

9.0 **Worry-Free™**

Business Security

Standard- und Advanced-Versionen

Service Pack 1

Installations- und Upgrade-Handbuch

Securing Your Journey to the Cloud



Protected Cloud



Web Security

Trend Micro Deutschland GmbH behält sich das Recht vor, Änderungen an diesem Dokument und den hierin beschriebenen Produkt ohne Vorankündigung vorzunehmen. Lesen Sie vor der Installation und Verwendung von Produkt die Readme-Dateien, die Anmerkungen zu dieser Version und/oder die neueste Version der auf der Trend Micro Website verfügbaren Dokumentation durch:

<http://docs.trendmicro.com/de-de/smb/worry-free-business-security.aspx>

Trend Micro, das Trend Micro T-Ball-Logo, TrendProtect, TrendSecure, Worry-Free, OfficeScan, ServerProtect, PC-cillin, InterScan und ScanMail sind Marken oder eingetragene Marken von Trend Micro Deutschland GmbH. Alle anderen Produkt- oder Firmennamen können Marken oder eingetragene Marken ihrer Eigentümer sein.

Copyright © 2014. Trend Micro Deutschland GmbH. Alle Rechte vorbehalten.

Dokument-Nr.: WFGM96728/141021

Release-Datum: September 2014

Geschützt durch U.S. Patent-Nr.: 5,951,698 und 7,188,369

Diese Dokumentation enthält eine Beschreibung der wesentlichen Funktionen von Produkt und/oder Installationsanweisungen für eine Produktionsumgebung. Lesen Sie die Dokumentation vor der Installation und Verwendung von Produkt.

Detaillierte Informationen zur Verwendung bestimmter Funktionen in Produkt können Sie in der Trend Micro Online-Hilfe und/oder der Trend Micro Knowledge Base finden.

Trend Micro ist stets bemüht, die Dokumentation zu verbessern. Setzen Sie sich mit uns in Verbindung, wenn Sie Fragen, Kommentare oder Vorschläge zu diesem oder einem anderen Trend Micro Dokument haben: docs@trendmicro.com.

Bewerten Sie diese Dokumentation auf der folgenden Website:

<http://www.trendmicro.com/download/documentation/rating.asp>

Inhaltsverzeichnis

Vorwort

Vorwort	v
Worry-Free Business Security Dokumentation	vi
Zielpublikum	vi
Textkonventionen	vii

Kapitel 1: Installation und Upgrade vorbereiten

Produktversionen	1-2
Lizenzen, Registrierung und Aktivierung	1-3
Das Worry-Free Business Security Netzwerk	1-5
Security Server	1-5
Agents	1-7
Webkonsole	1-8

Kapitel 2: Den Security Server installieren

Voraussetzungen für Installation und Upgrade	2-2
Überlegungen zur Installation des Security Servers	2-2
IPv6-Voraussetzungen für den Security Server	2-2
Standort des Security Servers	2-3
Anzahl der Clients	2-4
Netzwerkverkehr	2-4
Dedizierter Server	2-6
Kompatibilitätsprobleme	2-6
WFBS Ports	2-7
Installations-Checkliste	2-9
Den Security Server installieren	2-13
Phase 1: Security Server Installation starten	2-15
Phase 2: Einstellungen gemäß Setup-Typ konfigurieren	2-24

Einstellungen für eine typische Installation oder eine Minimalinstallation konfigurieren	2-24
Einstellungen für eine benutzerdefinierte Installation konfigurieren	2-29
Phase 3: Installation	2-51
Mehrere Security Server mit der unbeaufsichtigten Installation installieren	2-55
Eine Installationssitzung aufnehmen	2-55
Die unbeaufsichtigte Installation starten	2-57
Die Installation überprüfen	2-57

Kapitel 3: Upgrades für Security Server und Agents

Voraussetzungen für Installation und Upgrade	3-2
Überlegungen zum Upgrade	3-2
IPv6-Voraussetzungen für Upgrades	3-2
Bewährte Upgrade-Methoden	3-3
Upgrades der Vorgängerversion	3-4
Upgrade-Methode 1: Upgrade mit dem Installationspaket	3-5
Upgrade-Methode 2: Agents nach Security Server 9.0 SP1 verschieben	3-9
Vollversion-Upgrades oder Advanced Edition Upgrades	3-11
Vollversion-Upgrade oder Advanced Edition Upgrade	3-12

Anhang A: Hilfe anfordern

Die Knowledge Base von Trend Micro	A-2
Kontaktaufnahme mit dem technischen Support	A-2
Case Diagnostic Tool	A-3
Support-Anfrage beschleunigen	A-3
Kontaktinformationen	A-4
Verdächtige Dateien an Trend Micro senden	A-4
Sicherheitsinformationen	A-4
TrendLabs	A-5

Anregungen und Kritik	A-5
-----------------------------	-----

Stichwortverzeichnis

Stichwortverzeichnis	IN-1
----------------------------	------

Vorwort

Vorwort

Willkommen beim *Installations- und Upgrade-Handbuch* für Trend Micro™ Worry-Free™ Business Security. In diesem Dokument finden Sie die Voraussetzungen und Verfahren für:

- Den Security Server installieren
- Upgrades für Security Server und Agents

Weitere Informationen zur Installation von Agents finden Sie im *Administratorhandbuch*.

Worry-Free Business Security Dokumentation

Die Worry-Free Business Security Dokumentation umfasst folgende Komponenten:

TABELLE 1. Worry-Free Business Security Dokumentation

DOKUMENTATION	BESCHREIBUNG
Installations- und Upgrade-Handbuch	Ein PDF-Dokument, in dem Anforderungen und Verfahren zum Installieren des Security Servers sowie zum Upgrade des Servers und der Agents beschrieben werden
Administratorhandbuch	Ein PDF-Dokument mit folgenden Inhalten: Informationen über die ersten Schritte, Verfahren zur Client-Installation sowie Security Server- und Client-Verwaltung
Hilfe	Im WebHelp- oder CHM-Format erstellte HTML-Dateien, die Anleitungen, allgemeine Benutzerhinweise und feldspezifische Informationen enthalten.
Readme-Datei	Enthält eine Liste bekannter Probleme und grundlegende Installationshinweise. Die Datei kann auch neueste Produktinformationen enthalten, die noch nicht in der Hilfe oder in gedruckter Form zur Verfügung stehen.
Knowledge Base	Eine Online-Datenbank mit Informationen zur Problemlösung und Fehlerbehebung. Sie enthält die aktuellsten Hinweise zu bekannten Softwareproblemen. Die Knowledge Base finden Sie im Internet unter folgender Adresse: http://esupport.trendmicro.com

Die neuesten Versionen der PDF-Dateien und der Readme-Datei können Sie hier herunterladen:

<http://docs.trendmicro.com/de-de/smb/worry-free-business-security.aspx>

Zielpublikum

Die Worry-Free Business Security Dokumentation richtet sich an folgende Benutzer:

- **Security Administratoren:** Für die Verwaltung von Worry-Free Business Security verantwortlich, einschließlich Security Server und Agent Installation und Verwaltung. Es wird davon ausgegangen, dass diese Benutzer über umfassende Kenntnisse über Netzwerke und Server-Verwaltung verfügen.
- **Endbenutzer:** Benutzer, auf deren Computer der Security Agent installiert ist. Die Computerkenntnisse dieser Benutzergruppe reichen vom Anfänger bis zum erfahrenen Anwender.

Textkonventionen

Damit Sie Informationen leicht finden und einordnen können, werden in der Worry-Free Business Security Dokumentation folgende Konventionen verwendet:

TABELLE 2. Textkonventionen

KONVENTION	BESCHREIBUNG
NUR GROSSBUCHSTABEN	Akronyme, Abkürzungen und die Namen bestimmter Befehle sowie Tasten auf der Tastatur
Fettdruck	Menüs und Menübefehle, Befehlsschaltflächen, Registerkarten, Optionen und Tasks
<i>Kursivdruck</i>	Referenzen zu anderen Dokumenten oder neuen technischen Komponenten
<Text>	Text in spitzen Klammern soll durch Benutzerangaben ersetzt werden. Beispiel: C:\Programme\<Dateiname> kann C:\Programme\beispiel.jpg sein.
 Hinweis	Enthält Konfigurationshinweise oder -empfehlungen
 Tipp	Enthält Angaben zu bewährten Methoden und Trend Micro Empfehlungen
 Warnung!	Enthält Warnungen zu Vorgängen, die Computern im Netzwerk schaden können

Kapitel 1

Installation und Upgrade vorbereiten

In diesem Kapitel werden die nötigen Vorbereitungen für die Installation und Upgrades von **Worry-Free™ Business Security** beschrieben.

Produktversionen

Trend Micro bietet Ihnen die folgenden Versionen:

- Worry-Free Business Security **Standard**: Zum Schutz von Clients (Desktops, Laptops und Servern) in Ihrem lokalen Netzwerk. Die Version enthält die Komponenten Ausbruchsschutz, Firewall und Virensuche/Spyware-Suche. Im Lieferumfang enthalten sind außerdem technischer Support, Malware-/Viren-Pattern-Dateidownloads, Echtzeitsuche und Programm-Updates für ein Jahr.
- Worry-Free Business Security **Advanced**: Zum Schutz der Clients und Microsoft Exchange Server in Ihrem Netzwerk. Neben den Komponenten von Worry-Free Business Security Standard umfasst diese Version die Komponenten Anti-Spam, Content-Filter, Prävention vor Datenverlust und Sperren von Anhängen.

Die folgende Tabelle enthält die Funktionen, die in jeder einzelnen Version unterstützt werden.

TABELLE 1-1. Verfügbare Funktionen nach Produktversion

FUNKTIONEN	WORRY-FREE BUSINESS SECURITY STANDARD	WORRY-FREE BUSINESS SECURITY ADVANCED
Komponenten-Updates	Ja	Ja
Gerätesteuerung	Ja	Ja
Virenschutz/Anti-Spyware	Ja	Ja
Firewall	Ja	Ja
Web Reputation	Ja	Ja
URL-Filter	Ja	Ja
Verhaltensüberwachung	Ja	Ja
Benutzer-Tools	Ja	Ja
Mail Scan (POP3)	Ja	Ja
Anti-Spam (POP3)	Ja	Ja

FUNKTIONEN	WORRY-FREE BUSINESS SECURITY STANDARD	WORRY-FREE BUSINESS SECURITY ADVANCED
Mail Scan (IMAP)	Nein	Ja
Anti-Spam (IMAP)	Nein	Ja
Content-Filter für E-Mail-Nachrichten	Nein	Ja
Schutz vor Datenverlust in E-Mail-Nachrichten	Nein	Ja
Sperren von Anhängen	Nein	Ja

Lizenzen, Registrierung und Aktivierung

Beim Kauf von Worry-Free Business Security erhalten Sie eine Lizenz für das Produkt/die Produkte und einen Standard-Wartungsvertrag. Der Standard-Wartungsvertrag zwischen Ihrem Unternehmen und Trend Micro regelt, in welchem Umfang Sie nach Zahlung der entsprechenden Gebühren Anrecht auf den Erhalt von technischem Support und Produkt-Updates haben.

Eine Lizenz für die Trend Micro Software enthält üblicherweise das Recht auf Produkt- und Pattern-Datei-Updates und grundlegenden technischen Support für ein (1) Jahr ab Kaufdatum. Nach dem ersten Jahr müssen Sie den Wartungsvertrag jährlich zu den jeweils aktuellen Trend Micro-Wartungsgebühren aktualisieren.



Hinweis

Der Wartungsvertrag läuft ab, Ihre Lizenzvereinbarung jedoch nicht. Auch nach Ablauf des Wartungsvertrags kann eine Virensuche durchgeführt werden. Allerdings können Sie die Malware-/Viren-Pattern-Dateien, die Scan Engine und die Programmdateien nicht mehr aktualisieren (auch nicht manuell). Ebenso endet ab diesem Zeitpunkt Ihr Anspruch auf technischen Support von Trend Micro.

Registrieren und aktivieren Sie Ihre Lizenz für Worry-Free Business Security, um den vollständigen Funktionsumfang des Produkts zu aktivieren.

Registrierungsschlüssel

Beim Kauf von Worry-Free Business Security erhalten Sie zudem einen Registrierungsschlüssel. Dieser besteht aus 22 Zeichen (inklusive Bindestrichen) und hat das folgende Format:

XX-XXXX-XXXXX-XXXXX-XXXXX

Mit diesem lizenzierten Registrierungsschlüssel können Sie Worry-Free Business Security auf der Trend Micro Website unter <https://clp.trendmicro.com> registrieren.

Aktivierungscode

Nach der Registrierung erhalten Sie per E-Mail einen lizenzierten Aktivierungscode. Ein Aktivierungscode besteht aus 37 Zeichen (inklusive Bindestrichen) und sieht folgendermaßen aus:

XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Während der Installation des Security Servers geben Sie den Aktivierungscode ein, sobald Sie dazu aufgefordert werden. Wenn Sie dieses Feld frei lassen, installiert Worry-Free Business Security die 30-tägige Testversion der Software. Führen Sie ein Upgrade für die lizenzierte Vollversion durch, bevor die Testversion ausläuft.

Lizenzstatus

Die folgende Tabelle enthält die Funktionen, die gemäß Lizenzstatus unterstützt werden.

TABELLE 1-2. Lizenzstatus

FUNKTION	LIZENZIERTER VOLLVERSION	TESTLIZENZ (30 TAGE)	ABGELAUFEN
Benachrichtigung über den Lizenzablauf	Ja	Ja	Ja
Komponenten- Updates	Ja	Ja	Nein
Programm-Updates	Ja	Ja	Nein
Technischer Support	Ja	Nein	Nein

FUNKTION	LIZENZIERTE VOLLVERSION	TESTLIZENZ (30 TAGE)	ABGELAUFEN
Echtzeitsuche	Ja	Ja	Ja, aber die Echtzeitsuche verwendet veraltete Komponenten

Wenn der Aktivierungscode einer lizenzierten Vollversion abgelaufen ist, können Sie keine aktuelle Pattern-Datei oder Scan Engine mehr herunterladen. Im Gegensatz zum Aktivierungscode einer Testversion bleiben allerdings auch nach Ablauf des Aktivierungscodes einer lizenzierten Vollversion alle Konfigurationen und anderen Einstellungen wirksam. Dadurch bleibt ein Mindestmaß an Schutz bestehen, falls Sie die Lizenz nicht rechtzeitig verlängert haben.

Die Vollversion von Worry-Free Business Security können Sie durch den erneuten Abschluss eines Wartungsvertrages verlängern. Zur Installation der Vollversionen benötigen Sie einen Aktivierungscode.

Weitere Informationen zur Registrierung finden Sie auf der Trend Micro Support-Website unter:

<http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326>

Das Worry-Free Business Security Netzwerk

Worry-Free Business Security besteht aus Folgendem:

- *Security Server auf Seite 1-5*
- *Agents auf Seite 1-7*
- *Webkonsole auf Seite 1-8*

Security Server

Die zentrale Komponente von Worry-Free Business Security ist der Security Server. Auf dem Security Server befindet sich die Webkonsole, die zentrale webbasierte

Management-Konsole für Worry-Free Business Security. Der Security Server installiert Agents auf den Clients im Netzwerk und stellt eine Agent-Server-Verbindung her. Er ermöglicht das Anzeigen von Informationen über den Sicherheitsstatus und von Agents, das Konfigurieren von Sicherheitsfunktionen und den Komponenten-Download von einem zentralen Speicherort. Außerdem enthält der Security Server die Datenbank, in der Protokolle über die von den Agents berichteten Internet-Bedrohungen gespeichert sind.

Der Security Server hat folgende wichtige Funktionen:

- Er installiert, überwacht und verwaltet die Agents.
- Er lädt von Agents benötigte Komponenten herunter. Standardmäßig lädt der Security Server Komponenten vom Trend Micro ActiveUpdate Server herunter und verteilt diese dann auf die Agents.

Suchserver

Der Sicherheitsserver beinhaltet einen Dienst namens Suchserver, der während der Installation des Security Servers automatisch installiert wird. Daher muss er nicht gesondert installiert werden. Der Suchserver wird unter dem Prozessnamen `iCRCSERVICE.exe` ausgeführt und von der Microsoft Management Console als **Trend Micro Smart Scan-Dienst** angezeigt.

Wenn Security Agents eine Suchmethode mit dem Namen **Smart Scan** verwenden, hilft der Suchserver diesen Agents dabei, die Suchen effizienter auszuführen. Der Smart Scan-Vorgang kann wie folgt beschrieben werden:

- Der Security Agent durchsucht den Client mit Hilfe des **Smart Scan Agent Pattern**, einer abgespeckten Version des herkömmlichen Viren-Pattern, nach Sicherheitsbedrohungen. Das Smart Scan Agent-Pattern beinhaltet die meisten im Viren-Pattern verfügbaren Bedrohungssignaturen.
- Ein Security Agent, der das Risiko der Datei während der Suche nicht ermitteln kann, überprüft dies, indem er eine Suchabfrage an den Suchserver sendet. Der Suchserver überprüft das Risiko mit Hilfe des **Smart Scan-Pattern**, der die Bedrohungssignaturen enthält, die auf dem Smart Scan Agent-Pattern nicht verfügbar sind.

- Der Security Agent legt die Suchabfrageergebnisse des Suchservers zur Verbesserung der Suchleistung in einem Zwischenspeicher ab.

Durch die Bereitstellung einiger Bedrohungsdefinitionen unterstützt der Suchserver die Reduzierung des Bandbreitenverbrauchs des Security Agent beim Herunterladen von Komponenten. Security Agents laden anstatt des Viren-Pattern das Smart Scan Agent-Pattern herunter, das deutlich kleiner ist.

Wenn Security Agents keine Verbindung zum Suchserver aufbauen können, können sie Suchabfragen an das Trend Micro Smart Protection Network senden, das die gleiche Funktion wie der Suchserver hat.

Es ist nicht möglich, den Suchserver separat vom Security Server zu deinstallieren. Wenn Sie den Suchserver nicht verwenden möchten:

1. Öffnen Sie die Microsoft Management Console im Computer Security Server und deaktivieren Sie **Trend Micro Smart Scan Service**.
2. Ändern Sie in der Webkonsole die Einstellung bei Security Agents in herkömmliche Suche, indem Sie zu **Voreinstellungen > Allgemeine Einstellungen > und zur Registerkarte Desktop/Server** navigieren und die Option **Smart Scan Dienst deaktivieren** wählen.

Agents

Agents schützen Clients vor Sicherheitsbedrohungen. Clients umfassen Desktops, Server und Microsoft Exchange Server. Es gibt folgende WFBS Agents:

TABELLE 1-3. WFBS Agents

AGENT	BESCHREIBUNG
Security Agent	Schützt Desktops und Server vor Sicherheitsbedrohungen und Eindringversuchen.
Messaging Security Agent (nur Advanced)	Schützt Microsoft Exchange Server vor Sicherheitsbedrohungen in E-Mails.

Der Agent berichtet an den Security Server, von dem aus er installiert wurde. Damit der Security Server stets über die aktuellen Client-Informationen verfügt, sendet der Agent

Ereignis- und Statusinformationen in Echtzeit. Agents berichten beispielsweise über Ereignisse wie entdeckte Bedrohungen, das Starten und Herunterfahren, den Startzeitpunkt einer Suche oder einen abgeschlossenen Update-Vorgang.

Webkonsole

Die Webkonsole ist die zentrale Stelle zur Überwachung von Clients in Ihrem gesamten Netzwerk. Sie enthält verschiedene Standardeinstellungen und -werte, die Sie entsprechend Ihren Sicherheitsanforderungen und -voraussetzungen konfigurieren können. Die Webkonsole verwendet alle gängigen Internet-Technologien wie Java, CGI, HTML und HTTP.

Verwenden Sie die Webkonsole, um:

- Agents auf Clients zu verteilen.
- Agents zur gleichzeitigen Konfiguration und Verwaltung in logische Gruppen organisieren.
- Produkteinstellungen konfigurieren und die manuelle Suche in einer einzelnen oder mehreren Gruppen starten.
- Benachrichtigungen empfangen und Protokolle zu Bedrohungsaktivitäten einsehen.
- Benachrichtigungen empfangen und Ausbruchswarnungen per E-Mail versenden, wenn Bedrohungen auf Clients entdeckt werden.
- Virenausbrüche durch die Konfiguration und Aktivierung des Ausbruchsschutzes überwachen.

Kapitel 2

Den Security Server installieren

Machen Sie sich vor der Installation des Security Servers mit den Informationen aus diesem Kapitel vertraut.

Voraussetzungen für Installation und Upgrade

Besuchen Sie die folgende Website, um eine vollständige Liste der Systemvoraussetzungen für die Installation und Upgrades zu erhalten:

<http://docs.trendmicro.com/de-de/smb/worry-free-business-security.aspx>

Überlegungen zur Installation des Security Servers

Beachten Sie Folgendes, wenn Sie den Security Server installieren:

- *IPv6-Voraussetzungen für den Security Server auf Seite 2-2*
- *Standort des Security Servers auf Seite 2-3*
- *Anzahl der Clients auf Seite 2-4*
- *Netzwerkverkehr auf Seite 2-4*
- *Dedizierter Server auf Seite 2-6*
- *Kompatibilitätsprobleme auf Seite 2-6*

IPv6-Voraussetzungen für den Security Server

Für den Security Server gelten folgende IPv6-Voraussetzungen:

- Der Server muss auf Windows Server 2008/2012, SBS 2008/2011, 7, 8 oder Vista installiert sein. Er darf nicht auf Windows XP oder Server/SBS 2003 installiert sein, da diese Betriebssysteme die IPv6-Adressierung nur teilweise unterstützen.
- Der Server muss einen IIS Webserver verwenden. Der Apache Webserver unterstützt keine IPv6-Adressierung.
- Wenn der Server IPv4- und IPv6-Agents verwaltet, muss er eine IPv4- wie auch eine IPv6-Adresse haben und über seinen Hostnamen identifiziert werden. Wenn der Server über seine IPv4-Adresse identifiziert wird, können reine IPv6-Agents

keine Verbindung zum Server herstellen. Dasselbe Problem tritt auf, wenn reine IPv4-Clients eine Verbindung mit einem Server herstellen, der über seine IPv6-Adresse identifiziert wird.

- Wenn der Server nur IPv6-Agents verwaltet, ist mindestens eine IPv6-Adresse erforderlich. Der Server kann über seinen Hostnamen oder seine IPv6-Adresse identifiziert werden. Wenn der Server über seinen Hostnamen identifiziert wird, sollte vorzugsweise sein vollqualifizierter Domänenname (FQDN) verwendet werden. Der Grund hierfür ist, dass ein WINS Server in einer reinen IPv6-Umgebung einen Hostnamen nicht in seine entsprechende IPv6-Adresse übersetzen kann.
- Vergewissern Sie sich, dass die IPv6- oder IPv4-Adresse des Host-Computers abgerufen werden kann. Verwenden Sie dazu z. B. den Befehl "ping" oder "nslookup".
- Wenn Sie den Security Server auf einem reinen IPv6-Computer installieren, richten Sie einen Dual-Stack Proxy-Server ein, der zwischen IPv4- und IPv6-Adressen konvertieren kann (wie etwa DeleGate). Platzieren Sie den Proxy-Server zwischen den Security Server und das Internet, damit der Server sich erfolgreich mit den von Trend Micro verwalteten Diensten verbinden kann, z. B. dem ActiveUpdate Server, der Online-Registrierungswebsite und dem Smart Protection Network.

Standort des Security Servers

WFBS kann an unterschiedlichste Netzwerkumgebungen angepasst werden. Sie können beispielsweise eine Firewall zwischen dem Trend Micro Security Server und den Clients errichten, auf denen Security Agent ausgeführt wird, oder sowohl den Trend Micro Security Server als auch die Clients gemeinsam hinter einer Netzwerk-Firewall anordnen.

Wenn Sie mehr als einen Standort verwalten, sollten Sie am Hauptstandort und an jedem verwalteten Standort einen Security Server installieren, damit die Bandbreitennutzung zwischen dem Hauptstandort und den verwalteten Standorten reduziert und die Verteilung der Pattern-Dateien beschleunigt wird.

Ist auf den Clients die Windows Firewall aktiviert, fügt WFBS sie automatisch zur Ausnahmeliste hinzu.



Hinweis

Befindet sich zwischen dem Trend Micro Security Server und den Clients eine Firewall, müssen Sie diese so konfigurieren, dass der Datenverkehr zwischen den Listening-Ports der Clients und des Trend Micro Security Server zugelassen wird.

Anzahl der Clients

Ein Client ist ein Computer, auf dem ein Security Agent oder ein Messaging Security Agent installiert werden soll. Dazu zählen Desktops, Server und Laptops sowie Computer von Außendienst- und Telemitarbeitern.

Eine einzelne Security Server Installation kann bis zu 2.500 Clients verwalten. Bei einer größeren Anzahl Clients sollten Sie mehr als einen Security Server installieren.

Netzwerkverkehr

Wenn der WFBS Server mit den Security Servern und Agents kommuniziert, tritt eine bestimmte Netzwerkauslastung auf.

Der Security Server/Suchserver erzeugt Netzwerkverkehr bei Ausführung der folgenden Aktionen:

- Beim Benachrichtigen der Agents über Konfigurationsänderungen
- Beim Auffordern der Agents zum Download aktualisierter Komponenten
- Bei der Verbindung zum Trend Micro ActiveUpdate Server, um nach aktualisierten Komponenten zu suchen und diese herunterzuladen
- Bei der Reaktion auf Suchabfragen von Agents, die Smart Scan verwenden
- Beim Senden von Feedback an das Trend Micro Smart Protection Network

Agents erzeugen Netzwerkverkehr bei Ausführung der folgenden Aktionen:

- Beim Systemstart
- Beim Herunterfahren des Computers

- Beim Erstellen von Protokollen
- Beim Durchführen zeitgesteuerter Updates
- Beim Durchführen manueller Updates ('Jetzt aktualisieren')
- Bei der Verbindung mit dem Suchserver für Suchabfragen

**Hinweis**

Mit Ausnahme der Updates wirken sich diese Aktionen nur geringfügig auf den Netzwerkverkehr aus.

Netzwerkverkehr während eines Komponenten-Updates

Beim Update von Security Server Komponenten kommt es zu erheblichem Netzwerkverkehr. Um den bei Komponenten-Updates entstehenden Netzwerkverkehr zu verringern, dupliziert Security Server Komponenten. Anstatt bei der Aktualisierung die vollständige Pattern-Datei herunterzuladen, lädt Security Server nur die 'inkrementellen' Pattern (kleinere Versionen der vollständigen Pattern-Datei) herunter und führt diese nach dem Download mit der alten Pattern-Datei zusammen.

Ein regelmäßig aktualisierter Security Server lädt nur das inkrementelle Pattern herunter. Anderenfalls wird die vollständige Pattern-Datei heruntergeladen.

Trend Micro veröffentlicht regelmäßig neue Pattern-Dateien. Darüber hinaus stellt Trend Micro eine neue Pattern-Datei bereit, sobald sich im Umlauf befindliche, schädliche Viren/Malware entdeckt werden.

Update-Agents zur Reduzierung der Bandbreitenauslastung verwenden

Wenn in Ihrem Netzwerk Abschnitte zwischen Security Agents und dem Security Server mit geringer Bandbreite oder mit viel Datenverkehr vorhanden sind, können Sie Security Agents als Update-Adresse (Update-Agents) für andere Agents festlegen. Dadurch wird die Verteilung von Komponenten auf alle Agents optimiert.

Wenn Ihr Netzwerk beispielsweise nach Standorten segmentiert ist und das Datenaufkommen über die Netzwerkverbindung besonders hoch ist, sollten Sie mindestens einen Security Agent pro Segment als Update-Agent einrichten.

Dedizierter Server

Beim Auswählen des Clients, auf dem Sie den WFBS Server hosten, beachten Sie Folgendes:

- Die CPU-Auslastung des Clients
- Andere Aufgaben des Clients

Falls der Ziel-Client noch andere Funktionen zu erfüllen hat, wählen Sie einen anderen Client, auf dem keine kritischen oder ressourcenintensiven Anwendungen ausgeführt werden.

Kompatibilitätsprobleme

Dieser Abschnitt erläutert Kompatibilitätsprobleme, die mit bestimmten Anwendungen anderer Hersteller auftreten können. Weitere Informationen über die Kompatibilität von Programmen anderer Hersteller, die auf einem Computer mit dem Security Server und anderen Worry-Free Komponenten ausgeführt werden, finden Sie in der Dokumentation der jeweiligen Software-Hersteller.

Sonstige Endpunkt-Sicherheitssoftware

Trend Micro empfiehlt, vor der Installation des Security Servers sonstige Endpunkt-Software manuell vom Zielcomputer zu entfernen, da diese die Installation behindern oder die Leistung des Security Servers nach der Installation beeinträchtigen kann.

Sicherheitsanwendungen in Windows SBS und EBS 2008

WFBS ist mit Windows Small Business Server (SBS) 2008 und Windows Essential Business Server (EBS) 2008 kompatibel. Bei einigen Sicherheitsanwendungen, die entweder auf diesen Betriebssystemen installiert sind oder über sie verwaltet werden, kann es jedoch zu Kompatibilitätskonflikten mit WFBS kommen. Daher müssen diese Sicherheitsanwendungen ggf. deinstalliert werden.

Messaging Security Agent und Forefront

Der Messaging Security Agent kann nicht auf Microsoft Exchange Servern mit Forefront (Microsoft Forefront Security for Exchange Server) installiert werden. Deinstallieren Sie Forefront, und stellen Sie sicher, dass Microsoft Exchange Information Store Services vor der Installation des Messaging Security gestartet wurde.

Security Agents und OneCare

Obwohl der Security Server zusammen mit Microsoft Windows Live™ OneCare for Server installiert werden kann, kann der Security Agent nicht mit dem OneCare Client installiert werden. Der Security Agent Installer entfernt OneCare automatisch von den Clients.

Datenbanken

Das Suchen in Datenbanken kann jedoch bei Anwendungen, die auf die Datenbanken zugreifen, zu Leistungseinbußen führen. Daher sollten Datenbanken und deren Sicherungsordner von der Echtzeitsuche ausgeschlossen werden. Erforderliche Suchvorgänge in einer Datenbank sollten manuell oder zeitgesteuert bei geringem Netzaufkommen durchgeführt werden, um die Leistung des Systems so wenig wie möglich zu beeinträchtigen.

Weitere Firewall-Anwendungen

Trend Micro empfiehlt, andere Firewall-Anwendungen vor der Installation der WFBS Firewall zu deinstallieren oder zu deaktivieren, z. B.:

- Windows Internet Connection Firewall (ICF)
- Windows Firewall (WF)

Wenn Sie allerdings ICF oder Firewall-Software anderer Hersteller verwenden möchten, fügen Sie die Trend Micro Security Server Listening-Ports zur Ausschlussliste der Firewall hinzu. (Weitere Informationen über Listening-Ports finden Sie unter [WFBS Ports auf Seite 2-7](#). Informationen über die Konfiguration von Ausschlusslisten finden Sie in Ihrer Firewall-Dokumentation).

WFBS Ports

WFBS verwendet die folgenden Ports:

- **Server-Listening-Port (HTTP-Port):** Für den Zugriff auf den Security Server. Standardmäßig verwendet WFBS einen der folgenden Ports:
 - **Standard-Website des IIS-Servers:** Dieselbe Portnummer wie der TCP-Port Ihres HTTP-Servers.

- **Virtuelle Website des IIS-Servers:** 8059
- **Apache Server:** 8059
- **Client-Listening-Port:** Eine zufällig erstellte Portnummer, über die der Security Agent und Messaging Security Agent Befehle vom Security Server empfängt.

Die Listening-Ports können aber nur während der Installation geändert werden.



Warnung!

Die heutigen Cyberkriminellen gelangen über HTTP-Datenverkehr in das System und leiten ihre Angriffe an die Ports 80 und/oder 8080 weiter. In den meisten Unternehmen werden diese beiden Ports standardmäßig als TCP-(Transmission Control Protocol-)Ports für den HTTP-Datenverkehr verwendet. Falls in Ihrem Unternehmen einer dieser beiden Ports als HTTP-Port verwendet wird, sollte ein anderer Port ausgewählt werden.



Hinweis

Um herauszufinden, welchen Port Ihre Security Agents bei der Verbindung mit dem Suchserver verwenden, öffnen Sie im Ordner, in dem der Server installiert ist, die Datei SSCFG.ini.

- **Ports des Suchservers:** Werden vom Scan Server verwendet, um für Suchabfragen mit Security Agents zu kommunizieren.

TABELLE 2-1. Ports des Suchservers

PORTTYP	IIS-STANDARD	IIS VIRTUAL	VORINSTALLIERT ER APACHE	NEUE APACHE- INSTALLATION
Kein SSL-Port	Kein SSL-Port auf Webserver	Erster offener Port im Bereich 8082 bis 65536	Kein SSL-Port auf Webserver	Kein SSL-Port auf Webserver
SSL-Port SSL verwenden	SSL-Port auf Webserver	Erster offener Port im Bereich 4345 bis 65536	n. v.	SSL-Port auf Webserver

PORTTYP	IIS-STANDARD	IIS VIRTUAL	VORINSTALLIERT ER APACHE	NEUE APACHE- INSTALLATION
SSL-Port SSL nicht verwenden	Erster offener Port im Bereich 4345 bis 65536	Erster offener Port im Bereich 4345 bis 65536	n. v.	Erster offener Port im Bereich 4345 bis 65536

- **Trend Micro Security (für Mac) Kommunikationsport:** Zur Kommunikation des Trend Micro Security (für Mac) Servers mit Mac-Clients. Der Standardport ist 61617.
- **SMTP-Port:** Wird vom Security Server zum Senden von Berichten und Nachrichten per E-Mail an den Administrator verwendet. Der Standardport ist 25.
- **Proxy-Port:** Wird für Verbindungen über einen Proxy-Server verwendet.

Installations-Checkliste

Bei der Installation des Security Servers fordert Sie das Setup-Programm zur Eingabe folgender Informationen auf:

TABELLE 2-2. Installations-Checkliste

INFORMATIONEN	STANDARDWERTE	IHR WERT
Security Server (einschließlich des Suchservers)		
Aktivierungscode	Von Trend Micro zur Verfügung gestellt	
Installationspfad	Einer der folgenden (abhängig vom Betriebssystem): • C:\Programme\Trend Micro\Security Server • C:\Programme (x86)\Trend Micro \Security Server	

INFORMATIONEN	STANDARDWERTE	IHR WERT
Pfad der Suchserver-Datenbank	Entspricht dem Installationspfad des Security Servers (benutzerdefinierbar)	
IPv4/IPv6-Adresse	Benutzerdefiniert	
Vollqualifizierter Domänenname (FQDN)	Benutzerdefiniert	
NetBIOS (Host-) Name	Benutzerdefiniert	
Webserver	Wählen Sie eine Option aus: • Apache • IIS (Standard-Website) • Virtuelle IIS-Website	
Listening-Port (HTTP)	8059	
Listening-Port (HTTPS)	4343	
Kennwort der Web-Konsole	Benutzerdefiniert	
Security Agent Deinstallationskennwort	Benutzerdefiniert	
(Optional) SMTP-Einstellungen für Security Server-Berichte und Benachrichtigungen per E-Mail		
IPv4/IPv6-Adresse	Benutzerdefiniert	
Vollqualifizierter Domänenname (FQDN)	Benutzerdefiniert	
NetBIOS (Host-) Name	Benutzerdefiniert	
Port	25	
Empfänger	Benutzerdefiniert	

INFORMATIONEN	STANDARDWERTE	IHR WERT
(Optional) Proxy-Einstellungen für die Verbindung des Security Servers mit von Trend Micro bereitgestellten Diensten		
IPv4/IPv6-Adresse	Benutzerdefiniert	
Vollqualifizierter Domänenname (FQDN)	Benutzerdefiniert	
NetBIOS (Host-) Name	Benutzerdefiniert	
Benutzername zur Authentifizierung	Benutzerdefiniert	
Authentifizierungskennwort	Benutzerdefiniert	
Security Agents		
Listening-Port	Vom Installationsprogramm zufällig generiert	
Installationspfad	Einer der folgenden (abhängig vom Betriebssystem): • C:\Programme\Trend Micro\Security Agent • C:\Programme (x86)\Trend Micro \Security Agent	
(Optional) Proxy-Authentifizierung für Funktionen des Security Agent (Verhaltensüberwachung, Web Reputation und Smart Scan)		
 Hinweis Security Agents verwenden die in Internet Explorer konfigurierten Proxy-Einstellungen.		

INFORMATIONEN	STANDARDWERTE	IHR WERT
Benutzername zur Authentifizierung	Benutzerdefiniert	
Authentifizierungskennwort	Benutzerdefiniert	
(Optional) Messaging Security Agents		
IPv4/IPv6-Adresse des Microsoft Exchange Servers	Benutzerdefiniert	
Vollqualifizierter Domänenname (FQDN) des Microsoft Exchange Servers	Benutzerdefiniert	
NetBIOS (Host)-Name des Microsoft Exchange Servers	Benutzerdefiniert	
Domänenadministratorkonto und -kennwort für die Anmeldung am Microsoft Exchange Server	Benutzerdefiniert	
Listening-Port	16372	
Installationspfad	Einer der folgenden (abhängig vom Betriebssystem): - C:\Programme\TrendMicro\Messaging Security Agent - C:\Programme(x86)\Trend Micro\Messaging Security Agent	

INFORMATIONEN	STANDARDWERTE	IHR WERT
Temporärer Ordner (die Installationsdateien werden in diesem Ordner entpackt)	C\$	

Den Security Server installieren

Die Installation des Security Servers besteht aus folgenden Phasen:

PHASEN	WICHTIGE AUFGABEN
Phase 1: Security Server Installation starten	• Lesen Sie alle Richtlinien zur Vorbereitung der Installation. • Starten Sie das Installationspaket. • Akzeptieren Sie die Bedingungen der Lizenzvereinbarung. • Wählen Sie einen Setup-Typ. • Typische Installation (empfohlen) • Minimal • Benutzerdefiniert • Geben Sie Ihren Aktivierungscode ein.

PHASEN	WICHTIGE AUFGABEN
Phase 2: Einstellungen gemäß des gewählten Setup-Typs konfigurieren	Konfigurieren Sie die Grundeinstellungen für eine typische Installation oder eine Minimalinstallation, einschließlich: • Installationsspeicherort des Security Servers • Kennwörter für das Administratorkonto • Einstellungen des SMTP-Servers und Empfänger von Benachrichtigungen • Smart Protection Network
	Konfigurieren Sie für eine benutzerdefinierte Installation alle benutzerdefinierbaren Einstellungen, einschließlich: • Grundeinstellungen • Installationsspeicherort des Security Servers • Speicherort der Suchserver-Datenbank • Installation des Security Agents oder Messaging Security Agents auf demselben Computer wie der Security Server oder an einem anderen Installationsort • Einstellungen des Security Servers • Webserver • Kennwort für das Administratorkonto • Einstellungen des SMTP-Servers und Empfänger von Benachrichtigungen • Smart Protection Network • Allgemeine Proxy-Einstellungen • Einstellungen des Security Agents • Security Agent Installationspfad • Zu aktivierende Funktionen des Security Agents • Proxy-Einstellungen für zusätzliche Dienste • Einstellungen des Messaging Security Agents • Einstellungen des Microsoft Exchange Servers • Installationsspeicherort des Messaging Security Agents

PHASEN	WICHTIGE AUFGABEN
Phase 3: Installation	Warten Sie, bis die Installation beendet ist, und schließen Sie das Setup.

Phase 1: Security Server Installation starten

Vorbereitungen

- Melden Sie sich am Computer mit Domänenadministratorrechten oder lokalen Administratorrechten an.
- Schließen Sie vor der Installation von WFBS alle aktiven Anwendungen. Der Installationsvorgang dauert möglicherweise länger, wenn vor der Installation nicht alle Anwendungen geschlossen werden.
- Stellen Sie sicher, dass der Security Server nicht auf einem Computer installiert wird, auf dem aktive Anwendungen den IIS blockieren. Dadurch könnte eine erfolgreiche Installation verhindert werden. Weitere Informationen finden Sie in der Dokumentation des IIS.
- Die Installation des Trend Micro Security Servers erfordert keinen Neustart des Computers. Konfigurieren Sie nach Abschluss der Installation sofort die Einstellungen auf der Webkonsole und fahren Sie anschließend mit der Installation des Security Agents auf den Clients fort.

Installationspaket starten

Doppelklicken Sie auf das Installationspaket (.exe-Datei).

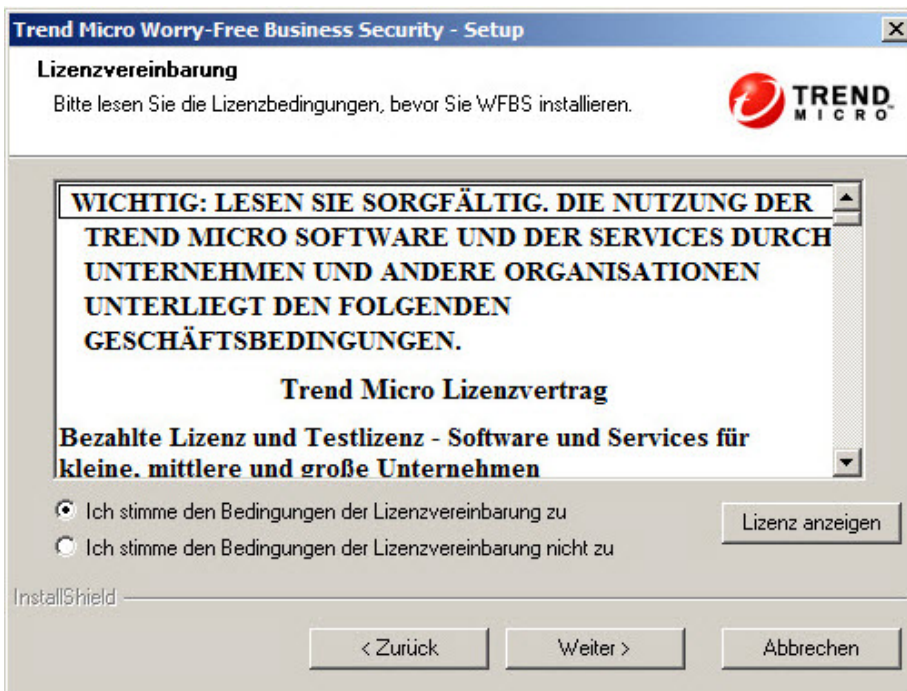


Die Installationsdateien werden in das gleiche Verzeichnis wie die .exe-Datei entpackt. Um den Pfad zu ändern, klicken Sie auf **Durchsuchen** und wählen das neue Verzeichnis aus.

Wenn Sie auf **Start** klicken, wird die Extraktion der Dateien gestartet. Der Entpackstatus wird in der Statusleiste unten im Fenster angezeigt. Wenn das Entpacken abgeschlossen ist, wird das Begrüßungsfenster angezeigt.



Lizenzvereinbarung



Lesen Sie die Lizenzvereinbarung. Wenn Sie sich mit den Bedingungen einverstanden erklären, klicken Sie auf **Ich akzeptiere die Bedingungen der Lizenzvereinbarung**.

Setup-Typ



Wählen Sie eine der folgenden Optionen aus:

Typische Installation (empfohlen)

Diese Methode eignet sich für Security Server, auf denen bis zu 100 Agents verwaltet werden.

Bei einer typischen Installation:

- Die folgenden Funktionen sind nach der Installation automatisch aktiviert:
 - Virenschutz/Anti-Spyware
 - Verhaltensüberwachung (nur auf Desktop-Plattformen wie Windows 7)

- Web Reputation
- URL-Filter
- Intelligente Suche



Hinweis

Security Agents müssen die Mindestsystemvoraussetzungen erfüllen, um Smart Scan auszuführen. Eine Liste der Voraussetzungen erhalten Sie unter <http://docs.trendmicro.com/de-de/smb/worry-free-business-security.aspx>.

- Falls nicht vorhanden, wird der Security Agent automatisch auf dem gleichen Computer wie der Security Server installiert.



Hinweis

Installieren Sie den Security Agent auf andere Clients im Netzwerk und verwalten Sie diese von der Webkonsole aus. Einzelheiten zu den verschiedenen Methoden zur Installation des Security Agents erhalten Sie im Administratorhandbuch.

- Ist eine andere Endpunkt-Sicherheitssoftware auf dem Computer installiert, wird zuerst die Software deinstalliert und anschließend der Security Agent installiert.



Hinweis

Manchmal wird die Endpunkt-Sicherheitssoftware nur erkannt, aber nicht deinstalliert. Deinstallieren Sie in diesem Fall die Software zuerst manuell.

Auf der folgenden Website erhalten Sie eine Liste der Endpunkt-Sicherheitssoftwareprodukte, die deinstalliert oder erkannt, aber nicht deinstalliert werden:

<http://esupport.trendmicro.com/solution/en-US/1060980.aspx>

Minimal Installation

Bei einer Minimalinstallation:

- Nach der Installation ist nur die Virenschutz/Anti-Spyware-Funktion aktiviert.
- Falls nicht vorhanden, wird der Security Agent automatisch auf dem gleichen Computer wie der Security Server installiert.

**Hinweis**

Installieren Sie den Security Agent auf andere Clients im Netzwerk und verwalten Sie diese von der Webkonsole aus. Einzelheiten zu den verschiedenen Methoden zur Installation des Security Agents erhalten Sie im Administratorhandbuch.

- Ist eine andere Endpunkt-Sicherheitssoftware auf dem Computer installiert, wird zuerst die Software deinstalliert und anschließend der Security Agent installiert.

**Hinweis**

Manchmal wird die Endpunkt-Sicherheitssoftware nur erkannt, aber nicht deinstalliert. Deinstallieren Sie in diesem Fall die Software zuerst manuell.

Auf der folgenden Website erhalten Sie eine Liste der Endpunkt-Sicherheitssoftwareprodukte, die deinstalliert oder erkannt, aber nicht deinstalliert werden:

<http://esupport.trendmicro.com/solution/en-US/1060980.aspx>

Benutzerdefinierte Installation

Bei der benutzerdefinierten Installation haben Sie die Flexibilität, Einstellungen für den Security Server und Agents auf Ihre Netzwerksicherheitsstrategie abgestimmt zu konfigurieren. Diese Methode ist geeignet, wenn der Security Server eine große Anzahl von Agents verwalten wird.

Bei einer benutzerdefinierten Installation sind die folgenden Einstellungen **optional**:

- Falls nicht vorhanden, installieren Sie den Security Agent auf dem gleichen Computer wie den Security Server.

**Hinweis**

Installieren Sie den Security Agent auf andere Clients im Netzwerk und verwalten Sie diese von der Webkonsole aus. Einzelheiten zu den verschiedenen Methoden zur Installation des Security Agents erhalten Sie im Administratorhandbuch.

- Ist eine andere Endpunkt-Sicherheitssoftware auf dem Computer installiert, wird zuerst die Software deinstalliert und anschließend der Security Agent installiert.

**Hinweis**

Manchmal wird die Endpunkt-Sicherheitssoftware nur erkannt, aber nicht deinstalliert. Deinstallieren Sie in diesem Fall die Software zuerst manuell.

Auf der folgenden Website erhalten Sie eine Liste der Endpunkt-Sicherheitssoftwareprodukte, die deinstalliert oder erkannt, aber nicht deinstalliert werden:

<http://esupport.trendmicro.com/solution/en-US/1060980.aspx>

- Installieren Sie den Messaging Security Agent auf dem gleichen Computer wie den Security Server (wenn ein Microsoft Exchange Server vorhanden ist) oder auf Remote-Clients.

Produktaktivierung

The screenshot shows the 'Trend Micro Worry-Free Business Security - Setup' window. The title bar is blue with white text. Below the title bar, the window has a light gray background. On the left, the text 'Produktaktivierung' is followed by 'Zur Verwendung von Worry-Free Business Security ist eine Aktivierung erforderlich'. On the right is the Trend Micro logo. Below this, instructions state: 'Geben Sie den Aktivierungscode für vollständigen Schutz ein. Wenn keine Eingabe in dieses Feld erfolgt, wird eine 30-Tage-Testversion installiert.' This is followed by the label 'Aktivierungscode:' and a text input field. Below the input field is a placeholder string of 30 'X' characters. Further down, text explains that users can register online to retrieve their activation code. An 'Online registrieren' button is provided. At the bottom left is the 'InstallShield' logo. At the bottom right are three buttons: '< Zurück', 'Weiter >', and 'Abbrechen'.

Trend Micro Worry-Free Business Security - Setup

Produktaktivierung

Zur Verwendung von Worry-Free Business Security ist eine Aktivierung erforderlich

Geben Sie den Aktivierungscode für vollständigen Schutz ein.

Wenn keine Eingabe in dieses Feld erfolgt, wird eine 30-Tage-Testversion installiert.

Aktivierungscode:

{XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX}

Wenn Sie über einen Registrierungsschlüssel verfügen, registrieren Sie sich online, um Ihren persönlichen Aktivierungscode abzurufen.

InstallShield

Geben Sie im Feld **Aktivierungscode** den Aktivierungscode ein.

Wenn Sie über keinen Aktivierungscode verfügen, haben Sie Ihre Version von WFBS möglicherweise noch nicht registriert. Klicken Sie auf die Schaltfläche **Online registrieren**, um ein neues Browser-Fenster zu öffnen. Folgen Sie den Anweisungen im Fenster 'Registrierung'. Klicken Sie alternativ auf **Weiter**, um die Testversion zu installieren. Wenn Sie Ihre 30-Tage-Testversion noch vor Ablauf auf die Vollversion upgraden, werden alle Programmeinstellungen übernommen.

Überblick über die Installation



Das Fenster 'Überblick über die Installation' zeigt die Komponenten an, die Sie zur Installation von Trend Micro Security Server, des Security Agent oder des Messaging Security Agent konfigurieren müssen.

Nachdem Sie auf **Weiter** geklickt haben:

- Wenn Sie die typische Installation/Minimalinstallation auswählen, gehen Sie wie folgt vor:
 - *Einstellungen für eine typische Installation oder eine Minimalinstallation konfigurieren auf Seite 2-24*
 - *Phase 3: Installation auf Seite 2-51*
- Wenn Sie die benutzerdefinierte Installation auswählen, gehen Sie wie folgt vor:
 - *Einstellungen für eine benutzerdefinierte Installation konfigurieren auf Seite 2-29*
 - *Phase 3: Installation auf Seite 2-51*

Phase 2: Einstellungen gemäß Setup-Typ konfigurieren

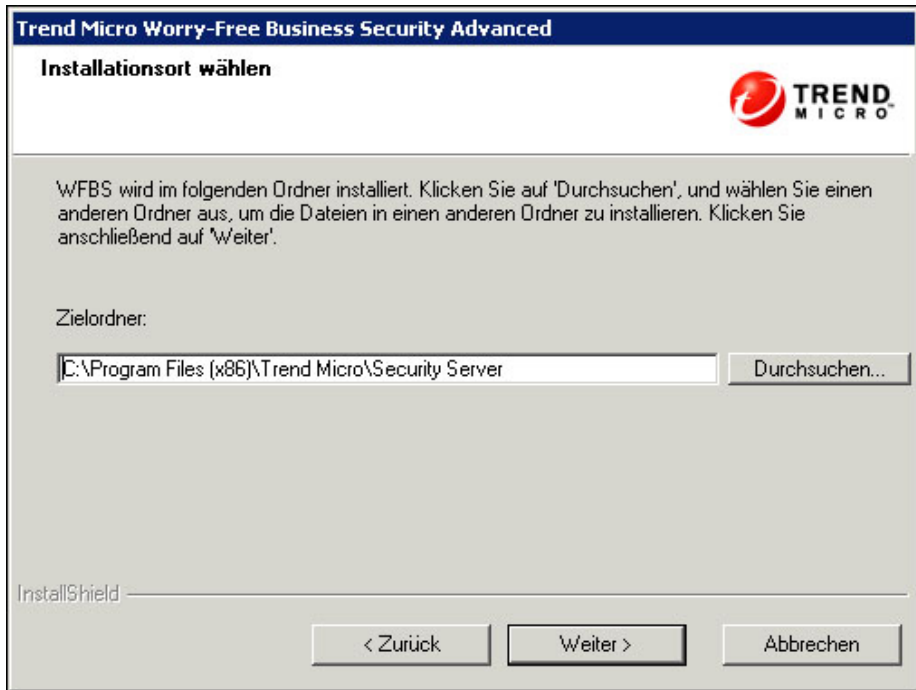
Die in Phase 2 zu konfigurierenden Einstellungen hängen vom Setup-Typ ab, den Sie in Phase 1 auswählen.

- *Einstellungen für eine typische Installation oder eine Minimalinstallation konfigurieren auf Seite 2-24*
- *Einstellungen für eine benutzerdefinierte Installation konfigurieren auf Seite 2-29*

Einstellungen für eine typische Installation oder eine Minimalinstallation konfigurieren

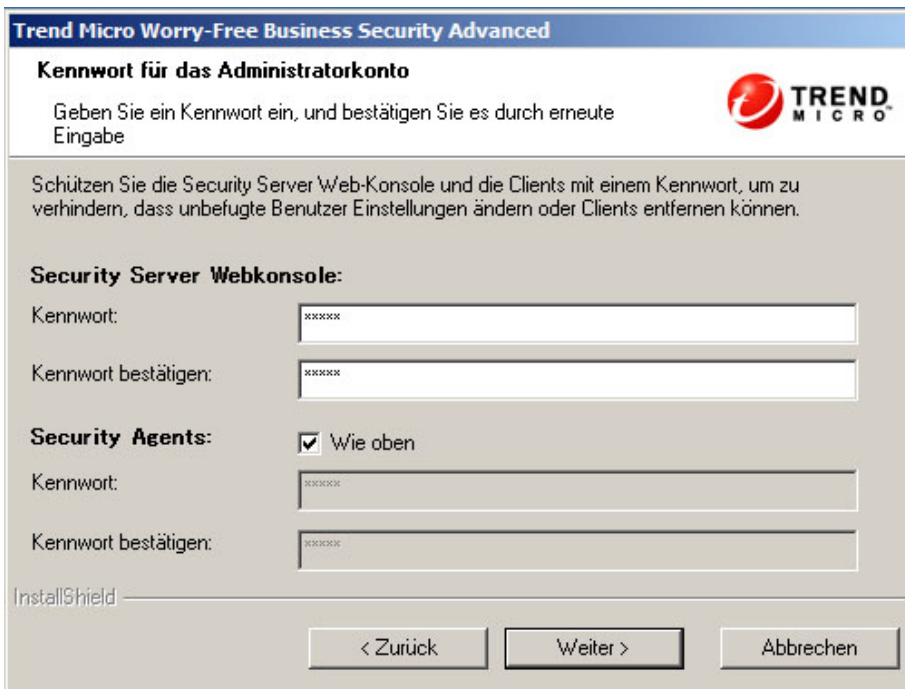
Wenn Sie eine typische Installation oder Minimalinstallation durchführen, werden folgende Fenster der Reihe nach angezeigt:

Installationsspeicherort



Standardmäßig ist als WFBS Installationsordner C:\Programme\Trend Micro\Security Server oder C:\Programme (x86)\Trend Micro\Security Server festgelegt. Klicken Sie auf **Durchsuchen**, wenn Sie WFBS in einem anderen Ordner installieren möchten.

Kennwort für das Administratorkonto



Trend Micro Worry-Free Business Security Advanced

Kennwort für das Administratorkonto

Geben Sie ein Kennwort ein, und bestätigen Sie es durch erneute Eingabe

Schützen Sie die Security Server Web-Konsole und die Clients mit einem Kennwort, um zu verhindern, dass unbefugte Benutzer Einstellungen ändern oder Clients entfernen können.

Security Server Webkonsole:

Kennwort:

Kennwort bestätigen:

Security Agents: ☒ Wie oben

Kennwort:

Kennwort bestätigen:

InstallShield

< Zurück Weiter > Abbrechen

Richten Sie verschiedene Kennwörter für die Security Server Webkonsole und den Security Agent ein.

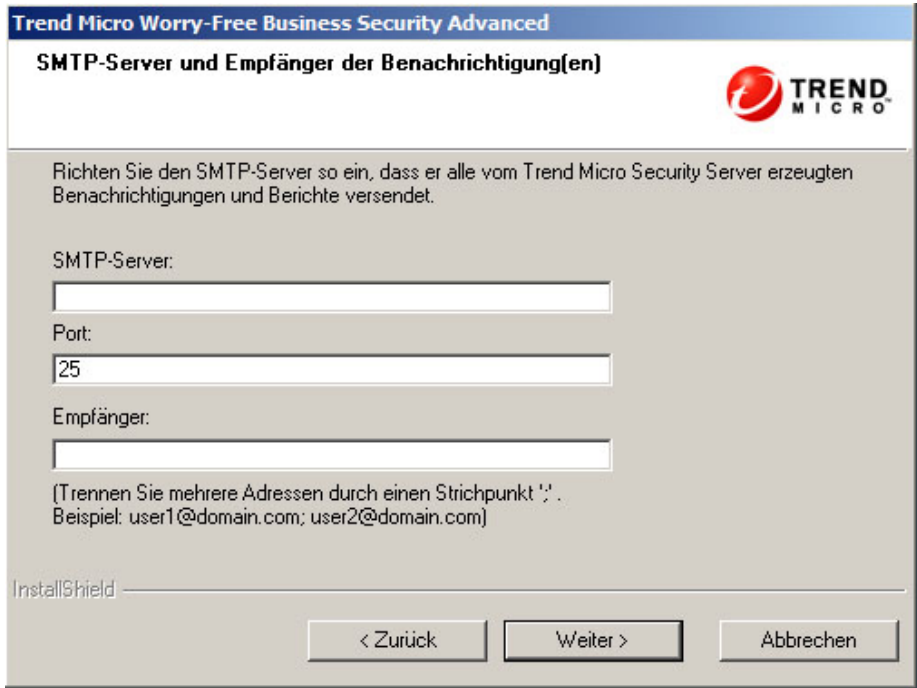
- **Security Server Webkonsole:** Erforderlich für die Anmeldung an der Webkonsole
- **Security Agents:** Erforderlich für die Deinstallation oder das Beenden des Security Agents aus Clients



Hinweis

Das Kennwortfeld erlaubt bis zu 24 Zeichen und unterscheidet zwischen Groß- und Kleinschreibung.

SMTP-Server und Empfänger der Benachrichtigung(en)



Trend Micro Worry-Free Business Security Advanced

SMTP-Server und Empfänger der Benachrichtigung(en)

Richten Sie den SMTP-Server so ein, dass er alle vom Trend Micro Security Server erzeugten Benachrichtigungen und Berichte versendet.

SMTP-Server:

Port:

Empfänger:

(Trennen Sie mehrere Adressen durch einen Strichpunkt ';'.
 Beispiel: user1@domain.com; user2@domain.com)

InstallShield

< Zurück Weiter > Abbrechen

Geben Sie die folgenden Informationen an:

- **SMTP-Server:** Die IP-Adresse des E-Mail-Servers



Hinweis

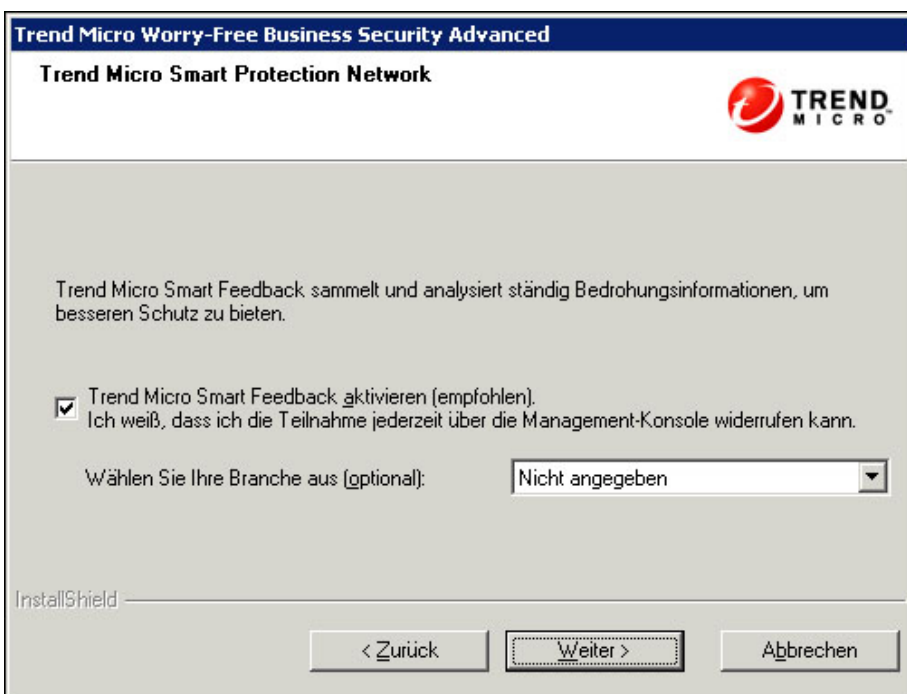
Wenn sich der SMTP-Server auf demselben Computer wie WFBS befindet und Port 25 verwendet, erkennt das Installationsprogramm den Namen des SMTP-Servers und aktualisiert die Felder SMTP-Server und Port.

- **Port:** Der Port, über den der SMTP-Server kommuniziert

- **Empfänger:** Die E-Mail-Adresse(n), an die der SMTP-Server Alarmbenachrichtigungen versendet. Sie können mehrere E-Mail-Adressen eingeben, wenn mehrere Personen benachrichtigt werden müssen.

Weitere Informationen finden Sie in den Mail-Server-Einstellungen Ihres ISPs. Sind Ihnen diese Einstellungen nicht bekannt, fahren Sie mit dem nächsten Schritt fort. Sie können die SMTP-Einstellungen nach der Installation aktualisieren. Weitere Hinweise finden Sie im Administratorhandbuch.

Smart Protection Network



The screenshot shows a window titled "Trend Micro Worry-Free Business Security Advanced" with a subtitle "Trend Micro Smart Protection Network". The Trend Micro logo is in the top right. The main text explains that Trend Micro Smart Feedback collects and analyzes threat information to provide better protection. A checkbox is checked, indicating that the user wants to activate Trend Micro Smart Feedback (recommended). Below this, a note states that the user can withdraw participation at any time via the Management Console. There is a label "Wählen Sie Ihre Branche aus (optional):" followed by a dropdown menu currently set to "Nicht angegeben". At the bottom left is the "InstallShield" logo. At the bottom right are three buttons: "< Zurück", "Weiter >" (which is highlighted with a dashed border), and "Abbrechen".

Wählen Sie, ob Sie am Trend Micro Smart Protection Network Feedback-Programm teilnehmen möchten.

Über diese optionale Funktion erhält Trend Micro Feedback zu Malware-Infektionen. Trend Micro empfiehlt, den Standardwert zu übernehmen, da mit Hilfe der weltweiten WFBS Feedback-Daten die Wirksamkeit der Anti-Malware-Lösungen optimiert werden soll. Sie können die Zustimmung zur Teilnahme später auf der Webkonsole rückgängig machen.

Einstellungen für eine benutzerdefinierte Installation konfigurieren

Wenn Sie eine benutzerdefinierte Installation durchführen, werden nacheinander die folgenden Fenster angezeigt:

Installationsspeicherort



Standardmäßig ist als WFBS Installationsordner C:\Programme\Trend Micro\Security Server oder C:\Programme (x86)\Trend Micro\Security Server festgelegt. Klicken Sie auf **Durchsuchen**, wenn Sie WFBS in einem anderen Ordner installieren möchten.

Speicherort der Suchserver-Datenbank

Trend Micro Worry-Free Business Security Advanced

Wählen Sie den Speicherort für die Smart Scan

Die Scan Server-Datenbank wird standardmäßig in dem Ordner gespeichert, in dem auch der Security Server zu finden ist.

Wählen Sie 'Anderen Speicherort angeben' nur aus, wenn der Security Server-Computer über eine andere Festplatte mit mindestens 3 GB freien Speicherplatz verfügt. Geben Sie einen absoluten Pfad an (zugewiesene Laufwerke und UNC-Pfade sind nicht zulässig).

☒ Installationsordner verwenden

C:\Program Files (x86)\Trend Micro\Security Server

☐ Anderen Speicherort angeben:

C:\Program Files (x86)\Trend Micro\Security Server Durchsuchen...

InstallShield

< Zurück Weiter > Abbrechen

Wählen Sie **Installationsort verwenden**, um die Suchserver-Datenbank im gleichen Ordner wie den Security Server zu speichern oder wählen Sie **Anderen Speicherort angeben**, und tippen Sie den absoluten Pfad zu einem anderen Speicherort auf dem Security Server ein. Es ist nicht möglich, einen zugeordneten Laufwerk- oder UNC-Pfad anzugeben.

Komponenten auswählen



Wählen Sie die Komponenten aus, die Sie auf dem Zielcomputer installieren möchten:

- **Security Server** (erforderlich): Auf dem Security Server befindet sich die zentrale Webkonsole.
- **Security Agent** (Optional): Der Agent, der Desktops und Server schützt
- **Messaging Security Agent** (Optional): Bei einer Installation des Security Server auf einem Computer, auf dem auch ein Microsoft Exchange Server installiert ist, werden Sie aufgefordert, einen lokalen Messaging Security Agent zu installieren (nur Advanced).
- **Remote Messaging Security Agent** (optional): Bei einer Installation von Security Server auf einem Computer, der das Vorhandensein von lokalen Microsoft

Exchange Servern nicht erkennt, werden Sie aufgefordert, den Remote Messaging Security Agent auf Remote-Servern zu installieren (nur Advanced).

**Hinweis**

Wenn auf dem Computer, auf dem Sie den Security Server installieren, bereits ein Exchange Server vorhanden ist, wird der Remote Messaging Security Agent nicht im Fenster 'Komponenten auswählen' angezeigt. Es wird nur der lokale Messaging Security Agent angezeigt.

Security Server konfigurieren



Das Fenster Security Server konfigurieren umfasst die Einstellungen des Security Server, die Sie konfigurieren müssen.

Webserver



Bei einer neuen Installation wird überprüft, ob bereits ein Webserver auf dem Zielcomputer vorhanden ist.

SZENARIO	ERGEBNIS	HINWEISE
Während des Setups werden sowohl IIS als auch Apache Webserver erkannt.	• Bei einer typischen oder Minimalinstallation wird automatisch IIS verwendet. • Benutzerdefinierte Installation: • Es wird automatisch IIS verwendet, wenn die Version des Apache Webservers nicht unterstützt wird (es werden lediglich Version 2.0.54, 2.0.55, 2.0.6x und 2.2.22 unterstützt). • Wenn die Version des Apache Webservers unterstützt wird, haben Sie freie Wahl.	Wenn auf dem Computer Windows Vista, Windows 7, 8 oder 8.1 ausgeführt wird, empfiehlt Trend Micro die benutzerdefinierte Installation und Apache als Webserver.
Während des Setups wird nur ein IIS Webserver erkannt.	• Bei einer typischen oder Minimalinstallation wird automatisch IIS verwendet. • Bei einer benutzerdefinierten Installation haben Sie die freie Wahl zwischen beiden Webservern. Wenn Sie sich für Apache entscheiden, wird automatisch Apache 2.2.22 installiert.	

SZENARIO	ERGEBNIS	HINWEISE
Während des Setups wird nur ein Apache Webserver erkannt.	- Es wird Apache verwendet, wenn es sich um Version 2.0.54, 2.0.55, 2.0.6x oder 2.2.22 handelt. - Andere Versionen von Apache können nicht installiert werden. Ziehen Sie folgende Maßnahmen in Betracht: - Deinstallation von Apache, wenn keine Anwendung diesen Webserver verwendet - Aktualisierung auf Apache 2.0.54, 2.0.55, 2.0.6x oder 2.2.22, sofern eine dieser Versionen mit den Anwendungen kompatibel ist, die Apache verwenden - Auswahl eines anderen Computers, auf dem der Security Server installiert werden soll	Die folgenden Plattformen verwenden IIS und werden vom Security Server unterstützt: - Windows Server 2003/2003 R2 - Windows SBS 2003/2003 R2 - Windows Home Server - Windows Server 2008/2008 R2 - Windows SBS 2008 - Windows EBS 2008 - Windows SBS 2011 Standard/Essentials - Windows Server 2012/2012 R2 Wenn IIS nicht auf diesen Plattformen entdeckt wird, wurde IIS möglicherweise (standardmäßig oder vom Systemadministrator) deaktiviert. Aktivieren Sie IIS in diesem Fall.
Während des Setups wird kein Webserver erkannt.	Es wird automatisch Apache Webserver 2.2.22 installiert.	

Bei Upgrades, wenn Apache derzeit als Webserver verwendet wird:

- Wenn der Apache Webserver vom Setupprogramm von WFBS 6.x/7.x/8.x installiert wurde, wird Apache automatisch auf Version 2.2.22 aktualisiert.
- Wurde er dagegen von einem anderen Programm installiert, wird die bestehende Version von Apache beibehalten.

Kennwort für das Administratorkonto

Trend Micro Worry-Free Business Security Advanced

Kennwort für das Administratorkonto

Geben Sie ein Kennwort ein, und bestätigen Sie es durch erneute Eingabe

Schützen Sie die Security Server Web-Konsole und die Clients mit einem Kennwort, um zu verhindern, dass unbefugte Benutzer Einstellungen ändern oder Clients entfernen können.

Security Server Webkonsole:

Kennwort:

Kennwort bestätigen:

Security Agents: ☒ Wie oben

Kennwort:

Kennwort bestätigen:

InstallShield

< Zurück Weiter > Abbrechen

Richten Sie verschiedene Kennwörter für die Security Server Webkonsole und den Security Agent ein.

- **Security Server Webkonsole:** Erforderlich für die Anmeldung an der Webkonsole
- **Security Agents:** Erforderlich für die Deinstallation oder das Beenden des Security Agents aus Clients



Hinweis

Das Kennwortfeld erlaubt bis zu 24 Zeichen und unterscheidet zwischen Groß- und Kleinschreibung.

SMTP-Server und Empfänger der Benachrichtigung(en)

Trend Micro Worry-Free Business Security Advanced

SMTP-Server und Empfänger der Benachrichtigung(en)

Richten Sie den SMTP-Server so ein, dass er alle vom Trend Micro Security Server erzeugten Benachrichtigungen und Berichte versendet.

SMTP-Server:

Port:

Empfänger:

(Trennen Sie mehrere Adressen durch einen Strichpunkt ';'.
Beispiel: user1@domain.com; user2@domain.com)

InstallShield

< Zurück Weiter > Abbrechen

Geben Sie die folgenden Informationen an:

- **SMTP-Server:** Die IP-Adresse des E-Mail-Servers



Hinweis

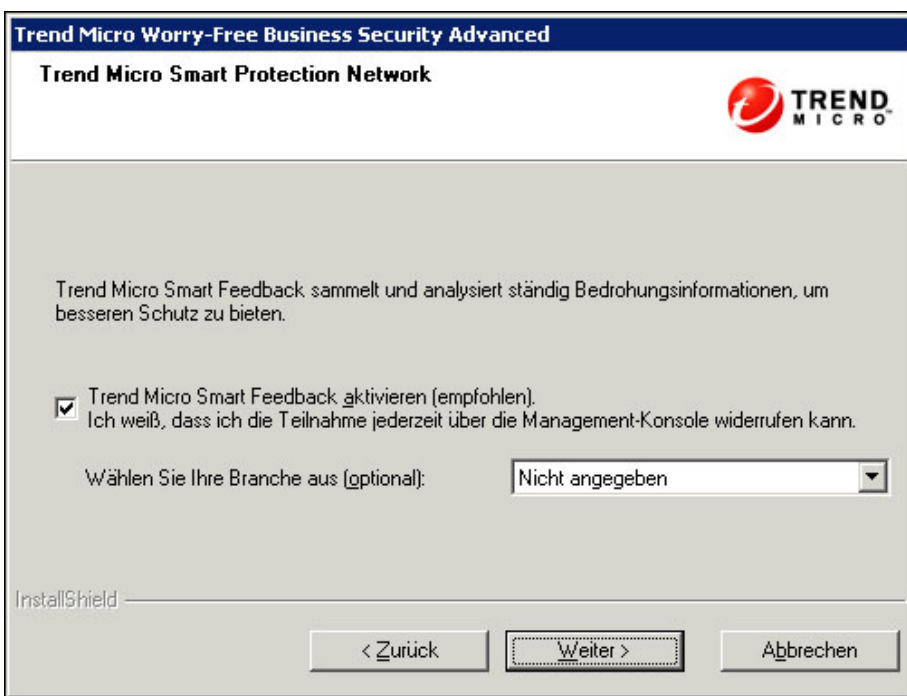
Wenn sich der SMTP-Server auf demselben Computer wie WFBS befindet und Port 25 verwendet, erkennt das Installationsprogramm den Namen des SMTP-Servers und aktualisiert die Felder SMTP-Server und Port.

- **Port:** Der Port, über den der SMTP-Server kommuniziert

- **Empfänger:** Die E-Mail-Adresse(n), an die der SMTP-Server Alarmbenachrichtigungen versendet. Sie können mehrere E-Mail-Adressen eingeben, wenn mehrere Personen benachrichtigt werden müssen.

Weitere Informationen finden Sie in den Mail-Server-Einstellungen Ihres ISPs. Sind Ihnen diese Einstellungen nicht bekannt, fahren Sie mit dem nächsten Schritt fort. Sie können die SMTP-Einstellungen nach der Installation aktualisieren. Weitere Hinweise finden Sie im Administratorhandbuch.

Smart Protection Network

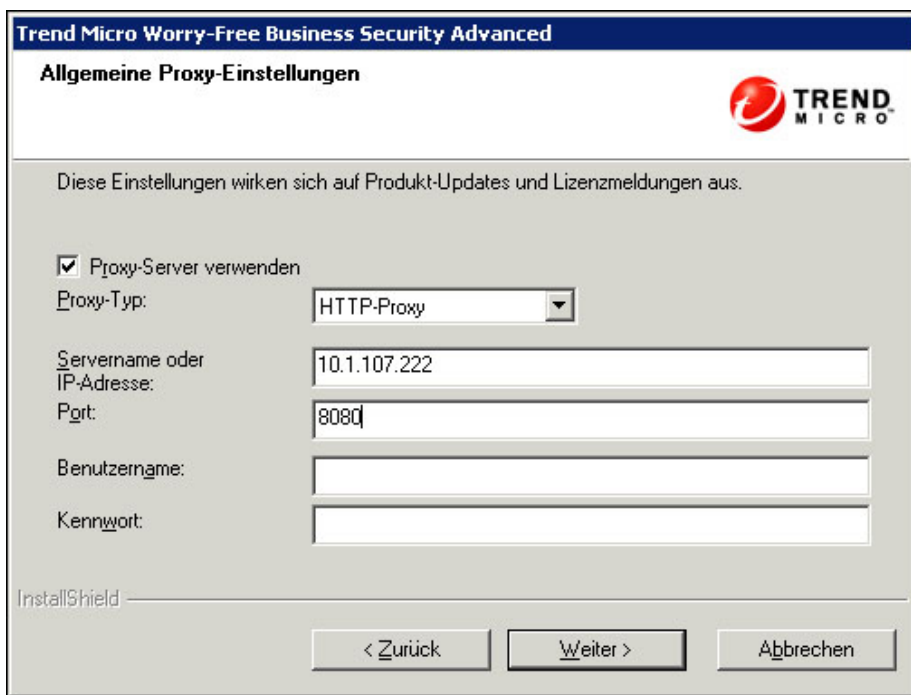


The screenshot shows a window titled "Trend Micro Worry-Free Business Security Advanced" with a subtitle "Trend Micro Smart Protection Network". The Trend Micro logo is in the top right. The main text explains that Trend Micro Smart Feedback collects and analyzes threat information to provide better protection. A checkbox labeled "Trend Micro Smart Feedback aktivieren (empfohlen)." is checked, with a note below it: "Ich weiß, dass ich die Teilnahme jederzeit über die Management-Konsole widerrufen kann." Below this is a label "Wählen Sie Ihre Branche aus (optional):" followed by a dropdown menu currently showing "Nicht angegeben". At the bottom left is the "InstallShield" logo. At the bottom right are three buttons: "< Zurück", "Weiter >" (highlighted with a dashed border), and "Abbrechen".

Wählen Sie, ob Sie am Trend Micro Smart Protection Network Feedback-Programm teilnehmen möchten.

Über diese optionale Funktion erhält Trend Micro Feedback zu Malware-Infektionen. Trend Micro empfiehlt, den Standardwert zu übernehmen, da mit Hilfe der weltweiten WFBS Feedback-Daten die Wirksamkeit der Anti-Malware-Lösungen optimiert werden soll. Sie können die Zustimmung zur Teilnahme später auf der Webkonsole rückgängig machen.

Allgemeine Proxy-Einstellungen



Trend Micro Worry-Free Business Security Advanced

Allgemeine Proxy-Einstellungen

Die Trend Micro Logo ist in der oberen rechten Ecke zu sehen.

Diese Einstellungen wirken sich auf Produkt-Updates und Lizenzmeldungen aus.

☒ Proxy-Server verwenden

Proxy-Typ: HTTP-Proxy

Servername oder IP-Adresse: 10.1.107.222

Port: 8080

Benutzername:

Kennwort:

InstallShield

< Zurück Weiter > Abbrechen

Wenn für die Verbindung zum Internet ein Proxy-Server erforderlich ist, aktivieren Sie das Kontrollkästchen **Proxy-Server verwenden**, und geben Sie folgende Informationen an:

- **Proxy-Server-Typ**

- **Servername oder IP-Adresse**
- **Port**
- **Benutzername und Kennwort:** nur erforderlich, wenn der Proxy-Server eine Authentifizierung erfordert.

Security Agent konfigurieren



Das Fenster 'Security Agent konfigurieren' umfasst die Einstellungen des Security Agent, die Sie konfigurieren müssen.

Installieren Sie nach der Installation des Security Server den Security Agent auf Clients im Netzwerk. Einzelheiten zu den verschiedenen Methoden zur Installation des Security Agent erhalten Sie im Administratorhandbuch.

Security Agent Installationspfad

Trend Micro Worry-Free Business Security Advanced

Security Agent Installationspfad

Standard-Zielordner für alle Security Agents:

Legen Sie mit einer der folgenden Variablen den Security Agent-Installationspfad fest:

\$BOOTDISK: Laufwerksbuchstabe der Startfestplatte
 \$WINDIR: Windows-Installationsordner
 \$ProgramFiles: Programmordner

Wenn Sie den Installationspfad zu einem späteren Zeitpunkt ändern möchten, können Sie dies mit der Webkonsole tun (Einstellungen > Globale Einstellungen > System > Abschnitt Security Agent-Installation).

Security Agent Listening-Port:

InstallShield

< Zurück Weiter > Abbrechen

Legen Sie folgende Komponenten fest:

- **Installationspfad:** Der Zielordner, in dem die Security Agent-Dateien installiert werden
- **Security Agent Listening-Port:** Die Portnummer, die für die Kommunikation zwischen dem Security Agent und dem Security Server verwendet wird

Einstellungen des Security Agents



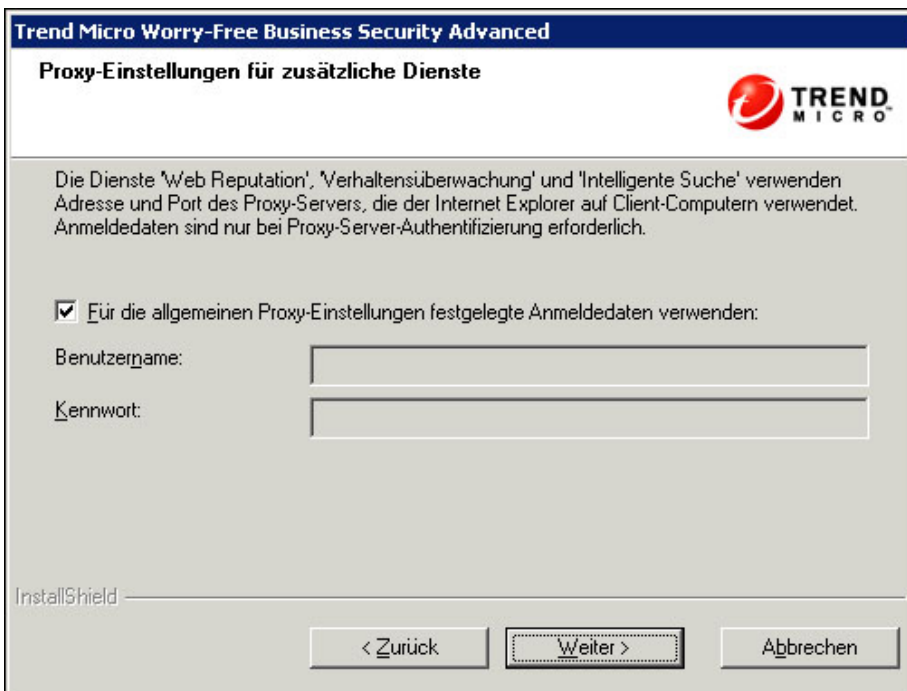
Einstellungen des Security Agents für Server und Desktops

- **Server:** Security Agents unter Windows Server-Plattformen (z. B. Windows Server 2008) werden zur Standard-Servergruppe hinzugefügt, wenn Sie sie erstmals zur Webkonsole hinzufügen. Sie können je nach Anforderung unterschiedliche Technologien für diese Gruppe aktivieren.
- **Desktops:** Security Agents unter Windows Desktop-Plattformen (z. B. Windows Vista) werden zur Standard-Desktopgruppe hinzugefügt, wenn Sie sie erstmals zur Webkonsole hinzufügen. Sie können je nach Anforderung unterschiedliche Technologien für diese Gruppe aktivieren.

In jeder Gruppe können Sie folgende Komponenten konfigurieren:

- **Smart Scan:** Smart Scan verwendet einen zentralen Suchserver auf dem Netzwerk, der den Clients einen Teil der Virensuche abnimmt.
- **Virenschutz und Anti-Spyware:** Dateien auf böstigen Code durchsuchen, wenn auf sie zugegriffen wird oder sie erstellt werden
- **Firewall:** Errichtet eine Barriere zwischen Clients und Netzwerk und schützt dadurch Clients vor Malware-Angriffen und Netzwerkviren.
- **Web-Reputation:** Blockiert böstige Websites durch Überprüfen der Glaubwürdigkeit von Webdomänen und durch Zuweisen eines Reputationswerts auf Basis mehrerer identifizierender Faktoren.
- **URL-Filter:** Blockiert angegebene Website-Kategorien (z. B. pornografische Inhalte, soziale Netzwerke) entsprechend der Firmenpolitik.
- **Verhaltensüberwachung:** Analysiert das Programmverhalten, um bekannte und unbekannte Bedrohungen proaktiv zu erkennen.
- **Vertrauenswürdiges Programm:** Häufig verwendete I/O-Anwendungen können in der Benutzeroberfläche konfiguriert werden.
- **Gerätesteuerung:** Reguliert den Zugriff auf externe Speichergeräte und Netzwerkressourcen

Proxy-Einstellungen für zusätzliche Dienste



The screenshot shows a window titled "Trend Micro Worry-Free Business Security Advanced" with a subtitle "Proxy-Einstellungen für zusätzliche Dienste". The Trend Micro logo is in the top right. The main text explains that services like 'Web Reputation', 'Verhaltensüberwachung', and 'Intelligente Suche' use the proxy server address and port. It states that login data is only required for proxy server authentication. A checkbox is checked, indicating that the general proxy settings' login data should be used. Below this are input fields for "Benutzername:" and "Kennwort:". At the bottom, there are three buttons: "< Zurück", "Weiter >", and "Abbrechen". The "InstallShield" logo is visible in the bottom left corner of the window.

Trend Micro Worry-Free Business Security Advanced

Proxy-Einstellungen für zusätzliche Dienste

Die Dienste 'Web Reputation', 'Verhaltensüberwachung' und 'Intelligente Suche' verwenden Adresse und Port des Proxy-Servers, die der Internet Explorer auf Client-Computern verwendet. Anmeldedaten sind nur bei Proxy-Server-Authentifizierung erforderlich.

☒ Für die allgemeinen Proxy-Einstellungen festgelegte Anmeldedaten verwenden:

Benutzername:

Kennwort:

InstallShield

< Zurück Weiter > Abbrechen

Die Dienste **Smart Scan**, **Web Reputation** und **Verhaltensüberwachung** verwenden die Adresse und den Port des Proxy-Servers, die bzw. den der Internet Explorer auf Client-Computern verwendet. Erfordert der Proxy-Server eine Authentifizierung, verwenden Sie dieses Fenster, um die Anmeldedaten anzugeben.

Messaging Security Agent konfigurieren

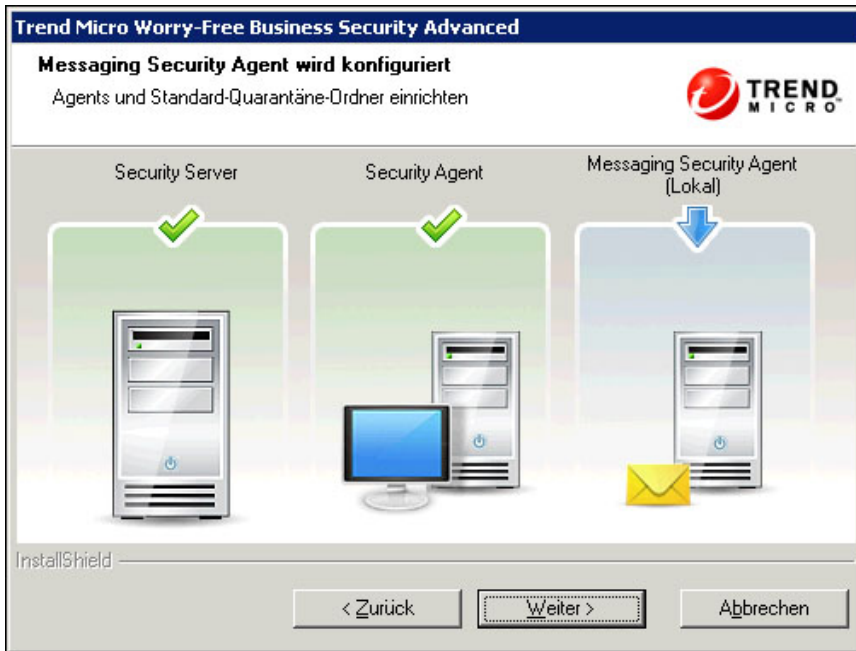
Führen Sie die Installation des Messaging Security Agents während der Installation des Security Servers durch.

Installationshinweise:

- Die Microsoft Exchange-Dienste müssen weder vor noch nach der Installation angehalten oder neu gestartet werden.
- Der Messaging Security Agent kann nicht erfolgreich installiert werden, wenn auf dem Client Informationen zu einer vorherigen Messaging Security Agent Installation vorhanden sind. Mit dem Windows Installer Cleanup Utility können Sie Überreste einer früheren Installation entfernen. Eine Download-Version des Windows Installer Cleanup Utility finden Sie unter:
<http://support.microsoft.com/kb/290301/en-us>
- Bei Installation des Messaging Security Agent auf einem Server, auf dem Lockdown-Tools ausgeführt werden, entfernen Sie das Lockdown-Tool, damit es den IIS Dienst nicht deaktiviert und die Installation nicht fehlschlägt.
- Der Messaging Security Agent kann nach der Installation des Security Servers auch über die Webkonsole installiert werden. Weitere Informationen finden Sie im Administratorhandbuch.

Setup fordert Sie zur Installation des Messaging Security Agents auf, wenn:

- Wenn eine Installation des Security Servers auf einem Computer durchgeführt wird, auf dem auch ein Microsoft Exchange Server installiert ist, werden Sie vom Setup aufgefordert, einen **lokalen** Messaging Security Agent zu installieren.



- Wenn eine Installation des Security Servers auf einem Computer durchgeführt wird, der das Vorhandensein von lokalen Microsoft Exchange Servern nicht

erkennt, werden Sie vom Setup aufgefordert, den **Remote-Messaging Security Agent** auf Remote-Servern zu installieren.



Messaging Security Agent installieren

Trend Micro Worry-Free Business Security Advanced

Messaging Security Agent installieren

Sie können zudem den Messaging Security Agent von der Management-Konsole aus installieren. Um die Einschränkungen der Benutzerzugriffskontrolle (UAC) zu umgehen, geben Sie das integrierte Domänenadministratorkonto an.

☐ Nein, die Installation des Messaging-Schutzes ist abgeschlossen.

☒ Ja, der Messaging-Schutz soll auf dem folgenden Server installiert werden.

Exchange Server:

Domänenadministratorkonto (Domäne\Konto)

Konto:

Kennwort:

InstallShield

< Zurück Weiter > Abbrechen

Geben Sie folgende Informationen an:

- **Exchange Server**



Hinweis

Das Installationsprogramm erkennt den Namen des lokalen Exchange Servers automatisch und füllt das Feld 'Exchange Server' aus, wenn sich der Exchange Server auf demselben Computer wie der Security Server befindet. Wenn ein Exchange Server auf demselben Computer installiert ist, der Name des Exchange Servers jedoch nicht automatisch eingegeben wird, prüfen Sie, ob Ihre Umgebung die Messaging Security Agent-Systemvoraussetzungen erfüllt.

- Domänenadministratorkonto
- Kennwort

**Hinweis**

Der Installer kann Kennwörter mit Sonderzeichen, also nicht alphanumerischen Zeichen, möglicherweise nicht an den Exchange Server Computer weitergeben. In diesem Fall kann der Messaging Security Agent nicht installiert werden. Um dieses Problem zu umgehen, ändern Sie vorübergehend das Kennwort für das integrierte Domänenadministratorkonto, oder installieren Sie den Messaging Security Agent direkt auf dem Exchange Server.

Einstellungen des Messaging Security Agents

Trend Micro Worry-Free Business Security Advanced

Einstellungen des Messaging Security Agents

Wählen Sie den Exchange Server aus

Zielordner: C:\Program Files\Trend Micro\Messaging Security Agent

Temp-Ordner: C\$

Die Installationsdateien werden in den angegebenen Freigabeordner auf dem Computer kopiert, von dem aus MSA installiert wird

Spam-Verwaltung

☐ End User Quarantine

☒ Junk-Mail-Ordner in Outlook

InstallShield

< Zurück Weiter > Abbrechen

Konfigurieren Sie das Folgende:

- **Zielordner:** Der Ordner, in dem die Messaging Security Agent-Dateien installiert werden.
- **Temp-Ordner:** Der Ordner, in dem die Installationsdateien entpackt werden.
- **End User Quarantine:** Wenn diese Option aktiviert ist, erstellt WFBS in Microsoft Outlook zusätzlich zum Ordner Junk-Mail einen separaten Spam-Ordner.
- **Junk-Mail-Ordner in Outlook:** Wenn diese Option aktiviert ist, speichert WFBS Spam-Mails in diesem Ordner. Da Microsoft Outlook Spam-Nachrichten aus dem Ordner End User Quarantine (EUQ) in der Regel in den Ordner Junk-Mail verschiebt, empfiehlt Trend Micro, diese Option auszuwählen.



Hinweis

Sie können nur zwischen EUQ und dem Junk-Mail-Ordner wählen, wenn auf dem Computer Exchange Server 2003 ausgeführt wird. Beim Exchange Server 2007 und 2010 ist die EUQ-Option standardmäßig deaktiviert.

Klicken Sie auf **Weiter**, und das Programm beginnt mit der Installation des Messaging Security Agents.

Nachdem Sie den Messaging Security Agent aus der Ferne installiert haben, wiederholen Sie den Agent-Installationsvorgang, um Messaging Security Agents remote auf anderen Microsoft Exchange Servern zu installieren.

Phase 3: Installation

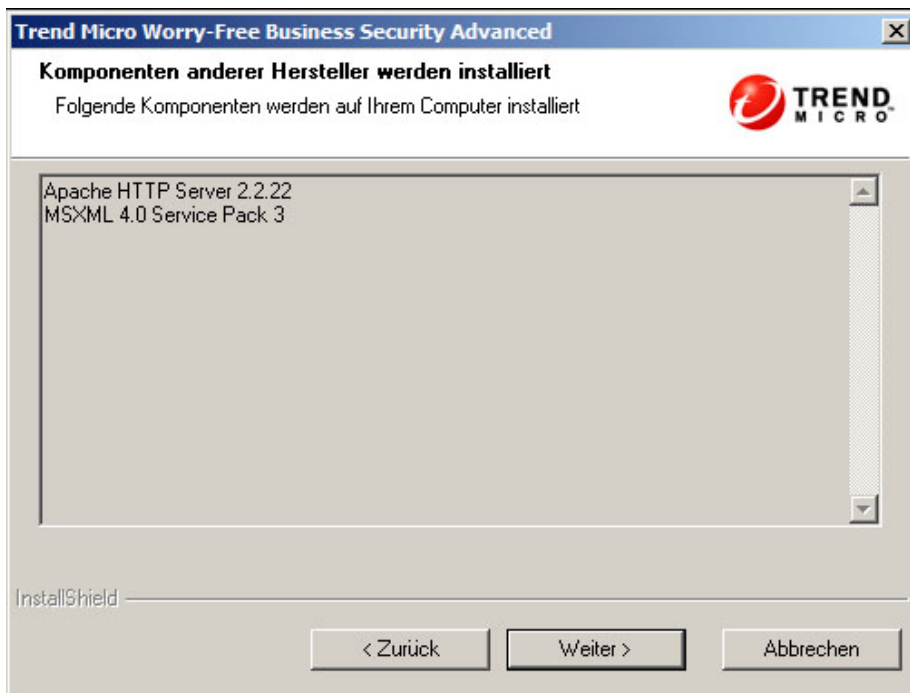
Dateien werden kopiert



Das Fenster Dateien werden kopiert zeigt eine Zusammenfassung aller Parameter an, die bei der Installation von WFBS verwendet werden.

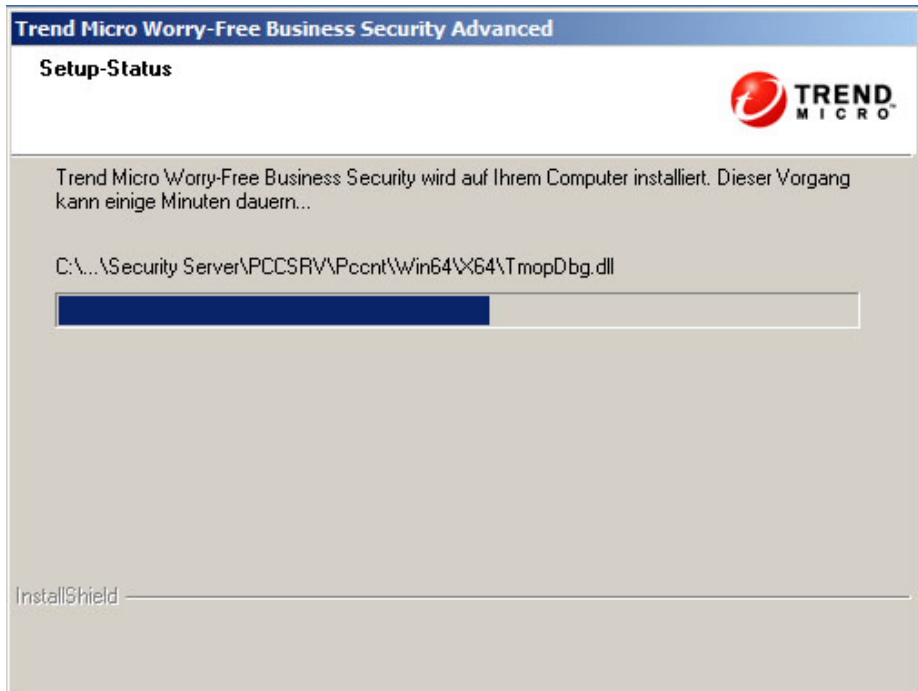
Klicken Sie auf **Zurück**, wenn Sie die bisherigen Installationseinstellungen überprüfen möchten, oder auf **Weiter**, um mit der aktuellen Installation fortzufahren.

Komponenten anderer Hersteller installieren



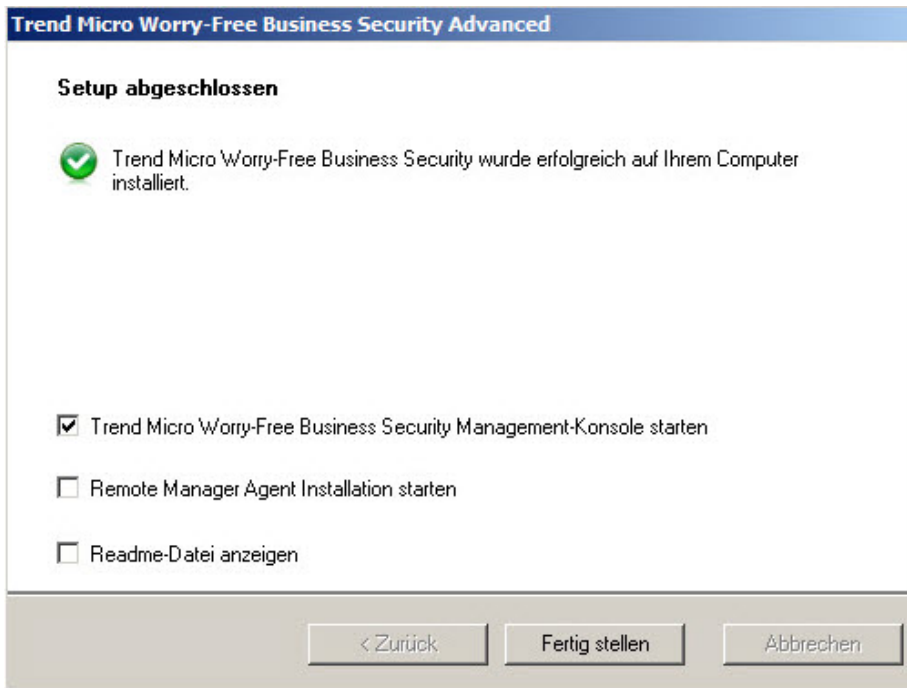
Dieses Fenster enthält Informationen über die Komponenten anderer Hersteller, die installiert werden. Klicken Sie auf **Weiter**, um mit der Installation der ausgewählten Komponenten zu beginnen.

Setup-Status



Der gesamte Installationsvorgang kann einige Zeit dauern. Während der Installation wird der Fortschritt in einem Statusfenster angezeigt.

Setup abgeschlossen



Wählen Sie optional die entsprechenden Kontrollkästchen, um folgende Aktionen auszuführen:

- Die webbasierte Management-Konsole öffnen (Standardauswahl)
- Remote Manager Agent installieren (siehe *Administratorhandbuch* für Informationen zum Verfahren)
- Readme-Datei anzeigen

Klicken Sie auf **Fertig stellen**, um den Installationsvorgang zu beenden.

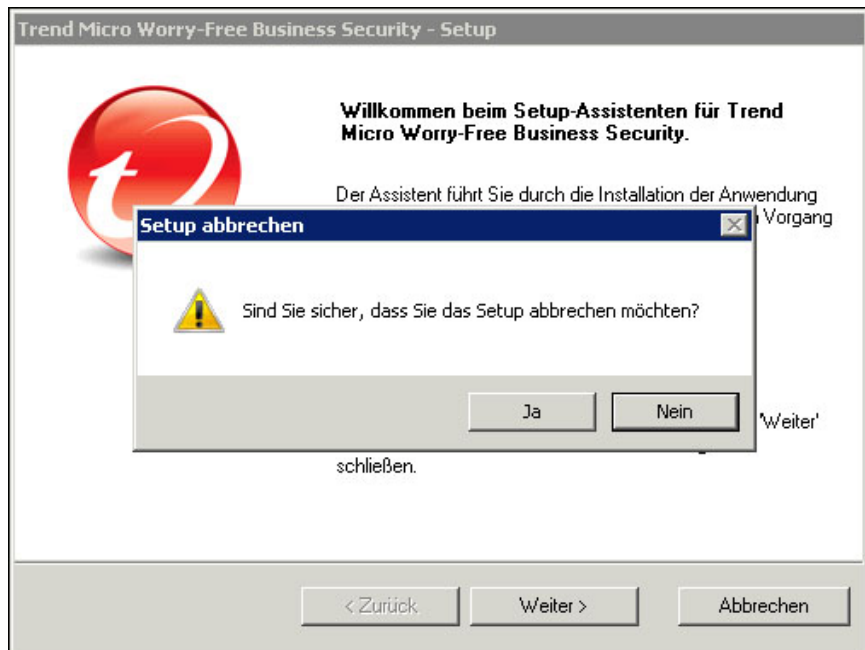
Mehrere Security Server mit der unbeaufsichtigten Installation installieren

Verwenden Sie die unbeaufsichtigte Installation, um mehrere identische Installationen auf verschiedenen Netzwerken vorzunehmen. Sie können die Installationseinstellungen einer Sitzung des Setup-Assistenten speichern und anschließend auf Grundlage dieser Einstellungen automatische Installationen generieren.

Eine Installationssitzung aufnehmen

Prozedur

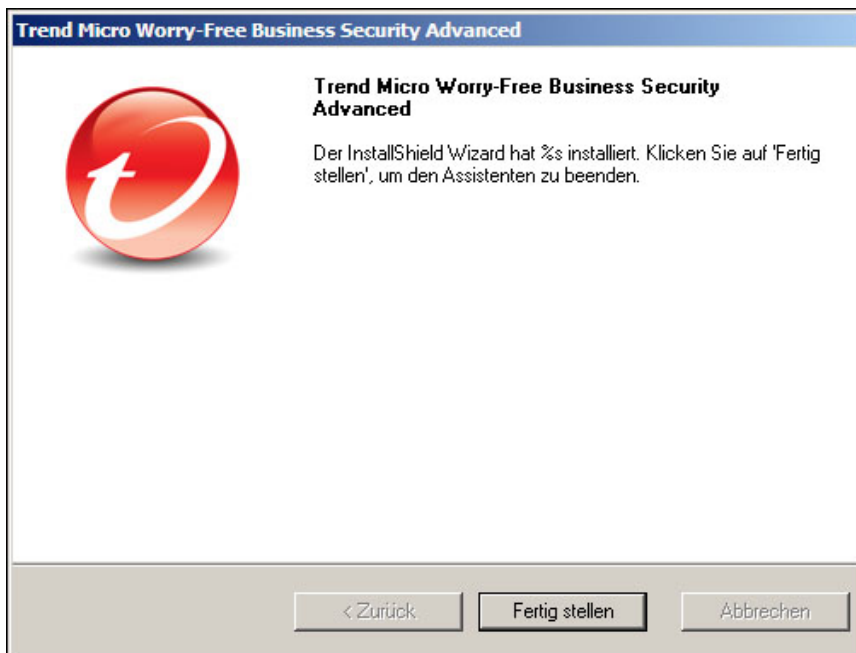
1. Laden Sie die Dateien für die Installation von WFBS auf die Festplatte herunter, und entpacken Sie sie. Sobald der Setup-Assistent mit der Erfassung der Installationseinstellungen beginnt, klicken Sie auf **Abbrechen** > **Ja** > **Fertig stellen**.



2. Navigieren Sie im Eingabeaufforderungsmodus zu dem Verzeichnis, in dem sich die entpackten WFBS-Installationsdateien befinden, z. B. C:\Extract\WFBS\CSM
3. Geben Sie an der Eingabeaufforderung `Setup.exe /r /f1"c:\silent-install.iss"` ein, und drücken Sie die **Eingabetaste**.

Der Setup-Assistent wird erneut gestartet. Ihre Eingaben werden aufgezeichnet und auf Laufwerk C: in der Datei silent-install.iss gespeichert.

4. Folgen Sie den Anweisungen auf dem Bildschirm. Die Anweisungen entsprechen denen, die in *Den Security Server installieren auf Seite 2-13* beschrieben werden.
5. Am Ende der Aufzeichnungssitzung wird das folgende Bestätigungsfenster angezeigt. Klicken Sie auf **Fertig stellen**, um die Aufnahmesitzung zu beenden und zum Befehlszeilenmodus zurückzukehren.



Die unbeaufsichtigte Installation starten

Prozedur

1. Navigieren Sie im Eingabeaufforderungsmodus zu dem Verzeichnis, in dem sich die entpackten WFBS-Installationsdateien befinden, z. B. `C:\Extract\WFBS\CSM`

2. Geben Sie an der Eingabeaufforderung `Setup.exe /s /f1"c:\silent-install.iss"` ein, und drücken Sie die **Eingabetaste**.

Die unbeaufsichtigte WFBS Installation wird automatisch gestartet und dauert dabei genauso lange wie eine normale Installation.

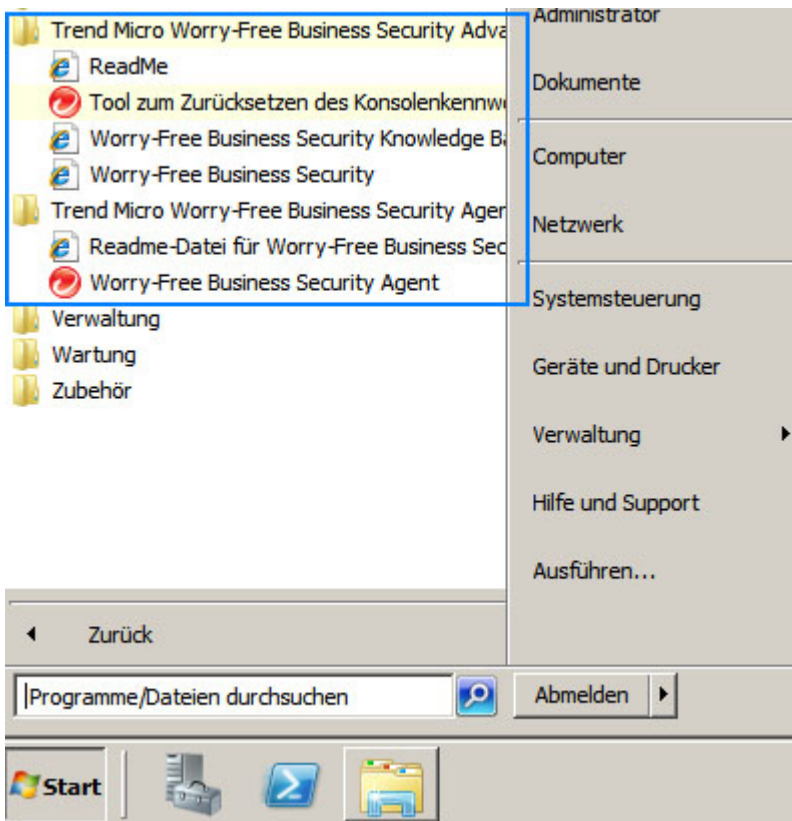
Während der unbeaufsichtigten Installation wird der Fortschritt nicht auf dem Bildschirm angezeigt

3. Um zu überprüfen, ob die Installation erfolgreich war, öffnen Sie die Datei `c:\setup.log`. Ist der Ergebniscode `ResultCode=0`, war die Installation erfolgreich.
 4. Wiederholen Sie die Schritte 1 bis 3 auf allen anderen Computern im Netzwerk.
-

Die Installation überprüfen

Prozedur

- Klicken Sie auf **Start > Alle Programme**, um festzustellen, ob der Security Server und der Security Agent in der Liste angezeigt werden.



- Klicken Sie auf **Start > Systemsteuerung > Software > Programm deinstallieren**, um festzustellen, ob das WFBS Programm und der Security Agent in der Liste angezeigt werden.
- Melden Sie sich mit dem URL des Servers an der Management-Konsole an:
https://{Name_des_Servers}:{Portnummer}/SMB



Hinweis

Wenn Sie nicht SSL (Security Socket Layer) verwenden, geben Sie [http](http://) statt [https](https://) ein.

Kapitel 3

Upgrades für Security Server und Agents

Machen Sie sich mit den Informationen aus diesem Kapitel vertraut, bevor Sie Upgrades des Security Servers und der Agents durchführen.

Voraussetzungen für Installation und Upgrade

Besuchen Sie die folgende Website, um eine vollständige Liste der Systemvoraussetzungen für die Installation und Upgrades zu erhalten:

<http://docs.trendmicro.com/de-de/smb/worry-free-business-security.aspx>

Überlegungen zum Upgrade

Beachten Sie Folgendes, wenn Sie ein Upgrade des Security Servers und der Agents durchführen.

- *IPv6-Voraussetzungen für Upgrades auf Seite 3-2*
- *Bewährte Upgrade-Methoden auf Seite 3-3*

IPv6-Voraussetzungen für Upgrades

Für den Security Server gelten folgende IPv6-Voraussetzungen:

- Der Security Server, auf dem das Upgrade durchgeführt werden soll, muss auf Windows Server 2008, SBS 2008/2011, 7 und Vista installiert sein. Auf Security Servern auf Windows XP, Server 2003 und SBS 2003 kann kein Upgrade durchgeführt werden, da diese Betriebssysteme die IPv6-Adressierung nur teilweise unterstützen.
- Der Security Server muss bereits einen IIS Webserver verwenden. Der Apache Webserver unterstützt keine IPv6-Adressierung.
- Weisen Sie dem Security Server eine IPv6-Adresse zu. Zusätzlich muss der Server über seinen Hostnamen identifiziert werden, vorzugsweise seinen vollqualifizierten Domännennamen (FQDN). Wenn der Server über seine IPv6-Adresse identifiziert wird, verlieren alle aktuell vom Server verwalteten Clients ihre Verbindung mit dem Server. Wenn der Server über seine IPv4-Adresse identifiziert wird, kann der Server den Agent nicht an reine IPv6-Clients verteilen.

- Vergewissern Sie sich, dass die IPv6- oder IPv4-Adresse des Host-Computers des Security Servers abgerufen werden kann. Verwenden Sie dazu z. B. den Befehl ping oder den Befehl nslookup.

Bewährte Upgrade-Methoden

Sie können die Client-Einstellungen beibehalten, wenn Sie ein Upgrade auf die neueste Version von WFBS durchführen. Damit die vorhandenen Einstellungen nach einem fehlgeschlagenen Upgrade problemlos wiederhergestellt werden können, empfiehlt Trend Micro Folgendes:

- Die Security Server Datenbank sichern
- Alle Protokolldateien vom Security Server löschen

Die Security Server Datenbank sichern

Prozedur

1. Beenden Sie den Trend Micro Security Server Master-Dienst.
 2. Navigieren Sie im Windows Explorer zum Security Server Ordner und kopieren Sie den Inhalt aus dem Verzeichnis \PCCSRV\HTTPDB an einen anderen Speicherort (beispielsweise in einen anderen Ordner auf demselben Server, auf einen anderen Computer oder auf ein Wechsellaufwerk).
-

Protokolldateien vom Security Server löschen

Prozedur

1. Wechseln Sie zu **Berichte > Wartung > Manuelle Protokolllöschung**.
2. Stellen Sie für einen Protokolltyp **Protokolle löschen, die älter sind als** auf den Wert 0 ein.
3. Klicken Sie auf **Löschen**.

4. Wiederholen Sie die Schritte 2 bis 3 für alle Protokolltypen.
-

Upgrades der Vorgängerversion

Diese Produktversion unterstützt Upgrades von einer beliebigen der folgenden WFBS oder WFBS-Advanced Versionen:

- 9.0
- 8.x (8.0 und 8.0 SP1)
- 7.x (7.0 und 7.0 SP1)
- 6.x (6.0, SP1, SP2 und SP3)

Diese Produktversion unterstützt keine Upgrades von:

- WFBS oder WFBS-Advanced 5.x
- Alle Upgrades, die Windows 2000 unterstützt haben
- Client/Server/Messaging Security 3.6 (außer japanische Version)
- Client Server Messaging Security 3.5
- Client Server Messaging Security 3.0
- Client/Server Security 3.0
- Client/Server Suite 2.0
- Client/Server/Messaging Suite 2.0
- OfficeScan oder ScanMail for Microsoft Exchange
- Einer Sprache zur anderen

Abhängig von der Netzwerkbandbreite und der Anzahl der Agents, die der Security Server verwaltet, können Sie die Agent-Upgrades staffeln oder das Upgrade für alle Agents direkt im Anschluss an das Upgrade des Servers durchführen.

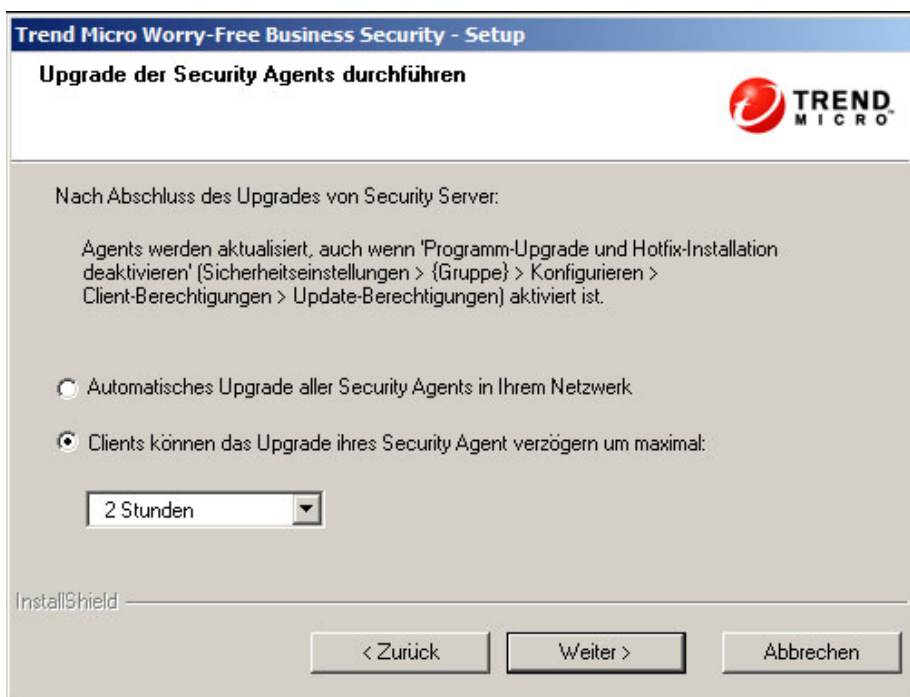
Upgrade-Methode 1: Upgrade mit dem Installationspaket

Sie benötigen das Installationspaket für diese Produktversion. Führen Sie die Datei `Setup.exe` auf dem Security Server-Computer aus. Wenn das Setup erkennt, dass ein Security Server auf dem Computer vorhanden ist, werden Sie zur Durchführung des Upgrades aufgefordert, wie in folgender Abbildung gezeigt.



Folgen Sie den Bildschirmanweisungen, um den Security Server zu aktualisieren.

Wählen Sie an einem der Installationsbildschirme eine der folgenden Upgrade-Optionen für den Security Agent aus:



UPGRADE-OPTION DES SECURITY AGENTS	DETAILS
Automatisches Upgrade aller Security Agents in Ihrem Netzwerk	Wenn Sie über eine geringe Anzahl von Security Agents verfügen, lassen Sie zu, dass das Upgrade aller Agents sofort nach dem Upgrade des Security Servers durchgeführt wird. Das Upgrade wird auf allen Agents durchgeführt, auch wenn die Option Upgrade des Security Agents und Hotfix-Installation deaktivieren auf der Webkonsole unter Sicherheitseinstellungen > {Gruppe} > Konfigurieren > Client-Berechtigungen aktiviert ist.  Hinweis Die Option Upgrade des Security Agents und Hotfix-Installation deaktivieren verhindert nur Build-Upgrades (z. B. vom Beta-Build zum Release-Build) jedoch keine Version-Upgrades. Wenn die Option zurzeit aktiviert ist, wird diese Option nach dem Upgrade automatisch deaktiviert. Reaktivieren Sie die Option, falls erforderlich.

UPGRADE-OPTION DES SECURITY AGENTS	DETAILS
Clients können das Upgrade ihres Security Agents um maximal ____ Stunden verzögern	Wählen Sie diese Option aus, wenn Sie viele Upgrades von Security Agents durchführen. Geben Sie die Anzahl der Stunden (2, 4, 8, 12 oder 24 Stunden) an, um die das Upgrade verzögert werden soll. Nach dem Upgrade des Security Servers sendet dieser Upgrade-Benachrichtigungen an alle Security Agents. Der Benutzer sieht eine Popup-Meldung mit einer Upgrade-Aufforderung auf seinem Computer.  • Wenn der Benutzer Jetzt upgraden anklickt, startet das Upgrade sofort. • Wenn der Benutzer nichts unternimmt, startet das Upgrade 5 Minuten nach Anzeige der Meldung automatisch. • Wenn der Benutzer auf Später erinnern klickt, zeigt der Security Agent die Popup-Meldung alle 30 Minuten an, bis das Upgrade vom Benutzer oder automatisch gestartet wird (wenn der Benutzer nichts unternimmt oder nachdem die von Ihnen angegebene Anzahl von Stunden abgelaufen ist). Die maximale Stundenzahl gilt, wenn die zuerst angezeigte Popup-Meldung bei jeder Verzögerung des Upgrades durch den Benutzer nicht zurückgesetzt oder wenn der Client-Computer ausgeschaltet oder neu gestartet wird. Agents, deren Upgrade noch nicht durchgeführt wurde, erhalten immer noch Komponenten-Updates (wie z. B. Pattern-Dateien), um ihren Schutz aktuell zu halten.

Upgrade-Ergebnisse

- Je nach ausgewählter Upgrade-Option wird das Upgrade der Online Security Agents sofort oder nach einer bestimmten Anzahl von Stunden durchgeführt.
- Das Upgrade von Online Messaging Security Agents erfolgt sofort.
- Das Upgrade von Offline-Agents erfolgt, wenn sie wieder online sind.
 - Überprüfen Sie bei Offline Messaging Security Agents den Verbindungsstatus zum Security Server.
 - Weisen Sie im Fall von Offline Security Agents die Benutzer an, eine Verbindung zum Netzwerk aufzubauen, so dass die Agents online gehen. Weisen Sie im Fall von Security Agents, die seit längerer Zeit offline sind, die Benutzer an, den Agent vom Client zu deinstallieren und anschließend mit Hilfe einer geeigneten Agent-Installationsmethode (wie dem Client Packager), die im *Administratorhandbuch* beschrieben wird, den Agent zu installieren.



Hinweis

Alle früheren Einstellungen des Agents, mit Ausnahme der Update-Agent-Berechtigungen, bleiben beim Aktualisieren auf diese Version erhalten. Update-Agents werden somit nach dem Upgrade zu Security Agents. Sie können sie über die Verwaltungskonsole wieder als Update-Agents festlegen. Weitere Informationen hierzu finden Sie unter <http://esupport.trendmicro.com/solution/en-US/1057531.aspx>.

Upgrade-Methode 2: Agents nach Security Server 9.0 SP1 verschieben

Führen Sie die Erstinstallation des Security Servers durch und verschieben Sie anschließend Agents (Security Agents und Messaging Security Agents) zu diesem Server. Die Agents werden beim Verschieben automatisch auf Version 9.0 SP1 aktualisiert.

Teil 1: Erstinstallation von Security Server 9.0 SP1 durchführen

Prozedur

1. Führen Sie eine Erstinstallation des Security Servers auf einem Computer aus. Weitere Informationen finden Sie unter *Den Security Server installieren auf Seite 2-13*.
2. Notieren Sie sich folgende Informationen über Security Server 9.0 SP1. Geben Sie beim Verschieben von Agents diese Informationen über Security Server 6.x, 7.x, 8.x oder 9.0 an.

- Hostname oder IP-Adresse:
- Server-Listening-Port

Den Host-Namen und Listening-Port finden Sie im Fenster Sicherheitseinstellungen des Security Servers über dem Bereich Aufgaben.

Teil 2: Agent-Upgrade durchführen

Prozedur

1. Navigieren Sie über die Webkonsole von Security Server 6.x, 7.x, 8.x oder 9.0 zu **Sicherheitseinstellungen**.
2. Wählen Sie eine Gruppe und anschließend die Agents aus, um Security Agents zu verschieben. Wählen Sie einen Messaging Security Agent aus, um ihn zu verschieben.



Tipp

Um mehrere aufeinanderfolgende Security Agents auszuwählen, klicken Sie auf den ersten Agent des Bereichs. Halten Sie die Umschalttaste gedrückt und klicken Sie dann auf den letzten Agent des Bereichs. Um mehrere nicht unmittelbar aufeinanderfolgende Agents auszuwählen, klicken Sie auf den ersten Agent des Bereichs. Halten Sie die STRG-Taste gedrückt und klicken Sie dann auf die Agents, die Sie auswählen möchten.

3. Klicken Sie auf **Verschieben**.

Ein neues Fenster wird angezeigt.

4. Geben Sie den Host-Namen und Listening-Port von Security Server 9.0 SP1 ein, zu dem die Agents verschoben werden.

5. Klicken Sie auf **Verschieben**.

Upgrade-Ergebnisse

- Die Verschiebung und das Upgrade der Online-Agents beginnt. Nach dem Upgrade:
 - Je nach Betriebssystem des Clients werden die Security Agents in der Gruppe **Desktops (Standard)** oder **Server (Standard)** in Security Server 9.0 SP1 gruppiert. Der Agent übernimmt die Einstellungen der neuen Gruppe automatisch.
 - Ein Messaging Security Agent bildet im Security Server 9.0 SP1 seine eigene Gruppe und behält seine Einstellungen bei.
- Das Upgrade von Offline-Agents erfolgt, wenn sie wieder online sind.
 - Überprüfen Sie bei Offline Messaging Security Agents den Verbindungsstatus zum Security Server.
 - Weisen Sie im Fall von Offline Security Agents die Benutzer an, eine Verbindung zum Netzwerk aufzubauen, so dass die Agents online gehen. Weisen Sie im Fall von Security Agents, die seit längerer Zeit offline sind, die Benutzer an, den Agent vom Client zu deinstallieren und anschließend mit Hilfe einer geeigneten Agent-Installationsmethode (wie dem Client Packager), die im *Administratorhandbuch* beschrieben wird, den Agent zu installieren.

Vollversion-Upgrades oder Advanced Edition Upgrades

Verwenden Sie an der Webkonsole das Fenster Produktlizenz:

- Führen Sie das Upgrade von der Test- auf die Vollversion durch.
- Führen Sie das Upgrade von der Standard auf die Advanced Edition des Produkts durch.

Test- und Vollversionen

Bei Ablauf Ihrer Testversion wird eine Benachrichtigung im Fenster Live-Status der Webkonsole angezeigt. Über die Webkonsole können Sie von einer Testversion auf eine lizenzierte Vollversion upgraden. Dabei werden Ihre Konfigurationseinstellungen beibehalten. Beim Kauf einer Lizenz für eine Vollversion erhalten Sie entweder einen Registrierungsschlüssel oder einen Aktivierungscode.

Standard und Advanced Editionen

Trend Micro bietet zwei vergleichbare Produkte zum Schutz von Clients und Netzwerken: Worry-Free Business Security Standard und Worry-Free Business Security Advanced.

TABELLE 3-1. Produktversionen

PRODUKTVERSION	WORRY-FREE BUSINESS SECURITY STANDARD	WORRY-FREE BUSINESS SECURITY ADVANCED
Client-seitige Lösung	Ja	Ja
Server-seitige Lösung	Ja	Ja
Lösung für Microsoft Exchange Server	Nein	Ja

Mit einem Aktivierungscode von Trend Micro können Sie von Worry-Free Business Security auf Worry-Free Business Security Advanced upgraden.

Vollversion-Upgrade oder Advanced Edition Upgrade

Prozedur

1. Navigieren Sie an der Webkonsole zu **Voreinstellungen > Produktlizenz**.

2. Wenn Ihnen Ihr Aktivierungscode bekannt ist, klicken Sie auf **Neuen Code eingeben**, geben Sie ihn in das Feld **Neuer Aktivierungscode** ein und klicken Sie auf **Aktivieren**.

Wenn Sie keinen Aktivierungscode haben, gehen Sie auf die Trend Micro Website unter <http://olr.trendmicro.com>, um sich online zu registrieren und Ihren Aktivierungscode zu erhalten.

Anhang A

Hilfe anfordern

In diesem Anhang wird erläutert, wie Sie Hilfe anfordern, zusätzliche Informationen erhalten und Kontakt mit Trend Micro aufnehmen können.

Die Knowledge Base von Trend Micro

Die Knowledge Base befindet sich auf der Website von Trend Micro. Sie enthält aktuelle Antworten auf Fragen zu den Produkten. Wenn Sie in der Produktdokumentation keine Antwort auf Ihre Frage finden, können Sie die Frage auch über die Knowledge Base an das Supportteam richten. Zugriff auf die Knowledge Base erhalten Sie unter:

<http://esupport.trendmicro.com/en-us/business/default.aspx>

Trend Micro aktualisiert die Einträge in der Knowledge Base regelmäßig und erweitert sie täglich um neue Lösungen. Wenn Sie keine Lösung für Ihr Problem finden, können Sie dieses auch in einer E-Mail schildern und direkt an einen Support-Mitarbeiter von Trend Micro senden, der das Problem untersucht und Ihnen schnellstmöglich weiterhilft.

Kontaktaufnahme mit dem technischen Support

Bevor Sie sich an den technischen Support von Trend Micro wenden, sollten Sie zunächst das Case Diagnostic Tool ausführen (siehe *Case Diagnostic Tool auf Seite A-3*).

Trend Micro bietet allen registrierten Benutzern technischen Support, Pattern-Downloads und Programm-Updates für die Dauer eines (1) Jahres. Nach Ablauf dieser Frist muss der Wartungsvertrag verlängert werden. Setzen Sie sich mit uns in Verbindung, wenn Sie Hilfe benötigen oder eine Frage haben. Wir freuen uns ebenso über Ihre Anregungen.

- Technischer Support:

<http://esupport.trendmicro.com/en-us/business/pages/technical-support.aspx>

- Online-Übertragung eines Support-Falls:

<http://esupport.trendmicro.com/srf/srfmain.aspx>

- Wenn Sie lieber per E-Mail kommunizieren möchten, wenden Sie sich an die folgende Adresse:

support@trendmicro.com

- In den USA steht außerdem die folgende gebührenfreie Rufnummer zur Verfügung:

(877) TREND-877 oder 877-873-6328

- Trend Micro Produktdokumentation:

<http://docs.trendmicro.com/de-de/smb.aspx>

Case Diagnostic Tool

Bei Problemen können mit dem Trend Micro Case Diagnostic Tool (CDT) die notwendigen Debugging-Informationen zum Produkt des Kunden zusammengestellt werden. Das Tool aktiviert und deaktiviert automatisch den Debug-Status und sammelt je nach Problemkategorie die erforderlichen Dateien. Diese Informationen helfen Trend Micro bei der Lösung produktbezogener Probleme.

Führen Sie das Tool auf allen Plattformen aus, die von WFBS unterstützt werden. Das Tool und die zugehörige Dokumentation können Sie von Ihrem Support-Anbieter beziehen.

Support-Anfrage beschleunigen

Bei der Kontaktaufnahme mit Trend Micro sollten Sie folgende Informationen bereithalten:

- Version von Microsoft Windows und des Service Packs
- Art des Netzwerks
- Marke und Modell des Computers sowie zusätzliche Hardware, die an den Client angeschlossen ist
- Größe des Arbeitsspeichers und des freien Festplattenspeichers auf Ihrem Client
- Ausführliche Beschreibung der Installationsumgebung
- Genauer Wortlaut eventueller Fehlermeldungen
- Schritte, um das Problem nachvollziehen zu können

Kontaktinformationen

In Deutschland erreichen Sie einen Trend Micro Vertriebspartner telefonisch, per Fax oder E-Mail unter:

Trend Micro Deutschland GmbH, Zeppelinstraße 1, 85399 Hallbergmoos

Gebührenfrei: +49 (0) 811 88990-700 Fax: +1 (408) 257-2003

Internet-Adresse: www.trendmicro.com

E-Mail: support@trendmicro.com

Verdächtige Dateien an Trend Micro senden

Wenn Sie bei einer Datei eine Infektion vermuten, die Scan Engine diese jedoch nicht entdeckt oder gesäubert hat, können Sie die verdächtige Datei an Trend Micro senden.

Außerdem können Sie an Trend Micro URLs von Websites schicken, hinter denen Sie eine Phishing-Website oder einen Infektionsüberträger vermuten, d. h. eine Quelle von Internet-Bedrohungen, wie z. B. Spyware und Viren.

- Wenden Sie sich mit der folgenden URL an den Support:
<http://esupport.trendmicro.com/en-us/business/default.aspx>

Sicherheitsinformationen

Umfassende Sicherheitsinformationen finden Sie auf der Trend Micro Website unter:

- Liste mit Viren und böartigen mobilen Codes, die zum jeweiligen Zeitpunkt im Umlauf und aktiv sind
- Viren-Falschmeldungen (Hoaxes)
- Beratung zu Internet-Bedrohungen
- Wöchentlicher Virenbericht

- Bedrohungenzyklopädie, die eine ausführliche Liste von Namen und Symptomen bekannter Viren und bösartigen mobilen Codes enthält

<http://about-threats.trendmicro.com/threatencyclopedia.aspx>

- Glossar

TrendLabs

TrendLabsSM ist das globale Netzwerk für Antiviren-Forschung und Support von Trend Micro. Auf drei Kontinenten und mit über 250 Virenforschern und -experten, die rund um die Uhr im Einsatz sind, stellt TrendLabs Service und Support für Sie und alle Trend Micro Kunden bereit.

Nach dem Kauf eines Trend Micro Produkts stehen Ihnen folgende Service-Leistungen zur Verfügung:

- Regelmäßige Viren-Pattern-Updates für alle bekannten "In-the-zoo"- und "In-the-wild"-Client-Viren und bösartigen Codes
- Notfall-Support bei Virenausbruch
- E-Mail-Kontakt mit Antiviren-Technikern
- Knowledge Base, die Online-Datenbank von Trend Micro mit Informationen über bekannte Probleme

TrendLabs besitzt die ISO-9002-Qualitätssicherungszertifizierung.

Anregungen und Kritik

Das Trend Micro Team ist stets bemüht, die Dokumentationen zu verbessern. Bei Fragen, Anmerkungen oder Anregungen zu diesem oder einem anderen Dokument von Trend Micro besuchen Sie diese Website:

<http://www.trendmicro.com/download/documentation/rating.asp>

Stichwortverzeichnis

A

Anregungen und Kritik, A-5

C

Case Diagnostic Tool, A-3

D

Dokumentation, vi

K

Knowledge Base, A-2

Kontaktaufnahme, A-2–A-5

 Anregungen und Kritik, A-5

 Knowledge Base, A-2

 Technischer Support, A-2

 Trend Micro, A-2–A-5

 Verdächtige Dateien senden, A-4

O

OfficeScan server

 Funktionen, 2-6

P

port

 Server-Listening-Port, 3-10

S

Sicherheitsinformationen, A-4

T

Technischer Support, A-2

TrendLabs, A-5

Trend Micro

 Knowledge Base, A-2

 Kontaktinformationen, A-4

 Sicherheitsinformationen, A-4

 TrendLabs, A-5

V

Verdächtige Dateien, A-4

W

Webkonsole, 1-8

 Info über, 1-8

WFBS

 Dokumentation, vi



TREND MICRO INCORPORATED

Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland

Tel.: +49 (0) 811 88990-700 Fax: +49 811 88990799 info@trendmicro.com

www.trendmicro.com

Item Code: WFGM96728/141021