TREND MICRO™

10.0 Worry-Free™ Business Security Standard e Advanced Edition

Guida all'installazione e all'aggiornamento

Securing Your Journey to the Cloud

Protected Cloud

Web Security

Trend Micro Incorporated si riserva il diritto di apportare modifiche a questa documentazione e al prodotto in essa descritto senza alcun obbligo di notifica. Prima di installare e utilizzare il prodotto, leggere con attenzione i file readme, le note sulla versione e/o l'ultima edizione della documentazione appropriata, disponibili sul sito Web Trend Micro all'indirizzo:

http://docs.trendmicro.com/it-it/smb/worry-free-business-security.aspx

Trend Micro, il logo della sfera con una T di Trend Micro, TrendProtect, TrendSecure, Worry-Free, OfficeScan, ServerProtect, PC-cillin, InterScan e ScanMail sono marchi o marchi registrati di Trend Micro Incorporated. Tutti gli altri nomi di prodotti o società potrebbero essere marchi o marchi registrati dei rispettivi proprietari.

Copyright © 2018. Trend Micro Incorporated. Tutti i diritti riservati.

Codice documento: WFIM108204/180326

Data di pubblicazione: Giugno 2018

Protetto da brevetto U.S.: 5.951.698 e 7.188.369

Questa documentazione illustra le caratteristiche principali del prodotto e/o fornisce le istruzioni per l'installazione in un ambiente di produzione. Prima installare o utilizzare il prodotto, leggere attentamente la documentazione.

Informazioni dettagliate sull'utilizzo di caratteristiche specifiche del prodotto sono disponibili nella guida in linea di Trend Micro e nella Knowledge Base di Trend Micro.

Trend Micro si impegna continuamente a migliorare la propria documentazione. Per domande, commenti o suggerimenti riguardanti questo o qualsiasi documento Trend Micro, scrivere all'indirizzo docs@trendmicro.com.

È possibile esprimere un giudizio sulla documentazione al seguente indirizzo:

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

Sommario

Prefazione

Capitolo 1: Preparazione all'installazione e all'aggiornamento

Capitolo 2: Installazione di Security Server

Capitolo 3: Aggiornamento dei Security Server e dei Security Agent

Appendice A: Assistenza tecnica

Indice

Prefazione

Prefazione

Guida all'installazione e all'aggiornamento di Trend Micro™ Worry-Free™ Business Security. Questo documento illustra requisiti e procedure per:

- Installazione di Security Server
- Aggiornamento di Security Server e agenti

Per informazioni sull'installazione degli agent, consultare la *Guida per l'amministratore*.

Documentazione Worry-Free Business Security

La documentazione di Worry-Free Business Security include:

TABELLA 1. Documentazione Worry-Free Business Security

DOCUMENTAZIONE	DESCRIZIONE
Guida all'installazione e all'aggiornamento	un documento PDF che illustra i requisiti e le procedure di installazione del Security Server e l'aggiornamento del server e degli agenti
Guida dell'amministratore	un documento PDF contenente le informazioni introduttive, le procedure per l'installazione del client e la gestione di Security Server e agente
Guida	File HTML compilati in formato WebHelp o CHM che forniscono procedure, consigli di utilizzo e informazioni specifiche
File Readme	contiene un elenco di problemi noti e la procedura di base per l'installazione. Contiene inoltre le informazioni più recenti sul prodotto che non è stato possibile inserire nella documentazione nel software né in quella stampata
Knowledge Base	Un database online contenente informazioni utili per la risoluzione dei problemi. Fornisce le informazioni più recenti sui problemi noti riscontrati nell'utilizzo dei prodotti. Per accedere alla Knowledge Base, visitare il seguente sito Web: http://esupport.trendmicro.com

Le versioni aggiornate dei documenti PDF e del file Readme sono disponibili per il download alla pagina seguente:

http://docs.trendmicro.com/it-it/smb/worry-free-business-security.aspx

Destinatari

La documentazione di Worry-Free Business Security è destinata agli utenti seguenti:

- **Amministratori della sicurezza**: responsabili della gestione di Worry-Free Business Security, comprese le attività di gestione e installazione di Security Server e agent. Si presuppone che questi utenti abbiano conoscenze avanzate di reti e gestione dei server.
- **Utenti finali**: utenti che hanno il client Security Agent installato nei propri computer. Le conoscenza informatiche di questi utenti variano da principiante a utente esperto.

Convenzioni utilizzate nella documentazione

Per facilitare l'individuazione e l'interpretazione delle informazioni, la documentazione di Worry-Free Business Security segue le convenzioni illustrate di seguito:

TABELLA 2. Convenzioni utilizzate nella documentazione

CONVENZIONE	DESCRIZIONE
TUTTO MAIUSCOLO	Acronimi, abbreviazioni e nomi di alcuni comandi e tasti della tastiera
Grassetto	Menu e comandi dei menu, pulsanti dei comandi, schede, opzioni e attività
Corsivo	Riferimenti ad altra documentazione o a componenti di nuova tecnologia
<Testo>	Indica che il testo all'interno delle parentesi angolari deve essere sostituito da dati effettivi. Ad esempio, `C:\Programmi\<nome_file>` può corrispondere a `C:\Programmi\esempio.jpg`.
 **Nota**	Indica note per la configurazione o raccomandazioni
 **Suggerimento**	Indica informazioni su procedure ottimali e consigli di Trend Micro

CONVENZIONE	DESCRIZIONE
 **AVVERTENZA!**	Indica avvisi relativi ad attività che possono comportare danni per i computer della rete

Capitolo 1

Preparazione all'installazione e all'aggiornamento

In questo capitolo sono descritte le operazioni preliminari necessarie prima dell'installazione o dell'aggiornamento di Worry-Free™ Business Security.

Edizioni del prodotto

Trend Micro mette a disposizione le seguenti edizioni:

- Worry-Free Business Security**Standard**: progettato per proteggere gli endpoint (desktop, computer portatili e server) sulla rete locale. Questa versione comprende il firewall e la scansione antivirus/anti-spyware. Inoltre, è dotata di supporto tecnico, download dei pattern di virus/minacce informatiche, scansione in tempo reale e aggiornamenti del programma per un anno intero.
- Worry-Free Business Security**Avanzato**: progettato per proteggere gli endpoint e i server Microsoft Exchange nella rete. Oltre alle funzioni presenti in Worry-Free Business Security Standard, questa versione include anti-spam, filtro dei contenuti, prevenzione della perdita di dati e blocco allegati.

La seguente tabella elenca le funzioni supportate da ciascuna edizione.

TABELLA 1-1. Funzioni disponibili per le edizioni del prodotto

FUNZIONALITÀ	WORRY-FREE BUSINESS SECURITY STANDARD	WORRY-FREE BUSINESS SECURITY ADVANCED
Aggiornamento dei componenti	Sì	Sì
Controllo dispositivo	Sì	Sì
Antivirus/Anti-spyware	Sì	Sì
Firewall	Sì	Sì
Reputazione Web	Sì	Sì
Filtro URL	Sì	Sì
Intelligenza computazionale predittiva	Sì	Sì
Monitoraggio del comportamento	Sì	Sì
Strumenti utente	Sì	Sì

FUNZIONALITÀ	WORRY-FREE BUSINESS SECURITY STANDARD	WORRY-FREE BUSINESS SECURITY ADVANCED
Mail Scan (POP3)	Sì	Sì
Anti-Spam (POP3)	Sì	Sì
Mail Scan (IMAP)	No	Sì
Anti-Spam (IMAP)	No	Sì
Filtro del contenuto dei messaggi e-mail	No	Sì
Prevenzione perdita di dati dei messaggi e-mail	No	Sì
Blocco allegati	No	Sì

Licenze, registrazione e attivazione

Quando si acquista Worry-Free Business Security, si ricevono una licenza per i prodotti e un Contratto di manutenzione standard. Il Contratto di manutenzione standard è un contratto tra la propria organizzazione e Trend Micro sul diritto di ricevere assistenza tecnica e aggiornamenti del prodotto a fronte del pagamento delle tariffe applicabili.

In genere la licenza del software Trend Micro dà diritto alla ricezione degli aggiornamenti del prodotto e dei file pattern, nonché all'assistenza tecnica generale per la durata di un (1) anno dalla data di acquisto. Dopo il primo anno è necessario rinnovare annualmente il Contratto di manutenzione dietro il pagamento delle tariffe di manutenzione Trend Micro correnti per tale periodo.

Nota

Il Contratto di manutenzione scade, il contratto di licenza non scade. Se il Contratto di manutenzione scade, la scansione può ancora essere effettuata, ma non è possibile aggiornare i file di pattern per malware/virus, il motore di scansione o i file di programma (neanche manualmente). Non si ha inoltre il diritto di riceve assistenza tecnica da parte di Trend Micro.

Registrare e attivare la propria licenza Worry-Free Business Security per attivare tutte le fuzionalità del prodotto.

Chiave di registrazione

Insieme all'acquisto di Worry-Free Business Security si riceve una chiave di attivazione. È costituita da 22 caratteri (compresi i trattini) e ha il formato indicato di seguito:

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

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

Utilizzare una chiave di registrazione con licenza completa per registrare Worry-Free Business Security sul sito Web di Trend Micro all'indirizzo https://clp.trendmicro.com.

Codice di attivazione

Dopo la registrazione si riceve via e-mail un codice di attivazione con licenza completa. Il codice di attivazione è costituito da 37 caratteri (compresi i trattini) e ha il formato indicato di seguito:

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

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

Durante l'installazione di Security Server, quando richiesto immettere il codice di attivazione. Se si lascia il campo vuoto, Worry-Free Business Security installa la versione di prova della durata di 30 giorni. Prima della scadenza della versione di prova, passare alla versione con licenza completa.

Stato della licenza

La tabella di seguito elenca le funzioni supportate secondo lo stato della licenza.

TABELLA 1-2. Stato della licenza

FUNZIONE	LICENZA COMPLETA	VERSIONE DI PROVA (30 GIORNI)	SCADUTO
Notifica di scadenza	Sì	Sì	Sì
Aggiornamento dei componenti	Sì	Sì	No

FUNZIONE	LICENZA COMPLETA	VERSIONE DI PROVA (30 GIORNI)	SCADUTO
Aggiornamenti del programma	Sì	Sì	No
Assistenza tecnica	Sì	No	No
Scansione in tempo reale	Sì	Sì	Sì, ma la scansione in tempo reale utilizza componenti non aggiornati

Quando un codice di attivazione con licenza completa scade, non è più possibile scaricare aggiornamenti del motore di scansione o dei file di pattern. Tuttavia, a differenza di un codice di attivazione di una versione di prova, quando un codice di attivazione di una versione con licenza scade, tutte le configurazioni esistenti e altre impostazioni restano invariate. In tal modo si mantiene un livello di protezione nel caso in cui si lasci scadere accidentalmente la licenza.

È possibile rinnovare una versione completa di Worry-Free Business Security acquistando un rinnovo di manutenzione. Per installare le versioni complete è necessario un codice di attivazione.

Per eventuali domande sul processo di registrazione, consultare il sito Web di assistenza di Trend Micro all'indirizzo:

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

Rete Worry-Free Business Security

Worry-Free Business Security è composto dai seguenti componenti:

- *Security Server a pagina 1-6*
- *Agent a pagina 1-7*
- *Console Web a pagina 1-8*

Security Server

Security Server rappresenta il fulcro di Worry-Free Business Security Advanced. Security Server ospita la console Web, una console di gestione centralizzata Web per Worry-Free Business Security. Il Security Server consente di installare gli agent sui client presenti in una rete e, unitamente agli agent, forma una relazione agent-server. Con Security Server è possibile consultare le informazioni sullo stato, visualizzare gli Agent, configurare la sicurezza del sistema e scaricare i componenti da una postazione centralizzata. Security Server contiene inoltre il database in cui memorizza i registri delle minacce informatiche segnalate dagli agent.

Security Server esegue queste importanti funzioni:

- Installa, controlla e gestisce gli agent.
- Scarica i componenti necessari per gli agent. Per impostazione predefinita, il Security Server scarica i componenti dal server Trend Micro ActiveUpdate, per poi distribuirli agli agent.

Server di scansione

Il Security Server comprende un servizio chiamato Scan Server, installato automaticamente durante l'installazione del Security Server. Per questo motivo non è necessario installarlo separatamente. Lo Scan Server funziona con il nome di processo `iCRCService.exe` e compare come **Trend Micro Smart Scan Service** in Microsoft Management Console.

Quando i Security Agent utilizzano un metodo di scansione denominato **smart scan**, lo Scan Server permette a questi agent di eseguire le scansioni in maniera più efficiente. Il processo smart scan è il seguente:

- Il Security Agent esegue la scansione del client in cerca di minacce alla sicurezza utilizzando **Pattern agente Smart Scan**, versione ridotta del tradizionale Virus Pattern. Pattern agente Smart Scan contiene la maggior parte di firme di minacce disponibili nel Virus Pattern.
- Un Security Agent non in grado di determinare il rischio del file durante la scansione, verifica il rischio inviando una query di scansione allo Scan Server. Lo Scan Server verifica il rischio sfruttando il **Pattern per Smart Scan**, che contiene tutte le firme di minacce non disponibili nel Pattern agente Smart Scan.

- Il Security Agent memorizza nella cache il risultato della query di scansione fornito dal server di scansione per migliorare le prestazioni della scansione.

Conservando in hosting alcune delle definizioni delle minacce, lo Scan Server aiuta a ridurre il consumo di banda per i Security Agent durante il download dei componenti. Invece di scaricare il Virus Pattern, i Security Agent scaricano Pattern agente Smart Scan che è di dimensioni significativamente inferiori.

Se i Security Agent non sono in grado di connettersi allo Scan Server, inviano query di scansione a Trend Micro Smart Protection Network, che ha il medesimo ruolo dello Scan Server.

Non è possibile disinstallare lo Scan Server separatamente dal Security Server. Per non utilizzare lo Scan Server:

1. Sul computer del Security Server, aprire Microsoft Management Console e disattivare il servizio **Trend Micro Smart Scan Service**.

2. Nella console Web, far passare i Security Agent alla scansione tradizionale da **Amministrazione** > **Impostazioni globali** > **scheda Desktop/Server** e selezionare l'opzione **Disattiva Smart Scan Service**.

Agent

Gli agent proteggono i client dalle minacce alla sicurezza. I client includono desktop, server e server Microsoft Exchange. Gli agent Worry-Free Business Security sono:

TABELLA 1-3. Agent Worry-Free Business Security

AGENT	DESCRIZIONE
Security Agent	Protegge desktop e server dalle minacce alla sicurezza e dalle intrusioni
Messaging Security Agent (solo Advanced)	Protegge i server Microsoft Exchange da minacce alla sicurezza trasmesse tramite e-mail

Un agent invia notifiche al Security Server dal quale è stato installato. Per fornire al Security Server i dati più aggiornati riguardanti il client, l'agent invia informazioni sullo stato degli eventi in tempo reale. L'agent riporta eventi quali il rilevamento di minacce,

l'avvio e lo spegnimento, l'avvio di una scansione e il completamento di un aggiornamento.

Console Web

La console Web è l'elemento centrale per il monitoraggio dei Security Agent in tutta la rete aziendale. La console è dotata di un insieme di impostazioni e valori predefiniti che è possibile configurare in base ai propri requisiti e alle proprie specifiche di sicurezza. La console Web utilizza tecnologie Internet standard quali Java, CGI, HTML e HTTP.

Utilizzare la console Web per:

- Implementare gli agent sugli endpoint.
- Organizzare gli agent in gruppi logici, per poterli configurare e gestire contemporaneamente.
- Configurare le impostazioni di prodotto e avviare Scansione manuale negli endpoint.
- Ricevere le notifiche e visualizzare i rapporti di registro per le attività correlate alle minacce.
- Ricevere le notifiche e inviare gli avvisi sulle infezioni mediante messaggi e-mail al rilevamento delle minacce negli endpoint.

Capitolo 2

Installazione di Security Server

In questo capitolo vengono fornite le informazioni necessarie per l'installazione del Security Server.

Requisiti di installazione e aggiornamento

Visitare il sito Web seguente per un elenco completo dei requisiti per l'installazione e per gli aggiornamenti:

http://docs.trendmicro.com/it-it/smb/worry-free-business-security.aspx

Considerazioni sull'installazione del Security Server

Durante l'installazione del Security Server, prendere in considerazione le seguenti informazioni:

Requisiti IPv6 del Security Server

Di seguito sono elencati i requisiti IPv6 per il Security Server:

- Se il server deve gestire agent IPv4 e IPv6, deve disporre sia dell'indirizzo IPv4 che IPv6 e deve essere identificato tramite il nome host. Se il server viene identificato tramite il suo indirizzo IPv4, gli agent IPv6 puri non possono collegarsi al server. Lo stesso problema si verifica se client IPv4 puri si collegano a un server identificato tramite il suo indirizzo IPv6.
- Se il server deve gestire solo agent IPv6, il requisito minimo è un indirizzo IPv6. Il server può essere identificato tramite il nome host o l'indirizzo IPv6. Se il server viene identificato tramite il nome host, è preferibile utilizzare il suo nome di

dominio completo (FQDN). Infatti, in un ambiente IPv6 puro, un server WINS non può tradurre un nome host nel suo corrispondente indirizzo IPv6.

- Verificare che l'indirizzo IPv6 o IPv4 della macchina host possa essere recuperato usando, ad esempio, il comando "`ping`" o "`nslookup`".
- Per installare il Security Server su un computer IPv6 puro, configurare un server proxy dual-stack in grado di convertire tra indirizzi IPv4 e IPv6 (come DeleGate). Posizionare il server proxy tra il Security Server e la rete Internet, al fine di consentire al server di collegarsi ai servizi gestiti da Trend Micro, ad esempio il server ActiveUpdate, il sito Web di registrazione online e Smart Protection Network.

Posizione del Security Server

Worry-Free Business Security è in grado di adattarsi a diversi ambienti di rete. Ad esempio, è possibile posizionare un firewall tra Trend Micro Security Server e i client su cui è in esecuzione il Security Agent o posizionare sia Trend Micro Security Server che tutti i client dietro un unico firewall di rete.

In caso di gestione più siti, si consiglia di installare Security Server presso il sito centrale e in ogni sito gestito, in modo da ridurre l'utilizzo della larghezza di banda tra i siti gestiti e quello centrale e quindi rendere più veloce l'implementazione dei file di pattern.

Se i client hanno il firewall di Windows XP attivato, Worry-Free Business Security lo aggiungerà automaticamente all'elenco Eccezioni.

Nota

Se un firewall è posizionato tra Trend Micro Security Server e i relativi client, sarà necessario configurare il firewall per consentire il traffico tra la porta di ascolto dei client e la porta di ascolto di Trend Micro Security Server.

Numero di client

Un client è il computer dove si intende installare un Security Agent o un Messaging Security Agent. Sono client i computer desktop, server e portatili, compresi quelli di utenti che svolgono il telelavoro.

Un solo Security Server è in grado di gestire fino a 2.500 client. Se si dispone di una quantità superiore di client, Trend Micro consiglia di installare più di un Security Server.

Traffico di rete

Worry-Free Business Security genera traffico di rete quando Security Server e agent comunicano tra di loro.

Il Security Server/server di scansione genera traffico quando:

- Invia notifiche agli agent su modifiche alla configurazione
- Invia notifiche agli agent sulla disponibilità di componenti aggiornati per il download
- Si collega al server Trend Micro ActiveUpdate per verificare la presenza di componenti aggiornati e scaricarli
- Risponde alle query di scansione ricevute dagli agent che utilizzano smart scan
- Invia un riscontro a Trend Micro Smart Protection Network

Gli agent generano traffico quando:

- Si avviano
- Si spengono
- Generano dei registri
- Eseguono aggiornamenti pianificati
- Eseguono aggiornamenti manuali ("Aggiorna ora")
- Si collegano allo Scan Server per le query di scansione

Nota

Ad eccezione degli aggiornamenti, tutte le altre operazioni generano una quantità di traffico minima.

Traffico di rete durante gli aggiornamenti dei componenti

Il Security Server genera un significativo traffico di rete quando aggiorna i componenti. Per ridurre il traffico di rete generato durante l'aggiornamento dei componenti, il Security Server duplica i componenti. Piuttosto che scaricare un file di pattern completo aggiornato, il Security Server scarica solo pattern "incrementali" (versioni più piccole del file di pattern completo) e li unisce con la precedente versione del file di pattern al termine del download.

Un Security Server aggiornato regolarmente scarica solo pattern incrementali. In caso contrario, scarica il file di pattern completo.

Trend Micro pubblica i nuovi file di pattern a cadenza regolare. Se è in circolazione un virus o un malware particolarmente dannoso, Trend Micro pubblica il nuovo file di pattern non appena questi vengono scoperti.

Uso degli Update Agent per ridurre il consumo della larghezza di banda

Se all'interno della propria rete si identificano sezioni tra i Security Agent e Security Server a "banda ridotta" o "a traffico pesante", è possibile specificare che i Security Agent agiscano come origini di aggiornamento (Update Agent) per altri agent. Questa operazione consente di distribuire il carico dell'implementazione dei componenti su tutti gli agent.

Ad esempio, se la rete è segmentata per sede e il collegamento di rete tra i segmenti è caratterizzato da un carico di traffico pesante, Trend Micro consiglia di fare in modo che almeno un Security Agent di ogni segmento agisca da Update Agent.

Server dedicato

Quando si seleziona il client per ospitare il server Worry-Free Business Security, tenere presenti gli aspetti seguenti:

- Il carico CPU gestito dal client
- Se il client svolge altre funzioni

Se il client di destinazione svolge altre funzioni, scegliere un altro client che non esegua applicazioni critiche oppure a elevato utilizzo di risorse.

Problemi di compatibilità

In questa sezione sono illustrati problemi di compatibilità riscontrabili con determinate applicazioni di terze parti. Fare sempre riferimento alla documentazione di tutte le applicazioni di terze parti installate nello stesso computer in cui verranno installati Security Server e gli altri componenti Worry Free.

Altro software di protezione endpoint

Prima di installare il Security Server, Trend Micro consiglia di rimuovere manualmente gli altri software di protezione endpoint dal computer di destinazione, in quanto potrebbero bloccare l'installazione o influire sulle prestazioni del Security Server dopo l'installazione.

Applicazioni di sicurezza in Windows SBS e EBS 2008

Worry-Free Business Security è compatibile sia con Windows Small Business Server (SBS) 2008 che con Windows Essential Business Server (EBS) 2008. Tuttavia, alcune applicazioni di sicurezza installate o gestite mediante questi sistemi operativi potrebbero creare conflitti con Worry-Free Business Security. Pertanto, potrebbe essere necessario rimuovere queste applicazioni di sicurezza.

Messaging Security Agent e Forefront

Non è possibile installare il Messaging Security Agent sui server Microsoft Exchange dotati di Forefront (Microsoft Forefront Security per Exchange Server). Disinstallare Forefront e assicurarsi che il servizio Archivio informazioni di Microsoft Exchange sia stato avviato prima di installare il Messaging Security Agent.

Messaging Security Agent e Microsoft Server Enterprise

Messaging Security Agent non supporta alcune funzioni di Microsoft Exchange Server Enterprise come il gruppo di disponibilità dei dati (DAG).

Security Agent e Windows Defender

L'installazione di Security Agent disattiva Windows Defender.

Database

La scansione dei database potrebbe compromettere le prestazioni delle applicazioni che accedono ai database. Trend Micro consiglia di escludere i database e le relative cartelle

di backup dalla scansione in tempo reale. Se è necessario eseguire la scansione di un database, eseguire la scansione manuale o pianificata nelle ore non di punta per ridurre al minimo l'impatto della scansione.

Altre applicazioni firewall

Prima di installare il firewall Worry-Free Business Security, Trend Micro consiglia di rimuovere o disabilitare qualsiasi altra applicazione firewall, inclusi:

- Firewall di connessione Internet Windows (ICF)
- Windows Firewall (WF)

Tuttavia, se si desidera eseguire Firewall connessione Internet o qualsiasi altro firewall terze parti, aggiungere le porte di ascolto di Trend Micro Security Server all'elenco delle eccezioni del firewall (vedere *Porte Worry-Free Business Security a pagina 2-7* per ulteriori informazioni sulle porte di ascolto e fare riferimento alla documentazione del firewall per ulteriori dettagli su come configurare gli elenchi delle eccezioni).

Porte Worry-Free Business Security

Worry-Free Business Security utilizza le seguenti porte:

- **Porta di ascolto del server (porta HTTP)**: utilizzata per accedere al Security Server. Per impostazione predefinita, Worry-Free Business Security utilizza una delle seguenti porte:
  - **Sito Web predefinito del server IIS**: lo stesso numero di porta TCP del server HTTP.
  - **Sito Web virtuale del server IIS**: 8059
  - **Server Apache**: 8059
- **Porta di ascolto del client**: numero porta generato casualmente attraverso il quale Security Agent e Messaging Security Agent ricevono comandi dal Security Server.

  È possibile modificare le porte di ascolto solo durante l'installazione.

AVVERTENZA!

Molti attacchi virus e hacker utilizzano il protocollo HTTP e sono diretti alle porte 80 e/o 8080, utilizzate da molte aziende come porte TCP (Transmission Control Protocol) predefinite per le comunicazioni HTTP. Se l'azienda utilizza una di queste porte come porta HTTP, Trend Micro consiglia di scegliere un altro numero di porta.

Nota

Per individuare quale porta viene utilizzata dai Security Agent per collegarsi allo Scan Server, aprire SSCFG.ini nella cartella di installazione del server.

- **Porte del server di scansione**: utilizzate dallo Scan Server per comunicare con i Security Agent per le query di scansione.

TABELLA 2-1. Porte del server di scansione

TIPO PORTA	IIS PREDEFINITA	IIS VIRTUALE	APACHE PREINSTALLATO	NUOVA INSTALLAZIONE APACHE
Porta non SSL	Porta non SSL sul server Web	Prima porta aperta nell'intervallo 8082-65536	Porta non SSL sul server Web	Porta non SSL sul server Web
Porta SSL Utilizzando SSL	Porta SSL sul server Web	Prima porta aperta nell'intervallo 4345-65536	N/D	Porta SSL sul server Web
Porta SSL Senza utilizzare SSL	Prima porta aperta nell'intervallo 4345-65536	Prima porta aperta nell'intervallo 4345-65536	N/D	Prima porta aperta nell'intervallo 4345-65536

- **Porta di comunicazione Trend Micro Security (per Mac)**: utilizzata dal server Trend Micro Security (per Mac) per le comunicazioni con i client Mac. La porta predefinita è 61617.
- **Porta SMTP**: utilizzata dal Security Server per inviare rapporti e notifiche agli amministratori via e-mail. La porta predefinita è 25.

- **Porta proxy**: utilizzata per le connessioni attraverso un server proxy.

Lista di controllo per l'installazione

Durante l'installazione del Security Server, il programma di installazione richiede le seguenti informazioni.

TABELLA 2-2. Lista di controllo per l'installazione

INFORMAZIONI	VALORI PREDEFINITI	VALORE
Security Server (incluso Scan Server)		
Codice di attivazione	Fornito da Trend Micro	
Percorso di installazione	Uno dei seguenti (a seconda del sistema operativo): • C:\Programmi \TrendMicro\Security Server • C:\Program Files (x86)\Trend Micro \Security Server	
Percorso del database dello Scan Server	Lo stesso percorso di installazione del Security Server (personalizzabile)	
Indirizzo IPv4/IPv6	Definiti dall'utente	
FQDN (Fully Qualified Domain Name)	Definiti dall'utente	
Nome NetBIOS (host)	Definiti dall'utente	

INFORMAZIONI	VALORI PREDEFINITI	VALORE
Server Web	Sceglierne uno: • Apache • IIS (sito Web predefinito) • IIS (sito Web virtuale)	
Porta di ascolto (HTTP)	8059	
Porta di ascolto (HTTPS)	4343	
Password della console Web	Definiti dall'utente	
Password disinstallazione/ rimozione Security Agent	Definiti dall'utente	
(Facoltativo) Impostazioni SMTP per segnalazioni e notifiche del Security Server inviati per e-mail		
Indirizzo IPv4/IPv6	Definiti dall'utente	
FQDN (Fully Qualified Domain Name)	Definiti dall'utente	
Nome NetBIOS (host)	Definiti dall'utente	
Porta	25	
Destinatari	Definiti dall'utente	
(Facoltativo) Impostazioni proxy per la connessione del Security Server ai servizi in hosting Trend Micro		
Indirizzo IPv4/IPv6	Definiti dall'utente	
FQDN (Fully Qualified Domain Name)	Definiti dall'utente	

INFORMAZIONI	VALORI PREDEFINITI	VALORE
Nome NetBIOS (host)	Definiti dall'utente	
Nome utente di autenticazione	Definiti dall'utente	
Password di autenticazione	Definiti dall'utente	
Security Agent		
Porta di ascolto	Generata casualmente dal programma di installazione	
Percorso di installazione	Uno dei seguenti (a seconda del sistema operativo): • C:\Programmi \TrendMicro\Security Agent • C:\Program Files (x86)\Trend Micro \Security Agent	
(Facoltativo) Autenticazione proxy per le funzioni del Security Agent (Monitoraggio del comportamento, Reputazione Web e Smart Scan) **Nota** I Security Agent utilizzano le impostazioni proxy configurate in Internet Explorer.		
Nome utente di autenticazione	Definiti dall'utente	
Password di autenticazione	Definiti dall'utente	
(Facoltativo) Messaging Security Agent		
Indirizzo IPv4/IPv6 del server Microsoft Exchange	Definiti dall'utente	

Informazioni	Valori predefiniti	Valore
FQDN (Fully Qualified Domain Name) del server Microsoft Exchange	Definiti dall'utente	
Nome NetBIOS (host) del server Microsoft Exchange	Definiti dall'utente	
Account e password amministratore di dominio per accedere al server Microsoft Exchange	Definiti dall'utente	
Porta di ascolto	16372	
Percorso di installazione	Uno dei seguenti (a seconda del sistema operativo): • C:\Programmi \TrendMicro\Messaging Security Agent • C:\Program Files (x86)\Trend Micro \Messaging Security Agent	
Cartella Temp (il programma di installazione estrae i file di installazione in questa cartella)	C$	

Installazione di Security Server

L'installazione del Security Server comprende tra fasi:

Fasi	Operazioni principali

Fase 1: inizio dell'installazione del Security Server	• Leggere le linee guida pre-installazione.
	• Avviare il pacchetto di installazione.
	• Accettare i termini del contratto di licenza.
	• Scegliere un Tipo di installazione.
	  • Tipica (consigliata)
	  • Minima
	  • Personalizzato
	• Immettere il codice di attivazione.

Fasi	Operazioni principali
Fase 2: configurazione delle impostazioni in base al Tipo di installazione selezionato	Per un'installazione Tipica o Minima, configurare le impostazioni base tra cui: • Percorso di installazione del Security Server • Password account amministratore • Impostazioni server SMTP e destinatari notifiche • Smart Protection Network

	Per l'installazione Personalizzata, configurare tutte le impostazioni configurabili tra cui:
	• Impostazioni base
	  • Percorso di installazione del Security Server
	  • Posizione del database dello Scan Server
	  • Se si installa il Security Agent o il Messaging Security Agent sullo stesso computer del Security Server
	• Impostazioni di Security Server
	  • Server Web
	  • Password account amministratore
	  • Impostazioni server SMTP e destinatari notifiche
	  • Smart Protection Network
	  • Impostazioni proxy generali
	• Impostazioni Security Agent
	  • Percorso di installazione Security Agent
	  • Funzioni del Security Agent da attivare
	  • Impostazioni proxy per servizi aggiuntivi
	• Impostazioni del Messaging Security Agent
	  • Impostazioni del server Microsoft Exchange
	  • Percorso di installazione del Messaging Security Agent

Fasi	Operazioni principali
Fase 3: procedura di installazione	Attendere il completamento dell'installazione, quindi chiudere il programma di installazione.

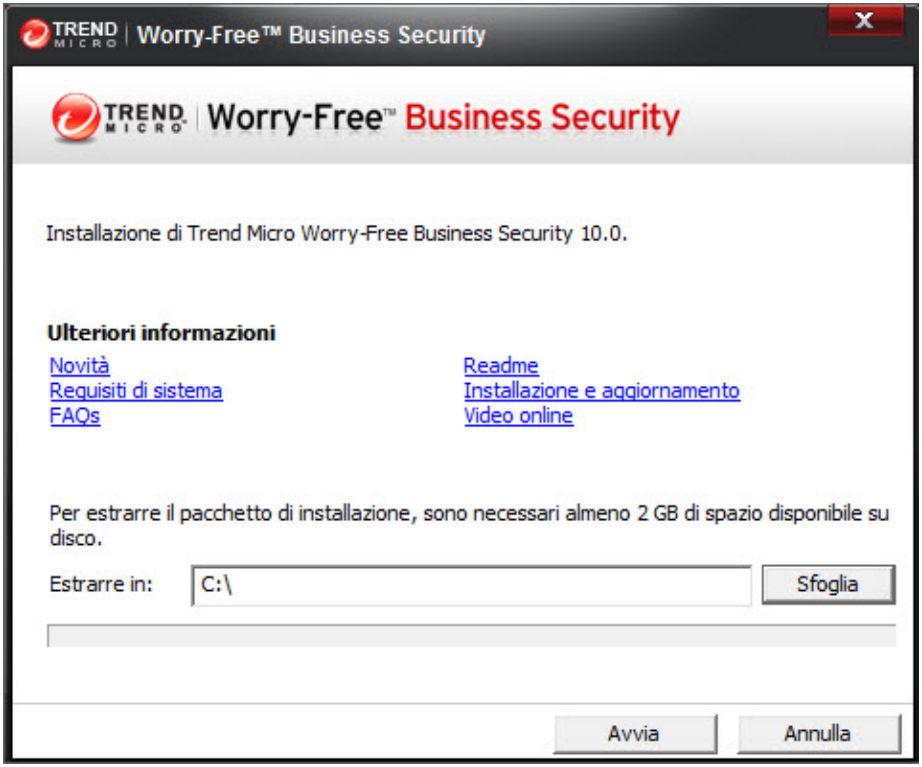
Fase 1: inizio dell'installazione del Security Server

Informazioni preliminari

- Accedere con un account dotato di dominio o privilegi di amministratore locale.
- Prima di installare Worry-Free Business Security, chiudere tutte le applicazioni in esecuzione. Se si esegue l'installazione mentre sono in esecuzione altre applicazioni, il completamento dell'installazione potrebbe richiedere più tempo.
- Non installare il Security Server su un computer che esegue applicazioni che possono bloccare il servizio IIS. L'installazione potrebbe non riuscire. Per ulteriori informazioni, consultare la documentazione IIS.
- Per installare Trend Micro Security Server non è necessario riavviare il computer. Al termine dell'installazione, configurare immediatamente le impostazioni e procedere all'installazione del Security Agent sui client.

Avvio del pacchetto di installazione

Fare doppio clic sul pacchetto di installazione (file `.exe`).



I file di installazione saranno estratti nella stessa directory in cui si trova il file `.exe`. Per modificare il percorso, fare clic su **Sfoglia** e individuare la directory.

Quando si fa clic su **Avvia**, il programma di installazione comincia l'estrazione dei file. Lo stato dell'estrazione viene visualizzato sulla barra di stato nella parte bassa della schermata. Al termine dell'estrazione viene visualizzata la schermata iniziale.


Installazione di Trend Micro Worry-Free Business Security
Benvenuti nelle procedura guidata di installazione di Trend Micro Worry-Free Business Security.
La procedura guidata permetterà di eseguire l'installazione dell'applicazione sul computer. Per continuare, fare clic su Avanti.
Nota: Trend Micro consiglia di chiudere tutte le finestre del browser e le applicazioni prima di fare clic su Avanti.
< Indietro
Avanti >
Annulla

Contratto di licenza

Leggere il contratto di licenza. Se si accettano i termini, selezionare **Accetto i termini del contratto di licenza**.

Tipo di installazione

Scegliere una delle seguenti opzioni:

Installazione tipica (consigliata)

Questo metodo è adatto a un Security Server che gestisce fino a 100 agenti.

Durante un'installazione tipica:

- Dopo l'installazione vengono abilitate automaticamente le funzioni seguenti:
  - Antivirus/Anti-spyware
  - Monitoraggio del comportamento (solo su piattaforme desktop, ad esempio Windows 7)

- Reputazione Web
- Filtro URL
- Smart Scan

Nota

Per eseguire Smart Scan i Security Agent devono essere conformi ai requisiti minimi di sistema. Per un elenco dei requisiti, visitare http://docs.trendmicro.com/it-it/smb/worry-free-business-security.aspx.

- Se non è già presente, il Security Agent viene installato automaticamente sullo stesso computer del Security Server.

Nota

Installare il Security Agent su altri client nella rete e gestirli dalla console Web. Per informazioni dettagliate sui diversi metodi di installazione dei Security Agent, consultare la Guida per l'amministratore.

- Se sul computer è installato un altro software di sicurezza endpoint, il programma di installazione disinstalla prima il software e quindi procede all'installazione del Security Agent.

Nota

Alcuni software di sicurezza endpoint potrebbero essere solo rilevati ma non disinstallati. In tal caso, disinstallare prima manualmente il software.

Per un elenco dei software di sicurezza endpoint che possono essere disinstallati o rilevati ma non disinstallati, visitare il seguente sito Web:

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

Installazione minima

Durante un'installazione minima:

- solo la funzione antivirus/anti-spyware è abilitata dopo l'installazione.
- Se non è già presente, il Security Agent viene installato automaticamente sullo stesso computer del Security Server.

Nota

Installare il Security Agent su altri client nella rete e gestirli dalla console Web. Per informazioni dettagliate sui diversi metodi di installazione dei Security Agent, consultare la Guida per l'amministratore.

- Se sul computer è installato un altro software di sicurezza endpoint, il programma di installazione disinstalla prima il software e quindi procede all'installazione del Security Agent.

Nota

Alcuni software di sicurezza endpoint potrebbero essere solo rilevati ma non disinstallati. In tal caso, disinstallare prima manualmente il software.

Per un elenco dei software di sicurezza endpoint che possono essere disinstallati o rilevati ma non disinstallati, visitare il seguente sito Web:

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

Installazione personalizzata

L'Installazione personalizzata offre la flessibilità di configurare le impostazioni per il Security Server e gli agent in base alla strategia di sicurezza della rete adottata. Questo metodo è adatto se il Security Server gestisce un numero elevato di agent.

Durante un'installazione personalizzata, le seguenti impostazioni sono **opzionali**:

- Se non è già presente, installare il Security Agent sullo stesso computer del Security Server.

Nota

Installare il Security Agent su altri client nella rete e gestirli dalla console Web. Per informazioni dettagliate sui diversi metodi di installazione dei Security Agent, consultare la Guida per l'amministratore.

- Se sul computer è installato un altro software di sicurezza endpoint, il programma di installazione disinstalla prima il software e quindi procede all'installazione del Security Agent.

Nota

Alcuni software di sicurezza endpoint potrebbero essere solo rilevati ma non disinstallati. In tal caso, disinstallare prima manualmente il software.

Per un elenco dei software di sicurezza endpoint che possono essere disinstallati o rilevati ma non disinstallati, visitare il seguente sito Web:

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

- Installare il Messaging Security Agent sullo stesso computer del Security Server (se è presente un server Microsoft Exchange) o su client remoti.

Attivazione prodotto

Digitare il codice di attivazione nel campo **Codice di attivazione**.

Se non si dispone di un codice di attivazione, è possibile che la copia di Worry-Free Business Security non sia stata ancora registrata. Per aprire una nuova finestra del browser, fare clic sul pulsante **Registrazione online**. Seguire le istruzioni sulla schermata Registrazione. Altrimenti, fare clic su **Avanti** per installare la versione di prova. Se si esegue l'aggiornamento alla versione completa prima che scadano i 30 giorni del periodo di prova, tutte le impostazioni del programma restano intatte.

Informazioni sull'installazione

Nella schermata Informazioni sull'installazione vengono visualizzati i componenti da configurare per poter installare Trend Micro Security Server, Security Agent o Messaging Security Agent.

Dopo aver fatto clic su **Avanti**:

- se si seleziona Installazione tipica/minima, continuare con:
  - *Configurazione delle impostazioni per un'installazione tipica o minima a pagina 2-24*
  - *Fase 3: procedura di installazione a pagina 2-51*
- se si seleziona Installazione personalizzata, continuare con:
  - *Configurazione delle impostazioni per un'installazione personalizzata a pagina 2-29*
  - *Fase 3: procedura di installazione a pagina 2-51*

Fase 2: configurazione delle impostazioni in base al Tipo di installazione

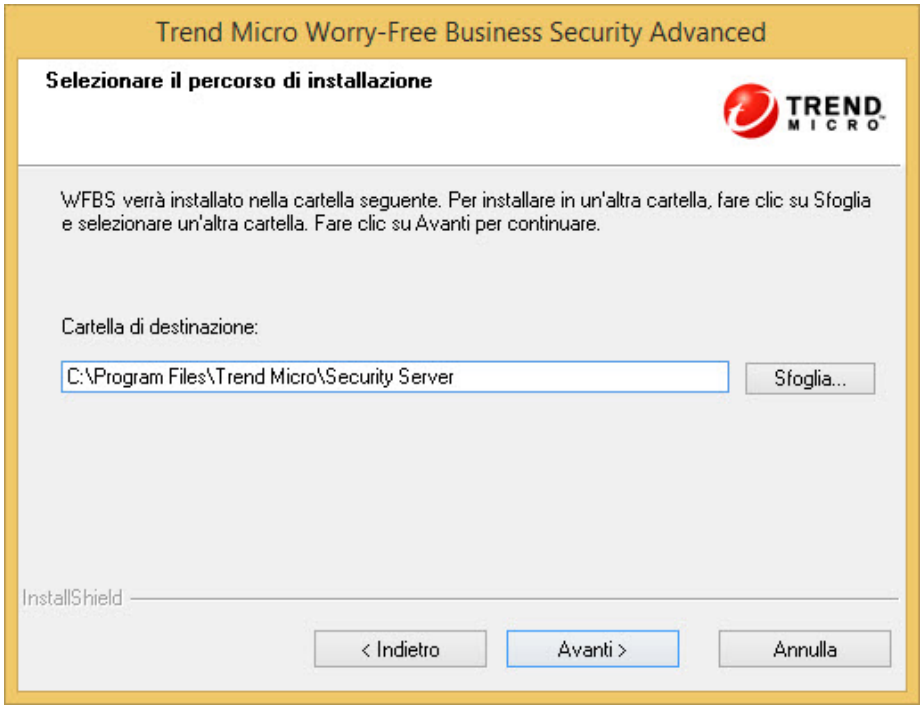
Le impostazioni da configurare nella Fase 2 dipendono dal tipo di installazione scelto nella Fase 1.

- *Configurazione delle impostazioni per un'installazione tipica o minima a pagina 2-24*
- *Configurazione delle impostazioni per un'installazione personalizzata a pagina 2-29*

Configurazione delle impostazioni per un'installazione tipica o minima

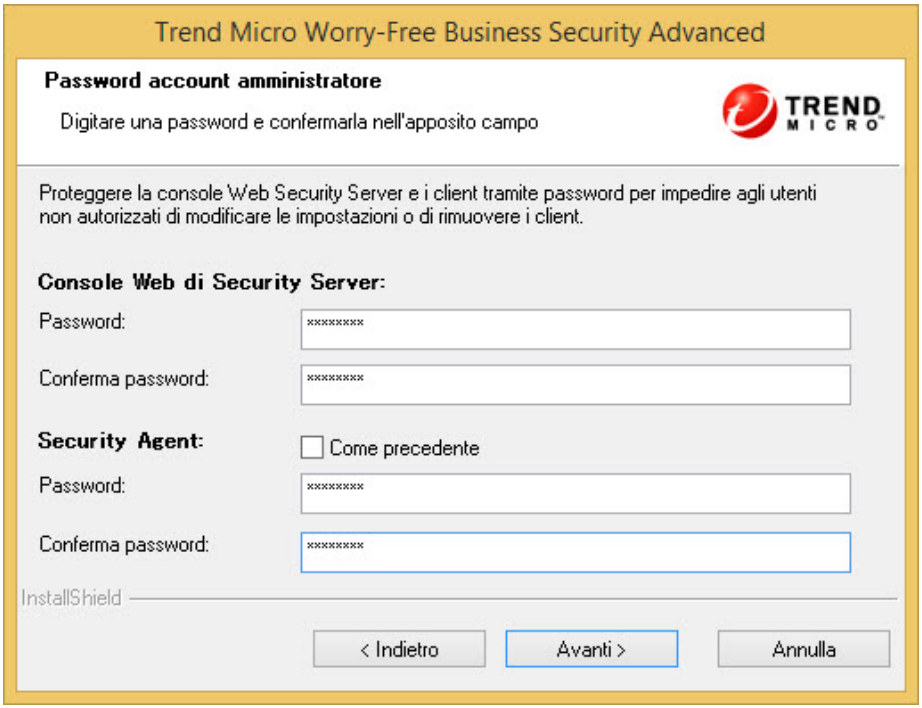
Se si esegue un'installazione tipica o minima, vengono visualizzate in sequenza le schermate seguenti:

Percorso di installazione



La cartella predefinita di installazione di Worry-Free Business Security è `C:\Programmi\Trend Micro\Security Server` o `C:\Programmi (x86)\Trend Micro\Security Server`. Fare clic su **Sfoglia** se si desidera installare Worry-Free Business Security in un'altra cartella.

Password account amministratore



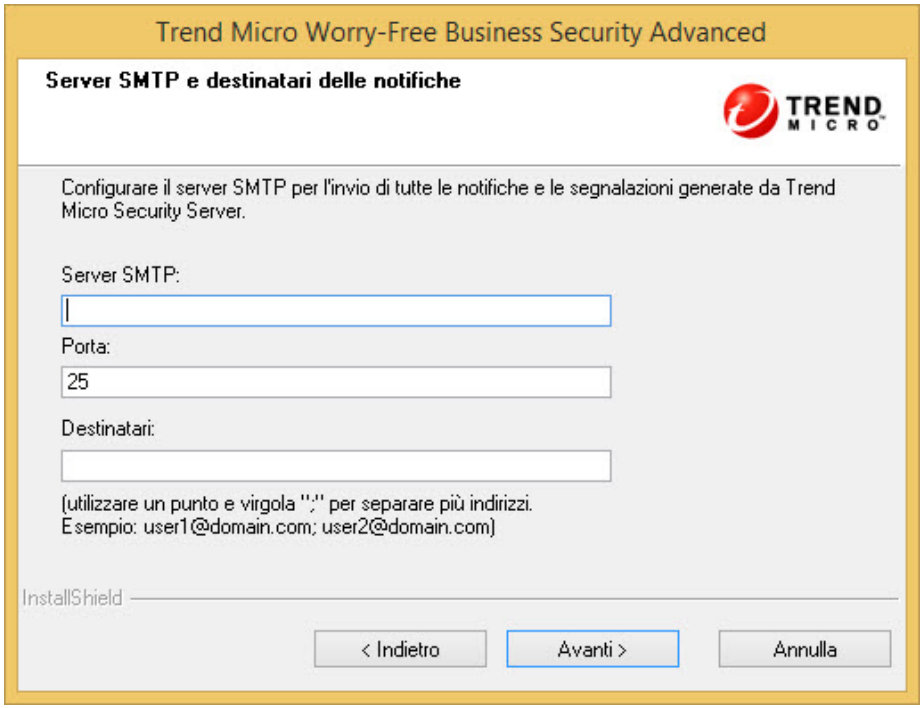
Specificare password diverse per la console Web di Security Server e per il Security Agent.

- **Console Web Security Server**: necessaria per eseguire l'accesso alla console Web
- **Security Agent**: richiesta per disinstallare o rimuovere i Security Agent dai client

Nota

Il campo Password contiene tra 1 e 24 caratteri e rileva la distinzione tra maiuscole e minuscole.

Server SMTP e destinatari delle notifiche



Inserire le seguenti informazioni:

- **Server SMTP**: l'indirizzo IP del server di posta elettronica

  Nota

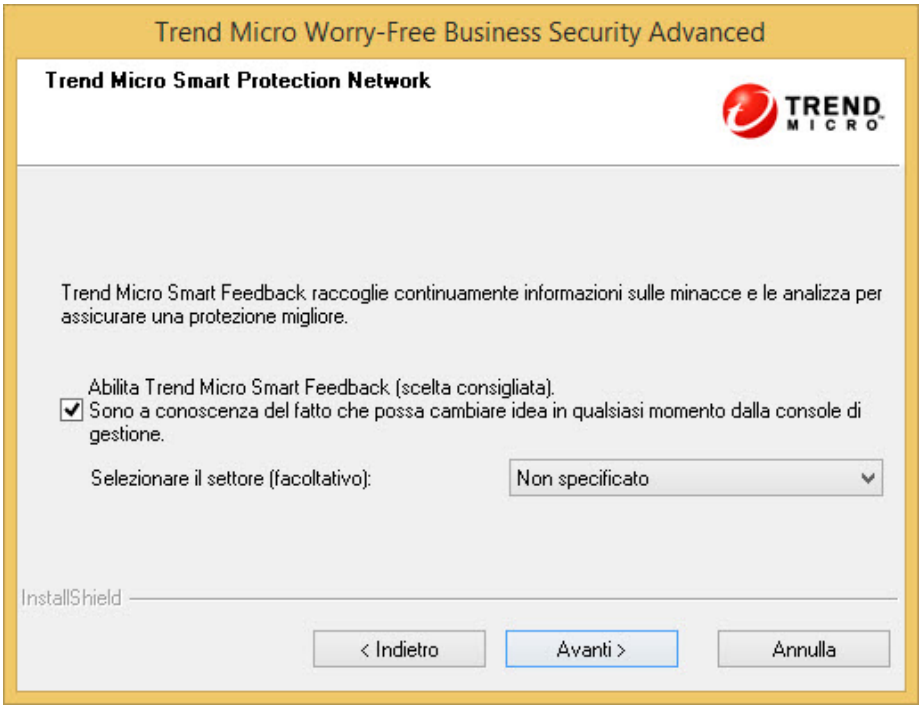
  Se il server SMTP si trova sullo stesso computer di WFBS e utilizza la porta 25, il programma di installazione rileva il nome del server SMTP e aggiorna i campi Server SMTP e Porta.

- **Porta**: la porta utilizzata dal server SMTP per le comunicazioni

- **Destinatari**: gli indirizzi di posta elettronica utilizzati dal server SMTP per inviare avvisi di notifica. È possibile immettere più indirizzi di posta elettronica quando tali notifiche vanno inviate a più utenti

Fare riferimento alle impostazioni del server di posta ISP. Se non si conoscono queste impostazioni, procedere con l'operazione successiva. È possibile aggiornare le impostazioni SMTP dopo l'installazione. Per istruzioni, consultare la Guida dell'amministratore.

Smart Protection Network



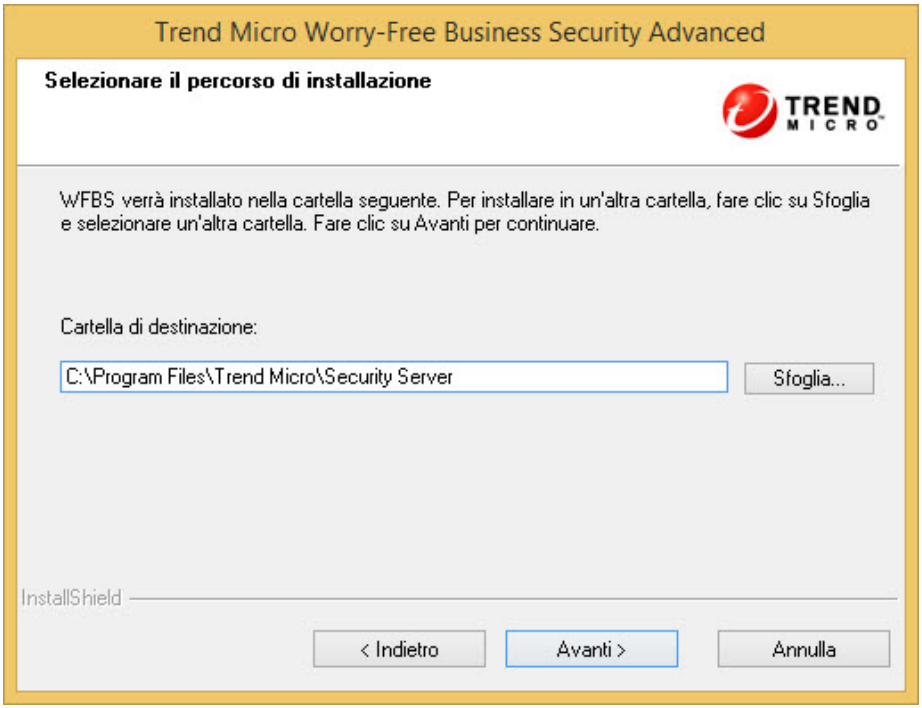
Scegliere se si desidera partecipare al programma di feedback su Trend Micro Smart Protection Network.

Questa funzionalità opzionale fornisce i feedback relativi a minacce informatiche riportati a Trend Micro. Trend Micro consiglia di lasciare abilitato il valore predefinito dal momento che utilizza i dati di feedback Worry-Free Business Security in tutto il mondo per aumentare l'efficacia delle soluzioni alle minacce informatiche. È possibile scegliere di annullare la partecipazione in un secondo momento, mediante la console Web.

Configurazione delle impostazioni per un'installazione personalizzata

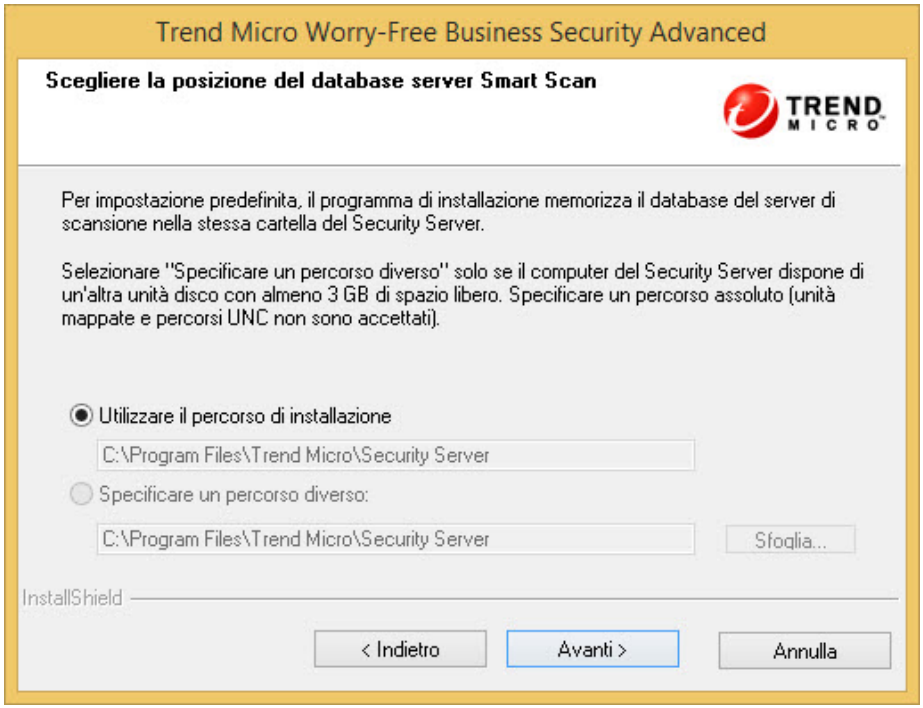
Durante un'installazione personalizzata, vengono visualizzate le seguenti schermate in sequenza:

Percorso di installazione



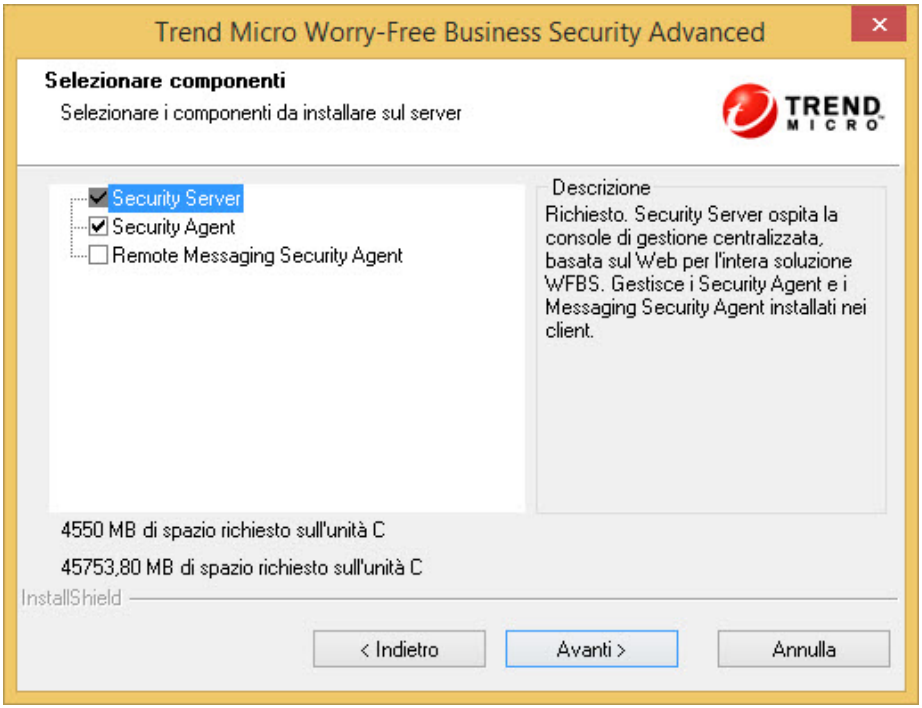
La cartella predefinita di installazione di Worry-Free Business Security è `C:\Programmi\Trend Micro\Security Server` o `C:\Programmi (x86)\Trend Micro\Security Server`. Fare clic su **Sfoglia** se si desidera installare Worry-Free Business Security in un'altra cartella.

Posizione del database server di scansione



Selezionare **Utilizzare il percorso di installazione** per memorizzare il database del server di scansione nella stessa cartella del Security Server oppure selezionare **Specificare un percorso diverso** e digitare il percorso assoluto di un'altra posizione sul Security Server. Non è possibile specificare un'unità mappata o un percorso UNC.

Seleziona componenti



Selezionare i componenti da installare sul computer di destinazione:

- **Security Server** (richiesto): Security Server ospita la console Web centralizzata
- **Security Agent** (opzionale): agent che protegge desktop e server
- **Messaging Security Agent** (opzionale): quando si installa Security Server su un computer in cui già è installato un server Microsoft Exchange, viene richiesto di effettuare l'installazione un Messaging Security Agent locale (solo Advanced).
- **Remote Messaging Security Agent** (opzionale): quando si installa Security Server su un computer che non riesce a rilevare la presenza di server Microsoft Exchange locali, viene richiesto di installare Messaging Security Agent remoto (solo Advanced) sui server remoti.

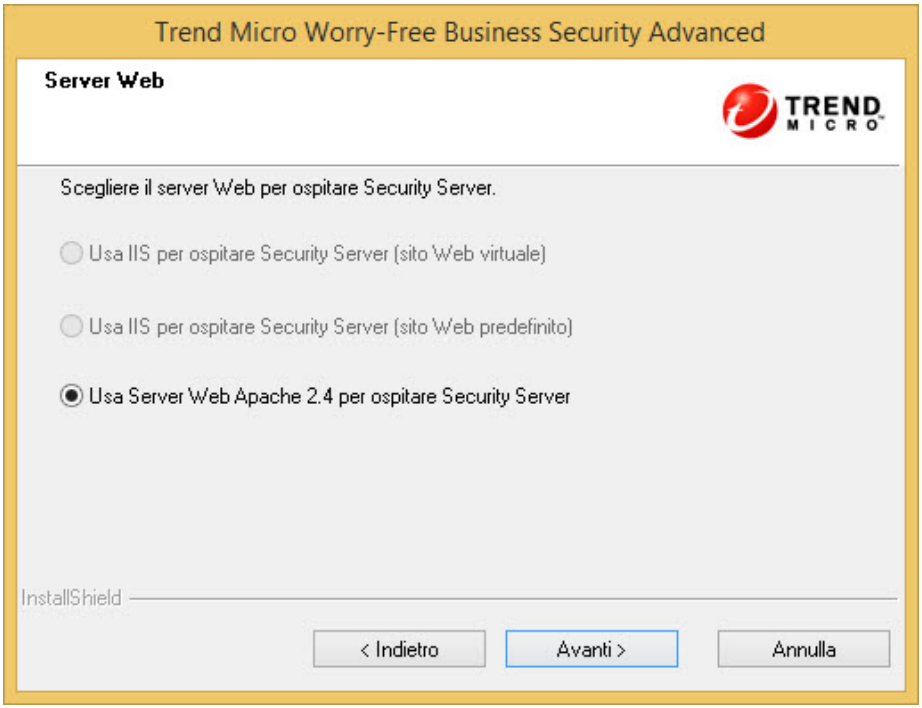
Nota

Se sul computer in cui viene installato Security Server è già presente un server Exchange, nella schermata Seleziona componenti non viene visualizzato Messaging Security Agent remoto, ma solo Messaging Security Agent locale.

Configura Security Server

Nella schermata Configura Security Server sono fornite le impostazioni di Security Server da configurare.

Server Web



Per l'installazione da zero, il programma di installazione verifica se esiste un server Web sul computer di destinazione.

SCENARIO	RISULTATO	NOTE

Il programma di installazione rileva i server Web IIS e Apache	• Per un'installazione tipica o minima, il programma di installazione utilizza IIS.
	• Per un'installazione personalizzata:
	  • Il programma di installazione utilizza automaticamente IIS se la versione del server Web Apache non è supportata.
	  • Scegliere uno dei due server Web se la versione del server Web Apache non è supportata.
		Se sul computer viene eseguito Windows 7, 8.1 o 10, Trend Micro consiglia di utilizzare un'installazione personalizzata, selezionando Apache come server Web.

Il programma di installazione rileva solo un server Web IIS	• Per un'installazione tipica o minima, il programma di installazione utilizza IIS. • Per un'installazione personalizzata, scegliere uno dei due server Web. Se si sceglie Apache, il programma di installazione installa automaticamente Apache versione 2.4.	

SCENARIO	RISULTATO	NOTE

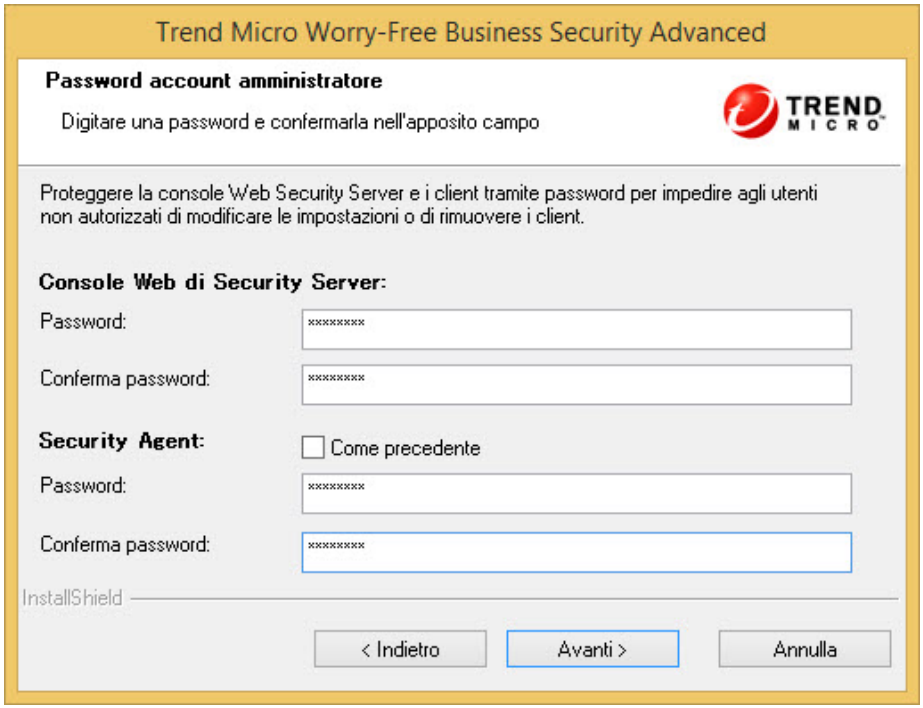
Il programma di installazione rileva solo un server Web Apache	• Il programma di installazione utilizza Apache se la versione di Apache è 2.4.
	• L'installazione non procede se esistono altre versioni di Apache. Prendere in considerazione le seguenti operazioni:
	  • Disinstallare Apache, se non utilizzato da altre applicazioni.
	  • Aggiornare Apache alla versione 2.4.
	  • Scegliere il computer sul quale installare il Security Server.
		Le seguenti piattaforme possiedono il server IIS e sono supportate dal Security Server:
		• Windows Server 2008/2008 R2
		• Windows SBS 2008
		• Windows EBS 2008
		• Windows SBS 2011 Standard/Essentials
		• Windows Server 2012/2012 R2
		• Windows Server 2016
		Se il programma di installazione non è in grado di rilevare il server IIS su queste piattaforme, IIS potrebbe non essere attivo (per impostazione predefinito o disabilitato dall'amministratore di sistema). In questo caso, abilitare il server IIS.

Il programma di installazione non rileva server Web	Il programma di installazione installa automaticamente il server Web Apache versione 2.4.	

Per gli aggiornamenti, se attualmente è utilizzato il server Web Apache:

- Il programma di installazione aggiorna automaticamente Apache alla versione 2.4 se il server Web Apache è stato installato dal programma di installazione di Worry-Free Business Security 8.x/9.x.
- Il programma di installazione mantiene la versione di Apache esistente se è stata installata da altri programmi.

Password account amministratore



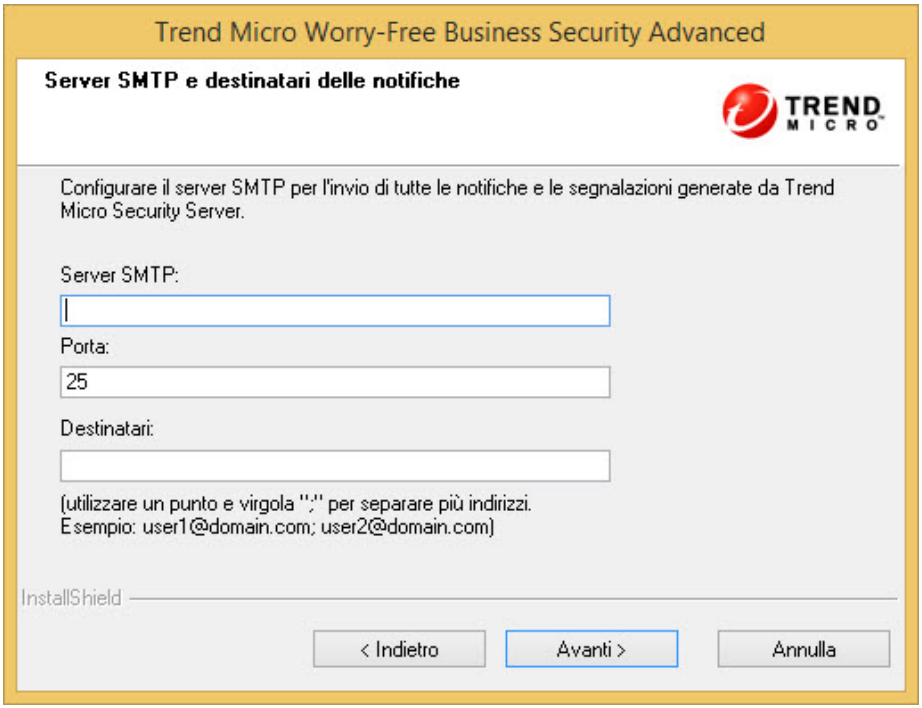
Specificare password diverse per la console Web di Security Server e per il Security Agent.

- **Console Web Security Server**: necessaria per eseguire l'accesso alla console Web
- **Security Agent**: richiesta per disinstallare o rimuovere i Security Agent dai client

Nota

Il campo Password contiene tra 1 e 24 caratteri e rileva la distinzione tra maiuscole e minuscole.

Server SMTP e destinatari delle notifiche



Inserire le seguenti informazioni:

- **Server SMTP**: l'indirizzo IP del server di posta elettronica

  Nota

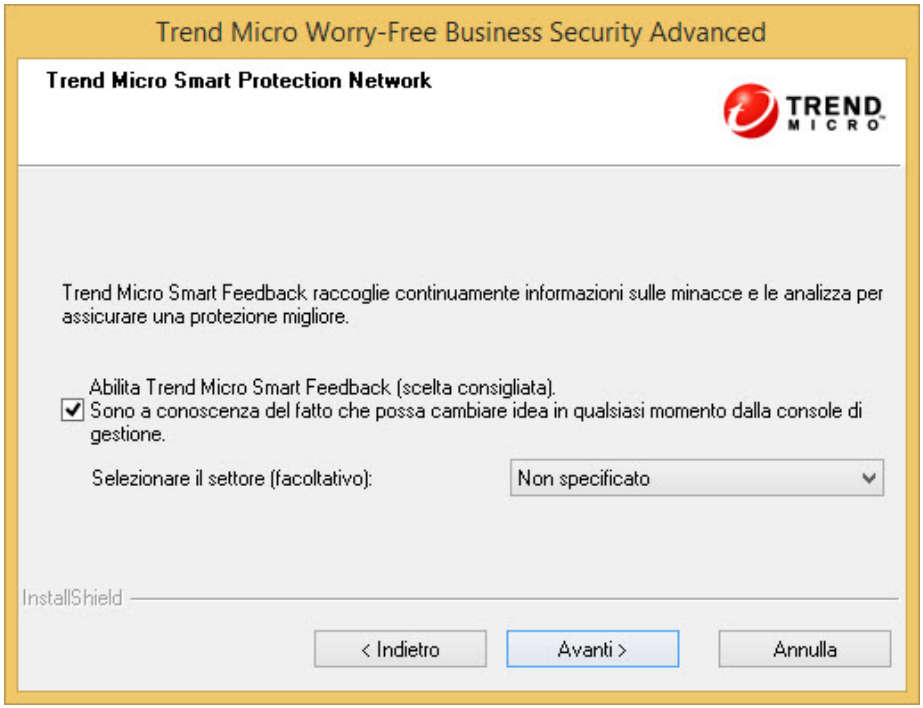
  Se il server SMTP si trova sullo stesso computer di WFBS e utilizza la porta 25, il programma di installazione rileva il nome del server SMTP e aggiorna i campi Server SMTP e Porta.

- **Porta**: la porta utilizzata dal server SMTP per le comunicazioni

- **Destinatari**: gli indirizzi di posta elettronica utilizzati dal server SMTP per inviare avvisi di notifica. È possibile immettere più indirizzi di posta elettronica quando tali notifiche vanno inviate a più utenti

Fare riferimento alle impostazioni del server di posta ISP. Se non si conoscono queste impostazioni, procedere con l'operazione successiva. È possibile aggiornare le impostazioni SMTP dopo l'installazione. Per istruzioni, consultare la Guida dell'amministratore.

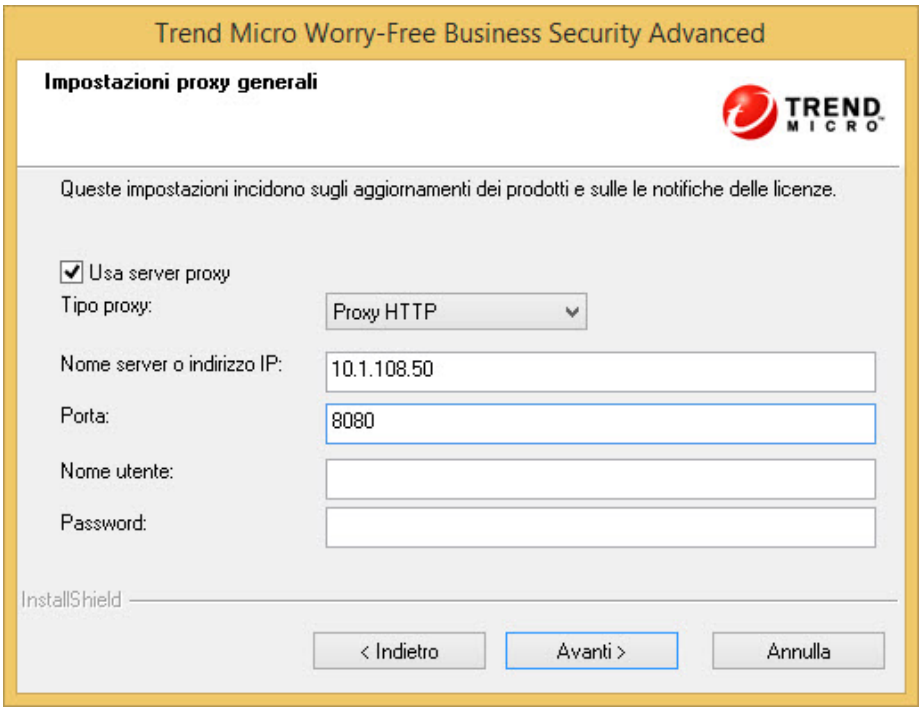
Smart Protection Network



Scegliere se si desidera partecipare al programma di feedback su Trend Micro Smart Protection Network.

Questa funzionalità opzionale fornisce i feedback relativi a minacce informatiche riportati a Trend Micro. Trend Micro consiglia di lasciare abilitato il valore predefinito dal momento che utilizza i dati di feedback Worry-Free Business Security in tutto il mondo per aumentare l'efficacia delle soluzioni alle minacce informatiche. È possibile scegliere di annullare la partecipazione in un secondo momento, mediante la console Web.

Impostazioni proxy generali



Se un server proxy deve accedere a Internet, selezionare la casella di controllo **Usa server proxy** e fornire le informazioni seguenti:

- **Tipo di server proxy**

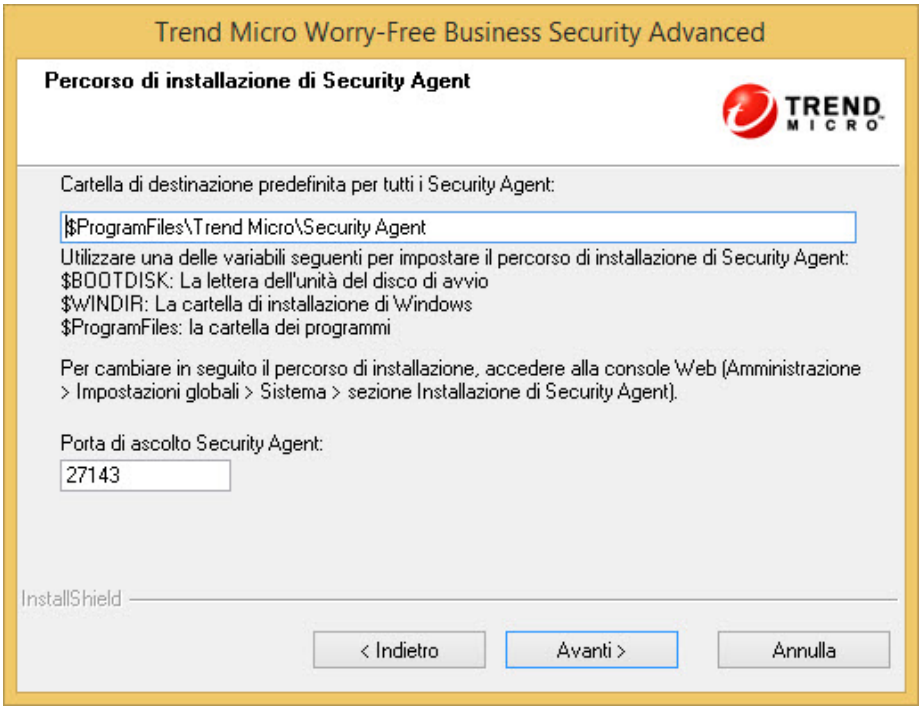
- **Nome server o indirizzo IP**
- **Porta**
- **Nome utente e password**: da specificare solo se il server proxy richiede l'autenticazione

Configura Security Agent

Nella schermata Configura Security Agent sono fornite le impostazioni di Security Agent da configurare.

Dopo aver installato il Security Server, installare il Security Agent sui client nella rete. Per informazioni dettagliate sui diversi metodi di installazione dei Security Agent, consultare la Guida per l'amministratore.

Percorso di installazione Security Agent



Impostare i seguenti elementi:

- **Percorso di installazione**: Cartella di destinazione in cui vengono installati i file del Security Agent
- **Porta di ascolto di Security Agent**: Il numero di porta utilizzato per la comunicazione tra Security Agent e Security Server

Impostazioni Security Agent

Configurare le impostazioni del Security Agent per i server e i desktop.

- **Server**: I Security Agent con piattaforme server Windows (come Windows Server 2008) vengono aggiunti al gruppo dei server predefiniti quando sono aggiunti alla console Web. È possibile abilitare tecnologie diverse per questo gruppo in base a esigenze specifiche.
- **Desktop**: I Security Agent con piattaforme desktop Windows (come Windows Vista 7) vengono aggiunti al gruppo dei desktop predefiniti quando sono aggiunti alla console Web. È possibile abilitare tecnologie diverse per questo gruppo in base a esigenze specifiche.

In ogni gruppo, è possibile configurare i componenti seguenti:

- **Smart Scan**: Smart Scan utilizza un server di scansione centrale sulla rete per alleggerire i client di parte del carico di lavoro legato alle scansioni.
- **Antivirus e Anti-Spyware**: Esegui scansione dei file per rilevare il codice dannoso al momento dell'accesso o della creazione
- **Firewall**: Consente di proteggere i client da malware e dai virus di rete tramite la creazione di una barriera tra il client e la rete
- **Reputazione Web**: blocca i siti Web dannosi mediante il rilevamento della credibilità dei domini Web e assegna un punteggio di reputazione in base a diversi fattori di identificazione
- **Filtro URL**: Blocca le categorie di siti Web specificate, ad esempio, siti pornografici e social network, in base alla politica della società.
- **Monitoraggio del comportamento**: analizza il comportamento del programma per rilevare tempestivamente le minacce note e sconosciute
- **Controllo dispositivo**: regola l'accesso ai dispositivi di memorizzazione esterni e alle risorse di rete
- **Intelligenza computazionale predittiva**: utilizza una tecnologia di intelligenza computazionale avanzata per correlare le informazioni sulle minacce ed eseguire analisi dei file approfondite allo scopo di rilevare i rischi di sicurezza sconosciuti emergenti attraverso le impronte digitali genetiche, la mappatura API e altre funzionalità relative ai file.

Impostazioni proxy per servizi aggiuntivi

I servizi **Smart Scan**, **Reputazione Web** e **Monitoraggio del comportamento** utilizzano l'indirizzo e la porta del server proxy specificati in Internet Explorer sui computer client. Se il server proxy richiede l'autenticazione, fornire le credenziali di accesso in questa schermata.

Configurazione di Messaging Security Agent

Installare Messaging Security Agent durante l'installazione di Security Server.

Note e promemoria per l'installazione:

- Non è necessario interrompere o avviare i servizi Microsoft Exchange prima o dopo l'installazione.

- Se sul client sono presenti informazioni derivanti da una precedente installazione di Messaging Security Agent non è possibile completare correttamente l'installazione di Messaging Security Agent. Utilizzare l'utilità Windows Installer Cleanup per disinfettare eventuali residui di un'installazione precedente. Per scaricare l'utilità Windows Installer Cleanup, visitare il sito:

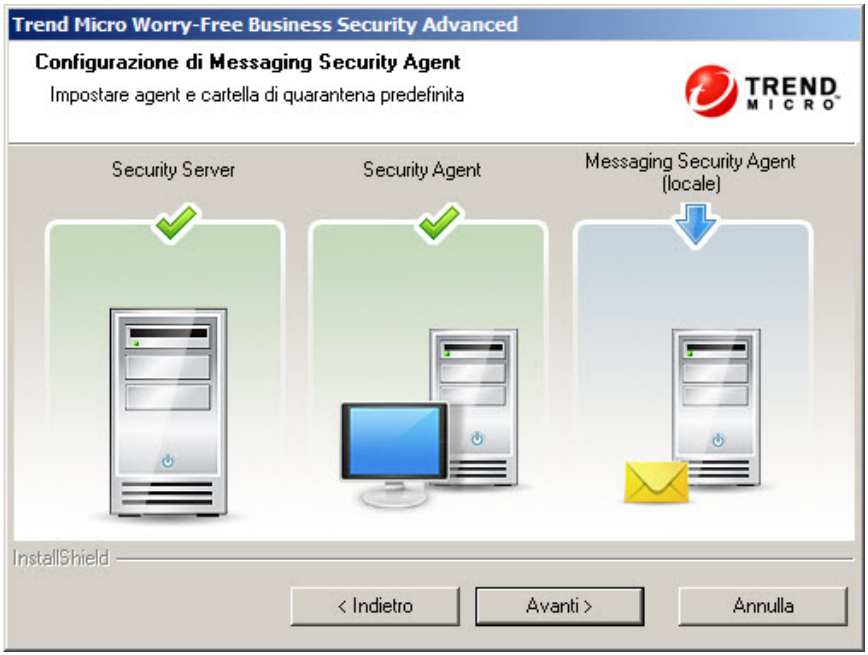
  https://support.microsoft.com/en-us/help/290301

- Se si sta installando Messaging Security Agent su un server che esegue strumenti di blocco, rimuovere lo strumento di blocco in modo da non disabilitare il servizio IIS e impedire il buon esito dell'installazione.

- È possibile installare Messaging Security Agent anche dalla console Web dopo l'installazione del Security Server. Per maggiori dettagli, vedere la Guida per l'amministratore.

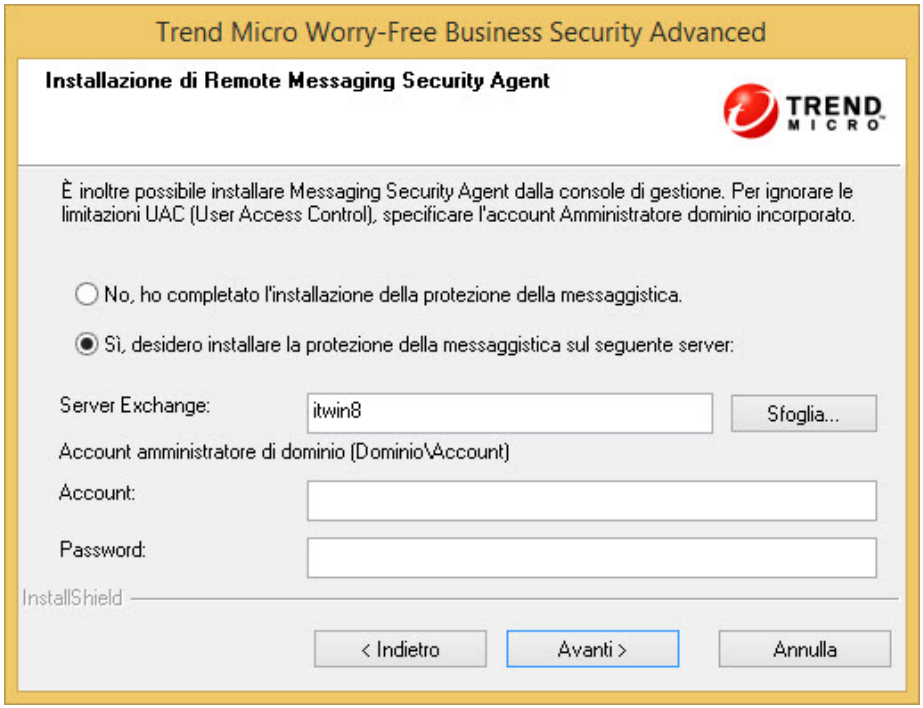
La procedura richiede l'installazione di Messaging Security Agent in uno di questi momenti:

- Quando si installa Security Server su un computer in cui è installato il server Microsoft Exchange, viene richiesto di installare un Messaging Security Agent **locale**.



- Quando si installa Security Server su un computer che non riesce a rilevare la presenza di server Microsoft Exchange locali, viene richiesto di installare Messaging Security Agent **remoto** sui server remoti.

Installazione di Messaging Security Agent



Inserire le seguenti informazioni:

- **Server Exchange**

> **Nota**
>
> Il programma di installazione rileva automaticamente il nome del server Exchange locale e completa il campo Server Exchange se questo si trova sullo stesso computer di Security Server. Se un server Exchange è installato sullo stesso computer ma il suo nome non viene inserito automaticamente, controllare che l'ambiente soddisfi i requisiti di sistema di Messaging Security Agent.

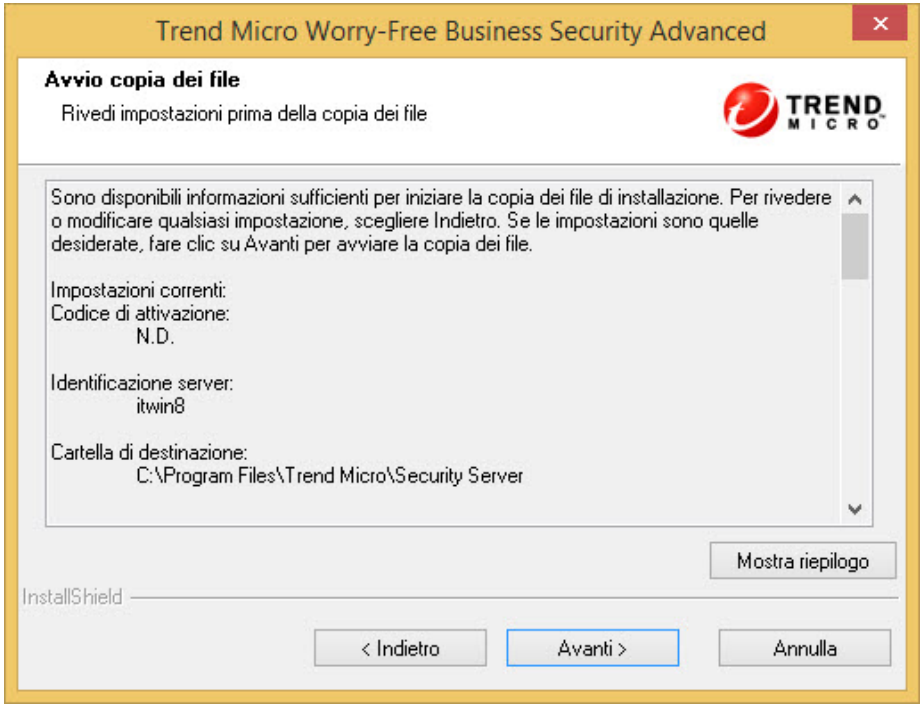
- **Account amministratore di dominio**
- **Password**

Nota

Il programma di installazione potrebbe non essere in grado di trasmettere password contenenti caratteri speciali non alfanumerici al computer su cui è installato il server Exchange. In questo caso è impedita l'installazione di Messaging Security Agent. Per risolvere questo problema, modificare provvisoriamente la password dell'account predefinito di amministratore di dominio oppure installare Messaging Security Agent direttamente sul server Microsoft Exchange.

Fase 3: procedura di installazione

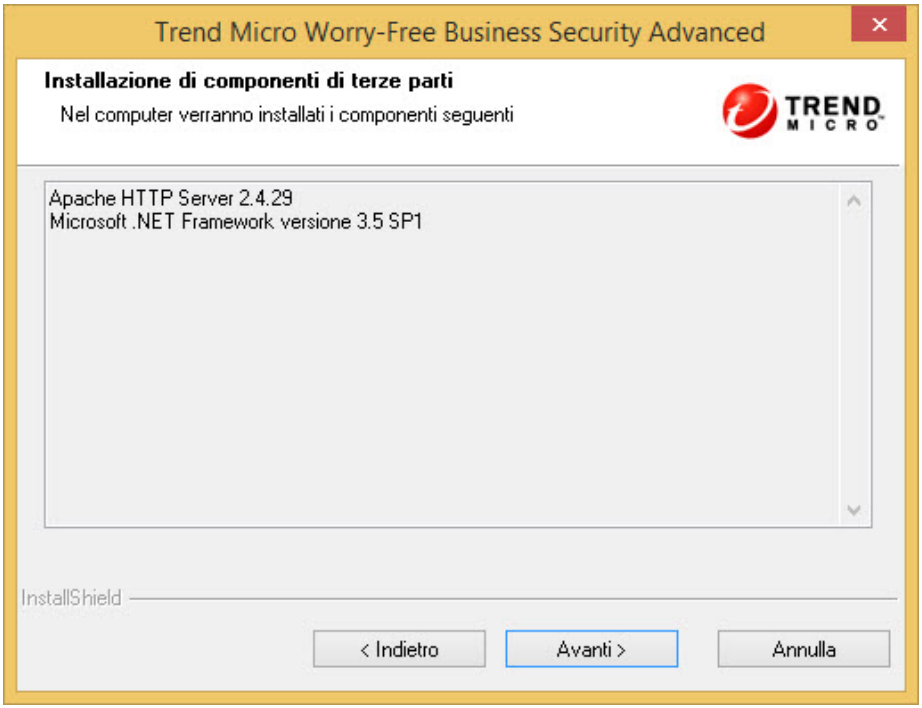
Avvio copia dei file



Nella schermata Avvio copia dei file è presente un riepilogo di tutti i parametri che verranno utilizzati durante l'installazione di Worry-Free Business Security.

Fare clic su **Indietro** se si desidera verificare le impostazioni dell'installazione precedente o fare clic su **Avanti** per continuare l'installazione.

Installare i componenti di terze parti

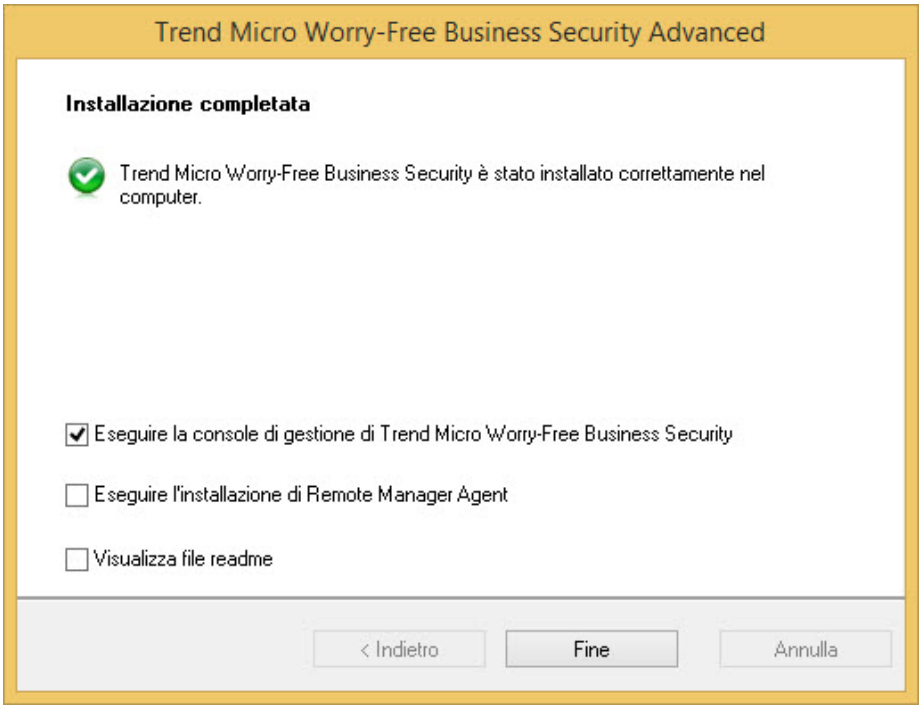


In questa schermata vengono visualizzati i componenti di terze parti che verranno installati. Per avviare l'installazione dei componenti selezionati, fare clic su **Avanti**.

Stato installazione

Il completamento del processo di installazione potrebbe richiedere qualche minuto. Durante l'installazione, viene visualizzata una schermata di stato che mostra l'avanzamento del processo.

Installazione completata



È possibile selezionare le caselle di controllo per:

- Aprire la console di gestione basata sul Web (selezionata per impostazione predefinita).
- Installare Remote Manager Agent (per la procedura, consultare la *Guida per l'amministratore*).
- Leggere il file readme

Per terminare la procedura di installazione, fare clic su **Fine**.

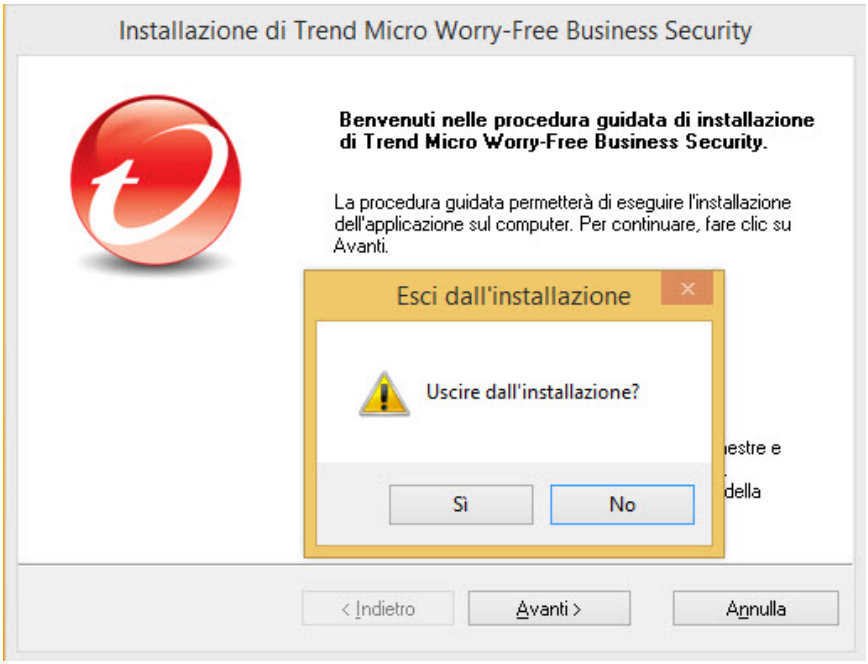
Installazione di più Security Server tramite l'installazione invisibile

È possibile utilizzare l'installazione invisibile per consentire l'esecuzione di più installazioni identiche su reti distinte. È possibile registrare le impostazioni di installazione in una sessione dell'installazione guidata e quindi utilizzare tali impostazioni per generare installazioni automatizzate.

Registrazione di una sessione di installazione

Procedura

1. Scaricare ed estrarre i file WFBS sul disco rigido. Quando l'installazione guidata inizia la raccolta delle impostazioni di installazione, fare clic su **Annulla** > **Sì** > **Fine**.



2. Nel prompt dei comandi, accedere alla directory in cui sono stati estratti i file di configurazione WFBS, ad esempio: `C:\Extract\WFBS\CSM`

3. Al prompt, digitare `Setup.exe /r /f1"c:\silent-install.iss"` e premere **Invio**.

   L'installazione guidata viene riavviata. I dati immessi vengono registrati nel file silent-install.iss sull'unità C.

4. Seguire le istruzioni visualizzate. Le istruzioni sono le stesse di quelle descritte in *Installazione di Security Server a pagina 2-12*.

5. Alla fine della sessione di registrazione, viene visualizzata la seguente schermata di conferma. Fare clic su **Fine** per terminare la sessione di registrazione e ritornare al prompt dei comandi.

Avvio dell'installazione invisibile

Procedura

1. Nel prompt dei comandi, accedere alla directory in cui sono stati estratti i file di configurazione WFBS, ad esempio: `C:\Extract\WFBS\CSM`
2. Al prompt, digitare `Setup.exe /s /f1"c:\silent-install.iss"` e premere **Invio**.

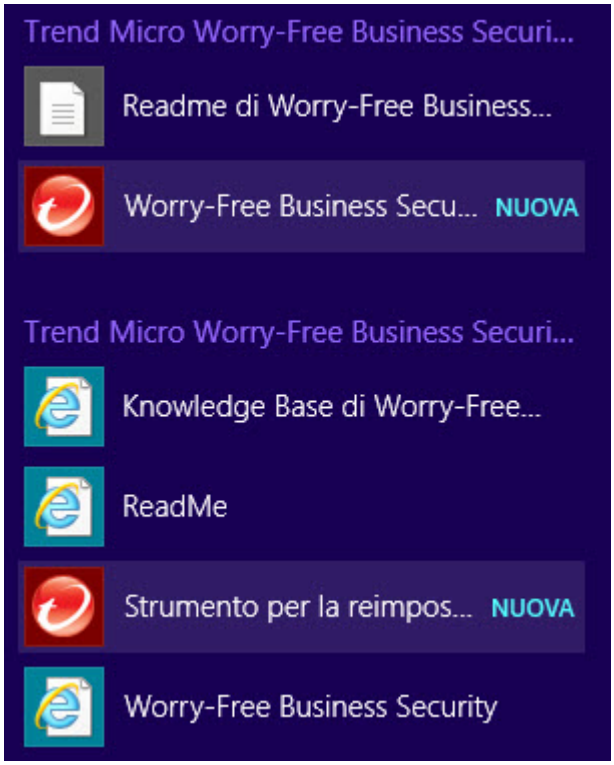
   L'installazione invisibile di WFBS viene avviata automaticamente e impiegherà lo stesso tempo di un'installazione normale.

   Durante l'installazione invisibile, non viene visualizzato alcun indicatore di avanzamento.
3. Per verificare che l'installazione sia stata completata correttamente, aprire il file `c:\setup.log`. Se `ResultCode=0`, significa che l'installazione è stata completata.
4. Ripetere le operazioni da 1 a 3 su tutti gli altri computer nella rete.

Verifica dell'installazione

Procedura

- Fare clic su **Start** > **Programmi** per verificare se il Security Server e il Security Agent sono visualizzati nell'elenco.



- Fare clic su **Start** > **Pannello di controllo** > **Programmi** > **Disinstalla un programma** per verificare se il programma WFBS e Security Agent vengono visualizzati nell'elenco.
- Accedere alla console di gestione con l'URL del server: `https://{nome_server}:{numero porta}/SMB`

Nota

Se non si utilizza Security Socket Layer (SSL), digitare `http` anziché `https`.

Capitolo 3

Aggiornamento dei Security Server e dei Security Agent

In questo capitolo vengono fornite le informazioni necessarie per l'aggiornamento di Security Server e Security Agent.

Requisiti di installazione e aggiornamento

Visitare il sito Web seguente per un elenco completo dei requisiti per l'installazione e per gli aggiornamenti:

http://docs.trendmicro.com/it-it/smb/worry-free-business-security.aspx

Considerazioni sull'aggiornamento

Quando si esegue l'aggiornamento del Security Server e degli agent occorre tenere presenti gli elementi riportati di seguito:

- *Requisiti IPv6 per gli aggiornamenti a pagina 3-2*
- *Migliori pratiche per l'aggiornamento a pagina 3-3*

Requisiti IPv6 per gli aggiornamenti

Di seguito sono elencati i requisiti IPv6 per il Security Server:

- È necessario che il Security Server da aggiornare sia installato su Windows 7, 8.1, 10, Server 2008, 2012, 2012 R2, 2016 e SBS 2008/2011. Non è possibile aggiornare i Security Server su Windows XP, Server 2003 e SBS 2003, in quanto tali sistemi operativi supportano solo parzialmente l'indirizzamento IPv6.
- Assegnare un indirizzo IPv6 al Security Server. Inoltre, il server deve essere identificato tramite il nome host, preferibilmente mediante il nome di dominio completo (FQDN). Se il server viene identificato tramite l'indirizzo IPv6, tutti i client attualmente gestiti dal server perderanno la connessione al server. Se il server è identificato tramite l'indirizzo IPv4, non potrà implementare l'agent su client IPv6 puri.
- Verificare che l'indirizzo IPv6 o IPv4 del computer host del Security Server possa essere recuperato usando, ad esempio, il comando "ping" o "nslookup".

Migliori pratiche per l'aggiornamento

Quando si esegue l'aggiornamento alla versione più recente di WFBS è possibile mantenere le impostazioni dei client. Per consentire un facile ripristino delle impostazioni esistenti in caso di aggiornamento non riuscito, Trend Micro consiglia di:

- Eseguire un backup del database del Security Server
- Eliminare tutti i file di registro dal Security Server

Backup del database del Security Server

Procedura

1. Arrestare Trend Micro Security Server Master Service.
2. In Esplora risorse, accedere alla cartella Security Server e copiare il contenuto di `\PCCSRV\HTTPDB` in un altro percorso, ad esempio in un'altra directory nello stesso server, in un altro computer o su un disco rimovibile.

Eliminazione dei file di registro dal Security Server

Procedura

1. Accedere a **Rapporti** > **Manutenzione** > **Eliminazione manuale dei registri**.
2. Per i tipi di registro che si desidera eliminare, impostare **Elimina i registri più datati di** su 0.
3. Scegliere uno dei metodi seguenti per eliminare i registri:
   - Fare clic su **Elimina** per ciascun tipo di registro.
   - Fare clic su **Elimina tutto** per eliminare tutti i registri.

Aggiornamenti dalla versione precedente

La presente versione del prodotto supporta l'aggiornamento da una qualsiasi delle seguenti versioni di Worry-Free Business Security o Worry-Free Business Security Advanced:

- 9.x (inclusi tutti i service pack)
- 8.x (8.0 e 8.0 SP1)

Questa versione del prodotto non supporta l'aggiornamento da:

- Worry-Free Business Security o Worry-Free Business Security - Advanced 7.x
- Worry-Free Business Security o Worry-Free Business Security - Advanced 6.x
- Worry-Free Business Security o Worry-Free Business Security - Advanced 5.x
- Tutti gli aggiornamenti che supportavano Windows 2000
- Client/Server Messaging Security 3.6 (tranne la versione in lingua giapponese)
- 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 o ScanMail per Microsoft Exchange
- Da una lingua all'altra

A seconda dell'ampiezza di banda della rete e del numero di agent gestiti dal Security Server, è possibile suddividere l'aggiornamento della versione degli agent in gruppi o eseguire l'aggiornamento di tutti gli agent immediatamente dopo gli aggiornamenti del server.

Metodo di aggiornamento 1: aggiornamento tramite il pacchetto di installazione

Procurarsi il pacchetto di installazione della versione del prodotto in questione ed eseguire `Setup.exe` sul computer del Security Server. Quando il programma di installazione rileva un Security Server sul computer, richiede di eseguire l'aggiornamento, come illustrato nell'immagine che segue.

Attenersi alle istruzioni visualizzate per aggiornare il Security Server.

Una volta completato l'aggiornamento:

- I Security Agent online vengono aggiornati immediatamente

- I Security Agent offline vengono aggiornati quando tornano online

  Richiedere agli utenti di connettersi alla rete in modo che Security Agent sia online. Per i Security Agent che rimangono offline per un periodo di tempo prolungato, richiedere agli utenti di disinstallare Security Agent dall'endpoint e utilizzare un metodo di installazione dell'agente idoneo (come Client Packager) indicato nella *Guida per l'amministratore* per installare Security Agent.

Nota

Dopo aver eseguito l'aggiornamento a questa versione, verranno mantenute tutte le impostazioni precedenti dell'agent, tranne i privilegi dell'Update Agent. Questo significa che gli Update Agent torneranno ad essere Security Agent in seguito all'aggiornamento. Riassegnarli come Update Agent dalla console di gestione.

Per informazioni dettagliate, consultare la sezione http://esupport.trendmicro.com/solution/en-US/1057531.aspx.

Metodo di aggiornamento 2: trasferimento degli agent a Security Server 10.0

Eseguire una nuova installazione di Security Server, quindi trasferire i Security Agent al server. Gli agent spostati vengono automaticamente aggiornati alla versione 10.0.

Parte 1: esecuzione di una nuova installazione di Security Server 10.0

Procedura

1. Eseguire una nuova installazione del Security Server su un computer. Per i dettagli, consultare *Installazione di Security Server a pagina 2-12*.
2. Registrare le seguenti informazioni relative a Security Server 10.0. Specificare queste informazioni nel Security Server supportato quando si spostano gli agenti.
   - Nome host o indirizzo IP
   - Porta di ascolto del server

Il nome host e la porta di ascolto si trovano sulla schermata Impostazioni di sicurezza del Security Server, sopra il pannello delle attività.

Parte 2: aggiornamento Agent

Procedura

1. Nella console Web del Security Server supportato, passare a **Impostazioni di sicurezza**.
2. Per spostare i Security Agent, selezionare un gruppo e quindi selezionare gli agent.

   Suggerimento

   Per selezionare più Security Agent adiacenti, fare clic sul primo agent dell'intervallo, tenere premuto il tasto MAIUSC e quindi fare clic sull'ultimo agent dell'intervallo. Per selezionare più agent non contigui, fare clic sul primo agent dell'intervallo, tenere premuto il tasto CTRL e quindi fare clic sugli agent da selezionare .

3. Fare clic su **Gestisci struttura client** > **Sposta client**.

   Viene visualizzata una nuova schermata.

4. Digitare il nome host e la porta di ascolto di Security Server 10.0 in cui verranno spostati gli agent.
5. Fare clic su **Sposta**.

Risultati dell'aggiornamento

- Inizia lo spostamento e l'aggiornamento della versione degli agent online. Dopo l'aggiornamento, a seconda del sistema operativo dell'endpoint, i Security Agent verranno riuniti sotto il gruppo **Desktop (predefiniti)** o **Server (predefiniti)** di Security Server 10.0. L'agente acquisisce le impostazioni del nuovo gruppo.
- L'aggiornamento della versione degli agent offline avviene quando questi tornano online. Richiedere agli utenti di connettersi alla rete in modo che l'agente sia online. Per i Security Agent che rimangono offline per un periodo di tempo prolungato,

richiedere agli utenti di disinstallare Security Agent dall'endpoint e utilizzare un metodo di installazione dell'agente idoneo (come Client Packager) indicato nella *Guida per l'amministratore* per installare Security Agent.

Aggiornamenti alla versione completa o ad Advanced Edition

Utilizzare la schermata Licenza del prodotto sulla console Web per:

- Eseguire l'aggiornamento dalla versione di prova alla versione completa del prodotto
- Eseguire l'aggiornamento dalla versione standard alla versione Advanced del prodotto.

Versioni di prova e complete

Quando la versione di prova sta per scadere, nella schermata Stato in tempo reale della console Web viene visualizzato un messaggio di notifica. È possibile effettuare l'aggiornamento da una versione di prova alla versione con licenza completa mediante la console Web. Le impostazioni di configurazione verranno salvate. Acquistando una licenza completa si riceve una chiave di registrazione o un codice di attivazione.

Edizioni standard e Advanced

Trend Micro offre due prodotti simili mirati alla protezione dei client e della rete: Worry-Free Business Security Standard e Worry-Free Business Security Advanced.

TABELLA 3-1. Versioni del prodotto

VERSIONE DEL PRODOTTO	WORRY-FREE BUSINESS SECURITY STANDARD	WORRY-FREE BUSINESS SECURITY ADVANCED
Soluzione lato client	Sì	Sì
Soluzione lato server	Sì	Sì
Soluzione Microsoft Exchange Server	No	Sì

È possibile eseguire l'aggiornamento da Worry-Free Business Security Standard a Worry-Free Business Security Advanced tramite un codice di attivazione ottenuto da Trend Micro.

Aggiornamento alla versione completa o ad Advanced Edition

Procedura

1. Nella console Web, andare su **Amministrazione** > **Licenza del prodotto**.
2. Se si dispone di un Codice di attivazione, selezionare **Immetti un nuovo codice**, digitarlo nel campo **Nuovo codice di attivazione** e fare clic su **Attiva**.

   Se non si è in possesso del codice di attivazione, accedere al sito Web di Trend Micro all'indirizzo http://olr.trendmicro.com per eseguire la registrazione online e ottenere il codice di attivazione.

Appendice A

Assistenza tecnica

Ulteriori informazioni sui seguenti argomenti:

Risorse per la risoluzione dei problemi

Prima di contattare l'assistenza tecnica, consultare le seguenti risorse online di Trend Micro.

Utilizzo del portale di supporto

Il portale Assistenza Trend Micro è una risorsa online attiva 24 ore su 24, sette giorni su sette, che contiene le informazioni più aggiornate su problemi sia comuni che insoliti.

Procedura

1. Accedere a http://esupport.trendmicro.com.
2. Effettuare la selezione tra i prodotti disponibili o fare clic sull'apposito pulsante per avviare la ricerca di soluzioni.
3. Per cercare le soluzioni possibili, utilizzare la casella **Cerca assistenza**.
4. Se non viene individuata alcuna soluzione, fare clic su **Contatta supporto** e selezionare il tipo di supporto necessario.

   Suggerimento

   Per segnalare un caso di assistenza online, visitare la pagina al seguente URL:

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

   Il caso viene esaminato da un addetto all'assistenza tecnica di Trend Micro e la risposta giungerà nell'arco di 24 al massimo.

Enciclopedia delle minacce

La maggior parte delle minacce informatiche di oggi è costituita da minacce miste, ovvero dalla combinazione di due o più tecnologie ideata per bypassare i protocolli di sicurezza dei computer. Trend Micro ostacola queste minacce complesse con prodotti

pensati per creare una strategia di difesa personalizzata. L'Enciclopedia delle minacce fornisce un elenco esauriente di nomi e sintomi delle varie miscele di minacce, incluse minacce informatiche conosciute, spam, URL dannosi, nonché vulnerabilità conosciute.

Per ulteriori informazioni, vedere http://about-threats.trendmicro.com/it/threatencyclopedia#malware:

- Minacce informatiche e codici mobili dannosi attualmente attivi o in circolazione
- Pagine informative sulle minacce correlate, per una descrizione degli attacchi Web completa.
- Avvisi sulle minacce Internet riguardanti gli attacchi mirati e le minacce per la sicurezza
- Informazioni sull'andamento online e sugli attacchi Web
- Rapporti settimanali sulle minacce informatiche

Come contattare Trend Micro

È possibile contattare gli addetti di Trend Micro via telefono o e-mail:

Indirizzo	TREND MICRO Italy S.r.l. Edison Park Center Viale Edison 110 - Edificio C 20099 Sesto San Giovanni (MI) Italia
Telefono	+39 02 925931
Sito Web	http://www.trendmicro.it
Indirizzo e-mail	sales@trendmicro.it

- Uffici di assistenza nel mondo:

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

- Come contattare Trend Micro:

  http://www.trendmicro.it/informazioni/contatti/index.html

- Documentazione dei prodotti Trend Micro

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

Semplificazione della chiamata all'assistenza tecnica

Per migliorare la risoluzione dei problemi, tenere a disposizione le seguenti informazioni:

- Passaggi che hanno causato il problema
- Informazioni sulla rete o sulle apparecchiature
- Marca e modello del computer ed eventuale hardware aggiuntivo o dispositivi collegati
- Quantità di memoria e spazio libero su disco
- Sistema operativo e versione del service pack
- Versione dell'Agent installato
- Numero di serie o codice di attivazione
- Descrizione dettagliata dell'ambiente di installazione
- Testo esatto di eventuali messaggi di errore ricevuti

Invio di contenuti sospetti a Trend Micro

Sono disponibili numerose opzioni per inviare contenuti sospetti a Trend Micro per ulteriore analisi.

Email Reputation Services

Inviare una query per la reputazione di un indirizzo IP specific e indicare un agente di trasferimento del messaggio da includere nell'elenco approvali globale:

https://ers.trendmicro.com/

Consultare il seguente articolo della Knowledge Base per esempi dei messaggi da inviare a Trend Micro:

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

Servizi di reputazione file

Raccogliere le informazioni di sistema e inviare il contenuto del file dannoso a Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Annotare il numero di pratica per riferimenti futuri.

Servizi di reputazione Web

Inviare una query sulla classificazione della sicurezza e sul tipo di contenuto di un URL sospettato di phishing o di altri cosiddetti "vettori di infezioni" (fonte intenzionale di minacce Internet quali spyware e minacce informatiche).

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

se la classificazione assegnata è corretta, reinviare una nuova richiesta di classificazione a Trend Micro.

Altre risorse

Oltre alle soluzioni e all'assistenza, online sono disponibili molte altre risorse per rimanere aggiornati, conoscere le innovazioni ed essere informati sulle ultime novità che riguardano la sicurezza.

Centro di download

Periodicamente, Trend Micro rilascia una patch per il problema noto riportato oppure un aggiornamento applicabile ad un servizio o a un prodotto specifico. Per consultare le patch disponibili, accedere a:

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

Se una patch non è stata applicata (ogni patch ha una data) aprire il file Readme e determinare se si tratta di una patch rilevante per l'ambiente di riferimento. Il file Readme contiene inoltre le istruzioni per l'installazione.

Riscontri sulla documentazione

Trend Micro si impegna continuamente a migliorare la propria documentazione. Per domande, commenti o suggerimenti riguardanti questo o qualsiasi documento Trend Micro, visitare il seguente sito:

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

Indice

TREND MICRO INCORPORATED

TREND MICRO Italy S.r.l. Edison Park Center Viale Edison 110 -
Edificio C 20099 Sesto San Giovanni (MI) Italia
Telefono: +39 02 925931 Fax: +39 02 92593401 info@trendmicro.com

www.trendmicro.com

Item Code: WFIM108204/180326