TREND MICRO

# 10.0 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

Dokument-Nr.: WFEM108678/190617

Release-Datum: Juni 2019

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



## Kapitel 1: Installation und Upgrade vorbereiten



## Kapitel 2: Den Security Server installieren

## Kapitel 3: Upgrades für Security Server und Agents



## Anhang A: Technischer Support

## Stichwortverzeichnis

# 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:<br><br>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 |
| *Kursivdruck* | 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 |

| Konvention | Beschreibung |
| --- | --- |
|  **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 Endpunkten (Desktops, Laptops und Servern) in Ihrem lokalen Netzwerk. Die Version enthält die Komponenten Firewall und Virenschutz/Anti-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 von Endpunkten und Microsoft Exchange Servern 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 |
| Vorausschauendes Maschinenlernen | Ja | Ja |
| Verhaltensüberwachung | Ja | Ja |
| Benutzer-Tools | Ja | Ja |

| Funktionen | Worry-Free Business Security Standard | Worry-Free Business Security Advanced |
|---|---|---|
| Mail Scan (POP3) | Ja | Ja |
| Anti-Spam (POP3) | Ja | Ja |
| 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 Produktlizenz sowie einen Standard-Wartungsvertrag. Der Standard-Wartungsvertrag ist ein Vertrag zwischen Ihrem Unternehmen und Trend Micro, der regelt, in welchem Umfang Sie nach Zahlung der entsprechenden Gebühren Anrecht auf technischen Support und Produkt-Updates haben.

Eine Lizenz für die Trend Micro-Software enthält umfasst 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. Nachdem der Wartungsvertrag abgelaufen ist, ist zwar noch eine Suche möglich, aber Sie können die Malware-/Viren-Pattern-Dateien, die Scan-Engine und die Programmdateien nicht mehr aktualisieren (auch nicht manuell). Ebenso haben Sie keinen Anspruch mehr auf technischen Support von Trend Micro.

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

### Registrierungsschlüssel

Beim Kauf von Worry-Free Business Security erhalten Sie einen Registrierungsschlüssel. Er besteht aus 22 Zeichen (einschließlich Bindestriche) und hat das folgende Format:

Worry-Free Business Security Standard: CS-xxxx-xxxxx-xxxxx-xxxxx

Worry-Free Business Security Advanced: CM-xxxx-xxxxx-xxxxx-xxxxx

Registrieren Sie Worry-Free Business Security auf der Trend Micro Website unter https://clp.trendmicro.com mit einem lizenzierten Registrierungsschlüssel.

### Aktivierungscode

Nach der Registrierung erhalten Sie per E-Mail einen lizenzierten Aktivierungscode. Ein Aktivierungscode besteht aus 37 Zeichen (einschließlich Bindestriche) und hat das folgende Format:

Worry-Free Business Security Standard: CS-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

Worry-Free Business Security Advanced: CM-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

Geben Sie während der Installation des Security Servers Aktivierungscode ein, wenn Sie dazu aufgefordert werden. Wenn Sie dieses Feld leer ist, lassen wird die 30-Tage-Testversion von Worry-Free Business Security installiert. Führen Sie ein Upgrade auf die lizenzierte Vollversion durch, bevor die Testversion ausläuft.

### Lizenzstatus

In der folgenden Tabelle sind die die gemäß Lizenzstatus unterstützten Funktionen aufgeführt.

**TABELLE 1-2. Lizenzstatus**

| FUNKTION | LIZENZIERTE 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 |
| Echtzeitsuche | Ja | Ja | Ja, aber bei der Echtzeitsuche werden veraltete Komponenten verwendet |

Nach Ablauf eines lizenzierten Aktivierungscodes können Sie keine Updates für die Scan Engine oder für Pattern-Dateien mehr herunterladen. Nach Ablauf des Aktivierungscodes einer lizenzierten Vollversion bleiben jedoch im Gegensatz zum Aktivierungscode einer Testversion alle vorhandenen Konfigurationen und anderen Einstellungen wirksam. Durch diese Vorkehrungen wird für den Fall, dass Sie Ihre Lizenz versehentlich ablaufen lassen, ein Mindestmaß an Schutz aufrechterhalten.

Durch den erneuten Abschluss eines Wartungsvertrags können Sie die Nutzung der Vollversion von Worry-Free Business Security verlängern. Zur Installation der Vollversionen benötigen Sie einen Aktivierungscode.

Wenn Sie Fragen zum Registrierungsvorgang haben, wenden Sie sich an die 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

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 Service** 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 **Agent-Pattern von Smart Scan**, einer abgespeckten Version des herkömmlichen Viren-Pattern, nach Sicherheitsbedrohungen. Das Agent-Pattern von Smart Scan 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 Agent-Pattern von Smart Scan 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 Agent-Pattern von Smart Scan 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 zur Registerkarte **Administration** > **Allgemeine Einstellungen** > **Desktop/Server** navigieren und die Option **Smart Scan Service deaktivieren** auswählen.

## Agents

Agents schützen Clients vor Sicherheitsbedrohungen. Clients umfassen Desktops, Server und Microsoft Exchange Server. Es gibt folgende Worry-Free Business Security Agents:

**Tabelle 1-3. Worry-Free Business Security 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 Security Agents 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 Endpunkten zu verteilen.
- Agents zur gleichzeitigen Konfiguration und Verwaltung in logische Gruppen organisieren.
- Produkteinstellungen zu konfigurieren und die manuelle Suche auf Endpunkten zu starten.

- Benachrichtigungen empfangen und Protokolle zu Bedrohungsaktivitäten einsehen.
- Benachrichtigungen zu empfangen und Ausbruchswarnungen per E-Mail zu versenden, wenn Bedrohungen auf Endpunkten entdeckt werden.

# 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

Für den Security Server gelten folgende IPv6-Voraussetzungen:

- 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

Worry-Free Business Security 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 verwalteteten 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 Worry-Free Business Security 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 Worry-Free Business Security 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 Worry-Free Business Security 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

Worry-Free Business Security 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 Worry-Free Business Security 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 Agent gestartet wurde.

### Messaging Security Agent und Microsoft Server Enterprise

Der Messaging Security Agent unterstützt einige Funktionen von Microsoft Exchange Server Enterprise nicht, wie beispielsweise die Datenverfügbarkeitsgruppe (Data Availability Group, DAG).

### Security Agents und Windows Defender

Durch die Installation des Security Agents wird Windows Defender deaktiviert.

### 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 Worry-Free Business Security 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 *Worry-Free Business Security Ports auf Seite 2-8*. Informationen über die Konfiguration von Ausschlusslisten finden Sie in Ihrer Firewall-Dokumentation).

## Worry-Free Business Security Ports

Worry-Free Business Security verwendet die folgenden Ports:

- **Server-Listening-Port (HTTP-Port)**: Für den Zugriff auf den Security Server. Standardmäßig verwendet Worry-Free Business Security 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 | VORINSTALLIERTER 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<br>SSL verwenden | SSL-Port auf Webserver | Erster offener Port im Bereich 4345 bis 65536 | n. v. | SSL-Port auf Webserver |
| SSL-Port<br>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):<br>• C:\Programme\Trend Micro\Security Server<br>• C:\Programme (x86)\Trend Micro \Security Server | |
| 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:<br>• Apache<br>• IIS (Standard-Website)<br>• IIS (virtuelle Website) | |
| Listening-Port (HTTP) | 8059 | |
| Listening-Port (HTTPS) | 4343 | |
| Kennwort der Web-Konsole | Benutzerdefiniert | |
| Security Agent Deinstallationskennwort | Benutzerdefiniert | |

| Informationen | Standardwerte | Ihr Wert |
|---|---|---|
| | | |
| **(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 | |
| | | |
| **(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 | |

| INFORMATIONEN | STANDARDWERTE | IHR WERT |
|---|---|---|
| Installationspfad | Einer der folgenden (abhängig vom Betriebssystem):<br>• C:\Programme\Trend Micro\Security Agent<br>• C:\Programme (x86)\Trend Micro \Security Agent | |
| **(Optional) Proxy-Authentifizierung für Funktionen des Security Agent (Verhaltensüberwachung, Web Reputation und Smart Scan)**<br><br>**Hinweis**<br>Security Agents verwenden die in Internet Explorer konfigurierten Proxy-Einstellungen. | | |
| Benutzername zur Authentifizierung | Benutzerdefiniert | |
| Authentifizierungskennwort | Benutzerdefiniert | |
| | | |
| **(Optional) Messaging Security Agents** | | |
| IPv4/IPv6-Adresse des Microsoft Exchange Servers | Benutzerdefiniert | |
| Vollqualifizierter Domänenname (FQDN)<br>des Microsoft Exchange Servers | Benutzerdefiniert | |
| NetBIOS (Host)-Name des Microsoft Exchange Servers | Benutzerdefiniert | |
| Domänenadministratorkonto und -kennwort für die Anmeldung am Microsoft Exchange Server | Benutzerdefiniert | |

| Informationen | Standardwerte | Ihr Wert |
|---|---|---|
| Listening-Port | 16372 | |
| Installationspfad | Einer der folgenden (abhängig vom Betriebssystem):<br>• C:\Programme \TrendMicro\Messaging Security Agent<br>• C:\Programme (x86)\Trend Micro \Messaging Security Agent | |
| 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.<br>• Starten Sie das Installationspaket.<br>• Akzeptieren Sie die Bedingungen der Lizenzvereinbarung.<br>• Wählen Sie einen Setup-Typ.<br>  • Typische Installation (empfohlen)<br>  • Minimal<br>  • Benutzerdefiniert<br>• 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:<br>• Installationsspeicherort des Security Servers<br>• Kennwörter für das Administratorkonto<br>• Einstellungen des SMTP-Servers und Empfänger von Benachrichtigungen<br>• Smart Protection Network |
| | Konfigurieren Sie für eine benutzerdefinierte Installation alle benutzerdefinierbaren Einstellungen, einschließlich:<br>• Grundeinstellungen<br>  • Installationsspeicherort des Security Servers<br>  • Speicherort der Suchserver-Datenbank<br>  • Installation des Security Agents oder Messaging Security Agents auf demselben Computer wie der Security Server oder an einem anderen Installationsort<br>• Einstellungen des Security Servers<br>  • Webserver<br>  • Kennwort für das Administratorkonto<br>  • Einstellungen des SMTP-Servers und Empfänger von Benachrichtigungen<br>  • Smart Protection Network<br>  • Allgemeine Proxy-Einstellungen<br>• Einstellungen des Security Agents<br>  • Security Agent Installationspfad<br>  • Zu aktivierende Funktionen des Security Agents<br>  • Proxy-Einstellungen für zusätzliche Dienste<br>• Einstellungen des Messaging Security Agents<br>  • Einstelllungen des Microsoft Exchange Servers<br>  • 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

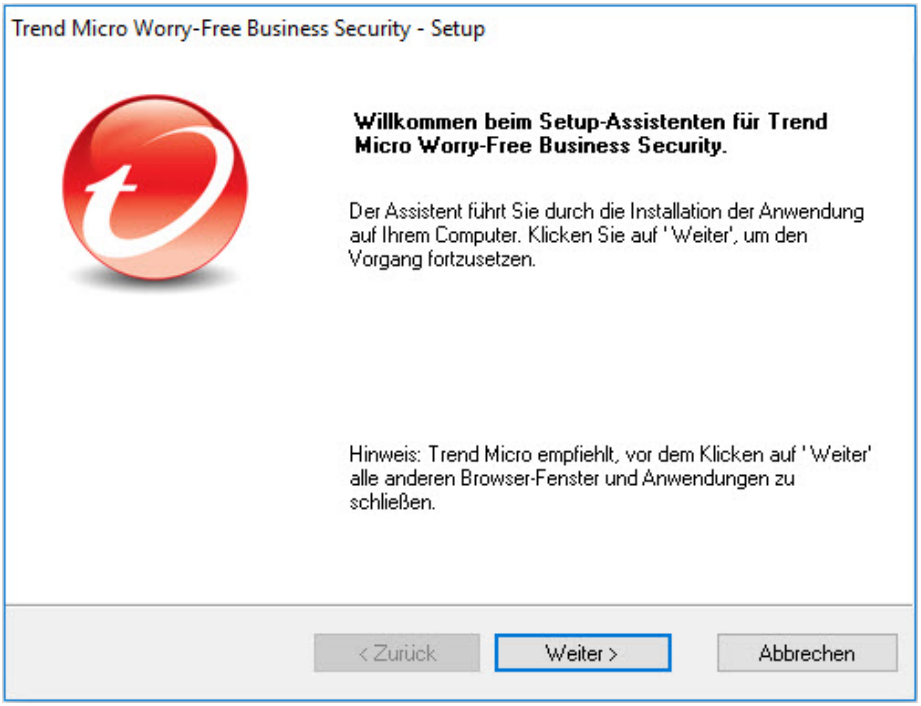
- Melden Sie sich am Computer mit Domänenadministratorrechten oder lokalen Administratorrechten an.
- Schließen Sie vor der Installation von Worry-Free Business Security alle aktiven Anwendungen. Der Installationsvorgang dauert möglicherweise länger, wenn vor der Installation nicht alle Anwendungen geschlossen 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

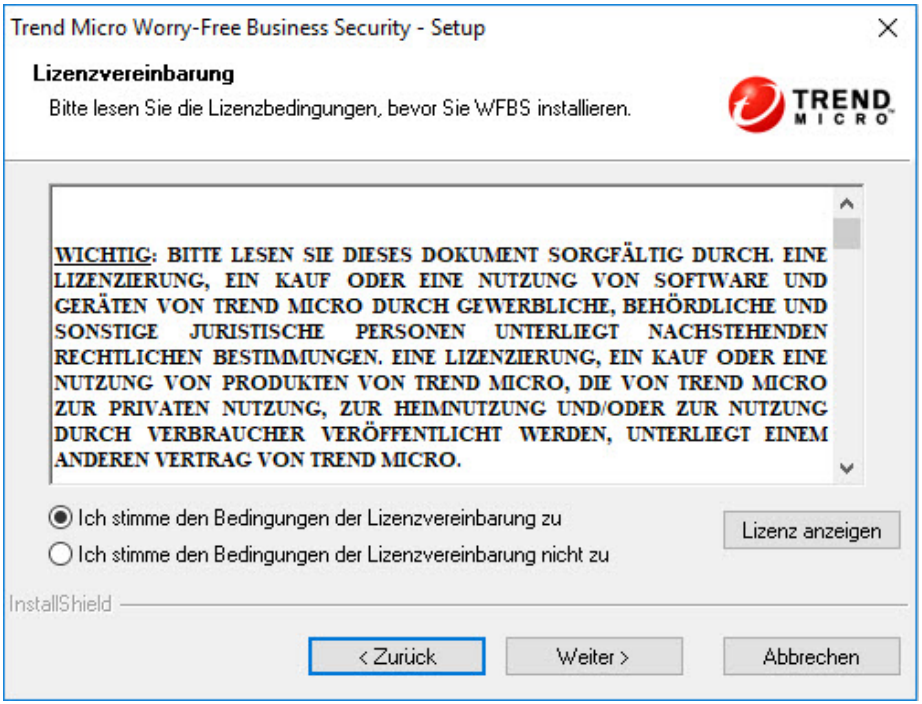
Doppelklicken Sie auf das Installationspaket (`.exe`-Datei).


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.

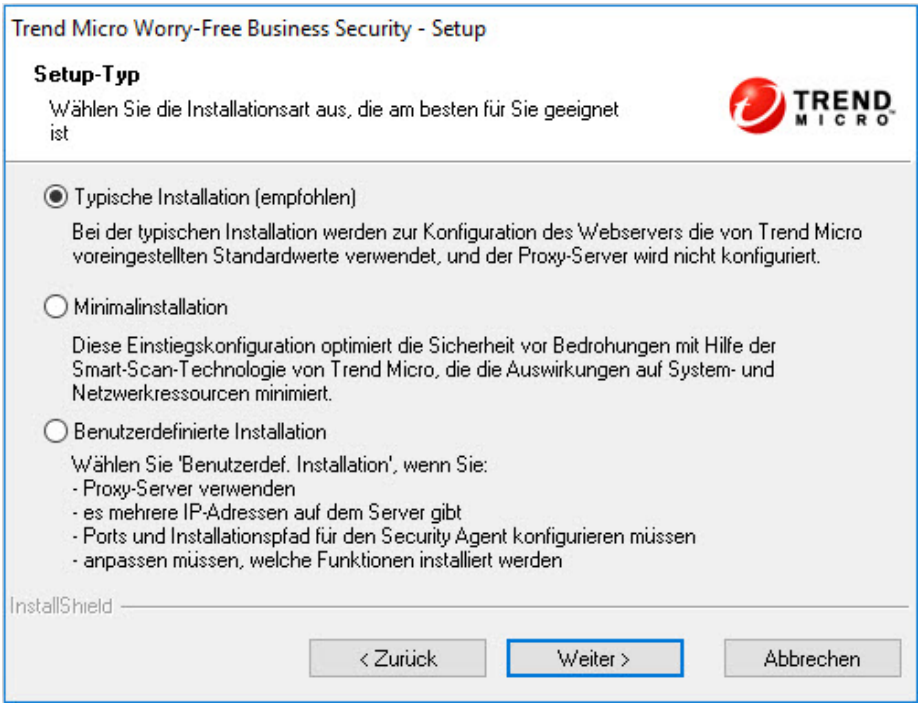

Trend Micro Worry-Free Business Security - Setup
Willkommen beim Setup-Assistenten für Trend Micro Worry-Free Business Security.
Der Assistent führt Sie durch die Installation der Anwendung auf Ihrem Computer. Klicken Sie auf 'Weiter', um den Vorgang fortzusetzen.
Hinweis: Trend Micro empfiehlt, vor dem Klicken auf 'Weiter' alle anderen Browser-Fenster und Anwendungen zu schließen.
< Zurück
Weiter >
Abbrechen

## Lizenzvereinbarung




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

## 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 10)
- Web Reputation
- URL-Filter
- Smart Scan

**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**

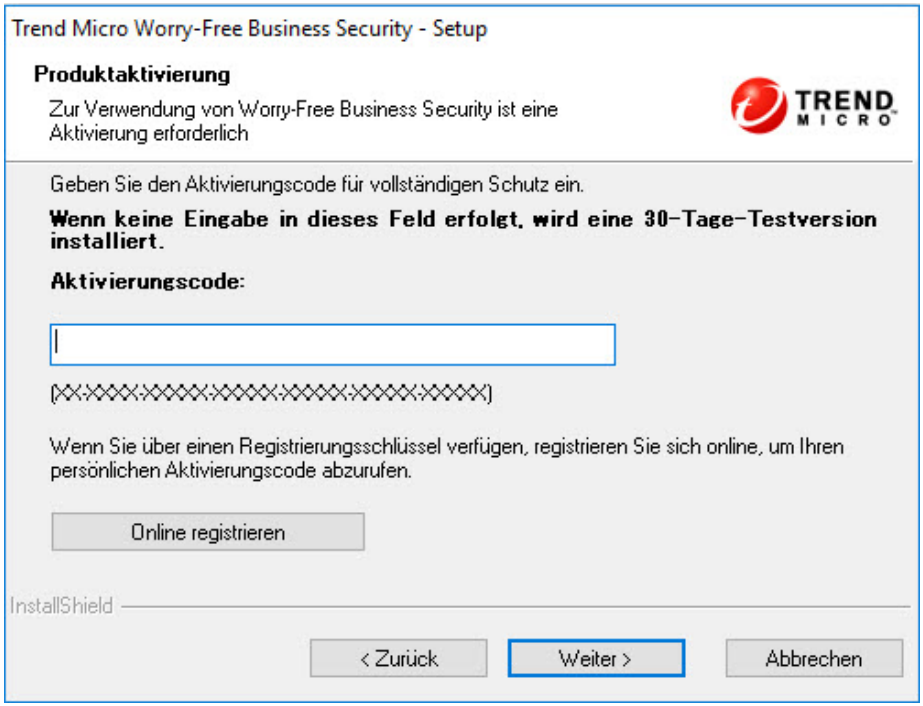
  Manchmal wird die Endpunkt-Sicherheitssoftware nur erkannt, aber nicht deinstalliert. Deinstallieren Sie in diesem Fall die Software zuerst manuell.

  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




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

Wenn Sie über keinen Aktivierungscode verfügen, haben Sie Ihre Version von Worry-Free Business Security 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 2-25*
  - *Phase 3: Installation auf Seite 2-53*

- Wenn Sie die benutzerdefinierte Installation auswählen, gehen Sie wie folgt vor:
  - *Einstellungen für eine benutzerdefinierte Installation konfigurieren auf Seite 2-31*
  - *Phase 3: Installation auf Seite 2-53*

## Phase 2: Einstellungen gemäß Setup-Typ konfigurieren

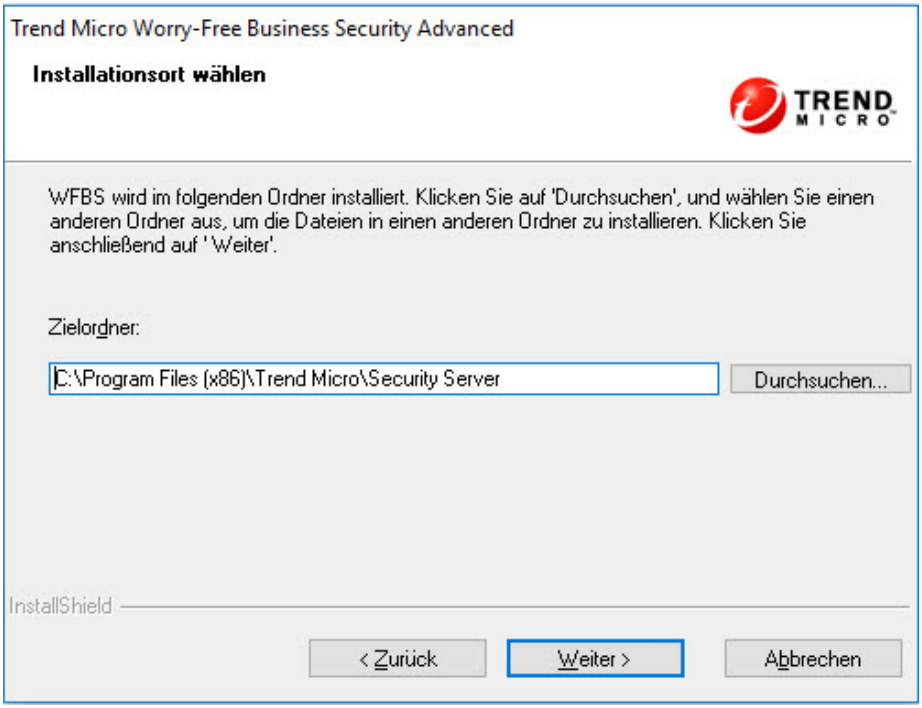
Die in Phase 2 zu konfigurierenden Einstellungen hängen vom Setup-Typ ab, den Sie in Phase 1 auswählen.

- *Einstellungen für eine typische Installation oder eine Minimalinstallation konfigurieren auf Seite 2-25*
- *Einstellungen für eine benutzerdefinierte Installation konfigurieren auf Seite 2-31*

## Einstellungen für eine typische Installation oder eine Minimalinstallation konfigurieren

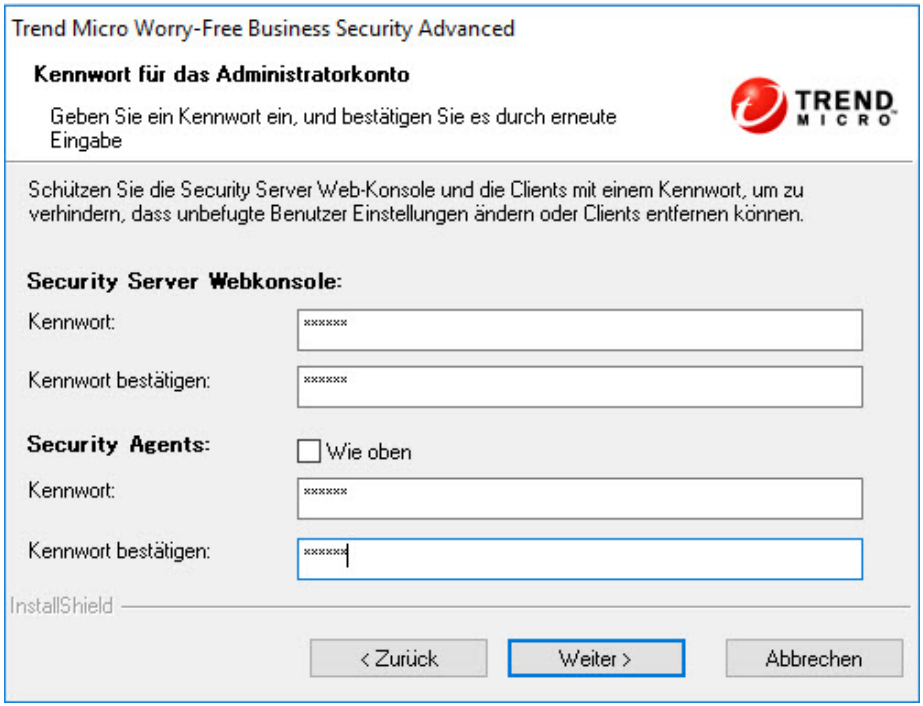
Wenn Sie eine typische Installation oder Minimalinstallation durchführen, werden folgende Fenster der Reihe nach angezeigt:

## Installationsspeicherort




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

## Kennwort für das Administratorkonto



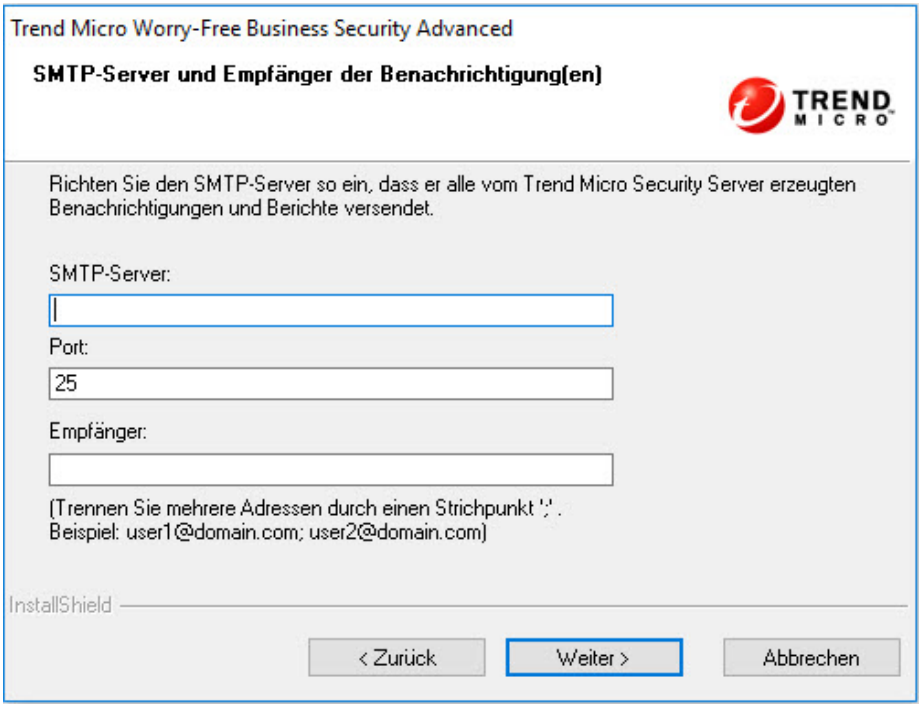

Richten Sie verschiedene Kennwörter für die Security Server Webkonsole und den Security Agent ein.

- **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)




Geben Sie die folgenden Informationen an:

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

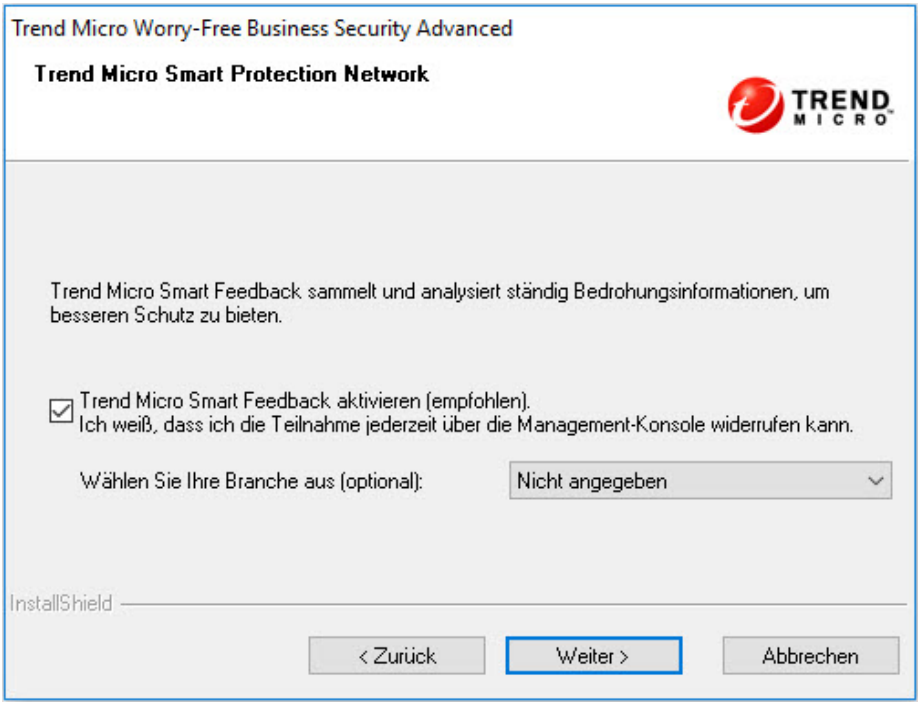
**Hinweis**

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



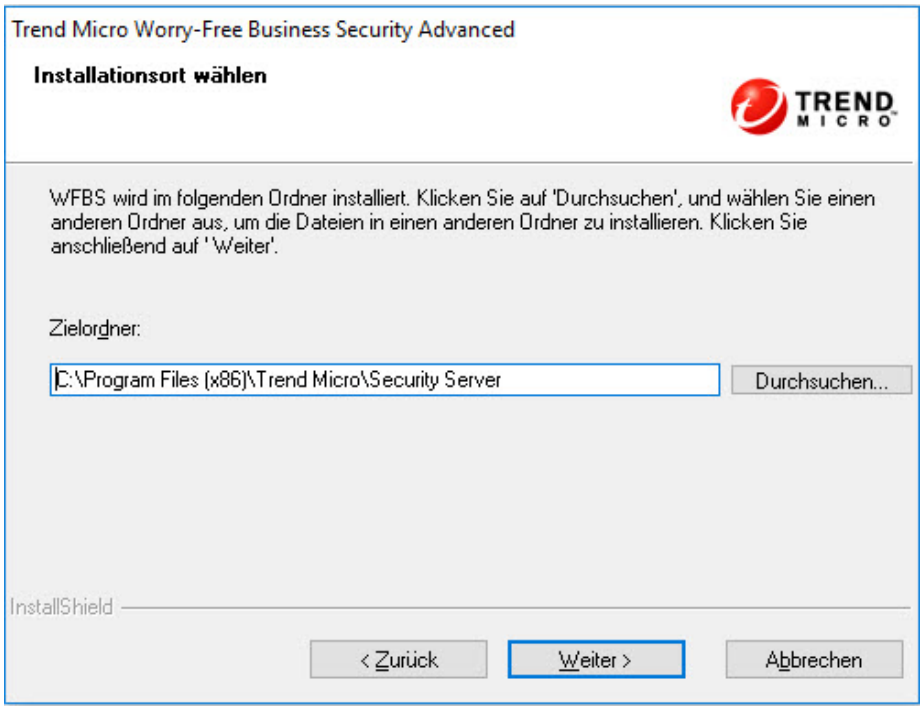

Wählen Sie, ob Sie am Trend Micro Smart Protection Network Feedback-Programm teilnehmen möchten.

Über diese optionale Funktion erhält Trend Micro Feedback zu Malware-Infektionen. Trend Micro empfiehlt, den Standardwert zu übernehmen, da mit Hilfe der weltweiten Worry-Free Business Security 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



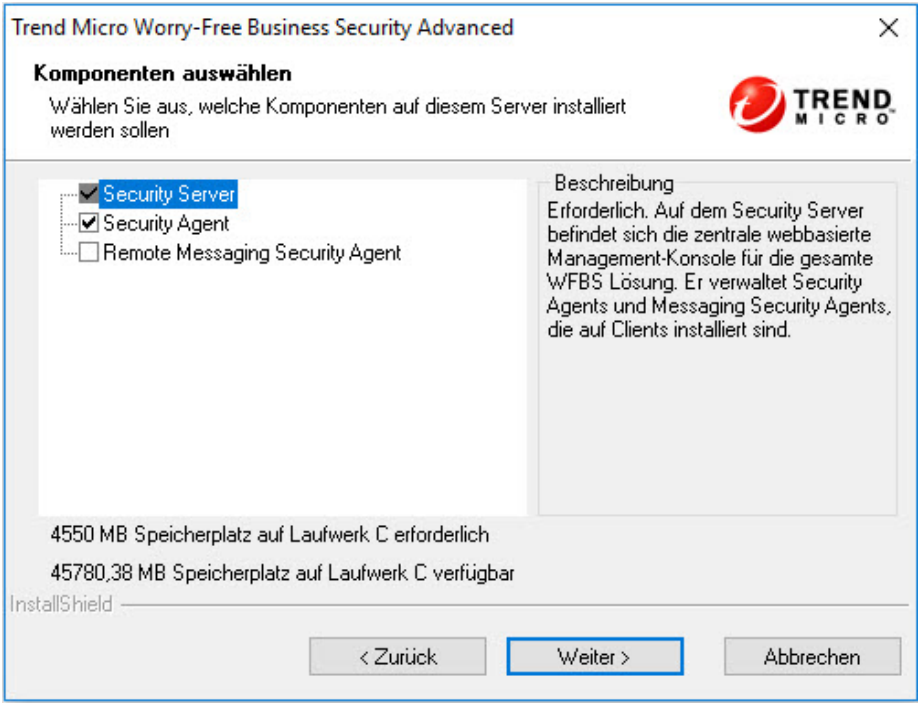

Standardmäßig ist als Worry-Free Business Security Installationsordner `C:\Programme\Trend Micro\Security Server` oder `C:\Programme (x86)\Trend Micro\Security Server` festgelegt. Klicken Sie auf

**Durchsuchen**, wenn Sie Worry-Free Business Security in einem anderen Ordner installieren möchten.

### Speicherort der Suchserver-Datenbank


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).

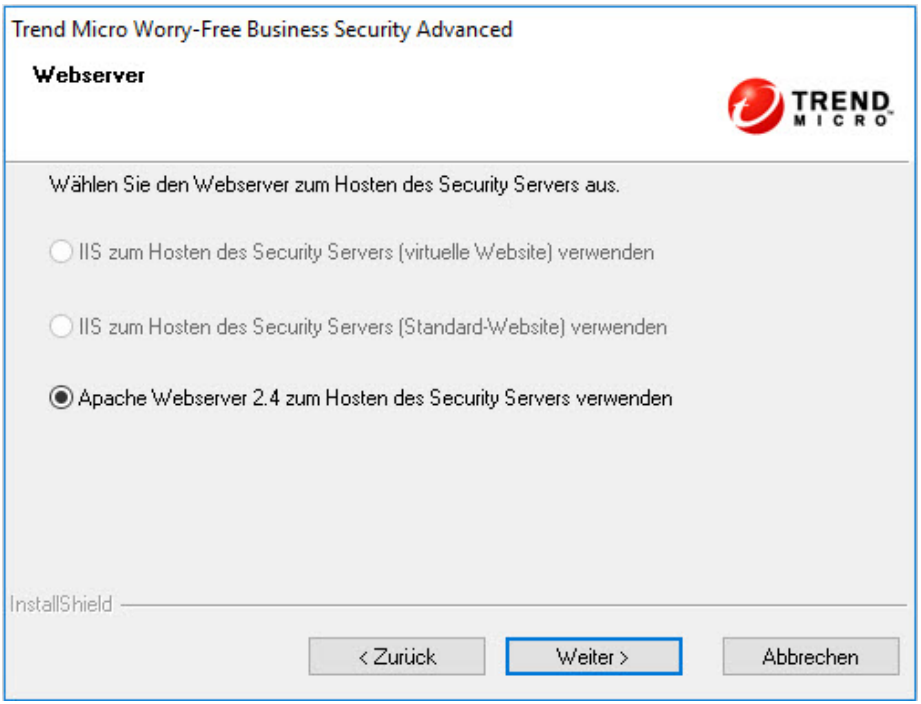
**Hinweis**

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.

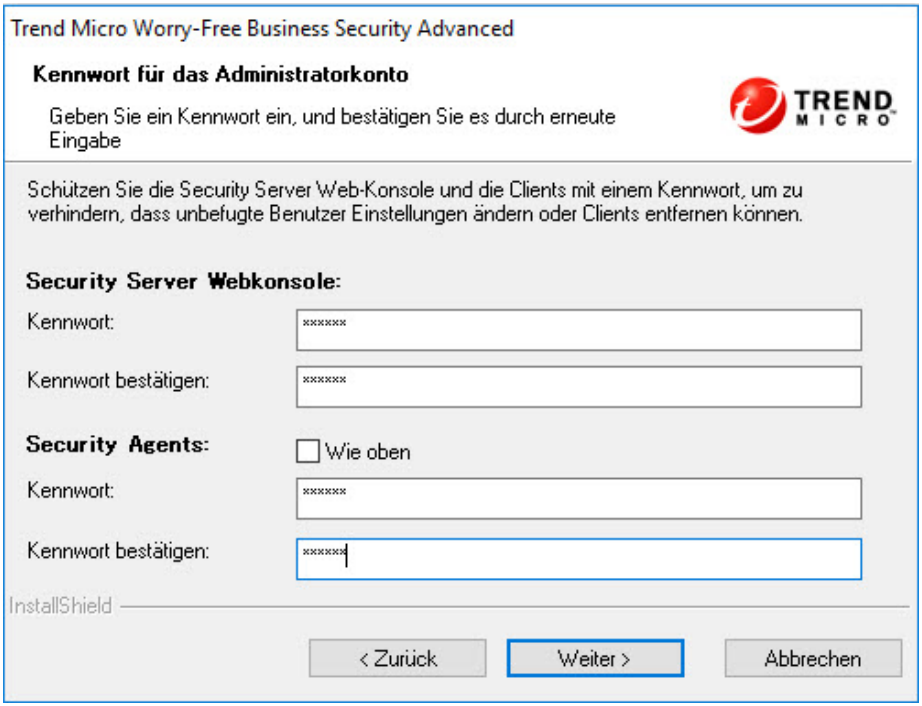
| Szenario | Ergebnis | Hinweise |
|---|---|---|
| Während des Setups werden sowohl IIS als auch Apache Webserver erkannt. | • Bei einer typischen oder Minimalinstallation wird automatisch IIS verwendet.<br>• Benutzerdefinierte Installation:<br>  • Es wird automatisch IIS verwendet, wenn die Version des Apache Webservers nicht unterstützt wird.<br>  • Wenn die Version des Apache Webservers unterstützt wird, haben Sie freie Wahl. | Wenn auf dem Computer Windows 7, 8.1 oder 10 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.<br>• Bei einer benutzerdefinierten Installation haben Sie die freie Wahl zwischen beiden Webservern. Wenn Sie sich für Apache entscheiden, wird automatisch Apache 2.4 installiert. | |

| Szenario | Ergebnis | Hinweise |
|---|---|---|
| Während des Setups wird nur ein Apache Webserver erkannt. | • Es wird Apache verwendet, wenn es sich um Version 2.4 handelt.<br>• Andere Versionen von Apache können nicht installiert werden. Ziehen Sie folgende Maßnahmen in Betracht:<br>  • Deinstallation von Apache, wenn keine Anwendung diesen Webserver verwendet<br>  • Upgrade von Apache auf Version 2.4.<br>  • Auswahl eines anderen Computers, auf dem der Security Server installiert werden soll | Die folgenden Plattformen verwenden IIS und werden vom Security Server unterstützt:<br>• Windows Server 2008/2008 R2<br>• Windows SBS 2008<br>• Windows EBS 2008<br>• Windows SBS 2011 Standard/ Essentials<br>• Windows Server 2012/2012 R2<br>• Windows Server 2016<br>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 2.4 installiert. | |

Bei Upgrades, wenn Apache derzeit als Webserver verwendet wird:

- Wenn der Apache Webserver vom Setupprogramm von Worry-Free Business Security 8.x/9.x installiert wurde, wird ein automatisches Upgrade von Apache auf Version 2.4 durchgeführt.
- Wurde er dagegen von einem anderen Programm installiert, wird die bestehende Version von Apache beibehalten.

## Kennwort für das Administratorkonto



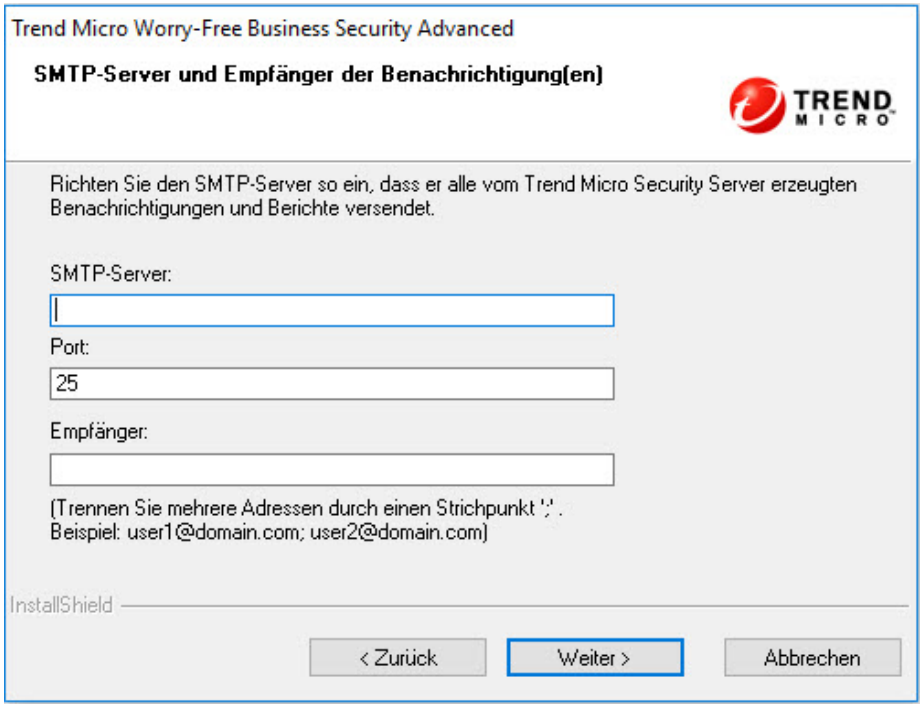

Richten Sie verschiedene Kennwörter für die Security Server Webkonsole und den Security Agent ein.

- **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)




Geben Sie die folgenden Informationen an:

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

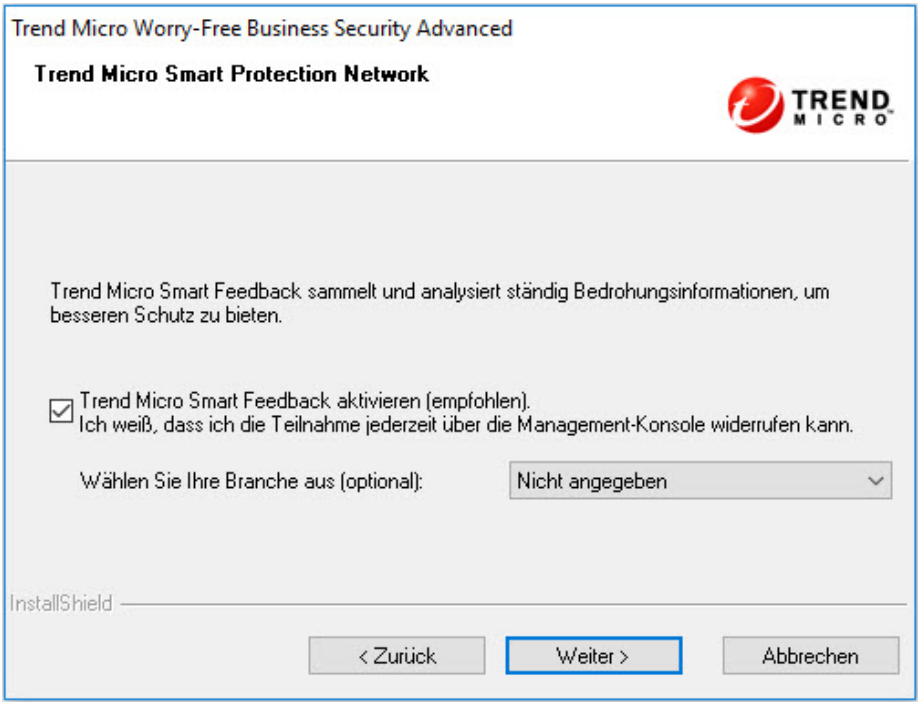
**Hinweis**

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.

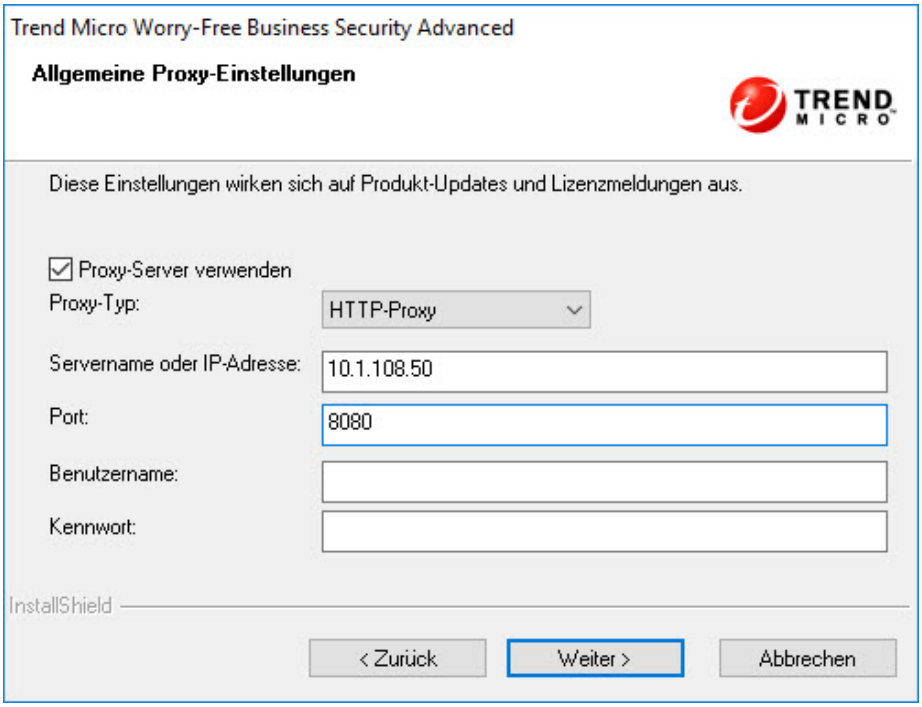
## Smart Protection Network




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 Worry-Free Business Security 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




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

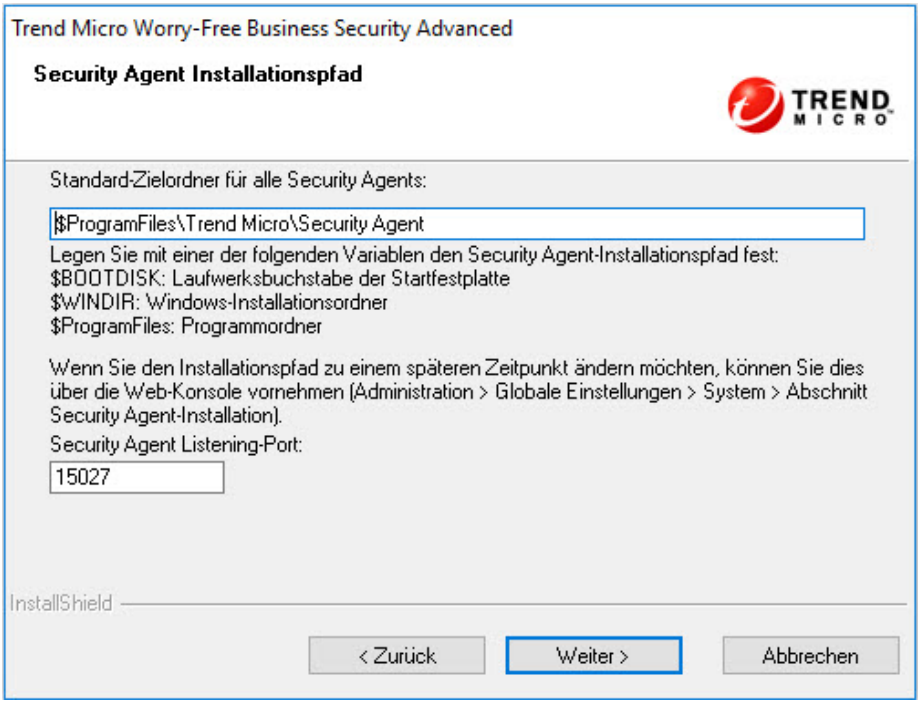
- **Proxy-Server-Typ**
- **Servername oder IP-Adresse**
- **Port**
- **Benutzername und Kennwort**: nur erforderlich, wenn der Proxy-Server eine Authentifizierung erfordert.

## 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.

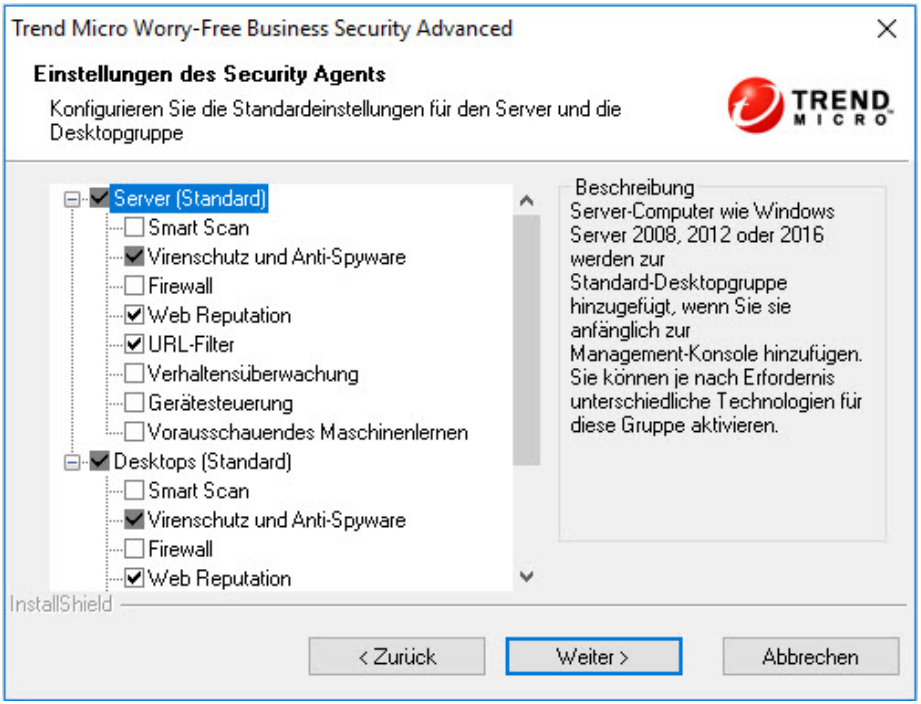
## Security Agent Installationspfad




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



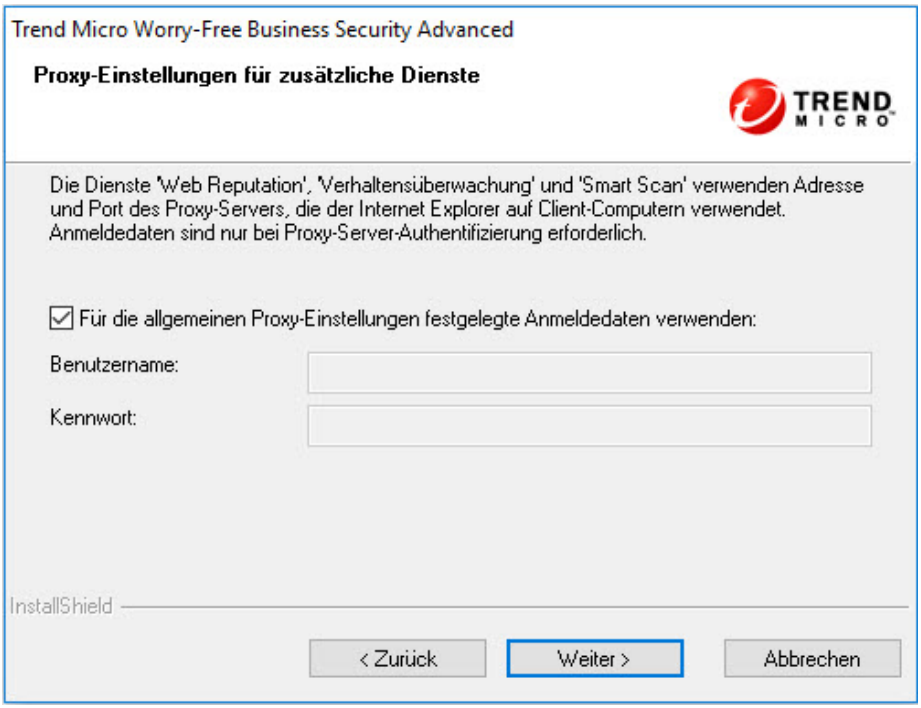

Einstellungen des Security Agents für Server und Desktops

- **Server**: Security Agents unter Windows Server-Plattformen (z. B. Windows Server 2016) 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 10) 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 bösartigen 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 bösartige 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.
- **Gerätesteuerung**: Reguliert den Zugriff auf externe Speichergeräte und Netzwerkressourcen
- **Vorausschauendes Maschinenlernen**: Verwendet eine hochentwickelte Technologie für das maschinelle Lernen zum Korrelieren von Bedrohungsinformationen und Durchführen umfassender Dateianalysen, um neue unbekannte Sicherheitsrisiken durch digitale DNA-Fingerabdrücke, API-Mapping und andere Dateifunktionen zu erkennen.

## Proxy-Einstellungen für zusätzliche Dienste




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 Endpunkt Informationen zu einer vorherigen Messaging Security Agent-Installation vorhanden sind. Mit der **Problembehandlung für Programminstallation und -deinstallation** können Sie Überreste einer früheren Installation entfernen.

  Weitere Informationen zur **Problembehandlung für Programminstallation und -deinstallation** finden Sie unter https://support.microsoft.com/en-us/help/17588/.
- 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.

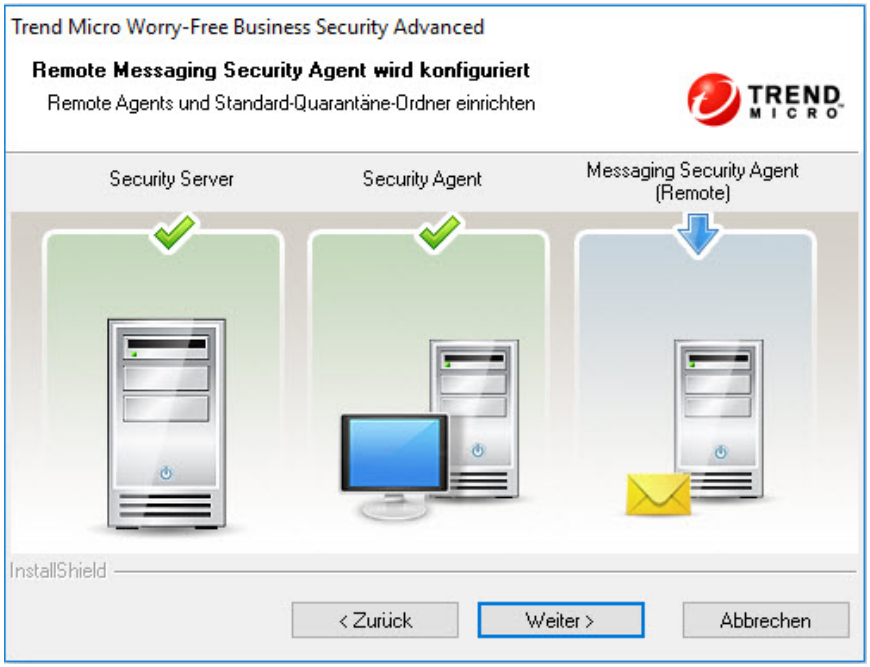
Setup fordert Sie zur Installation des Messaging Security Agents auf, wenn:

- Wenn eine Installation des Security Servers auf einem Computer durchgeführt wird, auf dem auch ein Microsoft Exchange Server

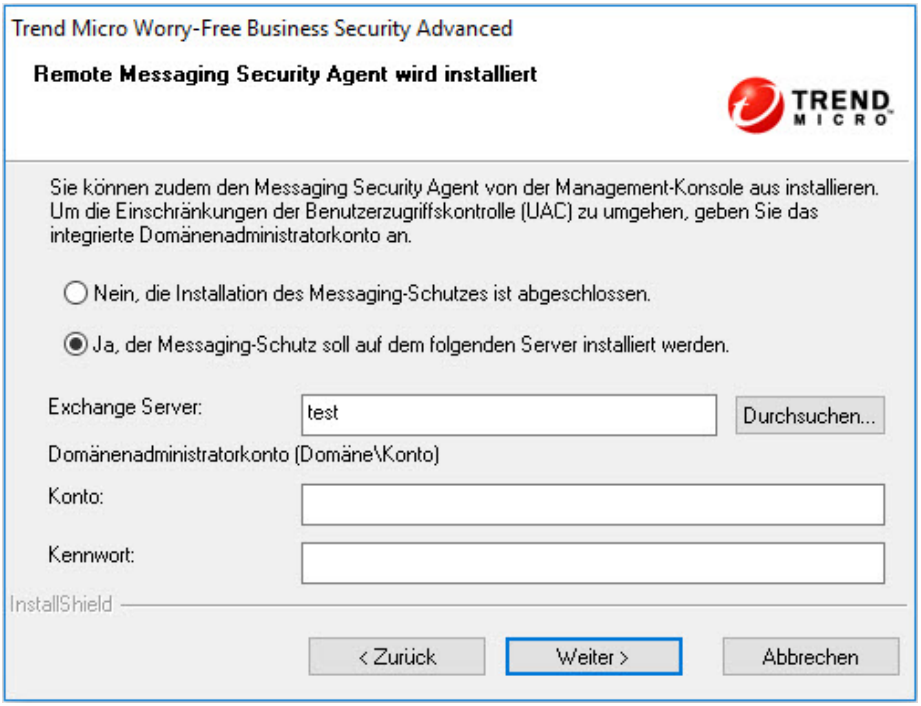
installiert ist, werden Sie vom Setup aufgefordert, einen **lokalen** Messaging Security Agent zu installieren.


- 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




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.

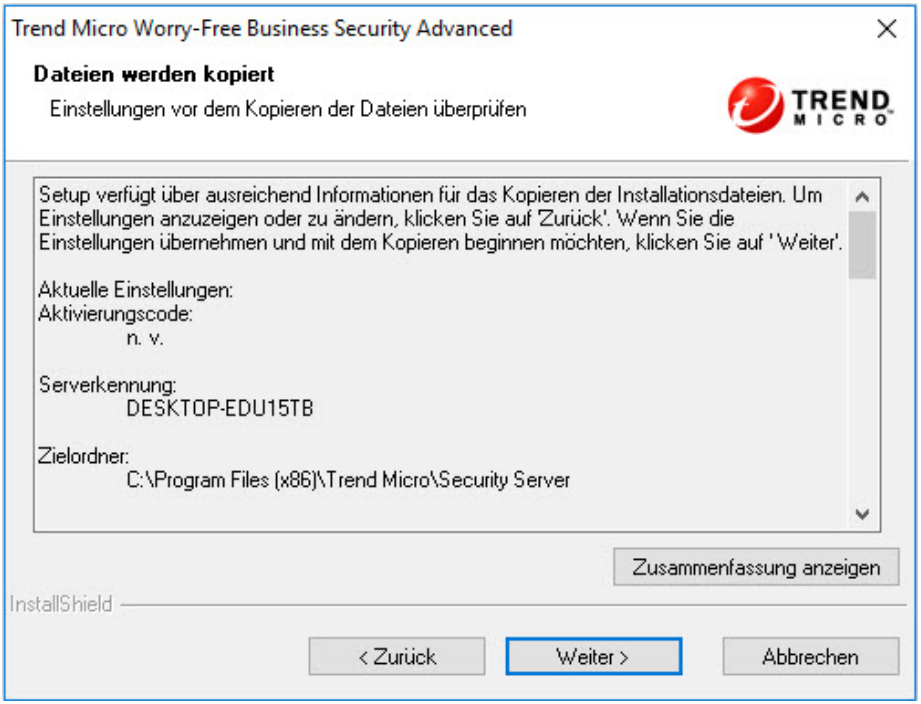
- **Domänenadministratorkonto**
- **Kennwort**

**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.

## Phase 3: Installation

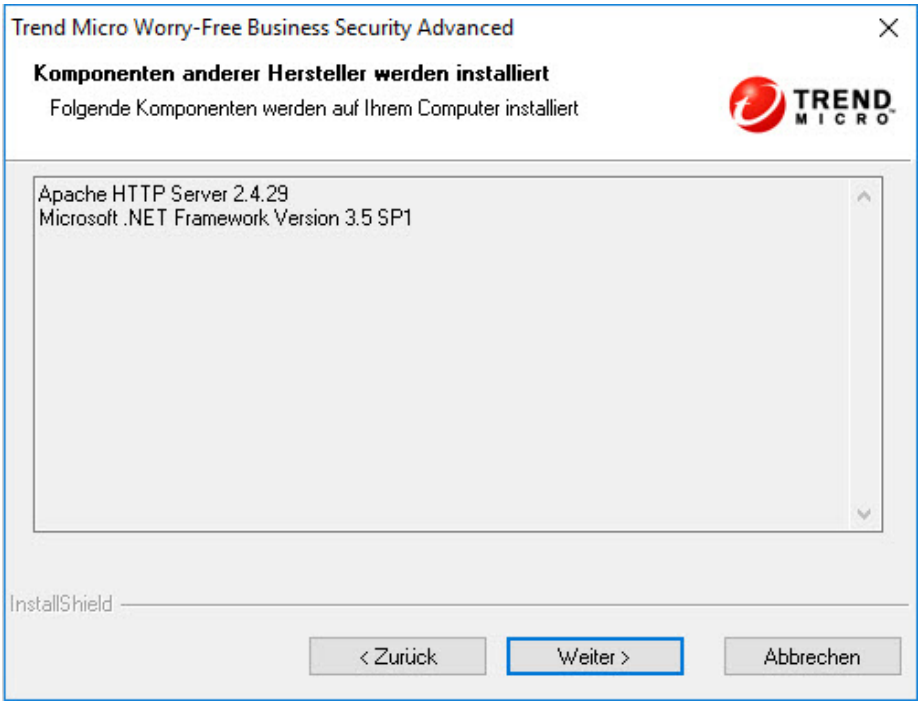
### Dateien werden kopiert




Das Fenster Dateien werden kopiert zeigt eine Zusammenfassung aller Parameter an, die bei der Installation von Worry-Free Business Security verwendet werden.

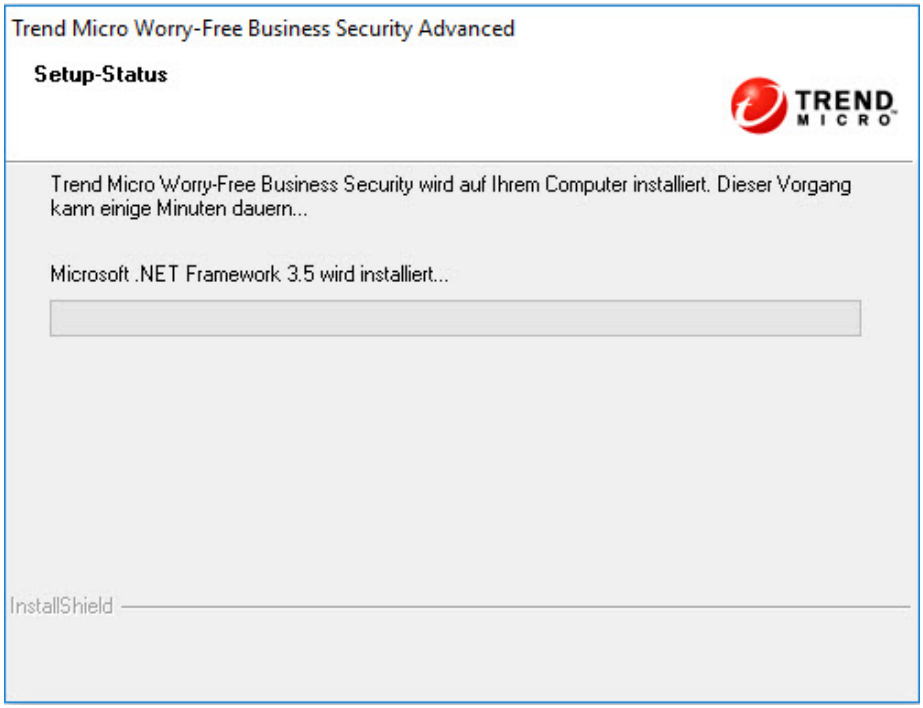
Klicken Sie auf **Zurück**, wenn Sie die bisherigen Installationseinstellungen überprüfen möchten, oder auf **Weiter**, um mit der aktuellen Installation fortzufahren.

## Komponenten anderer Hersteller installieren



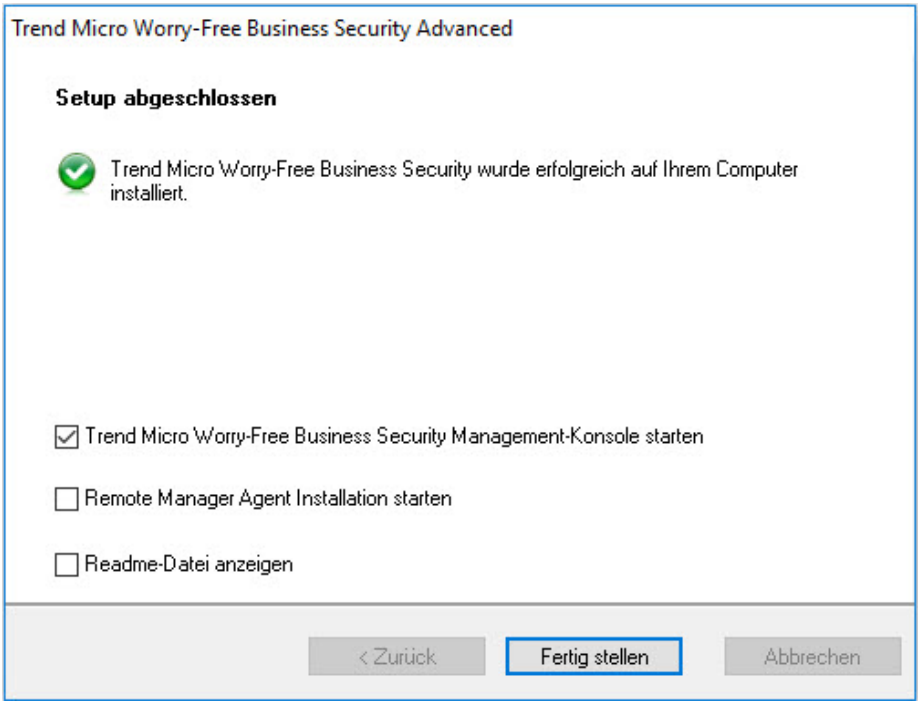

Dieses Fenster enthält Informationen über die Komponenten anderer Hersteller, die installiert werden. Klicken Sie auf **Weiter**, um mit der Installation der ausgewählten Komponenten zu beginnen.

## 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.

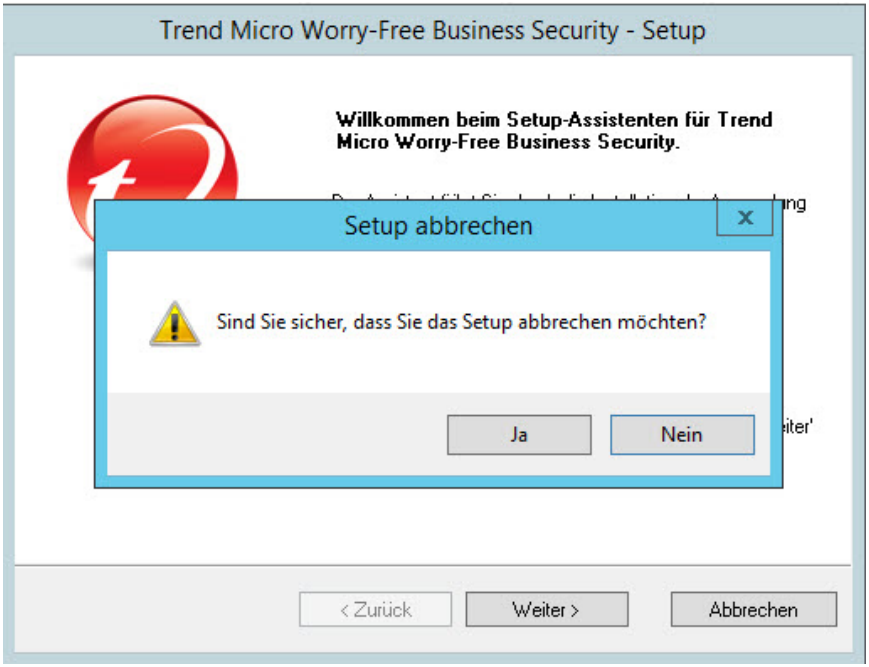
# Mehrere Security Server mit der unbeaufsichtigten Installation installieren

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

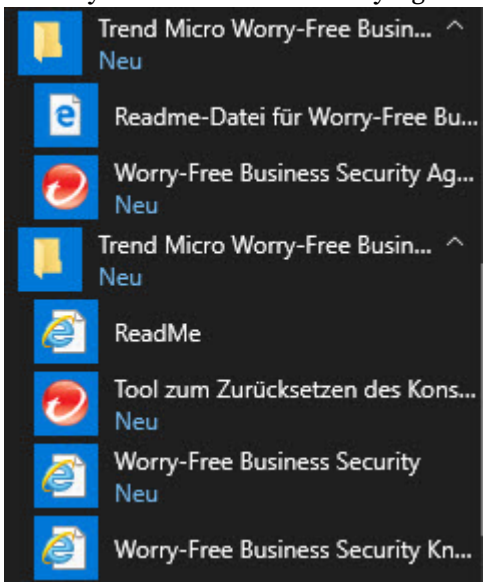
3. Um zu überprüfen, ob die Installation erfolgreich war, öffnen Sie die Datei `c:\setup.log`. Ist der Ergebniscode `ResultCode=0`, war die Installation erfolgreich.

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` statt `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, für den das Upgrade durchgeführt werden soll, muss auf Windows 7, 8.1, 10, Server 2008, 2012, 2012 R2, 2016, 2019 oder SBS 2008/2011 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.
- Weisen Sie dem Security Server eine IPv6-Adresse zu. Zusätzlich muss der Server über seinen Hostnamen identifiziert werden, vorzugsweise seinen vollqualifizierten Domänennamen (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. Legen Sie für die zu löschenden Protokolltypen die Option **Protokolle löschen, die älter sind als** auf 0 fest.
3. Wählen Sie eine der folgenden Methoden aus, um Protokolle zu löschen:
   - Klicken Sie auf **Löschen** in jedem Protokolltyp.
   - Klicken Sie auf **Alle löschen**, um alle Protokolle zu löschen.

# Upgrades der Vorgängerversion

Diese Produktversion unterstützt Upgrades von einer beliebigen der folgenden Worry-Free Business Security oder Worry-Free Business Security-Advanced Versionen:

- 10,0
- 9.x (einschließlich aller Servicepacks)
- 8.x (8.0 und 8.0 SP1)

Diese Produktversion unterstützt keine Upgrades von:

- Worry-Free Business Security oder Worry-Free Business Security-Advanced 7.x
- Worry-Free Business Security oder Worry-Free Business Security-Advanced 6.x
- Worry-Free Business Security oder Worry-Free Business Security-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.

Nach Abschluss des Upgrades:

- Upgrade der Security Agents, die online sind, wird sofort durchgeführt
- Upgrade der Security Agents, die offline sind, wird ausgeführt, wenn sie wieder online sind

  Weisen Sie die Benutzer an, eine Verbindung zum Netzwerk aufzubauen, sodass der Security Agent online gehen kann. Weisen Sie im Fall von Security Agents, die seit längerer Zeit offline sind, die Benutzer an, den Security Agent vom Endpunkt zu deinstallieren und anschließend mit Hilfe einer geeigneten Agent-Installationsmethode (wie dem Client Packager), die im *Administratorhandbuch* beschrieben wird, den Security 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: Security Agents auf Security Server 10.0 Service Pack 1 verschieben

Führen Sie eine Erstinstallation des Security Servers durch, und verschieben Sie anschließend die Security Agents auf diesen Server. Die Security Agents werden beim Verschieben automatisch auf Version 10.0 Service Pack 1 aktualisiert.

## Teil 1: Erstinstallation von Security Server 10.0 Service Pack 1 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 die Informationen von Security Server 10.0 Service Pack 1. Geben Sie beim Verschieben der Agents diese Informationen auf dem unterstützten Security Server 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 des unterstützten Security Servers zu **Sicherheitseinstellungen**.
2. Wählen Sie eine Gruppe und anschließend die Agents aus, um Security Agents 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 **Client-Hierarchie verwalten** > **Client verschieben**.

   Ein neues Fenster wird angezeigt.

4. Geben Sie den Host-Namen und Listening-Port des Security Servers 10.0 Service Pack 1 ein, auf den die Agents verschoben werden.

5. Klicken Sie auf **Verschieben**.

### Upgrade-Ergebnisse

- Die Verschiebung und das Upgrade der Online-Agents beginnt. Je nach Betriebssystem des Endpunkts werden die Security Agents nach dem Upgrade in der Gruppe **Desktops (Standard)** oder **Server (Standard)** in Security Server 10.0 Service Pack 1 zusammengefasst. Der Agent übernimmt die Einstellungen der neuen Gruppe automatisch.
- Das Upgrade von Offline-Agents erfolgt, wenn sie wieder online sind. Weisen Sie die Benutzer an, eine Verbindung zum Netzwerk aufzubauen, sodass die Agents online gehen können. Weisen Sie im Fall von Security Agents, die seit längerer Zeit offline sind, die Benutzer an, den Security Agent vom Endpunkt zu deinstallieren und anschließend mit Hilfe einer geeigneten Agent-Installationsmethode (wie dem Client Packager), die im *Administratorhandbuch* beschrieben wird, den Security 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 Standard auf Worry-Free Business Security Advanced upgraden.

## Vollversion-Upgrade oder Advanced Edition Upgrade

**Prozedur**

1. Navigieren Sie auf der Webkonsole zu **Administration** > **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

## Technischer Support

Erfahren Sie mehr über die folgenden Themen:

# Ressourcen zur Fehlerbehebung

Vor der Kontaktaufnahme mit dem technischen Support sollten Sie die folgenden Online-Ressourcen zu Trend Micro heranziehen.

## Support-Portal verwenden

Über das Trend Micro Support-Portal können Sie rund um die Uhr online auf die aktuellsten Informationen über allgemeine und ungewöhnliche Probleme zugreifen.

**Prozedur**

1. Gehen Sie zu http://esupport.trendmicro.com.
2. Wählen Sie unter den verfügbaren Produkten aus oder klicken Sie auf die entsprechende Schaltfläche, um nach Lösungen zu suchen.
3. Mit dem Feld **Support durchsuchen** können Sie nach verfügbaren Lösungen suchen.
4. Falls Sie keine Lösung finden, klicken Sie auf **Support kontaktieren** und wählen Sie den gewünschten Support aus.

**Tipp**

Um online eine Supportanfrage zu senden, besuchen Sie die folgende URL:

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

Das Problem wird von einem Support-Mitarbeiter von Trend Micro untersucht, der innerhalb von 24 Stunden oder weniger auf Ihre Anfrage reagiert.

## Bedrohungsenzyklopädie

Die meiste Malware besteht heutzutage aus komplexen Bedrohungen, bei denen zwei oder mehr Technologien miteinander kombiniert werden, um Computer-Sicherheitsprotokolle zu umgehen. Trend Micro bekämpft diese komplexe Malware mit Produkten, die eine benutzerdefinierte Verteidigungsstrategie verfolgen. Die Bedrohungsenzyklopädie enthält eine ausführliche Liste mit Namen und Symptomen von verschiedenen kombinierten Bedrohungen, wie etwa bekannte Malware, Spam, bösartige URLs und bekannte Schwachstellen.

Auf http://about-threats.trendmicro.com/de/threatencyclopedia#malware finden Sie weitere Informationen zu folgenden Themen:

- Malware und bösartige mobile Codes, die zum jeweiligen Zeitpunkt aktiv und im Umlauf sind
- Seiten mit Bedrohungsinformationen, die eine umfassende Ressource für Internet-Angriffe darstellen
- Beratung zu Internet-Bedrohungen bezüglich gezielten Angriffen und Sicherheitsbedrohungen
- Informationen zu Internet-Angriffen und Online-Trends
- Wöchentliche Malware-Berichte

# Kontaktaufnahme mit Trend Micro

Sie erreichen Ihre Trend Micro Ansprechpartner telefonisch oder per E-Mail:

| | |
|---|---|
| Adresse | Trend Micro Deutschland GmbH<br>Parkring 29<br>85748 Garching |
| Telefon | +49 (0)89 8393 29700 |
| Website | http://www.trendmicro.com |

| | |
|---|---|
| E-Mail-Adresse | salesinfo_de@trendmicro.com |

- Weltweite Support-Büros:

  http://www.trendmicro.com/us/about-us/contact/index.html

- Kontaktaufnahme mit Trend Micro:

  http://www.trendmicro.de/ueber-uns/kontakt/index.html

- Trend Micro Produktdokumentation:

  http://docs.trendmicro.com/de-de/home.aspx

## Problemlösung beschleunigen

Sie sollten die folgenden Informationen zur Hand haben, um die Problemlösung zu beschleunigen:

- Schritte, um das Problem nachvollziehen zu können
- Informationen zur Appliance und zum Netzwerk
- Marke und Modell des Computers sowie zusätzlich angeschlossene Hardware oder Geräte
- Größe des Arbeitsspeichers und des freien Festplattenspeichers
- Betriebssystem- und Service Pack-Version
- Version des installierten Agents
- Seriennummer oder Aktivierungscode
- Ausführliche Beschreibung der Installationsumgebung
- Genauer Wortlaut eventueller Fehlermeldungen

# Verdächtige Inhalte an Trend Micro senden

Es gibt mehrere Optionen, um verdächtige Inhalte an Trend Micro zur weiteren Analyse zu senden.

## Email Reputation Services

Fragen Sie die Reputation einer bestimmten IP-Adresse ab, und geben Sie einen Message Transfer Agent zum Hinzufügen zur Liste der allgemein zulässigen Adressen an:

https://ers.trendmicro.com/

Informationen zum Senden von Nachrichten an Trend Micro finden Sie im folgenden Knowledge Base-Artikel:

https://success.trendmicro.com/solution/1112106

## File-Reputation-Dienste

Sammeln Sie Systeminformationen, und senden Sie verdächtige Dateiinhalte an Trend Micro:

https://success.trendmicro.com/solution/1059565

Notieren Sie sich die Anfragenummer für die weitere Bearbeitung Ihrer Anfrage.

## Web Reputation-Dienste

Sie können die Sicherheitsbewertung und den Inhaltstyp einer URL abfragen, hinter der Sie eine Phishing-Website oder einen Infektionsüberträger vermuten, d. h. eine Quelle von Internet-Bedrohungen, wie z. B. Spyware und Viren:

http://global.sitesafety.trendmicro.com/

Falls die zugewiesene Bewertung nicht zutrifft, senden Sie eine Neuklassifizierungsanforderung an Trend Micro.

# Sonstige Ressourcen

Neben Lösungen und Support sind online viele zusätzliche hilfreiche Ressourcen verfügbar, damit Sie immer auf dem neuesten Stand sind, Innovationen kennenlernen und mit den neuesten Sicherheitstrends vertraut sind.

## Download Center

Trend Micro veröffentlicht in bestimmten Abständen Patches für gemeldete bekannte Probleme oder Upgrades zu bestimmten Produkten oder Diensten. Auf folgender Seite können Sie feststellen, ob Patches verfügbar sind:

http://downloadcenter.trendmicro.com/index.php?regs=de

Falls ein Patch nicht angewendet wurde (Patches sind datiert), öffnen Sie die Readme-Datei, um festzustellen, ob er für Ihre Umgebung relevant ist. In der Readme-Datei finden Sie außerdem Installationsanweisungen.

## 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


**TREND MICRO INCORPORATED**

Trend Micro Deutschland GmbH Zeppelinstraβe 1 Hallbergmoos, Bayern 85399 Deutschland

Tel.: +49 (0) 811 88990-700 Fax: +4981188990799 info@trendmicro.com

www.trendmicro.com

Item Code: WFGM108707/190701