

**SOPHOS**

Security made simple.

# Sophos Enterprise Console

## Guida di avvio avanzata

Per installazioni distribuite

Versione prodotto: 5.4  
Data documento: aprile 2016



# Sommario

1	Informazioni sulla guida.....	4
2	Pianificare l'installazione.....	5
2.1	Pianificare l'installazione di Enterprise Console.....	5
2.2	Pianificazione della protezione dei database.....	7
2.3	Pianificare i gruppi di computer.....	7
2.4	Pianificare i criteri di sicurezza.....	8
2.5	Pianificare la ricerca dei computer in rete.....	8
2.6	Pianificare la protezione dei computer.....	8
3	Requisiti di sistema.....	9
3.1	Hardware e sistema operativo.....	9
3.2	Software di sistema Microsoft.....	9
3.3	Requisiti porte.....	10
4	Account necessari.....	11
4.1	Account del database.....	11
4.2	Account del gestore aggiornamenti.....	11
5	Come stabilire dove installare i componenti di Enterprise Console.....	13
5.1	Database installati su server a parte.....	14
5.2	Il gestore degli aggiornamenti aggiuntivo è installato su un server a parte.....	14
6	Modalità 1: Database installati su server a parte.....	16
6.1	Download del programma di installazione.....	16
6.2	Installazione del database SEC.....	16
6.3	Installazione di SEC: console di gestione, server di gestione, gestore degli aggiornamenti.....	17
6.4	Installazione di una console di gestione SEC aggiuntiva.....	18
6.5	Download del software di sicurezza.....	19
7	Modalità 2: Gestore degli aggiornamenti aggiuntivo installato su un server a parte.....	22
7.1	Download del programma di installazione.....	22
7.2	Installazione di SEC: tutti i componenti.....	23
7.3	Installazione di una console di gestione SEC aggiuntiva.....	23
7.4	Installazione di un gestore degli aggiornamenti aggiuntivo.....	24
7.5	Download del software di sicurezza.....	25
8	Pubblicazione del software di sicurezza in un server web.....	32
9	Creazione di gruppi di computer.....	33
10	Impostazione dei criteri di sicurezza.....	34
10.1	Criteri predefiniti.....	34

10.2	Impostazione di un criterio del firewall.....	34
10.3	Creazione o modifica di un criterio.....	35
10.4	Applicazione di un criterio a un gruppo.....	35
11	Ricerca dei computer.....	36
12	Prepararsi alla protezione dei computer.....	37
12.1	Preparazione alla rimozione di software prodotti da terzi.....	37
12.2	Verifica del possesso di un account utilizzabile per l'installazione di software.....	37
12.3	Preparazione per l'installazione del software antivirus.....	38
13	Protezione dei computer.....	39
13.1	Protezione automatica dei computer Windows.....	39
13.2	Protezione manuale dei computer Windows o Mac.....	40
13.3	Protezione dei computer Linux o UNIX.....	40
14	Verifica dello stato della rete.....	41
15	Protezione dei computer autonomi.....	42
15.1	Invio delle informazioni necessarie ai computer autonomi.....	42
16	Supporto tecnico.....	43
17	Note legali.....	44

# 1 Informazioni sulla guida

Questa guida mostra come installare per la prima volta il software di sicurezza di Sophos in una rete complessa o con più di 1000 workstation. Viene descritta l'installazione su computer Windows e Mac.

**Nota:** Se non incluse nella licenza, alcune funzioni potrebbero non essere disponibili.

Se si esegue l'installazione in una rete semplice con meno di 1000 workstation aventi sistemi operativi Windows e Mac, invece che questa guida consultare la *Guida di avvio rapido di Sophos Enterprise Console*.

Per installazione su computer Linux o UNIX, consultare, oltre a questa guida, la *Guida di avvio per Linux e UNIX di Sophos Enterprise Console 9.7*.

Se si sta eseguendo l'upgrade, consultare invece la *Guida all'upgrade di Sophos Enterprise Console*.

La documentazione relativa a Sophos Enterprise Console è pubblicata su [www.sophos.com/it-it/support/documentation/enterprise-console.aspx](http://www.sophos.com/it-it/support/documentation/enterprise-console.aspx).

## 2 Pianificare l'installazione

Proteggere i computer seguendo questi passaggi chiave:

1. Installare Sophos Enterprise Console.
2. Scaricare il software di sicurezza in un percorso centrale della rete.
3. Pubblicare il software di sicurezza su un server web, se lo si desidera.
4. Creare i gruppi di computer.
5. Impostare criteri di sicurezza per tali gruppi.
6. Ricercare i computer in rete e inserirli nei gruppi.
7. Proteggere i computer.
8. Verificare lo stato della rete.
9. Proteggere tutti i computer autonomi.

**Nota:** Se si è utenti di Active Directory, alcuni dei passaggi possono essere svolti automaticamente.

Questa sezione aiuterà l'utente nelle scelte da compiere a ogni passaggio.

### 2.1 Pianificare l'installazione di Enterprise Console

Sophos Enterprise Console (**SEC**) consente di installare e gestire il software di sicurezza sui propri computer.

Enterprise Console include quattro componenti:

<b>Console di gestione</b>	Consente di proteggere e gestire i computer.
<b>Server di gestione</b>	Gestisce gli aggiornamenti e le comunicazioni.
<b>Database</b>	Memorizza i dati relativi ai computer collegati in rete.
<b>Gestore degli aggiornamenti</b>	Scarica il software Sophos e si aggiorna automaticamente da Sophos in un percorso centrale.

#### Console di gestione

Si può scegliere di installare un'altra istanza della console di gestione su un altro server per poter gestire i computer in rete in modo più conveniente. Ciò influisce sulla modalità in cui si desidera configurare l'amministrazione basata sui ruoli alla console di gestione e su come si desidera suddividere il proprio ambiente IT in sottoambienti:

- *L'amministrazione basata sui ruoli* alla console di gestione concerne l'impostazione dei ruoli, l'aggiunta dei diritti ai ruoli e l'assegnazione di utenti e gruppi Windows. Per esempio, un ingegnere di Help Desk può aggiornare e disinfettare i computer, ma non può configurare i criteri; responsabilità di un amministratore.
- I *sottoambienti* possono essere utilizzati per restringere i computer e i gruppi su cui gli utenti possono operare. È possibile dividere il proprio ambiente IT in sottoambienti a cui assegnare i gruppi di computer della console di gestione. È quindi possibile controllare

l'accesso ai sottoambienti assegnando loro utenti e gruppi Windows. Il sottoambiente predefinito comprende tutti i gruppi della console di gestione e **Nessun gruppo**.

Questa guida descrive come installare una console di gestione aggiuntiva. Per informazioni su come impostare l'amministrazione basata sui ruoli e creare sottoambienti, leggere l'articolo [www.sophos.com/it-it/support/knowledgebase/63556.aspx](http://www.sophos.com/it-it/support/knowledgebase/63556.aspx).

## Database

Se si desidera installare i database su altri computer, perché:

- È necessario più spazio per i database.
- Si è in possesso di un server dedicato SQL Server.
- Si desidera distribuire il carico dei processi su più computer.

Questa guida descrive come installare il database sullo stesso server degli altri componenti di Enterprise, o su un server dei database dedicato separato.

**Nota:** Se si desidera installare i database in un server sicuro utilizzando uno script, oppure in un ambiente cluster di SQL Server, consultare l'articolo [www.sophos.com/it-it/support/knowledgebase/33980.aspx](http://www.sophos.com/it-it/support/knowledgebase/33980.aspx).

**Importante:** Il database di Sophos Auditing, **SophosSecurity**, deve essere presente e funzionare congiuntamente agli altri database di Enterprise Console, anche se non si desidera utilizzare la funzionalità di Sophos Auditing. Ciò è necessario perché il database viene utilizzato per potenziare il controllo degli accessi, oltre che per la registrazione di eventi di controllo.

## Gestore degli aggiornamenti

Un gestore degli aggiornamenti consente di creare condivisioni contenenti il software del computer che si desidera distribuire. I computer che si desidera proteggere si aggiornano da queste condivisioni. Il gestore degli aggiornamenti viene sempre installato come parte di Enterprise Console. Per impostazione predefinita posiziona il software e gli aggiornamenti in una condivisione UNC di SophosUpdate. È possibile installare su altri server gestori degli aggiornamenti aggiuntivi e creare ulteriori condivisioni per poter scaricare e distribuire software su reti più grandi.

Come regola generale, si consiglia di installare un gestore degli aggiornamenti aggiuntivo per ogni 25.000 client presenti nella rete. Si consiglia inoltre di installare un gestore degli aggiornamenti aggiuntivo in un percorso remoto. Ciò consente di risparmiare larghezza di banda durante l'aggiornamento delle condivisioni degli aggiornamenti presenti in tale percorso, oltre che di garantire che le condivisioni siano completamente aggiornate anche nel caso in cui il collegamento non sia disponibile.

Se si utilizza un percorso UNC per l'aggiornamento della condivisione degli aggiornamenti, questa dovrebbe essere utilizzata da un massimo di 1.000 computer, a meno che non si trovi in un server file dedicato. Se si imposta un percorso Web di aggiornamento, sarà possibile effettuare l'aggiornamento di circa 10.000 computer.

## 2.2 Pianificazione della protezione dei database

### Controllo del database

Oltre alla protezione dei database di Enterprise Console, si consiglia un'ulteriore protezione al livello dell'istanza di SQL Server (se non ancora applicata), in modo tale da controllare l'attività degli utenti e le modifiche apportate in SQL Server.

Per esempio, se si esegue l'edizione di Enterprise del server SQL 2008, è possibile utilizzare la funzione di controllo di SQL Server. Le versioni precedenti di SQL Server potranno supportare il controllo accessi, il controllo basato su trigger, oltre che il controllo eventi grazie alla funzionalità di traccia incorporata.

Per ulteriori informazioni sulle funzionalità a disposizione per intraprendere operazioni di controllo, oltre che sulle modifiche al sistema SQL Server, consultare la documentazione relativa alla versione in uso di SQL Server. Per esempio:

- [SQL Server Audit \(Database Engine\)](#)
- [Controllo \(Motore di database\), SQL Server 2008 R2](#)
- [Auditing in SQL Server 2008](#)
- [Controllo \(Motore di database\), SQL Server 2008](#)

### Connessioni di cifratura del database

Si consiglia caldamente la cifratura di tutte le connessioni fra client e database di Enterprise Console. Per ulteriori informazioni, consultare la documentazione relativa a SQL Server.

- [Abilitazione di connessioni cifrate al Motore di database \(Gestione configurazione SQL Server\)](#)
- [Connessioni cifrate a SQL Server 2008 R2](#)
- [Come abilitare la cifratura SSL per un'istanza di SQL Server utilizzando Microsoft Management Console](#)

### Controllo dell'accesso ai backup del database

Verificare che un controllo dell'accesso restrittivo venga applicato in modo adeguato a tutti i backup o copie del database. Ciò consentirà di evitare che utenti non autorizzati accedano a file, li modifichino, o cancellino inavvertitamente.

**Nota:** I link presenti in questa sezione si riferiscono a informazioni aggiornate da terzi e sono stati inclusi come ulteriore riferimento per gli utenti. Nonostante l'impegno costante nel verificare l'accuratezza dei link citati nella documentazione, tali link potrebbero essere modificati a insaputa di Sophos.

## 2.3 Pianificare i gruppi di computer

È necessario decidere come raggruppare i computer che si desidera proteggere. Per consigli, leggere l'articolo [www.sophos.com/it-it/support/knowledgebase/63556.aspx](http://www.sophos.com/it-it/support/knowledgebase/63556.aspx).

## 2.4 Pianificare i criteri di sicurezza

Un *criterio di sicurezza* consiste in un insieme di impostazioni applicabili ai computer di uno o più gruppi.

Durante la creazione dei gruppi, Enterprise Console applica loro criteri predefiniti. È possibile modificare tali criteri o crearne dei nuovi, secondo quanto spiegato in questa guida. Per consigli su quali impostazioni utilizzare, consultare la *Guida all'impostazione dei criteri di Sophos Enterprise Console*.

## 2.5 Pianificare la ricerca dei computer in rete

Prima di poter installare il software di sicurezza sui computer della rete, è necessario aggiungere i computer alla lista presente in Enterprise Console. Per informazioni su come ricercare computer per aggiungerli all'elenco computer, consultare la guida in linea di Enterprise Console.

## 2.6 Pianificare la protezione dei computer

È possibile effettuare l'installazione automatica del software di sicurezza da Enterprise Console su computer Windows.

**Nota:** Non è possibile installare Sophos Client Firewall o sui computer che eseguono sistemi operativi server.

Se in rete sono presenti altri sistemi operativi, è necessario installare il software manualmente, tramite script oppure con un altro metodo (ad es. Active Directory). Questa guida fornisce dati relativi all'installazione manuale per i seguenti sistemi operativi:

- Windows
- Mac OS X

La guida di avvio *per Linux e UNIX* di Sophos Enterprise Console fornisce dati relativi all'installazione manuale per altri sistemi operativi.



## 3 Requisiti di sistema

**Suggerimento:** È possibile eseguire il programma di installazione di Enterprise Console per verificare che il server abbia i requisiti necessari per l'installazione di Enterprise Console, anche se non si desidera eseguire subito l'installazione. Si potranno consultare i risultati della verifica di sistema alla pagina **Verifica della proprietà di sistema** della procedura guidata di installazione. Una volta visionati questi risultati, cliccare su **Cancella** per chiudere la procedura guidata. Se si desiderano ulteriori informazioni sui risultati della verifica di sistema, leggere l'articolo <http://www.sophos.com/it-it/support/knowledgebase/113945.aspx>.

### 3.1 Hardware e sistema operativo

Per i requisiti di hardware e sistema operativo, consultare la pagina corrispondente del sito web di Sophos (<http://www.sophos.com/it-it/products/all-system-requirements.aspx>).

### 3.2 Software di sistema Microsoft

Enterprise Console richiede un software di sistema Microsoft specifico (per es. software di database).

Il programma di installazione di Enterprise Console cerca di installare tale software, se non già a disposizione nel server. Tuttavia, in alcuni casi, il software non è compatibile con il server, oppure deve essere installato manualmente.

**Nota:** dopo l'installazione del software di sistema richiesto potrebbe essere necessario riavviare il computer. Per ulteriori informazioni, leggere l'articolo <https://www.sophos.com/it-it/support/knowledgebase/65190.aspx>.

#### Installazione di SQL Server

Il programma di installazione tenterà di installare SQL Server 2012 Express Edition con Service Pack 2 (SP2), a meno che non si scelga di utilizzare un'istanza esistente di SQL Server 2005 Express o versioni successive. Notare che:

- Si raccomanda di non installare SQL Server 2008 su un controller di dominio.
- Se si desidera installare i database Enterprise Console in un server separato, verificare che sia possibile accedere in remoto all'istanza di SQL Server. Per ulteriori informazioni, leggere l'articolo <https://www.sophos.com/it-it/support/knowledgebase/118473.aspx>.

#### Installazione di .NET Framework

Il programma di installazione cerca di installare .NET Framework 4.5.2, a meno che non sia già stato installato.

**Importante:** Come parte dell'installazione di .NET Framework 4.5.2, alcuni servizi di sistema (quali IIS Admin Service) potrebbero essere riavviati.

Dopo avere installato .NET Framework 4.5.2, si potrebbe ricevere un messaggio in cui si richiede di riavviare il computer. In questo caso, si consiglia di riavviare il computer immediatamente o poco dopo l'installazione.

## Installazione di Microsoft Message Queuing

Il programma di installazione cerca di installare l'accodamento messaggi Microsoft (MSMQ), a meno che non sia già stato installato.

**Importante:** Durante l'installazione di MSMQ, verranno bloccati i seguenti servizi: MSDTC, MSSQLServer, SQLSERVERAGENT. Ciò blocca l'accesso al database di SQL Server. Accertarsi che questi servizi possano essere bloccati durante l'installazione e che siano riavviati una volta completata.

### 3.3 Requisiti porte

Per poter aprire Enterprise Console sono richieste determinate porte. Per ulteriori informazioni, leggere l'articolo [www.sophos.com/it-it/support/knowledgebase/38385.aspx](http://www.sophos.com/it-it/support/knowledgebase/38385.aspx).

## 4 Account necessari

Prima di installare il software di Sophos, creare gli account utente necessari:

- **Account del database:** è un account utente di Windows che consente al servizio di gestione di Enterprise Console di connettersi al database. Può essere utilizzato anche da altri servizi Sophos.

Attribuire il nome **SophosManagement** all'account del database.

- **Account del gestore aggiornamenti:** è un account utente di Windows che consente al computer endpoint di accedere alle cartelle in cui Enterprise Console colloca gli aggiornamenti per il software.

Attribuire il nome **SophosUpdateMgr** all'account di Update Manager.

### 4.1 Account del database

L'account del database deve:

- Poter accedere al computer dove verrà installato il Sophos Management Server (un componente di Enterprise Console).
- Poter leggere e scrivere nella directory di sistema temporanea, per esempio "windows\temp". Per impostazione predefinita, i membri del gruppo "Utenti" possono farlo.
- Avere un UPN (nome dell'entità utente) associato all'account, se si tratta di account di dominio.

Tutti gli altri diritti e le ulteriori appartenenze a gruppi necessari all'account vengono forniti automaticamente durante l'installazione.

Sophos consiglia che l'account:

- Non abbia nessuna data di scadenza o alcun'altra restrizione di accesso.
- Non sia un account d'amministrazione.
- Non venga cambiato dopo l'installazione.
- Abbia il nome **SophosManagement**.

Per consigli e istruzioni dettagliate, leggere l'articolo <https://www.sophos.com/it-it/support/knowledgebase/113954.aspx>.

### 4.2 Account del gestore aggiornamenti

L'account del gestore aggiornamenti dovrebbe avere accesso in lettura alla cartella in cui Enterprise Console colloca gli aggiornamenti per il software. Per impostazione predefinita, è: \\[nomeserver]\SophosUpdate

Sophos consiglia che l'account:

- Non abbia nessuna data di scadenza o alcun'altra restrizione di accesso.
- Non sia un account d'amministrazione.

- Abbia un UPN (nome dell'entità utente) associato all'account, se si tratta di account di dominio.
- Abbia il nome **SophosUpdateMgr**.

Per consigli e istruzioni dettagliate, leggere l'articolo  
<https://www.sophos.com/it-it/support/knowledgebase/113954.aspx>.

## 5 Come stabilire dove installare i componenti di Enterprise Console

Sophos Enterprise Console (SEC) include 4 componenti:

<b>Console di gestione</b>	Consente di proteggere e gestire i computer.
<b>Server di gestione</b>	Gestisce gli aggiornamenti e le comunicazioni.
<b>Database</b>	Memorizza i dati relativi ai computer collegati in rete.
<b>Gestore degli aggiornamenti</b>	Scarica il software Sophos e si aggiorna automaticamente da Sophos in un percorso centrale.

Se si installano i componenti SEC su server diversi, è consigliato unire tali server sotto lo stesso dominio.

Si raccomanda di non installare i database di SEC in un controller di dominio.

Questa guida descrive due modalità di installazione:

- Database installati su server a parte
- Gestore degli aggiornamenti aggiuntivo installato su un server a parte

In ogni modalità, i componenti di SEC vengono distribuiti nella rete in modo differente.

## 5.1 Database installati su server a parte

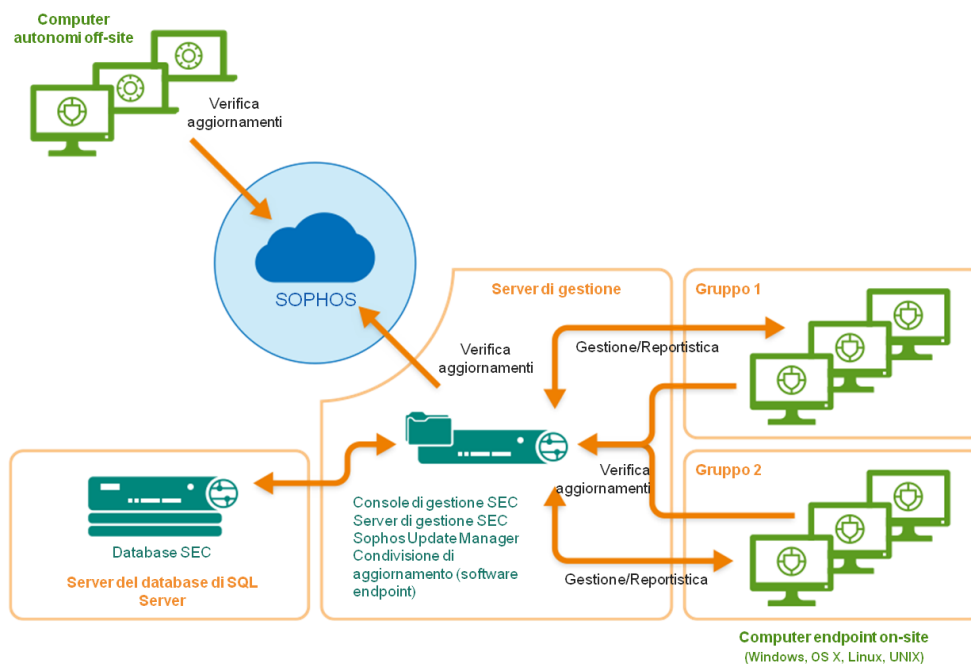


Figura 1: Esempio di modalità di installazione: Database installati su server a parte

Per utilizzare questa modalità di installazione, andare alla sezione [Modalità 1: Database installati su server a parte](#) a pagina 16.

## 5.2 Il gestore degli aggiornamenti aggiuntivo è installato su un server a parte

In questa modalità di installazione sono descritti due metodi per configurare le fonti da cui i gestori traggono gli aggiornamenti.

Il primo metodo consiste nel:

- Configurare il gestore degli aggiornamenti principale, installato insieme alla console di gestione SEC, perché si aggiorni direttamente da Sophos.
- Configurare il gestore degli aggiornamenti aggiuntivo per eseguire gli aggiornamenti dal gestore degli aggiornamenti principale.

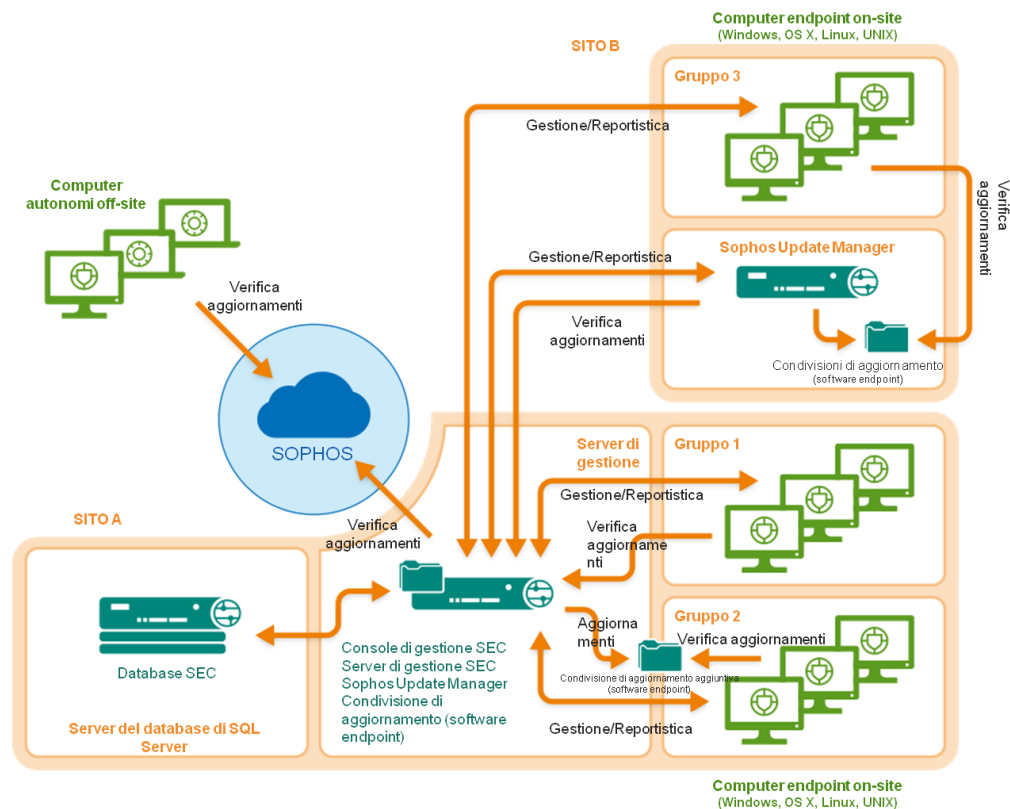


Figura 2: Esempio di modalità di installazione: Gestore degli aggiornamenti aggiuntivo che esegue gli aggiornamenti dal gestore degli aggiornamenti principale

Il secondo metodo consiste nel:

- Configurare il gestore degli aggiornamenti aggiuntivo in modo tale che possa eseguire gli aggiornamenti direttamente da Sophos.
- Configurare il gestore degli aggiornamenti, installato insieme alla console di gestione SEC, perché si aggiorni direttamente dal gestore degli aggiornamenti aggiuntivo.

A prescindere dal metodo selezionato, per utilizzare questa modalità di installazione andare alla sezione [Modalità 2: Gestore degli aggiornamenti aggiuntivo installato su un server a parte](#) a pagina 22.

## 6 Modalità 1: Database installati su server a parte

### 6.1 Download del programma di installazione

**Nota:** i programmi di installazione possono essere scaricati da qualsiasi computer, e copiati sui computer in cui si desidera utilizzarli.

1. Accedere a <https://www.sophos.com/it-it/support/downloads.aspx> utilizzando il proprio Sophos ID.

**Nota:** Se desiderate assistenza per il vostro Sophos ID, vi invitiamo a consultare l'[articolo 111195 della knowledgebase Sophos](#).

2. Se si è già effettuato l'accesso per i download in passato, verrà visualizzata la pagina **Download e aggiornamenti del prodotto**.

**Nota:** Se è la prima volta che si effettua l'accesso, verrà visualizzato il proprio profilo. Cliccare su **Endpoint Protection e Server Protection**, e successivamente su **Download e aggiornamenti**.

3. Sotto **Console**, cliccare sul link a **Sophos Enterprise Console** e scaricare il programma di installazione.

### 6.2 Installazione del database SEC

**Nota:** Se si desidera installare i database in un server sicuro utilizzando uno script, oppure in un ambiente cluster di SQL Server, consultare l'articolo [www.sophos.com/it-it/support/knowledgebase/33980.aspx](http://www.sophos.com/it-it/support/knowledgebase/33980.aspx).

Se il Controllo dell'account utente (UAC) (in Windows Server 2008 o successivi) è attivo, disattivarlo e riavviare il server. Dopo avere installato i database, è possibile riattivare l'UAC.

Accedere come amministratore.

- Se il server si trova in un dominio, utilizzare l'account di dominio che abbia diritti di amministratore locale.
  - Se il server si trova in un gruppo di lavoro, utilizzare l'account locale che abbia diritti di amministratore locale.
1. Trovare il programma di installazione di Enterprise Console scaricato in precedenza e cliccarvi due volte.
  2. Estrarre i file d'installazione e salvarli nella cartella di destinazione suggerita, o in un'altra a scelta. La cartella deve essere situata su questo server.  
Una procedura guidata di installazione accompagna durante l'installazione. Accettare le opzioni predefinite, eccezion fatta per quanto elencato di seguito.
    - a) Nella pagina **Selezione componenti**, assicurarsi che l'opzione **Database** sia selezionata e quelle **Console di gestione** e **Server di gestione** non lo siano.
    - b) Nella pagina **Dettagli database**, inserire i dati di un account che sia in grado di effettuare l'accesso sia all'attuale server, sia a quello su cui si desidera installare il server di



gestione di Enterprise Console. Se i server si trovano in un *dominio*, è possibile utilizzare un account di dominio. Se i server sono situati in un *gruppo di lavoro*, utilizzare un account locale che sia attivo su entrambi i server. Non deve trattarsi di un account amministratore.

**Nota:** L'account del database è stato creato in [Account Database](#) a pagina 11.

Una volta terminata la procedura guidata per Enterprise Console, riavviare il server se ciò viene richiesto.

Se si è disattivato il Controllo account utente, è ora possibile riattivarlo.

## 6.3 Installazione di SEC: console di gestione, server di gestione, gestore degli aggiornamenti

Andare al server in cui installare la console di gestione, il server di gestione e il gestore aggiornamenti di Enterprise Console. Assicurarsi che sia connesso a internet.

Il nome host di questo server deve essere diverso da quello degli altri server su cui si desidera installare un gestore degli aggiornamenti.

Se il Controllo dell'account utente (UAC) (in Windows Server 2008 o successivi) è attivo, disattivarlo e riavviare il server. È possibile riattivarlo dopo aver installato Enterprise Console e aver sottoscritto gli aggiornamenti Sophos.

Accedere come amministratore.

- Se il server si trova in un dominio, utilizzare l'account di dominio che abbia diritti di amministratore locale.
  - Se il server si trova in un gruppo di lavoro, utilizzare l'account locale che abbia diritti di amministratore locale.
1. Trovare il programma di installazione di Enterprise Console scaricato in precedenza e cliccarvi due volte.
  2. Estrarre i file d'installazione e salvarli nella cartella di destinazione suggerita, o in un'altra a scelta. La cartella deve essere situata su questo server.

Una procedura guidata di installazione accompagna durante l'installazione. Accettare le opzioni predefinite, eccezion fatta per quanto elencato di seguito.

- a) Nella pagina **Selezione componenti**, assicurarsi che le opzioni **Console di gestione** e **Server di gestione** siano selezionate e che quella **Database** non lo sia.
- b) Nella pagina **Dettagli database**, inserire il percorso e il nome del database di Enterprise Console creati nell'altro server. Inserire i dati di un account che sia in grado di effettuare l'accesso sia all'attuale server, sia a quello su cui è stato installato il database di Enterprise Console. Se i server si trovano in un *dominio*, è possibile utilizzare un account di dominio. Se i server sono situati in un *gruppo di lavoro*, utilizzare un account locale che sia attivo su entrambi i server. Non deve trattarsi di un account amministratore.

**Nota:** L'account del database è stato creato in [Account Database](#) a pagina 11.

Terminata l'installazione, chiudere la sessione o riavviare il server (l'ultima pagina della procedura guidata indica quale opzione scegliere). Quando si accede di nuovo, Enterprise Console si apre automaticamente e viene eseguita la procedura guidata di download del software di sicurezza. Chiuderla ed eseguirla quando verrà indicato in questa guida.

## 6.4 Installazione di una console di gestione SEC aggiuntiva

Si può scegliere di installare un'altra istanza della console di gestione Sophos Enterprise Console su un altro computer per poter gestire i computer in rete in modo più conveniente. Se non si desidera eseguire questa installazione, saltare questa sezione.

**Importante:** Occorre installare la stessa versione di Enterprise Console eseguita nel server di gestione.

**Nota:** La nuova console dovrà poter accedere al server in cui è installato il server di gestione di Enterprise Console. Se tale server esegue un firewall, potrebbe essere necessario configurare il firewall perché sia possibile l'accesso. Per istruzioni su come aggiungere una regola firewall per autorizzare il traffico DCOM dalla console remota al server di gestione, consultare l'[articolo 49028 della knowledge base](#).

Per installare una console di gestione aggiuntiva:

Se il Controllo dell'account utente (UAC) (in Windows Server 2008 o successivi e Windows Vista o successivi) è attivo, disattivarlo e riavviare il computer. Dopo avere installato la console di gestione, è possibile riattivare l'UAC.

Accedere come amministratore.

- Se il computer si trova in un dominio, utilizzare l'account di dominio che abbia diritti di amministratore locale.
  - Se il computer si trova in un gruppo di lavoro, utilizzare l'account locale che abbia diritti di amministratore locale.
1. Trovare il programma di installazione di Enterprise Console scaricato in precedenza e cliccarvi due volte.
  2. Estrarre i file d'installazione e salvarli nella cartella di destinazione suggerita, o in un'altra a scelta. La cartella deve essere situata su questo computer.

Una procedura guidata di installazione accompagna durante l'installazione. Accettare le opzioni predefinite, eccezion fatta per quanto elencato di seguito.

- a) Nella pagina **Installazione personalizzata**, assicurarsi che l'opzione **Console di gestione** sia selezionata e che le opzioni **Server di gestione** e **Database** non lo siano.
- b) Nella pagina **Server di gestione**, inserire il nome del server in cui si desidera installare il server di gestione Enterprise Console.

**Nota:** Se si cambia porta durante l'installazione del server di gestione, accertarsi di indicare la medesima porta in questa pagina.

- c) Se ci si trova in un ambiente di dominio, inserire l'account dell'utente che è stato utilizzato per accedere ai database di Enterprise Console.

L'account a cui ci si riferisce è quello inserito al momento dell'installazione dei database di Enterprise Console. È il medesimo utilizzato dal servizio Sophos Management Host nel server in cui si è installato il server di gestione di Enterprise Console.

Quando la procedura d'installazione guidata è completa, chiudere la sessione o riavviare il computer (l'ultima pagina della procedura guidata indica quale opzione scegliere). Quando si accede di nuovo, Enterprise Console si apre automaticamente. Se si avvia la **Procedura guidata per il download del software di sicurezza**, chiuderla.

Se si è disattivato il "Controllo dell'account utente" prima di eseguire l'installazione, è possibile riattivarlo.

Per permettere ad altri utenti di utilizzare la console di gestione aggiuntiva:

- Aggiungere tali utenti ai gruppi "**Sophos Console Administrators**" e "**Distributed COM Users**" sul server su cui è stato installato il server di gestione.
- Assegnare a tali utenti almeno un ruolo ed un sottoambiente Enterprise Console.

## 6.5 Download del software di sicurezza

Per eseguire il download del software di sicurezza in un percorso centrale, pronto per la distribuzione alle workstation, è necessario configurare il gestore degli aggiornamenti installato. È possibile utilizzare uno dei due seguenti metodi.

[Configurazione automatica del gestore aggiornamenti](#) a pagina 19 spiega come eseguire la procedura guidata che consente l'esecuzione del download di:

- Il software di sicurezza per tutte le piattaforme supportate.
- Solo la versione al momento supportata.
- Solo le sottocartelle della condivisione `\\nome_server\SophosUpdate`, in cui *nome\_server* è il nome del server in cui è installato il gestore degli aggiornamenti.

[Configurazione manuale del gestore aggiornamenti](#) a pagina 20 spiega come configurare direttamente il gestore degli aggiornamenti per abilitare l'esecuzione del download di:

- Software di sicurezza per tutte le piattaforme supportate.
- Versioni in anteprima o precedenti.
- Ad altre condivisioni, probabilmente su altri server.

### 6.5.1 Configurazione automatica del gestore aggiornamenti

1. In Enterprise Console, nel menu **Azioni**, cliccare su **Esegui la Procedura guidata di download del software di sicurezza**.
2. Nella pagina **Dati dell'account di download Sophos**, inserire il nome utente e la password stampati nell'allegato alla licenza. Se si accede a Internet tramite server proxy, selezionare la casella di spunta **Accedi a Sophos tramite server proxy**.
3. Nella pagina **Selezione piattaforma**, selezionare la piattaforma che si desidera proteggere. Quando si clicca su **Avanti**, Enterprise Console comincia a scaricare il software.
4. Nella pagina **Download del software**, viene visualizzato l'avanzamento del download. Cliccare su **Avanti** in qualsiasi momento.
5. Nella pagina **Importa computer da Active Directory**, selezionare la casella di spunta **Imposta gruppi per i computer**, se si desidera che Enterprise Console utilizzi i gruppi esistenti di Active Directory.

**Nota:** se uno stesso computer è stato aggiunto a più di un albero di Active Directory, ciò può generare problemi quali il continuo scambio di messaggi fra il computer e Enterprise Console.

Il software selezionato viene scaricato nella condivisione `\\nome_server\SophosUpdate`, in cui il *nome\_server* è il nome del server nel quale è installato il gestore aggiornamenti.

Se si è disattivato il Controllo account utente prima di eseguire l'installazione di Enterprise Console, è ora possibile riattivarlo.

Se necessario, è ora possibile configurare il gestore aggiornamenti manualmente. Andare alla sezione [Pubblicare il software di sicurezza su un server web, se lo si desidera](#) a pagina 32.

## 6.5.2 Configurazione manuale del gestore aggiornamenti

Se si è disattivato il Controllo account utente prima di eseguire l'installazione di Enterprise Console, è ora possibile riattivarlo.

1. In Enterprise Console, dal menu **Visualizza**, cliccare su **Update Managers**.
2. Se il gestore aggiornamenti *non* è stato configurato automaticamente, configurarlo in modo tale che utilizzi Sophos come fonte degli aggiornamenti:
  - a) Nel riquadro **Update manager**, selezionare il gestore aggiornamenti installato nel server. Cliccarvi col tasto destro del mouse e poi cliccare su **Visualizza/Modifica configurazione**.
  - b) Nella finestra di dialogo **Configura il gestore aggiornamenti**, nella scheda **Fonti**, cliccare su **Aggiungi**.
  - c) Nella finestra di dialogo **Dettagli fonte**, nella casella **Indirizzo**, selezionare **Sophos**. Nelle caselle **Nome utente** e **Password**, digitare le credenziali di download fornite da Sophos.
  - d) Se si accede alla fonte degli aggiornamenti tramite server proxy, selezionare la casella di spunta **Utilizza server proxy per la connessione**. Inserire l'**Indirizzo** e il numero di **Porta** del server proxy. Nelle caselle **Nome utente** e **Password**, digitare le credenziali che consentono l'accesso al server proxy. se il nome utente deve riportare il dominio, utilizzare la forma dominio\nome utente.
  - e) Cliccare su **OK** per chiudere la finestra di dialogo **Dettagli fonte**.  
**Sophos** è elencato nella scheda **Fonti**, nella finestra di dialogo **Configura il gestore aggiornamenti**.
  - f) Cliccare su **OK** per chiudere la finestra di dialogo **Configura il gestore aggiornamenti**.
3. Sottoscrivere il software che si desidera scaricare:
  - a) Riquadro **Sottoscrizioni software**:
    - Per cambiare una sottoscrizione esistente, cliccarvi due volte.
    - Per aggiungere una nuova sottoscrizione, cliccare su **Aggiungi** nella parte alta del riquadro.
  - b) Nella finestra di dialogo **Sottoscrizione al software**, se si sta aggiungendo una nuova sottoscrizione, digitare un nome per tale criterio nella casella **Nome sottoscrizione**.
  - c) Nell'elenco delle piattaforme, spuntare la casella accanto al software desiderato, e, nella finestra relativa alla versione, selezionare la versione richiesta.  
Solitamente si sottoscrivono le versioni **Consigliate**, in modo tale da garantire l'aggiornamento automatico del software. Per informazioni su quali altri tipi di versione sono disponibili, consultare la guida in linea di Enterprise Console, reperibile nella sezione relativa alla configurazione delle sottoscrizioni al software.
  - d) Cliccare su **OK** per chiudere la finestra di dialogo **Sottoscrizione software**.
  - e) Ripetere questi passaggi per tutte le sottoscrizioni che si desidera modificare o aggiungere.

4. Configurare il gestore aggiornamenti per l'utilizzo di queste sottoscrizioni:
  - a) Nel riquadro **Update manager**, selezionare il gestore aggiornamenti installato nel server. Cliccarvi col tasto destro del mouse e poi cliccare su **Visualizza/Modifica configurazione**.
  - b) Nella finestra di dialogo **Configura il gestore aggiornamenti**, nella scheda **Sottoscrizioni**, assicurarsi che le sottoscrizioni siano incluse nell'elenco **Sottoscritto a**. Se non lo sono, selezionare le sottoscrizioni dall'elenco **Disponibili** e cliccare sul pulsante **>** per spostarle nell'elenco **Sottoscritto a**.
5. Se si desidera effettuare il download su altre condivisioni, diverse da `\\nomeserver\SophosUpdate:`
  - a) Cliccare sulla scheda **Distribuzione**.
  - b) Assicurarsi che la sottoscrizione che si desidera utilizzare sia selezionata dall'elenco nella parte alta della scheda.
  - c) Cliccare su **Aggiungi**.
  - d) Nella finestra di dialogo **Cerca una cartella**, andare a una delle condivisioni. Cliccare su **OK**.
  - e) Selezionare la condivisione dall'elenco **Disponibile** e cliccare sul pulsante **>** per spostarla nell'elenco **Aggiorna a**.
  - f) Per inserire una descrizione per la condivisione, o credenziali per la scrittura, selezionare la condivisione e cliccare su **Configura**. Nella finestra di dialogo **Gestione condivisione**, inserire la descrizione e le credenziali.
  - g) Ripetere questi passaggi per tutte le condivisioni.
6. Cliccare su **OK** per chiudere la finestra di dialogo **Configura il gestore aggiornamenti**.  
Il software selezionato viene scaricato nelle condivisioni specificate.

L'installazione dei tool di gestione è terminata. Andare alla sezione [Pubblicare il software di sicurezza su un server web, se lo si desidera](#) a pagina 32.

## 7 Modalità 2: Gestore degli aggiornamenti aggiuntivo installato su un server a parte

In questa modalità di installazione sono descritti due metodi per configurare le fonti da cui i gestori traggono gli aggiornamenti.

Il primo metodo consiste nel:

- Configurare il gestore degli aggiornamenti principale, installato insieme alla console di gestione, perché si aggiorni direttamente da Sophos.
- Configurare il gestore degli aggiornamenti aggiuntivo per eseguire gli aggiornamenti dal gestore degli aggiornamenti principale.

Il secondo metodo consiste nel:

- Configurare il gestore degli aggiornamenti aggiuntivo in modo tale che possa eseguire gli aggiornamenti direttamente da Sophos.
- Configurare il gestore degli aggiornamenti, installato insieme alla console di gestione, perché si aggiorni direttamente dal gestore degli aggiornamenti aggiuntivo.

Il secondo metodo può essere utilizzato se non si desidera collegare il server principale di Enterprise Console a Internet.

Il metodo prescelto ha le seguenti ripercussioni:

- Incide sulla scelta del server da connettere a Internet. Nelle successive sezioni di installazione, verrà comunicato se il server su cui si esegue l'installazione richiede connessione a Internet.
- Condiziona il metodo scelto per eseguire il download del software di sicurezza in un percorso centrale, pronto per la distribuzione alle workstation. Scegliere la sezione adeguata quando si giunge a questo punto.
- Se si può, utilizzare la funzione di verifica patch in Enterprise Console. Per utilizzare questa funzione, è necessario eseguire il primo metodo descritto.

### 7.1 Download del programma di installazione

**Nota:** i programmi di installazione possono essere scaricati da qualsiasi computer, e copiati sui computer in cui si desidera utilizzarli.

1. Accedere a <https://www.sophos.com/it-it/support/downloads.aspx> utilizzando il proprio Sophos ID.

**Nota:** Se desiderate assistenza per il vostro Sophos ID, vi invitiamo a consultare l'[articolo 111195 della knowledgebase Sophos](#).

2. Se si è già effettuato l'accesso per i download in passato, verrà visualizzata la pagina **Download e aggiornamenti del prodotto**.

**Nota:** Se è la prima volta che si effettua l'accesso, verrà visualizzato il proprio profilo. Cliccare su **Endpoint Protection e Server Protection**, e successivamente su **Download e aggiornamenti**.

3. Sotto **Console**, cliccare sul link a **Sophos Enterprise Console** e scaricare il programma di installazione.

## 7.2 Installazione di SEC: tutti i componenti

Andare al server su cui si desidera installare i componenti di Enterprise Console. Se si desidera che il gestore aggiornamenti che verrà installato sul server si aggiorni direttamente da Sophos, assicurarsi che tale server sia connesso a internet.

Il nome host di questo server deve essere diverso da quello degli altri server su cui si desidera installare un gestore degli aggiornamenti.

Se il Controllo dell'account utente (UAC) (in Windows Server 2008 o successivi) è attivo, disattivarlo e riavviare il server. È possibile riattivarlo dopo aver installato Enterprise Console e aver sottoscritto gli aggiornamenti Sophos.

Accedere come amministratore.

- Se il server si trova in un dominio, utilizzare l'account di dominio che abbia diritti di amministratore locale.
  - Se il server si trova in un gruppo di lavoro, utilizzare l'account locale che abbia diritti di amministratore locale.
1. Trovare il programma di installazione di Enterprise Console scaricato in precedenza e cliccarvi due volte.
  2. Estrarre i file d'installazione e salvarli nella cartella di destinazione suggerita, o in un'altra a scelta. La cartella deve essere situata su questo server.

Una procedura guidata di installazione accompagna durante l'installazione. Accettare le opzioni predefinite, eccezion fatta per quanto elencato di seguito.

- a) Nella pagina **Selezione componenti**, assicurarsi che *tutti* i componenti siano selezionati.
- b) Nella pagina **Dettagli database**, inserire i dettagli di un account che possa accedere a questo server. Se il server si trova in un *dominio*, è possibile utilizzare un account di dominio. Se il server si trova in un *gruppo di lavoro*, utilizzare un account locale che sia attivo nel server. Non deve trattarsi di un account amministratore.

**Nota:** L'account del database è stato creato in [Account Database](#) a pagina 11.

Terminata l'installazione, chiudere la sessione o riavviare il server (l'ultima pagina della procedura guidata indica quale opzione scegliere). Quando si accede di nuovo, Enterprise Console si apre automaticamente e viene eseguita la procedura guidata di download del software di sicurezza. Chiuderla ed eseguirla quando verrà indicato in questa guida.

## 7.3 Installazione di una console di gestione SEC aggiuntiva

Si può scegliere di installare un'altra istanza della console di gestione Sophos Enterprise Console su un altro computer per poter gestire i computer in rete in modo più conveniente. Se non si desidera eseguire questa installazione, saltare questa sezione.

**Importante:** Occorre installare la stessa versione di Enterprise Console eseguita nel server di gestione.

**Nota:** La nuova console dovrà poter accedere al server in cui è installato il server di gestione di Enterprise Console. Se tale server esegue un firewall, potrebbe essere necessario configurare il firewall perché sia possibile l'accesso. Per istruzioni su come aggiungere una



regola firewall per autorizzare il traffico DCOM dalla console remota al server di gestione, consultare l'[articolo 49028 della knowledge base](#).

Per installare una console di gestione aggiuntiva:

Se il Controllo dell'account utente (UAC) (in Windows Server 2008 o successivi e Windows Vista o successivi) è attivo, disattivarlo e riavviare il computer. Dopo avere installato la console di gestione, è possibile riattivare l'UAC.

Accedere come amministratore.

- Se il computer si trova in un dominio, utilizzare l'account di dominio che abbia diritti di amministratore locale.
- Se il computer si trova in un gruppo di lavoro, utilizzare l'account locale che abbia diritti di amministratore locale.

1. Trovare il programma di installazione di Enterprise Console scaricato in precedenza e cliccarvi due volte.
2. Estrarre i file d'installazione e salvarli nella cartella di destinazione suggerita, o in un'altra a scelta. La cartella deve essere situata su questo computer.

Una procedura guidata di installazione accompagna durante l'installazione. Accettare le opzioni predefinite, eccezion fatta per quanto elencato di seguito.

- a) Nella pagina **Installazione personalizzata**, assicurarsi che l'opzione **Console di gestione** sia selezionata e che le opzioni **Server di gestione** e **Database** non lo siano.
- b) Nella pagina **Server di gestione**, inserire il nome del server in cui si desidera installare il server di gestione Enterprise Console.

**Nota:** Se si cambia porta durante l'installazione del server di gestione, accertarsi di indicare la medesima porta in questa pagina.

- c) Se ci si trova in un ambiente di dominio, inserire l'account dell'utente che è stato utilizzato per accedere ai database di Enterprise Console.

L'account a cui ci si riferisce è quello inserito al momento dell'installazione dei database di Enterprise Console. È il medesimo utilizzato dal servizio Sophos Management Host nel server in cui si è installato il server di gestione di Enterprise Console.

Quando la procedura d'installazione guidata è completa, chiudere la sessione o riavviare il computer (l'ultima pagina della procedura guidata indica quale opzione scegliere). Quando si accede di nuovo, Enterprise Console si apre automaticamente. Se si avvia la **Procedura guidata per il download del software di sicurezza**, chiuderla.

Se si è disattivato il "Controllo dell'account utente" prima di eseguire l'installazione, è possibile riattivarlo.

Per permettere ad altri utenti di utilizzare la console di gestione aggiuntiva:

- Aggiungere tali utenti ai gruppi "**Sophos Console Administrators**" e "**Distributed COM Users**" sul server su cui è stato installato il server di gestione.
- Assegnare a tali utenti almeno un ruolo ed un sottoambiente Enterprise Console.

## 7.4 Installazione di un gestore degli aggiornamenti aggiuntivo

**Importante:** Se si desidera installare una console di gestione di SEC aggiuntiva nel server in cui si vuole installare un ulteriore gestore degli aggiornamenti, è necessario installare la



console aggiuntiva per prima, secondo quanto spiegato nella sezione [Installazione di una console di gestione SEC aggiuntiva](#) a pagina 23.

Andare al server su cui si desidera installare un gestore degli aggiornamenti aggiuntivo. Se si desidera che il gestore aggiornamenti che verrà installato sul server si aggiorni direttamente da Sophos, assicurarsi che tale server sia connesso a internet.

Il nome host di questo server deve essere diverso da quello degli altri server su cui si desidera installare un gestore degli aggiornamenti.

Se "Individuazione rete" (in Windows Server 2008 o successivi) è disattivata, attivarla e riavviare il server.

Se il Controllo dell'account utente (UAC) (in Windows Server 2008 o successivi) è attivo, disattivarlo e riavviare il server. Potrà essere riattivato una volta installato il gestore degli aggiornamenti e sottoscritto gli aggiornamenti Sophos.

Accedere come amministratore.

- Se il server si trova in un dominio, utilizzare l'account di dominio che abbia diritti di amministratore locale.
  - Se il server si trova in un gruppo di lavoro, utilizzare l'account locale che abbia diritti di amministratore locale.
1. Trovare la cartella condivisa `SUMInstallSet`, nel server in cui è stata installata Enterprise Console.
  2. Cliccare due volte su `Setup.exe` per eseguire il programma di installazione.  
Una procedura guidata di installazione accompagna durante l'installazione. Accettare le opzioni predefinite.

È stato installato un gestore aggiornamenti gestito da Enterprise Console.

## 7.5 Download del software di sicurezza

In questa modalità di installazione sono descritti due metodi per configurare le fonti da cui i gestori traggono gli aggiornamenti. Scegliere quello più appropriato:

- [Esecuzione degli aggiornamenti da Sophos da parte del gestore degli aggiornamenti principale](#) a pagina 25
- [Esecuzione degli aggiornamenti da Sophos da parte del gestore aggiornamenti aggiuntivo](#) a pagina 29

### 7.5.1 Esecuzione degli aggiornamenti da Sophos da parte del gestore degli aggiornamenti principale

Configurazione del gestore degli aggiornamenti principale perché si aggiorni da Sophos

È necessario configurare il gestore degli aggiornamenti principale, installato insieme alla console di gestione SEC, perché si aggiorni direttamente da Sophos. È possibile utilizzare uno dei due seguenti metodi.

[Configurazione automatica del gestore aggiornamenti principale](#) a pagina 26 spiega come eseguire la procedura guidata che consente l'esecuzione del download di:

- Il software di sicurezza per tutte le piattaforme supportate.

- Solo la versione più recente.
- Solo le sottocartelle della condivisione `\\nome_server\SophosUpdate`, in cui *nome\_server* è il nome del server su cui è installato il gestore degli aggiornamenti principale.

[Configurazione manuale del gestore aggiornamenti principale](#) a pagina 26 spiega come configurare direttamente il gestore degli aggiornamenti per abilitare l'esecuzione del download:

- Il software di sicurezza per tutte le piattaforme supportate.
- Di versioni precedenti.
- Ad altre condivisioni, probabilmente su altri server.

Per informazioni su quali altri tipi di versione sono disponibili, consultare la guida in linea di Enterprise Console, reperibile nella sezione relativa alle sottoscrizioni.

## Configurazione del gestore degli aggiornamenti aggiuntivo per eseguire gli aggiornamenti dal gestore degli aggiornamenti principale

[Configurazione del gestore degli aggiornamenti aggiuntivo](#) a pagina 28 spiega come configurare il gestore aggiornamenti addizionale in modo tale che possa eseguire gli aggiornamenti direttamente dal gestore degli aggiornamenti principale.

### 7.5.1.1 Configurazione automatica del gestore aggiornamenti principale

1. In Enterprise Console, nel menu **Azioni**, cliccare su **Esegui la Procedura guidata di download del software di sicurezza**.
2. Nella pagina **Dati dell'account di download Sophos**, inserire il nome utente e la password stampati nell'allegato alla licenza. Se si accede a Internet tramite server proxy, selezionare la casella di spunta **Accedi a Sophos tramite server proxy**.
3. Nella pagina **Selezione piattaforma**, selezionare la piattaforma che si desidera proteggere. Quando si clicca su **Avanti**, Enterprise Console comincia a scaricare il software.
4. Nella pagina **Download del software**, viene visualizzato l'avanzamento del download. Cliccare su **Avanti** in qualsiasi momento.
5. Nella pagina **Importa computer da Active Directory**, selezionare la casella di spunta **Imposta gruppi per i computer**, se si desidera che Enterprise Console utilizzi i gruppi esistenti di Active Directory.

**Nota:** se uno stesso computer è stato aggiunto a più di un albero di Active Directory, ciò può generare problemi quali il continuo scambio di messaggi fra il computer e Enterprise Console.

Il software selezionato viene scaricato nella condivisione `\\nome_server\SophosUpdate`, in cui il *nome\_server* è il nome del server nel quale è installato il gestore aggiornamenti.

Se si è disattivato il Controllo account utente prima di eseguire l'installazione di Enterprise Console, è ora possibile riattivarlo.

Se necessario, è ora possibile configurare il gestore aggiornamenti manualmente. Quindi andare alla sezione [Configurazione del gestore degli aggiornamenti aggiuntivo](#) a pagina 28.

### 7.5.1.2 Configurazione manuale del gestore aggiornamenti principale

Se si è disattivato il Controllo account utente prima di eseguire l'installazione di Enterprise Console, è ora possibile riattivarlo.

1. In Enterprise Console, dal menu **Visualizza**, cliccare su **Update Managers**.

2. Se il gestore aggiornamenti *non* è stato configurato automaticamente, configurarlo in modo tale che utilizzi Sophos come fonte degli aggiornamenti:
  - a) Nel riquadro **Update manager**, selezionare il gestore aggiornamenti installato nel server. Cliccarvi col tasto destro del mouse e poi cliccare su **Visualizza/Modifica configurazione**.
  - b) Nella finestra di dialogo **Configura il gestore aggiornamenti**, nella scheda **Fonti**, cliccare su **Aggiungi**.
  - c) Nella finestra di dialogo **Dettagli fonte**, nella casella **Indirizzo**, selezionare **Sophos**. Nelle caselle **Nome utente** e **Password**, digitare le credenziali di download fornite da Sophos.
  - d) Se si accede alla fonte degli aggiornamenti tramite server proxy, selezionare la casella di spunta **Utilizza server proxy per la connessione**. Inserire l'**Indirizzo** e il numero di **Porta** del server proxy. Nelle caselle **Nome utente** e **Password**, digitare le credenziali che consentono l'accesso al server proxy. se il nome utente deve riportare il dominio, utilizzare la forma dominio\nome utente.
  - e) Cliccare su **OK** per chiudere la finestra di dialogo **Dettagli fonte**.  
**Sophos** è elencato nella scheda **Fonti**, nella finestra di dialogo **Configura il gestore aggiornamenti**.
  - f) Cliccare su **OK** per chiudere la finestra di dialogo **Configura il gestore aggiornamenti**.
3. Sottoscrivere il software che si desidera scaricare:
  - a) Riquadro **Sottoscrizioni software**:
    - Per cambiare una sottoscrizione esistente, cliccarvi due volte.
    - Per aggiungere una nuova sottoscrizione, cliccare su **Aggiungi** nella parte alta del riquadro.
  - b) Nella finestra di dialogo **Sottoscrizione al software**, se si sta aggiungendo una nuova sottoscrizione, digitare un nome per tale criterio nella casella **Nome sottoscrizione**.
  - c) Nell'elenco delle piattaforme, spuntare la casella accanto al software desiderato, e, nella finestra relativa alla versione, selezionare la versione richiesta.  
Solitamente si sottoscrivono le versioni **Consigliate**, in modo tale da garantire l'aggiornamento automatico del software. Per informazioni su quali altri tipi di versione sono disponibili, consultare la guida in linea di Enterprise Console, reperibile nella sezione relativa alla configurazione delle sottoscrizioni al software.
  - d) Cliccare su **OK** per chiudere la finestra di dialogo **Sottoscrizione software**.
  - e) Ripetere questi passaggi per tutte le sottoscrizioni che si desidera modificare o aggiungere.
4. Configurare il gestore aggiornamenti per l'utilizzo di queste sottoscrizioni:
  - a) Nel riquadro **Update manager**, selezionare il gestore aggiornamenti installato nel server. Cliccarvi col tasto destro del mouse e poi cliccare su **Visualizza/Modifica configurazione**.
  - b) Nella finestra di dialogo **Configura il gestore aggiornamenti**, nella scheda **Sottoscrizioni**, assicurarsi che le sottoscrizioni siano incluse nell'elenco **Sottoscritto a**. Se non lo sono, selezionare le sottoscrizioni dall'elenco **Disponibili** e cliccare sul pulsante **>** per spostarle nell'elenco **Sottoscritto a**.

5. Cliccare su **OK** per chiudere la finestra di dialogo **Configura il gestore aggiornamenti**.  
Il software selezionato viene scaricato sul gestore aggiornamenti installato nel server.

### 7.5.1.3 Configurazione del gestore degli aggiornamenti aggiuntivo

1. In Enterprise Console, dal menu **Visualizza**, cliccare su **Update Managers**.
2. Configurare il gestore degli aggiornamenti aggiuntivo in modo tale che utilizzi il gestore aggiornamenti principale come fonte degli aggiornamenti:
  - a) Nel riquadro **Update manager**, selezionare il gestore degli aggiornamenti aggiuntivo. Cliccarvi col tasto destro del mouse e poi cliccare su **Visualizza/Modifica configurazione**.
  - b) Nella finestra di dialogo **Configura il gestore aggiornamenti**, nella scheda **Fonti**, cliccare su **Aggiungi**.
  - c) Nella finestra di dialogo **Dettagli fonte**, nella casella **Indirizzo**, selezionare la condivisione in cui il gestore aggiornamenti principale scarica il software.  
  
Le caselle **Nome utente** e **Password** sono popolate automaticamente con le credenziali necessarie per accedere a questa condivisione.
  - d) Se si accede alla fonte degli aggiornamenti tramite server proxy, selezionare la casella di spunta **Utilizza server proxy per la connessione**. Inserire l'**Indirizzo** e il numero di **Porta** del server proxy. Nelle caselle **Nome utente** e **Password**, digitare le credenziali che consentono l'accesso al server proxy. se il nome utente deve riportare il dominio, utilizzare la forma dominio\nome utente.
  - e) Cliccare su **OK** per chiudere la finestra di dialogo **Dettagli fonte**.  
  
La condivisione in cui il gestore aggiornamenti principale scarica i software è elencata nella scheda **Fonti** della finestra di dialogo **Configura il gestore aggiornamenti**.
3. Configurare il gestore aggiornamenti per utilizzare le sottoscrizioni utilizzate in precedenza:
  - Nella scheda **Sottoscrizioni**, assicurarsi che le sottoscrizioni siano incluse nell'elenco **Sottoscritto a**. Se non lo sono, selezionare le sottoscrizioni dall'elenco **Disponibili** e cliccare sul pulsante **>** per spostarle nell'elenco **Sottoscritto a**.
4. Se si desidera effettuare il download su altre condivisioni, diverse da `\\nomeserver\SophosUpdate:`
  - a) Cliccare sulla scheda **Distribuzione**.
  - b) Assicurarsi che la sottoscrizione che si desidera utilizzare sia selezionata dall'elenco nella parte alta della scheda.
  - c) Cliccare su **Aggiungi**.
  - d) Nella finestra di dialogo **Cerca una cartella**, andare a una delle condivisioni. Cliccare su **OK**.
  - e) Selezionare la condivisione dall'elenco **Disponibile** e cliccare sul pulsante **>** per spostarla nell'elenco **Aggiorna a**.
  - f) Per inserire una descrizione per la condivisione, o credenziali per la scrittura, selezionare la condivisione e cliccare su **Configura**. Nella finestra di dialogo **Gestione condivisione**, inserire la descrizione e le credenziali.
  - g) Ripetere questi passaggi per tutte le condivisioni.

5. Cliccare su **OK** per chiudere la finestra di dialogo **Configura il gestore aggiornamenti**.

Il software selezionato viene scaricato nelle condivisioni specificate durante il prossimo aggiornamento pianificato.

L'installazione dei tool di gestione è terminata. Andare alla sezione [Pubblicare il software di sicurezza su un server web, se lo si desidera](#) a pagina 32.

## 7.5.2 Esecuzione degli aggiornamenti da Sophos da parte del gestore aggiornamenti addizionale

[Configurazione del gestore degli aggiornamenti aggiuntivo](#) a pagina 29 spiega come configurare il gestore aggiornamenti addizionale in modo tale che possa eseguire gli aggiornamenti direttamente da Sophos.

[Configurazione del gestore aggiornamenti principale](#) a pagina 30 spiega come configurare il gestore aggiornamenti principale, installato insieme alla console di gestione SEC per poter eseguire gli aggiornamenti dal gestore aggiornamenti addizionale.

### 7.5.2.1 Configurazione del gestore degli aggiornamenti aggiuntivo

Se si è disattivato il Controllo account utente prima di eseguire l'installazione di Enterprise Console, è ora possibile riattivarlo.

1. In Enterprise Console, dal menu **Visualizza**, cliccare su **Update Managers**.
2. Configurare il gestore aggiornamenti addizionale in modo tale che utilizzi Sophos come fonte degli aggiornamenti:
  - a) Nel riquadro **Update manager**, selezionare il gestore degli aggiornamenti aggiuntivo. Cliccarvi col tasto destro del mouse e poi cliccare su **Visualizza/Modifica configurazione**.
  - b) Nella finestra di dialogo **Configura il gestore aggiornamenti**, nella scheda **Fonti**, cliccare su **Aggiungi**.
  - c) Nella finestra di dialogo **Dettagli fonte**, nella casella **Indirizzo**, selezionare **Sophos**. Nelle caselle **Nome utente** e **Password**, digitare le credenziali di download fornite da Sophos.
  - d) Se si accede alla fonte degli aggiornamenti tramite server proxy, selezionare la casella di spunta **Utilizza server proxy per la connessione**. Inserire l'**Indirizzo** e il numero di **Porta** del server proxy. Nelle caselle **Nome utente** e **Password**, digitare le credenziali che consentono l'accesso al server proxy. se il nome utente deve riportare il dominio, utilizzare la forma dominio\nome utente.
  - e) Cliccare su **OK** per chiudere la finestra di dialogo **Dettagli fonte**.  
**Sophos** è elencato nella scheda **Fonti**, nella finestra di dialogo **Configura il gestore aggiornamenti**.
  - f) Cliccare su **OK** per chiudere la finestra di dialogo **Configura il gestore aggiornamenti**.
3. Sottoscrivere il software che si desidera scaricare:
  - a) Riquadro **Sottoscrizioni software**:
    - Per cambiare una sottoscrizione esistente, cliccarvi due volte.

- Per aggiungere una nuova sottoscrizione, cliccare su **Aggiungi** nella parte alta del riquadro.
  - b) Nella finestra di dialogo **Sottoscrizione al software**, se si sta aggiungendo una nuova sottoscrizione, digitare un nome per tale criterio nella casella **Nome sottoscrizione**.
  - c) Nell'elenco delle piattaforme, spuntare la casella accanto al software desiderato, e, nella finestra relativa alla versione, selezionare la versione richiesta.  
Solitamente si sottoscrivono le versioni **Consigliate**, in modo tale da garantire l'aggiornamento automatico del software. Per informazioni su quali altri tipi di versione sono disponibili, consultare la guida in linea di Enterprise Console, reperibile nella sezione relativa alla configurazione delle sottoscrizioni al software.
  - d) Cliccare su **OK** per chiudere la finestra di dialogo **Sottoscrizione software**.
  - e) Ripetere questi passaggi per tutte le sottoscrizioni che si desidera modificare o aggiungere.
4. Configurare il gestore aggiornamenti per l'utilizzo di queste sottoscrizioni:
- a) Nel riquadro **Update manager**, selezionare il gestore degli aggiornamenti aggiuntivo. Cliccarvi col tasto destro del mouse e poi cliccare su **Visualizza/Modifica configurazione**.
  - b) Nella finestra di dialogo **Configura il gestore aggiornamenti**, nella scheda **Sottoscrizioni**, assicurarsi che le sottoscrizioni siano incluse nell'elenco **Sottoscritto a**. Se non lo sono, selezionare le sottoscrizioni dall'elenco **Disponibili** e cliccare sul pulsante **>** per spostarle nell'elenco **Sottoscritto a**.
5. Cliccare su **OK** per chiudere la finestra di dialogo **Configura il gestore aggiornamenti**.  
Il software selezionato viene scaricato nel gestore degli aggiornamenti aggiuntivo.

### 7.5.2.2 Configurazione del gestore aggiornamenti principale

1. In Enterprise Console, dal menu **Visualizza**, cliccare su **Update Managers**.
2. Configurare il gestore aggiornamenti principale in modo tale che utilizzi il gestore degli aggiornamenti aggiuntivo come fonte degli aggiornamenti:
  - a) Nel riquadro **Update manager**, selezionare il gestore aggiornamenti installato nel server. Cliccarvi col tasto destro del mouse e poi cliccare su **Visualizza/Modifica configurazione**.
  - b) Nella finestra di dialogo **Configura il gestore aggiornamenti**, nella scheda **Fonti**, cliccare su **Aggiungi**.
  - c) Nella finestra di dialogo **Dettagli fonte**, nella casella **Indirizzo**, selezionare la condivisione in cui il gestore aggiornamenti aggiuntivo scarica il software.  
Le caselle **Nome utente** e **Password** sono popolate automaticamente con le credenziali necessarie per accedere a questa condivisione.
  - d) Se si accede alla fonte degli aggiornamenti tramite server proxy, selezionare la casella di spunta **Utilizza server proxy per la connessione**. Inserire l'**Indirizzo** e il numero di **Porta** del server proxy. Nelle caselle **Nome utente** e **Password**, digitare le credenziali che consentono l'accesso al server proxy. se il nome utente deve riportare il dominio, utilizzare la forma dominio\nome utente.
  - e) Cliccare su **OK** per chiudere la finestra di dialogo **Dettagli fonte**.

La condivisione in cui il gestore degli aggiornamenti aggiuntivo scarica i software è elencata nella scheda **Fonti** della finestra di dialogo **Configura il gestore aggiornamenti**.

3. Configurare il gestore aggiornamenti per utilizzare le sottoscrizioni utilizzate in precedenza:
  - Nella scheda **Sottoscrizioni**, assicurarsi che le sottoscrizioni siano incluse nell'elenco **Sottoscritto a**. Se non lo sono, selezionare le sottoscrizioni dall'elenco **Disponibili** e cliccare sul pulsante **>** per spostarle nell'elenco **Sottoscritto a**.
4. Se si desidera effettuare il download su altre condivisioni, diverse da \\*nomeserver*\SophosUpdate:
  - a) Cliccare sulla scheda **Distribuzione**.
  - b) Assicurarsi che la sottoscrizione che si desidera utilizzare sia selezionata dall'elenco nella parte alta della scheda.
  - c) Cliccare su **Aggiungi**.
  - d) Nella finestra di dialogo **Cerca una cartella**, andare a una delle condivisioni. Cliccare su **OK**.
  - e) Selezionare la condivisione dall'elenco **Disponibile** e cliccare sul pulsante **>** per spostarla nell'elenco **Aggiorna a**.
  - f) Per inserire una descrizione per la condivisione, o credenziali per la scrittura, selezionare la condivisione e cliccare su **Configura**. Nella finestra di dialogo **Gestione condivisione**, inserire la descrizione e le credenziali.
  - g) Ripetere questi passaggi per tutte le condivisioni.
5. Cliccare su **OK** per chiudere la finestra di dialogo **Configura il gestore aggiornamenti**.

Il software selezionato viene scaricato nelle condivisioni specificate durante il prossimo aggiornamento pianificato.

L'installazione dei tool di gestione è terminata. Andare alla sezione [Pubblicare il software di sicurezza su un server web, se lo si desidera](#) a pagina 32.

## 8 Pubblicazione del software di sicurezza in un server web

È possibile pubblicare il software di sicurezza Sophos su un server web, in modo tale che i computer vi accedano tramite HTTP. Ciò può essere particolarmente utile per i computer che non sono sempre connessi alla rete.

- Per pubblicare un software di sicurezza in un server web, consultare l'articolo [www.sophos.com/it-it/support/knowledgebase/38238.aspx](http://www.sophos.com/it-it/support/knowledgebase/38238.aspx).



## 9 Creazione di gruppi di computer

Se, per configurare i gruppi di computer (basati sui gruppi di Active Directory), è stata utilizzata la procedura guidata di download del software di sicurezza, saltare questa sezione. Andare alla sezione [Impostazione dei criteri di sicurezza](#) a pagina 34.

Prima di proteggere e gestire i computer, è necessario organizzarli in gruppi.

1. Se il riquadro **Gruppi** (a sinistra della finestra) non viene visualizzato, nel menu **Visualizza**, cliccare su **Computer**.
2. Cliccare ovunque all'interno del riquadro **Gruppi**. Verificare che il gruppo **Nessun gruppo** non sia selezionato.
3. Dal menu **Gruppi**, cliccare su **Crea gruppo**.

Viene aggiunto un **Nuovo gruppo** nel riquadro di sinistra, il cui nome appare evidenziato.

4. Inserire il nome da usare per il gruppo.
5. Per creare un altro gruppo di livello superiore, selezionare il server visualizzato in cima al riquadro **Gruppi** e ripetere i passaggi 3 e 4.  
Per creare un sottogruppo di un gruppo esistente, selezionare il gruppo esistente e ripetere i passaggi 3 e 4.

## 10 Impostazione dei criteri di sicurezza

Un *criterio di sicurezza* consiste in un insieme di impostazioni applicabili ai computer di uno o più gruppi.

Enterprise Console applica criteri predefiniti ai gruppi di computer. Questa sezione spiega:

- Quali sono i criteri predefiniti e se è necessario modificarli.
- Come creare e modificare un criterio.
- Come applicare un criterio a gruppi di computer.

### 10.1 Criteri predefiniti

Enterprise Console applica criteri di sicurezza predefiniti ai gruppi di computer. Non è necessario modificare tali criteri se non lo si desidera, fatta eccezione per i casi in cui:

- Si deve impostare subito un criterio firewall.
- Si devono modificare i criteri controllo applicazioni, controllo dati, controllo dispositivi, blocco rimozione, patch o web per poter utilizzare tali funzioni. Questa operazione può essere svolta in qualsiasi momento.

Per ulteriori informazioni sulle impostazioni dei criteri, consultare la *Guida all'impostazione dei criteri di Sophos Enterprise Console*.

### 10.2 Impostazione di un criterio del firewall

Per impostazione predefinita, il firewall blocca tutte le applicazioni non essenziali. È quindi necessario configurare il firewall prima di proteggere i computer.

1. Nel pannello **Criteri**, cliccare col tasto destro del mouse su **Firewall** e selezionare l'opzione **Crea criterio**.

Viene aggiunto un **Nuovo Criterio** all'elenco ed il suo nome sarà evidenziato. Inserire il nome da usare per il criterio.

2. Cliccare due volte sul criterio per modificarlo.

Viene avviata una procedura guidata.

3. Nella **procedura guidata di configurazione dei criteri del Firewall** si consiglia di selezionare quanto segue.

- a) Nella pagina **Configura firewall**, selezionare **Percorso singolo**, a meno che non si desideri che il firewall utilizzi impostazioni diverse a seconda del percorso in cui lo si utilizza.
- b) Nella pagina **Modalità operativa**, selezionare **Blocca il traffico in ingresso e consenti il traffico in uscita**.
- c) Nella pagina **Condivisione file e stampanti**, selezionare **Consenti condivisione file e stampanti**.

## 10.3 Creazione o modifica di un criterio

1. In Enterprise Console, se il riquadro **Criteri** (nella parte in fondo a sinistra della finestra) non viene visualizzato, nel menu **Visualizza**, cliccare su **Computer**.
2. Nel riquadro **Criteri**, svolgere una delle seguenti operazioni:
  - Per creare un nuovo criterio, cliccare col tasto destro del mouse sul tipo di criterio che si desidera creare, per es. **Aggiornamento** e cliccare su **Crea criterio**.
  - Per modificare un criterio predefinito, cliccare due volte sul tipo di criterio che si desidera modificare. Selezionare **Predefinito**.

Se si è creato un criterio, una voce **Nuovo criterio**, con il nome evidenziato, viene aggiunta all'elenco. Inserire il nome da usare per il criterio.

3. Cliccare due volte sul criterio. Inserire le impostazioni desiderate.

Se si crea un nuovo criterio, è necessario applicarlo a un gruppo di computer.

## 10.4 Applicazione di un criterio a un gruppo

- Nel riquadro **Criteri**, trascinare il criterio nel gruppo in cui si desidera applicare il criterio.  
**Nota:** in alternativa, è possibile cliccare col tasto destro del mouse su un gruppo e selezionare **Visualizza/Modifica dati dei criteri di gruppo**. È quindi possibile scegliere i criteri per quel gruppo dai menu a discesa.

# 11 Ricerca dei computer

Affinché Enterprise Console possa proteggere e gestire i computer in rete, è necessario innanzitutto cercarli.

1. Se il riquadro **Gruppi** (a sinistra della finestra) non viene visualizzato, nel menu **Visualizza**, cliccare su **Computer**.
2. Nel menu **Azioni**, cliccare su **Individuazione dei computer**.
3. Selezionare il metodo che si desidera utilizzare per cercare i computer.
4. Inserire i dati relativi all'account e, se necessario, indicare dove si desidera effettuare la ricerca.

Se si utilizza una delle opzioni di **Individua**, i computer vengono posizionati nella cartella **Nessun gruppo**.

## 12 Prepararsi alla protezione dei computer

### 12.1 Preparazione alla rimozione di software prodotti da terzi

Se si desidera che il programma di installazione Sophos rimuova tutti i software di sicurezza precedentemente installati:

1. Nei computer che utilizzano un software antivirus di altro fornitore, assicurarsi che l'interfaccia utente di tale software antivirus sia chiusa.
2. Nei computer che stanno eseguendo il firewall di altro fornitore o prodotto HIPS, assicurarsi che il firewall o il prodotto HIPS sia disattivato o configurato per consentire l'esecuzione del programma di installazione di Sophos.

Se i computer eseguono un tool di aggiornamento di terzi, sarà necessario rimuoverlo. Per ulteriori informazioni, consultare la Guida in linea di Enterprise Console.

### 12.2 Verifica del possesso di un account utilizzabile per l'installazione di software

Verrà richiesto di inserire dati relativi a un account utente di Windows che possa essere utilizzato per l'installazione del software di sicurezza. Deve:

- Avere diritti di amministratore locale sui computer che si desidera proteggere.
- Essere in grado di aprire una sessione sul computer in cui è stata installato Enterprise Console.
- Abbia accesso in lettura alla posizione dalla quale i computer si aggiorneranno. Per verificarlo, nel riquadro **Criteri**, cliccare due volte su **Aggiornamento**, quindi due volte su **Predefinito**.

**Nota:** Se il riquadro **Criteri** (in basso a sinistra della finestra) non viene visualizzato, nel menu **Visualizza**, cliccare su **Computer**.

Sophos consiglia che l'account:

- Non si tratti di un account amministratore di dominio e non sia stato configurato con deleghe vincolanti.
- Non abbia diritti di amministrazione o privilegi avanzati sui computer in cui sono installati Enterprise Console, gestioni di aggiornamenti aggiuntivi o message relay.
- Non abbia autorizzazioni di scrittura o modifica nel percorso da cui viene aggiornato il computer.
- È utilizzato per la protezione dei computer e non per operazioni amministrative generali.
- La password venga modificata frequentemente.

## 12.3 Preparazione per l'installazione del software antivirus

Potrebbe essere necessario preparare i computer prima di installare il software antivirus. Per informazioni, consultare la Guida alla distribuzione di Sophos ([https://downloads.sophos.com/tools/on-line/deployment\\_guide/it-it/index.html](https://downloads.sophos.com/tools/on-line/deployment_guide/it-it/index.html)), in particolare la sezione riguardante la preparazione dei computer per la distribuzione.

Si consiglia che i computer da proteggere abbiano il firewall abilitato.

**Nota:** Una volta protetti i computer in modo efficace e visualizzati come gestiti in Enterprise Console, disabilitare le eccezioni del firewall e create specificamente per consentire la distribuzione remota nei computer.

# 13 Protezione dei computer

## 13.1 Protezione automatica dei computer Windows

Questa sezione spiega come utilizzare Enterprise Console per proteggere i computer Windows in modo automatico.

È possibile utilizzare anche i propri tool o script per l'installazione del software di protezione nei computer Windows. Per dettagli, leggere l'articolo [www.sophos.com/it-it/support/knowledgebase/114191.aspx](http://www.sophos.com/it-it/support/knowledgebase/114191.aspx).

**Nota:** Quando si installa Sophos Client Firewall, vengono temporaneamente sconnesse tutte le schede di rete. Le conseguenze di ciò possono essere connessioni di rete non disponibili per un massimo di 20 secondi, e la sconnessione di applicazioni in rete quali Microsoft Remote Desktop.

1. In Enterprise Console, selezionare i computer che si desidera proteggere.
2. Effettuare una delle seguenti operazioni:
  - Se i computer appartengono a un gruppo, cliccare col tasto destro del mouse sul gruppo selezionato, quindi scegliere **Proteggi computer**.
  - Se i computer si trovano nel gruppo **Nessun gruppo**, basta semplicemente trascinarli nel gruppo prescelto.

Una procedura guidata accompagna nei passaggi dell'installazione del software di sicurezza Sophos. Accettare le opzioni predefinite, eccezion fatta per quanto elencato di seguito.

- a) Nella pagina **Seleziona funzioni**, selezionare le funzioni aggiuntive che si desidera installare:
- b) Nella pagina **Riepilogo protezione**, controllare i dati di eventuali problemi di installazione. Per ulteriore assistenza, consultare la sezione [Risoluzione dei problemi](#) a pagina 39.
- c) Nella pagina **Credenziali**, inserire i dati di un account utilizzabile per installare il software.

I computer selezionati sono ora protetti da un software di sicurezza. L'installazione avviene in più fasi, quindi il processo potrebbe richiedere un po' di tempo per essere completato su tutti i computer. Per alcuni computer, può essere necessario il riavvio per completare l'installazione.

Al termine dell'installazione, osservare nuovamente l'elenco dei computer. Nella colonna **In accesso**, la dicitura **Attivo** indica che il computer esegue la scansione in accesso delle minacce.

### 13.1.1 Risoluzione dei problemi

Quando si tenta di proteggere i computer Windows automaticamente, l'installazione di software di sicurezza può non riuscire per una serie di motivi diversi:

- L'installazione automatica non è attuabile sul sistema operativo in questione. Eseguire l'installazione manualmente. Consultare la sezione [Proteggere i computer Windows o Mac manualmente](#) a pagina 40 . Per gli altri sistemi operativi, consultare le ultime sezioni di questa guida.

- Impossibile determinare il sistema operativo. Ciò può essere dovuto al fatto che, durante la ricerca dei computer, il nome utente non è stato inserito nel formato dominio\nomeutente.
- Le regole del Firewall bloccano l'accesso, necessario per distribuire il software di sicurezza.
- Sui computer Windows XP, non è stata disattivata la funzione "Condivisione file semplice".
- Sui computer Windows Vista, non è stata disattivata la funzione "Usa procedura guidata condivisione".
- È stato scelto di installare una funzione non supportata da quel sistema operativo.

## 13.2 Protezione manuale dei computer Windows o Mac

Se in possesso di computer che non possono essere protetti automaticamente, è possibile proteggerli eseguendo un programma di installazione dalla cartella condivisa in cui è stato scaricato il software di sicurezza. Tale cartella corrisponde al percorso bootstrap.

È necessario utilizzare un account amministratore nei computer che si desidera proteggere.

Per proteggere manualmente i computer Windows o Mac:

1. In Enterprise Console, dal menu **Visualizza**, cliccare su **Percorsi Bootstrap**.

Viene visualizzato un elenco di percorsi. Memorizzare il percorso relativo a ciascun sistema operativo si desidera proteggere.

2. In tutti i computer che si desidera proteggere, andare al percorso bootstrap e fare quanto riportato qui di seguito:

- Per i computer Windows, trovare il file `setup.exe` e cliccarvi due volte.
- Per computer Mac, copiare il file del programma di installazione `Sophos Installer.app` e la directory `Sophos Installer Components` nel percorso prescelto (per es. sul desktop), quindi cliccarvi due volte.

Una procedura guidata accompagna nei passaggi dell'installazione. Accettare le opzioni predefinite, eccezion fatta per quanto elencato di seguito.

- Nei computer Windows, nella pagina **Dettagli account utente**, inserire i dettagli dell'account utilizzati per accedere a Update Manager Questa procedura è stata effettuata precedentemente, durante l'installazione di Enterprise Console in [Account del gestore aggiornamenti](#) a pagina 11.

**Suggerimento:** se non si è certi di quale account si tratti, utilizzare l'account a privilegi limitati che possa accedere al percorso bootstrap. In seguito, Enterprise Console applicherà un criterio di aggiornamento che includerà l'account utente corretto.

## 13.3 Protezione dei computer Linux o UNIX

Per informazioni su come proteggere i computer Linux o UNIX, consultare la *Guida di avvio di Enterprise Console per Linux e UNIX*.



## 14 Verifica dello stato della rete

Per verificare lo stato di salute della rete da Enterprise Console:

1. Eseguire il programma di installazione di Enterprise Console.

Se non già visualizzato, dal menu **Visualizza**, cliccare su **Pannello di controllo**.

Il Pannello di controllo mostra quanti computer:

- Presentano minacce.
- Non sono aggiornati.
- Non sono conformi ai criteri.

## 15 Protezione dei computer autonomi

Alcuni computer non sono mai collegati in rete e non sono di facile accesso, ad es. i computer che il personale utilizza a casa. Per proteggere tali computer, chiedere a ciascun utente di installare il software di sicurezza Sophos singolarmente utilizzando un programma di installazione "autonomo". Il software verrà quindi mantenuto aggiornato via Internet. Sono possibili due approcci:

- Gli utenti possono scaricare il software dalla pagina web [www.sophos.com/it-it/support/downloads/standalone-installers/esc-for-windows-2000-up.aspx](http://www.sophos.com/it-it/support/downloads/standalone-installers/esc-for-windows-2000-up.aspx). È possibile installare il software e configurarlo in modo tale che si aggiorni da Sophos.
- È possibile ripubblicare il software e tutti i successivi aggiornamenti sul proprio sito web. L'utente può scaricare il software dal sito web, installarlo e configurarlo in modo tale che scarichi gli aggiornamenti dal sito web. Per informazioni su come ripubblicare gli aggiornamenti Sophos sul proprio sito web, consultare l'articolo [www.sophos.com/it-it/support/knowledgebase/38238.aspx](http://www.sophos.com/it-it/support/knowledgebase/38238.aspx).

### 15.1 Invio delle informazioni necessarie ai computer autonomi

Inviare agli utenti che non sono in rete le seguenti informazioni:

- Il percorso dal quale possono scaricare il software di sicurezza (a meno che lo si fornisca su CD)
- V. la *Guida di avvio per computer autonomi di Sophos Endpoint Security and Control*.
- Il nome utente e la password necessari (sia che gli utenti effettuino il download direttamente da Sophos, sia dal sito web).

Quando si invia il nome utente e la password:

- Non inviare le credenziali per e-mail a un computer infetto, poiché potrebbero venire sottratte.
- Se necessario, inviare le credenziali per fax o per posta.

## 16 Supporto tecnico

È possibile ricevere supporto tecnico per i prodotti Sophos in uno dei seguenti modi:

- Visitando Sophos Community su [community.sophos.com/](https://community.sophos.com/) e cercando altri utenti con lo stesso problema.
- Visitando la knowledge base del supporto Sophos su [www.sophos.com/it-it/support.aspx](https://www.sophos.com/it-it/support.aspx).
- Scaricando la documentazione del prodotto su [www.sophos.com/it-it/support/documentation.aspx](https://www.sophos.com/it-it/support/documentation.aspx).
- Aprendo un ticket per il nostro supporto tecnico alla pagina <https://secure2.sophos.com/it-it/support/contact-support/support-query.aspx>.

## 17 Note legali

Copyright © 2009-2016 Sophos Limited. All rights reserved. Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero informazioni, o trasmessa, in qualsiasi forma o con qualsiasi mezzo, elettronico o meccanico, inclusi le fotocopie, la registrazione e altri mezzi, salvo che da un licenziatario autorizzato a riprodurre la documentazione in conformità con i termini della licenza, oppure previa autorizzazione scritta del titolare dei diritti d'autore.

Sophos, Sophos Anti-Virus e SafeGuard sono marchi registrati di Sophos Limited, Sophos Group e Utimaco Safeware AG. Tutti gli altri nomi citati di società e prodotti sono marchi o marchi registrati dei rispettivi titolari.

ACE™, TAO™, CIAO™, DAnCE™, e CoSMIC™

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™ (henceforth referred to as "DOC software") are copyrighted by [Douglas C. Schmidt](#) and his [research group](#) at [Washington University](#), [University of California, Irvine](#), and [Vanderbilt University](#), Copyright (c) 1993-2014, all rights reserved. Since DOC software is open-source, freely available software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with any code built using DOC software that you release. No copyright statement needs to be provided if you just ship binary executables of your software products.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not misappropriate the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, in a way that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let [us](#) know so we can promote your project in the [DOC software success stories](#).

The [ACE](#), [TAO](#), [CIAO](#), [DAnCE](#), and [CoSMIC](#) web sites are maintained by the [DOC Group](#) at the [Institute for Software Integrated Systems \(ISIS\)](#) and the [Center for Distributed Object Computing](#) of Washington University, St. Louis for the development of open-source software as part of the open-source software community. Submissions are provided by the submitter "as is" with no warranties whatsoever, including any warranty of merchantability, noninfringement of third party intellectual property, or fitness for any particular purpose. In no event shall the submitter be liable for any direct, indirect, special, exemplary, punitive, or consequential damages, including without limitation, lost profits, even if advised of the possibility of such damages. Likewise, DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A [number of companies](#) around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as

the underlying OS platform is Y2K-compliant. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, CoSMIC™, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let [me](#) know.

[Douglas C. Schmidt](#)

## Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license agreement for any such included software can be found at <http://www.apache.org/licenses/LICENSE-2.0>

## Boost C++ Libraries

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## Common Public License

Il software Sophos descritto in questo documento comprende o può comprendere programmi di software concessi in licenza (o sottolicenza) all'utente secondo i termini della Common Public License (CPL), la quale, tra gli altri diritti, permette all'utente di avere accesso al codice sorgente. La CPL richiede, per qualsiasi software concesso in licenza secondo i termini della stessa, e distribuito in formato codice oggetto, che il codice sorgente di tale software venga

messo a disposizione anche degli altri utenti del formato codice oggetto. Per qualsiasi software che rientri nei termini della CPL, il codice sorgente è disponibile tramite ordine postale inviandone richiesta a Sophos; per e-mail a [support@sophos.it](mailto:support@sophos.it) o tramite internet su <http://www.sophos.com/it-it/support/contact-support.aspx>. Una copia dei termini per tali software è reperibile all'indirizzo <http://opensource.org/licenses/cpl1.0.php>

## ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

## Loki

The MIT License (MIT)

Copyright © 2001 by Andrei Alexandrescu

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## OpenSSL Cryptography and SSL/TLS Toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

### **OpenSSL license**

Copyright © 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
 

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
 

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

### Original SSLey license

Copyright © 1995–1998 Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)) All rights reserved.

This package is an SSL implementation written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com))”

The word "cryptographic" can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

“This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com))”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

## WilsonORMapper

Copyright © 2007, Paul Wilson

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Windows Template Library (WTL)

Copyright © Microsoft Corporation. All rights reserved.



The use and distribution terms for this software are covered by the [Common Public License](#). Source code for this component is available here: <https://sourceforge.net/projects/wtl/files/>

## zlib data compression library

Copyright © 1995–2013 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly [jloup@gzip.org](mailto:jloup@gzip.org)

Mark Adler [madler@alumni.caltech.edu](mailto:madler@alumni.caltech.edu)