Endpoint Security Suite Enterprise for Linux

管理者ガイド v2.1

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。

警告: 物的損害、けが、または死亡の原因となる可能性があることを示しています。

2018 - 11

Rev. A01

目次

1

はじめに

『Endpoint Security Suite Enterprise for Linux Administrator Guide』(Endpoint Security Suite Enterprise for Linux の管理者ガイド)は、クライアントソフトウェアの導入とインストールに必要な情報が記載されています。

概要

Endpoint Security Suite Enterprise for Linux は、Dell Server からの集中管理によって、オペレーティングシステムおよびメモリのレイヤに Advanced Threat Prevention を適用します。集中管理、統合コンプライアンスレポート、コンソール脅威のアラートを使用すると、エンドポイントでのコンプライアンスの実施と証明が簡単にできます。セキュリティの専門知識は事前に定義されたポリシーおよびレポートテンプレートなどの機能に組み込まれており、ビジネスの IT 管理コストと複雑性の低減に役立ちます。

Security Management Server または Security Management Server Virtual - 一元化されたセキュリティポリシー管理を提供し、既存のエンタープライズディレクトリを統合し、レポートを作成します。ここでは、特定のバージョンに言及する必要 (Dell Security Management Server Virtual を使用する場合は手順が異なる場合など) がない限り、両方のサーバとも Dell Server と呼びます。

Advanced Threat Prevention for Linux には、3 つの RPM が入った tar.gz ファイルが 1 つあります。

Dell ProSupport へのお問い合わせ

デル製品向けの 24 時間 365 日対応電話サポート (877-459-7304、内線 4310039) にご連絡ください。

さらに、デル製品のオンラインサポートも dell.com/support からご利用いただけます。オンラインサポートでは、ドライバ、マニュアル、テクニカルアドバイザリー、よくあるご質問 (FAQ)、および緊急の問題を取り扱っています。

適切なサポート担当者に迅速におつなぎするためにも、お電話の際はお客様のサービスタグまたはエクスプレスサービスコードをご用意ください。

米国外の電話番号については、Dell ProSupport の各国の電話番号を記載したページを参照してください。

2

要件

本章では、クライアントのハードウェアとソフトウェアの要件を説明します。導入タスクを続行する前に、導入環境が要件を満たしていることを確認してください。

ハードウェア

次の表に、サポートされているコンピュータハードウェアの最小要件について詳しく示します。

ハードウェア

- 500 MB 以上の空きディスク容量
- 2 GB RAM
- 10/100/1000 または Wi-Fi ネットワークインタフェースカード

メモ: IPv6 は現在サポートされていません。

ソフトウェア

次の表では、サポートされているソフトウェアの詳細を説明します。

オペレーティングシステム（ 64 ビットカーネル ）

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

ポート

- ポート 443 (https) は通信用に使用されます。エージェントが管理コンソールと通信するためには、ファイアウォールで開く必要があります。ポート 443 が何らかの理由でブロックされている場合、アンチウイルス署名アップデート (DAT ファイル) をダウンロードできないので、コンピュータに最新の保護が装備されないことがあります。次に示すとおり、クライアントコンピュータが次にアクセスできることを確認してください。

使用	アプリケーションプロトコル	トランスポートプロトコル	ポート番号	宛先	方向
すべての通信	HTTPS	TCP	443	すべての https トラフィックを *.cylance.com に許可	アウトバウンド
Core Server 通信	HTTPS	TCP	8888	Core Server 通信を許可します。	インバウンド / アウトバウンド

- 詳細については、SLN303898 を参照してください。

Endpoint Security Suite Enterprise for Linux と依存関係

Endpoint Security Suite Enterprise for Linux は、Linux OS 上でのインストールとライセンス認証に、Mono と依存関係を使用します。インストーラは、必要な依存関係をダウンロードしてインストールします。パッケージの解凍後、次のコマンドを実行して、どの依存関係が使用されているかを確認できます。

```
./showdeps.sh
```

互換性

次の表に、Windows、Mac、Linux との互換性の詳細を示します。

n/a：このプラットフォームにはテクノロジが適用されません。

空白：Endpoint Security Suite Enterprise のポリシーはサポートされません。

機能	ポリシー	Windows	macOS	Linux
ファイルアクション				
	自動隔離（安全でない）	x	x	x
	自動隔離（異常）	x	x	x
	自動アップロード	x	x	x
	ポリシー安全リスト	x	x	x
メモリアクション				
	メモリ保護	x	x	x
攻略				
	スタックピボット	x	x	x
	スタック保護	x	x	x
	コード上書き	x	n/a	
	RAM スクレイピング	x	n/a	
	悪質なペイロード	x		
プロセスインジェクション				
	メモリのリモート割り当て	x	x	n/a
	メモリのリモートマッピング	x	x	n/a
	メモリへのリモート書き込み	x	x	n/a
	メモリへの PE のリモート書き込み	x	n/a	n/a
	リモートでのコード上書き	x	n/a	
	メモリのリモートアンマップ	x	n/a	
	リモートでのスレッド作成	x	x	

機能	ポリシー	Windows	macOS	Linux
	リモートでの APC スケジュール	x	n/a	n/a
	DYLD インジェクション		x	x
エスカレーション				
	LSASS 読み取り	x	n/a	n/a
	ゼロ割り当て	x	x	
保護設定				
	実行制御	x	x	x
	デバイスからのサービスシャットダウンを阻止する	x	x	
	安全でない実行中のプロセスとそのサブプロセスを強制終了する	x	x	x
	バックグラウンド脅威検知	x	x	x
	新しいファイルに注意する	x	x	x
	スキャンするアーカイブファイルの最大サイズ	x	x	x
	特定のフォルダを除外する	x	x	x
	ファイルサンプルのコピー	x		
アプリケーション制御				
	変更ウィンドウ	x		x
	フォルダの除外	x		
エージェントの設定				
	ログファイルの自動アップロードの有効化	x	x	x
	デスクトップ通知の有効化	x		
スクリプト制御				
	アクティブスクリプト	x		
	Powershell	x		
	Office マクロ	x		n/a
	Powershell コンソールの使用をブロック	x		
	当該フォルダ（およびサブフォルダ）内のスクリプトを承認	x		
	ロギングレベル	x		
	自己保護レベル	x		
	自動アップデート	x		
	検出の実行（エージェント UI から）	x		

機能	ポリシー	Windows	macOS	Linux
	隔離対象を削除 (エージェント UI およびコンソール UI)	x		
	接続切断モード	x		x
	詳細脅威データ	x		
	安全リストの検証	x	x	n/a
	マルウェアサンプルのコピー	x	x	x
	プロキシ設定	x	x	x
	手動ポリシーチェック(エージェント UI)	x	x	

3

タスク

インストール

このセクションでは、Endpoint Security Suite Enterprise for Linux のインストールについて詳しく説明します。

前提条件

デルでは、クライアントソフトウェアの導入時は IT のベストプラクティスに従うことをお勧めします。これには初期テストのための制御されたテスト環境、およびユーザーへのスタッガ化された導入が含まれますが、これらに限定されるものではありません。

このプロセスを開始する前に、次の前提条件が満たされていることを確認してください。

- Dell Server およびそのコンポーネントがすでにインストールされていることを確認します。

  Dell Server をまだインストールしていない場合は、以下の該当するガイドの指示に従います。

  Security Management Server Installation and Migration Guide（*Security Management Server* インストールおよびマイグレーションガイド）

  Security Management Server Virtual Quick Start Guide / *Installation Guide*（*Security Management Server Virtual* クイックスタートガイド / インストールガイド）
- Dell Server のホスト名とポートがあることを確認します。どちらもクライアントソフトウェアのインストールに必要です。
- ターゲットコンピュータが Dell Server にネットワークで接続できることを確認します。
- クライアントのサーバ証明書がない、または自己署名されている場合は、クライアント側のみで SSL 証明書の信頼を無効にする必要があります。

コマンドラインでのインストール

コマンドラインを使用して Endpoint Security Suite Enterprise クライアントをインストールするには、次の手順に従います。

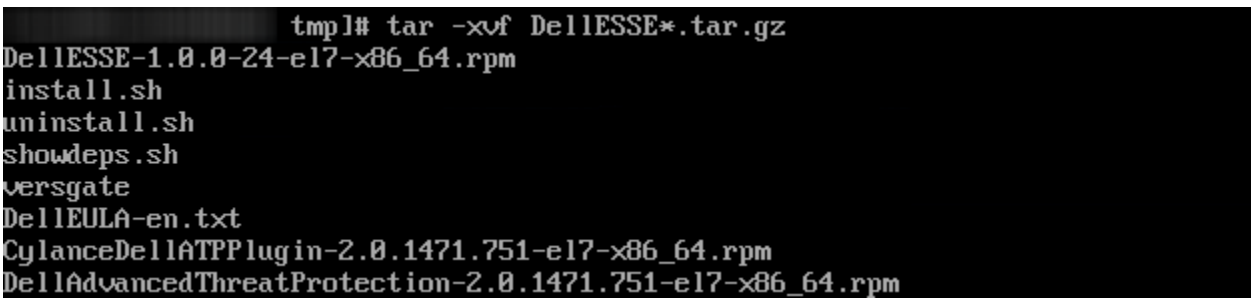
sudo コマンドは、インストール中に管理者権限を呼び出す際に使用する必要があります。プロンプトが表示されたら、資格情報を入力します。

指紋認証の承認は、最初のインストール時にのみ表示されます。

1 Dell FTP アカウントを使用して、インストールバンドル（DellESSE-1.x.x-xxx.tar.gz）を検索してダウンロードします。

2 次のコマンドを使用して、tar.gz を抽出します。

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



3 次のコマンドは、必要な RPM と依存関係のインストールスクリプトを実行します。

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

4 *Dell Security Management Server Host?* の行に、Dell Server の完全修飾ホスト名を入力して、ターゲットユーザーを管理します。例：server.organization.com

5 *Dell Security Management Server Port?* の行で、ポートが 8888 に設定されていることを確認します。

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

6 Dell ESSE パッケージおよびその依存関係のインストールのプロンプトが表示されたら、**y** を入力します。

```
 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 指紋認証の承認を求めるプロンプトが表示されたら、**y** を入力します。

```
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 *DellAdvancedThreatProtection* パッケージのインストールのプロンプトが表示されたら、**y** を入力します。

```
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 *CylanceDellATPPlugin* パッケージのインストールのプロンプトが表示されたら、**y** を入力します。

```
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 インストールが完了しました。

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

Complete!
```

11 「Verify Endpoint Security Suite Enterprise for Linux Installation」(Endpoint Security Suite Enterprise for Linux インストールの確認) を参照してください。

コマンドラインでのアンインストール

コマンドラインを使用して Endpoint Security Suite Enterprise for Linux をアンインストールするには、次の手順を実行します。

1 ターミナルウィンドウにアクセスします。

2 次のコマンドを使用して、パッケージをアンインストールします。

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

3 **Enter** を押します。

Endpoint Security Suite Enterprise for Linux がアンインストールされました。コンピュータを正常に使用できます。

詳細の表示

Endpoint Security Suite Enterprise Endpoint Security Suite Enterprise for Linux をインストールした後、Dell Server がエンドポイントとして認識されます。

atp -t

atp - t コマンドは、デバイスで検出されたすべての脅威および実行されたアクションを表示します。脅威とは、安全ではないファイルまたはプログラムとして新規に検出され、指示による修復が必要なイベントのカテゴリです。

```
Quarantined 17E76B830F9F30A39F078F5A69AD87B3838DB73A28EC893BD06EAF95D6E464E2 /tmp/threats/LINUXTarGz
Archive
Quarantined 20FBC1FDFCDC96A7E21FB1C700A6517A61711732A0D31FC25A60689710ECBE89 /tmp/threats/LINUXAutoB
lockNoService
Quarantined 2D49A3F81AF3362FE806E417DF2807C960314FF4F271B5B1360964163CB49886 /tmp/threats/LINUXGBL2
Quarantined 52D74BD1555D7C82746112C44F4D9A916B9DA286DD5B14D7665D4167BB1EB5D8 /tmp/threats/LINUXRunni
ngAutoQ
Quarantined 70F193F3C2023A7542338142CA89F1076A238AB7BAAD4202B2DCEDA7286E43D9 /tmp/threats/LINUXTest1
Quarantined 79D8C277F32CD176E4E2DD2198F730C9C79FA00A8F0158E0D519CEC1D868E222 /tmp/threats/LINUXRunni
ngApp
Quarantined B1BC7849F90FB403B9EDE88D40A92769D0AC28640B6A0D310FAF1D6B20E85F8A /tmp/threats/LINUXMaxAr
chive
Quarantined B31D57A77930E60FC151DEED085ED042423A172B4BED7782E33D4D09109BCCB6 /tmp/threats/LINUXGBL1
Quarantined F11C98AADB31D47AD571F6C0FA7F178A6413A8A7E84437098777711FB1CA6E31F /tmp/threats/LINUXAutoB
lockExecution
```

このエントリは、実行されたアクション、ハッシュ ID、脅威が検出された場所の詳細を説明します。

- **危険** マルウェアになる可能性のある不審なファイル
- **異常** - マルウェアになる場合のある不審なファイル
- **隔離済み** - 元の場所から移動したファイルで、隔離フォルダに保存され、デバイス上で実行できなくなります。
- **免除** - デバイスでの実行が許可されているファイル。
- **クリア** — 組織でクリアされているファイル。クリアされたファイルには、免除されたファイル、安全リストに追加されたファイル、デバイスの隔離フォルダから削除されたファイルが含まれます。

Advanced Threat Prevention の脅威分類の詳細については、Dell Server のリモート管理コンソールで *AdminHelp* を参照してください。

インストールの確認

オプションで、インストールが正常に完了したかどうかを確認することができます。

- クライアントで、ターミナルウィンドウにアクセスします。
- ポリシーシーケンスが受信される前に、クライアントは Dell サーバに登録します。
- */var/log/Dell/ESSE/DellAgent.00.log* ログ ファイルには、Dell サーバとプラグイン / サービスの連携に関する通信の詳細が記録されます。
  枠線で囲まれたテキストは、クライアントが Dell Server からポリシーを受信したという確認を示します。

```
2017.12.12 14:26:02.794 [02390] (00009) I Comm    : Received Id=ba150b8e-b1d3-44
5a-81e9-426e77fbb043
2017.12.12 14:26:02.795 [02390] (00009) I Comm    : ReceivedEdition enterprisesc
rver
2017.12.12 14:26:02.847 [02390] (00009) I Comm    : Successfully added memory ex
clusions to policy
2017.12.12 14:26:03.322 [02390] (00009) I Comm    : new policy seq# 9 received
2017.12.12 14:26:03.385 [02390] (00009) I Comm    : registered Centos7-3-64-MH w
ith server
2017.12.12 14:26:03.392 [02390] (00009) I Comm    : closing connection to https:
--More--(39%)
```

枠線で囲まれたテキストは、Advanced Threat Prevention プラグインをロードするために、Dell サービスが停止したという確認を示します。

```
//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 14:27:12.978 [02551] (00005) I Agent   : product name is "Dell Data P
```

枠線で囲まれたテキストは、3 つの Endpoint Security Suite Enterprise for Linux プラグインがロードされたという確認を示します。

```
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 80397403-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 - 次が含まれます。

- 登録ステータス
- シリアル番号 - この番号を使用してサポートに連絡します。この番号は、インストールの一意の識別子です。
- ポリシー

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

次のコマンドは、Endpoint Security Suite Enterprise for Linux のコマンドライン変数の詳細について説明します。

```
/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
```

Advanced Threat Prevention の *atp* コマンドは */usr/sbin* ディレクトリに追加されます。これは、通常のシェルの PATH 変数に含まれているため、ほとんどのケースで使用でき、明示的なパスが不要です。

トラブルシューティング

SSL 信頼証明書を無効にする

コンピュータのサーバ証明書がない、または自己署名されている場合は、クライアント側のみで SSL 証明書の信頼を無効にする必要があります。

一般的でない証明書を使用している場合は、ルート証明書を Linux 証明書ストアにインポートして、次のコマンドを実行して Endpoint Security Suite for Linux サービスを再起動します。`/usr/lib/dell/esse/agentservicecmd.sh restart`

1 ターミナルウィンドウにアクセスします。

2 CsfConfig アプリへのパスを入力します。

```
/usr/lib/dell/esse/CsfConfig
```

3 CsfConfig.app を実行します。

```
sudo ./CsfConfig
```

デフォルトの設定では、次が表示されます。

現在の設定：

ServerHost = deviceserver.company.com

ServerPort = 8888

DisableSSLCertTrust = False

DumpXmlInventory = False

DumpPolicies = False

4 **-help** を入力してオプションを一覧表示します。

5 ターゲットコンピュータで SSL 証明書の信頼を無効にするには、次のコマンドを実行します。

```
sudo /usr/lib/dell/esse/CsfConfig -disablecerttrust true
```

XML インベントリおよびポリシーの変更をログフォルダに追加します。

inventory.xml ファイルまたは policies.xml ファイルをログフォルダに追加します。

1 上記のとおり、*CsfConfig app* を実行します。

2 *DumpXmlInventory* を *True* に変更するには、次のコマンドを実行します。

```
sudo /usr/lib/dell/esse/CsfConfig -dumpinventory true
```

3 *DumpPolicies* を *True* に変更するには、次のコマンドを実行します。

```
sudo /usr/lib/dell/esse/CsfConfig -dumppolicies true
```

ポリシーファイルは、ポリシーの変更が発生した場合にのみダンプされます。

4 inventory.xml および policies.xml ログファイルを表示するには、*/var/log/Dell/Dell Data Protection* を参照してください。

メモ: CsfConfig の変更はすぐに適用されない場合があります。

ログファイルの収集

Endpoint Security Suite Enterprise for Linux のログは、*/var/log/Dell/ESSE* に保存されます。ログを生成するには、**./getlogs.sh** コマンドを使用します。

ログを収集する方法については、SLN303924 を参照してください。

テナントのプロビジョニング

Advanced Threat Prevention のポリシーの施行がアクティブになる前に、テナントが Dell Server にプロビジョニングされる必要があります。

前提条件

- システム管理者の役割を持つ管理者が実行する必要があります。
- Dell Server でプロビジョニングをするにはインターネット接続が必要です。
- 管理コンソールで Advanced Threat Prevention オンラインサービスの統合を表示するために、クライアント上でインターネット接続が必要です。
- プロビジョニングは、プロビジョニング中に証明書から生成されるトークンに基づいています。
- Advanced Threat Prevention のライセンスが Dell Server 内に存在している必要があります。

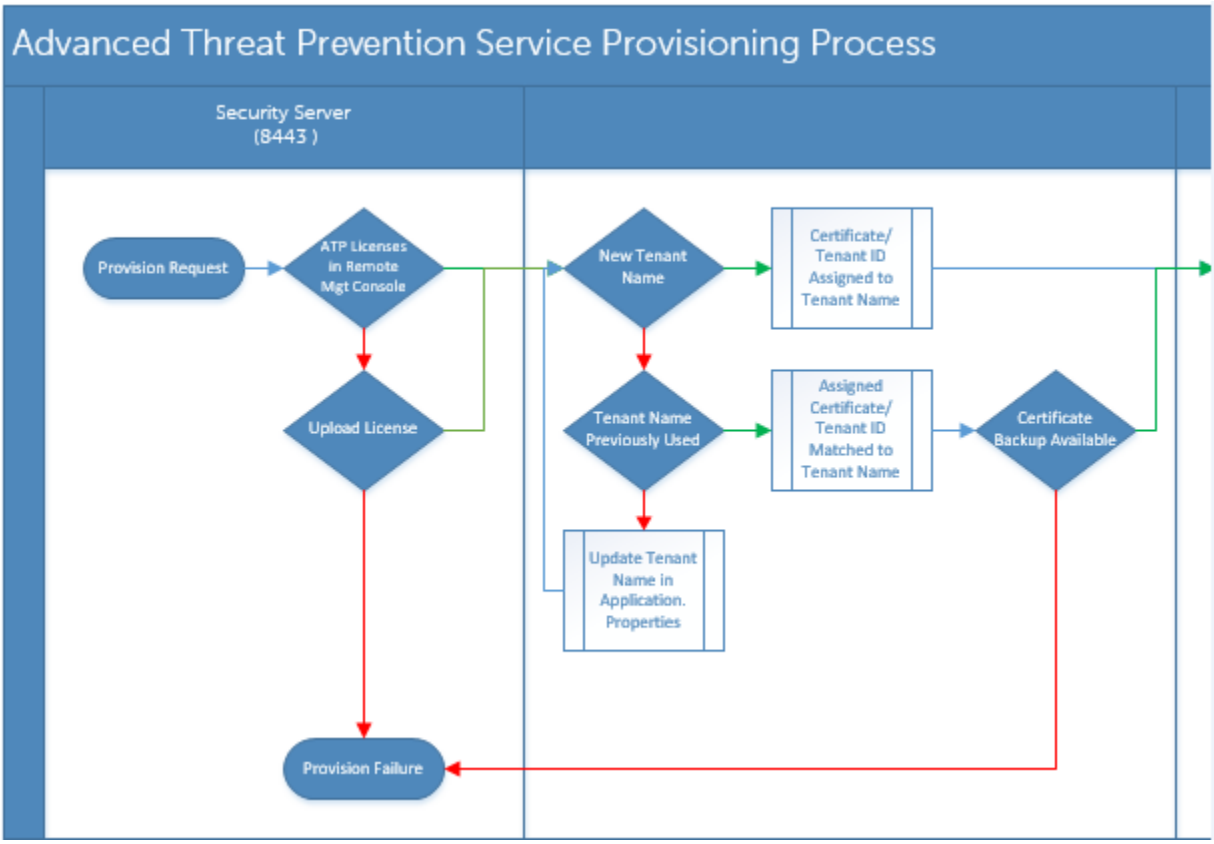
テナントのプロビジョニング

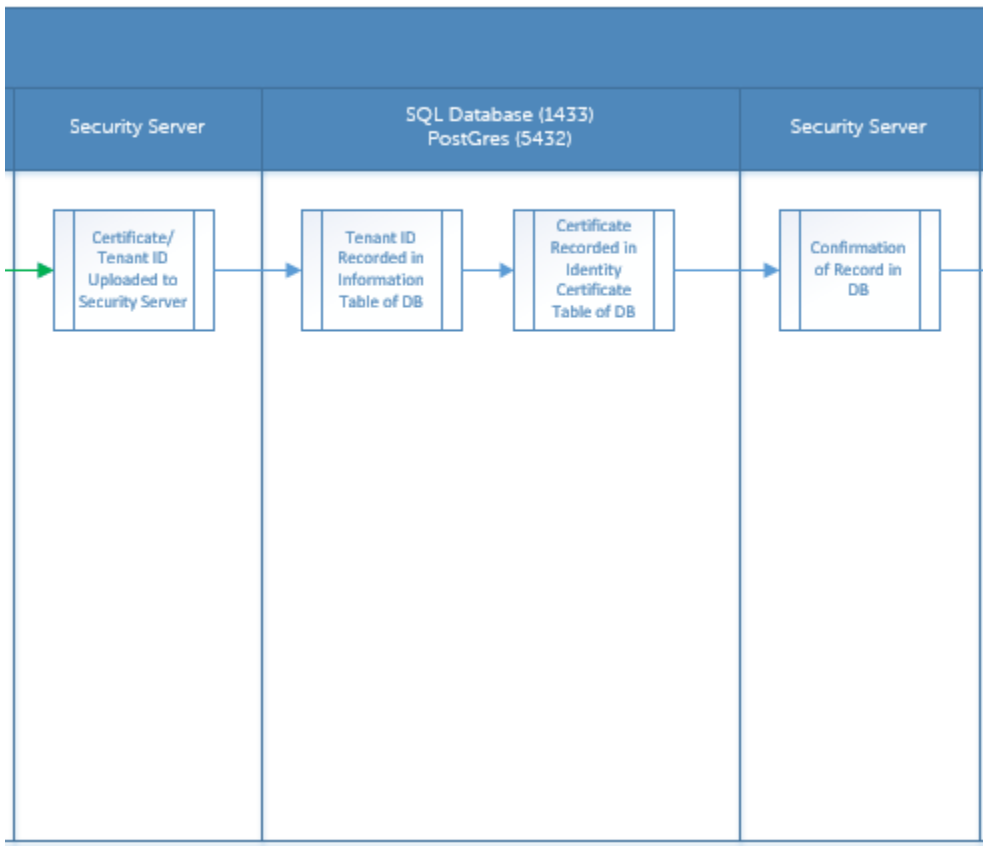
1 リモート管理コンソールに Dell 管理者としてログインします。
2 管理コンソールの左ペインで、**管理** > **サービス管理** を順にクリックします。
3 **Advanced Threat Protection サービスのセットアップ** をクリックします。この時点で不具合が発生する場合は、Advanced Threat Prevention ライセンスをインポートします。
4 ラインセンスがインポートされると、ガイド付きのセットアップが始まります。**次へ** をクリックして開始します。
5 EULA を読み、合意した後、**次へ** をクリックします。
6 テナントのプロビジョニングのために Dell Server に ID 資格情報を入力します。**次へ** をクリックします。*Cylance* ブランドの既存テナントのプロビジョニングはサポートされていません。
7 証明書をダウンロードします。これは Dell Server での災害シナリオが発生した場合のリカバリに必要です。この証明書は自動的にバックアップされません。別のコンピュータの安全な場所に証明書をバックアップします。証明書をバックアップしたことを確認するチェックボックスを選択してから **次へ** をクリックします。
8 セットアップが完了しました。**OK** をクリックします。

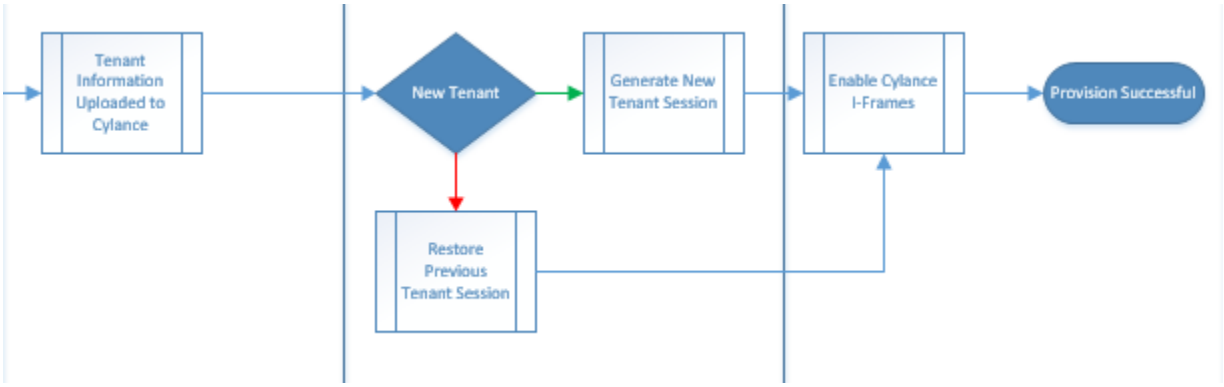
プロビジョニングのトラブルシューティング

プロビジョニングとエージェント通信

次の図は Advanced Threat Prevention サービスのプロビジョニングプロセスを表しています。


Advanced Threat Prevention Service Provisioning Process
Security Server
(8443)
Provision Request
ATP Licenses in Remote Mgt Console
Upload License
Provision Failure
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


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



次の図は Advanced Threat Prevention のエージェント通信プロセスを表しています。