Guida del client Symantec™ Endpoint Protection 14.3 RU1 per Mac

Novembre 2020

In che modo Symantec Endpoint Protection protegge il Mac

Symantec Endpoint Protection combina diversi livelli di protezione per proteggere il computer da virus e attacchi spyware, nonché da tentativi di intrusione.

Tipi di protezione descrive ogni livello di protezione.

Table 1: Tipi di protezione

Protezione	Descrizione
Protezione antivirus e antispyware	Symantec Endpoint Protection include scansioni antivirus pianificate, scansioni su richiesta e Auto-Protect, che viene eseguito in background e protegge il computer contro i virus. Quando viene rilevato un virus, Symantec Endpoint Protection lo elimina. In che modo le protezioni antivirus e antispyware proteggono il Mac
Protezione dalle minacce di rete	Symantec Endpoint Protection intercetta i dati a livello di rete. Questa funzione utilizza le firme per eseguire la scansione di pacchetti o flussi di pacchetti. ed esegue la scansione di ogni singolo pacchetto cercando i profili che corrispondono ad attacchi al browser o alla rete. La Protezione dalle minacce di rete include i seguenti elementi: • La prevenzione delle intrusioni, la quale rileva gli attacchi ai componenti del sistema operativo e a livello di applicazione. Quando Symantec Endpoint Protection rileva una minaccia per la rete, la blocca. • Il firewall, il quale consente o blocca il traffico di rete in base alle politiche e alle regole del firewall. (A partire dalla versione 14.2). In che modo la Protezione dalle minacce di rete protegge il Mac
Controllo periferiche	Gli amministratori di Symantec Endpoint Protection Manager configurano una politica di controllo delle periferiche. Le periferiche possono essere bloccate o sbloccate con questa politica in base a nome, fornitore, modello o numero di serie della periferica. In un client gestito, è possibile esaminare le impostazioni di Controllo periferiche nella scheda **Avanzate**. Il controllo delle periferiche non è disponibile per i client non gestiti. Informazioni sul controllo delle periferiche sul client Symantec Endpoint Protection per Mac
Endpoint Detection and Response	Gli amministratori di Symantec Endpoint Protection Manager configurano una politica del recorder delle attività che fornisce gli strumenti per rilevare ed esporre le attività di rete sospette.

Il client scarica automaticamente le definizioni dei virus, le definizioni IPS e gli aggiornamenti del prodotto nel computer.

Aggiornamento delle definizioni dei virus, delle definizioni di prevenzione delle intrusioni e del software del client

In che modo le protezioni antivirus e antispyware proteggono il Mac

Symantec Endpoint Protection utilizza le definizioni del virus per individuare i virus noti durante le scansioni pianificate e quelle manuali. Auto-Protect utilizza le definizioni dei virus per eseguire una scansione costante dell'attività del computer.

Symantec Endpoint Protection genera una notifica quando rileva un virus o un altro rischio per la sicurezza. Viene rilevato un virus o un altro rischio per la sicurezza quando si verifica una delle seguenti condizioni:

- Auto-Protect rileva un virus durante il monitoraggio del computer.
- Auto-Protect rileva un virus da una scansione pianificata o avviata manualmente.

Con le impostazioni predefinite attivate, Symantec Endpoint Protection cerca automaticamente di riparare tutti i virus trovati. Se non è possibile riparare il file, il client lo mette in quarantena per evitare che possa danneggiare il computer.

Il client esegue solitamente queste riparazioni senza la necessità di alcun intervento da parte dell'utente. Quando il computer trova un virus, è possibile inviare le informazioni sullo stesso a Symantec.

In alcuni casi il client chiede di scegliere se si desidera riparare, eliminare o ripristinare il file infetto rilevato. Le riposte determinano le successive azioni che il client esegue sul file infetto.

Risposta a messaggi riguardanti infezioni e rilevamenti di rischi

Attivazione o disattivazione dell'invio di informazioni sulla sicurezza a Symantec

In che modo Protezione dalle minacce di rete protegge il Mac

Protezione dalle minacce di rete include le seguenti tecnologie di protezione:

- Prevenzione delle intrusioni
- Firewall

Prevenzione delle intrusioni

La prevenzione delle intrusioni rileva e blocca automaticamente gli attacchi di rete. La prevenzione delle intrusioni rappresenta un livello interno di difesa per la protezione dei computer client. La prevenzione delle intrusioni è a volte denominata Sistema di prevenzione delle intrusioni (IPS).

La prevenzione delle intrusioni intercetta i dati al livello di rete. Questa funzione utilizza le firme per eseguire la scansione di pacchetti o flussi di pacchetti. ed esegue la scansione di ogni singolo pacchetto cercando i profili che corrispondono ad attacchi al browser o alla rete. La prevenzione delle intrusioni rileva gli attacchi ai componenti del sistema operativo e a livello di applicazione.

La prevenzione delle intrusioni utilizza le firme per identificare gli attacchi ai computer client. Per gli attacchi noti, la prevenzione delle intrusioni elimina automaticamente i pacchetti che corrispondono alle firme.

Firewall

Il firewall consente di monitorare il traffico di rete e blocca il traffico potenzialmente dannoso per proteggere il Mac. Il firewall Symantec Endpoint Protection non è disponibile nel client non gestito.

Il firewall Symantec Endpoint Protection monitora il traffico sui livelli trasporto e Internet. Il firewall integrato di Mac monitora il traffico al livello superiore applicazione, dopo che è stato monitorato dal firewall Symantec Endpoint Protection. Di conseguenza è possibile attivare entrambi i firewall ed eseguirli in parallelo.

Il firewall utilizza i seguenti tipi di regole firewall per autorizzare o bloccare il traffico di rete:

- Regole predefinite
- Regole personalizzate
- Regole integrate
- Regole di protezione

Queste regole includono il rilevamento della scansione delle porte, il rilevamento della negazione del servizio, lo spoofing anti-MAC, lo smart DHCP e lo smart DNS. Le impostazioni del firewall sono controllate interamente dall'amministratore di Symantec Endpoint Protection Manager. È possibile attivare o disattivare il firewall solo se l'amministratore autorizza il controllo client per il Mac.

La protezione firewall è stata aggiunta nella versione 14.2.

Gestione della prevenzione delle intrusioni

Gestione della protezione del firewall per il client Mac

Compatibilità del sistema operativo con Symantec Endpoint Protection per Mac

Symantec Endpoint Protection per Mac supporta le seguenti versioni del sistema operativo:

- macOS da 10.15 a 10.15.5
- macOS 10.14
- macOS 10.13

Per ulteriori informazioni sul supporto delle versioni precedenti del sistema operativo Mac, consultare la sezione Compatibilità Mac con il client di Endpoint Protection.

Informazioni sull'autorizzazione delle estensioni del kernel per Symantec Endpoint Protection per macOS 10.13 o versioni successive

Note di rilascio, nuove correzioni e requisiti di sistema per tutte le versioni di Endpoint Protection

Installazione del client Symantec Endpoint Protection per Mac

È possibile installare direttamente un client Symantec Endpoint Protection su un computer Mac se non è possibile o non si desidera utilizzare Push remoto. I passaggi sono simili sia se il client non è gestito sia se è gestito.

Il solo modo per installare un client gestito è utilizzare un pacchetto creato da Symantec Endpoint Protection Manager. È possibile convertire in qualunque momento un client non gestito in un client gestito importando le impostazioni di comunicazione client/server nel client Mac.

> **NOTE**
> Per preparare il client Symantec Endpoint Protection per Mac per l'uso con software di distribuzione remota di terze parti, consultare Exporting and Deploying a client Symantec Endpoint Protection via Apple Remote Desktop or Casper.

Table 2: Metodi per l'installazione del client Mac

Se il file di installazione è stato scaricato.	1. Estrarre il contenuto in una cartella su un computer Mac, quindi aprire la cartella. 2. Aprire `SEP_MAC`. 3. Copiare `Symantec Endpoint Protection.dmg` sul desktop del computer Mac. 4. Fare doppio clic su `Symantec Endpoint Protection.dmg` per installare il file come disco virtuale. È quindi possibile installare il client Symantec Endpoint Protection per Mac.
Se si dispone di un pacchetto di installazione client .zip dal Portale del supporto Broadcom.	1. Copiare il file sul desktop del computer Mac. Il file può essere denominato `Symantec Endpoint Protection .zip` o `Symantec_Endpoint_Protection_version_Mac_Client.zip`, doveversionè la versione del prodotto. 2. Fare clic con il pulsante destro del mouse su **Apri con > utilità di archiviazione** per estrarre i contenuti del file. 3. Aprire la cartella risultante. È quindi possibile installare il client Symantec Endpoint Protection per Mac.

La cartella o l'immagine del disco virtuale risultante contiene il programma di installazione dell'applicazione e una cartella denominata Additional Resources. Entrambi gli elementi devono essere presenti nello stesso percorso perché l'installazione vada a buon fine. Se si copia il programma di installazione in un altro percorso, è necessario anche copiare la cartella Additional Resources.

Per installare il client Symantec Endpoint Protection per Mac:

1. Fare doppio clic su `Installa Symantec Endpoint Protection`.
2. Per avviare l'installazione, fare clic su **Installa**.
3. Per installare uno strumento assistente necessario per l'installazione del client Symantec Endpoint Protection, immettere il nome utente e la password di amministratore del Mac, quindi fare clic su **Installa assistente**.
4. Dopo l'installazione, fare clic su **Continua** per terminare la configurazione del client Symantec Endpoint Protection.
5. Per configurare il client Symantec Endpoint Protection, procedere come segue:

Autorizzare l'estensione del sistema Symantec Endpoint Protection.	Nella finestra di dialogo **Sicurezza e Privacy** della scheda **Generale**, fare clic su **Consenti** per l'opzione **È stato bloccato il caricamento del software di sistema dall'applicazione Symantec Endpoint Protection**. Se necessario, fare clic sull'icona di blocco per apportare le modifiche richieste. È necessario autorizzare l'estensione del sistema per il corretto funzionamento di Symantec Endpoint Protection. Informazioni sull'autorizzazione delle estensioni del kernel per Symantec Endpoint Protection per macOS 10.15 o versioni successive
Consentire l'accesso completo al disco.	Nella finestra di dialogo **Sicurezza e Privacy** della scheda **Privacy**, accertarsi che l'**estensione di sistema Symantec** possa accedere ai dati e alle impostazioni di amministrazione per tutti gli utenti sulla propria periferica Mac. Se necessario, fare clic sull'icona di blocco per apportare le modifiche richieste.
Consentire le modifiche al profilo di rete.	Quando viene richiesto se autorizzare **l'applicazione di filtri al contenuto di rete da parte di Symantec Endpoint Protection**, fare clic su **Consenti**.

6. Fare clic su **Completato**.

Informazioni sull'autorizzazione delle estensioni del kernel per Symantec Endpoint Protection per macOS 10.15 o versioni successive

La richiesta di autorizzazione delle estensioni del sistema è una nuova funzionalità di sicurezza introdotta in macOS 10.15.È necessario autorizzare l'estensione del sistema per il corretto funzionamento di Symantec Endpoint Protection.

Per autorizzare l'estensione del sistema per Symantec Endpoint Protection durante la configurazione del client Symantec Endpoint Protection, nella finestra di dialogo **Sicurezza e Privacy** della scheda **Generale**, fare clic su **Consenti** per l'opzione **È stato bloccato il caricamento del software di sistema dall'applicazione Symantec Endpoint Protection**.

Installazione del client Symantec Endpoint Protection per Mac

Prompt dell'upgrade per il client Symantec Endpoint Protection per il Mac

Con le impostazioni per installazione del client, gli amministratori di Symantec Endpoint Protection Manager possono assegnare un pacchetto di installazione client per eseguire automaticamente l'upgrade dei computer client gestiti.

Se si è eseguito l'accesso al Mac, è possibile consultare un prompt per l'avvio per completare l'installazione. È possibile potere ritardare il riavvio basato sulle impostazioni dell'installazione del client.

Se non si è eseguito l'accesso al Mac, l'installazione riavvia automaticamente il Mac.

Guida introduttiva al client Symantec Endpoint Protection

Quando si apre il client Symantec Endpoint Protection, viene visualizzato il messaggio relativo alla **protezione** nella parte superiore della pagina, a meno che non si verifichi un problema che deve essere risolto. Fare clic su **Correggi** per risolvere eventuali problemi.

Il client Symantec Endpoint Protection visualizza le attività principali che è possibile eseguire.

Table 3: Pagine client Symantec Endpoint Protection

Opzione	Descrizione
Sicurezza	Mostra lo stato di protezione del computer.
Scansioni	Consente di eseguire la scansione del computer. È possibile scegliere di eseguire una scansione personalizzata o una scansione completa. È inoltre possibile rimuovere un file o una cartella da scansionare. Esecuzione di una scansione manuale
LiveUpdate	Esegue LiveUpdate per aggiornare le definizioni e i file del prodotto di Symantec Endpoint Protection. Aggiornamento immediato del contenuto in Symantec Endpoint Protection
Avanzate	Offre opzioni più dettagliate per Protezione antivirus e antispyware, Protezione dalle minacce di rete e LiveUpdate.

Gestione della protezione del Mac con Symantec Endpoint Protection

Le impostazioni predefinite di Symantec Endpoint Protection consentono di proteggere il Mac da numerosi tipi di malware. Il client gestisce automaticamente il malware oppure consente di scegliere come gestirlo.

A seconda delle impostazioni definite dall'amministratore, è necessario eseguire le seguenti operazioni per mantenere la protezione.

> **NOTE**
> L'amministratore potrebbe non avere concesso all'utente il controllo di queste operazioni.

Table 4: Protezione del computer

Passaggi	Descrizione
Passaggio 1: verificare che la Protezione antivirus e antispyware e che la Protezione dalle minacce di rete siano entrambe attivate.	Vengono visualizzati la pagina **Sicurezza** indicante un segno di spunta verde e il messaggio **Il computer è protetto** se le protezioni sono attivate. Attivazione e disattivazione di Protezione antivirus e antispyware Attivazione o disattivazione della Protezione dalle minacce di rete
Passaggio 2: verificare che il software e le definizioni siano aggiornate.	La pagina **Sicurezza** visualizza la data dell'ultimo aggiornamento delle definizioni per Protezione antivirus e antispyware e Protezione dalle minacce di rete. In **LiveUpdate** viene visualizzata la data dell'ultimo aggiornamento del prodotto. Per visualizzare il numero di versione del software, fare clic su **Guida > Informazioni**.
Passaggio 3: se necessario, aggiornare il software o le definizioni.	Nel client Symantec Endpoint Protection, fare clic su **LiveUpdate** per aggiornare immediatamente il software e le definizioni corrispondenti. Aggiornamento delle definizioni dei virus, delle definizioni di prevenzione delle intrusioni e del software del client
Passaggio 4: eseguire una scansione.	È possibile pianificare l'esecuzione delle scansioni a intervalli regolari oppure eseguirne una immediatamente. Configurazione delle scansioni pianificate Esecuzione di una scansione manuale

Gestione delle impostazioni della protezione antivirus e antispyware

Rinnovo della licenza del prodotto

È possibile che venga visualizzato un messaggio sotto l'icona del client Symantec Endpoint Protection sulla barra dei menu che indica che la licenza di Symantec Endpoint Protection è scaduta. Il client Symantec Endpoint Protection utilizza una licenza per aggiornare quanto segue:

- Il software client
- I file delle definizioni di protezione per la scansione di virus e spyware e la prevenzione delle intrusioni

Il client può utilizzare una licenza di prova o una licenza a pagamento. Se tale licenza è scaduta, il client non aggiorna le definizioni o il software client.

Per entrambi i tipi di licenza, è necessario contattare l'amministratore per aggiornare o rinnovare la licenza.

Risposta a messaggi riguardanti infezioni e rilevamenti di rischi

Attivazione o disattivazione del controllo periferiche sul client Symantec Endpoint Protection per Mac

Gli amministratori di Symantec Endpoint Protection Manager possono configurare i client gestiti con una politica di controllo delle periferiche. Le periferiche possono essere bloccate o sbloccate con questa politica in base a nome, fornitore, modello o numero di serie della periferica.

È possibile visualizzare le attività di controllo periferiche nella pagina **Avanzate** facendo clic su **Attività > Cronologia sicurezza**.

Le impostazioni nell'interfaccia client di Symantec Endpoint Protection per il **Controllo periferiche** consentono di attivare o disattivare il controllo delle periferiche. Se il controllo delle periferiche è attivato, è possibile attivare o disattivare le notifiche quando i dispositivi sono bloccati o sbloccati.

Per modificare le impostazioni, è necessario autenticarsi con le credenziali dell'amministratore Mac. Se queste impostazioni sono disabilitate, l'amministratore le ha bloccate per impedire di attivare o disattivare questa funzionalità.

Non è possibile aggiungere o modificare i dispositivi da bloccare o sbloccare attraverso l'interfaccia del client Symantec Endpoint Protection.

> **NOTE**
> La politica di controllo delle periferiche da Symantec Endpoint Protection Manager controlla le impostazioni del controllo delle periferiche. Al successivo heartbeat, tutte le modifiche apportate a queste impostazioni ritornano a ciò che indica la politica.

Il controllo delle periferiche non è disponibile per i client non gestiti.

Informazioni su WSS Traffic Redirection per client Mac

Web Security Service (WSS) Traffic Redirection (WTR) automatizza il reindirizzamento del traffico Web a Symantec Web Security Service e protegge il traffico Web in ogni computer che utilizza Symantec Endpoint Protection.

L'amministratore controlla le impostazioni utilizzate da WSS Traffic Redirection, tra cui l'URL di configurazione proxy e il certificato principale Symantec Web Security Service facoltativo. Solo l'amministratore Symantec Endpoint Protection Manager può configurare queste impostazioni, che non vengono visualizzate nell'interfaccia utente del client Symantec Endpoint Protection. È possibile visualizzare l'URL del file di configurazione proxy su Mac tramite **Preferenze di sistema > Rete**, nell'area **Proxy**. Il certificato Cloud Services viene visualizzato in **Keychain**.

I browser Web Safari, Chrome e Firefox (versione 65 e successive) supportano WSS Traffic Redirection. Le versioni di Symantec Endpoint Protection precedenti a 14.2 RU1 supportano solo Safari e Chrome.

Disinstallazione del client Symantec Endpoint Protection per Mac

Disinstallare il client Symantec Endpoint Protection per il Mac mediante l'icona del client sulla barra del menu. Disinstallare il client Symantec Endpoint Protection per il Mac richiede le credenziali amministrative dell'utente.

> **NOTE**
> Dopo avere disinstallato il client Symantec Endpoint Protection, viene richiesto di riavviare il computer client per completare la disinstallazione. Prima di iniziare, assicurarsi di aver salvato tutto il lavoro non finito o di chiudere tutte le applicazioni aperte.

Per disinstallare il client Symantec Endpoint Protection per Mac:

1. Nel computer client Mac, aprire il client Symantec Endpoint Protection e fare clic su **Symantec Endpoint Protection > Disinstalla Symantec Endpoint Protection**.
2. Fare clic nuovamente su **Disinstalla** per iniziare la disinstallazione.
3. Per installare uno strumento assistente necessario per la disinstallazione del client Symantec Endpoint Protection, immettere il nome utente e la password di amministratore del Mac, quindi fare clic su **Installa assistente**.
4. Nella finestra di dialogo **Symantec Endpoint Protection sta tentando di modificare un'estensione del sistema**, immettere il nome utente e la password di amministrazione del Mac, quindi fare clic su **OK**.

   Potrebbe anche venire richiesto di digitare una password per disinstallare il client. Questa password potrebbe essere diversa dalla password di amministrazione del Mac.
5. Al termine della disinstallazione, fare clic su **Riavvia ora**.

Se Symantec Uninstaller non riesce nell'operazione, potrebbe essere necessario utilizzare un altro metodo di disinstallazione. Consultare:

Disinstallazione di Symantec Endpoint Protection

Aggiornamento delle definizioni dei virus, delle definizioni di prevenzione delle intrusioni e del software del client

I prodotti Symantec si affidano a informazioni aggiornate per proteggere il computer dalle nuove minacce rilevate. Symantec fornisce queste informazioni a Symantec Endpoint Protection tramite LiveUpdate. LiveUpdate ottiene gli aggiornamenti dei prodotti e delle definizioni per il computer in uso tramite la connessione Internet.

Gli aggiornamenti delle definizioni sono i file che mantengono i prodotti Symantec aggiornati con le tecnologie di protezione dalle minacce più recenti. LiveUpdate recupera le nuove firme di prevenzione delle intrusioni o i nuovi file delle definizioni dei virus da un sito Internet Symantec e quindi sostituisce i file precedenti.

Gli aggiornamenti del programma sono miglioramenti al client installato. Gli aggiornamenti del prodotto sono creati solitamente per estendere la compatibilità dell'hardware o del sistema operativo, per risolvere un problema di prestazioni o per correggere errori del prodotto. Gli aggiornamenti del prodotto vengono rilasciati quando necessario. Il client riceve gli aggiornamenti dei prodotti direttamente dal server LiveUpdate. Gli aggiornamenti dei prodotti e delle definizioni vengono chiamati collettivamente aggiornamenti del contenuto.

Table 5: Modalità di aggiornamento del contenuto sul computer

Attività	Descrizione
Aggiornamento immediato del contenuto	È possibile eseguire LiveUpdate immediatamente. Aggiornamento immediato del contenuto in Symantec Endpoint Protection

Gestione della protezione Mac con Symantec Endpoint Protection

Aggiornamento immediato del contenuto in Symantec Endpoint Protection

È possibile aggiornare immediatamente i file delle definizioni e dei prodotti usando LiveUpdate. È necessario eseguire manualmente LiveUpdate per i seguenti motivi:

- Il software client è stato installato di recente.
- È trascorso molto tempo dall'ultima scansione.
- Si sospetta la presenza di un virus o di un altro problema di malware.

Per aggiornare immediatamente il contenuto in Symantec Endpoint Protection:

Avviare LiveUpdate in uno dei seguenti modi:

- Fare clic con il pulsante destro del mouse sull'icona Symantec Endpoint Protection nella barra dei menu, quindi fare clic su **LiveUpdate**.
- Aprire il client Symantec Endpoint Protection, quindi fare clic su **LiveUpdate**.

LiveUpdate si connette al server LiveUpdate configurato, cerca gli aggiornamenti disponibili, quindi li scarica e li installa automaticamente. Una barra di stato indica l'avanzamento del download.

Aggiornamento delle definizioni dei virus, delle definizioni di prevenzione delle intrusioni e del software del client

Aggiornamento pianificato del contenuto in Symantec Endpoint Protection

Pianificazioni sui client Mac gestiti

Per impostazione predefinita, i client Mac gestiti ricevono una pianificazione da Symantec Endpoint Protection Manager che esegue LiveUpdate ogni quattro ore. L'amministratore di Symantec Endpoint Protection Manager controlla la pianificazione. I client gestiti non possono rimuovere, modificare o visualizzare la pianificazione creata dall'amministratore o creare una nuova pianificazione.

Pianificazioni su client Mac non gestiti

È possibile pianificare l'esecuzione automatica di LiveUpdate a intervalli pianificati. È possibile pianificare l'esecuzione di LiveUpdate in un momento in cui il computer non viene utilizzato.

Per eseguire l’aggiornamento pianificato del contenuto in Symantec Endpoint Protection:

1. Nel client Symantec Endpoint Protection, nella pagina **Avanzate**, selezionare **Impostazioni prodotto**, quindi fare clic sull'icona delle impostazioni della **sessione di LiveUpdate pianificata**.

   Viene visualizzata la pianificazione corrente.

2. Selezionare un intervallo dal menu a discesa della pianificazione di LiveUpdate.

   L’impostazione iniziale prevede l’esecuzione ogni **4** ore. È inoltre possibile scegliere di eseguirla **ogni giorno** oppure **ogni settimana**, selezionando rispettivamente l’ora o il giorno e l’ora desiderati.

3. Fare clic su **Applica modifiche**.

Aggiornamento immediato del contenuto in Symantec Endpoint Protection

Aggiornamento delle definizioni dei virus, delle definizioni di prevenzione delle intrusioni e del software del client

Informazioni sulla connessione al server di gestione tramite un server proxy

È possibile che venga chiesto di consentire a Symantec Endpoint Protection di utilizzare le proprie credenziali per connettersi al server di gestione tramite un proxy. In questo caso, si riceve un messaggio che richiede se si desidera consentire l'accesso alle credenziali al processo `symdaemon`.

Fare clic su **Sempre** nella finestra del messaggio. In caso contrario, ogni volta che il client comunica con il server LiveUpdate viene visualizzato lo stesso messaggio. Se si fa clic su **Rifiuta**, il client non può ricevere aggiornamenti del software o delle definizioni.

Aggiornamento delle definizioni dei virus, delle definizioni di prevenzione delle intrusioni e del software del client

Gestione delle impostazioni della protezione antivirus e antispyware

Per impostazione predefinita, Symantec Endpoint Protection offre protezione contro i virus e i rischi per la sicurezza, tra cui le minacce alla rete, non appena viene avviato il computer. Protezione antivirus e antispyware include la funzione Auto-Protect, che controlla i programmi in esecuzione alla ricerca di virus. Esegue inoltre il monitoraggio di eventuali attività che possono indicare la presenza di virus o rischi per la sicurezza. L'intercettazione di Auto-Protect impedisce ai virus di infettare il computer. Si consiglia pertanto di mantenere Auto-Protect attivato.

Per i client gestiti, il controllo che si ha su queste impostazioni dipende da come l'amministratore ha configurato il client. Inoltre, tutte le modifiche applicate a queste impostazioni possono ritornare a ciò che indica la politica al successivo heartbeat.

La sezione Gestione della protezione antivirus e antispyware descrive le attività che è possibile eseguire per gestire la protezione da virus e spyware sul proprio Mac.

Table 6: Gestione della protezione antivirus e antispyware

Passaggi	Descrizione
Passaggio 1: Attivazione e disattivazione di Protezione antivirus e antispyware	È possibile attivare e disattivare con facilità Protezione antivirus e antispyware. Symantec consiglia di lasciarla attivata. Attivazione e disattivazione di Protezione antivirus e antispyware
Passaggio 2: Personalizzazione delle impostazioni di Auto-Protect	Auto-Protect è un componente importante di Protezione antivirus e antispyware. È possibile configurare queste opzioni nella pagina **Avanzate**. Configurazione delle impostazioni di Auto-Protect e di zone di scansione
Passaggio 3: Scansione antivirus del computer	È possibile configurare l'esecuzione immediata o pianificata di scansioni antivirus. Configurazione delle scansioni pianificate Sospensione, posticipo e interruzione di scansioni Esecuzione di una scansione manuale
Passaggio 4: Risposta in caso di rilevamento di un virus da parte di Symantec Endpoint Protection	Quando Symantec Endpoint Protection scansiona il computer, potrebbe: • Informare l'utente riguardo le azioni che è possibile eseguire. • Informare l'utente sulle azioni di protezione che sono state intraprese. Risposta a messaggi riguardanti infezioni e rilevamenti di rischi

Attivazione e disattivazione di Protezione antivirus e antispyware

Per impostazione predefinita, la Protezione antivirus e antispyware è attivata insieme ad Auto-Protect.

È possibile controllare Auto-Protect in modo più preciso impostando determinate opzioni.

Se la Protezione antivirus e antispyware è disattivata, una "x" rossa viene visualizzata nella pagina **Stato** insieme al messaggio **Protezione antivirus e antispyware disattivata**. Se la protezione è stata disattivata, è necessario attivarla al più presto.

> **NOTE**
> Le scansioni pianificate continuano ad avere luogo, indipendentemente dall'attivazione Protezione antivirus e antispyware. L'amministratore può limitare l'accesso ad alcune impostazioni di Symantec Endpoint Protection. È possibile che non sia consentito disattivare queste impostazioni, pianificare scansioni o personalizzare le opzioni di protezione.È possibile che si debba fornire la password di amministratore Mac per poter cambiare queste impostazioni.

Per attivare e disattivare la Protezione antivirus e antispyware:

1. Per attivare la Protezione antivirus e antispyware nel client Symantec Endpoint Protection, nella pagina **Avanzate** fare clic sull'opzione di **protezione del Mac**, quindi abilitare le **scansioni automatiche**.
2. Per disattivare la protezione antivirus e antispyware nel client Symantec Endpoint Protection, nella pagina **Avanzate** fare clic sull'opzione di **protezione del Mac**, quindi disattivare le **scansioni automatiche**.

Configurazione delle impostazioni di Auto-Protect e di zone di scansione

Gestione delle impostazioni della protezione antivirus e antispyware

Risposta a messaggi riguardanti infezioni e rilevamenti di rischi

Configurazione delle impostazioni di Auto-Protect e di zone di scansione

Nei client gestiti, se l'amministratore lo consente, è possibile personalizzare in che modo Auto-Protect controlla i virus e ripara i file infetti.

Le impostazioni di Auto-Protect vengono visualizzate come opzioni per la **protezione del Mac**. È necessario attivare le **scansioni automatiche** per abilitare Auto-Protect.

Le **impostazioni di zone di scansione** consentono di specificare i file da includere o escludere da una scansione.

Per configurare le impostazioni di Auto-Protect:

1. Nel client Symantec Endpoint Protection, nella pagina **Avanzate**, fare clic sull'opzione di **protezione del Mac**, quindi fare clic sull'icona delle impostazioni delle **scansioni automatiche**.
2. Impostare le seguenti opzioni:

Quarantena automatica	È possibile scegliere se mettere in quarantena i file che non possono essere riparati.
Riparazione automatica	È possibile scegliere di riparare automaticamente tutti i file infetti rilevati.
Scansione	È possibile scegliere **Dischi di dati** oppure **Tutti gli altri dischi**.
Esegui scansione di file compressi	È possibile scegliere se includere i file compressi in una scansione di Auto-Protect. La scansione include il file compresso e i file contenuti nello stesso.

WARNING
Se non si seleziona **Riparazione automatica**, i file infetti non vengono messi in quarantena, anche se si sceglie **Quarantena automatica**.Il programma chiede se si desidera riparare un file infetto. Se il file non viene riparato, rimane in tale stato nel computer. Se si seleziona **Riparazione automatica** ma non si seleziona **Quarantena automatica**, i file infetti vengono eliminati.

3. Fare clic su **Fine**.

Per configurare le impostazioni delle zone di scansione:

1. Nel client Symantec Endpoint Protection, nella pagina **Avanzate**, fare clic sull'**opzione di protezione del Mac**, quindi fare clic sull'icona delle impostazioni delle impostazioni di **Impostazioni zona di scansione**.
2. Impostare le seguenti opzioni:

Esegui scansione dell'intero sistema	Tutti i file e i processi sul computer vengono analizzati durante l'accesso.
Esegui solo scansione	La scansione include solo i file o le cartelle specificati.
Non eseguire la scansione	Tutti i file vengono analizzati, ad eccezione dei file o delle cartelle che si desidera escludere dalla scansione.

Usa impostazioni predefinite	Questa opzione esegue una scansione completa.

3. Fare clic su **OK**.

In che modo le protezioni antivirus e antispyware proteggono il Mac

Attivazione e disattivazione di Protezione antivirus e antispyware

Gestione dei file in quarantena

Configurazione delle scansioni pianificate

Se si utilizza un client gestito, Symantec Endpoint Protection esegue automaticamente una scansione predefinita. Se l'amministratore lo consente, è possibile configurare ulteriori scansioni pianificate.

> **NOTE**
> In un client non gestito, è necessario eseguire manualmente le scansioni.Symantec consiglia di eseguire una scansione manuale completa il prima possibile, quindi di configurare una scansione pianificata a intervalli regolari. È possibile interrompere o posticipare sia scansioni pianificate che manuali.

In un client gestito, la scansione predefinita viene eseguita ogni giorno alle ore 8:00 con l'opzione di riparazione automatica disattivata.

Esecuzione di una scansione manuale

Per configurare scansioni pianificate:

1. Nel client Symantec Endpoint Protection, nella pagina **Avanzate**, fare clic sull'opzione di **protezione del Mac**, quindi fare clic sull'icona delle impostazioni delle **scansioni pianificate**.
2. Nella finestra di dialogo visualizzata, fare clic su **Aggiungi scansioni pianificate** oppure su una scansione pianificata corrente, quindi selezionare **Modifica** per regolare le impostazioni per tale scansione.
3. Nella scheda **Elementi scansione** è possibile impostare le seguenti opzioni:

Unità	È possibile scegliere se eseguire la scansione dei **dischi rigidi** o delle **unità rimovibili**.
Cartelle	È possibile eseguire la scansione di **Home directory (utente attivo)**, della cartella **Applicazioni** e dei file della **Libreria**. Se nessun utente ha effettuato l'accesso al momento della scansione pianificata di una cartella Home, la scansione non viene eseguita.
Opzioni di scansione	Sono disponibili le seguenti opzioni: • **Esegui scansione di file compressi** • **Riparazione automatica** • **Quarantena automatica** • **Scansione nei tempi di inattività**

4. Nella scheda **Pianificazione scansione** è possibile impostare le seguenti opzioni:

Pianificazione scansione	È possibile configurare una scansione affinché venga eseguita a un intervallo specifico in ore, quotidianamente, settimanalmente o mensilmente. **Esegui a un intervallo specifico** è l'opzione predefinita quando si pianifica una nuova scansione.
Esegui ogni	Disponibile quando l'opzione **Esegui a un intervallo specifico** è selezionata per **Pianificazione scansione**.
Ora di inizio	Disponibile quando si seleziona **Giornaliera**, **Settimanale** o **Mensile** per la pianificazione della scansione. È possibile selezionare l'ora di esecuzione della scansione. Si consiglia di scegliere un'ora in cui normalmente non si è al lavoro, perché le scansioni possono rallentare le prestazioni del computer.

Attivata	Disponibile quando si seleziona **Settimanale** o **Mensile** per la pianificazione della scansione. È possibile selezionare il giorno della settimana o il mese di esecuzione della scansione. Si consiglia di scegliere un periodo in cui normalmente non si è al lavoro, perché le scansioni possono rallentare le prestazioni del computer.

5. Nella scheda **Sintonizzazione**, è possibile modificare la modalità di ottimizzazione delle prestazioni della scansione.
6. Fare clic su **OK**.
7. Fare clic su **Fine**.

Sospensione, posticipo e interruzione di scansioni

Gestione della protezione Mac con Symantec Endpoint Protection

Risposta a messaggi riguardanti infezioni e rilevamenti di rischi

Attivazione o disattivazione dell'invio di informazioni sulla sicurezza a Symantec

Esecuzione di una scansione manuale

Potrebbe essere necessario eseguire la scansione manuale di alcuni file. Ad esempio, si potrebbe voler eseguire la scansione dei file salvati nel computer prima dell'installazione di Symantec Endpoint Protection, oppure si potrebbe decidere di esaminare alcuni file esclusi da una scansione pianificata.

> **NOTE**
> È possibile interrompere o posticipare sia scansioni pianificate che manuali.

Per eseguire una scansione manuale:

Nel client Symantec Endpoint Protection, nella pagina **Scansioni**, effettuare una delle seguenti operazioni:

- Per avviare una scansione rapida, fare clic su **Scansione rapida**, quindi selezionare **Avvia una scansione rapida**.
- Per avviare una scansione completa, fare clic su **Scansione completa**, quindi selezionare **Avvia una scansione completa**.
- Per eseguire la scansione di un file o di una cartella, fare clic su **Scansione file**, quindi su **Seleziona un file**.Viene visualizzato il Finder ed è possibile scegliere di **visualizzare i file nascosti** oppure **eseguire la scansione dei file compressi**. È inoltre possibile attivare le opzioni **Ripara automaticamente** e **Quarantena automatica**.

Sospensione, posticipo e interruzione di scansioni

Configurazione delle scansioni pianificate

Attivazione o disattivazione dell'invio di informazioni sulla sicurezza a Symantec

Sospensione, posticipo e interruzione di scansioni

La funzionalità di pausa consente di interrompere una scansione e di riprenderla in un altro momento. È possibile interrompere e annullare una scansione in qualsiasi momento. Per utilizzare queste funzioni, non è necessario disporre di privilegi di amministratore.

Quando una scansione si riattiva, si avvia da dove si era arrestata la scansione.

> **NOTE**
> Se si sospende una scansione mentre è in corso la scansione di un file compresso da parte di un client, potrebbero essere necessari parecchi minuti per rispondere alla richiesta di interruzione.

È anche possibile posticipare una scansione, se tale funzionalità è attivata, ma solo prima dell'inizio della scansione. Non è possibile posticipare una scansione in corso.

Per sospendere o interrompere una scansione pianificata in esecuzione:

1. Nella finestra di dialogo dell'avanzamento della scansione, fare clic su **Sospendi**.
2. Nella finestra di dialogo dell'avanzamento della scansione, fare clic su **Riprendi** per continuare la scansione oppure su **Interrompi** per interromperla. È inoltre possibile fare clic su **Fine** per chiudere la finestra.

Per sospendere o interrompere una scansione manuale in esecuzione:

1. Nella finestra di dialogo dell'avanzamento della scansione, fare clic su **Sospendi** per sospendere la scansione.
2. Fare clic su **Annulla** per interrompere una scansione manuale in esecuzione o su **Riprendi** per procedere con la scansione.

Per posticipare una scansione che sta per iniziare:

1. Nella finestra visualizzata, fare clic sul menu a discesa per selezionare un valore per il posticipo. È possibile posticipare la scansione di soltanto 15 minuti o anche di un giorno.
2. Fare clic su **OK** per sospendere la scansione.

   Se si intende eseguire la scansione come previsto, non è necessario effettuare alcuna operazione.

Configurazione delle scansioni pianificate

Esecuzione di una scansione manuale

Risposta a messaggi riguardanti infezioni e rilevamenti di rischi

È possibile verificare se il computer è infetto ed eseguire attività aggiuntive se si desidera ottenere maggiore sicurezza o prestazioni migliori.

L'amministratore può gestire il client oppure eseguire un client non gestito. Le attività di protezione svolte dipendono dalla misura del controllo esercitato dall'amministratore sul client.

Se Symantec Endpoint Protection individua un virus o un rischio per la sicurezza, è possibile che venga chiesto di intervenire su tale rischio. In base alle impostazioni scelte dall'amministratore, è possibile che si venga informati automaticamente sull'azione intrapresa dal client.

Table 7: Risposta a messaggi riguardanti infezioni

Contenuto del messaggio	Azione obbligatoria
File infetti riparati	Nessuna
Viene richiesta l'approvazione dell'utente per riparare il file infetto.	Approvare la riparazione. Questa opzione dipende dalle preferenze di Auto-Protect. Gestione delle impostazioni della protezione antivirus e antispyware Se l'opzione di riparazione automatica dei file infetti non è selezionata, l'utente deve riparare il file manualmente. Riparazione di file infetti
Impossibile riparare i file infetti	Gestire i file infetti in quarantena. Gestione dei file in quarantena

In che modo le protezioni antivirus e antispyware proteggono il Mac

Riparazione di file infetti

Se un file infetto non viene riparato o collocato in quarantena automaticamente, è possibile ripararlo dall'elenco dei risultati della scansione. È possibile riparare manualmente i file nel disco rigido del computer o su supporto rimovibile.

Per riparare i file infetti:

1. Nell'elenco dei risultati della scansione, selezionare il file da riparare e scegliere **Ripara**.

   È inoltre possibile fare clic con il pulsante destro del mouse su qualsiasi file nel **Finder del Mac** o nel menu **Cerca**.
2. Ripetere se necessario.
3. Eseguire un'altra scansione per controllare che non vi siano altri file infetti.
4. Verificare i file riparati per assicurarsi che funzionino correttamente.

Gestione delle impostazioni della protezione antivirus e antispyware

Gestione dei file in quarantena

Gestione dei file in quarantena

Per impostazione predefinita, se il client rileva un virus in un file, prova a rimuoverlo. Se non è possibile rimuovere il virus, il file viene trasferito in quarantena. Se Symantec Endpoint Protection rileva un rischio per la sicurezza in un file, per prima cosa lo mette in quarantena e gli effetti del rischio vengono quindi riparati.

Quando il computer viene aggiornato con le nuove definizioni dei virus, il client verifica automaticamente l'area di quarantena. È possibile sottoporre di nuovo a scansione gli elementi nell'area di quarantena. Le definizioni più recenti potrebbero consentire di pulire o riparare i file precedentemente messi in quarantena.

Per gestire i file in quarantena:

1. Nel client Symantec Endpoint Protection, nella pagina **Avanzate**, fare clic su **Attività > Cronologia sicurezza > Quarantena**.
2. Selezionare il file che si desidera gestire, quindi scegliere l'opzione appropriata:

Ripara	Scegliere questa opzione per tentare di riparare un file in quarantena. Verificare che le definizioni dei virus siano successive alla data di messa in quarantena del file.
Elimina	Scegliere questa opzione per eliminare i file non più necessari dalla quarantena.
Ripristina	Se si ha la certezza che il file in quarantena non contenga virus, è possibile ripristinarlo nella posizione originale del computer. Questa opzione non esegue la scansione del file e non tenta di ripararlo.

Risposta a messaggi riguardanti infezioni e rilevamenti di rischi

Attivazione o disattivazione dell'invio di informazioni sulla sicurezza a Symantec

Symantec Endpoint Protection può inviare a Symantec informazioni pseudonimizzate sulle minacce rilevate. Symantec utilizza queste informazioni per proteggere i computer client da minacce recenti, mirate e in evoluzione. I dati inviati migliorano la capacità di Symantec di rispondere alle minacce e di personalizzare la protezione per il computer.

I dati di telemetria raccolti da Symantec possono includere elementi pseudonimizzati che non sono identificabili direttamente. Symantec non necessita né desidera utilizzare i dati di telemetria per identificare i singoli utenti.

Per impostazione predefinita, il computer client invia informazioni sulle rilevazioni a Symantec. È possibile disattivare l'invio sebbene Symantec consigli di lasciare attivata questa impostazione.

Questa opzione invia solamente informazioni sulle rilevazioni di virus.

NOTE
Symantec consiglia di lasciare l'opzione attivata.

Per attivare o disattivare l’invio a Symantec di informazioni anonime sulla sicurezza:

Nel client Symantec Endpoint Protection, nella pagina **Avanzate**, fare clic su **Impostazioni prodotto**, quindi attivare o disattivare **l'invio delle informazioni sulla sicurezza**.

Configurazione delle scansioni pianificate

Esecuzione di una scansione manuale

Gestione della prevenzione delle intrusioni

Le impostazioni predefinite per la prevenzione delle intrusioni hanno lo scopo di proteggere il client Mac. Tuttavia, se si desidera gestire la propria protezione, è possibile gestire la prevenzione delle intrusioni come parte di Protezione dalle minacce di rete.

Table 8: Gestione della prevenzione delle intrusioni

Passaggi	Descrizione
Passaggio 1: Informazioni sulla prevenzione delle intrusioni.	È importante comprendere come gli attacchi di rete vengono rilevati e bloccati dalla prevenzione delle intrusioni. In che modo la Protezione dalle minacce di rete protegge il Mac
Passaggio 2: Download delle firme IPS più recenti.	Per impostazione predefinita, le firme più recenti vengono scaricate nel client. È tuttavia possibile scaricare immediatamente le firme. Aggiornamento immediato del contenuto in Symantec Endpoint Protection
Passaggio 3: Attivazione o disattivazione della prevenzione delle intrusioni.	Può essere necessario disattivare la prevenzione delle intrusioni per la risoluzione dei problemi o se il computer client rileva un numero eccessivo di falsi positivi. Normalmente si consiglia di non disattivare la prevenzione delle intrusioni. Attivazione o disattivazione della Protezione dalle minacce di rete
Passaggio 4: Attivazione delle notifiche di prevenzione delle intrusioni.	È possibile configurare le notifiche in modo che vengano visualizzate quando Symantec Endpoint Protection rileva un attacco. Attivazione o disattivazione delle notifiche di Protezione dalle minacce di rete

Gestione della protezione del firewall per il client Mac

Il firewall Symantec Endpoint Protection per Mac fornisce una protezione firewall che si integra completamente con Symantec Endpoint Protection e include eventi, politiche e comandi. Il firewall Symantec Endpoint Protection è disponibile solo per i client gestiti.

NOTE
Il firewall Symantec Endpoint Protection per Mac non si integra con il firewall incorporato del sistema operativo. Viene eseguito in parallelo. Il firewall del sistema operativo ispeziona il livello applicazione, mentre il firewall Symantec Endpoint Protection ispeziona i livelli inferiori (IP e trasporto).Il firewall Symantec Endpoint Protection per Mac non dispone di regole di blocco peer-to-peer, anche se tali regole possono essere implementate in parte mediante regole firewall personalizzate.

Table 9: Gestione della protezione firewall

Passaggi	Descrizione
Passaggio 1: Ulteriori informazioni sulla protezione firewall.	Informazioni su come la protezione firewall implementa il monitoraggio del traffico e la protezione da attacchi comuni. In che modo la Protezione dalle minacce di rete protegge il Mac
Passaggio 2: Attivazione o disattivazione del firewall.	Può essere necessario disattivare il firewall per la risoluzione di problemi, ad esempio se viene bloccato il traffico che normalmente sarebbe consentito. In genere la disattivazione del firewall non è necessaria. Attivazione o disattivazione di Protezione dalle minacce di rete

Attivazione o disattivazione di Protezione dalle minacce di rete

In genere quando si disattivano i componenti di Protezione dalle minacce di rete il computer è meno sicuro. Tuttavia, può essere necessario disattivare la prevenzione delle intrusioni per evitare falsi positivi o disattivare il firewall per risolvere problemi di blocco del traffico. La prevenzione delle intrusioni e il firewall fanno parte di Protezione dalle minacce di rete.

Per i client gestiti, il controllo che si ha su queste impostazioni dipende da come l'amministratore ha configurato il client. Inoltre, tutte le modifiche applicate a queste impostazioni possono ritornare a ciò che indica la politica al successivo heartbeat.

Per i client non gestiti, il firewall non è disponibile.

Per attivare o disattivare la Protezione dalle minacce di rete:

1. Nel client Symantec Endpoint Protection, nella pagina **Avanzate**, fare clic su **Protezione dalle minacce di rete**.
2. Per attivare o disattivare la prevenzione delle intrusioni, fare clic su **Prevenzione delle intrusioni**.
3. Per abilitare o disabilitare il **firewall** sarà necessario attivarlo o disattivarlo.
4. Per abilitare o disabilitare le notifiche per la prevenzione delle intrusioni e il firewall, fare clic sull'icona delle impostazioni della **protezione delle vulnerabilità**, quindi selezionare o deselezionare l'opzione di **visualizzazione delle notifiche di protezione della vulnerabilità** nella finestra di dialogo corrispondente.
5. Fare clic su **Fine**.

Se si disattivano questi componenti è consigliabile riattivarli appena possibile per garantire la massima protezione del computer.

Gestione della prevenzione delle intrusioni

Gestione della protezione del firewall per il client Mac


Symantec
A Division of Broadcom