SOPHOS

Cybersecurity made simple.

Sophos Endpoint Security and Control

Guida per installazioni in sistemi distribuiti per fornitori di servizio gestito

Versione prodotto: 5.5

Sommario

1 Informazioni sulla guida

Questa guida si rivolge ai provider di servizi gestiti (MSP) che offrono ai clienti Sophos Endpoint Security and Control gestito. Descrive come impostare Sophos Endpoint Security and Control (SESC) in modo da poterlo gestire in remoto per conto di un cliente (oltre che proteggere i propri computer) in sistemi distribuiti.

Nota
Se si desidera utilizzare un server singolo piuttosto che un sistema distribuito, consultare la guida ai provider di servizi gestiti per server singolo di Sophos Endpoint Security and Control.

In questa guida si presuppone che si conosca e si stia utilizzando un sistema di monitoraggio e gestione remota (remote monitoring and management system, o RMM), quale Kaseya, N-able, LevelPlatforms o Zenith, per offrire ai propri clienti e utenti servizi remoti di installazione, gestione e monitoraggio del software.

Si consiglia la lettura di questa guida e di consultare il proprio Sophos Sales Engineer per informazioni e supporto. Se non si è stati ancora assegnati a un Sales Engineer di riferimento, contattate il proprio responsabile commerciale Sophos.

La documentazione di Sophos è pubblicata alla pagina web http://www.sophos.com/it-it/support/documentation.aspx.

2 Il software Sophos

Questa sezione descrive i prodotti Sophos necessari per gestire in modo efficace la protezione dei computer:

- Sophos Enterprise Console
- Sophos Update Manager
- Sophos Endpoint Security and Control

2.1 Sophos Enterprise Console

Sophos Enterprise Console è un tool di amministrazione che distribuisce e gestisce i software per endpoint Sophos utilizzando gruppi e criteri. Fornisce, inoltre, allarmi e report dettagliati sullo stato dei computer e sulle minacce rilevate.

Sophos Enterprise Console include e gestisce Sophos Update Manager.

2.1.1 Reporting Interface e Log Writer

Sophos Reporting Interface e Sophos Reporting Log Writer sono tool aggiuntivi utilizzabili congiuntamente con Sophos Enterprise Console. Consentono l'utilizzo di software di reportistica e monitoraggio prodotti da terzi che generano report sui dati relative a minacce ed eventi in Sophos Enterprise Console. Per maggiori informazioni, consultare:

- La pagina Web dedicata alla documentazione relativa a Sophos Reporting Interface
- La pagina Web dedicata alla documentazione relativa a Sophos Reporting Log Writer
- Articolo 112873

2.2 Sophos Update Manager

Sophos Update Manager scarica automaticamente, direttamente da Sophos, software e aggiornamenti in un percorso centrale. Consente di accedere agli aggiornamenti collocandoli in cartelle di aggiornamento condivise. I computer endpoint si possono quindi aggiornare direttamente da queste cartelle.

Sophos Update Manager può essere installato come parte di Sophos Enterprise Console o separatamente. L'installazione di sicurezza per un endpoint gestito richiede due copie dell'Sophos Update Manager, *padre* e *figlio*. L'Sophos Update Manager padre ottiene gli aggiornamenti da Sophos utilizzando Internet. L'Sophos Update Manager figlio ottiene gli aggiornamenti dall'Sophos Update Manager padre.

I computer dei clienti ricevono gli aggiornamenti dall'Sophos Update Manager figlio. Se si proteggono computer localizzati nella rete LAN con il software di sicurezza Sophos, tali computer riceveranno aggiornamenti dall'Sophos Update Manager padre.

2.3 Sophos Endpoint Security and Control

Sophos Endpoint Security and Control (SESC) si riferisce sia all'intera suite di software di sicurezza Sophos, come descritto in questa sezione, sia all'agente che viene eseguito sui computer endpoint, proteggendoli ed interagendo con i tool di amministrazione.

Sophos Endpoint Security and Control (per endpoint) comprende i seguenti componenti:

- Sophos AutoUpdate: si auto-aggiorna e aggiorna anche gli altri componenti da Sophos Update Manager.
- **Sophos Remote Management System** (RMS): gestisce la comunicazione con Sophos Enterprise Console tramite TCP sulle porte 8192 e 8194.
- Sophos Anti-Virus: include funzioni di antivirus, HIPS, controllo dati e controllo dispositivi.
- **Protezione web** (opzionale): offre una protezione ancora più efficace contro le minacce del web. Include le seguenti funzioni:
  - Filtraggio URL in tempo reale: consente di bloccare l'accesso a siti web noti per ospitare malware. Questa funzione opera una ricerca in tempo reale all'interno del database online di Sophos in cui vengono raccolti i siti web infetti.
  - Scansione del contenuto: esegue la scansione dei dati e dei file scaricati da Internet (o Intranet) e rileva contenuto malevolo in modo proattivo. Questa funzione esegue la scansione di contenuti ospitati in qualsiasi percorso, compresi quelli non facenti parte del database dei siti web infetti.
    - Grazie al controllo dei siti web (opzionale), è possibile controllare l'utilizzo del web da parte degli utenti, in base a 14 categorie di siti web: Adulti/Sessualmente esplicito, Alcool e tabacco, Anonimizzatore Proxy, Attività criminali, Azzardo, Hacking, Sostanze illecite, Intolleranza e razzismo, Phishing e truffe, URL di spam, Spyware, Cattivo gusto/Offensivo, Violenza e Armi.
- **Sophos Client Firewall** (opzionale): permette l'accesso alla rete o a Internet solo alle applicazioni o alle classi di applicazioni specificate.
- **Sophos Patch** (opzionale): Sophos Enterprise Console consente di verificare che i computer abbiano sempre installate le patch di protezione più recenti. SophosLabs fornisce livelli di valutazione delle minacce che consentono di determinare i problemi critici relativi alle patch, per poterli risolvere il più rapidamente possibile. I livelli di minaccia forniti da SophosLabs prendono in considerazione i fenomeni più recenti e possono quindi non corrispondere ai livelli di pericolosità stabiliti dai fornitori.

3 Funzionamento di Sophos Endpoint Security and Control per fornitori di servizio gestito

Sophos Endpoint Security and Control gestito opera nel modo illustrato di seguito:

I **fornitori di servizio gestito** (Managed Service Provider, o MSP) offrono servizi informatici gestiti a **clienti** remoti tramite Internet.

Sophos Enterprise Console (SEC) viene eseguito nel server ospitato dai fornitori (nel *server SEC*). In questo modo è possibile gestire gruppi di computer e criteri di sicurezza, oltre che visualizzare dettagliatamente lo stato dei computer ed eventuali allarmi.

Sophos Update Manager (SUM padre) viene eseguito nel server SEC. Ottiene i file di installazione del software e gli aggiornamenti da Sophos e li pubblica in cartelle condivise nella rete LAN.

Sophos Update Manager (SUM figlio) è in esecuzione su un server web nel propria DMZ (*Sophos DMZ Server*). Si procura i file di installazione del software e gli aggiornamenti da SUM e li pubblica in cartelle condivise nel DMZ.

è necessario che il server Sophos DMZ esegua anche il server web Microsoft IIS (Internet Information Services), per poter pubblicare su Internet, utilizzando HTTP, le cartelle di aggiornamento condivise di Sophos.

Sophos Endpoint Security and Control (SESC) viene eseguito nel server SEC, nel server Sophos DMZ e nei computer dei clienti, per proteggerli da eventuali minacce e inviare report a Sophos Enterprise Console.

Sophos Endpoint Security and Control include **Sophos AutoUpdate** (SAU), che si aggiorna direttamente dalle cartelle condivise gestite dal SUM installato nel server di Sophos Enterprise Console su HTTP (tramite IIS).

Remote Management System (RMS) viene eseguito su tutti i computer (compresi server di Sophos Enterprise Console e client) mettendo a disposizione modalità di comunicazione bidirezionale per criteri, stato dei client e allarmi.

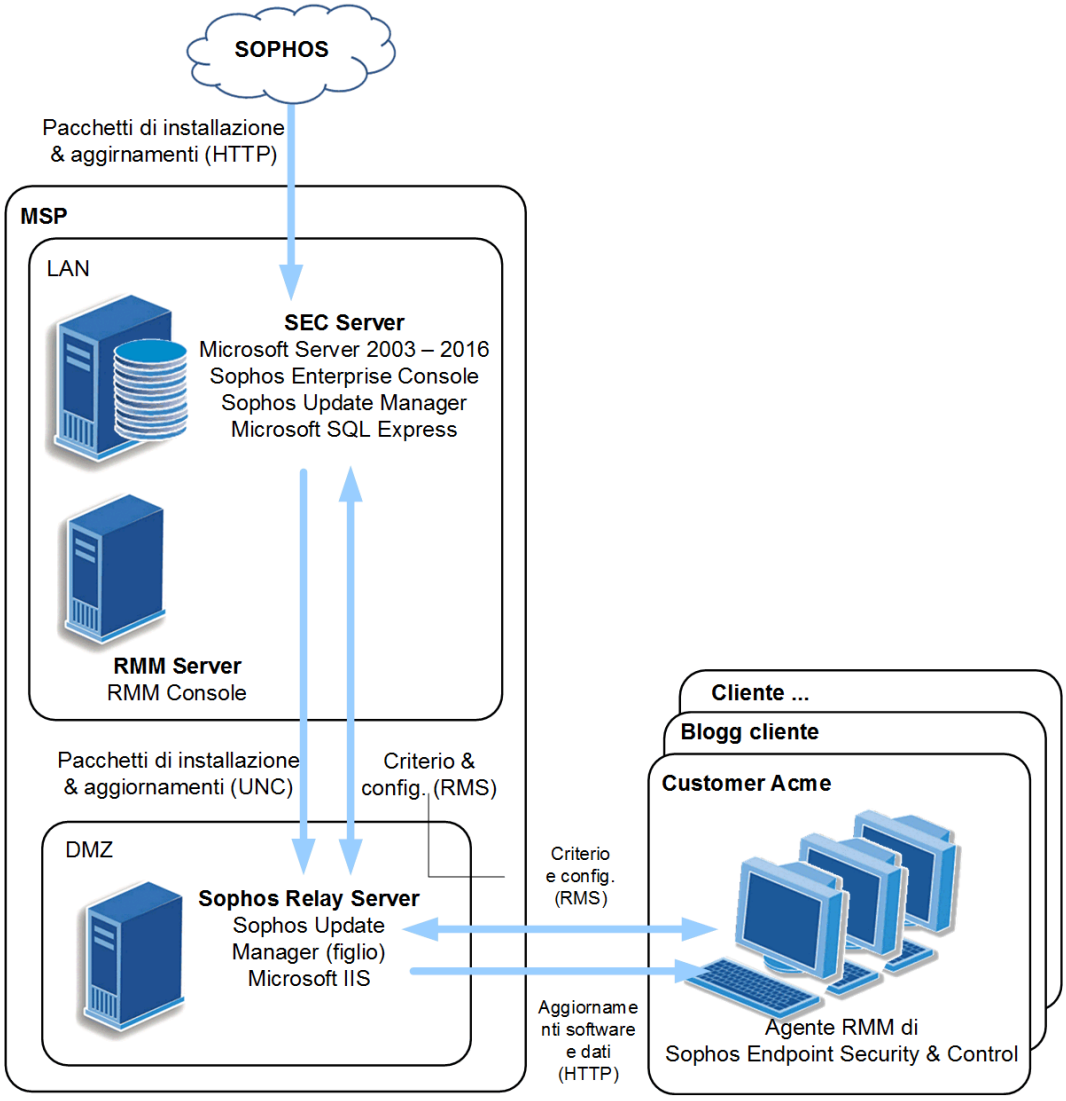
Il sistema di monitoraggio remoto (RMM) (ad esempio Kaseya) consiste in una console per MSP, oltre che in agenti installati su ciascun computer gestito.

Il sistema RMM:

- Distribuisce un pacchetto di installazione personalizzato di Sophos Endpoint Security and Control a tutti i computer endpoint.
- Esegue tale pacchetto e installa Sophos Endpoint Security and Control in tutti i computer endpoint.
- Esegue regolarmente uno script su ciascun computer che invii richieste a Sophos Endpoint Security and Control, consentendo alla console RMM di visualizzarne lo stato ed eventuali allarmi.
- Gestisce nello stesso modo anche ad altri software per endpoint prodotti da terzi.

Esistono molti prodotti RMM commercializzati da diversi fornitori e pensati per situazioni e applicazioni specifiche.

La configurazione e i metodi di comunicazione fra i componenti di RMM sono di proprietà riservata e non rientrano nelle competenze di questa guida.



Nota

è inoltre possibile scegliere di proteggere altri computer nella rete LAN di MSP, come descritto nella sezione Protezione di server di Sophos Enterprise Console (pagina 13); per questioni di chiarezza, ciò non verrà però illustrato in questa guida. Allo stesso modo, le modalità di comunicazioni di rete dei RMM sono diverse a seconda del sistema utilizzato e per questo non verranno trattate in questa guida.

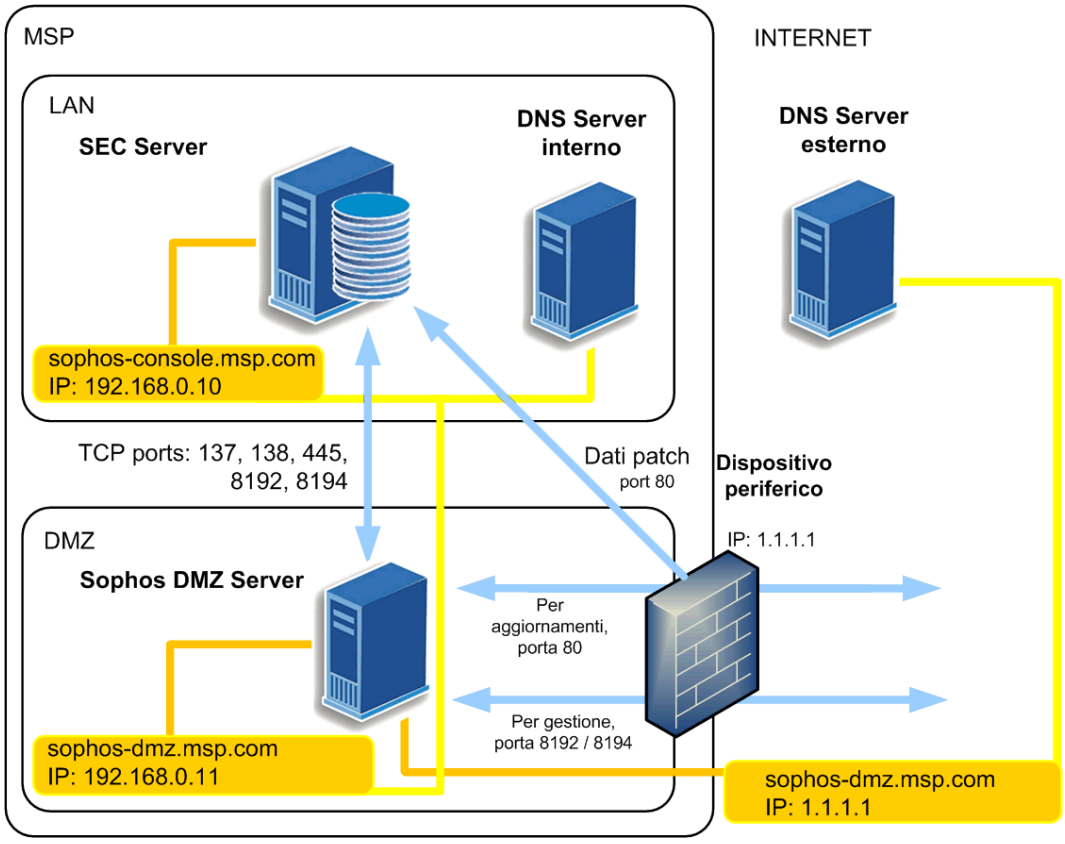
Nota

A partire dalla versione 5.4.0, Sophos Enterprise Console (incluso il componente della console di gestione remota) non è più supportata su Windows Server 2003, Windows Server 2003 R2, Windows XP e Windows Vista.

4 Modalità di gestione dei client da parte di server di Sophos Enterprise Console

Questa sezione spiega come configurare i diversi componenti di rete per abilitare la comunicazione fra server di Sophos Enterprise Console, Sophos DMZ Server e gli endpoint gestiti dei clienti.

Il diagramma qui sotto mostra l'interazione fra i diversi server, domini, porte, indirizzi IP interni ed esterni. Gli indirizzi IP riportati nel diagramma sono solamente esempi, e devono essere sostituiti con indirizzi IP veri.



Il Sophos DMZ Server viene riferito, sia internamente che esternamente, allo stesso nome di dominio, sophos-dmz.msp.com. I server DNS interni ed esterni invece riconducono sophos-dmz.msp.com a differenti indirizzi IP, come mostrato di seguito.

Si presuppone che il sito web della directory virtuale utilizzi la porta 80 per le connessioni in ingresso. Tutte le porte citate nell'esempio qui sopra sono porte TCP.

Nell'esempio, il dispositivo periferico ha l'indirizzo IP 1.1.1.1 che corrisponde all'interfaccia esterna del firewall. Le porte 80, 8192 e 8194 vengono nattate utilizzando questa interfaccia.

Se si desidera utilizzare Sophos Patch, nel dispositivo periferico sarà necessario configurare il Proxy inverso in modo che reindirizzi al server di Sophos Enterprise Console tutto il traffico che corrisponde all'indirizzo http://<1.1.1.1>/Sophos/Management/Patch/EndpointCommunicator/.

Si consiglia l'utilizzo di un Proxy di cache trasparente nella rete dei clienti per limitare il traffico dovuto agli aggiornamenti delle patch o dei computer endpoint.

Nota
Se necessario è possibile utilizzare porte alternative, per esempio nel caso in cui un'altra applicazione sia già collegata alla porta 80. Quando si esegue la configurazione degli aggiornamenti del client, il percorso di riferimento deve essere indicato nel formato standard Per esempio, se si desidera utilizzare la porta 8085, il percorso di aggiornamento deve essere: http://sophos-dmz.msp.com:8085/sophos.

4.1 Requisiti di rete

Tutti i computer, incluso il server di Sophos Enterprise Console, devono riuscire a risolvere il nome di dominio completo (FQDN). Se il server utilizza un indirizzo IP privato (RFC 1918), ma è raggiungibile pubblicamente tramite NAT, sophos-dmz.msp.com si risolve con l'indirizzo IP interno del Sophos DMZ Server (per es. 192.168.0.2). Per i computer remoti, il FQDN si risolve con l'indirizzo IP esterno del Sophos DMZ Server (per es. 1.1.1.1).

1. Creare un record DNS A, denominato sophos-dmz.msp.com, SIA per i sistemi DNS interni SIA per quelli esterni, come mostrato qui di seguito:
   a) Creare un record dell'indirizzo interno che punti all'indirizzo IP interno del Sophos DMZ Server (per es. 192.168.0.11)
   b) Creare un record DNS A esterno (Internet) che si risolva con l'interfaccia pubblica del Sophos DMZ Server (per es. 1.1.1.1).
2. Configurare il firewall Internet del Sophos DMZ Server, in modo da reindirizzare (con NAT) le porte TCP 8192 e 8194.

5 Passaggi chiave

I passaggi chiave sono:

- Installare Sophos Enterprise Console su uno dei server ospitati (server di Sophos Enterprise Console). È incluso anche Sophos Update Manager padre.
- Collegarsi a Sophos e scaricare il software di sicurezza richiesto.
- Proteggere il server di Sophos Enterprise Console con il software di sicurezza Sophos.
- Impostare il proprio DMZ modificando il file di configurazione, installando Update Manager figlio cambiando i valori di registro.
- Pubblicare la cartella condivisa da cui i computer dei clienti possono aggiornarsi.
- Configurare il server di Sophos Enterprise Console creando gruppi per ciascun cliente e adattando i criteri di aggiornamento.
- Verifica delle configurazioni
- Proteggere il Sophos DMZ Server con il software di sicurezza Sophos.
- Creare un pacchetto di installazione.
- Controllare il pacchetto di installazione.
- Distribuire tale pacchetto di installazione ai computer dei clienti (utilizzando il sistema RMM).
- Gestire il software di sicurezza per endpoint.

6 Installazione di Sophos Enterprise Console sul server di Sophos Enterprise Console

Le seguenti istruzioni spiegano come eseguire l'installazione di Sophos Enterprise Console nel server di Sophos Enterprise Console.

6.1 Prepararsi per l'installazione di Sophos Enterprise Console

Nel server che risponde ai requisiti di sistema relativi ai server di Sophos Enterprise Console (v. l'articolo 118635 della knowledge base):

1. Assicurarsi che sia connesso a Internet.
2. Accertarsi di avere accesso all'installazione del sistema operativo Windows e di essere in possesso dei CD relativi ai Service Pack. Potrebbero essere richiesti durante l'installazione.
3. Se la versione di Microsoft SQL Server del server di Sophos Enterprise Console è precedente alla 2005 SP4, effettuarne l'upgrade. In caso contrario, SQL Server Express è incluso in Sophos Enterprise Console (SQL Server Express 2012 SP4 è incluso in Sophos Enterprise Console 5.5.1).
4. Se il server sta eseguendo Windows Server 2008 o successivo, disattivare il "Controllo account utente" (UAC) e riavviare il server.
   Una volta completata l'installazione e il download del software di sicurezza, sarà possibile riattivare lo UAC.

6.2 Installazione di Sophos Enterprise Console

Per installare Sophos Enterprise Console:

1. Accedere come amministratore:
   a) Se il computer si trova in un dominio, accedere come amministratore di dominio.
   b) Se il computer si trova in un gruppo di lavoro, accedere come amministratore locale.
2. Andare alla pagina web relativa ai download, citata nell'e-mail di registrazione/download
3. Eseguire il download del pacchetto di installazione di Sophos Enterprise Console.
4. Cliccare due volte sul pacchetto scaricato.
5. Nella finestra di dialogo **Sophos Enterprise Console**, cliccare su **Avanti**. Una procedura guidata accompagna nei passaggi dell'installazione. È necessario procedere come illustrato di seguito:
   a) Accettare le impostazioni predefinite dove possibile.
   b) Nella finestra di dialogo **Selezione dei componenti**, selezionare tutti e tre i componenti: **Management Server**, **Management Console** e **Database**.
6. Una volta portata a termine l'installazione, potrebbe essere richiesto IL riavvio del computer. Cliccare su **Sì** o su **Fine**.

Per ulteriori informazioni sull'installazione e l'impostazione dei criteri, consultare la *Guida di avvio rapido di Sophos Enterprise Console* e la *Guida all'impostazione dei criteri di Sophos Enterprise Console*.

7 Scaricamento del nuovo software di sicurezza da Sophos

Quando si riaccede alla console (o quando essa viene riavviata) per la prima volta dopo averne eseguito l'installazione, Sophos Enterprise Console si apre automaticamente e ha inizio la procedura guidata per la selezione e il download del software di sicurezza per computer endpoint.

Se si è utilizzato Remote Desktop per eseguire l'installazione di Sophos Enterprise Console, la console non si aprirà automaticamente. Aprirla dal menu Start.

Durante l'esecuzione della procedura guidata:

1. Nella pagina **Dettagli dell'account di download di Sophos**, digitare il nome utente e la password dell'allegato di licenza Sophos. Se si accede a Internet tramite server proxy, selezionare la casella di spunta **Accedi a Sophos tramite server proxy** e inserire le proprie impostazioni proxy.
2. Nella pagina **Selezione piattaforma**, selezionare solo le piattaforme che si desidera proteggere subito.

   Quando si clicca su **Avanti**, Sophos Enterprise Console comincia a scaricare il software.

   Nota
   sarà poi possibile aggiungere altre piattaforme modificando la sottoscrizione al software nella vista di Update Manager

3. Nella pagina **Download del software**, viene visualizzato l'avanzamento del download. Cliccare su **Avanti** in qualsiasi momento.
4. Se si desidera proteggere i computer presenti nella rete LAN utilizzando il software di sicurezza Sophos ed essere in possesso della relativa licenza, nella pagina **Importa computer da Active Directory** selezionare **Imposta gruppi per i computer**.

Viene, in questo modo, creata una cartella di installazione condivisa nel server di Sophos Enterprise Console, contenente versioni installabili del software Sophos per computer endpoint relative a tutti i sistemi operativi che si desidera proteggere. Viene condivisa come `\\<SEC-Server>\SophosUpdate\CIDs`. La fonte della condivisione si trova nella seguente cartella:

Windows Server	Percorso predefinito
2003	C:\Documents and Settings\All Users\Application Data\Sophos\Update Manager\Update Manager\CIDs\
2008, 2008 R2, 2012, 2012 R2, 2016	C:\ProgramData\Sophos\Update Manager\Update Manager\CIDs\

I file di installazione e aggiornamento di Sophos Endpoint Security and Control per Windows sono situati nella sottodirectory `\S000\SAVSCFXP\`.

Nota
È possibile visualizzare il percorso della CID relativa a ogni piattaforma da Sophos Enterprise Console: Nel menu **Visualizza**, cliccare su **Percorsi Bootstrap**.

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

8 Protezione di server di Sophos Enterprise Console

Per fini di test, si consiglia di proteggere il server SEC.

1. Installare Sophos Endpoint Security and Control. Per far ciò, nel computer che si desidera proteggere, eseguire l'installazione dal percorso CID elencato sopra (parte finale della sezione Scaricamento del nuovo software di sicurezza da Sophos (pagina 11)).
2. Verificare che l'installazione sia avvenuta.
   Per far ciò, aprire Enterprise Console. Nella scheda **Stato**, nella colonna **Aggiornato** viene visualizzata la dicitura "sì".

Per ulteriori informazioni sull'installazione di Sophos Endpoint Security and Control, consultare la *Guida all'upgrade di* Sophos Endpoint Security and Control.

9 Impostazione del Sophos DMZ Server

Per impostare il proprio Sophos DMZ Server:

1. Modificare il file di configurazione nel server di Sophos Enterprise Console, in modo tale che possa comunicare col Sophos DMZ Server.
2. Installare Sophos Update Manager in Sophos DMZ Server.
3. Modificare i valori di registro nel Sophos DMZ Server in modo tale che possa comunicare col server di Sophos Enterprise Console e i computer client.

9.1 Modifica del file di configurazione

Nel server di Sophos Enterprise Console:

1. Cercare la cartella SUMInstaller.

Versione di Windows	Percorso predefinito
32 bit	C:\Programmi\Sophos\Enterprise Console\SUMInstaller
64 bit	C:\Program Files (x86)\Sophos\Enterprise Console\SUMInstaller

2. Trovare il file **MRinit.conf** e modificare i valori relativi a **MRParentAddress** e **ParentRouterAddress**.

   MRParentAddress viene utilizzato dal Sophos DMZ Server per connettersi al server di Sophos Enterprise Console, mentre il ParentRouterAddress viene utilizzato dal computer client per connettersi a Sophos DMZ Server.

   Esempio del valore predefinito:

   ```
   "MRParentAddress"="sophos-console.abc.sophos,sophos-console"
   "ParentRouterAddress"="sophos-console.abc.sophos,sophos-console"
   ```

   Esempio del criterio modificato:

   Includere un indirizzo IP accessibile esternamente e il nome di NetBIOS locale relativo al server di Sophos Enterprise Console e al Sophos DMZ Server.

   ```
   "MRParentAddress"="192.168.0.10, sophos-console.msp.com, sophos-
   console"
   "ParentRouterAddress"="sophos-dmz,sophos-dmz.msp.com"
   ```

   Salvare il file e chiuderlo. Un esempio di file MRinit.conf modificato, consultare Appendice: contenuto del file MRinit.conf (pagina 35).

9.2 Installazione di Sophos Update Manager

Questa sezione spiega come eseguire l'installazione dell'Sophos Update Manager figlio su un server presente in DMZ (Sophos DMZ Server), e come configurarlo per poter ottenere aggiornamenti dall'Sophos Update Manager padre, presente nel server di Sophos Enterprise Console.

9.2.1 Preparazione dell'installazione di Sophos Update Manager

Andare al Sophos DMZ Server.

- Verificare che le seguenti porte accettino traffico in entrata e uscita per la rete LAN: 137, 138, 139 e 445.
- Se sul server è in esecuzione una versione di Windows che include la funzione "Individuazione rete" e tale funzione è disattivata, attivarla e riavviare il computer.
- Verificare che il Sophos DMZ Server riesca a copiare i file dal server SEC utilizzando un percorso condiviso, quale \\<sophos-dmz.msp.com>\SophosUpdate\.

Nota

— Le istruzioni sopracitate danno per scontato che si stia utilizzando un collegamento di rete UNC fra il server di Sophos Enterprise Console e Sophos DMZ Server. Per informazioni su altri protocolli di rete, quali HTTP, rivolgersi al proprio responsabile alle vendite di Sophos.

— Se il server sta eseguendo *Windows Server 2008*, disattivare il "Controllo account utente" (UAC) e riavviare il server. Potrà essere riattivato una volta installato il gestore degli aggiornamenti e sottoscritto gli aggiornamenti Sophos.

9.2.2 Installazione di Sophos Update Manager

1. Accedere a Sophos DMZ Server come amministratore.
   a) Se il server si trova in un *dominio*, accedere come amministratore di dominio.
   b) Se il server si trova in un *gruppo di lavoro*, accedere come amministratore locale.
2. Trovare la cartella condivisa `SUMInstallSet` nel server SEC.
   Esempio: \\<sophos-console.msp.com>\SUMInstallSet
3. Cliccare due volte su `Setup.exe` per eseguire il programma di installazione.
4. Nella finestra di dialogo **Sophos Update Manager**, cliccare su **Avanti**.
   Una procedura guidata accompagna nei passaggi dell'installazione. Accettare le opzioni predefinite.

Nel Sophos DMZ Server è stato:

- Installato Sophos Update Manager gestito da Sophos Enterprise Console.
- Creata la cartella di installazione condivisa `\\<sophos-dmz.msp.com>\SophosUpdate\`

I file di installazione nella cartella di installazione condivisa vengono utilizzati per installare Sophos Endpoint Security and Control nel Sophos DMZ Server, oltre che come fonte per la creazione di un pacchetto di installazione.

Andare a Sophos Enterprise Console, nel server di Sophos Enterprise Console, e assicurarsi che il nuovo Sophos Update Manager sia presente sotto "Gestori aggiornamenti". Sottoscrivere il nuovo Sophos Update Manager al pacchetto "consigliato" e impostare il server di Sophos Enterprise Console come sua fonte. Il download del pacchetto in Sophos DMZ Server potrebbe richiedere fino a 15 minuti.

Per informazioni su come apportare modifiche ai criteri di aggiornamento e alle password di Update Manager, consultare l'articolo 65318 della knowledge base.

9.3 Modifica dei valori di registro

In Sophos DMZ Server:

1. Aprire la finestra **Editor del registro di sistema**. Per aprirla, cliccare su **Start**, cliccare su **Esegui**, digitare `regedit` e quindi cliccare su **OK**.
2. Effettuare il backup del registro di sistema.
   Per informazioni su come effettuare il backup del registro di sistema, consultare la documentazione Microsoft.
3. Nella finestra **Editor del registro di sistema**, modificare i **due** valori di registro riportati qui di seguito:
   - Sophos Message Router
   - Router

   Per fare ciò:

   a) Andare alla chiave di registro di Sophos Message Router:

Versione di Windows	Percorso predefinito
32 bit o 64 bit	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sophos Message Router\

   b) Nel riquadro a destra, selezionare la voce **ImagePath**.

   c) Nel menu **Modifica**, cliccare su **Modifica**.

   d) In **Dati valore** modificare il valore come mostrato di seguito:

   - **Computer a 32 bit:**

     Valore predefinito:

     "C:\Program Files\Sophos\Remote Management System\RouterNT.exe" -service -name Router -ORBListenEndpoints iiop://:8193/ssl_port=8194

     Modifica valore:

     Modificare il valore per includere il testo aggiuntivo e il nome di dominio completo risolvibile esternamente, come indicato nelle diciture **in grassetto**.

     "C:\Program Files\Sophos\Remote Management System\RouterNT.exe" -service -name Router **-ORBDottedDecimalAddresses 0** -ORBListenEndpoints iiop://:8193/ssl_port=8194**&hostname_in_ior=sophos-dmz.msp.com**

   - **Computer a 64 bit:**

     Valore predefinito:

"C:\Program Files (x86)\Sophos\Remote Management System\RouterNT.exe" -service -name Router -ORBListenEndpoints iiop://:8193/ssl_port=8194

Modifica valore:

Modificare il valore per includere il testo aggiuntivo e il nome di dominio completo risolvibile esternamente, come indicato nelle diciture **in grassetto**.

"C:\Program Files (x86)\Sophos\Remote Management System\RouterNT.exe" -service -name Router **-ORBDottedDecimalAddresses 0** -ORBListenEndpoints iiop://:8193/ssl_port=8194**&hostname_in_ior=sophos-dmz.msp.com**

e) Cercare la chiave di registro del router:

Versione di Windows	Percorso predefinito
32 bit	HKEY_LOCAL_MACHINE\SOFTWARE\Sophos\Messaging System\Router\
64 bit	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Sophos\Messaging System\Router\

f) Nel riquadro a destra, selezionare la voce **ServiceArgs**.

g) Dal menu **Modifica**, cliccare su **Modifica**.

h) In **Dati valore** modificare il valore come mostrato di seguito:

Valore predefinito:

-ORBListenEndpoints iiop://:8193/ssl_port=8194

Cambiare con:
Modificare il valore per includere il testo aggiuntivo e il nome di dominio completo risolvibile esternamente, come indicato nelle diciture **in grassetto**.

-ORBDottedDecimalAddresses 0 -ORBListenEndpoints iiop://:8193/ssl_port=8194**&hostname_in_ior=sophos-dmz.msp.com**

4. Riavviare il servizio Sophos Message Router.

I seguenti articoli della knowledge base forniscono ulteriori informazioni a riguardo:

- Articolo 50832 (il secondo scenario è solitamente quello più comune)
- Articolo 14635

10 Pubblicazione della cartella di aggiornamento dei clienti

Quando si installa Update Manager, viene creata automaticamente una cartella condivisa denominata "Sophos Update" nel seguente percorso del Sophos DMZ Server `\\<sophos-dmz.msp.com>\SophosUpdate`. Questa cartella deve essere accessibile da http per consentire ai computer dei clienti di utilizzarla per gli aggiornamenti.

1. Andare al server di Sophos Enterprise Console e aprire Sophos Enterprise Console.
2. In Sophos Enterprise Console, selezionare la vista Gestori aggiornamento. Nel Sophos DMZ Server, trovare e cliccare col tasto destro del mouse sul Sophos Update Manager figlio.
3. Dal menu **Visualizza/Modifica configurazione**, selezionare **Sottoscrizioni** ed assicurarsi che il pacchetto consigliato venga sottoscritto a `\\<sophos-dmz.msp.com>\SophosUpdate`.
   Il server di Sophos Enterprise Console comunicherà col Sophos DMZ Server e creerà una nuova cartella condivisa in `SophosUpdate`. Ciò può richiedere fino a un massimo di 15 minuti.
4. Nel Sophos DMZ Server, creare un account *sophosupd* con password complessa e accesso di sola lettura a `SophosUpdate`.
5. Installare e configurare Microsoft IIS nel Sophos DMZ Server e proteggerlo in modo adeguato.
6. In IIS, creare una directory virtuale denominata `SophosUpdate`, con condivisione `\\<sophos-dmz.msp.com>\SophosUpdate`, che attribuisce diritti al nuovo account *sophosupd*.

   Se si utilizza un percorso locale invece che UNC, il percorso della CID predefinito è:

Windows Server	Percorso predefinito
2003	C:\Documents and Settings\All Users\Application Data\Sophos\Update Manager\Update Manager\
2008, 2008 R2, 2012, 2012 R2, 2016	C:\ProgramData\Sophos\Update Manager\Update Manager\

7. Configurare i tipi MIME. Per motivi di test, è possibile aggiungere .* come tipo MIME.

   Per informazioni su come creare una Web CID e configurare i tipi MIME, consultare l'articolo 38238 della knowledge base.

Nota
HTTPS non è supportato per gli aggiornamenti del client. Si consiglia di utilizzare NTLM (autenticazione integrata di Windows) o la funzione "Autenticazione del digest" per verificare che le credenziali siano protette. Queste impostazioni possono essere configurate in IIS in modo tale che i client possano utilizzare automaticamente le opzioni più sicure.

11 Configurazione di server di Sophos Enterprise Console per la gestione dei clienti

Una volta eseguito il download del software di sicurezza, è necessario configurare il server di Sophos Enterprise Console perché gestisca i clienti e i loro computer.

11.1 Creazione di gruppi

I computer vengono organizzati creando gruppi in Sophos Enterprise Console. Si consiglia di creare almeno un gruppo per il fornitore di servizio gestito, e uno per ogni cliente. Se i clienti hanno sistemi che richiedono criteri specifici, all'interno del gruppo relativo a un determinato cliente sarà possibile creare sottogruppi, per esempio "Server" e "Desktop". Ciascun gruppo potrà quindi essere soggetto a criteri specifici. Dividere i computer gestiti in gruppi consente di modificare un determinato criterio di sicurezza per un solo cliente, senza interferire con i computer degli altri clienti o con i propri.

Per creare un nuovo gruppo di computer:

1. Nella vista **Computer,** nel riquadro **Gruppi** (lato sinistro della console), scegliere dove si desidera creare il gruppo.
   Se si desidera creare un nuovo gruppo al livello superiore, cliccare sul nome del computer in alto.
   Se si desidera creare un sottogruppo, cliccare su un gruppo esistente.
2. Cliccare sull'icona **Crea gruppo** posta sulla barra degli strumenti.
   Un "Nuovo Gruppo" viene aggiunto all'elenco, con il nome evidenziato.
3. Digitare il nome del gruppo.
   I criteri vengono applicati automaticamente al nuovo gruppo. È possibile modificare tali criteri oppure applicare criteri differenti.

   Se il nuovo gruppo è un sottogruppo, inizialmente utilizzerà le stesse impostazioni del gruppo nel quale si trova.

Per i propri computer, è possibile importare gruppi da Microsoft Active Directory.

Per informazioni su come impostare i gruppi, consultare la *Guida in linea* di Sophos Enterprise Console e l'articolo 63155 della knowledge base.

11.2 Creazione di criteri aggiornamento

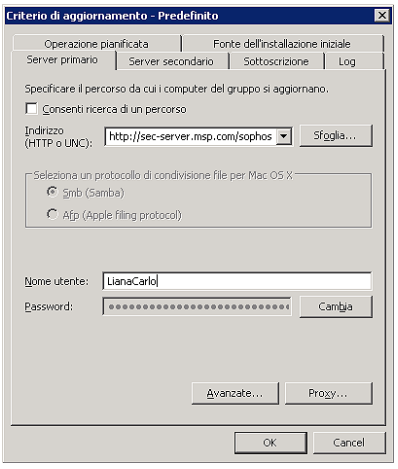
È necessario creare un nuovo criterio di aggiornamento e configurarlo in modo tale da utilizzare l'indirizzo HTTP impostato precedentemente in IIS (Pubblicazione della cartella di aggiornamento dei clienti (pagina 18)).

Per creare un nuovo criterio di aggiornamento:

1. Nel pannello **Criteri**, cliccare col tasto destro del mouse su **Aggiornamento** e selezionare l'opzione **Crea criterio**.
   Inserire il nome di un criterio.
2. Cliccare due volte sul nome del criterio. Nella finestra di dialogo **Criterio di aggiornamento**, nella scheda **Server primario**, inserire l'indirizzo e le credenziali che verranno usate per accedere al

server. L'**indirizzo** deve essere il nome di dominio completo o l'indirizzo IP (per es. http://sophos-dmz.msp.com/SophosUpdate o http://1.1.1.1/SophosUpdate).

Come **Nome utente** e **Password**, inserire le credenziali dell'account utilizzate dai client per scaricare gli aggiornamenti. Si consiglia l'utilizzo di un account personale per ogni cliente, avente diritti di sola lettura.



Se necessario modificare altri dati, quindi cliccare su **OK** per chiudere la finestra di dialogo del Criterio di aggiornamento.

3. Nel riquadro **Gruppi**,selezionare il gruppo che utilizzerà il criterio di aggiornamento configurato semplicemente trascinando il criterio sul gruppo, o cliccando col tasto destro del mouse sul gruppo, quindi cliccando su Visualizza/Modifica dettagli dei criteri di gruppo e infine selezionando il nuovo criterio dall'elenco a discesa relativo agli aggiornamenti.
   Ripetere questa procedura per ciascun gruppo a cui applicare questo criterio di aggiornamento.

12 Verifica delle configurazioni

La configurazione è ora completata. Per verificare che le impostazioni selezionate siano corrette, si consiglia di eseguire i test elencati qui di seguito:

1. Dal Sophos DMZ Server, verificare che sia possibile collegarsi alla porta 8192 utilizzando il nome di dominio completo (FQDN) del server Sophos DMZ.

   Si deve ricevere una risposta che inizi con la dicitura "IOR". Questa operazione può essere eseguita utilizzando un tool quale Telnet. Per esempio, nella finestra del prompt di comando, digitare `telnet sophos-dmz.msp.com 8192`.

   Se ciò non funziona, inserire la dicitura “localhost” al posto del nome di dominio completo (FQDN) per stabilire se si tratta di un problema di routing DNS/IP.

   Ripetere gli stessi passaggi anche per il server di Sophos Enterprise Console. Per esempio, tramite Telnet, nella finestra del prompt di comando, digitare `telnet sec-server 8192`.
2. Dal client esterno, ripetere il passaggio descritto qui sopra per verificare che il server DMZ sia accessibile esternamente. Esempio: digitare `telnet sophos-dmz.msp.com 8192`.
3. Verificare che il sistema di gestione sia configurato col nome di dominio completo (FQDN). Per fare ciò:

   a) Nel server Sophos DMZ Server, aprire l'**Editor del registro di sistema**.
   Per aprirla, cliccare su **Start**, cliccare su **Esegui**, digitare `regedit` e quindi cliccare su **OK**.

   b) Andare alla chiave di registro `HKEY_LOCAL_MACHINE\SOFTWARE`.

   c) Cliccare sul tasto destro del mouse su `SOFTWARE` e quindi su **Cerca**.

   d) In **Oggetto ricerca** inserire il nome di dominio completo del Sophos DMZ Server.

   e) Una volta trovata l'istanza desiderata, premere **F3** per lanciare nuovamente la ricerca e trovare un'altra istanza.

   Nota
   Dovrebbero essere presenti due istanze del nome FQDN.

   Una volta verificato che siano presenti due istanze del nome, chiudere la finestra dell'**Editor del Registro di sistema**.

4. Dal client esterno, verificare che sia possibile collegarsi a IIS dalla porta 80 utilizzando il nome FQDN del Sophos DMZ Server attraverso il browser web. Dalla struttura delle cartelle (oppure, se la "Visualizzazione directory" è disabilitata, indicando il percorso della directory locale) verificare che sia possibile eseguire il download dei file.
   Per esempio, scaricare il file .pem dal momento che non fa parte dell'elenco dei tipi di IIS MIME. Con le impostazioni iniziali predefinite attive, il percorso per il download del file .pem sarà:

   http://<sophos-dmz.msp.com>/SophosUpdate/CIDs/s000/SAVSCFXP/cac.pem

Una volta eseguiti i test citati qui sopra, continuare nella procedura di protezione del Sophos DMZ Server.

13 Protezione di Sophos DMZ Server

È ora necessario proteggere il Sophos DMZ Server in cui si è appena installato Sophos Update Manager.

1. Dal Sophos DMZ Server, eseguire il file di installazione dal percorso della condivisione di installazione presente nel DMZ Server e citato sopra, nella sezione Installazione di Sophos Update Manager (pagina 15).
2. Da Enterprise Console
   a) Impostare il Sophos DMZ Server come membro di un gruppo MSP.
   b) Rendere il Sophos DMZ Server conforme ai criteri.
   c) Verificare che il Sophos DMZ Server non presenti allarmi o errori e, se necessario, provvedere riavviando il sistema.

Sophos DMZ Server è ora protetto.

14 Creazione di un pacchetto di installazione

14.1 Il tool Deployment Packager

È possibile installare Sophos Endpoint Security and Control (SESC) nei computer endpoint client utilizzando il tool Deployment Packager, a disposizione sul sito web di Sophos. Il Deployment Packager crea un singolo file di archivio autoestraente da una serie di file di installazione di Sophos, per installare Sophos Endpoint Security and Control nei computer client. Il file del pacchetto comprende opzioni di configurazione quali: installazione invisibile/interattiva, scelte per il pacchetto di installazione e per i parametri di installazione, aggiornamento di percorso/credenziali e appartenenza ad un gruppo di computer.

I pacchetti creati con il Deployment Packager cercheranno sempre di rimuovere altri software di protezione che potrebbero creare conflitti al momento dell'installazione.

Potrebbe essere necessario produrre diversi pacchetti, ognuno dei quali soddisfi i requisiti dei diversi tipi di computer.

È possibile avviare il tool Deployment Packager mediante interfaccia utente grafica ("graphical user interface", o GUI) o interfaccia della riga di comando ("command-line interface", o CLI).

- L'opzione GUI è più semplice nel caso di installazioni singole.
- L'opzione CLI è più versatile, ed è efficace in caso di installazioni ripetute.

  Una stringa che richiami la versione della riga di comando e tutte le opzioni scelte può venire memorizzata in un file di testo, oppure eseguita da un file batch pianificato, garantendo che i pacchetti di installazione siano sempre aggiornati. Quindi, se si gestiscono numerosi computer e si ha bisogno di frequenti installazioni, è preferibile utilizzare l'opzione CLI.

Le istruzioni per l'uso del Deployment Packager tramite riga di comando si trovano su Creazione di un pacchetto di protezione mediante interfaccia della riga di comando (pagina 33).

Requisiti di sistema

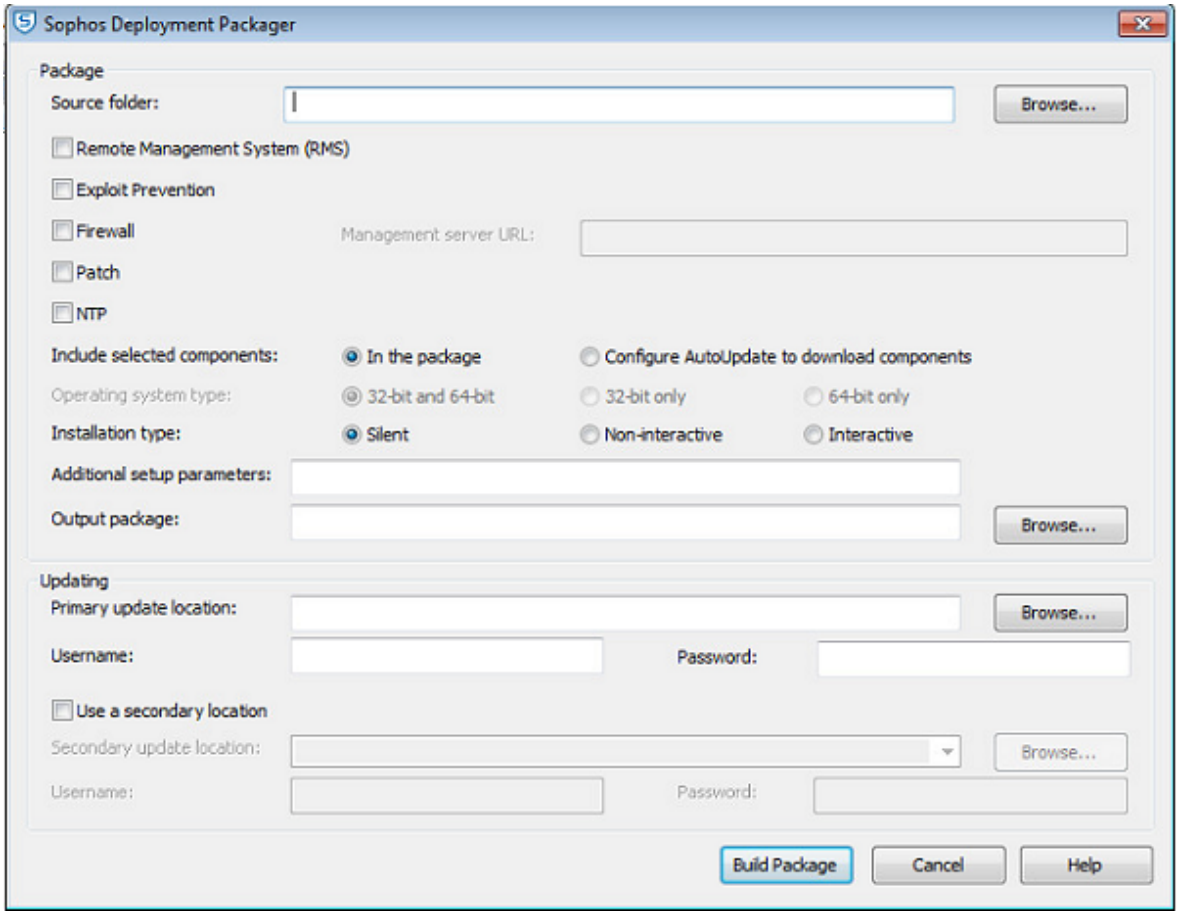
I requisiti minimi per eseguire il tool Deployment Packager sono i seguenti:

- Sistemi operativi Windows: consultare l'articolo 118635 della knowledge base
- Spazio su disco: 1 GB
- Memoria: 1 GB
- Processore: 2 GHz Pentium o equivalente

È inoltre necessario essere a conoscenza dei requisiti di sistema dei componenti endpoint del pacchetto. Consultare l'articolo 118620 della knowledge base.

14.2 Creazione di un pacchetto di protezione mediante l'interfaccia utente grafica

1. Per creare un pacchetto di protezione, eseguire il comando `DeploymentPackager.exe`. Viene visualizzata la finestra di dialogo del **Sophos Deployment Packager**.



2. In **Source Folder**, specificare il percorso della directory di installazione centrale contenente i file di installazione del software per gli endpoint. Può essere un percorso UNC o una cartella locale.
3. Selezionare tra le seguenti opzioni:

   - **Remote Management System (RMS)**

     Esegue l'installazione e abilita Sophos Remote Management System che, a sua volta, consente a Sophos Enterprise Console di controllare Sophos Endpoint Security and Control. Per i sistemi gestiti, è imperativo abilitare questo componente.

     Nota
     quando è selezionata questa opzione, gli endpoint ottengono il percorso di aggiornamento e le credenziali da Enterprise Console tramite RMS.

   - **Exploit Prevention**

     Questo componente installa Sophos Exploit Prevention.

- **Firewall**

  Questo componente installa Sophos Client Firewall.

  Nota
  se si desidera installare questo componente, verificare i requisiti di sistema dei computer endpoint, alla pagina web www.sophos.com/it-it/products/all-system-requirements.aspx.

- **Patch**

  Consente l'installazione del Sophos Patch Agent. È inoltre necessario indicare l'indirizzo in cui è installato il Management server sotto **Management Server URL**. L'indirizzo deve esser un nome di dominio completo. Esempio: http://<nome server>.

  Se si seleziona questa opzione, è possibile selezionare **Operating system type**.

- **NTP**

  Con questa opzione viene installata e abilitata Sophos Network Threat Protection (NTP).

- Nel riquadro **Include selected components**, eseguire una delle seguenti operazioni:

  Per includere nel pacchetto di distribuzione i componenti prescelti, selezionare **In the package**.

  Per scaricare i componenti selezionati dalla fonte degli aggiornamenti, cliccare su **Configure AutoUpdate to download components**.

  il programma di installazione per endpoint non è in grado di utilizzare un server proxy. Se l'accesso al percorso di aggiornamento avviene tramite server proxy, allora i componenti per endpoint richiesti devono venire inclusi nel pacchetto.

Se si seleziona **Remote Management (RMS)** e quindi si clicca su **In the package** in **Include selected components**, Sophos Enterprise Console comunica dati degli aggiornamenti.

I pacchetti di Sophos System Protection e Sophos Endpoint Defense verranno aggiunti automaticamente al pacchetto generato (se fanno parte dei pacchetti concessi in licenza), in quanto non sono componenti opzionali.

4. In **Operating system type**, scegliere il tipo di sistema operativo del pacchetto. Questa opzione è applicabile solo se si installa Patch dal pacchetto di distribuzione. Se si seleziona l'opzione **32-bit** o **64-bit** il pacchetto può essere installato solo in sistemi operativi a 32 o 64 bit. Se si seleziona l'opzione **32-bit and 64-bit**, il pacchetto potrà essere installato sia in sistemi operativi a 32 bit, sia a 64, ma ciò comporterà un incremento delle dimensioni del pacchetto.
5. In **Installation type**, scegliere la modalità di esecuzione del programma di installazione sui computer endpoint.
   - Selezionare **Silent**: il programma viene eseguito senza richiedere alcuna interazione con l'utente. Lo stato dell'installazione non viene visualizzato nei computer.
   - Selezionare **Non-interactive**: il programma viene eseguito senza richiedere alcuna interazione con l'utente. Lo stato dell'installazione viene visualizzato nei computer.
   - Selezionare **Interactive**: il programma viene eseguito e richiede l'interazione dell'utente. L'utente deve controllare lo stato dell'installazione.
6. In **Additional setup parameters**, specificare le opzioni di installazione per i computer endpoint. L'appartenenza a un gruppo va sempre specificata usando l'opzione -g, per rendere ciascun programma di installazione specifico di un determinato gruppo e per far sì che i computer ricevano le impostazioni necessarie a renderli membri di tale gruppo.

   Per queste opzioni, il Packager non svolge alcun controllo alla ricerca di errori.

Per ulteriori informazioni, consultare l'articolo www.sophos.com/it-it/support/knowledgebase/12570.aspx.

7. In **Output package**, specificare il percorso di destinazione del pacchetto di installazione creato. È inoltre possibile specificare un nome file opzionale; se non viene fornito, il Deployment Packager ne userà uno predefinito.
8. Nel pannello **Updating**, per i computer gestiti in maniera indiretta o dove la gestione remota è abilitata ma non inclusa nel pacchetto, inserire il percorso di aggiornamento e le credenziali. È possibile impostare il ":<numero di porta>" dopo un URL HTTP; se non viene impostato, quello predefinito è 80.

   Nota
   - Verificare che tutti i componenti selezionati possano essere aggiornati dal percorso di aggiornamento specificato (per es. Patch). Nel caso si desideri utilizzare un percorso diverso per determinati componenti, è possibile configurarlo come percorso di aggiornamento secondario.
   - Le credenziali vengono occultate nel pacchetto; tuttavia, è bene che gli account impostati per permettere agli endpoint di leggere i percorsi dei server per gli aggiornamenti siano sempre il più restrittivo possibile, consentendo esclusivamente un accesso di sola lettura.
   - I computer cercheranno di utilizzare le impostazioni Proxy di sistema solo se programmati all'utilizzo delle variabili ambientali http_proxy o all_proxy. Le impostazioni proxy in "Opzioni Internet" nel Pannello di controllo di Windows o in Internet Explorer vengono ignorate. I valori della variabile proxy hanno il formato _proxy=[protocollo://][utente:password@]host[:port], per esempio http_proxy=http://utente:password@proxy:8080

9. Cliccare su **Build Package** per creare l'archivio autoestraente.

15 Verifica del pacchetto di installazione

Una volta creato il pacchetto di installazione, si consiglia di verificare che si riesca a eseguire installazioni, aggiornamenti e a gestire computer utilizzando il pacchetto appena creato.

Per fare ciò:

1. Scegliere un computer autonomo che faccia parte della rete locale e utilizzarlo come computer endpoint.
2. Distribuire il pacchetto di installazione al computer endpoint.
3. Verificare che l'installazione sia avvenuta e controllare le seguenti funzioni:
   - Aggiornamento: per verificare che il computer endpoint esegua il download degli aggiornamenti da Sophos Enterprise Console, cliccare col tasto destro del mouse sull'icona del sistema di protezione Sophos nell'area di notifica, quindi cliccare su **Aggiorna ora**. Il computer endpoint dovrebbe eseguire il download degli aggiornamenti da Sophos Enterprise Console.
   - Gestione: per verificare che Sophos Enterprise Console stia gestendo i computer endpoint. Nella finestra di Sophos Enterprise Console, verificare che l'icona del sistema di protezione Sophos non sia grigia, non abbia una croce rossa o non abbia un punto esclamativo giallo.

   Una volta verificato il funzionamento del pacchetto di installazione, distribuirlo ai computer dei clienti.

16 Distribuzione del pacchetto di installazione sui computer dei clienti

Utilizzare il proprio sistema RMM per distribuire ed eseguire il o i pacchetti di installazione sui computer dei clienti. Le istruzioni specifiche su come svolgere ciò dipendono dal sistema utilizzato, e non rientrano nelle competenze di questa guida.

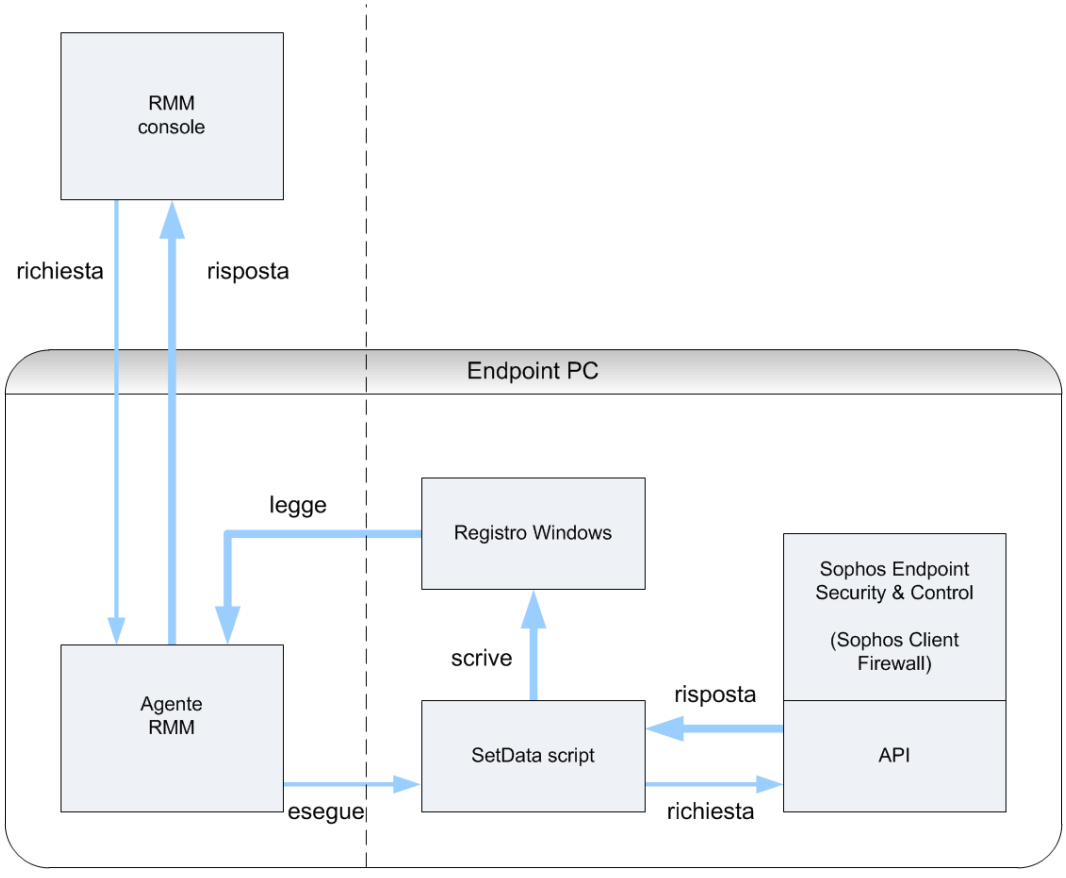
17 Monitoraggio della sicurezza endpoint

Una volta installato Sophos Endpoint Security and Control sugli endpoint, i gruppi, i criteri e le altre impostazioni vengono gestiti tramite Sophos Enterprise Console, che fornisce una reportistica completa del loro stato. Per ulteriori informazioni, consultare la *Guida in linea* e la *Guida per l'impostazione dei criteri* di Sophos Enterprise Console.

La maggior parte degli MSP utilizza il proprio sistema RMM per il regolare monitoraggio dello stato dei computer, mentre utilizza Sophos Enterprise Console solo per la configurazione di gruppi/criteri e nell'eventualità di un problema di sicurezza. Il sistema RMM presente sul computer viene utilizzato come metodo primario per la gestione e il monitoraggio del software di tutti gli endpoint (non solamente Sophos Endpoint Security and Control).

Questa sezione descrive come utilizzare lo script SetData per fornire al sistema RMM del computer le informazioni più importanti sullo stato del computer.

Il diagramma qui di seguito mostra come il sistema RMM usi lo script SetData per conoscere lo stato dell'endpoint.



17.1 Lo script SetData

Lo script `MSPSetData.vbs` può essere eseguito da Windows o richiamato dalla riga di comando o da un file batch. MSPSetData:

- Legge i parametri da Sophos Endpoint Security and Control,

- Trascrive i parametri di Sophos Endpoint Security and Control nel registro Windows dell'endpoint.
- Può essere eseguito solo con privilegi di amministratore LOCAL_SYSTEM.
- Deve essere eseguito in un ambiente a 32 bit. Per le versioni a 64 bit di Windows, la versione a 32 bit del prompt di comando è disponibile su `%WINDIR%\SysWOW64\cmd.exe`

Per eseguire lo script SetData nella modalità riga di comando, utilizzare il seguente formato

```
MSPSetData <base_key> [logFileName]
```

Dove `<base_key>` è la chiave di base in HKEY_LOCAL_MACHINE per scrivere i parametri del computer, e `<logFileName>` è un percorso opzionale per il file di log.

Nota
richiamando SetData con il parametro logFileName, i dati del log verranno aggiunti a tutti i file di log già esistenti. Se si richiama SetData spesso, il file di log potrebbe raggiungere dimensioni molto grandi.

Esempio:

```
MSPSetData "SOFTWARE\Sophos\ESCStatus" "c:\MSPSetDataLog.txt"
```

In questo modo, tutti i parametri verranno scritti in `HKEY_LOCAL_MACHINE\SOFTWARE\Sophos\ESCStatus` e il log su `c:\MSPSetDataLog.txt`.

17.2 I parametri del computer

Lo script SetData legge i parametri da Sophos Endpoint Security and Control e Sophos Client Firewall, e li scrive nel registro del computer Windows come descritto qui di seguito, in una radice di percorso hive configurabile in `HKEY_LOCAL_MACHINE`.

Se Sophos Endpoint Security and Control o Sophos Client Firewall non sono presenti o non sono in esecuzione, i parametri REG_DWORD vengono impostati su -1 e quelli REG_SZ su zero.

Se Sophos Endpoint Security and Control o Sophos Client Firewall stanno effettuando un aggiornamento, tutti i loro parametri REG_DWORD ad eccezione di UpdateInProgress vengono impostati su -1, e tutti i loro parametri REG_SZ su zero.

Lista dei parametri

Percorso hive del registro	Parametro/Chiave	Descrizione	Digitare REG_
\SAVService\Status \Infected	ControlledAppDetected	0: Nessuna applicazione controllata rilevata 1: Applicazione controllata rilevata (& messa in quarantena)	DWORD
	MalwareDetected	0: Nessun malware rilevato 1: Malware rilevato & messo in quarantena	

Percorso hive del registro	Parametro/Chiave	Descrizione	Digitare REG_
	PUADetected	0: Nessuna PUA rilevata 1: Rilevata PUA	
	SuspiciousBehaviorDetected	0: Nessun comportamento sospetto rilevato 1: L'endpoint mostra un comportamento sospetto	
	SuspiciousFileDetected	0: Nessun file sospetto rilevato 1: Rilevato file sospetto	
\SAVService\Status \LastScan	SystemScan	Ora/data dell'ultima scansione (valore di periodo) ad es. 1268337010	
	NormalScan		
	EnterpriseScan		
\SAVService\Status \Policy	AppControlComplies	0: Non conforme ai criteri SEC 1: Conforme ai criteri SEC	
	SAVComplies		
	DataControlComplies		
	DevControlComplies		
\SAVService\Application	Managed	0: Independente 1: Gestito da SEC	
\SAVService\Version	Data	Numero di versione SAV dei dati del virus, ad es. 4.50 G	SZ
	Major	Numero di versione SAV principale # ad es. 9	DWORD
	Minor	Numero di versione SAV secondario # ad es. 5	
	Extra	Informazioni aggiuntive sul numero di versione SAV, ad es. beta	SZ
\SAVService\Status \Policy	OnAccessEnabled	0: Scansione in accesso disabilitata 1: Scansione in accesso attiva	DWORD
\SAVService\Update	UpdateInProgress	0: Nessun aggiornamento in corso 1: Aggiornamento	

Percorso hive del registro	Parametro/Chiave	Descrizione	Digitare REG_
	IDECount	Numero di file di identità dei virus Sophos presenti	
	LastUpdated	Ora/data dell'ultimo aggiornamento gg.mm.aaaa oo:mm:ss ad es. 02.03.2010 18:56:30	SZ
\Sophos Client Firewall \Config	ActiveLocation	1: Percorso primario 2: Percorso secondario	DWORD
	DetectedLocation		
	Disabilitato	0: Operativo 1: Consente ogni traffico	
	Mode	0: Interattiva 1: Blocca il traffico sconosciuto 2: Consenti il traffico sconosciuto	
\Sophos Client Firewall \Update	UpdateInProgress	0: Nessun aggiornamento in corso 1: Aggiornamento	
\Sophos Client Firewall \Version	FirewallVersion	Versione del Firewall # ad es. 2.0	SZ

17.3 Utilizzare l'RMM per leggere i parametri degli endpoint

Le istruzioni qui riportate hanno un valore generale, dal momento che le implementazioni della gestione remota possono differire le une dalle altre.

1. Copiare lo script SetData sui computer endpoint gestiti.
2. Configurare la propria console RMM affinché esegua lo script periodicamente (per es. una volta ogni quattro ore), leggere i valori contenuti nel registro dei parametri e visualizzarli insieme agli allarmi relativi a condizioni critiche.

È possibile eseguire lo script manualmente, per controllarne il funzionamento e monitorare i valori scritti nel registro Windows del computer, utilizzando regedit.

18 Creazione di un pacchetto di protezione mediante interfaccia della riga di comando

Prima di leggere questa sezione, consultare Creazione di un pacchetto di protezione mediante l'interfaccia utente grafica (pagina 24).

Per eseguire il Deployment Packager in modalità riga di comando, utilizzare il seguente comando:

```
DeploymentPackager.exe-cli -mng yes -cidpath <percorsoCID> -sfxpath
<percorsoSFX> -crt R
```

dove `<percorsoCID>` è il percorso che porta alla directory di installazione centrale pertinente e `<percorsoSFX>` è il percorso del pacchetto di output. **-crt R** rimuove automaticamente il software di protezione prodotto da terzi.

Il packager riporta un valore pari a zero quando viene eseguito correttamente, e un valore diverso da zero se si è verificato un errore.

Opzioni della riga di comando

È inoltre possibile utilizzare altri modificatori di riga di comando, come quelli elencati qui sotto.

-mng yes

Abilita Remote Management.

-mngcfg

Indica il percorso dei file di configurazione personalizzati di Remote Management.

-scf

Installa Sophos Client Firewall

-ntp

Installa Sophos Network Threat Protection.

-hmpa

Installa Sophos Exploit Prevention.

-patch <URL di Management Server>

Installare Sophos Patch Agent utilizzando l'indirizzo del Management Server. L'indirizzo deve esser un nome di dominio completo. Esempio: http://<nome server>.

-sauonly

Include solamente Creazione di un pacchetto di protezione mediante l'interfaccia utente grafica (pagina 24) (i componenti di gestione remota, firewall, NTP e SSP prescelti vengono scaricati dalla fonte degli aggiornamenti). Se questa opzione non è selezionata, i componenti prescelti vengono inclusi nel pacchetto.

-arch <32bit, 64bit>

Indica l'architettura del pacchetto che si desidera creare, a 32 o 64 bit.

Nota
questa opzione è applicabile solo se si installa Patch. Se si seleziona l'opzione **32-bit** o **64-bit** il pacchetto può essere installato solo in sistemi operativi a 32 o 64 bit. Se non si sceglie un'architettura specifica, viene creato un pacchetto singolo che potrà essere installato sia in sistemi operativi a 32 bit, sia a 64, ma ciò comporterà un incremento delle dimensioni del pacchetto.

-updp <aggiorna_percorso>

Aggiorna il percorso.

-user <unomeutente>

-pwd <password>

Nome utente e password. Il Packager occulta questi dati nel pacchetto di installazione. Se, però, nome utente e password vengono salvati non codificati in un file di testo o batch, collocare tale file in un percorso sicuro.

-opwd <password_occultata>

Password occultata. Per informazione su come offuscare le password, consultare l'articolo della knowledge base *"Come offuscare nome utente e password"* alla pagina Web www.sophos.com/it-it/support/knowledgebase/13094.aspx.

-s

Esegue un'installazione invisibile.

-ni

Esegue un'installazione non interattiva.

Altre opzioni

Altre opzioni vengono incluse nel pacchetto di installazione ed eseguite durante l'installazione stessa.

19 Appendice: contenuto del file MRinit.conf

Segue un esempio del file MRinit.conf modificato:

```
[Config]
"NotifyRouterUpdate"="EM"
"ClientIIOPPort"=dword:00002001
"ClientSSLPort"=dword:00002002
"ClientIORPort"=dword:00002000
"IORSenderPort"=dword:00002000
"DelegatedManagerCertIdentityKey"="NOChhZvtx8i59YN4OVkvtaOYHsA="
"ManagedAppCertIdentityKey"="KeDbiqpDTPaiKSPwXhiS/FxPMaE="
"RouterCertIdentityKey"="+Z3KILDInN7HZn0jbZu4zsLSyfg="
"ServiceArgs"=""
"MRParentAddress"="192.168.0.10, sophos-console.msp.com, sophos-console"
"ParentRouterAddress"="sophos-dmz,sophos-dmz.msp.com"
```

20 Supporto tecnico

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

- Visitare la Sophos Community su community.sophos.com/ e cercare altri utenti che hanno riscontrato lo stesso problema.
- Visitare la knowledge base del supporto Sophos su www.sophos.com/it-it/support.aspx.
- Scaricando la documentazione del prodotto su 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.

21 Note legali

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 Software License

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

The Sophos software that is referenced in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.com or via the web at https://www.sophos.com/en-us/support/contact-support.aspx. A copy of the license agreement for any such included software can be found at http://opensource.org/licenses/cpl1.0.php

ConvertUTF

crt

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS 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 REGENTS 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 Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase "this text" refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase "This material" refers to portions of the system documentation. This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at fttp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License. Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

"3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors."

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins

Director, Office of Technology Licensing
University of California, Berkeley

dtoa.c

The author of this software is David M. Gay.

Copyright © 1991, 2000 by Lucent Technologies.

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHOR NOR LUCENT MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

ICU

ICU version 1.8.1 or later

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1995–2008 International Business Machines Corporation and others

All rights reserved.

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, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

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 OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

IEEE Software Taggant Library

This software was developed by The Institute of Electrical and Electronics Engineers, Incorporated (IEEE), through the Industry Connections Security Group (ICSG) of its Standards Association.

Portions of it include software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/), and those portions are governed by the OpenSSL Toolkit License.

IEEE License

Copyright (c) 2012 IEEE. 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 IEEE Industry Connections Security Group (ICSG)".
4. The name "IEEE" must not be used to endorse or promote products derived from this software without prior written permission from the IEEE Standards Association (stds.ipr@ieee.org).
5. Products derived from this software may not contain "IEEE" in their names without prior written permission from the IEEE Standards Association (stds.ipr@ieee.org).
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the IEEE Industry Connections Security Group (ICSG)".

THIS SOFTWARE IS PROVIDED "AS IS" AND "WITH ALL FAULTS." IEEE AND ITS CONTRIBUTORS EXPRESSLY DISCLAIM ALL WARRANTIES AND REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION: (A) THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE; (B) ANY WARRANTY OF NON-INFRINGEMENT; AND (C) ANY WARRANTY WITH RESPECT TO THE QUALITY, ACCURACY, EFFECTIVENESS, CURRENCY OR COMPLETENESS OF THE SOFTWARE.

IN NO EVENT SHALL IEEE 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 AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

THIS SOFTWARE USES STRONG CRYPTOGRAPHY, WHICH MAY BE SUBJECT TO LAWS AND REGULATIONS GOVERNING ITS USE, EXPORTATION OR IMPORTATION. YOU ARE SOLELY RESPONSIBLE FOR COMPLYING WITH ALL APPLICABLE LAWS AND REGULATIONS, INCLUDING, BUT NOT LIMITED TO, ANY THAT GOVERN YOUR USE, EXPORTATION OR IMPORTATION OF THIS SOFTWARE. IEEE AND ITS CONTRIBUTORS DISCLAIM ALL LIABILITY ARISING FROM YOUR USE OF THE SOFTWARE IN VIOLATION OF ANY APPLICABLE LAWS OR REGULATIONS.

Info-ZIP

Copyright © 1990–2007 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, “Info-ZIP” is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided “as is,” without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use 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. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions—including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP—must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.
4. Info-ZIP retains the right to use the names “Info-ZIP,” “Zip,” “UnZip,” “UnZipSFX,” “WiZ,” “Pocket UnZip,” “Pocket Zip,” and “MacZip” for its own source and binary releases.

Jansson

Copyright (c) 2009-2013 Petri Lehtinen <petri@digip.org>

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.

Lua

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Lua License. A copy of the license agreement for any such included software can be found at http://www.lua.org/copyright.html

Microsoft software

This Sophos product may include certain Microsoft software, licensed to Sophos for inclusion and use herein.

Mersenne Twister (mt19937ar.c)

Copyright (c) 1997–2002 Makoto Matsumoto and Takuji Nishimura. 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. The names of its contributors may not be used to endorse or promote products derived from this software without specific prior written permission.

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 COPYRIGHT OWNER 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.

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.

OpenSSL license

Copyright © 1998–2016 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.
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). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

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

This package is an SSL implementation written by Eric Young (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).

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)”

   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)”

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.]

Protocol Buffers (libprotobuf)

Copyright 2008, Google Inc.

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.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

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 COPYRIGHT OWNER 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.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

pstdint

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. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "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 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.

Simple ECMAScript Engine (SEE)

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. Neither the name of David Leonard nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

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 COPYRIGHT OWNER 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.

SQLCipher

strcasestr.c

Udis86

Unicode

notice appear in associated documentation, and (c) there is clear notice in each modified Data File or in the Software as well as in the documentation associated with the Data File(s) or Software that the data or software has been modified.

THE DATA FILES AND SOFTWARE ARE 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 OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in these Data Files or Software without prior written authorization of the copyright holder.

UnRAR

The source code of UnRAR utility is freeware. This means:

1. All copyrights to RAR and the utility UnRAR are exclusively owned by the author - Alexander Roshal.
2. The UnRAR sources may be used in any software to handle RAR archives without limitations free of charge, but cannot be used to re-create the RAR compression algorithm, which is proprietary. Distribution of modified UnRAR sources in separate form or as a part of other software is permitted, provided that it is clearly stated in the documentation and source comments that the code may not be used to develop a RAR (WinRAR) compatible archiver.
3. The UnRAR utility may be freely distributed. It is allowed to distribute UnRAR inside of other software packages.
4. THE RAR ARCHIVER AND THE UnRAR UTILITY ARE DISTRIBUTED “AS IS”. NO WARRANTY OF ANY KIND IS EXPRESSED OR IMPLIED. YOU USE AT YOUR OWN RISK. THE AUTHOR WILL NOT BE LIABLE FOR DATA LOSS, DAMAGES, LOSS OF PROFITS OR ANY OTHER KIND OF LOSS WHILE USING OR MISUSING THIS SOFTWARE.
5. Installing and using the UnRAR utility signifies acceptance of these terms and conditions of the license.
6. If you don’t agree with terms of the license you must remove UnRAR files from your storage devices and cease to use the utility.

Thank you for your interest in RAR and UnRAR.

Alexander L. Roshal

Windows Template Library (WTL)

This product may contain Windows Template Library (WTL) and/or WixToolset code, which are licensed under the Common Public License 1.0. The source code for the components is available from Sophos, upon request, by emailing TPCRequest@sophos.com

wow64ext library

This is used in Sophos Virus Removal Tool as a shared library (wow64ext.dll), which may be removed or subsituted without affecting other functionality. Its use is covered by the following license:

GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc.

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

- **0. Additional Definitions.**

  As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

  "The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

  An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

  A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

  The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

  The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. **Exception to Section 3 of the GNU GPL.**

   You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. **Conveying Modified Versions.**

   If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

   a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

   b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. **Object Code Incorporating Material from Library Header Files.**

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. **Combined Works.**

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. **Combined Libraries.**

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. **Revised Versions of the GNU Lesser General Public License.**

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.