Endpoint Security Suite Enterprise for Linux

Guida dell'amministratore v2.1

Messaggi di N.B., Attenzione e Avvertenza

N.B.: un messaggio N.B. (Nota Bene) indica informazioni importanti che contribuiscono a migliorare l'utilizzo del prodotto.

ATTENZIONE: Un messaggio di ATTENZIONE indica un danno potenziale all'hardware o la perdita di dati, e spiega come evitare il problema.

AVVERTENZA: Un messaggio di AVVERTENZA indica un rischio di danni materiali, lesioni personali o morte.

2018 - 11

Rev. A01

Sommario

1

Introduzione

La Guida dell'amministratore di Endpoint Security Suite Enterprise per Linux fornisce le informazioni necessarie per installare e distribuire il software client.

Panoramica

Endpoint Security Suite Enterprise per Linux offre Advanced Threat Prevention a livello di sistema operativo e memoria, il tutto gestito centralmente da Dell Server. Grazie alla gestione centralizzata, alla creazione di report di conformità consolidati e agli avvisi di minaccia alla console, le organizzazioni possono facilmente applicare e dimostrare la conformità degli endpoint. L'esperienza della protezione è integrata con diverse funzioni, come ad esempio criteri predefiniti e modelli di rapporto, per aiutare le aziende a ridurre i costi di gestione IT e la complessità.

Security Management Server o Security Management Server Virtual - assicura l'amministrazione centralizzata dei criteri di sicurezza, si integra con le directory aziendali esistenti e crea rapporti. Ai fini del presente documento, entrambi i server sono indicati come Dell Server, a meno che non sia necessario indicare una versione specifica (ad esempio, se una procedura è diversa quando si utilizza Security Management Server Virtual).

Advanced Threat Prevention per Linux ha un file tar.gz, che contiene i tre RPM.

Contattare Dell ProSupport

Per assistenza telefonica sui prodotti Dell, chiamare il numero 877-459-7304, interno 4310039, 24h su 24, 7 giorni su 7.

Inoltre, il supporto online per i prodotti Dell è disponibile all'indirizzo dell.com/support. L'assistenza online comprende driver, manuali, consulenze tecniche, FAQ e problemi emergenti.

Assicurarsi di avere a portata di mano il codice di matricola o il codice di servizio rapido per essere messi rapidamente in contatto con l'esperto tecnico più adatto.

Per i numeri di telefono al di fuori degli Stati Uniti, vedere Numeri di telefono internazionali di Dell ProSupport.

2

Requisiti

In questo capitolo sono specificati i requisiti hardware e software client. Prima di continuare con le attività di distribuzione, accertarsi che l'ambiente di distribuzione soddisfi i requisiti.

Hardware

La tabella seguente descrive in dettaglio l'hardware minimo supportato.

Hardware

- Almeno 500 MB di spazio libero su disco
- 2 GB RAM
- Scheda di interfaccia di rete 10/100/1000 o Wi-Fi

N.B.: IPv6 non è attualmente supportato.

Software

La tabella seguente descrive in dettaglio il software supportato.

Sistemi operativi (kernel a 64 bit)

- CentOS Linux v7.1 - v7.5
- Red Hat Enterprise Linux v7.1 - v7.5

Porte

- La porta 443 (https) viene utilizzata per le comunicazioni e deve essere aperta sul firewall affinché gli agenti possano comunicare con la Management Console. Se la porta 443 è bloccata per qualsiasi motivo, è impossibile scaricare gli aggiornamenti, quindi i computer potrebbero non disporre della protezione più recente. Accertarsi che i computer client abbiano accesso a quanto riportato di seguito:

Utilizzo	Protocollo dell'applicazione	Protocollo di trasporto	Numero di porta	Destinazione	Direzione
Tutte le comunicazioni	HTTPS	TCP	443	Consentire tutto il traffico https per *.cylance.com	In uscita
Comunicazioni con Dell Core Server	HTTPS	TCP	8888	Consente le comunicazioni con Dell Core Server	In entrata/in uscita

- Per ulteriori informazioni, vedere SLN303898.

Endpoint Security Suite Enterprise for Linux e dipendenze

Endpoint Security Suite Enterprise for Linux utilizza Mono e le relative dipendenze per l'installazione e l'attivazione sul sistema operativo Linux. Il programma di installazione scaricherà e installerà le dipendenze richieste. Dopo l'estrazione del pacchetto, è possibile visualizzare le dipendenze utilizzate mediante il comando seguente:

```
./showdeps.sh
```

Compatibilità

La tabella seguente descrive in dettaglio la compatibilità con Windows, Mac e Linux.

n/d - La tecnologia non è applicata a questa piattaforma.

Campo vuoto - Il criterio non è supportato con Endpoint Security Suite Enterprise.

Funzioni	Criteri	Windows	macOS	Linux
Azioni file				
	Quarantena automatica (non sicuro)	x	x	x
	Quarantena automatica (anomalo)	x	x	x
	Caricamento automatico	x	x	x
	Criterio Elenco file sicuri	x	x	x
Azioni memoria				
	Protezione della memoria	x	x	x
Sfruttamento				
	Manipolazione dello stack	x	x	x
	Protezione dello stack	x	x	x
	Sovrascrivi codice	x	n/d	
	RAM scraping	x	n/d	
	Payload dannoso	x		
Aggiunta di processo				
	Allocazione remota di memoria	x	x	n/d
	Mapping remoto di memoria	x	x	n/d
	Scrittura remota in memoria	x	x	n/d
	Scrittura remota di PE in memoria	x	n/d	n/d

Funzioni	Criteri	Windows	macOS	Linux
	Codice di sovrascrittura remoto	x	n/d	
	Annullamento mapping remoto di memoria	x	n/d	
	Creazione remota di thread	x	x	
	APC remoto pianificato	x	n/d	n/d
	Aggiunta di DYLD		x	x
Escalation				
	Lettura di LSASS	x	n/d	n/d
	Allocazione di zero	x	x	
Impostazioni protezione				
	Controllo delle esecuzioni	x	x	x
	Impedisci arresto del servizio dal dispositivo	x	x	
	Termina processi principali e relativi processi secondari non sicuri in esecuzione	x	x	x
	Rilevamento delle minacce in background	x	x	x
	Controlla file nuovi	x	x	x
	Dimensione massima del file di archivio da sottoporre a scansione	x	x	x
	Escludi cartelle specifiche	x	x	x
	Copia campioni di file	x		
Controllo delle applicazioni				
	Modifica finestra	x		x
	Esclusioni cartella	x		
Impostazioni agente				
	Abilita caricamento automatico dei file di registro	x	x	x
	Abilita notifiche desktop	x		
Controllo script				
	Script attivo	x		
	PowerShell	x		
	Macro di Office	x		n/d
	Blocca utilizzo console PowerShell	x		

Funzioni	Criteri	Windows	macOS	Linux
	Approva script in cartelle (e sottocartelle)	x		
	Livello registrazione	x		
	Livello protezione automatica	x		
	Aggiornamento automatico	x		
	Esegui un rilevamento (da UI agente)	x		
	Elimina messi in quarantena (UI agente e UI console)	x		
	Modalità disconnessa	x		x
	Dati dettagliati sulla minaccia	x		
	Elenco certificati sicuri	x	x	n/d
	Copia campioni di malware	x	x	x
	Impostazioni proxy	x	x	x
	Controllo manuale dei criteri (UI agente)	x	x	

Attività

L'installazione

Questa sezione guida l'utente nel processo di installazione di Endpoint Security Suite Enterprise per Linux.

Prerequisiti

Dell invita a seguire le procedure consigliate durante la distribuzione del software client. In queste procedure sono compresi, a titolo esemplificativo, ambienti di testing controllati per i test iniziali e distribuzioni scaglionate agli utenti.

Prima di iniziare questo processo, accertarsi che siano soddisfatti i seguenti prerequisiti:

- Assicurarsi che Dell Server e i suoi componenti siano già installati.

  Se non è ancora stato installato Dell Server, seguire le istruzioni nella guida appropriata di seguito.

  Guida alla migrazione e all'installazione di Security Management Server

  Guida introduttiva e all'installazione di Security Management Server Virtual
- Assicurarsi di disporre del nome e della porta host di Dell Server. Sono entrambi necessari per l'installazione del software client.
- Verificare che il computer di destinazione abbia connettività di rete a Dell Server.
- Se un certificato del server del client è mancante o presenta una firma automatica, è necessario disattivare l'affidabilità del certificato SSL solo sul lato client.

Installazione dalla riga di comando

Per installare il client Endpoint Security Suite Enterprise utilizzando la riga di comando, attenersi alla seguente procedura.

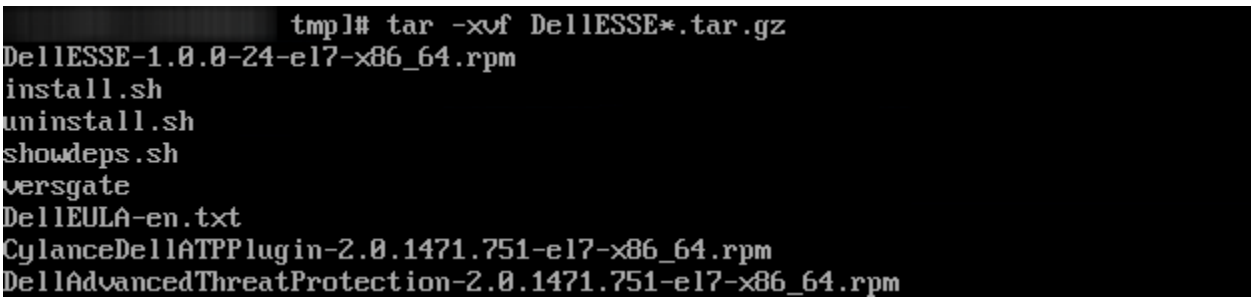
Il comando **sudo** deve essere utilizzato per richiamare i privilegi amministrativi durante l'installazione. Quando richiesto, immettere le proprie credenziali.

L'approvazione delle impronte digitali viene visualizzata solo durante la prima installazione.

1 Individuare e scaricare il bundle di installazione (DellESSE-1.x.x -xxx.tar.gz) utilizzando l'account Dell FTP.

2 Decomprimere il file tar.gz utilizzando il seguente comando:

```
tar -xvf DellESSE*.tar.gz
```



3 Il seguente comando esegue lo script di installazione per gli RPM e le dipendenze richiesti:

```
sudo ./install.sh
```

4 In *Dell Security Management Server Host?* immettere il nome host completo di Dell Server per gestire l'utente di destinazione. Ad esempio, server.organization.com.

5 In *Dell Security Management Server Port?* verificare che la porta sia impostata su 8888.

```
Dell Endpoint Security Suite Enterprise (ESSE) Installation
Dell Security Management Server Host?
Dell Security Management Server Port?
```

6 Immettere **y** quando viene richiesto di installare il pacchetto DellESSE e le relative dipendenze.

```
 libXfixes      x86_64 5.0.3-1.el7             base                       18
 libXrender     x86_64 0.9.10-1.el7            base                       26
 libXxf86vm     x86_64 1.1.4-1.el7             base                       18
 libexif        x86_64 0.6.21-6.el7            base                      347
 libjpeg-turbo x86_64 1.2.90-5.el7             base                      134
 libpng         x86_64 2:1.5.13-7.el7_2        base                      213
 libtiff        x86_64 4.0.3-27.el7_3          base                      170
 libxcb         x86_64 1.12-1.el7              base                      211
 libxshmfence   x86_64 1.2-1.el7               base                      7.2
 lyx-fonts      noarch 2.2.3-1.el7             epel                      159
 mesa-libEGL    x86_64 17.0.1-6.20170307.el7 base                         82
 mesa-libGL     x86_64 17.0.1-6.20170307.el7 base                        155
 mesa-libgbm    x86_64 17.0.1-6.20170307.el7 base                         32
 mesa-libglapi x86_64 17.0.1-6.20170307.el7 base                         41
 pixman         x86_64 0.34.0-1.el7            base                      248

Transaction Summary
================================================================================
Install  1 Package (+27 Dependent packages)

Total size: 96 M
Total download size: 3.8 M
Installed size: 104 M
Is this ok [y/d/N]:
```

7 Immettere **y** se richiesto per approvare l'*Impronta digitale*.

```
Total                                                   452 kB/s | 4.9 MB 00:00:11
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Importing GPG key 0xF4A80EB5:
 Userid         : "CentOS-7 Key (CentOS 7 Official Signing Key) <security@centos.org>"
 Fingerprint    : 6341 ab27 53d7 8a78 a7c2 7bb1 24c6 a8a7 f4a0 0eb5
 Package        : centos-release-7-3.1611.el7.centos.x86_64 (@anaconda)
 From           : /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Is this ok [y/N]:
```

8 Immettere **y** quando viene richiesto di installare il pacchetto *DellAdvancedThreatProtection*.

```
Dependencies Resolved

================================================================================
 Package  Arch   Version      Repository                                   Size
================================================================================
Installing:
 DellAdvancedThreatProtection
         x86_64 2.0.1461-739 /DellAdvancedThreatProtection-2.0.1461.739-el7-x86_64 149 M

Transaction Summary
================================================================================
Install  1 Package

Total size: 149 M
Installed size: 149 M
Is this ok [y/d/N]:
```

9 Immettere **y** quando viene richiesto di installare il pacchetto *CylanceDellATPPlugin*.

```
Dependencies Resolved

================================================================================
 Package     Arch   Version Repository                                   Size
================================================================================
Installing:
 CylanceDellATPPlugin
             x86_64 2.2.4-0 /CylanceDellATPPlugin-2.0.1461.739-el7-x86_64 439 k

Transaction Summary
================================================================================
Install  1 Package

Total size: 439 k
Installed size: 439 k
Is this ok [y/d/N]:
```

10 L'installazione è completata.

```
Installed:
  DellAdvancedThreatProtection.x86_64 0:2.0.1461-739

Complete!
```

11 Fare riferimento alla sezione Verifica dell'installazione di Endpoint Security Suite Enterprise per Linux.

Disinstallazione dalla riga di comando

Per disinstallare Endpoint Security Suite Enterprise per Linux utilizzando la riga di comando, attenersi alla seguente procedura.

1 Accedere a una finestra terminale.

2 Disinstallare il pacchetto utilizzando il seguente comando:

```
sudo ./uninstall.sh
```

3 Premere **Invio**.

Endpoint Security Suite Enterprise per Linux è ora disinstallato e il computer può essere utilizzato normalmente.

Visualizzazione dei dettagli

Dopo aver installato Endpoint Security Suite Enterprise per Linux, questo viene riconosciuto da Dell Server come endpoint.

atp -t

Il comando **atp - t** consente di visualizzare tutte le minacce individuate nel dispositivo e l'azione intrapresa. Le minacce sono una categoria di eventi appena rilevati come file o programmi potenzialmente pericolosi e necessitano di misure correttive.

Queste voci forniscono i dettagli dell'azione intrapresa, l'ID hash e la posizione della minaccia.

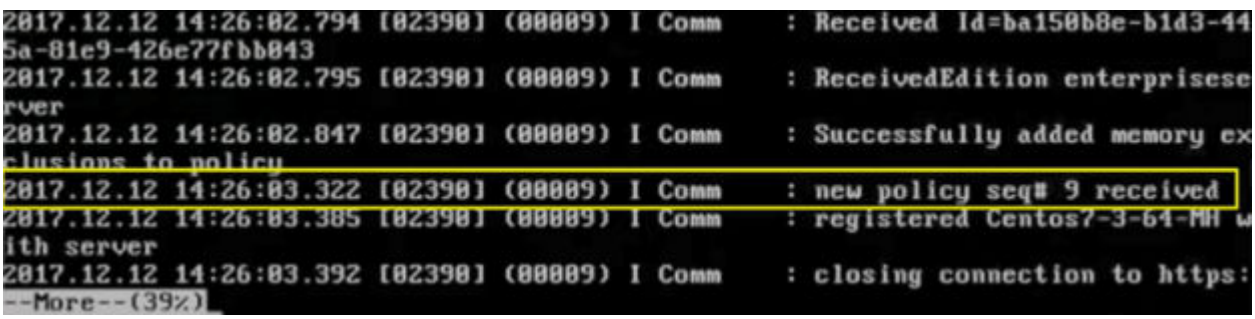
- **Non sicuro** - Un file sospetto di essere un probabile malware
- Anormale - Un file sospetto che può essere un malware
- **Spostato in quarantena** - Un file spostato dalla sua posizione originale, memorizzato nella cartella Quarantena e la cui esecuzione viene impedita sul dispositivo.
- **Ignorato** - un file la cui esecuzione è consentita sul dispositivo.
- **Cancellato** - un file cancellato all'interno dell'organizzazione. I file cancellati includono quelli ignorati che vengono aggiunti all'Elenco file sicuri ed eliminati dalla cartella Quarantena nel dato dispositivo.

Per ulteriori informazioni sulle classificazioni delle minacce di Advanced Threat Prevention consultare *AdminHelp*, disponibile nella Remote Management Console del Dell Server.

Verifica dell'installazione

Se si desidera, è possibile verificare che l'installazione sia stata completata correttamente.

- Sul client, accedere a una finestra terminale.
- Prima di ricevere una sequenza di criteri, il client si registra con Dell Server.
- Il file */var/log/Dell/ESSE/DellAgent.00.log* riporta in dettaglio le comunicazioni con Dell Server e l'interazione tra plugin e servizio.
  Il testo incluso conferma che il client ha ricevuto i criteri da Dell Server:



  Il testo incluso conferma che il servizio Dell è stato interrotto per caricare il plugin Advanced Threat Prevention:

```
//cedmz.credce.com:8888/agent
2017.12.12 14:27:05.883 [02390] (00009) I Comm    : next contact with server sch
eduled for 12/12/2017 8:27:05 PM
2017.12.12 14:27:10.442 [02390] (00005) I Agent   : Dell Data Protection stopped
---date--- ----time---- --pid-- -thrid-   -subsys-  ----------------------------
--message-------------------------------
2017.12.12 14:27:12.968 [02551] (00005) I Agent   : service name is "DellMgmtAge
nt"
2017.12.12 14:27:12.970 [02551] (00005) I Agent   : product name is "Dell Data P
```

Il testo incluso conferma che i tre plugin Endpoint Security Suite Enterprise per Linux sono stati caricati:

```
2018.02.18 10:51:36.951 [01077] (00005) I Agent   : machine name is "centosvm2.ddsdemos.com"
2018.02.18 10:51:36.951 [01077] (00005) I Agent   : process is 64-bit
2018.02.18 10:51:36.952 [01077] (00005) I Agent   : domain is "(none)"
2018.02.18 10:51:37.059 [01077] (00005) I Agent   : loaded plugin "Server Communication Manager" 1.
 Id={CAA1A89F-AF21-4C1E-9407-1E185FFEEB5C} in 69 ms
2018.02.18 10:51:37.059 [01077] (00005) I Agent   : loaded plugin "Auditing and Reporting Service"
.0 Id={0E969074-3164-467F-BF3D-D9E695F48240} in <1 ms
2018.02.18 10:51:37.069 [01077] (00005) I AdvATP  : Advanced Threat Prevention Cylance component lo
ging initialized
2018.02.18 10:51:37.069 [01077] (00005) I Agent   : loaded plugin "Advanced Threat Prevention" 1.0
d={96BBD97F-9BF0-4D61-94F8-A9884F8DC287} in 8 ms
2018.02.18 10:51:37.069 [01077] (00005) I Agent   : loaded 3 plugins
2018.02.18 10:51:37.090 [01077] (00010) I Comm    : AgentID 00397403-c05f-4cbf-b6b4-e15dd577186a
2018.02.18 10:51:37.102 [01077] (00011) I AdvATP  : AdvancedAtpManager Starting
2018.02.18 10:51:37.125 [01077] (00011) I AdvATP  : management is active
2018.02.18 10:51:37.129 [01077] (00011) I AdvATP  : processing new policies - Policy list count=1
```

`atp -s` - Include quanto segue:

- Stato di registrazione
- N. seriale - Utilizzare questo numero quando si contatta il supporto tecnico. Il presente è l'identificatore univoco dell'installazione.
- Criterio

```
[dell@Centos7-3-64-MH ~]$ /opt/cylance/desktop/atp -s
Registration Status: Registered
Serial Number: 0088ab40-ce18-43fa-a959-85f44e5ff251
Policy:  (Online)
```

Il comando seguente riporta in dettaglio le variabili della riga di comando per Endpoint Security Suite Enterprise per Linux:

`/opt/cylance/desktop/atp --help`

```
[dell@Centos7-3-64-MH ~]$ /opt/cylance/desktop/atp --help
usage: atp <options>
options:
    -r, --register=token    : register with Dell Data Security servers with the
provided token
    -s, --status            : get status of Advanced Threat Prevention
    -u, --checkupdates      : check for updates
    -b, --start-bg-scan     : start background scan
    -B, --stop-bg-scan      : stop background scan
    -d, --scan-dir=dir      : scan directory
    -l, --getloglevel       : get current log level
    -L, --setloglevel=level : set log level
    -P, --getpolicytime     : get the policy update time
    -p, --checkpolicy       : check for policy updates
    -t, --threats           : list threats
    -q, --quarantine=id     : quarantine a file by id (hash)
    -w, --waive=id          : waive a file by id (hash)
    -v, --version           : print this tools version
    -h, --help              : atp help
```

Il comando *atp* di Advanced Threat Prevention viene aggiunto alla directory */usr/sbin*, che è normalmente inclusa in una variabile PATH della shell al fine di essere utilizzata nella maggior parte dei casi senza un percorso esplicito.

Risoluzione dei problemi

Disattivazione di un certificato di attendibilità SSL

Se un certificato del server del computer è mancante o presenta una firma automatica, è necessario disattivare l'attendibilità del certificato SSL solo sul lato client.

Se si utilizza un certificato non comune, importare il certificato radice nell'archivio certificati Linux, quindi riavviare i servizi Endpoint Security Suite per Linux con il seguente comando: `/usr/lib/dell/esse/agentservicecmd.sh restart`

1 Accedere a una finestra terminale.

2 Inserire il percorso per l'app CsfConfig:
```
/usr/lib/dell/esse/CsfConfig
```

3 Eseguire CsfConfig.app:
```
sudo ./CsfConfig
```

Di seguito vengono visualizzate le impostazioni predefinite:

Impostazioni correnti:

ServerHost = deviceserver.company.com

ServerPort = 8888

DisableSSLCertTrust = Falso

DumpXmlInventory = Falso

DumpPolicies = Falso

4 Digitare **-** help per elencare le opzioni disponibili.

5 Per disattivare l'attendibilità del certificato SSL sul computer di destinazione, immettere il seguente comando:
```
sudo /usr/lib/dell/esse/CsfConfig -disablecerttrust true
```

Aggiungere l'inventario XML e le modifiche ai criteri per la cartella Accessi

Per aggiungere i file inventory.xml o policies.xml alla cartella Accessi:

1 Eseguire l'*app CsfConfig* come descritto in precedenza.

2 Per impostare *DumpXmlInventory* su *Vero*, immettere il seguente comando:
```
sudo /usr/lib/dell/esse/CsfConfig -dumpinventory true
```

3 Per impostare *DumpPolicies* su *Vero*, immettere il seguente comando:
```
sudo /usr/lib/dell/esse/CsfConfig -dumppolicies true
```

I file dei criteri sono messi da parte solo se si è verificata una modifica dei criteri.

4 Per visualizzare i file di registro inventory.xml e policies.xml, andare in */var/log/Dell/Dell Data Protection*.

N.B.: Le modifiche di CsfConfig potrebbero non diventare subito effettive.

Raccogliere i file di registro

I registri per Endpoint Security Suite Enterprise si trovano nel seguente percorso: */var/log/Dell/ESSE*. Per generare i registri, utilizzare il seguente comando: **./getlogs.sh**

Per informazioni su come raccogliere i registri, vedere SLN303924.

Provisioning di un tenant

Deve essere eseguito il provisioning di un tenant nel Dell Server prima che diventi attiva l'applicazione dei criteri di Advanced Threat Prevention.

Prerequisiti

- Deve essere eseguito da un amministratore con il ruolo di amministratore di sistema.
- Deve essere dotato di connettività ad Internet per eseguire il provisioning sul Dell Server.
- Deve essere dotato di connettività a Internet nel client per visualizzare l'integrazione del servizio online di Advanced Threat Prevention nella Management Console.
- Il provisioning è basato su un token generato da un certificato durante il provisioning.
- Le licenze di Advanced Threat Prevention devono essere presenti nel Dell Server.

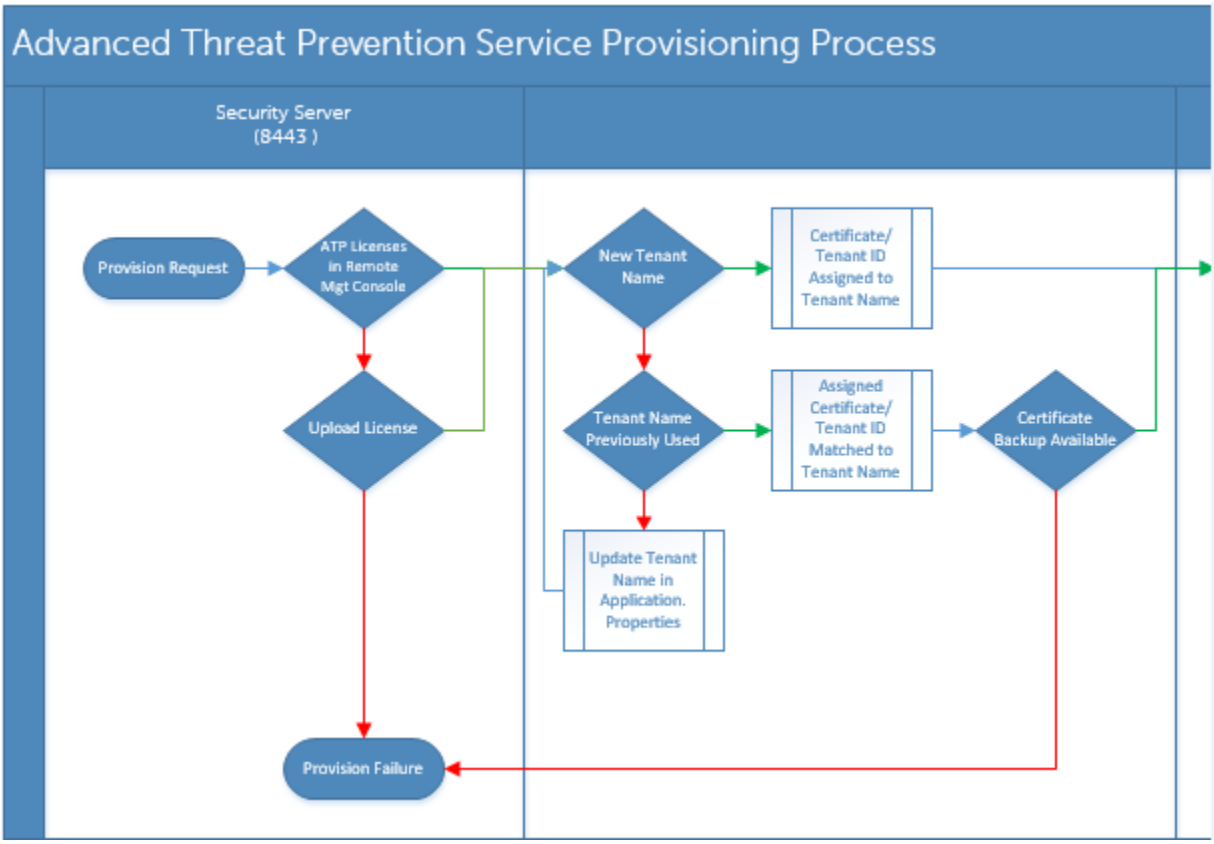
Eseguire il provisioning di un tenant

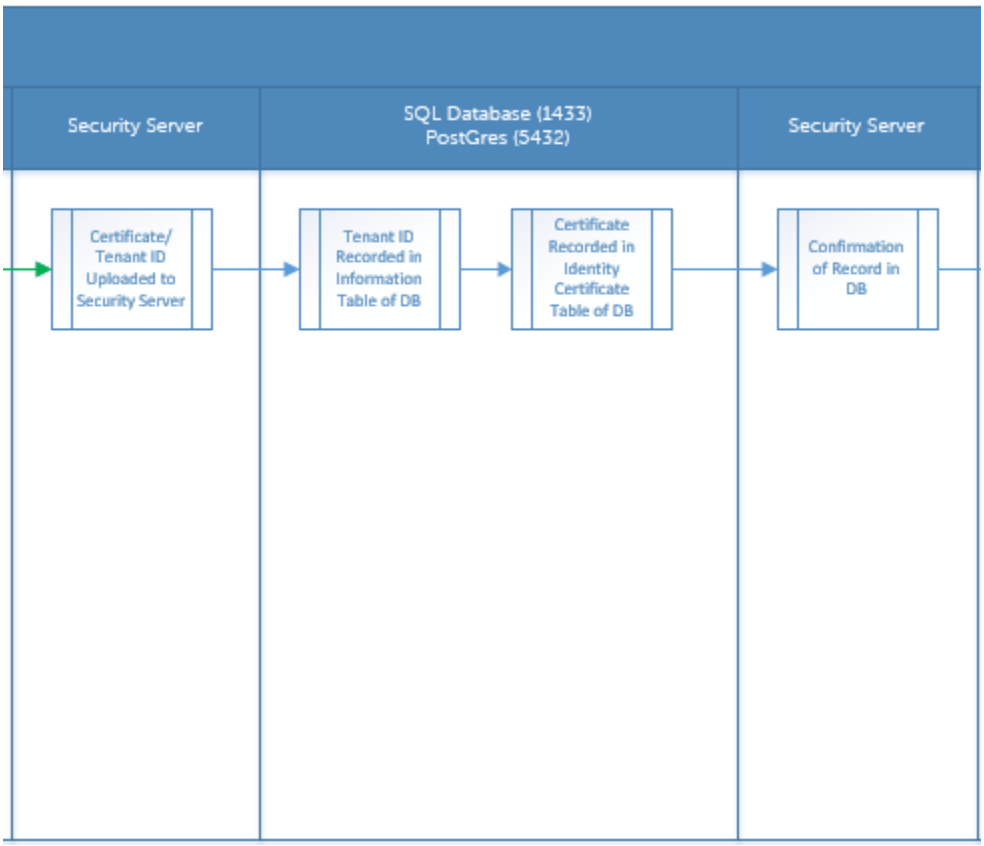
1. Eseguire l'accesso alla Remote Management Console come amministratore Dell.
2. Nel riquadro sinistro della Management Console, fare clic su **Gestione > Gestione dei servizi**.
3. Fare clic su **Imposta il servizio Advanced Threat Protection**. Se si verifica un guasto a questo punto, importare le licenze di Advanced Threat Prevention.
4. La procedura guidata di installazione si avvia quando le licenze vengono importate. Fare clic su **Avanti** per iniziare.
5. Leggere e accettare l'EULA e fare clic su **Avanti**.
6. Fornire le credenziali di identificazione al Dell Server per il provisioning del tenant. Fare clic su **Avanti**. *Il provisioning di un tenant esistente che è prodotto da Cylance non è supportato.*
7. Scaricare il certificato. Questa operazione è necessaria per il ripristino in caso di emergenza con il Dell Server. Il certificato non viene automaticamente sottoposto a backup. Eseguire il backup del certificato in una posizione sicura su un altro computer. Selezionare la casella di controllo per confermare che è stato eseguito il backup del certificato e fare clic su **Avanti**.
8. La configurazione è stata completata. Fare clic su **OK**.

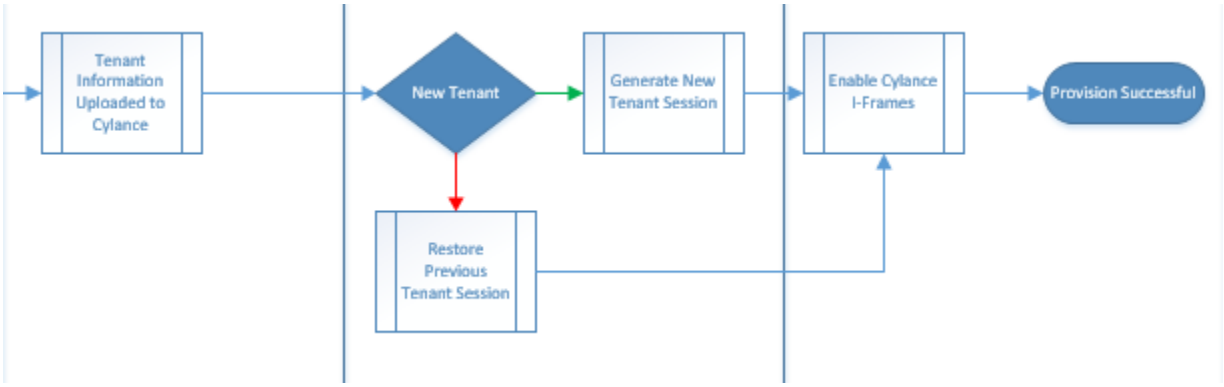
Risoluzione dei problemi del provisioning

Provisioning e comunicazione agente

I diagrammi seguenti illustrano il processo di provisioning del servizio di Advanced Threat Prevention.


Advanced Threat Prevention Service Provisioning Process
Security Server
(8443)
Provision Request
ATP Licenses in Remote Mgt Console
Upload License
New Tenant Name
Certificate/ Tenant ID Assigned to Tenant Name
Tenant Name Previously Used
Assigned Certificate/ Tenant ID Matched to Tenant Name
Certificate Backup Available
Update Tenant Name in Application. Properties
Provision Failure


Security Server
SQL Database (1433)
PostGres (5432)
Security Server
Certificate/ Tenant ID Uploaded to Security Server
Tenant ID Recorded in Information Table of DB
Certificate Recorded in Identity Certificate Table of DB
Confirmation of Record in DB



Il diagramma seguente illustra il processo di comunicazione dell'agente di Advanced Threat Prevention.