protokolldatenbank. Greifen Sie auf die Detailberichtansicht über die Hauptseite zu, wenn Sie einen zusammenfassenden Bericht angezeigt haben und dazu detailliertere Informationen benötigen.

Sie können von jeder Zeile eine Detailansicht anfordern. Wenn Sie jedoch einen Detailbericht basierend auf Hits anfordern, empfiehlt es sich, von einer Zeile zu starten, die weniger als 100.000 Hits enthält. Wenn eine Zeile über mehr als 100.000 Hits verfügt, wird der Wert für die Hits in roter Schrift angezeigt. Dies ist ein Warnhinweis, dass das Generieren eines Detailberichts einen längeren Zeitraum in Anspruch nehmen könnte.

Die Detailberichtansicht wird *flexibel* genannt, da Sie damit Ihren persönlichen Bericht konzipieren können. Sie können Spalten mit Informationen hinzufügen oder löschen und die Reihenfolge der angezeigten Spalten ändern. Die Information wird entsprechend der Reihenfolge der Spalten sortiert. Sie können sogar die Sortierreihenfolge innerhalb einer beliebigen Spalte von aufsteigend in absteigend (oder umgekehrt) ändern.

Untersuchungsberichte in Websense werden durch den Prozessor und den verfügbaren Speicher des Computers, auf dem Websense Manager ausgeführt wird, sowie durch einige Netzwerkressourcen eingeschränkt. Anforderungen für große Berichte können aufgrund einer Zeitüberschreitung abgebrochen werden. Wenn Sie einen langen

Bericht anfordern, werden Ihnen Optionen für das Generieren des Berichts ohne Zeitüberschreitung angeboten.

> **Wichtig**
>
> In Dropdown- oder Wertelisten können einige Optionen in roter Schrift angezeigt werden. Die rote Schrift weist darauf hin, dass die Auswahl dieser Option zu einem sehr großen Bericht führen kann. Es erweist sich in der Regel als effektiver, vor der Auswahl dieser Optionen einen höheren Detaillierungsgrad auszuwählen.

1. Generieren Sie einen zusammenfassenden Bericht oder Bericht mit mehreren Ebenen auf der Hauptseite der Untersuchungsberichte. (Siehe *Zusammenfassende Berichte*, Seite 125, oder *Zusammenfassende Berichte mit mehreren Ebenen*, Seite 130.)
2. Wählen Sie einen höheren Detaillierungsgrad der Ergebnisse, um sich auf die für Sie wichtigen Informationen zu konzentrieren.

   Wenn Sie einen Bericht über Hits generieren, empfiehlt es sich, einen höheren Detaillierungsgrad eines Eintrags zu wählen, der weniger als 100.000 Hits enthält, bevor Sie die Detailberichtansicht wählen.
3. Klicken Sie auf die Zahl oder den Balken in der Zeile, die Sie genauer betrachten möchten. Wenn Sie mehrere Zeilen in einem Bericht anzeigen möchten, aktivieren Sie das jeweilige Kontrollkästchen, bevor Sie auf die Zahl oder den Balken in der Zeile klicken.

   Ein Popup-Fenster informiert Sie über den Fortschritt, während der Detailbericht geladen wird.

   > **Hinweis**
   >
   > Wenn das Generieren des Berichts einen langen Zeitraum in Anspruch nimmt, sollten Sie ihn als Favorit speichern, indem Sie im Informationsfenster für den Ladevorgang auf den entsprechenden Link klicken und die Ausführung für einen späteren Zeitpunkt planen. Siehe *Als Favoriten gekennzeichnete Untersuchungsberichte*, Seite 143.

4. Prüfen Sie die Informationen im ursprünglichen Bericht.

   Die Standardspalten variieren je nachdem, ob Sie einen Bericht über Hits, die Bandbreite oder die Navigationsdauer generieren, und je nach getroffener Auswahl auf der Seite "Optionen". (Siehe *Standardeinstellungen für Datenbankverbindung und Berichte*, Seite 355.)
5. Klicken Sie im oberen Bereich der Seite auf **Bericht ändern**.

   Die Liste **Aktueller Bericht** im Dialogfeld "Bericht ändern" zeigt an, welche Spalten im aktuellen Detailbericht angezeigt werden.

6. Wählen Sie in den Listen **Verfügbaren Spalten** oder **Aktueller Bericht** einen Spaltennamen aus, und klicken Sie auf die Schaltfläche mit dem nach rechts (>) oder nach links weisenden Pfeil (<), um diese Spalte in die andere Liste zu verschieben.

   Sie können maximal 7 Spalten für den Bericht auswählen. Die Spalte mit der Maßeinheit (Hits, Bandbreite, Navigationsdauer) des ursprünglichen zusammenfassenden Berichts wird immer in der äußerst rechten Spalte angezeigt. Sie steht bei der Änderung des Berichts nicht als Auswahlmöglichkeit zur Verfügung.

   Eine Liste der verfügbaren Spalten sowie eine jeweiligen Beschreibung finden Sie unter *Spalten für flexible Detailberichte*, Seite 134.

7. Wählen Sie einen Spaltennamen in der Liste **Aktueller Bericht**, und verwenden Sie die Schaltflächen mit dem nach oben und nach unten weisenden Pfeil, um die Reihenfolge der Spalten zu verändern.

   Die Spalte ganz oben in der Liste "Aktueller Bericht" wird im Bericht links angeordnet.

8. Klicken Sie auf die Links **Zusammenfassung** oder **Detailliert** über dem Bericht, um zwischen den zwei Anzeigen umzuschalten.

Option	Beschreibung
Zusammenfassung	Sie müssen die Spalte "Uhrzeit" entfernen, um einen zusammenfassenden Bericht anzuzeigen. In zusammenfassenden Berichten werden alle Einträge, die über ein gemeinsames Element verfügen, in einem einzelnen Eintrag gruppiert. Das jeweilige Element variiert entsprechend der im Bericht enthaltenen Informationen. In der Regel stellt die Spalte äußerst rechts vor der Maßeinheit das zusammengefasste Element dar.
Detailliert	Mit der Option "Detailliert" wird jeder Eintrag als separate Zeile angezeigt. Die Spalte "Uhrzeit" kann angezeigt werden.

9. Klicken Sie auf **Übergeben**, um den von Ihnen definierten Bericht zu generieren.
10. Verwenden Sie die folgenden Optionen, um den angezeigten Bericht zu ändern.
    - Verwenden Sie die Optionen über dem Bericht unter **Anzeigen**, um den im Bericht enthaltenen Zeitraum zu ändern.
    - Klicken Sie auf den nach oben oder unten weisenden Pfeil in einer Spaltenüberschrift, um die Sortierreihenfolge dieser Spalte und den damit verbundenen Daten umzukehren.
    - Verwenden Sie die Links **Nächste Anzeige** und **Vorheriger** über und unter dem Bericht, um ggf. weitere Seiten des Berichts anzuzeigen. Standardmäßig enthält jede Seite 100 Zeilen. Dies kann Ihren Bedürfnissen entsprechend angepasst werden. Siehe *Anzeige- und Ausgabeoptionen*, Seite 357.
    - Klicken Sie auf die URL, um die angeforderte Website in einem neuen Fenster zu öffnen.

11. Klicken Sie auf **Als Favoriten definierte Berichte**, wenn der Bericht gespeichert werden soll, damit Sie ihn unkompliziert oder in wiederkehrender Zeitfolge generieren können (siehe *Speichern eines Berichts als Favorit*, Seite 143).

Spalten für flexible Detailberichte

Verwandte Themen:

- *Flexible Detailberichte*, Seite 131
- *Als Favoriten gekennzeichnete Untersuchungsberichte*, Seite 143
- *Planen von Untersuchungsberichten*, Seite 145

Die untenstehende Tabelle beschreibt die für Detailberichte verfügbaren Spalten (siehe *Flexible Detailberichte*, Seite 131).

Es sind nicht immer alle Spalten verfügbar. Wenn z. B. die Spalte "Benutzer" angezeigt wird, ist die Spalte "Gruppe" nicht verfügbar, und wenn die Spalte "Kategorie" angezeigt wird, ist die Spalte "Risikoklasse" nicht verfügbar.

Spaltenname	Beschreibung
Benutzer	Name des Benutzers, der die Anforderung gestellt hat. Die Benutzerinformationen müssen in der Protokolldatenbank verfügbar sein, um sie in Berichte zu übernehmen. Bei Berichten, die auf Benutzer basieren, sind keine Gruppeninformationen verfügbar.
Tag	Datum, an dem die Anforderung gestellt wurde.
URL-Hostname	Domänenname (auch Hostname genannt) der angeforderten Website.
Domäne	Verzeichnisdienstdomäne des verzeichnisbasierten Clients (Benutzer oder Gruppe, Domäne oder Organisationseinheit), der die Anforderung gestellt hat.
Gruppe	Name der Gruppe, zu der der Anfragende gehört. In gruppenbasierten Berichten werden keine persönlichen Benutzernamen genannt. Wenn der Benutzer, der die Website angefordert hat, zu mehr als einer Gruppe im Verzeichnisdienst gehört, werden in dieser Spalte mehrere Gruppen aufgelistet.
Risikoklasse	Die der Kategorie zugewiesene Risikoklasse, zu der die angeforderte Website gehört. Wenn die Kategorie zu mehreren Risikoklassen gehört, werden alle relevanten Risikoklassen aufgelistet. Siehe *Zuweisen von Risikoklassen an Kategorien*, Seite 324.
Verzeichnisobjekt	Verzeichnispfad für den Benutzer, der die Anforderung gestellt hat, ohne Angabe des Benutzernamens. In der Regel führt dies zu mehreren Zeilen für denselben Datenverkehr, da jeder Benutzer zu mehreren Pfaden gehört. Wenn Sie ein nicht-LDAP-basierten Verzeichnisdienst verwenden, steht diese Spalte nicht zur Verfügung.

Spaltenname	Beschreibung
Maßnahme	Aktion der Websense-Software in Reaktion auf die Anforderung, wie das Zulassen oder Sperren der Kategorie.
Quellserver	IP-Adresse des Computers, der die Anforderung an den Filtering Service sendet. Dies ist der Computer, auf dem entweder das Integrationsprodukt oder Websense Network Agent ausgeführt wird.
Protokoll	Protokoll der Anforderung.
Protokollgruppe	Gruppe in der Master Database, zu der das angeforderte Protokoll gehört.
Quell-IP	IP-Adresse des Computers, von dem die Anforderung gestellt wurde.
Ziel-IP	IP-Adresse der angeforderten Website.
Vollständige URL	Domänenname und Pfad der angeforderten Website (Beispiel: http://www.meinedomaene.com/produkte/elementeins/). Wenn Sie nicht vollständige URLs protokollieren, ist diese Spalte leer. Siehe *Konfigurieren der Protokollierung der vollständigen URL*, Seite 346.
Monat	Kalendermonat, in dem die Anforderung gestellt wurde.
Port	TCP/IP-Port, über den der Benutzer mit der Website kommuniziert hat.
Bandbreite	Die Summe der Datenmenge der ursprünglichen Anforderung des Benutzers und der Antwort der Website in Kilobyte. Dies ist die Summe der Gesamtwerte unter "Gesendet" und "Empfangen". Beachten Sie, dass einige Integrationsprodukte diese Informationen nicht an die Websense-Software senden. Beispiele dafür sind Check Point FireWall-1 und Cisco PIX Firewall. Wenn das von Ihnen verwendete Integrationsprodukt diese Informationen nicht sendet und der Websense Network Agent installiert ist, aktivieren Sie die Option **HTTP-Anforderungen protokollieren** für die entsprechende Netzwerkschnittstellenkarte, um einen Bericht der Bandbreitendaten zu ermöglichen. Siehe *Konfigurieren der Einstellungen für die Netzwerkschnittstellenkarte (NIC)*, Seite 369.
Gesendete Bytes	Die Anzahl der Bytes, die im Rahmen der Internetanforderung gesendet wurden. Dies stellt die übermittelte Datenmenge dar, bei der es sich sowohl um eine einfache Anforderung einer URL als auch um eine bedeutendere Übertragung handeln kann, bei der sich der Benutzer z. B. für eine Website registriert.

Spaltenname	Beschreibung
Empfangene Bytes	Die Anzahl der Bytes, die als Antwort auf eine Anforderungen vom Internet empfangen wurde. Dies beinhaltet sämtlichen Text sowie alle Grafiken und Skripte, die in der Website enthalten sind. Bei gesperrten Websites variiert die Anzahl Bytes je nach Software, die den Protokolleintrag erstellt. Wenn die Einträge von Websense Network Agent protokolliert werden, stellt die Anzahl empfangener Bytes einer gesperrten Website die Größe der Sperrseite dar. Wenn der Protokolleintrag von Websense Security Gateway erstellt wird, stellt die Anzahl Bytes empfangener Daten aufgrund des Scannings in Echtzeit die Größe der gescannten Seite dar. Weitere Informationen über das Scanning in Echtzeit finden Sie unter *Analysieren des Inhalts mit den Echtzeit-Optionen*, Seite 153. Wenn ein anderes Integrationsprodukt die Protokolleinträge erstellt, können die für eine gesperrte Website empfangenen Bytes Null (0) lauten, die Größe der Sperrseite wiedergeben oder einen von der angeforderten Website erhaltenen Wert darstellen.
Uhrzeit	Uhrzeit, zu der die Website angefordert wurde. Die Anzeige erfolgt im Format HH:MM:SS mit 24-Stunden-Darstellung.
Kategorie	Kategorie, unter der die Anforderung gefiltert wurde. Dabei kann es sich um eine Kategorie der Websense Master Database oder um eine benutzerdefinierte Kategorie handeln.

Detailberichte zu Benutzeraktivitäten

Verwandte Themen:

- *Untersuchungsberichte*, Seite 123

Klicken Sie auf den Link **Benutzer nach Tag/Monat**, um einen Detailbericht zu Benutzeraktivitäten für einen Benutzer zu erstellen. Dieser Bericht bietet eine grafische Darstellung der Internetaktivitäten des Benutzers für einen einzelnen Tag oder einen vollständigen Monat.

Generieren Sie zunächst einen Bericht für einen Benutzer für einen ausgewählten Tag. Von diesem Bericht können Sie einen Bericht der Aktivitäten desselben Benutzers für einen vollständigen Monat generieren. Detaillierte Anweisungen finden Sie unter:

- *Detailinformationen zu Benutzeraktivitäten nach Tag*, Seite 137
- *Detailinformationen zu Benutzeraktivitäten nach Monat*, Seite 138

Detailinformationen zu Benutzeraktivitäten nach Tag

Verwandte Themen:

- *Untersuchungsberichte*, Seite 123
- *Detailberichte zu Benutzeraktivitäten*, Seite 136
- *Detailinformationen zu Benutzeraktivitäten nach Monat*, Seite 138

Der Bericht mit Detailinformationen zu Benutzeraktivitäten nach Tag bietet eine detailliertere Ansicht der Aktivitäten eines bestimmten Benutzers an einem Tag.

1. Wählen Sie im oberen Bereich der Hauptseite die Option **Benutzer nach Tag/ Monat**. Das Dialogfeld "Benutzerspezifische Detailinformationen nach Tag" wird angezeigt.
2. Geben Sie den vollständigen Namen oder einen Teil des Namens des Benutzers im Feld **Nach Benutzer suchen** ein, und klicken Sie anschließend auf **Suchen**.

   Das Suchergebnis enthält eine Liste mit Bildlaufleiste mit bis zu 100 passenden Benutzernamen aus der Protokolldatenbank.
3. Wählen Sie Einträge in der Liste **Benutzer auswählen** aus.
4. Übernehmen Sie im Feld **Tag auswählen** entweder das standardmäßig angezeigte letzte Datum für Aktivitäten, oder wählen Sie ein anderes Datum aus.

   Sie können das neue Datum eingeben oder auf das Kalendersymbol klicken, um ein Datum auszuwählen. Das Kalenderauswahlfeld zeigt den Datumsbereich an, der von der aktiven Protokolldatenbank abgedeckt wird.
5. Klicken Sie auf **Zu Benutzer nach Tag**, um einen detaillierten Bericht der Aktivitäten dieses Benutzer am angeforderten Datum anzuzeigen.

   Der ursprüngliche Bericht enthält eine in 5-Minuten-Schritte eingeteilte Zeitachse der Benutzeraktivität. Jede Anforderung wird als Symbol angezeigt, das einer Kategorie in der Websense Master Database entspricht. Sämtliche benutzerdefinierten Kategorien werden durch ein einzelnes Symbol repräsentiert. (Die Farbe der Symbole gibt die Risikogruppe wieder, die in den Berichten über die Benutzeraktivitäten nach Monat enthalten sind. Siehe *Detailinformationen zu Benutzeraktivitäten nach Monat*, Seite 138.)

   Setzen Sie den Mauszeiger auf ein Symbol, um die genaue Uhrzeit, Kategorie und Aktion der damit verbundenen Anforderung anzuzeigen.

   Verwenden Sie die unten aufgeführten Steuerungen, um die Berichtsanzeige zu ändern oder eine Legende anzuzeigen.

Option	Beschreibung
Vorheriger Tag/ Nächster Tag	Zeigt die Internetaktivitäten dieses Benutzers am vorherigen oder nächsten Kalendertag an.
Tabellenansicht	Zeigt eine Liste aller angeforderter URLs mit dem Datum und der Uhrzeit der Anforderung, der Kategorie und der erfolgten Aktion (gesperrt, zugelassen oder sonstiges) an.

Option	Beschreibung
Detailansicht	Zeigt die ursprüngliche, grafische Darstellung des Berichts an.
Ähnliche Hits in Gruppen zusammenfassen/ Alle Hits anzeigen	Kombiniert alle Anforderungen, die in einem Abstand von höchstens 10 Sekunden gestellt wurden und über dieselbe Domäne, Kategorie und Aktion verfügen. Dies führt zu einer kürzeren, zusammengefassten Darstellung der Informationen. Der standardmäßige Schwellenwert für den Zeitraum ist 10 Sekunden. Informationen über das Ändern dieses Wertes finden Sie unter *Anzeige- und Ausgabeoptionen*, Seite 357. Nachdem Sie auf den Link geklickt haben, wechselt er zu "Alle Hits anzeigen", mit dem die ursprüngliche Liste der einzelnen Anforderungen wiederhergestellt wird.
Kategorieansicht	Zeigt eine Liste jeder Kategorie im aktuellen Bericht an, die sowohl den Kategorienamen als auch das Symbol enthält, das die Kategorie repräsentiert. Steuern Sie, welche Kategorien im Bericht angezeigt werden, indem Sie die Kontrollkästchen der entsprechenden Kategorien aktivieren. Klicken Sie anschließend auf **OK**, um den Bericht entsprechend Ihrer Auswahl zu aktualisieren.

6. Klicken Sie über dem Bericht auf **Detailinformationen zu Benutzeraktivitäten nach Monat**, um die Aktivitäten desselben Benutzers für einen vollen Monat anzuzeigen. Weitere Informationen dazu finden Sie unter *Detailinformationen zu Benutzeraktivitäten nach Monat*, Seite 138.

Detailinformationen zu Benutzeraktivitäten nach Monat

Verwandte Themen:

- *Untersuchungsberichte*, Seite 123
- *Detailberichte zu Benutzeraktivitäten*, Seite 136
- *Detailinformationen zu Benutzeraktivitäten nach Tag*, Seite 137
- *Zuordnung von Kategorien*, Seite 139

Sie können bei geöffnetem Bericht "Detailinformationen zu Benutzeraktivitäten nach Tag" zu einer Darstellung der Aktivitäten dieses Benutzers in einem Monat wechseln.

1. Öffnen Sie einen Bericht "Detailinformationen zu Benutzeraktivitäten nach Tag". Siehe *Detailinformationen zu Benutzeraktivitäten nach Tag*, Seite 137.
2. Klicken Sie oben auf **Detailinformationen zu Benutzeraktivitäten nach Monat**.

   Der neue Bericht enthält die Abbildung eines Kalenders, in dem die Internetaktivität des Benutzers pro Tag mit kleinen farbigen Blöcken dargestellt

wird. Anforderungen von Websites in benutzerdefinierten Kategorien werden als graue Blöcke dargestellt.

3. Klicken Sie oben links auf **Legende für Datenbankkategorien**, um die Farbverteilung bei niedrigem bis zu hohem potentiellem Risiko für die angeforderte Website anzuzeigen.

   Die Kategoriezuweisungen können nicht geändert werden. Siehe *Zuordnung von Kategorien*, Seite 139.

4. Klicken Sie auf **Vorheriger** oder **Nächste Anzeige**, um die Internetaktivitäten dieses Benutzers für den vorherigen oder nächsten Monat anzuzeigen.

Zuordnung von Kategorien

Verwandte Themen:

- *Untersuchungsberichte*, Seite 123
- *Detailberichte zu Benutzeraktivitäten*, Seite 136
- *Detailinformationen zu Benutzeraktivitäten nach Monat*, Seite 138

Die folgende Liste bestimmt, welche Kategorien in den Berichten "Detailinformationen zu Benutzeraktivitäten nach Tag" und "Detailinformationen zu Benutzeraktivitäten nach Monat" durch die jeweiligen Farben dargestellt werden.

Beachten Sie, dass Kategorienamen in der Master Database geändert werden können. Darüber hinaus können Kategorien jeder Zeit hinzugefügt oder gelöscht werden.

Farbe	Kategorien
Grau	Benutzerdefinierte Kategorien Nicht-HTTP-basierter Datenverkehr
Dunkelblau	**Wirtschaft und Handel** und alle damit verbundenen Unterkategorien **Bildung** und alle damit verbundenen Unterkategorien **Gesundheit** **Informationstechnologie**, einschließlich der Unterkategorien "Suchmaschinen und Portale" und "Web Hosting" **Verschiedenes**, Unterkategorien "Netzwerke für die Bereitstellung von Inhalten", "Dynamische Inhalte (CGI-BIN)", "Bilder (Medien)", "Image-Server" und "Private IP-Adressen" **Produktivität**/Werbung
Hellblau	**Arzneimittel**/Verschreibungspflichtige Medikamente **Staat & Regierung** und die Unterkategorie "Militär" **Informationstechnologie**/Webseiten zur URL-Übersetzung **Verschiedenes**, nur übergeordnete Kategorie **Nachrichten & Medien**, nur übergeordnete Kategorie **Besondere Ereignisse**

Farbe	Kategorien
Gelb Grün	**Schwangerschaftsabbruch** und alle damit verbundenen Unterkategorien **Nicht jugendfreies Material**/Aufklärung & Sexualerziehung **Bandbreite**, einschließlich der Unterkategorien "Internetradio & Internet-TV", "Private Netzwerkspeicherung/-sicherung" und "Streaming Media" **Unterhaltung**, einschließlich der Unterkategorie "MP3" **Spiele** **Staat & Regierung**/Politische Gruppen **Informationstechnologie**/Computersicherheit **Internet-Kommunikation**/Webbasierte E-Mail **Verschiedenes**/Server für das Herunterladen von Dateien **Verschiedenes**/Netzwerkfehler **Nachrichten & Medien**/Alternative Journale **Produktivität**, einschließlich der Unterkategorien "Instant Messaging", "Nachrichten-Boards und Foren" und "Online-Brokerage und Trading" **Religion** und die Unterkategorien "Nichttraditionelle Religionen, Okkultismus und volkstümliche Glaubensrichtungen" und "Traditionelle Religionen" **Sicherheit**, nur übergeordnete Kategorie **Online-Shopping** und alle damit verbundenen Unterkategorien **Soziale Organisationen** und alle damit verbundenen Unterkategorien **Gesellschaft & Lifestyle,** einschließlich der Unterkategorien "Schwule, Lesben und Bisexuelle", "Hobbys", "Persönliche Sites" und "Restaurants und Gastronomie" **Sport** und alle damit verbundenen Unterkategorien **Reisen** **Benutzerdefiniert** **Kraftfahrzeuge**

Farbe	Kategorien
Orange	**Nicht jugendfreies Material**/Nacktheit **Meinungsgruppen** **Bandbreite**/Internet-Telefonie **Arzneimittel** und seine Unterkategorien "Drogen- und Arzneimittelmissbrauch", "Marihuana" und "Präparate und Substanzen ohne gesetzliche Regelung" **Informationstechnologie**/Umgehung durch Proxy **Internet-Kommunikation** und die Unterkategorie "Web Chat" **Jobsuche** **Verschiedenes**/Keiner Kategorie zugeordnet **Produktivität**, Unterkategorien "Freeware/Software-Download" und "Pay-to-Surf" **Religion** **Gesellschaft & Lifestyle**, Unterkategorien "Alkohol, Tabak" und "Partnersuche" **Geschmackloses** **Waffen**
Rot	**Nicht jugendfreies Material** und die folgenden Unterkategorien: "Nicht jugendfreie Inhalte", "Unterwäsche & Bademode" und "Sex" **Bandbreite**/Peer-to-Peer **Glücksspiel** **Rechtswidrig oder Bedenklich** **Informationstechnologie**/Hacking **Militantes und Extremismus** **Rassismus und Hass** **Sicherheit**, Unterkategorien "Keylogger", "Bösartige Webseiten", "Phishing" und "Spyware" **Gewalt**

Standardberichte

Verwandte Themen:

- *Untersuchungsberichte*, Seite 123
- *Als Favoriten gekennzeichnete Untersuchungsberichte*, Seite 143
- *Planen von Untersuchungsberichten*, Seite 145

Mit Standardberichten können Sie bestimmte Informationen unkompliziert anzeigen, ohne zuvor den Detaillierungsgrad ändern zu müssen.

1. Klicken Sie auf der Hauptseite der Untersuchungsberichte auf den Link **Standardberichte**.

2. Wählen Sie den Bericht, der die gewünschten Informationen enthält. Die folgenden Berichte stehen zur Verfügung.

Stärkste verzeichnete Aktivität
• Benutzer mit den meisten Hits • Wichtigste 10 Benutzer für die 10 am häufigsten besuchten URL-Adressen • Aktivität der wichtigsten 5 Benutzer bei "Online-Shopping", "Unterhaltung" und "Sport" • Wichtigste 5 URL-Adressen der 5 am häufigsten besuchten Kategorien
Stärkste Belegung von Bandbreite
• Gruppen, die am meisten Bandbreite belegen • Gruppen, die am meisten Bandbreite bei "Streaming Media" belegen • Detaillierter Bericht der URL-Adressen für Benutzer nach Minderung der Netzwerkbandbreite • Wichtigste 10 Gruppen für Kategorien "Bandbreite"
Längste Online-Verweildauer
• Welche Benutzer haben am meisten Zeit online verbracht • Welche Benutzer haben am meisten Zeit auf Sites der Kategorien "Produktivität" verbracht
Meiste Sperrungen
• Benutzer mit den meisten Sperrungen • Sites mit den meisten Sperrungen • Detaillierter Bericht der URL-Adressen für Benutzer, die gesperrt wurden • Wichtigste 10 gesperrte Kategorien
Höchstes Sicherheitsrisiko
• Wichtigste Kategorien, die ein Sicherheitsrisiko darstellen • Wichtigste Benutzer des Peer-to-Peer-Protokolls • Wichtigste Benutzer von Sites der Kategorien "Sicherheit" • URL-Adressen für die 10 Computer mit der stärksten Spyware-Aktivität
Gesetzliche Haftung
• Risiko in Bezug auf gesetzliche Haftung nach Kategorie • Wichtigste Benutzer in als nicht jugendfrei eingestuften Kategorien

3. Zeigen Sie den daraufhin generierten Bericht an.
4. Speichern Sie den Bericht als Favorit, wenn Sie ihn in wiederkehrender Zeitfolge ausführen möchten. Siehe *Als Favoriten gekennzeichnete Untersuchungsberichte*, Seite 143.

Als Favoriten gekennzeichnete Untersuchungsberichte

Verwandte Themen:

- *Untersuchungsberichte*, Seite 123
- *Planen von Untersuchungsberichten*, Seite 145

Sie können die meisten Untersuchungsberichte als **Favoriten** speichern. Dazu gehören auch Berichte, die Sie generieren, indem Sie einen höheren Detaillierungsgrad für bestimmte Informationen, Standardberichte und Detailberichte wählen, die Sie auf Ihre persönlichen Bedürfnisse angepasst haben. Führen Sie dann den als Favorit gekennzeichneten Bericht zu einem beliebigen Zeitpunkt aus, oder planen Sie ihn für bestimmte Tage und Uhrzeiten.

Bei Organisationen, die die delegierte Verwaltung verwenden, wird die Berechtigung für das Speichern und Planen von Favoriten vom übergeordneten Administrator (Super Administrator) erteilt. Administratoren, die über diese Berechtigung verfügen, können nur Favoriten ausführen und planen, die sie selbst gespeichert haben. Sie haben keinen Zugriff auf Favoriten, die von anderen Administratoren gespeichert wurden.

Detaillierte Anweisungen für das Arbeiten mit als Favoriten definierten Berichten finden Sie unter:

- *Speichern eines Berichts als Favorit*, Seite 143
- *Generieren oder Löschen eines als Favoriten definierten Berichts*, Seite 144
- *Ändern eines als Favoriten definierten Berichts*, Seite 145

Speichern eines Berichts als Favorit

Verwandte Themen:

- *Als Favoriten gekennzeichnete Untersuchungsberichte*, Seite 143
- *Ändern eines als Favoriten definierten Berichts*, Seite 145

Verwenden Sie die folgenden Vorgehensweise, um einen Bericht als Favoriten zu speichern.

1. Generieren Sie einen Untersuchungsbericht. Stimmen Sie dabei das Format und die enthaltenen Informationen auf Ihre Bedürfnisse ab.
2. Klicken Sie auf **Als Favoriten definierte Berichte**.
3. Übernehmen oder ändern Sie den von Websense Manager angezeigten Namen.

   Der Name darf Buchstaben, Zahlen und den Unterstrich (_) enthalten. Leerschritte oder Sonderzeichen sind nicht zulässig.

4. Klicken Sie auf **Hinzufügen**.

   Der Berichtsname wird der Liste der Favoriten hinzugefügt.

5. Wählen Sie einen Bericht aus dieser Liste aus, und wählen Sie anschließend eine Option für die Berichtsverwaltung. Je nach gewählter Option finden Sie weitere Informationen unter:

   - *Generieren oder Löschen eines als Favoriten definierten Berichts*, Seite 144
   - *Planen von Untersuchungsberichten*, Seite 145

Generieren oder Löschen eines als Favoriten definierten Berichts

Verwandte Themen:

- *Als Favoriten gekennzeichnete Untersuchungsberichte*, Seite 143
- *Ändern eines als Favoriten definierten Berichts*, Seite 145

Sie können zu jedem Zeitpunkt einen als Favoriten definierten Bericht generieren oder aber löschen, wenn er veraltet ist.

1. Klicken Sie auf **Als Favoriten definierte Berichte**, um eine Liste mit Berichten anzuzeigen, die als Favoriten gespeichert wurden.

   Hinweis

   Wenn in Ihrer Organisation die delegierte Verwaltung verwendet wird, enthält diese Liste keine als Favoriten definierten Berichte, die von anderen Administratoren gespeichert wurden.

2. Wählen Sie einen Bericht aus der Liste aus.

   Wenn der gewünschte Bericht nicht als Favorit gespeichert wurde, finden Sie weitere Informationen unter *Speichern eines Berichts als Favorit*, Seite 143.

3. Gehen Sie dann entsprechend Ihrer persönlichen Bedürfnisse vor:

   - Klicken Sie auf **Jetzt ausführen**, um den gewählten Bericht umgehend zu generieren und anzuzeigen.
   - Klicken Sie auf **Planen**, um einen Bericht für eine spätere Ausführung oder eine Ausführung in wiederkehrender Zeitfolge zu planen. Weitere Informationen dazu finden Sie unter *Planen von Untersuchungsberichten*, Seite 145.
   - Klicken Sie auf **Löschen**, um den Bericht aus der Liste der Favoriten zu entfernen.

Ändern eines als Favoriten definierten Berichts

Verwandte Themen:

- *Untersuchungsberichte*, Seite 123
- *Als Favoriten gekennzeichnete Untersuchungsberichte*, Seite 143

Sie können ganz einfach einen neuen als Favoriten definierten Bericht erstellen, der einem vorhandenen Bericht ähnelt. Gehen Sie dabei wie folgt vor.

1. Klicken Sie auf **Als Favoriten definierte Berichte**, um eine Liste mit Berichten anzuzeigen, die als Favoriten gespeichert wurden.

   Hinweis
   Wenn in Ihrer Organisation die delegierte Verwaltung verwendet wird, enthält diese Liste keine als Favoriten definierten Berichte, die von anderen Administratoren gespeichert wurden.

2. Wählen Sie einen vorhandenen als Favoriten definierten Bericht, der dem neuen Bericht, den Sie erstellen möchten, am ähnlichsten ist, und führen Sie ihn aus. (Siehe *Generieren oder Löschen eines als Favoriten definierten Berichts*, Seite 144.)
3. Nehmen Sie die gewünschten Änderungen am angezeigten Bericht vor.
4. Klicken Sie auf **Als Favoriten definierte Berichte**, um die überarbeitete Anzeige als einen als Favoriten definierten Bericht unter einem neuen Namen zu speichern. (Siehe *Speichern eines Berichts als Favorit*, Seite 143.)

Planen von Untersuchungsberichten

Verwandte Themen:

- *Als Favoriten gekennzeichnete Untersuchungsberichte*, Seite 143
- *Speichern eines Berichts als Favorit*, Seite 143
- *Verwalten geplanter Jobs für Untersuchungsberichte*, Seite 148

Sie müssen einen Untersuchungsbericht als Favoriten speichern, bevor er für eine Ausführung zu einem späteren Zeitpunkt oder in wiederkehrender Zeitfolge geplant werden kann. Wenn der geplante Berichterstellungsjob ausgeführt wird, werden die resultierenden Berichte per E-Mail an die von Ihnen festgelegten Empfänger gesendet. Berücksichtigen Sie bei der Erstellung geplanter Jobs, dass Ihr E-Mail-Server die Größe und Menge der angehängten Berichtsdateien verarbeiten können muss.

Die Berichtsdateien geplanter Berichte werden im folgenden Verzeichnis gespeichert:

```
<Installationspfad>\webroot\Explorer\<Name>\
```

Der Standardinstallationspfad lautet C:\Program Files\Websense. Wenn der geplante Job nur über einen Empfänger verfügt, steht <Name> für den ersten Teil der E-Mail-Adresse (vor dem @-Zeichen). Im Falle mehrerer Empfänger werden die Berichte in einem Verzeichnis namens "Other" gespeichert.

> **Hinweis**
>
> Die von einem sich wiederholenden Job gespeicherten Berichte verwenden immer denselben Dateinamen. Wenn Sie Dateien für länger als einen Jobzyklus speichern möchten, ändern Sie den Dateinamen oder kopieren Sie die Datei an einen anderen Speicherort.
>
> Je nach Größe und Anzahl der geplanten Berichte kann dieses Verzeichnis einen großen Speicherplatz beanspruchen. Löschen Sie regelmäßig nicht benötigte Berichtsdateien.

1. Speichern Sie einen oder mehrere Berichte als Favoriten. (Siehe *Speichern eines Berichts als Favorit*, Seite 143.)
2. Klicken Sie auf **Als Favoriten definierte Berichte**, um eine Liste mit Berichten anzuzeigen, die als Favoriten gespeichert wurden.

   > **Hinweis**
   >
   > Wenn in Ihrer Organisation Rollen für die delegierte Verwaltung verwendet werden, enthält diese Liste keine als Favoriten definierten Berichte, die von anderen Administratoren gespeichert wurden.

3. Markieren Sie bis zu 5 Berichte, die im Rahmen des Jobs ausgeführt werden.
4. Klicken Sie auf **Planen**, um einen geplanten Berichtsjob zu erstellen, und machen Sie dann die auf der Seite "Bericht planen" erforderlichen Angaben.

   Es wird empfohlen, Berichterstellungsjobs für verschiedene Tage oder verschiedene Uhrzeiten zu planen, um eine Überlastung der Protokolldatenbank und eine herabgesetzte Leistung der Protokollierung und interaktiven Berichterstellung zu vermeiden.

Feld	Beschreibung
Wiederholungsintervall	Wählen Sie die Häufigkeit ("Nur einmal ausführen", "Täglich wiederholen", "Wöchentlich wiederholen", "Monatlich wiederholen") der Ausführung des Berichtsjobs.
Startdatum	Wählen Sie den Wochentag oder das Kalenderdatum für die erste (oder einmalige) Ausführung des Jobs.

Feld	Beschreibung
Zeitpunkt der Ausführung	Legen Sie die Uhrzeit der Jobausführung fest.
Per E-Mail senden an	Verwenden Sie das Feld **Zusätzliche E-Mail-Adressen**, um dieser Liste die erforderlichen Adressen hinzuzufügen. Markieren Sie eine oder mehrere E-Mail-Adressen, an die die Berichte in diesem Job gesendet werden sollen. (Stellen Sie sicher, dass Empfänger deaktiviert sind, die die Berichte nicht erhalten sollen.)
Zusätzliche E-Mail-Adressen	Geben Sie eine E-Mail-Adresse ein, und klicken Sie anschließend auf **Hinzufügen**, um sie der Liste **Per E-Mail senden an** hinzuzufügen. Die neue E-Mail-Adresse wird automatisch gemeinsam mit den anderen ausgewählten E-Mail-Adressen markiert.
Betreff und Textkörper der E-Mail anpassen	Aktivieren Sie dieses Kontrollkästchen, um die Betreffzeile und den Textkörper der E-Mail anzupassen. Wenn dieses Kontrollkästchen nicht aktiviert wurde, werden die Standardbetreffzeile und der Standardtext verwendet.
Betreff der E-Mail	Geben Sie den Text ein, der als Betreffzeile der E-Mail angezeigt werden soll, wenn geplante Berichte gesendet werden. Die Standardbetreffzeile lautet: Geplanter Job für Untersuchungsbericht
Text der E-Mail	Geben Sie einen Text ein, der in die E-Mail für den Versand der geplanten Berichte eingefügt wird. Die E-Mail lautet wie folgt, wobei Ihr Text die Textstellen <BENUTZERDEFINIERTER TEXT> ersetzt. Die Funktion für die Berichtsplanung hat die angehängte(n) Datei(en) generiert am <Datum Uhrzeit>. <BENUTZERDEFINIERTER TEXT> Klicken Sie auf folgende(n) Link(s), damit der oder die generierten Berichte angezeigt werden. Hinweis: Der Link funktioniert nur dann, wenn der Empfänger Zugriff auf den Web-Server hat, von dem der Job gesendet wurde.
Name des geplanten Jobs	Weisen Sie dem geplanten Job einen eindeutigen Namen zu. Der Name kennzeichnet diesen Job in der Warteschlange für Jobs. Siehe *Verwalten geplanter Jobs für Untersuchungsberichte*, Seite 148.

Feld	Beschreibung
Ausgabeformat	Wählen Sie das Dateiformat für die geplanten Berichte: **PDF**: PDF-Dateien (Portable Document Format) werden im Adobe Reader angezeigt. **Excel**: XLS-Dateien (Excel Spreadsheet) werden in Microsoft Excel angezeigt.
Datumsbereich	Legen Sie den Datumsbereich fest, den die Berichte in diesem Job abdecken sollen. **Alle Daten**: alle in der Protokolldatenbank verfügbaren Daten. **Relativ**: Wählen Sie einen Zeitraum ("Tage", "Wochen" oder "Monate") sowie eine genauere Bestimmung des Zeitraums ("Diese/r", "Letzte/r", "Letzte 2" usw.). **Bestimmte**: Legen Sie bestimmte Daten oder einen Datumsbereich für die Berichte in diesem Job fest.

5. Klicken Sie auf **Weiter**, um die Seite "Bestätigung der Planung" anzuzeigen.
6. Klicken Sie auf **Speichern**, um Ihre Auswahl zu speichern und zur Seite "Warteschlange für Jobs" zu wechseln (siehe *Verwalten geplanter Jobs für Untersuchungsberichte*, Seite 148).

Verwalten geplanter Jobs für Untersuchungsberichte

Verwandte Themen:

- *Untersuchungsberichte*, Seite 123
- *Planen von Präsentationsberichten*, Seite 116

Wenn Sie einen geplanten Job für Untersuchungsberichte erstellen, wird die Seite **Warteschlange für Jobs** angezeigt, die den neuen Job und eine Liste der vorhandenen geplanten Jobs enthält. Sie können auf diese Seite auch zugreifen, indem Sie auf der Hauptseite für Untersuchungsberichte auf den Link **Warteschlange für Jobs** klicken.

Hinweis

Wenn in Ihrer Organisation die delegierte Verwaltung verwendet wird, enthält diese Seite keine geplanten Jobs, die von anderen Administratoren gespeichert wurden.

Der Abschnitt **Detailinformationen des geplanten Berichts** enthält eine Liste aller geplanter Jobs in der Reihenfolge, in der sie erstellt wurden. Die Einträge bieten einen

Überblick über den definierten Zeitplan und den Jobstatus. Darüber hinaus stehen die folgenden Optionen zur Verfügung.

Option	Beschreibung
Bearbeiten	Zeigt den für diesen Job definierten Zeitplan, den Sie an dieser Stelle auch sofern erforderlich ändern können.
Löschen	Löscht den Job und fügt einen Eintrag im Abschnitt "Statusprotokoll" hinzu, der den Job als "Gelöscht" kennzeichnet.

Der Abschnitt **Statusprotokoll** protokolliert jeden Job, der in irgendeiner Form geändert wurde. Diese Einträge enthalten die geplante Startzeit, die tatsächliche Endzeit und den Status des Jobs.

Klicken Sie auf **Inhalt des Statusprotokolls löschen**, um alle Einträge im Abschnitt "Statusprotokoll" zu löschen.

Berichte über Sonderfälle

Verwandte Themen:

- *Untersuchungsberichte*, Seite 123
- *Zusammenfassende Berichte*, Seite 125

Ein Bericht über Sonderfälle informiert darüber, welche Benutzer die ungewöhnlichste Internetaktivität in der Datenbank aufweisen. Die Websense-Software berechnet die durchschnittliche Aktivität aller Benutzer pro Kategorie, pro Tag, pro Aktion (auch Maßnahme genannt) und pro Protokoll. Daraufhin wird die Benutzeraktivität angezeigt, die die statistisch größte Abweichung vom Durchschnitt aufweist. Die Abweichung wird als Standardabweichung vom Mittelwert berechnet.

1. Generieren Sie auf der Hauptseite für Untersuchungsberichte einen zusammenfassenden Bericht, der die Informationen enthält, für die Sie Sonderfälle anzeigen möchten. Die Auswahl im Bericht, die neben dem Feld "Internetnutzung nach" unterstrichen und in blauer Schrift angezeigt wird, wird in den Bericht für Sonderfälle übernommen.

   Wenn Sie z. B. Sonderfälle in Bezug auf Hits für eine bestimmte Kategorie anzeigen möchten, wählen Sie in der Liste **Internetnutzung nach** die Option **Kategorie**, und wählen Sie **Hits** als **Maßeinheit**.

   Hinweis

   Für die Navigationsdauer können keine Berichte für Sonderfälle generiert werden. Wenn die Grundlage ein zusammenfassender Bericht über die Navigationsdauer ist, basiert der Bericht für Sonderfälle auf Hits.

2. Klicken Sie auf **Sonderfälle**.

   Die Zeilen werden in absteigender Reihenfolge mit der höchsten Abweichung an erster Stelle angezeigt. Jede Zeile enthält die folgenden Informationen:

   - Gesamtwert (Hits oder Bandbreite) für den Benutzer, die Kategorie, das Protokoll, den Tag und die Aktion.
   - Durchschnitt (Hits oder Bandbreite) für alle Benutzer, diese Kategorie, dieses Protokoll, diesen Tag und diese Aktion.
   - Abweichung vom Durchschnitt für diesen Benutzer.

3. Wenn Sie die Aktivität eines bestimmten Benutzers in dieser Kategorie im Zeitablauf anzeigen möchten, klicken Sie auf den entsprechenden Benutzernamen.

   Wenn z. B. die Aktivität eines Benutzers an einem bestimmten Tag besonders hoch ist, klicken Sie auf den Benutzernamen, um einen Bericht anzuzeigen, der einen tieferen Einblick in die Gesamtaktivität des Benutzers erlaubt.

Ausgabe in Datei

Verwandte Themen:

- *Untersuchungsberichte*, Seite 123
- *Drucken von Untersuchungsberichten*, Seite 151

Nachdem Sie einen Untersuchungsbericht generiert haben, können Sie den Bericht mit den Schaltflächen über dem Bericht als Datei speichern. Die unterschiedlichen Schaltflächen bestimmen das jeweilige Format der Ausgabedatei.

Option	Beschreibung
	Speichert den Bericht im XLS-Format. Wenn Microsoft Excel 2003 (oder höher) auf dem Computer installiert ist, von dem aus Sie auf Websense Manager zugreifen, können Sie wählen, ob der Bericht angezeigt oder gespeichert werden soll. Anderenfalls werden Sie dazu aufgefordert, ein Verzeichnis und einen Dateinamen für den gespeicherten Bericht auszuwählen. Verwenden Sie die Optionen in Microsoft Excel für das Drucken oder Speichern des Berichts, bzw. dessen Versand per E-Mail.
	Generiert einen Bericht im PDF-Format. Wenn Adobe Reader Version 7.0 (oder höher) auf dem Computer installiert ist, von dem aus Sie auf Websense Manager zugreifen, können Sie wählen, ob der Bericht angezeigt oder gespeichert werden soll. Anderenfalls werden Sie dazu aufgefordert, ein Verzeichnis und einen Dateinamen für den gespeicherten Bericht auszuwählen. Verwenden Sie die Optionen in Adobe Reader für das Drucken oder Speichern des Berichts, bzw. dessen Versand per E-Mail.

Drucken von Untersuchungsberichten

Verwandte Themen:

- *Untersuchungsberichte*, Seite 123
- *Ausgabe in Datei*, Seite 150

Sie können Untersuchungsberichte auf folgende Weise drucken:

- Durch Verwenden der Druckfunktion im Webbrowser während der Anzeige des Berichts.
- Durch Erstellen einer PDF- oder XLS-Datei und anschließendem Verwenden der Druckfunktion in Adobe Reader oder Microsoft Excel (siehe *Ausgabe in Datei*, Seite 150).

Obwohl die Berichte so konzipiert wurden, dass ein Druck vom Browser möglich ist, empfiehlt es sich, zunächst das Druckergebnis zu testen.

Der Druck von Berichten über Detailinformationen zu Benutzeraktivitäten nach Monat wurde im Querformat konfiguriert. Bei allen anderen Berichten wurde das Hochformat festgelegt.

Wenn Sie Ihren eigenen Bericht konzipieren (siehe *Flexible Detailberichte*, Seite 131), variieren die Spaltenbreiten entsprechend der enthaltenen Informationen. Die Seitenausrichtung wechselt zum Querformat, wenn der Bericht breiter als 8 1/2 Zoll (21,59 cm) ist.

Der Inhalt der Seite ist entweder 7 1/2 Zoll (19,05 cm) oder 10 Zoll (25,40 cm) breit. Wenn auf DIN-A4 gedruckt wird, sind die Seitenränder etwas schmaler, befinden sich jedoch ebenfalls innerhalb des Druckbereichs. (Die Standardpapiergröße ist Letter, bzw. 8,5 x 11 Zoll (21,59 x 27,94 cm). Wenn Sie auf Papier im DIN-A4-Format drucken, müssen Sie diese Einstellung in der Datei wse.ini ändern. Siehe *Anzeige- und Ausgabeoptionen*, Seite 357.)

Zugreifen auf eigene Berichte

Verwandte Themen:

- *Untersuchungsberichte*, Seite 123
- *Konfigurieren von Vorgaben für die Berichterstellung*, Seite 326
- *Eigene Berichte erstellen*, Seite 360

Die Erstellung eigener Berichte in Websense ermöglicht Ihnen das Bewerten und Anpassen Ihrer eigenen Navigationsaktivitäten im Internet, um die Richtlinien Ihrer Organisation einzuhalten. Darüber hinaus werden mit dieser Funktion Vorgaben

seitens der Regierung eingehalten, die Organisationen dazu verpflichten, Benutzern offen zu legen, welche Art von Informationen gesammelt wird.

Wenn die Erstellung eigener Berichte in Ihrer Organisation aktiviert wurde, greifen Sie darauf vom Browser aus zu:

1. Geben Sie die vom Websense Administrator bereitgestellte URL ein, oder klicken Sie auf der Anmeldeseite von Websense Manager auf den Link für die Erstellung eigener Berichte, um auf die entsprechende Seite zuzugreifen.
2. Wenn bei **Policy Server** eine Dropdown-Liste angezeigt wird, wählen Sie die IP-Adresse für den Policy Server, der Informationen über Ihre Internetaktivität protokolliert.

   Hilfe dazu erhalten Sie von dem für Sie zuständigen Websense Administrator.
3. Geben Sie den **Benutzernamen** und das **Passwort** an, mit dem Sie sich im Netzwerk anmelden.
4. Klicken Sie auf **Anmelden**.

Websense Manager wird mit einem Untersuchungsbericht geöffnet, der Ihre Internetaktivität sortiert nach Risikoklasse anzeigt. Klicken Sie auf die verschiedenen Links und Elemente auf der Seite, um auf weitere Optionen für Alternativansichten der Informationen zuzugreifen, die über Ihre Aktivität gespeichert wurden. Bei Fragen bei der Arbeit mit den Berichten konsultieren Sie die **Hilfe**.

7 Analysieren des Inhalts mit den Echtzeit-Optionen

Verwandte Themen:

- *Scanningoptionen*, Seite 155
- *Kategoriezuordnung von Inhalten und Scans nach Bedrohungen*, Seite 156
- *Scanning von Dateien*, Seite 158
- *Entfernung von Inhalten*, Seite 159
- *Erstellen von Berichten über Scanningaktivitäten in Echtzeit*, Seite 162

Die Websense-Filtersoftware filtert Internetaktivitäten basierend auf Ihren aktiven Richtlinien und den Informationen, die in der Stammdatenbank (Master Database) gespeichert sind. Wenn Sie sich bei Websense Content Gateway oder Websense Web Security Gateway anmelden, können Sie den Inhalt von Websites und Dateien sogar in Echtzeit analysieren.

Abhängig von Ihrer Subskription sind zwei Echtzeit-Analyseoptionen verfügbar: Kategoriezuordnung von Inhalten und Sicherheits-Scanning in Echtzeit.

- Verwenden Sie die **Kategoriezuordnung von Inhalten**, um den Inhalt von URLs zu überprüfen, die nicht bereits gesperrt sind (basierend auf Ihren aktiven Richtlinien und auf der Kategoriezuordnung der Websense-Stammdatenbank für URLs). Anschließend erfolgt die Rückgabe einer Kategorie für die Verwendung beim Filtern.
- Wenn Sie sich bei Websense Web Security Gateway anmelden, sind drei Optionen für **Das Sicherheits-Scanning in Echtzeit** verfügbar.
  - **Content Scanning (Scanning von Inhalten)** untersucht den Webinhalt, um Sicherheitsbedrohungen, wie z. B. Phishing, URL-Umleitung, Web-Exploits und Umgehung durch Proxy, zu finden.
  - **File Scanning (Scanning von Dateien)** untersucht den Dateiinhalt auf Bedrohungskategorien hin – z. B. Virus, Trojanisches Pferd oder Wurm.
  - **Content Stripping (Entfernung von Inhalten)** entfernt aktiven Inhalt aus den angeforderten Webseiten.

Wenn eine dieser Optionen aktiviert ist, werden nur die Sites analysiert, die **nicht** bereits basierend auf Ihren aktiven Richtlinien und der Kategoriezuordnung der Websense-Stammdatenbank gesperrt sind. Weitere Informationen finden Sie unter *Scanningoptionen*, Seite 155.

> **Wichtig**
>
> Filter für die Zugriffsbeschränkung und ungefilterte URLs ersetzen die Kategoriezuordnung in Echtzeit.
>
> Wenn ein Benutzer eine Site anfordert, die einem aktiven Filter für die Zugriffsbeschränkung unterliegt (siehe *Benutzer auf eine festgelegte Liste von Internetsites einschränken*, Seite 178) oder in der Liste der ungefilterten URLs enthalten ist (siehe *Filter für bestimmte Sites neu definieren*, Seite 193), wird die Anforderung zugelassen, auch wenn ein Scanvorgang in Echtzeit durchgeführt wird und Bedrohungen entdeckt werden.

Nutzen Sie die Vorteile dieser Echtzeit-Sicherheitsfunktionen, indem Sie einen Subskriptionsschlüssel eingeben, der Support für Websense Content Gateway oder Websense Web Security Gateway in zwei Tools einschließt:

- In Websense Manager (**Einstellungen > Konto**)
- In der Management-Oberfläche von Websense Content Gateway (**Konfigurieren > My Proxy > Subscription > Subscription Management**)

Es dauert einige Minuten, um für beide Produkte die erforderlichen Datenbanken herunterzuladen und alle Echtzeit-Funktionen in den zwei Management-Tools zu synchronisieren und anzuzeigen.

Websense-Echtzeitoptionen

Die Websense-Echtzeitoptionen gewährleisten die Netzwerksicherheit. Verwenden Sie diese Optionen, um Webinhalte zu scannen und die Inhalte einer Filterkategorie zuzuordnen. Das Echtzeitergebnis wird an Filtering Service gesendet. Dieser Dienst filtert die Site basierend auf der Aktion, die der Echtzeit-Kategoriezuordnung in der aktiven Richtlinie zugewiesen ist.

Datenbank-Download

Die Echtzeitoptionen basieren auf kleinen Datenbanken, die mit Websense Web Security Gateway installiert wurden. Dieses Tool sucht regelmäßig nach Datenbankupdates. Diese Datenbanken werden unabhängig von der Aktualisierung aller Stammdatenbanken aktualisiert (einschließlich Datenbankupdates in Echtzeit und Real-Time Security Updates).

Jedes Mal, wenn Sie den Befehl **./WCGAdmin start** verwenden, um Websense Security Gateway zu starten, wird ein Datenbank-Download initiiert. Wenn beim Herunterladen ein Fehler auftritt, wird alle 15 Minuten ein neuer Versuch gestartet, bis das Update erfolgreich heruntergeladen wurde.

In der Standardeinstellung wird alle 15 Minuten nach Datenbankupdates gesucht. Sie können den Abstand ändern, indem Sie auf dem Websense Content Gateway-Computer in der Datei **/opt/bin/downloadservice.ini** den Wert **PollInterval** bearbeiten.

Nachdem die Datei **downloadservice.ini** bearbeitet wurde, muss Websense Content Gateway gestoppt und über die Befehlszeile neu gestartet werden.

- Um den Dienst zu stoppen, geben Sie Folgendes ein:
  /opt/WCG/WCGAdmin stop
- Um den Dienst neu zu starten, geben Sie Folgendes ein:
  /opt/WCG/WCGAdmin start

Scanningoptionen

Aktivieren und konfigurieren Sie die Echtzeitoptionen unter **Einstellungen > Scanning in Echtzeit**. Die einzelnen Scanningoptionen werden in den nachfolgenden Abschnitten ausführlich beschrieben.

- *Kategoriezuordnung von Inhalten und Scans nach Bedrohungen*, Seite 156
- *Scanning von Dateien*, Seite 158
- *Entfernung von Inhalten*, Seite 159

Für jede Option gibt es mindestens zwei Möglichkeiten:

- **Off** (Aus). Scanning in Echtzeit oder eine Sperrung werden nicht durchgeführt. Diese Option bietet keine zusätzliche Sicherheit.
- **Recommended** (Empfohlen) oder **On** (Ein). Wenn Ihre Site für Scanning in Echtzeit konfiguriert wurde, bietet diese Einstellung die beste Leistung. Die Scans basieren auf zwei Faktoren:
  - den Listen "Immer scannen" und "Nie scannen" unter **Einstellungen > Scanning in Echtzeit > Ausnahmen** (siehe *Optimieren des Scanvorgangs*, Seite 160).
  - Ob die Websense-Software dynamischen Inhalt in der Site festgestellt hat. Sites, für die angegeben ist, dass sie dynamischen Inhalt enthalten, werden gescannt. Die Markierung, die für eine Site angibt, dass sie dynamischen Inhalt enthält, kann nicht vom Benutzer konfiguriert werden.

    Sites mit dynamischem Inhalt, die in der Liste "Nie scannen" aufgeführt sind, werden nicht gescannt.
- **Alle.** Alle angeforderten Webseiten werden gescannt. Die einzigen Ausnahmen sind die Webseiten, die in der Liste "Nie scannen" aufgeführt sind.

Diese Option bietet die höchste Sicherheit, kann die Systemleistung aber beträchtlich verringern.

Warnung

Sites in der Liste "Nie scannen" werden unter keinen Umständen analysiert. Wenn eine Site in der Liste "Nie scannen" eine Gefährdung darstellt, können Echtzeitoptionen den bösartigen Code nicht analysieren oder erkennen.

Kategoriezuordnung von Inhalten und Scans nach Bedrohungen

Verwandte Themen:

- *Scanningoptionen*, Seite 155
- *Scanning von Dateien*, Seite 158
- *Entfernung von Inhalten*, Seite 159
- *Optimieren des Scanvorgangs*, Seite 160
- *Erstellen von Berichten über Scanningaktivitäten in Echtzeit*, Seite 162

Webinhalt ändert sich schnell. Statistiken zeigen, dass der Großteil des Webinhalts dynamisch ist. Darüber hinaus wird im Internet ein höherer Anteil an Inhalt gehostet, der von Benutzern erstellt wurde, z. B. der Inhalt auf Social Networking-Sites. Dieses Material unterliegt nicht den Inhalts- und Formatierungsrichtlinien, die Unternehmens-Websites regeln.

Wenn die Kategoriezuordnung von Inhalten aktiviert ist, werden die ausgewählten Sites in Echtzeit kategorisiert. Das Ergebnis der Kategoriezuordnung wird an die Websense-Filtersoftware weitergeleitet und abhängig von der aktiven Richtlinie gesperrt oder zugelassen.

Wichtig

Aktivieren Sie die Protokollierung der vollständigen URL (siehe *Konfigurieren der Protokollierung der vollständigen URL*, Seite 346), wenn Sie die Erstellung von Berichten über die Echtzeit-Scanningaktivitäten planen. Sonst enthalten die Protokolleinträge nur die Domäne (www.domain.com) der kategorisierten Site, auch wenn einzelne Seiten der Website u. U. zu unterschiedlichen Kategorien gehören.

Wenn Ihre Site URLs ohne Kategoriezuordnung über WebCatcher an Websense, Inc. meldet (siehe *Konfigurieren von WebCatcher*, Seite 337), werden URLs, die durch die Kategoriezuordnung von Inhalten kategorisiert werden, zur Aufnahme in die Stammdatenbank weitergeleitet.

Wenn Websense Security Gateway in Ihrer Subskription enthalten ist, können Sie auch angeben, dass Sites nach Sicherheitsbedrohungen gescannt werden.

Geben Sie unter **Einstellungen > Scanning in Echtzeit > Allgemeine Optionen** an, in welchen Fällen Kategoriezuordnung von Inhalten und Scanning von Inhalten durchgeführt werden soll.

1. Wählen Sie im Bereich "Kategoriezuordnung von Inhalten" die Option **Aus** oder **On** (Standardeinstellung), um festzulegen, ob ein Scanvorgang durchgeführt wird. Siehe *Scanningoptionen*, Seite 155.

   Nachdem die Kategorie festgelegt wurde, werden alle anderen konfigurierten Echtzeitoptionen angewendet, um die Sicherheit zu erhöhen.
2. (*Websense Security Gateway*) Wählen Sie im Bereich "Scanning von Inhalten" die Option **Aus** (Standardeinstellung), **Empfohlen** oder **Alle**, um die Scan-Ebene festzulegen.
3. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie die Registerkarte **Ausnahmen**, um Sites zu den Listen "Nie scannen" oder "Immer scannen" hinzuzufügen. Siehe *Optimieren des Scanvorgangs*, Seite 160.
   - Öffnen Sie die Seite **Allgemeine Optionen**, um die Einstellungen für andere Echtzeitoptionen zu ändern. Siehe *Scanning von Dateien*, Seite 158 und *Entfernung von Inhalten*, Seite 159.
4. Wenn Sie fertig sind, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst implementiert, wenn Sie auf **Alles speichern** klicken.

Präsentationsberichte können Einzelheiten über Zugriffsversuche auf Sites bieten, die Bedrohungen enthalten. Einzelheiten zum Ausführen von Websense-Berichten finden Sie unter *Präsentationsberichte*, Seite 102.

Scanning von Dateien

Verwandte Themen:

- *Scanningoptionen*, Seite 155
- *Kategoriezuordnung von Inhalten und Scans nach Bedrohungen*, Seite 156
- *Entfernung von Inhalten*, Seite 159
- *Optimieren des Scanvorgangs*, Seite 160
- *Erstellen von Berichten über Scanningaktivitäten in Echtzeit*, Seite 162

Beim Scannen von Dateien wird Inhalt in eingehenden Anwendungsdateien untersucht, die Benutzer im Remotemodus herunterladen oder öffnen. Über diese Echtzeitoption erfolgt die Rückgabe einer Kategorie an die Websense-Filtersoftware, und die Datei wird dementsprechend zugelassen oder gesperrt.

Die beste Vorgehensweise ist es, alle **ausführbaren** Dateien zu scannen (z. B. Dateien mit den Erweiterungen **.exe** und **.dll**). Sie können außerdem zusätzliche Dateitypen angeben, die gescannt werden sollen, und eine maximale Größe für zu scannende Dateien festlegen.

Hinweis
Nur PAD-Dateien für Windows (32-Bit-Version) werden gescannt.

Geben Sie über **Einstellungen > Scanning in Echtzeit > Allgemeine Optionen** an, in welchen Fällen Dateien gescannt werden sollen.

1. Wählen Sie im Bereich "Scanning von Dateien" die Option **Aus**, **Empfohlen** (Standardeinstellung) oder **Alle**, um die Scan-Ebene festzulegen. Siehe *Scanningoptionen*, Seite 155.
2. Klicken Sie auf **Erweiterte Einstellungen**.
3. **Alle Dateitypen mit ausführbarem Inhalt scannen** ist die Standardeinstellung. Deaktivieren Sie das Kontrollkästchen, wenn Sie stattdessen die zu scannenden Dateierweiterungen einzeln angeben möchten.
4. Geben Sie die Dateierweiterung ein, um zusätzliche Dateitypen festzulegen, die gescannt werden sollen (z. B. **.ppt** oder **.wmv**), und klicken Sie anschließend auf **Hinzufügen**. Die Dateierweiterung darf nur alphanumerische Zeichen, einen Unterstrich (_) oder einen Bindestrich (-) enthalten. Der Punkt vor der Erweiterung wird nicht angegeben.

   Sie können eine Dateierweiterung aus der Liste "Ausgewählte Dateierweiterungen" löschen, indem Sie die Erweiterung auswählen und auf **Entfernen** klicken.

5. Geben Sie unter "Optionen" die maximale Größe für zu scannende Dateien ein (in der Standardeinstellung 10 MB). Wählen Sie die Option **Benutzerdefiniert**, um eine Größe von bis zu 4.096 MB (4 GB) einzugeben. Dateien, die die angegebene Größe überschreiten, werden nicht gescannt.
6. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie die Registerkarte **Ausnahmen**, um Sites zu den Listen "Nie scannen" oder "Immer scannen" hinzuzufügen. Siehe *Optimieren des Scanvorgangs*, Seite 160.
   - Wenn Sie die Einstellungen für andere Echtzeitoptionen ändern möchten, öffnen Sie die Registerkarte **Allgemeine Optionen**. Siehe *Kategoriezuordnung von Inhalten und Scans nach Bedrohungen*, Seite 156, und *Entfernung von Inhalten*, Seite 159.
7. Wenn Sie fertig sind, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst implementiert, wenn Sie auf **Alles speichern** klicken.

Einzelheiten über Versuche, Dateien herunterzuladen, die Sicherheitsrisiken enthalten, werden in verschiedenen Präsentationsberichten bereitgestellt. Anweisungen zum Ausführen von Websense-Berichten finden Sie unter *Präsentationsberichte*, Seite 102.

Siehe *Datenverkehr basierend auf Dateitypen verwalten*, Seite 205, um Informationen zum Sperren von Dateien basierend auf der Typ- und URL-Kategorie zu erhalten.

Entfernung von Inhalten

Verwandte Themen:

- *Scanningoptionen*, Seite 155
- *Kategoriezuordnung von Inhalten und Scans nach Bedrohungen*, Seite 156
- *Scanning von Dateien*, Seite 158
- *Optimieren des Scanvorgangs*, Seite 160
- *Erstellen von Berichten über Scanningaktivitäten in Echtzeit*, Seite 162

Bedrohungen für Ihr System können sich in aktivem Inhalt verbergen, der über Webseiten gesendet wird. Eine Möglichkeit, die Integrität des Systems zu schützen, besteht in der Sicherstellung, dass dieser Inhalt nicht ankommt.

Die Echtzeitoptionen von Websense ermöglichen die Angabe, dass Inhalt in bestimmten Skriptsprachen (ActiveX, JavaScript oder VB Script) aus eingehenden Webseiten entfernt wird. Wenn die Entfernung von Inhalten aktiviert ist, wird der gesamte Inhalt in den entsprechenden Skriptsprachen aus den Sites entfernt, für die

angegeben ist, dass sie dynamischen Inhalt enthalten, oder die auf der Liste "Immer scannen" aufgeführt sind (siehe *Scanningoptionen*, Seite 155).

Der Inhalt wird erst entfernt, nachdem die Echtzeitoptionen die Site einer Kategorie zugeordnet haben und die Websense-Filtersoftware die anzuwendende Richtlinie identifiziert hat.

Wichtig

Webseiten funktionieren nicht wie erwartet, wenn der entfernte aktive Inhalt ein erforderlicher Bestandteil war. Um den vollständigen Zugriff auf Sites zu ermöglichen, die aktiven Inhalt benötigen, deaktivieren Sie die Entfernung von Inhalten oder fügen Sie die Sites zu der Liste "Nie scannen" hinzu.

Wenn ein Benutzer eine Seite mit aktivem Inhalt anfordert, erhält er keine Benachrichtigung, dass Inhalt entfernt wurde.

Legen Sie über **Einstellungen > Scanning in Echtzeit > Allgemeine Optionen** fest, in welchen Fällen Inhalte aus Sites mit dynamischem Inhalt entfernt werden sollen.

1. Wählen Sie im Bereich "Entfernung von Inhalt" aus, welche Arten von aktivem Inhalt aus eingehenden Webseiten entfernt werden sollen.
2. Informationen zum Ändern der Einstellungen für andere Echtzeitoptionen finden Sie unter:
   - *Kategoriezuordnung von Inhalten und Scans nach Bedrohungen*, Seite 156
   - *Scanning von Dateien*, Seite 158.
3. Wenn Sie fertig sind, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst implementiert, wenn Sie auf **Alles speichern** klicken.

Um die Entfernung von Inhalten für ausgewählte Sprachen aufzuheben, deaktivieren Sie das entsprechende Kontrollkästchen.

Optimieren des Scanvorgangs

Verwandte Themen:

- *Scanningoptionen*, Seite 155
- *Kategoriezuordnung von Inhalten und Scans nach Bedrohungen*, Seite 156
- *Scanning von Dateien*, Seite 158
- *Entfernung von Inhalten*, Seite 159

Verwenden Sie die Listen "Immer scannen" und "Nie scannen", um das Verhalten der Scanoptionen "Empfohlen" und "Alle" anzupassen.

- Wenn eine Echtzeitoption auf "Empfohlen" oder "On" eingestellt ist, werden Sites mit dynamischem Inhalt und Sites in der Liste "Immer scannen" gescannt (siehe *Scanningoptionen*, Seite 155). Sites in der Liste "Nie scannen" werden ignoriert.
- Wenn eine Echtzeitoption auf "Alle" eingestellt ist, werden Sites in der Liste "Nie scannen" ignoriert. Diese Einstellung kann die Leistung verbessern.

Verwenden Sie die Liste "Nie scannen" mit Vorsicht. Wenn eine Site in dieser Liste eine Gefährdung darstellt, wird das Sicherheitsproblem nicht erkannt, da Websense Security Gateway diese Site nicht scannt.

Die Listen "Immer scannen" und "Nie scannen" können über **Einstellungen > Scanning in Echtzeit > Ausnahmen** ergänzt und bearbeitet werden.

So fügen Sie Sites zu den Listen "Immer scannen" und "Nie scannen" hinzu:

1. Geben Sie im Feld **URLs** die Namen der Sites ein.

   Geben Sie nur den Hostnamen ein (z. B. **diesesite.com**). Es ist nicht erforderlich, die vollständige URL einzugeben. Geben Sie sowohl die Domäne als auch die Erweiterung ein – **diesesite.com** und **diesesite.net** sind unterschiedliche Einträge.

   Sie können mehrere Hostnamen gleichzeitig eingeben.
2. Wählen Sie in der Spalte **Optionen** aus, welche Echtzeitoptionen für alle Sites zutreffen, die Sie eingegeben haben. Sie können eine oder mehrere Optionen auswählen. Hinweis: Die Option **Sicherheitsbedrohungen** bezieht sich nur auf das Scannen von Inhalten, nicht das Scannen von Dateien. Die Listen "Immer scannen" und "Nie scannen" haben keine Auswirkung auf das Scannen von Dateien.

   Wenn auf einzelne Sites verschiedene Optionen anwendbar sind, geben Sie die Sites getrennt ein.
3. Wählen Sie die Optionen **Hinzufügen zu 'Immer scannen'** oder **Hinzufügen zu 'Nie scannen'** aus.

   Eine Site kann nur in einer der beiden Listen aufgeführt sein. Sie können z. B. nicht festlegen, dass eine Site immer auf Bedrohungen hin gescannt werden soll, aber der Inhalt dieser Site nie entfernt werden darf.

   - Um zu ändern, in welcher Liste eine Site aufgeführt ist, wählen Sie zuerst die Site aus und verwenden Sie dann die Schaltfläche mit dem nach rechts weisenden Pfeil (>) oder dem nach links weisenden Pfeil (>), um die Site in eine neue Liste zu verschieben.
   - Sie können eine Site aus einer Liste löschen, indem Sie die Site auswählen und auf **Entfernen** klicken.
4. Wenn Sie fertig sind, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst implementiert, wenn Sie auf **Alles speichern** klicken.

So ändern Sie die Scanoptionen, die einer Site zugeordnet sind:

1. Wählen Sie die Site in der Liste "Immer scannen" oder "Nie scannen" aus, und klicken Sie auf **Bearbeiten**.
2. Wählen Sie im Feld "Edit Rules" die neuen Optionen für diesen Hostnamen aus:
   - **Keine Änderung** – die aktuelle Einstellung bleibt bestehen.
   - **On** – zeigt an, dass der Inhalt für die angegebene Option, z. B. Kategoriezuordnung von Inhalten, gescannt wird.
   - **Aus** – zeigt an, dass für die angegebene Option kein Scanvorgang durchgeführt wird. Durch die Deaktivierung einer Option kann die Leistung verbessert werden, aber gleichzeitig wird die Sicherheit beeinträchtigt.
3. Wenn Sie alle Änderungen vorgenommen haben, klicken Sie im Feld "Edit Rules" auf **OK**, um zur Registerkarte "Ausnahmen" zurückzukehren.
4. Klicken Sie erneut auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst implementiert, wenn Sie auf **Alles speichern** klicken.

Erstellen von Berichten über Scanningaktivitäten in Echtzeit

Verwandte Themen:

- *Scanningoptionen*, Seite 155
- *Kategoriezuordnung von Inhalten und Scans nach Bedrohungen*, Seite 156
- *Scanning von Dateien*, Seite 158
- *Entfernung von Inhalten*, Seite 159

Wenn Ihre Subskription Echtzeit-Scanningfunktionen umfasst, können Sie die Auswirkungen dieser Funktionen anhand von Präsentations- und Untersuchungsberichten analysieren.

Auf der Seite "Präsentationsberichte" ist eine Berichtsgruppe für Echtzeit-Sicherheitsbedrohungen verfügbar. Diese Berichte konzentrieren sich auf Aktivitäten in Zusammenhang mit Bedrohungen. Sie können – wie bei allen anderen Präsentationsberichten – auch einen Bericht über Sicherheitsbedrohungen kopieren und die Berichtsfilter bearbeiten, damit die gewünschten Informationen enthalten sind, wenn Sie einen Bericht aus dieser Kopie erstellen.

Einige Berichte über Sicherheitsbedrohungen enthalten eine Spalte mit Bedrohungs-IDs. Klicken Sie auf eine bestimmte Bedrohungs-ID, um die Seite "Websense Security Labs" zu öffnen, in der die Art der Bedrohung beschrieben ist.

Darüber hinaus enthalten andere Präsentationsberichte Informationen über Echtzeit-Scanningaktivitäten sowie standardmäßige Filterungsaktivitäten. Kopieren sie einen vordefinierten Bericht und bearbeiten Sie die enthaltenen Filter, um einen Bericht zu erstellen, der sich nur auf Echtzeit-Scanningaktivitäten bezieht.

Wichtig

Aktivieren Sie die Protokollierung der vollständigen URL (siehe *Konfigurieren der Protokollierung der vollständigen URL*, Seite 346), um sicherzustellen, dass Berichte über Echtzeit-Scanningaktivitäten aussagekräftig sind. Sonst enthalten die Berichte nur die Domäne (www.domain.com) der kategorisierten Site, auch wenn einzelne Seiten der Website u. U. zu unterschiedlichen Kategorien gehören oder unterschiedliche Bedrohungen enthalten.

Beispiel: Der Bericht über die Details der vollständigen URLs nach Kategorie, der sich in der Gruppe "Internetaktivität" des Berichtskatalogs befindet, enthält eine ausführliche Auflistung aller URLs, auf die in jeder Kategorie zugegriffen wurde. Kopieren Sie den Bericht über die Details der vollständigen URLs nach Kategorie und bearbeiten Sie die Berichtsfilter, um einen Bericht zu erstellen, der sich auf das Scannen in Echtzeit bezieht. Wählen Sie auf der Registerkarte "Actions" (Aktionen) nur die zugelassenen und gesperrten Aktionen aus, die sich auf das Scannen in Echtzeit beziehen. Ändern Sie auf der Registerkarte "Optionen" den Titel des Berichtskatalogs und den Namen des Berichts, damit erkenntlich ist, dass es sich dabei um einen Bericht über Echtzeit-Scanningaktivitäten handelt. Sie können den Namen und Titel z. B. folgendermaßen ändern: Echtzeit: Details der vollständigen URLs nach Kategorie.

Untersuchungsberichte können auch verwendet werden, um Einblicke in Echtzeit-Scanningaktivitäten zu erhalten.

1. Wählen Sie in der Dropdownliste **Internetnutzung nach** die Option "Aktion" aus.
2. Klicken Sie im Ergebnisbericht auf eine Echtzeit-Aktion, z. B. "Kategorie gesperrt (Echtzeit)", um eine Liste mit Drilldownoptionen anzuzeigen.
3. Klicken Sie auf die gewünschte Drilldownoption, z. B. "Category" oder "User".
4. Klicken Sie auf den Wert "Hits" oder die Leiste in einer beliebigen Zeile, um zugehörige Einzelheiten anzuzeigen.
5. Klicken Sie im oberen Bereich der Seite auf **Bericht ändern**, um die Spalte "Vollständige URL" in den Bericht einzufügen.

   Einzelheiten zur Verwendung aller Funktionen des Untersuchungsberichts finden Sie unter *Untersuchungsberichte*, Seite 123.

Protokollieren der Echtzeit-Scanningaktivitäten

Beachten Sie bei der Verwendung von Echtzeit-Scanningoptionen, dass es Unterschiede bei der Protokollierung von standardmäßigen Webfilterungsaktivitäten und Echtzeit-Scanningaktivitäten gibt.

Für die standardmäßige Webfilterung stehen verschiedene Optionen zur Verfügung, um die Größe der Protokolldatenbank zu verringern.

- Aktivieren Sie die Option **Besuche**, um für jede angeforderte Website nur einen Eintrag zu protokollieren. Siehe *Konfigurieren von Log-Cachedateien*, Seite 333.
- Aktivieren Sie die Option **Konsolidierung**, um mehrere Anforderungen mit bestimmten gemeinsamen Elementen in einem einzelnen Protokolleintrag zu kombinieren. Siehe *Konfigurieren von Konsolidierungsoptionen*, Seite 335.
- Deaktivieren Sie die **Protokollierung der vollständigen URL**, um für jede Anforderung nur den Domänennamen zu protokollieren (www.domain.com) – und nicht den Pfad zu der bestimmten Seite in der Domäne (/Produkte/ProduktA). Siehe *Konfigurieren der Protokollierung der vollständigen URL*, Seite 346.
- Aktivieren Sie die Option **Selektive Protokollierung von Kategorien**, um die Protokollierung auf ausgewählte Kategorien zu beschränken, die für Ihre Organisation wichtig sind. Siehe *Konfigurieren von Filtering Service für die Protokollierung*, Seite 326.

Echtzeit-Scanningfunktionen sind von diesen Einstellungen nur teilweise betroffen. Wenn eine Site durch einen Echtzeit-Scanvorgang analysiert wird, werden zwei separate Protokolleinträge erstellt.

- Die Option **Web filter records** nutzt alle Einstellungen zur Verringerung der Größe, die implementiert wurden und für alle Webfilterungsberichte verfügbar sind.
- Die Option **Real-time records** ignoriert die meisten Einstellungen für die Verringerung der Größe. Jeder einzelne Hit wird protokolliert, Anforderungen in allen Kategorien werden protokolliert und keine der Einträge werden konsolidiert. Ein Echtzeit-Eintrag wird unabhängig davon erstellt, ob die Site nach dem Scannen in Echtzeit gesperrt oder zugelassen wird. Einzig die Einstellung für die Protokollierung der vollständigen URL wird für Echtzeit-Einträge beachtet.

Wenn Sie Optionen zur Verringerung der Protokolldatenbankgröße aktiviert haben, stimmen die Zahlen in den Echtzeit-Berichten u. U. **nicht** mit den Zahlen in den Standardfilterungsberichten überein – auch wenn die Berichte für dieselben Benutzer, Zeitperioden und Kategorien konfiguriert wurden. Beispiel: Wenn Sie die Besuche protokollieren und ein Benutzer eine Site anfordert, die von Echtzeit-Scanningfunktionen analysiert wird, erscheint die Anforderung dieses Benutzers in Standardfilterungsberichten als ein Besuch. In Echtzeit-Berichten werden dagegen u. U: mehrere Hits angezeigt.

Deaktivieren Sie die Einstellungen für die Verringerung der Protokolldatenbankgröße, wenn Sie vergleichbare Daten für die Standard- und Echtzeitfilterung erhalten möchten. Infolgedessen ist es möglich, dass die Datenbank sehr schnell sehr groß wird. Stellen Sie deshalb sicher, dass der Computer, auf dem die

Protokolldatenbank installiert ist, über genügend Festplattenspeicher sowie ausreichende Verarbeitungsleistung und Speicherkapazität verfügt.

Weitere Informationen zur Konfiguration der Einstellungen für die Größenverringerung finden Sie unter *Verwaltung der Berichterstellung*, Seite 321. Informationen zur Erstellung von Berichten sind unter *Präsentationsberichte*, Seite 102, und *Untersuchungsberichte*, Seite 123, zu finden.

8 Filtern von Remote Clients

Verwandte Themen

- *Funktionsweise des Remote Filtering*, Seite 168
- *Einstellungen für Remote Filtering konfigurieren*, Seite 174

Bei vielen Unternehmen ist es üblich, dass Mitarbeiter mit ihren Laptops auch außerhalb des Netzwerks arbeiten. Wenn auf den Remote-Computern ein Windows-Betriebssystem ausgeführt wird, können Sie die Internetanforderungen filtern, indem Sie Websense Remote Filtering implementieren. Hierbei handelt es sich um eine optionale Funktion, die für Websense Web Security und Websense Web Filter verfügbar ist.

Remote Filtering überwacht den HTTP-, SSL- und FTP-Datenverkehr und wendet dabei die Richtlinie "Standard" oder die Richtlinie an, die dem einzelnen Benutzer oder der Gruppe zugewiesen wurde, je nach Anmeldemethode des Benutzers am Remote-Computer. Remote Filtering filtert nicht auf Basis der Richtlinien, die einem Computer oder einem Netzwerkbereich zugewiesen sind. Weitere Informationen finden Sie unter *Remotebenutzer identifizieren*, Seite 171.

Bandbreitenbasierte Filterung wird für Remote Clients nicht unterstützt (siehe *Bandbreite mit Bandwidth Optimizer verwalten*, Seite 203). Die Bandbreite, die durch Remote-Datenverkehr verbraucht wird, wird nicht von der Bandbreitenmessung und -berichterstellung erfasst.

Remote Filtering von FTP- und SSL-Anforderungen, z. B. HTTPS, kann nur gesperrt oder zugelassen werden. Wenn ein Remotebenutzer z. B. eine FTP- oder HTTPS-Site von einer Kategorie anfordert, der z. B. die Aktion "Quote" oder "Bestätigen" zugeordnet wurde, wird die Site für Remote Filtering-Clients gesperrt. Wenn sich diese Computer innerhalb des Netzwerks befinden, werden die Filteraktionen "Quote" und "Bestätigen" normal angewendet.

Folgende Komponenten müssen installiert werden, um Remote Filtering zu implementieren:

- Remote Filtering Server muss sich innerhalb der äußersten Firewall befinden. Die Kommunikation zwischen Remote-Computern und dem Server muss zugelassen werden. Der Server wird üblicherweise in der *Demilitarized Zone* (DMZ) installiert, und zwar außerhalb der Firewall, die den Rest des Netzwerks schützt.

Sie können bis zu drei Remote Filtering Server installieren, um Ausfälle auszugleichen.

- Auf jedem außerhalb des Netzwerks verwendeten Computer mit dem Betriebssystem Windows muss Remote Filtering Client installiert sein.

> **Hinweis**
>
> Befolgen Sie die Empfehlungen des *Implementierungshandbuch*, um diese Komponenten sorgfältig zu implementieren. Weitere Anweisungen zur Installation finden Sie im *Installationshandbuch*.
>
> Wenn Sie die Websense-Software ohne Integrationsprodukt im Standalone-Modus verwenden, konfigurieren Sie Network Agent, so dass dieser den Remote Filtering Server **nicht** überwacht (siehe *Konfigurieren globaler Einstellungen*, Seite 366).

Die gesamte Kommunikation zwischen Remote Filtering Client und Remote Filtering Server wird authentifiziert und verschlüsselt.

Funktionsweise des Remote Filtering

Verwandte Themen

- *Innerhalb des Netzwerks*, Seite 169
- *Außerhalb des Netzwerks*, Seite 170
- *Remotebenutzer identifizieren*, Seite 171
- *Fehlschlagen der Kommunikation mit dem Server*, Seite 172
- *Virtual Private Network (VPN)*, Seite 173
- *Einstellungen für Remote Filtering konfigurieren*, Seite 174

Wenn ein Remote-Computer eine HTTP-, SSL- oder FTP-Anforderung stellt, kommuniziert Remote Filtering Client mit Remote Filtering Server. Remote Filtering Server kommuniziert mit Websense Filtering Service, um die anzuwendende Aktion zu ermitteln. Remote Filtering Server antwortet Remote Filtering Client und lässt die Site zu oder sendet die entsprechende Sperrmeldung.

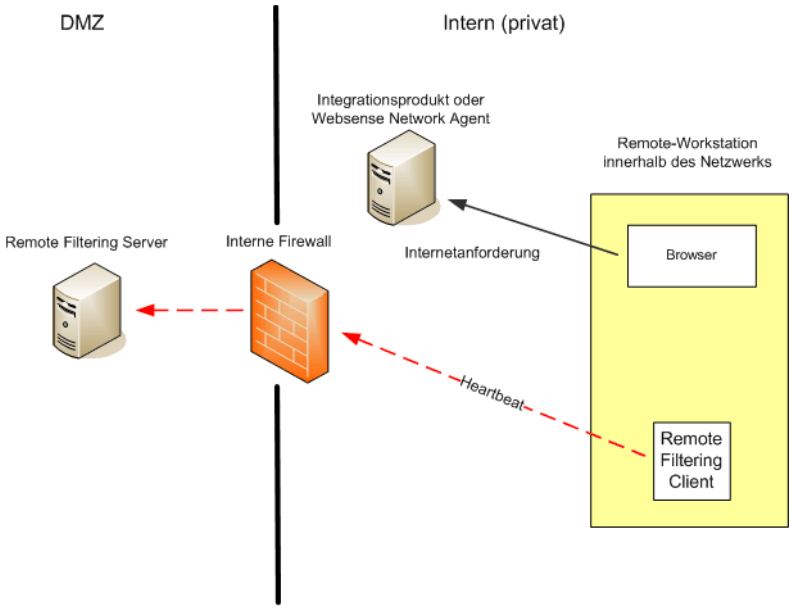
Wenn der Browser von einem Computer, auf dem Remote Filtering Client ausgeführt wird, eine Anforderung über HTTP, SSL oder FTP stellt, muss Remote Filtering Client entscheiden, ob die Anforderung bei Remote Filtering Server angefragt wird. Diese Entscheidung wird durch den Standort des Computers in Bezug auf das Netzwerk bestimmt.

Innerhalb des Netzwerks

Verwandte Themen

- *Funktionsweise des Remote Filtering*, Seite 168
- *Außerhalb des Netzwerks*, Seite 170
- *Remotebenutzer identifizieren*, Seite 171
- *Fehlschlagen der Kommunikation mit dem Server*, Seite 172
- *Virtual Private Network (VPN)*, Seite 173
- *Einstellungen für Remote Filtering konfigurieren*, Seite 174

Wenn ein Computer *innerhalb* des Netzwerk gestartet wird, versucht Remote Filtering Client ein **Herzschlagsignal** an Remote Filtering Server in der DMZ zu senden. Das Herzschlagsignal ist erfolgreich, weil der entsprechende Port der internen Firewall geöffnet ist.



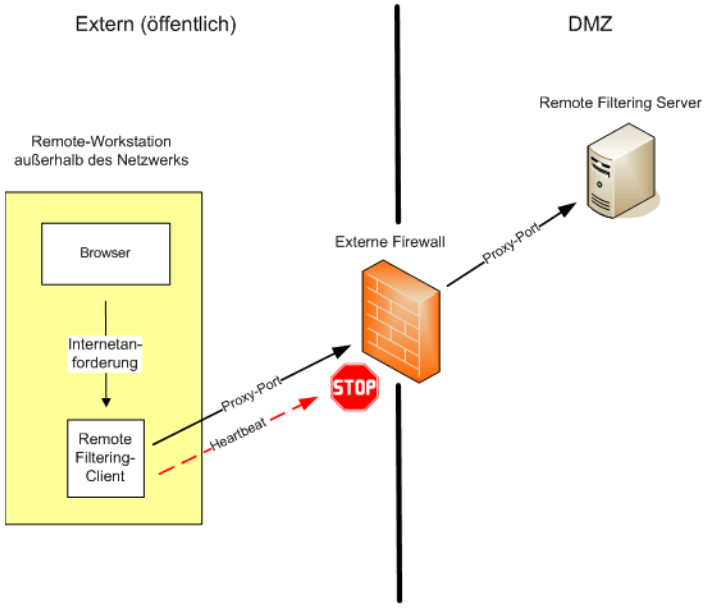
In diesem Fall wird Remote Filtering Client passiv und fragt die Internetanforderung nicht beim Remote Filtering Server an. Stattdessen werden diese Anforderungen direkt an das Integrationsprodukt (z. B. Cisco Pix, Microsoft ISA Server) oder Websense Network Agent weitergeleitet. Die Anforderung wird wie jede andere interne Anforderung gefiltert.

Außerhalb des Netzwerks

Verwandte Themen

- *Funktionsweise des Remote Filtering*, Seite 168
- *Innerhalb des Netzwerks*, Seite 169
- *Remotebenutzer identifizieren*, Seite 171
- *Fehlschlagen der Kommunikation mit dem Server*, Seite 172
- *Virtual Private Network (VPN)*, Seite 173
- *Einstellungen für Remote Filtering konfigurieren*, Seite 174

Wenn ein Computer von *außerhalb* des Netzwerks gestartet wird, versucht Remote Filtering Client, ein Herzschlagsignal an Remote Filtering Server zu senden. Das Herzschlagsignal schlägt fehl, weil der entsprechende Port der externen Firewall nicht geöffnet ist.



Das Fehlschlagen des Herzschlagsignals führt dazu, dass Remote Filtering Client eine Anfrage über jede HTTP-, SSL- oder FTP-Anforderung über den konfigurierten Port (standardmäßig Port 80) an Remote Filtering Server in der DMZ sendet. Remote Filtering Server leitet die Filteranforderung an Websense Filtering Service innerhalb des Netzwerks weiter. Filtering Service bewertet die Anforderung und sendet eine Antwort an Remote Filtering Server. Die Antwort wird dann an den Remote-Computer gesendet. Wenn die Site blockiert wird, fordert Remote Filtering Client eine entsprechende Sperrseite an und erhält diese. Die Seite wird dem Benutzer angezeigt.

Remote Filtering Client verzögert jede gefilterte Anforderung, bis eine Antwort von Remote Filtering Server eingetroffen ist. Je nach Antwort, lässt Remote Filtering Client die Site zu oder zeigt eine Sperrseite an.

Die Aktivitäten von Remote Filtering werden in einer Protokolldatei verfolgt: das Anmelden am und Abmelden vom Netzwerk, das Auftreten der Bedingungen "Bei Fehlschlag geöffnet" und "Bei Fehlschlag geschlossen" und das Neustarten von Clients. Remote Filtering Client erstellt beim ersten Start eine Protokolldatei. Sie können das Vorhandensein und die Größe der Protokolldatei überprüfen. Siehe *Einstellungen für Remote Filtering konfigurieren*, Seite 174.

Remotebenutzer identifizieren

Verwandte Themen

- *Funktionsweise des Remote Filtering*, Seite 168
- *Innerhalb des Netzwerks*, Seite 169
- *Außerhalb des Netzwerks*, Seite 170
- *Fehlschlagen der Kommunikation mit dem Server*, Seite 172
- *Virtual Private Network (VPN)*, Seite 173
- *Einstellungen für Remote Filtering konfigurieren*, Seite 174

Von der Art, wie sich ein Benutzer an einem Remote-Computer anmeldet, hängt es ab, welche Richtlinie umgesetzt wird.

Wenn sich ein Benutzer mit im Cache zwischengespeicherten Domäneanmeldeinformationen anmeldet (Anmeldeinformationen des Netzwerkverzeichnisses), kann Websense Filtering Service den Benutzernamen auflösen und die entsprechende benutzer- und gruppenbasierte Richtlinie auf den Remote-Computer anwenden. Zusätzlich wird die Internetaktivität unter dem Netzwerkbenutzernamen protokolliert.

Wenn sich der Benutzer mit einem Benutzerkonto lokal am Computer anmeldet, kann Filtering Service den Benutzernamen nicht auflösen und wendet stattdessen die Richtlinie "Standard" an. Die Internetaktivität wird unter dem lokalen Benutzernamen protokolliert. Remote Filtering filtert nicht auf Basis der Richtlinien, die einem Computer oder einem Netzwerkbereich zugewiesen sind.

Hinweis

Remotebenutzer werden immer entsprechend ihrer Anmeldeinformationen gefiltert (wie hier beschrieben). Selektive Authentifizierungseinstellungen gelten nicht für diese Benutzer.

Fehlschlagen der Kommunikation mit dem Server

Verwandte Themen

- *Funktionsweise des Remote Filtering*, Seite 168
- *Innerhalb des Netzwerks*, Seite 169
- *Außerhalb des Netzwerks*, Seite 170
- *Remotebenutzer identifizieren*, Seite 171
- *Virtual Private Network (VPN)*, Seite 173
- *Einstellungen für Remote Filtering konfigurieren*, Seite 174

Die Filterung wird ausgeführt, wenn ein außerhalb des Netzwerks befindlicher Computer mit Remote Filtering Client erfolgreich mit Remote Filtering Server in der DMZ des Netzwerks kommuniziert. Manchmal schlägt die Kommunikation jedoch fehl.

Die Aktion, die Remote Filtering Client bei fehlendem Kontakt zu Remote Filtering Server ausführt, ist konfigurierbar. Standardmäßig verwendet Remote Filtering Client die Einstellung **Bei Fehlschlag geöffnet**, die alle HTTP-, SSL- und FTP-Anforderungen zulässt, wenn die Kommunikation zwischen diesen Komponenten nicht hergestellt werden konnte. Remote Filtering Client versucht weiterhin, Kontakt zu Remote Filtering Server aufzunehmen. Wenn die Kommunikation erfolgreich verlaufen ist, kann die entsprechende Filterrichtlinie umgesetzt werden.

Wenn Remote Filtering Client auf **Bei Fehlschlaggeschlossen** konfiguriert wurde, wird ein Wert für das Zeitüberschreitungslimit angewendet. Standardmäßig sind dies 15 Minuten. Die Uhr beginnt zu laufen, wenn der Remote-Computer gestartet wurde. Remote Filtering Client versucht sofort eine Verbindung zu Remote Filtering Server herzustellen und durchläuft die verfügbaren Remote Filtering Server solange, bis eine Verbindung hergestellt werden konnte.

Wenn der Benutzer beim Start über einen Internetzugriff verfügt, wird keine Filterung ausgeführt, bis Remote Filtering Client eine Verbindung mit Remote Filtering Server hergestellt hat. Alle Anforderungen werden zugelassen. Ist dies der Fall, wird die entsprechende Filterrichtlinie umgesetzt.

Wenn Remote Filtering Client innerhalb des eingestellten Zeitüberschreitungslimits keine Verbindung herstellen kann, wird der gesamte Internetzugriff gesperrt ("Bei Fehlschlag geschlossen"), bis eine Verbindung zu Remote Filtering Server hergestellt werden konnte.

> **Hinweis**
> Wenn Remote Filtering Server aus einem beliebigen Grund keine Verbindung zu Websense Filtering Service herstellen konnte, wird ein Fehler an den Remote Filtering Client zurückgegeben. Der Filter wird immer bei Fehlschlag geöffnet.

Das Zeitüberschreitungslimit erlaubt Benutzern, die auf Reisen für ihren Internetzugriff bezahlen, den Computer zu starten und eine Verbindung herzustellen, ohne gesperrt zu werden. Wenn der Benutzer vor Ablauf der 15 Minuten Zeitüberschreitungslimit keinen Internetzugriff herstellen kann, kann der Internetzugriff während dieser Sitzung nicht mehr hergestellt werden. Der Benutzer muss den Computer neu starten, damit das Zeitüberschreitungslimit wieder von vorn beginnt.

Wie Sie die Einstellungen "Bei Fehlschlag geöffnet"/"Bei Fehlschlag geschlossen" oder den Wert für das Zeitüberschreitungslimit ändern können, erfahren Sie unter *Einstellungen für Remote Filtering konfigurieren*, Seite 174.

Virtual Private Network (VPN)

Verwandte Themen

- *Funktionsweise des Remote Filtering*, Seite 168
- *Innerhalb des Netzwerks*, Seite 169
- *Außerhalb des Netzwerks*, Seite 170
- *Remotebenutzer identifizieren*, Seite 171
- *Fehlschlagen der Kommunikation mit dem Server*, Seite 172
- *Einstellungen für Remote Filtering konfigurieren*, Seite 174

Websense Remote Filtering unterstützt VPN-Verbindungen, einschließlich Split-Tunnel-VPN. Wenn sich ein Remote-Computer über VPN (nicht über Split-Tunnel-VPN) mit einem internen Netzwerk verbindet, kann Remote Filtering Client ein Herzschlagsignal an Remote Filtering Server senden. Daraufhin wird Remote Filtering Client deaktiviert. Alle HTTP-, SSL- und FTP-Anforderungen vom Remote-Computer werden, wie auch die Anforderungen anderer Computer innerhalb des Netzwerks, über das interne Integrationsprodukt oder Network Agent gefiltert.

Wenn ein Remote-Computer über einen Split-Tunnel-VPN-Client eine Verbindung zu einem internen Netzwerk herstellt, erkennt Remote Filtering Client dies und sendet kein Herzschlagsignal an Remote Filtering Server. Remote Filtering Client geht davon aus, dass der Computer extern operiert und sendet Filteranforderungen an Remote Filtering Server.

Die Websense-Software unterstützt Split-Tunnel bei folgenden VPN-Clients:

- Checkpoint SecureClient
- Cisco
- Juniper/Netscreen
- Microsoft PPTP
- Nokia
- Nortel
- SonicWALL

Einstellungen für Remote Filtering konfigurieren

Verwandte Themen

- *Funktionsweise des Remote Filtering*, Seite 168
- *Innerhalb des Netzwerks*, Seite 169
- *Außerhalb des Netzwerks*, Seite 170
- *Remotebenutzer identifizieren*, Seite 171
- *Fehlschlagen der Kommunikation mit dem Server*, Seite 172
- *Virtual Private Network (VPN)*, Seite 173

Übergeordnete Administratoren, für die keine Bedingungen gelten, können über die Seite **Einstellungen > Allgemein > Remote Filtering** die Optionen konfigurieren, die sich auf alle dieser Installation zugeordnete Remote Filtering Clients auswirken.

Ausführliche Informationen zur Funktionsweise von Remote Filtering finden Sie unter *Funktionsweise des Remote Filtering*, Seite 168.

1. Wählen Sie das Kontrollkästchen **Bei Fehlschlag geschlossen**, um den Internetzugriff von Remote Filtering Clients zu sperren, solange die Computer nicht mit Remote Filtering Server kommunizieren.

   Standardmäßig ist dieses Kontrollkästchen nicht ausgewählt. Remotebenutzer verfügen also über einen ungefilterten Internetzugriff, wenn ihre Computer nicht mit Remote Filtering Server kommunizieren können.

2. Wenn Sie die Option "Bei Fehlschlag geschlossen" auswählen, wählen Sie im Feld **Zeitüberschreitung für 'Bei Fehlschlag geschlossen'**, eine Zahl unter 60 oder **Kein Zeitlimit** aus. Standardmäßig beträgt das Zeitüberschreitungslimit 15 Minuten.

   Innerhalb des Zeitlimits werden alle HTTP-, SSL- und FTP-Anforderungen zugelassen.

   Wenn Remote Filtering Client innerhalb des Zeitlimits nicht mit Remote Filtering Server kommunizieren kann, wird der gesamte Internetzugriff gesperrt ("Bei Fehlschlag geschlossen").

   Wenn die Option **Kein Zeitlimit** gewählt wurde, wird ein Remote-Computer unter Umständen gesperrt, bevor er eine Internetverbindung von einem Hotel oder einem anderen, Pay-for-Use-Provider aus hergestellt hat. Remote Filtering Client versucht zusätzlich, weiterhin mit Remote Filtering Server zu kommunizieren.

   Warnung

   Websense Inc. empfiehlt, die Option **Kein Zeitlimit** nicht zu wählen. Weiterhin wird empfohlen, das Zeitlimit nicht auf einen sehr niedrigen Wert zu setzen.

3. Wählen Sie eine **Maximale Größe für den lokalen Protokoll-Cache** von bis zu 10 Megabyte. Wählen Sie **Kein Protokoll**, um die Protokollierung zu deaktivieren.

   Hierdurch wird gesteuert, ob der Remote-Computer eine Protokolldatei erstellt, wenn er zum ersten Mal eine Verbindung mit Remote Filtering Server herstellt, und wie groß diese sein darf. In der Protokolldatei werden folgende Ereignisse aufgezeichnet:

   - das Abmelden des Computers aus dem Netzwerk
   - das erneute Anmelden des Computers am Netzwerk
   - der Neustart von Remote Filtering Client
   - das Auftreten der Bedingung "Bei Fehlschlag geöffnet"
   - das Auftreten der Bedingung "Bei Fehlschlag geschlossen"
   - eine Richtlinienaktualisierung für Remote Filtering Client

   Der Computer speichert die zwei aktuellsten Protokolle. Diese Protokolle können für das Beheben von Verbindungs- und anderen Problemen mit Remote Filtering verwendet werden.

9 Filterrichtlinien verfeinern

Im einfachsten Fall ist für das Filtern der Internetnutzung eine einzige Richtlinie erforderlich, die rund um die Uhr einen Kategoriefilter und einen Protokollfilter anwendet. Die Websense-Software bietet jedoch Tools, mit denen Sie mehr erreichen können, als eine elementare Filterung. Mit diesen Tools können Sie die Internetnutzung so maßgeschneidert filtern, wie Sie es wünschen. Sie können:

- **Filter für die Zugriffsbeschränkung** erstellen, um bestimmten Benutzern ausschließlich den Zugriff auf eine festgelegte Liste von Sites zu ermöglichen (siehe *Benutzer auf eine festgelegte Liste von Internetsites einschränken*, Seite 178).
- **Benutzerdefinierte Kategorien** erstellen, um neu zu definieren, wie ausgewählte Sites gefiltert werden (siehe *Arbeiten mit Kategorien*, Seite 186).
- Mit der Option **URLs anderen Kategorien zuordnen** spezifische Sites einer anderen von Websense definierten oder benutzerdefinierten Kategorie zuordnen als ihrer standardmäßigen Kategorie in der Stammdatenbank (siehe *URLs anderen Kategorien zuordnen*, Seite 195).
- **Ungefilterte URLs** definieren, um Benutzern den Zugriff auf bestimmte Sites zu erlauben, selbst wenn diese Sites im aktiven Kategoriefilter zu einer gesperrten Kategorie gehören (siehe *Ungefilterte URLs definieren*, Seite 194).
- **Bandbreiten** beschränkungen implementieren, die verhindern, dass Benutzer auf ansonsten zugelassene Kategorien und Protokolle zugreifen, wenn die Bandbreitenauslastung einen festgelegten Schwellenwert erreicht hat.
- **Schlüsselworte** definieren, mit denen ansonsten zugelassene Sites gesperrt werden, solange die Sperrfunktion für Schlüsselworte aktiviert ist (siehe *Auf Schlüsselwort basierte Filterung*, Seite 191).
- **Dateitypen** definieren, mit denen der Download der ausgewählten Dateitypen aus ansonsten zugelassenen Kategorien gesperrt wird, solange die Sperrfunktion für Dateitypen aktiviert ist (siehe *Datenverkehr basierend auf Dateitypen verwalten*, Seite 205).

Benutzer auf eine festgelegte Liste von Internetsites einschränken

Verwandte Themen:

- *Filter für die Zugriffsbeschränkung und Filterprioritäten*, Seite 179
- *Einen Filter für die Zugriffsbeschränkung erstellen*, Seite 180
- *Einen Filter für die Zulassungsbeschränkung bearbeiten*, Seite 181

Mit Filtern für die Zugriffsbeschränkung kann der Internetzugriff äußerst genau gefiltert werden. Jeder Filter für die Zugriffsbeschränkung besteht aus einer Liste von individuellen Websites. Filter für die Zugriffsbeschränkung werden einer Richtlinie ähnlich wie Kategoriefilter hinzugefügt und während eines festgelegten Zeitraums umgesetzt. Wenn ein Filter für die Zugriffsbeschränkung in einer Richtlinie aktiviert ist, können Benutzer, für die diese Richtlinie gilt, ausschließlich auf die Sites auf dieser Liste zugreifen. Alle übrigen Sites werden gesperrt.

Wenn beispielsweise die oberste Richtlinie einen Filter für die Zugriffsbeschränkung umsetzt, der nur Bildungs- oder Referenzsites enthält, können Studenten, für die diese oberste Richtlinie gilt, nur auf diese Sites zugreifen. Andere Sites sind für diese Studenten nicht verfügbar.

Wichtig

Wenn ein Filter für die Zugriffsbeschränkung aktiviert wurde, überprüft die Websense-Software lediglich, ob die angeforderte Site im Filter enthalten ist. Andere Aspekte werden nicht überprüft.

Das bedeutet, dass Benutzer weiterhin auf eine zugelassene Site zugreifen können, auch wenn diese Site von einem bösartigen Code befallen wurde. Der Zugriff erfolgt unabhängig von der Kategorisierung der Site in der Stammdatenbank oder durch das Scanning in Echtzeit.

Wenn ein Filter für die Zugriffsbeschränkung aktiviert ist, wird eine Sperrseite für alle nicht im Filter enthaltenen URLs angezeigt.

Die Websense-Software unterstützt bis zu 2.500 Filter für die Zugriffsbeschränkung mit insgesamt 25.000 URLs.

Filter für die Zugriffsbeschränkung und Filterprioritäten

In einigen Fällen können mehrere Filterrichtlinien für einen einzigen Benutzer gelten. Dies ist der Fall, wenn ein Benutzer zu mehr als einer Gruppe gehört und für die Gruppen verschiedene Richtlinien gelten. Darüber hinaus kann eine URL gleichzeitig zu einem Filter für die Zugriffsbeschränkung gehören und als ungefilterte URL definiert sein.

Wenn für einen Benutzer mehrere Gruppenrichtlinien gelten, wird durch die Einstellung **Restriktivere Filterung verwenden** festgelegt, wie der Benutzer gefiltert wird (siehe *Filterreihenfolge*, Seite 84). Diese Einstellung ist standardmäßig deaktiviert.

Die Websense-Software legt fest, welche Filtereinstellung auf dem Filterlevel weniger restriktiv ist. Wenn ein Benutzer mit mehreren Richtlinien gefiltert wird, wovon eine Richtlinie einen Filter für die Zugriffsbeschränkung verwendet, kann es manchmal unlogisch erscheinen, eine weniger restriktive Filterung anzuwenden.

Wenn die Einstellung **Restriktivere Filterung verwenden DEAKTIVIERT** ist:

- Wenn der Kategoriefilter **Alles sperren** und ein Filter für die Zugriffsbeschränkung angewendet werden können, wird der Filter für die Zugriffsbeschränkung immer als der weniger restriktive betrachtet.
- Wenn ein anderer Kategoriefilter und ein Filter für die Zugriffsbeschränkung angewendet werden können, wird der Kategoriefilter als der weniger restriktive betrachtet.

  Wenn also der Filter für die Zugriffsbeschränkung eine Site zulässt und der Kategoriefilter die Seite sperrt, wird die Seite gesperrt.

Wenn die Einstellung **Restriktivere Filterung verwenden AKTIVIERT** ist, wird der Filter für die Zugriffsbeschränkung als restriktiver angesehen als alle Kategoriefilter, ausgenommen der Filter "Alles sperren".

In der Tabelle wird zusammengefasst, wie sich die Einstellung **Restriktivere Filterung verwenden** auf die Filterung auswirkt, wenn mehrere Richtlinien gelten:

	***Restriktivere Filterung verwenden* DEAKTIVIERT**	***Restriktivere Filterung verwenden* AKTIVIERT**
Filter für die Zugriffsbeschränkung +Kategoriefilter **Alles sperren**	Filter für die Zugriffsbeschränkung (Anforderung zugelassen)	**Alles sperren** (Anforderung gesperrt)
Filter für die Zugriffsbeschränkung + zugelassene Kategorie	Kategoriefilter (Anforderung zugelassen)	Filter für die Zugriffsbeschränkung (Anforderung zugelassen)
Filter für die Zugriffsbeschränkung + gesperrte Kategorie	Kategoriefilter (Anforderung gesperrt)	Filter für die Zugriffsbeschränkung (Anforderung zugelassen)

	Restriktivere Filterung verwenden **DEAKTIVIERT**	*Restriktivere Filterung verwenden* **AKTIVIERT**
Filter für die Zugriffsbeschränkung + Kategorie "Quote/ Bestätigen"	Kategoriefilter (Anforderung durch "Quote/ Bestätigen" beschränkt)	Filter für die Zugriffsbeschränkung (Anforderung zugelassen)
Filter für die Zugriffsbeschränkung + ungefilterte URL	ungefilterte URL (Anforderung zugelassen)	Filter für die Zugriffsbeschränkung (Anforderung zugelassen)

Einen Filter für die Zugriffsbeschränkung erstellen

Verwandte Themen:

- *Arbeiten mit Filtern*, Seite 51
- *Benutzer auf eine festgelegte Liste von Internetsites einschränken*, Seite 178
- *Einen Filter für die Zulassungsbeschränkung bearbeiten*, Seite 181

Geben Sie über die Seite **Filter für die Zugriffsbeschränkung hinzufügen** Ihrem Filter einen eindeutigen Namen, und beschreiben Sie ihn. Der Zugriff auf die Seite erfolgt über die Seiten **Filter** oder **Richtlinie bearbeiten**. Nachdem Sie den Filter erstellt haben, geben Sie eine Liste zugelassener URLs ein, weisen Sie den Filter einer Richtlinie zu, und wenden Sie die Richtlinie auf Clients an.

1. Geben Sie einen eindeutigen **Filternamen** ein. Der Name muss mindestens 1 und maximal 50 Zeichen lang sein und darf keine der folgenden Zeichen enthalten:

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Filternamen dürfen keine Leerzeichen, Bindestriche und Apostrophe enthalten.
2. Geben Sie eine kurze **Beschreibung** des Filters ein. Die Beschreibung wird auf der Seite "Filter" neben dem Filternamen im Bereich "Filter für die Zugriffsbeschränkung" angezeigt und sollte den Zweck des Filters erklären. Mit Hilfe der Beschreibungen können Administratoren die Richtlinien besser über längere Zeiträume hinweg verwalten.

   Die Zeichenbeschränkungen, die für Filternamen gelten, gelten mit zwei Ausnahmen auch für die Beschreibungen: Beschreibungen dürfen Punkte (.) und Kommas (,) enthalten.
3. Um die neuen Filter anzuzeigen und zu bearbeiten, klicken Sie auf **OK**. Um Ihre Änderungen zu verwerfen und auf die Seite "Filter" zurückzukehren, klicken Sie auf **Abbrechen**.

Wenn Sie einen neuen Filter für die Zugriffsbeschränkung erstellen, wird dieser zur Liste **Richtlinienverwaltung > Filter > Filter für die Zugriffsbeschränkung** hinzugefügt. Klicken Sie zum Bearbeiten des Filters auf den Filternamen.

Fahren Sie mit *Einen Filter für die Zulassungsbeschränkung bearbeiten* fort, um das Anpassen Ihres neuen Filters abzuschließen.

Einen Filter für die Zulassungsbeschränkung bearbeiten

Verwandte Themen:

- *Benutzer auf eine festgelegte Liste von Internetsites einschränken*, Seite 178
- *Filter für die Zugriffsbeschränkung und Filterprioritäten*, Seite 179
- *Einen Filter für die Zugriffsbeschränkung erstellen*, Seite 180
- *Bearbeiten einer Richtlinie*, Seite 81

Ein Filter für die Zugriffsbeschränkung besteht aus einer Liste von Websites (URLs oder IP-Adressen) und regulären Ausdrücken, mit denen spezifische Sites identifiziert werden, auf die Benutzer zugreifen können. Wenn der Filter auf Clients angewendet wird, können diese Clients ausschließlich auf Sites zugreifen, die auf der Liste stehen.

Wichtig

Wenn ein Filter für die Zugriffsbeschränkung aktiviert wurde, überprüft die Websense-Software lediglich, ob die angeforderte Site im Filter enthalten ist. Andere Aspekte werden nicht überprüft.

Das bedeutet, dass Benutzer weiterhin auf eine zugelassene Site zugreifen können, auch wenn diese Site von einem bösartigen Code befallen wurde. Der Zugriff erfolgt unabhängig von der Kategorisierung der Site in der Stammdatenbank oder durch das Scanning in Echtzeit.

Auf der Seite **Richtlinienverwaltung > Filter > Filter für die Zugriffsbeschränkung bearbeiten** können Sie Änderungen an vorhandenen Filtern für die Zugriffsbeschränkung vornehmen. Sie können den Filternamen und die Beschreibung ändern, eine Liste der Richtlinien anzeigen, die Filter umsetzen, sowie verwalten, welche Sites im Filter enthalten sein sollen.

Wenn Sie einen Filter für die Zugriffsbeschränkung bearbeiten, wirken sich die Änderungen auf alle Richtlinien aus, die den Filter umsetzen.

1. Überprüfen Sie den Filternamen und die Beschreibung. Klicken Sie auf **Umbenennen**, um den Filternamen zu ändern, und geben Sie dann einen neuen Namen ein. Der Name wird in allen Richtlinien aktualisiert, die den ausgewählten Filter für die Zugriffsbeschränkung umsetzen.

2. Im Feld **Folgende Richtlinien verwenden diesen Filter** können Sie anzeigen, wie viele Richtlinien diesen Filter momentan umsetzen. Wenn eine oder mehrere Richtlinien den Filter umsetzen, klicken Sie auf **Richtlinien anzeigen**. Die Richtlinien werden in einer Liste aufgeführt.
3. Geben Sie unter "Sites hinzufügen oder entfernen" die URLs oder IP-Adressen ein, die Sie dem Filter für die Zugriffsbeschränkung hinzufügen möchten. Geben Sie eine URL oder eine IP-Adresse pro Zeile ein.

   Sie müssen das Präfix "http://" nicht eingeben.

   Wenn eine Site nach ihrer Kategorie in der Stammdatenbank gefiltert wird, gleicht die Websense-Software die URL mit der entsprechenden IP-Adresse ab. Dies geschieht nicht bei Filtern für die Zugriffsbeschränkung. Fügen Sie die URL und IP-Adresse einer Site hinzu, um beide zuzulassen.
4. Klicken Sie auf den nach rechts weisenden Pfeil (>), um die URLs und IP-Adressen auf die Liste der zugelassenen Sites zu übernehmen.
5. Neben individuellen Sites können Sie reguläre Ausdrücke zum Filter für die Zugriffsbeschränkung hinzufügen, mit denen mehrere Sites abgeglichen werden. Klicken Sie auf **Erweitert**, um einen regulären Ausdruck zu erstellen.
   - Geben Sie einen regulären Ausdruck pro Zeile ein. Klicken Sie dann auf den nach rechts weisenden Pfeil, um die Ausdrücke in die Liste "Zugelassene Sites" zu übernehmen.
   - Klicken Sie auf **Testen**, um zu überprüfen, ob ein regulärer Ausdruck auf die gewünschten Sites zutrifft.
   - Ausführliche Informationen zur Verwendung von regulären Ausdrücken für die Filterung finden Sie unter *Reguläre Ausdrücke verwenden*, Seite 208.
6. Überprüfen Sie die URLs, IP-Adressen und regulären Ausdrücke in der Liste **Zugelassene Sites**.
   - Wenn Sie eine Site oder einen Ausdruck ändern möchten, wählen Sie diesen aus, und klicken Sie auf **Bearbeiten**.
   - Wenn Sie Sites oder Ausdrücke aus der Liste entfernen möchten, wählen Sie diese aus, und klicken Sie auf **Löschen**.
7. Klicken Sie nach dem Bearbeiten des Filters auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Kehren Sie dann zur Seite "Filter" zurück. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Site über die Seite "Richtlinie bearbeiten" hinzufügen

Verwandte Themen:

- *Benutzer auf eine festgelegte Liste von Internetsites einschränken*, Seite 178
- *Filter für die Zugriffsbeschränkung und Filterprioritäten*, Seite 179
- *Einen Filter für die Zugriffsbeschränkung erstellen*, Seite 180
- *Bearbeiten einer Richtlinie*, Seite 81

Mit der Seite **Richtlinien > Richtlinie bearbeiten > Sites hinzufügen** können Sie Sites zum Filter für die Zugriffsbeschränkung hinzufügen.

Geben Sie eine URL oder eine IP-Adresse pro Zeile ein. Wenn Sie kein Protokoll festlegen, fügt die Websense-Software automatisch das Präfix **HTTP://** hinzu.

Klicken Sie auf **OK**, wenn Sie die Änderungen abgeschlossen haben, und kehren Sie zur Seite "Richtlinie bearbeiten" zurück. Durch das Klicken auf **OK** auf der Seite "Richtlinie bearbeiten" werden die Änderungen auch im Cache zwischengespeichert. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Änderungen, die an einem Filter für die Zugriffsbeschränkung vorgenommen werden, wirken sich auf alle Richtlinien aus, die den Filter umsetzen.

Filter und Richtlinien in Rollen kopieren

Verwandte Themen:

- *Erstellen von Kategoriefiltern*, Seite 52
- *Erstellen von Protokollfiltern*, Seite 55
- *Einen Filter für die Zugriffsbeschränkung erstellen*, Seite 180
- *Erstellen einer Richtlinie*, Seite 80

Übergeordnete Administratoren können mit Hilfe der Seiten **Filter > Filter zu Rolle kopieren** und **Richtlinien > Richtlinie zu Rolle kopieren** einen oder mehrere Filter bzw. eine oder mehrere Richtlinien in die Rolle eines delegierten Administrators kopieren. Wenn der Filter oder die Richtlinie kopiert wurde, können delegierte Administratoren ihre gemanagten Clients mit diesen Filtern oder Richtlinien filtern.

- In der Zielrolle wird an das Ende des Filter- oder Richtliniennamens das Kennzeichen "(Kopiert)" hinzugefügt. Wenn der Filter oder die Rolle mehrfach kopiert wurden, werden Zahlen hinzugefügt.

- Delegierte Administratoren können Filter oder Richtlinien, die in ihre Rolle kopiert wurden, umbenennen oder bearbeiten.
- Kategoriefilter, die in die Rolle eines delegierten Administrators kopiert wurden, setzen die Filteraktion für in dieser Rolle erstellte, benutzerdefinierte Kategorien auf "Zulassen". Delegierte Administratoren sollten die kopierten Kategoriefilter aktualisieren, um die gewünschte Aktion für ihre rollenspezifischen, benutzerdefinierten Kategorien einzustellen.
- Wenn delegierte Administratoren an einem Filter oder einer Richtlinie, die von einem übergeordneten Administrator in ihre Rolle kopiert wurde, Änderungen vornehmen, wirken sich diese Änderungen nicht auf die ursprünglichen Filter und Richtlinien des übergeordneten Administrators aus. Die Änderungen wirken sich auch nicht auf Filter oder Richtlinien aus, die in andere Rollen kopiert wurden.
- Beschränkungen der Filter-Fixierung wirken sich nicht auf die ursprünglichen Filter oder Richtlinien des übergeordneten Administrators aus. Sie wirken sich jedoch auf die kopierten Filter oder Richtlinien des delegierten Administrators aus.
- Da sich Beschränkungen der Filter-Fixierung auf delegierte Administratoren auswirken, können die Kategorie- und Protokollfilter "Alles zulassen" nicht in die Rolle eines delegierten Administrators kopiert werden.

So kopieren Sie einen Filter oder eine Richtlinie:

1. Überprüfen Sie auf den Seiten "Filter zu Rolle kopieren" oder "Richtlinie zu Rolle kopieren", dass die korrekten Filter oder Richtlinien in der Liste im oberen Bereich der Seite angezeigt werden.
2. Wählen Sie mit Hilfe der Dropdownliste **Rolle auswählen** eine Zielrolle aus.
3. Klicken Sie auf **OK**.

   In einem Popup-Dialogfenster wird angezeigt, dass die ausgewählten Filter oder Richtlinien kopiert werden. Der Kopiervorgang kann eine Weile in Anspruch nehmen.

   Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Nach Abschluss des Kopiervorgangs stehen den delegierten Administratoren in der ausgewählten Rolle die kopierten Filter und Richtlinien bei der nächsten Anmeldung beim Websense Manager zur Verfügung. Wenn delegierte Administratoren an einer Rolle mit Richtlinienzugriff angemeldet sind, während Filter oder Richtlinien kopiert werden, werden den Administratoren die neuen Filter und Richtlinien erst angezeigt, nachdem sich diese abgemeldet und erneut angemeldet haben.

Filterkomponenten erstellen

Über die Seite **Richtlinienverwaltung > Filterkomponenten** können Sie auf Tools zugreifen, mit denen Sie die Art und Weise verfeinern und anpassen können, wie die Websense-Software die Richtlinien für den Internetzugriff in Ihrem Unternehmen umsetzt. Die vier Schaltflächen auf dem Bildschirm sind den folgenden Aufgaben zugeordnet:

Kategorien bearbeiten	• Eine URL einer anderen Kategorie zuordnen (siehe *Filter für bestimmte Sites neu definieren*, Seite 193). Wenn die Kategorie "Online-Shopping" beispielsweise durch Ihre Internetfilterrichtlinien gesperrt ist, Sie aber den Zugriff auf bestimmte Zulieferer oder Partnersites zulassen möchten, können Sie diese Sites in eine zugelassene Kategorie übernehmen, z. B. "Handel und Wirtschaft". • Benutzerdefinierte Kategorien definieren oder bearbeiten (siehe *Eine benutzerdefinierte Kategorie erstellen*, Seite 189). Erstellen Sie zusätzliche Unterkategorien innerhalb der übergeordneten, in Websense definierten oder benutzerdefinierten Kategorien, und weisen Sie den neuen Kategorien URLs zu. • Einer Kategorie Schlüsselworte zuweisen (siehe *Auf Schlüsselwort basierte Filterung*, Seite 191). Definieren Sie zunächst die Schlüsselworte, und aktivieren Sie die Sperrfunktion für Schlüsselworte, um den Zugriff auf Sites zu sperren bzw. Sites neu zuzuordnen, deren URLs eine bestimmte Zeichenfolge enthalten. • Erstellen Sie reguläre Ausdrücke (siehe *Reguläre Ausdrücke verwenden*, Seite 208), Muster oder Vorlagen, mit denen mehrere URLs abgeglichen werden, und weisen Sie diese einer Kategorie zu.
Protokolle bearbeiten	Definieren oder bearbeiten Sie benutzerdefinierte Protokolldefinitionen (siehe *Ein benutzerdefiniertes Protokoll erstellen*, Seite 201, und *Benutzerdefinierte Protokolle bearbeiten*, Seite 198). Wenn Mitarbeiter Ihres Unternehmens beispielsweise ein benutzerdefiniertes Messaging-Tool verwenden möchten, können Sie eine benutzerdefinierte Protokolldefinition erstellen, um die Verwendung des Tools zu ermöglichen, gleichzeitig aber andere Instant Messaging- und Chatprotokolle zu sperren.
Dateitypen	Erstellen oder bearbeiten Sie Dateitypdefinitionen, mit denen bestimmte Dateitypen innerhalb sonst erlaubten Kategorien gesperrt werden (siehe *Datenverkehr basierend auf Dateitypen verwalten*, Seite 205).
Ungefilterte URLs	Definieren Sie spezifische, für alle Clients zugelassene Sites, selbst wenn diese Sites zu einer gesperrten Kategorie gehören (siehe *Ungefilterte URLs definieren*, Seite 194). Beachten Sie, dass das Hinzufügen einer URL zu dieser Liste den Kategoriefilter "Alles sperren" oder Filter für die Zugriffsbeschränkung nicht außer Kraft setzt.

Arbeiten mit Kategorien

Verwandte Themen:

- *Kategorien und deren Attribute bearbeiten*, Seite 186
- *Eine benutzerdefinierte Kategorie erstellen*, Seite 189
- *Auf Schlüsselwort basierte Filterung*, Seite 191
- *Filter für bestimmte Sites neu definieren*, Seite 193

Die Websense-Software bietet mehrere Methoden für das Filtern von Sites, die nicht in der Stammdatenbank enthalten sind, und für das Ändern der Art und Weise, wie individuelle Sites in der Stammdatenbank gefiltert werden.

- Erstellen Sie **benutzerdefinierte Kategorien**, um eine genauere Filterung und Berichterstellung zu ermöglichen.
- Verwenden Sie **URLs, die anderen Kategorien zugeordnet wurden**, um Kategorien für nicht kategorisierte Sites zu definieren, oder um die Kategorie für Sites zu ändern, die in der Stammdatenbank angezeigt werden.
- Definieren Sie **Schlüsselworte**, um alle Sites neuen Kategorien zuzuordnen, deren URL eine bestimmte Zeichenfolge enthält.

Kategorien und deren Attribute bearbeiten

Verwandte Themen:

- *Eine benutzerdefinierte Kategorie erstellen*, Seite 189
- *Alle benutzerdefinierten Kategorieattribute überprüfen*, Seite 188
- *Globale Änderungen an Kategoriefiltern vornehmen*, Seite 188
- *Auf Schlüsselwort basierte Filterung*, Seite 191
- *Filter für bestimmte Sites neu definieren*, Seite 193

Über die Seite **Richtlinienverwaltung > Filterkomponenten > Kategorien bearbeiten** können Sie benutzerdefinierte Kategorien, anderen Kategorien zugeordnete URLs und Schlüsselworte erstellen und modifizieren.

Die vorhandenen, von Websense definierten und benutzerdefinierten Kategorien werden im linken Bereich des Inhaltsfensters aufgeführt. Wählen Sie eine Kategorie aus der Liste, um aktuelle benutzerdefinierte Einstellungen anzuzeigen, die einer Kategorie zugeordnet sind, oder um neue benutzerdefinierte Definitionen zu erstellen.

Klicken Sie in der Symbolleiste im oberen Bereich der Seite auf **Alle benutzerdefinierten URLs/Schlüsselworte anzeigen**, um eine Liste aller benutzerdefinierten URLs, Schlüsselworte und regulären Ausdrücke anzuzeigen, die

allen Kategorien zugeordnet sind. Weitere Informationen finden Sie unter *Alle benutzerdefinierten Kategorieattribute überprüfen*, Seite 188.

- Klicken Sie auf **Hinzufügen**, und gehen Sie auf *Eine benutzerdefinierte Kategorie erstellen*, Seite 189, um weitere Anleitungen zu erhalten.

  Um eine vorhandene, benutzerdefinierte Kategorie zu entfernen, wählen Sie die Kategorie, und klicken Sie auf **Löschen**. Sie können keine Kategorien löschen, die von Websense definiert wurden.
- Um den Namen oder die Beschreibung einer benutzerdefinierten Kategorie zu ändern, wählen Sie die Kategorie, und klicken Sie auf **Umbenennen** (siehe *Eine benutzerdefinierte Kategorie umbenennen*, Seite 189).
- Klicken Sie auf **Aktion ändern**, um die Filteraktion zu ändern, die einer Kategorie in allen Kategoriefiltern zugewiesen ist (siehe *Globale Änderungen an Kategoriefiltern vornehmen*, Seite 188).
- Die Liste **URLs, die anderen Kategorien zugeordnet wurden** zeigt an, welche neu zugeordneten Sites (URLs und IP-Adressen) dieser Kategorie zugewiesen wurden.
  - Klicken Sie auf **URLs hinzufügen**, um der Liste eine Site hinzuzufügen. Weitere Anleitungen erhalten Sie unter *URLs anderen Kategorien zuordnen*, Seite 195.
  - Um eine vorhandene neu zugeordnete Site zu ändern, wählen Sie die URL oder IP-Adresse aus, und klicken Sie auf **Bearbeiten**.
- In der Liste **Schlüsselworte** wird aufgeführt, welche Schlüsselworte dieser Kategorie zugeordnet sind.
  - Um ein Schlüsselwort zu definieren, wählen Sie die Kategorie, und klicken Sie auf **Schlüsselworte hinzufügen**. Weitere Anleitungen erhalten Sie unter *Auf Schlüsselwort basierte Filterung*, Seite 191.
  - Um eine vorhandene Schlüsselwortdefinition zu ändern, wählen Sie das Schlüsselwort, und klicken Sie auf **Bearbeiten**.
- Sie können für die Kategorie neben URLs und Schlüsselworten auch **Reguläre Ausdrücke** definieren. Jeder reguläre Ausdruck ist ein Muster oder eine Vorlage, die mehreren Sites in der Kategorie zugeordnet werden kann.

  Klicken Sie auf **Erweitert**, um reguläre Ausdrücke für die Kategorie anzuzeigen oder zu erstellen.
  - Um einen regulären Ausdruck zu definieren, klicken Sie auf "Ausdrücke hinzufügen" (siehe *Reguläre Ausdrücke verwenden*, Seite 208).
  - Um einen vorhandenen regulären Ausdruck zu ändern, wählen Sie den Ausdruck, und klicken Sie auf **Bearbeiten**.
- Um neu zugeordnete URLs, Schlüsselworte oder reguläre Ausdrücke zu löschen, wählen Sie das Element aus, und klicken Sie auf **Löschen**.

Wenn Sie auf der Seite "Kategorien bearbeiten" Änderungen vorgenommen haben, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Kehren Sie dann auf die Seite "Filterkomponenten" zurück. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Alle benutzerdefinierten Kategorieattribute überprüfen

Über die Seite **Filterkomponenten > Kategorien bearbeiten > Alle benutzerdefinierten URLs/Schlüsselworte anzeigen** können Sie benutzerdefinierte Definitionen für URLs, Schlüsselworte und reguläre Ausdrücke überprüfen. Sie können auch Definitionen löschen, die nicht mehr benötigt werden.

Die Seite enthält drei ähnlich angeordnete Tabellen, eine für jedes Kategorieattribut: benutzerdefinierte URLs, Schlüsselworte oder reguläre Ausdrücke. In jeder Tabelle werden die Attribute neben dem Namen der Kategorie aufgeführt, der sie zugeordnet sind.

Um ein Kategorieattribut zu löschen, wählen Sie das entsprechende Kontrollkästchen, und klicken Sie auf **Löschen**.

Klicken Sie auf **Schließen**, um auf die Seite "Kategorien bearbeiten" zurückzukehren. Wenn Sie auf der Seite "Alle benutzerdefinierten URLs/Schlüsselworte anzeigen" Elemente gelöscht haben, klicken Sie auf der Seite "Kategorien bearbeiten" auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Globale Änderungen an Kategoriefiltern vornehmen

Über die Seite **Filterkomponenten > Kategorien bearbeiten > Aktion ändern** können Sie die Aktion ändern, die einer Kategorie in allen vorhandenen Kategoriefiltern zugeordnet ist. Hiermit wird auch die Standardaktion festgelegt, die in neuen Filtern auf die Kategorie angewendet wird.

Diese Änderung setzt die Aktion außer Kraft, die der Kategorie in allen vorhandenen Filtern zugeordnet ist. Administratoren können diese Filter jedoch später bearbeiten, um eine andere Aktion zuzuordnen.

Überprüfen Sie zunächst, dass der korrekte Kategoriename neben **Ausgewählte Kategorie** angezeigt wird, bevor Sie die Filtereinstellungen ändern, die auf eine Kategorie angewendet werden. Danach können Sie:

1. eine neue **Aktion** auswählen ("Zulassen", "Sperren", "Bestätigen" oder "Quote"). Weitere Informationen finden Sie unter *Filteraktionen*, Seite 47.

   Standardmäßig ist **Aktuelle Einstellungen nicht ändern** für alle Optionen auf der Seite ausgewählt.
2. Legen Sie fest, ob die Einstellung **Schlüsselworte sperren** aktiviert sein soll. Weitere Informationen finden Sie unter *Auf Schlüsselwort basierte Filterung*, Seite 191.
3. Legen Sie fest, ob die Einstellung **Dateitypen sperren** aktiviert sein soll, und passen Sie die Einstellungen für das Sperren an. Weitere Informationen finden Sie unter *Datenverkehr basierend auf Dateitypen verwalten*, Seite 205.

4. Legen Sie unter **Erweiterte Filterfunktionen** fest, ob Bandwidth Optimizer verwendet werden soll, um den Zugriff auf HTTP-Sites zu verwalten und die Einstellungen für das Sperren anzupassen. Weitere Informationen finden Sie unter *Bandbreite mit Bandwidth Optimizer verwalten*, Seite 203.

   Wichtig
   Die hier vorgenommenen Änderungen wirken sich auf alle vorhandenen Kategoriefilter aus, ausgenommen auf die Filter **Alles sperren** und **Alles zulassen**.

5. Klicken Sie auf **OK**, um zur Seite "Kategorien bearbeiten" zurückzukehren (siehe *Kategorien und deren Attribute bearbeiten*, Seite 186). Die Änderungen werden erst im Cache zwischengespeichert, wenn Sie auf der Seite "Kategorien bearbeiten" auf **OK** geklickt haben.

Eine benutzerdefinierte Kategorie umbenennen

Über die Seite **Filterkomponenten > Kategorien bearbeiten > Kategorie umbenennen** können Sie den Namen oder die Beschreibung ändern, die einer benutzerdefinierten Kategorie zugeordnet ist.

- Über das Feld **Name des Filters** können Sie den Kategorienamen bearbeiten. Der neue Name muss eindeutig sein und darf maximal 50 Zeichen lang sein.

  Der Name darf keines der folgenden Zeichen enthalten:

  ```
  * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
  ```

- Über das Feld **Beschreibung** können Sie die Beschreibung der Kategorie bearbeiten. Die Beschreibung darf maximal 255 Zeichen lang sein.

  Die Zeichenbeschränkungen, die für Filternamen gelten, gelten mit zwei Ausnahmen auch für die Beschreibungen: Beschreibungen dürfen Punkte (.) und Kommas (,) enthalten.

Klicken Sie auf **OK**, wenn Sie die Änderungen abgeschlossen haben, und kehren Sie zur Seite "Kategorien bearbeiten" zurück. Die Änderungen werden erst im Cache zwischengespeichert, wenn Sie auf der Seite "Kategorien bearbeiten" auf **OK** geklickt haben.

Eine benutzerdefinierte Kategorie erstellen

Verwandte Themen:

- *Kategorien und deren Attribute bearbeiten*, Seite 186
- *Auf Schlüsselwort basierte Filterung*, Seite 191
- *Filter für bestimmte Sites neu definieren*, Seite 193

Sie können die mehr als 90 von Websense definierten Kategorien der Stammdatenbank verwenden und zusätzlich Ihre eigenen **benutzerdefinierten**

Kategorien festlegen, um eine genauere Filterung und Berichterstellung zu erreichen. Sie können beispielsweise folgende benutzerdefinierte Kategorien erstellen:

- **Geschäftsreisen**: um Sites von genehmigten Anbietern zusammenzustellen, bei denen Mitarbeiter Flugtickets kaufen, Autos mieten und Hotelzimmer reservieren können.
- **Referenzmaterial**: um Sites von Online-Wörterbüchern und Enzyklopädien zusammenzustellen, die für Grundschüler geeignet sind.
- **Berufliche Fortbildung**: um Sites mit Schulungen und anderen Ressourcen zusammenzustellen, die Mitarbeiter für die Fortbildung ihrer Fähigkeiten verwenden sollen.

Über die Seite **Richtlinienverwaltung > Filterkomponenten > Kategorien bearbeiten > Kategorie hinzufügen** können Sie benutzerdefinierte Kategorien zu übergeordneten Kategorien hinzufügen. Sie können bis zu 100 benutzerdefinierte Kategorien erstellen.

1. Geben Sie einen eindeutigen, beschreibenden **Kategorienamen** ein. Der Name darf keines der folgenden Zeichen enthalten:

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

2. Geben Sie eine **Beschreibung** für die neue Kategorie ein.

   Die Zeichenbeschränkungen, die für Filternamen gelten, gelten mit zwei Ausnahmen auch für die Beschreibungen: Beschreibungen dürfen Punkte (.) und Kommas (,) enthalten.

3. Wählen Sie eine übergeordnete Kategorie aus der Liste **Hinzufügen zu**. Standardmäßig ist **Alle Kategorien** ausgewählt.
4. Geben Sie die Sites (URLs oder IP-Adressen) ein, die Sie zu dieser Kategorie hinzufügen möchten. Weitere Informationen finden Sie unter *URLs anderen Kategorien zuordnen*, Seite 195.

   Sie können diese Liste auch bearbeiten, nachdem Sie die Kategorie erstellt haben.
5. Geben Sie die Schlüsselworte ein, die Sie dieser Kategorie zuordnen möchten. Weitere Informationen finden Sie unter *Auf Schlüsselwort basierte Filterung*, Seite 191.

   Sie können diese Liste auch bearbeiten, nachdem Sie die Kategorie erstellt haben.
6. Definieren Sie eine Standardfilter **aktion**, die auf diese Kategorie in allen vorhandenen Kategoriefiltern angewendet werden soll. Sie können diese Aktion später in individuellen Filtern bearbeiten.

   Hinweis

   Kategoriefilter, die in die Rolle eines delegierten Administrators kopiert wurden, setzen die Filteraktion für in dieser Rolle erstellte, benutzerdefinierte Kategorien auf "Zulassen". Delegierte Administratoren sollten die kopierten Kategoriefilter aktualisieren, um die gewünschte Aktion für ihre rollenspezifischen, benutzerdefinierten Kategorien einzustellen.

7. Aktivieren Sie alle **erweiterte Filteraktionen** (Sperrfunktion für Schlüsselworte, Sperrfunktion für Dateitypen oder Sperrfunktion für Bandbreite), die dieser Kategorie in allen vorhandenen Kategoriefiltern zugewiesen werden soll.
8. Wenn Sie die neuen Kategorien definiert haben, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Kehren Sie dann zur Seite "Kategorien bearbeiten" zurück. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Die neue Kategorie wird zur Liste "Kategorien" hinzugefügt. Die benutzerdefinierte URL und die Schlüsselwortinformationen für die Kategorie werden angezeigt.

Auf Schlüsselwort basierte Filterung

Verwandte Themen:

- *URLs anderen Kategorien zuordnen*, Seite 195
- *Konfigurieren von Websense-Filtereinstellungen*, Seite 60
- *Erstellen von Kategoriefiltern*, Seite 52
- *Bearbeiten eines Kategoriefilters*, Seite 53
- *Arbeiten mit Kategorien*, Seite 186

Schlüsselworte werden Kategorien zugeordnet und dann für den Schutz vor Sites eingesetzt, die nicht explizit zur Stammdatenbank hinzugefügt oder als benutzerdefinierte URLs festgelegt wurden. Drei Schritte sind notwendig, um die Sperrfunktion für Schlüsselworte zu aktivieren:

1. Aktivieren der Sperrfunktion für Schlüsselworte auf globalem Level (siehe *Konfigurieren von Websense-Filtereinstellungen*, Seite 60).
2. Definieren von Schlüsselworten, die Kategorien zugeordnet sind (siehe *Schlüsselworte definieren*, Seite 192).
3. Aktivieren der Sperrfunktion für Schlüsselworte für die Kategorie in einem aktiven Kategoriefilter (siehe *Bearbeiten eines Kategoriefilters*, Seite 53).

Wenn Schlüsselworte festgelegt wurden und die Sperrfunktion für Schlüsselworte für eine spezifische Kategorie aktiviert wurde, sperrt die Websense-Software alle Sites, in deren URLs ein Schlüsselwort enthalten ist und protokolliert die Site als zur spezifischen Kategorie zugehörig. Die Site wird gesperrt, auch wenn andere URLs in der Kategorie zugelassen werden.

Wenn Sie beispielsweise die Kategorie "Sport" in einem aktiven Kategoriefilter zulassen, Sie aber den Zugriff auf Sites über Basketball sperren möchten, können Sie der Kategorie "Sport" das Schlüsselwort "NBA" zuordnen und die Sperrfunktion für Schlüsselworte aktivieren. Folgende URLs werden gesperrt und als zur Kategorie "Sport" zugehörig protokolliert:

- sports.espn.go.com/**nba**/
- moder**nba**kery.com
- moder**nba**biesandchildren.com
- fashio**nba**r.com

Gehen Sie beim Definieren von Schlüsselworte sorgfältig vor, um nicht unbeabsichtigt zu viele Sites zu sperren.

> **Wichtig**
> Wenn Sie Websense Web Security verwenden, ordnen Sie den Unterkategorien "Erweiterter Schutz" keine Schlüsselworte zu. Die Sperrfunktion für Schlüsselworte wird für diese Kategorien nicht umgesetzt.

Wenn eine Anforderung auf Grund eines Schlüsselworts gesperrt wird, wird der Benutzer auf der Sperrseite von Websense darauf hingewiesen.

Schlüsselworte definieren

Verwandte Themen:

- *Bearbeiten eines Kategoriefilters*, Seite 53
- *Arbeiten mit Kategorien*, Seite 186
- *Auf Schlüsselwort basierte Filterung*, Seite 191
- *Reguläre Ausdrücke verwenden*, Seite 208

Bei einem Schlüsselwort handelt es sich um eine Zeichenfolge (ein Wort, eine Phrase, ein Akronym), das in einer URL enthalten sein kann. Weisen Sie die Schlüsselworte einer Kategorie zu, und aktivieren Sie dann die Sperrfunktion für Schlüsselworte in einem Kategoriefilter.

Über die Seite **Richtlinienverwaltung > Filterkomponenten > Kategorien bearbeiten > Schlüsselworte hinzufügen** können Sie Schlüsselworte zu Kategorien zuordnen. Über die Seite **Schlüsselworte bearbeiten** können Sie die Definition eines Schlüsselwortes ändern.

Gehen Sie beim Definieren von Schlüsselworten sorgfältig vor, um nicht unbeabsichtigt zu viele Sites zu sperren. Sie beabsichtigen beispielsweise, nicht jugendfreie Seiten mit Hilfe des Schlüsselworts "Sex" zu sperren, sperren dadurch aber auch Suchanfragen mit Wörtern wie "City of Essex" und Sites wie m**sex**change.org (Kategorie "Informationstechnologie"), vega**sex**perience.com (Kategorie "Reisen") und sci.esa.int/mar**sex**press (Kategorie "Bildungseinrichtung").

Geben Sie ein Schlüsselwort pro Zeile ein.

- Schlüsselworte dürfen keine Leerzeichen enthalten. URLs und CGI-Zeichenfolgen dürfen zwischen den Wörtern keine Leerzeichen enthalten.
- Fügen Sie vor folgenden Sonderzeichen einen Backslash (\) ein:

  ```
  . , # ? * +
  ```

  Wenn Sie keinen Backslash einfügen, ignoriert die Websense-Software die Sonderzeichen.

- Wenn Sie Websense Web Security verwenden, ordnen Sie den Unterkategorien "Erweiterter Schutz" keine Schlüsselworte zu. Die Sperrfunktion für Schlüsselworte wird für diese Kategorien nicht umgesetzt.

Wenn Sie die Schlüsselworte hinzugefügt oder bearbeitet haben, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Kehren Sie dann zur Seite "Kategorien bearbeiten" zurück. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Gehen Sie außerdem wie folgt vor, um die Sperrfunktion für Schlüsselworte zu aktivieren:

1. Sperrfunktion für Schlüsselworte aktivieren über die Seite **Einstellungen > Filterung (Filtering)** (siehe *Konfigurieren von Websense-Filtereinstellungen*, Seite 60).
2. Sperrfunktion für Schlüsselworte in einem oder mehreren aktiven Kategoriefiltern aktivieren (siehe *Bearbeiten eines Kategoriefilters*, Seite 53).

Filter für bestimmte Sites neu definieren

Verwandte Themen:

- *Eine benutzerdefinierte Kategorie erstellen*, Seite 189
- *Auf Schlüsselwort basierte Filterung*, Seite 191
- *Ungefilterte URLs definieren*, Seite 194
- *URLs anderen Kategorien zuordnen*, Seite 195

Mit Hilfe von benutzerdefinierten URLs können Sie:

- Filtern Sie Sites genauer, die nicht in der Websense-Stammdatenbank enthalten sind. Standardmäßig werden diese Sites mit der Aktion gefiltert, die der Kategorie **Verschiedenes\Ohne Kategoriezuordnung** zugeordnet ist.
- Filtern Sie Sites auf andere Weise, als die Kategorie in der Stammdatenbank vorgibt.

Die Websense-Software sucht zunächst nach benutzerdefinierten URL-Definitionen für eine Site und erst danach in der Stammdatenbank. Die Site wird also nach der Kategorie gefiltert, die der benutzerdefinierten URL zugeordnet ist.

Es gibt zwei Typen benutzerdefinierter URLs: ungefilterte URLs und URLs, die anderen Kategorien zugeordnet wurden.

- Ungefilterte URLs werden für alle Benutzer zugelassen. Ausgenommen sind Benutzer, für die der Kategoriefilter "Alles sperren" oder ein Filter für die Zugriffsbeschränkung gilt. (siehe *Ungefilterte URLs definieren*, Seite 194).
- URLs, die anderen Kategorien zugeordnet wurden, wurden von der Kategorie der Stammdatenbank in eine andere in Websense definierte oder benutzerdefinierte Kategorie übernommen (siehe *URLs anderen Kategorien zuordnen*, Seite 195).

Eine URL, die einer anderen Kategorie zugeordnet wurde, wird nicht standardmäßig blockiert. Die URL wird nach der Aktion gefiltert, die ihrer neuen Kategorie in jedem aktiven Kategoriefilter zugeordnet ist.

Wenn eine Site nach ihrer Kategorie in der Stammdatenbank gefiltert wird, gleicht die Websense-Software die URL mit der entsprechenden IP-Adresse ab. Dies geschieht nicht bei benutzerdefinierten URLs. Um zu ändern, wie eine Site gefiltert wird, definieren Sie sowohl die URL als auch die IP-Adresse als benutzerdefinierte URL.

Wenn über mehrere URLs auf eine Site zugegriffen werden kann, definieren Sie jede dieser URLs als benutzerdefinierte URL, um sicherzustellen, dass die Site wie gewünscht zugelassen oder gesperrt wird.

Wenn eine Site auf eine neue Domain umgezogen ist und Benutzer über eine HTTP-Umleitung zur neuen URL geleitet werden, wird die neue URL nicht automatisch so gefiltert, wie die Site, von der umgeleitet wurde. Erstellen Sie eine neue, benutzerdefinierte URL, um sicherzustellen, dass die neue Adresse angemessen gefiltert wird.

Ungefilterte URLs definieren

Verwandte Themen:

- *Arbeiten mit Kategorien*, Seite 186
- *Filter für bestimmte Sites neu definieren*, Seite 193
- *URLs anderen Kategorien zuordnen*, Seite 195

Über die Seite **Richtlinienverwaltung > Filterkomponenten > Ungefilterte URLs** können Sie eine Liste der Sites definieren, auf die jeder Benutzer zugreifen kann. Ausgenommen sind Benutzer, für die der Kategoriefilter "Alles sperren" oder ein Filter für die Zugriffsbeschränkung gilt.

In der Liste **Zugelassene Sites** im rechten Bereich des Inhaltsfensters werden die ungefilterten Sites (URLs und IP-Adressen) und die regulären Ausdrücke angezeigt, die Sie definiert haben (siehe *Reguläre Ausdrücke verwenden*, Seite 208). Jede Site ist einer Kategorie zugeordnet.

- Die URL kann einer Kategorie der Stammdatenbank oder einer anderen Kategorie zugeordnet werden.
- Wenn ein Benutzer auf eine ungefilterte URL zugreifen möchte, wird die Anforderung als zugelassene benutzerdefinierte URL in der Kategorie protokolliert, der sie zugeordnet ist.

So fügen Sie eine ungefilterte URL hinzu:

1. Geben Sie unter **Ungefilterte URLs definieren** eine URL oder IP-Adresse pro Zeile ein, und klicken Sie auf den nach rechts weisenden Pfeil (>).

   Die Websense-Software gleicht eine benutzerdefinierte URL nicht mit der entsprechenden IP-Adresse ab. Um sowohl die URL als auch die IP-Adresse für eine Site zuzulassen, fügen Sie beide zur Liste "Ungefilterte URLs" hinzu.

2. Klicken Sie auf **Erweitert**, um reguläre Ausdrücke hinzuzufügen, mit denen mehrere Sites abgeglichen werden. Geben Sie einen regulären Ausdruck pro Zeile ein. Klicken Sie dann auf den nach rechts weisenden Pfeil, um die Ausdrücke in die Liste "Ungefilterte URLs" zu übernehmen. Klicken Sie auf **Testen**, um zu überprüfen, ob ein Muster auf die gewünschten Sites zutrifft.

   Ausführliche Informationen finden Sie unter *Reguläre Ausdrücke verwenden*, Seite 208.

3. Wenn Sie alle Eingaben vorgenommen haben, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Kehren Sie dann zur Seite "Kategorien bearbeiten" zurück. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Um eine Site aus der Liste "Ungefilterte URLs" zu entfernen, wählen Sie die URL, IP-Adresse oder den regulären Ausdruck und klicken Sie auf **Löschen**.

URLs anderen Kategorien zuordnen

Verwandte Themen:

- *Arbeiten mit Kategorien*, Seite 186
- *Filter für bestimmte Sites neu definieren*, Seite 193
- *Ungefilterte URLs definieren*, Seite 194

Über die Seite **Richtlinienverwaltung > Filterkomponenten > Kategorien bearbeiten > URLs anderen Kategorien zuordnen** können Sie jeder Kategorie individuelle Sites zuordnen. Auf der Seite **URLs bearbeiten** können Sie Änderungen an vorhandenen Sites vornehmen, die anderen Kategorien zugeordnet wurden.

Ordnen Sie URLs anderen Kategorien zu, damit individuelle Sites anders gefiltert und protokolliert werden. Beachten Sie Folgendes, wenn Sie Sites hinzufügen, die anderen Kategorien zugeordnet wurden:

- Geben Sie jede URL oder IP-Adresse in eine separate Zeile ein.
- Fügen Sie für alle Nicht-HTTP-Sites das Protokoll hinzu. Wurde kein Protokoll eingegeben, filtert die Websense-Software die Site als HTTP-Site.

  Geben Sie für HTTP-Sites auch die Portnummern ein (https://63.212.171.196:443/, https://www.onlinebanking.com:443/).
- Die Websense-Software erkennt benutzerdefinierte URLs genau so, wie sie eingegeben wurden. Wenn die Kategorie "Suchmaschinen und Portale" gesperrt wurde, **www.yahoo.com** jedoch einer zugelassenen Kategorie zugeordnet wurde, wird die Site nur dann zugelassen, wenn der Benutzer die vollständige Adresse eingibt. Wenn ein Benutzer "images.search.yahoo.com" oder "just yahoo.com" eingibt, wird die Site weiterhin gesperrt. Wenn Sie jedoch **yahoo.com** einer anderen Kategorie zuordnen, werden alle Sites zugelassen, deren Adressen "yahoo.com" enthalten.

Wenn Sie Sites hinzugefügt oder bearbeitet haben, die anderen Kategorien zugeordnet wurden, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Kehren Sie dann zur Seite "Kategorien bearbeiten" zurück. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Verwenden Sie nach der Speicherung der URLs, die einer anderen Kategorie zugeordnet wurden, das Tool **URL-Kategorie** im rechten Teilfenster für Verknüpfungen, um zu überprüfen, ob die Site der korrekten Kategorie zugeordnet wurde. Siehe *Filterverhalten mit der Toolbox überprüfen*, Seite 209.

Arbeiten mit Protokollen

Die Websense-Stammdatenbank enthält Protokolldefinitionen, mit denen andere Internetprotokolle als HTTP, HTTPS und FTP gefiltert werden. Zu diesen Definitionen gehören Internetanwendungen und Datenübertragungsmethoden wie Sofortnachrichten, Streaming Media, gemeinsame Nutzung von Dateien, Datentransfer, Internet-E-Mail sowie andere Netzwerk- und Datenbankoperationen.

Mit diesen Protokolldefinitionen können selbst Protokolle und Anwendungen gefiltert werden, die an der Firewall vorbei Ports verwenden, die normalerweise von HTTP-Datenverkehr genutzt werden. Daten von Sofortnachrichten können beispielsweise in ein Netzwerk gelangen, das Protokolle von Sofortnachrichten sperrt, indem die Sofortnachrichten einen HTTP-Port nutzen. Die Websense-Software identifiziert diese Protokolle und filtert sie entsprechend der von Ihnen konfigurierten Richtlinien.

> **Hinweis**
> Network Agent wird aufgefordert, die protokollbasierte Filterung zu aktivieren.

Sie können zusätzlich zu den in Websense definierten Protokolldefinitionen benutzerdefinierte Protokolle für die Filterung festlegen. Definitionen von benutzerdefinierten Protokollen können auf IP-Adressen oder Portnummern basieren und bearbeitet werden.

Um Verkehr über einen bestimmten Port zu sperren, ordnen Sie der Portnummer ein benutzerdefiniertes Protokoll zu, und weisen Sie dem Protokoll eine der Standardaktionen für **Sperren** zu.

Um mit benutzerdefinierten Protokolldefinitionen zu arbeiten, gehen Sie auf **Richtlinienverwaltung > Filterkomponenten**, und klicken Sie auf **Protokolle**. Weitere Informationen finden Sie unter *Benutzerdefinierte Protokolle bearbeiten*, Seite 198, und *Ein benutzerdefiniertes Protokoll erstellen*, Seite 201.

Protokolle filtern

Verwandte Themen:

- *Arbeiten mit Protokollen*, Seite 196
- *Benutzerdefinierte Protokolle bearbeiten*, Seite 198
- *Ein benutzerdefiniertes Protokoll erstellen*, Seite 201
- *Protokollkennungen hinzufügen oder bearbeiten*, Seite 199
- *Elemente zu einem in Websense definierten Protokoll hinzufügen*, Seite 202

Wenn Network Agent installiert wurde, kann die Websense-Software Internetinhalte sperren, die über bestimmte Ports übermittelt werden, bestimmte IP-Adressen verwenden oder durch bestimmte Signaturen markiert sind, unabhängig von der Beschaffenheit der Daten. Durch die Sperrung eines Ports werden standardmäßig sämtliche Internetinhalte abgefangen, die sonst über diesen Port in Ihr Netzwerk gelangen würden, unabhängig von ihrer Quelle.

Hinweis

Gelegentlich wird interner Netzwerkverkehr über einen bestimmten Port nicht gesperrt, obwohl das Protokoll gesperrt ist, das den Port verwendet. Das Protokoll kann über einen internen Server Daten schneller senden, als Network Agent diese erfassen und verarbeiten kann. Dies trifft auf Daten, die von außerhalb des Netzwerks stammen, nicht zu.

Wenn ein Protokoll angefordert wird, geht die Websense-Software wie folgt vor, um zu entscheiden, ob die Anforderung gesperrt oder zugelassen wird:

1. Bestimmen des Protokollnamens oder des Namens der Internetanwendung.
2. Identifizieren des Protokolls basierend auf der angeforderten Zieladresse.
3. Suchen nach verknüpften Portnummern oder IP-Adressen in den Definitionen der benutzerdefinierten Protokolle.
4. Suchen nach verknüpften Portnummern, IP-Adressen oder Signaturen in den in Websense definierten Protokolldefinitionen.

Wenn die Websense-Software diese Informationen nicht ermitteln kann, werden alle dem Protokoll zugeordneten Inhalte zugelassen.

Benutzerdefinierte Protokolle bearbeiten

Verwandte Themen:

- *Arbeiten mit Protokollen*, Seite 196
- *Ein benutzerdefiniertes Protokoll erstellen*, Seite 201
- *Erstellen von Protokollfiltern*
- *Bearbeiten eines Protokollfilters*
- *Arbeiten mit Kategorien*

Über die Seite **Richtlinienverwaltung > Filterkomponenten > Protokolle bearbeiten** können Sie benutzerdefinierte Protokolldefinitionen erstellen und bearbeiten sowie in Websense definierte Protokolldefinitionen überprüfen. Von Websense definierte Protokolle können nicht bearbeitet werden.

In der Liste "Protokolle" sind alle benutzerdefinierten und von Websense definierten Protokolle enthalten. Klicken Sie auf ein Protokoll oder eine Protokollgruppe, um Informationen über das ausgewählte Element im rechten Bereich des Inhaltsfensters anzuzeigen.

Um ein neues, benutzerdefiniertes Protokoll hinzuzufügen, klicken Sie auf **Protokoll hinzufügen**, und fahren Sie mit *Ein benutzerdefiniertes Protokoll erstellen*, Seite 201 fort.

So bearbeiten Sie eine Protokolldefinition:

1. Wählen Sie das Protokoll aus der Liste "Protokolle" aus. Die Protokolldefinition wird rechts neben der Liste angezeigt.
2. Klicken Sie auf **Aktion ändern**, um die Filteraktion zu ändern, die diesem Protokoll in allen Protokollfiltern zugewiesen ist (siehe *Globale Änderungen an Protokollfiltern vornehmen*, Seite 200).
3. Klicken Sie auf **Kennung hinzufügen**, um zusätzliche Protokollkennungen für dieses Protokoll hinzuzufügen (siehe *Protokollkennungen hinzufügen oder bearbeiten*, Seite 199).
4. Wählen Sie eine Kennung aus der Liste aus, und klicken Sie auf **Bearbeiten**, um den **Port**, den **IP-Adressbereich** oder die **Transportmethode** zu ändern, die durch diese Kennung definiert werden.
5. Wenn Sie fertig sind, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Um eine Protokolldefinition zu löschen, klicken Sie auf das Element in der Liste "Protokolle" und anschließend auf **Löschen**.

Protokollkennungen hinzufügen oder bearbeiten

Über die Seite **Filterkomponenten > BearbeitenProtokolle > Protokollkennung hinzufügen** können Sie zusätzliche Protokollkennungen für ein vorhandenes benutzerdefiniertes Protokoll hinzufügen. Über die Seite **Protokollkennung bearbeiten** können Sie Änderungen an einer zuvor definierten Kennung vornehmen.

Überprüfen Sie, ob der korrekte Protokollname neben **Ausgewähltes Protokoll** angezeigt wird, bevor Sie eine Kennung erstellen oder bearbeiten.

Denken Sie bei der Arbeit mit Protokollkennungen daran, dass mindestens ein Kriterium für jedes Protokoll eindeutig sein muss (Port, IP-Adresse oder Transportmethode).

1. Legen Sie fest, welche **Ports** in dieser Kennung enthalten sein sollen.
   - Wenn Sie **Alle Ports** auswählen, überschneidet sich das Kriterium mit anderen Ports oder IP-Adressen, die in die Protokolldefinitionen eingegeben werden.
   - Portbereiche gelten nicht als eindeutig, wenn sie sich überschneiden. Dies ist z. B. der Fall, wenn sich der Portbereich 80-6000 mit dem Portbereich 4000-9000 überschneidet.
   - Gehen Sie vorsichtig vor, wenn Sie ein Protokoll für die Ports 80 oder 8080 definieren. Network Agent wartet auf Internetanforderungen über diese Ports.

     Benutzerdefinierte Protokolle haben eine höhere Priorität als in Websense definierte Protokolle. Wenn Sie also ein benutzerdefiniertes Protokoll definieren, dass Port 80 verwendet, werden alle anderen Protokolle, die Port 80 verwenden, wie benutzerdefinierte Protokolle gefiltert und protokolliert.
2. Legen Sie fest, welche **IP-Adressen** in dieser Kennung enthalten sein sollen.
   - Wenn Sie das Kriterium **Alle externen IP-Adressen** auswählen, überschneidet sich das Kriterium mit allen anderen IP-Adressen, die in andere Protokolldefinitionen eingegeben wurden.
   - IP-Adressbereiche gelten nicht als eindeutig, wenn sie sich überschneiden.
3. Legen Sie fest, welche **Protokolltransport**methode in der Kennung enthalten sein soll.
4. Klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Kehren Sie dann zur Seite "Protokolle bearbeiten" zurück. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Ein benutzerdefiniertes Protokoll umbenennen

Über die Seite **Filterkomponenten > Protokolle bearbeiten > Protokoll umbenennen** können Sie den Namen eines benutzerdefinierten Protokolls ändern oder das Protokoll in eine andere Protokollgruppe übernehmen.

- Über das Feld **Name** können Sie den Protokollnamen bearbeiten. Der neue Name darf maximal 50 Zeichen lang sein.

Der Name darf keines der folgenden Zeichen enthalten:

```
* < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
```

- Um das Protokoll in eine andere Protokollgruppe zu übernehmen, wählen Sie die neue Gruppe im Feld **In Gruppe** aus.

Klicken Sie auf **OK**, wenn Sie die Änderungen abgeschlossen haben, und kehren Sie zur Seite "Protokolle bearbeiten" zurück. Durch das Klicken auf **OK** auf der Seite "Protokolle bearbeiten" werden die Änderungen im Cache zwischengespeichert.

Globale Änderungen an Protokollfiltern vornehmen

Über die Seite **Filterkomponenten > Protokolle bearbeiten > Aktion ändern** können Sie ändern, wie ein Protokoll in allen vorhandenen Protokollfiltern gefiltert wird. Hiermit wird auch die Standardaktion festgelegt, die in neuen Filtern auf das Protokoll angewendet wird.

Diese Änderung setzt die Filteraktion außer Kraft, die dem Protokoll in allen vorhandenen Protokollfiltern zugeordnet ist. Administratoren können diese Filter jedoch später bearbeiten, um eine andere Aktion zuzuordnen.

1. Überprüfen Sie, ob der korrekte Protokollname neben **Ausgewähltes Protokoll** angezeigt wird.
2. Wählen Sie eine neue **Aktion** ("Zulassen" oder "Sperren"), die auf dieses Protokoll angewendet werden soll. Standardmäßig ist **Keine Änderung** ausgewählt. Weitere Informationen finden Sie unter *Filteraktionen*, Seite 47.
3. Legen Sie neue Optionen für die **Protokollierung** fest. Datenverkehr auf bestimmten Protokollen muss protokolliert werden, damit er in Berichten angezeigt werden kann und Alerts zur Nutzung von Protokollen aktiviert werden können.
4. Legen Sie fest, ob **Bandwidth Optimizer** verwendet werden soll, um den Zugriff auf dieses Protokoll zu verwalten. Weitere Informationen finden Sie unter *Bandbreite mit Bandwidth Optimizer verwalten*, Seite 203.

   Wichtig

   Die hier vorgenommenen Änderungen wirken sich auf alle vorhandenen Protokollfilter auf, ausgenommen auf die Filter **Alles sperren** und **Alles zulassen**.

5. Klicken Sie auf **OK**, wenn Sie die Änderungen abgeschlossen haben, und kehren Sie zur Seite "Protokolle bearbeiten" zurück (siehe *Benutzerdefinierte Protokolle bearbeiten*, Seite 198). Durch das Klicken auf **OK** auf der Seite "Protokolle bearbeiten" werden die Änderungen im Cache zwischengespeichert.

Ein benutzerdefiniertes Protokoll erstellen

Verwandte Themen:

- *Arbeiten mit Protokollen*, Seite 196
- *Protokolle filtern*, Seite 197
- *Benutzerdefinierte Protokolle bearbeiten*, Seite 198
- *Elemente zu einem in Websense definierten Protokoll hinzufügen*, Seite 202

Über die Seite **Filterkomponenten > Protokolle > Protokoll hinzufügen** können Sie ein neues, benutzerdefiniertes Protokoll definieren.

1. Geben Sie einen **Namen** für das Protokoll ein.

   Der Name darf keines der folgenden Zeichen enthalten:

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Einem benutzerdefinierten Protokoll kann der gleiche Name wie einem in Websense definierten Protokoll zugewiesen werden, um die Anzahl der IP-Adressen oder Ports zu erhöhen, die dem ursprünglichen Protokoll zugeordnet ist. Weitere Informationen finden Sie unter *Elemente zu einem in Websense definierten Protokoll hinzufügen*, Seite 202.
2. Erweitern Sie die Dropdownliste **Protokoll zu dieser Gruppe hinzufügen**, und wählen Sie eine Protokollgruppe. Das neue Protokoll wird in allen Protokolllisten und -filtern in dieser Gruppe angezeigt.
3. Legen Sie eine eindeutige **Protokollkennung** (Satz aus **Ports**, **IP-Adressen** und **Transportmethoden**) für diese Gruppe fest. Sie können später von der Seite "Protokolle bearbeiten" aus zusätzliche Kennungen hinzufügen.

   Befolgen Sie folgende Anweisungen, um Protokollkennungen zu erstellen:

   - Mindestens ein Kriterium muss für jede Protokolldefinition eindeutig sein (Port, IP-Adresse oder Transportmethode).
   - Wenn Sie die Kriterien **Alle Ports** oder **Alle externen IP-Adressen** auswählen, überschneiden sich diese Kriterien mit allen anderen Ports oder IP-Adressen, die in andere Protokolldefinitionen eingegeben wurden.
   - Port- oder IP-Adressbereiche gelten nicht als eindeutig, wenn sie sich überschneiden. Dies ist z. B. der Fall, wenn sich der Portbereich 80-6000 mit dem Portbereich 4000-9000 überschneidet.

   Hinweis

   Gehen Sie vorsichtig vor, wenn Sie ein Protokoll für die Ports 80 oder 8080 definieren. Network Agent wartet auf Internetanforderungen über diese Ports.

   Benutzerdefinierte Protokolle haben eine höhere Priorität als in Websense definierte Protokolle. Wenn Sie also ein benutzerdefiniertes Protokoll definieren, dass Port 80 verwendet, werden alle anderen Protokolle, die Port 80 verwenden, wie benutzerdefinierte Protokolle gefiltert und protokolliert.

In der folgenden Tabelle sind Beispiele von gültigen und ungültigen Protokolldefinitionen aufgeführt:

Port	IP- Adresse	Transportmethode	Zugelassene Kombination?
70	ALLE	TCP	Ja – durch die Portnummer wird jede Protokollkennung eindeutig.
90	ALLE	TCP	

Port	IP- Adresse	Transportmethode	Zugelassene Kombination?
70	ALLE	TCP	Nein – die IP-Adressen sind nicht eindeutig. 10.2.1.201 ist im Satz "ALLE" enthalten.
70	10.2.1.201	TCP	

Port	IP- Adresse	Transportmethode	Zugelassene Kombination?
70	10.2.3.212	TCP	Ja – die IP-Adressen sind eindeutig.
70	10.2.1.201	TCP	

4. Legen Sie unter "Standardfilteraktion" die Standardaktion fest, die diesem Protokoll in allen aktiven Protokollfiltern zugewiesen werden soll (**Zulassen** oder **Sperren**):
   - Legen Sie fest, ob Datenverkehr, der dieses Protokoll verwendet, **protokolliert** werden soll. Datenverkehr auf bestimmten Protokollen muss protokolliert werden, damit er in Berichten angezeigt werden kann und Alerts zur Nutzung von Protokollen aktiviert werden können.
   - Geben Sie an, ob dieses Protokoll vom **Bandwidth Optimizer** verwaltet werden soll (siehe *Bandbreite mit Bandwidth Optimizer verwalten*, Seite 203).
5. Klicken Sie auf **OK**, wenn Sie die Änderungen abgeschlossen haben, und kehren Sie zur Seite "Protokolle bearbeiten" zurück. Die neuen Protokolldefinitionen werden in der Liste "Protokolle" angezeigt.
6. Klicken Sie erneut auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Elemente zu einem in Websense definierten Protokoll hinzufügen

Sie können einem in Websense definierten Protokoll nicht direkt eine Portnummer oder IP-Adresse hinzufügen. Sie können jedoch ein benutzerdefiniertes Protokoll mit demselben Namen wie das in Websense definierte Protokoll erstellen und die Ports und IP-Adressen zu dessen Definition hinzufügen.

Wenn ein benutzerdefiniertes Protokoll und ein in Websense definiertes Protokoll denselben Namen haben, sucht die Websense-Software an den Ports und IP-Adressen beider Definitionen nach Datenverkehr auf bestimmten Protokollen.

In Berichten erhalten benutzerdefinierte Protokolle das Präfix "C_". Wenn Sie beispielsweise ein benutzerdefiniertes Protokoll für SQL_NET erstellt und zusätzliche Portnummern festgelegt haben, wird in den Berichten C_SQL_NET angezeigt, wenn das Protokoll die Portnummern des benutzerdefinierten Protokolls verwendet.

Bandbreite mit Bandwidth Optimizer verwalten

Verwandte Themen:

- *Arbeiten mit Kategorien*, Seite 186
- *Arbeiten mit Protokollen*, Seite 196
- *Die Standardgrenzwerte für Bandwidth Optimizer konfigurieren*, Seite 204

Wenn Sie einen Kategorie- oder Protokollfilter erstellt haben, können Sie den Zugriff auf eine Kategorie oder ein Protokoll basierend auf der Bandbreitennutzung beschränken.

- Sperren Sie den Zugriff auf Kategorien oder Protokolle basierend auf der gesamten Bandbreitennutzung im Netzwerk.
- Sperren Sie den Zugriff auf Kategorien basierend auf der gesamten Bandbreitennutzung durch HTTP-Datenverkehr.
- Sperren Sie den Zugriff auf ein bestimmtes Protokoll basierend auf der Bandbreitennutzung durch das Protokoll.

Zum Beispiel:

- Sperren Sie das AOL Instant Messaging-Protokoll, wenn die gesamte Bandbreitennutzung im Netzwerk 50 % der verfügbaren Bandbreite oder die aktuelle Bandbreitennutzung des AOL Instant Messaging-Protokolls 10 % der gesamten Netzwerkbandbreite überschreitet.
- Sperren Sie die Kategorie "Sport", wenn die gesamte Bandbreitennutzung im Netzwerk 75 % erreicht, oder die Bandbreitennutzung des gesamten HTTP-Datenverkehrs 60 % der verfügbaren Netzwerkbandbreite erreicht.

Die Protokollbandbreitennutzung umfasst den Datenverkehr über alle Ports, IP-Adressen oder Signaturen, die für das Protokoll definiert wurden. Wenn also ein Protokoll oder eine Internetanwendung mehrere Ports für die Datenübertragung verwendet, wird der gesamte Datenverkehr über alle in den Protokolldefinitionen enthaltenen Ports hinweg zur Protokollbandbreitennutzung gezählt. Wenn eine Internetanwendung einen Port verwendet, der nicht in der Protokolldefinition

enthalten ist, wird der Datenverkehr über diesen Port nicht zur Protokollbandbreitennutzung gezählt.

Die Websense-Software zeichnet die Bandbreitennutzung durch gefilterte TCP- und UDP-basierte Protokolle auf.

Websense Inc. aktualisiert die Websense-Protokolldefinitionen regelmäßig, um sicherzustellen, dass die Bandbreitenmessung korrekt ist.

Network Agent sendet Daten zur Netzwerkbandbreite in vorgegebenen Abständen an Filtering Service. Dadurch wird sichergestellt, dass die Websense-Software die Bandbreitennutzung genau überwacht und Messdaten erhält, die dem Durchschnitt am nächsten kommen.

Wenn bandbreitenbasierte Filteroptionen aktiv sind, beginnt die Websense-Software die bandbreitenbasierte Filterung 10 Minuten nach der ersten Konfiguration und 10 Minuten nach jedem Neustart des Websense Policy Servers. Durch diese Verzögerung wird die genaue Messung der Bandbreitendaten und die Verwendung dieser Daten bei der Filterung sichergestellt.

Wenn eine Anforderung wegen Bandbreitenbeschränkungen gesperrt wurde, zeigt Websense Informationen dazu im Feld **Grund** an. Weitere Informationen finden Sie unter *Sperren von Seiten*, Seite 89.

Die Standardgrenzwerte für Bandwidth Optimizer konfigurieren

Verwandte Themen:

- *Bearbeiten eines Kategoriefilters*, Seite 53
- *Bearbeiten eines Protokollfilters*, Seite 56
- *Bandbreite mit Bandwidth Optimizer verwalten*, Seite 203

Überprüfen Sie den standardmäßig eingestellten Schwellenwert für die Bandbreite, bei dem bandbreitenbasierte Filtereinstellungen in Kraft treten, bevor Sie Bandbreiteneinstellungen in Richtlinien festlegen. Die in Websense definierten Werte sind:

- Standardbandbreite für Netzwerk: **50 %**
- Standardbandbreite pro Protokoll: **20 %**

Die Werte für die Standardbandbreite werden vom Policy Server gespeichert und von allen zugeordneten Instanzen des Network Agent umgesetzt. Wenn Sie über mehrere Policy Server verfügen, wirken sich Änderungen der Standardbandbreite auf einem Policy Server nicht auf die anderen Policy Server aus.

So ändern Sie die Werte für Standardbandbreiten:

1. Wechseln Sie in Websense Manager zu **Einstellungen > Filterung**.

2. Geben Sie die Grenzwerte für die Bandbreitennutzung ein, bei denen bei aktivierter Bandbreitenfilterung die bandbreitenbasierte Filterung in Kraft treten soll.
   - Der Wert **Standardbandbreite für Netzwerk** stellt den Standardschwellenwert dar, zu dem eine Kategorie oder ein Protokoll gesperrt wird, basierend auf dem Datenverkehr im gesamten Netzwerk.
   - Der Wert **Standardbandbreite pro Protokoll** stellt den Standardschwellenwert dar, zu dem eine Kategorie oder ein Protokoll gesperrt wird, basierend auf dem durch das Protokoll verursachten Datenverkehr.

   Sie können die Standardschwellenwerte für jede Kategorie oder jedes Protokoll in jedem Kategorie- oder Protokollfilter außer Kraft setzen.
3. Wenn Sie fertig sind, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Alle Änderungen an den Standardwerten können sich potentiell auf alle Kategorie- und Protokollfilter auswirken, die Beschränkungen von Bandwidth Optimizer umsetzen.

- Bearbeiten Sie die aktiven Protokollfilter, um die Bandbreitennutzung zu verwalten, die einem bestimmten Protokoll zugeordnet ist.
- Bearbeiten Sie die aktiven Kategoriefilter, um die Bandbreitennutzung zu verwalten, die einer bestimmten URL-Kategorie zugeordnet ist.

  Wenn Sie Kategorien basierend auf der Bandbreitennutzung durch HTTP-Datenverkehr filtern, misst die Websense-Software die gesamte Bandbreitennutzung durch HTTP-Datenverkehr über alle in der Websense-Software als HTTP-Ports definierte Ports hinweg.

Datenverkehr basierend auf Dateitypen verwalten

Wenn Sie einen Kategoriefilter erstellen, können Sie die Filterung auf den Dateierweiterungen basieren und den Zugriff auf bestimmte Dateitypen von Sites in bestimmten Kategorien beschränken. Sie können zum Beispiel die Kategorie "Sport" zulassen, aber Videodateien von Sites der Kategorie "Sport" sperren.

Die Websense-Software stellt verschiedene, vordefinierte Dateitypen oder Zusammenstellungen von Dateierweiterungen bereit, die für ähnliche Zwecke verwendet werden. Diese Dateitypdefinitionen werden in der Stammdatenbank gepflegt und können im Zuge der Aktualisierung der Stammdatenbank geändert werden.

Sie können die Filterung entsprechend der vordefinierten Dateitypen implementieren, die vorhandenen Definitionen der Dateitypen ändern oder neue Dateitypen erstellen. Beachten Sie jedoch, dass Sie keine in Websense definierten Dateitypen oder diesen Dateitypen zugeordnete Dateierweiterungen löschen können.

Wenn ein Benutzer eine Site anfordert, ermittelt die Websense-Software zunächst die Kategorie der Site und überprüft dann die Dateierweiterung.

> **Hinweis**
> Wenn Sie eine vollständige Filterung von Video- und Audiodateien aus dem Internet implementieren wollen, kombinieren Sie die protokollbasierte Filterung mit der Filterung von Dateitypen. In diesem Fall bearbeitet die Protokollfilterung die Streaming Media. Die Filterung nach Dateitypen bearbeitet Dateien, die heruntergeladen und abgespielt werden können.

Wenn ein Benutzer versucht auf eine Datei zuzugreifen, deren Erweiterung gesperrt ist, wird auf der Sperrseite in Websense im Feld **Grund** angezeigt, dass der Dateityp gesperrt wurde. Weitere Informationen finden Sie unter *Sperren von Seiten*, Seite 89.

> **Hinweis**
> Die Standardsperrseite wird nicht angezeigt, wenn eine gesperrte GIF- oder JPEG-Datei nur ein Bestandteil einer zugelassenen Seite ist. Der Bereich des Bildes wird leer angezeigt. Dadurch wird verhindert, dass kleine Teile von Sperrseiten in mehreren Bereichen einer ansonsten zugelassenen Seite angezeigt werden.

Die Definitionen der Dateitypen können so viele oder so wenige Dateierweiterungen enthalten, wie für die Filterzwecke sinnvoll ist. In Websense definierte Dateitypen umfassen z. B. folgende Dateierweiterungen:

Audio	Komprimierte Dateien		Ausführbare Dateien	Video	
.aif	.ace	.mim	.bat	.asf	.mpg
.aifc	.arc	.rar	.exe	.asx	.mpv2
.aiff	.arj	.tar		.avi	.qt
.m3u	.b64	.taz		.ivf	.ra
.mid	.bhx	.tgz		.m1v	.ram
.midi	.cab	.tz		.mov	.wm
.mp3	.gz	.uu		.mp2	.wmp
.ogg	.gzip	.uue		.mp2v	.wmv
.rmi	.hqx	.xxe		.mpa	.wmx
.snd	.iso	.z		.mpe	.wxv
.wav	.jar	.zip			
.wax	.lzh				
.wma					

Alle Dateierweiterungen, die einem in Websense definierten Dateityp zugeordnet sind, können zu einem benutzerdefinierten Dateityp hinzugefügt werden. Die Dateierweiterung wird dann entsprechend der Einstellungen gefiltert und protokolliert, die dem benutzerdefinierten Dateityp zugeordnet sind.

Gehen Sie auf **Richtlinienverwaltung > Filterkomponenten,** und klicken Sie auf **Dateitypen**, um die vorhandenen Definitionen von Dateitypen anzuzeigen, Dateitypen zu bearbeiten oder benutzerdefinierte Dateitypen zu erstellen. Weitere Informationen finden Sie unter *Mit Dateitypen arbeiten*, Seite 207.

Mit Dateitypen arbeiten

Verwandte Themen:

- *Datenverkehr basierend auf Dateitypen verwalten*, Seite 205
- *Bearbeiten eines Kategoriefilters*, Seite 53
- *Filtern einer Site*, Seite 85

Über die Seite **Richtlinienverwaltung > Filterkomponenten > Bearbeiten Dateitypen** können Sie bis zu 32 **Dateitypen** erstellen und verwalten. Bei Dateitypen handelt es sich um Gruppen von Dateierweiterungen, die in Kategoriefiltern explizit gesperrt werden können (siehe *Datenverkehr basierend auf Dateitypen verwalten*, Seite 205).

- Klicken Sie auf einen Dateityp, um die zugehörige Dateierweiterung anzuzeigen.
- Klicken Sie auf **Erweiterungen hinzufügen**, um Dateierweiterungen zum ausgewählten Dateityp hinzuzufügen. Befolgen Sie anschließend die Anweisungen unter *Dateierweiterungen zu einem Dateitypen hinzufügen*, Seite 208.
- Klicken Sie auf **Dateityp hinzufügen**, um einen neuen Dateityp zu erstellen. Befolgen Sie anschließend die Anweisungen unter *Benutzerdefinierte Dateitypen hinzufügen*, Seite 208.
- Um benutzerdefinierte Dateitypen oder -erweiterungen zu löschen, wählen Sie das Element aus, und klicken Sie auf **Löschen**.

  Sie können keine in Websense definierten Dateitypen oder diesen Dateitypen zugeordnete Dateierweiterungen löschen.

  Sie können jedoch Dateierweiterungen, die einem in Websense definierten Dateityp zugeordnet ist, zu einem benutzerdefiniertem Dateityp hinzufügen. Die Dateierweiterung wird dann entsprechend der Einstellungen gefiltert und protokolliert, die dem benutzerdefinierten Dateityp zugeordnet sind. Sie können dieselbe Dateierweiterung nicht mehreren benutzerdefinierten Dateitypen zuordnen.

Klicken Sie auf **OK**, wenn Sie die Änderungen an den Dateitypdefinitionen abgeschlossen haben. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Benutzerdefinierte Dateitypen hinzufügen

Über die Seite **Filterkomponenten > Dateitypen bearbeiten > Dateityp hinzufügen** können Sie benutzerdefinierte Dateitypen hinzufügen.

1. Geben Sie einen eindeutigen **Namen des Dateityps** ein.

   Sie können benutzerdefinierte Dateitypen mit demselben Namen wie ein in Websense definierter Dateityp erstellen, um zum vorhandenen Dateityp zusätzliche Dateierweiterungen hinzuzufügen.
2. Geben Sie in die Liste **Dateierweiterungen** eine Dateierweiterung pro Zeile ein. Sie müssen den Punkt (.) vor jeder Erweiterung nicht eingeben.
3. Klicken Sie auf **OK**, um zur Seite "Dateitypen bearbeiten" zurückzukehren. Die neuen Dateitypen werden in der Liste "Dateitypen" angezeigt.
4. Wenn Sie die Arbeit an den Dateitypdefinitionen abgeschlossen haben, klicken Sie auf der Seite "Dateitypen bearbeiten" auf **OK**. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Dateierweiterungen zu einem Dateitypen hinzufügen

Über die Seite **Filterkomponenten > Dateitypen bearbeiten > Dateierweiterungen hinzufügen** können Sie Dateierweiterungen zu den ausgewählten Dateitypen hinzufügen.

1. Überprüfen Sie, ob der gewünschte Dateityp neben **Ausgewählter Dateityp** angezeigt wird.
2. Geben Sie in die Liste **Dateierweiterungen** eine Dateierweiterung pro Zeile ein. Sie müssen den Punkt (.) vor jeder Erweiterung nicht eingeben.
3. Klicken Sie auf **OK**, um zur Seite "Dateitypen bearbeiten" zurückzukehren. Die neuen Dateierweiterungen werden in der Liste "Benutzerdefinierte Dateierweiterungen" angezeigt.
4. Wenn Sie die Arbeit an den Dateitypdefinitionen abgeschlossen haben, klicken Sie auf der Seite "Dateitypen bearbeiten" auf **OK**. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Reguläre Ausdrücke verwenden

Ein **regulärer Ausdruck** ist eine Vorlage oder ein Muster, die bzw. das zum Abgleichen mehrerer Zeichenfolgen oder Gruppen von Zeichen verwendet wird. Sie können reguläre Ausdrücke bei Filtern für die Zugriffsbeschränkung verwenden, oder um benutzerdefnierte URLs oder Schlüsselworte zu definieren. Beim Filtern versucht die Websense-Software, das allgemeine (und nicht das spezifische) Muster mit einer einzelnen URL oder einem Schlüsselwort abzugleichen.

Nachfolgend sehen Sie einen einfachen regulären Ausdruck:

```
domain.(com|org|net)
```

Dieser Ausdruck passt zu folgenden URLs:

- domain.com
- domain.org
- domain.net

Setzen Sie reguläre Ausdrücke sehr sorgfältig ein. Sie stellen ein wirkungsvolles Filtertool dar. Durch reguläre Ausdrücke können jedoch auch Sites gesperrt oder zugelassen werden, bei denen dies nicht erwünscht ist. Ein schlecht ausgewählter regulärer Ausdruck kann zu beträchtlichem Filteraufwand führen.

> **Wichtig**
> Wenn Sie reguläre Ausdrücke als Filterkriterium verwenden, kann die CPU-Auslastung ansteigen. In Tests hat sich gezeigt, dass die durchschnittliche CPU-Auslastung des Computers mit Filtering Service durch 100 reguläre Ausdrücke um 20 % steigt.

Die Websense-Software unterstützt die meisten regulären Ausdrücke in der Perl-Syntax. Es gibt jedoch einige Ausnahmen. Teile der nicht unterstützten Syntax sind für das Abgleichen von Zeichenfolgen, wie sie in URLs vorkommen, nicht von Nutzen.

Zur nicht unterstützten Syntax von regulären Ausdrücken gehört:

```
(?<=pattern)string
\N{name}
(?(condition)pat1)
(?(condition)pat1|pat2)
(?{code})
(?<!pattern)string
(?imsx-imsx)
\pP
\PP
??{code})
```

Weitere Informationen zu regulären Ausdrücken finden Sie unter:

en.wikipedia.org/wiki/Regular_expression

www.regular-expressions.info/

Filterverhalten mit der Toolbox überprüfen

Das rechte Teilfenster für Verknüpfungen in Websense Manager enthält eine **Toolbox**, mit der Sie Ihre Filtereinrichtung schnell überprüfen können.

Klicken Sie auf den Namen eines Tools, um auf dieses zuzugreifen. Klicken Sie erneut auf den Namen, um die Liste der Tools anzuzeigen. Weitere Informationen zur Verwendung von Tools finden Sie unter:

- *URL-Kategorie*, Seite 210
- *Richtlinie überprüfen*, Seite 210

- *Filtertest*, Seite 211
- *URL-Zugriff*, Seite 211
- *Benutzer untersuchen*, Seite 211

Klicken Sie alternativ auf **Unterstützungsportal**, um in einer neuen Registerkarte oder einem neuen Fenster Ihres Browsers auf die Website für technischen Support von Websense zuzugreifen. Sie können auf dem Unterstützungsportal über die Knowledge Base auf Lerntexte, Tipps, Artikel und Dokumentationen zugreifen.

URL-Kategorie

So finden Sie heraus, wie eine Site aktuell kategorisiert ist:

1. Klicken Sie in der Toolbox auf **URL-Kategorie**.
2. Geben Sie eine URL oder IP-Adresse ein.
3. Klicken Sie auf **Los**.

Die aktuelle Kategorie der Site wird in einem Popup-Fenster angezeigt. Falls Ihr Unternehmen die URL einer anderen Kategorie zugeordnet hat, wird die neue Kategorie angezeigt.

Die Kategorisierung der Site ist abhängig von der Version der verwendeten Stammdatenbank (einschließlich Aktualisierungen in Echtzeit).

Richtlinie überprüfen

Mit diesem Tool können Sie ermitteln, welche Richtlinie für einen bestimmten Client gilt. Die Ergebnisse gelten für den aktuellen Tag und die aktuelle Uhrzeit.

1. Klicken Sie in der Toolbox auf **Richtlinie überprüfen**.
2. Um einen Verzeichnis- oder Computer-Client zu identifizieren, geben Sie eine der folgenden Informationen ein:
   - Einen vollständig qualifizierten Benutzernamen

     Klicken Sie auf **Benutzer suchen**, um das Verzeichnis nach einem Benutzer zu durchsuchen (siehe *Einen Benutzer für die Tools "Richtlinie überprüfen" oder "Filtertest" identifizieren*, Seite 212).
   - Eine IP-Adresse
3. Klicken Sie auf **Los**.

Der Name von einer oder mehreren Richtlinien wird in einem Popup-Fenster angezeigt. Mehrere Richtlinien werden nur dann angezeigt, wenn dem Benutzer selbst keine Richtlinie zugewiesen wurde, jedoch mehreren Gruppen, Domänen oder Organisationseinheiten, zu denen der Benutzer gehört.

Selbst wenn mehrere Richtlinien angezeigt werden, wird zu jedem Zeitpunkt nur eine Richtlinie für einen Benutzer umgesetzt (siehe *Filterreihenfolge*, Seite 84).

Filtertest

So finden Sie heraus, was geschieht, wenn ein bestimmter Client eine bestimmte Site anfordert.

1. Klicken Sie in der Toolbox auf **Filtertest**.
2. Um einen Verzeichnis- oder Computer-Client zu identifizieren, geben Sie eine der folgenden Informationen ein:
   - Einen vollständig qualifizierten Benutzernamen

     Klicken Sie auf **Benutzer suchen**, um das Verzeichnis nach einem Benutzer zu durchsuchen (siehe *Einen Benutzer für die Tools "Richtlinie überprüfen" oder "Filtertest" identifizieren*, Seite 212).
   - Eine IP-Adresse
3. Geben Sie die URL oder IP-Adresse der Site ein, die Sie überprüfen möchten.
4. Klicken Sie auf **Los**.

In einem Popup-Fenster werden die Kategorie der Site, die zugehörige Filteraktion und der Grund für die Aktion angezeigt.

URL-Zugriff

So zeigen Sie an, ob Benutzer innerhalb der vergangenen zwei Wochen bis einschließlich des aktuellen Datums auf die Seite zugreifen wollten:

1. Klicken Sie in der Toolbox auf **URL-Zugriff**.
2. Geben Sie die vollständige URL oder IP-Adresse der Site ein, die Sie überprüfen möchten, oder Teile davon.
3. Klicken Sie auf **Los**.

In einem Untersuchungsbericht wird angezeigt, ob auf die Site zugegriffen wurde. War dies der Fall, wird der Zeitpunkt angezeigt.

Sie können mit diesem Tool nach Erhalt eines Sicherheits-Alerts überprüfen, ob Ihr Unternehmen Sites mit bösartigen Inhalten ausgesetzt war (Phishing, Viren).

Benutzer untersuchen

So überprüfen Sie den Verlauf der Internetnutzung eines Client in den vergangenen zwei Wochen, ausschließlich des aktuellen Datums:

1. Klicken Sie in der Toolbox auf **Benutzer untersuchen**.
2. Geben Sie den vollständigen Namen oder die IP-Adresse des Computers ein, oder Teile davon.
3. Klicken Sie auf **Los**.

In einem Untersuchungsbericht wird der Verlauf der Internetnutzung des Clients angezeigt.

Einen Benutzer für die Tools "Richtlinie überprüfen" oder "Filtertest" identifizieren

Über die Seite **Benutzer suchen** können Sie einen Benutzerclient (Verzeichnisclient) für die Tools "Richtlinie überprüfen" oder "Filtertest" identifizieren.

Wenn die Seite geöffnet wird, ist die Option **Benutzer** ausgewählt. Erweitern Sie den Ordner **Verzeichniseinträge**, um das Verzeichnis zu durchsuchen, oder klicken Sie auf **Suchen**. Die Suchfunktion ist nur dann verfügbar, wenn Sie einen LDAP-basierten Verzeichnisdienst verwenden.

So durchsuchen Sie das Verzeichnis nach einem Benutzer:

1. Geben Sie den vollständigen **Namen** des Benutzers ein oder Teile davon.
2. Erweitern Sie den Ordner **Verzeichniseinträge**, und identifizieren Sie einen Suchkontext.

   Klicken Sie auf einen Ordner (DC, OU oder CN) in der Baumstruktur, um den Kontext festzulegen. Hierdurch wird ein Feld unter der Baumstruktur ausgefüllt.
3. Klicken Sie auf **Suchen**. Einträge, die zu Ihrem Suchbegriff passen, werden unter **Suchergebnisse** aufgeführt.
4. Klicken Sie auf einen Benutzernamen oder auf **Erneut suchen**, um einen neuen Suchbegriff oder -kontext einzugeben.

   Klicken Sie auf **Suche abbrechen**, um zur Suche im Verzeichnis zurückzukehren.
5. Wenn der richtige, vollständig qualifizierte Benutzername im Feld **Benutzer** angezeigt wird, klicken Sie auf **Los**.

Wenn Sie das Tool "Filtertest" verwenden, stellen Sie sicher, dass eine URL oder IP-Adresse im Feld **URL** angezeigt wird, bevor Sie auf **Los** klicken.

Klicken Sie auf **IP-Adresse**, um einen Computer-Client und statt eines Benutzers zu identifizieren.

10 Benutzeridentifikation:

Die Websense-Software muss den Benutzer, der eine Site anfordert, anhand der ursprünglichen IP-Adresse identifizieren können. Erst dann kann die Software auf Benutzer und Gruppen Richtlinien anwenden. Es sind verschiedene Identifikationsmethoden verfügbar:

- Ein Integrationsgerät oder eine Integrationsanwendung identifizieren und authentifizieren die Benutzer und leiten die Benutzerinformationen an die Websense-Software weiter. Weitere Informationen finden Sie im *Installationshandbuch*.
- In Websense arbeitet ein Agent für die transparente Identifikation im Hintergrund, um mit einem Verzeichnisdienst zu kommunizieren und Benutzer zu identifizieren (siehe *Transparente Identifikation*).
- Die Websense-Software fordert Benutzer auf, ihre Netzwerk-Anmeldeinformationen einzugeben und sich anzumelden, wenn sie einen Webbrowser verwenden (siehe *Manuelle Authentifizierung*, Seite 215).

Transparente Identifikation

Verwandte Themen

- *Manuelle Authentifizierung*, Seite 215
- *Methoden für die Benutzeridentifikation konfigurieren*, Seite 216

Mit **transparente Identifikation** wird jede von der Websense-Software verwendete Methode beschrieben, mit der Benutzer in Ihrem Verzeichnisdienst identifiziert werden, ohne dass von ihnen Anmeldeinformationen angefordert werden. Dazu gehören die Integration der Websense-Software mit Geräten oder Anwendungen, die Benutzerinformationen zur Verwendung in der Filterung bereitstellen, oder der Einsatz von optionalen Agenten für die transparente Identifikation in Websense.

- Websense *DC Agent*, Seite 225,wird zusammen mit einem Windows-basierten Verzeichnisdienst verwendet. Der Agent fragt Domänencontroller periodisch nach Sitzungen mit Benutzeranmeldung ab, um den Anmeldestatus zu überprüfen. Zu diesem Zweck fragt der Agent auch Clientcomputer ab. Der Agent wird auf einem

Windows-Server ausgeführt und kann in jeder Domäne eines Netzwerks installiert werden.

- Websense *Logon Agent*, Seite 229, identifiziert Benutzer bei der Anmeldung bei Windows-Domänen. Der Agent wird auf einem Linux- oder Windows-Server ausgeführt, die mit dem Agenten zusammenhängende Anmeldeanwendung jedoch nur auf Windows-Computern.
- Websense *RADIUS Agent*, Seite 232, kann zusammen mit einem Windows- oder LDAP-basierten Verzeichnisdienst verwendet werden. Der Agent arbeitet mit einem RADIUS-Server und -Client zusammen, um Benutzer zu identifizieren, die sich von fernen Standorten aus anmelden.
- Websense *eDirectory Agent*, Seite 237, wird zusammen mit Novell eDirectory verwendet. Der Agent nutzt die Authentifizierung über Novell eDirectory, um Benutzer IP-Adressen zuzuordnen.

Anleitungen zur Installation der Agenten finden Sie im *Installationshandbuch*. Agenten können eigenständig aber auch in bestimmten Kombinationen eingesetzt werden (siehe *Mehrere Agenten konfigurieren*, Seite 244).

Hinweiss

Wenn Sie eine integrierte NetCache-Anwendung verwenden, muss NetCache die Benutzernamen in WinNT-, LDAP- oder RADIUS-Format an die Websense-Software senden, damit die transparente Identifikation ordnungsgemäß funktioniert.

Wenn Sie über einen Proxy-Server verfügen und einen Agenten für die transparente Identifikation einsetzen, ist die anonyme Authentifizierung beim Proxy Server empfehlenswert.

Die allgemeinen Einstellungen für die Benutzeridentifikation und die spezifischen Agenten für die transparente Identifikation werden im Websense Manager konfiguriert. Klicken Sie im linken Teilfenster für Navigation auf die Registerkarte **Einstellungen** und anschließend auf **Benutzeridentifikation**.

Ausführliche Anleitungen zur Konfiguration finden Sie unter *Methoden für die Benutzeridentifikation konfigurieren*, Seite 216.

In einigen Fällen kann die Websense-Software die Benutzerinformationen nicht von einem Agenten für die transparente Identifikation erhalten. Dies ist der Fall, wenn ein Computer mehr als einem Benutzer zugewiesen wurde, bzw. der Benutzer anonym oder ein Gast ist. Es gibt auch noch andere Gründe. In diesen Fällen können Sie den Benutzer auffordern, sich über den Browser anzumelden (siehe *Manuelle Authentifizierung*, Seite 215).

Transparente Identifikation von Remotebenutzern

In bestimmten Konfigurationen kann die Websense-Software Benutzer transparent identifizieren, die sich von einem fernen Standort aus an Ihrem Netzwerk anmelden.

- Wenn Sie Remote Filtering Server und Remote Filtering Client von Websense einsetzen, kann die Websense-Software alle Remotebenutzer identifizieren, die sich mit zwischengespeicherten Domäne-Anmeldeinformationen über ein Domänenkonto anmelden. Weitere Informationen finden Sie unter *Filtern von Remote Clients*, Seite 167.
- Wenn Sie DC Agent einsetzen und sich Remotebenutzer direkt an benannten Windows-Domänen in Ihrem Netzwerk anmelden, kann DC Agent diese Benutzer identifizieren (siehe *DC Agent*, Seite 225).
- Wenn Sie einen RADIUS-Server zur Authentifizierung von Remotebenutzern verwenden, kann RADIUS Agent diese Benutzer transparent identifizieren, so dass Sie auf Benutzern oder Gruppen basierende Filterrichtlinien anwenden können (siehe *RADIUS Agent*, Seite 232).

Manuelle Authentifizierung

Verwandte Themen

- *Transparente Identifikation*, Seite 213
- *Authentifizierungsregeln für spezifische Computer einrichten*, Seite 218
- *Sichere manuelle Authentifizierung*, Seite 221
- *Methoden für die Benutzeridentifikation konfigurieren*, Seite 216

Die transparente Identifikation ist nicht immer in allen Umgebungen verfügbar oder erwünscht. Mit Hilfe der **manuellen Authentifizierung** können Sie in Unternehmen, die keine transparente Identifikation einsetzen, und in Fällen, in denen keine transparente Identifikation verfügbar ist, Benutzer weiterhin über benutzer- und gruppenbasierte Richtlinien filtern.

Bei der manuellen Authentifizierung werden Benutzer beim ersten Zugriff auf das Internet mit einem Browser aufgefordert, einen Benutzernamen und ein Passwort einzugeben. Die Websense-Software gleicht das Passwort mit einem unterstützten Verzeichnisdienst ab und ruft dann die Richtlinieninformationen für den Benutzer ab.

Sie können die Websense-Software so konfigurieren, dass sie die manuelle Authentifizierung immer dann zulässt, wenn keine transparente Identifikation verfügbar ist (siehe *Methoden für die Benutzeridentifikation konfigurieren*, Seite 216). Sie können alternativ eine Liste spezifischer Computer mit benutzerdefinierten Authentifizierungseinstellungen erstellen, an denen Benutzer beim Öffnen des

Browsers aufgefordert werden, sich anzumelden (siehe *Authentifizierungsregeln für spezifische Computer einrichten*, Seite 218).

Wenn die manuelle Authentifizierung aktiviert ist, erhalten Benutzer unter Umständen HTTP-Fehlermeldungen und können nicht auf das Internet zugreifen. Dies kann folgende Ursachen haben:

- Die Benutzer haben drei Mal das falsche Passwort eingegeben. Der Benutzername oder das Passwort sind ungültig.
- Die Benutzer haben auf **Abbrechen** geklickt, um die Aufforderung zur Authentifizierung zu umgehen.

Wenn die manuelle Authentifizierung aktiviert ist, wird verhindert, dass nicht identifizierbare Benutzer auf das Internet zugreifen.

Methoden für die Benutzeridentifikation konfigurieren

Verwandte Themen

- *Transparente Identifikation*, Seite 213
- *Manuelle Authentifizierung*, Seite 215
- *Arbeiten mit Benutzern und Gruppen*, Seite 66

Über die Seite **Einstellungen > Benutzeridentifikation** können Sie verwalten, wann und wie die Websense-Software versucht, Benutzer im Netzwerk zu identifizieren, um benutzer- oder gruppenbasierte Richtlinien anzuwenden.

- Konfigurieren Sie Policy Server, um mit Agenten für die transparente Identifikation zu kommunizieren.
- Überprüfen und aktualisieren Sie die Einstellungen des Agenten für die transparente Identifikation.
- Legen Sie mit Hilfe einer globalen Regel fest, wie die Websense-Software reagiert, wenn ein Benutzer nicht durch einen Agenten für die transparente Identifikation oder ein Integrationsgerät identifiziert werden kann.
- Identifizieren Sie Computer in Ihrem Netzwerk, für welche die globalen Regeln für die Benutzeridentifikation nicht gelten. Legen Sie fest, ob und wie Benutzer dieser Computer authentifiziert werden sollen.

Wenn Sie Agenten für die transparente Identifikation in Websense verwenden, werden diese Agenten unter **Agenten für die transparente Identifikation** aufgeführt:

- **Server** zeigt die IP-Adresse oder den Namen des Computers an, der als Host für Agenten für die transparente Identifikation dient.
- **Port** zeigt den Port an, den die Websense-Software für die Kommunikation mit dem Agenten verwendet.

- **Typ** zeigt an, ob es sich bei der festgelegten Instanz um DC Agent, Logon Agent, RADIUS Agent oder eDirectory Agent handelt. (Eine Einführung in jeden Agententyp finden Sie unter *Transparente Identifikation*, Seite 213.)

Um einen Agenten hinzuzufügen, wählen Sie einen Agententyp aus der Dropdownliste **Agent hinzufügen**. Klicken Sie auf einen der folgenden Links, um Anleitungen zur Konfiguration zu erhalten:

- *DC Agent konfigurieren*, Seite 226
- *Logon Agent konfigurieren*, Seite 230
- *RADIUS Agent konfigurieren*, Seite 234
- *eDirectory Agent konfigurieren*, Seite 239

Um eine Instanz des Agenten aus der Liste zu entfernen, wählen Sie das Kontrollkästchen neben der Agenteninformation in der Liste und klicken Sie auf **Löschen**.

Legen Sie unter **Zusätzliche Authentifizierungsoptionen** fest, wie die Websense-Software standardmäßig reagieren soll, wenn Benutzer von Agenten, Integrationsgeräten oder -anwendungen nicht transparent identifiziert werden können:

- Klicken Sie auf **Computer- oder Netzwerkrichtlinie anwenden**, um benutzer- oder gruppenbasierte Richtlinien zugunsten von computer- oder netzwerkbasierten Richtlinien oder der Richtlinie "Standard" zu ignorieren.
- Klicken Sie auf **Benutzer zur Eingabe von Anmeldeinformationen auffordern**, um den Benutzer aufzufordern, beim Öffnen des Browsers Anmeldeinformationen einzugeben. Danach können benutzer- und gruppenbasierte Richtlinien angewendet werden (siehe *Manuelle Authentifizierung*, Seite 215).
- Legen Sie den Standarddomänen **kontext** fest, den die Websense-Software immer dann verwenden soll, wenn ein Benutzer zur Eingabe seiner Anmeldeinformationen aufgefordert wird. In dieser Domäne sind die Anmeldeinformationen des Benutzers gültig.

  Wenn Sie über die Liste "Ausnahmen" Computer festlegen, an denen Benutzer aufgefordert werden, Anmeldeinformationen einzugeben, müssen Sie selbst dann einen Standarddomänenkontext festlegen, wenn die globale Regel eine computer- und netzwerkbasierte Richtlinie anwendet.

Nachdem Sie mit einer allgemeinen Regel festgelegt haben, wann und wie Benutzer durch die Websense-Software identifiziert werden sollen, können Sie Ausnahmen für diese Regel erstellen.

Wenn Sie für die Benutzeridentifikation beispielsweise einen Agenten für die transparente Identifikation oder ein Integrationsprodukt verwenden und die manuelle Authentifizierung aktiviert haben, um nicht transparent identifizierbare Benutzer zur Eingabe ihrer Anmeldeinformationen aufzufordern, können Sie spezifische Computer mit folgenden Einstellungen festlegen:

- Benutzer, die nicht identifiziert werden können, werden nie dazu aufgefordert, ihre Anmeldeinformationen einzugeben. Anders formuliert: Wenn die transparente Identifikation fehlschlägt, wird nicht versucht, den Benutzer manuell

zu authentifizieren. Die computer- oder netzwerkbasierte Richtlinie oder die Richtlinie "Standard" wird angewendet.

- Die Benutzerinformation wird auch dann ignoriert, wenn Sie verfügbar ist. Benutzer werden immer dazu aufgefordert, ihre Anmeldeinformationen einzugeben.
- Benutzerinformationen werden immer ignoriert, selbst wenn sie verfügbar sind. Benutzer werden nie aufgefordert, ihre Anmeldeinformationen einzugeben. Die computer- oder netzwerkbasierte Richtlinie oder die Richtlinie "Standard" wird immer angwendet.

Um eine Ausnahme zu erstellen, klicken Sie auf **Ausnahmen**, und lesen Sie den Abschnitt *Authentifizierungsregeln für spezifische Computer einrichten*, Seite 218.

Wenn Sie die Änderungen auf dieser Seite eingegeben haben, klicken Sie zum Speichern auf **OK**. Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen nicht speichern möchten.

Authentifizierungsregeln für spezifische Computer einrichten

Verwandte Themen

- *Methoden für die Benutzeridentifikation konfigurieren*, Seite 216
- *Manuelle Authentifizierung*, Seite 215
- *Sichere manuelle Authentifizierung*, Seite 221

Mit selektiver Authentifizierung können Sie bestimmen, ob Benutzer, die von einem bestimmten Clientcomputer aus auf das Internet zugreifen möchten, aufgefordert werden, ihre Anmeldeinformationen über den Browser einzugeben. Setzen Sie selektive Authentifizierung ein, um:

- andere Authentifizierungsregeln für einen Computer in einem öffentlichen Verkaufsstand festzulegen, als für Mitarbeiter des Unternehmens, die den Verkaufsstand versorgen.
- sicherzustellen, dass Benutzer eines Computers, der sich im Untersuchungszimmer einer Arztpraxis befindet, immer identifizieren müssen, bevor sie auf das Internet zugreifen können.

Computer, die spezielle Einstellungen bei der Benutzeridentifikation anwenden, werden auf der Seite **Einstellungen > Benutzeridentifikation** aufgeführt. Klicken Sie auf **Ausnahmen**, um spezifische Einstellungen der Benutzeridentifikation für einige Computer in Ihrem Netzwerk festzulegen, oder um zu überprüfen, ob für bestimmte Computer spezifische Einstellungen definiert wurden.

Klicken Sie auf **Hinzufügen**, um einen Computer zur Liste hinzuzufügen. Weitere Anweisungen finden Sie unter *Ausnahmen für die Einstellungen der Benutzeridentifikation definieren*, Seite 219.

Wenn Sie Computer oder Netzwerkbereiche zur Liste hinzugefügt haben, klicken Sie auf **OK**. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Ausnahmen für die Einstellungen der Benutzeridentifikation definieren

Verwandte Themen

- *Transparente Identifikation*, Seite 213
- *Manuelle Authentifizierung*, Seite 215
- *Methoden für die Benutzeridentifikation konfigurieren*, Seite 216

Über die Seite **Einstellungen > Benutzeridentifikation > IP-Adressen hinzufügen** können Sie Computer identifizieren, auf die spezifische Regel bei der Benutzeridentifikation angewendet werden sollen.

1. Geben Sie eine **IP-Adresse** oder einen **IP-Adressbereich** ein, um die Computer zu identifizieren, auf welche die spezifische Authentifizierungsmethode angewendet werden soll. Klicken Sie dann auf die Schaltfläche mit dem nach rechts weisenden Pfeil, um die Computer zur Liste **Ausgewählte Objekte** hinzuzufügen.

   Wenn dieselbe Regel auf mehrere Computer angewendet werden soll, fügen Sie alle entsprechenden Computer zur Liste hinzu.
2. Wählen Sie in der Liste **Benutzeridentifikation** einen Eintrag aus, um anzugeben, ob die Websense-Software versuchen soll, Benutzer dieses Computers transparent zu identifizieren.
   - Wählen Sie **Transparente Identifikation des Benutzers versuchen**, um Benutzerinformationen von einem Agenten für die transparente Identifikation oder einem Integrationsgerät anzufordern.
   - Wählen Sie **Benutzerinformationen ignorieren**, um zu verhindern, dass transparente Methoden zur Benutzeridentifikation angewendet werden.
3. Geben Sie an, ob Benutzer aufgefordert werden sollen, Anmeldeinformationen über den Browser einzugeben. Diese Einstellung wird angewendet, wenn Benutzerinformationen nicht verfügbar sind, weil andere Identifikationsmethoden fehlgeschlagen sind oder Benutzerinformationen ignoriert wurden.
   - Wählen Sie **Benutzer zur Eingabe von Anmeldeinformationen auffordern**, um Benutzer zur Eingabe von Anmeldeinformationen aufzufordern.

     Wenn die Option **Transparente Identifikation des Benutzers versuchen** ebenfalls gewählt wurde, erhalten Benutzer die Eingabeaufforderung über den Browser nur dann, wenn sie nicht transparent identifiziert werden konnten.
   - Wählen Sie die Option **Computer- oder Netzwerkrichtlinie anwenden**, um sicherzustellen, dass Benutzer niemals aufgefordert werden, ihre Anmeldeinformationen einzugeben.

Wenn die Option **Transparente Identifikation des Benutzers versuchen** ebenfalls ausgewählt wurde, können Benutzer mit der entsprechenden benutzerbasierten Richtlinie gefiltert werden, deren Anmeldeinformationen transparent verifiziert werden konnten.

4. Klicken Sie auf **OK**, um zur Seite "Benutzeridentifikation" zurückzukehren.
5. Klicken Sie auf **OK**, wenn Sie die Liste "Ausnahmen" aktualisiert haben, um Ihre Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Ausnahmen für die Einstellungen zur Benutzeridentifikation überarbeiten

Verwandte Themen

- *Transparente Identifikation*, Seite 213
- *Manuelle Authentifizierung*, Seite 215
- *Methoden für die Benutzeridentifikation konfigurieren*, Seite 216

Über die Seite **Einstellungen > Benutzeridentifikation > IP-Adressen bearbeiten** können Sie Änderungen an den Einträgen in der Liste "Ausnahmen" vornehmen. Änderungen, die Sie auf dieser Seite vornehmen, wirken sich auf alle über ihre IP-Adresse oder ihren IP-Adressbereich identifizierten Computer aus, die in der Liste "Ausgewählte Objekte" angezeigt werden.

1. Wählen Sie in der Liste **Benutzeridentifikation** einen Eintrag aus, um anzugeben, ob die Websense-Software versuchen soll, Benutzer dieses Computers transparent zu identifizieren.
   - Wählen Sie **Transparente Identifikation des Benutzers versuchen**, um Benutzerinformationen von einem Agenten für die transparente Identifikation oder einem Integrationsgerät anzufordern.
   - Wählen Sie **Benutzerinformationen ignorieren**, um zu verhindern, dass transparente Methoden zur Benutzeridentifikation angewendet werden.
2. Geben Sie an, ob Benutzer aufgefordert werden sollen, Anmeldeinformationen über den Browser einzugeben. Diese Einstellung wird angewendet, wenn Benutzerinformationen nicht verfügbar sind, weil die transparente Identifikation fehlgeschlagen ist oder ignoriert wurde.
   - Wählen Sie **Benutzer zur Eingabe von Anmeldeinformationen auffordern**, um Benutzer aufzufordern, Anmeldeinformationen einzugeben.

     Wenn die Option **Transparente Identifikation des Benutzers versuchen** ebenfalls gewählt wurde, erhalten Benutzer die Eingabeaufforderung über den Browser nur dann, wenn sie nicht transparent identifiziert werden konnten.
   - Wählen Sie die Option **Computer- oder Netzwerkrichtlinie anwenden**, um sicherzustellen, dass Benutzer niemals aufgefordert werden, ihre Anmeldeinformationen einzugeben.

Wenn die Option **Transparente Identifikation des Benutzers versuchen** ebenfalls ausgewählt wurde, können Benutzer mit der entsprechenden benutzerbasierten Richtlinie gefiltert werden, deren Anmeldeinformationen transparent verifiziert werden konnten.

3. Klicken Sie auf **OK**, um zur Seite "Benutzeridentifikation" zurückzukehren.
4. Klicken Sie auf **OK**, wenn Sie die Liste "Ausnahmen" aktualisiert haben, um Ihre Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Sichere manuelle Authentifizierung

Verwandte Themen

- *Methoden für die Benutzeridentifikation konfigurieren*, Seite 216
- *Manuelle Authentifizierung*, Seite 215
- *Authentifizierungsregeln für spezifische Computer einrichten*, Seite 218
- *Sichere manuelle Authentifizierung aktivieren*, Seite 223

Bei der sicheren manuellen Authentifizierung in Websense wird die Secure Sockets Layer (SSL)-Verschlüsselung verwendet, um Authentifizierungsdaten zu schützen, die zwischen den Clientcomputern und der Websense-Software übertragen werden. Ein integrierter SSL-Server in Filtering Service sorgt für die Verschlüsselung von Benutzernamen und Passwörtern, die zwischen Clientcomputern und Filtering Service übertragen werden. Die sichere manuelle Authentifizierung ist standardmäßig deaktiviert.

Hinweis

Die sichere manuelle Authentifizierung kann nicht zusammen mit Remote Filtering eingesetzt werden. Remote Filtering Server kann keine Sperrseiten an Clients übertragen, wenn er einer Filtering Service-Instanz zugeordnet wurde, bei der die sichere manuelle Authentifizierung aktiviert wurde.

Um diese Funktion zu aktivieren, müssen Sie folgende Schritte ausführen:

1. Erstellen Sie SSL-Zertifikate und -Schlüssel, und legen Sie diese an einem Ort ab, auf den die Websense-Software zugreifen kann und von dem die Zertifikate und Schlüssel durch Filtering Service ausgelesen werden können (siehe *Zertifikate und Schlüssel erstellen*, Seite 222).
2. Aktivieren Sie die sichere manuelle Authentifizierung (siehe *Sichere manuelle Authentifizierung aktivieren*, Seite 223) und die sichere Kommunikation mit dem Verzeichnisdienst.

3. Importieren Sie die Zertifikate in den Browser (siehe *Das Zertifikat im Browser des Clients zulassen*, Seite 224).

Zertifikate und Schlüssel erstellen

Verwandte Themen

- *Manuelle Authentifizierung*, Seite 215
- *Authentifizierungsregeln für spezifische Computer einrichten*, Seite 218
- *Sichere manuelle Authentifizierung*, Seite 221
- *Sichere manuelle Authentifizierung aktivieren*, Seite 223
- *Das Zertifikat im Browser des Clients zulassen*, Seite 224

Ein Zertifikat besteht aus einem öffentlichen Schlüssel für die Datenverschlüsselung und einem privaten Schlüssel, mit dem die Daten entschlüsselt werden. Zertifikate werden von einer Zertifizierungsstelle (Certificate Authority – CA) ausgegeben. Sie können von einem internen Zertifikatsserver aus ein Zertifikat erzeugen oder von einem Drittanbieter wie VeriSign ein Client-Zertifikat erhalten.

Die Zertifizierungsstelle, die das Client-Zertifikat ausgibt, muss von der Websense-Software als vertrauenswürdig eingestuft sein. Üblicherweise wird dies durch eine Browsereinstellung bestimmt.

- Informationen zu privaten Schlüsseln, CSRs und Zertifikaten finden Sie unter httpd.apache.org/docs/2.2/ssl/ssl_faq.html#aboutcerts.
- Um mehr über das Erzeugen eigener privater Schlüssel, CSRs und Zertifikate zu erfahren, besuchen Sie die Website www.akadia.com/services/ssh_test_certificate.html.

Sie können viele Tools zum Erzeugen von selbstsignierten Zertifikaten einsetzen, einschließlich OpenSSL-Toolkit. Das Toolkit ist unter www.openssl.org verfügbar.

Gehen Sie unabhängig von der von Ihnen gewählten Methode wie folgt vor:

1. Erzeugen Sie einen privaten Schlüssel (**server.key**).
2. Erzeugen Sie mit dem privaten Schlüssel ein CSR (Certificate Signing Request).

Wichtig

Wenn Sie aufgefordert werden, den Wert "CommonName" einzugeben, geben Sie die IP-Adresse des Computers ein, auf dem Filtering Service ausgeführt wird. Wenn Sie diesen Schritt auslassen, zeigen die Browser des Clients einen Fehler beim Sicherheitszertifikat an.

3. Erstellen Sie mit Hilfe des CSR ein selbstsigniertes Zertifikat (**server.crt**).

4. Speichern Sie die Dateien **server.crt** und **server.key** an einem Ort, auf den die Websense-Software zugreifen kann und an dem die Dateien von Filtering Service ausgelesen werden können.

Sichere manuelle Authentifizierung aktivieren

Verwandte Themen

- *Manuelle Authentifizierung*, Seite 215
- *Authentifizierungsregeln für spezifische Computer einrichten*, Seite 218
- *Sichere manuelle Authentifizierung*, Seite 221
- *Zertifikate und Schlüssel erstellen*, Seite 222
- *Das Zertifikat im Browser des Clients zulassen*, Seite 224

1. Stoppen Sie Websense Filtering Service (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).
2. Navigieren Sie auf dem Computer, auf dem Filtering Service ausgeführt wird, zum Installationsverzeichnis von Websense. Standardmäßig ist dies **C:\Programme \Websense\bin** oder **/opt/Websense/bin/**.
3. Machen Sie die Datei **eimserver.ini** ausfindig, und erstellen Sie eine Sicherungskopie der Datei in einem anderen Verzeichnis.
4. Öffnen Sie die ursprüngliche INI-Datei in einem Texteditor.
5. Machen Sie den Abschnitt **[WebsenseServer]** ausfindig, und fügen Sie folgende Zeile hinzu:

   ```
   SSLManualAuth=on
   ```

6. Fügen Sie unter der vorhergehenden Zeile Folgendes hinzu:

   ```
   SSLCertFileLoc=[path]
   ```

   Ersetzen Sie **[path]** mit dem vollständigen Pfad zum SSL-Zertifikat, einschließlich dem Dateinamen des Zertifikats, z. B. C:\secmanauth\server.crt.
7. Fügen Sie außerdem Folgendes hinzu:

   ```
   SSLKeyFileLoc=[path]
   ```

   Ersetzen Sie **[path]** mit dem vollständigen Pfad zum SSL-Schlüssel, einschließlich dem Dateinamen des Schlüssels, z. B. C:\secmanauth\server.key.
8. Speichern und schließen Sie die Datei **eimserver.ini**.
9. Starten Sie Websense Filtering Service.

Nach dem Start wartet Filtering Service auf Anforderungen über den standardmäßig eingestellten, sicheren HTTP-Port **15872**.

Mit den vorhergehenden Schritten haben Sie die sichere Kommunikation zwischen dem Clientcomputer und der Websense-Software sichergestellt. Um eine sichere Kommunikation zwischen der Websense-Software und dem Verzeichnisdienst

sicherzustellen, vergewissern Sie sich, dass auf der Seite **Einstellungen > Verzeichnisdienste** die Option **SSL verwenden** gewählt wurde. Ausführliche Informationen erhalten Sie unter *Erweiterte Verzeichniseinstellungen*, Seite 70.

Das Zertifikat im Browser des Clients zulassen

Verwandte Themen

- *Manuelle Authentifizierung*, Seite 215
- *Authentifizierungsregeln für spezifische Computer einrichten*, Seite 218
- *Sichere manuelle Authentifizierung*, Seite 221
- *Zertifikate und Schlüssel erstellen*, Seite 222
- *Sichere manuelle Authentifizierung aktivieren*, Seite 223

Wenn Sie das erste Mal mit einem Browser zu einer Website navigieren, zeigt der Browser eine Warnmeldung zum Sicherheitszertifikat an. Installieren Sie das Zertifikat im Zertifikatsspeicher, um diese Warnmeldung in Zukunft zu vermeiden.

Microsoft Internet Explorer (Version 7)

1. Öffnen Sie den Browser, und navigieren Sie zu einer Website.

   In einer Warnmeldung wird angezeigt, dass ein Problem mit dem Sicherheitszertifikat besteht.
2. Klicken Sie auf **Laden dieser Website fortsetzen (nicht empfohlen)**.

   Wenn Sie aufgefordert werden, sich zu authentifizieren, klicken sie auf **Abbrechen**.
3. Klicken Sie auf das Feld **Zertifikatfehler** rechts neben der Adressleiste im oberen Bereich des Browserfensters. Klicken Sie anschließend auf **Zertifikate anzeigen**.
4. Klicken Sie auf der Registerkarte "Allgemein" im Dialogfeld "Zertifikat" auf **Zertifikat installieren**.
5. Wählen Sie **Zertifikatspeicher automatisch auswählen (auf dem Zertifikatstyp basierend)**, und klicken Sie auf **Weiter**.
6. Klicken Sie auf **Fertig stellen**.
7. Klicken Sie auf **Ja**, wenn Sie gefragt werden, ob das Zertifikat installiert werden soll.

Die Benutzer erhalten keine weiteren Warnmeldungen zur Zertifikatssicherheit, die mit Filtering Service auf diesem Computer zusammenhängen.

Mozilla Firefox (Version 2.x)

1. Öffnen Sie den Browser, und navigieren Sie zu einer Website.

   Eine Warnmeldung wird angezeigt.
2. Klicken Sie auf **Dieses Zertifikat immer akzeptieren**.

3. Geben Sie Ihre Anmeldeaufforderungen ein, wenn Sie dazu aufgefordert werden.
4. Gehen Sie auf **Extras > Einstellungen** und anschließend auf **Erweitert**.
5. Gehen Sie auf die Registerkarte **Verschlüsselung**, und klicken Sie auf **Zertifikate anzeigen**.
6. Wählen Sie die Registerkarte **Websites**, und vergewissern Sie sich, dass das Zertifikat aufgeführt wird.

Die Benutzer erhalten keine weiteren Warnmeldungen zur Zertifikatssicherheit, die mit Filtering Service auf diesem Computer zusammenhängen.

Mozilla Firefox (Version 3.x)

1. Öffnen Sie den Browser, und navigieren Sie zu einer Website.

   Eine Warnmeldung wird angezeigt.
2. Klicken Sie auf **Oder Sie können eine Ausnahme hinzufügen**.
3. Klicken Sie auf **Ausnahme hinzufügen**.
4. Stellen Sie sicher, dass die Option **Diese Ausnahme dauerhaft speichern** ausgewählt ist, und klicken Sie anschließend auf **Sicherheits-Ausnahmeregel bestätigen**.

Die Benutzer erhalten keine weiteren Warnmeldungen zur Zertifikatssicherheit, die mit Filtering Service auf diesem Computer zusammenhängen.

DC Agent

Verwandte Themen

- *Transparente Identifikation*, Seite 213
- *DC Agent konfigurieren*, Seite 226
- *Verschiedene Einstellungen für eine Instanz eines Agenten konfigurieren*, Seite 246

Websense DC Agent wird unter Windows ausgeführt und erkennt Benutzer in einem Windows-Netzwerk, in dem NetBIOS-, WINS- oder DNS-Netzwerkdienste ausgeführt werden.

DC Agent und User Service sammeln Netzwerkbenutzerdaten und senden diese an Websense Filtering Service. Die Geschwindigkeit der Datenübertragung wird durch mehrere Variablen bestimmt, einschließlich der Größe Ihres Netzwerks und des Umfangs des vorhandenen Netzwerkdatenverkehrs.

So aktivieren Sie die transparente Identifikation mit DC Agent:

1. Installieren Sie DC Agent. Weitere Informationen finden Sie im Installationshandbuch im Abschnitt zur separaten Installation der Websense-Komponenten.

   Hinweis

   Führen Sie DC Agent mit Domänenadministratorberechtigungen aus. Das Domänenadministratorkonto muss auf dem Computer, auf dem DC Agent ausgeführt wird, zur Administratorengruppe gehören.

   Dies ist erforderlich, damit DC Agent vom Domänencontroller Anmeldeinformationen von Benutzern abrufen kann. Wenn Sie DC Agent nicht mit Domänenadministratorberechtigung installieren können, konfigurieren Sie nach der Installation Administratorberechtigungen für diese Dienste. Weitere Informationen finden Sie unter *Die Websense-Software wendet keine Benutzer- oder Gruppenrichtlinien an*, Seite 388.

2. Konfigurieren Sie DC Agent, damit er mit anderen Websense-Komponenten und den Domänencontrollern in Ihrem Netzwerk kommuniziert (siehe *DC Agent konfigurieren*).
3. Fügen Sie zu filternde Benutzer und Gruppen mit Websense Manager hinzu (siehe *Hinzufügen eines Clients*, Seite 73).

Die Websense-Software kann Benutzer dazu auffordern, sich zu identifizieren, wenn DC Agent die Benutzer nicht transparent identifizieren kann. Weitere Informationen finden Sie unter *Manuelle Authentifizierung*, Seite 215.

DC Agent konfigurieren

Verwandte Themen:

- *Transparente Identifikation*
- *Manuelle Authentifizierung*
- *Methoden für die Benutzeridentifikation konfigurieren*
- *DC Agent*
- *Mehrere Agenten konfigurieren*

Über die Seite **Einstellungen > Benutzeridentifikation > DC Agent** können Sie eine neue Instanz von DC Agent und die globalen Einstellungen konfigurieren, die auf alle Instanzen von DC Agent angewendet werden.

Um eine neue Instanz von DC Agent hinzuzufügen, stellen Sie zunächst die allgemeinen Informationen bereit: wo der Agent installiert wurde und wie Filtering Service mit diesem kommunizieren soll. Diese Einstellungen können für jede Instanz des Agenten eindeutig sein.

1. Geben Sie unter "Basiskonfiguration für Agenten" die IP-Adresse und den Namen des **Servers** ein, auf dem der Agent installiert wurde.

   Hinweis

   Namen von Computern müssen mit einem Buchstaben (a-z) beginnen. Sie dürfen nicht mit einem numerischen oder Sonderzeichen beginnen.

   Namen von Computern, die bestimmte erweiterte ASCII-Zeichen enthalten, können unter Umständen nicht ordnungsgemäß aufgelöst werden. Wenn Sie eine nicht-englische Version der Websense-Software verwenden, geben Sie statt des Computernamens eine IP-Adresse ein.

2. Geben Sie den **Port** ein, den DC Agent verwenden soll, um mit anderen Websense-Komponenten zu kommunizieren. Der Standardwert ist 30600.
3. Wählen Sie das Kontrollkästchen **Authentifizierung aktivieren**, und geben Sie anschließend das **Passwort** für die Verbindung ein, um eine authentifizierte Verbindung zwischen Filtering Service und DC Agent herzustellen.

Passen Sie als nächstes die globalen Einstellungen für die Kommunikation mit DC Agent, die Fehlerbehebung, die Abfragen von Domänencontrollern und Computern an. Standardmäßig wirken sich alle hier vorgenommenen Änderungen auf alle Instanzen von DC Agent aus. Mit einem Stern (*) markierte Einstellungen können in der Konfigurationsdatei eines Agenten außer Kraft gesetzt werden, um das Verhalten der Instanz des Agenten anzupassen (siehe *Verschiedene Einstellungen für eine Instanz eines Agenten konfigurieren*, Seite 246).

1. Geben Sie unter Kommunikation mit DC Agent den **Kommunikationsport** ein, der für die Kommunikation zwischen DC Agent und anderen Websense-Komponenten verwendet werden soll. Der Standardwert ist 30600.

   Nehmen Sie nur dann Änderungen an den Einstellungen des **Diagnose-Ports** vor, wenn Sie von der technischen Unterstützung von Websense dazu aufgefordert werden. Der Standardwert ist 30601.
2. Markieren Sie unter "Abfrage von Domänencontrollern" die Option **Abfragen von Domänencontrollern aktivieren**, damit DC Agent den Domänencontroller nach Sitzungen mit Benutzeranmeldung abfragen kann.

   Sie können in der Konfigurationsdatei des Agenten festlegen, welche Domänencontroller jede Instanz von DC Agent abfragt. Ausführliche Informationen erhalten Sie unter *Mehrere Agenten konfigurieren*, Seite 244.
3. Im Feld **Abfrageintervall** können Sie festlegen, in welchen Abständen (in Sekunden) DC Agent Domänencontroller abfragen soll.

   Wenn Sie die Abfrageintervalle verkürzen, können Sitzungen mit Benutzeranmeldung genauer erfasst werden. Der allgemeine

Netzwerkdatenverkehr wird hierdurch jedoch erhöht. Wenn Sie die Abfrageintervalle vergrößern, wird der Netzwerkdatenverkehr zwar reduziert, die Erfassung einiger Sitzungen mit Benutzeranmeldung verzögert sich jedoch oder wird verhindert. Der Standardwert beträgt 10 Sekunden.

4. Mit dem Feld **Zeitüberschreitungslimit für Benutzereinträge** können Sie festlegen, in welchen Abständen (in Stunden) DC Agent die Benutzereinträge in seinen Zuordnungen aktualisiert. Der Standardwert beträgt 24 Stunden.
5. Wählen Sie das Kontrollkästchen **Computerabfrage aktivieren**, damit DC Agent Computer nach Sitzungen mit Benutzeranmeldung abfragt. Dazu können Computer außerhalb der Domäne gehören, die der Agent bereits abfragt.

   DC Agent verwendet WMI (Windows Management Instruction) für das Abfragen von Computern. Wenn Sie das Abfragen von Computern aktiviert haben, konfigurieren Sie die Windows Firewall auf den Clientcomputern so, dass die Kommunikation über Port **135** zugelassen wird.
6. Legen Sie ein **Intervall für die Überprüfung von Benutzerzuordnungen** fest, nach dem DC Agent Clientcomputer abfragt, um zu überprüfen, welche Benutzer angemeldet sind. Der Standardwert beträgt 15 Minuten.

   DC Agent vergleicht die Abfrageresultate mit den Paaren aus Benutzernamen und IP-Adressen in der Benutzerzuordnung, die er an Filtering Service sendet. Wenn Sie dieses Intervall verkürzen, werden die Benutzerzuordnungen genauer. Der Netzwerkdatenverkehr erhöht sich jedoch. Wenn Sie dieses Intervall vergrößern, wird der Netzwerkdatenverkehr zwar reduziert, die Zuordnungen werden jedoch ungenauer.
7. Geben Sie ein **Zeitüberschreitungslimit für Benutzereinträge** ein, mit dem festgelegt wird, wie oft DC Agent die durch Abfragen der Computer erfassten Einträge in der Benutzerzuordnung aktualisiert. Der Standardwert beträgt 1 Stunde.

   DC Agent entfernt alle Einträge aus Benutzernamen und IP-Adresse, die älter als das Zeitüberschreitungslimit sind, und die DC Agent nicht als momentan angemeldet ermitteln kann. Wenn Sie dieses Intervall vergrößern, wird die Benutzerzuordnung ungenauer, weil die Zuordnung alte Benutzernamen für einen längeren Zeitraum beibehält.

   Hinweis

   Geben Sie für das Zeitüberschreitungslimit für Benutzereinträge einen größeren Wert ein, als für das Intervall für die Überprüfung von Benutzerzuordnungen. Andernfalls können Benutzernamen aus den Benutzerzuordnungen entfernt werden, bevor diese verifiziert wurden.
8. Klicken Sie auf **OK**, um Ihre Änderungen sofort zu speichern und zu implementieren.

Logon Agent

Verwandte Themen:

- *Transparente Identifikation*, Seite 213
- *Logon Agent konfigurieren*, Seite 230
- *Verschiedene Einstellungen für eine Instanz eines Agenten konfigurieren*, Seite 246

Websense Logon Agent identifiziert Benutzer bei der Anmeldung bei Domänen in Echtzeit. Dadurch wird verhindert, dass Benutzeranmeldungen nicht erfasst werden, weil die Abfrageintervalle möglicherweise zu lang sind.

Logon Agent (auch Authentication Server genannt) kann auf einem Computer installiert werden, der Windows oder Linux ausführt. Der Agent arbeitet mit der Anmeldeanwendung von Websense (LogonApp.exe) auf Clientcomputern, auf denen Windows ausgeführt wird, um Benutzer zu identifizieren, die sich an Windows-Domänen anmelden.

In den meisten Fällen genügt es, DC Agent oder Logon Agent einzusetzen. Sie können jedoch auch beide Agenten zusammen einsetzen. In diesem Fall hat Logon Agent Priorität vor DC Agent. DC Agent leitet nur in dem unwahrscheinlichen Fall Daten einer Benutzeranmeldung an Filtering Service weiter, dass Logon Agent ein Ereignis nicht erfasst hat.

Installieren Sie Logon Agent, und stellen Sie dann von einem zentralen Standort aus die Anmeldeanwendung auf den Clientcomputern bereit. Weitere Informationen finden Sie im *Installationshandbuch*.

Konfigurieren Sie den Agenten nach der Installation so, dass dieser mit Clientcomputern und Websense Filtering Service kommuniziert (siehe *Logon Agent konfigurieren*).

Hinweis

Wenn Sie Active Directory (Native Mode) von Windows verwenden und User Service auf einem Computer installiert ist, der Linux ausführt, befolgen Sie die zusätzlichen Konfigurationsschritte unter *User Service unter Linux*, Seite 395.

Logon Agent konfigurieren

Verwandte Themen:

- *Transparente Identifikation*, Seite 213
- *Manuelle Authentifizierung*, Seite 215
- *Methoden für die Benutzeridentifikation konfigurieren*, Seite 216
- *Logon Agent*, Seite 229
- *Mehrere Agenten konfigurieren*, Seite 244

Über die Seite **Einstellungen > Benutzeridentifikation > Logon Agent** können Sie eine neue Instanz von Logon Agent und die globalen Einstellungen konfigurieren, die auf alle Instanzen von Logon Agent angewendet werden.

So fügen Sie eine neue Instanz von Logon Agent hinzu:

1. Geben Sie unter "Basiskonfiguration für Agenten" die IP-Adresse und den Namen des **Servers** ein, auf dem der Agent installiert wurde.

   Hinweis

   Namen von Computern müssen mit einem Buchstaben (a-z) beginnen. Sie dürfen nicht mit einem numerischen oder Sonderzeichen beginnen.

   Namen von Computern, die bestimmte erweiterte ASCII-Zeichen enthalten, können unter Umständen nicht ordnungsgemäß aufgelöst werden. Wenn Sie eine nicht-englische Version der Websense-Software verwenden, geben Sie statt des Computernamens eine IP-Adresse ein.

2. Geben Sie den **Port** ein, den Logon Agent verwenden soll, um mit anderen Websense-Komponenten zu kommunizieren. Der Standardwert ist 30602.
3. Wählen Sie das Kontrollkästchen **Authentifizierung aktivieren**, und geben Sie anschließend das **Passwort** für die Verbindung ein, um eine authentifizierte Verbindung zwischen Filtering Service und Logon Agent herzustellen.
4. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern, oder geben Sie im nächsten Bildschirmabschnitt zusätzliche Konfigurationsinformationen ein.

Passen Sie als nächstes die globalen Einstellungen für die Kommunikation mit Logon Agent an. Standardmäßig wirken sich alle hier vorgenommenen Änderungen auf alle Instanzen von Logon Agent aus.

1. Geben Sie unter "Kommunikation mit Logon Agent" den **Kommunikationsport** ein, der für die Kommunikation zwischen Logon Agent und anderen Websense-Komponenten verwendet werden soll. Der Standardwert ist 30602.

2. Nehmen Sie nur dann Änderungen an den Einstellungen des **Diagnose-Ports** vor, wenn Sie von der technischen Unterstützung von Websense dazu aufgefordert werden. Der Standardwert ist 30603.
3. Legen Sie unter "Kommunikation mit Anmeldeanwendung" den **Verbindungsport** fest, den die Anmeldeanwendung zur Kommunikation mit Logon Agent verwenden soll. Der Standardwert ist 15880.
4. Geben Sie einen Wert bei **Maximal zulässige Anzahl von Verbindungen** ein, den jede Instanz von Logon Agent zulassen soll. Der Standardwert ist 200.

   Wenn Sie über ein großes Netzwerk verfügen, müssen Sie diese Zahl unter Umständen erhöhen. Wenn Sie diese Zahl erhöhen, erhöht sich auch der Netzwerkdatenverkehr.
5. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern, oder geben Sie im nächsten Bildschirmabschnitt zusätzliche Konfigurationsinformationen ein.

Um die Standardeinstellungen zu konfigurieren, mit denen die Gültigkeit der Benutzereinträge bestimmt wird, müssen Sie zunächst ermitteln, ob Logon Agent und die Client-Anmeldeanwendung im **Persistenzmodus** oder im **nicht persistenten Modus** (Standard) arbeiten.

Der nicht persistente Modus wird aktiviert, indem der Parameter /NOPERSIST beim Start von **LogonApp.exe** einbezogen wird. (Weitere Informationen sind in der Datei **LogonApp_ReadMe.txt** verfügbar, die zu Ihrer Installation von Logon Agent gehört.)

- Im Persistenzmodus stellt Logon Agent periodisch einen Kontakt zur Anmeldeanwendung her, um die Informationen zur Benutzeranmeldung zu übertragen.

  Wenn Sie den Persistenzmodus verwenden, legen Sie ein **Abfrageintervall** fest, mit dem bestimmt wird, wie häufig die Anmeldeanwendung Anmeldeinformationen überträgt.

  > **Hinweis**
  > Wenn Sie diesen Wert ändern, tritt die Änderung erst nach Ablauf des vorhergehenden Abfrageintervalls in Kraft. Wenn Sie beispielsweise das Intervall von 15 Minuten auf 5 Minuten verkürzen, muss das 15-Minuten-Intervall zunächst beendet werden, bevor die Abfrage alle 5 Minuten erfolgt.

- Im nicht persistenten Modus sendet die Anmeldeanwendung Informationen zur Benutzeranmeldung nur einmal pro Anmeldung an Logon Agent.

  Wenn Sie den nicht persistenten Modus verwenden, legen Sie einen Zeitraum für die Einstellung **Gültigkeitsablauf für Benutzereinträge** fest. Wenn dieser Wert erreicht wird, wird der Benutzereintrag aus der Benutzerzuordnung entfernt.

Wenn Sie die Änderungen an der Konfiguration vorgenommen haben, klicken Sie zum Speichern Ihrer Einstellungen auf **OK**.

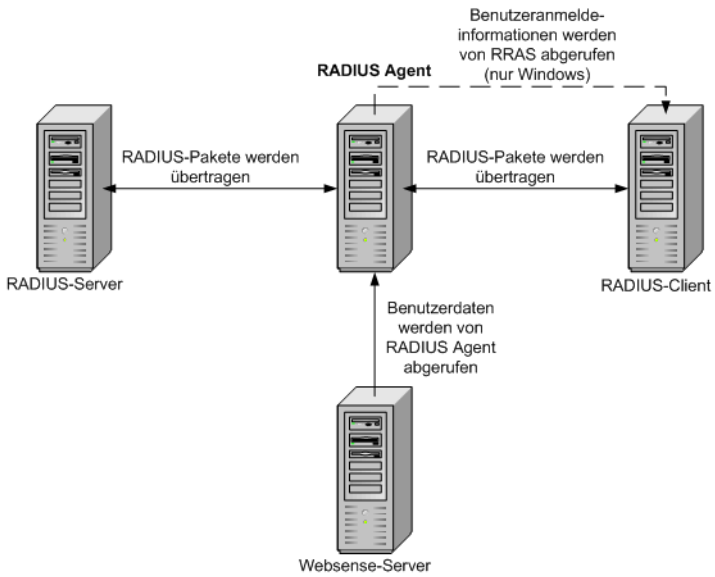
RADIUS Agent

Verwandte Themen:

- *Transparente Identifikation*, Seite 213
- *RADIUS-Datenverkehr verarbeiten*, Seite 233
- *Die RADIUS-Umgebung konfigurieren*, Seite 233
- *RADIUS Agent konfigurieren*, Seite 234
- *Den RADIUS-Client konfigurieren*, Seite 236
- *Den RADIUS-Server konfigurieren*, Seite 237
- *Verschiedene Einstellungen für eine Instanz eines Agenten konfigurieren*, Seite 246

Mit RADIUS Agent von Websense können Sie benutzer- und gruppenbasierte Richtlinien anwenden, wobei die Authentifizierung durch einen RADIUS-Server erfolgt. Mit RADIUS Agent können Sie Benutzer transparent identifizieren, die über Einwahl, VPN, DSL oder einen anderen Fernzugriff auf Ihr Netzwerk zugreifen.

RADIUS Agent arbeitet mit dem RADIUS-Server und RADIUS-Client in Ihrem Netzwerk zusammen, um den Datenverkehr auf dem RADIUS-Protokoll zu verarbeiten und zu verfolgen. RADIUS steht für Remote-Zugriff Dial-In User Service. Hierdurch können Sie lokalen Benutzern oder Gruppen bzw. Benutzern oder Gruppen, die über Fernzugriff auf Ihr Netzwerk zugreifen, bestimmte Filterrichtlinien zuweisen.



Wenn Sie RADIUS Agent installieren, wird der Agent mit den vorhandenen Websense-Komponenten integriert. Sie müssen RADIUS Agent, den RADIUS-Server und den RADIUS-Client dennoch entsprechend konfigurieren (siehe *RADIUS Agent konfigurieren*, Seite 234).

RADIUS-Datenverkehr verarbeiten

RADIUS Agent von Websense fungiert als Proxy, der RADIUS-Nachrichten zwischen einem RADIUS-Client und einem RADIUS-Server bzw. mehreren RADIUS-Clients und -Servern weiterleitet.

RADIUS Agent authentifiziert Benutzer nicht direkt. Der Agent identifiziert Remotebenutzer und ordnet diese IP-Adressen zu, so dass ein RADIUS-Server diese Benutzer authentifizieren kann. Im Idealfall leitet der RADIUS-Server Authentifizierungsanforderungen an einen LDAP-basierten Verzeichnisdienst weiter.

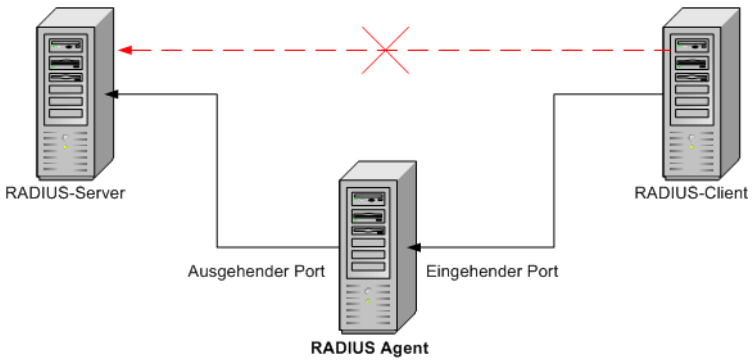
RADIUS Agent speichert Datenpaare aus Benutzernamen und IP-Adressen in einer Benutzerzuordnung. Wenn Ihr RADIUS-Client die Kontoführung oder die Verfolgung von Benutzeranmeldungen unterstützt und die Kontoführung aktiviert ist, sammelt RADIUS Agent aus den erhaltenen RADIUS-Nachrichten mehr Daten über Sitzungen mit Benutzeranmeldung.

Wenn RADIUS Agent von Websense ordnungsgemäß konfiguriert wurde, erfasst und verarbeitet RADIUS Agent alle RADIUS-Protokollpakete der folgenden Typen:

- **Access-Request**: Wird von einem RADIUS-Client gesendet, um die Genehmigung für einen Zugriffsversuch auf das Netzwerk zu erlangen.
- **Access-Accept**: Wird von einem RADIUS-Server als Antwort auf eine Access-Request-Meldung gesendet und meldet dem RADIUS-Client, dass der Verbindungsversuch genehmigt und authentifiziert wurde.
- **Access-Reject**: Wird von einem RADIUS-Server als Antwort auf eine Access-Request-Meldung gesendet und meldet dem RADIUS-Client, dass der Verbindungsversuch abgelehnt wurde.
- **Accounting-Stop-Request**: Wird von einem RADIUS-Client gesendet, um dem RADIUS-Server aufzufordern, die Verfolgung von Benutzeraktivitäten zu stoppen.

Die RADIUS-Umgebung konfigurieren

RADIUS Agent von Websense fungiert als Proxy zwischen einem RADIUS-Client und einem RADIUS-Server. Die Abbildung zeigt eine vereinfachte Übersicht darüber, wie sich der Einsatz von RADIUS Agent von einem standardmäßigen RADIUS-Setup unterscheidet.



Installieren Sie RADIUS Agent und den RADIUS-Server auf verschiedenen Computern. Agent und Server müssen verschiedene IP-Adresse haben und verschiedene Ports verwenden.

Konfigurieren Sie RADIUS Agent nach der Installation in Websense Manager (siehe *RADIUS Agent konfigurieren*, Seite 234). Führen Sie außerdem folgende Schritte durch:

- Konfigurieren Sie den RADIUS-Client (üblicherweise ein Netzzugangsserver), so dass dieser mit RADIUS Agent und nicht direkt mit dem RADIUS-Server kommuniziert.
- Konfigurieren Sie den RADIUS-Server so, dass dieser RADIUS Agent als Proxy verwendet (siehe Dokumentation zum RADIUS-Server). Wenn Sie über mehrere RADIUS-Server verfügen, konfigurieren Sie jeden separat.

Hinweis

Wenn Sie einen Lucent RADIUS-Server und RRAS verwenden, konfigurieren Sie den RADIUS-Server, so dass dieser das PAP-Protokoll (Password Authentication Protocol) verwendet. Konfigurieren Sie den RRAS-Server, so dass dieser nur PAP-Anforderungen zulässt. Weitere Informationen finden Sie in der entsprechenden Produktdokumentation.

RADIUS Agent konfigurieren

Verwandte Themen:

- *Transparente Identifikation*, Seite 213
- *Manuelle Authentifizierung*, Seite 215
- *Methoden für die Benutzeridentifikation konfigurieren*, Seite 216
- *RADIUS Agent*, Seite 232
- *Mehrere Agenten konfigurieren*, Seite 244

Über die Seite **Einstellungen > Benutzeridentifikation > RADIUS Agent** können Sie eine neue Instanz von RADIUS Agent und die globalen Einstellungen konfigurieren, die auf alle Instanzen von RADIUS Agent angewendet werden.

So fügen Sie eine neue Instanz von RADIUS Agent hinzu:

1. Geben Sie unter "Basiskonfiguration für Agenten" die IP-Adresse und den Namen des **Servers** ein, auf dem der Agent installiert wurde.

   > **Hinweis**
   >
   > Namen von Computern müssen mit einem Buchstaben (a-z) beginnen. Sie dürfen nicht mit einem numerischen oder Sonderzeichen beginnen.
   >
   > Namen von Computern, die bestimmte erweiterte ASCII-Zeichen enthalten, können unter Umständen nicht ordnungsgemäß aufgelöst werden. Wenn Sie eine nicht-englische Version der Websense-Software verwenden, geben Sie statt des Computernamens eine IP-Adresse ein.

2. Geben Sie den **Port** ein, den RADIUS Agent verwenden soll, um mit anderen Websense-Komponenten zu kommunizieren. Der Standardwert ist 30800.
3. Wählen Sie das Kontrollkästchen **Authentifizierung aktivieren**, und geben Sie anschließend das **Passwort** für die Verbindung ein, um eine authentifizierte Verbindung zwischen Filtering Service und RADIUS Agent herzustellen.
4. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern, oder geben Sie im nächsten Bildschirmabschnitt zusätzliche Konfigurationsinformationen ein.

Passen Sie als nächstes die globalen Einstellungen für RADIUS Agent an. Standardmäßig wirken sich alle hier vorgenommenen Änderungen auf alle Instanzen von RADIUS Agent aus. Mit einem Stern (*) markierte Einstellungen können in der Konfigurationsdatei eines Agenten außer Kraft gesetzt werden, um das Verhalten der Instanz des Agenten anzupassen (siehe *Verschiedene Einstellungen für eine Instanz eines Agenten konfigurieren*, Seite 246).

1. Geben Sie den **Kommunikationsport** ein, der für die Kommunikation zwischen RADIUS Agent und anderen Websense-Komponenten verwendet werden soll. Der Standardwert ist 30800.
2. Nehmen Sie nur dann Änderungen an den Einstellungen des **Diagnose-Ports** vor, wenn Sie von der technischen Unterstützung von Websense dazu aufgefordert werden. Der Standardwert ist 30801.
3. Geben Sie unter "RADIUS-Server" **IP oder Name des RADIUS-Servers** ein. RADIUS Agent leitet Authentifizierungsanforderungen an den RADIUS-Server weiter und muss den Computer identifizieren können.
4. Wenn Sie Microsoft RRAS verwenden, geben Sie die IP-Adresse des **RRAS-Computers** ein. Die Websense-Software fragt diesen Computer nach Sitzungen mit Benutzeranmeldung ab.
5. Geben Sie einen Wert in das Feld **Zeitüberschreitungslimit für Benutzereinträge** ein, mit dem festgelegt wird, wie oft RADIUS Agent seine Benutzerzuordnung aktualisiert. Unter normalen Umständen ist der standardmäßig eingestellte Wert von 24 Stunden optimal.

6. Mit den Einstellungen **Ports für die Authentifizierung** und **Kontoführungsports** können Sie festlegen, welche Ports RADIUS Agent verwenden soll, um Authentifizierungs- und Kontoführungsanforderungen zu senden und zu empfangen. Sie können für jeden Kommunikationstyp festlegen, welcher Port für die Kommunikation zwischen folgenden Komponenten genutzt werden sollen:
   - RADIUS Agent und RADIUS-Server
   - RADIUS Agent und RADIUS-Client
7. Klicken Sie nach Abschluss auf **OK**, um Ihre Änderungen sofort zu speichern.

Den RADIUS-Client konfigurieren

Konfigurieren Sie den RADIUS-Client so, dass dieser Authentifizierungs- und Kontoführungsanforderungen über RADIUS Agent an den RADIUS-Server übermitteln kann.

Ändern Sie die Konfiguration des RADIUS-Client, so dass folgende Prozesse möglich sind:

- Der RADIUS-Client sendet Authentifizierungsanforderungen an den Computer und Port, auf dem RADIUS Agent auf die Authentifizierungsanforderungen wartet. Dies ist der **Authentifizierungsport**, der während der Konfiguration von RADIUS Agent festgelegt wurde.
- Der RADIUS-Client sendet Kontoführungsanforderungen an den Computer und Port, auf dem RADIUS Agent auf die Kontoführungssanforderungen wartet. Dies ist der **Kontoführungsport**, der während der Konfiguration von RADIUS Agent festgelegt wurde.

Die genaue Vorgehensweise bei der Konfiguration eines RADIUS-Client variiert je nach Clienttyp. Weitere Informationen finden Sie in der Dokumentation zum RADIUS-Client.

Hinweis

In den vom RADIUS-Client gesendeten Authentifizierungs- und Kontoführungsnachrichten müssen die Attribute **User-Name** und **Framed-IP-Address** enthalten sein. RADIUS Agent verwendet diese Attribute, um die Paare aus Benutzernamen und IP-Adressen auszuwerten und zu speichern. Wenn Ihr RADIUS-Client diese Information nicht standardmäßig erzeugt, konfigurieren Sie ihn so, dass er dies tut (siehe Dokumentation zum RADIUS-Client).

Den RADIUS-Server konfigurieren

So gewährleisten Sie die ordnungsgemäße Kommunikation zwischen RADIUS Agent von Websense und dem RADIUS-Server:

- Fügen Sie die IP-Adresse des Computers, auf dem RADIUS Agent ausgeführt wird, zur Client-Liste des RADIUS-Servers hinzu. Weitere Anweisungen finden Sie in der Dokumentation zum RADIUS-Server.
- Definieren Sie geteilte Geheimnisse zwischen dem RADIUS-Server und allen RADIUS-Clients, die den Agenten zur Kommunikation mit dem RADIUS-Server verwenden. Geteilte Geheimnisse werden üblicherweise als Sicherheitsoptionen für die Authentifizierung festgelegt.

  Wenn Sie für die RADIUS-Clients und den RADIUS-Server geteilte Geheimnisse konfigurieren, gewährleisten Sie die sichere Übertragung von RADIUS-Nachrichten. Bei einem geteilten Geheimnis handelt es sich typischerweise um einen normale Textzeichenfolge. Weitere Anweisungen finden Sie in der Dokumentation zum RADIUS-Server.

> **Hinweis**
> In den vom RADIUS-Server gesendeten Authentifizierungs- und Kontoführungsnachrichten sollten die Attribute **User-Name** und **Framed-IP-Address** enthalten sein. RADIUS Agent verwendet diese Attribute, um die Paare aus Benutzernamen und IP-Adressen auszuwerten und zu speichern. Wenn Ihr RADIUS-Server diese Information nicht standardmäßig erzeugt, konfigurieren Sie ihn so, dass er dies tut (Siehe Dokumentation zum RADIUS-Server).

eDirectory Agent

Verwandte Themen:

- *Transparente Identifikation*, Seite 213
- *eDirectory Agent konfigurieren*, Seite 239
- *Verschiedene Einstellungen für eine Instanz eines Agenten konfigurieren*, Seite 246

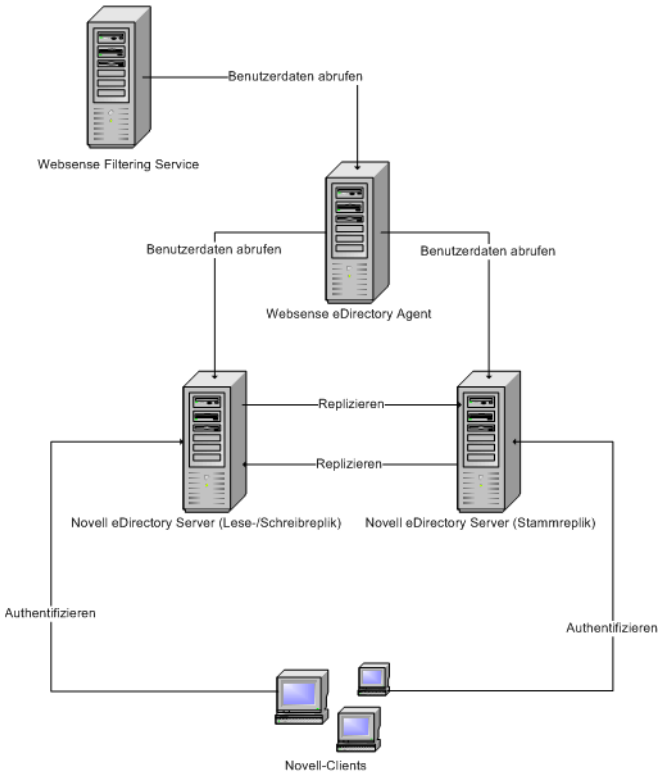
Der eDirectory Agent von Websense arbeitet mit Novell eDirectory zusammen, um Benutzer transparent zu identifizieren, so dass die Websense-Software diese entsprechend der Richtlinien filtern kann, die Benutzern, Gruppen, Domänen oder Organisationseinheiten zugewiesen sind.

eDirectory Agent fragt die Informationen von Sitzungen mit Benutzeranmeldung von Novell eDirectory ab, die den Benutzer authentifizieren, der sich am Netzwerk

anmeldet. Der Agent ordnet dann jedem authentifizierten Benutzer eine IP-Adresse zu und speichert den Benutzernamen zusammen mit der IP-Adresse in einer lokalen Benutzerzuordnung ab. eDirectory Agent leitet diese Informationen an Filtering Service weiter.

> **Hinweis**
>
> Von einem Novell-Client, auf dem Windows ausgeführt wird, können sich mehrere Benutzer an einem einzigen Novell eDirectory Server anmelden. Der Novell eDirectory Server ordnet mehreren Benutzern eine IP-Adresse zu. In diesem Szenario speichert eDirectory Agent nur für den letzten Benutzer, der sich von der entsprechenden IP-Adresse aus angemeldet hat, das Paar aus Benutzernamen und IP-Adresse in der Benutzerzuordnung ab.

Eine Instanz von eDirectory Agent von Websense kann einen Novell eDirectory-Master sowie eine beliebige Anzahl von Repliken von Novell eDirectory unterstützen.



Spezielle Bedingungen bei der Konfiguration

- Beachten Sie Folgendes, wenn Sie Cisco Content Engine v5.3.1.5 oder höher mit der Websense-Software integriert haben:
  - Führen Sie die folgenden Websense-Dienste auf demselben Computer aus, auf dem auch Cisco Content Engine läuft:

    Websense eDirectory Agent
    Websense User Service
    Websense Filtering Service
    Websense Policy Server
  - Stellen Sie sicher, dass alle Repliken von Novell eDirectory auf demselben Computer zur Datei **wsedir.ini** hinzugefügt werden.
  - Löschen Sie die Datei **eDirAgent.bak**.

  Führen Sie die Reporting Tool-Dienste von Websense auf einem **separaten** Computer aus, auf dem Cisco Content Engine und die Websense-Software nicht ausgeführt werden.
- Die Websense-Software unterstützt die Verwendung von NMAS zsammen mit eDirectory Agent. Um eDirectory Agent mit aktiviertem NMAS zu verwenden, muss eDirectory Agent auf einem Computer installiert sein, auf dem auch der Novell-Client ausgeführt wird.

eDirectory Agent konfigurieren

Verwandte Themen:

- *Transparente Identifikation*, Seite 213
- *Manuelle Authentifizierung*, Seite 215
- *Methoden für die Benutzeridentifikation konfigurieren*, Seite 216
- *eDirectory Agent*, Seite 237
- *eDirectory Agent für die Verwendung von LDAP konfigurieren*, Seite 242
- *Mehrere Agenten konfigurieren*, Seite 244

Über die Seite **Einstellungen > Benutzeridentifikation > eDirectory Agent** können Sie eine neue Instanz von eDirectory Agent und die globalen Einstellungen konfigurieren, die auf alle Instanzen von eDirectory Agent angewendet werden.

So fügen Sie eine neue Instanz von eDirectory Agent hinzu:

1. Geben Sie unter "Basiskonfiguration für Agenten" die IP-Adresse und den Namen des **Servers** ein, auf dem der Agent installiert wurde.

   > **Hinweis**
   >
   > Namen von Computern müssen mit einem Buchstaben (a-z) beginnen. Sie dürfen nicht mit einem numerischen oder Sonderzeichen beginnen.
   >
   > Namen von Computern, die bestimmte erweiterte ASCII-Zeichen enthalten, können unter Umständen nicht ordnungsgemäß aufgelöst werden. Wenn Sie eine nicht-englische Version der Websense-Software verwenden, geben Sie statt des Computernamens eine IP-Adresse ein.

2. Geben Sie den **Port** ein, den eDirectory Agent verwenden soll, um mit anderen Websense-Komponenten zu kommunizieren. Der Standardwert ist 30700.
3. Wählen Sie das Kontrollkästchen **Authentifizierung aktivieren**, und geben Sie anschließend das **Passwort** für die Verbindung ein, um eine authentifizierte Verbindung zwischen Filtering Service und eDirectory Agent herzustellen.
4. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern, oder geben Sie im nächsten Bildschirmabschnitt zusätzliche Konfigurationsinformationen ein.

Passen Sie als nächstes die globalen Einstellungen für die Kommunikation mit eDirectory Agent an. Standardmäßig wirken sich alle hier vorgenommenen Änderungen auf alle Instanzen von eDirectory Agent aus. Mit einem Stern (*) markierte Einstellungen können in der Konfigurationsdatei eines Agenten außer Kraft gesetzt werden, um das Verhalten der Instanz des Agenten anzupassen (siehe *Verschiedene Einstellungen für eine Instanz eines Agenten konfigurieren*, Seite 246).

1. Geben Sie den **Kommunikationsport** ein, der für die Kommunikation zwischen eDirectory Agent und anderen Websense-Komponenten verwendet werden soll. Der Standardwert ist 30700.
2. Nehmen Sie nur dann Änderungen an den Einstellungen des **Diagnose-Ports** vor, wenn Sie von der technischen Unterstützung von Websense dazu aufgefordert werden. Der Standardwert ist 30701.
3. Legen Sie unter "eDirectory Server" eine **Suchbasis** (Root-Kontext) für eDirectory Agent fest, die als Ausgangspunkt verwendet wird, wenn das Verzeichnis nach Benutzerinformationen durchsucht wird.
4. Stellen Sie die Informationen zum Benutzerkonto mit Administratorberechtigungen bereit, die eDirectory Agent für die Kommunikation mit dem Verzeichnis verwenden soll:
   a. Geben Sie den **Definierten Namen des Administrators** für ein Benutzerkonto mit Administratorberechtigungen in Novell eDirectory ein.
   b. Geben Sie das **Passwort** ein, das vom Konto verwendet wird.

c. Legen Sie ein **Zeitüberschreitungslimit für Benutzereinträge** fest, mit dem angegeben wird, wie lange Einträge in der Benutzerzuordnung des Agenten beibehalten werden.

Dieser Zeitraum sollte ungefähr 30 % länger sein als eine durchschnittliche Sitzung mit Benutzeranmeldung. Hierdurch wird verhindert, dass Einträge aus der Benutzerzuordnung entfernt werden, bevor die Benutzer den Internetzugriff beendet haben.

Für die meisten Szenarien wird der standardmäßig eingestellte Wert von 24 Stunden empfohlen.

> **Hinweis**
> In einigen Umgebungen kann es angemessen sein, eDirectory Server in regelmäßigen Intervallen nach Aktualisierungen bei Benutzeranmeldungen abzufragen, statt mit einem Zeitüberschreitungslimit für Benutzereinträge festzulegen, wie oft eDirectory Agent seine Benutzerzuordnung aktualisieren soll. Siehe *Vollständige Abfragen von eDirectory Server aktivieren*, Seite 243.

5. Fügen Sie den eDirectory Server-Master sowie alle Repliken zur Liste **Repliken von eDirectory** hinzu Klicken Sie auf **Hinzufügen**, um einen eDirectory Server-Master oder Repliken zur Liste hinzuzufügen. Befolgen Sie dann die Anweisungen unter *Eine Replik von eDirectory Server hinzufügen*, Seite 241.

Wenn Sie die Änderungen an der Konfiguration vorgenommen haben, klicken Sie zum Speichern Ihrer Einstellungen auf **OK**.

Eine Replik von eDirectory Server hinzufügen

Eine Instanz von eDirectory Agent von Websense kann einen Novell eDirectory-Master sowie eine beliebige Anzahl von Repliken von Novell eDirectory unterstützen, die auf verschiedenen Computern ausgeführt werden.

eDirectory Agent muss mit allen Computern kommunizieren können, die eine Replik des Verzeichnisdienstes ausführen. Dadurch wird sichergestellt, dass der Agent die aktuellsten Anmeldeinformationen so schnell wie möglich erhält und nicht auf die Replikation von eDirectory wartet.

Novell eDirectory repliziert das Attribut, das einen angemeldeten Benutzer eindeutig identifiziert, nur alle fünf Minuten. Trotz dieser zeitlichen Verzögerung bei der Replikation, erfasst eDirectory Agent neue Sitzungen mit Benutzeranmeldung sowie sich ein Benutzer an einer Replik von eDirectory anmeldet.

So konfigurieren Sie die Installation von eDirectory Agent für die Kommunikation mit eDirectory:

1. Fügen Sie im Bildschirm "Replik von eDirectory hinzufügen" die IP-Adresse oder den Namen von eDirectory **Server** hinzu (Master oder Replik).

2. Geben Sie den **Port** ein, den eDirectory Agent verwenden soll, um mit dem Computer zu kommunizieren, auf dem eDirectory ausgeführt wird.
3. Klicken Sie auf **OK**, um zur Seite "eDirectory Agent" zurückzukehren. Die neuen Einträge werden in der Liste "Repliken von eDirectory" angezeigt.
4. Wiederholen Sie diese Vorgehensweise für alle weiteren eDirectory-Servercomputer.
5. Klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Klicken Sie anschließend auf **Alle Änderungen speichern**.
6. Stoppen Sie eDirectory Agent, und starten Sie diesen erneut, damit der Agent mit den neuen Repliken kommunizieren kann. Anweisungen erhalten Sie unter *Anhalten und Starten der Websense-Dienste*, Seite 302.

eDirectory Agent für die Verwendung von LDAP konfigurieren

eDirectory Agent von Websense kann das NCP-Protokoll (Netware Core Protocol) oder das LDAP-Protokoll (Lightweight Directory Access Protocol) verwenden, um die Anmeldeinformationen von Benutzern von Novell eDirectory zu erfassen. Standardmäßig verwendet eDirectory Agent unter Windows das NCP-Protokoll. Unter Linux muss eDirectory Agent das LDAP-Protokoll verwenden.

Wenn Sie eDirectory Agent unter Windows ausführen, jedoch das LDAP-Protokoll für die Abfrage von Novell eDirectory verwenden möchten, konfigurieren Sie den Agenten entsprechend. Das NCP-Protokoll bietet jedoch einen effizienteren Abfragemechanismus.

So konfigurieren Sie eDirectory Agent unter Windows für die Verwendung des LDAP-Protokolls:

1. Stellen Sie sicher, dass Sie über mindestens eine Replik von Novell eDirectory verfügen, in der alle Verzeichnisobjekte enthalten sind, um Ihr Netzwerk zu überwachen und zu filtern.
2. Stoppen Sie den eDirectory Agent-Dienst von Websense (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).
3. Navigieren Sie zum Installationsverzeichnis von eDirectory Agent (Standardpfad **\Programme\Websense\bin**), und öffnen Sie die Datei **wsedir.ini** in einem Texteditor.
4. Ändern Sie den Eintrag **QueryMethod** wie folgt:

   ```
   QueryMethod=0
   ```

   Damit wird der Agent so eingestellt, dass er das LDAP-Protokoll für die Abfrage von Novell eDirectory verwendet. (Der Standardwert für das NCP-Protokoll ist 1.)
5. Speichern und schließen Sie die Datei.
6. Starten Sie den Websense eDirectory Agent-Dienst erneut.

Vollständige Abfragen von eDirectory Server aktivieren

In kleinen Netzwerken können Sie Websense eDirectory Agent so konfigurieren, dass eDirectory Server in regelmäßigen Abständen nach allen angemeldeten Benutzern abgefragt wird. Hierdurch kann der Agent sowohl neu angemeldete Benutzer erfassen, als auch Benutzer, die sich seit der letzten Abfrage abgemeldet haben, und seine Benutzerzuordnung entsprechend aktualisieren.

Wichtig

Es wird nicht empfohlen, eDirectory Agent in größeren Netzwerken für die vollständige Abfrage zu konfigurieren, weil der Zeitraum für die Erfassung der Abfrageresultate von der Anzahl der angemeldeten Benutzer abhängt. Je mehr Benutzer angemeldet sind, desto stärker wirkt sich die Abfrage auf die Leistung aus.

Wenn Sie die vollständige Abfrage für eDirectory Agent aktivieren, wird das **Zeitüberschreitungslimit für Benutzereinträge** nicht angewendet, weil Benutzer, die sich abgemeldet haben, durch die Abfrage ermittelt werden. Standardmäßig wird die Abfrage alle 30 Sekunden durchgeführt.

Die Aktivierung dieser Funktion erhöht die Verarbeitungszeit von eDirectory Agent auf zwei Arten:

- durch die Zeit, die für die Erfassung der Namen der angemeldeten Benutzer bei jeder Abfrage erforderlich ist
- durch die Zeit, die für die Verarbeitung der Informationen zu den Benutzernamen erforderlich ist: das Entfernen veralteter Einträge aus der Benutzerzuordnung und das Hinzufügen neuer Einträge basierend auf der aktuellsten Abfrage

eDirectory Agent überprüft nach jeder Abfrage die gesamte Benutzerzuordnung, statt lediglich die neuen Anmeldungen zu identifizieren. Die für diesen Prozess erforderliche Zeit ist von der Anzahl der Benutzer abhängig, die von jeder Abfrage erfasst werden. Daher kann sich der Abfrageprozess auf die Reaktionszeiten von eDirectory Agent und Novell eDirectory Server auswirken.

So aktivieren Sie vollständige Abfragen:

1. Navigieren Sie auf dem Computer, auf dem eDirectory Agent ausgeführt wird, zum Websense-Verzeichnis **bin**. Standardmäßig lautet der Pfad "C:\Programme\Websense\bin" oder "/opt/Websense/bin".
2. Machen Sie die Datei **wsedir.ini** ausfindig, und erstellen Sie eine Sicherungskopie der Datei in einem anderen Verzeichnis.
3. Öffnen Sie die Datei **wsedir.ini** in einem Texteditor wie Notepad oder vi.
4. Gehen Sie in der Datei zum Abschnitt **[eDirAgent]**, und machen Sie den folgenden Eintrag ausfindig:

   ```
   QueryMethod=<N>
   ```

   Notieren Sie sich den Wert für den Eintrag "QueryMethod" für den Fall, dass Sie diese Einstellung später auf den Standardwert zurücksetzen möchten.

5. Aktualisieren Sie den Wert **QueryMethod** wie folgt:
   - Wenn der aktuelle Wert "0" lautet, erfolgt die Kommunikation mit dem Verzeichnis über das LDAP-Protokoll. Ändern Sie diesen Wert in **2**.
   - Wenn der aktuelle Wert "1" lautet, erfolgt die Kommunikation mit dem Verzeichnis über das NCP-Protokoll. Ändern Sie diesen Wert in **3**.

   Hinweis
   Wenn die Änderung dieses Wertes die Systemleistung heruntersetzt, setzen Sie den Wert im Eintrag "QueryMethod" auf den vorigen Wert zurück.

6. Wenn das standardmäßige Abfrageintervall (30 Sekunden) in Ihrer Umgebung nicht angemessen ist, bearbeiten Sie den Wert **PollInterval** entsprechend.

   Beachten Sie, dass die Intervallzeit in **Millisekunden** angegeben wird.
7. Speichern und schließen Sie die Datei.
8. Starten Sie den eDirectory Agent-Dienst von Websense erneut (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).

Mehrere Agenten konfigurieren

Verwandte Themen:
- *DC Agent*, Seite 225
- *Logon Agent*, Seite 229
- *RADIUS Agent*, Seite 232
- *eDirectory Agent*, Seite 237

Sie können mehrere Agenten für die transparente Identifikation innerhalb desselben Netzwerks kombinieren. Wenn Ihre Netzwerkkonfiguration mehrere Agenten erfordert, installieren Sie jeden Agenten auf einer separaten Maschine. In einigen Fällen können Sie die Websense-Software so konfigurieren, dass diese mit mehreren Agenten auf einem einzigen Computer zusammenarbeitet.

Folgende Kombinationen von Agenten für die transparente Identifikation werden unterstützt:

Kombination	Derselbe Computer?	Dasselbe Netzwerk?	Konfiguration erforderlich
Mehrere DC Agents	Nein	Ja	Stellen Sie sicher, dass alle Instanzen von DC Agent mit Filtering Service kommunizieren können.
Mehrere RADIUS Agents	Nein	Ja	Konfigurieren Sie jede Instanz für die Kommunikation mit Filtering Service.
Mehrere eDirectory Agents	Nein	Ja	Konfigurieren Sie jede Instanz für die Kommunikation mit Filtering Service.
Mehrere Logon Agents	Nein	Ja	Konfigurieren Sie jede Instanz für die Kommunikation mit Filtering Service.
DC Agent + RADIUS Agent	Ja	Ja	Installieren Sie diese Agenten in separaten Verzeichnissen. Konfigurieren Sie jeden Agenten für die Kommunikation mit Filtering Service über verschiedene Kommunikationsports.
DC Agent + eDirectory Agent	Nein	Nein	Die Websense-Software unterstützt die Kommunikation mit den Verzeichnisdiensten von Windows und Novell nicht innerhalb der gleichen Implementierung. Sie können jedoch beide Agenten installieren und nur einen davon aktivieren.
DC Agent + Logon Agent	Ja	Ja	Konfigurieren Sie beide Agenten für die Kommunikation mit Filtering Service. Standardmäßig verwendet jeder Agent einen eindeutigen Port. Es sollten keine Portkonflikte auftreten, solange die Portzuweisung nicht geändert wurde.
eDirectory Agent + Logon Agent	Nein	Nein	Die Websense-Software unterstützt die Kommunikation mit den Verzeichnisdiensten von Windows und Novell nicht innerhalb der gleichen Implementierung. Sie können jedoch beide Agenten installieren und nur einen davon aktivieren.

Kombination	Derselbe Computer?	Dasselbe Netzwerk?	Konfiguration erforderlich
RADIUS Agent + eDirectory Agent	Ja	Ja	Konfigurieren Sie jeden Agenten für die Kommunikation mit Filtering Service über verschiedene Kommunikationsports.
DC Agent + Logon Agent + RADIUS Agent	Ja	Ja	Diese Kombination wird trotz ihrer Seltenheit unterstützt. Installieren Sie jeden Agenten in einem separaten Verzeichnis. Konfigurieren Sie alle Agenten für die Kommunikation mit Filtering Service über verschiedene Kommunikationsports.

Verschiedene Einstellungen für eine Instanz eines Agenten konfigurieren

Die Konfigurationseinstellungen von Agenten für die transparente Identifikation in Websense Manager sind global und werden auf alle Instanzen des Agenten angewendet, die Sie installiert haben. Wenn Sie über mehrere Instanzen eines Agenten verfügen, können Sie jedoch eine Instanz unabhängig von den anderen konfigurieren.

Die spezifischen Einstellungen, die Sie für einen bestimmten Agenten festlegen, setzten die globalen im Dialogfenster "Einstellungen" vorgenommenen Einstellungen außer Kraft. Einstellungen, die außer Kraft gesetzt werden können, sind mit einem Stern (*) markiert.

1. Stoppen Sie den Agenten für die transparente Identifikation (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).
2. Navigieren Sie am Computer, der die Instanz des Agenten ausführt, zum Installationsverzeichnis des Agenten. Öffnen Sie die entsprechende Datei in einem Texteditor:
   - für DC Agent: **transid.ini**
   - für Logon Agent: **authserver.ini**
   - für eDirectory Agent: **wsedir.ini**
   - für RADIUS Agent: **wsradius.ini**
3. Machen Sie den Parameter ausfindig, der für diese Instanz des Agenten geändert werden muss (siehe *Parameter der INI-Datei*, Seite 248).

   Sie können beispielsweise eine authentifizierte Verbindung zwischen dieser Instanz des Agenten und anderen Websense-Diensten aktivieren. Geben Sie hierzu in die INI-Datei einen Wert für den Parameter **Passwort** ein.

   ```
   password=[xxxxxx]
   ```
4. Ändern Sie die anderen Werte wie erwünscht.
5. Speichern Sie und schließen die INI-Datei.

6. Wenn Sie die Einstellungen von **DC Agent** geändert haben, entfernen Sie zwei Dateien aus dem Verzeichnis **bin** in Websense. Der Standardpfad lautet C:\Programme\Websense\bin:
   a. Stoppen Sie alle Websense-Dienste auf Computern, die DC Agent ausführen (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).
   b. Löschen Sie die folgenden Dateien:

      ```
      Journal.dat
      XidDcAgent.bak
      ```

      Diese Dateien werden neu erstellt, wenn Sie den DC Agent-Dienst von Websense starten.
   c. Starten Sie die Websense-Dienst erneut, einschließlich DC Agent, und fahren Sie mit **Schritt 8** fort.
7. Starten Sie den Dienst für Agenten für die transparente Identifikation neu.
8. Aktualisieren Sie die Einstellungen der Agenten in Websense Manager:
   a. Gehen Sie auf **Einstellungen > Benutzeridentifikation**.
   b. Wählen Sie den Agenten unter **Agenten für die transparente Identifikation**, und klicken Sie dann auf **Bearbeiten**.

      Hinweis

      Wenn Sie den Wert für **Port** für diese Instanz des Agenten geändert haben, entfernen Sie den Agenten, und fügen Sie ihn erneut hinzu. Wählen Sie zunächst den vorhandenen Eintrag des Agenten. Klicken Sie dann auf **Löschen** und anschließend auf **Agent hinzufügen**.

   c. Überprüfen Sie die Werte für **IP oder Name des Servers** und den **Port**, den diese Instanz des Agenten verwendet. Wenn Sie in der INI-Datei einen eindeutigen Port festgelegt haben, stellen Sie sicher, dass Ihr Eintrag mit dem Wert übereinstimmt.
   d. Wenn Sie in der INI-Datei ein eindeutiges Passwort festgelegt haben, stellen Sie sicher, dass das hier angezeigte **Passwort** korrekt ist.
   e. Klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst dann übernommen, wenn Sie auf **Alle Änderungen speichern** geklickt haben.

Parameter der INI-Datei

Feldkennzeichnung in Websense Manager	Namen der Parameter in der INI-Datei	Beschreibung
Kommunikationsport (*Alle Agenten*)	port	Der Port, über den der Agent mit anderen Websense-Diensten kommuniziert.
Diagnose-Port (*Alle Agenten*)	DiagServerPort	Der Port, über den das Agenten-Fehlerbehebungs-Tool Daten vom Agenten erwartet.
Passwort (*Alle Agenten*)	password	Das Passwort, das der Agent verwendet, um die Verbindungen zu anderen Websense-Dienste zu authentifizieren. Legen Sie ein Passwort fest, um die Authentifizierung zu aktivieren.
Abfrageintervall (*DC Agent*)	QueryInterval	Das Intervall, in dem DC Agent den Domänencontroller abfragt.
IP oder Name des Servers Port (*eDirectory Agent*)	Server=IP:port	Die IP-Adresse und Portnummer des Computers, der eDirectory Agent ausführt.
Suchbasis (*eDirectory Agent*)	SearchBase	Die Suchbasis (Root-Kontext) des Servers, der Novell eDirectory ausführt.
Definierter Name des Administrators (*eDirectory Agent*)	DN	Der Name des Benutzers mit Administratorfunktion für den Server, der Novell eDirectory ausführt.
Passwort (*eDirectory Agent*)	PW	Das Passwort für den Benutzer mit Administratorfunktion für den Server, der Novell eDirectory ausführt.
IP oder Name des RADIUS-Servers	RADIUSHost	Die IP-Adresse oder der Name des Computers, der als RADIUS-Server fungiert.
IP des RRAS-Computer (nur für Windows) (*RADIUS Agent*)	RRASHost	Die IP-Adresse des Computers, der RRAS ausführt. Websense fragt diesen Computer nach Sitzungen mit Benutzeranmeldungen ab.
Authentifizierungsport: Zwischen RADIUS Agent und RADIUS-Server	AuthOutPort	Der Port, über den der RADIUS-Server Authentifizierungsanforderungen erwartet.
Authentifizierungsport: Zwischen RADIUS-Clients und RADIUS Agent	AuthInPort	Der Port, über den RADIUS Agent Authentifizierungsanforderungen zulässt.

Feldkennzeichnung in Websense Manager	Namen der Parameter in der INI-Datei	Beschreibung
Kontoführungsport: Zwischen RADIUS Agent und RADIUS-Server	AccOutPort	Der Port, über den der RADIUS-Server RADIUS-Kontoführungsnachrichten erwartet.
Kontoführungsports: Zwischen RADIUS-Clients und RADIUS Agent:	AccInPort	Der Port, über den RADIUS Agent Kontoführungsanforderungen zulässt.

Einen Agenten für das Ignorieren bestimmter Benutzernamen konfigurieren

Sie können einen Agenten für die transparente Identifikation so konfigurieren, dass er Anmeldenamen ignoriert, die nicht tatsächlichen Benutzern zugeordnet sind. Mit dieser Funktion wird häufig die Art und Weise behandelt, mit der einige Dienste unter Windows 200x- und Windows XP den Kontakt zum Domänencontroller im Netzwerk herstellen.

Beispielsweise meldet sich **Benutzer1** am Netzwerk an und wird vom Domänencontroller als **ComputerA/Benutzer1** identifiziert. Der Benutzer wird von der Websense-Richtlinie gefiltert, die **Benutzer1** zugewiesen wurde. Wenn auf dem Computer des Benutzers ein Dienst startet, der die Identität **ComputerA/Dienstname** annimmt, um Kontakt zum Domänencontroller herzustellen, können Probleme bei der Filterung auftreten. Die Websense-Software behandelt **ComputerA/Dienstname** als neuen Benutzer, dem keine Richtlinie zugewiesen wurde und filtert diesen Benutzer nach der Richtlinie für den Computer oder nach der Richtlinie **Standard**.

So behandeln Sie dieses Problem:

1. Stoppen Sie den Dienst des Agenten (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).
2. Navigieren Sie zum Verzeichnis **\Websense\bin**, und öffnen Sie die Datei **ignore.txt** in einem Texteditor.
3. Geben Sie jeden Benutzernamen in eine separate Zeile ein. Fügen Sie keine Platzhalterzeichen wie einen Stern (*) ein.

   ```
   maran01
   WindowsServiceName
   ```

   Die Websense-Software ignoriert diese Benutzernamen, unabhängig davon, welchem Computer sie zugeordnet sind.

   Um die Websense-Software aufzufordern, den Benutzernamen innerhalb einer spezifischen Domäne zu ignorieren, verwenden Sie das Format **Benutzername, Domäne**.

   ```
   aperez, engineering1
   ```

4. Wenn Sie die Eingaben abgeschlossen haben, speichern und schließen Sie die Datei.
5. Starten Sie den Dienst des Agenten neu.

Der Agent ignoriert die festgelegten Benutzernamen. Die Websense-Software berücksichtigt diese Benutzernamen bei der Filterung nicht.

11 Delegierte Verwaltung

Verwandte Themen:

- *Einführung in die Administratorrollen*, Seite 252
- *Administratoren*, Seite 253
- *Erste Schritte mit den Administratorrollen*, Seite 257
- *Einrichten des Zugriffs auf Websense Manager*, Seite 266
- *Verwenden der delegierten Verwaltung*, Seite 270
- *Zugriff auf Websense Manager durch mehrere Administratoren*, Seite 281
- *Definieren von Filtereinschränkungen für alle Rollen*, Seite 282

Die delegierte Verwaltung bietet leistungsstarke, flexible Methoden, um die Filterung der Internetaktivitäten und Berichterstellung für bestimmte Client-Gruppen zu verwalten. Es handelt sich dabei um eine effektive Methode, die Zuständigkeit für die Verwaltung des Zugriffs auf das Internet und die Berichterstellung auf die einzelnen Manager zu verteilen, wenn sich alle Benutzer an einem zentralen Standort befinden. Sie ist besonders effektiv in größeren Organisationen, die mehrere Standorte in verschiedenen geografischen Regionen umfassen, da die lokalen Administratoren für die Benutzer in ihrem Gebiet mit diesem Verfahren den Zugriff auf das Internet verwalten und Berichte über Filterungsaktivitäten erstellen können.

Bei der Implementierung der delegierten Verwaltung wird für jede Gruppe von Clients, die von denselben Administratoren verwaltet wird, eine Administratorrolle erstellt. Einzelne Administratoren in jeder Rolle können die Berechtigung erhalten, Richtlinien zu verwalten oder Berichte für ihre Clients zu erstellen – oder beides. Siehe *Erste Schritte mit den Administratorrollen*, Seite 257.

Die Rolle des übergeordneten Administrators wird vorinstalliert. Sie umfasst den Standardbenutzer mit Administratorfunktion: WebsenseAdministrator. Übergeordnete Administratoren haben Zugriff auf eine größere Vielzahl von Richtlinien- und Konfigurationseinstellungen als Administratoren in anderen Rollen. Siehe *Übergeordnete Administratoren*, Seite 253.

Einführung in die Administratorrollen

Verwandte Themen:

- *Administratoren*, Seite 253
- *Erste Schritte mit den Administratorrollen*, Seite 257

Eine Administratorrolle ist eine Sammlung von verwalteten Clients – Benutzern, Gruppen, Domänen, Organisationseinheiten, Computern und Netzwerkbereichen –, die von mindestens einem Administrator verwaltet wird. Sie gewähren den einzelnen Administratoren die Berechtigungen, Richtlinien auf die Clients ihrer Rolle anzuwenden, Berichte zu erstellen oder beides.

Die Rolle des übergeordneten Administrators ist in der Websense-Software vordefiniert. Es gibt außerdem einen Standardbenutzer, WebsenseAdministrator, der automatisch ein Mitglied der Rolle des übergeordneten Administrators ist. Sie können Administratoren zu dieser Rolle hinzufügen, aber den Standardadministrator können Sie nicht löschen.

Wichtig

Die vordefinierte Rolle des übergeordneten Administrators kann nicht gelöscht werden. Der Standardbenutzer, WebsenseAdministrator, ist ein Administrator in der Rolle des übergeordneten Administrators, wird in der Rolle aber nicht aufgeführt. Sie können die Berechtigungen für WebsenseAdministrator nicht löschen oder ändern.

Sie können so viele Rolle erstellen, wie Sie für Ihre Organisation benötigen. Beispielsweise können Sie eine Rolle für jede Abteilung erstellen – mit dem Abteilungsleiter als Administrator und den Mitarbeitern in der Abteilung als verwaltete Clients. In einer geografisch verteilten Organisation können Sie für jeden Standort eine Rolle erstellen und alle Benutzer an dem Standort als verwaltete Clients dieser Rolle zuweisen. Weisen Sie anschließend mindestens einen Mitarbeiter an diesem Standort als Administrator zu.

Informationen über die Optionen zum Definieren der Administratoren finden Sie unter *Administratoren*, Seite 253.

Anweisungen zum Erstellen von Rollen und Konfigurieren von Berechtigungen finden Sie unter *Verwenden der delegierten Verwaltung*, Seite 270.

Administratoren

Administratoren haben Zugriff auf Websense Manager, um Richtlinien zu verwalten oder Berichte für eine Gruppe von Clients zu erstellen. Die einzelnen Berechtigungen, die verfügbar sind, hängen vom Typ der Rolle ab.

- Bei den übergeordneten Administratoren handelt es sich um eine besondere Rolle, die in Websense Manager vordefiniert ist. Diese Rolle bietet die größte Flexibilität für die Definition der Zugriffsberechtigungen. Siehe *Übergeordnete Administratoren*, Seite 253.
- Rollen für die delegierte Verwaltung können nur von einem übergeordneten Administrator erstellt werden. Administratoren in diesen Rollen verfügen nur über eingeschränkte Zugriffsberechtigungen. Siehe *Delegierte Administratoren*, Seite 255.

Darüber hinaus können Sie Rollen für die delegierte Verwaltung nur für die Berichterstellung einrichten, sodass einzelne Benutzer Berichte erstellen können, ohne für die Verwaltung der Richtlinien zuständig zu sein.

Sie können Administratoren zu Rollen zuweisen, indem Sie ihre Netzwerkanmeldeinformationen verwenden, oder Sie können besondere Konten erstellen, die nur für den Zugriff auf Websense Manager verwendet werden. Siehe *Einrichten des Zugriffs auf Websense Manager*, Seite 266.

Übergeordnete Administratoren

Verwandte Themen:

- *Administratoren*, Seite 253
- *Delegierte Administratoren*, Seite 255
- *Administratoren in mehreren Rollen*, Seite 256

Die Rolle des übergeordneten Administrators wird während der Installation erstellt. Der Standardbenutzer, WebsenseAdministrator, wird dieser Rolle automatisch zugewiesen. Wenn Sie sich also zuerst mit diesem Benutzernamen und dem Passwort anmelden, das während der Installation eingerichtet wurde, haben Sie Zugriff mit umfassenden Administratorrechten auf alle Richtlinien-, Berichterstellungs- und Konfigurationseinstellungen in Websense Manager.

Um den umfassenden Zugriff für dieses Konto zu schützen, wird WebsenseAdministrator in der Liste der Administratoren für die Rolle des übergeordneten Administrators nicht aufgeführt. Dieses Konto kann nicht gelöscht und die Berechtigungen können nicht geändert werden.

Sie können Administratoren zur Rolle des übergeordneten Administrators Ihren Anforderungen entsprechend hinzufügen. Für jeden Administrator können Berechtigungen wie folgt erteilt werden:

- **Richtlinienberechtigungen** ermöglichen es den übergeordneten Administratoren, Rollen für die delegierte Verwaltung zu erstellen und zu bearbeiten und ggf. Filter und Richtlinien in diese Rollen zu kopieren. Sie können außerdem Filterkomponenten, Filter und Richtlinien erstellen und bearbeiten und Richtlinien auf Clients anwenden, die nicht von einer anderen Rolle verwaltet werden.

  Darüber hinaus können übergeordnete Administratoren mit Richtlinienberechtigungen das Überwachungsprotokoll anzeigen, und sie erhalten wie folgt Zugriff auf die Websense-Konfiguration und andere Optionen:

  - **Ohne Bedingung:** Diese Berechtigungen ermöglichen einem übergeordneten Administrator Zugriff auf alle Systemkonfigurationseinstellungen für die Websense-Installation, z. B. die Einstellungen für Konto, Policy Server und Remote Filtering Server, die Zuordnung zu Risikoklassen und Protokollierungsoptionen.

    Übergeordnete Administratoren, für die keine Bedingungen gelten, können eine Filter-Fixierung erstellen, die bestimmte Kategorien und Protokolle für alle Benutzer sperrt, die von den delegierten Verwaltungsrollen verwaltet werden. Weitere Informationen finden Sie unter *Definieren von Filtereinschränkungen für alle Rollen*, Seite 282.

    Übergeordnete Administratoren, für die keine Bedingungen gelten, können die Rolle des übergeordneten Benutzers ändern und ggf. Administratoren hinzufügen und löschen. Sie können außerdem Rollen für die delegierte Verwaltung löschen oder Administratoren oder Clients aus diesen Rollen löschen.

  - **Mit Bedingungen:** Über diese Berechtigungen erhält der übergeordnete Administrator Zugriff auf den Datenbank-Download, auf Verzeichnisdienste, auf die Identifikation von Benutzern und die Konfiguration der Einstellungen für Network Agent. Übergeordnete Administratoren, für die Bedingungen gelten, und die auch über Berechtigungen für die Berichterstellungsfunktion verfügen, können auf Konfigurationseinstellungen für die Reporting Tools zugreifen.

    Übergeordnete Administratoren, für die Bedingungen gelten, können Websense-Benutzerkonten hinzufügen, aber nicht löschen. Sie können Rollen für die delegierte Verwaltung erstellen und bearbeiten, aber sie können keine Rollen, Administratoren oder die ihnen zugewiesenen verwalteten Clients löschen. Sie können außerdem keine Administratoren aus der Rolle des übergeordneten Administrators löschen.

- **Berichterstellung:** Diese Berechtigungen ermöglichen es den übergeordneten Administratoren, auf alle Berichterstellungsfunktionen zuzugreifen und Berichte für alle Benutzer zu erstellen. Übergeordnete Administratoren, für die keine Bedingungen gelten, verfügen automatisch über Berechtigungen für die Berichterstellungsfunktion.

Wenn einem Administrator nur Berechtigungen für die Berichterstellungsfunktion erteilt werden, sind die Optionen "Richtlinie erstellen", "URL anderer Kategorie zuordnen" und "URL entsperren" in der Liste "Allgemeine Tasks" nicht verfügbar. Die Option "Richtlinie überprüfen" ist in der Toolbox ebenfalls nicht verfügbar.

Richten Sie mehrere übergeordnete Administratoren ein, für die keine Bedingungen gelten, um sicherzustellen, dass ein Administrator Zugriff auf alle Websense-Richtlinien- und Konfigurationseinstellungen hat, falls der primäre übergeordnete Administrator abwesend ist.

Hinweis: Zwei Administratoren können sich nicht gleichzeitig anmelden, um die Richtlinie für dieselbe Rolle zu verwalten. Informationen zur Vermeidung von Konflikten finden Sie unter *Zugriff auf Websense Manager durch mehrere Administratoren*, Seite 281.

Die einzigartigen Berechtigungen der Rolle des übergeordneten Administrators ermöglichen einem Administrator in dieser Rolle den Zugriff auf alle Rollen. Um nach der Anmeldung zu einer anderen Rolle zu wechseln, wählen Sie im Banner in der Dropdownliste **Rolle** eine Rolle aus.

Nach dem Ändern der Rollen verfügen Sie nur über die Richtlinienberechtigungen, die für die Rolle für die delegierte Verwaltung verfügbar sind. Die von Ihnen erstellten Filter und Richtlinien stehen nur den Administratoren in dieser Rolle zur Verfügung. Sie können nur auf verwaltete Clients in dieser Rolle angewendet werden. Siehe *Delegierte Administratoren*, Seite 255.

Berechtigungen für die Berichterstellungsfunktion sind kumulativ, d. h., dass Sie die kombinierten Berechtigungen aller Rollen erhalten, denen Sie als Administrator zugewiesen sind. Übergeordnete Administratoren, für die keine Bedingungen gelten, verfügen über die vollständigen Berechtigungen für die Berichterstellungsfunktion, unabhängig davon, auf welche Rolle zugegriffen wird.

Delegierte Administratoren

Verwandte Themen:

- *Administratoren*, Seite 253
- *Übergeordnete Administratoren*, Seite 253
- *Administratoren in mehreren Rollen*, Seite 256

Delegierte Administratoren verwalten Clients, die einer bestimmten Rolle zugewiesen wurden. Ordnen Sie jedem Administrator Richtlinien- und/oder Berichterstellungsfunktion zu.

Delegierte Administratoren, die über **Richtlinienberechtigungen** verfügen, wenden die Richtlinien auf die Clients an, die ihrer Rolle zugewiesen wurden, und legen dadurch fest, welchen Internetzugang jeder Client erhält. Im Rahmen ihrer Zuständigkeit können delegierte Administratoren Richtlinien und Filter erstellen, bearbeiten und löschen, die den Beschränkungen der Filter-Fixierung unterliegen, die

vom übergeordneten Administrator eingerichtet wurde. Siehe *Definieren von Filtereinschränkungen für alle Rollen*, Seite 282.

> **Hinweis**
>
> Delegierte Administratoren haben erhebliche Kontrolle über die Internetaktivitäten ihrer verwalteten Clients. Um sicherzustellen, dass diese Kontrolle verantwortlich und in Einklang mit den in Ihrer Organisation geltenden Nutzungsrichtlinien ausgeübt wird, sollte der übergeordnete Administrator die Seite "Überwachungsprotokoll" verwenden, um die Änderungen zu überwachen, die von den Administratoren vorgenommen wurden. Siehe *Anzeigen und Exportieren des Überwachungsprotokolls*, Seite 300.

Delegierte Administratoren können die Richtlinie "Standard" nicht löschen.

Sie können die Filterkomponenten bearbeiten, wobei jedoch einige Einschränkungen gelten. Weitere Informationen finden Sie unter *Erstellen von Richtlinien und Filtern*, Seite 264.

Administratoren mit Richtlinienberechtigungen, die sich bei Websense Manager mit einem Websense-Benutzerkonto anmelden, können auch ihr eigenes Websense-Passwort ändern. (Siehe *Websense-Benutzerkonten*, Seite 268.)

Die Optionen, die für die delegierten Administratoren mit Berechtigungen für die **Berichterstellungsfunktion** verfügbar sind, hängen davon ab, wie die Rolle konfiguriert wurde. Sie können entweder nur für die Clients Berichte erstellen, die von ihrer Rolle verwaltet werden, oder für alle Clients. Sie können Zugriff auf alle oder nur auf einige Berichterstellungsfunktionen haben. Weitere Informationen finden Sie unter *Rollen bearbeiten*, Seite 272.

Ein Administrator, der nur über Berechtigungen für die Berichterstellungsfunktion verfügt, hat im rechten Teilfenster für Verknüpfungen nur eine begrenzte Anzahl an Optionen zur Auswahl ("Allgemeine Tasks" und "Toolbox").

Administratoren in mehreren Rollen

Verwandte Themen:

- *Administratoren*, Seite 253
- *Übergeordnete Administratoren*, Seite 253
- *Delegierte Administratoren*, Seite 255

Abhängig von den Anforderungen Ihrer Organisation kann derselbe Administrator mehreren Rollen zugewiesen werden. Administratoren, die mehreren Rollen zugewiesen wurden, müssen bei der Anmeldung eine Rolle auswählen, die sie verwalten.

Nach der Anmeldung verfügen Sie über die folgenden Berechtigungen:

- **Richtlinie:** Sie können Filter und Richtlinien für die Rolle hinzufügen und bearbeiten, die Sie bei der Anmeldung ausgewählt haben, und Richtlinien auf die Clients anwenden, die in dieser Rolle verwaltet werden. Auf der Seite "Delegierte Verwaltung" werden alle Rollen aufgeführt, denen Sie zugewiesen sind, und die verwalteten Clients und Berichterstellungsberechtigungen werden für jede Rolle angezeigt.
- **Berichterstellung:** Sie verfügen über alle Berichterstellungsberechtigungen Ihrer gesamten Rollen. Angenommen, Sie sind drei Rollen zugewiesen, die über die folgenden Berechtigungen für die Berichterstellungsfunktion verfügen:
  - Rolle 1: Keine Berichterstellungsfunktion
  - Rolle 2: Berichterstellung nur für verwaltete Clients, nur Untersuchungsberichte
  - Rolle 3: Berichterstellung für alle Clients, umfassender Zugriff auf alle Berichterstellungsfunktionen

  In dieser Situation sind Sie unabhängig von der während der Anmeldung gewählten Rolle berechtigt, Berichte auf den Seiten "Heute" und "Verlauf" anzuzeigen. Außerdem können Sie Berichte für alle Clients und unter Verwendung aller Berichterstellungsfunktionen erstellen.

  Wenn Sie sich nur für die Berichterstellung angemeldet haben, wird in der Bannerleiste im Feld "Rolle" angezeigt, ob Sie über die Berechtigung "Vollständige Berichterstellung" (Berichte für alle Clients) oder "Eingeschränkte Berichterstellung" (Berichte nur für die verwalteten Clients) verfügen.

Erste Schritte mit den Administratorrollen

Verwandte Themen:

- *Einführung in die Administratorrollen*, Seite 252
- *Benachrichtigen von Administratoren*, Seite 260
- *Aufgaben der delegierten Administratoren*, Seite 261

Um die delegierte Verwaltung einzurichten, muss der übergeordnete Administrator die folgenden Aufgaben fertigstellen:

- Legen Sie fest, wie Administratoren sich bei Websense Manager anmelden. Siehe *Einrichten des Zugriffs auf Websense Manager*, Seite 266.
- Fügen Sie Rollen hinzu und konfigurieren Sie sie anschließend. Siehe *Verwenden der delegierten Verwaltung*, Seite 270.
- Informieren Sie die Administratoren über ihre Zuständigkeiten und Optionen. Siehe *Benachrichtigen von Administratoren*, Seite 260.

Neben diesen erforderlichen Aufgaben gibt es noch einige optionale Aufgaben, die mit der delegierten Verwaltung verbunden sind.

Einrichten der Filter-Fixierung

Übergeordnete Administratoren, für die keine Bedingungen gelten, können eine Filter-Fixierung einrichten, die für bestimmte Kategorien und Protokolle festlegt, dass diese für verwaltete Clients in allen Rollen für die delegierte Verwaltung gesperrt sind. Diese Einschränkungen gelten automatisch für alle Filter, die in einer Rolle für die delegierte Verwaltung erstellt oder kopiert werden; sie können vom delegierten Administrator nicht geändert werden.

> **Hinweis**
> Die Filter-Fixierung gilt nicht für Clients, die von der Rolle des übergeordneten Administrators verwaltet werden.

Die Filter-Fixierung kann Dateitypen und Schlüsselworte sperren und fixieren, die mit ausgewählten Kategorien verbunden sind, und die Aufzeichnung ausgewählter Protokolle veranlassen. Siehe *Erstellen einer Filter-Fixierung*, Seite 283.

Verschieben von Clients

Wenn Sie auf der Seite "Clients" einen Client hinzufügen, während Sie als übergeordneter Administrator angemeldet sind, wird dieser Client der Rolle des übergeordneten Administrators zugewiesen. Dieser Client kann einer Rolle für die delegierte Verwaltung nicht auf der Seite "Rolle bearbeiten" hinzugefügt werden. Die beste Vorgehensweise ist es, Clients direkt zu einer Rolle hinzuzufügen, statt eine Richtlinie in der Rolle eines übergeordneten Administrators zuzuweisen. Das ist allerdings nicht immer möglich.

Wählen Sie auf der Seite "Clients" die Option **Verschieben zu Rolle** aus, um Clients aus der Rolle des übergeordneten Administrators in eine andere Rolle zu verschieben. Siehe *Verschieben von Clients zu Rollen*, Seite 75.

Beim Verschieben wird die Richtlinie, die in der Rolle des übergeordneten Administrators angewendet wird, in die Rolle für die delegierte Verwaltung kopiert. Die Filter, die von dieser Richtlinie durchgesetzt werden, werden auch kopiert. Während des Kopiervorgangs werden die Filter aktualisiert, die ggf. die Einschränkungen der Filter-Fixierung durchsetzen.

In der Zielrolle wird an das Ende des Filter- oder Richtliniennamens das Kennzeichen "(Kopiert)" hinzugefügt. Administratoren für diese Rolle können das neue Element schnell identifizieren und entsprechend aktualisieren.

> **Hinweis**
>
> Jedes Mal, wenn ein Filter oder eine Richtlinie in dieselbe Rolle kopiert wird, erhält das Kennzeichen "(Kopiert)" eine Nummer, die bei jeder neuen Kopie erhöht wird: (1 kopiert), (2 kopiert) usw. Jedes Element wird ein separater Filter bzw. eine separate Richtlinie in der Rolle.
>
> Administratoren in der Rolle sollten die Filter und Richtlinien umbenennen und den Anforderungen entsprechend bearbeiten, damit die Einstellungen deutlich sind und Duplikate auf ein Minimum beschränkt werden. Durch diese Änderungen kann der zukünftige Wartungsaufwand vereinfacht werden.

Die Filter "Alles zulassen" in der Rolle des übergeordneten Administrators ermöglichen den Zugriff auf alle Kategorien oder Protokolle. Sie können nicht bearbeitet werden. Diese Filter können auch nicht in eine Rolle für die delegierte Verwaltung kopiert werden, damit der übergeordnete Administrator immer in der Lage ist, eine Filter-Fixierung einzurichten.

Wenn die Richtlinie, die dem zu verschiebenden Client zugewiesen ist, den Filter "Alles zulassen" durchsetzt, kann der Client erst dann verschoben werden, wenn Sie eine Richtlinie anwenden, die nicht den Filter "Alles zulassen" verwendet.

Nachdem der Client zu der neuen Rolle verschoben wurde, kann nur ein Administrator in dieser Rolle die Richtlinie dieses Clients oder die durchgesetzten Filter ändern. Änderungen an der ursprünglichen Richtlinie oder den ursprünglichen Filtern in der Rolle des übergeordneten Administrators haben keine Auswirkung auf Kopien der Richtlinie oder Filter in den Rollen für die delegierte Verwaltung.

Kopieren von Filtern und Richtlinien

Filter und Richtlinien, die von einem übergeordneten Administrator erstellt werden, stehen nur den Administratoren in der Rolle des übergeordneten Administrators zur Verfügung. Sie können die Option **Kopieren zu Rolle** verwenden, um Filter und Richtlinien in eine Rolle für die delegierte Verwaltung zu kopieren, ohne einen Client in diese Rolle zu verschieben. Siehe *Filter und Richtlinien in Rollen kopieren*, Seite 183.

Beim direkten Kopieren von Filtern und Richtlinien werden dieselben Beschränkungen durchgesetzt, die gelten, wenn Filter und Richtlinien beim Verschieben eines Clients kopiert werden.

- Während des Kopiervorgangs werden die Einschränkungen der Filter-Fixierung implementiert.
- Kategorie- und Protokollfilter für "Alles zulassen" können nicht kopiert werden.

- Kopierte Filter und Richtlinien werden in der Rolle durch die Namensergänzung "(Kopiert)" identifiziert.

Richtlinienbeschreibungen sollten vor dem Kopiervorgang bearbeitet werden, um sicherzustellen, dass sie für die Administratoren in den Zielrollen nützlich sind.

Anwenden von Richtlinien für die verbleibenden Clients

Clients, die nicht ausdrücklich einer Rolle für die delegierte Verwaltung zugewiesen sind, werden von übergeordneten Administratoren verwaltet. Für die Rolle des übergeordneten Administrators gibt es keine Liste mit verwalteten Clients.

Um auf diese Clients Richtlinien anzuwenden, fügen Sie sie unter "Richtlinienverwaltung > Clients" hinzu. Siehe *Hinzufügen eines Clients*, Seite 73. Clients, denen keine bestimmte Richtlinie zugewiesen wurde, unterliegen der Richtlinie "Standard", die für ihre Rolle gilt.

Es kann vorkommen, dass Sie keine Clients zur Seite "Clients" hinzufügen können. Das kann daran liegen, dass der Client Mitglied eines Netzwerks, einer Gruppe, Domäne oder Organisationseinheit ist, das bzw. die einer anderen Rolle zugewiesen wurde. Wenn der Administrator der anderen Rolle eine Richtlinie auf einzelne Mitglieder des Netzwerks oder der Gruppe angewendet hat, können diese Clients nicht zur Rolle des übergeordneten Administrators hinzugefügt werden.

Benachrichtigen von Administratoren

Verwandte Themen:

- *Einführung in die Administratorrollen*, Seite 252
- *Erste Schritte mit den Administratorrollen*, Seite 257

Nachdem Sie einzelne Benutzer als Administratoren in einer beliebigen Administratorrolle zugewiesen haben, geben Sie ihnen die folgenden Informationen.

- Die URL für die Anmeldung bei Websense Manager. Standardmäßig:

  ```
  https://<ServerIP>:9443/mng/
  ```

  Verwenden Sie statt <ServerIP> die IP-Adresse des Computers, auf dem Websense Manager ausgeführt wird.
- Welcher Policy Server ggf. während der Anmeldung ausgewählt werden soll. In einer Umgebung mit mehreren Policy Servern müssen Administratoren bei der Anmeldung einen Policy Server auswählen. Sie müssen den Policy Server auswählen, der für die Kommunikation mit dem Verzeichnisdienst konfiguriert wurde, der die verwalteten Clients authentifiziert.
- Ob sie das Konto für die Netzwerkanmeldung oder ein Websense-Benutzerkonto verwenden sollen, wenn sie sich bei Websense Manager anmelden. Wenn sich Administratoren mit Websense-Benutzerkonten anmelden, stellen Sie den Benutzernamen und das Kennwort bereit.
- Die Berechtigungen, entweder um Richtlinien für Clients in der Rolle zu erstellen und anzuwenden und/oder um Berichte zu erstellen.

Administratoren, die sowohl über Richtlinien- als auch über Berichterstellungsfunktionen verfügen, sollten überlegen, welche Aktivitäten sie während der Sitzung durchführen möchten. Wenn sie nur die Erstellung von Berichten planen, wird empfohlen, dass sie im Banner im Feld **Rolle** die Optionen **Freigeben Richtlinie Berechtigungen** auswählen. Dadurch wird die Richtlinienberechtigung für die Rolle freigegeben, sodass ein anderer Administrator Zugriff auf Websense Manager hat und die Richtlinien für diese Rolle verwalten kann.

- Wie sie die Liste der Clients finden können, die von ihrer Rolle verwaltet werden. Administratoren können zu "Richtlinienverwaltung > Delegierte Verwaltung" wechseln und auf den Namen ihrer Rolle klicken, um die Seite "Rolle bearbeiten" anzuzeigen, auf der eine Liste der verwalteten Clients enthalten ist.
- Einschränkungen, die durch die Filter-Fixierung auferlegt werden, wenn Kategorien oder Protokolle gesperrt oder fixiert wurden.
- Die Aufgaben, die gewöhnlich von Administratoren durchgeführt werden. Siehe *Aufgaben der delegierten Administratoren*, Seite 261.

Benachrichtigen Sie die delegierten Administratoren, wenn Sie benutzerdefinierte Dateitypen und Protokolle ergänzen oder ändern. Diese Komponenten werden automatisch in Filtern und Richtlinien für alle Rollen übernommen. Deswegen ist es wichtig, dass die betroffenen Administratoren erfahren, wenn Änderungen vorgenommen wurden.

Aufgaben der delegierten Administratoren

Verwandte Themen:

- *Einführung in die Administratorrollen*, Seite 252
- *Erste Schritte mit den Administratorrollen*, Seite 257
- *Benachrichtigen von Administratoren*, Seite 260

Delegierte Administratoren, die über **Richtlinienberechtigungen** verfügen, können die folgenden Aufgaben durchführen.

- *Anzeigen des Benutzerkontos*, Seite 262
- *Anzeigen der Rollendefinition*, Seite 262
- *Hinzufügen von Clients zur Seite "Clients"*, Seite 263
- *Erstellen von Richtlinien und Filtern*, Seite 264
- *Anwenden von Richtlinien auf Clients*, Seite 265

Berichterstellungsberechtigungen können einzeln erteilt werden. Die spezifischen Berichterstellungsberechtigungen, die für Ihre Rolle erteilt wurden, legen fest, welche der folgenden Aufgaben für Administratoren mit Berichterstellungsberechtigungen verfügbar sind. Siehe *Erstellen von Berichten*, Seite 266.

Anzeigen des Benutzerkontos

Verwandte Themen:

- *Aufgaben der delegierten Administratoren*, Seite 261
- *Anzeigen der Rollendefinition*, Seite 262
- *Hinzufügen von Clients zur Seite "Clients"*, Seite 263
- *Erstellen von Richtlinien und Filtern*, Seite 264
- *Anwenden von Richtlinien auf Clients*, Seite 265

Wenn Sie sich bei Websense Manager mit Netzwerk-Anmeldeinformationen anmelden, werden Passwortänderungen über Ihren Netzwerkverzeichnisdienst verwaltet. Bitten Sie Ihren Systemadministrator um Hilfe.

Wenn Ihnen ein Websense-Benutzername und -Passwort zugewiesen wurde, können Sie in Websense Manager Informationen über Ihr Konto anzeigen und das Passwort ändern.

1. Wechseln Sie zu **Richtlinienverwaltung > Delegierte Verwaltung**.
2. Klicken Sie im oberen Bereich der Seite auf **Websense-Benutzerkonten verwalten**.
3. Klicken Sie auf **Passwort ändern**, wenn Sie das Passwort ändern möchten. Siehe *Ändern des Passworts eines Websense-Benutzers*, Seite 269.
4. Klicken Sie auf **Anzeigen**, um eine Liste mit Rollen anzuzeigen, in denen Sie als Administrator zugewiesen sind.

Anzeigen der Rollendefinition

Verwandte Themen:

- *Aufgaben der delegierten Administratoren*, Seite 261
- *Anzeigen des Benutzerkontos*, Seite 262
- *Hinzufügen von Clients zur Seite "Clients"*, Seite 263
- *Erstellen von Richtlinien und Filtern*, Seite 264
- *Anwenden von Richtlinien auf Clients*, Seite 265

Öffnen Sie die Seite "Delegierte Verwaltung" und klicken Sie auf den Namen Ihrer Rolle, um die Seite "Rolle bearbeiten" anzuzeigen, auf der die verwalteten Clients der Rolle aufgeführt sind. Auf dieser Seite werden außerdem die Berichterstellungsfunktionen angezeigt, die für die Administratoren verfügbar sind, die Berechtigungen für die Berichterstellungsfunktion in dieser Rolle besitzen.

Administratoren, die nur über Berichterstellungsfunktionen verfügen, können diese Seite nicht anzeigen. Diese Administratoren haben nur auf die angegebenen Berichterstellungsfunktionen Zugriff.

Hinzufügen von Clients zur Seite "Clients"

Verwandte Themen:

- *Aufgaben der delegierten Administratoren*, Seite 261
- *Anzeigen des Benutzerkontos*, Seite 262
- *Anzeigen der Rollendefinition*, Seite 262
- *Erstellen von Richtlinien und Filtern*, Seite 264
- *Anwenden von Richtlinien auf Clients*, Seite 265

Übergeordnete Administratoren weisen verwaltete Clients einer Rolle zu, aber delegierte Administratoren müssen sie zur Seite "Clients" hinzufügen, bevor sie Richtlinien anwenden. Anweisungen dazu finden Sie unter *Hinzufügen eines Clients*, Seite 73.

Sobald Clients zur Liste der verwalteten Clients einer Rolle hinzugefügt wurden, werden sie von der Richtlinie "Standard" dieser Rolle gefiltert. Clients, die aus der Seite "Clients" des übergeordneten Administrators in die Rolle verschoben wurden, unterliegen der Richtlinie, die vom übergeordneten Administrator angewendet wurde. Diese wurde in die Rolle kopiert, als der Client verschoben wurde.

Jeder Client, der unter "Delegierte Verwaltung > Rolle bearbeiten" für Ihre Rolle aufgeführt ist, kann zur Seite "Clients" hinzugefügt werden, und ihm kann eine Richtlinie zugewiesen werden. Sie können außerdem einzelne Benutzer oder Computer hinzufügen, die Mitglied einer Gruppe, Domäne, Organisationseinheit oder eines Netzwerkbereichs sind, die bzw. der als verwalteter Client in Ihrer Rolle zugewiesen wurde.

Da ein Benutzer zu mehreren Gruppen, Domänen oder Organisationseinheiten gehören kann, können in dem Fall, dass die Gruppen, Domänen oder Organisationseinheiten mit gemeinsamen Mitgliedern von unterschiedlichen Rollen verwaltet werden, Konflikte entstehen, wenn einzelne Benutzer aus einer größeren Client-Gruppe hinzugefügt werden. Wenn Administratoren in unterschiedlichen Rollen gleichzeitig auf Websense Manager zugreifen, könnten sie denselben Client (z. B. ein einzelnes Mitglied einer Gruppe) zu ihrer Seite "Clients" hinzufügen. In einer solchen Situation unterliegt die Filterung der Internetaktivitäten für diesen Client der Rangordnung (Präzedenz), die für die jeweilige Rolle festgelegt wurde. Siehe *Verwalten von Rollenkonflikten*, Seite 279.

Erstellen von Richtlinien und Filtern

Verwandte Themen:

- *Aufgaben der delegierten Administratoren*, Seite 261
- *Anzeigen des Benutzerkontos*, Seite 262
- *Anzeigen der Rollendefinition*, Seite 262
- *Hinzufügen von Clients zur Seite "Clients"*, Seite 263
- *Anwenden von Richtlinien auf Clients*, Seite 265

Bei der Erstellung Ihrer Rolle wurden automatisch die Richtlinie "Standard", der Kategorie- und der Protokollfilter, die vorinstalliert waren, mit der Definition zu diesem Zeitpunkt übernommen. Darüber hinaus kann der übergeordnete Administrator andere Richtlinien und Filter zu Ihrer Rolle kopieren.

Abgesehen von Richtlinien und Filtern werden auch alle benutzerdefinierten Dateitypen und Protokolle, die vom übergeordneten Administrator erstellt wurden, übernommen.

Sie können die Richtlinien und Filter, die Sie vom übergeordneten Administrator übernehmen, Ihren Anforderungen entsprechend bearbeiten. Die von Ihnen vorgenommenen Änderungen haben nur auf Ihre Rolle eine Auswirkung. Änderungen, die der übergeordnete Administrator an den Richtlinien und Filtern vornimmt, die Sie bereits übernommen haben, wirken sich nicht auf Ihre Rolle aus.

Hinweis

Änderungen, die der übergeordnete Administrator an benutzerdefinierten Dateitypen und Protokollen vornimmt, wirken sich automatisch auf die Filter und Richtlinien in Ihrer Rolle aus.

Wenn Sie von Ihrem übergeordneten Administrator über Änderungen an diesen Komponenten informiert werden, überprüfen Sie Ihre Filter und Richtlinien, um sicherzustellen, dass sie ordnungsgemäß gehandhabt werden.

Sie können so viele neue Filter und Richtlinien erstellen, wie Sie benötigen. Filter und Richtlinien, die von einem delegierten Administrator erstellt werden, sind nur für die Administratoren verfügbar, die sich in Ihrer Rolle angemeldet haben. Anweisungen zum Erstellen von Richtlinien finden Sie unter *Arbeiten mit Richtlinien*, Seite 79. Anweisungen zum Erstellen von Filtern finden Sie unter *Arbeiten mit Filtern*, Seite 51.

Sie können Filterkomponenten für Ihre Rolle bearbeiten. Dabei gelten aber einige Einschränkungen.

- **Kategorien:** Fügen Sie benutzerdefinierte Kategorien hinzu und bearbeiten Sie die Stammdatenbank (Master Database) sowie die benutzerdefinierten Kategorien; definieren Sie URLs, die anderen Kategorien zugeordnet wurden, und Schlüsselworte für die Verwendung in ihrer Rolle; ändern Sie die Aktion und die erweiterte Filteroption, die standardmäßig in den erstellten Kategoriefiltern angewendet werden. (Änderungen an der Standardaktion einer Kategorie werden nur implementiert, wenn die Kategorie nicht durch die Filter-Fixierung fixiert ist.)
- **Protokolle:** Ändern Sie die Aktion und die erweiterten Filteroptionen, die standardmäßig in den erstellten Protokollfiltern angewendet werden. (Änderungen an der Standardaktion eines Protokolls werden nur implementiert, wenn das Protokoll nicht durch die Filter-Fixierung fixiert ist.) Delegierte Administratoren können keine Protokolldefinitionen hinzufügen oder löschen.
- **Dateitypen:** Zeigen Sie die Dateierweiterungen an, die jedem Dateityp zugewiesen sind. Delegierte Administratoren können keine Dateitypen hinzufügen oder Erweiterungen ändern, die einem Dateityp zugewiesen sind.
- **Ungefilterte URLs:** Fügen Sie URLs und reguläre Ausdrücke hinzu, die Sites darstellen, die nur für alle verwalteten Clients in ihrer Rolle zugelassen werden sollen.

Weitere Informationen finden Sie unter *Filterkomponenten erstellen*, Seite 185.

Wenn ein übergeordneter Administrator Einschränkungen der Filter-Fixierung implementiert hat, werden manche Kategorien oder Protokolle u. U. automatisch gesperrt und können in den Filtern nicht geändert werden, die Sie erstellen und bearbeiten. Siehe *Definieren von Filtereinschränkungen für alle Rollen*, Seite 282.

Anwenden von Richtlinien auf Clients

Verwandte Themen:

- *Aufgaben der delegierten Administratoren*, Seite 261
- *Anzeigen des Benutzerkontos*, Seite 262
- *Anzeigen der Rollendefinition*, Seite 262
- *Hinzufügen von Clients zur Seite "Clients"*, Seite 263
- *Erstellen von Richtlinien und Filtern*, Seite 264

Nachdem Sie eine Richtlinie erstellt haben, können Sie diese Richtlinie direkt auf Clients anwenden, die bereits zur Seite "Clients" hinzugefügt wurden, indem Sie auf die Schaltfläche **Auf Clients anwenden** klicken. Siehe *Zuweisen einer Richtlinie an Clients*, Seite 83.

Sie können außerdem die Seite "Clients" öffnen und die Clients hinzufügen, für die diese Richtlinie gelten soll. Siehe *Arbeiten mit Clients*, Seite 64.

Erstellen von Berichten

Wenn Sie Berechtigungen für die Berichterstellungsfunktion besitzen, werden die spezifischen Berichterstellungsfunktionen, über die Sie verfügen, vom übergeordneten Administrator eingerichtet. Gehen Sie zur Seite "Delegierte Verwaltung" und klicken Sie auf den Namen der Rolle, um zu erfahren, welche Funktionen Sie verwenden können. Auf der Seite "Rolle bearbeiten" werden die Berichterstellungsfunktionen angezeigt, für die Sie Berechtigungen besitzen. Weitere Informationen finden Sie unter *Rollen bearbeiten*, Seite 272.

Einrichten des Zugriffs auf Websense Manager

Wenn Sie Rollen für die delegierte Verwaltung konfigurieren, können Sie festlegen, auf welche Websense Manager-Funktionen der Administrator Zugriff hat. Um sicherzustellen, dass die einzelnen Benutzer, die sich bei Websense Manager anmelden, über die richtigen Funktionen verfügen, muss bei der Anmeldung ein Benutzername und ein Passwort angegeben werden. Es stehen zwei Kontoarten zur Verfügung:

- **Netzwerkkonten** verwenden die Anmeldeinformationen, die in Ihrem Netzwerkverzeichnisdienst festgelegt sind (siehe *Verzeichniskonten*, Seite 266).
- **Websense-Benutzerkonten** ermöglichen die Erstellung eines Benutzernamens und Passworts speziell für die Verwendung in Websense Manager (siehe *Websense-Benutzerkonten*, Seite 268).

Verzeichniskonten

Verwandte Themen:

- *Einrichten des Zugriffs auf Websense Manager*, Seite 266
- *Websense-Benutzerkonten*, Seite 268

Übergeordnete Administratoren, für die keine Bedingungen gelten, können über **Einstellungen > Allgemein > Anmeldungsverzeichnis** die erforderlichen Verzeichnisdienstinformationen eingeben, damit Administratoren sich bei Websense Manager mit ihren Netzwerkanmeldeinformationen anmelden können.

Hinweis

Die Informationen werden nur zur Authentifizierung von Websense Manager-Benutzern verwendet. Sie werden nicht auf die Filterung von Clients angewendet. Verzeichnisdienstinformationen für den Client werden über "Einstellungen > Verzeichnisdienst" konfiguriert (siehe *Verzeichnisdienste*, Seite 67).

Die Netzwerkanmeldeinformationen der Websense Manager-Benutzer müssen gegen einen einzelnen Verzeichnisdienst authentifiziert werden. Wenn Ihr Netzwerk mehrere Verzeichnisdienste umfasst, muss zwischen dem Anmeldungsverzeichnisdienst, den Sie in Websense Manager konfigurieren, und den anderen Diensten eine vertrauenswürdige Beziehung bestehen.

Wenn es nicht möglich ist, einen einzelnen Verzeichnisdienst für die Verwendung mit Websense Manager zu definieren, können Sie Websense-Benutzerkonten für die Administratoren erstellen (siehe *Websense-Benutzerkonten*, Seite 268).

Um den Verzeichnisdienst zu definieren, den Websense Manager für die Authentifizierung von Administratoren verwenden sollte, stellen Sie zuerst sicher, dass das Kontrollkästchen für die Verwendung eines Verzeichnisdienstes zur Authentifizierung von Administratoren aktiviert ist, und wählen Sie anschließend aus der Liste der **Verzeichnisdienste** einen Typ aus.

Wenn Sie die Standardeinstellung, **Windows NT Directory/Active Directory (Mixed Mode)**, wählen, ist keine weitere Konfiguration erforderlich. Klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Geben Sie bei Auswahl von **Active Directory (Native Mode)** oder **Anderes LDAP-Verzeichnis** die folgenden zusätzlichen Informationen an:

1. Geben Sie die IP-Adresse oder den Namen des Computers ein, auf dem der Verzeichnisdienst installiert ist.

   Wenn Sie die Option "Active Directory (Native Mode)" verwenden und Sie die globalen Katalogserver mit Ausfallsicherung konfiguriert haben, können Sie stattdessen den DNS-Domänennamen eingeben.
2. Geben Sie den **Port** für die Kommunikation mit dem Verzeichnisdienst ein.
3. Aktivieren Sie die Option **SSL verwenden**, um die Kommunikation mit dem Verzeichnisdienst zu verschlüsseln.
4. Geben Sie den **definierten Benutzernamen** und das **Passwort** ein, mit denen die Websense-Software eine Verbindung mit dem Verzeichnisdienst herstellen soll.
5. Geben Sie den **Standarddomänenkontext** ein, den die Websense-Software für die Authentifizierung der Administratoren verwenden soll.
   - Wenn Sie die Option "Active Directory (Native Mode)" verwenden, ist die Konfiguration abgeschlossen. Klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.
   - Wenn Sie einen anderen LDAP-basierten Verzeichnisdienst verwenden, fahren Sie mit den folgenden Schritten fort.
6. Geben Sie ggf. die **Attribute für Benutzeranmelde-ID** und den **Filter für die Suche nach Benutzern** ein, mit denen bzw. mit dem die Websense-Software die Benutzerauthentifizierung beschleunigen soll.

   Diese Informationen werden auch auf der Seite **Einstellungen > Verzeichnisdienste** unter **Erweiterte Verzeichniseinstellungen** angezeigt. Sie können diese Werte ggf. kopieren und einfügen.

7. Geben Sie unter "Optionen für Gruppe" an, ob Ihr LDAP-Schema das Attribut **memberOf** enthalten soll:
   - Wenn "memberOf" nicht verwendet wird, geben Sie den **Filter für die Suche nach Benutzergruppen** an, den die Websense-Software für die Authentifizierung von Administratoren anwenden sollte.
   - Wenn "memberOf" verwendet wird, geben Sie das **Attribut für Gruppe** an, die angewendet werden soll.
8. Wenn Ihr LDAP-Schema verschachtelte Gruppen enthält, aktivieren Sie die Option **Zusätzliche Suche nach verschachtelten Gruppen**.
9. Wenn Ihr Verzeichnisdienst LDAP-Verweise verwendet, geben Sie an, ob die Websense-Software die Verweise verwenden oder ignorieren soll.
10. Klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Websense-Benutzerkonten

Verwandte Themen:

- *Einrichten des Zugriffs auf Websense Manager*, Seite 266
- *Hinzufügen von Websense-Benutzerkonten*, Seite 269

Übergeordnete Administratoren erstellen über **Delegierte Verwaltung > Websense-Benutzerkonten verwalten** Konten für die Administratoren, über die sie auf Websense Manager ohne Eingabe der Anmeldeinformationen für das Netzwerkverzeichnis zugreifen können. Auf dieser Seite können übergeordnete Administratoren auch das Passwort für Websense-Benutzerkonten ändern und die Rollen anzeigen, denen ein Websense-Benutzer als Administrator zugewiesen ist.

Übergeordnete Administratoren, für die keine Bedingungen gelten, können über diese Seite auch die Websense-Benutzerkonten löschen.

Delegierte Administratoren verwenden diese Seite, um ihr Websense-Passwort zu ändern und die Rollen anzuzeigen, denen sie als Administratoren zugewiesen sind.

Option	Beschreibung
Hinzufügen	Öffnet die Seite zum Erstellen eines neuen Websense-Benutzerkontos. Siehe *Hinzufügen von Websense-Benutzerkonten*, Seite 269.
Passwort ändern	Öffnet die Seite zum Ändern des Passworts für das zugehörige Konto. Siehe *Ändern des Passworts eines Websense-Benutzers*, Seite 269.
Anzeigen	Zeigt eine Liste mit Rollen an, denen dieser Benutzer als Administrator zugewiesen ist.
Löschen	Aktivieren Sie das Kontrollkästchen für veraltete Benutzerkonten und klicken Sie anschließend auf diese Schaltfläche, um sie zu löschen.
Schließen	Führt Sie zur Seite "Delegierte Verwaltung" zurück.

Hinzufügen von Websense-Benutzerkonten

Verwandte Themen:

- *Einrichten des Zugriffs auf Websense Manager*, Seite 266
- *Websense-Benutzerkonten*, Seite 268
- *Ändern des Passworts eines Websense-Benutzers*, Seite 269

Verwenden Sie die Seite **Delegierte Verwaltung > Websense-Benutzerkonten verwalten > Websense-Benutzer hinzufügen**, um Websense -Benutzerkonten hinzuzufügen.

1. Geben Sie einen eindeutigen **Benutzernamen** aus maximal 50 Zeichen ein.

   Der Name muss mindestens 1 und maximal 50 Zeichen lang sein und darf keine der folgenden Zeichen enthalten:

   ```
   * < > " { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Leerstellen und Gedankenstriche dürfen in Benutzernamen verwendet werden.
2. Geben Sie für diesen Benutzer ein **Passwort** (4 bis 255 Zeichen) ein und bestätigen Sie es.

   Es wird empfohlen, ein starkes Passwort zu verwenden, das mindestens acht Zeichen lang ist und mindestens ein Zeichen aus jeder der folgenden Kategorien enthält:

   - Großbuchstaben
   - Kleinbuchstaben
   - Ziffern
   - Sonderzeichen (z. B. Bindestrich, Unterstrich oder Leerstelle)
3. Wenn Sie alle Änderungen vorgenommen haben, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern und zur Seite "Websense-Benutzerkonten verwalten" zurückzukehren. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Ändern des Passworts eines Websense-Benutzers

Verwandte Themen:

- *Einrichten des Zugriffs auf Websense Manager*, Seite 266
- *Websense-Benutzerkonten*, Seite 268
- *Hinzufügen von Websense-Benutzerkonten*, Seite 269

Auf der Seite **Delegierte Verwaltung > Websense-Benutzerkonten verwalten > Passwort ändern** können delegierte Administratoren das Passwort für ihr eigenes Websense-Benutzerkonto ändern. Übergeordnete Administratoren können auf dieser Seite das Passwort für jedes Websense-Benutzerkonto ändern.

1. Überprüfen Sie, ob im oberen Bereich der Seite der richtige **Benutzername** angezeigt wird.
2. Geben Sie für diesen Benutzer das neue **Passwort** (4 bis 255 Zeichen) ein und bestätigen Sie es.

   Es wird empfohlen, ein starkes Passwort zu verwenden, das mindestens acht Zeichen lang ist und mindestens ein Zeichen aus jeder der folgenden Kategorien enthält:

   - Großbuchstaben
   - Kleinbuchstaben
   - Ziffern
   - Sonderzeichen (z. B. Bindestrich, Unterstrich oder Leerstelle)
3. Wenn Sie alle Änderungen vorgenommen haben, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern und zur Seite "Websense-Benutzerkonten verwalten" zurückzukehren. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Verwenden der delegierten Verwaltung

Verwandte Themen:

- *Einführung in die Administratorrollen*, Seite 252
- *Verwalten von Rollenkonflikten*, Seite 279

Auf der Seite **Richtlinienverwaltung > Delegierte Verwaltung** werden abhängig davon, ob die Seite von einem übergeordneten oder von einem delegierten Administrator angezeigt wird, verschiedene Optionen bereitgestellt.

Übergeordnete Administratoren können eine Liste aller aktuell definierten Rollen anzeigen und verfügen über die folgenden Optionen:

Option	Beschreibung
Hinzufügen	Klicken Sie, um eine neue Rolle hinzuzufügen. Siehe *Rollen hinzufügen*, Seite 271.
Rolle	Klicken Sie, um die Rolle anzuzeigen oder zu konfigurieren. Siehe *Rollen bearbeiten*, Seite 272.
Löschen	Klicken Sie, um alle Rollen zu löschen, die in der Liste gekennzeichnet sind. Diese Optionen stehen nur übergeordneten Administratoren, für die keine Bedingungen gelten, zur Verfügung. Informationen darüber, wie die Clients einer Rolle verwaltet werden, nachdem die Rolle gelöscht wurde, finden Sie unter *Überlegungen*, Seite 280.

Option	Beschreibung
Erweitert	Klicken Sie, um auf die Funktion "Rollenpräzedenz verwalten" zuzugreifen.
Rollenpräzedenz verwalten	Klicken Sie, um anzugeben, von welcher Rolle die Richtlinieneinstellungen verwendet werden sollen, wenn derselbe Client in mehreren Gruppen enthalten ist, die von verschiedenen Rollen verwaltet werden. Siehe *Verwalten von Rollenkonflikten*, Seite 279.
Websense-Benutzerkonten verwalten	Klicken Sie, um Benutzernamen und Passwörter für Konten hinzuzufügen, zu bearbeiten und zu löschen, die nur für den Zugriff auf Websense Manager verwendet werden. Siehe *Websense-Benutzerkonten*, Seite 268.
Benutzerdefinierte LDAP-Gruppen verwalten	Klicken Sie, um benutzerdefinierte LDAP-Gruppen hinzuzufügen, zu bearbeiten und zu löschen, die als verwaltete Clients in einer Rolle für die delegierte Verwaltung zugewiesen werden können. Siehe *Arbeiten mit benutzerdefinierten LDAP-Gruppen*, Seite 71. Diese Option ist nicht verfügbar, wenn für den konfigurierten Verzeichnisdienst "Windows NT/Active Directory (Mixed Mode)" ausgewählt wurde.

Delegierte Administratoren können nur die Rollen anzeigen, in denen sie als Administrator zugewiesen sind. Außerdem haben sie nur auf einige Optionen Zugriff.

Option	Beschreibung
Rolle	Klicken Sie, um die Clients, die der Rolle zugewiesen sind, und die spezifischen erteilten Berichterstellungsberechtigungen anzuzeigen. Siehe *Rollen bearbeiten*, Seite 272.
Websense-Benutzerkonten verwalten	Klicken Sie, um auf Optionen für die Änderung Ihres Websense Manager-Passworts und die Anzeige Ihrer zugewiesenen Rollen zuzugreifen. Siehe *Websense-Benutzerkonten*, Seite 268.

Rollen hinzufügen

Verwandte Themen:

- *Rollen bearbeiten*, Seite 272
- *Überlegungen*, Seite 280

Geben Sie über die Seite **Delegierte Verwaltung > Rolle hinzufügen** einen Namen und eine Beschreibung für die neue Rolle an.

1. Geben Sie einen **Namen** für die neue Rolle ein.

   Der Name muss mindestens 1 und maximal 50 Zeichen lang sein und darf keine der folgenden Zeichen enthalten:

   ```
   * < > " { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

Leerstellen und Gedankenstriche dürfen in Rollennamen verwendet werden.

2. Geben Sie eine **Beschreibung** für die neue Rolle ein.

   Die Beschreibung kann bis zu 255 Zeichen umfassen. Die Einschränkungen für die Verwendung der Zeichen, die für Rollennamen gelten, gelten auch für Beschreibungen. Es gibt allerdings zwei Ausnahmen: Beschreibungen dürfen Punkte (.) und Kommas (,) enthalten.

3. Klicken Sie auf **OK**, um die Seite **Rolle bearbeiten** anzuzeigen und die Merkmale dieser Rolle zu definieren. Siehe *Rollen bearbeiten*, Seite 272.

   Die neue Rolle wird im Banner zur Dropdownliste "Rolle" hinzugefügt, wenn Sie sich das nächste Mal bei Websense Manager anmelden.

Rollen bearbeiten

Verwandte Themen:

- *Verwenden der delegierten Verwaltung*, Seite 270
- *Rollen hinzufügen*, Seite 271
- *Verwalten von Rollenkonflikten*, Seite 279

Delegierte Administratoren können auf der Seite **Delegierte Verwaltung > Rolle bearbeiten** die Liste der Clients, die von ihrer Rolle verwaltet werden, und die spezifischen erteilten Berichterstellungsberechtigungen anzeigen.

Übergeordnete Administratoren können auf dieser Seite – wie weiter unten beschrieben – die Administratoren und Clients für eine Rolle auswählen und Administratorberechtigungen festlegen. Nur übergeordnete Administratoren, für die keine Bedingungen gelten, können Administratoren und Clients aus einer Rolle löschen.

1. Ändern Sie den **Namen** und die **Beschreibung** der Rolle gemäß Ihren Anforderungen.

   Hinweis
   Der Name der Rolle des übergeordneten Administrators kann nicht geändert werden.

2. Fügen Sie für diese Rolle Administratoren hinzu oder löschen Sie sie. (Diese Option ist nur für übergeordnete Administratoren verfügbar. Wenn Sie als delegierter Administrator angemeldet sind, wird diese Seite nicht angezeigt.)

Element	Beschreibung
Benutzername	Benutzername des Administrators
Kontotyp	Gibt an, ob ein Benutzer im Netzwerkverzeichnisdienst (Verzeichnis) oder als Websense-Benutzerkonto (Websense) definiert ist.

Element	Beschreibung
Berichterstellung	Aktivieren Sie das Kontrollkästchen, um dem Administrator die Berechtigung zur Verwendung der Reporting Tools zu erteilen.
Richtlinie	Aktivieren Sie dieses Kontrollkästchen, um dem Administrator die Berechtigung zu erteilen, Filter und Richtlinien zu erstellen und Richtlinien auf die verwalteten Clients der Rolle anzuwenden. In der Rolle des übergeordneten Administrators können Administratoren mit Richtlinienberechtigung auch bestimmte Websense-Konfigurationseinstellungen verwalten. Siehe *Übergeordnete Administratoren*, Seite 253.
Ohne Bedingung	Nur für die Rolle des übergeordneten Administrators verfügbar. Aktivieren Sie dieses Kontrollkästchen, um dem Administrator die Berechtigungen zu erteilen, alle Websense-Konfigurationseinstellungen und die Filter-Fixierung zu verwalten. Nur übergeordnete Administratoren, für die keine Bedingungen gelten, können einem neuen Administrator Berechtigungen, für die keine Bedingungen gelten, erteilen.
Hinzufügen	Öffnet die Seite **Administratoren hinzufügen**. Siehe *Hinzufügen von Administratoren*, Seite 276.
Löschen	Entfernt alle Administratoren aus der Rolle, die in der Administratorliste gekennzeichnet sind. (Nur für übergeordnete Administratoren verfügbar, für die keine Bedingungen gelten.)

3. Fügen Sie dieser Rolle **Verwaltete Clients** hinzu bzw. löschen Sie sie. (Änderungen können nur von übergeordneten Administratoren vorgenommen werden. Delegierte Administratoren können die Clients anzeigen, die ihrer Rolle zugewiesen sind.)

Element	Beschreibung
<Name>	Zeigt den Namen jedes Clients an, der einer Rolle ausdrücklich zugewiesen ist. Administratoren in der Rolle müssen die Clients auf der Seite "Clients" hinzufügen, damit die Richtlinien angewendet werden können. Siehe *Aufgaben der delegierten Administratoren*, Seite 261.
Hinzufügen	Öffnet die Seite **Verwaltete Clients hinzufügen**. Siehe *Hinzufügen von verwalteten Clients*, Seite 277.
Löschen	Nur verfügbar für übergeordnete Administratoren, für die keine Bedingungen gelten. Über diese Schaltfläche werden aus der Rolle alle Clients entfernt, die in der Liste der verwalteten Clients gekennzeichnet sind. Einige Clients können aus der Liste der verwalteten Clients nicht direkt entfernt werden. Weitere Informationen finden Sie unter *Überlegungen*, Seite 280.

4. Wählen Sie im Bereich **Berechtigungen für die Berichterstellungsfunktion** die Funktionen aus, die für Administratoren in dieser Rolle verfügbar sind, die Zugriff auf Berichterstellungsfunktionen haben.

   a. Wählen Sie für die Berichterstellungsberechtigungen die allgemeine Einstellung aus:

Option	Beschreibung
Erstellung von Berichten für alle Clients	Wählen Sie diese Option, um den Administratoren die Berechtigung zu erteilen, Berichte für alle Benutzer im Netzwerk zu erstellen. Verwenden Sie die übrigen Optionen im Bereich "Berechtigungen für die Berichterstellungsfunktion", um die spezifischen Berechtigungen für Administratoren in dieser Rolle einzurichten.
Erstellung von Berichten nur für verwaltete Clients	Wählen Sie diese Option, um die Berechtigungen von Administratoren auf die Erstellung von Berichten für verwaltete Clients einzuschränken, die dieser Rolle zugewiesen sind. Wählen Sie anschließend die Untersuchungsberichtsfunktionen aus, auf die diese Administratoren Zugriff erhalten. Administratoren, deren Berechtigungen auf die Erstellung von Berichten für verwaltete Clients eingeschränkt sind, können auf den Seiten "Heute" und "Verlauf" keine Präsentationsberichte oder benutzerbasierte Berichte anzeigen. Sie können außerdem keine Einstellungen der Protokolldatenbank verwalten.

   b. Aktivieren Sie das Kontrollkästchen für jede Berichterstellungsfunktion, auf die die entsprechenden Administratoren in der Rolle Zugriff haben.

Option	Beschreibung
Zugriff auf Präsentationsberichte	Ermöglicht den Zugriff auf Präsentationsberichtsfunktionen. Diese Option ist nur verfügbar, wenn Administratoren Berichte für alle Clients erstellen können. Siehe *Präsentationsberichte*, Seite 102.
Anzeigen von Berichten auf den Seiten "Heute" und "Verlauf"	Aktiviert die Anzeige von Diagrammen, die die Internetaktivitäten auf diesen Seiten veranschaulichen. Siehe *Heute: Zustand, Sicherheit und Nutzen seit Mitternacht*, Seite 22 und *Verlauf: Letzte 30 Tage*, Seite 25. Wenn diese Option deaktiviert ist, können Administratoren nur die Bereiche "Zustandsbezogene Alerts" und "Wert" auf der Seite "Heute" sowie "Schätzwerte" auf der Seite "Verlauf" anzeigen.

Option	Beschreibung
Zugriff auf Untersuchungsberichte	Ermöglicht den Zugriff auf einfache Untersuchungsberichtsfunktionen. Wenn diese Option aktiviert ist, können noch zusätzliche Untersuchungsberichtsfunktionen ausgewählt werden. Siehe *Untersuchungsberichte*, Seite 123.
Anzeigen von Benutzernamen in Untersuchungsberichten	Ermöglicht Administratoren in dieser Rolle die Anzeige von Benutzernamen, wenn diese angemeldet sind. Siehe *Konfigurieren von Filtering Service für die Protokollierung*, Seite 326. Deaktivieren Sie diese Option, um statt Namen nur vom System erstellte Identifizierungscodes anzuzeigen. Diese Option ist nur verfügbar, wenn für die Administratoren der Zugriff auf Untersuchungsberichte eingerichtet wurde.
Speichern von Untersuchungsberichten als Favoriten	Ermöglicht es Administratoren in dieser Rolle, Untersuchungsberichte als Favoriten zu erstellen. Siehe *Als Favoriten gekennzeichnete Untersuchungsberichte*, Seite 143. Diese Option ist nur verfügbar, wenn für die Administratoren der Zugriff auf Untersuchungsberichte eingerichtet wurde.
Planung von Untersuchungsberichten	Ermöglicht es Administratoren in dieser Rolle, Untersuchungsberichte zu planen, die zu einem späteren Zeitpunkt oder in einer wiederkehrenden Zeitfolge ausgeführt werden sollen. Siehe *Planen von Untersuchungsberichten*, Seite 145. Diese Option ist nur verfügbar, wenn den Administratoren die Berechtigungen erteilt wurden, Untersuchungsberichte als Favoriten zu speichern.
Verwaltung der Protokolldatenbank	Ermöglicht Administratoren den Zugriff auf die Seite "Einstellungen > Protokolldatenbank". Siehe *Protokolldatenbank-Verwaltungseinstellungen*, Seite 343. Diese Option ist nur verfügbar, wenn Administratoren Berichte für alle Clients erstellen können.

5. Wenn Sie alle Änderungen vorgenommen haben, klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Kehren Sie dann zur Seite "Delegierte Verwaltung" zurück. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Hinzufügen von Administratoren

Verwandte Themen:

- *Rollen bearbeiten*, Seite 272
- *Einrichten des Zugriffs auf Websense Manager*, Seite 266

Übergeordnete Administratoren können auf der Seite **Delegierte Verwaltung > Rolle bearbeiten** > **Administratoren hinzufügen** angeben, welche Benutzer Administratoren für eine Rolle sind.

> **Hinweis**
> Administratoren können zu mehreren Rollen hinzugefügt werden. Diese Administratoren müssen bei der Anmeldung eine Rolle auswählen. In diesem Fall erhält der Administrator die kombinierten Berichterstellungsberechtigungen für alle Rollen.

Delegierte Administratoren haben erhebliche Kontrolle über die Internetaktivitäten ihrer verwalteten Clients. Um sicherzustellen, dass diese Kontrolle verantwortlich und in Einklang mit den in Ihrer Organisation geltenden Nutzungsrichtlinien ausgeübt wird, sollte der übergeordnete Administrator die Seite "Überwachungsprotokoll" verwenden, um die Änderungen zu überwachen, die von den Administratoren vorgenommen wurden. Siehe *Anzeigen und Exportieren des Überwachungsprotokolls*, Seite 300.

1. Wenn Sie Verzeichniskonten als delegierte Administratoren hinzufügen möchten, stellen Sie sicher, dass Sie bei dem Policy Server angemeldet sind, dessen Verzeichnisdienstkonfiguration (siehe *Verzeichnisdienste*, Seite 67) mit der Konfiguration des Anmeldungsverzeichnisses übereinstimmt (siehe *Verzeichniskonten*, Seite 266).

   Wenn Sie nur Websense-Benutzerkonten als Administratoren hinzufügen, können Sie bei jedem Policy Server angemeldet sein.
2. Aktivieren Sie das Kontrollkästchen unter **Verzeichniskonten** für einen oder mehrere Benutzer und klicken Sie dann auf die Schaltfläche mit dem nach rechts weisenden Pfeil (>), um sie in die Liste **Ausgewählte Objekte** zu verschieben.

   > **Hinweis**
   > Benutzerdefinierte LDAP-Gruppen können nicht als Administratoren hinzugefügt werden.

   Wenn Sie in Ihrer Umgebung die Option "Active Directory (Native Mode)" oder einen anderen LDAP-basierten Verzeichnisdienst verwenden, können Sie das Verzeichnis durchsuchen, um die Namen von bestimmten Benutzern, Gruppen, Domänen oder Organisationseinheiten zu finden. Siehe *Durchsuchen des Verzeichnisdienstes*, Seite 74.

3. Aktivieren Sie das Kontrollkästchen unter **Websense-Benutzerkonten** für einen oder mehrere Benutzer und klicken Sie dann auf die Schaltfläche mit dem nach rechts weisenden Pfeil, um die hervorgehobenen Benutzer in die Liste **Ausgewählte Objekte** zu verschieben.
4. Legen Sie die **Berechtigungen** für Administratoren in dieser Rolle fest.

Option	Beschreibung
Richtlinie	Aktivieren Sie diese Option, damit Administratoren in dieser Rolle Richtlinien auf ihre verwalteten Clients anwenden können. Auf diese Weise wird außerdem Zugriff auf bestimmte Websense-Konfigurationseinstellungen gewährt.
Ohne Bedingung	Aktivieren Sie diese Option, um Zugriff auf alle Websense-Konfigurationseinstellungen zu gewähren. Diese Option ist nur verfügbar, wenn ein übergeordneter Administrator, für den keine Bedingungen gelten, Administratoren zur Rolle des übergeordneten Administrators mit Richtlinienberechtigungen hinzufügt.
Berichterstellung	Aktivieren Sie diese Option, um Zugriff auf die Reporting Tools zu gewähren. Legen Sie auf der Seite "Rolle bearbeiten" die entsprechenden erlaubten Berichterstellungsfunktionen fest.

5. Wenn Sie alle Änderungen vorgenommen haben, klicken Sie auf **OK**, um zur Seite "Rolle bearbeiten" zurückzukehren.
6. Klicken Sie auf der Seite "Rolle bearbeiten" auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Hinzufügen von verwalteten Clients

Verwandte Themen:

- *Verwenden der delegierten Verwaltung*, Seite 270
- *Rollen bearbeiten*, Seite 272

Verwaltete Clients sind die Benutzer und Computer, die einer Rolle zugewiesen sind. Ihre Richtlinien werden von den Administratoren der Rolle festgelegt. Verzeichnisclients (Benutzer, Gruppen, Domänen und Organisationseinheiten), Computer und Netzwerke werden als verwaltete Clients definiert.

Übergeordnete Administratoren können auf der Seite **Delegierte Verwaltung > Rolle bearbeiten > Verwaltete Clients hinzufügen** so viele Clients zu einer Rolle hinzufügen wie erforderlich. Jeder Client kann nur einer Rolle zugewiesen werden.

Wenn Sie einen Netzwerkbereich als verwalteten Client in einer Rolle hinzufügen, können Sie einzelne IP-Adressen in diesem Bereich nicht einer anderen Rolle hinzufügen. Außerdem können Sie einen Benutzer, eine Gruppe, Domäne oder Organisationseinheit nicht direkt zwei unterschiedlichen Rollen zuweisen. Sie können

einen Benutzer jedoch einer Rolle zuweisen und dann eine Gruppe, Domäne oder Organisationseinheit, bei der der Benutzer Mitglied ist, einer anderen Rolle zuweisen.

> **Hinweis**
> Wenn eine Gruppe ein verwalteter Client in einer Rolle ist und der Administrator dieser Rolle eine Richtlinie auf jedes Mitglied der Gruppe anwendet, können einzelne Benutzer in dieser Gruppe später nicht einer anderen Rolle zugewiesen werden.

Wenn Sie verwaltete Clients hinzufügen, überlegen Sie, welche Clienttypen einbezogen werden sollen. Wenn Sie IP-Adressen zu einer Rolle hinzufügen, können Administratoren in dieser Rolle Berichte für **alle** Aktivitäten der angegebenen Computer erstellen. Wenn Sie Benutzer zu einer Rolle hinzufügen, können Administratoren Berichte für alle Aktivitäten dieser Benutzer erstellen, unabhängig davon, an welchem Computer die Aktivität erfolgt ist.

Administratoren sind nicht automatisch als verwaltete Clients in den Rollen enthalten, die sie verwalten, da sie dann ihre eigenen Richtlinien festlegen könnten. Aktivieren Sie die Option Eigene Berichte:, damit Administratoren Berichte über ihre eigene Internetnutzung anzeigen können (siehe *Eigene Berichte erstellen*, Seite 360).

Wenn in Ihrer Organisation mehrere Policy Server installiert sind, und die Policy Server mit verschiedenen Verzeichnissen kommunizieren, wählen Sie den Policy Server aus, der mit dem Verzeichnis verbunden ist, in dem die Clients enthalten sind, die Sie hinzufügen möchten.

> **Hinweis**
> Optimale Vorgehensweisen sehen vor, dass alle verwalteten Clients in derselben Rolle vom selben Verzeichnisdienst stammen.

1. Wählen Sie Clients für die Rolle aus:
   - Aktivieren Sie das Kontrollkästchen für einen oder mehrere Benutzer unter **Verzeichnis**.

     Wenn Sie in Ihrer Umgebung die Option "Active Directory (Native Mode)" oder einen anderen LDAP-basierten Verzeichnisdienst verwenden, können Sie das Verzeichnis durchsuchen, um die Namen von bestimmten Benutzern, Gruppen, Domänen oder Organisationseinheiten zu finden. Siehe *Durchsuchen des Verzeichnisdienstes*, Seite 74.
   - Geben Sie unter **Computer** die IP-Adresse eines Computers ein, die zu dieser Rolle hinzugefügt werden soll.
   - Geben Sie unter **Netzwerk** die erste und letzte IP-Adresse einer Reihe von Computern ein, die als Einheit hinzugefügt werden sollen.
2. Klicken Sie auf die Schaltfläche mit dem nach rechts weisenden Pfeil (>), der sich neben dem Clienttyp befindet, um die Clients in die Liste **Ausgewählte Objekte** zu verschieben.

3. Wenn Sie alle Änderungen vorgenommen haben, klicken Sie auf **OK**, um zur Seite "Rolle bearbeiten" zurückzukehren.
4. Klicken Sie auf der Seite "Rolle bearbeiten" auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Verwalten von Rollenkonflikten

Verwandte Themen:

- *Verwenden der delegierten Verwaltung*, Seite 270
- *Hinzufügen von verwalteten Clients*, Seite 277

Verzeichnisdienste ermöglichen es, das Benutzer zu verschiedenen Gruppen gehören können. Infolgedessen kann ein einzelner Benutzer mehreren Gruppen angehören, die von verschiedenen delegierten Verwaltungsrollen verwaltet werden. Dasselbe gilt für Domänen und Organisationseinheiten.

Außerdem ist es möglich, dass ein Benutzer von einer Rolle verwaltet wird und zu einer Gruppe, Domäne oder Organisationseinheit gehört, die von einer anderen Rolle verwaltet wird. Wenn die Administratoren für beide Rollen gleichzeitig angemeldet sind, könnte der Administrator, der für den Benutzer zuständig ist, eine Richtlinie auf den Benutzer anwenden, und der für die Gruppe zuständige Administrator könnte zum gleichen Zeitpunkt eine Richtlinie auf die einzelnen Mitglieder der Gruppe anwenden.

Legen Sie auf der Seite **Delegierte Verwaltung > Rollenpräzedenz verwalten** die Vorgehensweise für die Websense-Software in Fällen fest, in denen wegen einer Überschneidung verschiedene Richtlinien auf denselben Benutzer angewendet wurden. Wenn ein Konflikt auftritt, wendet die Websense-Software die Filterrichtlinie der Rolle an, die an oberster Stelle der Liste aufgeführt ist.

1. Wählen Sie eine beliebige Rolle in der Liste – mit Ausnahme der Rolle des übergeordneten Administrators.

   Hinweis
   Die Rolle des übergeordneten Administrators befindet sich immer ganz oben auf der Liste. Sie kann nicht verschoben werden.

2. Klicken Sie auf **Nach oben verschieben** oder **Nach unten verschieben**, um die Position in der Liste zu verändern.
3. Wiederholen Sie die Schritte 1 und 2, bis alle Rollen über die gewünschte Rangordnung (Präzedenz) verfügen.
4. Wenn Sie alle Änderungen vorgenommen haben, klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Kehren Sie dann zur Seite "Delegierte Verwaltung" zurück. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Überlegungen

Verwandte Themen:

- *Verwenden der delegierten Verwaltung*, Seite 270
- *Rollen bearbeiten*, Seite 272

Überprüfen Sie die folgenden Informationen, bevor Sie Rollen für die delegierte Verwaltung oder verwaltete Clients aus einer Rolle löschen.

Löschen von Rollen

Übergeordnete Administratoren, für die keine Bedingungen gelten, können auf der Seite **Delegierte Verwaltung** alle veralteten Rollen löschen.

Wenn eine Rolle gelöscht wird, werden auch alle Clients entfernt, die die Administratoren der Rolle zur Seite "Clients" hinzugefügt haben. Nachdem die Rolle gelöscht wurde, unterliegen diese Clients, wenn sie zu Netzwerken, Gruppen oder Domänen gehören, die von anderen Rollen verwaltet werden, der entsprechenden Richtlinie dieser Rollen (siehe *Filterreihenfolge*, Seite 84). Andernfalls unterliegen sie der Richtlinie "Standard" des übergeordneten Administrators.

1. Aktivieren Sie auf der Seite **Delegierte Verwaltung** das Kontrollkästchen neben jeder Rolle, die gelöscht werden soll.

   Hinweis
   Die Rolle des übergeordneten Administrators kann nicht gelöscht werden.

2. Klicken Sie auf **Löschen**.
3. Bestätigen Sie die Löschaufforderung, um die ausgewählten Rollen aus der Seite "Delegierte Verwaltung" zu entfernen. Die Änderungen werden erst dann dauerhaft implementiert, wenn Sie auf **Alles speichern** klicken.

   Die gelöschte Rolle wird im Banner aus der Dropdownliste "Rolle" entfernt, wenn Sie sich das nächste Mal bei Websense Manager anmelden.

Löschen von verwalteten Clients

Clients können nicht direkt aus der Liste der verwalteten Clients gelöscht werden (Delegierte Verwaltung > Rolle bearbeiten), wenn Folgendes zutrifft:

- Der Administrator hat eine Richtlinie auf den Client angewendet.
- Der Administrator hat eine Richtlinie auf mindestens ein Mitglied eines Netzwerks, einer Gruppe, Domäne oder Organisationseinheit angewendet.

Darüber hinaus können Probleme auftreten, wenn der übergeordnete Administrator bei der Anmeldung bei Websense einen anderen Policy Server auswählt als den Server, der mit dem Verzeichnisdienst kommuniziert, auf dem die zu löschenden

Clients enthalten sind. In einer solchen Situation erkennen der aktuelle Policy Server und der Verzeichnisdienst die Clients nicht.

Ein übergeordneter Administrator, für den keine Bedingungen gelten, kann folgendermaßen sicherstellen, dass die richtigen Clients gelöscht werden.

1. Melden Sie sich bei Websense Manager an und wählen Sie den Policy Server aus, dessen Verzeichnisdienst die zu löschenden verwalteten Clients enthält. Sie müssen sich als übergeordneter Administrator mit Berechtigungen anmelden, für die keine Bedingungen gelten.
2. Öffnen Sie im Banner die Liste **Rolle** und wählen Sie die Rolle aus, aus der verwaltete Clients gelöscht werden sollen.
3. Wechseln Sie zu **Richtlinienverwaltung > Clients**, um eine Liste aller Clients anzuzeigen, auf die der delegierte Administrator ausdrücklich eine Richtlinie angewendet hat.

   Dazu können Clients gehören, die in der Liste der verwalteten Clients der Rolle ausdrücklich identifiziert sind, sowie Clients, die Mitglied von Netzwerken, Gruppen, Domänen oder Organisationseinheiten in der Liste der verwalteten Clients sind.
4. Löschen Sie die entsprechenden Clients.
5. Klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern.
6. Öffnen Sie im Banner die Liste **Rolle** und wählen Sie die Rolle **Übergeordneter Administrator** aus.
7. Wechseln Sie zu **Richtlinienverwaltung > Delegierte Verwaltung > Rolle bearbeiten**.
8. Löschen Sie die gewünschten Clients aus der Liste der verwalteten Clients und klicken Sie auf **OK**, um den Löschvorgang zu bestätigen.
9. Klicken Sie auf der Seite "Rolle bearbeiten" auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Zugriff auf Websense Manager durch mehrere Administratoren

Verwandte Themen:

- *Administratoren*, Seite 253
- *Einrichten des Zugriffs auf Websense Manager*, Seite 266

Administratoren in unterschiedlichen Rollen können gleichzeitig auf Websense Manager zugreifen und alle Aktivitäten durchführen, die die Berechtigungen ihrer Rolle erlauben. Beispiel: Administratoren in Rolle A und in Rolle B, die beide über Richtlinienberechtigungen verfügen, können sich gleichzeitig bei Websense Manager

anmelden. Da sie verschiedene Clients verwalten, können sie Richtlinien erstellen und anwenden, ohne Konflikte zu verursachen.

Eine andere Situation ist es, wenn Administratoren sich gleichzeitig anmelden, die Richtlinienberechtigungen in derselben Rolle haben. Um die Integrität der Richtlinienstruktur und -zuweisungen zu bewahren, können sich nie mehrere Administratoren derselben Rolle gleichzeitig mit Richtlinienberechtigungen bei Websense Manager anmelden. Wenn ein Administrator angemeldet ist und sich ein zweiter Administrator mit Richtlinienberechtigungen derselben Rolle anmelden möchte, wird der zweite Administrator vor die folgende Wahl gestellt:

- Wenn er über Berichterstellungsberechtigungen verfügt, kann er sich nur für die Berichterstellung anmelden.
- Er kann sich bei einer anderen Rolle anmelden, wenn er noch anderen Rollen zugewiesen ist.
- Oder er kann sich später anmelden, wenn sich der erste Administrator abgemeldet hat.

Wenn sich Administratoren mit Richtlinien- und Berichterstellungsberechtigungen anmelden, um Berichte zu erstellen, sollten sie ihre Richtlinienberechtigungen unverzüglich freigeben, sodass andere Administratoren in der Rolle Richtlinienverwaltungsaktivitäten durchführen können.

- Öffnen Sie im Banner die Dropdownliste **Rolle** und wählen Sie **Richtlinienberechtigungen freigeben** aus.

Eine andere Möglichkeit ist es, für jede Rolle ein spezielles Websense-Benutzerkonto zu erstellen (siehe *Websense-Benutzerkonten*, Seite 268) und diesem Benutzer lediglich Berichterstellungsberechtigungen zu erteilen. Geben Sie diese Anmeldeinformationen (Benutzername und Passwort) den Administratoren in der Rolle, die über Richtlinien- und Berichterstellungsberechtigungen verfügen. Wenn ein Administrator Berichte ausführen muss, kann er sich als Berichterstellungsadministrator anmelden, und ein anderer Administrator kann sich mit Richtlinienberechtigungen anmelden.

Definieren von Filtereinschränkungen für alle Rollen

Verwandte Themen:

- *Administratoren*, Seite 253
- *Erstellen einer Filter-Fixierung*, Seite 283

Die Websense-Software ermöglicht es übergeordneten Administratoren, für die keine Bedingungen gelten, eine Filter-Fixierung einzurichten, die Kategorien und Protokolle für alle Clients sperrt, die von delegierten Verwaltungsrollen verwaltet werden. Weitere Informationen finden Sie unter *Erstellen einer Filter-Fixierung*, Seite 283.

Administratoren in diesen Rollen können beliebige Filteraktionen auf andere Kategorien und Protokolle in ihren Richtlinien anwenden, aber die Kategorien und Protokolle, die in der Filter-Fixierung gesperrt sind, sind nicht zugelassen.

Änderungen an der Filter-Fixierung werden für alle verwalteten Clients implementiert, sobald die Änderungen gespeichert werden. Delegierte Administratoren, die mit Websense Manager arbeiten, wenn die Änderungen vorgenommen werden, können die Änderungen in ihren Filtern erst sehen, wenn sie sich das nächste Mal anmelden.

> **Hinweis**
> Wenn ein Filter aus der Rolle des übergeordneten Administrators in eine andere Rolle kopiert wird, werden die Einschränkungen der Filter-Fixierung in der Kopie übernommen.

Übergeordnete Administratoren werden durch die Filter-Fixierung nicht eingeschränkt. Sie können Richtlinien definieren, die den Zugriff auf Kategorien und Protokolle ermöglichen, die für delegierte Verwaltungsrollen gesperrt und fixiert sind. Aus diesem Grund sollten einzelne Benutzer, die spezielle Zugriffsrechte benötigen, von der Rolle des übergeordneten Administrators verwaltet werden.

Erstellen einer Filter-Fixierung

Verwandte Themen:

- *Definieren von Filtereinschränkungen für alle Rollen*, Seite 282
- *Fixieren von Kategorien*, Seite 284
- *Fixieren von Protokollen*, Seite 285

Auf der Seite **Richtlinien-Verwaltung > Filter-Fixierung** haben Sie die Wahl, ob Sie die Kategorien oder Protokolle so bearbeiten möchten, dass sie für alle verwalteten Clients in Rollen für die delegierte Verwaltung gesperrt sind. Jede Kategorie- oder Protokollfunktion, die in der Filter-Fixierung gesperrt ist, wird als **gesperrt und fixiert** angesehen.

- Klicken Sie auf die Schaltfläche **Kategorien**, um bestimmte Kategorien oder Kategorieelemente (Schlüsselworte und Dateitypen) zu sperren und zu fixieren. Siehe *Fixieren von Kategorien*, Seite 284.
- Klicken Sie auf die Schaltfläche **Protokolle**, um Protokolle oder die Aufzeichnung der Protokolle zu sperren und zu fixieren. Siehe *Fixieren von Protokollen*, Seite 285.

Fixieren von Kategorien

Verwandte Themen:

- *Definieren von Filtereinschränkungen für alle Rollen*, Seite 282
- *Erstellen einer Filter-Fixierung*, Seite 283
- *Fixieren von Protokollen*, Seite 285

Wählen Sie auf der Seite **Richtlinienverwaltung > Filter-Fixierung > Kategorien** die Kategorien aus, die für alle Mitglieder der delegierten Verwaltungsrollen gesperrt und fixiert werden sollen. Sie können Schlüsselworte und Dateitypen auch für eine Kategorie sperren und fixieren.

1. Wählen Sie in der Struktur eine Kategorie aus.

   Delegierte Administratoren haben keinen Zugriff auf benutzerdefinierte Kategorien, die von übergeordneten Administratoren erstellt wurden. Aus diesem Grund werden benutzerdefinierte Kategorien nicht in dieser Struktur angezeigt.

2. Legen Sie die Einschränkungen für diese Kategorie in dem Feld fest, das neben der Kategoriestruktur angezeigt wird.

Option	Beschreibung
Kategorie fixieren	Sperrt und fixiert den Zugriff auf Sites in dieser Kategorie.
Schlüsselworte fixieren	Sperrt und fixiert den Zugriff basierend auf den Schlüsselworten, die für diese Kategorie in jeder Rolle definiert sind.
Dateitypen fixieren	Sperrt und fixiert die ausgewählten Dateitypen für Sites in dieser Kategorie. Aktivieren Sie das Kontrollkästchen für jeden Dateityp, der gesperrt und fixiert werden soll. Benutzerdefinierte Dateitypen, die vom übergeordneten Administrator erstellt werden, sind in dieser Liste enthalten, weil sie für delegierte Verwaltungsrollen verfügbar sind.
Auf Unterkategorien anwenden	Wendet dieselben Einstellungen auf alle Unterkategorien dieser Kategorie an.

   Sie können ausgewählte Elemente für alle Kategorien ggf. sofort sperren und fixieren. Klicken Sie in der Struktur auf die Option **Alle Kategorien** und wählen Sie danach die Elemente aus, die für alle Kategorien gesperrt werden sollen. Klicken Sie anschließend auf die Option **Auf Unterkategorien anwenden**.

3. Wenn Sie alle Änderungen vorgenommen haben, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Kehren Sie dann zur Seite "Filter-Fixierung" zurück. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Fixieren von Protokollen

Verwandte Themen:

- *Definieren von Filtereinschränkungen für alle Rollen*, Seite 282
- *Erstellen einer Filter-Fixierung*, Seite 283
- *Fixieren von Kategorien*, Seite 284

Öffnen Sie die Seite **Richtlinienverwaltung > Filter-Fixierung > Protokolle**, um für alle Clients, die von delegierten Verwaltungsrollen verwaltet werden, den Zugriff auf ausgewählte Protokolle zu sperren und zu fixieren bzw. die Aufzeichnung ausgewählter Protokolle zu fixieren.

Hinweis

Die Aufzeichnung von Protokollen ist mit Alerts zur Nutzung von Protokollen verbunden. Sie können für ein Protokoll nur dann nutzungsbezogene Alerts erstellen, wenn die Aufzeichnung in mindestens einem Protokollfilter eingerichtet ist. Durch die Aktivierung der Option **Protokollierung für Protokoll fixieren** in der Filter-Fixierung wird sichergestellt, dass für das Protokoll nutzungsbezogene Alerts erstellt werden können. Siehe *Konfigurieren der Alerts zur Nutzung von Protokollen*, Seite 309.

1. Wählen Sie in der Struktur ein Protokoll aus.

   Rollen für die delegierte Verwaltung haben Zugriff auf benutzerdefinierte Protokolle, die vom übergeordneten Administrator erstellt werden. Aus diesem Grund werden in der Struktur benutzerdefinierte Protokolle angezeigt.

2. Legen Sie die Einschränkungen für dieses Protokoll in dem Feld fest, das neben der Protokollstruktur angezeigt wird.

Option	Beschreibung
Protokoll fixieren	Sperrt und fixiert den Zugriff auf Anwendungen und Websites, die dieses Protokoll verwenden.
Protokollierung für Protokoll fixieren	Zeichnet Informationen über den Zugriff auf dieses Protokoll auf und verhindert, dass delegierte Administratoren die Aufzeichnung deaktivieren.
Auf Gruppe anwenden	Wendet dieselben Einstellungen auf alle Protokolle in der Gruppe an.

3. Wenn Sie alle Änderungen vorgenommen haben, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Kehren Sie dann zur Seite "Filter-Fixierung" zurück. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

12 Websense-Serververwaltung

Verwandte Themen:

- *Websense-Produktkomponenten*, Seite 288
- *Arbeiten mit Policy Server*, Seite 294
- *Anzeigen und Exportieren des Überwachungsprotokolls*, Seite 300
- *Anhalten und Starten der Websense-Dienste*, Seite 302
- *Alerts*, Seite 303
- *Sichern und Wiederherstellen der Websense-Daten*, Seite 312

Für die Filterung der Internetnutzung sind Interaktionen zwischen verschiedenen Websense-Softwarekomponenten erforderlich.

- Benutzeranforderungen von Websites gehen in Network Agent oder einem Integrationsprodukt eines anderen Herstellers ein.
- Die Anforderungen werden an Websense Filtering Service zur Verarbeitung gesendet.
- Filtering Service kommuniziert mit Policy Server und Policy Broker, um für die Anforderung die geeignete Richtlinie anzuwenden.

In den meisten Umgebungen enthält die Policy Database Client-, Filter-, Richtlinien- und allgemeine Konfigurationsinformationen – unabhängig davon, ob es sich um einen oder mehrere Policy Server handelt.

Jede Instanz von Websense Manager ist einer einzelnen Policy Database zugewiesen und kann für die Konfiguration von jedem Policy Server verwendet werden, der der Datenbank zugewiesen ist.

Da die in Websense Manager durchgeführte Richtlinienkonfiguration in der zentralen Datenbank gespeichert ist, stehen die Richtlinieninformationen automatisch für alle Policy Server bereit, die dieser Policy Database zugewiesen sind.

Websense-Produktkomponenten

Verwandte Themen:

- *Filterkomponenten*, Seite 289
- *Reporting-Komponenten*, Seite 291
- *Komponenten für die Identifikation von Benutzern*, Seite 292
- *Arbeiten mit Policy Server*, Seite 294
- *Anhalten und Starten der Websense-Dienste*, Seite 302
- *Überprüfen des aktuellen Systemstatus*, Seite 311

Die Websense-Software besteht aus verschiedenen Komponenten, die zusammen die Identifikation von Benutzern, die Filterung von Internetaktivitäten und die Berichterstellung ermöglichen. In diesem Abschnitt finden Sie eine Übersicht über jede Komponente, die die Filterumgebung verständlich erklärt und Ihnen dabei hilft, Ihre Umgebung zu verwalten.

Zu den primären Websense-Komponenten gehören die Folgenden:

- Policy Database
- Policy Broker
- Policy Server
- Filtering Service
- Network Agent
- Master Database
- Websense Manager
- Usage Monitor
- User Service
- Log Server
- Protokolldatenbank

Die Websense-Software umfasst außerdem optionale Agenten für die transparente Identifikation:

- DC Agent
- RADIUS Agent
- eDirectory Agent
- Logon Agent

Weitere optionale Komponenten sind u. a.:

- Remote Filtering Server
- Remote Filtering Client

- Websense Content Gateway

Filterkomponenten

Komponente	Beschreibung
Policy Database	Speichert Websense-Softwareeinstellungen und Richtlinieninformationen.
Policy Broker	Verwaltet Anfragen von Websense-Komponenten nach Richtlinien- und allgemeinen Konfigurationsinformationen.
Policy Server	• Identifiziert und verfolgt den Speicherort und Status der anderen Websense-Komponenten. • Speichert Konfigurationsinformationen, die speziell für eine einzelne Policy Server-Instanz gelten. • Kommuniziert Konfigurationsdaten an Filtering Service, die für die Filterung von Internetanforderungen verwendet werden. Konfigurieren Sie Policy Server-Einstellungen in Websense Manager (siehe *Arbeiten mit Policy Server*, Seite 294). Policy Server, die eine Policy Database gemeinsam verwenden, verfügen über dieselben Richtlinien- sowie die meisten anderen Konfigurationseinstellungen (siehe *Arbeiten in einer Umgebung mit mehreren Policy Servern*, Seite 295).
Filtering Service	Bietet in Verbindung mit Network Agent oder einem Integrationsprodukt eines anderen Herstellers die Filterung von Internetaktivitäten. Wenn ein Benutzer eine Site anfordert, erhält Filtering Service die Anforderung und bestimmt, welche Richtlinie gilt. • Filtering Service muss ausgeführt werden, damit Internetanforderungen gefiltert und protokolliert werden. • Jede Filtering Service-Instanz lädt ihr eigenes Exemplar der Websense-Stammdatenbank (Websense Master Database) herunter. Konfigurieren Sie die Filterung und das Filtering Service-Verhalten in Websense Manager (siehe *Filter für die Internetnutzung*, Seite 39, und *Konfigurieren von Websense-Filtereinstellungen*, Seite 60).
Network Agent	• Verbessert die Filter- und Protokollfunktionen. • Aktiviert die Protokollverwaltung. • Aktiviert die Filterung in einer Standalone-Umgebung. Weitere Informationen finden Sie unter *Netzwerkkonfiguration*, Seite 363.

Komponente	Beschreibung
Master Database	• Umfasst über 36 Millionen Websites, die in über 90 Kategorien und Unterkategorien eingeteilt sind. • Enthält über 100 Protokolldefinitionen zur Verwendung in Filterungsprotokollen. Laden Sie die Websense Master Database herunter, um die Filterung von Internetaktivitäten zu aktivieren, und stellen Sie sicher, dass sich die Datenbank immer auf dem neuesten Stand befindet. Wenn die Master Database über zwei Wochen alt ist, ist keine Filterung möglich. Weitere Informationen finden Sie unter *Die Websense Master Database*, Seite 32.
Websense Manager	Dienst als Oberfläche für die Konfiguration und Verwaltung der Websense-Software. Verwenden Sie Websense Manager, um Richtlinien für den Zugriff auf das Internet zu definieren und anzupassen, Clients für die Filterung hinzuzufügen oder zu entfernen, Websense-Softwarekomponenten zu konfigurieren u. v. m. Weitere Informationen finden Sie unter *Arbeiten in Websense Manager*, Seite 17.
Usage Monitor	Aktiviert Alerts basierend auf der Internetnutzung. Usage Monitor verfolgt den Zugriff auf URL-Kategorien und Protokolle und generiert Alerts gemäß dem Alert-Verhalten, das Sie konfiguriert haben. Weitere Informationen finden Sie unter *Alerts*, Seite 303.
Remote Filtering Client	• Befindet sich auf einem Clientcomputer außerhalb der Netzwerk-Firewall. • Identifiziert die Computer als Clients, die gefiltert werden müssen, und kommuniziert mit Remote Filtering Server. Weitere Informationen finden Sie unter *Filtern von Remote Clients*, Seite 167.
Remote Filtering Server	• Erlaubt die Filterung von Clients außerhalb einer Netzwerk-Firewall. • Kommuniziert mit Filtering Service, um für ferne Computer den Zugriff auf das Internet zu verwalten. Weitere Informationen finden Sie unter *Filtern von Remote Clients*, Seite 167.

Komponente	Beschreibung
Websense Content Gateway	• Bietet eine stabile Proxy- und Cache-Plattform. • Kann den Inhalt von Websites und Dateien in Echtzeit analysieren, um Sites ohne Kategoriezuordnung zu kategorisieren. Siehe *Analysieren des Inhalts mit den Echtzeit-Optionen*, Seite 153.
Websense Security Gateway	Zusätzlich zu den Standardfunktionen von Websense Content Gateway: • Analysiert HTML-Code, um Sicherheitsbedrohungen zu finden (z. B. Phishing, URL-Umleitung, Web-Exploits und Umgehung durch Proxy). • Untersucht den Inhalt der Dateien und weist eine Bedrohungskategorie zu (z. B. Virus, Trojanisches Pferd oder Wurm). • Entfernt aktiven Inhalt aus bestimmten Webseiten. Siehe *Analysieren des Inhalts mit den Echtzeit-Optionen*, Seite 153.

Reporting-Komponenten

Komponente	Beschreibung
Log Server	Protokolliert Internetanfragedaten, einschließlich: • Die Anfragequelle • Die Kategorie oder das Protokoll, die bzw. das der Anfrage zugewiesen ist • Ob die Anfrage zugelassen oder gesperrt wurde • Ob eine Sperrfunktion für Schlüsselworte oder Dateitypen, Quotenzuordnungen, Bandbreitenebenen oder Passwortschutz angewendet wurden. Zusammen mit Network Agent und einigen Integrationsprodukten speichert Log Server außerdem Informationen über die Menge der verwendeten Bandbreite. Log Server muss auf einem Windows-Computer installiert sein, um in Websense Manager Untersuchungs- und Präsentationsberichte sowie Diagramme auf den Seiten "Heute" und "Verlauf" zu ermöglichen. Nach der Installation von Log Server muss Filtering Service so konfiguriert werden, dass die Protokolldaten an die korrekte Position weitergeleitet werden (siehe *Konfigurieren von Filtering Service für die Protokollierung*, Seite 326).
Log Database	Speichert Internetanfragedaten, die von Log Server erfasst wurden, für die Verwendung durch Websense Reporting Tools.

Komponenten für die Identifikation von Benutzern

Komponente	Beschreibung
User Service	• Kommuniziert mit Ihrem Verzeichnisdienst. • Vermittelt benutzerbezogene Informationen, einschließlich Benutzer-/Gruppen- und Benutzer-/Domänenbeziehungen, die für die Anwendung von Filterrichtlinien verwendet werden, an Policy Server und Filtering Service. Wenn Sie einen Agenten für die transparente Identifikation von Websense installiert und konfiguriert haben (siehe *Transparente Identifikation*, Seite 213), hilft User Service bei der Interpretation der Informationen über Benutzeranmeldesitzungen und verwendet diese Informationen für die Bereitstellung der Zuweisungen zwischen Benutzername und IP-Adresse an Filtering Service. Wenn Sie Benutzer und Gruppen als Websense-Clients hinzufügen (siehe *Hinzufügen eines Clients*, Seite 73), stellt User Service Namen- und Pfadinformationen aus dem Verzeichnisdienst für Websense Manager bereit. Informationen über die Konfiguration des Zugriffs auf Verzeichnisdienste finden Sie unter *Verzeichnisdienste*, Seite 67.
DC Agent	• Bietet für Benutzer in einem Windows-basierten Verzeichnisdienst eine transparente Identifikation von Benutzern. • Kommuniziert mit User Service, um die neuesten Informationen über Benutzeranmeldesitzungen der Websense-Software zur Verwendung bei der Filterung bereitzustellen. Weitere Informationen finden Sie unter *DC Agent*, Seite 225.
Logon Agent	• Zeichnet sich durch unübertroffene Genauigkeit bei der transparenten Identifikation von Benutzern in Linux- und Windows-Netzwerken aus. • Benötigt keinen Verzeichnisdienst oder andere Zwischendienste für die Erfassung von Benutzeranmeldesitzungen. • Erkennt Benutzeranmeldesitzungen, wenn sie vorkommen. Logon Agent kommuniziert mit der Anmeldeanwendung auf Clientcomputern, um sicherzustellen, dass einzelne Benutzeranmeldesitzungen von der Websense-Software direkt erfasst und verarbeitet werden. Weitere Informationen finden Sie unter *Logon Agent*, Seite 229.

Komponente	Beschreibung
eDirectory Agent	• Arbeitet mit Novell eDirectory zusammen, um Benutzer transparent zu identifizieren. • Erfasst Informationen über die Benutzeranmeldesitzung von Novell eDirectory, wodurch Benutzer authentifiziert werden, die sich im Netzwerk anmelden. • Weist jedem authentifizierten Benutzer eine IP-Adresse zu und arbeitet anschließend mit User Service zusammen, um die Informationen an Filtering Service weiterzuleiten. Weitere Informationen finden Sie unter *eDirectory Agent*, Seite 237.
RADIUS Agent	Ermöglicht die transparente Identifikation von Benutzern, die auf das Netzwerk über eine Einwahlverbindung oder über VPN (Virtual Private Network), DSL (Digital Subscriber Line) bzw. eine andere ferne Verbindung zugreifen. Weitere Informationen finden Sie unter *RADIUS Agent*, Seite 232.

Policy Database

Die Websense Policy Database speichert sowohl die Richtliniendaten (einschließlich Clients, Filter, Filterkomponenten und Einstellungen für die delegierte Verwaltung) als auch globale Konfigurationseinstellungen, die in Websense Manager angegeben sind. Einstellungen, die speziell für eine einzelne Policy Server-Instanz gelten, werden getrennt gespeichert.

In den meisten Umgebungen mit mehreren Policy Servern enthält eine einzelne Policy Database die Richtlinien- und allgemeinen Konfigurationsdaten für mehrere Policy Server.

1. Beim Start fordert jede Websense-Komponente die zutreffenden Konfigurationsinformationen von der Policy Database über Policy Broker an.
2. Ausgeführte Komponenten prüfen häufig auf Änderungen an der Policy Database.
3. Die Policy Database wird jedes Mal aktualisiert, wenn Administratoren Änderungen in Websense Manager vornehmen und auf die Option "Alles speichern" klicken.
4. Nach einer Änderung in der Policy Database werden von jeder Komponente die Änderungen angefordert und erhalten, die Auswirkungen auf ihre Funktionalität haben.

Sichern Sie die Policy Database regelmäßig, um wichtige Konfigurations- und Richtlinieninformationen zu schützen. Weitere Informationen finden Sie unter *Sichern und Wiederherstellen der Websense-Daten*, Seite 312.

Arbeiten mit Policy Server

Policy Server ist die Websense-Softwarekomponente, die die Richtlinieninformationen verwaltet und durch die Kommunikation mit Filtering Service die Richtliniendurchsetzung unterstützt. Policy Server ist auch dafür zuständig, andere Komponenten zu identifizieren und ihren Speicherort sowie Status zu verfolgen.

Wenn Sie sich bei Websense Manager anmelden, erfolgt die Anmeldung bei der grafischen Benutzeroberfläche von Policy Server.

- Sie können sich erst dann bei Websense Manager anmelden, wenn die Software für die Kommunikation mit Policy Server konfiguriert wurde.
- Wenn Ihre Websense-Installation mehrere Policy Server umfasst, können Sie bei der Anmeldung eine Policy Server-Instanz auswählen.
- Sie können eine Policy Server-Instanz in Websense Manager hinzufügen oder entfernen.

In der Standardeinstellung wird die Kommunikation zwischen Websense Manager und einer zentralen Policy Server-Instanz während der Installation von Websense Manager eingerichtet.

In den meisten Umgebungen wird nur ein Policy Server benötigt. Lastenausgleich wird dadurch ermöglicht, dass ein einzelner Policy Server mit mehreren Filtering Service- und Network Agent-Instanzen kommunizieren kann. In sehr großen Organisationen (über 10.000 Benutzer) kann es jedoch vorteilhaft sein, mehrere Policy Server-Instanzen zu installieren. Wenn Sie zusätzliche Policy Server installieren, fügen Sie jede Instanz zu Websense Manager hinzu (siehe *Hinzufügen und Bearbeiten von Policy Server-Instanzen*, Seite 294).

Hinzufügen und Bearbeiten von Policy Server-Instanzen

Auf der Seite **Einstellungen > Policy Server** können Sie Policy Server-Instanzen zu Websense Manager hinzufügen oder vorhandene Policy Server konfigurieren oder entfernen.

So fügen Sie eine Policy Server-Instanz hinzu:

1. Klicken Sie auf **Hinzufügen**. Die Seite "Policy Server hinzufügen" wird geöffnet.
2. Geben Sie im Feld **IP oder Name des Servers** die IP-Adresse oder den Hostnamen des Policy Server-Computers ein.
3. Geben Sie den **Port** ein, den Websense Manager für die Kommunikation mit dieser Policy Server-Instanz verwenden soll. Der Standardwert ist **55806**.
4. Klicken Sie auf **OK**, um zur Seite "Policy Server" zurückzukehren. Die neue Policy Server-Instanz wird in der Liste angezeigt.
5. Klicken Sie auf **OK**, um alle Änderungen auf der Seite "Policy Server" im Cache zwischenzuspeichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Wählen Sie in der Liste der Policy Server eine IP-Adresse oder einen Hostnamen aus und klicken Sie auf **Bearbeiten**, um eine Policy Server-Instanz zu bearbeiten (wenn sich z. B. die IP-Adresse oder der Name des Policy Server-Computers ändert).

Um eine Policy Server-Instanz zu löschen, wählen Sie in der Liste der Policy Server eine IP-Adresse oder einen Hostnamen aus und klicken Sie auf **Löschen**. Wenn Sie auf "Löschen" klicken, wird die Policy Server-Instanz aus Websense Manager entfernt, aber der Policy Server-Dienst von Websense wird nicht deinstalliert oder angehalten. Wenn in der Liste nur eine Policy Server-Instanz enthalten ist, kann diese Instanz nicht gelöscht werden.

Arbeiten in einer Umgebung mit mehreren Policy Servern

In einigen verteilten Umgebungen mit einer hohen Anzahl von Benutzern ist es u. U. vorteilhaft, mehrere Policy Server zu installieren. Dabei sind einige besondere Überlegungen anzustellen.

- Wenn Sie eine Konfiguration implementieren, die es zulässt, dass derselbe Client – abhängig von der aktuellen Last – von verschiedenen Policy Servern verwaltet wird, implementieren Sie **keine** Richtlinien-Aktionen, die auf der Zeit basieren:
  - Mit Passwort freigeben
  - Bestätigen
  - Quote

  Die zeitbezogenen Informationen, die mit diesen Funktionen verbunden sind, werden von den Policy Servern nicht freigegeben, und Clients könnten mehr oder weniger Internetzugriff erhalten, als beabsichtigt ist.

  Denken Sie daran, dass die Richtlinie "Standard" immer dann durchgesetzt wird, wenn keine andere Richtlinie auf einen Client angewendet werden kann. Wenn Clients mehreren Policy Servern unterliegen können, sollten Sie sicherstellen, dass die Richtlinie "Standard" keine Kategoriefilter durchsetzt, die zeitbezogene Aktionen durchsetzen.
- Da Richtlinieninformationen in der Policy Database gespeichert werden, werden Änderungen an den Richtlinien automatisch an alle Policy Server weitergegeben, wenn Sie auf **Alles speichern** klicken.
- Viele globale Konfigurationseinstellungen (z. B. Klassendefinitionen und Alert-Optionen) gelten ebenfalls für alle Policy Server.
- Konfigurationseinstellungen, die nur für einen einzelnen Policy Server gelten (z. B. die Filtering Service- und Network Agent-Verbindungen) werden von jedem Policy Server lokal gespeichert und nicht verteilt.

So wechseln Sie zwischen Policy Servern in Websense Manager, um die Einstellungen zu prüfen bzw. zu konfigurieren, die für eine einzelne Policy Server-Instanz gelten:

1. Erweitern Sie im Websense-Banner die Liste der **Policy Server** und wählen Sie eine IP-Adresse aus.

2. Wenn es nicht gespeicherte Änderungen in der aktuellen Instanz von Policy Server gibt, wird eine Warnmeldung angezeigt. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Abbrechen**, um bei der aktuellen Instanz von Policy Server angemeldet zu bleiben, damit Sie die Änderungen speichern können.
   - Klicken Sie auf **OK**, um die Änderungen zu verwerfen und sich bei einem neuen Policy Server anzumelden.
   - Klicken Sie auf **Zurück**, um mit der Konfiguration des aktuellen Policy Servers fortzufahren.

   Wenn keine ungespeicherten Änderungen vorkommen, wird das Fenster für die Anmeldung direkt geöffnet.
3. Geben Sie in diesem Fenster einen Benutzernamen und ein Passwort ein, um sich beim ausgewählten Policy Server anzumelden, und klicken Sie anschließend auf **Anmelden**.

Ändern der IP-Adresse des Policy Servers

Halten Sie alle Websense-Dienste auf dem Computer an, bevor Sie die IP-Adresse des Policy Server-Computers ändern. Wenn Websense Manager auf dem Computer installiert ist, gilt das auch für die Apache2Websense- und ApacheTomcatWebsense-Dienste.

Nachdem Sie die IP-Adresse geändert haben, müssen Sie die Websense-Konfigurationsdateien, die von Websense Manager, Policy Server und anderen Websense-Diensten verwendet werden, manuell aktualisieren, bevor Sie mit der Filterung fortfahren.

Schritt 1: Aktualisieren der Websense Manager-Konfiguration

Aktualisieren Sie Websense Manager, um die neue IP-Adresse für die Verbindung mit Policy Server zu verwenden.

1. Halten Sie ggf. auf dem Websense Manager-Computer die **Apache2Websense-** und **ApacheTomcatWebsense-**Dienste an.

   Wenn Websense Manager und Policy Server auf demselben Computer installiert sind, sollten die Apache-Dienste bereits angehalten worden sein.
2. Wechseln Sie zum folgenden Verzeichnis:
   - Windows:

     `C:\Program Files\Websense\tomcat\conf\Catalina\localhost\`
   - Linux:

     `/opt/Websense/tomcat/conf/Catalina/localhost/`
3. Suchen Sie nach der Datei **mng.xml** und erstellen Sie eine Sicherungskopie der Datei in einem anderen Verzeichnis.
4. Öffnen Sie die Datei **mng.xml** in einem Texteditor (z. B. in Editor oder vi) und ersetzen Sie jede Instanz der alten IP-Adresse des Policy Servers durch die neue.

Die IP-Adresse des Policy Servers wird zweimal angezeigt: als der Wert **ps/default/host** und als der Wert **psHosts**.

5. Speichern Sie anschließend die Datei und schließen Sie sie.

Starten Sie die Apache-Dienste erst dann neu, wenn Sie die übrigen Konfigurationsaktualisierungen in diesem Abschnitt abgeschlossen haben.

Schritt 2: Aktualisieren der Policy Server-Konfiguration

Aktualisieren Sie die Konfigurationsdatei des Policy Servers sowie die Initialisierungsdatei, die verwendet wird, um die Kommunikation zwischen Websense-Komponenten zu konfigurieren.

1. Halten Sie auf dem Policy Server-Computer alle Websense-Dienste an, falls das noch nicht geschehen ist (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).
2. Wechseln Sie zum Websense-Verzeichnis **bin**.
   - Windows:

     `C:\Program Files\Websense\bin`
   - Linux:

     `/opt/Websense/bin`
3. Suchen Sie nach der Datei **config.xml**, und erstellen Sie eine Sicherungskopie der Datei in einem anderen Verzeichnis.
4. Öffnen Sie die Datei **config.xml** in einem Texteditor und ersetzen Sie jede Instanz der alten IP-Adresse des Policy Servers durch die neue.
5. Speichern Sie anschließend die Datei und schließen Sie sie.
6. Suchen Sie im Verzeichnis **bin** nach der Datei **websense.ini** und erstellen Sie eine Sicherungskopie der Datei in einem anderen Verzeichnis.
7. Öffnen Sie die Datei **websense.ini** in einem Texteditor und ersetzen Sie jede Instanz der alten IP-Adresse des Policy Servers durch die neue.
8. Speichern Sie anschließend die Datei und schließen Sie sie.

Schritt 3: Überprüfen der Protokolldatenbank-Verbindung

Verwenden Sie Windows ODBC Data Source Administrator auf dem Policy Server-Computer, um die ODBC-Verbindung mit der Protokolldatenbank zu überprüfen.

1. Klicken Sie auf **Start > Einstellungen > Systemsteuerung > Verwaltung > Datenquellen (ODBC)**.
2. Wählen Sie auf der Registerkarte **System-DSN** einen geeigneten Datenquellennamen aus (in der Standardeinstellung **wslogdb70**) und klicken sie auf **Konfigurieren**.
3. Überprüfen Sie, dass der richtige Datenbankservercomputer ausgewählt ist und klicken Sie auf **Weiter**.
4. Geben Sie die Anmeldeinformationen ein, die für die Verbindung mit der Datenbank verwendet werden, und klicken Sie auf **Weiter**.

5. Übernehmen Sie in den nächsten beiden Anzeigen die Standardwerte und klicken Sie auf **Datenquelle testen**.

   Hinweis

   Wenn der Test fehlschlägt, prüfen Sie den Namen des Datenbankservercomputers und versuchen Sie es erneut.

   Wenn der Computername richtig ist, aber der Test weiterhin fehlschlägt, überprüfen Sie, ob der richtige Verbindungsport verwendet wird und ob die Firewall die Kommunikation am ausgewählten Port zulässt.

Schritt 4: Neustarten des Websense-Dienstes

1. Starten Sie den Policy Server-Computer neu. Stellen Sie sicher, dass alle Websense-Dienste auf dem Computer ordnungsgemäß gestartet werden.
2. Wenn der Websense Manager, der für die Konfiguration dieses Policy Servers verwendet wurde, auf einem anderen Computer installiert ist, starten Sie die **Apache2Websense-** und **ApacheTomcatWebsense-**Dienste auf diesem Computer neu.

   Hinweis

   Wenn Websense Manager auf demselben Computer wie Policy Server installiert ist, müssen die Administratoren die neue IP-Adresse verwenden, um sich anzumelden.

Arbeiten mit Filtering Service

Filtering Service ist die Websense-Softwarekomponente, die zusammen mit Network Agent oder einem Integrationsprodukt eines anderen Herstellers die Internetaktivität filtert. Wenn ein Benutzer eine Site anfordert, erhält Filtering Service diese Anforderung, bestimmt, welche Richtlinie gültig ist, und verwendet die zutreffende Richtlinie, um festzustellen, wie die Site gefiltert werden soll.

Jede Filtering Service-Instanz lädt ihr eigenes Exemplar der Websense-Stammdatenbank (Websense Master Database) herunter und verwendet diese, um festzustellen, wie die Internetanforderungen gefiltert werden sollen.

Filtering Service sendet Informationen über Internetaktivitäten auch an Log Server, damit diese aufgezeichnet und für die Berichterstellung verwendet werden können.

Wenn Sie sich bei Websense Manager anmelden, werden auf der Seite "Status > Heute" unter **Zusammenfassung des Filtering Service** die IP-Adresse und der aktuelle Status von jeder Filtering Service-Instanz aufgeführt, die dem aktuellen Policy Server zugewiesen sind. Klicken Sie auf die IP-Adresse eines Filtering Service, um ausführlichere Informationen über den ausgewählten Filtering Service anzuzeigen.

Prüfen der Filtering Service-Details

Prüfen Sie den Status einer einzelnen Filtering Service-Instanz auf der Seite **Status > Heute > Detailinformationen für Filtering Service**.

Auf der Seite ist Folgendes aufgeführt:

- Die IP-Adresse des Filtering Service
- Ob die ausgewählte Instanz ausgeführt wird
- Die Filtering Service-Version

  Diese sollte mit der Version Ihrer Websense-Software übereinstimmen – einschließlich der angewendeten Hotfixes.
- Das Betriebssystem, das auf dem Filtering Service-Computer ausgeführt wird
- Die Websense-Softwareplattform

  Aus dieser Angabe ist ersichtlich, ob die Websense-Software im Standalone-Modus ausgeführt wird oder mit einem Produkt eines anderen Herstellers integriert ist.
- Die IP-Adresse und der Status aller Network Agent-Instanzen, mit denen der ausgewählte Filtering Service kommuniziert

Klicken Sie auf **Schließen**, um zur Seite "Heute" zurückzukehren.

Überprüfen des Download-Status der Stammdatenbank (Master Database)

Jede Filtering Service-Instanz in Ihrem Netzwerk lädt ihre eigene Kopie der Stammdatenbank (Master Database) herunter. Wenn Sie in Websense Manager arbeiten, wird auf der Seite "Status > Heute" in der Zusammenfassung der zustandsbezogenen Alerts eine Statusmeldung angezeigt, wenn ein Download-Vorgang der Stammdatenbank (Master Database) durchgeführt wird oder wenn der Download-Vorgang fehlschlägt.

Klicken Sie in der Symbolleiste auf der Seite "Heute" auf **Datenbank-Download**, um ausführliche Informationen über vor Kurzem durchgeführte oder aktuelle Datenbank-Downloads herunterzuladen. Auf der Seite "Datenbank-Download" gibt es einen Eintrag für jede Filtering Service-Instanz, die dem aktuellen Policy Server zugewiesen ist.

Auf der Seite "Datenbank-Download" wird zunächst eine Kurzübersicht über die Downloads angezeigt, die die folgenden Informationen enthält: wo die Datenbank heruntergeladen wurde, welche Datenbankversion heruntergeladen wurde und ob der Download erfolgreich war. In der Übersichtsansicht stehen die folgenden Optionen bereit:

- Initiieren Sie einen Datenbank-Download für einen einzelnen Filtering Service (klicken Sie auf **Aktualisieren**).
- Initiieren Sie Datenbank-Downloads für alle aufgeführten Filtering Service-Instanzen (klicken Sie auf **Alles aktualisieren**).

- Brechen Sie eine oder alle laufenden Aktualisierungen ab.

Klicken Sie in der Liste auf der rechten Seite auf eine IP-Adresse, um ausführlichere Statusdaten über den Datenbank-Download des ausgewählten Filtering Service zu überprüfen.

- Wenn beim Download des ausgewählten Filtering Service Probleme aufgetreten sind, wird möglicherweise eine Empfehlung angezeigt, wie sich das Problem am besten bewältigen lässt.
- Klicken Sie auf **Aktualisieren**, um für den ausgewählten Filtering Service einen Datenbank-Download manuell zu initiieren.

Während des Datenbank-Downloads werden in der Statusanzeige detaillierte Verlaufsinformationen für jede Phase des Download-Vorgangs bereitgestellt. Klicken Sie auf **Schließen**, um die Verlaufsinformationen auszublenden und mit der Arbeit in Websense Manager fortzufahren.

Wieder aufnehmbare Downloads der Stammdatenbank (Master Database)

Wenn der Download der Stammdatenbank (Master Database) unterbrochen wird, versucht die Websense-Software automatisch, den Download-Vorgang wieder aufzunehmen. Wenn Filtering Service die Verbindung zum Download-Server wiederherstellen kann, wird der Download-Vorgang an der Stelle wieder aufgenommen, an der er unterbrochen wurde.

Sie können einen fehlgeschlagenen oder unterbrochenen Download-Vorgang manuell neu starten. In dem Fall wird der Download-Vorgang nicht an der Stelle wieder aufgenommen, an der er unterbrochen wurde, sondern am Anfang neu gestartet.

1. Wechseln Sie in Websense Manager zu **Status > Heute** und klicken Sie auf **Datenbank-Download**.
2. Klicken Sie auf **Alle Aktualisierungen stoppen**, um den unterbrochenen Vorgang zu beenden.
3. Wählen Sie eine Filtering Service-Instanz aus und klicken Sie auf **Aktualisieren**, oder klicken Sie auf **Alles aktualisieren**, um den Download-Vorgang neu zu starten.

Anzeigen und Exportieren des Überwachungsprotokolls

Die Websense-Software stellt ein Überwachungsprotokoll bereit, in dem angezeigt wird, welche Administratoren auf Websense Manager zugegriffen haben und welche Änderungen an Richtlinien und Einstellungen vorgenommen wurden. Diese Informationen stehen nur den übergeordneten Administratoren (Super Administrators) zur Verfügung, denen Richtlinienberechtigungen erteilt wurden (siehe *Übergeordnete Administratoren*, Seite 253).

Delegierte Administratoren haben erhebliche Kontrolle über die Internetaktivitäten ihrer verwalteten Clients. Indem Sie ihre Änderungen über das Protokoll überwachen, können Sie sicherstellen, dass die Kontrolle verantwortlich und in Einklang mit den in Ihrer Organisation geltenden Nutzungsrichtlinien ausgeübt wird.

Auf der Seite **Status > Überwachungsprotokoll** können Sie das Überwachungsprotokoll anzeigen und ausgewählte Abschnitte davon an ein Excel-Arbeitsblatt (XLS) exportieren.

Datensätze aus Überwachungsprotokollen werden 60 Tage lange gespeichert. Um diese Datensätze länger als 60 Tage aufzubewahren, exportieren Sie das Protokoll mit der Exportoption auf regelmäßiger Basis. Durch das Exportieren werden keine Datensätze aus dem Überwachungsprotokoll entfernt.

Wenn die Seite "Überwachungsprotokoll" geöffnet wird, wird der neueste Datensatz angezeigt. Verwenden Sie die Bildlaufleiste und die Seitenschaltflächen über dem Protokoll, um ältere Datensätze anzuzeigen.

Im Protokoll werden die folgenden Informationen angezeigt. Wenn ein Element abgeschnitten ist, klicken Sie auf den angezeigten Eintrag, um den vollständigen Datensatz in einem Popup-Dialogfeld anzuzeigen.

Spalte	Beschreibung
Datum	Datum und Uhrzeit der Änderung, an die Zeitzone angepasst. Um sicherzustellen, dass die Daten im Überwachungsprotokoll einheitlich sind, müssen die Datums- und Uhrzeiteinstellungen auf allen Computern synchronisiert werden, auf denen Websense-Komponenten ausgeführt werden.
Benutzer	Benutzername des Administrators, der die Änderung vorgenommen hat.
Server	IP-Adresse oder Name des Computers, auf dem der Policy Server ausgeführt wird, der von der Änderung betroffen ist. Diese Angabe wird nur für Änderungen angezeigt, die den Policy Server betreffen, z. B. Änderungen, die auf der Registerkarte "Einstellungen" vorgenommen wurden.
Rolle	Rolle für die delegierte Verwaltung, die von der Änderung betroffen ist. Wenn eine Änderung einen Client betrifft, der in der Rolle für die delegierte Verwaltung ausdrücklich als verwalteter Client zugewiesen wurde, wird für diese Änderung angezeigt, dass sie sich auf die Rolle des übergeordneten Administrators auswirkt. Wenn eine Änderung einen Client betrifft, der Mitglied eines Netzwerkbereichs, einer Gruppe, Domäne oder Organisationseinheit ist, der bzw. die der Rolle zugewiesen ist, wird für die Änderung angezeigt, dass sie sich auf die Rolle für die delegierte Verwaltung auswirkt.
Typ	Das geänderte Konfigurationselement, z. B. Richtlinie, Kategoriefilter oder An-/Abmeldung.
Element	Kennung des spezifischen geänderten Objekts, z. B. Name des Kategoriefilters oder der Rolle.

Spalte	Beschreibung
Aktion	Art der vorgenommenen Änderung, z. B. Hinzufügen, Löschen, Ändern, Anmelden usw.
Vorher	Wert vor der Änderung.
aktuell	Neuer Wert nach der Änderung.

Es werden nicht alle Elemente für alle Datensätze angezeigt. Für An- und Abmeldungsdatensätze wird die Rolle z. B. nicht angezeigt.

So exportieren Sie Datensätze des Überwachungsprotokolls:

1. Wählen Sie aus der Liste **Exportbereich** eine Zeitperiode aus.

   Wählen Sie die Option **Letzte 60 Tage**, um die gesamte Überwachungsprotokolldatei zu exportieren.
2. Klicken Sie auf **Starten**.

   Wenn Microsoft Excel auf dem Computer installiert ist, auf dem Websense Manager ausgeführt wird, wird die exportierte Datei geöffnet. Speichern oder drucken Sie die Datei mit den Excel-Optionen.

   Wenn Microsoft Excel auf dem Computer, auf dem Websense Manager ausgeführt wird, nicht installiert ist, führen Sie die Anweisungen auf dem Bildschirm aus, um entweder die Software zu finden oder die Datei zu speichern.

Anhalten und Starten der Websense-Dienste

Websense-Dienste sind so konfiguriert, dass sie jedes Mal gestartet werden, wenn der Computer neu gestartet wird. In manchen Fällen ist es allerdings erforderlich, eine oder mehrere Produktkomponenten unabhängig vom Neustart des Computers anzuhalten oder zu starten.

> **Hinweis**
> Wenn Filtering Service die Stammdatenbank (Master Database) herunterlädt, wird der Dienst solange ausgeführt, bis der Download-Vorgang abgeschlossen ist.

Wenn Sie alle Websense-Dienste anhalten, beenden Sie die folgenden Dienste – in der angezeigten Reihenfolge – immer zuletzt:

1. Websense Policy Server
2. Websense Policy Broker
3. Websense Policy Database

Hinweis: Wenn ein Problem nicht speziell mit Policy Broker oder der Policy Database zusammenhängt, ist es in den meisten Fällen nicht erforderlich, diese Services neu zu starten. Es ist besser, diese Dienste nicht neu zu starten, wenn es nicht unbedingt erforderlich ist.

Wenn Sie alle Websense-Dienste starten, starten Sie die folgenden Dienste – in der angezeigten Reihenfolge – immer zuerst:

1. Websense Policy Database
2. Websense Policy Broker
3. Websense Policy Server

Windows

1. Öffnen Sie das Dialogfeld von Windows Services (**Start > Einstellungen > Systemsteuerung > Verwaltung > Dienste**).
2. Klicken Sie mit der rechten Maustaste auf den Websense-Dienstnamen und wählen Sie **Stop** oder **Start** aus.

Linux

Auf Linux-Computern werden alle Dienste zusammen angehalten oder gestartet, wenn Sie diese Vorgehensweise einsetzen.

1. Wechseln Sie zum Verzeichnis **/opt/Websense**.
2. Überprüfen Sie den Status der Websense-Dienste mit dem Befehl:
   - `./WebsenseAdmin status`
3. Verwenden Sie die folgenden Befehle, um alle Websense-Dienste anzuhalten, zu starten oder neu zu starten:
   - `./WebsenseAdmin stop`
   - `./WebsenseAdmin start`
   - `./WebsenseAdmin restart`

Warnung

Verwenden Sie nicht den Befehl **kill**, um einen Websense-Dienst zu beenden, da der Dienst dadurch beschädigt werden könnte.

Alerts

Verwandte Themen:

- *Kontrolle der Anzahl von Alerts*, Seite 304
- *Konfigurieren allgemeiner Alert-Optionen*, Seite 305
- *Konfigurieren von System-Alerts*, Seite 307
- *Konfigurieren der Alerts zur Nutzung von Kategorien*, Seite 308
- *Konfigurieren der Alerts zur Nutzung von Protokollen*, Seite 309

Um die Verfolgung und Verwaltung der Websense-Software und der Internetaktivität der Clients zu erleichtern, können übergeordnete Administratoren Alerts so konfigurieren, dass sie gesendet werden, wenn ausgewählte Ereignisse auftreten.

- **System-Alerts**: Benachrichtigung über den Subskriptionsstatus und die Aktivität der Stammdatenbank (Master Database).
- **Nutzungsbezogene Alerts**: Benachrichtigung, wenn die Internetaktivität für bestimmte Kategorien oder Protokolle konfigurierte Schwellenwerte erreicht.

Alerts können an ausgewählte Empfänger per E-Mail, in Form von Popup-Nachrichten auf dem Bildschirm (Windows **Net Send** Nachrichten) oder per SNMP gesendet werden.

> **Hinweis**
> Popup-Alerts auf dem Bildschirm können nicht an Linux-Computer gesendet werden. Vorausgesetzt, dass der Samba-Client auf dem Linux-Computer installiert ist, können sie jedoch von einem Linux-Computer, auf dem Policy Server ausgeführt wird, an Windows-Computer gesendet werden. Siehe *Implementierungshandbuch*.

Nutzungsbezogene Alerts können sowohl für von Websense definierte als auch benutzerdefinierte Kategorien oder Protokolle erstellt werden.

Kontrolle der Anzahl von Alerts

Verwandte Themen:

- *Alerts*, Seite 303
- *Konfigurieren allgemeiner Alert-Optionen*, Seite 305
- *Konfigurieren der Alerts zur Nutzung von Kategorien*, Seite 308
- *Konfigurieren der Alerts zur Nutzung von Protokollen*, Seite 309

Integrierte Steuerelemente für nutzungsbezogene Alerts verhindern, dass eine übermäßige Anzahl von Alert-Nachrichten erzeugt wird. Schränken Sie über die Einstellung **Maximale Anzahl von Alerts pro Nutzungstyp** die Anzahl der Alerts ein, die in Reaktion auf Benutzeranforderungen von bestimmten Kategorien und Protokollen gesendet werden. Weitere Informationen finden Sie unter *Konfigurieren allgemeiner Alert-Optionen*, Seite 305.

Sie können auch für die einzelnen Alerts zur Nutzung von Kategorien und Protokollen Schwellenwerte festlegen. Wenn Sie für eine bestimmte Kategorie z. B. einen Schwellenwert von 10 festlegen, wird ein Alert generiert, nachdem diese Kategorie (von einer beliebigen Kombination von Clients) 10-mal angefordert wurde. Weitere Informationen finden Sie unter *Konfigurieren der Alerts zur Nutzung von Kategorien*, Seite 308, und *Konfigurieren der Alerts zur Nutzung von Protokollen*, Seite 309.

Angenommen, dass für die maximale Anzahl von Alerts 20 eingestellt ist und der Kategorie-Schwellenwert 10 beträgt, werden Administratoren nur die ersten 20 Male benachrichtigt, wenn Kategorieanforderungen den Schwellenwert überschreiten. Das bedeutet, dass nur für die ersten 200 Anforderungen Alert-Nachrichten generiert werden (Schwellenwert von 10 multipliziert mit einem Grenzwert für Alerts von 20).

Konfigurieren allgemeiner Alert-Optionen

Verwandte Themen:

- *Alerts*, Seite 303
- *Konfigurieren von System-Alerts*, Seite 307
- *Konfigurieren der Alerts zur Nutzung von Kategorien*, Seite 308
- *Konfigurieren der Alerts zur Nutzung von Protokollen*, Seite 309

Die Websense-Software kann Administratoren über verschiedene Arten von Systemereignissen benachrichtigen, z. B. Updates an Kategorien der Stammdatenbank (Master Database) und Subskriptionsprobleme sowie die Überschreitung definierter Schwellenwerte für die Internetnutzung.

Auf der Seite **Einstellungen > Alerts und Benachrichtigungen > Alerts** können Sie – wie weiter unten beschrieben – die gewünschten Benachrichtigungsmethoden auswählen und konfigurieren. Aktivieren Sie anschließend auf den anderen Seiten im Bereich "Einstellungen > Alerts und Benachrichtigungen" die Alerts, die Sie erhalten möchten.

1. Geben Sie im Feld **Maximale Anzahl von Alerts pro Nutzungstyp** eine Zahl ein, um die Gesamtanzahl der Alerts zu beschränken, die täglich für jede Kategorie und jedes Protokoll, die bzw. das für nutzungsbezogene Alerts definiert wurde, generiert werden.

   Sie können die Einstellungen z. B. so konfigurieren, dass ein nutzungsbezogenes Alert jedes fünfte Mal (Schwellenwert) gesendet wird, wenn jemand eine Site in der Kategorie "Sport" anfordert. Abhängig von der Anzahl der Benutzer und ihren Verhaltensmustern bei der Internetnutzung könnten auf diese Weise täglich Hunderte von Alerts generiert werden.

   Wenn Sie als maximale Anzahl von Alerts pro Nutzungstyp 10 eingeben, werden jeden Tag nur 10 Alert-Nachrichten für die Kategorie "Sport" generiert. In diesem Beispiel werden Sie von den Nachrichten über die ersten 50 Anforderungen nach Sport-Sites benachrichtigt (5 Anforderungen pro Alert multipliziert mit 10 Alerts).

2. Wählen Sie das Kontrollkästchen **E-Mail-Alerts aktivieren** aus, um Alerts und Benachrichtigungen per E-Mail zu senden. Konfigurieren Sie anschließend die E-Mail-Einstellungen.

IP oder Name des SMTP-Servers	IP-Adresse oder Name des SMTP-Servers, über den E-Mail-Alerts weitergeleitet werden sollten.
E-Mail-Adresse des Absenders	E-Mail-Adresse, die als Absender der E-Mail-Alerts verwendet werden soll.
E-Mail-Adresse des Administrators (An)	E-Mail-Adresse des Hauptempfängers der E-Mail-Alerts.
E-Mail-Adresse des Empfängers (Cc)	E-Mail-Adressen von bis zu 50 zusätzlichen Empfängern. Jede Adresse muss in einer separaten Zeile eingegeben werden.

3. Wählen Sie das Kontrollkästchen **Popup-Alerts aktivieren** aus, um Popup-Nachrichten auf bestimmten Computern anzuzeigen. Geben Sie anschließend in separaten Zeilen die IP-Adresse oder den Computernamen von bis zu 50 **Empfängern ein**.

Hinweis

Popup-Alerts können nicht an Linux-Computer gesendet werden. Vorausgesetzt, dass der Samba-Client auf dem Linux-Computer installiert ist, können sie jedoch von einem Linux-Computer, auf dem Policy Server ausgeführt wird, an Windows-Computer gesendet werden. Siehe *Implementierungshandbuch*.

4. Wählen Sie das Kontrollkästchen **SNMP-Alerts aktivieren** aus, um Alert-Nachrichten über ein SNMP-Trap-System zu senden, das in Ihrem Netzwerk installiert ist. Geben Sie anschließend die Daten über das SNMP-Trap-System ein.

Communityname	Name der Trap-Community auf Ihrem SNMP-Trap-Server.
IP oder Name des Servers	IP-Adresse oder Name des SNMP-Trap-Servers.
Port	Portnummer, die die SNMP-Nachrichten verwenden.

5. Wenn Sie fertig sind, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Konfigurieren von System-Alerts

Verwandte Themen:

- *Alerts*, Seite 303
- *Konfigurieren allgemeiner Alert-Optionen*, Seite 305
- *Überprüfen des aktuellen Systemstatus*, Seite 311

Auf der Seite **Status > Alerts** (detaillierte Informationen) werden von Websense Manager detaillierte Informationen über den Systemzustand und -status angezeigt. Siehe *Überprüfen des aktuellen Systemstatus*, Seite 311.

Stellen Sie sicher, dass Administratoren über bedeutende Systemereignisse – z. B. Fehler bei Datenbank-Downloads oder eine Subskription, die bald abläuft – benachrichtigt werden, auch wenn sie nicht bei Websense Manager angemeldet sind, indem Sie Websense-System-Alerts so konfigurieren, dass sie per E-Mail, in Form einer Popup-Nachricht oder über das SNMP-Trap-System verteilt werden.

Wählen Sie auf der Registerkarte "Einstellungen" über die Seite **Alerts und Benachrichtigungen > System** aus, welche Methode verwendet wird, um diese Alerts an die Websense-Administratoren zu senden, und welche Alerts gesendet werden sollen.

1. Wählen Sie für jeden Alert die zu verwendende Sendemethode aus. Abhängig von den Methoden, die auf der Seite "Alerts" ausgewählt sind, können Sie **E-Mail**, **Popup** und **SNMP** auswählen.

   Hinweis
   Es werden nicht nur Alerts generiert, sondern auch Informationen über Fehler beim Herunterladen der Stammdatenbank (Master Database) und überschrittene Subskriptionsebenen im Windows Event Viewer (nur Windows) und in der Datei "Websense.log" (Windows und Linux) protokolliert.

   Alerts sind u. a. für folgende Ereignisse verfügbar:

   - Ihre Subskription läuft in einer Woche ab.
   - Suchmaschinen, die für die Suchfilterung unterstützt werden, haben sich geändert.
   - Ein Download der Websense-Stammdatenbank (Websense Master Database) ist fehlgeschlagen.
   - Eine Kategorie oder ein Protokoll wurde der Stammdatenbank (Master Database) hinzugefügt bzw. aus der Datenbank entfernt.
   - Die Anzahl der aktuellen Benutzer überschreitet Ihre Subskriptionsebene.
   - Die Anzahl der aktuellen Benutzer hat 90% der Subskriptionsebene erreicht.
   - Ihre Subskription läuft in einem Monat ab.

- Die Websense-Stammdatenbank (Websense Master Database) wurde aktualisiert.

2. Wenn Sie fertig sind, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Konfigurieren der Alerts zur Nutzung von Kategorien

Verwandte Themen:

- *Alerts*, Seite 303
- *Kontrolle der Anzahl von Alerts*, Seite 304
- *Konfigurieren allgemeiner Alert-Optionen*, Seite 305
- *Hinzufügen von Alerts zur Nutzung von Kategorien*, Seite 309

Die Websense-Software kann Sie benachrichtigen, wenn die Internetaktivität für bestimmte URL-Kategorien einen definierten Schwellenwert erreicht. Sie können Alerts für zugelassene Anforderungen oder für gesperrte Anforderungen in der Kategorie definieren.

Sie möchten z. B. jedes Mal benachrichtigt werden, wenn 50 Anforderungen von Sites in der Kategorie "Online-Shopping" zugelassen wurden, um eine fundierte Entscheidung darüber treffen zu können, ob in dieser Kategorie Beschränkungen eingerichtet werden sollen. Oder Sie können jedes Mal Alerts erhalten, wenn 100 Anforderungen von Sites in der Kategorie "Unterhaltung" gesperrt wurden, um festzustellen, ob die Benutzer sich an eine neue Richtlinie für die Internetnutzung gewöhnen.

Auf der Registerkarte "Einstellungen" können Sie über die Seite **Alerts und Benachrichtigungen > Nutzung von Kategorien** die Alerts anzeigen, die bereits eingerichtet wurden, und Kategorien für nutzungsbezogene Alerts hinzufügen oder löschen.

1. Die Listen **Alerts zur Nutzung zugelassener Kategorien** und **Alerts zur Nutzung gesperrter Kategorien** informieren Sie darüber, welche Kategorien für Alerts konfiguriert, welche Schwellenwerte für jede Kategorie festgelegt und welche Alert-Methoden ausgewählt wurden.
2. Klicken Sie unter der gewünschten Liste auf **Hinzufügen**, um die Seite "Alerts zur Nutzung von Kategorien hinzufügen" zu öffnen (siehe *Hinzufügen von Alerts zur Nutzung von Kategorien*, Seite 309) und Alerts für zusätzliche URL-Kategorien zu konfigurieren.
3. Aktivieren Sie das Kontrollkästchen für jede Kategorie, die aus der Liste gelöscht werden soll, und klicken Sie unter der entsprechenden Liste auf **Löschen**.
4. Klicken Sie anschließend auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern und zur Seite "Nutzung von Kategorien" zurückzukehren. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Hinzufügen von Alerts zur Nutzung von Kategorien

Verwandte Themen:

- *Alerts*, Seite 303
- *Konfigurieren allgemeiner Alert-Optionen*, Seite 305
- *Konfigurieren der Alerts zur Nutzung von Kategorien*, Seite 308

Die Seite **Alerts zur Nutzung von Kategorien hinzufügen** wird angezeigt, wenn Sie auf der Seite "Nutzung von Protokollen" auf "Hinzufügen" klicken. Auf dieser Seite können Sie neue Kategorien für nutzungsbezogene Alerts auswählen, Schwellenwerte für diese Alerts festlegen und die Alert-Methoden auswählen.

1. Aktivieren Sie das Kontrollkästchen neben jeder Kategorie, die mit demselben Schwellenwert und denselben Alert-Methoden hinzugefügt werden soll.

   Hinweis
   Für Kategorien, die von der Protokollierung ausgeschlossen sind, können keine nutzungsbezogenen Alerts hinzugefügt werden. Siehe *Konfigurieren von Filtering Service für die Protokollierung*, Seite 326.

2. Legen Sie den **Schwellenwert** fest, indem Sie die Anzahl von Anforderungen auswählen, bei der ein Alert generiert wird.
3. Aktivieren Sie das Kontrollkästchen für jede gewünschte Alert-Methode (**E-Mail**, **Popup**, **SNMP**) für diese Kategorien.

   Zur Auswahl stehen nur die Alert-Methoden, die auf der Seite "Alerts" aktiviert wurden (siehe *Konfigurieren allgemeiner Alert-Optionen*, Seite 305).
4. Klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern und zur Seite "Nutzung von Protokollen" zurückzukehren (siehe *Konfigurieren der Alerts zur Nutzung von Kategorien*, Seite 308). Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Konfigurieren der Alerts zur Nutzung von Protokollen

Verwandte Themen:

- *Alerts*, Seite 303
- *Kontrolle der Anzahl von Alerts*, Seite 304
- *Konfigurieren allgemeiner Alert-Optionen*, Seite 305
- *Hinzufügen von Alerts zur Nutzung von Protokollen*, Seite 310

Die Websense-Software kann Sie benachrichtigen, wenn die Internetaktivität für ein bestimmtes Protokoll einen definierten Schwellenwert erreicht. Sie können für das ausgewählte Protokoll Alerts für zugelassene oder gesperrte Anforderungen definieren.

Sie möchten z. B. jedes Mal benachrichtigt werden, wenn 50 Anforderungen eines bestimmten Protokolls für Sofortnachrichten zugelassen wurden, um eine fundierte Entscheidung darüber treffen zu können, ob für dieses Protokoll Beschränkungen eingerichtet werden sollen. Sie können auch jedes Mal einen Alert erhalten, wenn 100 Anforderungen für ein bestimmtes Protokoll für die gemeinsame Nutzung von Dateien über Peer-to-Peer-Datenaustausch (P2P) gesperrt wurden, um festzustellen, ob die Benutzer sich an eine neue Richtlinie für die Internetnutzung gewöhnen.

Auf der Registerkarte "Einstellungen" können Sie über die Seite **Alerts und Benachrichtigungen > Nutzung von Protokollen** die Alerts anzeigen, die bereits eingerichtet wurden, und Protokolle für nutzungsbezogene Alerts hinzufügen oder löschen.

1. Die Listen **Alerts zur Nutzung zugelassener Protokolle** und **Alerts zur Nutzung gesperrter Protokolle** informieren Sie darüber, welche Protokolle für Alerts konfiguriert, welche Schwellenwerte für jedes Protokoll festgelegt und welche Alert-Methoden ausgewählt wurden.
2. Klicken Sie unter der gewünschten Liste auf **Hinzufügen**, um die Seite "Alerts zur Nutzung von Protokollen hinzufügen" zu öffnen (siehe *Hinzufügen von Alerts zur Nutzung von Protokollen*, Seite 310) und Alerts für zusätzliche Protokolle zu konfigurieren.
3. Aktivieren Sie das Kontrollkästchen für die zu löschenden Protokolle und klicken Sie anschließend unter der entsprechenden Liste auf **Löschen**.
4. Klicken Sie anschließend auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern und zur Seite "Nutzung von Protokollen" zurückzukehren. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Hinzufügen von Alerts zur Nutzung von Protokollen

Verwandte Themen:

- *Alerts*, Seite 303
- *Konfigurieren allgemeiner Alert-Optionen*, Seite 305
- *Konfigurieren der Alerts zur Nutzung von Protokollen*, Seite 309

Auf der Seite **Nutzung von Protokollen > Alerts zur Nutzung von Protokollen hinzufügen** können Sie neue Protokolle für nutzungsbezogene Alerts auswählen, Schwellenwerte für diese Alerts einrichten und die Alert-Methode auswählen.

1. Aktivieren Sie das Kontrollkästchen neben jedem Protokoll, das mit demselben Schwellenwert und denselben Alert-Methoden hinzugefügt werden soll.

   HinweisHinweis

   Sie können für ein Protokoll nur dann Alerts auswählen, wenn die Aufzeichnung in mindestens einem Protokollfilter konfiguriert ist.

   Protokollbezogene Alerts spiegeln nur die Nutzung durch Clients wider, die einem Protokollfilter unterliegen, der das Protokoll aufzeichnet.

2. Legen Sie den **Schwellenwert** fest, indem Sie die Anzahl von Anforderungen auswählen, bei der ein Alert generiert wird.
3. Wählen Sie für diese Protokolle jede gewünschte Alert-Methode (**E-Mail**, **Popup**, **SNMP**) aus.

   Zur Auswahl stehen nur die Alert-Methoden, die auf der Seite "Alerts" aktiviert wurden (siehe *Konfigurieren allgemeiner Alert-Optionen*, Seite 305).
4. Klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern und zur Seite "Nutzung von Protokollen" zurückzukehren (siehe *Konfigurieren der Alerts zur Nutzung von Protokollen*, Seite 309). Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Überprüfen des aktuellen Systemstatus

Auf der Seite **Status > Alerts** finden Sie Informationen über Probleme, die den Status der Websense-Software beeinträchtigen, und erhalten Tipps für die Problembehandlung. Außerdem können Sie Details über neue Echtzeit-Updates an der Websense-Stammdatenbank (Master Database) überprüfen.

Der Status der überwachten Websense-Softwarekomponenten wird in der Liste **Aktive Alerts** angezeigt.

- Klicken Sie über der Liste der Alert-Nachrichten auf **Was wird überwacht?**, um ausführliche Informationen über die überwachten Komponenten anzuzeigen.
- Klicken Sie neben der Fehler- oder Warnmeldung auf die Schaltfläche **Lösungen**, um ein Problem zu beheben.
- Um eine Alert-Nachricht auszublenden, klicken Sie auf **Erweitert**. Wenn Log Server, Network Agent oder User Service in Ihrer Organisation nicht verwendet werden bzw. Sie nicht planen, WebCatcher zu aktivieren, wählen Sie das entsprechende Kontrollkästchen aus, um den zugehörigen Alert auszublenden. Klicken Sie anschließend auf **OK**, um die Änderung vorzunehmen.

  Klicken Sie erneut auf **Erweitert**, um die erweiterten Optionen auszublenden.

Die Liste **Datenbankupdates in Echtzeit** enthält folgende Informationen über Notfallupdates an der Websense-Stammdatenbank (Master Database):

- Datum des Updates
- Art des Updates
- Die neue Versionsnummer der Datenbank
- Grund für das Update
- IP-Adresse der Filtering Service-Instanz, die aktualisiert wurde

Diese ergänzenden Updates erfolgen zusätzlich zu den regelmäßigen, geplanten Updates an der Stammdatenbank (Master Database). Sie können z. B. durchgeführt werden, um eine Site neu zu kategorisieren, die kurzfristig falsch kategorisiert wurde. Die Websense-Software prüft einmal in der Stunde auf Datenbankupdates.

Die Seite Alerts enthält eine dritte Liste für die Benutzer von Websense Web Security: **Real-Time Security Updates**. Diese Liste weist dasselbe Format wie die Liste "Datenbankupdates in Echtzeit" auf, enthält aber insbesondere sicherheitsbezogene Datenbankupdates.

Werden Sicherheitsupdates umgehend nach ihrer Erstellung installiert, wird die Verwundbarkeit durch Bedrohungen wie neues Phishing (Identitätsdiebstahl), falsche Anwendungen und bösartigen Code, die populäre Websites oder Anwendungen befallen können, eliminiert.

Weitere Informationen zu Real-Time Security Updates finden Sie unter *Real-Time Security Updates™*, Seite 34.

Klicken Sie im oberen Bereich der Seite auf die Schaltfläche **Drucken**, um ein zweites Fenster mit einer druckbaren Version des Alerts-Bereichs zu öffnen. Verwenden Sie die Optionen des Browsers zum Drucken dieser Seite. Die Navigationsoptionen auf der Hauptseite von Websense Manager werden beim Druck nicht berücksichtigt.

Sichern und Wiederherstellen der Websense-Daten

Verwandte Themen:

- *Planen von Sicherungen*, Seite 315
- *Ausführen von sofortigen Sicherungen*, Seite 316
- *Verwalten der Sicherungsdateien*, Seite 317
- *Wiederherstellen der Websense-Daten*, Seite 317
- *Unterbrechen geplanter Sicherungen*, Seite 318
- *Befehlsreferenz*, Seite 319

Das Dienstprogramm zum Sichern von Websense erleichtert es, die Websense-Softwareeinstellungen und -Richtliniendaten zu sichern und zur vorherigen Konfiguration zurückzukehren. Daten, die vom Dienstprogramm gespeichert wurden, können auch verwendet werden, um die Websense-Konfigurationsinformationen nach einem Update zu importieren.

Mit dem Dienstprogramm zum Sichern wird Folgendes gespeichert:

- Globale Konfigurationsinformationen, einschließlich Client- und Richtliniendaten, die in der Richtliniendatenbank gespeichert sind.
- Lokale Konfigurationsinformationen, z. B. Filtering Service- und Log Server-Einstellungen, die von jedem Policy Server gespeichert sind.
- Websense-Komponenteninitialisierungs- und -konfigurationsdateien.

Der Sicherungsprozess wird wie folgt durchgeführt:

1. Initiieren Sie eine umgehende Sicherung (siehe *Ausführen von sofortigen Sicherungen*, Seite 316) oder definieren Sie einen Sicherungsplan (siehe *Planen von Sicherungen*, Seite 315).
   - Starten Sie zu einem beliebigen Zeitpunkt eine Sicherung manuell.
   - Sicherungsdateien werden in einem Verzeichnis gespeichert, das beim Ausführen oder Planen der Sicherung angegeben wird.
2. Das Dienstprogramm zum Sichern prüft alle Websense-Komponenten auf dem Computer, erfasst die Daten, die gesichert werden sollen, und erstellt eine Archivierungsdatei. Der Dateiname hat das folgende Format:

   `wsbackup_jjjj-mm-tt_hhmmss.tar.gz`

   In diesem Fall stellt *jjjj-mm-tt_hhmmss* das Datum und die Uhrzeit der Sicherung dar. **tar.gz** ist ein übertragbares komprimiertes Dateiformat.

   Auf diese Sicherungsdateien können nur Benutzer mit Root-Berechtigungen (Linux) und Mitglieder der Administratorgruppe (Windows) zugreifen.

Führen Sie das Websense-Dienstprogramm zum Sichern auf jedem Computer aus, auf dem Websense-Komponenten installiert sind. Das Tool identifiziert und speichert alle der folgenden Dateien, die sich auf dem aktuellen Computer befinden:

Pfad	Dateiname
\Program Files\Websense\bin *oder* **/opt/Websense/bin**	authserver.ini BrokerService.cfg config.xml eimserver.ini LogServer.ini netcache.conf securewispproxy.ini transid.ini upf.conf websense.ini WebUI.ini wsauthserver.ini wscitrix.ini WSE.ini wsedir.ini wsradius.ini wsufpserver.ini
bin/i18n	i18n.ini
bin/postgres/data	postgresql.conf pg_hba.conf
BlockPages/*/Custom	Alle benutzerdefinierten Sperrseiteneinstellungen
tomcat/conf/Catalina/ Localhost	mng.xml
Windows\system32	isa_ignore.txt
Windows\system32\bin	ignore.txt
/etc/wsLib	wsSquid.ini

Speichern Sie die Websense-Sicherungsdateien an einem sicheren Speicherort. Diese Dateien sollten Bestandteil der regelmäßigen Sicherungsprozeduren Ihrer Organisation sein.

So stellen Sie eine frühere Konfiguration wieder her:

1. Rufen Sie die Sicherungsdateien aus der Speicherungs-Site ab.
2. Kopieren Sie jede Sicherungsdatei auf den Websense-Computer, auf dem sie erstellt wurde.

3. Führen Sie das Dienstsprogramm zum Sichern im Wiederherstellungsmodus aus.

> **Wichtig**
>
> Verwenden Sie immer das Dienstprogramm zum Sichern, um eine Websense-Softwarekonfiguration wiederherzustellen. Verwenden Sie keine anderen Dienstprogramme zum Extrahieren, um die Dateien aus dem Archiv zu extrahieren.
>
> Wenn die Sicherungsdatei beschädigt ist, können Sie die Einstellungen nicht wiederherstellen.

Während des Wiederherstellungsprozesses werden Fehler- oder Warnmeldungen ggf. auf dem Computer angezeigt, auf dem die Wiederherstellung durchgeführt wird.

Planen von Sicherungen

Verwandte Themen:

- *Ausführen von sofortigen Sicherungen*, Seite 316
- *Verwalten der Sicherungsdateien*, Seite 317
- *Wiederherstellen der Websense-Daten*, Seite 317
- *Unterbrechen geplanter Sicherungen*, Seite 318
- *Befehlsreferenz*, Seite 319

Um Sicherungen zu planen, öffnen Sie eine Befehls-Shell und navigieren Sie zum Websense-Verzeichnis "bin" (in der Standardeinstellung **C:\Program Files\Websense\bin** oder **opt/Websense/bin**). Geben Sie den folgenden Befehl ein.

```
wsbackup -s -t "<m> <h> <Tag_des_Monats> <Monat>
<Tag_der_Woche>" -d <Verzeichnis>
```

Hinweis: Diese Informationen verwenden das Format **crontab**; die Anführungszeichen und Leerstellen sind erforderlich.

Ersetzen Sie die Variablen im Beispiel durch die folgenden Informationen:

Variable	Informationen
<m>	0 - 59 Geben Sie den Start der Sicherung auf die Minute genau an.
<h>	0 - 23 Geben Sie an, in welcher Stunde die Sicherung gestartet werden soll.

Variable	Informationen
<Tag_des_Monats>	1 - 31 Geben Sie das Datum für die Sicherung an. Wenn Sie eine Sicherung für die Monatstage 29 bis 31 planen, verwendet das Dienstprogramm die standardmäßige Ersetzungsprozedur des Betriebssystems für Monate, in denen es diese Tage nicht gibt.
<Monat>	1 - 12 Geben Sie den Monat an, in dem die Sicherung ausgeführt werden soll.
<Tag_der_Woche>	0 - 6 Geben Sie einen Wochentag an. "0" steht für Sonntag.

In jedem Feld kann eine Nummer, ein Stern oder eine Parameterliste eingegeben werden. Details finden Sie in den **crontab**-Referenzen.

Ausführen von sofortigen Sicherungen

Verwandte Themen:

- *Planen von Sicherungen*, Seite 315
- *Verwalten der Sicherungsdateien*, Seite 317
- *Wiederherstellen der Websense-Daten*, Seite 317
- *Unterbrechen geplanter Sicherungen*, Seite 318
- *Befehlsreferenz*, Seite 319

Um eine sofortige Sicherung zu planen, öffnen Sie eine Befehls-Shell und navigieren Sie zum Websense-Verzeichnis "bin" (in der Standardeinstellung **C:\Program Files\Websense\bin** oder **opt/Websense/bin**). Geben Sie den folgenden Befehl ein.

```
wsbackup -b -d <Verzeichnis>
```

Verzeichnis gibt in diesem Fall das Zielverzeichnis für das Sicherungsarchiv an.

Warnung

Speichern Sie keine Sicherungsdateien im Websense-Verzeichnis **bin**. Dieses Verzeichnis wird gelöscht, wenn Sie die Websense-Software deinstallieren.

Wenn Sie eine sofortige Sicherung initiieren, werden alle Fehlermeldungen und Benachrichtigungen in einem Feld auf dem Computer angezeigt, auf dem die Sicherung ausgeführt wird.

Verwalten der Sicherungsdateien

Verwandte Themen:

- *Planen von Sicherungen*, Seite 315
- *Ausführen von sofortigen Sicherungen*, Seite 316
- *Wiederherstellen der Websense-Daten*, Seite 317
- *Unterbrechen geplanter Sicherungen*, Seite 318
- *Befehlsreferenz*, Seite 319

Wenn eine Sicherung durchgeführt wird, wird eine Konfigurationsdatei (**WebsenseBackup.cfg**) erstellt und mit dem Sicherungsarchiv gespeichert. In der Konfigurationsdatei ist Folgendes angegeben:

- Wie lang das Sicherungsarchiv im Sicherungsverzeichnis gespeichert wird
- Maximaler Festplattenspeicherplatz, der für alle Sicherungsdateien im Verzeichnis verfügbar ist.

Bearbeiten Sie die Datei **WebsenseBackup.cfg** in einem beliebigen Texteditor, um einen dieser Parameter zu ändern:

Parameter	Wert
KeepDays	Anzahl der Tage, die die Archivdateien im Sicherungsverzeichnis bleiben sollten. Der Standardwert ist 365.
KeepSize	Menge der für Sicherungsdateien vorgesehenen Bytes. Der Standardwert ist 10857600.

Alle Dateien, die älter als der **KeepDays**-Wert sind, werden aus dem Sicherungsverzeichnis gelöscht. Wenn der zugewiesene Festplattenspeicherplatz überschritten wurde, werden die ältesten Dateien aus dem Sicherungsverzeichnis gelöscht, um Speicherplatz für neuere Dateien freizugeben.

Wiederherstellen der Websense-Daten

Verwandte Themen:

- *Planen von Sicherungen*, Seite 315
- *Ausführen von sofortigen Sicherungen*, Seite 316
- *Verwalten der Sicherungsdateien*, Seite 317
- *Unterbrechen geplanter Sicherungen*, Seite 318
- *Befehlsreferenz*, Seite 319

Wenn Sie Websense-Konfigurationsdaten wiederherstellen, achten Sie darauf, dass Sie die Daten für die Komponenten wiederherstellen, die auf dem aktuellen Computer installiert sind.

Um den Wiederherstellungsprozess zu initiieren, öffnen Sie eine Befehls-Shell und navigieren Sie zum Websense-Verzeichnis "bin" (in der Standardeinstellung **C:\Program Files\Websense\bin** oder **opt/Websense/bin**). Geben Sie den folgenden Befehl ein.

```
wsbackup -r -f archive_file.tar.gz
```

Wichtig

Der Wiederherstellungsprozess kann mehrere Minuten in Anspruch nehmen. Halten Sie den Prozess nicht an, während die Wiederherstellung durchgeführt wird.

Während des Wiederherstellungsprozesses hält das Dienstprogramm zum Sichern alle Websense-Dienste an. Wenn das Dienstprogramm die Dienste nicht anhalten kann, sendet es eine Nachricht an den Benutzer, in der er aufgefordert wird, die Dienste manuell anzuhalten. Die Dienste müssen in der Reihenfolge angehalten werden, die unter *Anhalten und Starten der Websense-Dienste*, Seite 302 angegeben ist.

Das Dienstprogramm zum Sichern speichert einige Dateien, die für die Kommunikation mit Integrationsprodukten von anderen Herstellern verwendet werden. Da sich diese Dateien außerhalb der Websense-Verzeichnisstruktur befinden, müssen sie manuell wiederhergestellt werden, indem jede Datei in das korrekte Verzeichnis kopiert wird.

Zu den Dateien, die manuell wiederhergestellt werden müssen, gehören die Folgenden:

Dateiname	Wiederherstellen in
isa_ignore.txt	**Windows\system32**
ignore.txt	**Windows\system32\bin**
wsSquid.ini	**/etc/wsLib**

Unterbrechen geplanter Sicherungen

Verwandte Themen:

- *Planen von Sicherungen*, Seite 315
- *Ausführen von sofortigen Sicherungen*, Seite 316
- *Verwalten der Sicherungsdateien*, Seite 317
- *Wiederherstellen der Websense-Daten*, Seite 317
- *Befehlsreferenz*, Seite 319

Um die Daten im Sicherungsplan zu löschen und aktuell ausgeführte Sicherungen anzuhalten, öffnen Sie eine Befehls-Shell und navigieren Sie zum Websense-Verzeichnis "bin" (in der Standardeinstellung **C:\Program Files\Websense\bin** oder **opt/Websense/bin**). Geben Sie den folgenden Befehl ein:

```
wsbackup -u
```

Befehlsreferenz

Verwandte Themen:

- *Planen von Sicherungen*, Seite 315
- *Ausführen von sofortigen Sicherungen*, Seite 316
- *Verwalten der Sicherungsdateien*, Seite 317
- *Wiederherstellen der Websense-Daten*, Seite 317
- *Unterbrechen geplanter Sicherungen*, Seite 318

Das Dienstprogramm für die Sicherung kann nur von Benutzern mit Root-Berechtigungen (Linux) und Mitgliedern der Administratorgruppe (Windows) ausgeführt werden.

Um zu einem beliebigen Zeitpunkt eine vollständige Liste der Befehlsoptionen des Dienstprogramms zum Sichern anzuzeigen, geben Sie Folgendes ein:

```
wsbackup -h
```

oder

```
wsbackup --help
```

Für den Befehl **wsbackup** gibt es die folgenden Optionen:

- `-b` *oder* `--backup`
- `-d` *`directory_path`* *oder* `--dir` *`directory_path`*
- `-f` *`full_file_name`* *oder* `--file` *`full_file_name`*
- `-h` *oder* `--help` *oder* `-?`
- `-r` *oder* `--restore`
- `-s` *oder* `--schedule`
- `-t` *oder* `--time`
- `-u` *oder* `--unschedule`
- `-v` *oder* `--verbose [0...3]`

13 Verwaltung der Berichterstellung

Verwandte Themen:

- *Planen der Konfiguration*, Seite 322
- *Verwalten des Zugriffs auf die Reporting Tools*, Seite 322
- *Basiskonfiguration*, Seite 323
- *Dienstprogramm für die Konfiguration von Log Server*, Seite 328
- *Verwalten der Protokolldatenbank*, Seite 343
- *Konfigurieren von Untersuchungsberichten*, Seite 354
- *Eigene Berichte erstellen*, Seite 360

Websense Manager und die Reporting-Komponenten müssen auf einem Windows-Server installiert sein, damit Websense-Präsentationsberichte und -Untersuchungsberichte verwendet werden können. Zusätzlich muss die Websense-Software zur Protokollierung der Filterung von Internetaktivitäten konfiguriert sein.

Über die Protokollierung werden Einträge an Websense Log Server gesendet, der sie an eine Protokolldatenbank übergibt. Diese muss auf einem unterstützten Datenbankmodul installiert sein: Microsoft SQL Server Desktop Engine (in diesem Dokument als MSDE bezeichnet) oder Microsoft SQL Server Enterprise Edition oder Standard Edition (beide als Microsoft SQL Server bezeichnet). Weitere Informationen zur Installation dieser Reporting-Komponenten finden Sie im *Installationshandbuch* für Websense.

Wenn Sie einen Bericht generieren, zeigt Websense Manager Informationen aus der Protokolldatenbank abhängig von dem für den Bereicht definierten Filter an.

In Organisationen, bei denen Websense Manager auf einem Linux-Server installiert oder für die Berichterstellung bevorzugt Linux verwendet wird, kann zum Generieren der Berichte der separate Websense Explorer for Linux installiert werden. Dieses Produkt ist unabhängig von Websense Manager. Anweisungen zur Installation und Verwendung des Programms finden Sie im *Explorer for Linux Administrator's Guide*.

Planen der Konfiguration

Je nach dem Umfang des Internet-Datenverkehrs in Ihrem Netzwerk kann die Protokolldatenbank sehr groß werden. Berücksichtigen Sie bei der Ausarbeitung einer effektiven Protokollierungs- und Berichterstellungsstrategie folgende Fragen:

- Wann ist der Netzwerk-Datenverkehr am dichtesten?

  Achten Sie darauf, ressourcenintensive Datenbank- und Berichterstellungsjobs dann anzusetzen, wenn das Datenverkehrsvolumen geringer ist. Dadurch wird die Geschwindigkeit bei der Protokollierung und Berichterstellung in den Spitzennutzungszeiten erhöht. Siehe *Konfigurieren der Optionen für die Navigationsdauer im Internet*, Seite 347, und *Konfigurieren der Wartungsoptionen für die Protokolldatenbank*, Seite 349.

- Wie lange sollen Protokolldaten gespeichert werden, um den Verlauf der Berichterstellung nachvollziehen zu können?

  Erwägen Sie, Partitionen nach Erreichen dieses Zeitraums automatisch zu löschen. Dadurch wird die Größe des erforderlichen Speicherplatzes für die Protokolldatenbank reduziert. Siehe *Konfigurieren der Wartungsoptionen für die Protokolldatenbank*, Seite 349.

- Wie viele Informationen werden tatsächlich benötigt?

  Überlegen Sie, welche Protokolloptionen aktiviert werden sollen: Die Protokollierung von vollständigen URLs und Hits bedeutet auch eine größere Protokolldatenbank. Erwägen Sie Folgendes, wenn die Größe der Protokolldatenbank reduziert werden soll:

  - Deaktivieren der Protokollierung der vollständigen URL (siehe *Konfigurieren der Protokollierung der vollständigen URL*, Seite 346)
  - Protokollieren von Besuchen anstelle von Hits (siehe *Konfigurieren von Log-Cachedateien*, Seite 333)
  - Aktivieren der Konsolidierung (siehe *Konfigurieren von Konsolidierungsoptionen*, Seite 335)
  - Aktivieren der selektiven Protokollierung von Kategorien (siehe *Konfigurieren von Filtering Service für die Protokollierung*, Seite 326)

Erfolgreiche Berichterstellungs-Implementierungen werden auf Hardware bereitgestellt, die die Voraussetzungen für die erwarteten Anforderungen und die Speicherung von Verlaufsdaten erfüllt oder übertrifft.

Verwalten des Zugriffs auf die Reporting Tools

Wenn Websense Manager und die Reporting-Komponenten auf einem Windows-Server installiert sind, werden die Berichterstellungsoptionen in Websense Manager und dem Dienstprogramm zur Konfiguration von Log Server angezeigt.

Bei der Installation der Reporting-Komponenten wird eine Verbindung zwischen Log Server und einem bestimmten Policy Server hergestellt. Sie müssen diesen Policy

Server während der Anmeldung bei Websense Manager auswählen, um auf die Berichtsfunktionen zugreifen zu können. Wenn Sie sich bei einem anderen Policy Server anmelden, können Sie nicht auf die Präsentationsberichte oder Untersuchungsberichte auf der Registerkarte "Hauptseite" zugreifen.

In Organisationen, in denen nur das WebsenseAdministrator-Anmeldekonto verwendet wird, haben alle Personen, die mit Websense Manager arbeiten, auch Zugriff auf alle Berichterstellungsoptionen in Websense Manager. Dazu zählen auch Präsentationsberichte, Untersuchungsberichte und die Einstellungen für die Reporting Tools.

In Organisationen mit delegierter Verwaltung wird der Zugriff auf die Reporting Tools in Websense Manager über WebsenseAdministrator und die Mitglieder der Rolle des übergeordneten Administrators (Super Administrator) gesteuert. Beim Erstellen einer Rolle legt der übergeordnete Administrator fest, ob die Rolle über den Zugriff auf die bestimmten Berichterstellungsoptionen verfügt.

Informationen zur Konfiguration des Zugriffs auf die Reporting Tools finden Sie unter *Rollen bearbeiten*, Seite 272.

Auf das Dienstprogramm zur Konfiguration von Log Server kann über das Windows-Startmenü zugegriffen werden. Nur Personen mit Zugriff auf den Computer mit der Installation können dieses Dienstprogramm öffnen und die Log Server-Einstellungen ändern. Siehe *Dienstprogramm für die Konfiguration von Log Server*, Seite 328.

Wenn in Ihrer Organisation Websense Manager auf einem Linux-Server installiert ist oder anstelle der Reporting-Komponenten für Windows das Reporting-Programm Websense Explorer for Linux verwendet wird, werden die Berichterstellungsfunktionen nicht in Websense Manager angezeigt. Auf den Seiten "Heute" und "Verlauf" können keine Internet-Filterdiagramme angezeigt werden. Informationen zur Installation und Verwendung des Programms zur Generierung von Berichten finden Sie im *Explorer for Linux Administrator's Guide*.

Basiskonfiguration

Verwandte Themen:

- *Konfigurieren von Filtering Service für die Protokollierung*, Seite 326
- *Zuweisen von Risikoklassen an Kategorien*, Seite 324
- *Konfigurieren von Vorgaben für die Berichterstellung*, Seite 326
- *Dienstprogramm für die Konfiguration von Log Server*, Seite 328
- *Verwalten der Protokolldatenbank*, Seite 343

Es können eine Vielzahl von Konfigurationsoptionen verwendet werden, um die Berichterstellung für eine Umgebung anzupassen.

Websense Master Database organisiert Kategorien in **Risikoklassen**. Risikoklassen weisen auf mögliche Arten oder Ebenen der Verwundbarkeit hin, die von Sites in diesen Kategorien ausgehen. Auf der Seite "Allgemein > Risikoklassen" können Sie die Risikoklassen für Ihre Organisation anpassen. Sie können über die Registerkarte "Einstellungen" darauf zugreifen. Siehe *Zuweisen von Risikoklassen an Kategorien*, Seite 324.

Auf der Seite "Berichterstellung > Vorgaben" können Sie den E-Mail-Server konfigurieren, der zur Verteilung von Berichten und zur Aktivierung der Funktion für die Erstellung eigener Berichte verwendet wird. Sie können über die Registerkarte "Einstellungen" darauf zugreifen. Siehe *Konfigurieren von Vorgaben für die Berichterstellung*, Seite 326.

Protokollierung ist der Vorgang der Speicherung von Informationen über Websense-Filterungsaktivitäten in einer Protokolldatenbank, damit Berichte generiert werden können.

Auf der Seite "Allgemein > Protokollierung" können Sie die Protokollierung aktivieren, die zu protokollierenden Kategorien auswählen und festlegen, welche Benutzerinformationen protokolliert werden. Sie können über die Registerkarte "Einstellungen" darauf zugreifen. Weitere Informationen dazu finden Sie unter *Konfigurieren von Filtering Service für die Protokollierung*, Seite 326.

Mit dem Dienstprogramm zur Konfiguration von Log Server können Sie verwalten, auf welche Art Protokolleinträge verarbeitet und Verbindungen zur Protokolldatenbank hergestellt werden. Weitere Informationen dazu finden Sie unter *Dienstprogramm für die Konfiguration von Log Server*, Seite 328.

Auf der Seite "Berichterstellung > Protokolldatenbank", die über die Seite "Einstellungen" geöffnet werden kann, können Sie die Protokolldatenbank einschließlich der Überwachung der Navigationszeit im Internet, der Optionen der Datenbankpartitionen und der Fehlerprotokolle überwachen. Weitere Informationen dazu finden Sie unter *Verwalten der Protokolldatenbank*, Seite 343.

Zuweisen von Risikoklassen an Kategorien

Verwandte Themen:

- *Risikoklassen*, Seite 43
- *Sperren von Seiten*, Seite 89
- *Verwenden von Berichten für das Beurteilen der Filterrichtlinien*, Seite 99

Die Websense Master Database organisiert Kategorien in **Risikoklassen**. Risikoklassen weisen auf mögliche Arten oder Ebenen der Verwundbarkeit hin, die von Sites in diesen Kategorien ausgehen.

Risikoklassen werden hauptsächlich in der Berichterstellung verwendet. Die Seiten "Heute" und "Verlauf" bieten Diagramme, auf denen die Internetaktivitäten nach

Risikoklasse organisiert werden. Sie können nach Risikoklassen geordnete Präsentations- oder Untersuchungsberichte generieren.

Übergeordnete Administratoren können sich auf der Seite **Einstellungen > Risikoklassen** die einzelnen Kategorien anzeigen, die eine Risikoklasse bilden, oder diese ändern. Beispielsweise sind einige Unternehmen möglicherweise der Ansicht, dass Sites mit von Benutzern hochgeladenen Videos in die Risikoklassen für die gesetzliche Haftung und Minderung der Netzwerkbandbreite und Produktivität einzustufen sind. Führt Ihr Unternehmen dagegen eine bestimmte demographische Untersuchung des Marktes durch, werden diese Sites möglicherweise der Risikoklasse der arbeitsbezogenen Nutzung zugeordnet.

> **Hinweis**
> In den Standardkategorien wird unter der Klasse "Sicherheitsrisiko" die Sicherheitssperrseite für gesperrte Sites angezeigt. Änderungen der Kategorien in der Klasse "Sicherheitsrisiko" wirken sich auf die Berichterstellung aus, haben jedoch keinen Einfluss auf Sperrseiten. Siehe *Sperren von Seiten*, Seite 89.

Die auf dieser Seite festgelegten Zuordnungen werden in den Risikoklasseninformationen in Websense-Berichten dargestellt.

1. Wählen Sie einen Eintrag aus der Liste **Risikoklassen** aus.
2. Überprüfen Sie die Liste **Kategorien**, um zu sehen, welche Kategorien aktuell in der Risikoklasse enthalten sind.

   Ein Häkchen zeigt an, dass die Kategorie aktuell der ausgewählten Risikoklasse zugeordnet ist. Das blaue Symbol "W" kennzeichnet die Kategorien, die standardmäßig in der Risikoklasse enthalten sind.
3. Aktivieren oder deaktivieren Sie Einträge in der Baumstruktur "Kategorie", um der ausgewählten Risikoklasse eine Kategorie hinzuzufügen oder diese daraus zu entfernen. Kategorien können mehr als einer Risikoklasse zugeordnet werden.

   Folgende Optionen sind ebenfalls verfügbar:

Option	Beschreibung
Alles auswählen	Wählt alle Kategorien in der Baumstruktur aus.
Auswahl aufheben	Hebt die Auswahl aller Kategorien in der Baumstruktur auf.
Standardwerte wiederherstellen	Setzt die Kategorieauswahl der ausgewählten Risikoklasse auf den Anfangszustand in der Websense-Software zurück. Das blaue Symbol "W" bezeichnet eine Standardkategorie.

4. Wiederholen Sie diesen Vorgang bei allen Risikoklassen.
5. Klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** geklickt haben.

Konfigurieren von Vorgaben für die Berichterstellung

Verwandte Themen:

- *Eigene Berichte erstellen*, Seite 360
- *Planen von Präsentationsberichten*, Seite 116
- *Planen von Untersuchungsberichten*, Seite 145

Wenn Sie Präsentations- oder Untersuchungsberichte planen, die zu einem späteren Zeitpunkt oder in einer wiederkehrenden Zeitfolge ausgeführt werden sollen, werden die Berichte per E-Mail an die angegebenen Empfänger verteilt. Auf der Seite **Berichterstellung > Vorgaben**, auf die Sie über die Registerkarte "Einstellungen" zugreifen können, werden die wichtigsten Informationen für diese E-Mail-Nachrichten festgelegt.

Diese Seite wird außerdem für das Aktivieren der Erstellung eigener Berichte verwendet. Damit können einzelne Benutzer Berichte zu Ihrer eigenen Internetaktivität erstellen.

1. Geben sie die **E-Mail-Adresse** an, die im Feld "An" angezeigt werden soll, wenn geplante Berichte per E-Mail verteilt werden.
2. Geben Sie **IP oder Name des SMTP-Servers** für den E-Mail-Server ein, über den die geplanten Berichte per E-Mail verteilt werden.
3. Aktivieren Sie das Kontrollkästchen **Erstellung eigener Berichte zulassen**, um Endbenutzern in Ihrer Organisation die Möglichkeit zu geben, auf Websense Manager zuzugreifen und Untersuchungsberichte zu ihrer eigenen Internetaktivität zu erstellen. Siehe *Eigene Berichte erstellen*, Seite 360.
4. Klicken Sie zum Implementieren Ihrer Änderungen auf **Jetzt speichern**.

Konfigurieren von Filtering Service für die Protokollierung

Verwandte Themen:

- *Einführung in die Log Database*, Seite 341
- *Dienstprogramm für die Konfiguration von Log Server*, Seite 328

Unter der Registerkarte "Einstellungen" auf der Seite **Allgemein > Protokollierung** können Sie die IP-Adresse und den Port für das Senden der Protokolleinträge an Log Server angeben. Auf dieser Seite können Sie auch auswählen, welche Benutzerinformationen und URL-Kategorien von Websense Filtering Service an Log Server gesendet und für Berichte und Alerts zur Nutzung von Kategorien verfügbar gemacht werden sollen (siehe *Konfigurieren der Alerts zur Nutzung von Kategorien*, Seite 308).

Konfigurieren Sie in einer Umgebung mit mehreren Policy Servern die Seite "Allgemein > Protokollierung" für jeden Policy Server einzeln. Alle Filtering Services, die dem aktiven Policy Server zugeordnet sind, senden ihre Protokolleinträge an den Log Server, der auf dieser Seite bezeichnet ist.

Rufen Sie sich die folgenden Tatsachen ins Gedächtnis, wenn Sie mit mehreren Policy Servern arbeiten:

- Wenn bei einem Policy Server die IP-Adresse und der Port nicht angegeben sind, können von den diesem Policy Server zugeordneten Filtering Services keine Daten für die Berichterstellung oder für Alerts protokolliert werden.
- Jeder Filtering Service protokolliert Datenverkehr abhängig von den Einstellungen für den Policy Server, mit dem er verbunden ist. Wenn Sie die Protokollierungsauswahl für die Benutzerinformationen oder die Kategorie für verschiedene Policy Server ändern, werden die generierten Berichte der Benutzer, die verschiedenen Policy Servern zugeordnet sind, möglicherweise inkonsistent angezeigt.

Stellen Sie sicher, dass Sie sich auf jedem Policy Server separat anmelden, wenn Ihre Umgebung sowohl mehrere Policy Server als auch mehrere Log Server umfasst, und überprüfen Sie, dass die Kommunikation mit dem Log Server ordnungsgemäß funktioniert.

1. Aktivieren Sie **IP-Adressen protokollieren**, um Identifikationsinformationen von Computern zu protokollieren, die auf das Internet zugreifen.
2. Aktivieren Sie **Benutzernamen protokollieren**, um Identifikationsinformationen von Benutzern zu protokollieren, die auf das Internet zugreifen.

   Hinweis
   Wenn keine IP-Adressen oder Benutzernamen protokolliert werden, können in die Berichte keine Benutzerdaten aufgenommen werden. Dies wird gelegentlich als **anonyme Protokollierung** bezeichnet.

3. Geben Sie im Feld **IP-Adresse oder Name von Log Server** die IP-Adresse oder den Namen des Computers ein, auf dem Log Server installiert ist.

   Wichtig
   Wenn Log Server nicht auf demselben Computer wie Policy Server installiert ist, wird dieser Eintrag möglicherweise standardmäßig auf "localhost" festgelegt. Falls dies geschieht, geben Sie die korrekte IP-Adresse des Computers mit Log Server ein, um die Anzeige der Diagramme auf den Seiten "Heute" und "Verlauf" sowie andere Berichterstellungsfunktionen zu ermöglichen.

4. Geben Sie unter **Port** die Portnummer zum Senden von Protokolleinträgen an Log Server ein.
5. Klicken Sie auf **Status prüfen**, um festzustellen, ob Websense Manager mit dem angegebenen Log Server kommunizieren kann.

Eine Meldung gibt ab, ob der Verbindungstest erfolgreich war. Aktualisieren Sie ggf. die IP-Adresse oder den Computernamen und Port, bis der Test erfolgreich ist.

6. Klicken Sie auf die Schaltfläche **Selektive Protokollierung von Kategorien**, um den Bereich zu öffnen, in dem die zu protokollierenden URL-Kategorien angegeben werden können.

   Die hier ausgewählten Einstellungen gelten für alle Kategoriefilter in allen aktiven Richtlinien.

   > **Hinweis**
   >
   > Wenn Sie die Protokollierung für Kategorien mit der Einstellung von nutzungsbezogenen Alerts (siehe *Konfigurieren der Alerts zur Nutzung von Kategorien*, Seite 308) deaktivieren, können keine nutzungsbezogenen Alerts gesendet werden.
   >
   > Berichte können Informationen zu Kategorien enthalten, die nicht protokolliert werden.

   a. Sie können die übergeordneten Kategorien nach Wunsch ein- oder ausblenden, um die gewünschten Kategorien anzuzeigen.

   b. Wählen Sie die zu protokollierenden Kategorien aus, indem Sie die zugehörigen Kontrollkästchen aktivieren.

      Sie müssen alle Kategorien separat aktivieren oder deaktivieren. Durch die Auswahl einer übergeordneten Kategorie werden die zugehörigen Unterkategorien nicht automatisch mit ausgewählt. Klicken Sie als Hilfe auf **Alles auswählen** und **Auswahl aufheben**.

7. Klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** geklickt haben.

Dienstprogramm für die Konfiguration von Log Server

Verwandte Themen:

- *Verwalten des Zugriffs auf die Reporting Tools*, Seite 322
- *Basiskonfiguration*, Seite 323
- *Stoppen und Starten von Log Server*, Seite 340

Während der Installation werden verschiedene Aspekte für Log Server-Vorgänge konfiguriert, darunter auch die Art und Weise, wie Log Server mit den Websense-Filterkomponenten interagiert.

Mit dem Dienstprogramm Konfiguration von Log Server können Sie diese Einstellungen gegebenenfalls ändern und weitere Details zu Log Server-Vorgängen

konfigurieren. Das Dienstprogramm wird auf dem Computer installiert, auf dem sich auch Log Server befindet.

1. Wählen Sie im Windows-Startmenü die Optionen **Alle Programme > Websense > Dienstprogramme > Konfiguration von Log Server** aus.

   Das Dienstprogramm für die Konfiguration von Log Server wird geöffnet.
2. Wählen Sie eine Registerkarte aus, um die zugehörigen Optionen anzuzeigen, und nehmen Sie Ihre Änderungen vor. Ausführliche Anweisungen finden Sie unter:
   - *Konfigurieren der Log Server-Verbindungen*, Seite 329
   - *Konfigurieren der Datenbankoptionen für Log Server*, Seite 330
   - *Konfigurieren von Log-Cachedateien*, Seite 333
   - *Konfigurieren von Konsolidierungsoptionen*, Seite 335
   - *Konfigurieren von WebCatcher*, Seite 337
3. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.
4. Stoppen und Starten Sie Log Server über die Registerkarte **Verbindung** neu, damit die Änderungen wirksam werden.

WICHTIG

Klicken Sie auf **Anwenden**, nachdem Sie Änderungen auf einer Registerkarte der Konfiguration von Log Server vorgenommen haben. In diesem Fall **müssen** Sie Log Server stoppen und neu starten, damit die Änderungen wirksam werden. Damit Log Server nicht mehrere Male neu gestartet werden muss, nehmen Sie alle Änderungen in der Konfiguration von Log Server vor, bevor Sie Log Server neu starten.

Konfigurieren der Log Server-Verbindungen

Verwandte Themen:

- *Dienstprogramm für die Konfiguration von Log Server*, Seite 328
- *Konfigurieren der Datenbankoptionen für Log Server*, Seite 330
- *Konfigurieren von Log-Cachedateien*, Seite 333
- *Konfigurieren von Konsolidierungsoptionen*, Seite 335
- *Konfigurieren von WebCatcher*, Seite 337
- *Stoppen und Starten von Log Server*, Seite 340

Auf der Registerkarte **Verbindung** des Dienstprogramms zur Konfiguration von Log Server sind Optionen verfügbar, mit denen eine Verbindung zwischen Log Server und den Websense-Filterkomponenten erstellt und aufrechterhalten werden kann.

1. Akzeptieren Sie die Standardeinstellung für den **Eingabeport für Log Server** (55805), oder geben Sie einen anderen verfügbaren Port ein.

Dabei handelt es sich um den Port, über den Log Server mit Filtering Service kommuniziert. Der hier eingegebene Port muss mit dem Port übereinstimmen, der auf der Seite "Allgemein > Protokollierung" (Registerkarte "Einstellungen") von Websense Manager eingegeben wurde.

2. Geben Sie eine Stundenanzahl als **Aktualisierungsintervall für Benutzer/Gruppen** ein, um festzulegen, wie oft Log Server den Verzeichnisdienst für Aktualisierungen kontaktiert.

   Log Server kontaktiert den Verzeichnisdienst, um aktualisierte Informationen wie die vollständigen Benutzernamen und Gruppenzuweisungen der Benutzer abzurufen, über die Einträge in der Protokolldatenbank bestehen.

   Die Aktivität eines Benutzers, dessen Gruppe sich geändert hat, wird weiterhin in Berichten unter der vorherigen Gruppe erfasst, bis die nächste Aktualisierung stattfindet. Organisationen, die Ihren Verzeichnisdienst regelmäßig aktualisieren oder über eine große Benutzeranzahl verfügen, sollten die Benutzer-/Gruppeninformationen häufiger als jeweils nach den in den Standardeinstellungen festgelegten 12 Stunden aktualisieren.
3. Klicken Sie auf **Anwenden**, um eventuelle Änderungen zu speichern.
4. Mit der Schaltfläche im Bereich "Dienststatus" können Sie **Start** oder **Stoppen** für Log Server festlegen. Die Beschriftung der Schaltfläche ändert sich, um die Aktion zu bezeichnen, die ein Klick darauf zur Folge hat.

> **Hinweis**
> Wenn Log Server gestoppt ist, können keine Internetzugriffsaktivitäten protokolliert werden.

Im Dienstprogramm für die Konfiguration von Log Server vorgenommene Änderungen werden erst wirksam, wenn Log Server gestoppt und neu gestartet wird.

Konfigurieren der Datenbankoptionen für Log Server

Verwandte Themen:

- *Dienstprogramm für die Konfiguration von Log Server*, Seite 328
- *Konfigurieren der Log Server-Verbindungen*, Seite 329
- *Einrichten der Datenbankverbindung*, Seite 332
- *Konfigurieren von Log-Cachedateien*, Seite 333
- *Konfigurieren von Konsolidierungsoptionen*, Seite 335
- *Konfigurieren von WebCatcher*, Seite 337
- *Stoppen und Starten von Log Server*, Seite 340

Öffnen Sie die Registerkarte **Datenbank** des Dienstprogramms zur Konfiguration von Log Server, um zu konfigurieren, auf welche Art und Weise Log Server mit der Protokolldatenbank interagiert.

1. Wählen Sie aus den folgenden Optionen eine **Einfügemethode in Protokolle** aus.
   - Open Database Connectivity (ODBC): Einträge werden individuell in die Datenbank eingefügt. Dazu wird ein Datenbanktreiber verwendet, um Daten zwischen Log Server und der Protokolldatenbank verwalten zu können.
   - Massenkopierprogramm (BCP) *(empfohlen)*: Einträge werden in Gruppen, den sogenannten Batches, in die Protokolldatenbank eingefügt. Die Verwendung dieser Option wird empfohlen, da sie effizienter als die ODBC-Einfügemethode ist.

   Hinweis
   Die BCP-Option ist nur verfügbar, wenn die SQL Server-Clienttools auf dem Computer mit Log Server installiert sind.

2. Klicken Sie auf die Schaltfläche **Verbindung**, um die Protokolldatenbank auszuwählen, in der neue Informationen von Websense zum Internetzugriff gespeichert werden. Siehe *Einrichten der Datenbankverbindung*, Seite 332.

   Unter **ODBC-Datenquellenname (DSN)** und **ODBC-Anmeldename** werden die Einstellungen angezeigt, die für die Datenbankverbindung festgelegt wurden.
3. Wenn Sie unter Schritt 1 BCP als Einfügemethode in Protokolle ausgewählt haben, legen Sie die folgenden Optionen fest. Wenn Sie ODBC als Einfügemethode in Protokolle ausgewählt haben, überspringen Sie diesen Schritt.

Option	Beschreibung
Pfad zum Speicherort der BCP-Datei	Verzeichnispfad zum Speichern von BCP-Dateien. Es muss sich um einen Pfad handeln, für den Log Server über den Lese- und Schreibzugriff verfügt. Diese Option ist nur verfügbar, wenn Log Server auf dem Computer mit der Protokolldatenbank installiert ist oder die SQL Server-Clienttools auf dem Computer mit Log Server installiert sind.
Erstellungsrate für BCP-Datei	Die maximale Minutenanzahl, die Log Server Einträge in eine Batchdatei einfügt, bevor die Batchdatei abgeschlossen und eine neue Batchdatei erstellt wird. Diese Einstellung funktioniert in Kombination mit der Einstellung für die Batchgröße: Log Server erstellt eine neue Batchdatei, sobald eine der beiden Obergrenzen erreicht ist.
Maximale BCP-Batchgröße	Die maximale Anzahl der Protokolleinträge, bevor eine neue Batchdatei erstellt wird. Diese Einstellung funktioniert in Kombination mit der Einstellung für die Erstellungsrate: Log Server erstellt eine neue Batchdatei, sobald eine der beiden Obergrenzen erreicht ist.

4. Legen Sie die **Maximal zulässige Verbindungsanzahl** fest, um anzugeben, wie viele interne Verbindungen zwischen Log Server und dem Datenbankmodul hergestellt werden können. Die verfügbaren Optionen sind je nach dem verwendeten Datenbankmodul unterschiedlich.

- **MSDE**: Die Voreinstellung für diesen Wert beträgt "4" und kann nicht geändert werden.
- **SQL Server**: Es ist je nach Ihrer SQL Server-Lizenz ein Wert zwischen 4 und 50 eingestellt. Die Mindestanzahl der Verbindungen hängt von der ausgewählten Einfügemethode in Protokolle ab.

> **Hinweis**
> Eine Erhöhung der Zahl der Verbindungen kann die Verarbeitungsgeschwindigkeit von Protokolleinträgen erhöhen, sie kann sich jedoch auch auf weitere Prozesse im Netzwerk auswirken, die mit demselben SQL Server arbeiten. In den meisten Fällen sollten Sie die Anzahl der Verbindungen auf weniger als 20 festlegen. Wenden Sie sich für Unterstützung an Ihren Datenbankadministrator.

5. Aktivieren oder deaktivieren Sie **Erweiterte Protokollierung**, um diese Option zu aktiveren oder zu deaktivieren. Damit wird bestimmt, wie Log Server die Protokollierung fortsetzt, nachdem sie gestoppt wurde.

   Wenn diese Option deaktiviert ist (Standardeinstellung), nimmt Log Server die Verarbeitung nach einem Stopp am Anfang der ältesten Log-Cachedatei wieder auf. Dies führt zu einigen doppelten Einträgen in der Protokolldatenbank, hat jedoch auch eine schnellere Verarbeitung in Log Server zur Folge.

   Wenn diese Option aktiviert ist, verfolgt Log Server den Speicherort in der aktiven Log-Cachedatei nach. Nach einem Neustart nimmt Log Server die Verarbeitung an der Stelle auf, an der sie angehalten wurde. Die erweiterte Protokollierung kann die Verarbeitung in Log Server verlangsamen.
6. Klicken Sie auf **Anwenden**, um eventuelle Änderungen zu speichern, und starten Sie Log Server neu (siehe *Stoppen und Starten von Log Server*, Seite 340).

Einrichten der Datenbankverbindung

Verwandte Themen:

- *Konfigurieren der Log Server-Verbindungen*, Seite 329
- *Konfigurieren der Datenbankoptionen für Log Server*, Seite 330

Mit der Schaltfläche **Verbindung** auf der Registerkarte "Datenbank" des Dienstprogramms zum Konfigurieren von Log Server können Sie die Protokolldatenbank auswählen, in der eingehende Informationen zum Internetzugriff von Websense gespeichert werden. Dies wird automatisch während der Installation konfiguriert, kann jedoch jederzeit geändert werden, wenn die Datenbank zur Protokollierung geändert werden muss. (Die Datenbank muss bereits bestehen, damit eine Verbindung eingerichtet werden kann.)

1. Wählen Sie im Dialogfeld "Datenquelle" die Registerkarte **Computer-Datenquelle** aus.

2. Wählen Sie die ODBC-Verbindung für die Datenbank aus, in der die Protokollierung der neuen Informationen erfolgt.
3. Klicken Sie auf **OK**, um das Dialogfeld zur Anmeldung bei SQL Server anzuzeigen.
4. Wenn die Option **Vertrauenswürdige Verbindung verwenden** verfügbar ist, stellen Sie sicher, dass sie für Ihre Umgebung ordnungsgemäß eingerichtet wurde.

   MSDE-Benutzer: Deaktivieren Sie die Option für vertrauenswürdige Verbindungen.

   SQL Server-Benutzer: Bitten Sie Ihren Datenbankadministrator um Hilfe.

   Hinweis

   Wenn Sie für die Kommunikation zu SQL Server eine vertrauenswürdige Verbindung verwenden, müssen Sie möglicherweise mehrere Websense-Dienste mit dem vertrauenswürdigen Benutzernamen und Passwort konfigurieren. Ausführlichere Informationen finden Sie im *Installationshandbuch*.

5. Geben Sie die **Anmeldekennung** und das **Kennwort** an wie bei der Einrichtung der Datenbank festgelegt. Normalerweise entspricht dies der Benutzeranmelde-ID um dem Passwort, die während der Installation und Datenbankerstellung von Log Server festgelegt wurden.
6. Stoppen Sie Log Server, und starten Sie ihn erneut über die Registerkarte **Verbindung**, nachdem Sie diesen Vorgang abgeschlossen und eventuell weitere Änderungen im Dienstprogramm für die Konfiguration von Log Server vorgenommen haben.

Konfigurieren von Log-Cachedateien

Verwandte Themen:

- *Dienstprogramm für die Konfiguration von Log Server*, Seite 328
- *Konfigurieren der Log Server-Verbindungen*, Seite 329
- *Konfigurieren der Datenbankoptionen für Log Server*, Seite 330
- *Konfigurieren von Konsolidierungsoptionen*, Seite 335
- *Konfigurieren von WebCatcher*, Seite 337
- *Stoppen und Starten von Log Server*, Seite 340

Auf der Registerkarte **Einstellungen** im Dienstprogramm für die Konfiguration von Log Server können Sie die Erstellungsoptionen der Log-Cachedatei verwalten und angeben, ob Log Server die individuellen Dateien verfolgt, aus denen eine Website besteht, oder ob nur die Website selbst verfolgt wird.

1. Geben Sie den Pfad zum Speichern von Log-Cachdateien im Feld **Pfad zur Cachedatei** ein. Der Standardpfad ist **<Installationsverzeichnis>\bin\Cache**. (Der Standardinstallationspfad lautet "C:\Programme\Websense\").
2. Geben Sie unter **Erstellungsrate für Cachedatei** die maximale Minutenzahl an, die Log Server Informationen zum Internetzugriff an eine Log-Cachedatei senden soll (**log*n*.tmp**), bevor diese geschlossen und eine neue Datei erstellt wird.

   Diese Einstellung funktioniert in Kombination mit der Größeneinstellung: Log Server erstellt eine neue Log-Cachedatei, sobald eine der beiden Obergrenzen erreicht ist.
3. Geben Sie unter **Maximale Größe der Cachedatei** an, wie umfangreich eine Log-Cachedatei werden soll, bevor Sie von Log Server geschlossen und eine neue Datei erstellt wird.

   Diese Einstellung funktioniert in Kombination mit der Einstellung für die Erstellungsrate: Log Server erstellt eine neue Log-Cachedatei, sobald eine der beiden Obergrenzen erreicht ist.
4. Aktivieren Sie **Besuche aktivieren**, um einen Protokolleintrag für jede besuchte Website zu erstellen.

   Hinweis

   Das Verwalten der Größe der Protokolldatenbank ist ein wichtiger Aspekt bei Netzwerken mit hohen Datenvolumen. Eine Aktivierung der Option zur Protokollierung der Besuche ist eine Möglichkeit, wie Datenbankgröße und -wachstum gesteuert werden können.

   Wenn diese Option nicht aktiviert ist, wird ein separater Protokolleintrag für alle HTTP-Anfragen erstellt, mit denen die verschiedenen Seitenelemente aufgebaut werden, beispielsweise Grafiken und Werbung. Diese Option ist auch unter dem Begriff Hits protokollieren bekannt. Dadurch wird eine wesentlich umfangreichere Protokolldatenbank erstellt, die schnell größer wird.

   Wenn diese Option ausgewählt wird, kombiniert Log Server die individuellen Elemente, aus denen die Webseite besteht (beispielsweise Grafiken und Werbung), zu einem einzigen Protokolleintrag.

   Wenn Sie Websense Web Security Gateway installiert haben, werden Scanningaktivitäten in Echtzeit immer in Form von Hits in den Berichten angezeigt, die sich auf Scanning in Echtzeit beziehen. Dies ist auch dann der Fall, wenn die Protokollierung von Besuchen aktiviert ist. In diesem Fall sind die in

den Webfilterungsberichten angegebenen Zahlen, die gesperrten Datenverkehr durch Scanning in Echtzeit umfassen, niedriger als die Zahlen, die in Berichten zum Scannen in Echtzeit angegeben werden.

> **Hinweis**
> Es empfiehlt sich, eine neue Datenbankpartition zu erstellen, bevor die Methode der Protokollierung von Besuchen und Hits geändert wird. Informationen zum Erstellen einer neuen Datenbankpartition finden Sie auf der Seite "Berichterstellung" > Protokolldatenbank (Registerkarte "Einstellungen") in Websense Manager.

5. Klicken Sie auf **Anwenden**, um eventuelle Änderungen zu speichern, und starten Sie Log Server neu (siehe *Stoppen und Starten von Log Server*, Seite 340).

Konfigurieren von Konsolidierungsoptionen

Verwandte Themen:

- *Dienstprogramm für die Konfiguration von Log Server*, Seite 328
- *Konfigurieren der Log Server-Verbindungen*, Seite 329
- *Konfigurieren der Datenbankoptionen für Log Server*, Seite 330
- *Konfigurieren von Log-Cachedateien*, Seite 333
- *Konfigurieren von WebCatcher*, Seite 337
- *Stoppen und Starten von Log Server*, Seite 340

Auf der Registerkarte **Konsolidierung** im Dienstprogramm zur Konfiguration von Log Server können Sie die Konsolidierung aktivieren und Konsolidierungsvorgaben festlegen.

> **Hinweis**
> Das Verwalten der Größe der Protokolldatenbank ist ein wichtiger Aspekt bei Netzwerken mit hohen Datenvolumen. Das Aktivieren der Konsolidierung stellt eine Möglichkeit dar, Datenbankgröße und -wachstum zu steuern.

Durch die Konsolidierung wird die Größe der Protokolldatenbank verringert, indem Internetanforderungen kombiniert werden, die folgende Elemente gemein haben:

- Domänenname (zum Beispiel: www.websense.com)
- Kategorie
- Schlüsselwort
- Aktion (zum Beispiel: Kategorie gesperrt)

- Benutzer/Workstation

Berichte werden schneller erstellt, wenn die Protokolldatenbank nicht so umfangreich ist. Durch die Konsolidierung der Protokolldaten kann die Genauigkeit einiger Detailberichte jedoch abnehmen, da separate Einträge für die gleiche Domäne möglicherweise verloren gehen.

> **Wichtig**
> Durch Aktivieren der Konsolidierung kann die Genauigkeit einiger Berichtsdaten wie die Berechnung der Navigationsdauer im Internet verfälscht werden.

1. Aktivieren Sie die Option **Protokolleinträge konsolidieren**, um die Konsolidierung zu aktivieren. Dadurch werden mehrere ähnliche Internetanforderungen zu einem einzigen Protokolleintrag zusammengefasst.

   Wenn diese Option deaktiviert ist (Standardeinstellung), speichert die Protokolldatenbank alle Details der Hits oder Besuche jeder einzelnen Internetanforderung (abhängig von Ihrer Auswahl auf der Registerkarte "Einstellungen", siehe *Konfigurieren von Log-Cachedateien*, Seite 333). Dadurch werden mehr Details für die Berichterstellung bereitgestellt, die Protokolldatenbank wird jedoch auch größer.

   Durch Auswahl dieser Option wird eine kleinere Protokolldatenbank mit weniger Berichtsdetails geschaffen.

   > **Wichtig**
   > Um konsistente Berichte zu ermöglichen, sollte eine neue Datenbankpartition erstellt werden, wenn Sie die Konsolidierung aktivieren oder deaktivieren. Achten Sie außerdem darauf, Berichte aus Partitionen mit denselben Konsolidierungseinstellungen zu generieren.

   Wenn Sie Websense Web Security Gateway installiert haben, werden Scanningaktivitäten in Echtzeit immer in Form von separaten Hits in den Berichten angezeigt, die sich auf Scanning in Echtzeit beziehen. Dies ist auch dann der Fall, wenn die Konsolidierung aktiviert ist. In diesem Fall sind die in den Webfilterungsberichten angegebenen Zahlen, die gesperrten Datenverkehr durch Scanning in Echtzeit umfassen, niedriger als die Zahlen, die in Berichten zum Scannen in Echtzeit angegeben werden.

2. Geben Sie als **Zeitintervall für Konsolidierung** die maximale Zeit zwischen den ersten und letzten Einträgen an, die kombiniert werden können.

   Dies bezeichnet den größtmöglichen Zeitunterschied für die Kombination der frühesten und aktuellen Einträge, um einen Konsolidierungseintrag daraus zu erhalten.

   Verringern Sie das Intervall, um die Detailgenauigkeit bei der Berichterstellung zu erhöhen. Vergrößern Sie das Intervall, um die Konsolidierung zu maximieren. Berücksichtigen Sie außerdem, dass ein größerer Intervall die Auslastung der Systemressourcen wie Arbeitsspeicher, Prozessor und Speicherplatz vergrößern kann.

Wenn Sie die Option zur Protokollierung vollständiger URLs auf der Seite "Berichterstellung > Protokolldatenbank (Registerkarte "Einstellungen") aktiviert haben, enthält der konsolidierte Protokolleintrag den vollständigen Pfad (bis zu 255 Zeichen) der ersten passenden Site, die von Log Server gefunden wird.

Nehmen wir zum Beispiel an, ein Benutzer hat folgende Sites besucht, und alle wurden in der Kategorie "Online-Shopping" kategorisiert.

- www.domain.com/shoeshopping
- www.domain.com/purseshopping
- www.domain.com/jewelryshopping

Bei einer aktiven Protokollierung der vollständigen URL wird durch die Konsolidierung ein einzelner Protokolleintrag unter der URL www.domain.com/shoeshopping geschaffen.

3. Klicken Sie auf **Anwenden**, um eventuelle Änderungen zu speichern, und starten Sie Log Server neu (siehe *Stoppen und Starten von Log Server*, Seite 340).

Konfigurieren von WebCatcher

Verwandte Themen:

- *Dienstprogramm für die Konfiguration von Log Server*, Seite 328
- *Konfigurieren der Log Server-Verbindungen*, Seite 329
- *Konfigurieren der Datenbankoptionen für Log Server*, Seite 330
- *Konfigurieren von Log-Cachedateien*, Seite 333
- *Konfigurieren von Konsolidierungsoptionen*, Seite 335
- *Konfigurieren von WebCatcher*, Seite 337
- *WebCatcher-Authentifizierung*, Seite 339
- *Stoppen und Starten von Log Server*, Seite 340

WebCatcher ist eine optionale Funktion, mit der unerkannte URLs und sicherheitsrelevante URLs gesammelt und an Websense, Inc., gesendet werden. Dort werden Sie auf potenzielle Sicherheits- und Haftungsrisiken hin untersucht und kategorisiert. (Die WebCatcher-Verarbeitung setzt keine Protokollierung der vollständigen URL voraus.) Websense, Inc. überprüft die Informationen und aktualisiert die Master Database mit den neu kategorisierten URLs, wodurch eine verbesserte Filterung ermöglicht wird.

Wählen Sie die URL-Typen aus, die gesendet werden sollen, und legen Sie die Dateigröße und Verarbeitungszeit auf der Registerkarte **WebCatcher** im Dienstprogramm zur Konfiguration von Log Server fest.

> **Hinweis**
> In einer Umgebung mit mehreren Instanzen von Log Server ist WebCatcher nur für ein Instanz von Log Server aktiviert. Sobald WebCatcher aktiviert ist, kann diese Registerkarte nicht mehr ausgewählt werden, wenn das Tool zur Konfiguration von Log Server für andere Instanzen von Log Server ausgeführt wird.

Die Informationen, die an Websense, Inc. gesendet werden, umfassen lediglich die URLs und keine Benutzerinformationen.

Im folgenden Beispiel wird dargestellt, welche Informationen gesendet werden, wenn sie WebCatcher aktiviert haben. Die IP-Adresse in diesem Beispiel entspricht der Adresse des Computers, der die URL hostet, und nicht der IP-Adresse des Requestors.

```
<URL HREF="http://www.ack.com/uncategorized/" CATEGORY="153"
IP_ADDR="200.102.53.105" NUM_HITS="1" />
```

WebCatcher-Daten werden über HTTP Post an Websense, Inc. gesendet. Sie müssen möglicherweise Rollen erstellen oder andere Änderungen an Ihrem Proxy-Server oder Ihrer Firewall vornehmen, um den ausgehenden HTTP-Datenverkehr zuzulassen. Anweisungen dazu finden Sie in der Dokumentation Ihres Proxy-Servers oder Ihrer Firewall.

1. Wählen Sie eine der folgenden Optionen aus:
   - Mit **Ja, nur angegebene URLs an Websense senden** wird die WebCatcher-Verarbeitung aktiviert. Sie müssen angeben, welche URLs gesendet werden sollen. Fahren Sie mit Schritt 2 fort.
   - Mit **Nein, keine Informationen an Websense senden** wird die WebCatcher-Verarbeitung deaktiviert. Es werden keine weiteren Einträge benötigt, wenn Sie diese Option auswählen.
2. Aktivieren Sie **URLs ohne Kategoriezuordnung senden**, um eine Liste mit allen URLs ohne Kategoriezuordnung zu senden, die in der Protokolldatenbank gefunden werden.

   Die von Websense, Inc. empfangenen URLs ohne Kategoriezuordnung werden analysiert und zu den entsprechenden Kategorien der Master Database hinzugefügt. Dadurch verbessert sich die Filtergenauigkeit in allen Organisationen.

   > **Hinweis**
   > Intranetsites werden von WebCatcher nicht gesendet. Dazu gehören alle Sites mit IP-Adressen in den Bereichen 10.xxx.xxx.xxx, 172.16.xxx.xxx und 192.168.xxx.xxx.

3. Aktivieren Sie **Sicherheitsrelevante URLs senden**, um eine Liste mit allen sicherheitsrelevanten URLs zu senden, die in der Protokolldatenbank gefunden werden.

   Sicherheitsrelevante URLs werden von Websense, Inc. analysiert, um die Aktivität der Sites in den Kategorien "Keylogger", "Bösartige Webseiten", "Phishing und sonstige Fälschungen" und "Spyware" bestimmen zu können.
4. Wählen Sie unter **Wählen Sie das Land/die Region aus, das/die am ehesten Ihrem Standort entspricht** das Land aus, in dem die meisten Aktivitäten protokolliert werden.
5. Aktivieren Sie die Option **Kopie der an Websense gesendeten Daten speichern**, um eine Kopie der Daten zu speichern, die an Websense, Inc. gesendet werden.

   Wenn diese Option aktiviert ist, speichert WebCatcher die Daten in unverschlüsselten XML-Dateien im Verzeichnis Websense\Reporter. Diese Dateien verfügen über einen Zeitstempel für Datum und Uhrzeit.
6. Geben Sie unter **Maximale Größe der Uploaddatei** an, wie groß die Datei werden darf (zwischen 4.096 und 8.192 KB), bevor sie an Websense gesendet wird.

   Stellen Sie sicher, dass Ihr System eine Datei dieser Größe über HTTP Post senden kann.
7. Legen Sie für **Früheste tägliche Startzeit** die Startzeit fest, ab der WebCatcher die Datei senden kann, wenn der Schwellenwert für die Größe an diesem Tag nicht erreicht wurde.

   Dadurch wird sichergestellt, dass die Informationen mindestens einmal am Tag gesendet und aus dem System entfernt werden.
8. Klicken Sie auf die Schaltfläche **Authentifizierung**, wenn der Computer mit Log Server sich authentifizieren muss, um auf das Internet zugreifen zu können.

   Informationen zum sich daraufhin öffnenden Dialogfeld **Authentifizierung** finden Sie unter *WebCatcher-Authentifizierung*, Seite 339.
9. Klicken Sie auf **Anwenden**, um eventuelle Änderungen zu speichern, und starten Sie Log Server neu (siehe *Stoppen und Starten von Log Server*, Seite 340).

WebCatcher-Authentifizierung

Verwandte Themen:

- *Dienstprogramm für die Konfiguration von Log Server*, Seite 328
- *Konfigurieren von WebCatcher*, Seite 337
- *Stoppen und Starten von Log Server*, Seite 340

Das Dialogfeld "Authentifizierung" wird geöffnet, nachdem Sie auf der Registerkarte "WebCatcher" auf **Authentifizierung** geklickt haben.

1. Aktivieren Sie die Option **Proxy-Server benutzen**, wenn der Computer mit Log Server über einen Proxy-Server auf das Internet zugreift, und geben Sie dann die erforderlichen Informationen ein.

Feld	Beschreibung
Name des Proxy-Servers	Geben Sie den Namen des Computers oder die IP-Adresse des Proxy-Servers an, durch den Log Server auf das Internet zugreift.
Proxy-Server-Port	Geben Sie die Portnummer ein, über die der Proxy-Server kommuniziert.

2. Aktivieren Sie die Option **Standardauthentifizierung verwenden**, wenn der Computer mit Log Server sich authentifizieren muss, um auf das Internet zugreifen zu können. Geben Sie dann den Benutzernamen und das Passwort für die Authentifizierung ein.
3. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern, und kehren Sie dann zur Registerkarte "WebCatcher" zurück.

Stoppen und Starten von Log Server

Verwandte Themen:

- *Dienstprogramm für die Konfiguration von Log Server*, Seite 328
- *Konfigurieren der Log Server-Verbindungen*, Seite 329

Log Server empfängt Informationen von Filtering Service und speichert sie in der Protokolldatenbank, damit sie bei der Erstellung von Berichten verwendet werden können. Er wird als Windows-Dienst ausgeführt und startet normalerweise während der Installation. Danach wird er jedes Mal gestartet, wenn der Computer neu gestartet wird.

Im Dienstprogramm für die Konfiguration von Log Server vorgenommene Änderungen werden erst wirksam, wenn Log Server gestoppt und neu gestartet wird. Dies kann problemlos über die Registerkarte "Verbindung" im Dienstprogramm für die Konfiguration von Log Server erfolgen.

1. Wählen Sie im Windows-Startmenü die Optionen **Alle Programme > Websense > Dienstprogramme > Konfiguration von Log Server** aus.
2. Öffnen Sie die Registerkarte **Verbindungen**, und klicken Sie auf **Stop**.
3. Warten Sie einige Sekunden, und klicken Sie dann auf **Start**, um den Log Server-Dienst neu zu starten.

4. Klicken Sie auf **OK**, um das Dienstprogramm für die Konfiguration von Log Server zu schließen.

> **Hinweis**
> Websense kann keine Internetzugriffe protokollieren, die erfolgen, während Log Server gestoppt ist.

Einführung in die Log Database

Verwandte Themen:

- *Datenbankjobs*, Seite 342
- *Verwalten der Protokolldatenbank*, Seite 343

In der Log Database werden die Einträge zur Internetaktivität und den damit in Zusammenhang stehenden Websense-Filteraktionen gespeichert. Bei der Installation wird die Protokolldatenbank mit einer Katalogdatenbank und einer Datenbankpartition angelegt.

Die **Katalogdatenbank** stellt einen einzigen Verbindungspunkt für die verschiedenen Websense-Komponenten zur Verfügung, für die ein Zugang zur Protokolldatenbank erforderlich ist: Statusseiten, Log Server, Präsentationsberichte und Untersuchungsberichte. Sie enthält unterstützende Informationen für die Datenbankpartitionen einschließlich der Liste der Kategorienamen und Risikoklassendefinitionen, der Zuordnung von Benutzern zu Gruppen sowie der Datenbankjobs usw. Die Katalogdatenbank führt außerdem eine Liste aller verfügbarer Datenbankpartitionen.

In **Datenbankpartitionen** werden die individuellen Protokolleinträge zur Internetaktivität gespeichert. Für MSDE-Benutzer werden neue Partitionen erstellt, deren Grundlage die von der Websense-Software angelegten Regeln zur Größe bei Rollovern sind. Benutzer von Microsoft SQL Server können die Protokolldatenbank so konfigurieren, dass abhängig von der Partitionsgröße oder einem Datumsintervall eine neue Partition gestartet wird. (Weitere Informationen hierzu finden Sie unter *Konfiguration von Rollover-Optionen*, Seite 344.)

> **Hinweis**
> Datumsbasierte Partitionen sind nur dann möglich, wenn die Websense-Software mit SQL Server als Datenbankmodul verwendet wird.

Bei auf der Größe basierenden Partitionen werden alle eingehenden Protokolleinträge in die zuletzt angelegte aktive Partition, die die Größenregel erfüllt, eingefügt. Wenn die Partition die festgelegte maximale Größe erreicht, wird eine neue Partition erstellt, in die die neuen Protokolleinträge eingefügt werden.

Wenn die Partitionen auf dem Datum beruhen, werden neue Partitionen gemäß dem festgelegten Zyklus erstellt. Wenn das Rollover beispielsweise monatlich stattfindet, wird eine neue Partition erstellt, sobald neue Einträge für den neuen Monat empfangen werden. Eingehende Protokolleinträge werden nach ihrem Datum in die entsprechende Partition eingefügt.

Datenbankpartitionen bieten Vorteile in Bezug auf Flexibilität und Leistung. Beispielsweise können Sie Berichte aus einer einzelnen Partition generieren, um den Umfang der Daten zu begrenzen, die zum Suchen der gewünschten Informationen analysiert werden müssen.

Datenbankjobs

Die folgenden Datenbankjobs werden zusammen mit der Protokolldatenbank installiert. SQL Server Agent muss auf dem Computer ausgeführt werden, auf dem das Datenbankmodul (MSDE oder Microsoft SQL Server) aktiv ist.

- Der ETL-Job (Extract, Transform, and Load, Extrahieren, Transformieren und Laden) ist immer aktiv. Es werden pausenlos Daten von Log Server empfangen, verarbeitet und danach in die Partitionsdatenbank eingefügt. Der ETL-Job muss ausgeführt werden, damit Protokolleinträge in die Protokolldatenbank übernommen werden können.
- Der Datenbankwartungsjob führt die Datenbankwartungsaufgaben durch und bewahrt die optimale Leistung. Dieser Job wird standardmäßig jede Nacht ausgeführt.
- Der IBT-Job (Internet Browse Time, Navigationsdauer im Internet) analysiert die empfangenen Daten und errechnet die Navigationsdauer der einzelnen Clients. Der IBT-Datenbankjob ist ressourcenintensiv und wirkt sich auf annähernd alle Datenbankressourcen aus. Dieser Job wird standardmäßig jede Nacht ausgeführt.

Bestimmte Aspekte dieser Datenbankjobs können auf der Seite "Einstellungen > Protokolldatenbank" konfiguriert werden. Weitere Informationen dazu finden Sie unter *Protokolldatenbank-Verwaltungseinstellungen*, Seite 343.

Beim Konfigurieren der Startzeit für den Wartungsjob und den Job zur Navigationsdauer im Internet sollten die Systemressourcen und der Netzwerkdatenverkehr berücksichtigt werden. Diese Jobs sind ressourcenintensiv und können die Geschwindigkeit der Protokollierung und Berichterstellung reduzieren.

Verwalten der Protokolldatenbank

Verwandte Themen:

- *Protokolldatenbank-Verwaltungseinstellungen*, Seite 343
- *Konfiguration von Rollover-Optionen*, Seite 344
- *Konfigurieren der Optionen für die Navigationsdauer im Internet*, Seite 347
- *Konfigurieren der Protokollierung der vollständigen URL*, Seite 346
- *Konfigurieren der Wartungsoptionen für die Protokolldatenbank*, Seite 349
- *Konfigurieren der Partitionserstellung für die Protokolldatenbank*, Seite 351
- *Konfigurieren der verfügbaren Optionen*, Seite 352
- *Anzeigen von Fehlerprotokollen*, Seite 354

Die Verwaltung der Protokolldatenbank umfasst die Steuerung vieler Aspekte der Datenbankoperationen und befasst sich unter anderem mit den folgenden Fragen:

- Welche Vorgänge werden von den Datenbankjobs ausgeführt und wann sind sie aktiv?
- Welches sind die Bedingungen zum Erstellen neuer Datenbankpartitionen?
- Welche Partitionen stehen für die Berichterstellung zur Verfügung?

Diese und weitere Optionen verleihen der Person, die die Protokolldatenbank verwaltet, beträchtliche Steuerungsmöglichkeiten. Siehe *Protokolldatenbank-Verwaltungseinstellungen*, Seite 343.

Der übergeordnete Administrator legt bei der Erstellung von Rollen fest, wer Verwaltungsaufgaben für die Protokolldatenbank durchführen kann. Siehe *Rollen bearbeiten*, Seite 272.

Hinweis

Es empfiehlt sich, die Anzahl der Administratoren mit der Berechtigung zum Ändern der Protokolldatenbank-Einstellungen zu begrenzen.

Protokolldatenbank-Verwaltungseinstellungen

Verwandte Themen:

- *Verwalten der Protokolldatenbank*, Seite 343

Die Seite **Berichterstellung > Protokolldatenbank** kann über die Registerkarte "Einstellungen" geöffnet werden. Sie können damit verschiedene Protokolldatenbank-Vorgänge verwalten. Die Optionen werden in logische Abschnitte gruppiert, die separat beschrieben werden.

Sie müssen innerhalb eines Abschnitts auf die Schaltfläche "Jetzt speichern" klicken, damit die Änderungen in diesem Abschnitt aktiv werden. Durch Klicken auf **Jetzt speichern** werden die Änderungen in diesem Abschnitt sofort aufgezeichnet. (Es ist nicht erforderlich, zusätzlich auf "Alles speichern" zu klicken.)

Am Anfang der Seite werden der Name der aktiven Protokolldatenbank und der Link **Anzeige aktualisieren** angezeigt. Dieser Link zur Aktualisierung der Anzeige zeigt die Informationen erneut an, die aktuell auf der Protokolldatenbank-Seite zu sehen sind. Alle Änderungen, die nicht über die entsprechende Schaltfläche "Jetzt speichern" übernommen wurden, gehen verloren.

Klicken Sie auf den entsprechenden untenstehenden Link, um detaillierte Informationen zur Verwendung der einzelnen Abschnitte zu erhalten.

- Optionen für Datenbank-Rollover: *Konfiguration von Rollover-Optionen*, Seite 344.
- Protokollierung der vollständigen URL: *Konfigurieren der Protokollierung der vollständigen URL*, Seite 346.
- Konfiguration für die Navigationsdauer im Internet: *Konfigurieren der Optionen für die Navigationsdauer im Internet*, Seite 347.
- Konfiguration der Wartung: *Konfigurieren der Wartungsoptionen für die Protokolldatenbank*, Seite 349.
- Erstellung von Datenbankpartitionen: *Konfigurieren der Partitionserstellung für die Protokolldatenbank*, Seite 351.
- Verfügbare Partitionen: *Konfigurieren der verfügbaren Optionen*, Seite 352.
- Fehlerprotokollaktivität: *Anzeigen von Fehlerprotokollen*, Seite 354.

Konfiguration von Rollover-Optionen

Verwandte Themen:

- *Protokolldatenbank-Verwaltungseinstellungen*, Seite 343
- *Konfigurieren der Optionen für die Navigationsdauer im Internet*, Seite 347
- *Konfigurieren der Protokollierung der vollständigen URL*, Seite 346
- *Konfigurieren der Wartungsoptionen für die Protokolldatenbank*, Seite 349
- *Konfigurieren der Partitionserstellung für die Protokolldatenbank*, Seite 351
- *Konfigurieren der verfügbaren Optionen*, Seite 352
- *Anzeigen von Fehlerprotokollen*, Seite 354

Im Bereich **Optionen für Datenbank-Rollover** der Seite "Berichterstellung > Protokolldatenbank (Registerkarte "Einstellungen") können Sie angeben, wann von der Log Database eine neue Datenbankpartition (Rollover) erstellt werden soll.

1. Mit den Optionen **Rollover in folgenden Intervallen wiederholen** können Sie festlegen, ob für Datenbankpartitionen ein Rollover auf Grundlage der Größe (MB) oder des Datums (Wochen oder Monate) durchgeführt werden soll. Dies hängt vom verwendeten Datenbankmodul ab.

   Für MSDE-Benutzer ist nur die Option des Rollovers nach Größe verfügbar. Benutzer von Microsoft SQL Server können die Rollover nach Größe oder Datum durchführen.

   - Wählen Sie bei datumsbasierten Rollovern entweder **Wochen** oder **Monate** als Maßeinheit aus, und geben Sie an, wie viele volle Kalenderwochen oder -monate in einer Datenbankpartition gearbeitet werden soll, bevor eine neue erstellt wird.
   - Wählen Sie für größenbasierte Rollover **MB** aus, und geben Sie die Anzahl an MB an, nach deren Erreichen das Rollover gestartet werden soll.

     Microsoft SQL Server-Benutzer können die Größe auf bis zu 204.800 MB festlegen.

     MSDE-Benutzer können zwischen 100 MB and 1.536 MB als Größe angeben.

     Hinweis

     Wenn das Rollover zu einer Zeit mit viel Datenverkehr stattfindet, kann es während des Rollover-Vorgangs zu Leistungseinbußen kommen.

     Um dies zu vermeiden, wird in einigen Umgebungen das automatische Rollover nach einer langen Zeitperiode oder bei Erreichen einer beträchtlichen maximalen Größe ausgeführt. Dann werden regelmäßig manuelle Rollover durchgeführt, um automatischen Rollovern zuvorzukommen. Informationen zu manuellen Rollovern finden Sie unter *Konfigurieren der Partitionserstellung für die Protokolldatenbank*, Seite 351.

     Beachten Sie, dass es sich nicht empfiehlt, sehr große individuelle Partitionen anzulegen. Die Geschwindigkeit der Berichterstellung kann abnehmen, wenn Daten nicht auf mehrere kleinere Partitionen aufgeteilt werden.

   Beim Erstellen einer neuen Partitionsdatenbank wird automatisch die Berichterstellung für die Partition aktiviert (siehe *Konfigurieren der verfügbaren Optionen*, Seite 352).

2. Klicken Sie auf **Jetzt speichern**, um die Änderungen an den Rollover-Optionen für die Datenbank zu aktivieren.

Konfigurieren der Protokollierung der vollständigen URL

Verwandte Themen:

- *Protokolldatenbank-Verwaltungseinstellungen*, Seite 343
- *Konfiguration von Rollover-Optionen*, Seite 344
- *Konfigurieren der Optionen für die Navigationsdauer im Internet*, Seite 347
- *Konfigurieren der Wartungsoptionen für die Protokolldatenbank*, Seite 349
- *Konfigurieren der Partitionserstellung für die Protokolldatenbank*, Seite 351
- *Konfigurieren der verfügbaren Optionen*, Seite 352
- *Anzeigen von Fehlerprotokollen*, Seite 354

Im Bereich **Protokollierung der vollständigen URL** auf der Seite "Berichterstellung > Protokolldatenbank" (Registerkarte "Einstellungen") können Sie festlegen, welcher Teil der URL für die jeweiligen Internetanforderungen protokolliert wird.

Hinweis

Das Verwalten der Protokolldatenbank-Größe ist ein wichtiger Aspekt bei Netzwerken mit hohen Datenvolumen. Eine Deaktivierung der Option zur Protokollierung der vollständigen URL ist eine Möglichkeit, wie Datenbankgröße und -wachstum gesteuert werden können.

1. Aktivieren Sie **Aufzeichnung der vollständigen URL für jede angeforderte Site**, um die vollständige URL einschließlich der Domäne (www.domain.com) und dem Pfad zur entsprechenden Seite (/Produkte/ProduktA.html) zu protokollieren.

   Wichtig

   Aktivieren Sie die Protokollierung der vollständigen URL, wenn Sie die Erstellung von Berichten über die Scanningaktivitäten in Echtzeit planen (siehe *Erstellen von Berichten über Scanningaktivitäten in Echtzeit*, Seite 162). Sonst enthalten die Berichte nur die Domäne (www.domain.com) der kategorisierten Site, auch wenn einzelne Seiten der Website u. U. zu unterschiedlichen Kategorien gehören oder unterschiedliche Bedrohungen enthalten.

Wenn diese Option nicht aktiviert ist, werden nur Domänennamen protokolliert. Durch diese Auswahl verkleinert sich der Umfang der Datenbank, sie enthält jedoch auch weniger Einzelheiten.

Die Protokollierung vollständiger URLs erzeugt eine umfangreichere Protokolldatenbank, bietet dafür aber Informationen mit höherem Detaillierungsgrad.

Wenn Sie die Protokollierung der vollständigen URL bei aktiver Konsolidierung aktivieren, enthält der konsolidierte Eintrag die vollständige URL ab dem ersten Eintrag in der Konsolidierungsgruppe. Weitere Informationen dazu finden Sie unter *Konfigurieren von Konsolidierungsoptionen*, Seite 335.

2. Klicken Sie auf **Jetzt speichern**, um die Änderungen an den Optionen für die Protokollierung der vollständigen URL zu aktivieren.

Konfigurieren der Optionen für die Navigationsdauer im Internet

Verwandte Themen:

- *Protokolldatenbank-Verwaltungseinstellungen*, Seite 343
- *Konfiguration von Rollover-Optionen*, Seite 344
- *Konfigurieren der Protokollierung der vollständigen URL*, Seite 346
- *Konfigurieren der Wartungsoptionen für die Protokolldatenbank*, Seite 349
- *Konfigurieren der Partitionserstellung für die Protokolldatenbank*, Seite 351
- *Konfigurieren der verfügbaren Optionen*, Seite 352
- *Anzeigen von Fehlerprotokollen*, Seite 354

Die Berichte zur Navigationsdauer im Internet (IBT) vermitteln eine Übersicht über die Dauer, die ein Benutzer im Internet navigiert. Der jede Nacht durchgeführte Datenbankjob berechnet die Navigationsdauer der einzelnen Clients auf Grundlage der neuen Protokolleinträge, die an diesem Tag empfangen wurden. Legen Sie die Optionen für die Navigationsdauer im Bereich **Konfiguration für die Navigationsdauer im Internet** auf der Seite "Einstellungen > Protokolldatenbank" fest.

1. Wählen Sie für den IBT-Datenbankjob eine **Startzeit des Jobs** fest.

   Die Dauer zur Ausführung dieses Jobs und die dafür erforderlichen Systemressourcen sind je nach dem Umfang der an diesem Tag protokollierten Daten unterschielich. Es empfiehlt sich, diesen Job nicht während des nachts stattfindenden Wartungsjobs auszuführen (siehe *Konfigurieren der Wartungsoptionen für die Protokolldatenbank*, Seite 349) und eine Zeit mit wenig Datenverkehr im Netzwerk dafür zu wählen, um die Auswirkungen auf die Berichterstellung zu minimieren.

Der IBT-Datenbankjob ist ressourcenintensiv und wirkt sich auf annähernd alle Datenbankressourcen aus. Wenn Sie diesen Job aktivieren, legen Sie die Startzeit so fest, dass der Job die Leistungsfähigkeit des Datenbanksystems bei der Verarbeitung geplanter Berichte und anderer wichtiger Abläufe nicht beeiträchtigt. Sie sollten den Job zusätzlich überwachen, um feststellen zu können, ob eine stabilere Hardware für die Verarbeitung aller erforderlichen Vorgänge benötigt wird.

2. Legen Sie als **Schwellenwert für die Lesezeit** eine durchschnittliche Minutenanzahl für das Lesen einer bestimmten Website fest.

   Der Schwellenwert für die Lesezeit definiert die Navigationssitzungen für die Berichte über die Navigationsdauer im Internet. Durch das Öffnen eines Browsers wird HTTP-Datenverkehr erzeugt. Dies zeigt den Beginn einer Navigationssitzung an. Die Sitzung ist offen, solange innerhalb der hier festgelegten Zeit beständig HTTP-Datenverkehr erzeugt wird. Die Navigationssitzung wird als geschlossen angesehen, sobald diese Zeitdauer verstreicht, ohne dass HTTP-Datenverkehr erzeugt wird. Eine neue Navigationssitzung beginnt, wenn wieder HTTP-Datenverkehr generiert wird.

   Hinweis

   Der Schwellenwert für die Lesedauer sollte möglichst selten geändert werden. Zudem empfiehlt es sich, bei jeder Änderung eine neue Datenbankpartition zu beginnen.

   Damit keine inkonsistenten Daten in Berichten vorkommen, sollten IBT-Berichte aus Datenbankpartionen generiert werden, für die derselbe Schwellenwert für die Lesedauer festgelegt wurde.

   Beachten Sie, dass einige Websites eine automatische Aktualisierung verwenden, die Informationen in regelmäßigen Abständen aktualisiert. Ein Beispiel hierfür sind Nachrichten-Websites, die in einem Zyklus verschiedene Anzeigen mit den neuesten Nachrichten anzeigen. Durch die Aktualisierung wird neuer HTTP-Datenverkehr generiert. Aus diesem Grund werden bei jeder Aktualisierung der Website neue Protokolleinträge generiert, wenn eine Website dieser Art geöffnet ist. Es kommt zu keinem längeren Abbruch des HTTP-Datenverkehrs, sodass die Navigationssitzung nicht geschlossen wird.

3. Legen Sie einen Wert für die **Letzte Lesezeit** fest, um die Zeit messen zu können, die das Lesen der letzten Website vor dem Ende der Navigationssitzung in Anspruch genommen hat.

   Wenn die zeitliche Lücke im Datenverkehr den Schwellenwert für die Lesezeit überschreitet, wird die Sitzung beendet, und der Wert unter "Letzte Lesezeit" wird zur Sitzungszeit hinzugerechnet.

4. Klicken Sie auf **Jetzt speichern**, um die Änderungen in der Konfiguration der Navigationsdauer im Internet zu aktivieren.

Konfigurieren der Wartungsoptionen für die Protokolldatenbank

Verwandte Themen:

- *Protokolldatenbank-Verwaltungseinstellungen*, Seite 343
- *Konfiguration von Rollover-Optionen*, Seite 344
- *Konfigurieren der Optionen für die Navigationsdauer im Internet*, Seite 347
- *Konfigurieren der Protokollierung der vollständigen URL*, Seite 346
- *Konfigurieren der Partitionserstellung für die Protokolldatenbank*, Seite 351
- *Konfigurieren der verfügbaren Optionen*, Seite 352
- *Anzeigen von Fehlerprotokollen*, Seite 354

Über den Bereich **Konfiguration der Wartung** auf der Seite "Berichterstellung > Protokolldatenbank" (Registerkarte "Einstellungen") können bestimmte Aspekte der Datenbankverarbeitung wie die Zeit für die Ausführung des Datenbankwartungsjobs, einige der darüber ausgeführten Aufgaben und das Löschen von Datenbankpartitionen und Fehlerprotokollen gesteuert werden.

1. Wählen Sie als **Startzeit der Wartung** die Tageszeit aus, zu der der Datenbankwartungsjob ausgeführt werden soll.

   Die Dauer zur Ausführung dieses Jobs und die dafür erforderlichen Systemressourcen sind je nach den in diesem Bereich ausgewählten Aufgaben unterschiedlich. Es wird empfohlen, diesen Job zu einer Zeit mit wenig Datenverkehr im Netzwerk und nicht zeitgleich mit dem IBT-Job durchzuführen, um die Auswirkungen auf andere Aktivitäten und Systeme so gering wie möglich zu halten (siehe *Konfigurieren der Optionen für die Navigationsdauer im Internet*, Seite 347).
2. Aktivieren Sie die Option **Partitionen automatisch löschen**, und geben Sie die Anzahl der Tage (zwischen 2 und 365) an, nach denen die Partitionen automatisch gelöscht werden sollen.

   Warnung

   Nachdem eine Partition gelöscht wurde, können die Daten nicht wiederhergestellt werden. Eine alternative Möglichkeit zum Löschen von Partitionen finden Sie unter *Konfigurieren der verfügbaren Optionen*, Seite 352.
3. Aktivieren Sie die Option **Automatische Neuindexierung aktivieren**, und wählen Sie einen Wochentag aus, an dem dieser Vorgang jede Woche automatisch ausgeführt werden soll.

Die Neuindexierung der Datenbank ist wichtig, um die Datenbankintegrität erhalten und die Geschwindigkeit der Berichterstellung optimieren zu können.

> **Wichtig**
> Dieser Vorgang sollte möglichst bei wenig Datenverkehr im Netzwerk ausgeführt werden. Die Neuindexierung von Datenbankpartitionen ist ressourcenintensiv und sehr zeitaufwändig. Während dieses Prozesses sollten keine Berichte erstellt werden.

4. Aktivieren Sie die Option **Fehlgeschlagene Batches nach Ablauf folgender Frist (in Tagen) löschen**, und geben sie dann die Zahl der Tage (zwischen 0 und 90) ein, nach denen alle fehlgeschlagenen Batches gelöscht werden sollen.

   Wenn diese Option nicht aktiviert ist, werden fehlgeschlagene Batches unbegrenzt für zukünftige Vorgänge beibehalten.

   Wenn nicht genügend Speicherplatz für das Einfügen der Protokolleinträge in die Datenbank zur Verfügung steht oder die Datenbankberechtigungen unzureichend sind, werden die Einträge als **fehlgeschlagener Batch** gekennzeichnet. Normalerweise werden diese Batches erfolgreich erneut verarbeitet und im Rahmen des nachts durchgeführten Datenbankverwaltungsjobs in die Datenbank eingefügt.

   Diese erneute Verarbeitung kann jedoch nur dann erfolgreich sein, wenn das Problem mit dem Speicherplatz oder den Berechtigungen zwischenzeitlich gelöst wurde. Die fehlgeschlagenen Batches werden zudem nur dann erneut verarbeitet, wenn die Option **nicht verarbeitete Batches verarbeiten** aktiviert ist. Sie werden nach der hier festgelegten Zeit gelöscht.

5. Aktivieren Sie die Option **nicht verarbeitete Batches verarbeiten**, damit während dem nachts durchgeführten Datenbankwartungsjob die fehlgeschlagenen Batches erneut verarbeitet werden.

   Wenn diese Option nicht aktiviert wird, werden fehlgeschlagene Batches nie erneut verarbeitet. Sie werden gegebenenfalls nach dem oben festgelegten Zeitraum gelöscht.

6. Aktivieren Sie die Option **Fehlerprotokoll nach Ablauf folgender Frist (in Tagen) löschen**, und geben sie dann die Zahl der Tage (zwischen 0 und 90) ein, nach denen Fehlereinträge in der Datenbank aus der Katalogdatenbank gelöscht werden sollen.

   Wenn diese Option nicht ausgewählt ist, werden Fehlerprotokolle auf unbegrenzte Zeit beibehalten.

7. Klicken Sie auf **Jetzt speichern**, um die Änderungen an der Wartungskonfiguration zu aktivieren.

Konfigurieren der Partitionserstellung für die Protokolldatenbank

Verwandte Themen:

- *Protokolldatenbank-Verwaltungseinstellungen*, Seite 343
- *Konfiguration von Rollover-Optionen*, Seite 344
- *Konfigurieren der Optionen für die Navigationsdauer im Internet*, Seite 347
- *Konfigurieren der Protokollierung der vollständigen URL*, Seite 346
- *Konfigurieren der Wartungsoptionen für die Protokolldatenbank*, Seite 349
- *Konfigurieren der verfügbaren Optionen*, Seite 352
- *Anzeigen von Fehlerprotokollen*, Seite 354

Über den Bereich **Erstellung der Datenbank partition** auf der Seite "Berichterstellung > Protokolldatenbank" (Registerkarte "Einstellungen") können Sie die Merkmale neuer Datenbankpartitionen wie Speicherort- und Größenoptionen definieren. In diesem Bereich können Sie auch direkt eine neue Partition erstellen und müssen nicht darauf warten, dass das geplante Rollover durchgeführt wird (siehe *Konfiguration von Rollover-Optionen*, Seite 344).

1. Geben Sie den **Dateipfad** an, unter dem die **Daten**- und **Protokoll**dateien für neue Datenbankpartitionen erstellt werden sollen.
2. Legen Sie unter **Anfangsgröße** die anfängliche Dateigröße (zwischen 100 und 204.800 MB) für die **Daten**- und **Protokoll**dateien der neuen Datenbankpartitionen fest.

   Microsoft SQL Server-Benutzer: Der geltende Bereich liegt zwischen 100 und 204.800

   MSDE-Benutzer: Der geltende Bereich liegt zwischen 100 und 1.500

   Hinweis

   Es hat sich bewährt, die durchschnittliche Partitionsgröße über einen bestimmten Zeitraum zu berechnen. Aktualisieren Sie den Anfangswert dann auf diesen Wert. Auf diese Weise muss die Partition nicht so oft vergrößert werden, und es werden Ressourcen zur Verarbeitung von Daten in den Partitionen freigesetzt.

3. Legen Sie unter **Größenzuwachs** den Wert für die Vergrößerung der **Daten**- und **Protokoll** dateien einer Partition (in MB) fest, falls zusätzlicher Speicherplatz benötigt wird.

   Microsoft SQL Server-Benutzer: Der geltende Bereich liegt zwischen 1 und 999.999

   MSDE-Benutzer: Der geltende Bereich liegt zwischen 1 und 450

4. Klicken Sie auf **Jetzt speichern**, um die Änderungen an Pfad, Größe und Größenzuwachs zu implementieren.

   Nach diesen Änderungen erstellte Datenbankpartitionen verwenden die neuen Einstellungen.

5. Klicken Sie auf **Jetzt erstellen**, um unabhängig von den Einstellungen für automatische Rollover bei der nächsten Ausführung des ETL-Jobs eine neue Partition zu erstellen (siehe *Datenbankjobs*, Seite 342). Dieser Vorgang dauert normalerweise einige Minuten.

   Achten Sie darauf, auf **Jetzt speichern** und dann erst auf **Jetzt erstellen** zu klicken, damit die in diesem Abschnitt vorgenommenen Änderungen bei der Erstellung der neuen Partition berücksichtigt werden.

   Klicken Sie in regelmäßigen Abständen im Inhaltsfenster auf den Link "Anzeige aktualisieren". Im Bereich "Verfügbare Partitionen" wird nach Abschluss des Erstellungsprozesses die neue Partition angezeigt.

Konfigurieren der verfügbaren Optionen

Verwandte Themen:

- *Protokolldatenbank-Verwaltungseinstellungen*, Seite 343
- *Konfiguration von Rollover-Optionen*, Seite 344
- *Konfigurieren der Optionen für die Navigationsdauer im Internet*, Seite 347
- *Konfigurieren der Protokollierung der vollständigen URL*, Seite 346
- *Konfigurieren der Wartungsoptionen für die Protokolldatenbank*, Seite 349
- *Konfigurieren der Partitionserstellung für die Protokolldatenbank*, Seite 351
- *Anzeigen von Fehlerprotokollen*, Seite 354

Im Bereich **Verfügbare Partitionen** auf der Seite "Berichterstellung > Protokolldatenbank (Registerkarte "Einstellungen") werden alle für die Berichterstellung verfügbaren Datenbankpartitionen aufgeführt. In der Liste werden die abgedeckten Daten sowie Größe und Name der einzelnen Partitionen angezeigt.

Mithilfe dieser Liste können Sie steuern, welche Datenbankpartitionen in Berichten erfasst werden. Sie können außerdem individuelle Partitionen auswählen, die gelöscht werden sollen.

1. Aktivieren Sie neben den einzelnen Partitionen, die in den Berichten berücksichtigt werden sollen, die Option **Aktivieren**.

   Verwenden Sie gegebenenfalls die Optionen **Alle** und **Keine**, die über der Liste angezeigt werden.

Sie müssen mindestens eine Partition für die Berichterstellung aktivieren. Über die Option **Keine** können Sie alle Partitionen gleichzeitig deaktivieren und danach nur einige wenige aktivieren.

Verwenden Sie die diese Optionen, um die Anzahl der zu analysierenden Daten bei der Berichterstellung zu verwalten und die Berichtsverarbeitung zu beschleunigen. Wenn Sie beispielsweise eine Reihe von Berichten für Juni generieren möchten, deaktivieren Sie alle Partitionen, die kein Datum von Juni aufweisen.

Wichtig

Diese Auswahl wirkt sich sowohl auf geplante Berichte als auch auf interaktiv ausgeführte Berichte aus. Stellen Sie sicher, dass die relevanten Partitionen aktiviert sind, wenn eine Berichterstellung geplant ist, um die Generierung von Berichten ohne Daten zu vermeiden.

2. Klicken Sie neben einem Partitionsnamen auf die Option **Löschen**, wenn die Partition nicht mehr benötigt wird. Die Partition wird gelöscht, wenn der nachts ausgeführte Datenbankwartungsjob das nächste Mal ausgeführt wird.

Warnung

Lassen Sie bei der Verwendung dieser Option Vorsicht walten. Gelöschte Partitionen können nicht wiederhergestellt werden.

Das Löschen veralteter Partitionen reduziert die Anzahl der Partitionen in der Protokolldatenbank. Dadurch wird die Leistung der Datenbank und der Berichterstellung erhöht. Verwenden Sie die Option "Löschen", um gegebenenfalls einzelne Optionen zu löschen. Informationen zum Löschen älterer Partitionen nach einem Zeitplan finden Sie unter *Konfigurieren der Wartungsoptionen für die Protokolldatenbank*, Seite 349.

3. Klicken Sie auf **Jetzt speichern**, um die Änderungen an den Optionen für die verfügbaren Partitionen zu aktivieren.

Anzeigen von Fehlerprotokollen

Verwandte Themen:

- *Protokolldatenbank-Verwaltungseinstellungen*, Seite 343
- *Konfiguration von Rollover-Optionen*, Seite 344
- *Konfigurieren der Optionen für die Navigationsdauer im Internet*, Seite 347
- *Konfigurieren der Protokollierung der vollständigen URL*, Seite 346
- *Konfigurieren der Wartungsoptionen für die Protokolldatenbank*, Seite 349
- *Konfigurieren der Partitionserstellung für die Protokolldatenbank*, Seite 351
- *Konfigurieren der verfügbaren Optionen*, Seite 352

Im Bereich **Fehlerprotokollaktivität** auf der Seite "Berichterstellung > Protokolldatenbank (Registerkarte "Einstellungen") können Sie die Einträge der Fehler anzeigen, die während der Ausführung der Jobs in der Websense Protokolldatenbank aufgetreten sind (siehe *Datenbankjobs*, Seite 342). Diese Informationen können sich bei der Problembehandlung als nützlich erweisen.

Wählen Sie eine der folgenden Optionen aus.

- Wählen Sie eine Ziffer aus der Dropdownliste aus, um die entsprechende Anzahl an Fehlerprotokolleinträgen anzuzeigen.
- Wählen Sie **Anzeige aller** aus, um alle Fehlerprotokolleinträge anzuzeigen.
- Wählen Sie **Keine/n anzeigen** aus, um alle Fehlerprotokolleinträge auszublenden.

Konfigurieren von Untersuchungsberichten

Verwandte Themen:

- *Standardeinstellungen für Datenbankverbindung und Berichte*, Seite 355
- *Anzeige- und Ausgabeoptionen*, Seite 357

Mithilfe von Untersuchungsberichten können Sie sich interaktiv mit den Informationen zur Internetnutzung in Ihrer Organisation befassen. Siehe *Untersuchungsberichte*, Seite 123.

Über den Link "Optionen" auf der Hauptseite zu Untersuchungsberichten haben Sie die Möglichkeit, die Protokolldatenbank zu ändern, mit der die Berichterstellung

erfolgen soll. Zudem können Sie die Standardansicht von Detailberichten ändern. Siehe *Standardeinstellungen für Datenbankverbindung und Berichte*, Seite 355.

Mit der Datei **wse.ini** können Sie bestimmte Standardeinstellungen zum Anzeigen von Übersichtsberichten und Berichten über mehrere Ebenen konfigurieren. Sie können darüber auch die Standardseitengröße steuern, die bei der Ausgabe eines Berichts in PDF-Format verwendet wird. Siehe *Anzeige- und Ausgabeoptionen*, Seite 357.

Standardeinstellungen für Datenbankverbindung und Berichte

Verwandte Themen:

- *Konfigurieren von Untersuchungsberichten*, Seite 354
- *Anzeige- und Ausgabeoptionen*, Seite 357
- *Zusammenfassende Berichte*, Seite 125
- *Zusammenfassende Berichte mit mehreren Ebenen*, Seite 130

Auf der Seite **Untersuchungsberichte > Optionen** können Sie eine Verbindung zur gewünschten Protokolldatenbank herstellen und die Standardeinstellungen für die Detailansicht von Untersuchungsberichten festlegen.

Die Änderungen, die an dieser Seite vorgenommen werden, wirken sich auf die Berichte aus. Andere Administratoren oder auch Benutzer, die sich zum Erstellen eigener Berichte anmelden, können diese Werte für ihre eigenen Aktivitäten ändern.

1. Wählen Sie die Protokolldatenbank aus, mit der die Untersuchungsberichte erstellt werden sollen.
   - Aktivieren Sie die Option **Katalogdatenbank anzeigen**, um eine Verbindung zur Protokolldatenbank herzustellen, mit der Log Server die Protokollierung vornimmt. Fahren Sie mit Schritt 2 fort.
   - So greifen Sie auf die Protokolldatenbank zu
     a. Deaktivieren Sie die Option **Katalogdatenbank anzeigen**.
     b. Geben Sie die folgenden Informationen ein, um die gewünschte Protokolldatenbank zu identifizieren. (Untersuchungsberichte können aus Datenbanken der Version 6.3x oder 7.0 generiert werden.)

Feld	Beschreibung
Server	Geben Sie den Computernamen oder die IP-Adresse des Geräts ein, auf dem die Protokolldatenbank installiert ist.
Datenbank	Geben Sie den Namen der Protokolldatenbank ein.

Feld	Beschreibung
Benutzer-ID	Geben Sie die Benutzer-ID für ein Konto ein, das über die Berechtigung zum Zugriff auf die Datenbank verfügt. Lassen Sie das Feld leer, wenn Log Server zur Nutzung einer vertrauenswürdigen Verbindung zum Zugriff auf die Protokolldatenbank installiert wurde. Wenn Sie sich nicht sicher sind, geben Sie **sa** ein. Das ist die Standard-Benutzer-ID für MSDE und die Standard-Administrator-ID für Microsoft SQL Server.
Passwort	Geben Sie das Passwort für die angegebene Benutzer-ID ein. Füllen Sie dieses Feld bei einer vertrauenswürdigen Verbindung nicht aus.

2. Wählen Sie die folgenden Standardeinstellungen für Detailberichte.

Feld	Beschreibung
Standarddatumsbereich für Untersuchungsberichte auswählen	Wählen Sie den Datumsbereich für die anfängliche Anzeige der Übersichtsberichte aus.
Standardformat für Detailberichte auswählen	Wählen Sie **Auswahl intelligenter Spalten** aus, um Detailberichte mit den festgelegten Standardspalten für die in den Berichten vorkommenden Informationen anzuzeigen. Wählen Sie **Auswahl angepasster Spalten** aus, um die genauen Spalten für die anfängliche Anzeige aller Detailberichte anzugeben. Verwenden Sie die Liste "Verfügbare Spalten", um Ihre Auswahl zu treffen. Benutzer können Sie angezeigten Spalten modifizieren, nachdem der Bericht erstellt wurde.

Feld	Beschreibung
Berichtstyp auswählen	Wählen Sie aus, welche Ansicht beim ersten Öffnen des Berichts angezeigt werden soll: • **Detailinformationen**: Jeder Eintrag wird in einer separaten Spalte angezeigt; die Uhrzeit kann angezeigt werden. • **Zusammenfassung**: Fasst alle Einträge mit einem gemeinsamen Element in einem Eintrag zusammen. Das spezifische Element kann je nach den im Bericht erfassten Informationen unterschiedlich sein. Normalerweise wird in der am weitesten rechts stehenden Spalte vor der Maßeinheit das zusammengefasste Element angezeigt. Die Uhrzeit kann nicht angezeigt werden.
Verfügbare Spalten / Aktueller Bericht	Wählen Sie einen Spaltennamen in der Liste "Verfügbare Spalten" aus, und klicken Sie auf den entsprechenden Pfeil, um diese Spalte in die Liste "Aktueller Bericht" zu verschieben. Es können bis zu sieben Spalten in der Liste "Aktueller Bericht" übernommen werden. Nachdem in der Liste "Aktueller Bericht" alle Spalten für die anfänglichen Detailberichte enthalten sind, legen Sie die Reihenfolge der Spalten fest. Wählen Sie einen Eintrag aus der Liste aus, und verändern Sie seine Position mithilfe der Nach-oben- bzw. Nach-unten-Pfeilschaltflächen.

3. Klicken Sie auf **Optionen speichern**, um alle Änderungen sofort zu speichern.

Anzeige- und Ausgabeoptionen

Verwandte Themen:

- *Konfigurieren von Untersuchungsberichten*, Seite 354
- *Standardeinstellungen für Datenbankverbindung und Berichte*, Seite 355
- *Ausgabe in Datei*, Seite 150

Sie können die Anzeige von bestimmten Berichtauswahlen und Berichtergebnissen in Übersichtsberichten und Untersuchungsberichten über mehrere Ebenen anpassen sowie die Standard-Seitengröße für Berichte festlegen, die im PDF-Format ausgegeben werden.

Diese Konfigurationsoptionen für Untersuchungsberichte sind in der Datei **wse.ini** festgelegt. Der Standardspeicherort ist:

```
C:\Programme\Websense\webroot\Explorer\wse.ini
```

In der folgenden Tabelle werden die Parameter aufgeführt, die sich auf die Anzeige und Ausgabe von Untersuchungsberichten auswirken. Es wird außerdem erklärt, was dadurch gesteuert wird und welches der Standardwert ist. (Verändern Sie KEINE anderen Einstellungen in der Datei "wse.ini".

Parameter	Beschreibung
maxUsersMenu	Die Anzahl der Benutzer in der Datenbank muss unter diesem Wert liegen (standardmäßig 5.000), damit "Benutzer" als Berichtsoption in der Liste "Internetnutzung nach" aufgeführt wird.
maxGroupsMenu	Die Anzahl der Gruppen in der Datenbank muss unter diesem Wert liegen (standardmäßig 3.000), damit "Gruppe" als Berichtsoption in der Liste "Internetnutzung nach" aufgeführt wird. **Hinweis:** Es müssen mindestens zwei Gruppen vorhanden sein, damit "Gruppe" in der Liste "Internetnutzung nach" aufgeführt wird. Es müssen ebenfalls zwei Domänen vorhanden sein, damit "Domäne" in der Liste "Internetnutzung nach" aufgeführt wird. Es gibt keine Obergrenze für die Anzahl der Domänen.
maxUsersDrilldown	Diese Option arbeitet zusammen mit dem warnTooManyHits-Parameter, um zu überprüfen, wann die Option "Benutzer" rot angezeigt wird. Wenn die Buchstaben rot angezeigt werden, bedeutet das, dass die Auswahl von "Benutzer" einen sehr umfangreichen Bericht erzeugt, dessen Erstellung viel Zeit in Anspruch nimmt. Wenn die Anzahl der Benutzer diesen Wert übersteigt (standardmäßig liegt er bei 5.000) und es mehr Hits als den warnTooManyHits-Wert gibt, wird die Option "Benutzer" in verschiedenen Dropdownlisten und Wertelisten rot angezeigt. Wenn die Anzahl der Benutzer über diesem Wert liegt, es jedoch weniger Hits als im warnTooManyHits-Werts gibt, wird die Option "Benutzer" in normaler Farbe angezeigt. Der resultierende Bericht hat einen angemesseneren Umfang.
maxGroupsDrilldown	Die Option "Gruppe" wird bei hohem Detaillierungsgrad rot angezeigt, wenn die im geplanten Bericht enthaltene Anzahl der Gruppen diese Zahl überschreitet (standardmäßig 2.000). Wenn die Buchstaben rot angezeigt werden, bedeutet dass, dass die Auswahl von "Gruppe" einen sehr umfangreichen Bericht erzeugt, dessen Erstellung viel Zeit in Anspruch nimmt.

Parameter	Beschreibung
warnTooManyHits	Diese Option arbeitet zusammen mit dem maxUsersDrilldown-Parameter, um zu überprüfen, wann die Option "Benutzer" rot angezeigt wird. Wenn die Anzahl der Benutzer den maxUsersDrilldown-Wert überschreitet, jedoch weniger Hits als dieser Wert bestehen (standardmäßig 10.000), wird die Option "Benutzer" *nicht* rot angezeigt. Wenn die Anzahl der Benutzer den maxUsersDrilldown-Wert überschreitet, und mehr Hits als dieser Wert bestehen, wird die Option "Benutzer" rot angezeigt. Wenn die Buchstaben rot angezeigt werden, bedeutet das, dass die Auswahl von "Benutzer" einen sehr umfangreichen Bericht erzeugt, dessen Erstellung viel Zeit in Anspruch nimmt.
hitsPerPage	Hier wird die maximale Elementanzahl (standardmäßig 100) festgelegt, die pro Seite angezeigt werden. (Dies hat keinerlei Auswirkungen auf gedruckte Berichte.)
maxOutputBufferSize	Hier wird die maximale Datenmenge (in Byte) angegeben, die auf der Hauptseite der Untersuchungsberichte angezeigt werden können. Wenn die angeforderten Daten diesen Grenzwert überschreiten (standardmäßig 4.000.000 oder 4 Millionen Byte), wird am Ende des Berichts die Meldung angezeigt, dass einige Ergebnisse nicht angezeigt werden. Höhere Werte ermöglichen es, größere Datenmengen in einem Bericht anzuzeigen, falls dies zu einem Problem wird. Wenn jedoch Speicherfehler auftreten, sollten Sie diesen Wert herabsetzen.
sendMulti	In der Standardeinstellung ist diese Option deaktiviert (0). Legen Sie den Wert auf 1 (aktiviert) fest, um sehr umfangreiche, geplante Detailberichte in mehrere Dateien mit jeweils 10.000 Zeilen zu teilen. Die Dateien, aus denen ein Bericht besteht, werden gepackt und an die E-Mail-Empfänger gesendet. Die Berichtsdateien können mit allen gängigen Dateikomprimierungs-Dienstprogrammen extrahiert werden.
maxSlices	Dies bezeichnet die maximale Anzahl der verschiedenen Teile in einem Kreisdiagramm einschließlich dem Teil "Andere", in dem alle Werte zusammengefasst sind, die keinen eigenen Teil bilden.

Parameter	Beschreibung
timelineCompressionThreshold	Diese Option wird nur für "Detailinformationen zu Benutzeraktivitäten nach Tag" oder "Detailinformationen zu Benutzeraktivitäten nach Monat" verwendet, wenn die Option "Ähnliche Hits in Gruppen zusammenfassen" oder "Alle Hits anzeigen" verfügbar ist. Im Bericht werden alle Hits mit derselben Kategorie ausgeblendet, die innerhalb der hier angegebenen Anzahl an Sekunden auftreten (der Standardwert ist 10).
PageSize	Die Ergebnisse von Untersuchungsberichten können im PDF-Format (Portable Document Format) ausgegeben und so problemlos verteilt und ausgedruckt werden. Die Seitengröße (die Standardeinstellung ist "Letter") kann folgende Formate aufweisen: • A4 (8,27 x 11,69 Zoll) • Letter (8,5 x 11 Zoll)

Eigene Berichte erstellen

Verwandte Themen:

- *Konfigurieren von Vorgaben für die Berichterstellung*, Seite 326
- *Zugreifen auf eigene Berichte*, Seite 151
- *Untersuchungsberichte*, Seite 123

Sie können die Funktion zum Erstellen eigener Berichte aktivieren, um Benutzern zu ermöglichen, Untersuchungsberichte zu Ihrer persönlichen Internetaktivität zu erstellen. Dadurch können sie feststellen, welche Informationen über sie gesammelt und überwacht werden. Dies entspricht den Regularien der Regierungen in vielen Ländern. Zusätzlich bewegt das Anzeigen der eigenen Aktivitäten viele Benutzer dazu, Ihre Internetgewohnheiten zu ändern, um so die Internetrichtlinie ihrer Organisation zu erfüllen.

Hinweis

Das Erstellen eigener Berichte ist nur möglich, wenn Websense Manager und die Berichterstellungskomponenten auf einem Windows-Betriebssystem installiert sind. Weitere Informationen finden Sie im *Implementierungshandbuch*.

So lassen Sie das Erstellen eigener Berichte zu:

1. Navigieren Sie zu **Einstellungen > Allgemein > Verzeichnisdienste**, und konfigurieren Sie die Verzeichnisdienste für die Authentifizierung der Benutzer, die mit ihren Netzwerk-Anmeldeinformationen auf Websense Manager zugreifen. Dies kann bereits zu einem früheren Zeitpunkt geschehen sein, um die Filterung nach Benutzern und Gruppennamen zu ermöglichen. Siehe *Verzeichnisdienste*, Seite 67.

   Wenn Ihre Installation mehrere Policy Server umfasst, müssen sie sich bei jedem einzelnen anmelden und die Seite "Verzeichnisdienste" mit den Informationen für den entsprechenden Verzeichnisdienst konfigurieren.
2. Navigieren Sie zu **Einstellungen > Berichterstellung > Vorgaben**, und aktivieren Sie das Kontrollkästchen **Erstellung eigener Berichte zulassen**. Siehe *Konfigurieren von Vorgaben für die Berichterstellung*, Seite 326.

Achten Sie darauf, den Benutzern die erforderlichen Informationen zum Erstellen der Berichte zukommen zu lassen, nachdem Sie die Option aktiviert haben:

- Geben Sie die URL für den Zugriff auf die Oberfläche für das Erstellen eigener Berichte an. Erinnern Sie die Benutzer daran, dass sie die URL bei Ihren Favoriten speichern oder als Lesezeichen für zukünftige Zwecke ablegen können.

  Lesen Sie weiter, um ausführliche Informationen zur URL zu erhalten.
- Geben Sie an, welcher Policy Server bei der Anmeldung ausgewählt werden muss.

  In Netzwerken mit nur einem Policy Server ist dies nicht notwendig. Wenn es in Ihrem Netzwerk mehrere Policy Server gibt, geben Sie die IP-Adresse des Policy Servers an, der zur Kommunikation mit dem Verzeichnisdienst konfiguriert wurde, über den die Authentifizierung der Netzwerk-Anmeldeinformationen erfolgt. Dies ist auch der Policy Server, den Sie bei der Installation von Log Server angegeben haben.
- Geben Sie den Benutzernamen und das Passwort für die Anmeldung an.

  Benutzer, die eigene Berichte erstellen möchten, müssen Netzwerk-Benutzername und -Passwort bei der Anmeldung angeben.

Die **URL** für den Zugriff auf die Oberfläche für das Erstellen eigener Berichte lautet:

```
https://<ServerIP>:9443/mng/login/pages/
   selfReportingLogin.jsf
```

Verwenden Sie statt <ServerIP> die IP-Adresse des Computers, auf dem Websense Manager ausgeführt wird.

Administratoren und Benutzer können auch auf die Anmeldeseite für das Erstellen eigener Berichte zugreifen, indem sie die Anmeldeseite von Websense Manager öffnen und auf den Link zum Erstellen eigener Berichte klicken.

Wenn es in Ihrem Netzwerk **mehrere Policy Server** gibt, müssen Sie die Benutzer darüber informieren, welchen davon sie bei der Anmeldung zum Erstellen eigener Berichte auswählen müssen.

14 Netzwerkkonfiguration

Verwandte Themen:

- *Hardware-Konfiguration*, Seite 364
- *Konfigurieren von Network Agent*, Seite 365
- *Überprüfen der Konfiguration von Network Agent*, Seite 373

Wenn die Websense-Software im Standalone-Modus ausgeführt wird (in diesem Fall erfolgt keine Integration in ein Proxy- oder Firewall-Produkt), werden von Websense Network Agent folgende Aktionen ermöglicht:

- Filtern der Internetinhalte
- Netzwerkprotokollierung und Verwalten von Internetanwendungen
- Verwalten der Bandbreite
- Protokollierung der übertragenen Byte

In einer integrierten Websense-Softwareimplementierung können Benutzeranfragen über das Produkt eines Drittanbieters zur Filterung an die Websense-Software geleitet und gesperrte Seiten an den Client zurückgeleitet werden. In dieser Umgebung kann Network Agent dennoch zum Filtern von HTTP-Anfragen, für erweiterte Protokollierungsdetails oder für beides eingesetzt werden.

Network Agent überwacht ununterbrochen die gesamte Netzwerknutzung einschließlich der über das Netzwerk übertragenen Bytes. Der Agent leitet in zuvor festgelegten Abständen Nutzungszusammenfassungen an die Websense-Software. Jede Zusammenfassung enthält die Start- und Endzeit, die insgesamt verwendeten Byte und die pro Protokoll verwendeten Byte.

Standardmäßig übermittelt Network Agent auch Daten zur Bandbreitennutzung an Policy Server sowie Filterprotokolldaten an Filtering Service.

Network Agent ist normalerweise so konfiguriert, dass der gesamte Datenverkehr im Netzwerk angezeigt werden kann. Vom Agenten werden folgende Unterscheidungen getroffen:

- Anfragen, die von internen Computern an interne Computer gesendet werden (beispielsweise Hits auf einem Intranet-Server)

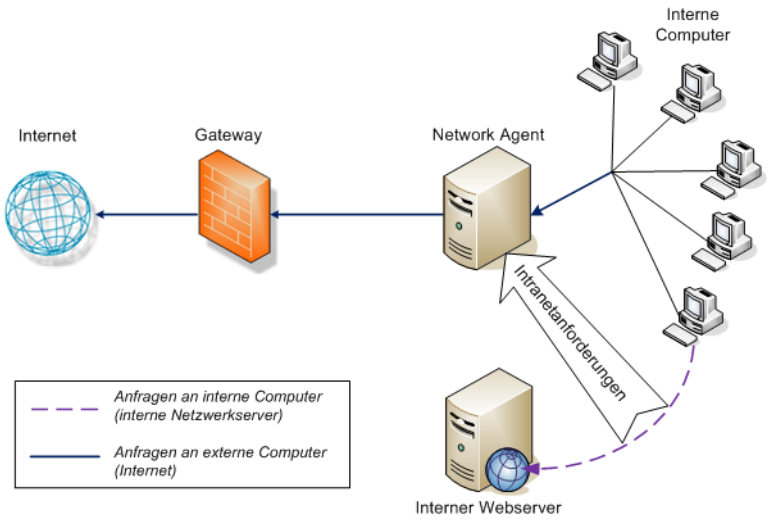
- Anfragen, die von internen Computern an externe Computer wie Webserver gesendet werden (beispielsweise Internetanfragen)

Der zuletzt genannte Aspekt hat bei der Überwachung der Internetnutzung durch Mitarbeiter die größte Bedeutung.

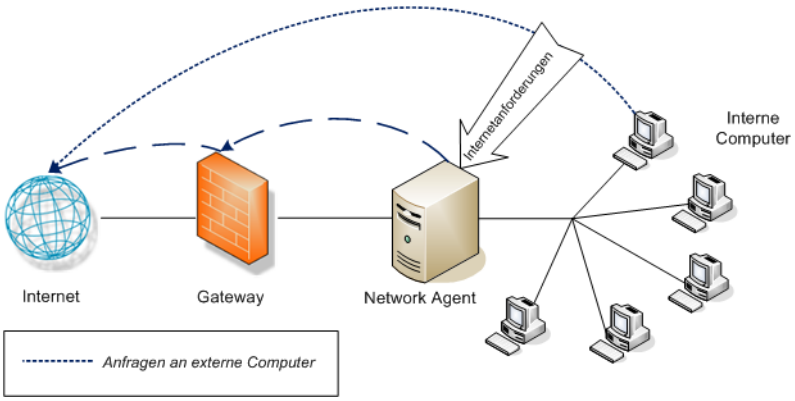
Hardware-Konfiguration

Jede Instanz von Network Agent überwacht den Datenverkehr **von** den Computern, die als dem Netzwerk zugehörig erkannt werden. Standardmäßig wird der Datenverkehr nur **zu** den internen Computern überwacht, die von Ihnen angegeben werden (beispielsweise interne Webserver).

Sie können festlegen, welche internen Computer (Netzwerksegmente) von den einzelnen Instanzen von Network Agent oder sogar von den einzelnen Netzwerkschnittstellenkarten (NICs) auf einem Computer mit Network Agent überwacht werden.



Überwachung von Anfragen an interne Computer



Überwachung von Anfragen an externe Computer

Für jede Instanz von Network Agent müssen folgende Voraussetzungen erfüllt sein:

- Sie muss über eine geeignete Position im Netzwerk verfügen, um den Datenverkehr zu und von allen überwachten Computern ermitteln zu können.
- Sie muss über mindestens eine NIC verfügen, die den Datenverkehr überwacht.

Network Agent kann auf einem Computer mit mehreren NICs installiert werden. Es können mehrere NICs für Überwachungsanfragen und das Senden gesperrter Seiten verwendet werden. Wenn Sie dem Computer mit Network Agent eine neue NIC hinzufügen, starten Sie den Network Agent-Dienst neu, und konfigurieren Sie danach die neue NIC (siehe *Konfigurieren der Einstellungen für die Netzwerkschnittstellenkarte (NIC)*, Seite 369).

> **Hinweis**
> Mit dem Dienstprogramm Network Traffic Detector können Sie ermitteln, ob Network Agent Datenverkehr in einem Netzwerksegment erkennen kann. Siehe *Überprüfen der Konfiguration von Network Agent*, Seite 373.

Weitere Informationen zur Platzierung von Network Agent und den NIC-Anforderungen finden Sie im *Implementierungshandbuch*.

Informationen zum Konfigurieren von Network Agent für die Überwachung interner Netzwerkressourcen, die Verwendung bestimmter NICs und die Durchführung der erweiterten Protokollierung finden Sie unter *Konfigurieren von Network Agent*, Seite 365.

Konfigurieren von Network Agent

Verwandte Themen:

- *Hardware-Konfiguration*, Seite 364
- *Konfigurieren globaler Einstellungen*, Seite 366
- *Konfigurieren lokaler Einstellungen*, Seite 367
- *Konfigurieren der Einstellungen für die Netzwerkschnittstellenkarte (NIC)*, Seite 369
- *Hinzufügen oder Bearbeiten von IP-Adressen*, Seite 372

Nach der Installation von Network Agent können Sie mit Websense Manager das Verhalten der Netzwerküberwachung konfigurieren. Die Einstellungen von Network Agent können in zwei Hauptbereiche geteilt werden:

- **Global** wirkt sich auf alle Instanzen von Network Agent aus. Mit diesen Einstellungen können Sie folgende Aktionen ausführen:
  - Identifizieren der Computer in Ihrem Netzwerk

- Auflisten der Computer im Netzwerk, die Network Agent für **eingehende** Anfragen überwachen soll (beispielsweise interne Webserver)
- Festlegen der Berechnung für die Bandbreite und das Verhalten bei der Protokollierung von Protokollen

- **Lokale Einstellungen** werden nur für die ausgewählte Instanz von Network Agent übernommen. Mit diesen Einstellungen können Sie folgende Aktionen ausführen:
  - Identifizieren der Instanz von Filtering Service, die einem einzelnen Network Agent zugeordnet ist
  - Ermitteln der Proxys und Caches der Computer, die dieser Network Agent überwacht
  - Konfigurieren der Art und Weise, wie die einzelnen Netzwerkkarten (NICs) auf dem Computer mit Network Agent verwendet werden (zum Überwachen von Anfragen, Senden von gesperrten Seiten oder beidem)

    Durch die Einstellungen der Netzwerkkarten wird zudem bestimmt, welches Netzwerksegment eine Instanz von Network Agent überwacht.

Konfigurieren globaler Einstellungen

Verwandte Themen:

- *Hardware-Konfiguration*, Seite 364
- *Konfigurieren lokaler Einstellungen*, Seite 367
- *Konfigurieren der Einstellungen für die Netzwerkschnittstellenkarte (NIC)*, Seite 369
- *Hinzufügen oder Bearbeiten von IP-Adressen*, Seite 372

Auf der Seite **Einstellungen > Network Agent > Global** können Sie das grundlegende Überwachungs- und Protokollierungsverhalten aller Instanzen von Network Agent definieren.

Auf der Liste **Interne Netzwerkdefinition** werden die Computer identifiziert, die zum Netzwerk gehören. Standardmäßig überwacht Network Agent den zwischen diesen Computern gesendeten Datenverkehr (interne Netzwerkkommunikation) nicht.

In den Standardeinstellungen sind verschiedene anfängliche Einträge enthalten. Sie können zusätzliche Einträge hinzufügen oder die bestehenden Einträge bearbeiten oder löschen.

Auf der Liste **Zu überwachender interner Datenverkehr** werden alle Computer aufgeführt, die unter "Interne Netzwerkdefinition" aufgelistet werden und deren Datenverkehr Network Agent **überwachen soll**. Dazu gehören beispielsweise auch interne Webserver, mit denen Sie interne Verbindungen verfolgen können.

Alle Anfragen, die von einem beliebigen Ort im Netzwerk an die angegebenen internen Computer gesendet werden, werden überwacht. Diese Liste ist standardmäßig leer.

- Klicken Sie auf **Hinzufügen**, um eine IP-Adresse oder einen Bereich der entsprechenden Liste hinzuzufügen. Weitere Informationen dazu finden Sie unter *Hinzufügen oder Bearbeiten von IP-Adressen*, Seite 372.
- Klicken Sie zum Bearbeiten eines Eintrags in einer Liste auf die IP-Adresse oder den Bereich. Weitere Informationen dazu finden Sie unter *Hinzufügen oder Bearbeiten von IP-Adressen*, Seite 372.
- Um einen Eintrag aus der Liste zu entfernen, wählen Sie das Kontrollkästchen neben der URL, die IP-Adresse oder den Bereich aus, und klicken Sie auf **Löschen**.

Mit den Optionen unter **Zusätzliche Einstellungen** können Sie bestimmen, wie oft Network Agent die Nutzung der Bandbreite berechnet und ob bzw. wie häufig Datenverkehr auf bestimmten Protokollen protokolliert wird.

Feld	Vorgehensweise
Intervall für die Berechnung der Bandbreite	Geben Sie eine Zahl zwischen 1 und 300 ein, um festzulegen, in welchen Abständen (in Sekunden) Network Agent die Nutzung der Bandbreite berechnen soll. Der Eintrag "300" gibt beispielsweise an, dass Network Agent die Bandbreite alle fünf Minuten berechnet. Der Standardwert beträgt 10 Sekunden.
Datenverkehr auf bestimmten Protokollen periodisch protokollieren	Wählen Sie diese Option, um das Feld "Protokollierungsintervall" zu aktivieren.
Protokollierungsintervall	Geben Sie eine Zahl zwischen 1 und 300 ein, um festzulegen, in welchen Abständen (in Minuten) Network Agent Protokolle protokolliert. Der Eintrag "60" gibt beispielsweise an, dass Network Agent jeweils nach Ablauf einer Stunde in die Protokolldatei schreibt. Der Standardwert beträgt 1 Minute.

Wenn Sie alle Änderungen vorgenommen haben, klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Konfigurieren lokaler Einstellungen

Verwandte Themen:

- *Hardware-Konfiguration*, Seite 364
- *Konfigurieren globaler Einstellungen*, Seite 366
- *Konfigurieren der Einstellungen für die Netzwerkschnittstellenkarte (NIC)*, Seite 369

Auf der Seite **Einstellungen > Network Agent > Lokale Einstellungen** können sie Filterverhalten, Proxyinformationen und weitere Einstellungen für die ausgewählte Instanz von Network Agent festlegen. Die IP-Adresse der ausgewählten Instanz von Network Agent wird in der Titelleiste des Inhaltsfensters angezeigt und im linken Navigationsfenster markiert.

Mit den Einstellungen **Filtering-Service-Definition** können Sie festlegen, welcher Filtering Service der ausgewählten Instanz von Network Agent zugewiesen ist und wie auf Internetanfragen reagiert werden soll, wenn Filtering Service nicht verfügbar ist.

Feld	Vorgehensweise
IP-Adresse von Filtering Service	Wählen Sie eine Instanz von Filtering Service, die einem einzelnen Network Agent zugeordnet ist
Maßnahme, wenn Filtering Service nicht verfügbar ist	Wählen Sie **Zulassen** aus, um alle Anfragen zuzulassen, oder **Sperren**, um alle Anfragen zu sperren, bis Filtering Service wieder verfügbar ist. Der Standardwert ist "Zulassen".

Geben Sie auf der Liste **Proxy- und Cacheserver** alle Proxy- oder Cacheserver an, die mit Network Agent kommunizieren, um sicherzustellen, dass alle Benutzeranfragen ordnungsgemäß überwacht, gefiltert und protokolliert werden.

- Klicken Sie auf **Hinzufügen**, um eine IP-Adresse oder einen Bereich zur Liste hinzuzufügen. Weitere Informationen dazu finden Sie unter *Hinzufügen oder Bearbeiten von IP-Adressen*, Seite 372.
- Klicken Sie zum Bearbeiten eines Eintrags in einer Liste auf die IP-Adresse oder den Bereich.
- Um einen Eintrag aus der Liste zu entfernen, wählen Sie das Kontrollkästchen neben der URL, die IP-Adresse oder den Bereich aus, und klicken Sie auf **Löschen**.

Auf der Liste **Netzwerkschnittstellenkarten** können Sie einzelne NICs konfigurieren. Klicken Sie auf eine Netzwerkschnittstellenkarte in der Spalte **Name**. Weitere Anweisungen finden Sie unter *Konfigurieren der Einstellungen für die Netzwerkschnittstellenkarte (NIC)*, Seite 369.

Falls HTTP-Anfragen in Ihrem Netzwerk durch einen nicht standardmäßigen Port geleitet werden, klicken Sie auf **Erweiterte Einstellungen für Network Agent**, um die richtigen Ports für die Überwachung durch Network Agent anzugeben. Standardmäßig sind für **Für HTTP-Datenverkehr verwendete Ports** die Ports **8080, 80** ausgewählt.

Weitere Einstellungen in diesem Abschnitt sollten nur dann geändert werden, wenn dies auf Anweisung der Mitarbeiter der technischen Unterstüzung von Websense erfolgt.

Feld	Beschreibung
Modus	• Keine (Standardeinstellung) • Allgemein • Fehler • Detailliert • Bandbreite
Ausgabe	• Datei (Standardeinstellung) • Fensteranzeige
Port	55870 (Standardeinstellung)

Wenn Sie alle Änderungen an den Einstellungen von Network Agent vorgenommen haben, klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Konfigurieren der Einstellungen für die Netzwerkschnittstellenkarte (NIC)

Verwandte Themen:

- *Hardware-Konfiguration*, Seite 364
- *Konfigurieren von Network Agent*, Seite 365
- *Konfigurieren der Überwachungseinstellungen einer Netzwerkschnittstellenkarte*, Seite 371
- *Hinzufügen oder Bearbeiten von IP-Adressen*, Seite 372

Auf der Seite **Network Agent > Lokale Einstellungen > Konfiguration von Netzwerkschnittstellenkarte (NIC)** können Sie festlegen, wie Network Agent mit den verfügbaren Netzwerkschnittstellenkarten (NICs) die Netzwerkauslastung überwacht und verwaltet.

Im Bereich **Informationen zu Netzwerkschnittstellenkarten (NICs)** ist der Kontext der von Ihnen vorgenommenen Änderungen angegeben, und es werden die **IP-Adresse**, eine kurze **Beschreibung** der Netzwerkschnittstellenkarte sowie der **Name** der Karte angegeben. Mithilfe dieser Informationen können Sie sicherstellen, dass Sie die richtige Netzwerkschnittstellenkarte konfigurieren.

Überwachung

In einer Konfiguration mit mehreren Netzwerkschnittstellenkarten können Sie festlegen, dass mit einer NIC der Datenverkehr im Netzwerk überwacht und mit einer anderen NIC Seiten gesperrt werden. Mindestens eine Netzwerkschnittstellenkarte muss zur Überwachung verwendet werden, der Datenverkehr kann von mehreren Netzwerkschnittstellenkarten überwacht werden.

Im Bereich **Überwachung** können Sie angeben, ob **Diese Netzwerkschnittstellenkarte (NIC) für die Überwachung des Datenverkehrs verwenden** aktiv sein soll.

- Wenn diese Netzwerkschnittstellenkarte nicht für die Überwachung verwendet wird, deaktivieren Sie das Kontrollkästchen, und fahren Sie mit dem nächsten Abschnitt fort.
- Wenn diese Netzwerkschnittstellenkarte für die Überwachung verwendet wird, aktivieren Sie das Kontrollkästchen, und klicken Sie dann auf **Konfigurieren**. Sie werden zur Seite für die Konfiguration des Überwachungsverhaltens weitergeleitet. Anleitungen hierzu finden Sie unter *Konfigurieren der Überwachungseinstellungen einer Netzwerkschnittstellenkarte*, Seite 371.

Weitere Optionen zur Netzwerkschnittstellenkarte

Zusätzlich zum Konfigurieren der Überwachungsoptionen haben Sie die Möglichkeit, weitere Verhalten der Netzwerkschnittstellenkarten zu bestimmen:

1. Stellen Sie unter "Sperre" sicher, dass die entsprechenden Netzwerkschnittstellenkarten im Feld **NIC zum Sperren** aufgeführt werden. Wenn Sie mehrere Netzwerkschnittstellenkarten konfigurieren, sollte für jede NIC in diesem Feld derselbe Wert angegeben sein. Das heißt, es wird nur eine NIC zum Sperren verwendet.
2. Wenn die Websense-Software im Modus **Standalone** ausgeführt wird, ist **HTTP-Anforderungen filtern und protokollieren** ausgewählt. Diese Einstellung kann nicht geändert werden.
3. Wenn die Websense-Software in das Gerät oder die Anwendung eines Drittanbieters integriert ist, können Sie unter den Optionen **Integrationen** angeben, wie HTTP-Anfragen gefiltert und protokolliert werden sollen. Optionen, die nicht auf Ihre Umgebung zutreffen, sind deaktiviert.
   - Wählen Sie **HTTP-Anforderungen protokollieren** aus, um die Genauigkeit in Websense-Berichten zu verbessern.
   - Wählen Sie **Filter all requests not sent over HTTP ports** aus, um nur die HTTP-Anfragen über Network Agent zu filtern, die nicht über das Integrationsprodukt gesendet wurden.
4. Geben Sie unter "Protokollmanagement" an, ob Nicht-HTTP-Protokolle von Network Agent mithilfe dieser Netzwerkschnittstellenkarte gefiltert werden sollen.
   - Aktivieren Sie die Option **Anforderungen für Nicht-HTTP-Internetprotokolle filtern**, um die Funktion für das Protkollmanagement zu aktivieren. Diese Funktion ermöglicht es, Internetanwendungen und

Datenübertragungsmethoden wie Sofortnachrichten, Streaming Media, gemeinsame Nutzung von Dateien, Datentransfer usw. mithilfe der Websense-Software zu filtern. Weitere Informationen finden Sie unter *Filtern von Kategorien und Protokollen*, Seite 40, und *Arbeiten mit Protokollen*, Seite 196.

- Aktivieren Sie die Option **Nutzung der Bandbreite nach Protokoll ermitteln**, um die Bandwidth Optimizer-Funktion zu aktivieren. Network Agent verwendet diese Netzwerkschnittstellenkarte, um die Auslastung der Netzwerkbandbreite nach Protokoll bzw. Anwendung nachzuverfolgen. Weitere Informationen dazu finden Sie unter *Bandbreite mit Bandwidth Optimizer verwalten*, Seite 203.

Konfigurieren der Überwachungseinstellungen einer Netzwerkschnittstellenkarte

Auf der Seite **Lokale Einstellungen > Konfiguration von Netzwerkschnittstellenkarte (NIC) > Überwachungsliste** können Sie angeben, welche Computer von Network Agent über die ausgewählte Netzwerkschnittstellenkarte (NIC) überwacht werden.

1. Geben Sie unter "Überwachungsliste" an, welche Anforderungen von Network Agent überwacht werden:
   - **Alle**: Network Agent überwacht die Anfragen aller Computer, die mithilfe der ausgewählten Netzwerkschnittstellenkarte erkannt werden. Normalerweise umfasst dies alle Computer des Netzwerksegments, in dem sich der aktuelle Computer mit Network Agent oder der Netzwerkschnittstellenkarte befindet.
   - **Keine**: Network Agent überwacht keine Anfragen.
   - **Bestimmte**: Network Agent überwacht nur die Netzwerksegmente, die in der Überwachungsliste aufgeführt sind.
2. Wenn Sie "Bestimmte" ausgewählt haben, klicken Sie auf **Hinzufügen**, und geben Sie dann die IP-Adressen der Computer an, die von Network Agent überwacht werden sollen. Weitere Informationen dazu finden Sie unter *Hinzufügen oder Bearbeiten von IP-Adressen*, Seite 372.

   Hinweis

   Es können keine IP-Adressbereiche eingegeben werden, die sich überschneiden. Wenn eine Überschneidung von Bereichen stattfindet, ist die Berechnung der Netzwerkbandbreite möglicherweise nicht korrekt, und es kann zu Fehlern bei der Anwendung der bandbreitenbasierten Filterung kommen.

   Aktivieren Sie das entsprechende Element in der Liste, um eine IP-Adresse oder einen Netzwerkbereich aus der Liste zu entfernen. Klicken Sie anschließend auf **Löschen**.
3. Geben Sie unter "Ausnahmen der Überwachungsliste" alle internen Computer an, die nicht durch Network Agent überwacht werden sollen.

Beispielsweise kann Network Agent alle Anfragen von CPM Server ignorieren. Auf diese Weise werden die Websense-Protokolldaten und andere Statusmonitorausgaben nicht mit Anfragen von CPM Server gefüllt.

a. Klicken Sie auf **Hinzufügen**, um einen Computer zu identifizieren, und geben Sie die zugehörige IP-Adresse ein.

b. Wiederholen Sie den Vorgang, um weitere Computer zu identifizieren.

4. Klicken Sie auf **OK**, um Ihre Änderungen im Cache zwischenzuspeichern und zur Seite "Konfiguration von Netzwerkschnittstellenkarte (NIC)" zurückzukehren. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Hinzufügen oder Bearbeiten von IP-Adressen

Verwandte Themen:

- *Konfigurieren globaler Einstellungen*, Seite 366
- *Konfigurieren lokaler Einstellungen*, Seite 367
- *Konfigurieren der Einstellungen für die Netzwerkschnittstellenkarte (NIC)*, Seite 369

Auf der Seite **IP-Adressen hinzufügen** oder **IP-Adressen bearbeiten** können Sie Änderungen an allen folgenden Network Agent-Listen vornehmen: Interne Netzwerkdefinition, Zu überwachender interner Datenverkehr, Proxy- und Cacheserver, Überwachungsliste oder Ausnahmen der Überwachungsliste.

- Wenn Sie einen IP-Adressbereich hinzufügen oder bearbeiten, stellen Sie sicher, dass der Bereich sich nicht mit einem bestehenden Eintrag (einzelne IP-Adresse oder Adressbereich) in der Liste überschneidet.
- Wenn Sie einen IP-Adressbereich hinzufügen oder bearbeiten, stellen Sie sicher, dass der Bereich sich nicht mit einem bestehenden Eintrag (einzelne IP-Adresse oder Adressbereich) in der Liste überschneidet.

So fügen Sie eine neue IP-Adresse oder einen IP-Adressbereich hinzu:

1. Wählen Sie das Optionsfeld **IP-Adresse** oder **IP-Adressbereich**.
2. Geben Sie eine gültige IP-Adresse oder einen gültigen IP-Adressbereich ein.
3. Klicken Sie auf **OK**, um auf die vorige Seite für "Erweiterte Einstellungen für Network Agent" zurückzukehren. Die neue IP-Adresse bzw. der IP-Adressbereich wird in der entsprechenden Tabelle angezeigt.

   Wenn Sie zur vorherigen Seite zurückkehren möchten, ohne Ihre Änderungen im Cache zwischenzuspeichern, klicken Sie auf **Abbrechen**.
4. Wiederholen Sie diesen Vorgang gegebenenfalls für zusätzliche IP-Adressen.

Wenn Sie eine bestehende IP-Adresse oder einen IP-Adressbereich bearbeiten, wird auf der Seite "IP-Adressen bearbeiten" das ausgewählte Element angezeigt. Das richtige Optionsfeld ist bereits ausgewählt. Nehmen Sie alle notwendigen Änderungen vor, und klicken Sie dann auf **OK**, um zur vorhergehenden Seite zurückzukehren.

Wenn Sie alle IP-Adressen hinzugefügt oder bearbeitet haben, klicken Sie auf der Seite "Einstellungen für Network Agent" auf **OK**. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** klicken.

Überprüfen der Konfiguration von Network Agent

Nachdem Network Agent in Websense Manager konfiguriert wurde, können Sie mit dem Detektor für Netzwerkdatenverkehr sicherstellen, dass die Computer in Ihrem Netzwerk von der Websense-Software erkannt werden können.

1. Navigieren Sie zum Starten des Tools zu **Start > Alle Programme > Websense > Dienstprogramme > Detektor für Netzwerkdatenverkehr**.
2. Wählen Sie aus der Dropdownliste **Netzwerkadapter** eine Netzwerkkarte aus.
3. Überprüfen Sie die Adressen, die in der Liste **Überwachte Netzwerkbereiche** angezeigt werden. Überprüfen Sie, ob alle entsprechenden Subnetze aufgeführt werden.
4. Verwenden Sie die Schaltflächen **Subnetz hinzufügen** und **Subnetz entfernen**, um festzulegen, welche Teile des Netzwerks getestet werden sollen.
5. Klicken Sie auf **Überwachung starten**.

   Der Detektor für Netzwerkdatenverkehr erkennt Computer im Netzwerk, indem er die Informationen überwacht, die diese über das Netzwerk senden. In der Liste **Anzahl der gefundenen Computer** wird die aktuelle Anzahl der gefundenen Computer angezeigt.
6. Um spezifische Informationen über die vom Tool gefundenen Computer anzuzeigen, wählen Sie ein Subnetz in der Liste "Überwachte Netzwerkbereiche". Klicken Sie dann auf **Gefundene Computer anzeigen**.

   Wenn ein bestimmter Computer nicht aufgeführt wird, überprüfen Sie, ob dieser Computer Netzwerkdatenverkehr verursacht. Gehen Sie hierzu zum entsprechenden Computer, starten Sie einen Internetbrowser, und rufen Sie eine Website auf. Kehren Sie anschließend zum Detektor für Netzwerkdatenverkehr zurück, und überprüfen Sie, ob der Computer im Dialogfeld **Gefundene Computer** angezeigt wird.
7. Wenn Sie die Sichtbarkeit des Netzwerkdatenverkehrs getestet haben, klicken Sie auf **Überwachung stoppen**.

Gehen Sie wie folgt vor, wenn einige Computer nicht erkannt werden:

- Überprüfen Sie die Anforderungen für die Netzwerkkonfiguration und die NIC-Platzierung (siehe *Hardware-Konfiguration*, Seite 364).
- Überprüfen Sie die ausführlicheren Informationen zur Netzwerkkonfiguration im *Installationshandbuch* Ihrer Websense-Software.
- Überprüfen Sie, ob die Überwachung der Netzwerkschnittstellenkarte ordnungsgemäß konfiguriert ist (*Konfigurieren der Einstellungen für die Netzwerkschnittstellenkarte (NIC)*, Seite 369).

15 Fehlerbehebung

Suchen Sie in diesem Abschnitt nach Lösungen für häufig auftretende Probleme, bevor Sie sich an die technische Unterstützung wenden.

Auf der Websense-Website unter www.websense.com/global/en/SupportAndKB/ finden Sie eine umfangreiche Wissensbasis (Knowledge Base). Sie können durch die Eingabe von Schlüsselworten oder Referenznummern nach Themen suchen oder die am häufigsten aufgerufenen Artikel durchsuchen.

Die Anleitungen zur Fehlerbehebung sind in den folgenden Abschnitten zusammengefasst:

Probleme mit der Installation und der Subskription

Die Ansicht für den Websense-Zustand zeigt ein Problem mit der Subskription an

Zum Herunterladen der Websense Master Database und zum Ausführen von Filtervorgängen für das Internet ist ein gültiger Subskriptionsschlüssel erforderlich. Wenn Ihr Subskriptionsschlüssel abgelaufen oder ungültig ist und die Master Database seit mehr als 2 Wochen nicht heruntergeladen wurde, wird in der Ansicht für den Websense-Zustand eine Warnmeldung angezeigt.

- Stellen Sie sicher, dass Sie Ihren Subskriptionsschlüssel korrekt eingegeben haben. Die Eingabe des Schlüssels muss unter Beachtung der Groß-/Kleinschreibung erfolgen.
- Stellen Sie sicher, dass Ihre Subskription nicht abgelaufen ist. Siehe *Subskriptionsschlüssel*, Seite 379.
- Stellen Sie sicher, dass die Master Database innerhalb der letzten 2 Wochen erfolgreich heruntergeladen wurde. Sie können den Download-Status in Websense Manager abfragen: Klicken Sie auf der Seite "Status > Heute" auf **Datenbank-Download**.

  Weitere Informationen zur Fehlerbehebung bei Problemen mit dem Herunterladen der Datenbank finden Sie unter *Die Master Database kann nicht heruntergeladen werden*, Seite 378.

Wenn Sie den Schlüssel korrekt eingegeben haben und dennoch ein Statusfehler ausgegeben wird oder wenn Ihre Subskription abgelaufen ist, wenden Sie sich an Websense, Inc. oder Ihren autorisierten Händler vor Ort.

Wenn Ihre Subskription abläuft, legen die Einstellungen in Websense Manager entweder fest, dass alle Benutzer ungefilterten Zugriff auf das Internet haben oder dass alle Internetanfragen blockiert werden. Weitere Informationen finden Sie unter *Ihre Subskription*, Seite 28.

Nach einem Upgrade fehlen Benutzer in Websense Manager

Wenn Sie Active Directory nach einem Upgrade der Websense-Software als Ihren Verzeichnisdienst festgelegt haben, werden Benutzernamen möglicherweise nicht in Websense Manager angezeigt. Dieser Fall tritt ein, wenn Benutzernamen Zeichen enthalten, die nicht Bestandteil des UTF-8-Zeichensatzes sind.

Damit Unterstützung für LDAP 3.0 geboten werden kann, ändert das Websense-Installationsprogramm den Zeichensatz während des Upgrades von MBCS in UTF-8. Dies führt dazu, dass Benutzernamen, die nicht im UTF-8-Satz enthaltene Zeichen aufweisen, nicht korrekt erkannt werden.

Um dieses Problem zu beheben, ändern Sie den Zeichensatz manuell in MBCS:

1. Wechseln Sie in Websense Manager zu **Einstellungen** > **Verzeichnisdienste**.
2. Stellen Sie sicher, dass unter dem Eintrag "Verzeichnisse" im oberen Bereich der Seite die Option **Active Directory (Native Mode)** ausgewählt ist.
3. Klicken Sie auf **Erweiterte Verzeichniseinstellungen**.

4. Klicken Sie unter dem Eintrag "Zeichensatz" auf **MBCS**. Möglicherweise müssen Sie auf der Seite nach unten scrollen, damit diese Option angezeigt wird.
5. Klicken Sie auf **OK**, um die Änderung im Cache zu speichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** geklickt haben.

Probleme mit der Master Database

Die Datenbank für erste Filteraktivitäten wird verwendet

Die Websense Master Database enthält die Kategorie- und die Protokolldefinitionen, die die Grundlage für das Filtern von Internetinhalten liefern.

Eine Teilversion der Master Database wird mit Ihrer Websense-Software auf jedem Computer installiert, auf dem Filtering Service ausgeführt wird. Diese Teildatenbank dient zur Aktivierung grundlegender Filterfunktionen ab dem Zeitpunkt, zu dem Sie Ihren Subskriptionsschlüssel eingeben.

Sie müssen die Vollversion der Datenbank herunterladen, damit die Filteraktivitäten uneingeschränkt ausgeführt werden können. Weitere Informationen finden Sie unter *Die Websense Master Database*, Seite 32.

Das Herunterladen der gesamten Datenbank kann einige Minuten, eventuell auch mehr als 60 Minuten in Anspruch nehmen, abhängig von Faktoren wie Geschwindigkeit der Internetverbindung, Bandbreite und verfügbarem Festplatten- und RAM-Speicher.

Die Master Database ist älter als eine Woche

Die Websense Master Database enthält die Kategorie- und die Protokolldefinitionen, die die Grundlage für das Filtern von Internetinhalten liefern. Die Websense-Software lädt Änderungen an der Master Database gemäß dem in Websense Manager festgelegten Zeitplan herunter. Standardmäßig wird der Download einmal täglich ausgeführt.

So leiten Sie einen Datenbank-Download manuell ein:

1. Wechseln Sie in Websense Manage zur Seite **Status > Heute** und klicken Sie auf **Datenbank-Download**.

2. Klicken Sie neben der gewünschten Instanz von Filtering Service auf **Aktualisieren**, um den Datenbank-Download einzuleiten, oder klicken Sie auf **Alles aktualisieren**, um mit dem Herunterladen auf alle Filtering Service-Computer zu beginnen.

   Hinweis
   Nachdem Sie die Aktualisierungen der Master Database heruntergeladen haben, kann die CPU-Auslastung während des Ladens der Datenbank in den lokalen Speicher kurzzeitig mehr als 90 % betragen. Es wird empfohlen, den Download nicht während Zeiten mit Spitzenauslastung durchzuführen.

3. Klicken Sie auf **Schließen**, um mit Ihrer Arbeit fortzufahren, während die Datenbank heruntergeladen wird.

   Um den Download-Status anzuzeigen, können Sie jederzeit auf die Schaltfläche **Datenbank-Download** klicken.

Wenn eine neue Version der Master Database Kategorien oder Protokolle hinzufügt oder entfernt, können Administratoren, die kategorie- und protokollbezogene Aufgaben im Rahmen der Richtlinienverwaltung durchführen (wie einen Kategoriesatz bearbeiten) möglicherweise während des Herunterladens Fehlermeldungen erhalten. Auch wenn solche Aktualisierungen nicht häufig vorkommen, sollten Sie nach Möglichkeit keine Änderungen an kategorie- und protokollbezogenen Daten vornehmen, während eine Datenbank aktualisiert wird.

Die Master Database kann nicht heruntergeladen werden

Wenn Sie die Websense Master Database nicht erfolgreich herunterladen können, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass Sie Ihren Subskriptionsschlüssel korrekt in Websense Manager eingegeben haben und dass der Schlüssel nicht abgelaufen ist (*Subskriptionsschlüssel*, Seite 379).
- Stellen Sie sicher, dass der Filtering Service-Computer auf das Internet zugreifen kann (*Internetzugang*, Seite 379).
- Prüfen Sie die Firewall- oder Proxy-Server-Einstellungen, um sicherzustellen, dass Filtering Service eine Verbindung mit dem Websense-Download-Server herstellen kann (*Überprüfen der Firewall- oder Proxy-Server-Einstellungen*, Seite 380).
- Stellen Sie sicher, dass auf dem Download-Computer ausreichend Festplattenspeicher (*Unzureichender Festplattenspeicher*, Seite 381) und RAM-Speicher (*Unzureichender RAM-Speicher*, Seite 382) verfügbar ist.
- Suchen Sie im Netzwerk nach Anwendungen wie Antivirensoftware, die möglicherweise das Herstellen einer Verbindung für das Herunterladen verhindern (*Einschränkende Anwendungen*, Seite 383).

Subskriptionsschlüssel

So stellen Sie sicher, dass der Schlüssel für die Subskription korrekt eingegeben wurde und nicht abgelaufen ist:

1. Wechseln Sie in Websense Manager zu **Einstellungen > Konto**.
2. Vergleichen Sie den Schlüssel, den Sie von Websense, Inc. oder Ihrem Händler vor Ort erhalten haben, mit dem Wert im Feld **Subskriptionsschlüssel**. Bei der Schlüsseleingabe muss die Groß-/Kleinschreibung der Schreibweise in Ihrem Schlüsseldokument entsprechen.
3. Überprüfen Sie das Datum neben **Ablaufdatum des Schlüssels**. Wenn das Datum bereits verstrichen ist, setzen Sie sich mit Ihrem Händler oder mit Websense Inc. in Verbindung, um Ihre Subskription zu erneuern.
4. Wenn Sie im Dialogfeld "Einstellungen" Änderungen am Schlüssel vorgenommen haben, klicken Sie auf **OK**, um den Schlüssel und den Datenbank-Download zu aktivieren.

Um einen Datenbank-Download manuell einzuleiten oder den Status des letzten Datenbank-Downloads zu überprüfen, klicken Sie in der Symbolleiste im oberen Bereich der Seite "Status" > "Heute" auf **Datenbank-Download**.

Internetzugang

Zum Herunterladen der Master Database, sendet der Filtering Service-Computer den Befehl **HTTP post** an die Download-Server unter den folgenden URLs:

download.websense.com
ddsdom.websense.com
ddsint.websense.com
portal.websense.com
my.websense.com

So stellen Sie sicher, dass Filtering Service über den für die Kommunikation mit dem Download-Server erforderlichen Internetzugang verfügt:

1. Öffnen Sie auf dem Computer, auf dem Filtering Service ausgeführt wird, einen Browser.
2. Geben Sie die folgende URL ein:

   http://download.websense.com/

   Wenn das Gerät eine HTTP-Verbindung mit der Website herstellen kann, wird eine Umleitungsseite aufgerufen. Anschließend zeigt der Browser die Websense-Homepage an.

   Sollte dies nicht der Fall sein, stellen Sie Folgendes sicher:

   - Der Computer kann über Port 80 oder den in Ihrem Netzwerk für den HTTP-Datenaustausch festgelegten Port kommunizieren.
   - Der Computer ist für das korrekte Durchführen von DNS-Suchvorgängen konfiguriert.

- Der Computer ist für die Verwendung erforderlicher Proxy-Server konfiguriert (siehe *Überprüfen der Firewall- oder Proxy-Server-Einstellungen*, Seite 380).

Stellen Sie außerdem sicher, dass Ihr Gateway keine Regeln enthält, die eine HTTP-Datenübertragung vom Filtering Service-Computer blockieren.

3. Verwenden Sie eine der folgenden Methoden, um zu überprüfen, ob der Computer mit der Download-Website kommunizieren kann:
   - Geben Sie in der Befehlszeile den folgenden Befehl ein:

     ```
     ping download.websense.com
     ```

     Überprüfen Sie, ob beim Pingtest eine Antwort vom Download-Server empfangen wird.
   - Verwenden Sie Telnet, um eine Verbindung zu **download.websense.com 80** herzustellen. Wenn ein Cursor angezeigt wird und kein Fehler ausgegeben wird, können Sie eine Verbindung zum Download-Server herstellen.

Überprüfen der Firewall- oder Proxy-Server-Einstellungen

Wenn die Master Database unter Verwendung einer Firewall oder eines Proxy-Servers heruntergeladen wird, für die bzw. den eine Authentifizierung erforderlich ist, stellen Sie sicher, dass ein Browser auf dem Filtering Service-Computer die Webseiten ordnungsgemäß laden kann. Wenn sich die Seiten normal öffnen lassen, die Master Database jedoch nicht heruntergeladen werden kann, überprüfen Sie die Proxy-Server-Einstellungen im Webbrowser.

Microsoft Internet Explorer:

1. Wählen Sie **Extras > Internetoptionen**.
2. Öffnen Sie die Registerkarte **Verbindungen**.
3. Klicken Sie auf **LAN-Einstellungen**. Die Proxy-Server-Konfiguration wird unter **Proxyserver** angezeigt.

   Notieren Sie sich die Proxy-Einstellungen.

Mozilla Firefox:

1. Wählen Sie **Extras > Einstellungen > Erweitert**.
2. Wählen Sie die Registerkarte **Netzwerk**.
3. Klicken Sie auf **Einstellungen**. Im Dialogfeld "Verbindungs-Einstellungen" wird angezeigt, ob der Browser für die Verbindung mit einem Proxy-Server konfiguriert ist.

   Notieren Sie sich die Proxy-Einstellungen.

Stellen Sie anschließend sicher, dass die Websense-Software für die Verwendung desselben Proxy-Servers konfiguriert ist, damit der Download durchgeführt werden kann.

1. Wechseln Sie in Websense Manager zu **Einstellungen > Datenbank-Download**.

2. Stellen Sie sicher, dass die Option **Proxy-Server oder Firewall verwenden** aktiviert ist und der korrekte Server und Port aufgelistet sind.
3. Vergewissern Sie sich, dass die Einstellungen unter **Authentifizierung** korrekt sind. Überprüfen Sie Benutzernamen und Passwort hinsichtlich Rechtschreibung und Groß-/Kleinschreibung.

   Wenn die Websense-Software Authentifizierungsinformationen bereitstellen muss, ist es erforderlich, dass die Firewall oder der Proxy-Server so konfiguriert sind, dass Klartext- und Basisauthentifizierung akzeptiert werden. Weitere Information zur Aktivierung der Basisauthentifizierung finden Sie in der Websense Knowledge Base.

Wenn eine Firewall zu dem Zeitpunkt, zu dem die Websense-Software in der Regel die Datenbank herunterlädt, den Zugriff auf das Internet einschränkt oder die Größe einer Datei begrenzt, die über HTTP übertragen werden kann, kann Websense die Datenbank nicht herunterladen. Um festzustellen, ob die Firewall die Ursache für das Problem ist, suchen Sie in den Firewall-Einstellungen nach einer Regel, die möglicherweise den Download blockiert. Ändern Sie außerdem ggf. die Download-Zeiten in Websense Manager (*Konfigurieren von Datenbank-Downloads*, Seite 34).

Unzureichender Festplattenspeicher

Die Websense Master Database ist im Verzeichnis **bin** von Websense gespeichert (standardmäßig /opt/Websense/bin oder C:\Programme\Websense\bin). Das Laufwerk, auf dem sich das Verzeichnis befindet, muss ausreichend Speicherplatz für das Herunterladen der komprimierten Datenbank sowie ausreichend Kapazitäten zum Dekomprimieren der Datenbank aufweisen.

Der freie Festplattenspeicher des Geräts sollte mindestens doppelt so groß sein wie die Master Database. Da die Einträge in der Master Database immer mehr werden, nimmt auch der für ein erfolgreiches Herunterladen erforderliche Speicherplatz zu. Websense, Inc. empfiehlt in der Regel mindestens 3 GB freien Festplattenspeicher auf dem Laufwerk, auf das der Download erfolgt.

Verwenden Sie in Windows den Windows Explorer, um den verfügbaren Festplattenspeicher zu ermitteln.

1. Wechseln Sie in Windows Explorer (nicht in Internet Explorer) zu **Arbeitsplatz**.
2. Wählen Sie das Laufwerk aus, auf dem die Websense-Software installiert ist. Standardmäßig befindet sich die Websense-Software auf Laufwerk C.
3. Klicken Sie mit der rechtem Maustaste im Popup-Menü auf **Eigenschaften**.
4. Überprüfen Sie auf der Registerkarte "Allgemein", ob mindestens 3 GB Festplattenspeicher verfügbar sind. Wenn das Laufwerk nicht ausreichend freien Speicherplatz aufweist, löschen Sie nicht benötigte Dateien, um mehr freien Speicher zu erhalten.

Verwenden Sie bei Linux-Systemen den Befehl **df**, um die Menge an freiem Speicherplatz in dem Dateisystem zu überprüfen, in dem die Websense-Software installiert ist:

1. Öffnen Sie eine Terminal-Sitzung.

2. Geben Sie in der Befehlszeile Folgendes ein:

   ```
   df -h /opt
   ```

   Die Websense-Software ist in der Regel im Verzeichnis /opt/Websense/bin installiert. Wenn sie an einem anderen Ort installiert ist, verwenden Sie den entsprechenden Pfad.

3. Stellen Sie sicher, dass mindestens 3 GB Speicherplatz verfügbar sind. Wenn das Laufwerk nicht ausreichend freien Speicherplatz aufweist, löschen Sie nicht benötigte Dateien, um mehr freien Speicher zu erhalten.

Wenn Sie sichergestellt haben, dass ausreichend Speicherplatz verfügbar ist, Sie jedoch weiterhin Probleme mit dem Herunterladen haben, beenden Sie alle Websense-Dienste (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302), löschen Sie die Dateien **Websense.xfr** und **Websense** (keine Erweiterung), starten Sie die Dienste und laden Sie eine neue Datenbank manuell herunter.

Unzureichender RAM-Speicher

Der erforderliche RAM-Speicher zum Ausführen der Websense-Software und Herunterladen der Master Database variiert je nach Größe des Netzwerks. Beispielsweise werden in einem kleinen Netzwerk 2 GB RAM für alle Plattformen empfohlen.

Systemempfehlungen finden Sie im *Implementierungshandbuch*.

So überprüfen Sie den RAM-Speicher in einem Windows-System:

1. Öffnen Sie den Task-Manager.
2. Wählen Sie die Registerkarte **Systemleistung**.
3. Überprüfen Sie den verfügbaren **Physikalischen Speicher**.
4. Wenn weniger als 2 GB installiert sind, führen Sie ein Upgrade für den RAM-Speicher des Computers aus.

Sie können auch Informationen unter **Systemsteuerung > Verwaltung > Leistung** abrufen.

So überprüfen Sie den RAM-Speicher in einem Linux-System:

1. Öffnen Sie eine Terminal-Sitzung.
2. Geben Sie in der Befehlszeile Folgendes ein:

   ```
   top
   ```

3. Ermitteln Sie den verfügbaren RAM-Speicher, indem Sie Folgendes hinzufügen: **Mem: av** und **Swap: av**.
4. Wenn weniger als 2 GB installiert sind, führen Sie ein Upgrade für den RAM-Speicher des Computers aus.

Einschränkende Anwendungen

Einige einschränkende Anwendungen wie Virenscanner, Anwendungen zur Größenbegrenzung oder IDSs (Intrusion Detection Systems) können das Herunterladen von Datenbanken behindern. Idealerweise sollte die Websense-Software so konfiguriert sein, dass sie direkt zum letzten Gateway springt, sodass keine Verbindung mit diesen Anwendungen hergestellt wird. Alternative:

1. Deaktivieren Sie die Einschränkungen in Bezug auf den Filtering Service-Computer und das Download-Verzeichnis der Master Database.

   Anleitungen zum Ändern der Konfiguration des Computers finden Sie in der Anwendungs- oder Softwaredokumentation.
2. Versuchen Sie, die Master Database herunterzuladen.

Wenn diese Änderung das Problem nicht beseitigt, konfigurieren Sie die Anwendung neu, sodass der Filtering Service-Computer einbezogen wird.

Der Download der Master Database findet nicht zum richtigen Zeitpunkt statt

Möglicherweise sind Systemdatum und -uhrzeit auf dem Filtering Service-Computer nicht korrekt eingestellt. Die Websense-Software verwendet die Systemuhr, um den richtigen Zeitpunkt für das Herunterladen der Master Database zu ermitteln.

Wenn überhaupt kein Download durchgeführt wird, beachten Sie die Hinweise unter *Die Master Database kann nicht heruntergeladen werden*, Seite 378.

Kontaktaufnahme mit der technischen Unterstützung bei Problemen mit dem Datenbank-Download

Wenn Sie weiterhin Probleme mit dem Herunterladen der Master Database haben, nachdem Sie die Schritte in diesem Abschnitt der Hilfe ausgeführt haben, senden Sie die folgenden Informationen an die technische Unterstützung von Websense:

1. Den exakten Text der Fehlermeldung, der im Dialogfeld für den Datenbank-Download angezeigt wird
2. Die externen IP-Adressen der Computer, die versuchen, die Datenbank herunterzuladen
3. Ihren Subskriptionsschlüssel für Websense
4. Das Datum und die Uhrzeit des letzten Download-Versuchs
5. Ggf. die Menge der übertragenen Bytes
6. Öffnen Sie eine Befehlszeile und geben Sie **nslookup** für **download.websense.com** ein. Wenn eine Verbindung zum Download-Server hergestellt wird, senden Sie die zurückgegebene IP-Adresse an die technische Unterstützung

7. Öffnen Sie eine Befehlszeile und geben Sie **tracert** für **download.websense.com** ein. Wenn eine Verbindung zum Download-Server hergestellt wird, senden Sie die Routenverfolgung an die technische Unterstützung
8. Eine Paketverfolgung oder Paketerfassung, die während eines Download-Versuchs für den Websense-Download-Server ausgeführt wurde
9. Eine Paketverfolgung oder Paketerfassung, die während desselben Download-Versuchs für das Netzwerk-Gateway ausgeführt wurde
10. Die folgenden Dateien aus dem Websense-Verzeichnis **bin**: **websense.ini**, **eimserver.ini** und **config.xml**.

Wechseln Sie zu www.websense.com/SupportPortal/default.aspx, um die Kontaktinformationen der technischen Unterstützung aufzurufen.

Probleme mit dem Filtern

Filtering Service wird nicht ausgeführt

Wenn Filtering Service nicht ausgeführt wird, können Internetanfragen nicht gefiltert und protokolliert werden.

Filtering Service kann in folgenden Fällen beendet werden:

- Wenn nicht ausreichend Festplattenspeicher auf dem Computer vorhanden ist, auf dem Filtering Service ausgeführt wird.
- Wenn das Herunterladen der Master Database aufgrund von unzureichendem Festplattenspeicher fehlschlägt (siehe *Die Master Database kann nicht heruntergeladen werden*, Seite 378).
- Wenn die Datei **websense.ini** fehlt oder beschädigt ist.
- Wenn Sie Filtering Service beenden (beispielsweise nach dem Erstellen benutzerdefinierter Sperrseiten) und das Programm nicht wieder starten.

Wenn Sie mehrere Websense-Dienste beendet und neu gestartet, bei dem Neustart jedoch nicht die richtige Reihenfolge eingehalten haben, kann es ebenfalls so wirken, als werde Filtering Service nicht mehr ausgeführt. Wenn Sie mehrere Dienste neu starten, starten Sie stets Policy Database, Policy Broker und Policy Server vor allen anderen Websense-Diensten.

So beheben Sie diese Probleme:

- Stellen Sie sicher, dass auf dem Filtering Service-Computer mindestens 3 GB an freiem Speicherplatz verfügbar sind. Möglicherweise ist es erforderlich, dass Sie nicht benötigte Dateien löschen, um mehr Speicherkapazität zu erhalten.
- Wechseln Sie zum Websense-Verzeichnis **bin** (standardmäßig C:\Programme\Websense\bin oder /opt/Websense/bin) und stellen Sie sicher, dass Sie **websense.ini** in einem Texteditor öffnen können. Wenn diese Datei beschädigt ist, ersetzen Sie sie durch eine Sicherungsdatei.
- Überprüfen Sie die Ereignisanzeige von Windows oder die Datei **websense.log** auf Fehlermeldungen von Filtering Service (siehe *Tools zur Fehlerbehebung*, Seite 422).
- Melden Sie sich bei Websense Manager ab, starten Sie Websense Policy Server neu und starten Sie anschließend Websense Filtering Service (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).

  Warten Sie eine Minute, bevor Sie sich erneut bei Websense Manager anmelden.

User Service ist nicht verfügbar

Wenn User Service nicht ausgeführt wird oder wenn Policy Server nicht mit User Service kommunizieren kann, kann die Websense-Software benutzerdefinierte Filterrichtlinien nicht richtig anwenden.

Möglicherweise kann es so wirken, als werde User Service nicht mehr ausgeführt, wenn Sie Policy Server erst nach dem Start anderer Websense-Dienste neu starten. So beheben Sie dieses Problem:

1. Starten Sie Websense Policy Server neu (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).
2. Starten Sie Websense User Service.
3. Schließen Sie Websense Manager.

   Warten Sie eine Minute, bevor Sie sich erneut bei Websense Manager anmelden.

Wenn der vorherige Schritt das Problem nicht behebt, gehen Sie folgendermaßen vor:

- Überprüfen Sie die Ereignisanzeige von Windows oder die Datei **websense.log** auf Fehlermeldungen von User Service (siehe *Tools zur Fehlerbehebung*, Seite 422).
- Wechseln Sie zum Websense-Verzeichnis **bin** (standardmäßig C:\Programme\Websense\bin oder /opt/websense/bin) und stellen Sie sicher, dass Sie **websense.ini** in einem Texteditor öffnen können. Wenn diese Datei beschädigt ist, ersetzen Sie sie durch eine Sicherungsdatei.

Websites werden fälschlich als Informationstechnologie kategorisiert

Internet Explorer 4.0 oder höher kann Suchvorgänge über die Adresszeile akzeptieren. Wenn diese Option aktiviert ist und ein Benutzer nur einen Domänennamen in die Adresszeile eingibt (beispielsweise **websense** anstelle von **http://www.websense.com**), interpretiert Internet Explorer die Eingabe als Suchanforderung, nicht als Anforderung zum Öffnen einer Website. Es werden die Sites angezeigt, nach denen der Benutzer vermutlich sucht, sowie eine Liste von Websites, die den Suchkriterien annähernd entsprechen.

Daher akzeptiert, blockiert oder begrenzt die Websense-Software die Anfrage basierend auf dem Status der Kategorien für Informationstechnologie/Suchmaschinen und Portale in den aktiven Richtlinien und nicht basierend auf der Kategorie der angeforderten Website. Wenn Sie möchten, dass die Websense-Software basierend auf der Kategorie der angeforderten Website filtert, müssen Sie die Adresszeilen-Suchfunktion deaktivieren:

1. Wählen Sie **Extras > Internetoptionen**.
2. Wechseln Sie zur Registerkarte **Erweitert**.
3. Wählen Sie unter der Überschrift "Suchen in Adressleiste" den Eintrag **Nicht in Adressleiste suchen**.
4. Klicken Sie auf **OK**.

> **Hinweis**
> Diese Schritte gelten für die Versionen 5, 6 und 7 von Internet Explorer.

Schlüsselworte werden nicht blockiert

Es gibt 2 mögliche Ursachen für dieses Problem: **Sperrfunktion für Schlüsselworte deaktivieren** ist ausgewählt oder die Website, deren URL das Schlüsselwort enthält, verwendet den Befehl **post**, um Daten an Ihren Webserver zu senden.

So stellen Sie sicher, dass die Sperrfunktion für Schlüsselworte aktiviert ist:

1. Wechseln Sie in Websense Manager zu **Einstellungen > Filterung**.
2. Überprüfen Sie unter "Allgemeine Filterfunktionen" die Liste **Optionen für die Schlüsselwortsuche**. Wenn **Sperrfunktion für Schlüsselworte deaktivieren** angezeigt wird, wählen Sie eine andere Option in der Liste. Weitere Informationen zu den verfügbaren Optionen finden Sie unter *Konfigurieren von Websense-Filtereinstellungen*, Seite 60.
3. Klicken Sie auf **OK**, um die Änderung im Cache zu speichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** geklickt haben.

Wenn eine Website den Befehl **post** verwendet, um Daten an Ihren Webserver zu senden, erkennt die Websense-Software die Filtereinstellungen für Schlüsselworte für diese URL nicht. Sofern Ihr Integrationsprodukt keine Daten erkennt, die über "post"

gesendet werden, können Benutzer auf URLs mit blockierten Schlüsselworte zugreifen.

Wenn Sie feststellen möchten, ob eine bestimmte Website den Befehl "post" verwendet, rufen Sie in Ihrem Browser die Quelle der Website auf. Wenn der Quellcode eine Zeichenfolge wie **<method=post>** aufweist, wird der Befehl "post" zum Laden dieser Site verwendet.

Benutzerdefinierte URLs oder URLs für Filter für die Zugriffsbeschränkung werden nicht wie gewünscht gefiltert

Wenn eine HTTPS-URL in einer Liste der Filter für die Zugriffsbeschränkung oder einer benutzerdefinierten URL-Liste (neu kategorisiert oder ungefiltert) nicht wie gewünscht gefiltert wird, wandelt möglicherweise ein Integrationsprodukt die URL in ein Format um, das Filtering Service nicht erkennt.

Nicht Proxy-basierte Integrationsprodukte wandeln URLs aus dem Domänenformat in das IP-Format um. Beispielsweise wird die URL **https://<Domäne>** als **https://<IP-Adresse>:443** gelesen. In diesem Fall kann Filtering Service die vom Integrationsprodukt empfangene URL nicht mit einer benutzerdefinierten URL oder einem Filter für die Zugriffsbeschränkung abgleichen und die Website nicht entsprechend filtern.

Um dieses Problem zu umgehen, fügen Sie sowohl die IP-Adressen als auch die URLs der Sites hinzu, die Sie mithilfe von benutzerdefinierten URLs oder Filtern für die Zugriffsbeschränkung filtern möchten.

Ein Benutzer kann nicht wie gewünscht auf ein Protokoll oder eine Anwendung zugreifen

Wenn Ihr Netzwerk Microsoft ISA Server umfasst, können bestimmte Konfigurationen für die Authentifizierungsmethode zu Unterbrechungen der Verbindung mit Benachrichtigungsanwendungen führen.

Wenn eine andere als die anonyme Authentifizierung aktiviert ist, versucht der Proxy-Server, die Datenpakete zu identifizieren, die empfangen werden, wenn Benutzer Anwendungsverbindungen anfordern. Der Proxy-Server kann das Datenpaket nicht identifizieren und die Verbindung wird unterbrochen. Dadurch kann die Protokollfilterung von Websense beeinträchtigt werden.

Der Zugriff auf ein Protokoll oder eine Internetanwendung kann auch dann gestört werden, wenn der von der Anwendung verwendete Port blockiert ist. Dieser Fall kann in folgenden Situationen auftreten:

- Der Port wird von einer Firewall blockiert.
- Ein blockiertes benutzerdefiniertes Protokoll schließt den Port (als einzelnen Port oder als Teil einer Gruppe von Ports) in alle seine Identifikationsdaten ein.

Eine FTP-Anfrage wird nicht wie gewünscht blockiert

Bei einer Integration mit Check Point®-Firewalls erfordert die Websense-Software die **Aktivierung der Ordneransicht** im Browser des Clients, damit FTP-Anfragen erkannt und gefiltert werden können.

Wenn die Ordneransicht nicht aktiviert ist, werden FTP-Anfragen, die an den FireWall-1-Proxy gesendet wurden, mit dem Präfix "http://" an die Websense-Software weitergeleitet. Aus diesem Grund filtert die Websense-Software diese Anfragen als HTTP-Anfragen und nicht als FTP-Anfragen.

Die Websense-Software wendet keine Benutzer- oder Gruppenrichtlinien an

Wenn die Websense-Software Computer- oder Netzwerkrichtlinien oder die Richtlinie **Standard** anwendet, auch nachdem Benutzer- oder Gruppenrichtlinien zugewiesen wurden, siehe *Probleme mit der Benutzeridentifikation*, Seite 391. Weitere Informationen erhalten Sie über die Knowledge Base.

Remote-Benutzer werden nicht unter Verwendung der korrekten Richtlinie gefiltert

Wenn ein Remote-Benutzer auf das Netzwerk zugreift, indem er sich anmeldet oder im Cache gespeicherte Anmeldedaten für eine Domäne verwendet (Anmeldeinformationen für das Netzwerk), wendet die Websense-Software die diesem Benutzer oder seiner Gruppe oder Domäne zugewiesene Richtlinie an, sofern erforderlich. Wenn dem Benutzer, der Gruppe oder der Domäne keine Richtlinie zugewiesen ist oder wenn sich der Benutzer über ein lokales Benutzerkonto auf dem Computer anmeldet, wendet die Websense-Software die Richtlinie "Standard" an.

Gelegentlich wird ein Benutzer nicht unter Verwendung einer Benutzer- oder Gruppenrichtlinie oder der Richtlinie "Standard" gefiltert. Dieser Fall tritt ein, wenn der Benutzer sich über ein lokales Benutzerkonto auf dem Remote-Computer anmeldet und sich der letzte Teil der MAC-Adresse (Media Access Control) des Remote-Computers mit einer im Netzwerk vorhandenen IP-Adresse überschneidet, der eine Richtlinie zugewiesen wurde. In diesem Fall wird die der IP-Adresse zugewiesene Richtlinie auf den Remote-Benutzer angewendet.

Probleme mit Network Agent

Network Agent ist nicht installiert

Für die Protokollfilterung ist Network Agent erforderlich. In Verbindung mit manchen Integrationen liefert Network Agent außerdem eine genauere Protokollierung.

Wenn Sie ein Integrationsprodukt verwenden und die Protokollfilterung oder Protokollierung durch Network Agent nicht benötigen, können Sie die Statusmeldung "Es ist kein Network Agent installiert" ausblenden. Anweisungen dazu finden Sie unter *Überprüfen des aktuellen Systemstatus*, Seite 311.

Bei Standalone-Installationen muss Network Agent zum Überwachen und Filtern des Netzwerkdatenverkehrs installiert sein. Anleitungen zur Installation finden Sie im *Installationshandbuch* und unter *Konfigurieren von Network Agent*, Seite 365.

Network Agent wird nicht ausgeführt

Für die Protokollfilterung ist Network Agent erforderlich. In Verbindung mit manchen Integrationen liefert Network Agent außerdem eine genauere Protokollierung.

Bei Standalone-Installationen muss Network Agent zum Überwachen und Filtern des Netzwerkdatenverkehrs ausgeführt werden.

So beheben Sie dieses Problem:

1. Überprüfen Sie das Dialogfeld für die Windows-Dienste (siehe *Das Dialogfeld für die Windows-Dienste*, Seite 422), um festzustellen, ob der Dienst **Websense Network Agent** gestartet wurde.
2. Starten Sie die Dienste **Websense Policy Broker** und **Websense Policy Server** neu (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).
3. Starten Sie den Dienst **Websense Network Agent**.
4. Schließen Sie Websense Manager.
5. Warten Sie eine Minute, bevor Sie sich erneut bei Websense Manager anmelden.

Falls das Problem weiterhin besteht, gehen Sie folgendermaßen vor:

- Überprüfen Sie die **Ereignisanzeige von Windows** auf Fehlermeldungen von Network Agent (siehe *Die Ereignisanzeige von Windows*, Seite 423).
- Überprüfen Sie die Datei **Websense.log** auf Fehlermeldungen von Network Agent (siehe *Die Websense-Protokolldatei*, Seite 423).

Network Agent überwacht keine Netzwerkschnittstellenkarten (NICs)

Network Agent muss zur Überwachung des Netzwerkdatenverkehrs mit mindestens einer Netzwerkschnittstellenkarte (NIC) verknüpft sein.

Wenn Sie dem Network Agent-Computer Netzwerkkarten hinzufügen oder sie entfernen, müssen Sie Ihre Network Agent-Konfiguration aktualisieren.

1. Wechseln Sie in Websense Manager zu **Einstellungen**.

2. Wählen Sie im linken Navigationsfenster unter dem Eintrag "Network Agent" die IP-Adresse des Network Agent-Computers aus.
3. Überprüfen Sie, ob alle NICs für das ausgewählte Gerät aufgelistet sind.
4. Stellen Sie sicher, dass mindestens eine NIC zur Überwachung des Netzwerkdatenverkehrs eingestellt ist.

Weitere Informationen finden Sie unter *Konfigurieren von Network Agent*, Seite 365.

Network Agent kann nicht mit Filtering Service kommunizieren

Network Agent muss mit Filtering Service kommunizieren können, um die Richtlinien zur Internetnutzung umsetzen zu können.

- Haben Sie die IP-Adresse des Filtering Service-Computers geändert oder Filtering Service neu installiert?

  Beachten Sie in diesem Fall die Informationen unter *Aktualisieren der Filtering Service-IP-Adresse und UID-Informationen*, Seite 390.

- Befinden sich mehr als 2 Netzwerkschnittstellenkarten (NICs) auf dem Network Agent-Computer?

  Beachten Sie in diesem Fall die Informationen unter *Netzwerkkonfiguration*, Seite 363, um Ihre Einstellungen für die Websense-Software zu überprüfen.

- Haben Sie den mit Network Agent verbundenen Switch neu konfiguriert?

  Beachten Sie in diesem Fall die Informationen im *Installationshandbuch*, um Ihr Hardware-Setup zu überprüfen, sowie die Informationen unter *Konfigurieren von Network Agent*, Seite 365, um Ihre Websense-Einstellungen zu kontrollieren.

Wenn keine der oben genannten Angaben zutrifft, siehe *Konfigurieren lokaler Einstellungen*, Seite 367. Hier finden Sie Informationen zur Verknüpfung von Network Agent und Filtering Service.

Aktualisieren der Filtering Service-IP-Adresse und UID-Informationen

Wenn Filtering Service deinstalliert oder neu installiert wurde, wird der interne Identifikator (UID) für Filtering Service nicht automatisch von Network Agent aktualisiert. Websense Manager versucht, mithilfe des alten UID, der nicht mehr vorhanden ist, Anfragen an Filtering Service zu senden.

Ebenso wird bei einer Änderung der IP-Adresse des Filtering Service-Computers diese Änderung nicht automatisch registriert.

So stellen Sie die Verbindung zu Filtering Service wieder her:

1. Öffnen Sie Websense Manager.

   Eine Statusmeldung gibt an, dass eine Instanz von Network Agent keine Verbindung mit Filtering Service herstellen kann.
2. Klicken Sie oben im linken Navigationsfenster auf **Einstellungen**.
3. Wählen Sie im linken Navigationsfenster unter dem Eintrag "Network Agent" die IP-Adresse des Network Agent-Computers aus.

4. Erweitern Sie oben auf der Seite unter "Filtering-Service-Definition" die Liste **IP-Adresse des Servers** und wählen Sie anschließend die IP-Adresse des Filtering Service-Computers aus.
5. Klicken Sie unten auf der Seite auf **OK**, um die Aktualisierung im Cache zu speichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** geklickt haben.

Probleme mit der Benutzeridentifikation

Verwandte Themen:

- *Probleme mit dem Filtern*, Seite 384
- *Remote-Benutzer werden nicht zur manuellen Authentifizierung aufgefordert*, Seite 401
- *Remote-Benutzer werden nicht richtig gefiltert*, Seite 402

Wenn die Websense-Software Computer- oder Netzwerkrichtlinien oder die Richtlinie **Standard** verwendet, um Internetanfragen zu filtern, selbst nachdem Sie benutzer- oder gruppenbasierte Richtlinien zugewiesen haben, oder wenn die falsche benutzer- oder gruppenbasierte Richtlinie angewendet wird, können Sie das Problem mithilfe der folgenden Schritte bestimmen:

- Wenn Sie Microsoft ISA Server verwenden und die Authentifizierungsmethode hierfür geändert haben, stellen Sie sicher, dass der Web-Proxy-Dienst neu gestartet wurde.
- Wenn Sie verschachtelte Gruppen in Windows Active Directory verwenden, werden Richtlinien, die einer übergeordneten Gruppen zugewiesen sind, auf Benutzer angewendet, die nicht direkt der übergeordneten Gruppen, sondern einer Untergruppe angehören. Weitere Informationen zu Benutzer- und Gruppenhierarchien finden Sie in der Dokumentation für den Verzeichnisdienst.
- Der Cache von User Service ist möglicherweise veraltet. User Service speichert die Zuweisungen zwischen Benutzername und IP-Adresse drei Stunden lang im Cache. Sie können den Cache von User Service dazu bringen, die Daten zu aktualisieren, indem Sie sämtliche Änderungen in Websense Manager im Cache speichern und anschließend auf **Alles speichern** klicken.
- Wenn der Benutzer, der nicht korrekt gefiltert wird, sich auf einem Gerät angemeldet hat, auf dem Windows XP SP2 ausgeführt wird, könnte das Problem auf die Windows Internet Connection Firewall (ICF) zurückzuführen sein, die standardmäßig in Windows XP SP2 enthalten und aktiviert ist. Weitere Informationen zur Windows ICF finden Sie in Artikel Nummer 320855 in der Microsoft Knowledge Base.

So können DC Agent und Logon Agent Anmeldeinformationen von Benutzern von einem Computer abrufen, auf dem Windows XP SP2 ausgeführt wird:

1. Wählen Sie im Windows-Menü **Start** des Client-Computers **Einstellungen** > **Systemsteuerung** > **Sicherheitscenter** > **Windows-Firewall**.
2. Wechseln Sie zur Registerkarte **Ausnahmen**.
3. Aktivieren Sie die Option **Datei- und Druckerfreigabe**.
4. Klicken Sie auf **OK**, um das Dialogfeld der ICF zu schließen. Schließen Sie anschließend alle anderen geöffneten Fenster.

Wenn Sie einen Agenten für transparente Identifikation von Websense verwenden, beachten Sie den entsprechenden Abschnitt für die Fehlerbehebung.

- *Fehlerbehebung für DC Agent*, Seite 392.
- *Fehlerbehebung für Logon Agent*, Seite 394.
- *Fehlerbehebung für eDirectory Agent*, Seite 397.
- *Fehlerbehebung für RADIUS Agent*, Seite 400.

Fehlerbehebung für DC Agent

So beheben Sie Probleme mit DC Agent hinsichtlich der Benutzeridentifikation:

1. Überprüfen Sie alle Netzwerkverbindungen.
2. Überprüfen Sie die Ereignisanzeige von Windows auf Fehlermeldungen (siehe *Die Ereignisanzeige von Windows*, Seite 423).
3. Überprüfen Sie die Websense-Protokolldatei (Websense.log) auf detaillierte Fehlermeldungen (siehe *Die Websense-Protokolldatei*, Seite 423).

Zu den häufigen Ursachen für DC-Agent-Probleme hinsichtlich der Benutzeridentifikation gehören folgende:

- Die Netzwerk- oder Windows-Dienste kommunizieren auf eine Weise mit dem Domänencontroller, die dazu führt, dass DC Agent den Dienst als neuen Benutzer erkennt, für den keine Richtlinie definiert wurde. Siehe *Benutzer werden von der Richtlinie "Standard" nicht korrekt gefiltert*, Seite 393.
- DC Agent oder User Service wurde möglicherweise als ein Dienst installiert, der das Gästekonto verwendet, für den Domänencontroller vergleichbar mit einem anonymen Benutzer. Wenn der Domänencontroller so eingestellt wurde, dass er keine Liste der Benutzer und Gruppen an einen anonymen Benutzer ausgibt, kann DC Agent die Liste nicht herunterladen. Siehe *Das manuelle Ändern von DC Agent- und User Service-Berechtigungen*, Seite 393.
- Der Cache von User Service ist veraltet. User Service speichert die Zuweisungen zwischen Benutzername und IP-Adresse standardmäßig drei Stunden lang im Cache. Der Cache wird jedes Mal, wenn Sie in Websense Manager Änderungen vornehmen und auf **Alles speichern** klicken, ebenfalls aktualisiert.

Benutzer werden von der Richtlinie "Standard" nicht korrekt gefiltert

Wenn ein Netzwerk oder Microsoft Windows 200x den Domänencontroller kontaktiert, kann der verwendete Kontoname dazu führen, dass die Websense-Software annimmt, dass ein nicht identifizierter Benutzer von einem gefilterten Computer aus auf das Internet zugreift. Da diesem Benutzer keine benutzergruppenbasierte Richtlinie zugewiesen wurde, wird die Computer- oder Netzwerkrichtlinie oder die Richtlinie "Standard" angewendet.

- Möglicherweise erfordern die Netzwerkdienste Domänenprivilegien, um auf Daten auf dem Netzwerk zugreifen zu können, und verwenden den Domänenbenutzernamen, unter dem sie ausgeführt werden, um den Domänencontroller zu kontaktieren.

  Informationen zur Behebung dieses Problems finden Sie unter *Einen Agenten für das Ignorieren bestimmter Benutzernamen konfigurieren*, Seite 249.

- Windows 200x-Dienste kontaktieren den Domänencontroller in regelmäßigen Abständen unter Verwendung eines Benutzernamens, der aus dem Computernamen gefolgt von einem Dollarzeichen besteht (Benutzer-computer$). DC Agent interpretiert den Dienst als neuen Benutzer, dem keine Richtlinie zugewiesen wurde.

  Um dieses Problem zu beheben, konfigurieren Sie DC Agent so, dass sämtliche Anmeldeinformationen mit dem Aufbau **computer$** ignoriert werden.

  1. Wechseln Sie auf dem DC Agent-Computer zum Websense-Verzeichnis **bin** (standardmäßig **C:\Program Files\Websense\bin**).
  2. Öffnen Sie die Datei **transid.ini** in einem Texteditor.
  3. Fügen Sie der Datei den folgenden Eintrag hinzu:

     ```
     IgnoreDollarSign=true
     ```

  4. Speichern und schließen Sie die Datei.
  5. Starten Sie DC Agent neu (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).

Das manuelle Ändern von DC Agent- und User Service-Berechtigungen

Auf dem Computer, auf dem der Domänencontroller ausgeführt wird:

1. Erstellen Sie ein Benutzerkonto, beispielsweise **Websense**. Sie können ein vorhandenes Konto verwenden, doch ein spezielles Websense-Konto ist besser geeignet, da hier das Passwort so eingestellt werden kann, dass es nicht abläuft. Es sind keine speziellen Berechtigungen erforderlich.

   Stellen Sie das Passwort so ein, dass es nie abläuft. Dieses Konto bietet nur einen Sicherheitskontext für den Zugriff auf Verzeichnisobjekte.

   Notieren Sie sich Benutzernamen und Passwort für dieses Konto, da diese Daten in den Schritten 6 und 7 eingegeben werden müssen.
2. Öffnen Sie auf jedem Websense DC Agent-Computer das Dialogfeld für die Windows-Dienste (unter **Start > Alle Programme > Verwaltung > Dienste**).

3. Wählen Sie den Eintrag **Websense DC Agent** und klicken Sie auf **Beenden**.
4. Doppelklicken Sie auf den Eintrag **Websense DC Agent**.
5. Wählen Sie auf der Registerkarte **Anmelden** die Option **Dieses Konto**.
6. Geben Sie den in Schritt 1 erstellten Benutzernamen für das Websense DC Agent-Konto ein. Beispiel: **DomäneName\websense**.
7. Geben Sie das Windows-Passwort für dieses Konto ein und bestätigen Sie es durch die erneute Eingabe.
8. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.
9. Wählen Sie im Dialogfeld "Dienste" den Eintrag **Websense DC Agent** und klicken Sie auf **Starten**.
10. Wiederholen Sie diesen Vorgang für jede Instanz von Websense User Service.

Fehlerbehebung für Logon Agent

Wenn einige Benutzer in Ihrem Netzwerk unter Verwendung der Richtlinie **Standard** gefiltert werden, da Logon Agent sie nicht identifizieren kann, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass Gruppenrichtlinienobjekte von Windows (Group Policy Objects, GPOs) korrekt auf die Computer dieser Benutzer angewendet werden (siehe *Gruppenrichtlinienobjekte*, Seite 394).
- Wenn User Service auf einem Linux-Computer installiert ist und Sie Windows Active Directory (Native Mode) verwenden, überprüfen Sie die Konfigurationen Ihres Verzeichnisdienstes (siehe *User Service unter Linux*, Seite 395).
- Stellen Sie sicher, dass der Client-Computer mit dem Domänencontroller kommunizieren kann, über den das Anmelde-Skript ausgeführt wird (siehe *Sichtbarkeit des Domänencontrollers*, Seite 395).
- Stellen Sie sicher, dass NetBIOS auf dem Client-Computer aktiviert ist (siehe *NetBIOS*, Seite 396).
- Stellen Sie sicher, dass das Benutzerprofil auf dem Client-Computer nicht beschädigt ist (siehe *Probleme mit dem Benutzerprofil*, Seite 396).

Gruppenrichtlinienobjekte

Nachdem Sie sichergestellt haben, dass Ihre Umgebung die im *Installationshandbuch* für Ihre Websense-Software beschriebenen Voraussetzungen erfüllt, überprüfen Sie, ob die Gruppenrichtlinienobjekte korrekt angewendet werden:

1. Öffnen Sie auf dem Active Directory-Computer die Windows-Systemsteuerung und wechseln Sie zu **Verwaltung > Active Directory-Benutzer und -Computer**.
2. Klicken Sie mit der rechten Maustaste auf den Domäneneintrag und wählen Sie **Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Gruppenrichtlinie** und wählen Sie die Domänenrichtlinie aus der Liste der Verknüpfungen für Gruppen-Domänenrichtlinienobjekte aus.

4. Klicken Sie auf **Bearbeiten** und erweitern Sie den Knoten "Benutzerkonfiguration" in der Verzeichnisstruktur.
5. Erweitern Sie den Knoten "Windows-Einstellungen" und wählen Sie **Skripts**.
6. Doppelklicken Sie im rechten Fenster auf **Anmeldung** und überprüfen Sie, ob die Datei **logon.bat** im Dialogfeld für die Anmeldeeigenschaften aufgelistet ist.

   Dieses Skript wird von der Client-Anwendung für die Anmeldung benötigt.

   - Wenn **logon.bat** sich nicht im Skript befindet, beachten Sie die Hinweise im Kapitel zur *Erstmaligen Einrichtung* im *Installationshandbuch* Ihrer Websense-Software.
   - Wenn **logon.bat** zwar im Skript angezeigt wird, Logon Agent jedoch nicht funktioniert, führen Sie die zusätzlichen Schritte zur Fehlerbehebung in diesem Abschnitt aus, um sicherzustellen, dass kein Problem mit der Netzwerkkonnektivität besteht. Alternativ können Sie auch die Informationen in der Websense Knowledge Base aufrufen.

User Service unter Linux

Wenn Sie Logon Agent für die transparente Identifikation von Benutzern verwenden und User Service auf einem Linux-Gerät installiert ist, müssen Sie die Websense-Software vorübergehend so installieren, dass sie mit Active Directory im Mixed Mode kommuniziert.

1. Wechseln Sie in Websense Manager zu **Einstellungen > Verzeichnisdienste**.
2. Notieren Sie sich Ihre aktuellen Verzeichniseinstellungen.
3. Wählen Sie unter "Verzeichnisse" den Eintrag **Windows NT(R) Directory/ Active Directory (Mixed Mode(R)**.
4. Klicken Sie auf **OK**, um Änderungen im Cache zu speichern, und klicken Sie anschließend auf **Alles speichern**.
5. Wählen Sie unter "Verzeichnisse" den Eintrag **Active Directory (Native Mode)**. Wenn Ihre ursprüngliche Konfiguration nicht angezeigt wird, verwenden Sie die in Schritt 2 gemachten Notizen, um Ihre Verzeichniseinstellungen wiederherzustellen. Weitere Anleitungen hierzu finden Sie unter *Windows Active Directory (Native Mode)*, Seite 68.
6. Wenn Sie mit dem Bearbeiten der Konfigurationen fertig sind, klicken Sie auf **OK** und anschließend auf **Alles speichern**.

Sichtbarkeit des Domänencontrollers

So stellen Sie sicher, dass der Client-Computer mit dem Domänencontroller kommunizieren kann:

1. Versuchen Sie, ein Laufwerk auf dem Client-Computer dem gemeinsamen Stammlaufwerk des Domänencontrollers zuzuweisen. Hier wird in der Regel das Anmeldeskript ausgeführt und hier ist auch **LogonApp.exe** gespeichert.

2. Öffnen Sie auf dem Client-Computer eine Windows-Befehlszeile und führen Sie folgenden Befehl aus:

   ```
   net view /domain:<Domänenname>
   ```

Wenn einer dieser Tests fehlschlägt, ziehen Sie die Dokumentation Ihres Windows-Betriebssystems zu Rate. Es besteht ein Problem mit der Netzwerkkonnektivität, das nicht mit der Websense-Software in Zusammenhang steht.

NetBIOS

NetBIOS über TCP/IP muss aktiviert ein und der Dienst TCP/IP NetBIOS Helper muss ausgeführt werden, damit das Websense-Anmeldeskript auf dem Computer des Benutzers ausgeführt werden kann.

So stellen Sie sicher, dass NetBIOS über TCP/IP auf dem Computer des Benutzers aktiviert ist:

1. Klicken Sie mit der rechten Maustaste auf **Netzwerkumgebung** und wählen Sie **Eigenschaften**.
2. Klicken Sie mit der rechten Maustaste auf **LAN-Verbindung** und wählen Sie **Eigenschaften**.
3. Wählen Sie **Internetprotokoll (TCP/IP)** und klicken Sie auf **Eigenschaften**.
4. Klicken Sie auf **Erweitert**.
5. Wählen Sie die Registerkarte **WINS** und überprüfen Sie, ob die korrekte NetBIOS-Option eingestellt ist.
6. Wenn Sie eine Änderung vornehmen, klicken Sie auf **OK** und anschließend noch zwei Mal auf **OK**, um die einzelnen Dialogfelder mit den Eigenschaften zu schließen und Ihre Änderungen zu speichern.

   Wenn keine Änderung erforderlich ist, klicken Sie auf **Abbrechen**, um die einzelnen Dialogfelder zu schließen, ohne Änderungen vorzunehmen.

Überprüfen Sie im Dialogfeld für die Windows-Dienste, ob der Dienst **TCP/IP NetBIOS Helper** auf dem Client-Computer ausgeführt wird (siehe *Das Dialogfeld für die Windows-Dienste*, Seite 422). Der Dienst TCP/IP NetBIOS Helper kann unter Windows 2000, Windows XP, Windows Server 2003 und Windows NT ausgeführt werden.

Probleme mit dem Benutzerprofil

Wenn das Benutzerprofil auf dem Client-Computer beschädigt ist, kann das Websense-Anmeldeskript (ebenso wie die Windows-GPO-Einstellungen) nicht ausgeführt werden. Sie können dieses Problem beheben, indem Sie das Benutzerprofil neu erstellen.

Wenn Sie ein Benutzerprofil neu erstellen, werden der vorhandenen Ordner "Eigene Dateien", die Favoriten und weitere benutzerdefinierte Daten und Einstellungen nicht automatisch auf das neue Profil übertragen. Löschen Sie das vorhandene, beschädigte Profil daher erst, wenn Sie sichergestellt haben, dass beim neuen Profil das Problem

nicht mehr auftritt, und Sie die vorhandenen Daten des Benutzers in das neue Profil kopiert haben.

So erstellen Sie ein Benutzerprofil neu:

1. Melden Sie sich als lokaler Administrator auf dem Client-Computer an.
2. Benennen Sie das Verzeichnis um, in dem das Benutzerprofil gespeichert ist:

   ```
   C:\Dokumente und Einstellungen\<Benutzername>
   ```

3. Starten Sie den Computer neu.
4. Melden Sie sich als der gefilterte Benutzer auf dem Computer an. Es wird automatisch ein neues Benutzerprofil erstellt.
5. Überprüfen Sie, ob der Benutzer wie gewünscht gefiltert wird.
6. Kopieren Sie die benutzerdefinierten Daten (wie die Inhalte des Ordners "Eigene Dateien") aus dem alten in das neue Profil. Verwenden Sie nicht den Assistent zum Übertragen von Dateien und Einstellungen, da es ansonsten zu einer Beschädigung des neuen Profils kommen könnte.

Fehlerbehebung für eDirectory Agent

Verwandte Themen:

- *Aktivieren der Diagnosefunktionen von eDirectory Agent*, Seite 398
- *eDirectory Agent unterlaufen Fehler beim Zählen der eDirectory Server-Verbindungen*, Seite 399
- *Ausführen von eDirectory Agent im Konsolenmodus*, Seite 399

Ein Benutzer wird möglicherweise nicht korrekt gefiltert, wenn der Benutzername nicht an eDirectory Agent weitergeleitet wird. Wenn sich ein Benutzer nicht beim Novell eDirectory-Server anmeldet, kann eDirectory Agent die Anmeldung nicht erkennen. Dies kann folgende Ursachen haben:

- Ein Benutzer meldet sich bei einer Domäne an, die nicht im Standard-Stammkontext der eDirectory-Benutzeranmeldesitzungen enthalten ist. Dieser Stammkontext wird während der Installation angegeben und muss mit dem für Novell eDirectory auf der Seite **Einstellungen** > **Verzeichnisdienste** angegebenen Stammkontext übereinstimmen.
- Ein Benutzer versucht, eine Anmeldeaufforderung zu umgehen, um nicht von Websense gefiltert zu werden.
- Ein Benutzer verfügt über kein Konto auf dem eDirectory-Server.

Wenn sich ein Benutzer nicht auf dem eDirectory-Server anmeldet, können auf diesen Benutzer keine benutzerspezifischen Richtlinien angewendet werden. Stattdessen wird die Richtlinie **Standard** verwendet. Wenn es in Ihrem Netzwerk gemeinsame Arbeitsplätze gibt, an denen sich Benutzer anonym anmelden, richten Sie eine Filterrichtlinie für diese Computer ein.

So stellen Sie fest, ob eDirectory Agent einen Benutzernamen empfängt und den entsprechenden Benutzer identifiziert:

1. Aktivieren Sie eDirectory Agent wie unter *Aktivieren der Diagnosefunktionen von eDirectory Agent*, Seite 398 beschrieben.
2. Öffnen Sie die von Ihnen angegebene Protokolldatei in einem Texteditor.
3. Suchen Sie nach einem Eintrag, der zu dem nicht korrekt gefilterten Benutzer passt.
4. Ein Eintrag wie der folgende gibt an, dass eDirectory Agent einen Benutzer identifiziert hat:

   ```
   WsUserData::WsUserData()
   User: cn=Admin,o=novell (10.202.4.78)
   WsUserData::~WsUserData()
   ```

   Im oben genannten Beispiel hat sich der Benutzer **Admin** auf dem eDirectory-Server angemeldet und wurde erfolgreich identifiziert.
5. Wenn ein Benutzer identifiziert, jedoch nicht wie gewünscht gefiltert wird, überprüfen Sie Ihre Richtlinienkonfiguration und stellen Sie sicher, dass die korrekte Richtlinie auf diesen Benutzer angewendet wird und dass der Benutzername in Websense Manager dem Benutzernamen in Novell eDirectory entspricht.

   Wenn der Benutzer *nicht* identifiziert wird, stellen Sie Folgendes sicher:

   - Der Benutzer verfügt über ein Novell eDirectory-Konto.
   - Der Benutzer meldet sich bei einer Domäne an, die im Standard-Stammkontext für die eDirectory-Benutzeranmeldung enthalten ist.
   - Der Benutzer versucht nicht, eine Anmeldeaufforderung zu umgehen.

Aktivieren der Diagnosefunktionen von eDirectory Agent

eDirectory Agent verfügt über integrierte Diagnosefunktionen, die jedoch standardmäßig nicht aktiviert sind. Sie können die Protokollierung und das Debugging während der Installation oder zu einem beliebigen anderen Zeitpunkt aktivieren.

1. Beenden Sie eDirectory Agent (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).
2. Wechseln Sie auf dem eDirectory Agent-Computer zum eDirectory-Installationsverzeichnis.
3. Öffnen Sie die Datei **wsedir.ini** in einem Texteditor.
4. Navigieren Sie zum Abschnitt **[eDirAgent]**.
5. Um die Protokollierung und das Debugging zu aktivieren, ändern Sie den Wert für **DebugMode** in **On**:

   ```
   DebugMode=On
   ```
6. Um die Protokolldetailebene anzugeben, bearbeiten Sie die folgende Zeile:

   ```
   DebugLevel=<N>
   ```

   N kann ein Wert zwischen 0 und 3 sein, wobei 3 die höchste Detailebene angibt.

7. Bearbeiten Sie die Zeile **LogFile**, sodass der Name der Protokollausgabedatei angegeben wird:

   ```
   LogFile=Dateiname.txt
   ```

   Standardmäßig erfolgt die Protokollausgabe an die eDirectory Agent-Konsole. Wenn Sie den Agenten im Konsolenmodus ausführen (siehe *Ausführen von eDirectory Agent im Konsolenmodus*, Seite 399), können Sie den Standardwert beibehalten.
8. Speichern Sie die Datei **wsedir.ini** und schließen Sie sie.
9. Starten Sie den eDirectory Agent-Dienst (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).

eDirectory Agent unterlaufen Fehler beim Zählen der eDirectory Server-Verbindungen

Wenn eDirectory Agent mehr als 1.000 Benutzer in Ihrem Netzwerk überwacht, jedoch nur 1.000 Verbindungen zum Novell eDirectory-Server anzeigt, kann dies an einer Begrenzung der Windows API liegen, die Informationen vom eDirectory-Server an Websense eDirectory Agent übermittelt. Dieser Fall tritt nur sehr selten ein.

Um diese Begrenzung zu umgehen, fügen Sie der Datei **wsedir.ini** einen Parameter hinzu, der die Serververbindungen akkurat zählt (nur Windows):

1. Beenden Sie den eDirectory Agent-Dienst (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).
2. Wechseln Sie zum Websense-Verzeichnis **bin** (standardmäßig **C:\Programme\Websense\bin**).
3. Öffnen Sie die Datei **wsedir.ini** in einem Texteditor.
4. Fügen Sie eine leere Zeile ein und geben Sie anschließend folgenden Wert ein:

   ```
   MaxConnNumber = <NNNN>
   ```

   In diesem Fall ist *<NNNN>* die maximal mögliche Anzahl an Verbindungen zum Novell eDirectory-Server. Wenn es beispielsweise 1.950 Benutzer in Ihrem Netzwerk gibt, können Sie 2.000 als maximale Anzahl eingeben.
5. Speichern Sie die Datei.
6. Starten Sie eDirectory Agent neu.

Ausführen von eDirectory Agent im Konsolenmodus

1. Führen Sie einen der folgenden Schritte aus:
   - Geben Sie in der Windows-Befehlszeile (**Start > Ausführen > cmd**) folgenden Befehl ein:

     ```
     eDirectoryAgent.exe -c
     ```
   - Geben Sie in der Linux-Befehlszeile folgenden Befehl ein:

     ```
     eDirectoryAgent -c
     ```
2. Drücken Sie die **Eingabetaste**, um den Agenten zu beenden. Es kann einige Sekunden dauern, bis der Agent beendet wird.

Fehlerbehebung für RADIUS Agent

RADIUS Agent verfügt über integrierte Diagnosefunktionen, die jedoch standardmäßig nicht aktiviert sind. So aktivieren Sie die Protokollierung und das Debugging für RADIUS Agent:

1. Beenden Sie den RADIUS Agent-Dienst (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).
2. Wechseln Sie auf dem RADIUS Agent-Computer zum Installationsverzeichnis des Agenten (standardmäßig **Websense\bin**).
3. Öffnen Sie die Datei **wsradius.ini** in einem Texteditor.
4. Navigieren Sie zum Abschnitt **[RADIUSAgent]**.
5. Um die Protokollierung und das Debugging zu aktivieren, ändern Sie den Wert für **DebugMode** in **On**:

   ```
   DebugMode=On
   ```

6. Um die Protokolldetailebene anzugeben, bearbeiten Sie die folgende Zeile:

   ```
   DebugLevel=<N>
   ```

   N kann ein Wert zwischen 0 und 3 sein, wobei 3 die höchste Detailebene angibt.
7. Bearbeiten Sie die Zeile **LogFile**, sodass der Name der Ausgabedatei angegeben wird:

   ```
   LogFile=Dateiname.txt
   ```

   Standardmäßig erfolgt die Protokollausgabe an die RADIUS Agent-Konsole. Wenn Sie den Agenten im Konsolenmodus ausführen (siehe *Ausführen von RADIUS Agent im Konsolenmodus*, Seite 400), können Sie optional auch den Standardwert beibehalten.
8. Speichern Sie die Datei **wsradius.ini** und schließen Sie sie.
9. Starten Sie den RADIUS Agent-Dienst (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).

Wenn Remote-Benutzer nicht wie gewünscht identifiziert und gefiltert werden, liegt dies wahrscheinlich an Kommunikationsproblemen zwischen RADIUS Agent und Ihrem RADIUS-Server. Überprüfen Sie Ihre RADIUS Agent-Protokolle auf Fehler, um die Ursache zu ermitteln.

Ausführen von RADIUS Agent im Konsolenmodus

Um RADIUS Agent im Konsolenmodus zu starten (als Anwendung), geben Sie Folgendes ein:

- In der Windows-Befehlszeile:

  ```
  RadiusAgent.exe -c
  ```

- In der Linux-Befehlszeile:

  ```
  ./RadiusAgent -c
  ```

Sie können den Agenten jederzeit beenden, indem Sie die **Eingabetaste** erneut drücken. Es kann einige Minuten dauern, bis der Agent beendet wird.

RADIUS Agent akzeptiert die folgenden Befehlszeilenparameter:

> **Hinweis**
> Bei einem Linux-Betriebssystem empfiehlt Websense, Inc. die Verwendung des Skripts zum Starten oder Beenden von Websense RADIUS Agent (**WsRADIUSAgent start|stop**) anstelle der Parameter -r und -s.

Parameter	Beschreibung
-i	Installiert den RADIUS Agent-Dienst/-Daemon.
-r	Führt den RADIUS Agent-Dienst/-Daemon aus.
-s	Beendet den RADIUS Agent-Dienst/-Daemon.
-c	Führt RADIUS Agent als Anwendungsprozess und nicht als Dienst oder Daemon aus. Im Konsolenmodus kann RADIUS Agent so konfiguriert werden, dass die Protokollausgabe an die Konsole oder an eine Textdatei erfolgt.
-v	Zeigt die Versionsnummer von RADIUS Agent an.
-? -h -help *<no option>*	Zeigt Nutzungsinformationen über die Befehlszeile an. Listet alle möglichen Befehlszeilenparameter auf und beschreibt sie.

Remote-Benutzer werden nicht zur manuellen Authentifizierung aufgefordert

Wenn Sie Remote-Benutzer so konfiguriert haben, dass sie beim Zugriff auf das Internet eine manuelle Authentifizierung vornehmen müssen, kann es gelegentlich vorkommen, dass einzelne Benutzer nicht nach der Authentifizierung gefragt werden. Dieser Fall kann eintreten, wenn einige netzwerkinterne IP-Adressen zum Umgehen der manuellen Authentifizierung konfiguriert wurden.

Wenn ein Remote-Benutzer auf das Netzwerk zugreift, liest die Websense-Software den letzten Teil der MAC-Adresse (Media Access Control) des Computers. Wenn dieser Wert mit einer im Netzwerk befindlichen IP-Adresse übereinstimmt, die für die Umgebung der manuellen Authentifizierung konfiguriert wurde, wird der Remote-Benutzer nicht dazu aufgefordert, beim Zugriff auf das Internet eine manuelle Authentifizierung vorzunehmen.

Eine Lösung für dieses Problem besteht darin, die netzwerkinterne IP-Adresse neu zu konfigurieren, sodass sie die manuelle Authentifizierung verwendet. Eine alternative Lösung besteht darin, die Anforderung einer manuellen Authentifizierung für den betroffenen Remote-Benutzer zu deaktivieren.

Remote-Benutzer werden nicht richtig gefiltert

Wenn Remote-Benutzer gar nicht oder nicht unter Verwendung der Ihnen zugewiesenen Richtlinie gefiltert werden, überprüfen Sie die RADIUS Agent-Protokolle auf die Meldung **Error receiving from server: 10060** (Windows) oder **Error receiving from server: 0** (Linux).

Diese Meldung wird in der Regel dann ausgegeben, wenn der RADIUS-Server RADIUS Agent nicht als Client (Quelle der RADIUS-Anfragen) erkennt. Stellen Sie sicher, dass Ihr RADIUS-Server korrekt konfiguriert ist (siehe *Die RADIUS-Umgebung konfigurieren*, Seite 233).

Sie können die integrierten Diagnosetools von RADIUS Agent verwenden, um Probleme mit dem Filtern zu beheben (siehe *Fehlerbehebung für RADIUS Agent*, Seite 400).

Wenn Sie die Funktion Remote Filtering implementiert haben (siehe *Filtern von Remote Clients*, Seite 167), können Remote-Benutzer nur dann gefiltert werden, wenn der Remote Filtering Client mit dem Remote Filtering Server innerhalb des Netzwerks kommunizieren kann.

Anleitungen zum Einrichten der Funktion Remote Filtering finden Sie im Beitrag *Remote Filtering*.

Probleme mit Sperrmeldungen

Für den blockierten Filtertyp wird keine Sperrseite angezeigt

Wenn die Sperrung nach Dateitypen erfolgt, ist die Sperrmeldung nicht in allen Fällen für den Benutzer sichtbar. Wenn sich beispielsweise eine herunterladbare Datei in einem internen Frame (IFRAME) auf einer zulässigen Website befindet, wird die an diesen Frame gesendete Sperrmeldung nicht angezeigt, da die Größe des Frames Null beträgt.

Dies ist lediglich ein Anzeigeproblem; Benutzer können nicht auf die gesperrte Datei zugreifen oder sie herunterladen.

Anstelle einer Sperrseite wird Benutzern ein Browserfehler angezeigt

Wenn Benutzern anstelle einer Sperrseite eine Fehlermeldung angezeigt wird, hat dies zumeist eine der beiden folgenden Ursachen:

- Der Browser des Benutzers ist für die Verwendung eines externen Proxy-Servers konfiguriert. Bei den meisten Browsern gibt es eine Einstellung zur Aktivierung der Verwendung eines externen Proxy-Servers. Stellen Sie sicher, dass der Browser nicht für die Verwendung eines externen Proxy-Servers eingestellt ist.
- Es liegt ein Problem mit der Identifizierung des Filtering Service-Computers oder mit der Kommunikation mit diesem Computer vor.

Wenn die Browsereinstellungen des Benutzers korrekt sind, stellen Sie sicher, das die IP-Adresse des Filtering Service-Computers korrekt in der Datei **eimserver.ini** aufgelistet ist.

1. Beenden Sie **Websense Filtering Service** (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).
2. Wechseln Sie zum Websense-Verzeichnis **bin** (standardmäßig C:\Programme\Websense\bin oder /opt/Websense/bin).
3. Öffnen Sie die Datei **eimserver.ini** in einem Texteditor.
4. Fügen Sie unter [WebsenseServer] eine leere Zeile ein und geben Sie Folgendes ein:

   ```
   BlockMsgServerName = <Filtering Service-IP-Adresse>
   ```

   Wenn beispielsweise die Filtering Service-IP-Adresse 10.201.72.15 lautet, geben Sie Folgendes ein:

   ```
   BlockMsgServerName = 10.201.72.15
   ```

5. Speichern und schließen Sie die Datei.
6. Starten Sie Filtering Service neu.

Wenn der Filtering Service-Computer mehr als eine NIC aufweist und die Sperrseite nach der Bearbeitung der Datei **eimserver.ini** noch immer nicht richtig angezeigt wird, versuchen Sie es mit den IP-Adressen der anderen NICs im Parameter **BlockMsgServerName**.

Wenn die Sperrseite noch immer nicht angezeigt wird, stellen Sie sicher, dass die Benutzer schreibgeschützten Zugriff auf die Dateien in den Websense-Sperrseitenverzeichnissen haben:

- Websense\BlockPages\en\Default
- Websense\BlockPages\en\Custom

Wenn das Problem mit der Sperrseite weiterhin besteht, beachten Sie die zusätzlichen Tipps zur Problembehebung in der Websense Knowledge Base.

Anstelle einer Sperrseite wird eine leere weiße Seite angezeigt

Wenn Werbeanzeigen blockiert werden oder wenn ein Browser die Codierung einer Sperrseite nicht richtig erkennt, wird den Benutzern möglicherweise statt einer Sperrseite eine leere weiße Seite angezeigt. Dafür gibt es folgende Ursachen:

- Wenn die Werbekategorie blockiert ist, interpretiert die Websense-Software gelegentlich eine Anfrage nach einer Grafik als Werbeanfrage und zeigt statt einer Sperrseite ein leeres Bild an (dies ist die normale Methode zum Blockieren von Werbung). Wenn die angeforderte URL die Endung .gif oder eine ähnliche Endung aufweist, muss der Benutzer die URL erneut eingeben, wobei die Endung *.gif weggelassen wird.
- Einige ältere Browser sind möglicherweise nicht in der Lage, die Codierung von Sperrseiten zu erkennen. Damit die Zeichen korrekt erkannt werden, konfigurieren Sie den Browser für die Anzeige des passenden Zeichensatzes (UTF-8 für Französisch, Deutsch, Italienisch, Spanisch, brasilianisches Portugiesisch, vereinfachtes Chinesisch, traditionelles Chinesisch oder Koreanisch; Shift_JIS für Japanisch). Beachten Sie die Anleitungen in Ihrer Browserdokumentation oder führen Sie ein Upgrade Ihres Browsers auf eine neuere Version durch.

Protokollsperrmeldungen werden nicht korrekt angezeigt

Aus folgenden Gründen kann es vorkommen, dass Protokollsperrmeldungen nicht angezeigt oder verspätet angezeigt werden:

- User Service muss auf einem Windows-Computer installiert sein, damit Protokollsperrmeldungen korrekt angezeigt werden können. Weitere Informationen hierzu finden Sie im *Installationshandbuch*.
- Es kann vorkommen, dass Protokollsperrmeldungen die Client-Computer nicht erreichen, wenn Network Agent auf einem Gerät mit mehreren NICs installiert ist und eine NIC ein anderes Netzwerksegment über Filtering Service überwacht. Stellen Sie sicher, dass der Filtering Service-Computer Zugriff auf das NetBIOS- oder Server Message Block-Protokoll der Client-Computer hat und dass Port 15871 nicht blockiert ist.
- Eine Protokollsperrmeldung kann leicht verzögert oder (statt auf dem Client-Computer) auf einem internen Gerät angezeigt werden, von dem die angeforderten Protokolldaten stammen, wenn Network Agent für die Überwachung von Anfragen konfiguriert ist, die an interne Computer **gesendet** werden.
- Wenn der gefilterte Client oder der Websense-Filtercomputer Windows 200x ausführt, muss der Dienst Windows **Messenger** ausgeführt werden, damit die Protokollsperrmeldung angezeigt wird. Überprüfen Sie im Dialogfeld für die Windows-Dienste auf dem Client-Computer, ob der Messenger-Dienst ausgeführt wird (siehe *Das Dialogfeld für die Windows-Dienste*, Seite 422). Obwohl die Sperrmeldung nicht angezeigt wird, werden Protokollanfragen weiterhin blockiert.

Anstelle einer Sperrseite wird eine Protokollsperrmeldung angezeigt

Wenn Ihr Integrationsprodukt keine HTTPS-Informationen an die Websense-Software sendet oder wenn die Websense-Software im Standalone-Modus ausgeführt wird, kann Network Agent eine HTTPS-Websiteanfrage, die über die Kategorieeinstellungen blockiert wird, unter Umständen als Protokollanfrage interpretieren. Aus diesem Grund wird dann eine Protokollsperrmeldung angezeigt. Die HTTPS-Anfrage wird ebenfalls als Protokollanfrage protokolliert.

Probleme mit Protokollen, Statusmeldungen und Alerts

Wo finde ich Fehlermeldungen für Websense-Komponenten?

Bei Fehlern oder Warnungen in Zusammenhang mit wichtigen Websense-Komponenten werden in der Liste **Zusammenfassung der zustandsbezogenen Alerts** oben auf der Seite **Status > Heute** in Websense Manager kurze Warnmeldungen angezeigt (siehe *Zustandsbezogene Websense-Alerts*, Seite 405).

- Klicken Sie auf eine Warnmeldung, um weitere Informationen auf der Seite **Status > Alerts** anzuzeigen.
- Wenn Sie Hilfe bei der Fehlerbehebung benötigen, klicken Sie neben einer Meldung auf der Seite "Status > Alerts" auf **Lösungen**.

Fehler, Warnungen und Meldungen von Komponenten der Websense-Software sowie Statusmeldungen zum Datenbank-Download werden in der Datei **websense.log** im Websense-Verzeichnis **bin** (standardmäßig C:\Programme\Websense\bin oder /opt/Websense/bin) gespeichert. Siehe *Die Websense-Protokolldatei*, Seite 423.

Bei Komponenten der Websense-Software, die auf einem Windows-Computer installiert sind, können Sie zudem die Ereignisanzeige von Windows überprüfen. Siehe *Die Ereignisanzeige von Windows*, Seite 423.

Zustandsbezogene Websense-Alerts

Die Zusammenfassung der zustandsbezogenen Alerts in Websense listet sämtliche potenziellen Probleme auf, die für die überwachten Komponenten Ihrer Websense-Software auftreten. Dazu gehören:

- Ein Filtering Service wird nicht ausgeführt
- User Service ist nicht verfügbar
- Ein Log Server wird nicht ausgeführt

- Es ist kein Log Server für einen Policy Server konfiguriert
- Die Protokolldatenbank ist nicht verfügbar
- Network Agent wird nicht ausgeführt
- Es ist kein Network Agent für einen Policy Server konfiguriert
- Es ist keine NIC für die Überwachung für einen Network Agent konfiguriert
- Es ist kein Filtering Service für einen Network Agent konfiguriert
- Die Datenbank für erste Filteraktivitäten wird verwendet
- Die Master Database wird zum ersten Mal heruntergeladen
- Die Master Database wird aktualisiert
- Die Master Database ist älter als eine Woche
- Die Master Database wurde nicht erfolgreich heruntergeladen
- WebCatcher ist nicht aktiviert
- Es liegt ein Problem mit der Subskription vor
- Der Subskriptionsschlüssel läuft bald ab
- Es wurde kein Subskriptionsschlüssel eingegeben

Die Seite "Alerts" liefert grundlegende Informationen zu Fehlern und Warnungen. Wenn Sie Informationen zur Fehlerbehebung benötigen, klicken Sie auf **Lösungen**.

Wenn Sie eine Fehler- oder Statusmeldung zu Komponenten erhalten, die Sie nicht verwenden oder die Sie deaktiviert haben, können Sie in einigen Fällen die Warnmeldungen ausblenden. Weitere Informationen finden Sie unter *Überprüfen des aktuellen Systemstatus*, Seite 311.

Für eine einzige Anfrage werden zwei Protokolleinträge erstellt

Wenn der QoS-Paketplaner von Windows auf demselben Computer wie Network Agent installiert ist, werden für jede einzelne HTTP- oder Protokollanfrage, die über den Network Agent-Computer gesendet wird, 2 Anfragen protokolliert. (Diese doppelte Protokollierung erfolgt nicht bei Anfragen, die von Client-Computern innerhalb Ihres Netzwerks gesendet werden.)

Um das Problem zu beheben, deaktivieren Sie auf dem Network Agent-Computer den Windows QoS-Paketplaner.

Das Problem tritt nicht auf, wenn Sie Network Agent für sämtliche Protokollierungen verwenden. Weitere Informationen hierzu finden Sie unter *Konfigurieren der Einstellungen für die Netzwerkschnittstellenkarte (NIC)*, Seite 369.

Probleme mit Policy Server und Policy Database

- *Ich habe mein Passwort vergessen*, Seite 407
- *Ich kann mich nicht bei Policy Server anmelden*, Seite 407
- *Die Websense Policy Database kann nicht gestartet werden*, Seite 407

Ich habe mein Passwort vergessen

Wenn Sie über die Berechtigungen eines übergeordneten Administrators (Super Administrator) oder eines delegierten Administrators verfügen, der ein Websense-Benutzerkonto für die Anmeldung bei Policy Server über Websense Manager verwendet, können Sie als Super Administrator, für den keine Bedingungen gelten, das Passwort zurücksetzen.

- Das Passwort für WebsenseAdministrator wird unter **Einstellungen > Konto** festgelegt.
- Die Passwörter für andere Administratorenkonten werden unter **Delegierte Verwaltung > Websense-Benutzerkonten verwalten** festgelegt.

Wenn Sie die delegierte Verwaltung nicht verwenden und das Passwort für WebsenseAdministrator vergessen haben, melden Sie sich bei MyWebsense an, um das Passwort zurückzusetzen.

- Der Subskriptionsschlüssel für das MyWebsense-Konto muss mit Ihrem aktuellen Subskriptionsschlüssel für Websense Web Security oder Websense Web Filter übereinstimmen.
- Wenn Sie über mehrere Subskriptionsschlüssel verfügen, müssen Sie den korrekten Schlüssel für Websense Web Security oder Websense Web Filter verwenden, damit das Passwort erfolgreich zurückgesetzt werden kann.
- Sie müssen Zugriff auf den Websense Manager-Computer haben, um diesen Vorgang auszuführen.

Ich kann mich nicht bei Policy Server anmelden

Stellen Sie sicher, dass die ausgewählte IP-Adresse für Policy Server korrekt ist. Wenn sich die Adresse des Policy Server-Computers seit dem Hinzufügen von Policy Server zu Websense Manager geändert hat, müssen Sie sich bei einem anderen Policy Server anmelden, die alte IP-Adresse aus Websense Manager entfernen und anschließend die neue IP-Adresse für Policy Server hinzufügen. Siehe *Hinzufügen und Bearbeiten von Policy Server-Instanzen*, Seite 294.

Wenn Websense Manager plötzlich beendet wird oder über die Befehle kill (Linux) oder End Task (Windows) beendet wurde, warten Sie einige Minuten, bevor Sie sich erneut anmelden. Die Websense-Software erkennt und schließt abgelaufene Sitzungen innerhalb von 3 Minuten.

Die Websense Policy Database kann nicht gestartet werden

Die Websense Policy Database wird als spezielles Konto ausgeführt: **WebsenseDBUser**. Wenn für dieses Konto Anmeldeprobleme auftreten, kann die Policy Database nicht gestartet werden.

Um dieses Problem zu beheben, ändern Sie das Passwort für das Konto WebsenseDBUser.

1. Melden Sie sich als lokaler Administrator auf dem Policy Database-Computer an.

2. Wechseln Sie zu **Start > Alle Programme > Verwaltung > Computerverwaltung**.
3. Erweitern Sie im Navigationsfenster unter "Systemprogramme" den Eintrag **Lokale Benutzer und Gruppen** und wählen Sie anschließend **Benutzer**. Die Benutzerinformationen werden im Inhaltsfenster angezeigt.
4. Klicken Sie mit der rechten Maustaste auf **WebsenseDBUser** und wählen Sie **Kennwort festlegen**.
5. Geben Sie das neue Passwort für dieses Benutzerkonto ein, bestätigen Sie es durch die erneute Eingabe und klicken Sie anschließend auf **OK**.
6. Schließen Sie das Dialogfeld "Computerverwaltung".
7. Wechseln Sie zu **Start > Alle Programme > Verwaltung > Dienste**.
8. Klicken Sie mit der rechten Maustaste auf **Websense Policy Database** und wählen Sie **Eigenschaften**.
9. Klicken Sie im Dialogfeld "Eigenschaften" auf die Registerkarte "Anmelden" und geben Sie das neue WebsenseDBUser-Passwort ein. Klicken Sie anschließend auf **OK**.
10. Klicken Sie erneut mit der rechten Maustaste auf Websense Policy Database und wählen Sie **Starten**.

    Wenn der Dienst gestartet wurde, schließen Sie das Dialogfeld "Dienste".

Probleme mit der delegierten Verwaltung

Verwaltete Clients können nicht aus der Rolle gelöscht werden

Clients können nicht direkt aus der Liste der verwalteten Clients auf der Seite "Delegierte Verwaltung" >"Rolle bearbeiten" gelöscht werden, wenn:

- der Administrator dem Client eine Richtlinie zugewiesen hat
- der Administrator mindestens einem Mitglied eines Netzwerks, einer Gruppe, einer Domäne oder einer Organisationseinheit eine Richtlinie zugewiesen hat

Darüber hinaus können Probleme auftreten, wenn der übergeordnete Administrator bei der Anmeldung bei Websense einen anderen Policy Server auswählt als den Server, der mit dem Verzeichnisdienst kommuniziert, auf dem die zu löschenden

Clients enthalten sind. In diesem Fall werden die Clients nicht vom aktuellen Policy Server und dem Verzeichnisdienst erkannt.

Hilfe beim Löschen verwalteter Clients finden Sie unter *Löschen von verwalteten Clients*, Seite 280.

Ich erhalte eine Fehlermeldung mit dem Hinweis, dass ein anderer Benutzer auf meinem Computer angemeldet ist

Beim Versuch, sich bei Websense Manager anzumelden, kann gelegentlich folgende Fehlermeldung ausgegeben werden: "Anmeldung fehlgeschlagen. Die Rolle <Rollenname> ist von <Benutzername> seit <Datum, Uhrzeit> auf dem Computer 127.0.0.1 verwendet worden". Die IP-Adresse 127.0.0.1 wird auch als Loopback-Adresse bezeichnet. Sie gibt in der Regel den lokalen Computer an.

Diese Meldung besagt, dass sich ein Benutzer auf dem Installationscomputer für Websense Manager mit derselben Rolle angemeldet hat, die Sie verwenden möchten. Sie können eine andere Rolle auswählen (wenn Sie mehrere Rollen verwalten), sich nur für die Berichterstellung anmelden oder warten, bis sich der andere Administrator abgemeldet hat.

Einige Benutzer haben keinen Zugriff auf eine Website in der Liste der ungefilterten URLs

Ungefilterte URLs haben nur Auswirkungen auf Clients, die von der Rolle verwaltet werden, der die URLs hinzugefügt wurden. Wenn beispielsweise ein übergeordneter Administrator (Super Administrator) eine ungefilterte URL hinzufügt, erhalten Clients, die von Rollen für die delegierte Verwaltung verwaltet werden, keinen Zugriff auf diese Websites.

Um die Site für Clients mit anderen Rollen verfügbar zu machen, kann der übergeordnete Administrator zu den einzelnen Rollen wechseln und die relevanten Sites der ungefilterten URL-Liste der jeweiligen Rolle hinzufügen.

Sites, die neuen Kategorien zugeordnet wurden, werden unter Verwendung der falschen Kategorie gefiltert

URLs, die neuen Kategorien zugeordnet wurden, haben nur Auswirkungen auf Clients, die von der Rolle verwaltet werden, der die URLs hinzugefügt wurden. Wenn beispielsweise ein übergeordneter Administrator (Super Administrator) URLs neuen Kategorien zuordnet, werden Clients, die von Rollen für die delegierte Verwaltung verwaltet werden, weiterhin entsprechend der Master Database-Kategorie für diese Websites gefiltert.

Um die Zuordnung zu neuen Kategorien auf Clients mit anderen Rollen anzuwenden, kann der übergeordnete Administrator zu den einzelnen Rollen wechseln und die relevanten Sites für die jeweilige Rolle neuen Kategorien zuordnen.

Ich kann kein benutzerdefiniertes Protokoll erstellen

Nur übergeordnete Administratoren (Super Administrators) können benutzerdefinierte Protokolle erstellen. Jedoch können delegierte Administratoren Filteraktionen für benutzerdefinierte Protokolle festlegen.

Wenn übergeordnete Administratoren (Super Administrators) benutzerdefinierte Protokolle erstellen, sollten Sie die passenden Standardaktionen für die meisten Clients einstellen. Informieren Sie delegierte Administratoren über neue Protokolle, damit sie die Filter für ihre Rolle entsprechend aktualisieren können.

Probleme mit der Berichterstellung

Log Server wird nicht ausgeführt

Wenn Log Server nicht ausgeführt wird oder wenn andere Websense-Komponenten nicht mit Log Server kommunizieren können, werden Informationen zur Internetnutzung nicht gespeichert und Sie können möglicherweise keine Berichte zur Internetnutzung erstellen.

In folgenden Fällen kann es vorkommen, dass Log Server nicht verfügbar ist:

- Wenn nicht ausreichend Festplattenspeicher auf dem Computer vorhanden ist, auf dem Log Server ausgeführt wird.
- Wenn Sie das Passwort für Microsoft SQL Server oder MSDE geändert haben, ohne die Konfiguration von ODBC oder Log Server zu aktualisieren.
- Wenn mehr als 14 Tage vergangen sind, seit die Master Database erfolgreich heruntergeladen wurde.
- Wenn die Datei logserver.ini fehlt oder beschädigt ist.
- Wenn Sie Log Server beendet haben, um das Protokollieren von Informationen zur Internetnutzung zu vermeiden.

So beheben Sie das Problem:

- Stellen Sie sicher, dass ausreichend freier Festplattenspeicher vorhanden ist; entfernen Sie ggf. nicht benötigte Dateien.
- Wenn Sie glauben, dass eine Passwortänderung die Ursache für das Problem ist, beachten Sie die Hinweise unter *Aktualisieren des Passworts für die Log Server-Verbindung*, Seite 415.
- Wechseln Sie zum Websense-Verzeichnis **bin** (standardmäßig C:\Programme\Websense\bin oder /opt/websense/bin) und stellen Sie sicher, dass Sie **logserver.ini** in einem Texteditor öffnen können. Wenn diese Datei beschädigt ist, ersetzen Sie sie durch eine Sicherungsdatei.
- Überprüfen Sie im Dialogfeld für die Windows-Dienste, ob Log Server gestartet wurde, und starten Sie den Dienst falls erforderlich neu (siehe *Anhalten und Starten der Websense-Dienste*, Seite 302).
- Überprüfen Sie die Ereignisanzeige von Windows und die Datei **websense.log** auf Fehlermeldungen von Log Server (siehe *Tools zur Fehlerbehebung*, Seite 422).

Für einen Policy Server ist kein Log Server installiert

Websense Log Server sammelt Informationen zur Internetnutzung und speichert sie in der Protokolldatenbank für die Verwendung in Untersuchungsberichten, Präsentationsberichten und den Diagrammen und Übersichten auf den Seiten "Heute" und "Verlauf" in Websense Manager.

Log Server muss installiert sein, damit die Berichterstellung ausgeführt werden kann.

Diese Meldung kann in folgenden Situationen angezeigt werden:

- Log Server ist auf einem anderen Computer installiert als Policy Server und die IP-Adresse für Log Server ist fälschlicherweie in Websense Manager auf "localhost" eingestellt.
- Log Server ist auf einem Linux-Computer installiert.
- Sie verwenden keine Websense Reporting Tools.

So stellen Sie sicher, dass die korrekte IP-Adresse für Log Server in Websense Manager eingestellt ist:

1. Wählen Sie die Registerkarte **Einstellungen** im linken Navigationsfenster und wechseln Sie zu **Allgemein > Protokollierung**.
2. Geben Sie die IP-Adresse des Log Server-Computers in das Feld **IP-Adresse oder Name von Log Server** ein.
3. Klicken Sie auf **OK**, um Ihre Änderungen im Cache zu speichern, und klicken Sie anschließend auf **Alles speichern**.

Wenn Log Server auf einem Linux-Computer installiert ist oder wenn Sie keine Websense Reporting Tools verwenden, können Sie die Warnmeldung in Websense Manager ausblenden.

1. Wählen Sie die Registerkarte "Hauptseite" im linken Teilfenster für die Navigation. Wählen Sie **Status > Heute**.
2. Klicken Sie unter dem Eintrag "Aktive Alerts" auf **Erweitert**.
3. Aktivieren Sie für die Meldung "Es ist kein Log Server installiert" die Option **Diesen Alert ausblenden**.
4. Klicken Sie auf **Jetzt speichern**. Die Änderung wird sofort gültig.

Die Protokolldatenbank wurde nicht erstellt

Gelegentlich kommt es vor, dass das Installationsprogramm die Protokolldatenbank nicht erstellen kann. In der folgenden Liste werden die häufigsten Ursachen für dieses Problem sowie entsprechende Lösungen beschrieben.

Problem:	Es existiert mindestens eine Datei, die die Namen verwendet, die ebenfalls von der Websense-Software für die Protokolldatenbank verwendet werden ((wslogdb70 und wslogdb70_1), jedoch sind diese Dateien nicht korrekt mit dem Datenbankmodul verbunden und können daher nicht vom Websense-Installationsprogramm verwendet werden.
Lösung:	Entfernen Sie die vorhandenen Dateien oder benennen Sie sie um. Führen Sie anschließend das Installationsprogramm erneut aus.
Problem:	Das Konto, das zur Anmeldung für die Installation verwendet wird, verfügt nicht über die erforderlichen Berechtigungen für das Laufwerk, auf dem die Datenbank installiert wird.
Lösung:	Aktualisieren Sie das Anmeldekonto, sodass es über Lese- und Schreibberechtigungen für das Installationsverzeichnis verfügt, oder melden Sie sich bei einem anderen Konto an, für das diese Berechtigungen bereits bestehen. Führen Sie anschließend das Installationsprogramm erneut aus.

Problem:	Es ist nicht genügend Festplattenspeicher vorhanden, um die Protokolldatenbank im angegebenen Verzeichnis zu erstellen und zu verwalten.
Lösung:	Schaffen Sie genug freien Speicher auf dem ausgewählten Laufwerk, damit die Protokolldatenbank installiert und verwaltet werden kann. Führen Sie anschließend das Installationsprogramm erneut aus. Alternativ können Sie auch einen anderen Speicherort auswählen.
Problem:	Das für die Anmeldung zur Installation verwendete Konto verfügt nicht über die erforderlichen SQL Server-Berechtigungen zum Erstellen einer Datenbank.
Lösung:	Aktualisieren Sie das Anmeldekonto oder melden Sie sich bei einem anderen Konto an, für das die erforderlichen Berechtigungen bereits bestehen. Führen Sie anschließend das Installationsprogramm erneut aus. Die erforderlichen Berechtigungen sind abhängig von der Version von Microsoft SQL Server: ■ SQL Server 2000 oder MSDE: **dbo**-Berechtigungen (Database Owner-Berechtigungen) erforderlich ■ SQL Server 2005: **dbo**- und **SQLServerAgentReader**-Berechtigungen erforderlich

Die Protokolldatenbank ist nicht verfügbar

Die Websense Protokolldatenbank speichert Informationen zur Internetnutzung für die Verwendung in Präsentationsberichten, Untersuchungsberichten und den Diagrammen und Übersichten auf den Seiten "Heute" und "Verlauf" in Websense Manager.

Wenn die Websense-Software keine Verbindung mit der Protokolldatenbank herstellen kann, stellen Sie zunächst sicher, dass das Datenbankmodul (Microsoft SQL Server oder Microsoft SQL Server Desktop Engine [MSDE]) auf dem Protokolldatenbank-Computer ausgeführt wird.

1. Öffnen Sie das Dialogfeld für die Windows-Dienste (siehe *Das Dialogfeld für die Windows-Dienste*, Seite 422) und stellen Sie sicher, dass die folgenden Dienste ausgeführt werden:
   - Microsoft SQL Server:
     - MSSQLSERVER
     - SQLSERVERAGENT
   - Microsoft SQL Desktop Engine (MSDE):
     - MSSQL$WEBSENSE (wenn Sie MSDE über Websense, Inc. erworben haben)
     - SQLAgent$WEBSENSE

2. Wenn ein Dienst beendet wurde, klicken Sie mit der rechten Maustaste auf den Namen des Dienstes und wählen Sie **Starten**.

   Wenn der Dienst nicht gestartet wird, überprüfen Sie die Ereignisanzeige von Windows (siehe *Die Ereignisanzeige von Windows*, Seite 423) auf Fehler- und Warnmeldungen für Microsoft SQL Server oder MSDE.

Wenn das Datenbankmodul ausgeführt wird:

- Stellen Sie sicher, dass SQL Server Agent auf dem Computer ausgeführt wird, auf dem auch das Datenbankmodul ausgeführt wird.
- Überprüfen Sie im Dialogfeld für die Windows-Dienste, ob der **Websense Log Server**-Dienst ausgeführt wird.
- Wenn Log Server und die Protokolldatenbank auf verschiedenen Computern installiert sind, stellen Sie sicher, dass beide Computer eingeschaltet sind und dass die Netzwerkverbindung zwischen den Geräten fehlerfrei funktioniert.
- Stellen Sie sicher, dass auf dem Protokolldatenbank-Computer ausreichend Festplattenspeicher vorhanden ist und dass der Protokolldatenbank genügend Speicherplatz zur Verfügung steht (siehe *Log Server zeichnet keine Daten in der Protokolldatenbank auf*, Seite 414).
- Stellen Sie sicher, dass das Passwort für Microsoft SQL Server oder MSDE nicht geändert wurde. Wenn das Passwort geändert wurde, müssen Sie die Passwortinformationen aktualisieren, die von Log Server zum Herstellen einer Verbindung mit der Datenbank verwendet werden. Siehe *Aktualisieren des Passworts für die Log Server-Verbindung*, Seite 415.

Größe der Protokolldatenbank

Die Größe der Protokolldatenbank ist stets ein wichtiger Aspekt. Wenn Sie erfolgreich Websense-Berichte erstellt haben und feststellen, dass es nun viel länger dauert, bis die Berichte angezeigt werden, oder wenn Sie Meldungen hinsichtlich einer Zeitüberschreitung von Ihrem Webbrowser erhalten, sollten Sie einige Datenbankpartitionen deaktivieren.

1. Wechseln Sie in Websense Manager zu **Einstellungen > Berichterstellung > Protokolldatenbank**.
2. Navigieren Sie zum Abschnitt **Verfügbare Partitionen**.
3. Deaktivieren Sie das Kontrollkästchen **Aktivieren** für sämtliche Partitionen, die für die aktuellen Berichterstellungsvorgänge nicht benötigt werden.
4. Klicken Sie auf **Jetzt speichern**, um die Änderungen zu übernehmen.

Log Server zeichnet keine Daten in der Protokolldatenbank auf

Wenn Log Server keine Daten mehr in die Protokolldatenbank schreiben kann, ist es in der Regel so, dass der Datenbank kein ausreichender Festplattenspeicher mehr zur Verfügung steht. Dieser Fall kann entweder dann eintreten, wenn das Festplattenlaufwerk voll ist oder, bei Microsoft SQL Server, wenn für die maximal zulässige Größe der Datenbank eine Beschränkung besteht.

Wenn das Festplattenlaufwerk, auf dem die Protokolldatenbank gespeichert ist, voll ist, müssen Sie zusätzlichen Festplattenspeicher hinzufügen, damit die Protokollierung wiederhergestellt werden kann.

Wenn Ihr Datenbankadministrator für SQL Server die Größe einer einzelnen Datenbank innerhalb von Microsoft SQL Server begrenzt hat, führen Sie einen der folgenden Schritte aus:

- Bitten Sie Ihren Datenbankadministrator für SQL Server, die zulässige Größe zu erhöhen.
- Finden Sie die maximal zulässige Größe heraus und wechseln Sie zu **Einstellungen > Berichterstellung > Protokolldatenbank**, um die Protokolldatenbank so zu konfigurieren, dass sie ein Rollover vornimmt, sobald etwa 90 % der Maximalgrößer erreicht sind. Siehe *Konfiguration von Rollover-Optionen*, Seite 344.

Wenn Ihre IT-Abteilung eine maximal zulässige Größe für den Festplattenspeicher für SQL Server-Vorgänge festgelegt hat, wenden Sie sich an den zuständigen Mitarbeiter.

Aktualisieren des Passworts für die Log Server-Verbindung

Wenn Sie das Passwort für das Konto ändern, das die Websense-Software zum Herstellen einer Verbindung mit der Protokolldatenbank verwendet, müssen Sie Log Server ebenfalls für die Verwendung des neuen Passworts aktualisieren.

1. Wechseln Sie auf dem Log Server-Computer zu **Start > Alle Programme > Websense > Dienstprogramme > Konfiguration von Log Server**. Das Dienstprogramm für die Konfiguration von Log Server wird geöffnet.
2. Klicken Sie auf die Registerkarte **Datenbank** und stellen Sie sicher, dass die korrekte Datenbank (standardmäßig **wslogdb70**) im Feld "ODBC-Datenquellenname (DSN)" angezeigt wird.
3. Klicken Sie auf **Verbindung**. Das Dialogfeld "Datenquelle auswählen" wird geöffnet.
4. Klicken Sie auf die Registerkarte **Computer-Datenquelle** und doppelklicken Sie anschließend auf **wslogdb70** (oder den Namen Ihrer Protokolldatenbank). Das Dialogfeld für die SQL Server-Anmeldung wird geöffnet.
5. Stellen Sie sicher, dass das Feld für die Anmelde-ID den richtigen Kontonamen enthält (in der Regel **sa**), und geben Sie das neue Passwort ein.
6. Klicken Sie auf **OK** und anschließend im Dialogfeld "Konfiguration von Log Server" auf **Anwenden**.
7. Klicken Sie auf die Registerkarte **Verbindung**. Beenden Sie Log Server und starten Sie das Programm anschließend neu.
8. Wenn Log Server wieder ausgeführt wird, klicken Sie auf **OK**, um das Dienstprogramm zu schließen.

Konfigurieren von Benutzerberechtigungen für Microsoft SQL Server 2005

Microsoft SQL Server 2005 definiert die Rollen von SQL Server Agent, denen die Zugreifbarkeit auf die Job-Grundstruktur unterliegt. Die Jobs von SQL Server Agent für SQL Server 2005 sind in der msdb-Datenbank von SQL Server gespeichert.

Damit Websense Log Server erfolgreich installiert werden kann, muss das Benutzerkonto, dem die Websense-Datenbank angehört, Mitglied in einer der folgenden Rollen der msdb-Datenbank sein:

- SQLAgentUserRole
- Rolle "SQLAgentReader"
- Rolle "SQLAgentOperator"

> **Hinweis**
> Das SQL-Benutzerkonto muss zusätzlich Mitglied der festen Serverrolle *DBCreator* sein.

Öffnen Sie Microsoft SQL Server 2005, um dem Benutzerkonto von SQL Server die erforderlichen Berechtigungen für die erfolgreiche Installation der Websense-Berichterstellungskomponenten zu gewähren.

1. Navigieren Sie auf dem Computer mit SQL Server zu **Start > Alle Programme > Microsoft SQL Server 2005 > Microsoft SQL Server Management Studio**.
2. Wählen Sie das Verzeichnis **Objekt-Explorer**.
3. Wählen Sie **Sicherheit > Anmeldungen**.
4. Wählen Sie das Anmeldekonto, das für die Installation verwendet wurde.
5. Klicken Sie mit der rechten Maustaste auf das Anmeldekonto, und wählen Sie für diesen Benutzer **Eigenschaften** aus.
6. Wählen Sie **Benutzerzuordnung** aus, und fahren Sie folgendermaßen fort:
   a. Wählen Sie bei der Datenbankzuordnung **msdb** aus.
   b. Gewähren Sie die Mitgliedschaft zu einer der folgenden Rollen:
      - SQLAgentUserRole
      - Rolle "SQLAgentReader"
      - Rolle "SQLAgentOperator"
   c. Klicken Sie auf **OK**, um zu speichern.
7. Wählen Sie **Serverrollen** und danach **dbcreator** aus. Die Rolle "dbcreator" wird erstellt.
8. Klicken Sie auf **OK**, um zu speichern.

Log Server kann keine Verbindung zum Verzeichnisdienst herstellen

Wenn einer der unten aufgelisteten Fehler auftritt, kann Log Server nicht auf den Verzeichnisdienst zugreifen, der für das Aktualisieren der Benutzer-Gruppen-Zuordnungen für die Berichte erforderlich ist. Diese Fehler werden in der Ereignisanzeige von Windows angezeigt (siehe *Die Ereignisanzeige von Windows*, Seite 423).

- EVENT ID:4096 - Directory Service kann nicht initialisiert werden. Möglicherweise ist der Websense-Server nicht verfügbar oder nicht erreichbar.
- EVENT ID:4096 - Es konnte keine Verbindung zum Verzeichnisdienst hergestellt werden. Die Gruppen für diesen Benutzer werden zum jetzigen Zeitpunkt nicht aufgelöst. Stellen Sie sicher, dass dieser Prozess auf den Verzeichnisdienst zugreifen kann.

Die häufigste Ursache ist die, dass sich Websense Log Server und Websense User Service auf verschiedenen Seiten einer Firewall befinden, die den Zugriff beschränkt.

Um dieses Problem zu beheben, konfigurieren Sie die Firewall so, dass der Zugriff über die für die Kommunikation zwischen diesen Komponenten verwendeten Ports gestattet ist.

Die Daten der Berichte über Navigationsdauern im Internet sind verfälscht

Beachten Sie, dass durch Konsolidierung die Daten der Berichte über Navigationsdauern im Internet verfälscht werden können. Diese Berichte zeigen die Dauer an, während der die Benutzer auf das Internet zugreifen. Sie können Angaben über die Dauer des Zugriff auf jede einzelne Website enthalten. Die Navigationsdauer im Internet wird mithilfe eines spezielle Algorithmus berechnet. Durch eine Konsolidierung kann die Genauigkeit der Berechnungen für diese Berichte beeinträchtigt werden.

Die Bandbreite ist größer als erwartet

Einige Websense-Integrationen, jedoch nicht alle, stellen Informationen zur Bandbreite bereit. Wenn Ihre Integration keine Angaben zur Bandbreite bereitstellt, können Sie Network Agent so konfigurieren, dass die Protokollierung unter Einbeziehung der Daten zur Bandbreite erfolgt.

Wenn ein Benutzer einen zulässigen Datei-Download anfordert, sendet das Integrationsprodukt oder Network Agent die gesamte Dateigröße, die von der Websense-Software in Form von empfangenen Bytes protokolliert wird.

Wenn der Benutzer den Download-Vorgang abbricht oder wenn die Datei nicht vollständig heruntergeladen wird, entspricht der Wert der empfangenen Bytes in der Protokolldatenbank dennoch der gesamten Dateigröße. In einem solchen Fall ist der

angegebene Wert der empfangenen Bytes größer als die tatsächliche Anzahl der empfangenen Bytes.

Dies hat Auswirkungen auf die Werte der Bandbreite, die aus einer Kombination aus empfangenen und gesendeten Bytes bestehen.

Einige Protokollanfragen werden nicht protokolliert

Einige Protokolle, wie die von ICQ und AOL verwendeten Protokolle, fordern Benutzer zur Anmeldung bei einem Server unter Angabe einer IP-Adresse auf und senden dann eine andere IP-Adresse und Portnummer für Nachrichtenzwecke an den Client. In diesem Fall können sämtliche gesendeten und empfangenen Nachrichten nicht von Websense Network Agent überwacht und protokolliert werden, da der Nachrichtenserver zum Zeitpunkt des Nachrichtenaustauschs nicht bekannt ist.

Daher kann es vorkommen, dass die Anzahl der protokollierten Anfragen nicht der Anzahl der tatsächlich gesendeten Anfragen entspricht. Dies hat Auswirkungen auf die Genauigkeit der von den Websense Reporting Tools erstellten Berichte.

Alle Berichte sind leer

Wenn für keinen Ihrer Berichte Daten vorliegen, stellen Sie Folgendes sicher:

- Die aktiven Datenbankpartitionen enthalten Informationen zu den in den Berichten enthaltenen Datumsangaben. Siehe *Datenbankpartitionen*, Seite 418.
- Der SQL Server Agent-Job in Microsoft SQL Server oder MSDE ist aktiv. Siehe *SQL Server Agent-Job*, Seite 419.
- Log Server ist derzeit so eingestellt, dass Protokollinformationen von Filtering Service empfangen werden. Siehe *Konfiguration von Log Server*, Seite 419.

Datenbankpartitionen

Die Websense-Protokolldateien werden in Partitionen innerhalb der Datenbank gespeichert. Neue Partitionen können basierend auf Größe oder Datum erstellt werden, je nach Datenbankmodul und Konfiguration.

Sie können einzelne Partitionen in Websense Manager aktivieren oder deaktivieren. Wenn Sie versuchen, Berichte basierend auf Informationen zu erstellen, die in deaktivierten Partitionen gespeichert sind, werden keine Informationen erkannt und der Bericht ist leer.

So stellen Sie sicher, dass die richtigen Datenbankpartitionen aktiv sind:

1. Wechseln Sie zu **Einstellungen > Berichterstellung > Protokolldatenbank**.
2. Scrollen Sie nach unten bis zum Abschnitt **Verfügbare Partitionen**.
3. Markieren Sie das Kontrollkästchen **Aktivieren** für jede Partition, die Daten enthält, die Sie in den Berichten berücksichtigen möchten.
4. Klicken Sie auf **Jetzt speichern**, um die Änderungen zu übernehmen.

SQL Server Agent-Job

Möglicherweise wurde der SQL Server Agent-Datenbankjob deaktiviert. Der Job muss ausgeführt werden, damit die Protokolle vom ETL-Datenbankjob in der Datenbank verarbeitet werden.

Wenn Sie MSDE verwenden:

1. Wechseln Sie zu **Start > Verwaltung > Dienste**.
2. Stellen Sie sicher, dass sowohl SQL Server als auch SQL Server Agent ausgeführt werden. Wenn Sie MSDE über Websense, Inc. erworben haben, lauten die Namen dieser Dienste MSSQL$WEBSENSE und SQLAgent$WEBSENSE.

Wenn Sie die Vollversion von Microsoft SQL Server ausführen, wenden Sie sich an Ihren Datenbankadministrator, um sicherzustellen, dass der SQL Server Agent-Job ausgeführt wird.

Konfiguration von Log Server

Die Konfigurationseinstellungen müssen sowohl in Websense Manager als auch in Log Server korrekt sein, damit sichergestellt ist, dass Log Server Protokollinformationen von Filtering Service empfängt. Andernfalls werden Protokolldaten niemals in der Protokolldatenbank verarbeitet.

Stellen Sie zunächst sicher, dass Websense Manager erfolgreich eine Verbindung zu Log Server herstellen konnte.

1. Melden Sie sich bei Websense Manager unter Verwendung der Berechtigungen eines übergeordneten Administrators (Super Administrator) an, für den keine Bedingungen gelten.
2. Wechseln Sie zu **Einstellungen > Allgemein > Protokollierung**.
3. Geben Sie den **Computernamen** oder die **IP-Adresse** des Geräts ein, auf dem Log Server installiert ist.
4. Geben Sie den **Port** ein, an dem Log Server lauscht (standardmäßig 55805).
5. Klicken Sie auf **Status prüfen**, um festzustellen, ob Websense Manager mit dem angegebenen Log Server kommunizieren kann.

   Eine Meldung gibt ab, ob der Verbindungstest erfolgreich war. Aktualisieren Sie ggf. die IP-Adresse oder den Computernamen und Port, bis der Test erfolgreich ist.
6. Wenn Sie fertig sind, klicken Sie auf **OK**, um die Änderungen im Cache zwischenzuspeichern. Die Änderungen werden erst gültig, wenn Sie auf **Alles speichern** geklickt haben.

Überprüfen Sie nun die Einstellungen im Dienstprogramm für die Konfiguration von Log Server.

1. Wechseln Sie auf dem Log Server-Computer zu **Start > Programme > Websense > Dienstprogramme > Log Server - Konfiguration**.
2. Überprüfen Sie auf der Registerkarte **Verbindungen**, ob der Port dem Wert in Websense Manager entspricht.

3. Klicken Sie auf **OK**, um eventuelle Änderungen zu speichern.
4. Verwenden Sie die Schaltfläche auf der Registerkarte **Verbindungen**, um Log Server zu beenden und neu zu starten.
5. Klicken Sie auf **Beenden**, um das Dienstprogramm für die Konfiguration von Log Server zu schließen.

Auf der Seite "Heute" oder "Verlauf" werden keine Diagramme angezeigt

Wenn in Ihrer Organisation die delegierte Verwaltung verwendet wird, überprüfen Sie die Berechtigungen für die Berichterstellung hinsichtlich der Rolle des delegierten Administrators. Wenn die Option **Anzeigen von Berichten auf den Seiten "Heute" und "Verlauf"** nicht aktiviert ist, werden diese Diagramme für delegierte Administratoren mit dieser Rolle nicht angezeigt.

In Umgebungen mit mehreren Policy Server-Instanzen, wird Log Server für die Kommunikation mit nur einem Policy Server installiert. Sie müssen sich bei diesem Policy Server anmelden, um die Diagramme auf den Seiten "Heute" und "Verlauf" anzeigen oder auf andere Berichtsfunktionen zugreifen zu können.

Ich kann auf bestimmte Berichtsfunktionen nicht zugreifen

Wenn für Ihren Webbrowser die Einstellungen zum Blockieren von Popups auf eine sehr hohe Sicherheitsstufe festgelegt sind, sind bestimmte Berichtsfunktionen möglicherweise gesperrt. Um diese Funktionen zu verwenden, müssen Sie die Sicherheitseinstellungen für das Blockieren auf eine niedrigere Stufe setzen oder das Blockieren von Popups vollständig deaktivieren.

Bei der Microsoft Excel-Ausgabe fehlen einige Berichtsdaten

Die größtmögliche Anzahl an Zeilen, die in einer Microsoft Excel-Tabelle geöffnet werden können, beträgt 65.536. Wenn Sie einen Bericht mit mehr als 65.536 Datensätzen in das Microsoft Excel-Format exportieren, sind alle Datensätze ab dem 65.537. Eintrag nicht in der Tabelle enthalten.

Um sicherzustellen, dass Sie auf alle Informationen im exportierten Bericht zugreifen können, führen Sie einen der folgenden Schritte aus:

- Bearbeiten Sie bei Präsentationsberichten den Berichtsfilter, um eine kleinere Berichtsgröße einzustellen, beispielsweise indem Sie einen kleineren Datenbereich festlegen und weniger Benutzer und Gruppen oder weniger Aktionen auswählen.
- Wählen Sie bei Untersuchungsberichten detailliertere Daten aus, um einen kleineren Bericht festzulegen.
- Wählen Sie ein anderes Exportformat.

Speichern von Präsentationsberichten im HTML-Format

Wenn Sie einen Bericht direkt über die Seite "Berichterstellung" > "Präsentationsberichte" erstellen, können Sie aus 3 Anzeigeformaten wählen: HTML, PDF und XLS. Wenn Sie das HTML-Anzeigeformat wählen, können Sie den Bericht im Websense Manager-Fenster anzeigen.

Das Drucken und Speichern von Präsentationsberichten direkt über den Browser ist nicht zu empfehlen. Die Druckausgabe enthält das gesamte Browserfenster und beim Öffnen einer gespeicherten Datei wird Websense Manager gestartet.

Um Berichte auf optimale Weise zu drucken oder zu speichern, wählen Sie PDF oder XLS als Ausgabeformat. Wenn die Anzeigesoftware (Adobe Reader oder Microsoft Excel) auf dem lokalen Computer installiert ist, können Sie diese Dateitypen sofort öffnen. Sie können die Datei auch auf Diskette speichern (wenn keine entsprechende Anzeigesoftware installiert ist, ist dies die einzige verfügbare Option).

Nachdem Sie einen Bericht in Adobe Reader oder Microsoft Excel geöffnet haben, verwenden Sie die Optionen zum Drucken und Speichern dieses Programms, um das gewünschte Ausgabeformat zu erstellen.

Probleme mit dem Durchsuchen von Untersuchungsberichten

Es gibt zwei potenzielle Probleme in Zusammenhang mit dem Durchsuchen von Untersuchungsberichten.

- Erweiterte ASCII-Zeichen können nicht eingegeben werden
- Suchmuster werden möglicherweise nicht gefunden

Erweiterte ASCII-Zeichen

Die Suchfelder über dem Balkendiagramm auf der Hauptseite für Untersuchungsberichte ermöglichen Ihnen, das von Ihnen ausgewählte Diagrammelement nach einem spezifischen Begriff oder einer Textzeichenfolge zu durchsuchen.

Wenn Sie Mozilla Firefox auf einem Linux-Server verwenden, um auf Websense Manager zuzugreifen, können Sie in diese Felder keine erweiterten ASCII-Zeichen eingeben. Dies ist ein bekanntes Problem von Firefox in Kombination mit Linux.

Wenn Sie einen Untersuchungsbericht nach Text durchsuchen, der erweiterte ASCII-Zeichen enthält, greifen Sie über einen Windows-Server auf Websense Manager zu und verwenden Sie einen beliebigen unterstützten Browser.

Suchmuster nicht gefunden

Gelegentlich kann die Komponente für Untersuchungsberichte keine URLs finden, die mit einem Suchmuster verknüpft sind, das in die Suchfelder auf der Hauptseite für Untersuchungsberichte eingegeben wurde. Wenn dieser Fall eintritt und Sie sicher sind, dass das Muster innerhalb der URLs existiert, versuchen Sie es mit der Eingabe eines anderen Musters, das ebenfalls zum Auffinden der gewünschten URLs führen muss.

Allgemeine Probleme mit Untersuchungsberichten

- Einige Abfragen nehmen sehr viel Zeit in Anspruch. Möglicherweise wird ein leerer Bildschirm angezeigt oder Sie erhalten eine Meldung mit dem Hinweis, dass eine Zeitüberschreitung eingetreten ist. Dies kann folgende Ursachen haben:
  - Zeitüberschreitung des Webservers
  - Zeitüberschreitung bei MSDE oder Microsoft SQL Server
  - Zeitüberschreitung des Proxy- oder Caching-Servers

  Möglicherweise müssen Sie die Zeitbegrenzung für diese Komponenten manuell auf einen höheren Wert setzen.
- Wenn Benutzer keiner Gruppe angehören, werden sie auch nicht in einer Domäne angezeigt. Die Auswahlmöglichkeiten für Gruppen und Domänen sind beide inaktiv.
- Auch wenn Log Server keine Hits, sondern Besuche protokolliert, werden diese Informationen von Untersuchungsberichten als **Hits** gekennzeichnet.

Tools zur Fehlerbehebung

- *Das Dialogfeld für die Windows-Dienste*, Seite 422
- *Die Ereignisanzeige von Windows*, Seite 423
- *Die Websense-Protokolldatei*, Seite 423

Das Dialogfeld für die Windows-Dienste

Auf Microsoft Windows-Computern werden Filtering Service, Network Agent, Policy Server, User Service und alle Websense-Agenten für transparente Identifikation als Dienste ausgeführt. Sie können den Status dieser Dienste über das Dialogfeld für die Windows-Dienste überprüfen.

1. Öffnen Sie in der Systemsteuerung von Windows den Ordner **Verwaltung**.
2. Doppelklicken Sie auf **Dienste**.
3. Suchen Sie in der Liste der Dienste nach dem Dienst, für den Sie die Fehlerbehebung ausführen möchten.

   Der Diensteintrag enthält den Dienstnamen, eine kurze Beschreibung, den Status des Dienstes (gestartet oder beendet), Informationen zum Starten des Dienstes und Angaben zum Konto, das der Dienst für seine Aufgaben verwendet.
4. Doppeklicken Sie auf einen Dienstnamen. Es wird ein Dialogfeld mit detaillierten Angaben zum Dienst geöffnet.

Die Ereignisanzeige von Windows

Die Windows Ereignisanzeige zeichnet Fehlermeldungen zu Windows-Ereignissen, einschließlich Dienstaktivitäten, auf. Diese Meldungen können Ihnen dabei helfen, Netzwerk- oder Dienstfehler zu erkennen, die Probleme mit dem Filtern der Internetaktivitäten oder mit der Benutzeridentifikation verursachen können.

1. Öffnen Sie in der Systemsteuerung von Windows den Ordner **Verwaltung**.
2. Doppelklicken Sie auf **Ereignisanzeige**.
3. Klicken Sie in der Ereignisanzeige auf **Anwendung**, um eine Liste der Fehler-, Warn- und Informationsmeldungen aufzurufen.
4. Suchen Sie in der Liste nach Fehler- oder Warnmeldungen von Websense-Diensten.

Die Websense-Protokolldatei

Die Websense-Software schreibt Fehlermeldungen in die Datei **websense.log**, die sich im Websense-Verzeichnis **bin** befindet (standardmäßig C:\Programme\Websense\bin oder /opt/Websense/bin).

Die Informationen in dieser Datei sind mit denen in der Ereignisanzeige von Windows vergleichbar. In Windows-Umgebungen präsentiert die Ereignisanzeige Meldungen in einem etwas benutzerfreundlicheren Format. Die Datei **websense.log** ist jedoch auf Linux-Systemen vorhanden und kann an die technische Unterstützung von Websense gesendet werden, wenn Sie Hilfe beim Beheben eines Problems benötigen.

Index

B

C

D

G

H

I

J

K

L

M

N

O

P

Q

R

T

U

V

W

X

Z